MÓDULOS 10 – 13: EXAMEN DE SEGURIDAD L2 Y WLAN RESPUESTAS

30/08/2021 CCNA 2 v7 Respuestas

Spread the love

Última actualización: octubre 13, 2024

Examen de punto de control: Examen de seguridad L2 y WLAN Respuestas

Módulos 10 – 13 del currículo Principios básicos de routing, switching y redes inalámbricas CCNA2 – v7.0 (SRWE) Español

1. ¿Cuál es el resultado de un ataque de agotamiento de DHCP?

- Los clientes legítimos no pueden arrendar direcciones IP.
- El atacante proporciona información incorrecta de DNS y gateway predeterminado a los clientes.
- Se secuestran las direcciones IP asignadas a los clientes legítimos.
- Los clientes reciben asignaciones de direcciones IP de un servidor DHCP dudoso.

> **Explique:** Los ataques de agotamiento de DHCP los realiza un atacante con la intención de crear un DoS para los clientes de DHCP. Para lograr este objetivo, el atacante usa una herramienta que envía muchos mensajes de DHCPDISCOVER para arrendar el conjunto completo de direcciones IP disponibles, para así negárselas a los hosts legítimos.

2. ¿Qué representa una práctica recomendada en relación con protocolos de descubrimiento como CDP y LLDP en dispositivos de red?

- Utilice el LLDP estándar abierto en lugar de CDP.
- Deshabilite ambos protocolos en todas las interfaces donde no sean necesarios.
- Utilice la configuración predeterminada del enrutador para CDP y LLDP.
- Habilite CDP en dispositivos perimetrales y habilite LLDP en dispositivos interiores.

> **Explique:** Ambos protocolos de descubrimiento pueden proporcionar a los hackers información confidencial de la red. No deben habilitarse en dispositivos perimetrales y deben deshabilitarse globalmente o por interfaz si no es necesario. CDP está habilitado por defecto.

3. ¿Qué declaración describe el comportamiento de un conmutador cuando la tabla de direcciones MAC está llena?

- Trata las tramas como unidifusión desconocida e inunda todas las tramas entrantes a todos los puertos a través de varios conmutadores.
- Trata las tramas como unidifusión desconocida e inunda todas las tramas entrantes a todos los puertos dentro del dominio de colisión.
- Trata las tramas como unidifusión desconocida e inunda todas las tramas entrantes a todos los puertos del switch.
- Trata las tramas como unidifusión desconocida e inunda todas las tramas entrantes a todos los puertos dentro de la VLAN local.

Explique: Cuando la tabla de direcciones MAC está llena, el conmutador trata la trama como una unidifusión desconocida y comienza a inundar todo el tráfico entrante a todos los puertos solo dentro de la VLAN local.

4. ¿Qué característica de un switch lo hace vulnerable a los ataques de salto de VLAN?

- el tamaño limitado del espacio de memoria direccionable por contenido
- la función de puerto troncal automático habilitada para todos los puertos de forma predeterminada
- compatibilidad de ancho de banda de puertos mixtos habilitada para todos los puertos de forma predeterminada
- el modo dúplex mixto habilitado para todos los puertos de forma predeterminada

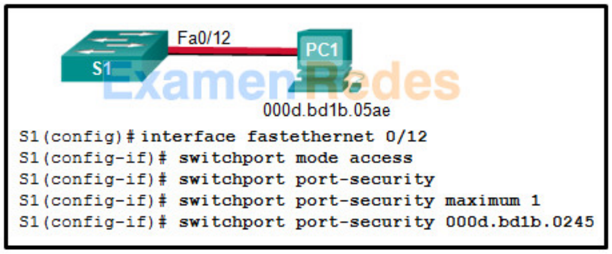
Explique: El VLAN Hopping permite que una VLAN pueda ver el tráfico de otra VLAN sin cruzar primero un router. En un ataque de salto de VLAN básico, el atacante configura un host para que actúe como un switch, para aprovechar la función de puerto de enlace automático habilitada de forma predeterminada en la mayoría de los puertos del switch.

5. ¿Qué componente de AAA se utiliza para determinar los recursos a los que puede acceder el usuario y las operaciones que tiene permitido realizar?

- Registro
- Autorización
- Auditoría
- Autenticación

Explique: Uno de los componentes de AAA es la Autorización. Una vez que se autentica usuario a través de AAA, los servicios de autorización determinan a qué recursos puede acceder el usuario y qué operaciones tiene permitido realizar.

6. Consulte la ilustración. La seguridad del puerto se ha configurado en la interfaz Fa 0/12 del conmutador S1. ¿Qué acción ocurrirá cuando PC1 esté conectado al conmutador S1 con la configuración aplicada?



Módulos 10 – 13: Examen de seguridad L2 y WLAN Respuestas 14

- Se eliminarán las tramas de PC1 y se creará un mensaje de registro.
- Las tramas de PC1 se reenviarán a su destino, pero no se creará una entrada de registro.
- Las tramas de PC1 provocarán que la interfaz se cierre inmediatamente y se realizará una entrada de registro.
- Las tramas de PC1 se eliminarán y no habrá registro de la infracción.
- Las tramas de PC1 se reenviarán ya que falta el comando switchport port-security violation .
- Las tramas de PC1 se reenviarán a su destino y se creará una entrada de registro.

Explique: Se ha introducido la configuración manual de la única dirección MAC permitida para el puerto fa0/12.PC1 tiene una dirección MAC diferente y cuando está conectado hará que el puerto se cierre (la acción predeterminada), se cree automáticamente un mensaje de registro y se incremente el contador de infracciones. Se recomienda la acción predeterminada de apagado porque la opción restringir podría fallar si se está ejecutando un ataque.

7. Un administrador de red configura la seguridad de puertos en un switch de Cisco. La política de seguridad de la compañía especifica que cuando se produce una violación, los paquetes con direcciones de origen desconocidas deben descartarse y no se debe enviar ninguna notificación. ¿Qué modo de violación se debe configurar en las interfaces?

- protect
- shutdown
- Off
- restrict

Explique: En un switch de Cisco, se puede configurar una interfaz para uno de tres modos de violación con la acción específica que se debe realizar si se produce una violación:
Protección : los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. No hay ninguna notificación de que se produjo una violación de seguridad.

Restricción : los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. En este modo, hay una notificación de que se produjo una violación de seguridad.
Apagado : la interfaz se inhabilita de inmediato por errores y se apaga el LED del puerto.

8. ¿Qué beneficio de seguridad se obtiene al habilitar la protección BPDU en interfaces habilitadas para PortFast?

- evitar que se agreguen conmutadores no fiables a la red
- protección contra bucles de capa 2
- preventing buffer overflow attacks
- aplicar la colocación de puentes raíz

Explique: BPDU guard – inmediatamente inhabilita un puerto que recibe un BPDU. Esto evita que se agreguen conmutadores no fiables a la red. La protección BPDU solo debe aplicarse a todos los puertos de usuario final.

9. ¿Qué tipo de ataque de salto de VLAN se puede evitar designando una VLAN no utilizada como VLAN nativa?

- VLAN double-tagging
- Inanición de DHCP
- DTP spoofing
- Suplantación de identidad de DHCP

Explique: La suplantación de mensajes DTP obliga a un conmutador a entrar en modo de enlace troncal como parte de un ataque de salto de VLAN, pero el doble etiquetado de VLAN funciona incluso si los puertos troncales están deshabilitados. Cambiar la VLAN nativa de la predeterminada a una VLAN no utilizada reduce la posibilidad de este tipo de ataque. La suplantación de DHCP y la inanición de DHCP aprovechan las vulnerabilidades en el intercambio de mensajes DHCP.

10. Un administrador de red ingresa la siguiente secuencia de comandos en un switch Cisco 1.

```
SW1 (config) # Interface range fa0/5 – 10
SW1 (config-if) # ip dhcp snooping limit rate 6
```

¿Cuál es el efecto después de ingresar estos comandos?

- Si alguno de los puertos FastEthernet 5 a 10 recibe más de 6 mensajes DHCP por segundo, el puerto se apagará.

- Los puertos FastEthernet 5 a 10 pueden recibir hasta 6 mensajes de descubrimiento DHCP por segundo.
- Los puertos FastEthernet 5 a 10 pueden recibir hasta 6 mensajes DHCP por segundo de cualquier tipo.
- Si alguno de los puertos FastEthernet 5 a 10 recibe más de 6 mensajes DHCP por segundo, el puerto seguirá funcionando y se enviará un mensaje de error al administrador de la red.

> **Explique:** Cuando se configura la inspección DHCP, la cantidad de mensajes de descubrimiento de DHCP que los puertos no confiables pueden recibir por segundo debe tener una velocidad limitada mediante el uso del comando ip dhcp snooping limit rate en la nterface. Cuando un puerto recibe más mensajes de los que permite la velocidad, se eliminarán los mensajes adicionales.

11. ¿Qué dos comandos se pueden usar para habilitar la protección BPDU en un switch? (Escoja dos opciones).

- S1(config-if)# enable spanning-tree bpduguard
- S1(config-if)# spanning-tree bpduguard enable
- S1(config)# spanning-tree portfast bpduguard default
- S1(config-if)# spanning-tree portfast bpduguard
- S1(config)# spanning-tree bpduguard default

> **Explique:** El comando spanning-tree portfast bpduguard default del modo de configuración global habilita la protección BPDU en todos los puertos con PortFast habilitado. Utilice el comando del modo de configuración de interfaz spanning-tree bpduguard enable para habilitar la protección de BPDU en un puerto.

12. ¿Cuáles son los dos métodos utilizados por una NIC inalámbrico para descubrir un AP? (Elija dos).

- entrega de una trama de difusión
- envío de una solicitud de ARP
- comienzo de un protocolo de enlace de tres vías
- recepción de una trama de señal de difusión
- transmisión de una solicitud de sondeo

> **Explique:** Un dispositivo inalámbrico puede utilizar dos métodos para descubrir un punto de acceso y registrarse en él: el modo pasivo y el modo activo. En el modo pasivo, el AP envía una trama de señal de difusión que contiene el SSID y otros parámetros de configuración inalámbrica. En el modo activo, el

dispositivo inalámbrico se debe configurar manualmente para el SSID y, a continuación, el dispositivo transmite por difusión una solicitud de sondeo.

13. ¿Qué topología de red inalámbrica se usaría por los ingenieros de redes para brindar una red inalámbrica para un edificio entero universitarios?

- Modo mixto
- pública
- Infraestructura
- Ad hoc

Explique: El modo ad hoc (también conocido como conjunto de servicios básicos independientes o IBSS) se utiliza en una red inalámbrica peer-to-peer cuando se utiliza la tecnología Bluetooth, por ejemplo. Se produce una variación de la topología ad hoc cuando se permite que un smartphone o una tablet PC con acceso celular a datos creen una zona de cobertura inalámbrica personal. El modo mixto permite que las NIC inalámbricas más antiguas se conecten a un punto de acceso que puede utilizar un estándar inalámbrico más nuevo.

14. ¿Qué es un modo de seguridad inalámbrica que requiere un servidor RADIUS para autenticar usuarios inalámbricos?

- personal
- WEP
- empresa
- clave compartida

Explique: Existen dos tipos de WPA y WPA2: Personal y Enterprise. Personal se utiliza en redes domésticas y de oficinas pequeñas. La clave compartida admite tres técnicas de autenticación diferentes: (1) WEP, (2) WPA y (3) 802.11i/WPA2. WEP es un método de cifrado.

15. Un técnico configura el canal en un router inalámbrico en 1, 6 u 11. ¿Cuál es la finalidad de ajustar el canal?

- Evitar la interferencia de dispositivos inalámbricos próximos.
- Proporcionar modos de seguridad más sólidos.
- Desactivar la transmisión de SSID.
- Habilitar distintos estándares 802.11.

Explique: Los canales 1, 6 y 11 se seleccionan porque son cinco canales separados, lo que minimiza la interferencia con los canales adyacentes. La frecuencia de canal puede interferir con los canales a cada lado de la frecuencia principal. Todos los dispositivos inalámbricos deben utilizarse en canales no adyacentes.

16. Se le pide a un administrador de red que actualice el acceso inalámbrico para usuarios finales en un edificio. Para proporcionar velocidades de datos de hasta 1,3 Gb/s y seguir siendo compatible con dispositivos más antiguos, ¿qué estándar inalámbrico debe implementarse?

- 802.11b
- 802.11n
- 802.11ac
- 802.11g

Explique: El estándar 802.11ac proporciona velocidades de datos de hasta 1,3 Gb/s y sigue siendo compatible con dispositivos 802.11a/b/g/n. 802.11g y 802.11n son estándares más antiguos que no pueden alcanzar velocidades superiores a 1 Gb/s. 802.11ad es un estándar más reciente que puede ofrecer velocidades teóricas de hasta 7 Gb/s.

17. En un panel WLC de Cisco 3504, ¿qué opción proporciona acceso al menú completo de funciones?

- Network Summary
- Avanzado
- Puntos de acceso
- Rogues

Explique: El panel WLC 3504 de Cisco se muestra cuando un usuario inicia sesión en el WLC. La mayoría de los WLC tienen configuraciones básicas y menús que los usuarios pueden accesar rápidamente para implementar una variedad de configuraciones comunes. Al hacer clic en el botón Avanzado , el usuario accederá a la página Resumen avanzado y accederá a todas las funciones del WLC.

18. ¿Qué protocolo se puede utilizar para supervisar la red?

- DHCP
- AAA

- RADIUS
- SNMP

Explique: El protocolo simple de administración de redes (SNMP) es un protocolo de capa de aplicación utilizado para monitorear y administrar la red.

19. ¿Qué servicio se puede utilizar en un enrutador inalámbrico para priorizar el tráfico de red entre diferentes tipos de aplicaciones, de modo que los datos de voz y vídeo se prioricen sobre los datos de correo electrónico y web?

- NAT
- DHCP
- DNS
- QoS

Explique: Muchos routers inalámbricos tienen una opción para configurar la Calidad de Servicio (QoS). Al configurar la QoS, puede garantizar que ciertos tipos de tráfico, como voz y video, tengan prioridad respecto del tráfico sin plazos, como el correo electrónico y la navegación web.

20. ¿Qué paso se requiere antes de crear una nueva WLAN en un WLC de la serie 3500 de Cisco?

- Cree o tenga disponible un servidor SNMP.
- Cree o tenga disponible un servidor RADIUS.
- Cree un nuevo SSID.
- Crear una nueva interfaz VLAN.

Explique: Cada nueva WLAN configurada en un WLC de la serie 3500 de Cisco necesita su propia interfaz VLAN. Por lo tanto, es necesario que se cree primero una nueva interfaz VLAN antes de que se pueda crear una nueva WLAN.

21. Un administrador de red está trabajando para mejorar el rendimiento de la WLAN en un enrutador inalámbrico de doble banda. ¿Cuál es una forma simple de lograr un resultado dividido en el tráfico?

- Asegúrese de que se utilizan diferentes SSID para las bandas de 2,4 GHz y 5 GHz.
- Agregue un extensor de alcance Wi-Fi a la WLAN y configure el AP y el extensor de alcance para que sirvan diferentes bandas.
- Requerir que todos los dispositivos inalámbricos utilicen el estándar 802.11n.

- Mantenga el firmware del router inalámbrico actualizado

> **Explique:** Los routers y APs de doble banda usan el mismo nombre de red tanto en la banda de 2.4 Ghz como en la de 5 Ghz de manera predeterminada. La manera mas sencilla de segmentar el trafico es renombrar una de las redes inalámbricas.

22. Un administrador de red está agregando una nueva WLAN en un WLC de la serie 3500 de Cisco. La configuración requiere una contraseña secreta compartida. ¿Cuál es el propósito de la contraseña secreta compartida?

- El servidor RADIUS lo utiliza para autenticar a los usuarios de WLAN.
- Se utiliza para cifrar los mensajes entre el WLC y el servidor RADIUS.
- Permite a los usuarios autenticar y acceder a la WLAN.
- Se utiliza para autenticar y cifrar datos de usuario en la WLAN.

> **Explique:** El protocolo RADIUS utiliza características de seguridad para proteger las comunicaciones entre el servidor RADIUS y los clientes. Esta es la contraseña que se usa entre el WLC y el servidor RADIUS. No es para usuarios finales.

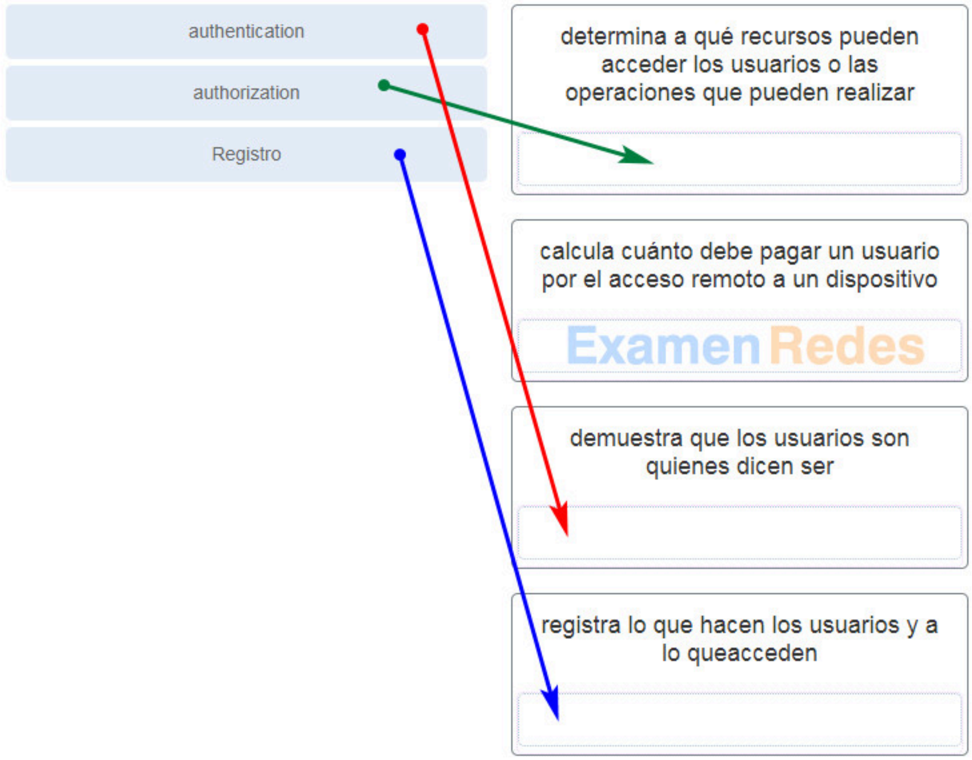
23. ¿Qué componente de control de acceso, implementación o protocolo audita las acciones de los usuarios que se realizan en la red?

- Registro
- Autorización
- 802.1x
- Autenticación

24. ¿Qué tipo de red inalámbrica utiliza transmisores para proporcionar servicios inalámbricos en una gran región urbana?

- wireless wide-area network
- wireless local-area network
- wireless personal-area network
- wireless metropolitan-area network

25. Haga coincidir cada componente funcional de AAA con su descripción. (No se utilizan todas las opciones).



Módulos 10 – 13: Examen de seguridad L2 y WLAN Respuestas 67

26. ¿Qué dos soluciones de Cisco ayudan a prevenir los ataques de inanición de DHCP? (Escoja dos opciones).

- Web Security Appliance
- Detección DHCP
- Seguridad de puertos
- Protección de la IP de origen
- Inspección dinámica de ARP

Explique: Cisco proporciona soluciones para ayudar a mitigar los ataques de la capa 2 incluyendo:

IP Source Guard (IPSG) – previene los ataques de suplantación de direcciones MAC e IP

La inspección dinámica de ARP (DAI) previene la suplantación de ARP y los ataques de envenenamiento de ARP.

La detección DHCP – impide el agotamiento de direcciones DHCP y los ataques de suplantación de DHCP.

Seguridad de puertos (Port Security) – previene muchos tipos de ataques, incluidos los ataques de desbordamiento de la tabla MAC y los ataques de agotamiento de DHCP

Cisco Web Security Appliance (WSA) es una tecnología de mitigación para amenazas basadas en la web.

27. ¿Cuáles son tres técnicas de mitigación de ataques de VLAN? (Elija tres opciones.)

- Habilitar la protección BPDU.

- Configurar la VLAN nativa en una VLAN sin usar.
- Desactivar el DTP.
- Habilitar la protección de origen.
- Usar VLAN privadas.
- Habilitar manualmente los enlaces troncales.

Explique: La mitigación de un ataque de VLAN puede realizarse deshabilitando el protocolo de enlace troncal dinámico (DTP), configurando manualmente los puertos en modo de enlace troncal y estableciendo la VLAN nativa de enlaces troncales a las VLAN que no están en uso.

28. Consulte la ilustración. ¿Qué se puede determinar sobre la seguridad de puertos a partir de la información que se muestra?

```
ATC_S2# show port-security interface fastethernet 0/3
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 2
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 1
Last Source Address:Vlan     : 00D0.D3B6.C26B:10
Security Violation Count     : 0
```


Módulos 10 – 13: Examen de seguridad L2 y WLAN Respuestas 70

- El puerto tiene dos dispositivos conectados.
- El modo de violación de puertos es el modo predeterminado para todos los puertos que tengan habilitada la seguridad de puertos.
- El puerto se desconectó.
- El puerto tiene la cantidad máxima de direcciones MAC que admiten los puertos de switch de capa 2 configurados para la seguridad de puertos.

Explique: La línea de seguridad de puertos muestra simplemente un estado Enabled (Habilitado) si se ingresó el comando switchport port-security (sin opciones) para un puerto de switch en particular. Si se ha producido una violación de seguridad de puertos, aparece otro mensaje de error, por ejemplo, Secure-shutdown (Apagado seguro). El número máximo de direcciones MAC admitido es 50. La línea Maximum MAC Addresses (Cantidad máxima de direcciones MAC) se utiliza para mostrar cuántas direcciones MAC pueden descubrirse (2 en este caso). La línea Sticky MAC Addresses (Direcciones MAC persistentes) muestra que el switch solo detectó automáticamente un dispositivo que se ha conectado. Esta configuración podría utilizarse cuando un puerto es compartido por los empleados que comparten dos cubículos que incorporan equipos portátiles diferentes.

29. Un administrador de red de una universidad está configurando el proceso de autenticación de usuario de WLAN. Los usuarios inalámbricos deben introducir credenciales de nombre de usuario y contraseña que serán verificadas por un servidor. ¿Qué servidor prestaría tal servicio?

- AAA
- NAT
- SNMP
- RADIUS

> **Explique:** El Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un protocolo y software de servidor que proporciona autenticación basada en usuarios para una organización. Cuando se configura una WLAN para utilizar un servidor RADIUS, los usuarios introducirán las credenciales de nombre de usuario y contraseña verificadas por el servidor RADIUS antes de permitir la WLAN.

30. Un técnico está solucionando problemas con una WLAN lenta que consta de dispositivos 802.11b y 802.11g. Se ha implementado un nuevo router de doble banda 802.11n/ac en la red para reemplazar el antiguo router 802.11g. ¿Qué puede hacer el técnico para abordar la velocidad inalámbrica lenta?

- Cambiar SSID predeterminado.
- Configure los dispositivos para que utilicen un canal diferente.
- Dividir el trafico inalambrico entre las bandas 802.11n de 2.4 GHz y 5 GHz.
- Actualice el firmware en el nuevo enrutador.

> **Explique:** Dividir el tráfico inalámbrico entre la banda 802.11n 2.4 GHz y la banda 5 GHz permitirá que el 802.11n utilice las dos bandas como dos redes inalámbricas separadas para ayudar a administrar el tráfico, mejorando así el rendimiento inalámbrico.

31. Estados del manual de la empresa que los empleados tengan hornos microondas en sus oficinas. En cambio, todos los empleados deben utilizar hornos microondas ubicados en la cafetería de los empleados. ¿Qué riesgo de seguridad inalámbrica es la empresa que intenta evitar?

- dispositivos configurados incorrectamente
- puntos de acceso no autorizados
- Intercepción de datos
- interferencia accidental

Explique: Los ataques por denegación de servicio pueden ser el resultado de la configuración incorrecta de los dispositivos, lo que puede deshabilitar la WLAN. La interferencia accidental de dispositivos como los hornos de microondas y los teléfonos inalámbricos puede afectar la seguridad y el rendimiento de una WLAN. Los ataques man-in-the-middle (intermediario) pueden permitir que un atacante intercepte datos. Los puntos de acceso no autorizados pueden permitir que accedan usuarios sin autorización a la red inalámbrica.

32. ¿Cuál es la función proporcionada por el protocolo CAPWAP en una red inalámbrica corporativa?

- CAPWAP crea un túnel en puertos TCP (Protocolo de control de transmisión) para permitir que un WLC configure un punto de acceso autónomo.
- CAPWAP proporciona la encapsulación y reenvío del tráfico de usuario inalámbrico entre un punto de acceso y un controlador LAN inalámbrico.
- CAPWAP proporciona el cifrado del tráfico de usuario inalámbrico entre un punto de acceso y un cliente inalámbrico.
- CAPWAP proporciona conectividad entre un punto de acceso que utiliza direccionamiento IPv6 y un cliente inalámbrico que utiliza direccionamiento IPv4.

Explique: CAPWAP es un protocolo estándar IEEE que permite que un WLC administre múltiples AP y WLANs. CAPWAP también es responsable de la encapsulación y el reenvío del tráfico del cliente WLAN entre un AP y un WLC.

33. Abra la actividad de PT. Realice las tareas en las instrucciones de la actividad y luego responda la pregunta.
¿Qué evento tendrá lugar si hay una violación de seguridad de puerto en la interfaz Fa0/1 del switch S1?

- Se registra un mensaje de syslog.
- La interfaz entra en el estado deshabilitado por error.
- Se envía una notificación.
- Se descartan los paquetes con direcciones de origen desconocidas.

Explique: El modo de violación puede verse emitiendo el comando show port-security interface . <int> command. La interfaz FastEthernet 0/1 se configura con el modo de violación de protección. Si hay una violación, la interfaz FastEthernet 0/1 descartará los paquetes con direcciones MAC desconocidas.

34. ¿Qué método de autenticación almacena nombres de usuario y contraseñas en el router y es ideal para redes pequeñas?

- AAA basado en servidor
- AAA local sobre RADIUS
- AAA local sobre TACACS+
- AAA local
- AAA basado en servidor sobre TACACS+
- AAA basado en servidor sobre RADIUS

> **Explique:** En una red pequeña con algunos dispositivos de red, la autenticación AAA se puede implementar con la base de datos local y con nombres de usuario y contraseñas almacenados en los dispositivos de red. La autenticación con el protocolo TACACS+ o RADIUS requerirá servidores ACS dedicados, aunque esta solución de autenticación se escala bien en una red grande.

35. ¿Qué protocolo se debe usar para mitigar la vulnerabilidad de usar Telnet para administrar dispositivos de red de forma remota?

- TFTP
- SNMP
- SSH
- SCP

> **Explique:** Telnet utiliza texto sin formato para comunicarse en una red. El nombre de usuario y la contraseña se pueden capturar si se intercepta la transmisión de datos. SSH cifra las comunicaciones de datos entre dos dispositivos de red. TFTP y SCP se utilizan para la transferencia de archivos a través de la red. SNMP se utiliza en soluciones de administración de red.

36. ¿Qué dispositivo se considera un suplicante durante el proceso de autenticación de 802.1x?

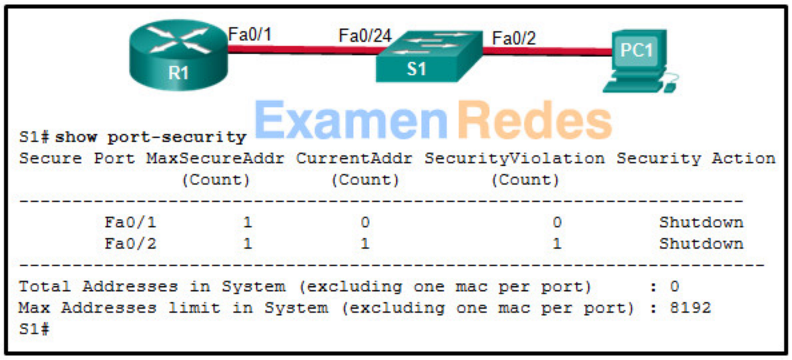
- el servidor de autenticación que realiza la autenticación del cliente
- el router que funciona como gateway predeterminado
- el switch que controla el acceso a la red
- el cliente que solicita la autenticación

> **Explique:** Los dispositivos involucrados en el proceso de autenticación de 802.1x son los siguientes:
> El suplicante, que es el cliente que solicita acceso a la red
> El autenticador, que es el switch al que se conecta el cliente y que está controlando realmente el acceso

físico a la red

El servidor de autenticación, que realiza la autenticación real

37. Consulte la ilustración. La interfaz Fa0/2 del conmutador S1 se ha configurado con el comando switchport port-security mac-address 0023.189d.6456 y se ha conectado una estación de trabajo. ¿Cuál podría ser la razón por la que la interfaz Fa0/2 se apaga?

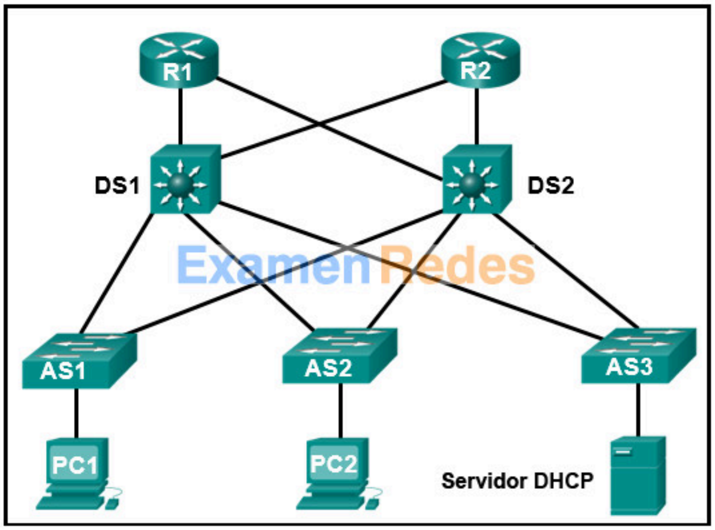


Módulos 10 – 13: Examen de seguridad L2 y WLAN Respuestas 12

- La dirección MAC de PC1 que se conecta a la interfaz Fa0/2 no es la dirección MAC configurada.
- La conexión entre S1 y PC1 se realiza a través de un cable cruzado.
- La interfaz Fa0/24 de S1 está configurada con la misma dirección MAC que la interfaz Fa0/2.
- S1 se ha configurado con un comando switchport port-security aging .

Explique: El contador de infracciones de seguridad para Fa0/2 se ha incrementado (como prueba 1 en la columna SecurityViolation). Las direcciones más seguras permitidas en el puerto Fa0/2 es 1 y esa dirección se introdujo manualmente. Por lo tanto, PC1 debe tener una dirección MAC diferente a la configurada para el puerto Fa0/2. Las conexiones entre los dispositivos finales y el conmutador, así como las conexiones entre un enrutador y un conmutador, se realizan con un cable directo.

38. Consulte la ilustración. La PC1 y la PC2 deberían poder obtener las asignaciones de direcciones IP del servidor DHCP. ¿Cuántos puertos entre los switches se deben asignar como puertos confiables como parte de la configuración de detección DHCP?



Módulos 10 – 13: Examen de seguridad L2 y WLAN Respuestas 18

- 7
- 5
- 1
- 3

Explique: La configuración de detección DHCP incluye la creación de la base de datos de vinculación a la detección DHCP y la asignación de los puertos confiables que sean necesarios en los switches. Un puerto confiable se dirige a los servidores DHCP legítimos. En este diseño de red, ya que el servidor DHCP está conectado a AS3, se deben asignar siete puertos de switch como puertos confiables, uno en AS3 dirigido al servidor DHCP, otro en DS1 hacia AS3, otro en DS2 hacia AS3 y dos conexiones en AS1 y AS2 (hacia DS1 y DS2), para sumar un total de siete.

39. Un administrador de red está configurando DAI en un conmutador con el comando ip arp inspection validate src-mac . ¿Cuál es el objetivo de este comando de configuración?

- Comprobar la dirección MAC de destino en el encabezado de Ethernet contra la tabla dirección MAC
- Comprobar la dirección dirección MAC de destino en el encabezado de Ethernet contra las ACL ARP configuradas por el usuario
- Comprueba la dirección de origen L2 en el encabezado de Ethernet contra la dirección del remitente L2 en el cuerpo ARP.
- Comprueba la dirección de origen L2 en el encabezado de Ethernet contra la dirección de destino L2 en el cuerpo ARP.

Explique: DAI se puede configurar para comprobar si hay dirección MAC e IP de destino o de origen:
– MAC de destino : comprueba la dirección MAC de destino en el encabezado de Ethernet con la

dirección MAC de destino en el cuerpo ARP.
MAC de origen Comprueba la dirección MAC de origen en el encabezado de Ethernet con la dirección MAC del remitente en el cuerpo ARP.
Direcciones IP – Comprueba el cuerpo ARP para Direcciones IP no válidas e inesperadas, incluidas las direcciones 0.0.0.0, 255.255.255.255 y todas las direcciones de multidifusión IP.

40. Como parte de la nueva política de seguridad, todos los switches de la red están configurados para aprender automáticamente las direcciones MAC de cada puerto. Todas las configuraciones en ejecución se guardan en el inicio y cierre de cada día hábil. Una tormenta fuerte causa un corte de energía prolongado varias horas después del cierre de negocio. Cuando los switches se vuelven a activar, estos conservan las direcciones MAC aprendidas dinámicamente. ¿Qué configuración de seguridad de puertos habilitó esto?

- direcciones MAC autoprotegidas
- direcciones MAC seguras estáticas
- direcciones MAC seguras persistentes
- direcciones MAC seguras dinámicas

Explique: Con las direcciones MAC seguras persistentes, las direcciones MAC pueden detectarse de forma dinámica o configurarse de forma manual y luego almacenarse en la tabla de direcciones para agregarse a la configuración en ejecución. En cambio, las direcciones MAC seguras dinámicas posibilitan las direcciones MAC descubiertas dinámicamente que se almacenan solo en la tabla de direcciones.

41. ¿Qué tipo de antena inalámbrica es más adecuado para proporcionar cobertura en espacios abiertos grandes, como entradas o salas de conferencias grandes?

- direccional
- Yagi
- omnidireccional
- plato

Explique: Las antenas omnidireccionales envían las señales de radio en un patrón de 360º alrededor de la antena. Esto brinda cobertura a los dispositivos ubicados en cualquier lugar alrededor del punto de acceso. Las antenas parabólicas, direccionales y Yagi dirigen las señales de radio en una única dirección, por lo que son menos adecuadas para cubrir áreas extensas y abiertas.

42. Durante una conferencia, los participantes utilizan computadoras portátiles para obtener conectividad de red. Cuando uno de los disertantes intenta conectarse a la red, la computadora portátil no puede mostrar

ninguna red inalámbrica disponible. ¿En qué modo debe de estar funcionando el punto de acceso?

- Abierta
- pasiva
- mixto
- activa

Explique: El modo activo se utiliza para configurar un punto de acceso de modo que los clientes deban conocer el SSID para conectarse a dicho AP. Los AP y los routers inalámbricos pueden funcionar en modo mixto, lo que significa que admiten varios estándares inalámbricos. El modo abierto es un modo de autenticación para un punto de acceso que no afecta la lista de redes inalámbricas disponibles para un cliente. Cuando un punto de acceso está configurado en modo pasivo, el SSID se transmite por difusión de modo que el nombre de la red inalámbrica aparezca en la lista de redes disponibles para los clientes.

43. En una página Resumen del WLC 3504 de Cisco (Avanzado > Resumen), ¿qué pestaña permite a un administrador de red configurar una WLAN determinada con una directiva WPA2?

- ADMINISTRACIÓN
- Redes de área local inalámbrica (WLAN)
- SEGURIDAD
- INALÁMBRICO

Explique: La pestaña WLANs en la página de Summary de Cisco 3504 WLC le permite al usuario acceder a la configuración de WLAN incluyendo seguridad, QoS y mapeo de políticas.

44. Un administrador de red implementa un enrutador inalámbrico en un pequeño bufete de abogados. Los portátiles de los empleados se unen a la WLAN y reciben direcciones IP en la red 10.0.10.0/24. ¿Qué servicio se utiliza en el enrutador inalámbrico para permitir que las computadoras portátiles de los empleados accedan a Internet?

- DNS
- DHCP
- RADIUS
- NAT

Explique: Cualquier dirección con el 10 en el primer octeto es una dirección IPv4 privada y no se puede enrutar en Internet. El router utilizará un proceso llamado Traducción de direcciones de red (NAT) para convertir las direcciones IPv4 privadas en direcciones IPv4 enrutables por Internet.

45. Un ingeniero de red resuelve problemas en una red inalámbrica que se implementó recientemente y que utiliza los últimos estándares 802.11. Cuando los usuarios acceden a servicios de ancho de banda elevado, como la transmisión de video, el rendimiento de la red inalámbrica es deficiente. Para mejorar el rendimiento, el ingeniero de red decide configurar un SSID de banda de frecuencia de 5 Ghz y capacitar a los usuarios para utilizar ese SSID para los servicios de transmisión de medios. ¿Por qué esta solución podría mejorar el rendimiento de la red inalámbrica para ese tipo de servicio?

- Requerir a los usuarios que cambien a la banda de 5 Ghz para la transmisión de medios es engorroso y dará como resultado que haya menos usuarios que accedan a esos servicios.
- La banda de 5 Ghz tiene un mayor alcance; por lo tanto, no tiende a sufrir interferencias.
- Los únicos usuarios que pueden pasar a la banda de 5 Ghz son aquellos que cuentan con las NIC inalámbricas más recientes, lo que reduce el uso.
- La banda de 5 Ghz tiene más canales y está menos poblada que la banda de 2,4 GHz, lo que la hace más adecuada para la transmisión de medios.

Explique: El alcance inalámbrico está determinado por la antena y la potencia de salida del punto de acceso, no por la banda de frecuencia que se utiliza. En esta situación, se indica que todos los usuarios tienen NIC inalámbricas que cumplen con los estándares más recientes, por lo que todos pueden acceder a la banda de 5 Ghz. Aunque es posible que para algunos usuarios cambiar a la banda de 5 Ghz para acceder a los servicios de transmisión sea engorroso, lo que mejora el rendimiento de la red no es solo la disminución de la cantidad de usuarios, sino la mayor cantidad de canales.

46. ¿Qué tres parámetros deberían cambiarse si se están implementando las mejores prácticas para un AP inalámbrico doméstico? (Escoja tres opciones).

- tiempo de baliza inalámbrica
- SSID
- frecuencia de antena
- wireless network password
- AP password
- contraseña del sistema operativo del cliente inalámbrico

Explique: Tan pronto como se saca un AP de una caja, se deben establecer la contraseña predeterminada del dispositivo, el SSID y los parámetros de seguridad (contraseña de red inalámbrica). La frecuencia de una antena inalámbrica se puede ajustar, pero no es necesario hacerlo. La hora del indicador no está configurada normalmente. La contraseña del sistema operativo del cliente inalámbrico no se ve afectada por la configuración de una red inalámbrica doméstica.

47. ¿Qué componente de control de acceso, implementación o protocolo se implementa localmente o como una solución basada en servidor?

- 802.1x
- Registro
- autenticación
- autorización

48. ¿Qué tipo de red inalámbrica utiliza comúnmente dispositivos Bluetooth o ZigBee?

- wireless metropolitan-area network
- wireless wide-area network
- wireless local-area network
- wireless personal-area network

49. ¿Qué componente de AAA permite que un administrador realice un seguimiento de las personas que acceden a los recursos de la red y de los cambios que se hacen en dichos recursos?

- Autenticación
- Registro
- Accesibilidad
- Autorización

Explique: Uno de los componentes de AAA es registro. Después de que un usuario se autentica a través de AAA, los servidores AAA mantienen un registro detallado de las acciones precisas que realiza el usuario autenticado en el dispositivo.

50. ¿Qué característica o configuración de un switch lo hace vulnerable a ataques de doble etiquetado de VLAN?

- la función de puerto troncal automático habilitada para todos los puertos de forma predeterminada
- modo dúplex mixto habilitado para todos los puertos de forma predeterminada
- el tamaño limitado del espacio de memoria direccionable por contenido
- la VLAN nativa del puerto de enlace troncal es la misma que una VLAN de usuario

Explique: El ataque con salto de VLAN de etiquetado doble (o de encapsulado doble) aprovecha la manera en que el hardware opera en algunos switches. Algunos switches realizan solo un nivel de desencapsulación de 802.1Q, lo que permite que, en ciertas situaciones, un atacante incorpore una segunda etiqueta 802.1Q dentro de la trama. Esta etiqueta permite que la trama se envíe a una VLAN a la cual la etiqueta original 802.1Q no especificó. Una característica importante del ataque de salto de VLAN de doble encapsulado es que funciona incluso si los puertos troncal están deshabilitados, porque un host normalmente envía una trama en un segmento que no es un enlace troncal. Un ataque de VLAN Double-tagging es unicast, y funciona unidireccional, y funciona cuando el atacante está conectado a un puerto que reside en la misma VLAN que la VLAN nativa del puerto troncal.

51. ¿Qué tipo de red inalámbrica utiliza transmisores para proporcionar cobertura en un área geográfica extensa?

- wireless wide-area network
- wireless personal-area network
- wireless metropolitan-area network
- wireless local-area network

52. ¿Cuál es una de las ventajas de usar SSID en lugar de FTP?

- Es la mejor forma de asegurar una red inalámbrica.
- Los clientes deberán identificar manualmente el SSID para conectarse a la red.
- Brinda acceso a internet gratuito en lugares públicos donde conocer el SSID de ninguna preocupación.
- Los SSID son muy difícil de determinar porque los AP no transmiten los.

Explique: El ocultamiento del SSID es una característica de seguridad poco eficaz que llevan a cabo los AP y algunos routers inalámbricos por medio de permitir que se deshabilite la trama de señal SSID. Si bien los clientes deben identificar el SSID de forma manual para que se conecte a la red, se puede detectar fácilmente. La mejor forma de proporcionar seguridad a una red inalámbrica es utilizar sistemas de autenticación y de cifrado. El ocultamiento del SSID no proporciona acceso gratuito a Internet en lugares públicos, pero en ese caso se puede utilizar una autenticación de sistema abierto.

53. Una empresa implementó recientemente una red inalámbrica 802.11n. Algunos usuarios se quejan de que la red inalámbrica es demasiado lenta. ¿Cuál es el mejor método para mejorar el rendimiento de la red inalámbrica?

- Dividir el tráfico entre las bandas de frecuencia de 2,4 GHz y 5 GHz.

- Reemplazar las NIC inalámbricas en las computadoras que experimentan conexiones lentas.
- Actualizar el firmware en el punto de acceso inalámbrico.
- Deshabilitar DHCP en el punto de acceso y asignar direcciones estáticas a los clientes inalámbricos.

Explique: Debido a que algunos usuarios se quejan de que la red es muy lenta, la opción correcta sería dividir el tráfico de modo que haya dos redes que utilicen diferentes frecuencias al mismo tiempo. El reemplazo de la NIC inalámbrica no necesariamente soluciona el problema de lentitud de la red y podría ser costoso para la empresa. DHCP en comparación con el direccionamiento estático no debería modificar la lentitud de la red, y sería demasiado trabajo asignar direcciones estáticas a todos los usuarios para que obtengan una conexión inalámbrica. Siempre es una buena idea actualizar el firmware en el punto de acceso inalámbrico. Sin embargo, si algunos usuarios experimentan una conexión de red lenta, es probable que esto no mejore considerablemente el rendimiento de la red.

54. Un especialista en seguridad de TI habilita la seguridad de puertos en un puerto de switch de un switch de Cisco. ¿Cuál es el modo de violación predeterminado que se usa hasta que el puerto de switch se configura para que use otro modo de violación?

- Protección
- Restricción
- shutdown
- deshabilitado

Explique: Si no se especifica ningún modo de violación cuando se habilita la seguridad de puertos en un puerto de switch, el modo de violación de seguridad se establece de forma predeterminada en apagado.

55. Una computadora portátil no se puede conectar a un punto de acceso inalámbrico. ¿Cuáles son los dos pasos de resolución de problemas que se deben llevar a cabo primero? (Elija dos opciones).

- Asegurarse de que la antena de la computadora portátil esté conectada.
- Asegurarse de que se hayan seleccionado los medios de red correctos.
- Asegurarse de que la NIC inalámbrica esté habilitada.
- Asegurarse de que se haya elegido el SSID inalámbrico.
- Asegurarse de que la NIC esté configurada para la frecuencia adecuada.

Explique: Generalmente, las computadoras portátiles inalámbricas no poseen antenas conectadas, a menos que se le haya hecho una reparación recientemente. Si se habilita la NIC inalámbrica, se utilizarán los medios correctos, es decir, la radio. Cuando la NIC detecta un punto de acceso, se utiliza la frecuencia correcta automáticamente.

56. Un técnico está por instalar y configurar una red inalámbrica en una sucursal pequeña. ¿Cuál es la primera medida de seguridad que el técnico debe aplicar de forma inmediata al encender el router inalámbrico?

- Habilitar el filtrado de direcciones MAC en el router inalámbrico.
- Deshabilitar la transmisión del SSID de la red inalámbrica.
- Configurar la encriptación del router inalámbrico y de los dispositivos inalámbricos conectados.
- Cambiar el nombre de usuario y contraseña predeterminados en el router inalámbrico.

Explique: La primera acción que debe realizar un técnico para aportar seguridad a una red inalámbrica nueva es cambiar el nombre de usuario y contraseña predeterminados en el router inalámbrico. Por lo general, la siguiente acción sería configurar la encriptación. Una vez que el grupo inicial de hosts inalámbricos se conecta a la red, se habilitaría el filtrado de direcciones MAC y se deshabilitaría la transmisión del SSID. Esto evita que nuevos hosts no autorizados encuentren la red inalámbrica y se conecten a ella.

57. ¿Cuáles son dos protocolos que utiliza AAA para autenticar a los usuarios contra una base de datos central de nombres de usuario y contraseña? (Escoja dos opciones).

- RADIUS
- SSH
- NTP
- TACACS+
- HTTPS
- CHAP

Explique: Mediante el uso de TACACS+ o RADIUS, AAA puede autenticar a los usuarios desde una base de datos de nombres de usuario y contraseñas almacenadas de forma centralizada en un servidor, como un servidor Cisco ACS.

58. ¿Qué componente de control de acceso, implementación o protocolo se basa en las funciones de dispositivo del suplicante, autenticador y servidor de autenticación?

- 802.1x
- Autenticación

- Autorización
- Registro

59. ¿Qué dos estándares inalámbricos IEEE 802.11 operan solo en el rango de 5 GHz? (Escoja dos opciones).

- 802.11ad
- 802.11b
- 802.11g
- 802.11ac
- 802,11a
- 802.11n

> **Explique:** Los estándares 802.11a y 802.11ac funcionan solo en el rango de 5 GHz. Los estándares 802.11b y 802.11g funcionan solo en el rango de 2,4 GHz. El estándar 802.11n funciona en los rangos de 2,4 y 5 GHz. El estándar 802.11ad funciona en los rangos de 2,4, 5 y 60 GHz.

60. ¿Qué tipo de trama de administración puede ser transmitido regularmente por un AP?

- autenticación
- beacon
- respuesta de la sonda
- solicitud de sondeo

> **Explique:** Las señales son las únicas tramas de administración que un AP puede transmitir en forma regular. Las tramas de sondeo, autenticación y asociación se utilizan solamente durante el proceso de asociación (o reasociación).

61. ¿Qué tipo de red inalámbrica utiliza transmisores de baja potencia para una red de corto alcance, generalmente de 20 a 30 pies (6 a 9 metros)?

- wireless wide-area network
- wireless personal-area network
- wireless local-area network
- wireless metropolitan-area network

62. ¿Qué componente de control de acceso, implementación o protocolo controla a quién se le permite acceder a una red?

- autorización
- autenticación
- 802.1x
- Registro

63. ¿Qué componente de control de acceso, implementación o protocolo indica éxito o fallo de un servicio solicitado por el cliente con un mensaje PASS o FAIL?

- Autenticación
- Registro
- autorización
- 802.1x

64. ¿Qué componente de control de acceso, implementación o protocolo controla lo que los usuarios pueden hacer en la red?

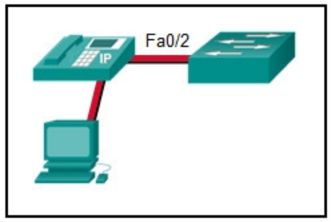
- Registro
- Autenticación
- 802.1x
- Autorización

65. ¿Qué tipo de red inalámbrica es adecuada para proporcionar acceso inalámbrico a una ciudad o distrito?

- wireless wide-area network
- wireless personal-area network
- wireless local-area network
- wireless metropolitan-area network

66. Consulte la exhibición. El puerto Fa0/2 ya se configuró adecuadamente. El teléfono IP y la computadora funcionan de manera correcta. ¿Cuál sería la configuración de switch más adecuada para el puerto Fa0/2 si el administrador de red tuviera los siguientes objetivos?

- Nadie debe poder desconectar el teléfono IP o la computadora ni conectar otro dispositivo por cable.
- Si se conecta un dispositivo diferente, el puerto Fa0/2 se debe desactivar.
- El switch debe detectar automáticamente la dirección MAC del teléfono IP y de la computadora, y agregar esas direcciones a la configuración en ejecución.



SWA(config-if)# switchport port-security

SWA(config-if)# switchport port-security maximum 2

SWA(config-if)# switchport port-security mac-address sticky

SWA(config-if)# switchport port-security violation restrict

SWA(config-if)# switchport port-security mac-address sticky

SWA(config-if)# switchport port-security maximum 2

SWA(config-if)# switchport port-security

SWA(config-if)# switchport port-security mac-address sticky

SWA(config-if)# switchport port-security

SWA(config-if)# switchport port-security maximum 2

SWA(config-if)# switchport port-security mac-address sticky

> **Explique:** El modo predeterminado para una violación de seguridad de puertos es apagar el puerto para que el comando switchport port-security violation no sea necesario. El comando switchport port-security se debe introducir sin opciones adicionales para habilitar la seguridad del puerto. Luego, pueden agregarse opciones adicionales de seguridad de puertos.

67. ¿Qué componente de control de acceso, implementación o protocolo registra comandos EXEC y configuración configurados por un usuario?

- Autenticación
- Registro
- 802.1x
- Autorización

68. ¿Qué tipo de red inalámbrica es adecuada para las comunicaciones nacionales y globales?

- wireless local-area network
- wireless metropolitan-area network
- wireless wide-area network
- wireless personal-area network

69. ¿Que tipo de red inalambrica utiliza transmisores para cubrir una red de tamaño mediano, generalmente de hasta 300 pies (91.4metros)?

- wireless metropolitan-area network
- wireless local-area network
- wireless wide-area network
- wireless personal-area network

70. ¿Qué tipo de red inalámbrica se basa en el estándar 802.11 y una frecuencia de radio de 2.4 GHz o 5 GHz?

- wireless metropolitan-area network
- wireless local-area network
- wireless wide-area network
- wireless personal-area network

71. ¿Qué tipo de red inalámbrica a menudo hace uso de dispositivos montados en edificios?

- wireless wide-area network
- wireless metropolitan-area network
- wireless personal-area network
- wireless local-area network

72. ¿Qué componente de control de acceso, implementación o protocolo se basa en nombres de usuario y contraseñas?

- 802.1x
- autorización
- Registro
- autenticación

73. ¿Qué tipo de red inalámbrica es adecuada para su uso en un hogar u oficina?

- wireless local-area network
- wireless personal-area network
- wireless metropolitan-area network
- wireless wide-area network