DUMPSBOSS.

Certified Wireless Specialist

CWNP CWS-100

Version Demo

Total Demo Questions: 8

Total Premium Questions: 82

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, WLAN Basics	34
Topic 2, WLAN Hardware and Software	18
Topic 3, WLAN Security	12
Topic 4, WLAN Design, Installation and Troubleshooting	18
Total	82

QUESTION NO: 1

What is the primary security improvement introduced by WPA3-Personal over WPA2-Personal?

A. Simultaneous Authentication of Equals (SAE)

B. Temporal Key Integrity Protocol (TKIP)

C. Wired Equivalent Privacy (WEP)

D. Open System Authentication

ANSWER: A

Explanation:

Simultaneous Authentication of Equals (SAE) is the primary authentication improvement in WPA3-Personal. WPA2-Personal uses a pre-shared key authentication method, while WPA3-Personal uses SAE, a password-authenticated key exchange based on the Dragonfly handshake. SAE provides stronger resistance to offline password-guessing attacks using captured wireless authentication traffic and provides forward secrecy properties. WPA3-Personal continues to provide password-based WLAN access, but it improves the security of the authentication process compared with WPA2-Personal. See the Wi-Fi Alliance Wi-Fi security overview.

QUESTION NO: 2

What is the maximum data rate specified in the 802.11 standard for the HT (802.11n) PHY (Physical Layer)?

A. 65 Mbps

B. 600 Mbps

C. 150 Mbps

D. 400 Mbps

ANSWER: B

Explanation:

The correct answer is **600 Mbps**. IEEE 802.11n, also identified as the High Throughput (HT) PHY amendment, specifies a maximum theoretical PHY data rate of 600 Mbps. This maximum is reached when the radio uses four spatial streams, 40 MHz channel bonding, the short guard interval, and the highest HT modulation and coding scheme. The rate is a PHY signaling rate, not the payload throughput that an application will necessarily receive. Actual usable throughput is lower because wireless transmissions include MAC headers, management and control traffic, contention-based medium access, acknowledgments, retransmissions, interference effects, and environmental limitations. HT introduced important capacity improvements including MIMO spatial multiplexing, 20 MHz and optional 40 MHz channels, frame aggregation, and short guard interval support. For CWNP purposes, 600 Mbps is the headline maximum data rate associated with 802.11n HT operation. IEEE's published description of the 802.11n amendment identifies its high-throughput wireless LAN enhancements at IEEE 802.11n. Additional technical context on 802.11n data rates and MIMO operation is available from CWNP.

QUESTION NO: 3

In what frequency band does an 802.11g (ERP) device operate?

A. 60 GHz

B. 2.4 GHz

C. 5 GHz

D. Sub-1 GHz

ANSWER: B

Explanation:

2.4 GHz is correct because IEEE 802.11g, whose PHY is called Extended Rate PHY (ERP), operates in the 2.4 GHz ISM frequency band. It was designed to extend 802.11b capabilities by using OFDM modulation to support data rates up to 54 Mb/s while retaining interoperability mechanisms for legacy 802.11b devices. In practical Wi-Fi channel planning, 802.11g uses the same 2.4 GHz channel range as 802.11b, with channels commonly spaced 5 MHz apart and 20 MHz-wide transmissions. The 2.4 GHz band remains widely used, although its limited nonoverlapping channel capacity and susceptibility to interference are important deployment considerations. The IEEE 802.11 working group identifies 802.11g as an amendment for higher-rate operation in the 2.4 GHz band, and the Wi-Fi Alliance's educational material likewise places 802.11b/g/n operation in this spectrum. See the IEEE 802.11g standard page and the Wi-Fi Alliance overview of Wi-Fi frequency bands.

QUESTION NO: 4

Which one of the following is considered a data-intensive application?

A. Web Browsing

B. Cloud Storage

C. E-Mail

D. Voice over IP (VoIP)

ANSWER: B

Explanation:

Cloud Storage is a data-intensive application because its normal operation involves transferring, synchronizing, uploading, downloading, and sometimes replicating potentially large files or data sets. Unlike applications whose traffic is primarily characterized by strict timing requirements, cloud-storage traffic is commonly measured by the volume of data transferred and can consume substantial WLAN capacity for extended periods. For example, a user synchronizing a photo library, backing up a device, or retrieving shared project files may generate sustained downstream or upstream traffic. In wireless planning and troubleshooting, these applications matter because their throughput demand can affect airtime availability and the experience of other clients sharing the same access point and RF channel. CWNP identifies cloud storage among applications that can place significant capacity demands on a wireless network, making it an appropriate example of a data-intensive workload. See CWNP's overview of wireless networking concepts at CWNP and the discussion of cloud-storage synchronization behavior in Google Drive for desktop documentation.

QUESTION NO: 5

What kind of antenna is most frequently used with indoor APs?

A. Grid

B. Parabolic dish

C. Internal

D. Yagi

ANSWER: C

Explanation:

Internal is correct because most enterprise indoor access points are designed with antennas integrated into the AP enclosure. This design provides a compact, unobtrusive installation appropriate for offices, classrooms, retail spaces, and similar indoor environments. Internal antenna arrays are typically engineered to provide broad coverage around and below the access point, supporting the normal cell shapes used in indoor WLAN deployments. Modern indoor APs commonly use multiple integrated antenna elements to support MIMO operation, beamforming, and spatial-stream capabilities while avoiding external antenna hardware.

Using integrated antennas also simplifies installation and helps maintain a consistent RF pattern when APs are mounted according to the vendor's guidance. For most standard indoor coverage designs, the installer selects AP placement, mounting orientation, transmit power, and channel plan rather than selecting and attaching a separate antenna. Cisco's indoor AP documentation describes integrated antenna models and their intended indoor deployment use, while CWNP's WLAN fundamentals materials emphasize antenna selection and coverage patterns as key RF design considerations. See Cisco Catalyst 9130AX Series access point documentation and CWNP.

QUESTION NO: 6

What is the name given to the WPA2 implementation that uses a PSK (Pre-Shared Key)?

A. Corporate

B. Private

C. Personal

D. Enterprise

ANSWER: C

Explanation:

Personal is the correct name for the WPA2 implementation that uses a pre-shared key (PSK). WPA2-Personal is designed for home and small-office networks where users share a single configured passphrase to authenticate to the wireless network. That passphrase is used in the PSK authentication process to derive the cryptographic material that protects wireless traffic. In Wi-Fi Alliance naming, this mode is commonly presented as WPA2-Personal, and it may also be called WPA2-PSK in product documentation and access-point configuration interfaces. The passphrase must be sufficiently strong and unique because everyone with the same PSK can join the network and because weak, captured PSK handshakes may be susceptible to offline password-guessing attacks. WPA2-Personal uses AES-CCMP protection when configured according to WPA2 requirements. For current deployments, Wi-Fi Alliance certification guidance also promotes WPA3-Personal, which replaces the PSK authentication exchange with SAE while retaining a password-based user experience. See the Wi-Fi Alliance Wi-Fi security overview and the CWNP 802.11i security overview.

QUESTION NO: 7

What kind of security constraint can always be legally enforced on an organization?

A. Industry guidelines

B. Organizational procedures

C. Industry standards

D. Regulatory

ANSWER: D

Explanation:

Regulatory is correct because regulations are mandatory requirements imposed by a government agency or other authority that has legal jurisdiction over an organization. When a regulation applies to the organization's business, data, personnel, facilities, or wireless operations, the organization is obligated to comply. Failure to meet applicable regulatory security

requirements can result in enforcement actions such as fines, corrective-action orders, restrictions on operations, or other statutory penalties. In security planning, regulatory constraints therefore establish non-optional baseline obligations that must be identified and addressed through policies, technical controls, operational processes, and evidence of compliance.

For wireless environments, regulatory authority is especially important because radio spectrum use is governed by national regulators. In the United States, the Federal Communications Commission establishes and enforces rules for radio-frequency devices and spectrum operation, including requirements relevant to Wi-Fi equipment authorization and lawful use. Organizations must also account for security and privacy regulations applicable to their sector and the information they handle. NIST describes regulatory compliance as a key consideration in managing organizational risk and implementing security controls. See the FCC equipment authorization information and NIST SP 800-53.

QUESTION NO: 8

What access method is used by 802.11 stations to reduce the likelihood of transmitting at the same time as another station?

A. CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

B. Token passing

C. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

D. Circuit switching

ANSWER: C

Explanation:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is correct because Wi-Fi stations listen to the wireless medium before transmitting and use contention procedures intended to avoid simultaneous transmissions. A station that senses the channel as idle waits for the required interframe interval and then uses a randomized backoff before transmitting. If the medium is busy, the station defers and continues its backoff process when the medium becomes available.

Unlike Ethernet's historical CSMA/CD approach, a wireless station generally cannot reliably detect a collision while it is transmitting. 802.11 therefore relies on collision avoidance, acknowledgments, retransmissions, and other medium-access mechanisms to coordinate use of the shared RF medium.