CHAPTER 4

Comunicación y seguridad de la red

Este dominio incluye preguntas de los siguientes temas:

- Modelos OSI y TCP/IP
- Tipos de protocolo y problemas de seguridad
- Tecnologías LAN, WAN, MAN, intranet y extranet
- Medios de transmisión
- Tecnologías inalámbricas
- Dispositivos y servicios de red
- Gestión de la seguridad de las comunicaciones
- Tecnologías de acceso remoto
- Amenazas y ataques
- Redes definidas por software
- Redes de distribución de contenido
- Protocolos multicapa

• Tecnologías de red convergentes

Una red forma la columna vertebral de la infraestructura de TI de una organización. Sin él, los sistemas no podían comunicarse y los usuarios no podían compartir recursos en tiempo real. Debido a la miríada de protocolos, tecnologías y conceptos involucrados en el networking, es uno de los temas más complejos que necesita entender para el examen CISSP y en su papel como profesional de la seguridad. Los muchos tipos diferentes de dispositivos, protocolos y mecanismos de seguridad dentro de un entorno proporcionan diferentes funcionalidades. Debe comprender cómo funcionan las tecnologías, cómo interactúan entre sí, cómo están configuradas y cómo deben protegerse.

PREGUNTAS Q

1 . La capa 2 del modelo OSI tiene dos subcapas. ¿Cuáles son esas subcapas y cuáles son dos estándares IEEE que describen las tecnologías en esa capa?

R. LCL y MAC; IEEE 802.2 y 802.3

B. LCL y MAC; IEEE 802.1 y 802.3

C. Red y MAC; IEEE 802.1 y 802.3

D. LLC y MAC; IEEE 802.2 y 802.3

2 . ¿Cuál de las siguientes no es una contramedida efectiva contra el spam?

R. Abrir servidores de retransmisión de correo

B. Servidores de retransmisión de correo configurados correctamente

C. Filtrado en una puerta de enlace de correo electrónico

D. Filtrado en el cliente

3 . Robert es responsable de implementar una arquitectura común utilizada cuando los clientes necesitan acceder a información confidencial a través de conexiones a Internet. ¿Cuál de los siguientes describe mejor este tipo de arquitectura?

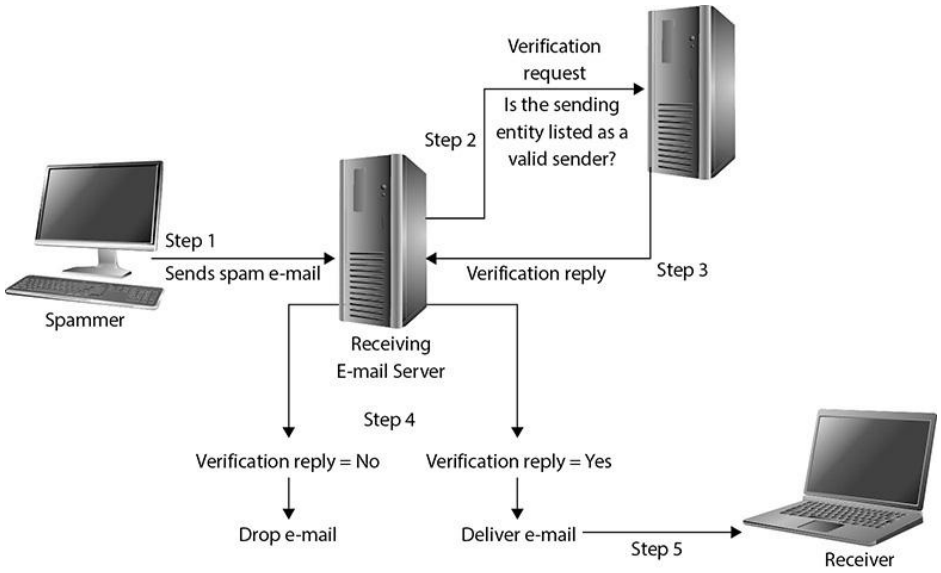
R. Modelo de dos niveles

B. Subred proyectada

C. Modelo de tres niveles

D. Zonas DNS públicas y privadas

4 . Desde el envío de spam (mensajes no deseados) ha aumentado con los años y el correo electrónico se ha convertido en una forma común de enviar enlaces maliciosos y malware, la industria ha desarrollado diferentes maneras de combatir estos problemas. Un enfoque es usar un marco de directivas de remitente, que es un sistema de validación de correo electrónico. En el gráfico siguiente, ¿qué tipo de sistema recibe la solicitud en el paso 2 y responde en el paso 3?



R. Servidor DNS

B. Servidor de correo electrónico

C. Servidor RADIUS

D. Servidor de autenticación

5 . ¿Cuál de los siguientes indica a un paquete a dónde ir y cómo comunicarse con el servicio o protocolo correcto en el equipo de destino?

R. enchufe

B. dirección IP

C. puerto

D. marco

6 . Varios protocolos de tunelización diferentes se pueden utilizar en situaciones de acceso telefónico. ¿Cuál de los siguientes sería mejor utilizar como una solución de tunelización VPN?

R. L2P

B. PPTP

C. IPSec

D. L2TP

7 . ¿Cuál de los siguientes describe correctamente Bluejacking?

R. El bluejacking es un ataque dañino y malicioso.

B. Es el proceso de hacerse cargo de otro dispositivo portátil a través de un dispositivo habilitado para Bluetooth.

C. Se utiliza comúnmente para enviar información de contacto.

D. El término fue acuñado por el uso de un dispositivo Bluetooth y el acto de secuestrar otro dispositivo.

8 . DNS es un objetivo popular para los atacantes debido a su papel estratégico en Internet. ¿Qué tipo de ataque utiliza consultas recursivas para envenenar la memoria caché de un servidor DNS?

R. Secuestro de DNS

B. Manipulación del archivo hosts

C. Ingeniería social

D. Litigio de dominio

9 . Las redes de telefonía IP requieren las mismas medidas de seguridad que las implementadas en una red de datos IP. ¿Cuál de los siguientes es exclusivo de la telefonía IP?

R. Limitar las sesiones ip que pasan por puertas de enlace de medios

B. Identificación de dispositivos falsos

C. Implementación de la autenticación

D. Cifrado de paquetes que contienen información confidencial

10. Angela quiere agrupar computadoras por departamento para facilitarles el uso compartido de recursos de red. ¿Cuál de los siguientes le permitirá agrupar computadoras lógicamente?

R. VLAN

B. Arquitectura de red abierta

C. intranet

D. furgoneta

11. ¿Cuál de las siguientes describe incorrectamente cómo se lleva a cabo el enrutamiento comúnmente en Internet?

R. El EGP se utiliza en las áreas "entre" cada AS.

B. Las regiones de nodos que comparten características y comportamientos se denominan AS.

C. Los CA son nodos específicos que son responsables de enrutar a nodos fuera de su región.

D. Cada AS utiliza el IGP para realizar la funcionalidad de ruteo.

12. Tanto los protocolos interiores de facto como los propios están en uso hoy en día. ¿Cuál de los siguientes es un protocolo interior propietario que elige la mejor ruta entre la fuente y el destino?

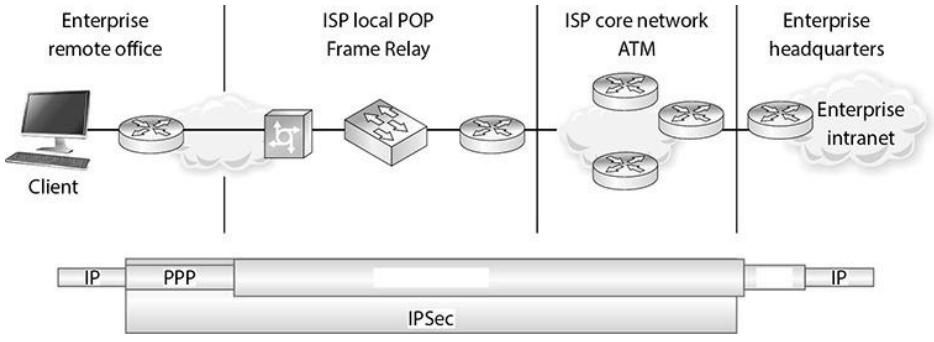
R. IGRP

B. SI1

C. Bgp

D. Ospf

13. Cuando un sistema necesita enviar datos a un usuario final, es posible que esos datos tengan que viajar a través de diferentes protocolos de red para llegar al destino. Los diferentes tipos de protocolo dependen de hasta qué punto geográficamente deben viajar los datos, los tipos de dispositivos intermedios implicados y cómo estos datos deben protegerse durante la transmisión. En el gráfico siguiente, ¿qué dos protocolos WAN faltan y cuál es el mejor razonamiento para su funcionalidad en el escenario de transmisión que se está ilustrando?



R. PPTP se está utilizando ya que el tráfico necesita viajar a través de diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones multiplexado.

B. L2FP se está utilizando ya que el tráfico necesita viajar a través de diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones en serie.

C. L2TP se está utilizando ya que el tráfico necesita viajar sobre diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones en serie.

D. El modo de túnel IPSec se está utilizando ya que el tráfico necesita viajar sobre diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones multiplexado.

14. ¿Cuál de las siguientes opciones NO describe la seguridad de la telefonía IP?

R. Las redes VoIP deben protegerse con los mismos controles de seguridad utilizados en una red de datos.

B. Los softphones son más seguros que los teléfonos IP.

C. Como puntos finales, los teléfonos IP pueden convertirse en el objetivo de los ataques.

D. La arquitectura actual de Internet sobre la cual se transmite la voz es menos segura que las líneas telefónicas físicas.

15. Cuando una organización divide las zonas de nomenclatura, los nombres de sus hosts a los que solo se puede acceder desde una intranet se ocultan de Internet. ¿Cuál de las siguientes describe mejor por qué se hace esto?

R. Para evitar que los atacantes accedan a los servidores

B. Para evitar la manipulación del archivo hosts

C. Para evitar proporcionar a los atacantes información valiosa que se puede utilizar para preparar un ataque

D. Para evitar proporcionar a los atacantes la información necesaria para la ocupación cibernética

16. ¿Cuál de las siguientes describe mejor por qué se ejecuta fácilmente la suplantación de correo electrónico?

R. SMTP carece de un mecanismo de autenticación adecuado.

B. Los administradores a menudo olvidan configurar un servidor SMTP para evitar conexiones SMTP entrantes para dominios que no sirve.

C. El filtrado de palabras clave es técnicamente obsoleto.

D. Las listas negras son independables.

17. ¿Cuál de los siguientes no beneficia a VoIP?

R. costar

B. convergencia

C. flexibilidad

D. seguridad

18. Hoy en día, los satélites se utilizan para proporcionar conectividad inalámbrica entre diferentes ubicaciones. ¿Qué dos requisitos previos se necesitan para que dos ubicaciones diferentes se comuniquen a través de enlaces satelitales?

R. Deben estar conectados a través de una línea telefónica y tener acceso a un módem.

B. Deben estar dentro de la línea de visión y huella del satélite.

C. Deben tener banda ancha y un satélite en órbita terrestre baja.

D. Deben tener un transpondedor y estar dentro de la huella del satélite.

19. Brad es un gerente de seguridad en Thingamabobs, Inc. Está preparando una presentación para los ejecutivos de su empresa sobre los riesgos de usar mensajería instantánea (IM) y sus razones para querer prohibir su uso en la red de la compañía. ¿Cuál de los siguientes no debe incluirse en su presentación?

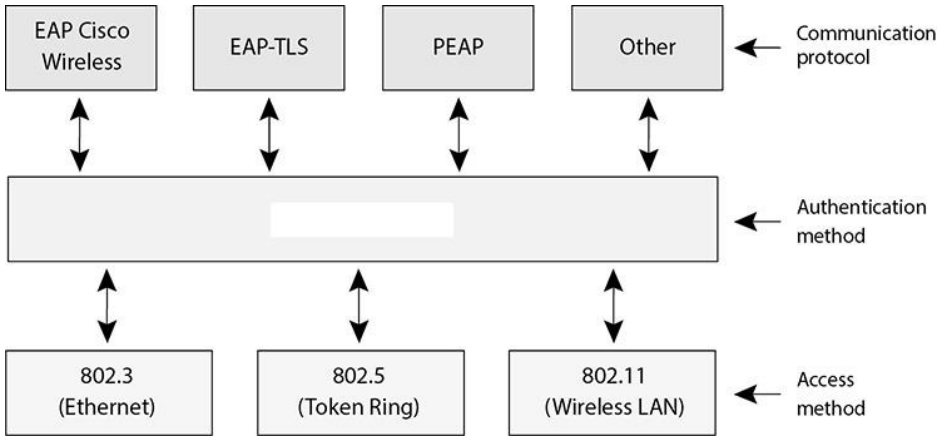
R. Los datos y archivos confidenciales se pueden transferir de un sistema a otro a través de mensajería instantánea.

B. Los usuarios pueden recibir información, incluido el malware, de un atacante que se hace pasar por un remitente legítimo.

C. El uso de mensajería instantánea se puede detener simplemente bloqueando puertos específicos en los firewalls de red.

D. Se necesita una directiva de seguridad que especifique las restricciones de uso de mensajería instantánea.

20. Hay varios tipos diferentes de tecnologías de autenticación. ¿Qué tipo se muestra en el gráfico que sigue?



A. 802.1X

B. Protocolo de autenticación extensible

C. Espectro de dispersión de salto de frecuencia

D. Multiplexación ortogonal de división de frecuencias

21. ¿Qué tipo de componente de cifrado de seguridad falta en la tabla siguiente?

	802.1X Dynamic WEP	Wi-Fi Protected Access	Robust Security Network
Access Control	802.1X	802.1X or preshared key	802.1X or preshared key
Authentication	EAP methods	EAP methods or preshared key	EAP methods or preshared key
Encryption	WEP		CCMP (AES Counter Mode)
Integrity	None	Michael MIC	CCMP (AES CBC-MAC)

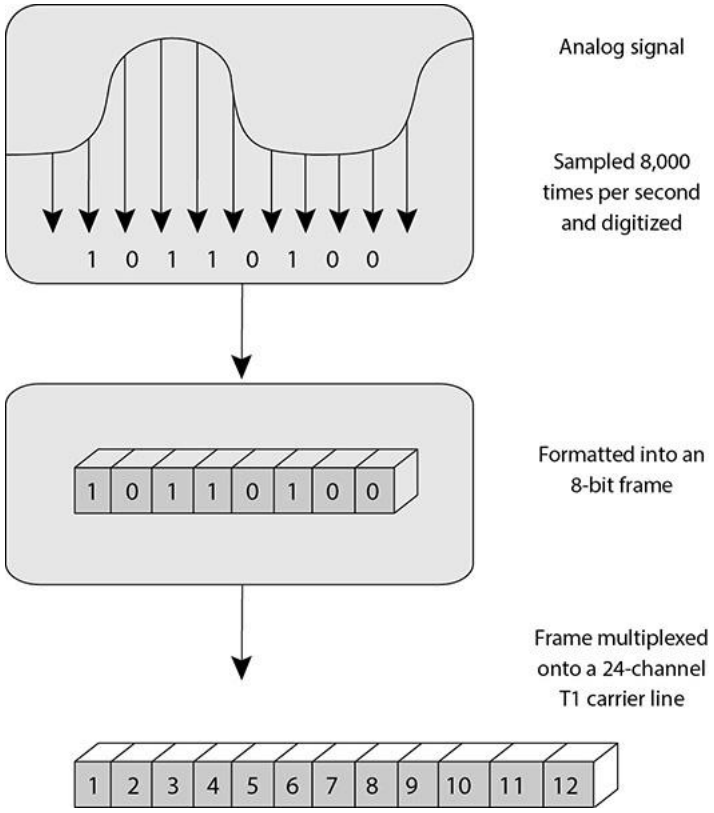
R. ID de conjunto de servicios

B. Protocolo de integridad de la clave temporal

C. Ad hoc WLAN

D. Autenticación abierta del sistema

22. ¿Qué tipo de tecnología se representa en el gráfico que sigue?



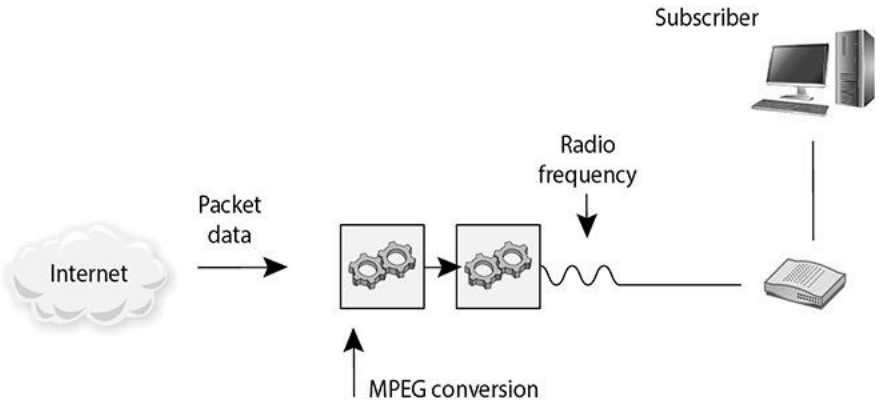
A. Modo de transferencia asíncrono

B. Redes ópticas sincrónicas

C. Multiplexación de división de frecuencia

D. multiplexación

23. ¿Qué tipo de tecnología de telecomunicaciones se ilustra en el gráfico que sigue?



R. Línea de suscriptores digitales

B. Red Digital de Servicios Integrados

C. BRI ISDN

D. Módem de cable

24. ¿Qué tipo de protocolo de tunelización WAN falta en la tabla derecha del gráfico siguiente?

PPTP
Internetwork Must Be IP Based
No Header Compression
No Tunnel Authentication
Built-In PPP Encryption

Internetwork Can Be IP Frame Relay, x.25, or ATM Based
Header Compression
Tunnel Authentication
Uses IPSec Encryption

R. IPSec

B. Fddi

C. L2TP

D. CSMA/CD

25. IPv6 tiene muchas características y funcionalidades nuevas y diferentes en comparación con IPv4. ¿Cuál de los siguientes es una funcionalidad o característica incorrecta de IPv6?

i. IPv6 permite direcciones no vinculadas, lo que permite a un administrador restringir direcciones específicas para servidores específicos o intercambio de archivos e impresión, por ejemplo.

ii. IPv6 tiene IPSec integrado en la pila de protocolos, que proporciona transmisión y autenticación seguras basadas en aplicaciones.

iii. IPv6 tiene más flexibilidad y capacidades de enrutamiento en comparación con IPv4 y permite asignar valores de prioridad de calidad de servicio (QoS) a transmisiones sensibles al tiempo.

iv. El protocolo ofrece la autoconfiguración, lo que hace que la administración sea mucho más fácil en comparación con IPv4, y no requiere traducción de direcciones de red (NAT) para ampliar su espacio de direcciones.

A. i, iii

B. i, ii

C. ii, iii

D. ii, iv

26. Hanna es un nuevo gerente de seguridad para una empresa de consultoría informática. Ella ha descubierto que la compañía ha perdido propiedad intelectual en el pasado porque los empleados maliciosos instalaron dispositivos falsos en la red, que se utilizaron para capturar tráfico sensible. Hanna necesita implementar una solución que garantice que solo se permita el acceso a dispositivos autorizados a la red de la empresa. ¿Cuál de las siguientes normas IEEE se desarrolló para este tipo de protección?

R. IEEE 802.1AR

B. IEEE 802.1AE

C. IEEE 802.1AF

D. IEEE 802.1XR

27. _____

R. Registros de recursos

B. Traslado de zona

C. DNSSEC

D. Transferencia de recursos

28. ¿Cuál de los siguientes describe mejor la diferencia entre un firewall virtual que funciona en modo puente frente a uno que está incrustado en un hipervisor?

R. El firewall virtual en modo puente permite al firewall supervisar enlaces de tráfico individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema host.

B. El firewall virtual en modo puente permite al firewall supervisar enlaces de red individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema invitado.

C. El firewall virtual en modo puente permite al firewall supervisar enlaces de tráfico individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema invitado.

D. El firewall virtual en modo puente permite al firewall supervisar sistemas invitados individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema de red.

29. ¿Cuál de las siguientes tecnologías de redes definidas por software (SDN) especifica?

R. La asignación entre las direcciones MAC y las direcciones IP en el software

B. Las tablas de enrutamiento estático de los nodos finales de forma dinámica

C. Cómo los routers comunican sus tablas de ruteo entre sí a medida que ocurren los eventos

D. Cómo mueven los paquetes los routers en función de las instrucciones de un controlador administrado de forma centralizada

30. Determinar la ubicación geográfica de una dirección IP del cliente para enrutarla hacia la fuente topológica más proximal del contenido web es un ejemplo de ¿qué tecnología?

R. Red de distribución de contenido (CDN)

B. Servicio de nombres distribuidos (DNS)

C. Servicio web distribuido (DWS)

D. Distribución de dominios de contenido (CDD)

31. ¿Cuál de los siguientes protocolos o conjunto de protocolos se utiliza en Voz sobre IP (VoIP) para la identificación de llamadas?

R. Protocolo de transporte en tiempo real (RTP) y/o Protocolo de transporte seguro en tiempo real (SRTP)

B. Protocolo de transporte en tiempo real (RTP) y protocolo de control de transporte en tiempo real (RTCP)

C. Protocolo de inicio de sesión (SIP)

D. Intercambio público de telefonía/sucursal telefónica conmutada (RTC/PBX)

32. El cifrado puede ocurrir en diferentes capas de un sistema operativo y una pila de red. ¿Dónde se lleva a cabo el cifrado PPTP?

R. Capa de enlace de datos

B. Dentro de las aplicaciones

C. Capa de transporte

D. Enlace de datos y capas físicas

33. ¿Cuál de los siguientes describe incorrectamente la suplantación de IP y el secuestro de sesiones?

R. La suplantación de dirección ayuda a un atacante a secuestrar sesiones entre dos usuarios sin ser notado.

B. La suplantación de IDENTIDAD hace que sea más difícil localizar a un atacante.

C. El secuestro de sesión se puede prevenir con autenticación mutua.

D. La suplantación de IP se utiliza para secuestrar comunicaciones seguras SSL e IPSec.

34. El equipo de seguridad de TI de una pequeña institución médica se ha visto abrumado por tener que operar y mantener IDS, firewalls, soluciones antimalware en toda la empresa, tecnologías de prevención de fugas de datos y gestión centralizada de registros. ¿Cuál de las siguientes describe mejor qué tipo de solución debe implementar esta organización para permitir operaciones de seguridad estandarizadas y optimizadas?

R. Gestión unificada de amenazas

B. Tecnología de monitoreo continuo

C. Sistemas centralizados de control de acceso

D. Solución de seguridad basada en la nube

35. ¿Cuál de los siguientes protocolos desenfoca las líneas entre las capas del modelo OSI, realizando las tareas de varios a la vez?

R. Protocolo de red distribuida 3 (DNP3)

B. Protocolo de transferencia de archivos (FTP)

C. Protocolo de control de transmisión (TCP)

D. Sistema de nombres de dominio (DNS)

36. ¿Cuál de las siguientes describe correctamente la relación entre SSL y TLS?

R. TLS es la versión de comunidad abierta de SSL.

B. Los desarrolladores pueden modificar SSL para ampliar las capacidades del protocolo.

C. TLS es un protocolo propietario, mientras que SSL es un protocolo de comunidad abierta.

D. SSL es más extensible y compatible con TLS.

37. Los usuarios utilizan el cifrado de extremo a extremo y los proveedores de servicios utilizan el cifrado de vínculos. ¿Cuál de las siguientes describe correctamente estas tecnologías?

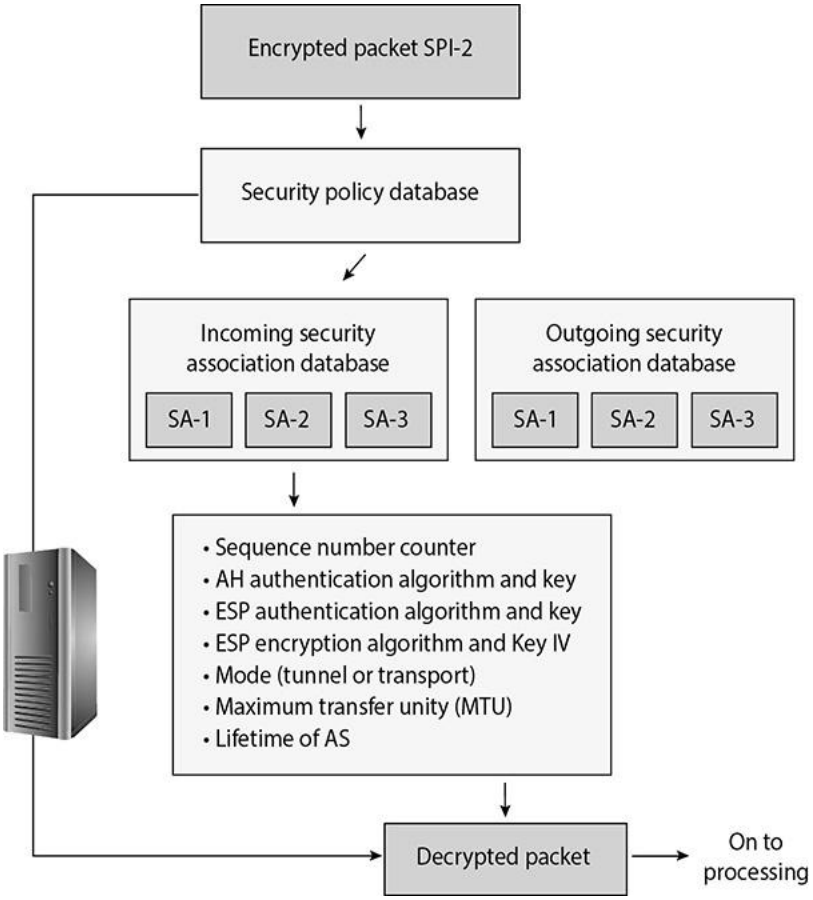
R. El cifrado de vínculos no cifra los encabezados y los trailers.

B. El cifrado de enlaces cifra todo menos la mensajería de enlaces de datos.

C. El cifrado de extremo a extremo requiere que los encabezados se descifran en cada salto.

D. El cifrado de extremo a extremo cifra todos los encabezados y trailers.

38. ¿Qué representan los valores SA en el gráfico de IPSec que sigue?



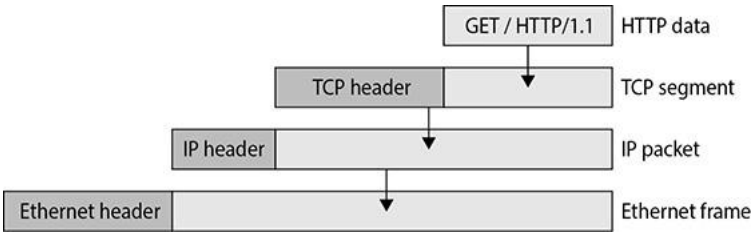
R. Índice de parámetros de seguridad

B. Capacidad de seguridad

C. Asociación de seguridad

D. Asistente de seguridad

39. ¿Cuál es el proceso descrito en la ilustración siguiente conocida como?



R. Modelo TCP/IP

B. acodo

C. encapsulación

D. Modelo OSI

40. ¿Cuál de las siguientes es una finalidad de la capa de transporte?

R. La entrega salto a salto de paquetes de una red a otra

B. Representar datos en una estructura que pueden ser entendidos por procesos en los puntos finales

C. Encapsulación del paquete IP para el transporte

D. Garantizar una transferencia de datos fiable

41. ¿Cuál de las siguientes instrucciones NO es cierto acerca de la dirección IPv4 192.168.10.129\25?

R. Es una dirección privada especificada por RFC 1918.

B. La máscara de red para esta dirección es 255.255.255.0.

C. La dirección de red de la red que especifica es 192.168.10.128\25.

D. La parte del host de esta dirección de 32 bits es el orden bajo 7 bits.

42. ¿Cuál de las siguientes declaraciones describe un protocolo "convergente"?

R. Es un término utilizado para describir una situación en la que dos protocolos independientes, que a menudo funcionan en la misma capa, se convierten en uno, como con Fibre Channel (FC) a través de Ethernet (FCoE).

B. Es cualquier situación donde un protocolo se encapsula con otro, como con TCP dentro de IP (TCP/IP).

C. Se refiere a cuando dos protocolos en la misma capa comienzan a hacer esencialmente lo mismo, como HTTP y HTTPS.

D. Es cualquier situación donde un Protocolo se encapsula dentro de otro protocolo de una manera que dobla o rompe el modelo OSI, como con IPv6 sobre la encapsulación de ruteo genérico (GRE) sobre IPv4.

43. Ethernet utiliza un medio compartido para todas las estaciones en una LAN para comunicarse, y utiliza un enfoque de acceso múltiple de sentido portador con detección de colisión (CSMA/CD) para administrar las comunicaciones entre estaciones. ¿Cuál de las siguientes declaraciones sobre este protocolo explica mejor cómo funciona?

R. Una trama de control se pasa de estación en estación, concediendo permiso para que esa estación transmita una vez que se recibe.

B. Cada estación es necesaria para monitorear el medio para las transmisiones y transmitir solamente cuando todas las demás estaciones son silenciosas. Cada estación también es responsable de alertar a todas las demás estaciones si observa más de una estación que transmite al mismo tiempo.

C. Cada estación es necesaria para monitorear el medio para las transmisiones y transmitir solamente cuando todas las demás estaciones son silenciosas. Cada estación también es responsable de señalar su intención de transmitir antes de hacerlo.

D. Una estación primaria es responsable de determinar cuál de las otras estaciones debe transmitir, sondeando cada una de ellas a intervalos regulares para determinar qué estación tiene datos que transmitir.

44. Dentro del ámbito de los componentes de red, ¿qué son los "puntos finales" y por qué plantean desafíos de seguridad tan difíciles?

R. Los puntos de conexión son los sistemas cliente de una red. Debido a que establecen conexiones a servidores internos y externos, sus actividades pueden ser difíciles de supervisar y controlar, y las descargas de software malicioso en el entorno son comunes.

B. Los puntos de conexión son los servidores a los que se conectan todos los clientes para la autenticación, el uso compartido de archivos y otros servicios. Debido al alto volumen de conexiones que soportan, puede ser difícil monitorear y detectar actividades maliciosas dirigidas a ellas, enterradas entre las actividades normales.

C. Los puntos de conexión son todo excepto los dispositivos de comunicación de red, incluidos escritorios, servidores, dispositivos móviles y otros sistemas integrados. Los desafíos de administración que plantean incluyen conectividad intermitente, falta de infraestructura de administración para algunas plataformas y la falta de disponibilidad de actualizaciones de software para otras.

D. Los puntos de conexión son principalmente sistemas móviles y de escritorio, que pueden existir o no estáticamente en la red. Como resultado, realizar un seguimiento de ellos para mantener el parcheo actualizado y la configuración adecuada puede ser difícil.

45. ¿Cuál de los siguientes describe el mejor uso del Network Access Control (NAC)?

R. El uso del Protocolo de autenticación extensible (EAP) IEEE 802.1X para autenticar los puntos de conexión antes de permitirles unirse a una red

B. El uso combinado de una infraestructura de clave pública (PKI) y un módulo de plataforma segura de hardware (TPM) para realizar la autenticación de punto de conexión basada en certificados y establecer un vínculo seguro a través del intercambio de claves simétricas

C. La combinación de EAP para la autenticación de punto final y la autenticación de usuario multifactor para el control altamente granular

D. El uso de EAP tanto para la autenticación de punto final como para la inspección de los niveles de parches del sistema operativo de punto final y las actualizaciones antimalware, con el objetivo de colocar sistemas que no son de confianza en un segmento VLAN en cuarentena

46. ¿Cuál es la mayor debilidad, y por lo tanto preocupación, con las redes virtualizadas?

R. Dado que las tarjetas de interfaz de red (NIC) están virtualizadas (vNICs), los datos que viajan entre ellos simplemente se copian de una ubicación de memoria a otra mediante la capa de hipervisor en un único host físico.

B. La ausencia de una red física hace imposible implementar firewalls o sistemas de detección de intrusiones para regular y supervisar el tráfico entre los sistemas virtuales.

C. Las redes virtuales son esencialmente nubes sin topologías bien definidas. Esto hace que las rutas de acceso de red entre sistemas virtuales sean imposibles de saber.

D. Las NIC virtuales tienen rendimientos mucho más altos que los físicos. Como resultado, los modernos sistemas de detección de intrusiones basados en red (NIDS) no pueden inspeccionar su tráfico a velocidades en tiempo real.

CLAVE DE RESPUESTA RÁPIDA

1. D

2. un

3. C

4. un

5. un

6. B

7 . C

8 . un

9 . un

10. A

11. C

12. A

13. C

14. B

15. C

16. A

17. D

18. B

19. C

20. A

21. B

22. D

23. D

24. C

25. B

26. A

27. C

28. A

29. D

30. A

31. C

32. A

33. D

34. A

35. A

36. A

37. B

38. C

39. C

40. D

41. B

42. A

43. B

44. C

45. D

46. A

RESPUESTAS A

1 . La capa 2 del modelo OSI tiene dos subcapas. ¿Cuáles son esas subcapas y cuáles son dos estándares IEEE que describen las tecnologías en esa capa?

R. LCL y MAC; IEEE 802.2 y 802.3

B. LCL y MAC; IEEE 802.1 y 802.3

C. Red y MAC; IEEE 802.1 y 802.3

D. LLC y MAC; IEEE 802.2 y 802.3

☑ **D.** La capa de enlace de datos, o capa 2, del modelo OSI es responsable de agregar un encabezado y un remolque a un paquete para preparar el paquete para la red de área local o el formato binario de tecnología de red de área amplia para la transmisión de línea adecuada. La capa 2 se divide en dos subcapas funcionales. La subcapa superior es el Logical Link Control (LLC) y se define en la especificación IEEE 802.2. Se comunica con la capa de red, que está inmediatamente por encima de la capa de enlace de datos. Debajo de la LLC está

la subcapa media access control (MAC), que especifica la interfaz con los requisitos de protocolo de la capa física. Por lo tanto, la especificación para esta capa depende de la tecnología de la capa física. La especificación IEEE MAC para Ethernet es 802.3, token ring es 802.5, la LAN inalámbrica es 802.11, y así sucesivamente. Cuando usted ve una referencia a un estándar IEEE, tales como 802.11 o 802.16, se refiere al protocolo que trabaja en la subcapa MAC de la capa de link de datos de la pila de protocolos.

☒ **A** es incorrecto porque LCL es un distracter. El acrónimo correcto para la subcapa superior de la capa de enlace de datos es LLC. Significa el Control de vínculos lógicos. Al proporcionar mecanismos de multiplexación y control de flujo, la LLC permite la coexistencia de protocolos de red dentro de una red multipunto y su transporte a través de los mismos medios de red.

☒ **B** es incorrecto porque LCL es un distracter. Las subcapas de la capa de link de datos son el Logical Link Control (LLC) y el Media Access Control (MAC). Además, la LLC se define en la especificación IEEE 802.2, no en 802.1. Las especificaciones IEEE 802.1 se refieren a capas de protocolo por encima de las capas MAC y LLC. Aborda la arquitectura LAN/MAN, la administración de redes, el trabajo por Internet entre LAN y WANs y la seguridad de los enlaces.

☒ **C** es incorrecto porque la red no es una subcapa de la capa de vínculo de datos. Las subcapas de la capa de link de datos son el Logical Link Control (LLC) y el Media Access Control (MAC). El LLC se encuentra entre la capa de red (la capa inmediatamente por encima de la capa de enlace de datos) y la subcapa MAC. Además, la LLC se define en la especificación IEEE 802.2, no en IEEE 802.1. Como se acaba de explicar, los estándares 802.1 abordan áreas de arquitectura LAN/MAN, administración de redes, internet entre LAN y WANs, y seguridad de enlaces.

2 . ¿Cuál de las siguientes no es una contramedida efectiva contra el spam?

R. Abrir servidores de retransmisión de correo

B. Servidores de retransmisión de correo configurados correctamente

C. Filtrado en una puerta de enlace de correo electrónico

D. Filtrado en el cliente

☑ **R.** Un servidor de retransmisión de correo abierto no es una contramedida efectiva contra el spam; de hecho, los spammers a menudo los utilizan para distribuir spam, ya que permiten a un atacante enmascarar su identidad. Una retransmisión de correo abierto es un servidor SMTP que está configurado para permitir conexiones SMTP entrantes de cualquier persona y a cualquier persona en Internet. Así es como se creó Internet originalmente, pero muchos relés ahora están configurados correctamente para evitar que los atacantes los usen para distribuir spam o pornografía.

☒ **B** es incorrecto porque un servidor de retransmisión de correo configurado correctamente solo permite que el correo electrónico destinado o originario de usuarios conocidos pase a través de él. De esta manera, un servidor de retransmisión de correo cerrado ayuda a evitar la distribución de spam. Para que se considere cerrado, se debe configurar un servidor SMTP para aceptar y reenviar mensajes de direcciones IP locales a buzones locales, desde direcciones IP locales hasta buzones no locales, desde direcciones IP conocidas y de confianza hasta buzones locales y desde clientes autenticados y autorizados. Los servidores que quedan abiertos se consideran el resultado de una mala administración de sistemas.

☒ **C** es incorrecto porque la implementación de filtros de spam en una puerta de enlace de correo electrónico es la contramedida más común contra el spam. Hacerlo ayuda a proteger la capacidad de red y servidor, reduce el riesgo de que se descarte el correo electrónico legítimo y ahorra tiempo a los usuarios. Una serie de filtros de spam comerciales basados en una variedad de algoritmos están disponibles. El software de filtrado acepta el correo electrónico como su entrada y reenvía el mensaje sin cambios al destinatario, redirige el mensaje para su entrega en otro lugar o descarta el mensaje.

☒ **D** es incorrecto porque filtrar en el cliente es una contramedida contra el spam. De hecho, el filtrado puede tener lugar en la puerta de enlace, que es el método más popular, en el servidor de correo electrónico o en el cliente. También hay diferentes métodos de filtrado. El filtrado basado en palabras clave fue una vez un método popular, pero desde entonces se ha vuelto obsoleto porque es propenso a falsos positivos y puede ser evitado fácilmente por los spammers. Ahora se utilizan filtros más sofisticados. Estos se basan en el análisis estadístico o el análisis de patrones de tráfico de correo electrónico.

3 . Robert es responsable de implementar una arquitectura común utilizada cuando los clientes necesitan acceder a información confidencial a través de conexiones a Internet. ¿Cuál de los siguientes describe mejor este tipo de arquitectura?

R. Modelo de dos niveles

B. Subred proyectada

C. Modelo de tres niveles

D. Zonas DNS públicas y privadas

☑ **C.** Muchas de las arquitecturas de comercio electrónico actuales utilizan un enfoque arquitectónico de tres niveles. La arquitectura de tres niveles es una arquitectura cliente/servidor en la que la interfaz de usuario, la lógica de procesos funcionales y el almacenamiento de datos se ejecutan como componentes independientes que se desarrollan y mantienen, a menudo en plataformas independientes. La arquitectura de tres niveles permite actualizar o

modificar cualquiera de los niveles según sea necesario sin afectar a los otros dos niveles debido a su modularidad. En el caso del comercio electrónico, la capa de presentación es un servidor web front-end con el que interactúan los usuarios. Puede servir contenido dinámico estático y almacenado en caché. La capa de lógica de negocios es donde se reformatea y procesa la solicitud. Normalmente, se trata de un servidor de aplicaciones dinámico de procesamiento de contenido y de nivel de generación. El almacenamiento de datos es donde se mantienen los datos confidenciales. Es una base de datos back-end que contiene los datos y el software del sistema de administración de bases de datos que se utiliza para administrar y proporcionar acceso a los datos. Los niveles independientes se pueden conectar con middleware y ejecutarse en servidores físicos independientes.

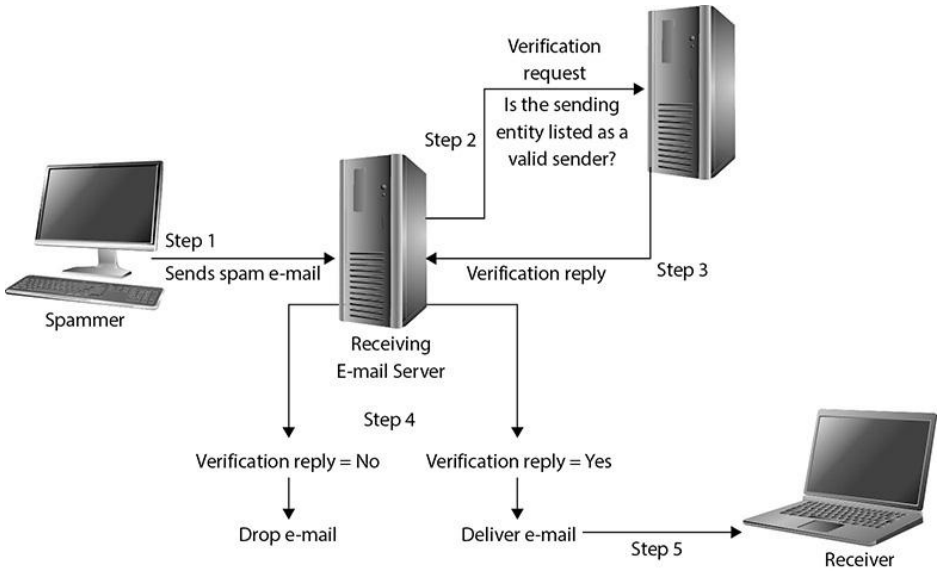
A es incorrecto porque dos niveles, o cliente/servidor, describe una arquitectura en la que un servidor proporciona servicios a uno o varios clientes que solicitan esos servicios. Muchas de las aplicaciones empresariales y protocolos de Internet actuales utilizan el modelo cliente/servidor. Esta arquitectura utiliza dos sistemas: un cliente y un servidor. El cliente es de un nivel y el servidor es otro nivel, de ahí la arquitectura de dos niveles. Cada instancia del software cliente está conectada a uno o varios servidores. El cliente envía su solicitud de información a un servidor, que procesa la solicitud y devuelve los datos al cliente. Una arquitectura de tres niveles es un mejor enfoque para proteger la información confidencial cuando las solicitudes llegan desde Internet. Proporciona un nivel adicional que un atacante debe aprovechar para obtener acceso a los datos confidenciales que se mantienen en el servidor back-end.

B es incorrecto porque una arquitectura de host con pantalla significa que hay un firewall para proteger un servidor, que es básicamente una arquitectura de un nivel. Un firewall externo y orientado al público examina las solicitudes procedentes de una red que no es de confianza como en Internet. Si el único nivel, el único firewall, se ve comprometido, el atacante puede obtener acceso a los datos confidenciales que residen en el servidor con relativa facilidad.

D es incorrecto porque al separar los servidores DNS en servidores públicos y privados proporciona protección, no es una arquitectura real utilizada para el propósito solicitado en la pregunta. Las organizaciones deben implementar DNS dividido (de cara pública y privada), lo que significa que un servidor DNS de la DMZ controla las solicitudes de resolución externas, mientras que un servidor DNS interno solo controla las solicitudes internas. Esto ayuda a garantizar que el DNS interno tenga capas de protección y no esté expuesto a conexiones a Internet.

4. Desde el envío de spam (mensajes no deseados) ha aumentado con los años y el correo electrónico se ha convertido en una forma común de enviar enlaces maliciosos y malware, la industria ha desarrollado diferentes maneras de combatir estos problemas. Un enfoque es usar un marco de directivas de

remitente, que es un sistema de validación de correo electrónico. En el gráfico siguiente, ¿qué tipo de sistema recibe la solicitud en el paso 2 y responde en el paso 3?



R. Servidor DNS

B. Servidor de correo electrónico

C. Servidor RADIUS

D. Servidor de autenticación

☑ **R.** Sender Policy Framework (SPF) es un sistema de validación de correo electrónico diseñado para prevenir el spam y el correo electrónico malintencionado mediante la detección de suplantación de correo electrónico. Los atacantes suelen suplantar direcciones de correo electrónico para tratar de engañar al receptor haciéndoles creer que el mensaje provenía de una fuente conocida y de confianza. SPF permite a los administradores de red especificar qué hosts pueden enviar correo desde un dominio determinado mediante la implementación de un registro SPF en el sistema de nombres de dominio (DNS). El servidor de correo electrónico está configurado para comprobar con el servidor DNS para comprobar que un correo electrónico procedente de un dominio específico se envió desde una dirección IP que ha sido sancionada por el administrador del dominio de envío. En el gráfico, el paso 2 es el servidor de correo electrónico que envía esta solicitud de validación a un servidor DNS y el paso 4 ilustra el proceso de validación resultante que se sigue.

☒ **B** es incorrecto porque el servidor de correo electrónico se está representando entre los pasos 1 y 2. El gráfico muestra cómo se envía un correo electrónico a un servidor de correo electrónico en un dominio específico. El servidor de correo electrónico está configurado para comprobar que el mensaje procede de un host que puede enviarlo comprobando con el servidor DNS del dominio de origen. Si el servidor DNS tiene un registro que indica que se permite el correo electrónico del host de envío, el servidor de correo electrónico reenviará el mensaje al

destino previsto. La dirección del remitente se envía al principio de una transmisión del Protocolo simple de transferencia de correo (SMTP). Si el servidor de correo electrónico rechaza el correo electrónico desde esa dirección específica, el cliente de envío recibirá un mensaje de rechazo. Si el cliente está retransmitiendo el mensaje en nombre de otra entidad (agente de transferencia de mensajes), se envía un mensaje rebotado a la dirección de envío original. SPF se ocupa de la suplantación de correo electrónico y no puede detectar ni prevenir la falsificación de direcciones de correo electrónico. Los atacantes suelen utilizar la suplantación de correo electrónico para llevar a cabo ataques de phishing con el objetivo de obtener información privada o confidencial de la víctima.

C es incorrecto porque radius no está implicado con este tipo de verificación. El servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un protocolo de red que proporciona la funcionalidad centralizada de autenticación, autorización y contabilidad (AAA) para los usuarios finales individuales que necesitan conectarse a un sistema remoto o a una red. RADIUS es un marco de autenticación utilizado para autenticar usuarios, no nombres de dominio o entidades de envío de correo electrónico. RADIUS es un protocolo cliente/servidor que se utiliza comúnmente con servidores de acceso a la red (NAS), servidores de acceso remoto (RAS) y autenticación de puertos 802.1X.

D es incorrecto porque el gráfico ilustra cómo un servidor DNS forma parte del proceso de validación de SPF. El servidor DNS no es un servidor de autenticación. Un servidor DNS contiene registros que contienen principalmente asignaciones de IP a nombre de host. En una configuración de SPF, el servidor DNS tendría un registro que indica qué servidores de envío puede aceptar el servidor de correo electrónico receptor, que es configurado por el administrador de red. SPF es necesario porque el Protocolo simple de transferencia de correo (SMTP) no tiene funcionalidad de seguridad inherente para detectar mensajes falsos. Un atacante podría suplantar una dirección de correo electrónico y esencialmente pretender ser cualquier dirección de origen, y no hay nada dentro de SMTP para identificar esta actividad. Los atacantes suelen llevar a cabo este tipo de ataque de suplantación de identidad con el objetivo de engañar a un usuario final para que acepte el mensaje y haga clic en un enlace malicioso o un archivo adjunto malicioso.

5 . ¿Cuál de los siguientes indica a un paquete a dónde ir y cómo comunicarse con el servicio o protocolo correcto en el equipo de destino?

R. enchufe

B. dirección IP

C. puerto

D. marco

☑ **R.** El Protocolo de datagramas de usuario (UDP) y el Protocolo de control de transmisión (TCP) son protocolos de transporte que las aplicaciones utilizan para obtener sus datos a través de una red. Ambos utilizan puertos para comunicarse con las capas superiores OSI y para realizar un seguimiento de varias conversaciones que tienen lugar simultáneamente. Los puertos también son el mecanismo utilizado para identificar cómo otros equipos acceden a los servicios. Cuando se forma un mensaje TCP o UDP, un origen y un puerto de destino están contenidos en la información del encabezado junto con las direcciones IP de origen y de destino. Esto conforma un socket, que es cómo los paquetes saben a dónde ir —por la dirección— y cómo comunicarse con el servicio o protocolo correcto en el otro equipo— por el número de puerto. La dirección IP actúa como puerta de acceso a un ordenador, y el puerto actúa como puerta al protocolo o servicio real. Para comunicarse correctamente, el paquete necesita conocer estas puertas.

☒ **B** es incorrecto porque una dirección IP no indica a un paquete cómo comunicarse con un servicio o protocolo. El propósito de una dirección IP es la identificación de la interfaz de host o de red y el direccionamiento de ubicación. Cada nodo de una red tiene una dirección IP única. Esta información, junto con los puertos de origen y destino, constituye un socket. La dirección IP indica el paquete a dónde ir, y el puerto indica cómo comunicarse con el servicio o protocolo correcto.

☒ **C** es incorrecto porque el puerto dice solamente el paquete cómo comunicarse con el servicio o protocolo correcto. No le dice al paquete a dónde ir. La dirección IP proporciona esta información. Un puerto es un punto de conexión de comunicaciones utilizado por los protocolos IP como TCP y UDP. Los puertos se identifican por un número. También están asociados con una dirección IP y un protocolo utilizado para la comunicación.

☒ **D** es incorrecto porque frame es el término utilizado para hacer referencia a un datagrama después de que se le dé un encabezado y un finalizador en la capa de enlace de datos. Se forma un mensaje y se pasa a la capa de aplicación desde un programa y se envía a través de la pila de protocolos. Cada protocolo de cada capa agrega su propia información (encabezados y finalizadores) al mensaje y la pasa al siguiente nivel. A medida que el mensaje se transmite por la pila, pasa por una especie de evolución, y cada etapa tiene un nombre específico que indica lo que está ocurriendo. Cuando una aplicación da formato a los datos que se transmitirán a través de la red, los datos se denominan mensaje. El mensaje se envía a la capa de transporte, donde TCP hace su magia en los datos. El conjunto de datos es ahora un segmento. El segmento se envía a la capa de red. La capa de red agrega enrutamiento y direccionamiento, y ahora el paquete se denomina datagrama. La capa de red pasa el datagrama a la capa de vínculo de datos, que enmarca el datagrama con un encabezado y un finalizador, y ahora se denomina fotograma.

6 . Varios protocolos de tunelización diferentes se pueden utilizar en situaciones de acceso telefónico. ¿Cuál de los siguientes sería mejor utilizar como una solución de tunelización VPN?

R. L2P

B. PPTP

C. IPSec

D. L2TP

☑ **B.** Una red privada virtual (VPN) es una conexión privada segura a través de una red pública o un entorno no seguro. Es una conexión privada porque los protocolos de cifrado y tunelización se utilizan para garantizar la confidencialidad e integridad de los datos en tránsito. Es importante recordar que la tecnología VPN requiere un túnel para funcionar, y asume el cifrado. Los protocolos que se pueden utilizar para los VPN son el Point-to-Point Tunneling Protocol (PPTP), la Seguridad del Protocolo de Internet (IPSec) y el Protocolo de tunelización de la capa 2 (L2TP). PPTP, un protocolo de Microsoft, permite a los usuarios remotos configurar una conexión PPP a un ISP local y luego crear una VPN segura a su destino. PPTP ha sido el protocolo de tunelización estándar de facto de la industria durante años, pero el nuevo estándar de facto para las VPN es IPSec. PPTP está diseñado para la conectividad cliente/servidor y establece una única conexión punto a punto entre dos equipos. Funciona en la capa de enlace de datos y transmite solamente a través de redes IP.

☒ **A** es incorrecto porque L2P no existe. Esta es una respuesta distraída.

☒ **C** es incorrecto porque aunque IPSec es uno de los tres protocolos de tunelización VPN primarios, no se utiliza sobre las conexiones de acceso telefónico. Sólo admite redes IP y funciona en la capa de red, proporcionando seguridad además de IP. IPSec controla varias conexiones al mismo tiempo y proporciona autenticación y cifrado seguros.

☒ **D** es incorrecto porque el L2TP no es un protocolo de tunelización que trabaja sobre una conexión de acceso telefónico. L2TP es un protocolo de tunelización que puede extender una VPN sobre varios tipos de red WAN (IP, X.25, frame relay). Un híbrido de L2F y PPTP, L2TP trabaja en la capa del link de datos y transmite sobre múltiples tipos de redes, no sólo IP. Sin embargo, se debe combinar con IPSec para la seguridad, por lo que no se considera una solución VPN por sí mismo.

7 . ¿Cuál de los siguientes describe correctamente Bluejacking?

R. El bluejacking es un ataque dañino y malicioso.

B. Es el proceso de hacerse cargo de otro dispositivo portátil a través de un dispositivo habilitado para Bluetooth.

C. Se utiliza comúnmente para enviar información de contacto.

D. El término fue acuñado por el uso de un dispositivo Bluetooth y el acto de secuestrar otro dispositivo.

☑ **C.** Bluetooth es vulnerable a un ataque llamado Bluejacking, que implica que un atacante envíe un mensaje no solicitado a un dispositivo que está habilitado para Bluetooth. Los bluejackers buscan un dispositivo receptor, como un dispositivo móvil o un portátil, y luego le envían un mensaje. A menudo, el Bluejacker está tratando de enviar su tarjeta de visita para ser añadido a la lista de contactos de la víctima en su libreta de direcciones. La contramedida consiste en poner el dispositivo habilitado para Bluetooth en modo nocuperable para que otros no puedan identificar este dispositivo en primer lugar. Si recibe algún tipo de mensaje de esta manera, simplemente mire a su alrededor. Bluetooth sólo funciona a una distancia de 10 metros, por lo que viene de alguien cerca.

☒ **A** es incorrecto porque Bluejacking es en realidad una molestia inofensiva en lugar de un ataque malicioso. Es el acto de enviar mensajes no solicitados a dispositivos habilitados para Bluetooth. El primer acto tuvo lugar en un banco en el que el atacante sondeó la red y encontró un teléfono Nokia activo. Luego envió el mensaje "Buy Ericsson".

☒ **B** es incorrecto porque Bluejacking no implica hacerse cargo de otro dispositivo. No da al atacante el control del dispositivo de destino. Más bien, el Bluejacker simplemente envía un mensaje no solicitado al dispositivo habilitado para Bluetooth. Estos mensajes suelen ser sólo texto, pero también es posible enviar imágenes o sonidos. Las víctimas a menudo no están familiarizadas con bluejacking y pueden pensar que su teléfono está funcionando mal o que han sido atacados por un virus o secuestrados por un caballo de Troya.

☒ **D** es incorrecto porque el término Bluejacking no tiene nada que ver con el secuestro, lo que significa hacerse cargo de algo. El nombre Bluejacking fue inventado por un consultor de TI malasio que envió el mensaje "Buy Ericsson" a otro dispositivo habilitado para Bluetooth.

8 . DNS es un objetivo popular para los atacantes debido a su papel estratégico en Internet. ¿Qué tipo de ataque utiliza consultas recursivas para envenenar la memoria caché de un servidor DNS?

R. Secuestro de DNS

B. Manipulación del archivo hosts

C. Ingeniería social

D. Litigio de dominio

☑ **R.** DNS desempeña un papel estratégico en la transmisión del tráfico en Internet. El DNS dirige el tráfico a la dirección adecuada asignando nombres de dominio a sus direcciones IP correspondientes. Las consultas DNS se pueden clasificar como recursivas o iterativas. En una consulta recursiva, el servidor DNS a menudo reenvía la consulta a otro servidor y devuelve la respuesta adecuada al investigador. En una consulta iterativa, el servidor DNS responde con una dirección para otro servidor DNS que podría responder a la pregunta y, a continuación, el cliente procede a preguntar al nuevo servidor DNS. Los atacantes usan consultas recursivas para envenenar la memoria caché de un servidor DNS. De esta manera, los atacantes pueden apuntar sistemas a un sitio web que controlan y que contiene malware o alguna otra forma de ataque. Así es como funciona: Un atacante envía una consulta recursiva a un servidor DNS de la víctima que solicita la dirección IP del dominio www.logicalsecurity.com (http://www.logicalsecurity.com). El servidor DNS reenvía la consulta a otro servidor DNS. Sin embargo, antes de que el otro servidor DNS responda, el atacante inyecta su propia dirección IP. El servidor víctima acepta la dirección IP y la almacena en su caché durante un período de tiempo específico. La próxima vez que un sistema consulta el servidor para resolver www.logicalsecurity.com (http://www.logicalsecurity.com) a su dirección IP, el servidor dirigirá a los usuarios a la dirección IP del atacante. Esto se denomina suplantación de DNS o intoxicación por DNS.

☒ **B** es incorrecto porque la manipulación del archivo hosts no utiliza consultas recursivas para envenenar la memoria caché de un servidor DNS. Un cliente consulta primero un archivo hosts antes de emitir una solicitud a un servidor DNS. Algunos virus añaden direcciones IP no válidas de los proveedores antivirus al archivo hosts para evitar la descarga de definiciones de virus y evitar la detección. Este es un ejemplo de manipulación del archivo hosts.

☒ **C** es incorrecto porque la ingeniería social no implica consultar un servidor DNS. La ingeniería social se refiere a la manipulación de individuos con el propósito de obtener acceso o información no autorizados. La ingeniería social aprovecha el deseo de las personas de ser útiles y/o confiadas. Es un ataque no tecnológico que puede utilizar la tecnología en su ejecución. Por ejemplo, un atacante podría hacerse pasar por administrador de un usuario y enviarle un correo electrónico falso solicitando la contraseña a una aplicación. Es probable que el usuario, que desea ayudar y mantener el favor de su administrador, proporcione la contraseña.

☒ **D** es incorrecto porque los litigios de dominio no implican envenenar la caché de un servidor DNS. Los nombres de dominio están sujetos a riesgos de marca comercial, incluida la falta de disponibilidad temporal o la pérdida permanente de un nombre de dominio establecido. Una empresa víctima podría perder toda su presencia en Internet como resultado de litigios de dominio. Las organizaciones interesadas sobre la posibilidad de disputas de marcas relacionadas con sus nombres de dominio deben establecer planes de

contingencia. Por ejemplo, una empresa puede establecer un segundo dominio no relacionado que todavía puede representar el nombre de la empresa.

9 . Las redes de telefonía IP requieren las mismas medidas de seguridad que las implementadas en una red de datos IP. ¿Cuál de los siguientes es exclusivo de la telefonía IP?

R. Limitar las sesiones ip que pasan por puertas de enlace de medios

B. Identificación de dispositivos falsos

C. Implementación de la autenticación

D. Cifrado de paquetes que contienen información confidencial

☑ **R.** Una puerta de enlace de medios es la unidad de traducción entre redes de telecomunicaciones dispares. Las puertas de enlace de medios VoIP realizan la conversión entre la voz de multiplexación por división de tiempo (TDM) al Protocolo de Voz sobre Internet (VoIP). Como medida de seguridad, el número de llamadas a través de puertas de enlace de medios debe limitarse. De lo contrario, las puertas de enlace de medios son vulnerables a ataques de denegación de servicio, secuestros y otros tipos de ataques.

☒ **B** es incorrecto porque es necesario identificar dispositivos no fiables tanto en la telefonía IP como en las redes de datos. En las redes de telefonía IP, es necesario buscar específicamente teléfonos IP rogue y softphones. Rogue significa que estos dispositivos no están autorizados. Por lo tanto, no son administrados o protegidos por TI y pueden introducir un riesgo adicional para la red. Un dispositivo rogue común que se encuentra en las redes de datos son los puntos de acceso inalámbricos. Un punto de acceso rogue puede proporcionar una entrada a la red para usuarios no autorizados.

☒ **C** es incorrecto porque se recomienda la autenticación para los datos y las redes de voz. En ambos casos, la autenticación le permite registrar usuarios y equipos en la red para que pueda verificar que son quienes dicen ser cuando intentan conectarse a la red. La autenticación también le permite denegar el acceso a usuarios y dispositivos que no están autorizados.

☒ **D** es incorrecto porque los datos confidenciales se pueden transmitir en una red de voz o datos y deben cifrarse en ambos casos. Espiar es una amenaza muy real para las redes VoIP. Considere todas las reuniones de ventas, reuniones de gestión, reuniones financieras, etc., que se llevan a cabo por teléfono. Cada palabra que se habla en esas reuniones es vulnerable a espiar. Cifrar datos de voz es una de las mejores maneras de proteger estos datos confidenciales.

10. Angela quiere agrupar computadoras por departamento para facilitarles el uso compartido de recursos de red. ¿Cuál de los siguientes le permitirá agrupar computadoras lógicamente?

R. VLAN

B. Arquitectura de red abierta

C. intranet

D. furgoneta

☑ **R.** Las LAN virtuales (VLAN) permiten la separación lógica y la agrupación de equipos en función de los requisitos de recursos, la seguridad o las necesidades empresariales a pesar de la ubicación física estándar de los sistemas. Esta tecnología permite a Angela colocar lógicamente todos los equipos dentro del mismo departamento en la misma red VLAN para que todos los usuarios puedan recibir los mismos mensajes de difusión y puedan acceder a los mismos tipos de recursos, independientemente de su ubicación física. Esto significa que los equipos se pueden agrupar incluso si no se encuentran en la misma red.

☒ **B** es incorrecto porque la arquitectura de red abierta describe tecnologías que pueden conformar una red. Es uno que ningún proveedor posee, que no es propietario, y que puede integrar fácilmente varias tecnologías e implementaciones de proveedores de esas tecnologías. El modelo OSI proporciona un marco para desarrollar productos que funcionarán dentro de una arquitectura de red abierta. Los proveedores utilizan el modelo OSI como blueprint y desarrollan sus propios protocolos e interfaces para generar funcionalidades distintas a las de otros proveedores. Sin embargo, dado que estos proveedores utilizan el modelo OSI como su lugar de partida, la integración de otros productos de proveedor es una tarea más sencilla y los problemas de interoperabilidad son menos gravosos que si los proveedores hubieran desarrollado su propio marco de trabajo de red desde cero.

☒ **C** es incorrecta porque una intranet es una red privada que una empresa utiliza cuando desea usar Internet y tecnologías basadas en web para redes internas. La empresa tiene servidores web y equipos cliente que utilizan navegadores web y utiliza el conjunto de protocolos TCP/IP. Las páginas web están escritas en HTML o XML y se accede a ellas a través de HTTP.

☒ **D** es incorrecta porque una red de valor agregado (VAN) es una infraestructura de intercambio electrónico de datos (EDI) desarrollada y mantenida por una oficina de servicio. Este es un ejemplo de cómo funciona una VAN: una tienda minorista como Target realiza un seguimiento de su inventario haciendo que los empleados analicen códigos de barras en artículos individuales. Cuando el inventario de un artículo, como mangueras de jardín, se vuelve bajo, un empleado envía una solicitud de más mangueras de jardín. La solicitud va a un buzón en un VAN que Target paga por usar y, a continuación, la solicitud se envían al proveedor de mangueras de jardín. Dado que Target trata con miles de proveedores, el uso de un VAN simplifica el proceso de pedido. No es necesario rastrear manualmente al proveedor adecuado y enviar un pedido de compra.

11. ¿Cuál de las siguientes describe incorrectamente cómo se lleva a cabo el enrutamiento comúnmente en Internet?

R. El EGP se utiliza en las áreas "entre" cada AS.

B. Las regiones de nodos que comparten características y comportamientos se denominan AS.

C. Los CA son nodos específicos que son responsables de enrutar a nodos fuera de su región.

D. Cada AS utiliza el IGP para realizar la funcionalidad de ruteo.

☑ **C.** Una CA, o entidad de certificación, es un tercero de confianza que proporciona certificados digitales para su uso en una infraestructura de clave pública. Los CA no tienen nada que ver con el enrutamiento. Un entorno PKI proporciona un modelo de confianza jerárquico, pero no trata con el enrutamiento del tráfico.

☒ **A** es incorrecta porque la instrucción es true. El Protocolo de puerta de enlace exterior (EGP) funciona entre cada sistema autónomo (AS). La arquitectura de Internet que soporta estos diversos AS se crea para que ninguna entidad que necesite conectarse a un AS específico tenga que conocer o comprender los protocolos interiores que se pueden utilizar. En su lugar, para que los AS se comuniquen, solo tienen que estar usando los mismos protocolos de enrutamiento exterior.

☒ **B** es incorrecta porque la instrucción es true; las regiones de nodos (redes) que comparten características y comportamientos se denominan sistemas autónomos (AS). Estos AS están controlados independientemente por diferentes corporaciones y organizaciones. Un AS se compone de ordenadores y dispositivos, que son administrados por una sola entidad y utilizan un Protocolo de puerta de enlace interior común (IGP). Los límites de estos AS están delineados por los routers de borde. Estos Routers conectan con el routers de borde de otros AS y funcionan con los protocolos de ruteo interior y exterior. Los routers internos conectan con otros routers dentro del mismo AS y funcionan con los protocolos de ruteo interior. Así que, en realidad, Internet es sólo una red formada por ASs y routing protocols.

☒ **D** es incorrecto porque un Interior Gateway Protocol (IGP) maneja las tareas de ruteo dentro de cada AS. Hay dos categorías de IGPs: protocolos de ruteo de vectores de distancia y protocolos de ruteo de estado de link. Los Protocolos de ruteo vectoriales a distancia incluyen el Routing Information Protocol (RIP) y el Interior Gateway Routing Protocol (IGRP). Los routers que utilizan estos protocolos no poseen información sobre toda la topología de red. Los nodos que utilizan protocolos de enrutamiento de estado de vínculo, por otro lado, poseen información sobre la topología de red completa. Algunos ejemplos de estos protocolos incluyen open shortest path first (OSPF) y Intermediate System to Intermediate System (IS-IS).

12. Tanto los protocolos interiores de facto como los propios están en uso hoy en día. ¿Cuál de los siguientes es un protocolo interior propietario que elige la mejor ruta entre la fuente y el destino?

R. IGRP

B. SI1

C. Bgp

D. Ospf

☑ **R.** El Interior Gateway Routing Protocol (IGRP) es un Protocolo de ruteo de vectores de distancia que fue desarrollado por, y es propietario de, Cisco Systems. Mientras que el Routing Information Protocol (RIP) utiliza un criterio para encontrar la mejor trayectoria entre la fuente y el destino, el IGRP utiliza cinco criterios para tomar una decisión de "mejor ruta". Un administrador de red puede establecer ponderaciones en estas métricas diferentes para que el protocolo funcione mejor en ese entorno específico.

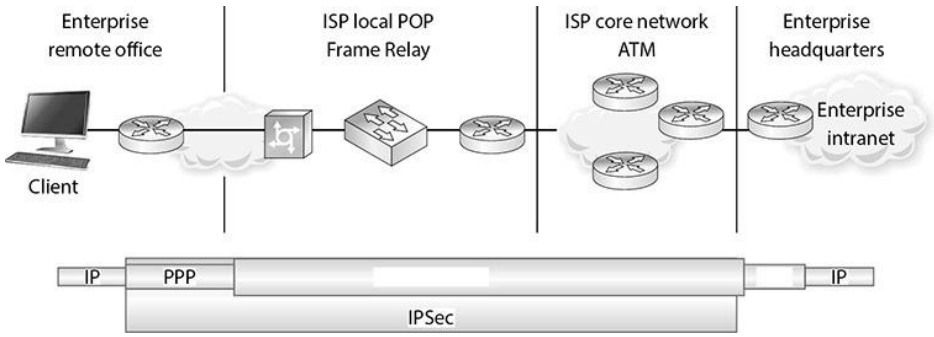
☒ **B** es incorrecto porque el Routing Information Protocol (RIP) no es propietario. El RIP es un estándar que describe cómo los routers intercambian los datos de la tabla de ruteo y se considera un protocolo de vector de distancia, lo que significa que calcula la distancia más corta entre la fuente y el destino. Se considera un protocolo heredado, debido a su rendimiento lento y la falta de funcionalidad. Sólo debe utilizarse en redes pequeñas. Rip versión 1 no tiene autenticación, y RIP versión 2 envía contraseñas en texto claro o hash con MD5.

☒ **C** es incorrecto porque el Border Gateway Protocol (BGP) es un Protocolo de puerta de enlace exterior (EGP). BGP permite a los Routers en diferentes ASs compartir la información de ruteo para garantizar un enrutamiento eficaz y eficiente entre las diferentes redes. BGP es comúnmente utilizado por los proveedores de servicios de Internet para enrutar los datos de una ubicación a la siguiente en Internet.

☒ **D** es incorrecto porque Open Shortest Path First (OSPF) no es propietario. OSPF utiliza algoritmos de estado de vínculo para enviar información de tabla de ruteo. El uso de estos algoritmos permite que se lleven a cabo actualizaciones de tablas de enrutamiento más pequeñas y frecuentes. Esto proporciona una red más estable que rip, pero requiere más memoria y recursos de CPU para admitir este procesamiento adicional. OSPF permite una red jerárquica de enrutamiento que tiene un vínculo de estructura básica que conecta todas las subredes juntas. OSPF es el protocolo preferido y ha reemplazado el RIP en muchas redes hoy en día. La autenticación puede tener lugar con contraseñas de texto claro o contraseñas hash, o usted puede elegir configurar ninguna autenticación en el Routers usando este protocolo.

13. Cuando un sistema necesita enviar datos a un usuario final, es posible que esos datos tengan que viajar a través de diferentes protocolos de red para llegar

al destino. Los diferentes tipos de protocolo dependen de hasta qué punto geográficamente deben viajar los datos, los tipos de dispositivos intermedios implicados y cómo estos datos deben protegerse durante la transmisión. En el gráfico siguiente, ¿qué dos protocolos WAN faltan y cuál es el mejor razonamiento para su funcionalidad en el escenario de transmisión que se está ilustrando?



A. PPTP se está utilizando ya que el tráfico necesita viajar sobre diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones multiplexado.

B. L2FP se está utilizando ya que el tráfico necesita viajar a través de diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones en serie.

C. L2TP se está utilizando ya que el tráfico necesita viajar sobre diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones en serie.

D. El modo de túnel IPSec se está utilizando ya que el tráfico necesita viajar sobre diferentes tecnologías WAN. Ppp se está utilizando porque la "última pierna" de la transmisión es sobre un link de telecomunicaciones multiplexado.

☑ **C.** El Protocolo punto a punto (PPP) es un protocolo de link de datos que lleva a cabo el encuadre y la encapsulación para las conexiones punto a punto. Los dispositivos de telecomunicaciones utilizan comúnmente ppp como su protocolo de link de datos, que encapsula los datos que se enviarán a través de enlaces de conexión serie. El Protocolo de tunelización de la capa 2 (L2TP) se utiliza cuando una conexión PPP necesita ser extendida a través de una red WAN no basada en IP. Túneles L2TP tráfico PPP sobre diversos tipos de red tales como ATM y Frame Relay. Esto significa que cuando dos redes están conectadas por links WAN, el dispositivo de puerta de enlace de cada red (es decir, el router de borde) se configura para utilizar el L2TP. Cuando el sistema de puerta de enlace de destino recibe los datos sobre el L2TP, "desenvuelce" los paquetes quitando los encabezados L2TP y envía los paquetes sobre la siguiente etapa de la transmisión, que en este gráfico es un link de telecomunicaciones usando el PPP.

A es incorrecto porque el PPTP se utiliza cuando una conexión PPP necesita ser extendida a través de una red basada en IP. PPTP no trabaja sobre las redes no IP tales como Frame Relay y ATM. PPTP es un protocolo más antiguo que no se utiliza para transmitir los datos sobre los links WAN complejos no IP tal y como se muestra en de este gráfico. PPTP utiliza la encapsulación de ruteo genérico (GRE) y tcp para encapsular los paquetes PPP y para extender una conexión PPP a través de una red IP. La segunda parte de la respuesta indica que el PPP se utiliza para los links de telecomunicaciones multiplexados, lo cual es incorrecto porque la multiplexación tiene lugar en la capa física y es llevada a cabo por los dispositivos, no en la capa del link de datos a través de un protocolo.

B es incorrecto porque no hay ningún protocolo llamado L2FP. Esta es una respuesta distraída. L2F es el protocolo propietario del reenvío de la capa 2 de Cisco utilizado para tunelización del tráfico PPP. Este protocolo se utiliza para crear conexiones privadas virtuales seguras a través de Internet. Varias funcionalidades de los protocolos L2F y PPTP se combinaron para crear el protocolo L2TP. Los dos puntos finales de un túnel L2TP se llaman ELC (concentrador de acceso L2TP) y el LNS (servidor de red L2TP). Una vez que se establece un túnel L2TP entre los dos extremos, el tráfico de red entre los pares es bidireccional.

D es incorrecto porque IPSec sólo puede trabajar sobre redes basadas en IP y no es una tecnología WAN VPN que extiende las conexiones PPP. Para que los datos viajen a través de vínculos WAN de este tipo, es necesario utilizar un protocolo de vínculo de datos y IPSec es un protocolo de capa de red. IPSec es un conjunto de protocolos desarrollados para proteger el tráfico que viaja a través de una red IP, porque el Protocolo de Internet básico (IP) no tiene ningún tipo de funcionalidad de seguridad integrada en ella. Cuando una conexión L2TP requiere la funcionalidad de seguridad que proporciona IPSec (autenticación, integridad, confidencialidad), los protocolos L2TP e IPSec se configuran para trabajar juntos para proporcionar el nivel necesario de protección. La segunda parte de la respuesta indica que el PPP se utiliza para los links de telecomunicaciones multiplexados, lo cual es incorrecto porque la multiplexación tiene lugar en la capa física y es llevada a cabo por los dispositivos, no en la capa del link de datos a través de un protocolo.

14. ¿Cuál de las siguientes opciones NO describe la seguridad de la telefonía IP?

R. Las redes VoIP deben protegerse con los mismos controles de seguridad utilizados en una red de datos.

B. Los softphones son más seguros que los teléfonos IP.

C. Como puntos finales, los teléfonos IP pueden convertirse en el objetivo de los ataques.

D. La arquitectura actual de Internet sobre la cual se transmite la voz es menos segura que las líneas telefónicas físicas.

☑ **B.** Los softphones IP deben utilizarse con precaución. Un softphone es una aplicación de software que permite al usuario realizar llamadas telefónicas a través de un ordenador a través de Internet. Un softphone, que reemplaza el hardware dedicado, se comporta como un teléfono tradicional. Se puede utilizar con un auricular conectado a la tarjeta de sonido de un PC o con un teléfono USB. Skype es un ejemplo de una aplicación softphone. En comparación con los teléfonos IP basados en hardware, los softphones hacen que una red IP sea más vulnerable. Sin embargo, los softphones no son peores que cualquier otra aplicación interactiva de Internet. Además, el malware centrado en datos puede entrar más fácilmente en una red a través de softphones porque no separan el tráfico de voz de los datos al igual que los teléfonos IP.

☒ **A** es incorrecta porque la instrucción describe correctamente la seguridad de la red de telefonía IP. Una red de telefonía IP utiliza la misma tecnología que una red IP tradicional, solo que puede soportar aplicaciones de voz. Por lo tanto, la red de telefonía IP es susceptible a las mismas vulnerabilidades que una red IP tradicional y debe protegerse en consecuencia. Esto significa que la red de telefonía IP debe diseñarse para tener la seguridad adecuada.

☒ **C** es incorrecta porque la instrucción es true. Los teléfonos IP en una red de telefonía IP son el equivalente a una estación de trabajo en una red de datos en términos de su vulnerabilidad a atacar. Por lo tanto, los teléfonos IP deben protegerse con muchos de los mismos controles de seguridad que se implementan en una estación de trabajo tradicional. Por ejemplo, se deben cambiar las contraseñas de administrador predeterminadas. Las características de acceso remoto innecesarias deben deshabilitarse. El registro debe estar habilitado y el proceso de actualización del firmware debe estar protegido.

☒ **D** es incorrecta porque la instrucción es true. En su mayor parte, la arquitectura actual de Internet sobre la cual se transmite la voz es menos segura que las líneas telefónicas físicas. Las líneas telefónicas físicas proporcionan conexiones punto a punto, que son más difíciles de aprovechar que los túneles basados en software que componen la mayor parte de Internet. Este es un factor importante a tener en cuenta al asegurar una red de telefonía IP porque la red ahora está transmitiendo dos activos invaluables: datos y voz. No es inusual que la información de identificación personal, la información financiera y otros datos confidenciales se hablen por teléfono. Interceptar esta información a través de una red de telefonía IP es tan fácil como interceptar datos regulares. Ahora el tráfico de voz también necesita ser cifrado.

15. Cuando una organización divide las zonas de nomenclatura, los nombres de sus hosts a los que solo se puede acceder desde una intranet se ocultan de Internet. ¿Cuál de las siguientes describe mejor por qué se hace esto?

R. Para evitar que los atacantes accedan a los servidores

B. Para evitar la manipulación del archivo hosts

C. Para evitar proporcionar a los atacantes información valiosa que se puede utilizar para preparar un ataque

D. Para evitar proporcionar a los atacantes la información necesaria para la ocupación cibernética

☑ **C.** Muchas empresas tienen sus propios servidores DNS internos para resolver sus nombres de host internos. Estas empresas suelen usar también los servidores DNS en sus ISP para resolver nombres de host en Internet. Un servidor DNS interno se puede usar para resolver nombres de host en toda la red, pero normalmente se utiliza más de un servidor DNS para que la carga se pueda dividir y para que la redundancia y la tolerancia a errores estén en su lugar. Dentro de los servidores DNS, las redes se dividen en zonas. Una zona puede contener todos los nombres de host para los departamentos de marketing y contabilidad, y otra zona puede contener nombres de host para los departamentos de administración, investigación y legal. Es una buena idea dividir las zonas DNS cuando sea posible para que los nombres de hosts a los que solo se puede acceder desde una intranet no sean visibles desde Internet. Esta información es valiosa para un atacante que está planeando un ataque porque puede conducir a otra información, como la estructura de red, la estructura organizativa o los sistemas operativos del servidor.

☒ **A** es incorrecto porque esta no es la mejor respuesta para esta pregunta. Las zonas de nomenclatura se dividen para que los atacantes no puedan obtener información sobre sistemas internos, como nombres, direcciones IP, funciones, etc. Uno de los ataques secundarios después de explotar un servidor DNS podría ser acceder a un servidor de forma no autorizada, pero garantizar el acceso no autorizado solo a los servidores no es la razón principal para dividir las zonas DNS.

☒ **B** es incorrecto porque dividir las zonas de nomenclatura tiene que ver con cómo se configuran los servidores DNS para resolver nombres de host, no para manipular el archivo hosts. El archivo hosts se puede manipular por varias razones, tanto para bien como para mal. El archivo hosts siempre asigna el nombre de host localhost a la dirección IP 127.0.0.1 (esta es la interfaz de red de loopback, que se definió originalmente en RFC 3330), así como otros hosts. Algunos virus agregan direcciones IP no válidas de proveedores antivirus al archivo hosts para evitar la detección. Al agregar direcciones IP visitadas con frecuencia al archivo hosts, puede aumentar la velocidad de navegación web. También puede bloquear el spyware y las redes publicitarias agregando listas de sitios de spyware y red publicitaria al archivo hosts y mapeándolos a la interfaz de red de bucle invertido. De esta manera, estos sitios siempre apuntan a la máquina del usuario y no se puede llegar a los sitios.

☒ **D** es incorrecto porque los piratas informáticos no necesitan información en un servidor DNS para llevar a cabo la ocupación cibernética. La ocupación

cibernética ocurre cuando un atacante compra una marca conocida o nombre de empresa, o variación de la misma, como un nombre de dominio con el objetivo de venderlo al propietario legítimo. Mientras tanto, la empresa puede ser tergiversada al público. La única manera en que una organización puede evitar la ocupación cibernética es registrando dominios adyacentes y variaciones en el dominio o a través de litigios de marcas comerciales.

16. ¿Cuál de las siguientes describe mejor por qué se ejecuta fácilmente la suplantación de correo electrónico?

R. SMTP carece de un mecanismo de autenticación adecuado.

B. Los administradores a menudo olvidan configurar un servidor SMTP para evitar conexiones SMTP entrantes para dominios que no sirve.

C. El filtrado de palabras clave es técnicamente obsoleto.

D. Las listas negras son independables.

☑ **R.** La suplantación de correo electrónico es fácil de ejecutar porque SMTP carece de un mecanismo de autenticación adecuado. Un atacante puede suplantar las direcciones del remitente de correo electrónico enviando un comando Telnet al puerto 25 de un servidor de correo seguido de una serie de comandos SMTP. Los spammers usan la suplantación de correo electrónico para ofuscar su identidad. A menudo, el supuesto remitente de un correo electrónico no deseado es en realidad otra víctima de spam cuya dirección de correo electrónico ha sido vendida o cosechada por un spammer.

☒ **B** es incorrecta porque la respuesta alude a abrir servidores de retransmisión de correo. El error al configurar un servidor SMTP para evitar conexiones SMTP para dominios a los que no sirve no es un error común. Es bien sabido que un relé de correo abierto permite a los spammers ocultar su identidad y es una herramienta principal en la distribución de spam. Por lo tanto, las retransmisiones de correo abiertas se consideran un signo de mala administración del sistema. No se requiere un relé abierto para la suplantación de correo electrónico.

☒ **C** es incorrecto porque el filtrado de palabras clave es una contramedida que se puede utilizar para ayudar a suprimir el spam. Mientras que el filtrado de palabras clave por sí mismo era popular en un momento, ya no es una contramedida efectiva cuando se utiliza solo por sí mismo. El filtrado de palabras clave es propenso a falsos positivos y los spammers han encontrado maneras creativas de evitarlo. Por ejemplo, las palabras clave pueden escribirse incorrectamente intencionalmente o una o dos letras de una palabra común intercambiada con un carácter especial.

☒ **D** es incorrecto porque las listas negras enumeran servidores de retransmisión de correo abierto que son conocidos por enviar spam. Los administradores pueden usar listas negras para evitar la entrega de correo

electrónico procedente de esos hosts en un esfuerzo por suprimir el spam. Sin embargo, las listas negras no pueden depender de una protección completa porque a menudo son administradas por organizaciones privadas e individuos de acuerdo con sus propias reglas.

17. ¿Cuál de los siguientes no beneficia a VoIP?

R. costar

B. convergencia

C. flexibilidad

D. seguridad

☑ **D.** El Protocolo de voz sobre Internet (VoIP) se refiere a las tecnologías de transmisión que ofrecen comunicaciones de voz a través de redes IP. La telefonía IP utiliza tecnologías similares a TCP/IP, por lo que sus vulnerabilidades también son similares. El sistema de voz es vulnerable a la manipulación de aplicaciones (como fraude y bloqueo de peaje), acceso administrativo no autorizado y mala implementación. En términos de la red y los medios de comunicación, también es vulnerable a los ataques de denegación de servicio contra las puertas de enlace y los recursos de red. Espiar también es una preocupación, ya que el tráfico de datos se envía con texto claro a menos que se cifra.

☒ **A** es incorrecto porque el costo es un beneficio de VoIP. El uso de VoIP significa que una empresa tiene que pagar y mantener una sola red, en lugar de una red dedicada a la transmisión de datos y otra red dedicada a la transmisión de voz. Las características de telefonía como llamadas a conferencias, reenvío de llamadas y redial automático están libres de implementaciones voIP de código abierto, mientras que las empresas tradicionales de telecomunicaciones cobran extra por ellas. Y, por último, los costos de VoIP son más bajos debido a la forma en que se facturan. Las llamadas VoIP se facturan por megabyte, mientras que las llamadas telefónicas regulares se facturan por minuto. En general, es más barato enviar datos a través de Internet durante un período de tiempo determinado que utilizar el teléfono regular durante esa misma cantidad de tiempo.

☒ **B** es incorrecto porque la convergencia es un beneficio de VoIP. Convergencia se refiere a la fusión de la red IP tradicional con la red telefónica analógica tradicional. Esto es un beneficio porque una empresa ya no tiene que pagar y mantener redes separadas para datos y voz. Sin embargo, si bien la convergencia ahorra dinero y gastos generales de administración, ciertas cuestiones de seguridad deben entenderse y tratarse.

☒ **C** es incorrecto porque la flexibilidad es un beneficio de VoIP. La tecnología admite fácilmente múltiples llamadas telefónicas a través de una sola conexión de banda ancha de Internet sin tener que añadir líneas adicionales. También

ofrece la independencia de la ubicación. Todo lo que se necesita para obtener una conexión telefónica WAN o MAN a un proveedor voIP es una conexión a Internet adecuada. VoIP también se puede integrar con otros servicios de Internet, como conversación de vídeo, intercambio de archivos durante una llamada y conferencias de audio.

18. Hoy en día, los satélites se utilizan para proporcionar conectividad inalámbrica entre diferentes ubicaciones. ¿Qué dos requisitos previos se necesitan para que dos ubicaciones diferentes se comuniquen a través de enlaces satelitales?

R. Deben estar conectados a través de una línea telefónica y tener acceso a un módem.

B. Deben estar dentro de la línea de visión y huella del satélite.

C. Deben tener banda ancha y un satélite en órbita terrestre baja.

D. Deben tener un transpondedor y estar dentro de la huella del satélite.

☑ **B.** Para que dos lugares diferentes se comuniquen a través de enlaces satelitales, deben estar dentro de la línea de visión y huella del satélite (área cubierta por el satélite). El remitente de información modula los datos en una señal de radio que se transmite al satélite. Un transpondedor en el satélite recibe esta señal, la amplifica y la transmite al receptor. El receptor debe tener un cierto tipo de antena, que es uno de esos componentes circulares, similares a platos en la parte superior de los edificios. La antena contiene uno o más receptores de microondas, dependiendo de cuántos satélites esté aceptando datos. El tamaño de la huella depende del tipo de satélite que se utilice. Puede ser tan grande como un país o sólo unos pocos cientos de pies en circunferencia.

☒ **A** es incorrecto porque una línea telefónica y un módem no son inalámbricos. Sin embargo, en la mayoría de los casos la banda ancha por satélite es un sistema híbrido que utiliza una línea telefónica regular y tecnologías similares a módems para los datos y solicitudes enviadas desde la máquina del usuario, pero emplea un enlace satelital para enviar datos al usuario.

☒ **C** es incorrecto porque el satélite proporciona transmisión de banda ancha. Se utiliza comúnmente para canales de televisión y acceso a Internet para PC. Si bien ciertamente es necesario tener un satélite en órbita, y los que están en órbita terrestre baja se utilizan comúnmente para la paginación bidireccional, la comunicación celular internacional, las estaciones de televisión y el uso de Internet, no es la mejor respuesta a esta pregunta.

D es incorrecto porque las dos ubicaciones no requieren un transpondedor. El transpondedor está en el propio satélite. El transpondedor recibe una señal, la amplifica y la envía al receptor. Sin embargo, es necesario que las dos ubicaciones estén dentro de la huella del satélite.

19. Brad es un gerente de seguridad en Thingamabobs, Inc. Está preparando una presentación para los ejecutivos de su empresa sobre los riesgos de usar mensajería instantánea (IM) y sus razones para querer prohibir su uso en la red de la compañía. ¿Cuál de los siguientes no debe incluirse en su presentación?

R. Los datos y archivos confidenciales se pueden transferir de un sistema a otro a través de mensajería instantánea.

B. Los usuarios pueden recibir información, incluido el malware, de un atacante que se hace pasar por un remitente legítimo.

C. El uso de mensajería instantánea se puede detener simplemente bloqueando puertos específicos en los firewalls de red.

D. Se necesita una directiva de seguridad que especifique las restricciones de uso de mensajería instantánea.

☑ **C.** La mensajería instantánea (IM) permite a las personas comunicarse entre sí a través de un tipo de sala de chat personal y en tiempo real. Alerta a las personas cuando alguien que está en su "lista de amigos" ha accedido a la intranet / Internet para que puedan enviar mensajes de texto de un lado a otro en tiempo real. La tecnología también permite transferir archivos de un sistema a otro. La tecnología está compuesta por clientes y servidores. El usuario instala un cliente de mensajería instantánea (AOL, ICQ, Yahoo Messenger, etc.) y se le asigna un identificador único. Este usuario da este identificador único a las personas con las que desea comunicarse a través de mensajería instantánea. El bloqueo de puertos específicos en los firewalls no suele ser eficaz porque el tráfico IM puede estar utilizando puertos comunes que necesitan estar abiertos (puerto HTTP 80 y puerto FTP 21). Muchos de los clientes de mensajería instantánea se configuran automáticamente para trabajar en otro puerto si su puerto predeterminado no está disponible y está bloqueado por el firewall.

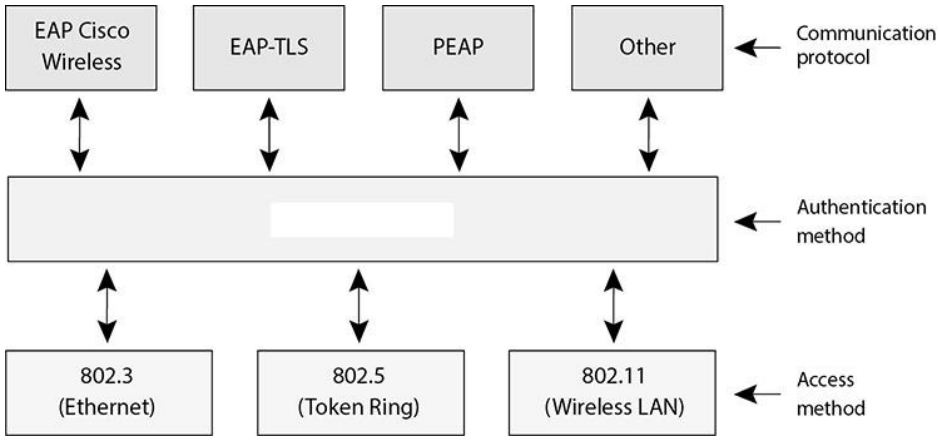
☒ **A** es incorrecto porque además de los mensajes de texto, la mensajería instantánea permite transferir archivos de un sistema a otro. Estos archivos podrían contener información sensible, poniendo a la empresa en riesgo comercial y legal. Y, por supuesto, compartir archivos a través de mensajería instantánea puede crear ancho de banda de red e afectar el rendimiento de la red como resultado.

☒ **B** es incorrecta porque la instrucción es true. Debido a la falta de autenticación sólida, las cuentas se pueden suplantar para que el receptor acepte información de un usuario malintencionado en lugar del remitente legítimo. También ha habido numerosos desbordamiento de búfer y ataques de paquetes malformados que han sido exitosos con diversos clientes im. Estos ataques se llevan a cabo generalmente con el objetivo de obtener acceso no autorizado al sistema de la víctima.

☒ **D** es incorrecto porque Brad debe incluir en su presentación la necesidad de una política de seguridad que especifique las restricciones de uso de mensajería

instantánea. Esta es solo una de las varias prácticas recomendadas para proteger un entorno de las infracciones de seguridad relacionadas con las mensajería instantáneas. Otras prácticas recomendadas incluyen la implementación de un producto antivirus/firewall integrado en todos los equipos, la configuración de firewalls para bloquear el tráfico de mensajería instantánea, la actualización del software de mensajería instantánea a versiones más seguras e la implementación de servidores de mensajería instantánea corporativa para que los empleados internos se comuniquen solo dentro de la red de la organización.

20. Hay varios tipos diferentes de tecnologías de autenticación. ¿Qué tipo se muestra en el gráfico que sigue?



A. 802.1X

B. Protocolo de autenticación extensible

C. Espectro de dispersión de salto de frecuencia

D. Multiplexación ortogonal de división de frecuencias

☑ **R.** El estándar 802.1X es un control de acceso a la red basado en puertos que garantiza que un usuario no pueda realizar una conexión de red completa hasta que se autentique correctamente. Esto significa que un usuario no puede acceder a los recursos de red y no se permite que el tráfico pase, excepto el tráfico de autenticación, del dispositivo inalámbrico a la red hasta que el usuario sea autenticado correctamente. Una analogía es tener una cadena en la puerta principal que le permite abrir la puerta ligeramente para identificar a una persona que llama antes de permitirle entrar en su casa. La autenticación de usuario proporciona un mayor grado de confianza y protección que la autenticación del sistema.

☒ **B** es incorrecto porque el Protocolo de autenticación extensible (EAP) no es una tecnología de autenticación específica; en su lugar, proporciona un marco para permitir que muchos tipos de técnicas de autenticación se utilicen durante las conexiones punto a punto (PPP). Como indica el nombre, amplía las posibilidades de autenticación de la norma (PAP y CHAP) a otros métodos como contraseñas de una sola vez, tarjetas de token, biometría, Kerberos y

mecanismos futuros. Así que cuando un usuario se conecta a un servidor de autenticación y ambos tienen capacidades EAP, pueden negociar entre una lista más larga de posibles métodos de autenticación.

☒ **C** es incorrecto porque el espectro de dispersión significa que algo está distribuyendo señales individuales a través de las frecuencias asignadas de alguna manera. Esto se utiliza en la comunicación inalámbrica y no es una tecnología de autenticación. El espectro de dispersión de salto de frecuencia (FHSS) toma la cantidad total de ancho de banda (espectro) y lo divide en subcanales más pequeños. El remitente y el receptor trabajan en uno de estos canales durante una cantidad específica de tiempo y luego se mueven a otro canal. El remitente pone la primera pieza de datos en una frecuencia, la segunda en una frecuencia diferente, y así sucesivamente. El algoritmo FHSS determina las frecuencias individuales que se utilizarán y en qué orden, y esto se conoce como secuencia de salto del remitente y del receptor.

☒ **D** es incorrecto porque el multiplexado ortogonal de división de frecuencia (OFDM) es un esquema de modulación multicarrier digital que compacta múltiples portadores modulados firmemente juntos, reduciendo el ancho de banda requerido. Las señales moduladas son ortogonales (perpendiculares) y no interfieren entre sí. OFDM utiliza un compuesto de bandas de canal estrecho para mejorar su rendimiento en bandas de alta frecuencia. Esto se utiliza en la comunicación inalámbrica y no es una tecnología de autenticación.

21. ¿Qué tipo de componente de cifrado de seguridad falta en la tabla siguiente?

	802.1X Dynamic WEP	Wi-Fi Protected Access	Robust Security Network
Access Control	802.1X	802.1X or preshared key	802.1X or preshared key
Authentication	EAP methods	EAP methods or preshared key	EAP methods or preshared key
Encryption	WEP		CCMP (AES Counter Mode)
Integrity	None	Michael MIC	CCMP (AES CBC-MAC)

A. Id. Id. conjunto de servicios

B. Protocolo de integridad de la clave temporal

C. Ad hoc WLAN

D. Autenticación abierta del sistema

☑ **B.** El Protocolo de integridad de clave temporal (TKIP) genera valores aleatorios utilizados en el proceso de cifrado, lo que hace que sea mucho más difícil para un atacante romper. Para permitir un nivel aún mayor de protección de cifrado, el estándar también incluye el nuevo algoritmo advanced encryption standard (AES) que se utilizará en las nuevas implementaciones de la red inalámbrica (WLAN). TKIP realmente funciona con el protocolo wired equivalent privacy (WEP) alimentándolo con material de clave, que son datos que se utilizarán para generar nuevas claves dinámicas. WEP utiliza el algoritmo de cifrado RC4, y la implementación actual del algoritmo proporciona muy poca

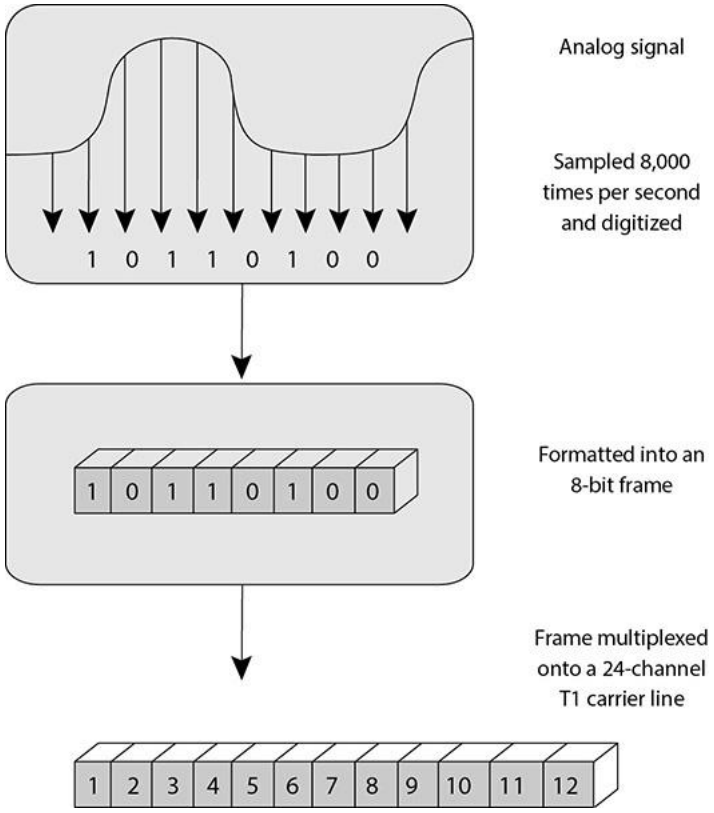
protección. Se agrega más complejidad al proceso de generación de claves con el uso de TKIP, lo que hace que sea mucho más difícil para los atacantes descubrir las claves de cifrado. El grupo de trabajo IEEE desarrolló TKIP para que los clientes solo necesiten obtener actualizaciones de firmware o software en lugar de comprar nuevos equipos para este tipo de protección.

A es incorrecto porque cuando los dispositivos inalámbricos trabajan en el modo de infraestructura, el Punto de acceso (AP) y los clientes inalámbricos forman un grupo referido como conjunto de servicios básicos (BSS). A este grupo se le asigna un nombre, que es el valor de IDENTIFICADOR de conjunto de servicios (SSID). Este valor no tiene nada que ver con el cifrado. Cualquier host que desee participar dentro de una red inalámbrica (WLAN) determinada se debe configurar con el SSID apropiado. Varios hosts se pueden segmentar en diversos WLAN mediante el uso de diferentes SSID. Las razones para segmentar una red inalámbrica (WLAN) en partes son las mismas razones por las que los sistemas cableados se segmentan en una red: los usuarios requieren acceso a diferentes recursos, tienen diferentes funciones empresariales o tienen diferentes niveles de confianza.

C es incorrecto porque una red inalámbrica (WLAN) ad hoc no tiene nada que ver con el cifrado, sino más bien con cómo se configuran los dispositivos inalámbricos en una red. Una red inalámbrica (WLAN) ad hoc no tiene puntos de acceso; los dispositivos inalámbricos se comunican entre sí a través de sus NIC inalámbricas en lugar de pasar por un dispositivo centralizado. Para construir una red ad hoc, el software del cliente inalámbrico se instala en hosts que contribuyen y se configura para el modo de operación punto a punto.

D es incorrecto porque la autenticación de sistema abierto (OSA) significa simplemente que un dispositivo inalámbrico no necesita probar que tiene una clave criptográfica específica para la autenticación. Dependiendo del producto y de la configuración, un administrador de red también puede limitar el acceso a direcciones MAC específicas. OSA no requiere que el dispositivo inalámbrico pruebe a un Punto de acceso que tiene una clave criptográfica específica para permitir para propósitos de autenticación. En muchos casos, el dispositivo inalámbrico necesita proporcionar solamente el valor correcto SSID. En las implementaciones de OSA, todas las transacciones están en cleartext porque no hay cifrado involucrado. Así que un intruso puede oler el tráfico, capturar los pasos necesarios de la autenticación, y caminar a través de los mismos pasos para ser autenticado y asociado a un AP.

22. ¿Qué tipo de tecnología se representa en el gráfico que sigue?



R. Modo de transferencia asíncrono

B. Redes ópticas sincrónicas

C. Multiplexación de división de frecuencia

D. multiplexación

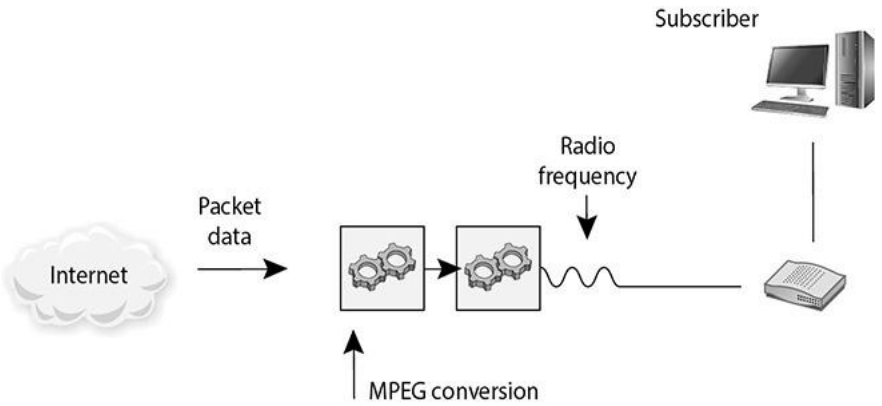
☑ **D.** Multiplexing es un método para combinar varios canales de datos a través de una sola ruta de transmisión. La transmisión es tan rápida y eficiente que los extremos no se dan cuenta de que están compartiendo una línea con muchas otras entidades. Los sistemas "piensan" que tienen la línea para sí mismos. Los sistemas telefónicos han existido durante unos 100 años, y comenzaron como sistemas analógicos basados en cobre. Las oficinas centrales de conmutación conectaban teléfonos individuales manualmente (a través de operadores humanos) al principio, y más tarde mediante el uso de equipos de conmutación electrónica. Después de conectar dos teléfonos, tenían una conexión de extremo a extremo, o un circuito de extremo a extremo. Varias llamadas telefónicas se dividieron y se colocaron en el mismo cable, que es multiplexante.

☒ **A** es incorrecto porque el modo de transferencia asincrónica (ATM) es una tecnología de red de alta velocidad que es utilizada en las implementaciones LAN y WAN por los operadores, isp, y las compañías telefónicas. Esta tecnología no es lo que se muestra en el gráfico. ATM encapsula los datos en las celdas fijas y se puede utilizar para entregar los datos a través de la red de redes ópticas sincrónicas (SONET). La analogía de una carretera y los coches se utiliza para describir la relación SONET y ATM. SONET es la carretera que proporciona la base (o la red) para que los coches —los paquetes ATM— viajen.

☒ **B** es incorrecto porque synchronous Optical Networks (SONET) es en realidad un estándar para las transmisiones de telecomunicaciones a través de cables de fibra óptica. Los operadores y las compañías telefónicas han desplegado redes SONET para América del Norte, y si siguen los estándares sonet correctamente, estas diversas redes pueden comunicarse con poca dificultad. Una red del área metropolitana (MAN) es generalmente una columna vertebral que conecta las LAN entre sí y las LAN a los WAN, Internet, y las redes de telecomunicaciones y cable. La mayoría de los MAN actuales son anillos SONET o FDDI proporcionados por los proveedores de servicios de telecomunicaciones.

☒ **C** es incorrecto porque la multiplexación de división de frecuencia es una forma de multiplexación de señal que implica asignar rangos de frecuencia no superpuestos a diferentes señales o a cada "usuario" de un medio. Este es un tipo de multiplexación, pero funciona sobre espectros de señal inalámbrica en lugar de un enfoque basado en el tiempo que se muestra en el gráfico. También se puede utilizar para combinar múltiples señales antes de la modulación final en una señal portadora. En este caso, las señales portadoras se conocen como subportadoras; cada frecuencia dentro del espectro se utiliza como un canal para mover datos. Un ejemplo es una transmisión FM estéreo.

23. ¿Qué tipo de tecnología de telecomunicaciones se ilustra en el gráfico que sigue?



R. Línea de suscriptores digitales

B. Red Digital de Servicios Integrados

C. BRI ISDN

D. Módem de cable

☑ **D.** Las compañías de televisión por cable han estado entregando servicios de televisión a los hogares durante años, y luego comenzaron a ofrecer servicios de transmisión de datos para los usuarios que tienen módems de cable y quieren conectarse a Internet a altas velocidades. Los módems de cable proporcionan acceso de alta velocidad, de hasta 50 Mbps, a Internet a través de las líneas coaxiales y de fibra de cable existentes. El módem de cable proporciona las

conversiones ascendentes y descendentes. No todas las compañías de cable proporcionan acceso a Internet como un servicio, principalmente porque no han actualizado su infraestructura para pasar de una red unidireccional a una red bidireccional. Una vez que se lleva a cabo esta conversión, los datos pueden bajar desde un punto central (conocido como la cabeza) a una casa residencial y volver a la cabeza y a Internet.

A es incorrecto porque Digital Subscriber Line (DSL) es otro tipo de tecnología de conexión de alta velocidad utilizada para conectar un hogar o negocio a la oficina central del proveedor de servicios. Utiliza líneas telefónicas existentes y proporciona una conexión de 24 horas a Internet. Esto realmente suena mejor que el pan en rodajas, pero sólo ciertas personas pueden obtener este servicio porque usted tiene que estar dentro de un radio de 2,5 millas del equipo del proveedor de servicios DSL. A medida que aumenta la distancia entre una residencia y la oficina central, las tasas de transmisión de DSL disminuyen. DSL no pasa por las líneas de televisión por cable y no tiene que pasar por la conversión de analógica a digital y de vuelta como se ilustra en el gráfico. DSL es una tecnología de banda ancha que puede proporcionar hasta una velocidad de transmisión de 52 Mbps sin reemplazar el cable de cobre del portador.

B es incorrecto porque Integrated Services Digital Network (ISDN) es un protocolo de comunicaciones proporcionado por compañías telefónicas e ISP que no necesita pasar por el proceso de conversión mostrado en el gráfico. Este protocolo y el equipo necesario permiten que los datos, la voz y otros tipos de tráfico viajen a través de un medio de una manera digital utilizada previamente sólo para la transmisión de voz analógica. Las compañías telefónicas fueron todas digitales hace muchos años, a excepción de los bucles locales, que consisten en los cables de cobre que conectan casas y negocios con las oficinas centrales de su proveedor de transportistas. Estas oficinas centrales contienen los equipos de conmutación de la compañía telefónica, y es aquí donde se lleva a cabo la transformación analógica a digital.

C es incorrecto porque el ISDN divide la línea telefónica en diferentes canales y transmite los datos en una forma digital en lugar de la forma analógica antigua. Isdn proporciona dos servicios básicos del hogar y del negocio: interfaz de tarifa básica (BRI) y interfaz de la tasa primaria (PRI). Bri tiene dos canales B que permiten transferir los datos y un canal D que proporciona la configuración de la llamada, la administración de la conexión, el control de errores, el IDENTIFICADOR de llamadas, y más. El ancho de banda disponible con bri es 144 Kbps, mientras que los módems superiores pueden proporcionar solamente 56 Kbps. El servicio BRI es común para uso residencial, y el PRI, que tiene 23 canales B y un canal D, es más comúnmente utilizado en las corporaciones.

24. ¿Qué tipo de protocolo de tunelización WAN falta en la tabla derecha del gráfico siguiente?

PPTP
Internetwork Must Be IP Based
No Header Compression
No Tunnel Authentication
Built-In PPP Encryption

Internetwork Can Be IP Frame Relay, x.25, or ATM Based
Header Compression
Tunnel Authentication
Uses IPSec Encryption

R. IPSec

B. Fddi

C. L2TP

D. CSMA/CD

☑ **C.** La tunelización es el ingrediente principal de una VPN porque así es como el VPN crea su conexión. Tres protocolos principales de tunelización se utilizan en las conexiones VPN: PPTP, L2TP, e IPSec. L2TP proporciona la funcionalidad del Point-to-Point Tunneling Protocol (PPTP), pero puede trabajar sobre redes que no sean solo IP, y proporciona un nivel más alto de seguridad cuando se combina con IPSec. L2TP no proporciona ningún servicio de cifrado o autenticación, por lo que necesita ser combinado con IPSec si se requieren esos servicios. Los procesos que L2TP utiliza para la encapsulación son similares a los utilizados por PPTP. La trama PPP se encapsula con el L2TP. Una limitación del PPTP es que puede trabajar solamente sobre las redes IP, así que otros protocolos se deben utilizar para mover los datos sobre el Frame Relay, X.25, y los links ATM.

☒ **A** es incorrecto porque el conjunto de protocolos de seguridad de protocolo de Internet (IPSec) proporciona un método de configuración de un canal seguro para el intercambio de datos protegidos entre dos dispositivos. Los dispositivos que comparten este canal seguro pueden ser dos servidores, dos enrutadores, una estación de trabajo y un servidor, o dos puertas de enlace entre diferentes redes. IPSec es un estándar ampliamente aceptado para proporcionar protección de capa de red. IPSec se utiliza comúnmente con L2TP para proporcionar protección para los datos que viajan sobre este tipo de trayectoria de comunicación como se muestra en el gráfico.

B es incorrecta porque la tecnología Fiber Distributed Data Interface (FDDI) es una tecnología de acceso multimedia de alta velocidad que pasa tokens. FDDI tiene una velocidad de transmisión de datos de hasta 100 Mbps y se utiliza generalmente como una red troncal utilizando cableado de fibra óptica. FDDI también proporciona tolerancia a fallos al ofrecer un segundo anillo de fibra contrarrotativo. El anillo principal tiene datos viajando en el sentido de las agujas del reloj y se utiliza para la transmisión regular de datos. El segundo anillo transmite los datos de manera en sentido contrario a las agujas del reloj y se invoca solamente si el timbre primario baja. Los sensores observan el anillo primario y, si baja, invocan una envoltura de anillo para que los datos se desvíen al segundo anillo. Cada nodo de la red FDDI tiene relés que están conectados a ambos anillos, así que si ocurre una rotura en el timbre, los dos anillos se pueden unir. L2TP se utiliza para las conexiones WAN, mientras que el FDDI se utiliza comúnmente para las conexiones MAN.

D es incorrecto porque el acceso múltiple del sentido portador con la detección de colisión (CSMA/CD) es un método de acceso a la red en el cual se utiliza un esquema de detección del portador. Una transmisión se denomina portadora, por lo que si un ordenador está transmitiendo tramas, está realizando una actividad portadora. Cuando los ordenadores utilizan el protocolo CSMA/CD, supervisan la actividad de transmisión, o actividad del portador, en el cable para que puedan determinar cuándo sería el mejor momento para transmitir datos. Cada nodo supervisa el cable continuamente y espera hasta que el cable esté libre antes de que transmita sus datos. Como analogía, considere a varias personas reunidas en un grupo hablando aquí y allá sobre esto y aquello. Si una persona quiere hablar, por lo general escucha la conversación actual y espera un descanso antes de que proceda a hablar. Si no espera a que la primera persona deje de hablar, hablará al mismo tiempo que la otra persona, y es posible que las personas que la rodean no puedan entender completamente lo que cada uno está tratando de decir.

25. IPv6 tiene muchas características y funcionalidades nuevas y diferentes en comparación con IPv4. ¿Cuál de los siguientes es una funcionalidad o característica incorrecta de IPv6?

i. IPv6 permite direcciones no vinculadas, lo que permite a un administrador restringir direcciones específicas para servidores específicos o intercambio de archivos e impresión, por ejemplo.

ii. IPv6 tiene IPSec integrado en la pila de protocolos, que proporciona transmisión y autenticación seguras basadas en aplicaciones.

iii. IPv6 tiene más flexibilidad y capacidades de enrutamiento en comparación con IPv4 y permite asignar valores de prioridad de calidad de servicio (QoS) a transmisiones sensibles al tiempo.

iv. El protocolo ofrece la autoconfiguración, lo que hace que la administración sea mucho más fácil en comparación con IPv4, y no requiere traducción de

direcciones de red (NAT) para ampliar su espacio de direcciones.

A. i, iii

B. i, ii

C. ii, iii

D. ii, iv

☑ **B.** IPv6 permite direcciones con ámbito, lo que permite a un administrador restringir direcciones específicas para servidores específicos o intercambio de archivos e impresión, por ejemplo. IPv6 tiene IPSec integrado en la pila de protocolos, que proporciona transmisión y autenticación seguras de extremo a extremo.

☒ **A** es incorrecto. IPv6 permite direcciones con ámbito, lo que permite a un administrador restringir direcciones específicas para servidores específicos o intercambio de archivos e impresión, por ejemplo. IPv6 tiene más flexibilidad y capacidades de enrutamiento y permite asignar valores de prioridad de calidad de servicio (QoS) a transmisiones sensibles al tiempo.

☒ **C** es incorrecto. IPv6 tiene más flexibilidad y capacidades de enrutamiento y permite asignar valores de prioridad de QoS a transmisiones sensibles al tiempo. IPv6 tiene IPSec integrado en la pila de protocolos, que proporciona transmisión y autenticación seguras de extremo a extremo.

☒ **D** es incorrecto porque IPv6 tiene IPSec integrado en la pila de protocolos, que proporciona transmisión y autenticación seguras de extremo a extremo. El protocolo ofrece la autoconfiguración, lo que facilita mucho la administración, y no requiere traducción de direcciones de red (NAT) para ampliar su espacio de direcciones.

26. Hanna es un nuevo gerente de seguridad para una empresa de consultoría informática. Ella ha descubierto que la compañía ha perdido propiedad intelectual en el pasado porque los empleados maliciosos instalaron dispositivos falsos en la red, que se utilizaron para capturar tráfico sensible. Hanna necesita implementar una solución que garantice que solo se permita el acceso a dispositivos autorizados a la red de la empresa. ¿Cuál de las siguientes normas IEEE se desarrolló para este tipo de protección?

R. IEEE 802.1AR

B. IEEE 802.1AE

C. IEEE 802.1AF

D. IEEE 802.1XR

☑ **R.** El estándar IEEE 802.1AR especifica identificadores únicos por dispositivo (DevID) y el enlace de administración y criptografía de un dispositivo (enrutador, conmutador, punto de acceso) a sus identificadores. Una identidad de dispositivo única verificable permite establecer la fiabilidad de los dispositivos; por lo tanto, facilita el aprovisionamiento seguro del dispositivo. Un identificador de dispositivo seguro (DevID) está enlazado criptográficamente a un dispositivo y admite la autenticación de la identidad del dispositivo. Las identidades localmente significativas se pueden asociar de forma segura con un DevID inicial aprovisionado por el fabricante y utilizarse en protocolos de aprovisionamiento y autenticación para permitir que un administrador de red establezca la fiabilidad de un dispositivo y seleccione las directivas adecuadas para la transmisión y recepción de datos y protocolos de control hacia y desde el dispositivo.

☒ **B** es incorrecto porque 802.1AE es el estándar IEEE MAC Security (MACSec), que define una infraestructura de seguridad para proporcionar confidencialidad de datos, integridad de datos y autenticación de origen de datos. Cuando una conexión VPN proporciona protección en las capas de red más altas, MACSec proporciona protección salto a salto en la capa 2.

☒ **C** es incorrecto porque 802.1AR proporciona un ID único para un dispositivo. 802.1AE proporciona funcionalidad de cifrado de datos, integridad y autenticación de origen. 802.1AF lleva a cabo funciones clave de acuerdo para las claves de sesión utilizadas para el cifrado de datos. Cada uno de estos estándares proporciona parámetros específicos para trabajar dentro de un marco EAP-TLS 802.1X.

☒ **D** es incorrecto porque esta es una respuesta distracter. Este no es un estándar válido.

27. _____

R. Registros de recursos

B. Traslado de zona

C. DNSSEC

D. Transferencia de recursos

☑ **C.** DNSSEC es un conjunto de extensiones a DNS que proporciona a los clientes DNS (solucionadores) autenticación de origen de datos DNS para reducir la amenaza de envenenamiento de DNS, suplantación de humo y tipos de ataque similares. DNSSEC es un conjunto de especificaciones del Grupo de Trabajo de Ingeniería de Internet (IETF) para proteger los servicios proporcionados por el DNS tal como se utiliza en las redes IP.

☒ **A** es incorrecto porque un servidor DNS contiene registros que asignan nombres de host a direcciones IP, que se denominan registros de recursos.

Cuando el equipo de un usuario necesita resolver un nombre de host en una dirección IP, busca en su configuración de red encontrar su servidor DNS. A continuación, el equipo envía una solicitud que contiene el nombre de host al servidor DNS para su resolución. El servidor DNS examina sus registros de recursos y encuentra el registro con este nombre de host determinado, recupera la dirección y responde al equipo con la dirección IP correspondiente.

☒ **B** es incorrecto porque los servidores DNS primarios y secundarios sincronizan su información a través de una transferencia de zona. Una vez que se producen cambios en el servidor DNS principal, esos cambios deben replicarse en el servidor DNS secundario. Es importante configurar el servidor DNS para permitir que las transferencias de zona solo se realicen entre los servidores específicos.

☒ **D** es incorrecto porque es una respuesta distracter.

28. ¿Cuál de los siguientes describe mejor la diferencia entre un firewall virtual que funciona en modo puente frente a uno que está incrustado en un hipervisor?

R. El firewall virtual en modo puente permite al firewall supervisar enlaces de tráfico individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema host.

B. El firewall virtual en modo Puente permite al firewall supervisar enlaces de red individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema invitado.

C. El firewall virtual en modo puente permite al firewall supervisar enlaces de tráfico individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema invitado.

D. El firewall virtual en modo puente permite al firewall supervisar sistemas invitados individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema de red.

☑ **R.** Los firewalls virtuales pueden ser productos en modo puente, que supervisan vínculos de tráfico individuales entre máquinas virtuales o se pueden integrar dentro del hipervisor de un entorno virtualizado. El hipervisor es el componente de software que lleva a cabo la gestión de máquinas virtuales y supervisa la ejecución de software del sistema invitado. Si el firewall está incrustado dentro del hipervisor, puede "ver" y supervisar todas las actividades que tienen lugar dentro del sistema host.

☒ **B** es incorrecto porque el firewall virtual en modo puente permite al firewall supervisar vínculos de tráfico individuales entre hosts, no vínculos de red. La integración de hipervisores permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema host, no un sistema invitado.

☒ **C** es incorrecto porque el firewall virtual en modo puente permite al firewall supervisar enlaces de tráfico individuales, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema host, no un sistema invitado. El hipervisor es el componente de software que lleva a cabo la gestión de máquinas virtuales y supervisa la ejecución de software del sistema invitado. Si el firewall está incrustado dentro del hipervisor, puede "ver" y supervisar todas las actividades que tienen lugar dentro del sistema.

☒ **D** es incorrecto porque un firewall virtual en modo puente permite al firewall supervisar el tráfico individual entre sistemas invitados, y la integración del hipervisor permite al firewall supervisar todas las actividades que tienen lugar dentro de un sistema host, no un sistema de red.

29. ¿Cuál de las siguientes tecnologías de redes definidas por software (SDN) especifica?

R. La asignación entre las direcciones MAC y las direcciones IP en el software

B. Las tablas de enrutamiento estático de los nodos finales de forma dinámica

C. Cómo los routers comunican sus tablas de ruteo entre sí a medida que ocurren los eventos

D. Cómo mueven los paquetes los routers en función de las instrucciones de un controlador administrado de forma centralizada

☑ **D.** Las redes definidas por software (SDN) están diseñadas para desacoplar la función lógica del router de tomar decisiones de enrutamiento y su función mecánica de pasar datos entre interfaces, y para hacer que las decisiones de enrutamiento sean más manejables de forma centralizada. La arquitectura SDN está diseñada para ser una forma basada en estándares de proporcionar lógica de control a los planos de datos de los routers de una manera escalable y programable.

☒ **A** es incorrecta porque la asignación entre las direcciones del Media Access Control (MAC) y el Protocolo de Internet (IP) es proporcionada por el Address Resolution Protocol (ARP). Esto es lo que permite la encapsulación de paquetes de la capa 3 OSI en tramas de capa 2 OSI adecuadas para su procesamiento por switches, concentradores y puntos de acceso inalámbricos.

☒ **B** es incorrecto porque las tablas de enrutamiento estático con las que se configuran la mayoría de los nodos finales están codificadas de forma dura por los administradores del sistema (típicas en el caso de los servidores) o proporcionadas a través del Protocolo de configuración dinámica de host (DHCP) para sistemas móviles y de escritorio.

☒ **C** es incorrecto porque el intercambio de configuración de la tabla de ruteo tradicional entre los dispositivos de ruteo se comunica más a menudo vía un Routing Protocol de vectores de distancia tal como el Routing Information

Protocol (RIP) o un Link-state Routing Protocol tal como Open Shortest Path First (OSPF). En estos casos, los Routers comparten la información entre ellos dentro de un dominio de ruteo, y después toman sus decisiones sobre cómo pasar los paquetes basados en la lógica interna.

30. Determinar la ubicación geográfica de una dirección IP del cliente para enrutarla hacia la fuente topológica más proximal del contenido web es un ejemplo de ¿qué tecnología?

R. Red de distribución de contenido (CDN)

B. Servicio de nombres distribuidos (DNS)

C. Servicio web distribuido (DWS)

D. Distribución de dominios de contenido (CDD)

☑ **R.** Las redes de distribución de contenido (CDN) están diseñadas para optimizar la entrega de contenido, principalmente a través del Protocolo de transferencia de hipertexto (HTTP), a los clientes en función de su posición topológica global. En tal diseño, varios servidores web hospedados en muchos puntos de presencia en Internet contienen el mismo contenido de una manera globalmente sincronizada, por lo que los clientes se pueden dirigir al origen más cercano, normalmente a través de la manipulación de registros DNS basados en algoritmos de geolocalización para la dirección IP del solicitante.

☒ **B** es incorrecto porque el servicio de nombres distribuidos es una respuesta distractante, ya que no existe tal protocolo. DNS se refiere correctamente al protocolo del servicio de nombres de dominio, que se utiliza más a menudo en las CDN para dirigir a los clientes al servidor más geográficamente proximal a ellos para el contenido solicitado.

☒ **C** es incorrecto porque el servicio web distribuido también es una respuesta distracter. El concepto de arquitectura de detección de servicios web distribuidos ha sido discutido por el IEEE y otros, pero no es un protocolo formal. Sus objetivos son ortogonales a la idea de una entrega eficiente de contenidos.

☒ **D** es incorrecto porque la distribución del dominio de contenido se proporciona como respuesta distracter para asegurarse de que el candidato cissp puede distinguir entre conceptos y acrónimos generalmente aceptados. No existe tal cosa como CDD en este contexto.

31. ¿Cuál de los siguientes protocolos o conjunto de protocolos se utiliza en Voz sobre IP (VoIP) para la identificación de llamadas?

R. Protocolo de transporte en tiempo real (RTP) y/o Protocolo de transporte seguro en tiempo real (SRTP)

B. Protocolo de transporte en tiempo real (RTP) y protocolo de control de transporte en tiempo real (RTCP)

C. Protocolo de inicio de sesión (SIP)

D. Intercambio público de telefonía/sucursal telefónica conmutada (RTC/PBX)

☑ **C.** El Protocolo de inicio de sesión se utiliza comúnmente para todas las transacciones VoIP excepto el intercambio de medios real entre las estaciones de llamada o recepción. Esto incluye la identificación y ubicación de la persona que llama, la configuración de llamadas y el desmontaje, etc. Está intermediado por un sistema de terceros de confianza mutua que contiene información de registro para cada estación/usuario.

☒ **A** es incorrecto porque RTP/SRTP son los protocolos comúnmente utilizados entre los nodos finales para la interacción directa de los medios. Mientras que la negociación de llamada se logra comúnmente vía el SORBO o incluso H.323 (arcaicamente) usando un servidor de ubicación, el intercambio de medios es típicamente punto a punto vía estos protocolos.

☒ **B** es incorrecto porque como se explica para la respuesta A, rtp es un protocolo de transporte de medios, no un protocolo de negociación. RTCP es un distractr adicional, ya que es un protocolo para monitorear el rendimiento de las redes VoIP, medir e informar sobre aspectos tales como latencia y fluctuación.

☒ **D** es incorrecto porque mientras que las tecnologías PSTN/PBX son importantes para las redes VoIP, no son centrales para la identificación de llamadas de la manera en que es el SORBO. Más bien, tal acrónimo normalmente se refiere a una forma de construir una interfaz entre una red VoIP y números de teléfono públicamente direccionables.

32. El cifrado puede ocurrir en diferentes capas de un sistema operativo y una pila de red. ¿Dónde se lleva a cabo el cifrado PPTP?

R. Capa de enlace de datos

B. Dentro de las aplicaciones

C. Capa de transporte

D. Enlace de datos y capas físicas

☑ **R.** El Protocolo de tunelización punto a punto (PPTP) es un método para implementar redes privadas virtuales (VPN). Es un protocolo VPN propiedad de Microsoft que funciona en la capa de vínculo de datos del modelo OSI. PPTP puede proporcionar solamente una sola conexión y puede trabajar solamente sobre las conexiones PPP.

☒ **B** es incorrecto porque el cifrado de extremo a extremo tiene lugar dentro de las aplicaciones. El cifrado de extremo a extremo significa que solo se cifra la

carga de datos. Si el cifrado funciona en cualquier capa del modelo OSI, los encabezados y los finalizadores también se pueden cifrar. Puesto que PPTP trabaja en la capa de enlace de datos, los encabezados y remolques de las capas superiores se pueden cifrar y proteger junto con la carga útil de datos.

☒ **C** es incorrecto porque SSL es un ejemplo de una tecnología de cifrado que funciona en la capa de transporte, no PPTP. SSL utiliza el cifrado de claves públicas y proporciona cifrado de datos, autenticación de servidor, integridad de mensajes y autenticación de cliente opcional para mostrar partes protegidas de un sitio web a un usuario. Cuando HTTP se ejecuta a través de SSL, tiene HTTP Secure (HTTPS). HTTP funciona en la capa de aplicación, pero SSL sigue funcionando en la capa de transporte.

☒ **D** es incorrecto porque PPTP trabaja en la capa de link de datos, pero no en la capa física. Las tecnologías de capa física convierten los bits de la capa de enlace de datos en algún tipo de formato de transmisión. Si la transmisión de datos se está llevando a cabo a través de una conexión UTP, los datos se convierten en voltaje electrónico en la capa física. Si la transmisión de datos se está llevando a cabo a través de líneas de fibra, los datos se convierten en fotones. Las especificaciones de la capa física incluyen la sincronización de los cambios de voltaje, los niveles de voltaje y los conectores físicos para la transmisión eléctrica, óptica y mecánica.

33. ¿Cuál de los siguientes describe incorrectamente la suplantación de IP y el secuestro de sesiones?

R. La suplantación de dirección ayuda a un atacante a secuestrar sesiones entre dos usuarios sin ser notado.

B. La suplantación de IDENTIDAD hace que sea más difícil localizar a un atacante.

C. El secuestro de sesión se puede prevenir con autenticación mutua.

D. La suplantación de IP se utiliza para secuestrar comunicaciones seguras SSL e IPSec.

☑ **D.** Secure Sockets Layer (SSL) e IPSec pueden proteger la integridad, autenticidad y confidencialidad del tráfico de red. Incluso si un atacante suplantó una dirección IP, no sería capaz de manipular o leer con éxito el tráfico cifrado SSL o IPSec, ya que no tendría acceso a las claves y otro material criptográfico requerido.

☒ **A** es incorrecta porque la instrucción es true. La suplantación de dirección ayuda a un atacante a secuestrar sesiones entre dos usuarios sin ser notado. Si un atacante quisiera hacerse cargo de una sesión entre dos computadoras, tendría que ponerse en medio de su conversación sin ser detectada. Herramientas como Juggernaut y el proyecto HUNT permiten al atacante espiar la conexión TCP y luego secuestrarla.

☒ **B** es incorrecta porque la instrucción es true. La suplantación es la presentación de información falsa, generalmente dentro de paquetes, para engañar a otros sistemas y ocultar el origen del mensaje. Esto es generalmente hecho por los piratas informáticos para que su identidad no pueda ser descubierta con éxito.

☒ **C** es incorrecta porque la instrucción es true. Si el secuestro de sesiones es una preocupación en una red, el administrador puede implementar un protocolo, como IPSec o Kerberos, que requiere autenticación mutua entre usuarios o sistemas.

34. El equipo de seguridad de TI de una pequeña institución médica se ha visto abrumado por tener que operar y mantener IDS, firewalls, soluciones antimalware en toda la empresa, tecnologías de prevención de fugas de datos y gestión centralizada de registros. ¿Cuál de las siguientes describe mejor qué tipo de solución debe implementar esta organización para permitir operaciones de seguridad estandarizadas y optimizadas?

A. Gestión unificada de amenazas

B. Tecnología de monitoreo continuo

C. Sistemas centralizados de control de acceso

D. Solución de seguridad basada en la nube

☑ **R.** Se ha vuelto muy difícil administrar la larga lista de soluciones de seguridad que casi todas las redes necesitan tener en su lugar. La lista incluye, pero no se limita a, firewalls, antimalware, antispam, IDS/IPS, filtrado de contenido, prevención de fugas de datos, capacidades vpn y monitoreo e informes continuos. Se han desarrollado productos unificados de dispositivos de gestión de amenazas (UTM) que proporcionan todas (o muchas) de estas funcionalidades en un único dispositivo de red. Los objetivos de UTM son la simplicidad, la instalación y el mantenimiento simplificados, el control centralizado y la capacidad de comprender la seguridad de una red desde un punto de vista holístico. Cada proveedor de productos de seguridad tiene su propia solución UTM, pero cada uno tiene objetivos similares de permitir a los administradores supervisar y administrar una variedad de aplicaciones y productos relacionados con la seguridad a través de una única consola de administración.

☒ **B** es incorrecto porque la supervisión continua en la industria de la seguridad se refiere más comúnmente a la supervisión continua de la seguridad de la información (ISCM), que permite a las empresas obtener conciencia situacional, conocimiento continuo de la seguridad de la información, vulnerabilidades y amenazas para apoyar las decisiones de gestión de riesgos empresariales. El monitoreo se centra en la recopilación de datos en lo que respecta a la postura de salud y seguridad de un entorno y no combina todas las tecnologías mencionadas en la pregunta. Cada dispositivo de red y solución de seguridad (es

decir, escáneres de vulnerabilidades, firewalls, IDS, IPS, etc.) genera sus propios registros, y es difícil monitorearlos individualmente para entender lo que realmente está ocurriendo dentro de un entorno en red empresarial. La supervisión puede realizarse a través de procesos manuales o automatizados, pero cuando abordamos específicamente la supervisión continua, esto generalmente se logra a través de la automatización. Las tecnologías automatizadas de monitoreo continuo intentan agregar y correlacionar estos diversos tipos de registros para proporcionar una única interfaz y comprensión holística del entorno. Las tecnologías de monitoreo continuo también llevan a cabo escaneos automatizados de sistemas críticos en lugar del enfoque lento y propenso a errores de los escaneos manuales y los procesos de certificación y acreditación. El Protocolo de automatización de contenido de seguridad (SCAP) fue una de las primeras especificaciones lanzadas que permite a diferentes proveedores de productos de seguridad implementar capacidades de supervisión continua de forma estandarizada.

C es incorrecto porque los sistemas de control de acceso centralizados no intentan combinar todos los productos y funciones de seguridad mencionados en la pregunta. Se utilizan sistemas de control de acceso centralizados para que el control de acceso se pueda practicar de forma estandarizada en varios sistemas dentro de un entorno en red. El control de acceso normalmente abarca la identificación, autenticación, autorización y responsabilidad de los usuarios que necesitan acceder a los recursos de una red. Los recursos de la red se proporcionan generalmente a través de diferentes tipos de sistemas (es decir, Windows, Unix, Linux, mainframes), y es un reto poder practicar el control de acceso en todos estos diversos sistemas de una manera estandarizada y predecible. El control de acceso centralizado permite a los administradores definir y mantener directivas de control de acceso en un entorno heterogéneo que admite las necesidades de acceso de varios usuarios.

D es incorrecta porque la solución de seguridad basada en la nube es una respuesta de distracción. Aunque hay servicios administrados por seguridad que permiten a una empresa subcontratada administrar y mantener los dispositivos y soluciones de seguridad de una empresa, esto no se considera una solución basada en la nube. Las soluciones basadas en la nube proporcionan un entorno de infraestructura, plataforma o aplicación a un cliente para que el cliente no necesite gastar tiempo y dinero en mantener estos artículos ellos mismos. Algunos proveedores de nube pueden proporcionar algunos de estos servicios de seguridad dentro de sus ofertas de infraestructura como servicio (IaaS), pero este no es el foco principal de una solución basada en la nube.

35. ¿Cuál de los siguientes protocolos desenfoca las líneas entre las capas del modelo OSI, realizando las tareas de varios a la vez?

R. Protocolo de red distribuida 3 (DNP3)

B. Protocolo de transferencia de archivos (FTP)

C. Protocolo de control de transmisión (TCP)

D. Sistema de nombres de dominio (DNS)

☑ **R.** DNP3 fue diseñado para su uso en sistemas SCADA, que históricamente se configuraron en una jerarquía de red plana, con dispositivos conectados en serie entre sí. Como tal, no se requería una funcionalidad de enrutamiento moderna. Por lo tanto, se comporta como un protocolo de capa de link serie, pero también realiza la función de un protocolo de capa de transporte también.

☒ **B** es incorrecto porque FTP es un poco extraño en que utiliza varios puertos: uno que proporciona esencialmente el comando y el control entre el cliente y el servidor, y otros que se utilizan para la transferencia de datos real. Sin embargo, todas las conexiones se llevan a cabo a través de TCP en la capa de transporte.

☒ **C** es incorrecto porque es más claramente un protocolo de capa de transporte solamente.

☒ **D** es incorrecto, porque aunque DNS utiliza TCP y UDP, ambos son protocolos de capa de transporte.

36. ¿Cuál de las siguientes describe correctamente la relación entre SSL y TLS?

R. TLS es la versión de comunidad abierta de SSL.

B. Los desarrolladores pueden modificar SSL para ampliar las capacidades del protocolo.

C. TLS es un protocolo propietario, mientras que SSL es un protocolo de comunidad abierta.

D. SSL es más extensible y compatible con TLS.

☑ **R.** Capa de sockets seguros (SSL) y seguridad de capa de transporte (TLS) son protocolos criptográficos que se utilizan para proteger las comunicaciones mediante el cifrado de segmentos de conexiones de red. Ambos protocolos funcionan en la capa de sesión de IPv4, sin embargo (ISC)[2] los considera protocolos de capa de presentación porque proporcionan cifrado. TLS es la versión de comunidad abierta de SSL. Dado que TLS es un protocolo de comunidad abierta, sus especificaciones pueden ser modificadas por los proveedores dentro de la comunidad para expandir lo que puede hacer y con qué tecnologías puede trabajar. SSL es un protocolo propietario, y TLS fue desarrollado por un organismo de estándares, lo que lo convierte en un protocolo de comunidad abierta.

☒ **B** es incorrecto porque SSL es un protocolo propietario desarrollado por Netscape. Esto significa que la comunidad tecnológica no puede extender fácilmente SSL para interoperar y expandirse en su funcionalidad. Si un protocolo es de naturaleza propia, como es SSL, la comunidad tecnológica no puede cambiar directamente sus especificaciones y funcionalidades. La razón

por la que se desarrolló TLS fue para estandarizar cómo se pueden transmitir datos de forma segura a través de un protocolo y cómo los proveedores pueden modificar el protocolo y seguir permitiendo la interoperabilidad.

☒ **C** es incorrecta porque la instrucción es hacia atrás. TLS no es propietario. Es la versión de comunidad abierta de SSL, que es propietaria.

☒ **D** es incorrecto porque TLS es realmente más extensible que SSL y no es compatible con SSL. TLS y SSL proporcionan el mismo tipo de funcionalidad y son muy similares, pero no lo suficientemente similares como para trabajar directamente juntos. Si dos dispositivos necesitan comunicarse de forma segura, deben usar TLS o SSL, no pueden usar un enfoque híbrido y aún así pueden comunicarse.

37. Los usuarios utilizan el cifrado de extremo a extremo y los proveedores de servicios utilizan el cifrado de vínculos. ¿Cuál de las siguientes describe correctamente estas tecnologías?

R. El cifrado de vínculos no cifra los encabezados y los trailers.

B. El cifrado de enlaces cifra todo menos la mensajería de enlaces de datos.

C. El cifrado de extremo a extremo requiere que los encabezados se descifran en cada salto.

D. El cifrado de extremo a extremo cifra todos los encabezados y trailers.

☑ **B.** El cifrado se puede realizar en diferentes niveles de comunicación, cada uno con diferentes tipos de protección e implicaciones. Dos modos generales de implementación de cifrado son el cifrado de vínculos y el cifrado de extremo a extremo. El cifrado de enlace cifra todos los datos a lo largo de una ruta de comunicación específica, como en un enlace satélite, una línea T3 o un circuito telefónico. No sólo se cifra la información de usuario, sino que también se cifran los datos de encabezado, finalizadores, direcciones y enrutamiento que forman parte de los paquetes. El único tráfico no cifrado en esta tecnología es la información de mensajería de control de vínculos de datos, que incluye instrucciones y parámetros que los diferentes dispositivos de enlace utilizan para sincronizar métodos de comunicación. El cifrado de enlaces proporciona protección contra los rastreadores de paquetes y los espías. En el cifrado de extremo a extremo, los encabezados, direcciones, enrutamiento e información del tráiler no se cifran, lo que permite a los atacantes obtener más información sobre un paquete capturado y hacia dónde se dirige. Con el cifrado de extremo a extremo solo se cifra la carga de datos.

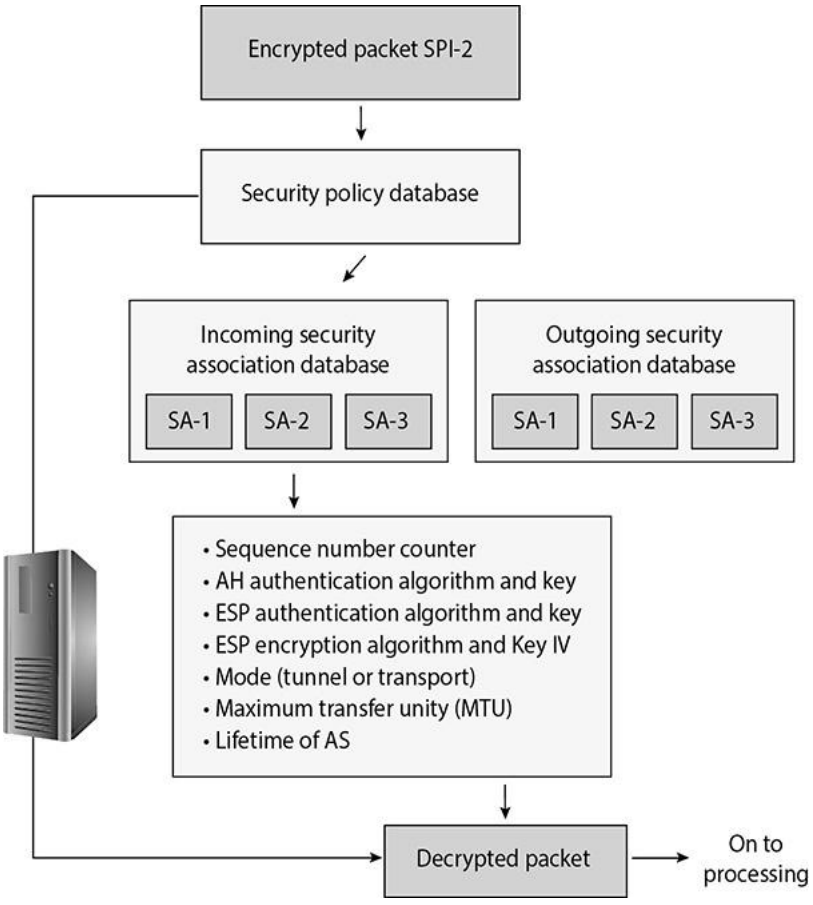
☒ **A** es incorrecto porque el cifrado de vínculos cifra los encabezados y los finalizadores. Esta es una ventaja importante para el uso de cifrado de vínculos: los encabezados, los trailers y la carga de datos se cifran excepto para la mensajería de vínculos de datos. También funciona perfectamente en una capa

inferior en el modelo OSI, por lo que los usuarios no necesitan hacer nada para iniciarlo.

☒ **C** es incorrecto porque los encabezados no se cifran con el cifrado de extremo a extremo, por lo que no hay necesidad de descifrarlos en cada salto. Esta es una ventaja de usar cifrado de extremo a extremo. Otras ventajas incluyen flexibilidad adicional para el usuario a la hora de elegir qué se cifra y cómo, y una mayor granularidad de funcionalidad porque cada aplicación o usuario puede elegir configuraciones específicas.

☒ **D** es incorrecto porque el cifrado de extremo a extremo no cifra ningún encabezado o finalizador. Como resultado, no están protegidos. Esta es la principal desventaja de usar el cifrado de extremo a extremo. Si es necesario proteger los encabezados y los finalizadores, se debe usar el cifrado de vínculos.

38. ¿Qué representan los valores SA en el gráfico de IPSec que sigue?



R. Índice de parámetros de seguridad

B. Capacidad de seguridad

C. Asociación de seguridad

D. Asistente de seguridad

☑ **C.** Cada dispositivo VPN IPSec tendrá al menos una asociación de seguridad (SA) para cada conexión segura que utilice. La SA, que es fundamental para la

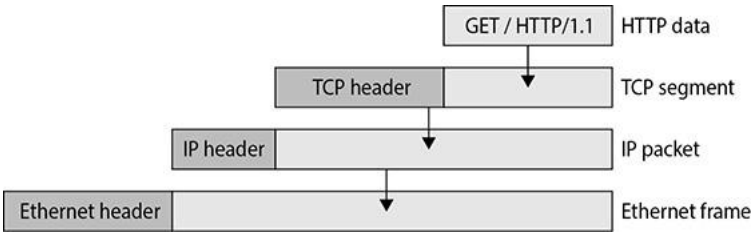
arquitectura IPSec, es un registro de las configuraciones que el dispositivo necesita para admitir una conexión IPSec a través de una conexión VPN. Cuando dos dispositivos completan su proceso de apretón de manos, lo que significa que han acordado una larga lista de parámetros que usarán para comunicarse, estos datos deben registrarse y almacenarse en algún lugar, que se encuentra en la SA. La SA puede contener las claves de autenticación y cifrado, los algoritmos acordados, la duración de la clave, la dirección IP de origen y otra información. Cuando un dispositivo recibe un paquete vía el protocolo IPSec, es el SA el que le dice al dispositivo qué hacer con el paquete. Así que si el dispositivo B recibe un paquete del dispositivo C vía el IPSec, el dispositivo B mirará a la SA correspondiente para decirle cómo descifrar el paquete, cómo autenticar correctamente la fuente del paquete, qué clave utilizar, y cómo responder al mensaje si es necesario.

A es incorrecto porque un índice de parámetros de seguridad (SPI) realiza un seguimiento de los diversos SAs. Los SAs son direccionales, por lo que un dispositivo tendrá una SA para el tráfico saliente y una SA diferente para el tráfico entrante para cada canal de comunicación individual. Si un dispositivo se conecta a tres dispositivos, tendrá al menos seis SAs, uno por cada conexión entrante o saliente por dispositivo remoto. Entonces, ¿cómo puede un dispositivo mantener todas estas SAs organizadas y asegurarse de que se invoca la SA correcta para la conexión correcta? Con el SPI, así es como. Cada dispositivo tiene un SPI que realiza un seguimiento de los diversos SAs y le dice al dispositivo cuál es apropiado invocar para los diversos paquetes que recibe.

B es incorrecto porque no hay ningún componente dentro de IPSec oficialmente conocido como capacidad de seguridad. Esta es una respuesta distraída.

D es incorrecto porque no hay ningún componente dentro de IPSec conocido oficialmente como asistente de seguridad. Esta es una respuesta distraída.

39. ¿Cuál es el proceso descrito en la ilustración siguiente conocida como?



R. Modelo TCP/IP

B. acodo

C. encapsulación

D. Modelo OSI

☑ **C.** La ilustración muestra los datos que se mueven por las capas de la pila del modelo TCP/IP. Los datos de la capa de aplicación se convierten en la carga útil de un segmento TCP, preendiéndole los datos del protocolo TCP como encabezado. El segmento TCP se convierte en un paquete IP preendiendo los datos del protocolo IP como encabezado. El paquete IP se convierte en una trama Ethernet preendiendo los datos del protocolo Ethernet a él como encabezado. (También se une un pie de página pequeño en esta capa, no se representa.) Esto se conoce como encapsulación.

☒ **A** es incorrecto porque, aunque la ilustración muestra el uso del modelo TCP/IP, el proceso representado de su uso es encapsulación.

☒ **B** es incorrecto porque, aunque también se representa la estratificación, el procesamiento descendente de los datos que pasan a través de las capas es encapsulación.

☒ **D** es incorrecto porque el modelo en uso en la ilustración es el modelo TCP/IP de cuatro capas, no el modelo OSI de siete capas.

40. ¿Cuál de las siguientes es una finalidad de la capa de transporte?

R. La entrega salto a salto de paquetes de una red a otra

B. Representar datos en una estructura que pueden ser entendidos por procesos en los puntos finales

C. Encapsulación del paquete IP para el transporte

D. Garantizar una transferencia de datos fiable

☑ **D.** TCP, en la capa de transporte, proporciona entrega de segmentos de datos fiables, secuenciación y control de flujo, entre otras garantías.

☒ **A** es incorrecto porque la entrega salto a salto de paquetes entre redes es responsabilidad del protocolo IP.

☒ **B** es incorrecto porque la administración de las estructuras de datos pasadas entre aplicaciones en los puntos finales es el trabajo de la capa de presentación.

☒ **C** es incorrecto porque los paquetes IP encapsulan los segmentos TCP, no al revés.

41. ¿Cuál de las siguientes instrucciones NO es cierto acerca de la dirección IPv4 192.168.10.129\25?

R. Es una dirección privada especificada por RFC 1918.

B. La máscara de red para esta dirección es 255.255.255.0.

C. La dirección de red de la red que especifica es 192.168.10.128\25.

D. La parte del host de esta dirección de 32 bits es el orden bajo 7 bits.

☑ **B.** La notación de enrutamiento entredominio (CIDR) sin clase \25 para esta dirección indica que los 25 bits de orden superior (más a la izquierda) comprenden la parte de red y los 7 bits restantes de orden bajo (más a la derecha) 7 son la parte del host. En binario, la representación de la máscara de red tendría el siguiente aspecto: 1111111 1111111 1111111 100000000. La notación decimal "quad punted quad" de esta máscara de red sería entonces 255.255.255.128.

☒ **A** es incorrecto porque es una instrucción verdadera, ya que la dirección está dentro del intervalo 192.168.0.0\16 especificado por RFC 1918 como reservado para uso privado.

☒ **C** es incorrecto porque es una instrucción verdadera, ya que la dirección de red es la dirección donde la parte del host es todo 0. En binario el último byte sería 100000000, que es 128 en decimal.

☒ **D** es incorrecto porque es una instrucción verdadera, ya que la parte del host de esta dirección de 32 bits es los bits de 7 de orden bajo.

42. ¿Cuál de las siguientes declaraciones describe un protocolo "convergente"?

R. Es un término utilizado para describir una situación en la que dos protocolos independientes, que a menudo funcionan en la misma capa, se convierten en uno, como con Fibre Channel (FC) a través de Ethernet (FCoE).

B. Es cualquier situación donde un protocolo se encapsula con otro, como con TCP dentro de IP (TCP/IP).

C. Se refiere a cuando dos protocolos en la misma capa comienzan a hacer esencialmente lo mismo, como HTTP y HTTPS.

D. Es cualquier situación donde un Protocolo se encapsula dentro de otro protocolo de una manera que dobla o rompe el modelo OSI, como IPv6 sobre la encapsulación de ruteo genérico (GRE) sobre el IPv4.

☑ **R.** FCoE, al permitir que las tramas fibre channel más antiguas pasen sobre las tramas Ethernet, es un ejemplo de un protocolo convergente, ya que de lo contrario son ambos protocolos de enlace de datos.

☒ **B** es incorrecto, ya que simplemente describe la encapsulación, no la convergencia. Convergencia es una forma de encapsulación que desenfoca las líneas del modelo de capas.

☒ **C** es incorrecto porque un protocolo "convergente" no se refiere a cuando dos protocolos en la misma capa comienzan a hacer esencialmente lo mismo. El ejemplo específico de HTTP y HTTPS no es una situación convergente, sino más bien el uso de la semántica HTTP en capas a través de SSL/TLS o no.

☒ **D** es incorrecto porque un protocolo "convergente" no se refiere a ninguna situación donde un protocolo se encapsula dentro de otro de una manera que dobla o rompe el modelo OSI. El ejemplo específico de capas IPv6 sobre GRE sobre IPv4 dobla nuestro modelo OSI, pero es un ejemplo de tunelización, no de convergencia.

43. Ethernet utiliza un medio compartido para todas las estaciones en una LAN para comunicarse, y utiliza un enfoque de acceso múltiple de sentido portador con detección de colisión (CSMA/CD) para administrar las comunicaciones entre estaciones. ¿Cuál de las siguientes declaraciones sobre este protocolo explica mejor cómo funciona?

R. Una trama de control se pasa de estación en estación, concediendo permiso para que esa estación transmita una vez que se recibe.

B. Cada estación es necesaria para monitorear el medio para las transmisiones y transmitir solamente cuando todas las demás estaciones son silenciosas. Cada estación también es responsable de alertar a todas las demás estaciones si observa más de una estación que transmite al mismo tiempo.

C. Cada estación se requiere para monitorear el medio para las transmisiones y transmitir solamente cuando todas las demás estaciones son silenciosas. Cada estación también es responsable de señalar su intención de transmitir antes de hacerlo.

D. Una estación primaria es responsable de determinar cuál de las otras estaciones debe transmitir, sondeando cada una de ellas a intervalos regulares para determinar qué estación tiene datos que transmitir.

☑ **B.** Cada una de las respuestas anteriores describe los métodos para compartir un medio de comunicaciones y administrar colisiones. Con CSMA/CD, cada estación detecta si otra estación ya está transmitiendo antes de comenzar a hacerlo, pero también detecta si se ha producido una colisión, y notificando a todas las demás estaciones que necesitan retroceder antes de intentarlo de nuevo.

☒ **A** es incorrecto porque describe el paso de token en lugar de cualquier forma de CSMA.

☒ **C** es incorrecto porque, mientras que describe un enfoque de "sentido portador de acceso múltiple", describe además "evitación de colisiones" o CSMA/CA. En este esquema, cada estación anuncia que transmitirá, notificando al resto de estaciones que tendrán que esperar. Una vez que la estación transmisora detecta que el medio es silencioso, puede transmitir.

☒ **D** es incorrecto porque describe un esquema de sondeo con estaciones primarias y secundarias, en el que las colisiones son administradas solo por la estación primaria.

44. Dentro del ámbito de los componentes de red, ¿qué son los "puntos finales" y por qué plantean desafíos de seguridad tan difíciles?

R. Los puntos de conexión son los sistemas cliente de una red. Debido a que establecen conexiones a servidores internos y externos, sus actividades pueden ser difíciles de supervisar y controlar, y las descargas de software malicioso en el entorno son comunes.

B. Los puntos de conexión son los servidores a los que se conectan todos los clientes para la autenticación, el uso compartido de archivos y otros servicios. Debido al alto volumen de conexiones que soportan, puede ser difícil monitorear y detectar actividades maliciosas dirigidas a ellas, enterradas entre las actividades normales.

C. Los puntos de conexión son todo excepto los dispositivos de comunicación de red, incluidos escritorios, servidores, dispositivos móviles y otros sistemas integrados. Los desafíos de administración que plantean incluyen conectividad intermitente, falta de infraestructura de administración para algunas plataformas y la falta de disponibilidad de actualizaciones de software para otras.

D. Los puntos de conexión son principalmente sistemas móviles y de escritorio, que pueden existir o no estáticamente en la red. Como resultado, realizar un seguimiento de ellos para mantener el parcheo actualizado y la configuración adecuada puede ser difícil.

☑ **C.** Un "punto final" de red es cualquier cosa y todo lo que no es un dispositivo de infraestructura. En un entorno de Active Directory, tanto los escritorios como los servidores pueden tener un sólido régimen de administración y aplicación de revisiones. Sin embargo, otros puntos finales incluyen impresoras, dispositivos móviles, sistemas de punto de venta (PDV), dispositivos de Internet de las Cosas (IoT) y dispositivos de sistemas de control industrial (ICS) como controladores de calefacción, ventilación y aire acondicionado (HVAC). Para muchas de estas plataformas, es posible que simplemente no haya ninguna infraestructura de administración a escala empresarial disponible, y es posible que no sea posible aplicar parches contra vulnerabilidades conocidas.

☒ **A** es incorrecto porque los puntos finales abarcan más que los sistemas cliente, como se describe en la explicación anterior. Además, mientras que la supervisión para la recuperación de clientes de malware puede ser difícil, está dentro del ámbito de la capacidad de administración.

☒ **B** es incorrecto porque los puntos finales abarcan más que los servidores, como se describe en la explicación de la respuesta correcta. Además, los sistemas y software diseñados para monitorear la actividad maliciosa dirigida a dispositivos del lado del servidor son bastante maduros y capaces y pueden manejar grandes volúmenes de conexiones.

☒ **D** es incorrecto porque, de nuevo, los puntos de conexión abarcan más que los sistemas de cliente móvil o de escritorio, e incluyen una matriz de sistemas para los que pueden ni siquiera existir plataformas de administración y sistemas de parches.

45. ¿Cuál de los siguientes describe el mejor uso del Network Access Control (NAC)?

R. El uso del Protocolo de autenticación extensible (EAP) IEEE 802.1X para autenticar los puntos de conexión antes de permitirles unirse a una red

B. El uso combinado de una infraestructura de clave pública (PKI) y un módulo de plataforma segura de hardware (TPM) para realizar la autenticación de punto de conexión basada en certificados y establecer un vínculo seguro a través del intercambio de claves simétricas

C. La combinación de EAP para la autenticación de punto final y la autenticación de usuario multifactor para un control altamente granular

D. El uso de EAP tanto para la autenticación de punto final como para la inspección de los niveles de parches del sistema operativo de punto final y las actualizaciones antimalware, con el objetivo de colocar sistemas que no son de confianza en un segmento VLAN en cuarentena

☑ **D.** El NAC puede y debe utilizar alguna forma de EAP para la autenticación del punto final, pero el mejor uso común de él es habilitar un sistema autenticado para ser inspeccionado en cuanto a su postura de seguridad. Si el sistema está atrasado en su nivel de parche o actualizaciones antimalware, o generalmente está mal configurado, debe colocarse en una VLAN que le dé acceso solamente a los sistemas que proporcionan las actualizaciones necesarias y la administración de la configuración. Una vez que el sistema cumple los requisitos de directiva, se puede reasignar al segmento LAN protegido adecuado.

☒ **A** es incorrecto porque no va lo suficientemente lejos. Como se acaba de explicar, el EAP también se debe utilizar para controlar el acceso concedido a un nodo autenticado.

☒ **B** es incorrecto porque, como arriba, no va lo suficientemente lejos. Los sistemas autenticados deben examinarse en cuanto al cumplimiento de sus configuraciones antes de que se les permita el acceso a redes protegidas.

☒ **C** es incorrecto porque, mientras que la autenticación de usuario multifactor es una buena idea, no es relevante para el NAC, que se orienta al sistema sí mismo, no al usuario que ha iniciado sesión en él.

46. ¿Cuál es la mayor debilidad, y por lo tanto preocupación, con las redes virtualizadas?

R. Dado que las tarjetas de interfaz de red (NIC) están virtualizadas (vNICs), los datos que viajan entre ellos simplemente se copian de una ubicación de memoria a otra mediante la capa de hipervisor en un único host físico.

B. La ausencia de una red física hace imposible implementar firewalls o sistemas de detección de intrusiones para regular y supervisar el tráfico entre los sistemas virtuales.

C. Las redes virtuales son esencialmente nubes sin topologías bien definidas. Esto hace que las rutas de acceso de red entre sistemas virtuales sean imposibles de saber.

D. Las NIC virtuales tienen rendimientos mucho más altos que los físicos. Como resultado, los modernos sistemas de detección de intrusiones basados en red (NIDS) no pueden inspeccionar su tráfico a velocidades en tiempo real.

☑ **R.** La red virtualizada significa que la transmisión de datos no cruza un vínculo físico, sino que es simplemente una operación de memoria dentro de un único host en el que residen todos los sistemas virtuales. En consecuencia, un único compromiso del hipervisor puede dar lugar esencialmente a un compromiso de la totalidad de la red virtual que proporciona.

☒ **B** es incorrecto porque se pueden implementar firewalls virtuales y sistemas de detección de intrusiones, aunque solo pueden regular y supervisar los vínculos virtuales entre los sistemas del hipervisor. Sin embargo, si el hipervisor en sí está comprometido, todavía se pueden eludir.

☒ **C** es incorrecto porque las redes virtuales pueden y tienen topologías bien definidas, con las rutas virtuales entre los sistemas virtuales diseñados hacia una infraestructura conocida y defendible. Sin embargo, todavía dependen de la seguridad del hipervisor dentro del cual se construyen.

☒ **D** es incorrecto. Si bien es cierto que el rendimiento de un vínculo virtual entre sistemas está definido por software y limitado a velocidades de CPU y memoria en lugar de las velocidades de las interfaces NIC físicas, también lo son las capacidades de los dispositivos de supervisión virtual implementados.