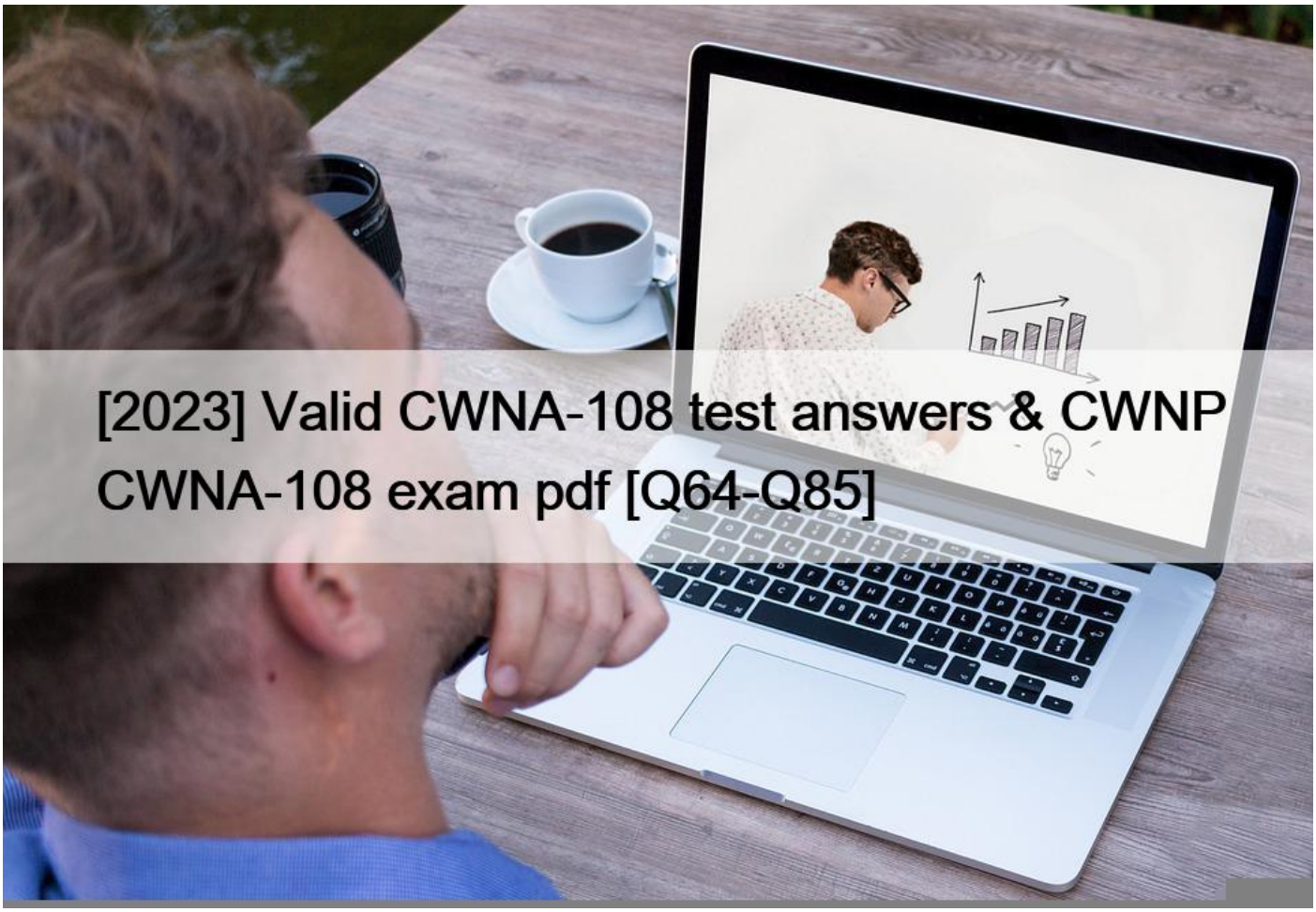
[2023 Valid CWNA-108 test answers & CWNP CWNA-108 exam pdf [Q64-Q85



[2023] Valid CWNA-108 test answers & CWNP CWNA-108 exam pdf
Verified CWNA-108 dumps Q&As - Pass Guarantee or Full Refund

Q64. An 802.11-based network uses an AP and has several connecting clients. The clients include iPhones, iPads, laptops and one desktop. What WLAN use case is represented?
* Ad-hoc
* WPAN
* BSS
* IBSS
Explanation

A BSS (Basic Service Set) is a WLAN use case that represents an 802.11-based network that uses an AP (Access Point) and has several connecting clients. The AP acts as a central point of coordination and communication for the clients, which can include iPhones, iPads, laptops, desktops, or any other devices that have Wi-Fi capabilities. A BSS can be identified by a unique BSSID (Basic Service Set Identifier), which is usually the MAC address of the AP’s radio interface. A BSS can also be associated with an SSID (Service Set Identifier), which is a human-readable name that identifies the network. References: , Chapter 1, page 23; , Section 1.1

Q65. ABC Company has just purchased a 6 dBi patch antenna. After performing some tests with the 6 dBi antenna, they have concluded that more antenna gain is needed to cover their outdoor courtyard. When choosing an antenna with higher gain, what other antenna characteristic will also always change?
* Fresnel Zone size
* Maximum input power
* Beamwidth
* Impedance
* VSWR Ratio

Q66. You are deploying a WLAN with the access points configured for 10 mW of output power on the 2.4 GHz radios and 20 mW of output power on the 5GHz radios. Some semi-directional antennas are also in use. What kind of deployment is described?
* SOHO
* Residential
* High density
* Standard office

Explanation/Reference:

Q67. What statement is true concerning the use of Orthogonal Frequency Division Multiplexing (OFDM) modulation method in IEEE 802.11 WLANs?
* OFDM was used by Frequency Hopping Spread Spectrum (FHSS) PHY devices.
* OFDM was first introduced in 802. 11a and is used by the ERP, HT and VHT PHYs as well
* OFDM implements BPSK modulation to allow for data rates up to 7 Gbps.
* OFDM modulation is used only in 5 GHz 802. 11 transmissions.

Q68. What phrase defines Equivalent Isotropically Radiated Power (EIRP)?
* Power supplied from the transmission line to the antenna input
* The power output from the radio after cable losses
* The power output from the radio into the RF cable
* The highest RF signal strength that is transmitted from a given antenna

Q69. An 802.11 WLAN transmitter that emits a 50 mW signal is connected to a cable with 3 dB of loss. The cable is connected to an antenna with 16 dBi of gain. What is the power level at the Intentional Radiator?
* 25 mW
* 250 mW
* 500 mW
* 1000 mW

Explanation

The power level at the Intentional Radiator (IR) is 250 mW. The IR is the point where the RF signal leaves the transmitter and enters the antenna system. To calculate the power level at the IR, we need to consider the output power level of the transmitter, the loss of the cable, and the gain of the antenna. The formula is:

Power level at IR (dBm) = Output power level (dBm) – Cable loss (dB) + Antenna gain (dBi) We can convert the output power level of 50 mW to dBm by using the formula:

Power level (dBm) = 10 * log10(Power level (mW))

Therefore, 50 mW = 10 * log10(50) = 16.99 dBm

We can plug in the values into the formula:

Power level at IR (dBm) = 16.99 – 3 + 16 = 29.99 dBm

We can convert the power level at IR from dBm to mW by using the inverse formula:

Power level (mW) = 10(Power level (dBm) / 10)

Therefore, 29.99 dBm = 10(29.99 / 10) = 999.96 mW

However, since we need to round off the answer to the nearest integer value, we get:

Power level at IR (mW) = 1000 mW

References: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-107], page 67; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106], page

57.

Q70. ABC Company is planning to install a new 802.11ac WLAN, but wants to upgrade its wired infrastructure first to provide the best user experience possible. ABC Company has hired you to perform the RF site survey.

During the interview with the network manager, you are told that the new Ethernet edge switches will support VoIP phones and 802.11 access points, both using 802.3 PoE.

After hearing this information, what immediate concerns do you note?
* The power budget in the edge switches must be carefully planned and monitored based on the number of supported PoE devices.
* The edge Ethernet switches should support Ether-channel to get the best results out of the network.
* VoIP phones and 802.11 access points should not be powered by the same edge switch due to distortion.
* If the switches are in optimal locations for VoIP phones, they are likely to be suboptimal locations for

802.11 APs
Explanation

An immediate concern that you note after hearing this information is that the power budget in the edge switches must be carefully planned and monitored based on the number of supported PoE devices. PoE stands for Power over Ethernet and is a technology that allows Ethernet switches to deliver power along with data to devices such as VoIP phones and 802.11 access points. PoE devices are classified into different classes based on their power consumption and output. The edge switches have a limited power budget that determines how many PoE devices they can support simultaneously. If the power budget is exceeded, some PoE devices may not receive enough power or may shut down unexpectedly. Therefore, it is important to plan and monitor the power budget in the edge switches based on the number and class of PoE devices connected to them. Using Ether-channel, placing switches in optimal locations, or avoiding distortion are not immediate concerns related to PoE devices. References: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-107], page 234; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106], page 224.

Q71. You are deploying a WLAN with the access points configured for 10 mW of output power on the 2.4 GHz radios and 20 mW of output power on the 5GHz radios. Some semi-directional antennas are also in use. What kind of deployment is described?
* SOHO
* Residential
* High density

* Standard office
Explanation

A high-density deployment is a wireless network that is designed to support a large number of users and devices in a relatively small area. This type of deployment is often used in enterprise environments, such as offices, schools, and hospitals.

The use of semi-directional antennas in the deployment described in the question is a good indication that it is a high-density deployment. Semi-directional antennas can be used to focus the signal from an access point in a specific direction. This can help to reduce interference and improve performance in high-density environments.

The other answer choices are less likely to be correct for the following reasons:

* SOHO (small office/home office) deployments are typically smaller and less complex than high-density deployments.

* Residential deployments are typically even smaller and less complex than SOHO deployments.

* Standard office deployments may be high-density, but they may also be lower-density.

It is important to note that the type of deployment is not determined solely by the output power of the access points. However, the use of 10 mW of output power on the 2.4 GHz radios and 20 mW of output power on the

5GHz radios is also consistent with a high-density deployment.

Here are some additional tips for deploying a high-density wireless network:

* Use a site survey to determine the optimal placement of access points.

* Configure the access points to use non-overlapping channels.

* Use semi-directional or directional antennas to focus the signal and reduce interference.

* Implement a wireless intrusion prevention system (WIPS) to detect and mitigate rogue access points and other security threats.

Q72. You are implementing a VHT-capable AP. Which one of the following channels is available in the

802.11-2016 standard that was not available before the ratification of 802.11 ac?
* 56
* 161
* 153
* 144
Explanation

Channel 144 is a new channel that was added to the 5 GHz band by the 802.11ac amendment, which defines the VHT (Very High Throughput) PHY for WLANs. Channel 144 has a center frequency of 5720 MHz and a bandwidth of 20 MHz. It can also be combined with adjacent channels to form wider channels of 40 MHz, 80 MHz, or 160 MHz. Channel 144 is available in some regions, such as North America and Europe, but not in others, such as Japan and China . References: [CWNA-109 Study Guide], Chapter 3: Antennas and Accessories, page 121; [CWNA-108 Study Guide], Chapter 3: Antennas and Accessories, page 115;

[Wikipedia], List of WLAN channels.

Q73. When using a spectrum to look for non Wi-Fi interference sources, you notice significant interference across the entire 2.4 GHz band (not on a few select frequencies) within the desktop area of a users workspace, but the interference disappears quickly after just 2 meters. What is the most likely cause of this interference?
* USB 3 devices in the user’s work area
* Bluetooth devices in the user’s work area
* Excess RF energy from a nearby AP
* Unintentional radiation from the PC power supply

Explanation

USB 3 devices in the user’s work area are the most likely cause of this interference when using a spectrum analyzer to look for non-Wi-Fi interference sources. A spectrum analyzer is a tool that measures and visualizes the radio frequency activity and interference in the wireless environment. A spectrum analyzer can show the spectrum usage and energy levels on each frequency band or channel and help identify and locate the sources of interference. Interference is any unwanted signal that disrupts or degrades the intended signal on a wireless channel. Interference can be caused by various sources, such as other Wi-Fi devices, non-Wi-Fi devices, or natural phenomena. Interference can affect WLAN performance and quality by causing signal loss, noise, distortion, or errors. USB 3 devices are non-Wi-Fi devices that use USB 3.0 technology to transfer data at high speeds between computers and peripherals, such as hard drives, flash drives, cameras, or printers. USB 3 devices can generate electromagnetic radiation that interferes with Wi-Fi signals in the 2.4 GHz band, especially when they are close to Wi-Fi devices or antennas. USB 3 devices can cause significant interference across the entire 2.4 GHz band (not on a few select frequencies) within the desktop area of a user’s workspace, but the interference disappears quickly after just 2 meters. This is because USB 3 devices emit broadband interference that affects all channels in the 2.4 GHz band with a high intensity near the source but a low intensity at a distance due to attenuation. The other options are not likely to cause this interference pattern when using a spectrum analyzer to look for non-Wi-Fi interference sources. Bluetooth devices in the user’s work area are non-Wi-Fi devices that use Bluetooth technology to communicate wirelessly between computers and peripherals, such as keyboards, mice, headphones, or speakers. Bluetooth devices can cause interference with Wi-Fi signals in the 2.4 GHz band, but they use frequency hopping spread spectrum (FHSS) technique that changes frequencies rapidly and randomly within a range of 79 channels. Therefore, Bluetooth devices do not cause significant interference across the entire 2.4 GHz band (not on a few select frequencies), but rather intermittent interference on some channels at different times. Excess RF energy from a nearby AP is not a non-Wi-Fi interference source but rather a Wi-Fi interference source that occurs when an AP transmits more power than necessary for its coverage area. Excess RF energy from a nearby AP can cause co-channel interference (CCI) with other APs or client devices that use the same channel within range of each other. CCI reduces performance and capacity because it causes contention and collisions on the wireless medium,

Q74. The IEEE 802.11-2012 standard requires VHT capable devices to be backward compatible with devices using which other 802.11 physical layer specification (PHY)?
* OFDM
* HR/DSSS
* ERP-PBCC
* DSSS

Q75. Which one of the following channels can be used for VHT transmissions?
* 44
* 1
* 7
* 13

Q76. What statement about 802.11 WLAN bridges is true?
* WLAN bridges only work in the 2.4 GHz frequency band and they support only SISO communications
* WLAN bridges must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally
* WLAN bridges may support MIMO communications, but only if used in the 5 GHz frequency band
* WLAN bridges must be implemented such that no interference occurs on the channel anywhere between the two endpoints used

to establish the bridge
Explanation

WLAN bridges must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally. A WLAN bridge is a device that connects two or more networks using the 802.11 protocol. A WLAN bridge must have a clear and strong signal between the two endpoints to ensure reliable and fast data transmission. The signal-to-noise ratio (SNR) is a measure of the quality of the signal, which depends on the distance, interference, obstacles, and antenna gain between the transceivers. A higher SNR means a better signal quality and a higher data rate. A lower SNR means a worse signal quality and a lower data rate. Therefore, a WLAN bridge must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally1.

Q77. You are implementing a multi-AP WLAN and fast secure roaming is essential.

Which one of the following methods is an IEEE 802.11 standard method for fast roaming?
* Band Steering
* FT
* OKC
* Load balancing
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-DesignGuide/Enterprise_Mobility_8-1_Deployment_Guide/Chapter-11.pdf

Q78. Lynne runs a small hotel, and as a value added service for his customers he has implemented a Wi-Fi hot-spot. Lynne has read news articles about how hackers wait at hot-spots trying to take advantage of unsuspecting users. He wants to avoid this problem at his hotel.

What is an efficient and practical step that Lynne can take to decrease the likelihood of active attacks on his customers’ wireless computers?
* Enable station-to-station traffic blocking by the access points in the hotel.
* Implement Network Access Control (NAC) and require antivirus and firewall software along with OS patches.
* Implement an SSL VPN in the WLAN controller that initiates after HTTPS login.
* Require EAP-FAST authentication and provide customers with a username/password on their receipt.

Q79. The requirements for a WLAN you are installing state that it must support unidirectional delays of less than 150 ms and the signal strength at all receivers can be no lower than -67 dBm. What application is likely used that demands these requirements?
* VoIP
* E-Mail
* FTP
* RTLS

Q80. You are configuring an access point to use channel 128. What important fact should be considered about this channel?
* It is a 2.4 GHz frequency band 40 MHz channel, so it should not be used
* It is a 22 MHz channel so it will overlap with the channels above and below it
* It is a channel that may require DFS when used
* It is a channel that is unsupported by all access points in all regulatory domains
Explanation

It is a channel that may require DFS when used is an important fact that should be considered about channel

128. Channel 128 is a 5 GHz frequency band 20 MHz channel that has a center frequency of 5.64 GHz.

Channel 128 is one of the channels that are subject to DFS (Dynamic Frequency Selection) rules, which require Wi-Fi devices to monitor and avoid using channels that are occupied by radar systems or other primary users. DFS is a feature that is defined in the IEEE 802.11h amendment and is mandated by some regulatory bodies, such as the FCC and the ETSI, to protect the licensed users of the 5 GHz band from interference by unlicensed Wi-Fi devices. DFS works by using a mechanism called channel availability check (CAC), which requires Wi-Fi devices to scan a channel for a certain period of time before using it. If a radar signal is detected during the CAC or while using the channel, the Wi-Fi devices must switch to another channel that is free from radar interference.

When configuring an access point to use channel 128, it is important to consider the implications of DFS rules, such as:

* The access point must support DFS and comply with the local regulations and standards that apply to DFS channels.

* The access point may experience delays or interruptions in its operation due to CAC or channel switching.

* The access point may have limited channel selection or availability due to radar interference or other Wi-Fi devices using DFS channels.

* The access point may have compatibility or interoperability issues with some client devices that do not support DFS or use different DFS parameters.

* The access point may have performance or quality issues due to co-channel or adjacent-channel interference from other Wi-Fi devices using non-DFS channels.

Therefore, it is advisable to use channel 128 only when necessary and after performing a thorough site survey and spectrum analysis to determine the best channel for the access point. References: 1, Chapter 3, page

117; 2, Section 3.2

Q81. A WLAN is implemented using wireless controllers. The APs must locate the controllers when powered on and connected to the network. Which one of the following methods is commonly used to locate the controllers by the APs?
* NTP
* DHCP
* SNMP
* GRE

Q82. Which one of the following 802.11 PHYs is more likely to be used in an industrial deployment but not likely to be used in standard office deployments?
* S1G
* VHT
* OFDM
* HT
Explanation

S1G is one of the 802.11 PHYs that is more likely to be used in an industrial deployment but not likely to be used in standard office deployments. This is because S1G stands for Sub-1 GHz, which means it operates in the frequency bands below 1 GHz, such as 900 MHz and 868 MHz. These bands offer better penetration and range than the higher frequency bands used by other 802.11 PHYs, such as 2.4 GHz and 5 GHz. This makes S1G suitable for industrial applications that require robust and reliable wireless communication in harsh environments, such as factories, warehouses, mines, and smart grids. S1G also supports low-power and low-data-rate devices, such as sensors, actuators, and meters, which are common in industrial Internet of Things (IoT) scenarios. VHT, OFDM, and HT are other 802.11 PHYs that are more commonly used in standard office deployments, as they offer higher data rates and capacity than S1G, but have lower range and penetration. References: CWNA-109 Study Guide, Chapter 3: Radio

Frequency Technologies, page 751

Q83. Which directional antenna types are commonly used by indoor Wi-Fi devices in a MIMO multiple spatial stream implementation?
* Dipole and yagi
* Grid and sector
* Patch and panel
* Dish and grid

Explanation

Patch and panel antennas are directional antenna types that are commonly used by indoor Wi-Fi devices in a MIMO multiple spatial stream implementation. These antennas have a flat rectangular shape and can be mounted on walls or ceilings to provide coverage in a specific direction. They have a moderate gain and a relatively wide beamwidth, making them suitable for multipath environments where signals can reflect off different surfaces and create multiple spatial streams. Patch and panel antennas can also support polarization diversity, which means they can transmit and receive both horizontally and vertically polarized waves, increasing the MIMO performance. References: 1, Chapter 2, page 72; 2, Section 2.4

Q84. When a STA has authenticated to an AP (AP-1), but still maintains a connection with another AP (AP-2), what is the state of the STA on AP-1?
* Transitional
* Unauthenticated and Unassociated
* Authenticated and Unassociated
* Authenticated and Associated

Explanation

Authenticated and Unassociated. According to one of the web search results1, a STA can be authenticated to multiple APs, but it can only be associated to one AP at a time. Association is the process of establishing a logical link between the STA and the AP, which allows the STA to send and receive data frames through the AP2. Therefore, when a STA has authenticated to an AP-1, but still maintains a connection with another AP-2, it means that the STA is authenticated to both APs, but only associated to AP-2. The state of the STA on AP-1 is authenticated and unassociated, which means that the STA can switch to AP-1 without repeating the authentication process, but it cannot send or receive data frames through AP-1 until it becomes associated.

Q85. Which one of the following 802.11 PHYs is more likely to be used in an industrial deployment but not likely to be used in standard office deployments?
* SIG
* VHT
* OFDM
* HT

The Certified Wireless Network Administrator (CWNA) gets guidelines and activities of 802.11 remote organizations. Obligations incorporate sending, overseeing, observing, and fundamental investigating of these organizations. The CWNA can depict gadgets and activities of current WLAN innovations. These are ensured in our **CWNP CWNA-108 practice exams** and **CWNP CWNA-108 practice exams**.

The CWNA test has no essentials; be that as it may, coming up next are suggested previously endeavoring the CWNA test:

- At least 1 year of work insight with remote LAN innovations- Basic information on systems administration (switches, switches, cabling, and so on)- Basic information on TCP/IP

The abilities and information estimated by this assessment are gotten from a Job Task Analysis (JTA) including remote systems administration specialists (CWNEs) and experts. The aftereffects of this JTA were utilized in gauging the branches of knowledge and guaranteeing that the weighting is illustrative of the relative significance of the substance.

The CWNA certification is a foundational level wireless LAN certification for the CWNP Program. To earn a CWNA certification, you must take the CWNA exam at a Pearson Vue Testing Center and pass with a 70% or higher. Instructors must pass with a 80% or higher. However you choose to prepare for the CWNA exam, you should start with the exam objectives, which cover the full list of skills tested on the exam. The CWNA certification is valid for three (3) years. To recertify, pass one of the professional level certifications exams (CWSP,CWDP, CWAP) BEFORE your CWNA expires. By doing so, the CWNA will be renewed for another three (3) years. Or retake the current version of the CWNA exam.

At the point when you finish the CWNA test, you acquire credit towards the CWSP, CWDP, CWAP, and CWNE accreditations and you procure the CWNA certificate.

CWNP CWNA-108 certification exam is an excellent way for individuals to validate their skills and knowledge in wireless networking. It covers a wide range of topics, and passing the exam can open up new career opportunities in the wireless networking industry. CWNP Certified Wireless Network Administrator Exam certification is globally recognized and highly respected, making it a valuable asset for professionals in this field.

To earn the CWNA-108 certification, candidates need to pass a 90-minute exam that consists of 60 multiple-choice questions. CWNA-108 exam is administered at Pearson VUE testing centers worldwide. Candidates are tested on their knowledge of wireless networking technologies, protocols, and standards. They are also tested on their ability to design and implement wireless LAN infrastructure, troubleshoot common wireless network problems, and perform network analysis. The CWNA-108 certification is valid for three years after which candidates need to recertify to maintain their certification status.

CWNA-108 Exam Questions – Valid CWNA-108 Dumps Pdf:
https://www.examslabs.com/CWNP/CWNA-Certification/best-CWNA-108-exam-dumps.html]