

# Taller Gestión de Redes

## Examen Final

### Análisis de Redes

---

Para encontrar el tiempo de respuesta desde su maquina a una maquina remota podria usar el comando ping?

- A. Si
- B. No

Para encontrar la ruta que un paquete IP sigue de su servidor a un servidor remoto podria usar el comando **netstat**?

- A. Si
- B. No

Para mostrar todas las interfaces IPv4 a la escucha en su servidor que comando usaria?

- A. lsof -i
- B. netstat
- C. lsof
- D. netstat 127.0.0.1
- E. ping localhost

### Monitoreo y Gestion de Redes

---

Monitoreo y Gerencia de Redes incluye los siguientes conceptos (chequee todos los que se aplican)

- A. Detectar problemas en la red cuando ocurren.
- B. Ver tendencias a largo plazo para ayudar a planificar expansión de la red y sus recursos
- C. Para generar tickets automáticamente cuando eventos inusuales ocurren
- D. Crear tablas de bases de datos relacionales de forma adecuada
- E. Cumplir con niveles de servicio acordados (SLAs).
- F. Todas las opciones anteriores

Cual de los siguientes paquetes de monitoreo y gerencia nos ayudan mejor a detectar "parpadeo" (jitter) en rutas de la red?

- A. Smokeping
- B. Nagios
- C. Cacti
- D. RANCID
- E. NetFlow

Podría usted medir la cantidad de espacio en disco disponible en un servidor remote via Cacti?

- A. Si
- B. No

Cual de los siguientes paquetes de software usted podría usar para determinar si un enrutador esta disponible o caído?

- A. Cacti
- B. Smokeping
- C. Nagios
- D. Swatch
- E. Todos los de arriba

Cual es el significado de SNMP?

- A. Simple Network Management Protocol
- B. Service for Network Management Project
- C. Simple NetBios Management Protocol
- D. Simplified Network Monitoring Protocol
- E. Serious New Measuring Project

Es el protocolo SNMP Version 2 encriptado?

- A. Si
- B. No

En que se diferencian las versiones 2c y version 3 de SNMP:

- 1) el tipo de autentificacion y encriptamiento
- 2) la informacion que provee el dispositivo al ser interrogado
- 3) ninguno de las dos anteriores

En el protocolo version 3 de SNMP se puede proteger (escoja la respuesta mas exacta)

- 1) La autentificacion via usuario/password com hash MD5 o SHA
- 2) Los datos de respuesta via encriptamiento DES
- 3) Ambas (1 y 2 arriba) son posibles

IPERF se usa para medir el ancho de banda de la red

- A. Si
- B. No

Un sistema de manejo de tickets es útil porque puede:

- A. Actuar como una base de datos de problemas ocurridos
- B. Mantener un registro de la interacción con un cliente de principio a fin
- C. Automáticamente notificar a un grupo de ingenieros cuando un sistema de monitoreo ha detectado un problema
- D. Ayuda a ver tendencias y planificar expansión futura
- E. Todos los de arriba.

Se puede utilizar Netflow para determinar la fuente de ataques de DDoS?

- A. Si
- B. No

Netflow solo funciona en enrutadores Cisco

- A. Si
- B. No

Un "flujo de datos" se define como una secuencia unidireccional de paquetes que tienen en común:

- A) Misma dirección IP fuente, y destino
  - Mismo número de protocolo de capa 3
  - Mismo puerto fuente, y destino
  - Mismo octeto de Tipo de Servicio
  - Mismo índice de la interfaz de entrada (ifIndex)

→ Pregunta sigue en la próxima pagina...

B) Misma dirección IP fuente, y destino  
Mismo número de protocolo de capa 3  
Mismo puerto fuente, y destino  
Misma versión de protocolo SNMP

C) Mismo octeto de Tipo de Servicio  
Mismo índice de la interfaz de entrada (ifIndex)  
Mismo consumo de CPU  
Misma longitud de paquete y MTU

Escoja la opción adecuada

El programa RT+Mailgate permite que Cacti, Nagios, Smokeping y otros puedan generar tickets automáticamente

- A. Si
- B. No

Puede RANCID especificar quien cometi' un error al efectuar un cambio en el fichero de configuración de un enrutador?

- A. Si
- B. No

Puede SWATCH, (the Simple log WATCHer), completar una de las tareas siguientes?

- A. Notificar si un usuario especifico intenta conectarse a un enrutador?
- B. Determinar la demora de procesamiento de los paquetes de salida en un servidor?
- C. Medir el parpadeo (jitter) de una conexión entre dos dispositivos de red?
- D. Despertarlo a usted antes de que alguien intente un ataque de DDoS contra su red?
- E. Calcular la cantidad maxima de ancho de banda utilizada por uno de sus clientes?

La siguientes lineas de configuracion de syslog (3 lineas siguientes) en un enrutador

```
logging 10.0.0.8  
logging facility local6  
logging trap errors
```

permiten:

- A) enviar trazas a 10.0.0.8 , etiqueta local6, notificaciones de nivel "errors" (nivel 3)
- B) enviar trazas a 10.0.0.8, etiqueta local6, notificaciones de nivel "errors" y menor prioridad (nivel 3 a 7)
- C) enviar trazas a 10.0.0.8, etiqueta local6, notificaciones de nivel "errors" y mayor prioridad (nivel 3 a 0)

Que comando SNMP usted utilizaría para hallar todos los valores de las OIDs disponibles en un dispositivo particular que implemente SNMP?

- A. snmpwalk
- B. snmpstatus
- C. snmpget
- D. snmpset
- E. snmptrap