- INICIO
- CCNA1 V5.1
- CCNA1 V6.0
- CCNA2 V6.0
- CCNA3 V6.0
- CCNA4 V6.0
- ITE V6.0

CCNA2 v6.0 Capítulo 5 Examen Español

CCNA2 v6.0 Capítulo 5 Examen Español

Gaby Gorgui CCNA2 v6.0

1. ¿Qué sentencia describe el LED de velocidad de puerto en el switch Cisco Catalyst 2960?

- Si el LED está verde, el puerto funciona a 100 Mb / s.
- Si el LED está apagado, el puerto no está funcionando.
- Si el LED parpadea en verde, el puerto funciona a 10 Mb / s.
- Si el LED está ámbar, el puerto funciona a 1000 Mb / s.

2. ¿Qué comando se utiliza para establecer la variable de entorno BOOT que define dónde encontrar el archivo de imagen IOS en un switch?

- config-register
- boot system
- boot loader
- confreg

3. ¿Qué es una función del cargador de arranque del switch?

- Acelerar el proceso de arranque
- Proporcionar seguridad para el estado vulnerable cuando el switch está arrancando
- Controlar cuánta RAM está disponible para el switch durante el proceso de arranque
- Proporcionar un entorno para operar cuando no se puede encontrar el sistema operativo del switch

4. ¿Qué interfaz es la ubicación predeterminada que contendría la dirección IP utilizada para administrar un switch Ethernet de 24 puertos?

- VLAN 1
- Fa0 / 0
- Fa0 / 1
- Interface conectada al gateway predeterminado
- VLAN 99

5. Un switch de producción se vuelve a cargar y termina con un indicador Switch>. ¿Qué dos hechos se pueden determinar? (Elija dos.)

- El POST ocurrió normalmente.
- El proceso de arranque se interrumpió.
- No hay suficiente RAM o flash en este router.
- Se encontró y cargó una versión completa del Cisco IOS.
- El switch no localizó el IOS de Cisco en la flash, por lo que fue de forma predeterminada a la ROM.

6. ¿Cuáles dos afirmaciones son verdaderas sobre el uso de Fast Ethernet full-duplex? (Elija dos.)

- El rendimiento se mejora con el flujo de datos bidireccional.
- La latencia se reduce porque el NIC procesa las tramas más rápidamente.
- Los nodos operan en full-duplex con flujo de datos unidireccional.
- El rendimiento se mejora porque la NIC es capaz de detectar colisiones.
- Fast Ethernet full-duplex ofrece una eficiencia del 100% en ambas direcciones.

7. ¿En qué situación un técnico usaría el comando show interfaces switch?

- Para determinar si el acceso remoto está habilitado
- Cuando los paquetes se están descartando de un host directamente conectado
- Cuando un dispositivo final puede llegar a dispositivos locales, pero no a dispositivos remotos
- Para determinar la dirección MAC de un dispositivo de red conectado directamente en una interfaz determinada

8. Consulte la ilustración. Un técnico de red está solucionando problemas de conectividad en una red Ethernet con el comando show interfaces fastEthernet 0/0. ¿A qué conclusión se puede llegar basándose en la salida parcial de la ilustración?

- Todos los hosts de esta red se comunican en modo full-dúplex.
- Algunas estaciones de trabajo pueden utilizar un tipo de cableado incorrecto para conectarse a la red.
- Hay colisiones en la red que producen tramas que tienen menos de 64 bytes de longitud.
- Una NIC que funciona incorrectamente puede causar que se transmitan tramas que son más largas que la longitud máxima permitida.

9. Consulte la ilustración. ¿Qué problema con los medios de comunicación puede existir en el enlace conectado a Fa0/1 basado en el comando show interface?

- El parámetro de ancho de banda en la interfaz puede ser demasiado alto.
- Podría haber un problema con una NIC defectuosa.
- Podría haber demasiada interferencia eléctrica y ruido en el enlace.
- El cable que une el host al puerto Fa0/1 puede ser demasiado largo.
- La interfaz puede configurarse como half-duplex.

10. Si un extremo de una conexión Ethernet está configurada para full-dúplex y el otro extremo de la conexión está configurado para half-duplex, ¿dónde se observarán colisiones tardías?

- En ambos extremos de la conexión
- En el extremo full-duplex de la conexión
- Solo en interfaces seriales
- En el extremo half-duplex de la conexión

11. ¿Cuál es una diferencia entre usar Telnet o SSH para conectarse a un dispositivo de red con fines de administración?

- Telnet utiliza UDP como protocolo de transporte, mientras que SSH utiliza TCP.
- Telnet no proporciona autenticación mientras que SSH proporciona autenticación.
- Telnet admite una GUI de host mientras que SSH solo admite una CLI de host.
- Telnet envía un nombre de usuario y una contraseña en texto sin formato, mientras que SSH cifra el nombre de usuario y la contraseña.

12. Consulte la ilustración. El administrador de red desea configurar Switch1 para permitir conexiones SSH y prohibir conexiones Telnet. ¿Cómo debe el administrador de red cambiar la configuración mostrada para satisfacer el requisito?

- Utilizar la versión 1 de SSH.
- Reconfigurar la clave RSA.
- Configurar SSH en una línea diferente.
- Modificar el comando transport input.

13. ¿Cuál es el efecto de usar el comando switchport port-security?

- Habilita la seguridad del puerto en una interfaz
- Habilita la seguridad de los puertos globalmente en el switch
- Desactiva automáticamente una interfaz si se aplica a un puerto troncal
- Detecta la primera dirección MAC en una trama que entra en un puerto y coloca esa dirección MAC en la tabla de direcciones MAC

14. ¿Dónde se almacenan las direcciones MAC dinámicamente aprendidas cuando el aprendizaje persistente está habilitado con el comando switchport port-security mac-address sticky?

- ROM
- RAM
- NVRAM
- flash

15. Un administrador de red configura la función de seguridad de puerto en un switch. La directiva de seguridad especifica que cada puerto de acceso debe permitir hasta dos direcciones MAC. Cuando se alcanza el número máximo de direcciones MAC, se elimina una trama con la dirección MAC de origen desconocida y se envía una notificación al servidor syslog. ¿Qué modo de violación de seguridad debe configurarse para cada puerto de acceso?

- Restrict
- Protect
- Warning
- Shutdown

16. ¿Cuáles dos afirmaciones son verdaderas con respecto a la seguridad del puerto de switch? (Elija dos.)

- Los tres modos de violación configurables registran todas las infracciones a través de SNMP.
- Las direcciones MAC seguras aprendidas dinámicamente se pierden cuando se reinicia el switch.
- Los tres modos de violación configurables requieren la intervención del usuario para volver a habilitar los puertos.
- Después de introducir el parámetro sticky, sólo las direcciones MAC posteriormente aprendidas se convierten en direcciones MAC seguras.
- Si se configuran de forma estática menos del número máximo de direcciones MAC de un puerto, las direcciones aprendidas dinámicamente se agregan a la CAM hasta que se alcanza el número máximo.

17. ¿Qué acción devolverá a un estado operativo un puerto de switch deshabilitado por error?

- Quitar y reconfigurar la seguridad del puerto en la interfaz.
- Emitir el comando switchport mode access en la interfaz.
- Borrar la tabla de direcciones MAC del switch.
- Emitir los comandos de interfaz shutdown y no shutdown.

18. Consulte la ilustración. El puerto Fa0 / 2 ya ha sido configurado adecuadamente. El teléfono IP y el PC funcionan correctamente. ¿Qué configuración de switch sería más apropiada para el puerto Fa0 / 2 si el administrador de red tiene los siguientes objetivos?

Nadie está autorizado a desconectar el teléfono IP o el PC y conectar algún otro dispositivo con cable.
Si hay un dispositivo diferente conectado, el puerto Fa0 / 2 se desactiva.
El switch debe detectar automáticamente la dirección MAC del teléfono IP y el PC y agregar esas direcciones a la configuración en ejecución.

- SWA(config-if)# switchport port-security
  SWA(config-if)# switchport port-security mac-address sticky
- 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 maximum 2
  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
  SWA(config-if)# switchport port-security violation restrict

19. Consulte la ilustración. ¿Qué se puede determinar sobre la seguridad del puerto a partir de la información que se muestra?

- El puerto se ha desactivado.
- El puerto tiene dos dispositivos conectados.
- El modo de violación de puerto es el predeterminado para cualquier puerto que tenga habilitada la seguridad de puertos.
- El puerto tiene el número máximo de direcciones MAC que es compatible con un puerto de switch de capa 2 que está configurado para la seguridad del puerto.

20. Consulte la ilustración. ¿Qué evento tendrá lugar si hay una violación de seguridad de puerto en la interfaz Fa0/1 del switch S1?

- Se envía una notificación.
- Se registra un mensaje syslog.
- Se eliminarán los paquetes con direcciones de origen desconocidas.
- La interfaz entrará en estado de desactivado por error.

21. Abra la Actividad PT. Realice las tareas en las instrucciones de actividad y luego responda a la pregunta.

Complete el espacio en blanco. No utilice abreviaturas. ¿Cuál es el comando que falta en S1? ip address 192.168.99.2 255.255.255.0

22. Una el paso con cada descripción de la secuencia de arranque del switch. (No se utilizan todas las opciones.)

23.

Identifique los pasos necesarios para configurar un switch para SSH. El orden de respuesta no importa. (No se utilizan todas las opciones.)

24. Una el

estado del enlace con el estado de la interfaz y el protocolo. (No se utilizan todas las opciones.)

Artículos Relacionados

Deja un comentario

Texto del comentario *

Nombre*

Email*

Sitio Web

Publicar comentario

Por favor confirma que eres humano Por favor confirma que eres humano

Busca en el sitio Buscar