CHAPTER 27

WWW and HTTP

1: \_ is a repository of information linked together from points all over the world.

a. The WWW

b. HTTP

c. HTML

d. none of the above

2: The WWW today is a

access a service using a server. a. limited

b. vast

c. distributed

d. none of the above

client-server service, in which a client using a browser can

3: The

a. URL

b. ULR

c. RLU

is a standard for specifying any kind of information on the Internet.

d. none of the above

4: In a URL, the a. path

b. protocol

c. host

is the client-server program used to retrieve the document.

d. none of the above

5: In a URL, the

is the computer on which the information is located.

a. path

b. protocol

c. host

d. none of the above

6: In a URL, an optional

separated from the host by a colon. a. path

b. protocol c. host

d. none of the above

can be inserted between the host and the path, and it is

7: In a URL, the

a. path

b. protocol c. host

is the full name of the file where the information is located.

d. none of the above

8: A cookie is made by the a. client; client

b. client; server

c. server; server

d. none of the above

\_ and eaten by the \_ .

9: The documents in the WWW can be grouped into \_

a. two b. three c. four

broad categories.

d. none of the above

10: A

\_ document is a fixed-content document that is created and stored in a server.

The client can get a copy of the document only.

a. static

b. dynamic c. active

d. none of the above

11:

a. HTTP

b. HTML

c. FTTP

is a language for creating Web pages.

d. none of the above

12: A

document.

\_ document is created by a Web server whenever a browser requests the

a. static

b. dynamic

c. active

d. none of the above

13:

a. GIC

b. CGI

c. GCI

\_ is a technology that creates and handles dynamic documents.

d. none of the above

14: Dynamic documents are sometimes referred to as \_

a. client-site

b. server-site

c. both a and b

d. none of the above

dynamic documents.

15: For many applications, we need a program or a script to be run at the client site. These

are called

a. static

b. dynamic

c. active

d. none of the above

documents.

16: One way to create an active document is to use \_

a. CGI

b. Java stand-alone programs

c. Java applets

d. none of the above

17: Active documents are sometimes referred to as

a. client-site

b. server-site

c. both a and b

d. none of the above

\_.

\_ dynamic documents.

18: HTTP uses the services of a. UDP

b. IP

c. TCP

d. none of the above

on well-known port 80.

19: In HTTP, the first line in a request message is called a \_

\_ line; the first line in the

response message is called the \_

a. request; response b. response; request c. response; status

d. none of the above

line.

20: In a

a. persistent

b. nonpersistent

connection, one TCP connection is made for each request/response.

c. both a and b

d. none of the above

21: In a

sending a response.

a. persistent

connection, the server leaves the connection open for more requests after

b. nonpersistent c. both a and b

d. none of the above

22: HTTP version 1.1 specifies a \_

a. persistent

b. nonpersistent c. both a and b

d. none of the above

connection by default.

23: In HTTP, a requests.

a. regular

server is a computer that keeps copies of responses to recent

b. proxy

c. both a and b

d. none of the above

24: An HTTP request message always contains . a. a header and a body

b. a request line and a header

c. a status line, a header, and a body d. none of the above

25: Which of the following is present in both an HTTP request line and a status line?

a. HTTP version number

b. URL

c. status code

d. none of the above

26: The HTTP request line contains a

server.

method to request a document from the

a. GET

b. POST

c. COPY

d. none of the above

27: A user needs to send the server some information. The request line method is . a. OPTION

b. PATCH

c. POST

28: The HTTP request line contains a without retrieving the document itself.

method to get information about a document

a. HEAD b. POST c. COPY

d. none of the above

29: A response message always contains . a. a header and a body

b. a request line and a header

c. a status line and a header

d. none of the above

30: An applet is \_ document application program. a. a static

b. an active c. a passive d. a dynamic

CHAPTER 28

Network Management: SNMP

1: SNMP defines the

versa.

to be sent from a manager to an agent and vice

a. format of the packets

b. encoding of the packets c. number of packets

d. none of the above

2: A manager is a host that runs the SNMP

a. client

b. server

c. both a and b

d. none of the above

process.

3: An agent is a host or computer that runs the SNMP

a. client

b. server

c. both a and b

d. none of the above

process.

4: SNMP uses two other protocols:

a. MIB; SMTP

\_ and .

b. SMI; MIB

c. FTP; SMI

d. none of the above

5: defines the general rules for naming objects, defining object types, and showing

how to encode objects and values. a. MIB

b. BER

c. SMI

d. none of the above

6: We can compare the task of network management to the task of writing a program. Both

tasks need rules. In network management this is handled by \_ . a. SMNP

b. MIB

c. SMI

d. none of the above

7: We can compare the task of network management to the task of writing a program. Both

tasks need variable declarations. In network management this is handled by \_ . a. SMNP

b. MIB

c. SMI

d. none of the above

8: We can compare the task of network management to the task of writing a program. Both tasks have actions performed by statements. In network management this is handled by

.

a. SMNP

b. MIB

c. SMI

d. none of the above

9: SMI emphasizes three attributes to handle an object: \_ \_, a. name; data type; size

b. name; size; encoding method

c. name; data type; encoding method

d. none of the above

\_, and \_.

10: To name objects globally, SMI uses an object identifier, which is a hierarchical identifier

based on a

a. linear

b. tree

c. graph

structure

d. none of the above

11: All objects managed by SNMP are given an object identifier. The object identifier always

starts with .

a. 1.3.6.1.2.1 b. 1.3.6.1.2.2 c. 1.3.6.1.2.3

d. none of the above

12: To define the data type, SMI uses fundamental definitions.

a. AMS.1 b. ASN.1 c. ASN.2

d. none of the above

\_ definitions and adds some new

13: SMI has two broad categories of data type:

a. simple; complex

b. simple; structured

c. structured; unstructured d. none of the above

\_ and .

14: The \_

\_ data types are atomic data types.

a. structure

b. simple

c. both a and b

d. none of the above

15: SMI defines two structured data types:

a. sequence; atomic

b. sequence; sequence of

c. a sequence of; array d. none of the above

16: SMI uses another standard, \_

network.

a. MIB

b. ANS.1

c. BER

d. none of the above

and \_ .

, to encode data to be transmitted over the

17: The \_

ordering enables a manager to access a set of variables one after another

by defining the first variable.

a. lexicographic

b. linear

c. non-linear

d. none of the above

18: The GetRequest PDU is sent from the a variable or a set of variables.

a. client; server

b. server; client

c. server; network

d. none of the above

19: The Response PDU is sent from the

GetNextRequest.

a. server; client b. client; server c. network; host

d. none of the above

to the

to the

to retrieve the value of

\_ in response to GetRequest or

20: The Trap PDU is sent from the

a. server; client b. client; server c. network; host

d. none of the above

\_ to the \_ to report an event.

21: SNMP uses the services of UDP on two well-known ports, \_

a. 161; 162 b. 160; 161 c. 160; 162

d. none of the above

\_ and .

22:

runs the SNMP client program;

a. A manager; a manager b. An agent; an agent

c. A manager; an agent

d. An agent; a manager

\_ runs the SNMP server program.

23: INTEGER, OCTET STRING, and ObjectIdentifier are \_

a. MIB

b. SNMP

c. ASN.1

d. none of the above

\_ definitions used by SMI.

24: Which of the following could be a legitimate MIB object identifier?

a. 1.3.6.1.2.1.1 b. 1.3.6.1.2.2.1 c. 2.3.6.1.2.1.2

d. none of the above

25: Which is a manager duty?

a. Retrieve the value of an object defined in an agent. b. Store the value of an object defined in an agent.

c. a and b

d. none of the above

26: For a 1-byte length field, what is the maximum value for the data length?

a. 127 b. 128 c. 255

d. none of the above

27: An object id defines a a. variable; table

b. table; variable

c. variable; variable contents

d. none of the above

28: An SNMP agent can send a. GetRequest

b. SetRequest c. Trap

d. none of the above

29: An SNMP agent can send

a. Response

b. GetRequest c. SetRequest

d. none of the above

. Add a zero suffix to define the .

messages.

messages.

30: The \_

\_ field in the SNMP PDU is an offset that points to the variable in error.

a. community b. enterprise

c. error index

d. none of the above

31: The \_

\_ field in the SNMP PDU reports an error in a response message.

a. community b. enterprise

c. error status

d. none of the above

32: The \_

\_ field in the SNMP PDU consists of a sequence of variables and their

corresponding values. a. version

b. community

c. VarBindList

CHAPTER 29

Multimedia

1: We can divide audio and video services into

a. three b. two c. four

d. none of the above

\_ broad categories.

2: audio/video refers to on-demand requests for compressed audio/video files. a. Streaming live

b. Streaming stored

c. Interactive

d. none of the above

3:

Internet.

audio/video refers to the broadcasting of radio and TV programs through the

a. Interactive

b. Streaming live

c. Streaming stored

d. none of the above

4:

applications.

\_ audio/video refers to the use of the Internet for interactive audio/video

a. Interactive

b. Streaming live

c. Streaming stored

d. none of the above

5: According to the Nyquist theorem, we need to sample an analog signal highest frequency.

a. three

b. two

c. four

d. none of the above

\_times the

6: In

\_ encoding, the differences between the samples are encoded instead of

encoding all the sampled values.

a. predictive

b. perceptual

c. both a and b

d. none of the above

7: encoding is based on the science of psychoacoustics, which is the study of

how people perceive sound. a. Predictive

b. Perceptual

c. both a and b

d. none of the above

8: \_ is used to compress images. a. MPEG

b. JPEG

c. either a or b

d. none of the above

9: \_ is used to compress video.

a. MPEG

b. JPEG

c. either a or b

d. none of the above

10: The first phase of JPEG is \_ .

a. DCT transformation

b. quantization

c. data compression

d. none of the above

11: The second phase of JPEG is . a. DCT transformation

b. quantization

c. data compression

d. none of the above

12: The third phase of JPEG is . a. DCT transformation

b. quantization

c. data compression

d. none of the above

13: Jitter is introduced in real-time data by the . a. error caused during transmission

b. delay between packets

c. both a and b

d. none of the above

14: To prevent \_

the playback time. a. error

b. jitter

c. either a or b

, we can timestamp the packets and separate the arrival time from

d. none of the above

15: A

buffer is required for real-time traffic.

a. playback

b. reordering c. sorting

d. none of the above

16: A

on each packet is required for real-time traffic. a. timestamp

b. sequence number

c. both a and b

d. none of the above

17: Real-time traffic needs the support of . a. broadcasting

b. multicasting

c. both a and b

d. none of the above

18:

means changing the encoding of a payload to a lower quality to match the

bandwidth of the receiving network.

a. Translation

b. Mixing

c. both a and b

d. none of the above

19:

means combining several streams of traffic into one stream. a. Translation

b. Mixing

c. both a and b

d. none of the above

20:

case of errors. a. UDP

b. TCP

is not suitable for interactive multimedia traffic because it retransmits packets in

c. both a and b

d. none of the above

21:

a. TCP

b. UDP

c. RTP

is the protocol designed to handle real-time traffic on the Internet.

d. none of the above

22: RTP uses a temporary even-numbered

port.

a. UDP

b. TCP

c. both a and b

d. none of the above

23:

a. RTP

\_ is a protocol for controlling the flow and quality of data.

b. RTCP

c. UDP

d. none of the above

24: RTCP uses an odd-numbered \_ \_ port number that follows the port number selected for RTP.

a. UDP

b. TCP

c. both a and b

d. none of the above

25:

\_ is an application protocol that establishes, manages, and terminates a

multimedia session a. RIP

b. SIP

c. DIP

d. none of the above

26:

is a standard to allow telephones on the public telephone network to talk to

computers connected to the Internet. a. SIP

b. H.323

c. Q.991

d. none of the above

27: A real-time video performance lasts 10 min. If there is jitter in the system, the viewer

spends

minutes watching the performance. a. less than 10

b. more than 10

c. exactly 10

d. none of the above

28: A

\_ shows the time a packet was produced relative to the first or previous packet.

a. timestamp

b. playback buffer

c. sequence number

d. none of the above

29:

are used to number the packets of a real-time transmission. a. Timestamps

b. Playback buffers

c. Sequence numbers

d. none of the above

30: In a real-time video conference, data from the server is a. unicast

b. multicast

c. broadcast

d. none of the above

to the client sites.

31: A

\_ adds signals from different sources to create a single signal.

a. timestamp

b. sequence number

c. mixer

d. none of the above

32: A

\_ changes the format of a high-bandwidth video signal to a lower quality narrow-

bandwidth signal.

a. timestamp

b. sequence number

c. translator

d. none of the above

33: An RTP packet is encapsulated in \_.

a. a UDP user datagram

b. a TCP segment c. an IP datagram

d. none of the above

34: When there is more than one source, the \_

a. synchronization source

b. contributor c. timestamp

d. none of the above

\_ identifier defines the mixer.

CHAPTER 30

Cryptography

1: is the science and art of transforming messages to make them secure and

immune to attacks.

a. Cryptography

b. Cryptoanalysis

c. either (a) or (b)

d. neither (a) nor (b)

2: The

\_is the original message before transformation. a. ciphertext

b. plaintext

c. secret-text

d. none of the above

3: The

\_ is the message after transformation.

a. ciphertext

b. plaintext

c. secret-text

d. none of the above

4: A(n)

algorithm transforms plaintext to ciphertext

a. encryption

b. decryption

c. either (a) or (b)

d. neither (a) nor (b)

5: A(n) \_ algorithm transforms ciphertext to plaintext. a. encryption

b. decryption

c. either (a) or (b)

d. neither (a) nor (b)

6: A combination of an encryption algorithm and a decryption algorithm is called a \_ .

a. cipher b. secret c. key

d. none of the above

7: The

a. cipher b. secret

c. key

is a number or a set of numbers on which the cipher operates.

d. none of the above

8: In a(n)

\_ cipher, the same key is used by both the sender and receiver.

a. symmetric-key

b. asymmetric-key

c. either (a) or (b)

d. neither (a) nor (b)

9: In a(n)

\_, the key is called the secret key.

a. symmetric-key

b. asymmetric-key

c. either (a) or (b)

d. neither (a) nor (b)

10: In a(n) \_

cipher, a pair of keys is used.

a. symmetric-key

b. asymmetric-key

c. either (a) or (b)

d. neither (a) nor (b)

11: In an asymmetric-key cipher, the sender uses the a. private

b. public

c. either (a) or (b)

key.

d. neither (a) nor (b)

12: In an asymmetric-key cipher, the receiver uses the

a. private

b. public

c. either (a) or (b)

d. neither (a) nor (b)

\_ key.

13: A

cipher replaces one character with another character.

a. substitution

b. transposition

c. either (a) or (b)

d. neither (a) nor (b)

14:

polyalphabetic.

ciphers can be categorized into two broad categories: monoalphabetic and

a. Substitution

b. Transposition

c. either (a) or (b)

d. neither (a) nor (b)

15: The \_

\_ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with

a modulus of 26.

a. transposition b. additive

c. shift

d. none of the above

16: The Caesar cipher is a \_

cipher that has a key of 3.

a. transposition b. additive

c. shift

d. none of the above

17: The \_

cipher reorders the plaintext characters to create a ciphertext.

a. substitution

b. transposition

c. either (a) or (b)

d. neither (a) nor (b)

18: A(n)

is a keyless substitution cipher with <i>N</i> inputs and <i>M</i> outputs that

uses a formula to define the relationship between the input stream and the output stream.

a. S-box b. P-box c. T-box

d. none of the above

19: A(n)

is a keyless transposition cipher with <i>N</i> inputs and <i>M</i> outputs

that uses a table to define the relationship between the input stream and the output stream. a. S-box

b. P-box

c. T-box

d. none of the above

20: A modern cipher is usually a complex \_ cipher made of a combination of different simple ciphers.

a. round

b. circle

c. square

d. none of the above

21: DES is a(n)

a. symmetric-key

b. asymmetric-key

c. either (a) or (b)

method adopted by the U.S. government.

d. neither (a) nor (b)

22: DES has an initial and final permutation block and a. 14

b. 15

c. 16

d. none of the above

\_ rounds.

23: The DES function has \_

a. 2 b. 3 c. 4

d. 5

components.

24: DES uses a key generator to generate sixteen a. 32-bit

b. 48-bit

c. 54-bit d. 42-bit

round keys.

25:

\_ DES was designed to increase the size of the DES key a. Double

b. Triple

c. Quadruple

d. none of the above

26:

data.

is a round cipher based on the Rijndael algorithm that uses a 128-bit block of

a. AEE b. AED c. AER d. AES

27: AES has a. two

b. three

c. four d. five

different configurations

28: ECB and CBC are

a. block

b. stream c. field

d. none of the above

ciphers.

29: One commonly used public-key cryptography method is the \_

a. RSS b. RAS c. RSA d. RAA

algorithm.

30: The \_

method provides a one-time session key for two parties.

a. Diffie-Hellman

b. RSA

c. DES

d. AES

31: The \_

attack can endanger the security of the Diffie-Hellman method if two

parties are not authenticated to each other.

a. man-in-the-middle b. ciphertext attack c. plaintext attack

d. none of the above

CHAPTER 31

Network Security

1: Message

means that the sender and the receiver expect privacy.

a. confidentiality

b. integrity

c. authentication

d. none of the above

2: Message

means that the data must arrive at the receiver exactly as sent.

a. confidentiality

b. integrity

c. authentication

d. none of the above

3: Message

\_ means that the receiver is ensured that the message is coming from the

intended sender, not an imposter. a. confidentiality

b. integrity

c. authentication

d. none of the above

4:

sent.

\_ means that a sender must not be able to deny sending a message that he

a. Confidentiality b. Integrity

c. Authentication

d. Nonrepudiation

5:

resources.

means to prove the identity of the entity that tries to access the system's

a. Message authentication

b. Entity authentication

c. Message confidentiality d. none of the above

6: A(n)

\_ can be used to preserve the integrity of a document or a message.

a. message digest

b. message summary c. encrypted message

d. none of the above

7: A(n)

function creates a message digest out of a message. a. encryption

b. decryption

c. hash

d. none of the above

8: A hash function must meet a. two

b. three

c. four

d. none of the above

criteria.

9: A

message digest is used as an MDC.

a. keyless

b. keyed

c. either (a) or (b)

d. neither (a) nor (b)

10: To authenticate the data origin, one needs a(n) \_ . a. MDC

b. MAC

c. either (a) or (b)

d. neither (a) nor (b)

11: A

entity.

signature is included in the document; a \_

a. conventional; digital

b. digital; digital

c. either (a) or (b)

d. neither (a) nor (b)

signature is a separate

12: Digital signature provides \_. a. authentication

b. nonrepudiation

c. both (a) and (b)

d. neither (a) nor (b)

13: Digital signature cannot provide \_

a. integrity

b. confidentiality

c. nonrepudiation d. authentication

for the message.

14: If \_

\_ is needed, a cryptosystem must be applied over the scheme.

a. integrity

b. confidentiality

c. nonrepudiation d. authentication

15: A digital signature needs a(n)

a. symmetric-key

b. asymmetric-key

system.

c. either (a) or (b)

d. neither (a) nor (b)

16: A witness used in entity authentication is . a. something known

b. something possessed c. something inherent

d. all of the above

17: In \_ \_, a claimant proves her identity to the verifier by using one of the three kinds of witnesses.

a. message authentication

b. entity authentication

c. message confidentiality d. message integrity

18: Password-based authentication can be divided into two broad categories: \_

.

a. fixed; variable

b. time-stamped; fixed

c. fixed; one-time

d. none of the above

and

19: In \_

sending it.

authentication, the claimant proves that she knows a secret without actually

a. password-based

b. challenge-response

c. either (a) or (b)

d. neither (a) nor (b)

20: Challenge-response authentication can be done using . a. symmetric-key ciphers

b. asymmetric-key ciphers c. keyed-hash functions

d. all of the above

21: A(n)

\_ is a trusted third party that assigns a symmetric key to two parties.

a. KDC

b. CA

c. KDD

d. none of the above

22: A(n)

a. CA b. KDC c. KDD

creates a secret key only between a member and the center.

d. none of the above

23: The secret key between members needs to be created as a members contact KDC.

a. public

b. session

c. complimentary

d. none of the above

key when two

24:

is a popular session key creator protocol that requires an authentication server

and a ticket-granting server. a. KDC

b. Kerberos

c. CA

d. none of the above

25: A(n)

is a federal or state organization that binds a public key to an entity and

issues a certificate. a. KDC

b. Kerberos

c. CA

d. none of the above

26: A(n)

a. KDC

b. PKI

c. CA

is a hierarchical system that answers queries about key certification.

d. none of the above

27: The \_

\_ criterion states that it must be extremely difficult or impossible to create the

message if the message digest is given.

a. one-wayness

b. weak-collision-resistance c. strong-collision-resistance

d. none of the above

28: The \_

criterion ensures that a message cannot easily be forged.

a. one-wayness

b. weak-collision-resistance

c. strong-collision-resistance d. none of the above

29: The \_

digest.

\_criterion ensures that we cannot find two messages that hash to the same

a. one-wayness

b. weak-collision-resistance

c. strong-collision-resistance

d. none of the above