# Administración de Redes Locales

## Bloque IV. Tema 9

Gestión de Sistemas e Informática

Curso 2017 - 18

Juan José Aguado Gil

08 Noviembre 2017

## 1. Gestión de Usuarios

### 1.1. Servicio de Directorio

La aplicación o conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red.

Son productos de directorio para gestión de usuarios: **Apache Directory Server**, **Microsoft Active Directory** y **OpenDS**.

### 1.2. LDAP: Lightweight Directory Access Protocol

LDAP is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory.

Ventajas del uso de directorios LDAP para la autenticación de usuarios:

- La mayoría de aplicaciones comerciales permiten su integración fácilmente.
- Están optimizados para las búsquedas, que es la operación más repetida a la hora de gestionar los usuarios.

- Permiten implantar sin ningún mecanismo adicional Single Sign On, ya que todas las aplicaciones pueden tener la autenticación a través del LDAP.

### 1.3. NIS: Network Information Service

Es un protocolo de servicios de directorios cliente-servidor desarrollado por Sun Microsystems para el envío de datos de configuración en sistemas distribuidos, tales como nombres de usuarios y hosts entre computadoras sobre una red.

A NIS system maintains and distributes a central directory of user and group information, hostnames, e-mail aliases and other text-based tables of information in a computer network. For example, in a common UNIX environment, the list of users for identification is placed in /etc/passwd, and secret authentication hashes in /etc/shadow. NIS adds another "global" user list which is used for identifying users on any client of the NIS domain

## 2. Monitorización y Control de Tráfico

### 2.1. Monitorización de Dispositivos

**Nagios** es una herramienta de código abierto para monitorizar los dispositivos de una red.

### 2.2. Comando ping (Packet Internet Groper)

ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams ("pings") have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of "pad" bytes used to fill out the packet.

## 3. SNMP: Simple Network Management Protocol

SNMP es un protocolo para obtener y organizar la información de una serie de dispositivos gestionados en redes IP y para modificar dicha información con el objeto de cambiar el comportamiento de los dispositivos.

SNMP es ampliamente usado en la Gestión y Monitorización de Redes. SNMP publica datos de gestión en la forma de variables de los dispositivos gestionados, organizados en cada dispositivo en una base de datos **Management Information Base (MIB)** la cual describe el estado y la configuración del dispositivo.

### 3.1. Componentes Básicos

El uso típico de SNMP consiste en tener uno o más ordenadores administrativos, llamados **managers** que monitorizan o gestionan un grupo de hosts o dispositivos en una red. Cada

sistema gestionado ejecuta un componente sotware llamado **agente**, el cual reporta información vía SNMP al manager.

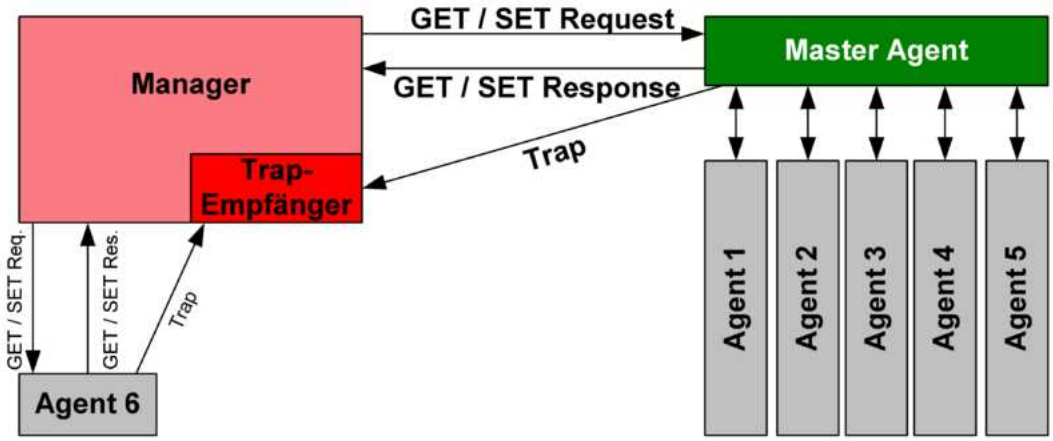


Figura 1: Principios de la Comunicación SNMP.

Una red gestionado por SNMP tiene tres componentes básicos:

- Dispositivo gestionado.
- Agente: software que se ejecuta en los dispositivos gestionados.
- **Network Management Station (NMS)**: software que se ejecuta en el manager.

## 3.2. Protocolo

SNMP opera en el Nivel de Aplicación del Modelo OSI. SNMP usa UDP.

### 3.2.1. Mensajes SNMP

SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

- **Versión**: Número de versión de protocolo que se está utilizando (por ejemplo 0 para SNMPv1, 1 para SNMPv2c, 2 para SNMPv2p y SNMPv2u, 3 para SNMPv3, ...);
- **Comunidad**: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada **public** y una comunidad de escritura llamada **private**;
- **SNMP PDU**: Contenido de la Unidad de Datos de Protocolo, el que depende de la operación que se ejecute.

#### 3.2.2. PDU: Protocol Data Unit

- **GetRequest**: manager-to-agent request para solicitar el valor de una variable o lista de variables.
- **SetRequest**: manager-to-agent request para cambiar el valor de una variable o lista de variables.
- **GetNextRequest**: manager-to-agent request para descubrir variables disponibles y sus valores.
- **GetBulkRequest**: manager-to-agent request para múltiples iteraciones de *GetNextRequest*. Versión optimizada de *GetNextRequest*.
- **Response**: agent-to-manager response. Devuelve valores de variables y ACK de los comandos Request descritos anteriormente.
- **Trap**: agent-to-manager notificación asíncrona. Permite a un agente notificar eventos significativos al manager.
- **InformRequest**: notificación asíncrona de ACK.
- **Report**: XXX

#### 3.2.3. Puertos

- El **manager** envía peticiones desde cualquier puerto disponible.
- El **agente SNMP** recibe peticiones en el **puerto UDP 161**.
- El **agente** puede generar notificaciones desde cualquier puerto disponible.
- El **manager** recibe notificaciones en el **puerto 162**. disponible.

### 3.3. MIB: Management Information Base

It is a database used for managing the entities in a communication network. The database is hierarchical (tree-structured) and each entry is addressed through an **object identifier (OID)**.

### 3.3.1. MIB Modules

MIB modules contain definitions of interrelated managed objects. MIB modules are occasionally updated to add new functionality, remove ambiguities and to fix defects. An example of a MIB module that has been updated many times is the important set of objects that was originally defined in RFC 1213, also known as **MIB-II**. MIB-II is a very important management group, because every device that supports SNMP must also support MIB-II. The section of RFC1213-MIB that defines the base OIDs for the mib-2 subtree looks like this:

| **Object** | **OID** |
|---|---|
| mib-2 | OBJECT IDENTIFIER ::= mgmt 1 |
| system | OBJECT IDENTIFIER ::= mib-2 1 |
| interfaces | OBJECT IDENTIFIER ::= mib-2 2 |
| at | OBJECT IDENTIFIER ::= mib-2 3 |
| ip | OBJECT IDENTIFIER ::= mib-2 4 |
| icmp | OBJECT IDENTIFIER ::= mib-2 5 |
| tcp | OBJECT IDENTIFIER ::= mib-2 6 |
| udp | OBJECT IDENTIFIER ::= mib-2 7 |
| egp | OBJECT IDENTIFIER ::= mib-2 8 |
| transmission | OBJECT IDENTIFIER ::= mib-2 10 |
| snmp | OBJECT IDENTIFIER ::= mib-2 11 |

Tabla 1: Categorías de UTP.

mib-2 is defined as **iso.org.dod.internet.mgmt.1**, or **1.3.6.1.2.1**. From here, we can see that the system group is mib-2 1, or 1.3.6.1.2.1.1, and so

## 3.4. Mejoras SNMPv3

Existen tres versiones de SNMP: SNMPv1, SNMPv2 y SNMPv3. **SNMPv1** constituye la primera definición e implementación del protocolo SNMP, estando descrito en las RFC 1155, 1157 y 1212 del IETF (Internet Engineering Task Force). El vertiginoso crecimiento de SNMP desde su aparición en 1988, puso pronto en evidencia sus debilidades, principalmente su imposibilidad de especificar de una forma sencilla la transferencia de grandes bloques de datos y la ausencia de mecanismos de seguridad; debilidades que tratarían de ser subsanadas en las posteriores definiciones del protocolo.

**SNMPv2** apareció en 1993, estando definido en las RFC 1441-1452. SNMPv1 y SNMPv2 tienen muchas características en común, siendo la principal mejora la introducción de tres nuevas operaciones de protocolo: **GetBulk** para que el gestor recupere de una forma eficiente grandes bloques de datos, tales como las columnas de una tabla; **Inform** para que un agente envíe información espontánea al gestor y reciba una confirmación; y **Report** para que el agente envíe de forma espontánea excepciones y errores de protocolo. SNMPv2 también incorpora un

conjunto mayor de códigos de error y más colecciones de datos. En 1995 apareció una revisión de SNMPv2, denominada SNMPv2c y descrita en las RFC 1901-1910, añadiendo como mejoras una configuración más sencilla y una mayor modularidad; pero manteniendo el sencillo e inseguro mecanismo de autentificación de SNMPv1 y SNMPv2 basado en la correspondencia del denominado nombre de comunidad.

La nueva y última versión de SNMP, **SNMPv3**, refuerza las prestaciones de seguridad, incluyendo **autenticación, privacidad y control de acceso**; y de administración de protocolo, con una mayor modularidad y la posibilidad de configuración remota. SNMPv3 apareció en 1997, estando descrito en las RFC 1902-1908 y 2271-2275. Cabe destacar que SNMPv3 no se trata de un estándar que reemplaza a SNMPv1 y/o SNMPv2, sino que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunción con SNMPv2 (preferiblemente) o SNMPv1. Estas mejoras harán que SNMP se constituya en un protocolo de gestión susceptible de ser utilizado con altas prestaciones en todo tipo de redes, desplazando a medio plazo a CMIP como estándar de gestión de las grandes redes de las operadoras de telecomunicación.

El modelo de seguridad basado en usuario o **USM (User-Based Security Model)** proporciona los servicios de autentificación y privacidad en SNMPv3. El mecanismo de autentificación en USM asegura que un mensaje recibido fue, de hecho, trasmitido por la entidad indicada en el campo correspondiente a la fuente en la cabecera del mensaje; y además, que el mensaje no fue alterado durante su tránsito y que no fue artificialmente retardado o repetido. Para conseguir la autentificación, el gestor y el agente que desean comunicarse deben compartir la misma clave de autentificación secreta configurada previamente fuera de SNMPv3 (no es almacenada en la MIB y no es accesible mediante SNMP). El protocolo de autentificación utilizado puede ser el HMAC- MD5-96 o el HMAC-SHA-96. Para asegurarse de que los mensajes llegan dentro de una ventana temporal razonable que descarte el posible retardo de mensajes y el ataque mediante mensajes repetidos, se utilizan mecanismos de sincronización entre emisor y receptor y el chequeo de la ventana temporal constituida por el momento de emisión del mensaje y su momento de recepción. Por otro lado, la facilidad de privacidad de USM posibilita a los gestores y a los agentes encriptar mensajes para prevenir que sean analizados por intrusos. De nuevo, el gestor y el agente deben compartir una clave secreta configurada previamente. El algoritmo de encriptación utilizado es el CBC (Cipher Block Chaining) de DES (Data Encryption Standard), conocido también por DES-56.

El modelo de control de acceso basado en vistas o VCAM (Views-Based Access Control Model) permite proporcionar diferentes niveles de acceso a las MIB de los agentes para los distintos gestores en SNMPv3. Un agente puede, de este modo, restringir el acceso de ciertos gestores a parte de su MIB o bien limitar las operaciones susceptibles de realizar por ciertos gestores sobre una parte de su MIB. La política de control de acceso a ser utilizada por el agente para cada gestor debe estar configurada previamente; consistiendo básicamente en una tabla que detalla los privilegios de acceso para los distintos gestores autorizados. Mientras que

la autentificación es realizada por usuario, el control de acceso es realizado por grupos, donde un grupo podría ser un conjunto de usuarios.

### 3.5. SNMP Traps

SNMPv1 and SNMPv2c, along with the associated Management Information Base (MIB), encourage trap-directed notification. The idea behind trap-directed notification is that if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical for the manager to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event.

After the manager receives the event, the manager displays it and can choose to take an action based on the event. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Trap-directed notification can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap, if the device has had a catastrophic outage.

SNMPv1 traps are defined in RFC 1157, with these fields:

- **Enterprise**: identifies the type of managed object that generates the trap.
- **Agent address**: provides the address of the managed object that generates the trap.
- **Generic trap type**: indicates one of a number of generic trap types.
- **Specific trap code**: indicates one of a number of specific trap codes.
- **Time stamp**: provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.
- **Variable bindings**: the data field of the trap that contains PDU. Each variable binding associates a particular MIB object instance with its current value.

Standard generic traps are: coldStart, warmStart, linkDown, linkUp, authentication Failure, egpNeighborLoss.

## 4. RMON: Remote Network Monitoring

RMON (Remote Network Monitoring) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area

networks (LANs) and interconnecting T-1/E-1 and T-2/E-3 lines from a central site. RMON specifically defines the information that any network monitoring system will be able to provide. It's specified as part of the Management Information Base (MIB) in Request for Comments 1757 as an extension of the Simple Network Management Protocol (SNMP). The latest level is RMON Version 2 (sometimes referred to as RMON 2 or RMON2).

RMON can be supported by hardware monitoring devices (known as probes) or through software or some combination. For example, Cisco's line of LAN switches includes software in each switch that can trap information as traffic flows through and record it in its MIB. A software agent can gather the information for presentation to the network administrator with a graphical user interface. A number of vendors provide products with various kinds of RMON support.

RMON collects nine kinds of information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that have occurred. A network administrator can find out how much bandwidth or traffic each user is imposing on the network and what Web sites are being accessed. Alarms can be set in order to be aware of impending problems.

In short, RMON is designed for "flow-based" monitoring, while SNMP is often used for "device-based" management. RMON is similar to other flow-based monitoring technologies such as NetFlow and SFlow because the data collected deals mainly with traffic patterns rather than the status of individual devices.

# 5. Modelo de Gestión de Red de OSI

El Modelo de Gestión de Red de OSI define:

- **CMIS (Common Management Information Service)**: un servicio de gestión.
- **CMIP (Common Management Information Protocol)**: un protocolo de gestión.
- Una base de datos.
- Otros conceptos relacionados.

## 5.1. Modelo de Arquitectura (CMIS)

Los elementos clave de este modelo de arquitectura son:

- **Aplicación de Gestión de Sistemas (SMAP: Systems Management Application Process)**: software local de un equipo (sistema) gestionado que implementa las funciones de gestión para ese sistema (host, router, etc.). Tiene acceso a los parámetros del sistema y puede, por tanto, gestionar todos los aspectos del sistema y coordinarse con SMAPs de otros sistemas.

- **Entidad de Aplicación de Gestión de Sistemas (SMAE: Systems Management Application Entity)**: entidad de nivel de aplicación responsable del intercambio de información de gestión con SMAEs de otros nodos, especialmente con el sistema que hace las funciones de centro de control de red. Para esta función se utiliza un protocolo normalizado (CMIP)
- **Entidad de Gestión de Nivel (LME: Layer Management Entity)**: proporciona funciones de gestión específicas de cada capa de la torre OSI.
- **Base de información de gestión (MIB)**:

## 6. MDM: Mobile Device Management

Mobile device management (MDM) is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.

MDM is a way to ensure employees stay productive and do not breach corporate policies. Many organizations control activities of their employees using MDM products/services. MDM primarily deals with corporate data segregation, securing emails, securing corporate documents on devices, enforcing corporate policies, integrating and managing mobile devices including laptops and handhelds of various categories. MDM implementations may be either on-premises or cloud-based.

MDM functionality can include over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, etc. Most recently laptops and desktops have been added to the list of systems supported as Mobile Device Management becomes more about basic device management and less about the mobile platform itself. MDM tools are leveraged for both company-owned and employee-owned (BYOD) devices across the enterprise or mobile devices owned by consumers. Consumer Demand for BYOD is now requiring a greater effort for MDM and increased security for both the devices and the enterprise they connect to, especially since employers and employees have different expectations concerning the types of restrictions that should be applied to mobile devices.

By controlling and protecting the data and configuration settings of all mobile devices in a network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime.

Algunas soluciones MDM son: **VMware AirWatch**, **BlackBerry UEM**, **IBM MaaS360**, **MobileIron** y **Citrix XenMobile**.

# 7. Preguntas de Exámenes

1. (GSI.PI.2016.B4.20). **Señale qué petición de SMNP v3 permite recuperar grandes cantidades de datos de forma eficiente:**

   *a*) GetNext
   *b*) GetBlock
   *c*) GetBulk
   *d*) GetTrap

2. (GSI.PI.2015.B4.01). **¿Qué modelo de seguridad utiliza por defecto SNMPv3?:**

   *a*) LTPA (Lightweight Third-Party Authentication).
   *b*) CredSSP (Credential Security Support Provider).
   *c*) USM (User-based Security Model).
   *d*) CMS (Credential Manager Service).

3. (GSI.PI.2015.B4.27). **¿Cuál de los siguientes elementos NO forma parte de una PDU de un Trap SNMP, según la RFC 1157?:**

   *a*) Time-stamp
   *b*) Generic-Trap
   *c*) Vendor-Trap
   *d*) Specific-Trap

4. (GSI.PI.2015.B4.28). **El puerto UDP que usa en general SNMP para el gestor es el:**

   *a*) 162
   *b*) 160
   *c*) 100
   *d*) 161

5. (GSI.PI.2014.B4.01, GSI.LI.2014.B4.01). **El comando ping es el acrónimo de:**

   *a*) Packet Internet Group.
   *b*) Packet Internet Gangway.
   *c*) Packet Internet Gate.
   *d*) Packet Internet Groper.

6. (GSI.PI.2014.B4.07, GSI.LI.2014.B4.17). **Señale cuál de las siguientes NO es una Protocol Data Unit (PDU) del protocolo SNMP v3:**

*a*) SetRequest PDU

*b*) InformRequest PDU

*c*) Report PDU

*d*) GetBackRequest PDU

7. (GSI.PI.2014.B4.18). **Señalar cuál de las siguientes NO es una ventaja del uso de directorios LDAP para la autenticación de usuarios:**

   *a*) La mayoría de aplicaciones comerciales permiten su integración fácilmente.

   *b*) Están optimizados para las búsquedas, que es la operación más repetida a la hora de gestionar los usuarios.

   *c*) Permiten implantar sin ningún mecanismo adicional Single Sign On, ya que todas las aplicaciones pueden tener la autenticación a través del LDAP.

   *d*) La replicación con los directorios /etc/passwd está automatizada, y por tanto la integración con las aplicaciones comerciales.

8. (GSI.PI.2013.B4.22). **¿Cómo se llama la base de datos que tiene los parámetros de gestión de una red?:**

   *a*) MIB (Management Information Base).

   *b*) NMD (Network Management database).

   *c*) NMS (Network Management System).

   *d*) Ninguna de los anteriores.

9. (GSI.PI.2013.B4.23). **¿Cuál de los siguientes puertos utiliza el protocolo SNMP?:**

   *a*) 110

   *b*) 119

   *c*) 161

   *d*) 25

10. (GSI.PI.2013.B4.24). **¿Se pueden controlar el número de impresiones que un usuario ha realizado en una impresora en red mediante el protocolo de gestión SNMP?:**

    *a*) Si, siempre y cuando en la MIB de la impresora se contemple este parámetro.

    *b*) No, necesitaría una base de datos externa para almacenarlo.

    *c*) Si, sólo mediante instalación de firmware nuevo en la impresora.

    *d*) Si, pero con protocolos propietarios de la impresora.

11. (GSI.PI.2013.B4.25, GSI.LI.2013.B4.19). **Señale cuál de las siguientes NO es una Protocol Data Unit (PDU) del protocolo SNMP v2/v3:**

*a*) GETREQUEST PDU

*b*) SETRESPONSE PDU

*c*) RESPONSE PDU

*d*) INFORMREQUEST PDU

12. (GSI.PI.2013.B4.26). **Indique la respuesta correcta en relación al comando SNMP GetBulkRequest:**

    *a*) Está disponible en todas las versiones de SNMP.

    *b*) Es utilizado por un sistema gestor de red para enviar un mensaje a otro gestor sobre objetos administrados.

    *c*) Es el que permite utilizar autenticación en SNMP v3.

    *d*) Es utilizado cuando se requiere una cantidad elevada de datos transmitidos.

13. (GSI.PI.2011.B4.02). **La aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red recibe el nombre de:**

    *a*) Sistema de ficheros.

    *b*) Servicio de nombres.

    *c*) Servicio de agente remoto.

    *d*) Servicio de directorio.

14. (GSI.PI.2011.B4.39). **Si deseamos monitorizar los dispositivos de una red con una herramienta de código abierto, deberíamos escoger:**

    *a*) Insight Manager.

    *b*) MTRG (Multi Router Traffic Grapher).

    *c*) Nagios.

    *d*) WireShark.

15. (GSI.PI.2011.B4.54). **¿Cuál de los siguientes NO es un producto de directorio para gestión de usuarios?:**

    *a*) Apache Directory Server.

    *b*) Apple Finder.

    *c*) Microsoft Active Directory.

    *d*) OpenDS.

16. (GSI.PI.2010.B4.27). **¿Cuál de las siguientes operaciones se incorpora en SNMP v2?:**

*a*) SetRequest.

*b*) GetBulkRequest.

*c*) GetNextRequest.

*d*) Trap.

17. (GSI.PI.2010.B4.29). **¿Cuál es el well-known port del protocolo SNMP en el modo petición-respuesta?:**

*a*) 169

*b*) 161

*c*) 171

*d*) 179

18. (GSI.PI.2008.B4.32). **En la herramienta de monitorización remota -RMON-, señale qué elemento genera la información estadística de los nodos:**

*a*) El cliente.

*b*) El servidor.

*c*) Los dos anteriores.

*d*) Ninguno de los anteriores.

19. (GSI.PI.2008.B4.33). **Señale cuál de las siguientes características está disponible en SNMP v3, y NO lo estaba en las versiones previas:**

*a*) Mensajes GetBulkRequest.

*b*) Sentencias username para auntenticación.

*c*) Mensajes GetNextRequest.

*d*) Saludo de tres vías y reconocimiento para la transferencia de mensajes.

20. (GSI.LI.2016.B4.17). **¿Cuál de las siguientes es una solución MDM (Mobile Device Management) para la gestión de dispositivos móviles?:**

*a*) Magento

*b*) Joomla

*c*) AirWatch

*d*) Kobli

21. (GSI.LI.2016.B4.18). **¿Qué puerto utiliza SNMP para los traps por defecto?:**

*a*) 391

*b*) 332

*c*) 162

*d*) 161

22. (GSI.LI.2015.B4.16). **El oid correspondiente a la mib-2 (o MIB-II) es:**

*a*) 1.3.6.1.1.1

*b*) 1.3.6.1.2.1

*c*) 1.3.6.1.3.1

*d*) 1.3.6.1.4.1

23. (GSI.LI.2015.B4.17). **¿Cuál de las siguientes herramientas podría usarse en una red con sistemas UNIX si queremos acceder a recursos comunes, asegurando que la lista de usuarios y grupos esté disponible en todas las máquina clientes?:**

*a*) SRM

*b*) UGMS

*c*) RNUM

*d*) NIS

24. (GSI.LI.2015.B4.24). **En el protocolo SNMP, los valores de comunidad por defecto son:**

*a*) Para lectura "Rmib" y para escritura "Wmib".

*b*) Para lectura "Rmib" y para escritura "Writemib".

*c*) Para lectura "public" y para escritura "private".

*d*) Para lectura "rmis" y para escritura "wmis".

25. (GSI.LI.2014.B4.Reserva.02). **¿Qué características de seguridad presenta SNMPv3, tal y como se mencionan en la RFC 3418 (MIB for the SNMP Protocol)?:**

*a*) Se recomienda que los implementadores usen el modelo de seguridad basado en usuario y el control de acceso basado en vistas.

*b*) Se obliga a que los implementadores usen el modelo basado en usuario y el control de acceso basado en vistas.

*c*) En dicha RFC no se menciona ningún elemento de seguridad.

*d*) En temas de seguridad, sólo hace mención al uso obligatorio del algoritmo de encriptación CBC (Cipher Block Chaining) de DES, conocido también por DES-56.

26. (GSI.LI.2013.B4.18). **En SNMP ¿qué puerto utilizan las traps y en qué sentido se transmiten?:**

*a*) Puerto 162 y las envía el agente al gestor.

*b*) Puerto 162 y las envía el gestor al agente.

*c*) Puerto 161 y las envía el agente al gestor.

*d*) Puerto 161 y las envía el gestor al agente.

27. (GSI.LI.2011.B4.02). **¿Puedo saber, utilizando SNMP, si una impresora de red tiene o no papel?:**

*a*) No, solo puedo conocer el estado de variables de red.

*b*) Sí, si tiene el agente activado.

*c*) No, los dispositivos de impresión se tienen que gestionar con programas propietarios.

*d*) Sí, si en su árbol MIB tiene una extensión CUPS.

28. (GSI.LI.2010.B4.16). **Un agente SNMP envía traps a un sistema administrador de red a través del puerto:**

*a*) 162.

*b*) 126.

*c*) 161.

*d*) 25.

29. (GSI.LI.2010.B4.17). **Una red administrada a través de SNMP contempla tres componentes claves. ¿Cuál de los siguientes NO es uno de ellos?:**

*a*) Dispositivos administrados.

*b*) Agentes.

*c*) Sistemas administradores de red (NMS).

*d*) Registro de ubicación de visitantes (VLR).

30. (GSI.LI.2010.B4.18). **Respecto al protocolo ligero de acceso a directorios (LDAPv3):**

*a*) No admite TCP/IP.

*b*) No es un protocolo abierto.

*c*) No requiere X.500.

*d*) Es dependiente del proveedor.

31. (GSI.LI.2010.B4.20). **¿Cuál de los siguientes NO se encuentra entre los elementos de un Sistema de Gestión de Red?:**

*a*) Gestor DHCP.

*b*) MIB.

*c*) Agente-SMAP.

*d*) NMS.

32. (GSI.LI.2008.B4.08). **Señale cuál de los siguientes protocolos de gestión de redes está basado en el modelo de referencia OSI de ISO:**

    *a*) CMIP
    *b*) SNMP
    *c*) SGMP
    *d*) TL-1

33. (GSI.LI.2008.B4.23). **Seleccione la respuesta correcta:**

    *a*) RMON monitoriza el tráfico de los routers de una red.
    *b*) SMON monitoriza el tráfico de los routers de una red.
    *c*) El standar RMON se define en la RFC 2613.
    *d*) SMON ofrece información sobre las redes locales virtuales VLAN.

34. (GSI.LI.2013.B4.25). **:**

    *a*)
    *b*)
    *c*)
    *d*)

    Indicar cuál de los siguientes NO es un modo de transferencia de datos utilizado por el protocolo HDLC (High Level Data Link Control): a) Modo de respuesta normal (NRM, Normal Response Mode). b) Modo balanceado asíncrono (ABM, Asynchronous Balanced Mode). c) Modo de respuesta asíncrono (ARM, Asynchronous Response Mode). d) Modo balanceado síncrono (SBM, Synchronous Balanced Mode).

## 8. Soluciones

1. C
2. C
3. C
4. A
5. D
6. D
7. D
8. A
9. C
10. A
11. B
12. D
13. D
14. C
15. B
16. B
17. B
18. B
19. B
20. C
21. C
22. B
23. D
24. C
25. A
26. A
27. B
28. A
29. D
30. C
31. A
32. A
33. A

## Referencias

[1] RD 1553/2005. Regula el DNI y sus certificados de firma electrónica. http://www.boe.es/boe/dias/2005/12/24/pdfs/A42090-42093.pdf