Seleccione la banda que principalmente está designada a las comunicaciones de telefonía satelital

Banda L

Banda S

Banda C

Banda X

Banda KU

Banda KA

Sobre el protocolo Mobile IP, seleccione la afirmación incorrecta

La tunelización solo es establecida para la comunicación entre los Agents

La comunicación entre los Agents es establecida sobre el protocolo UDP

La dirección temporal (Care of Address) que el Nodo Móvil recibe es asignada por el Foregin Agent

El Foreign Agent re-envía las respuestas que recibe al Nodo corresponsal

El Foreign Agent envía la dirección temporal (Care of Address) al Home Agent

N/A

Seleccione la definición incorrecta sobre el Mobile IP

Mobile Node: Dispositivo de comunicación portátil del usuario final

Home Agent: Típicamente, un router en la red local a la cual el Mobile Node está originalmente conectado

Foreign Network: Red actual donde el Mobile Node es un visitante sin IP asignado

Correspondent Node: Es un dispositivo en la Internet comunicándose al Mobile Node

Care of Address: Es la dirección temporal utilizada por un Mobile Node mientras no se encuentra en la cobertura de su red local

N/A

Seleccione la(s) definición(es) correcta(s) sobre la radio propagación de ondas

La reflexión provoca que la onda original cambie de dirección al pasar por un medio de diferente densidad

La difracción no permite a la onda atravesar otros medios al original rebotando en otras direcciones

La absorción ocurre cuando la onda cambia de dirección y/o intensidad cuando rodea un objeto u obstáculo

La refracción ocurre cuando la onda pasa a través de un medio y no es reflejada, pero es atenuada

La dispersión provoca que la señal original sea reflejada en múltiples ondas originales atenuadas

N/A

¿Cuál de las siguientes afirmaciones no corresponde al estándar 802.11n?

Banda base compatible con 2.4GHz y 5GHz

Ancho de banda de teórico de 600Mbps

Utiliza tecnología de múltiples antenas MIMO

Multiplexación OFDM

Compatible con los estándares a/b/g

N/A

Seleccione la(s) desventaja(s) de utilizar la versión 2 en lugar de la versión 3 del protocolo SNMP

No contar con Autenticación de grupo y usuario

Los dispositivos no implementan cifrado de datos

No contar con un Framework de configuración remota

No contar con MIB

No contar con Autenticación basada en Nombre de comunidad

Los dispositivos no envían cadenas de texto plano

¿Qué mensaje no está presente en ambas versiones (2 y 3) de SNMP?

TRAP

GET

SET

GET BULK

INFORM

N/A

Seleccione la(s) opción(es) falsa(s) sobre los OID de SNMP

Puede reunir información sobre un dispositivo que implementa SNMP

Cada OID define un tipo de dato

Un OID define un nivel de acceso (lectura y escritura)

Los OID están definidos en las MIB

Los OID solo pueden ser escalares

Cada OID es único y específico a un dispositivo o su tipo

Seleccione la opción falsa sobre los MIB de SNMP

Mantiene una base de datos de información que describe los parámetros de un dispositivo gestionado

Una MIB está compuesto por un conjunto de OID

Una MIB puede seguir el estándar RFC 1213

Una MIB no puede ser provista por fabricantes privados

Cada proveedor de equipo SNMP tiene un árbol exclusivo de MIB bajo su control

N/A

En referencia a SNMP seleccione la opción falsa

Opera utilizando datagramas UDP

Los mensajes SNMP contienen una cabecera y un PDU

El PDU depende del tipo de mensaje que está siendo enviado

SNMP versión 2 define la versión segura de SNMP

Almacena y recupera información de gestión según se define en la MIB

Recolecta información de gestión sobre su entorno local

Seleccione tres características que fueron agregadas en la versión 3 desde la versión 2 de SNMP

Integridad de mensaje

Autenticación

Cifrado

Compresión

Detección de errores

Autorización

Seleccione tres componentes de SNMP

Dispositivo gestionado

SNMP Manager

SNMP Agent

SysLog Server

NMA

NME

Seleccione dos afirmaciones que no representan ventajas de la técnica RPC

RPC provee una vista personalizada para establecer comunicaciones entre el cliente y servidor

RPC oculta la existencia de la red a la aplicación

RPC no permite la reutilización de código

El procedimiento invocado puede existir en un espacio de direcciones diferente del procedimiento invocador

RPC puede ser utilizado para el propósito de entornos locales y distribuidos

RPC soporta modelos orientados a procesos y a hilos

Seleccione la(s) opción(es) correcta(s) sobre un stub RPC

En el lado del servidor recibe el mensaje e invoca al procedimiento en el servidor

Empaqueta los parámetros en una forma transmisible sobre la red

En el lado del servidor, localiza el puerto

En el lado del cliente desempaqueta los parámetros del mensaje retornado

En el lado del cliente pasa el mensaje a la capa de transporte

Todas las otras opciones son correctas

Sobre el encoder HEVC seleccione la(s) opción(es) incorrecta(s)

Particionamiento menos flexible

Menor flexibilidad en los tamaños de bloques a ser procesados

Interpolación menos sofisticada

Predicción menos sofisticada

No permite el procesamiento paralelo

Todas las otras opciones son incorrectas

¿Qué proceso es opcional durante el streaming para el estándar H.265?

Reconstrucción

Transformada

Cuantización

Grabación

Codificación

Partición

Sobre el proceso de particionamiento con el estándar H.265, seleccione la afirmación incorrecta

Cada frame de video es trozado en slices

Cada slice es trozado en CTUs

Cada CTU es trozado en CUs rectangulares o cuadrados

El CTU es la unidad básica de codificación

El CTU es análogo al macroblock del estándar H.264

Cada CU se predice utilizando inter o intra predicción

Seleccione la afirmación correcta sobre la Integridad de un dato

Garantiza que el dato no ha sido modificado

Garantiza que el mensaje siempre llegue al destinatario

Asegura que solo el destinatario autorizado recibe el mensaje

Asegura que el dato está autorizado para ser entregado

Todas son correctas excepto N/A

N/A

Seleccione la afirmación que no corresponde con el ataque de Denegación de servicio distribuido (DDoS)

Múltiples sistemas atacan a una única víctima

La estación víctima es sobre cargada con paquetes provenientes de múltiples estaciones

Es difícil bloquear debido a que los ataques provienen de múltiples locaciones

Bots son utilizados principalmente para atacar en diferentes tiempos

Son difíciles de rastrear

N/A

En referencia a la seguridad de la red, seleccione el tipo de ataque que no corresponde al grupo

Interceptación

Interrupción

Modificación

Fabricación

Todas corresponden excepto N/A

N/A