

Monitoreo y Supervisión

Conceptos generales y SNMP

2021

Joaquín García
Álvaro Sánchez

Monitoreo y Supervisión

Agenda

- Conceptos generales
- SNMP
- SNMP v2
- SNMP v3
- Extensiones
- Cuestionario de Repaso'
- Anexo

Conceptos generales

Temas

- Gestión de Dispositivos y de Redes
- Modelos de gestor-agente y componentes básicos

La gestión

Conceptos básicos

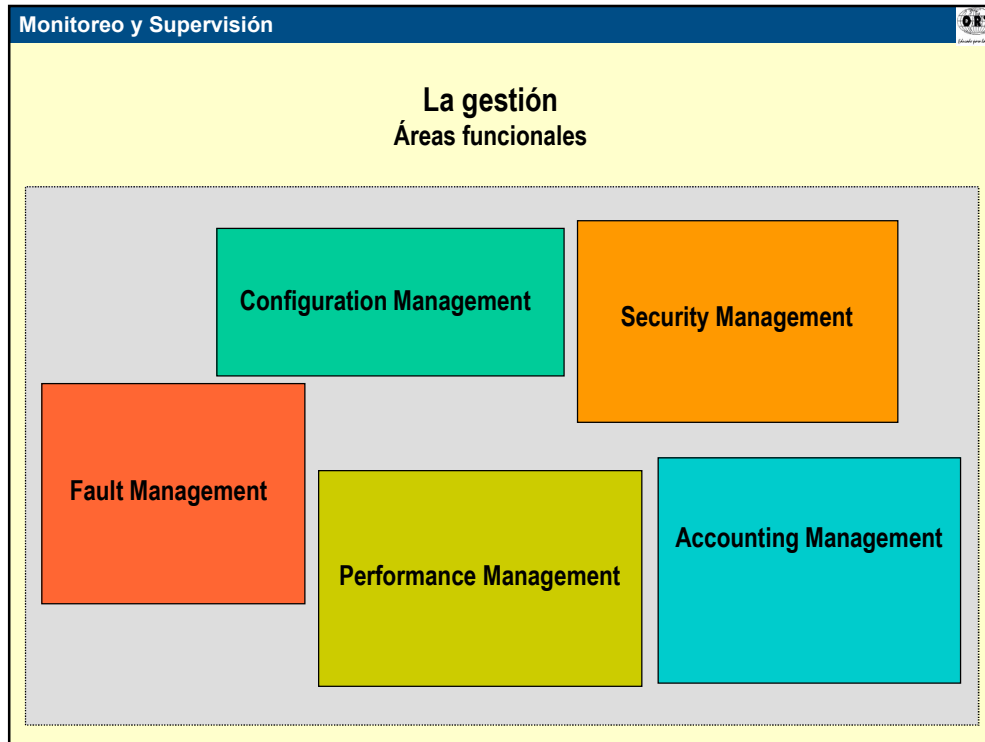


En general la arquitectura de gestión de una red incluye:

- Un sitio central en el cual residen un grupo de estaciones gestoras (Network Management System) desde las cuales se podrá actuar sobre los equipos remotos a gestionar, se recibirán notificaciones de dichos equipos y se presentará (normalmente en formato gráfico) la información de gestión de la red.

En dichas estaciones residen componentes de software para el análisis de la información y el inicio de acciones de recuperación ante fallos. Esas estaciones tienen la capacidad de controlar y supervisar los elementos remotos de la red, y poseen una base de datos integrada por información que reciben de los elementos remotos.

- Un conjunto de elementos de red a ser gestionados, en los cuales funciona un software (agente) que se encarga de recolectar información y de comunicarse con el sitio central.
- Un protocolo de comunicación, encargado de transmitir información entre el software del equipo y las estaciones gestoras.



Áreas funcionales

La gestión abarca diversas funciones que contribuyen al conocimiento pormenorizado del estado de sus componentes, lo cual permite el disparo de acciones preventivas y correctivas adecuadas. Dichas funciones se agrupan en áreas que ISO estandarizó del siguiente modo:

- Configuration Management - Conjunto de facilidades para el control, la identificación, y la comunicación de datos respecto de los objetos gestionados.
- Fault Management - Detección, aislamiento y corrección de situaciones anormales de los recursos.
- Performance Management - Evaluación del comportamiento de los objetos gestionados y efectividad de las comunicaciones.
- Security Management - Protección de los objetos gestionados, provisión de redundancia y empleo de la misma.
- Accounting Management - Contabilidad del uso de los recursos.

El control engloba las actividades de modificación de parámetros de funcionamiento y ejecución de acciones. Son las actividades preponderantes en la gestión de configuración y en la gestión de seguridad.

El **monitoreo** se dedica a la observación del estado de los dispositivos. Es la actividad preponderante en la gestión de fallos, en la gestión de rendimiento (performance) y en la gestión de contabilidad.

La gestión Áreas funcionales

Control de dispositivos y de red

Configuration Management

- Definiciones de funciones
- Activación de recursos
- Gestión de inventario
- Gestión de topología
- Gestión de servicios de directorio
- Gestión de SLA
- Gestión de incidencias
- Gestión de cambios de configuración

Security Management

- Registro de eventos
- Reportes de violaciones
- Uso de backups
- Perfiles de usuarios
- Funciones de protección
- Análisis de riesgos
- Implantación de sistemas de seguridad

Monitoreo de dispositivos y de red

La gestión Áreas funcionales

Control de dispositivos y de red

Fault Management

Detección de fallos
antes de que sucedan
(monitoreo de
tendencias)
Detección de fallos
Aislamiento del fallo
Diagnóstico
Resolución

Performance Management

Definición de indicadores
Monitoreo de indicadores
Análisis de indicadores
Disponibilidad
Latencia
Fiabilidad
Throughput
Utilización

Accounting Management

Recursos usados
Horas
Prioridades
Perfiles de usuario

Monitoreo de dispositivos y de red

La gestión

Gestión de Performance – Calidad de servicio (Quality Of Service) en redes IP

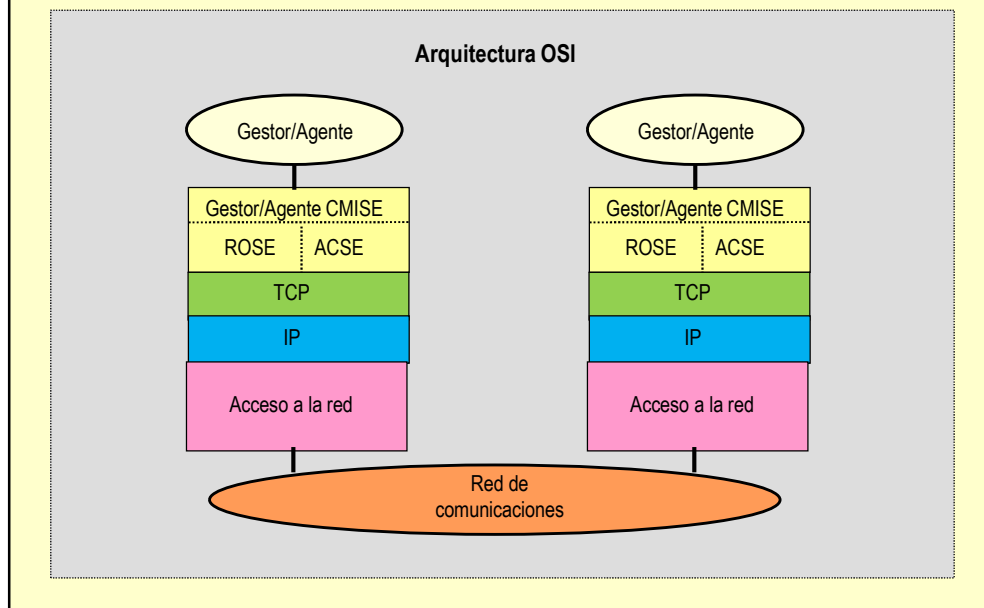
Medidas diferenciales para el tratamiento de los paquetes

- Priorización de tráfico sensible al retardo
- Limitación del tráfico por flujos
- Descarte selectivo y aleatorio

Mecanismos para garantizar calidad de servicio

- *Priorización* – Según el régimen de encolamiento seleccionado, varia el comportamiento.
 - Puede priorizarse en forma estricta un tipo de tráfico (*Priority Queuing*), lo cual significa que sólo si se vacía la cola prioritaria, se procede a despachar paquetes de las restantes colas.
 - Puede priorizarse en forma relativa, distribuyendo el tiempo de ciclo de atención de los buffers de modo que se asignen porcentajes del mismo a cada cola (*Custom Queuing*).
 - Pueden aplicarse mecanismos automáticos que reservan recursos para cada flujo en función de su historia reciente (*Weighted Fair Queuing*), y existen variantes que permiten que el administrador influya en el mecanismo (*Custom Based – WFQ*).
 - Finalmente pueden aplicarse mecanismos híbridos, tales como el *Low Latency Queuing*, que combina PQ (priorización estricta para paquetes de voz) con CB-WFQ (para datos).
- *Limitación del tráfico* (Committed Access Rate) – Consiste en la limitación de la velocidad en una interfaz según el tipo de tráfico. Si la oferta de un tipo de tráfico supera el valor máximo definido para el mismo, se descarta el exceso.
- *Descarte* – Weighted Random Early Discard técnica de prevención de congestión. Consiste en descartar paquetes en forma aleatoria de modo que no afecte a un flujo en particular, y que logre la reducción de las ventanas del TCP en forma no sincronizada.

Modelo de gestor-agente y componentes básicos



Common Management Information Protocol

Desarrollado por ISO. Es de propósito general, no restringido a TCP/IP. Es sofisticado, incluye comandos potentes pero complejos. Es más versátil pero no está tan difundido. Es orientado a conexión.

CMIP comunica los gestores de cada capa (Layer Management Entities) con las aplicaciones de gestión (System Management Application Entities). Cada LME opera en un nivel OSI y no da una visión global de la operación. A su vez hay un SMAE para cada LME. Los SMAE de diferentes dispositivos se comunican con CMIP para permitir al administrador la recolección y el análisis de los datos de la red como un todo, servicio llamado a veces Common Management Information Service.

Se definen las siguientes operaciones:

ACTION – Solicita se ejecute una acción de acuerdo con lo previsto en la estación gestionada.

GET – Solicita el valor de una instancia de un objeto gestionado.

SET – Establece el valor de una instancia de un objeto gestionado.

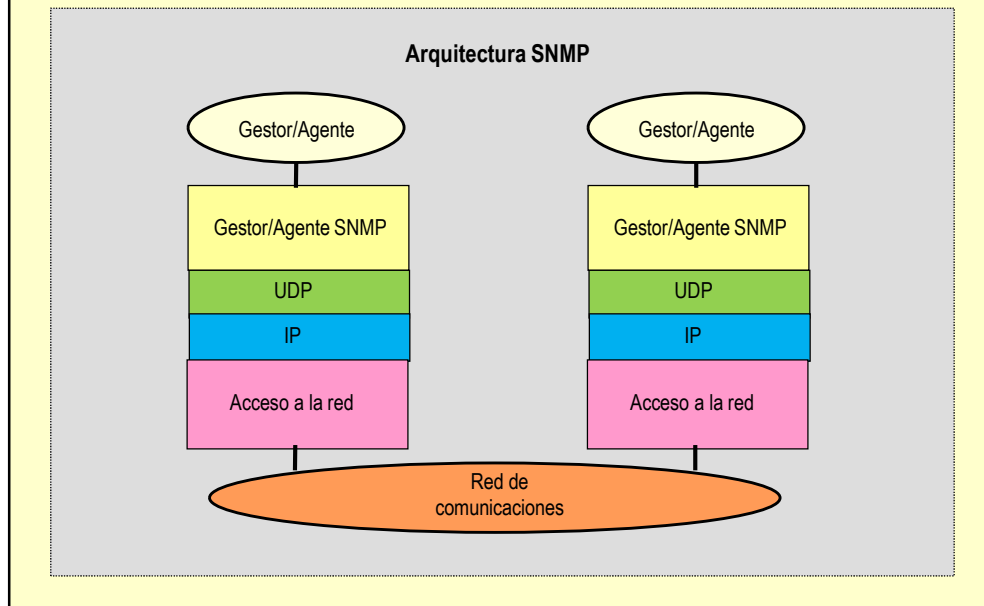
CANCEL_GET – Cancela una solicitud GET.

CREATE – Crea una instancia de un objeto gestionado.

DELETE – Elimina una instancia de un objeto gestionado.

CMIP over TCP/IP (CMOT)

Se definió por parte del Internet Architecture Board (IAB) como la solución de largo plazo que reemplazaría a SNMP.

Modelo de gestor-agente y componentes básicos**Simple Network Management Protocol**

Desarrollado por IETF se emplea ampliamente en ambientes TCP/IP. Es no orientado a conexión, emplea UDP y se sitúa en el nivel aplicación.

El agente reside en los dispositivos y emplea mínimos recursos para no perjudicar la performance. Colecciona datos y los almacena en la base que reside en el dispositivo.

Emplea UDP para las comunicaciones.

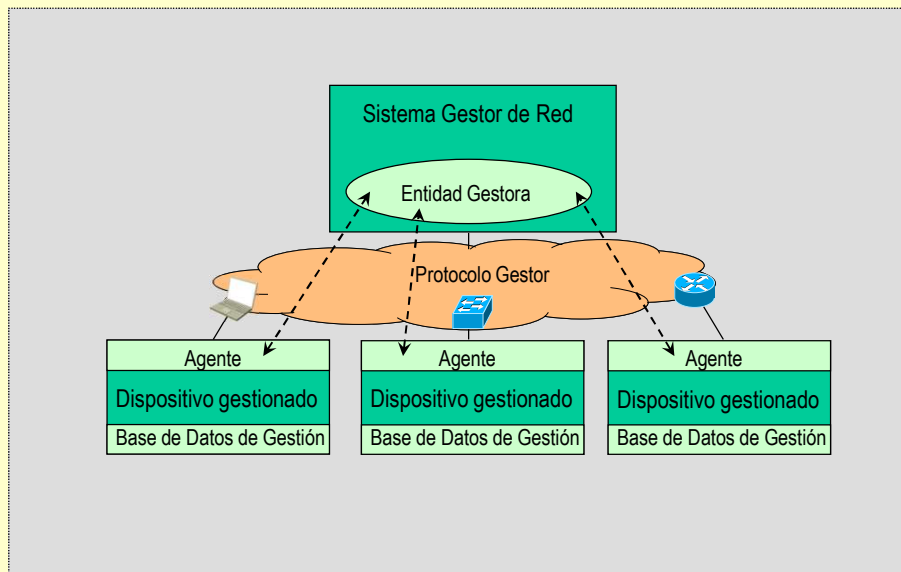
Comparación con CMIP

Las variables CMIP permiten ejecutar tareas y no sólo enviar información como en SNMP. CMIP es más seguro que SNMP porque soporta autorización, control de accesos, y registros de seguridad (logs). CMIP logra mayor eficiencia que SNMP con una sola solicitud. CMIP reporta mejor condiciones inusuales de la red.

Protocolo a analizar

A lo largo del curso se verán en detalle el funcionamiento, los formatos, y los alcances y limitaciones del protocolo SNMP, que actualmente es el de uso más difundido.

Modelo de gestor-agente y componentes básicos



Sistema gestor de red

Las funciones de gestión de red se efectúan con el apoyo de un sistema de información, que incluye un sistema operativo, una plataforma de base de datos, un protocolo de comunicaciones, un ambiente de ejecución de programas y una interfaz de usuario.

En el sistema hay dos principales protagonistas: el gestor (manager), que controla toda la actividad de gestión, y el agente (agent), que ajusta y controla los objetos gestionados que están bajo su responsabilidad, de acuerdo con las directivas del gestor, a quien le reporta los resultados.

En la RFC 1157 se define la NMS (Network Management Station) como una estación que ejecuta aplicaciones de gestión de red (Network Management Applications) que supervisan y controlan los elementos de red (Network Elements). En dichos elementos se emplea un agente de gestión (Management Agent) para llevar a cabo esas funciones. El SNMP permite la comunicación entre la NMS y los MA.

Protocolo de comunicaciones

Se requiere un protocolo de comunicación entre gestor y agentes. Sus funciones son:

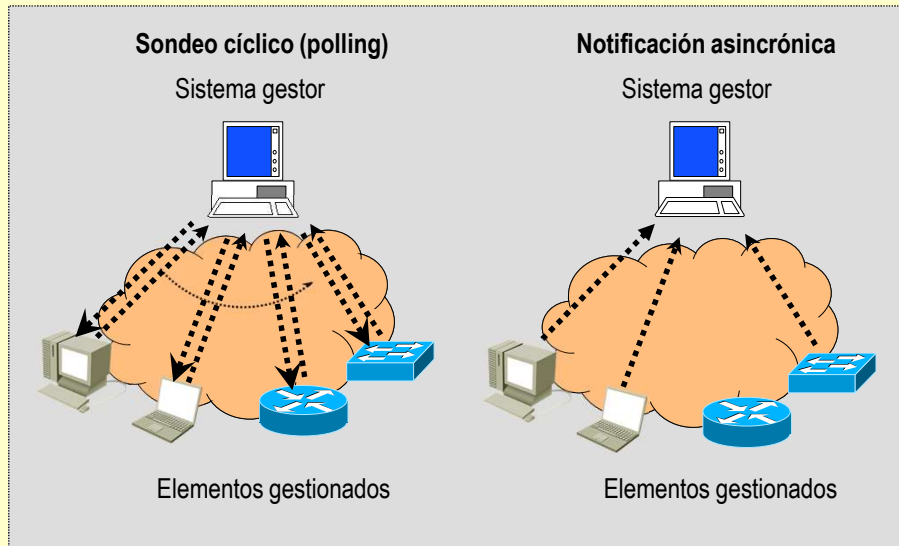
- leer y actualizar los atributos de los objetos gestionados
- ordenar la ejecución de funciones específicas a los objetos gestionados
- reportar los resultados obtenidos por los objetos gestionados
- crear y suprimir objetos gestionables

Base de Datos de Información (Management Information Base, MIB)

Modelo simplificado que permite efectuar la gestión en ambientes complejos.

Está constituido por "objetos", que corresponden a los recursos de red que admiten algún tipo de gestión.

Ejemplos: tarjeta NIC de una PC, interfaz serial de un router, CPU de un servidor.

Modelo de gestor-agente y componentes básicos**Sondeo cíclico (polling)**

Consiste en una interrogación periódica que la estación gestora efectúa a cada estación remota, a fin de relevar sus estado. Las estaciones remotas deben esperar la oportunidad de reportar sucesos que viene indicada por la estación gestora.

De ese modo se recoge el panorama completo de lo que sucede en la red.

La desventaja es la demora que puede tenerse entre la ocurrencia de un evento y el momento en que se produce el relevamiento del mismo.

Notificación asincrónica

Consiste en la posibilidad de reportar eventos por parte de las estaciones remotas en seguida que ocurren, sin necesidad de esperar el momento previsto en el ciclo.

SNMP (Simple Network Management Protocol)

Temas

- Generalidades de SNMP
- SNMP
- SNMPv2
- SNMPv3
- Extensiones

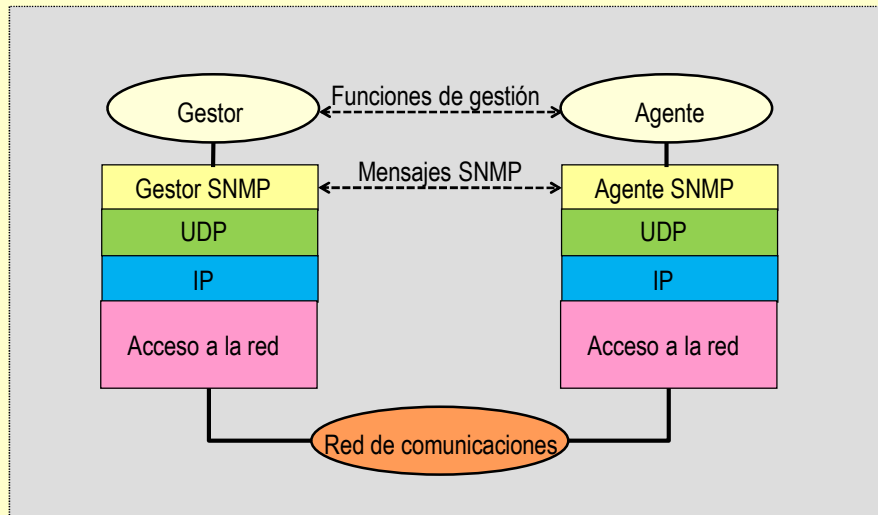
Generalidades de SNMP

Temas

- SNMP - Características
- Tipos de operaciones
- Estándares
- Proxies
- SMI
- MIB

Generalidades de SNMP

Simple Network Management Protocol - Características



Simple Network Management Protocol (SNMP)

El SNMP asiste al administrador en la localización y corrección de problemas en dispositivos y redes. El administrador ejecuta un programa cliente SNMP en una estación local desde la cual monitorea los equipamientos. El cliente SNMP se comunica con uno o varios servidores SNMP (agentes SNMP) que funcionan en máquinas remotas. Estos servidores mantienen un conjunto de variables que incluyen valores estadísticos de performance (paquetes recibidos y transmitidos, con y sin error), estructuras de datos (cache de ARP, tablas de enrutamiento). El funcionamiento se basa en dos tipos de operaciones:

- búsqueda (fetch) de valores contenidos en variables locales del servidor
- escritura (store) de valores en dichas variables

Como no se incluyen otras operaciones, el control remoto de dispositivos se debe ejecutar mediante la escritura en variables, y en su interpretación como comandos por parte del software del servidor.

Los eventos no planeados como por ejemplo el reseteo de un nodo, se registran en variables y son reportados por el servidor (traps SNMP). También se emplean los traps para reportar situaciones en las cuales se superan niveles preestablecidos de eventos (un exceso de errores puede disparar un trap). Este tipo de notificaciones vuelve mucho más escalable el monitoreo de la red, y reduce la carga de procesamiento y de ocupación del medio en relación con el método de sondeos periódicos por parte de la estación gestora.

Para los dispositivos no SNMP se pueden definir agentes Proxy que dialogan en SNMP con los clientes y en protocolos específicos no standard con los dispositivos.

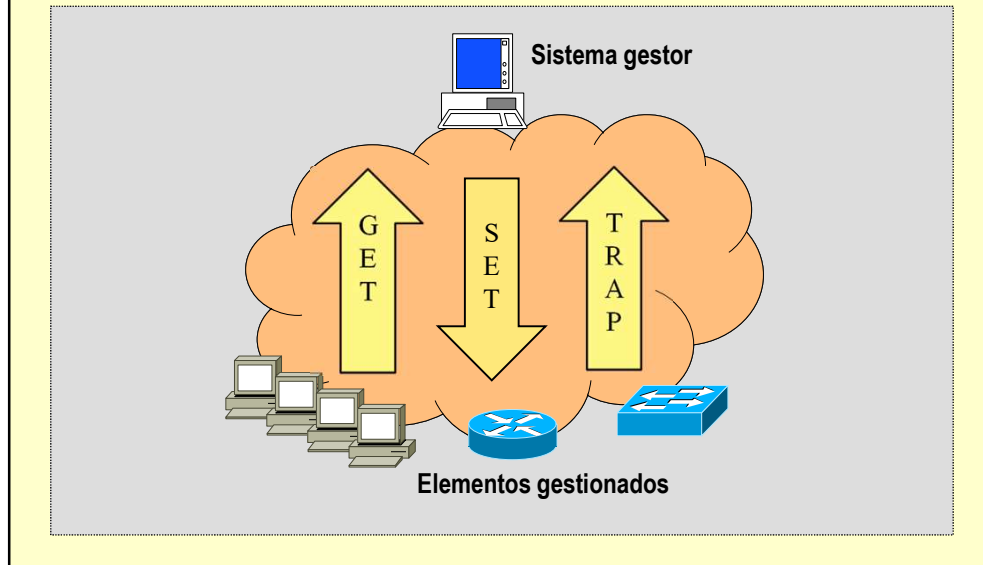
Transporte de SNMP

Usualmente se emplea UDP.

La razón de emplear UDP es que a menudo la gestión de red se necesita en momentos de mal funcionamiento, que suele ser acompañada de congestión y pérdida de paquetes. Si se empleara TCP, el control de congestión del TCP causaría que se redujera la tasa de envíos, y dejarían de enviarse los mensajes precisamente en el momento en el que el administrador de la red necesita enviar mensajes SNMP.

Generalidades de SNMP

Tipos de operaciones



Tipos de operaciones soportadas en SNMP

En SNMP sólo se soportan las operaciones de inspección y de alteración de variables preestablecidas que se describen a continuación.

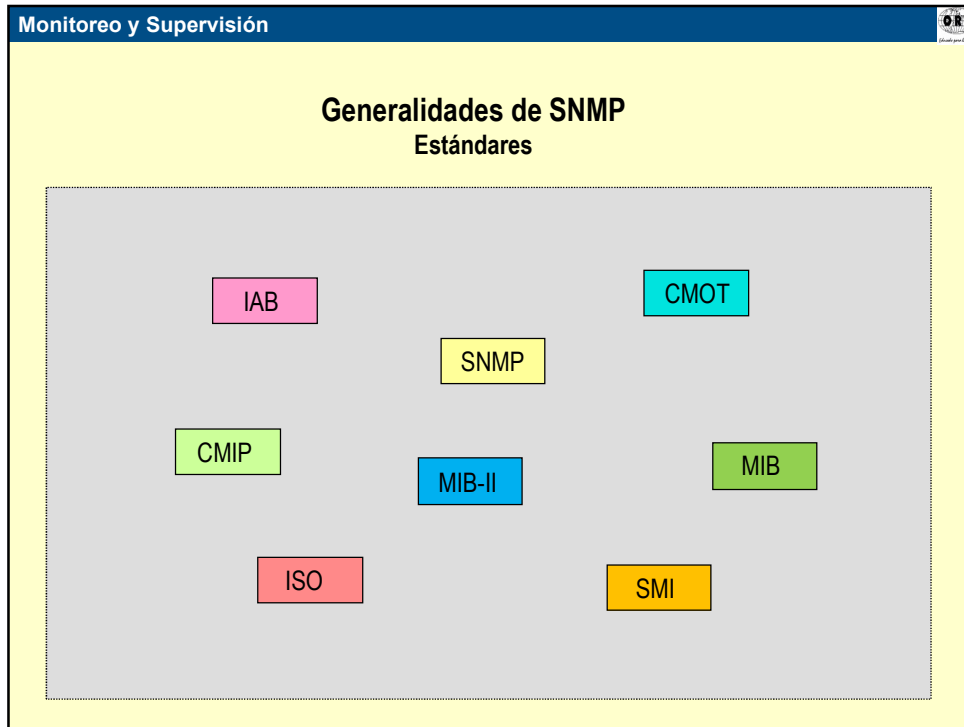
Get: la estación gestora obtiene el valor de un objeto escalar de un elemento gestionado.

Set: la estación gestora actualiza el valor de un objeto escalar en un elemento gestionado.

Trap: el elemento gestionado reporta a la estación gestora el valor de un objeto escalar de un elemento gestionado, sin que haya habido una solicitud de parte de ésta última (superación de un nivel o threshold, cambio de estado de una variable binaria, etc.).

No es posible alterar la estructura de datos agregando o quitando instancias de objetos. Además, sólo es posible acceder a las "hojas" del árbol de datos previsto, y no a puntos intermedios del mismo.

No es posible acceder a una tabla completa ni a una fila de una tabla mediante una sola operación. Lo anterior procura simplificar la implementación de SNMP, pero limita la eficiencia de la gestión.



Estándares

A continuación se indican los estándares más importantes.

SNMP (Simple Network Management Protocol) tiene status recomendado y se especifica en RFC 1157.

SMI ("Structure and Identification of Management Information") se especifica en RFC 1155.

MIB ("Management Information Base") para redes TCP/IP se especifica en RFC 1156.

MIB-II (MIB-II: Management Information Base for Network Management of TCP/IP-based Internets) para redes TCP/IP tiene status recomendado y se especifica en RFC 1213.

SNMP-DPI ("Simple Network Management Protocol Distributed Programming Interface" se especifica en RFC 1228

Modelo administrativo de SNMP se especifica en RFC 1351.

Protocolos de seguridad SNMP se especifican en RFC 1352.

CMIP (Common Management Information Protocol) y *CMIS* (Common Management Information Services) se definen en ISO/IEC 9595 y 9596.

CMOT (CMIS/CMIP Over TCP/IP) tiene status de electivo y se especifica en RFC 1189.

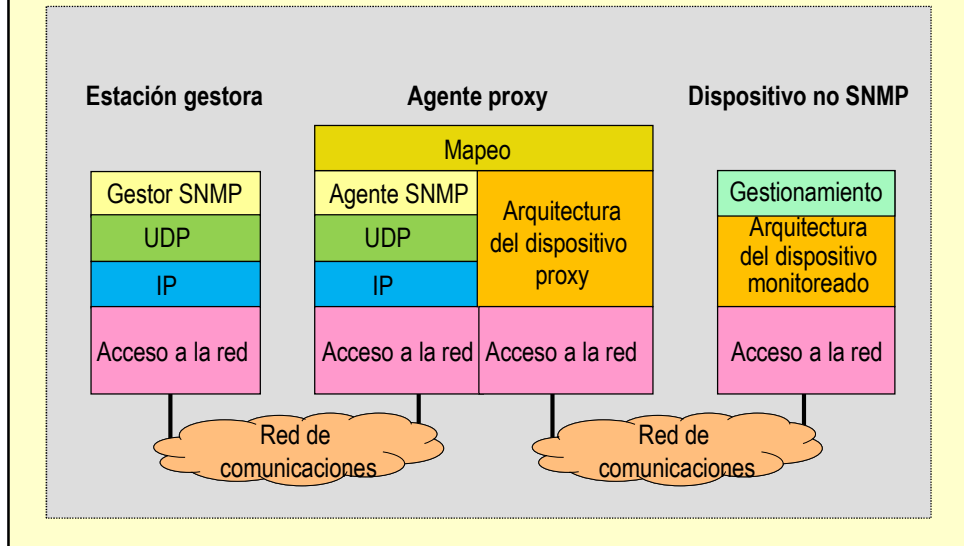
OIM-MIB-II (OSI Internet Management: MIB ("Management Information Base")) tiene status de electivo y se especifica en RFC 1214.

Recomendaciones del IAB para el desarrollo de estándares de gestión de red, se especifican en RFC 1052.

Servicios ISO de presentación sobre redes basadas en TCP/IP se especifican en RFC 1085.

Generalidades de SNMP

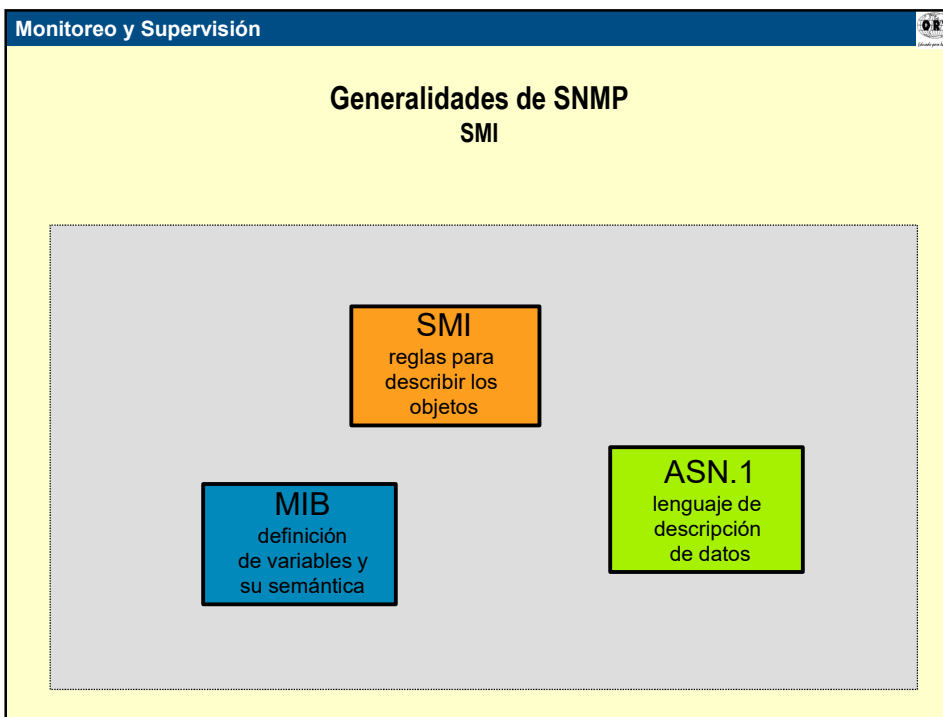
Proxies



Proxies

Algunos dispositivos, tales como ciertos PC's, controladores programables, etc., no soportan la pila TCP/IP, en la cual se basa SNMP.

A efectos de no recargar al SNMP, se desarrollan dispositivos proxy que compatibilizan los requerimientos SNMP con las funcionalidades de gestión implementadas en los dispositivos a gestionar.



SMI ("Structure and identification of Management Information")

El SMI define las reglas para describir los objetos gestionados y cómo los protocolos sometidos a la gestión pueden acceder a ellos.

La descripción de los objetos gestionados se hace utilizando un subconjunto de ASN.1 ("Abstract Syntax Notation 1, estándar ISO 8824), un lenguaje de descripción de datos. La definición del tipo de objeto consta de cinco campos:

Objeto: nombre textual, llamado *descriptor del objeto*, para el tipo del objeto, junto con su correspondiente *identificador de objeto*, definido abajo.

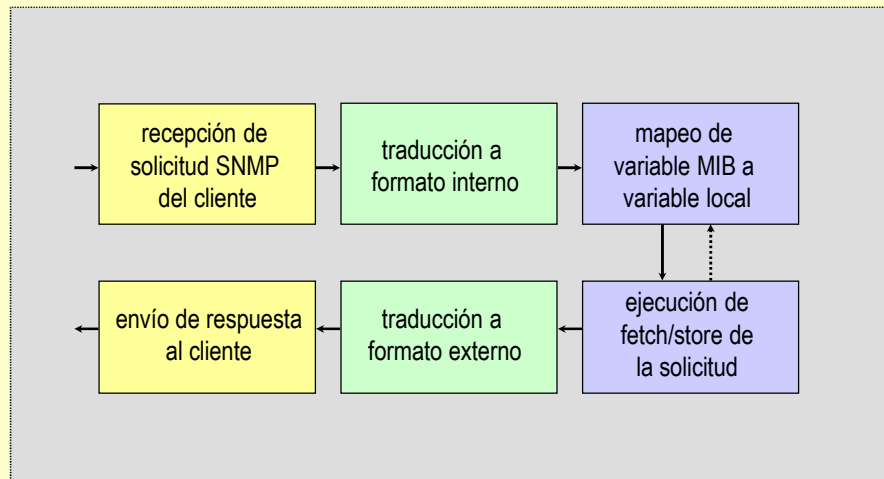
Sintaxis: la sintaxis abstracta para el tipo el objeto. Las opciones son SimpleSyntax (entero, octeto de caracteres, identificador de objeto, Null), ApplicationSyntax (dirección de red, contador, escala, ticks, opaco) u otro tipo de sintaxis de aplicación(ver el RFC 1155 para más detalles).

Definición: descripción textual de la semántica del tipo.

Acceso: sólo lectura, sólo escritura, lectura - escritura o inaccesible.

Status: obligatorio, opcional u obsoleto.

Generalidades de SNMP MIB



Management Information Base (MIB)

Un standard separado del SNMP, el MIB, define un conjunto de variables que el servidor de SNMP debe mantener y la semántica de cada variable.

No es necesariamente una base de datos que centralice la información.

La información de naturaleza dinámica (contador, estado de una interfaz) se almacena en el dispositivo mismo.

La información de mayor permanencia (topología de red) se almacena en lugares específicos.

La estructura general de la información se define en RFC 1155. Los objetos se definen en RFC 1213 (MIB-II).

Entendemos la MIB como el conjunto de valores que componen la base de datos, y trabajaremos con objetos (los registros)

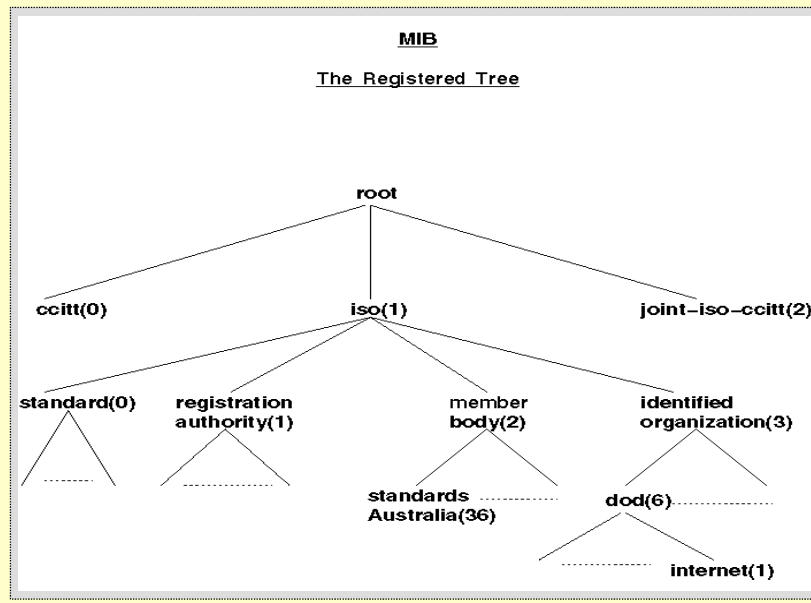
- Objeto:
 - Nombre
 - Permisos (Read, Read/Write, Write Only, No Accessible)
 - Tipo (Contador, String, Entero, Medidor)
 - Descripción
 - Estado
- La MIB tiene una estructura en Árbol.

Estructuras internas de datos

Las estructuras internas que emplean los dispositivos para su control, no siempre se corresponden directamente con las variables MIB. Por ello, el software SNMP debe procesar la traducción entre variables locales y variables MIB, pero de modo que el software cliente SNMP no lo perciba.

Generalidades de SNMP

MIB











Management Information Base (MIB)

- SNMP accede a instancias particulares de un objeto (si una consulta no devuelve un resultado puede deberse a que no existe una instancia para el objeto)
- Todas las instancias de un objeto residen como hojas en el árbol de MIB
- SNMP accede a instancias mediante un Object Identifier que tiene el siguiente formato: x.y donde "x" es el OID del objeto en la MIB, mientras "y" es un sufijo que identifica una instancia particular del objeto
- Para instancias simples se emplea "y" = 0
por ejemplo: *ipInReceives* (OID: 1.3.6.1.2.1.4.3) es referido por SNMP como 1.3.6.1.2.1.4.3.0 (*ipInReceives.0*)
- Para instancias simples de objetos en columna (de una tabla) se emplea el formato: "y" = I1.I2.I3.... (donde li son índices de la tabla)
- En la MIB las variables se guardan en orden lexicográfico, que significa el orden en que aparecen las hojas del árbol cuando se las recorre (sólo a las hojas) ordenadamente.

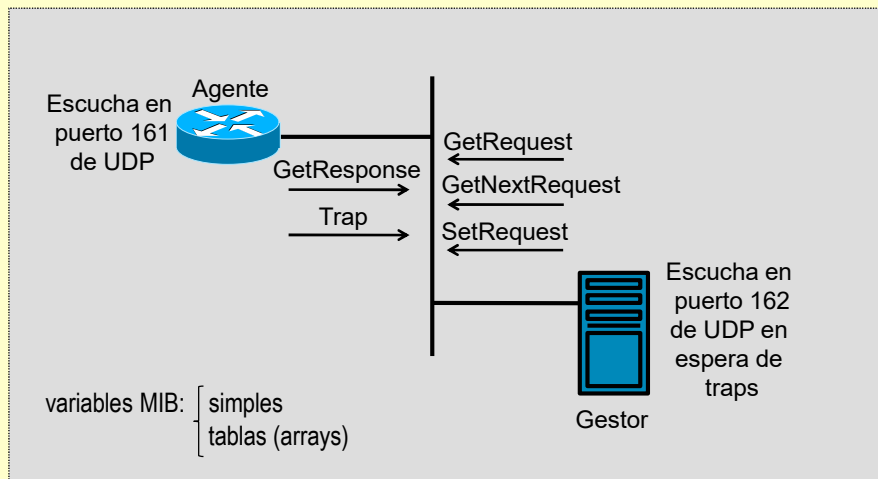
Generalidades de SNMP MIB

.1.3.6.1.4.1	.iso.org.dod.internet.private.enterprises
2021	OID: gestión de equipos
2021.4	cantidad de memoria disponible
2021.9.1	tamaño de los discos del equipo y utilización de los mismos
2021.10.1	carga del equipo
2021.10.1.5.1	carga del equipo en 1 minuto
2021.10.1.5.2	carga del equipo en 5 minutos
2324	OID: gestionredes
2324.1.0	systemId
2324.2.0	systemLoad
2324.3.0	systemLoadMax

**Generalidades de SNMP
MIB**

Object Name	Object Identifier	Object Type
 ucDavis	1.3.6.1.4.1.2021	MODULE-IDENTITY
 laTable	1.3.6.1.4.1.2021.10	OBJECT-TYPE
 laEntry	1.3.6.1.4.1.2021.10.1	OBJECT-TYPE
 laIndex	1.3.6.1.4.1.2021.10.1.1	OBJECT-TYPE
 laErrorFlag	1.3.6.1.4.1.2021.10.1.100	OBJECT-TYPE
 laErrorMessage	1.3.6.1.4.1.2021.10.1.101	OBJECT-TYPE
 laNames	1.3.6.1.4.1.2021.10.1.2	OBJECT-TYPE
 laLoad	1.3.6.1.4.1.2021.10.1.3	OBJECT-TYPE

Generalidades de SNMP MIB



Variables MIB

Las variables MIB se clasifican en dos clases: simples y tablas. Los dispositivos mantienen en general una versión de cada variable simple, que suele ser un número entero (ej.: n° de datagramas recibidos). Las tablas, en cambio, corresponden a un conjunto unidimensional de valores (array) que puede tener varias versiones de una variable (ej.: una entrada para cada interfaz de red). Una tabla puede tener varios campos, en cuyo caso se definen como un array de conjuntos de variables.

Las operaciones que se pueden solicitar son:

- *set-request*, para asignar un valor a una variable
- *get-request*, para leer el valor de una variable
- *get-next-request*, para obtener el valor de la variable que sucede en orden lexicográfico a la variable anterior (permite recorrer una tabla)
- *trap*, usada por el agente para informar asincrónicamente al NMS sobre un evento

Nivel transporte en SNMP

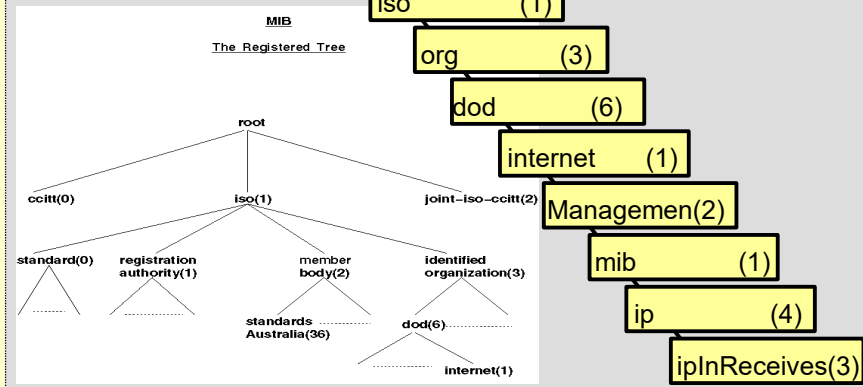
SNMP emplea UDP para el transporte, y se prevén el puerto 162 en el gestor y el 161 en el agente.

El estándar no prevé acciones en caso de pérdida de un mensaje.

Generalidades de SNMP

MIB

iso.org.dod.internet.mgmt.mib.ip.ipInReceives
1.3.6.1.2.1.4.3



ASN.1

MIB emplea ASN.1 para nombrar las variables. ASN.1 emplea una estructura jerárquica de nombres, de modo que cada nombre es único. La autoridad sobre los nombres es distribuida pero está cuidadosamente establecida. Los nombres tienen una sintaxis que consiste en una sucesión de etiquetas separadas por puntos: *iso.org.dod.internet.mgmt.mib.ip.ipInReceives*. ASN.1 prevé la representación numérica de las variables, para su empleo por parte del SNMP.

Por ejemplo, para la variable *ipInReceives* la notación numérica es: 1.3.6.1.2.1.4.3 y se le denomina Object Identifier (OID).

En los mensajes SNMP, a esa variable se le agrega un cero que representa que es la única versión que existe en la MIB: 1.3.6.1.2.1.4.3.0

El software SNMP local almacena y maneja sólo las terminaciones de las representaciones (*ip.ipInReceives*), de modo de identificar la variable con mejor performance. Al transmitir, el SNMP agrega el prefijo (*iso.org.dod.internet.mgmt.mib.*, o 1.3.6.1.2.1.) y al recibir, luego de verificarlo, lo elimina.

Generalidades de SNMP

MIB II

- La MIB-II representa la MIB standard definida por IETF que todo agente debe soportar.
- Definida en la RFC 1213
- Todos los objetos incluidos en ella son mandatory, es decir que su implementación es obligatoria por parte de todos los agentes.
- Se compone de aproximadamente 170 objetos de gestión.
- Se incluyeron elementos esenciales para control de fallas y configuración
- Se seleccionaron elementos que no produzcan problemas en las redes.
- No se consideraron limitantes en el número de elementos.
- No se incluyeron elementos que pueden derivarse de otros para evitar redundancia.

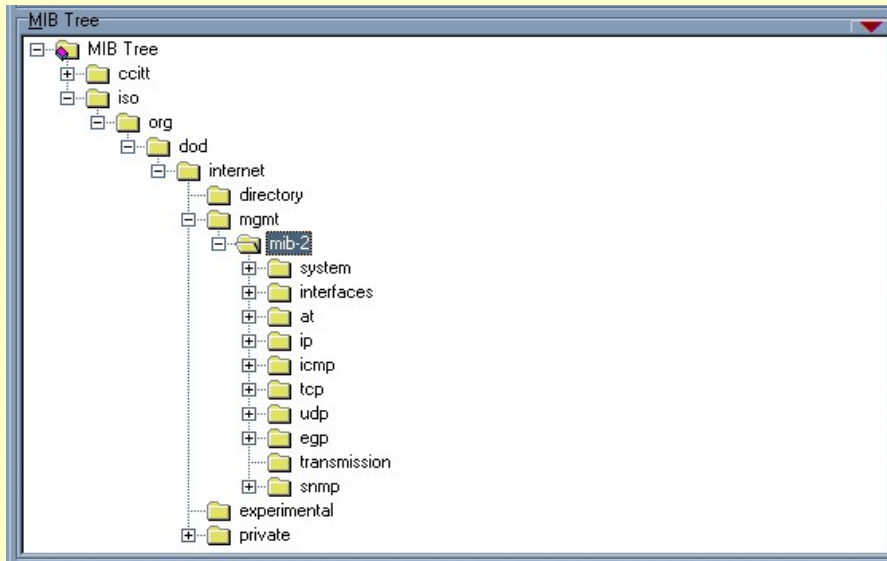
Introducción a MIB-II

MIB-II (RFC 1213) define una segunda versión de la MIB-I definida en la RFC1156, agregando a la misma algunos grupos.

Generalidades de SNMP

MIB II

- MIB-II en un MIB browser:



Introducción a MIB-II

Aquí se presenta visualmente el esquema de MIB-II.

Generalidades de SNMP

MIB II

- MIB-II, los grupos mas importantes :
 - system
 - interfaces
 - address-translation (at)
 - ip
 - icmp
 - tcp, udp
 - transmission

Introducción a MIB-II

Grupos en los que se subdivide la MIB-II:

- system (1) Contiene información general sobre el sistema
- Interfaces (2) Contiene información acerca de cada interface del sistema.
- at (address-translation) (3) sobre las tablas de ruteo (deprecated)
- ip (4) información acerca del protocolo IP.
- icmp (5) información acerca del protocolo ICMP
- tcp (6), udp (7) información acerca de los protocolos TCP y UDP (son dos ramas diferentes)
- Transmission (10) referencia sobre los medios de transmisión utilizados por el sistema

Se incluye en la información presentada el identificador para cada uno de los grupos, que define su ubicación en la estructura jerárquica, 1.3.6.1.2.1 corresponde a MIB-II y el subárbol correspondiente para cada grupo.

Una implementación compatible con MIB-II deberá implementar todos los subgrupos que sean aplicables a al sistema, por ejemplo si el mismo trabaja con el protocolo IP, se deberá implementar el subgrupo 4.

Generalidades de SNMP

MIB II

- **system:**
 - define varios objetos, en su mayoría textuales, que permiten configurar comentarios y descripciones varias acerca de un sistema.
 - los valores de estos objetos se especifican generalmente como parte de la configuración del agente (NO vía SNMP)
 - muy útiles en la practica
 - ejemplos :
 - sysDescr, sysUpTime, sysName, sysContact, sysLocation

Sub-grupo system (MIB-II)

Define información general sobre el sistema que se monitorea. Esta información no aporta en general datos que sean recolectados o información específica del comportamiento del sistema, aporta información acerca del funcionamiento general del mismo.

El subgrupo contiene los siguientes elementos:

- sysDescr (1). Contiene una descripción general del sistema, con elementos como ser hardware, sistema operativo etc.
- sysObjectID (2). Referencia a través de un OBJECT IDENTIFIER, del subsistema que contiene la información privada, brindada por el fabricante.
- sysUpTime (3). Contiene el tiempo transcurrido desde la última reiniciación del sistema.
- sysContact (4). Información sobre la identificación y forma de contacto con el administrador del sistema.
- sysName (5). Nombre administrativo del sistema.
- sysLocation (6). Ubicación física del sistema
- sysServices (7). Valor entero que indica los servicios primarios que ofrece el sistema. Estos se encuentran definidos según un código.

Generalidades de SNMP

MIB II

- **interfaces:**
 - información estadística genérica para los distintos tipos de interfaces de red, a nivel físico.
 - ifNumber contiene el numero de interfaces del sistema.
 - ifTable contiene una fila por interfaz con todos los valores estadísticos.
 - Ejemplos :
 - ifType, ifSpeed, ifPhysAddress, ifOperStatus, ifInOctects, ifOutOctects

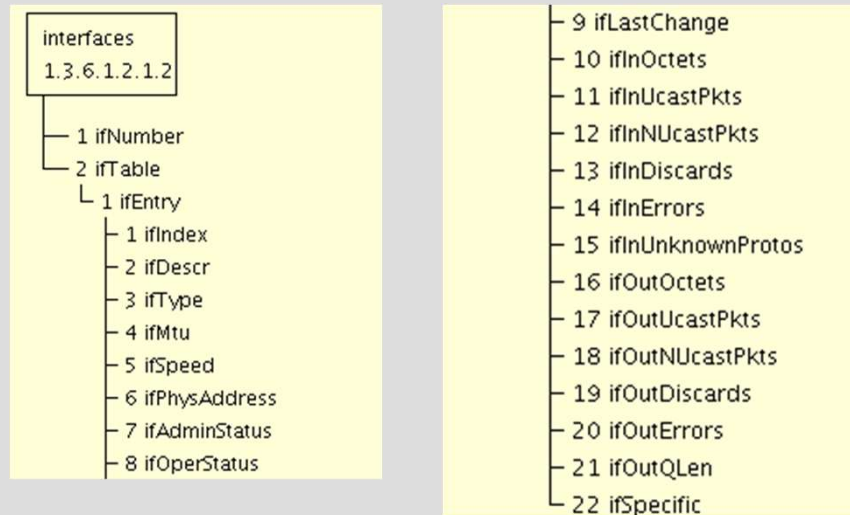
Sub-grupo interfaces (MIB-II)

Contiene información genérica acerca de las interfaces que conectan el sistema a la red, incluyendo información de su configuración y eventos ocurridos en la misma.

La misma se presenta definido con un objeto tipo escalar, ifNumber (1), que define la cantidad de interfaces que contiene el sistema, y un objeto tipo tabla ifTable (2), y un objeto ifEntry(1), que contiene información para cada una de las interfaces en concreto.

Generalidades de SNMP MIB II

- Grupo **interfaces**:



Sub-grupo interfaces (MIB-II)

El subgrupo contiene dentro del objeto ifTable, entre otros, los siguientes elementos:

- ifIndex (1). Valor único definido para cada interfaz. La identifica.
- ifDescr (2). Texto que describe la interfaz referida en el sub-árbol respectivo.
- ifType (3). Código que representa el tipo de interfaz. Estos valores se encuentran definidos en MIB-II.
- ifSpeed (5). Valor estimado de la tasa de transferencia de la interfaz
- ifPhyAddress (6). Dirección física de la interfaz. Depende de la tecnología de la misma.
- ifOperStatus (8). Estado operacional de la misma. Permite los siguientes valores: up(1), down(2), testing(3)
- ifInOctets (10). Cantidad total de octetos (bytes) recibidos por la interfaz.
- ifOutOctets (16). Cantidad total de octetos (bytes) transmitidos por la interfaz.

Se definen además otros elementos lo que pueden consultarse en la RFC1213 ifMtu, ifAdminStatus, ifLastChange, ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifInErrors, ifInUnknownProtos, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors, ifOutQLen, ifSpecific.

Generalidades de SNMP

MIB II

- **address-translation:**
 - información sobre la correspondencia entre direcciones físicas y direcciones de capa de red.
 - soporte para diferentes capas de enlace (Ethernet, IEEE 802.x, X.25)
 - soporte para diferentes protocolos de capa de red (IP, CNLP, X.25)

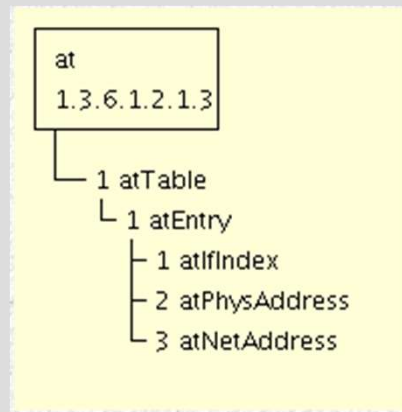
Sub-grupo at address-translation (MIB-II)

Este subgrupo está constituido por una tabla, donde cada fila corresponde a una interfaz de las existentes en el sistema, que provee la forma de mapeo entre la dirección de red y dirección física.

La dirección física depende de la red, por ejemplo en caso de tratarse de una LAN, las direcciones físicas serán MAC (ethernet address), mientras que en el caso de X.25 se tratará de una dirección X.121.

Generalidades de SNMP MIB II

- Grupo **address-translation**:



Sub-grupo at address-translation (MIB-II)

Para implementar la tabla, se cuenta con el objeto que la representa atTable (1) con los elementos atEntry (1) que contiene los siguientes elementos:

- atIfIndex (1) identifica la interfaz referenciada
- atPhysAddress (2) dirección física dependiente del medio
- atNetAddress(3) dirección de red referida (depende de la red).

Este grupo se encuentra en desuso, y se presenta definido solamente para mantener compatibilidad con MIB-I. El motivo de esto es que puede ocurrir que una interfaz deba soportar más de un protocolo, lo que no se encuentra definido.

Generalidades de SNMP MIB II

- Grupo **ip**:
 - Contadores y manejo de estadísticas a nivel de capa 3 (tanto IP como ICMP).
 - Objetos tablas para visualizar la tabla de enrutamiento IP.
 - Tablas para tener información sobre protocolos de ruteo OSPF, RIP y BGP.
 - Hay objetos de configuración general
 - Hay tres tablas, ipAddrTable, ipRouteTable, ipNetToMediaTable

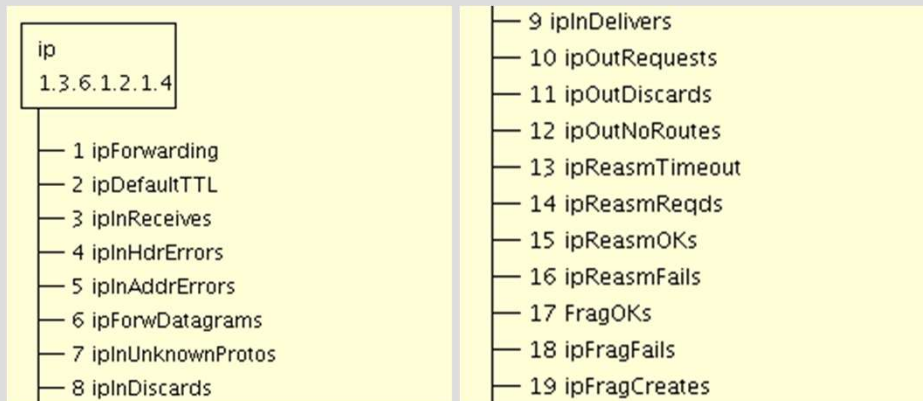
Sub-grupo ip (MIB-II)

Contiene elementos relevantes para la implementación y operación del protocolo IP en un nodo. El protocolo IP, funciona tanto en un nodo final (host) como en un nodo intermedio (router), y los datos que presenta la MIB, se pueden adaptar a ambas realidades.

Se puede obtener información acerca de los protocolos de ruteo utilizados en el nodo así como información general sobre el procesamiento realizado por el protocolo IP.

Generalidades de SNMP MIB II

- Grupo ip:



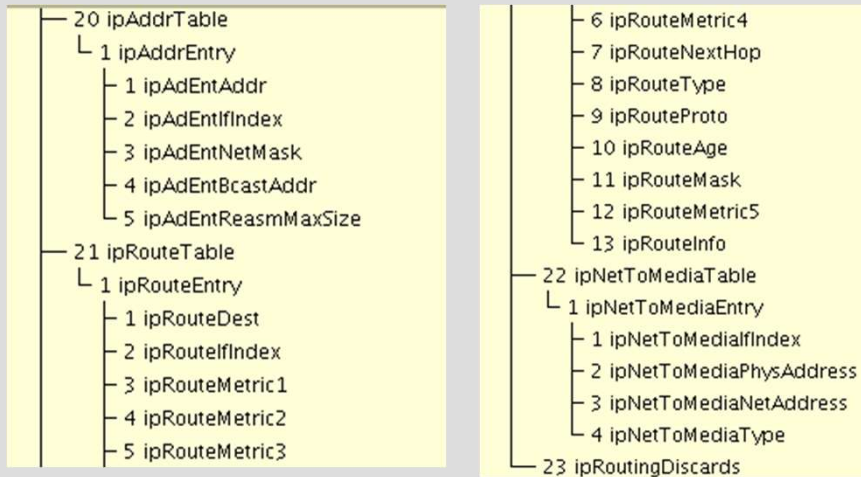
Sub-grupo ip (MIB-II)

Contiene los siguientes objetos escalares:

- ipForwarding. Indica si el equipo actúa como gateway. (forwarding(1), not-forwarding(2))
- ipDefaultTTL. Indica valor por defecto de Time-To-Live
- ipInReceives. Indica número total de datagramas recibidos, incluye los recibidos con error.
- ipInHdrErrors. Indica datagramas descartados por errores en el cabezal, esto incluye TTL excedido, checksums etc.
- ipInAddrErrors. Indica datagramas descartados por errores en dirección IP destino.
- ipForwDatagrams. Indica paquete forwardado (donde el equipo se utilizó como gateway)
- ipInUnknownProtos. Indica datagramas descartados por contener paquetes de protocolos no soportados.
- ipInDiscards. Indica datagramas descartados por otros motivos.
- ipInDelivers. Indica datagramas entregados correctamente.
- ipOutRequests. Indica datagramas enviados (incluye ICMP)
- ipOutDiscards. Indica datagramas no enviados
- ipOutNoRoutes. Indica datagramas descartados por no encontrar ruta.
- ipReasmTimeout, ipReasmReqds, ipReasmOKs, ipReasmFails. Indica información sobre datagramas reensamblados.
- ipFragOKs, ipFragFails, ipFragCreates. Indica información sobre datagramas fragmentados.

Generalidades de SNMP MIB II

- Grupo ip:



Sub-grupo ip (MIB-II)

Contiene tres tablas:

- ipAddrTable. Tabla que contiene la información de direcciones IP relativas al sistema.
- ipRouteTable. Tabla que contiene información sobre tablas de ruteo del sistema.
- ipNetToMediaTable. Tabla que contiene información para el mapeo de direcciones de red con direcciones físicas.

Generalidades de SNMP MIB II

- Grupo **tcp**:
 - Información relacionada con el funcionamiento del protocolo tcp en el agente.
 - Tres subgrupos de objetos:
 - Objetos conteniendo información de tipo general (configuración local)
 - Objetos contadores genéricos de segmentos
 - Objetos conteniendo información de conexiones individuales.

Sub-grupo tcp (MIB-II)

Contiene información acerca del protocolo de capa 4 TCP (orientado a conexión).

Este grupo es obligatorio para los sistemas que tienen implementado TCP.

La información brindada refiere a conexiones establecidas y en curso. Una vez finalizada la misma, se elimina la referencia.

Generalidades de SNMP

MIB II

- Grupo **tcp**:

- 1 tcpRtoAlgorithm
- 2 tcpRtoMin
- 3 tcpRtoMax
- 4 tcpMaxConn
- 5 tcpActiveOpens
- 6 tcpPassiveOpens
- 7 tcpAttemptFails
- 8 tcpEstabResets
- 9 tcpCurrEstab
- 10 tcpInSegs
- 11 tcpOutSegs
- 12 tcpRetransSegs
- 13 tcpConnTable
 - └ 1 tcpConnEntry
 - └ 1 tcpConnState
 - └ 2 tcpConnLocalAddress
 - └ 3 tcpConnLocalPort
 - └ 4 tcpConnRemAddress
 - └ 5 tcpConnRemPort
- 14 tcpInErrs
- 15 tcpOutRsts

Sub-grupo tcp (MIB-II)

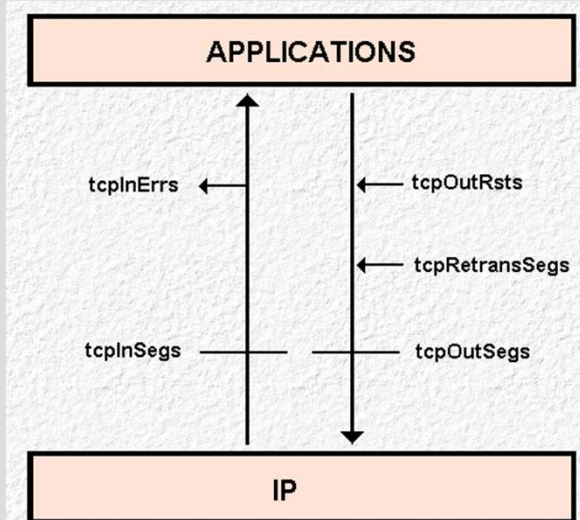
Contiene elementos escalares generales sobre la configuración del TCP en el equipo, y una tabla de conexiones (tcpConnTable).

Elementos constitutivos del subgrupo tcp:

- tcpRtoAlgorithm. Contiene información sobre el algoritmo utilizado para el cálculo del time-outs de TCP, para retransmisión. Valores posibles, other(1), constant(2), rsre(3), vanj(4).
- tcpRtoMin. Valor mínimo aceptado por TCP para tiempo de retransmisión.
- tcpRtoMax. Valor máximo aceptado por TCP para tiempo de retransmisión.
- tcpMaxConn. Máxima cantidad de conexiones simultaneas aceptadas.
- tcpActiveOpens. Cantidad de solicitudes de conexión que no obtienen resultado.
- tcpPassiveOpens. Cantidad de conexiones pasivas aceptadas.
- tcpAttemptFails. Cantidad de reconexiones solicitadas.
- tcpEstabResets. Cantidad de conexiones reseteadas.
- tcpCurrEstab. Cantidad de conexiones establecidas.
- tcpInSegs.. Cantidad de segmentos recibidos.
- tcpOutSegs. Cantidad de segmentos enviados.
- tcpRetransSegs. Cantidad de segmentos retransmitidos.

Generalidades de SNMP MIB II

- Grupo **tcp**:



Sub-grupo tcp (MIB-II)

El diagrama CASE presentado en la transparencia, contiene la lógica del cálculo de los segmentos recibidos y enviados por el protocolo.

Generalidades de SNMP MIB II

- Grupo **udp**:
 - UDP es un protocolo sumamente simple, no hay conexiones ni control de congestión.
 - Las variables miden:
 - Totales de datagramas en distintas condiciones
 - Una tabla de puertos de origen/puertos destino

Sub-grupo udp (MIB-II)

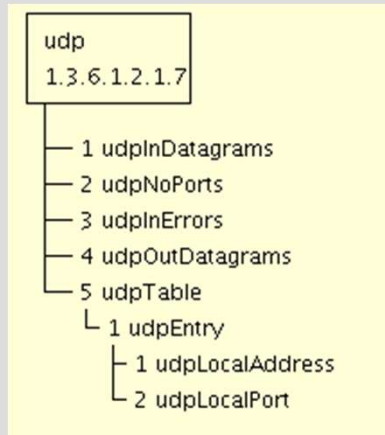
El protocolo UDP es parte del TCP/IP, y permite realizar envíos no orientados a conexión.

Para el presente subgrupo se mantiene la información general y una tabla de puertos origen y destino de segmentos.

Este subgrupo es obligatorio para sistemas que tienen implementado UDP.

Generalidades de SNMP MIB II

- Grupo **udp**



Sub-grupo **udp** (MIB-II)

Contiene elementos escalares generales sobre la configuración del UDP en el equipo, y una tabla puertos abiertos recibiendo datagramas (udpTable).

Elementos constitutivos del subgrupo udp:

- udpInDatagrams. Cantidad total de datagramas recibidos.
- udpNoPorts. Cantidad total de puertos UDP abiertos a la recepción de datagramas.
- udpInErrors. Cantidad total de datagramas no entregados a alguna aplicación.
- udpOutDatagrams. Cantidad total de datagramas enviados.

La tabla udpTable, contiene elementos udpEntry no accesibles del tipo SEQUENCE.

El contenido de udpEntry es el siguiente:

- udpLocalAddress. Dirección IP local del puerto UDP. En caso de ser cualquiera su valor es 0.0.0.0.
- udpLocalPort. Puerto local de atención.

Generalidades de SNMP MIB II

- Grupo **icmp**:
 - ICMP es el protocolo de control de Internet (*Internet Control Message Protocol*)
 - Es un protocolo muy sencillo, de mensajes sin confirmación.
 - El grupo ICMP solo lleva cuenta de distintos tipos de mensajes y de totales.

Sub-grupo icmp (MIB-II)

El *Internet Control Message Protocol* (ICMP) es el subprotocolo de diagnóstico y notificación de errores del IP. Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado

La diferencia de ICMP con los protocolos TCP o UDP se basa en que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping, que envía mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible y el tiempo que le toma a los paquetes en ir y regresar a ese host.

El subgrupo icmp, mantiene información de estado y utilización del mismo,

Su implementación se considera obligatoria en todos los sistemas.

Generalidades de SNMP MIB II

- Grupo **snmp**:
 - El grupo SNMP lleva la cuenta de los mensajes SNMP transmitidos, así como también de la cantidad de comandos recibidos, traps enviados, etc.

Sub-grupo snmp (MIB-II)

El grupo snmp, permite realizar un control de los mensajes SNMP recibidos y transmitidos por el sistema, contabilizando además errores ocurridos.

Este grupo es obligatorio para los sistemas que soportan SNMP.

Generalidades de SNMP

MIB II

- Otras MIB Standard:
 - Además de la MIB-II, el IETF ha definido algunas MIBs standard para determinadas familias de equipos:
 - Bridge MIB
 - Mail System MIB
 - Modem MIB
 - Otras...

Otras MIB Standard.

Existen MIB's definidas para diferentes sistemas o equipos que permiten el monitoreo de los equipos o sistemas referidos.

- Bridge MIB (RFC 1493). Contiene los elementos generales para la gestión y monitoreo de dispositivos tipo bridge de redes.
- Mail System MIB (RFC 2249) . Permite el monitoreo de MTA's. Define para esto 4 tablas, para el monitoreo de MTA's en particular y considerando las mismas como asociadas en un mismo sistema.
- Modem MIB (RFC 1696). Mantiene información general sobre los dispositivos Modem, y en particular de fabricantes.

En general es recomendable utilizar MIB's estandarizadas, ante la opción del diseño de alguna propia. Esto se plantea para permitir que los dispositivos gestionados y monitoreados puedan accederse a través de directivas ya estandarizadas.

SNMP

Temas

- Formatos
- Políticas de acceso
- Transmisión de mensajes
- Recepción de mensajes
- Operaciones

SNMP Formatos

Mensaje SNMP

Versión	Comunidad	PDU				
---------	-----------	-----	--	--	--	--

PDU GetRequest, GetNextRequest y SetRequest

Tipo de PDU	Id. de solicitud	0	0	Vínculos variables		
-------------	------------------	---	---	--------------------	--	--

PDU GetResponse

Tipo de PDU	Id. de solicitud	Status de error	Indicador de error	Vínculos variables		
-------------	------------------	-----------------	--------------------	--------------------	--	--

PDU Trap

Tipo de PDU	Tipo de objeto	Dirección del agente	Trap genérico	Trap específico	Hora	Vínculos variables
-------------	----------------	----------------------	---------------	-----------------	------	--------------------

Vínculos variables

Nombre 2	Valor 1	Nombre 2	Valor 2	Nombre n	Valor n
----------	---------	----------	---------	-------	----------	---------

Formatos en SNMP

SNMP prevé intercambio de mensajes entre gestor y agente como método de comunicación. En los mensajes se incluye la versión de SNMP en uso, una comunidad, y uno de los 5 posibles Protocol Data Units (PDU's) . Cada tipo de PDU es definido como un tipo de ASN.1 diferente, que sigue las reglas de Basic Encoding Rules.

La **comunidad** permite identificar un grupo de entidades de SNMP que corresponden a un agente determinado., y actúa como un password para autenticar mensajes de SNMP.

Cada solicitud de SNMP puede tener un número que la identifique (opcional).

Cuando se produce un error, el mismo es identificado tanto por su status (0-noError, 1-tooBig, 2-noSuchName, 4-readOnly, 5-genErr) como por su indicador, que identifica la variable que causó la excepción.

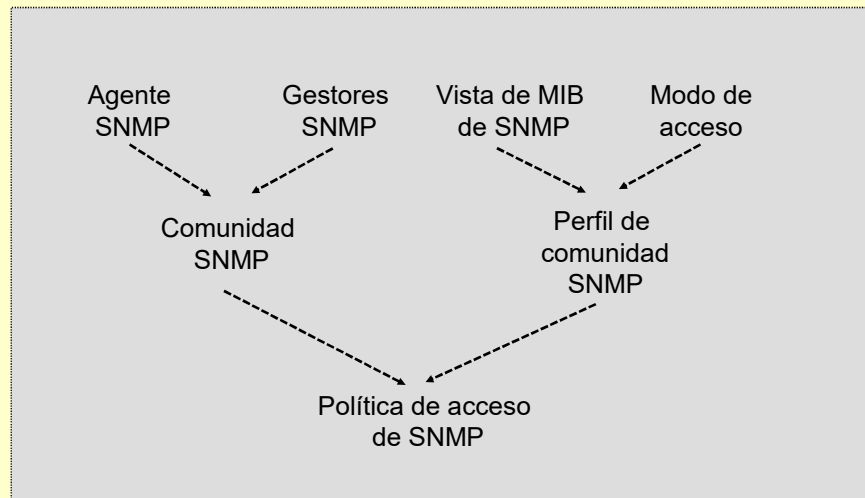
En SNMP es posible interrogar una "hoja" del árbol, que son valores escalares. Pero se prevé que en un mismo mensaje pueda agruparse un número de operaciones del mismo tipo (ya sea "get", o "set" o bien "trap"), lo cual reduce la carga de comunicaciones. El campo de vínculos variables (*variable bindings*) permite comunicar las instancias de los objetos, y sus respectivos valores.

Los traps genéricos comprenden: 0-coldStart, 1-warmStart, 3-linkDown, 4-authentication-Failure, 5-egpNeighborLoss, 6-enterprise-Specific. En caso que se trate de un trap específico de una empresa, debe describirse en el campo "Tipo específico".

La "hora" corresponde al tiempo transcurrido desde el último reinicio del dispositivo.

SNMP

Políticas de acceso



Seguridad y Política de Acceso en SNMP

Una estación gestionada puede mantener vínculos con varias estaciones gestoras. A su vez, una estación gestora puede comunicarse con varias estaciones gestionadas. Éstas últimas pueden dar acceso limitado a ciertas variables a ciertas estaciones, y adicionalmente, puede actuar como proxy para algunos elementos. Todo lo anterior implica aspectos de seguridad que en SNMP se prevé sean atendidos con el concepto de *comunidad*: relación entre gestores y agentes que definen *autenticación*, *control de acceso* y funciones de *proxy*. Es un concepto local, y a cada comunidad corresponde un nombre, que debe emplearse en cada operación *get* y *set*.

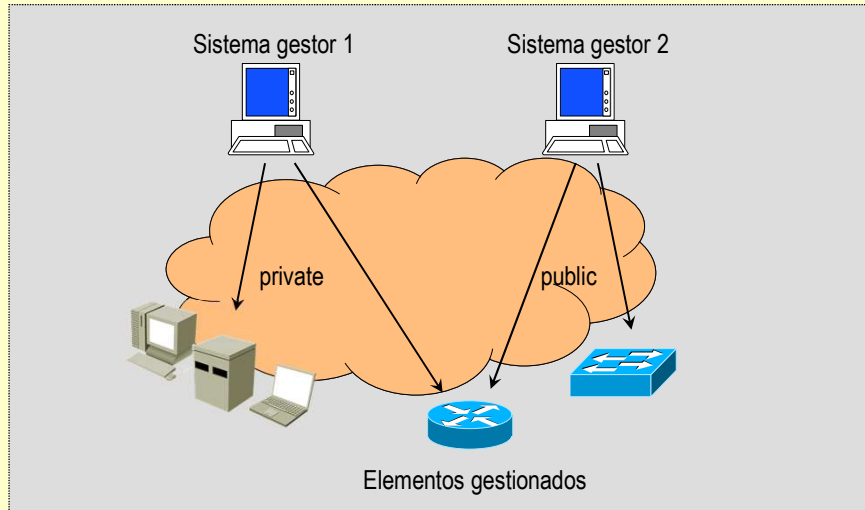
Para la autenticación de las estaciones clientes ante los servidores se emplean las comunidades que actúan como passwords que viajan por la red. En la versión 1 (SNMP) la password viaja en modo texto. En la versión 2 (SNMPv2) viaja encriptada.

Los servidores SNMP (agentes) pueden definir distintos modos de acceso para los administradores mediante tres elementos:

- el conjunto de administradores (comunidad SNMP, SNMP community) para los cuales se define la autenticación y el control de acceso para ese servidor
- el modo, que puede ser read-only o read-write
- el subconjunto de elementos de MIB (SNMP MIB **view**) sobre los cuales se aplicará el modo

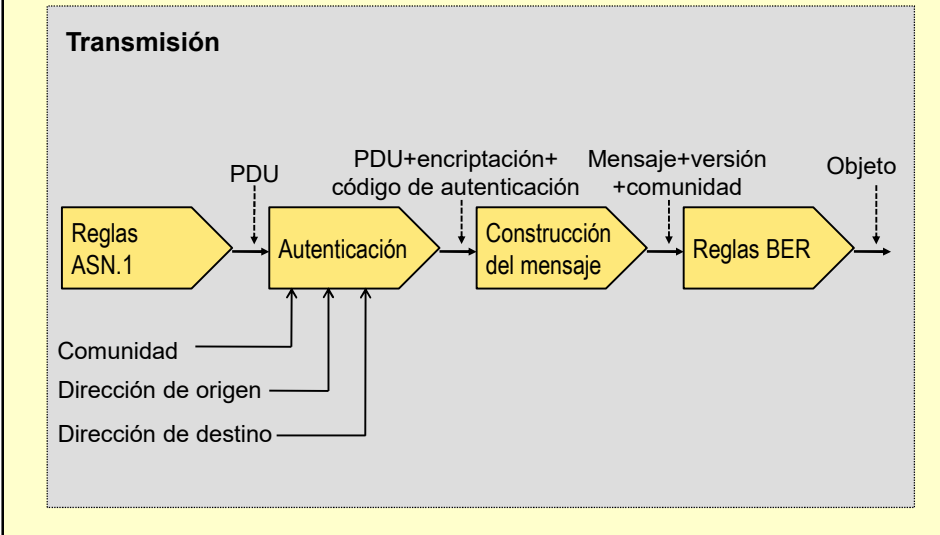
El modo y la SNMP MIB view definen el **perfil** de la comunidad SNMP (SNMP community profile).

La combinación de comunidad y perfil definen la **Política de Acceso SNMP**.

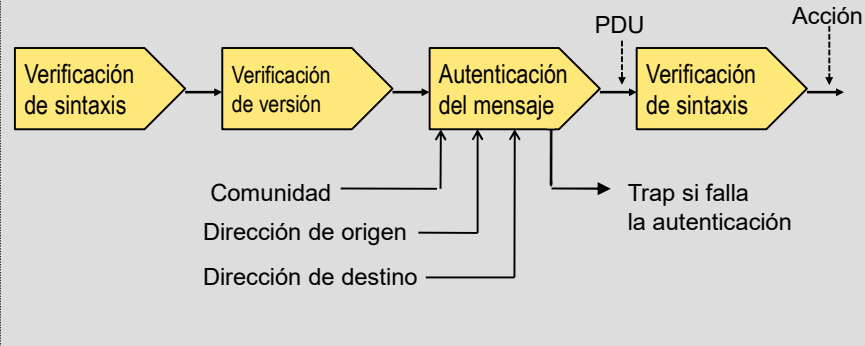
SNMP**Políticas de acceso****Comunidades**

Las comunidades son cadenas de caracteres que se utilizan como mecanismo de control de acceso a la información. Generalmente se emplean dos comunidades, y sus correspondientes conjuntos de variables (no necesariamente disjuntos), identificados por un nombre de comunidad configurable por el administrador del sistema. Una de dichas comunidades usualmente se llama comunidad pública, y sus variables pueden ser accedidas sólo para lectura. En cambio, los valores asociados a las variables correspondientes a la otra comunidad, denominada comunidad privada, pueden ser modificados.

Toda la seguridad se basa en que es necesario conocer el nombre asignado a una comunidad para conseguir el acceso a la información proporcionada por sus variables. El nivel de protección ofrecido por la versión original del protocolo es, por tanto, muy pobre.

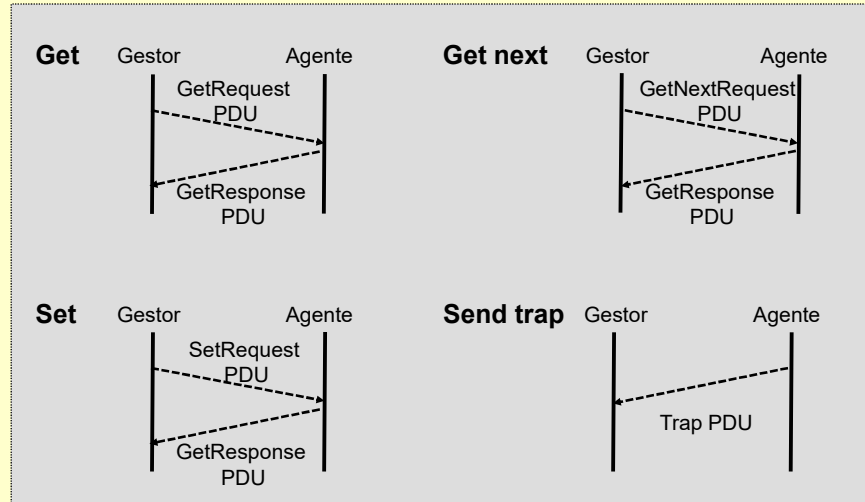
SNMP**Transmisión de mensajes****Transmisión de mensajes SNMP**

- 1- Se construye la PDU mediante ASN.1 (RFC 1157).
- 2- Se emplea el servicio de autenticación que verifica direcciones de origen y destino y comunidad, y efectúa el procesamiento que corresponda (encriptación, etc.).
- 3- Se construye el mensaje con el agregado de versión de SNMP y comunidad.
- 4- Se emplean las Basic Encoding Rules para codificar el objeto.

SNMP**Recepción de mensajes****Recepción****Recepción de mensajes SNMP**

- 1- Se verifica la sintaxis y se descarta el mensaje si se detectan anomalías en el análisis.
- 2- Se verifica la versión de SNMP y se descarta si no hay coincidencia.
- 3- Se analizan PDU, comunidad, y direcciones de origen y destino. Si la autenticación tiene éxito se pasa la PDU como un objeto de formato ASN.1. De lo contrario, se descarta el mensaje y se genera un trap.
- 4- Se verifica la sintaxis de la PDU. Si falla se descarta el mensaje. Si hay éxito, se emplea la comunidad para aplicar la correspondiente política de acceso y se procesa la PDU de acuerdo con ella.

SNMP Operaciones



Operaciones

GetRequest – Permite interrogar agentes y puede identificarse cada mensaje con un número que debe ser incluido en la correspondiente respuesta. No es un requisito la identificación de mensajes, ni es necesario que se respete un criterio monótonamente creciente de generación.

Si se emplean vínculos variables, es posible interrogar por varias instancias de un objeto, pero si una de ellas no está disponible, la respuesta es un mensaje de error y no se responde por ninguna de las solicitadas (comportamiento atómico).

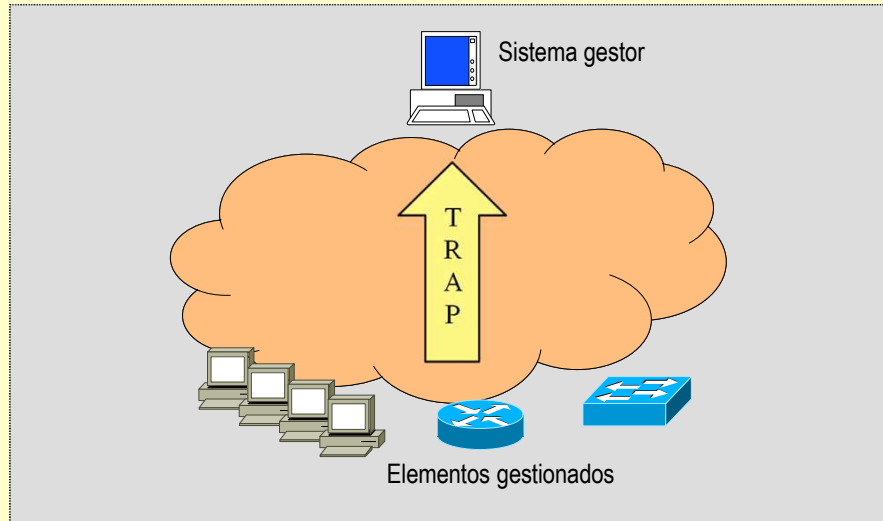
GetNextRequest – Es casi igual al anterior, pero solicita el valor de la siguiente instancia de un objeto (y no del siguiente objeto). Sigue las mismas reglas del caso anterior en cuanto a la entrega para vínculos variables, se entregan todos los valores o no se entrega ninguno (comportamiento atómico).

Este comando permite descubrir la estructura de una vista de una MIB, o recorrer una tabla cuyo contenido no se conoce.

SetRequest – Permite escribir valores en variables. Se comporta análogamente a los comandos anteriores: si una instancia no es posible que se actualice, no se actualiza ninguna (comportamiento atómico).

GetResponse – Respuesta a los comandos anteriores.

Trap – Permite notificaciones asincrónicas sobre eventos. Tiene un formato de PDU bastante diferente, que incluye la dirección IP de origen, el tipo de trap y la hora.

SNMP**Operaciones****Tipos de trap**

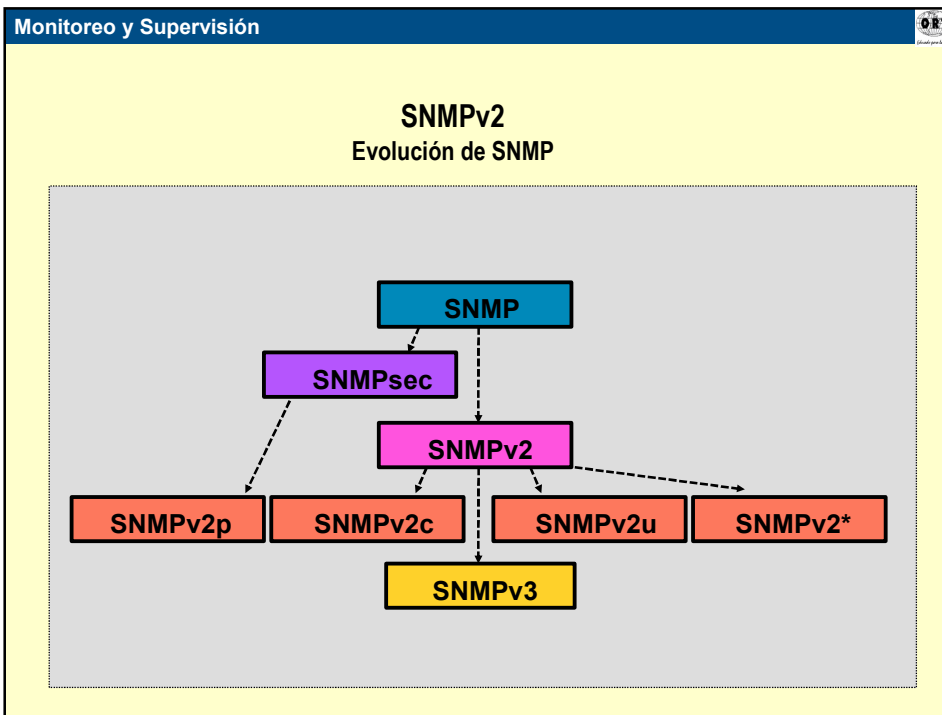
Cuando se genera un trap, el mismo se envía acompañado de la dirección de red del origen, el tipo de trap, un código de trap, la hora de generación, e información adicional. Los tipos posibles son:

- ColdStart - el dispositivo se reinició a sí mismo y su configuración puede cambiar en consecuencia
- WarmStart - el dispositivo se reinició a sí mismo pero su configuración no cambiará en consecuencia
- LinkDown - el dispositivo encuentra una interfaz caída
- LinkUp - una interfaz arrancó, ya sea porque recién se definió o porque estaba caída y levantó
- AuthenticationFailure - alguien intentó un login al dispositivo sin la autoridad requerida para hacerlo
- EGPNeighborLoss - un router que emplea EGP perdió un vecino (neighbor)
- EnterpriseSpecific - se produjo un evento específicamente definido por el fabricante (adición a la MIB)

SNMP v2

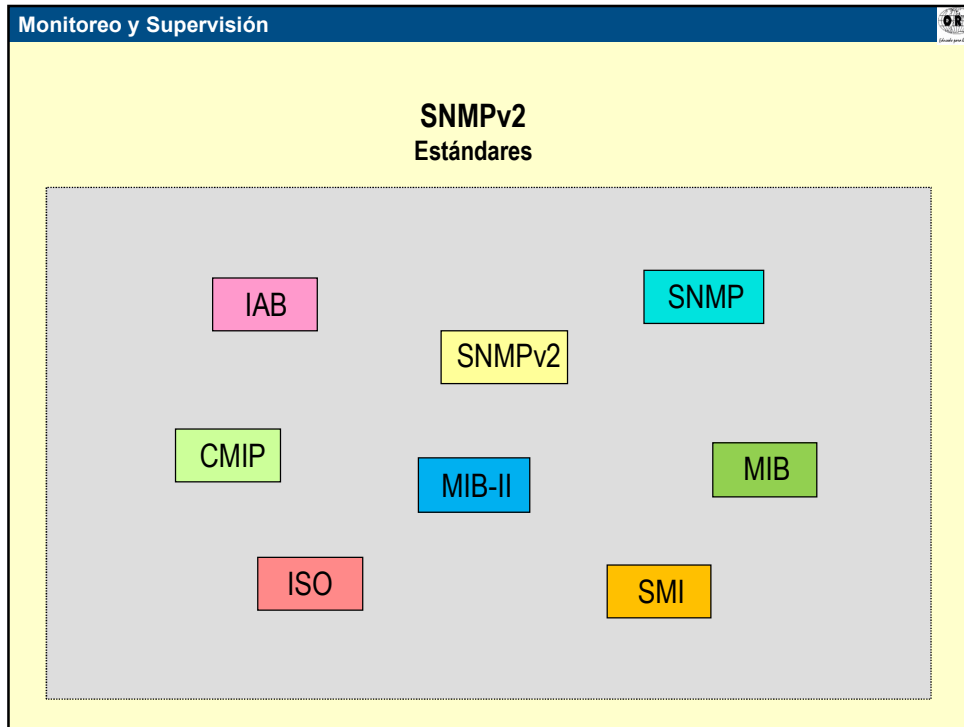
Temas

- Evolución de SNMP
- Estándares
- Formatos
- Operaciones
- Compatibilidad con SNMP



Evolución de SNMP

- SNMP tiene limitaciones: no es adecuado para grandes redes por la baja performance del sondeo, no es adecuado para recuperar grandes volúmenes de datos, no prevé reconocimiento para los traps, el modelo de MIB es limitado y no soporta la comunicación entre gestores (un gestor no puede aprender lo que otro conoce).
- SNMPsec fue un intento para incorporar mecanismos criptográficos de modo de asegurar privacidad, integridad de datos y autenticidad. Se basó en la noción de “party”: entidad que reúne un identificador, una localización en la red utilizando un protocolo de transporte determinado, una vista MIB sobre la que opera, un protocolo de autenticación y un protocolo de privacidad. SNMPsec se adopta inicialmente en SNMPv2 bajo el nombre de SNMPv2p, pero luego SNMPv2 se desprende de estándares de seguridad.
- SNMPv2 provee la infraestructura sobre la cual pueden construirse aplicaciones de gestión de red. Aquellas aplicaciones como manejo de alarmas, monitoreo de desempeño, accounting, y otros, esta fuera del alcance del estándar. SNMPv2 agrega dos nuevas PDU. SNMPv2 es un protocolo de gestión que permite el intercambio de información de gestión. Cada componente en la red mantiene una base de datos local (MIB) con información relevante para la gestión del comportamiento de la red. El estándar SNMPv2 define la estructura de esta información y los tipos de datos aceptables: SMI (Structure of Management Information, Estructura de Información de Gestión) para SNMPv2. El estándar también provee un numero de MIBs que son los mas comúnmente utilizados para gestión de redes.
- SNMPv2c (*Community-based SNMPv2*) utiliza el mismo modelo administrativo que la primera versión del protocolo SNMP, y por lo tanto no incluye mecanismos de seguridad. Introduce una mayor flexibilidad en los mecanismos de control de acceso: se permite la definición de políticas de acceso consistentes en asociar un nombre de comunidad con un perfil de comunidad formado por una vista MIB y los correspondientes derechos de acceso (*read-only* o *read-write*).
- SNMPv2* proporciona niveles de seguridad adecuados, pero no llegó a estandarizarse por IETF (*Internet Engineering Task Force*) adecuadamente.
- SNMPv2u (*User-based SNMPv2*) emplea los conceptos de la versión SNMPsec pero reemplaza la noción de party por la de usuario: para las comunicaciones es necesario identificar al usuario, el cual puede estar definido en varias entidades SNMP diferentes.



Estándares

Internet **A**rchitecture **B**oard define los estándares de SNMP.

A continuación se indican los estándares más importantes.

Introducción a SNMPv2 se especifica en RFC 1441

SMI para SNMPv2 se especifica en RFC 1442 => 1902 => 2578

Operaciones del Protocolo, PDUs se especifican en RFC 1448 => 1905 => 3416

Utilización de los mecanismos de Transporte se especifica en RFC 1449 => 1906 => 3417

MIB SNMPv2 se especifica en RFC 1450 => 1907 => 3418

M2M MIB SNMPv2 se especifica en RFC 1451

Otras definiciones se especifican en RFC 1444, 1445, 1446, 1447, 1452

Resumen de estándares de versiones de SNMP

SNMP RFC 1155-1157, 1212-1213

SNMPsec RFC 1351-1353

SNMPv2p RFC 1441-1452

SNMPv2c RFC 1901

SNMPv2u RFC 1910

SNMPv3 RFC 2271-2275

SNMPv2

Formatos y operaciones

Mensaje SNMP

Versión	Comunidad	PDU			
---------	-----------	-----	--	--	--

PDU GetRequest, GetNextRequest, SetRequest, InformRequest y SNMPv2-Trap

Tipo de PDU	Id. de solicitud	0	0	Vínculos variables
-------------	------------------	---	---	--------------------

PDU Response

Tipo de PDU	Id. de solicitud	Status de error	Indicador de error	Vínculos variables
-------------	------------------	-----------------	--------------------	--------------------

PDU GetBulkRequest

Tipo de PDU	Id. de solicitud	Non repeaters	Máx. repetitions	Vínculos variables
-------------	------------------	---------------	------------------	--------------------

Vínculos variables

Nombre 2	Valor 1	Nombre 2	Valor 2	Nombre n	Valor n
----------	---------	----------	---------	-------	----------	---------

Formatos y operaciones en SNMP v2

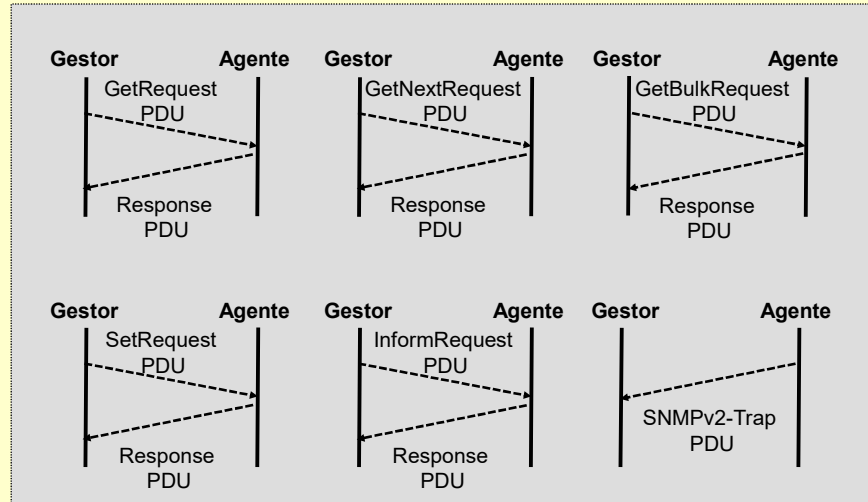
GetRequest, *GetNextRequest* y *SetRequest* - en SNMPv2 los comandos *GetRequest*, *GetNextRequest* y *SetRequest* son similares en formato y significado a los correspondientes de SNMP, con la excepción que no se aplica el comportamiento atómico, es decir, si se emplean vínculos variables, se devuelven todos los valores que pudieron obtenerse, aún cuando algunos de ellos no pudieran procesarse y responderse.

GetBulkRequest - es un comando nuevo diseñado para recuperar grandes cantidades de información. Sigue el mismo principio de *GetNextRequest*, en cuanto se selecciona la siguiente instancia del objeto en orden lexicográfico. Pero a diferencia de dicho comando, con *GetBulkRequest* es posible especificar múltiples sucesores lexicográficos. En efecto, en el comando se especifican dos valores: *non-repeaters*, que indica la cantidad de variables de la lista de vínculos variables para las cuales se devolverá sólo el valor de la siguiente instancia del objeto; *máx-repetitions*, que indica la cantidad de sucesores lexicográficos que deben devolverse por cada variable de las restantes de la lista.

SNMPv2-Trap - cumple el mismo roll del trap de SNMP, pero emplea el formato de *GetBulkRequest*, de modo de incrementar la eficiencia de la obtención de información.

SNMPv2

Operaciones



Formatos y operaciones en SNMP v2

InformRequest - es un nuevo comando que permite el intercambio de información entre entidades que actúan en rol de gestoras. Como consecuencia, se genera una respuesta con la misma identificación y mismos valores de variables, y con reporte de errores de la recepción.

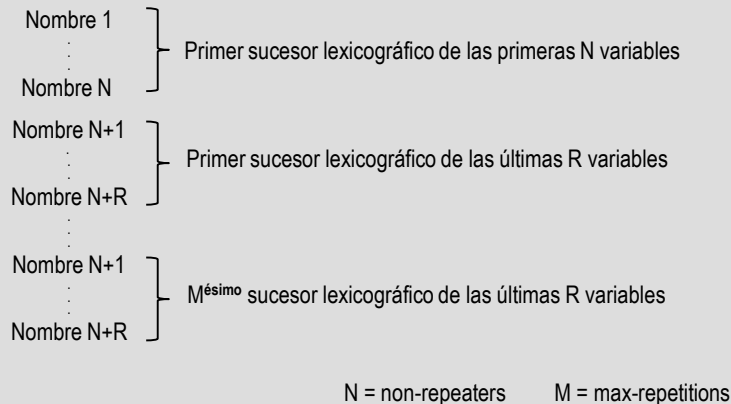
Response - es la respuesta que corresponde a todos los comandos anteriores con la excepción de SNMPv2-Trap.

Report - es un comando previsto pero no definido en formato y semántica.

SNMPv2

Operaciones

GetBulkRequest



Ejemplo de GetBulkRequest (extraído de Stallings)

Con GetBulkRequest se pueden conseguir los valores de sólo la siguiente variable o de las siguientes M variables con una sola solicitud.

Asumiendo la siguiente tabla ARP en un host que ejecuta un agente NMPv2:

Interface-Number	Type	Network-Address	Physical-Address
1	10.0.0.51	00:00:10:01:23:45	static
1	9.2.3.4	00:00:10:54:32:10	dynamic
2	10.0.0.15	00:00:10:98:76:54	dynamic

Un manager SNMPv2 envía la siguiente respuesta para conseguir sysUpTime y la tabla ARP completa:

GetBulkRequest [non-repeaters = 1, max-repetitions = 2] (sysUpTime, ipNetToMediaPhysAddress, ipNetToMediaType)

La entidad SNMPv2 que actúa como agente responde con la PDU Response:

Response ((sysUpTime.0 = "123456"), (ipNetToMediaPhysAddress.1.9.2.3.4 = "000010543210"), (ipNetToMediaType.1.9.2.3.4 = "dynamic"), (ipNetToMediaPhysAddress.1.10.0.0.51 = "000010012345"), (ipNetToMediaType.1.10.0.0.51 = "static"))

La entidad SNMPv2 que hace de manager continúa con:

GetBulkRequest [non-repeaters = 1, max-repetitions = 2] (sysUpTime, ipNetToMediaPhysAddress.1.10.0.0.51, ipNetToMediaType.1.10.0.0.51)

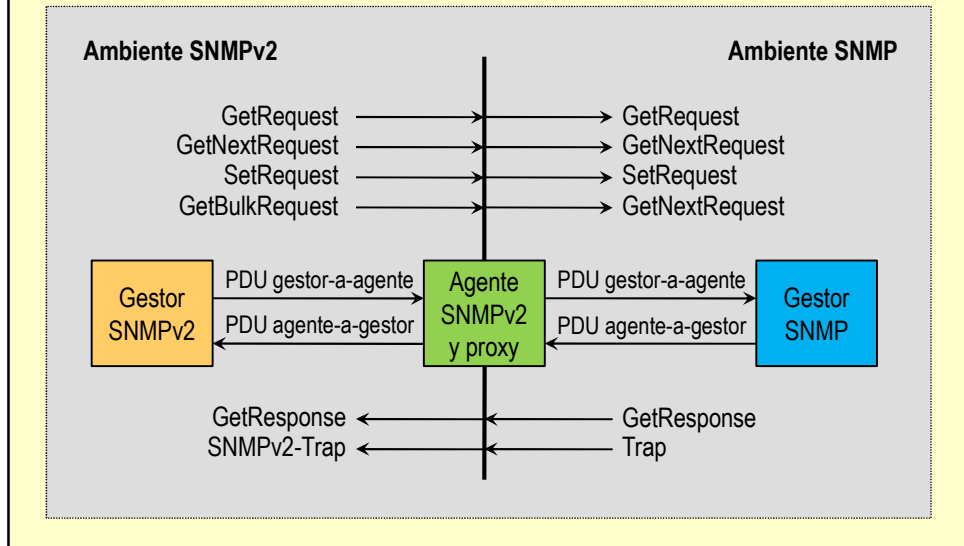
El agente responde con:

Response ((sysUpTime.0 = "123466"), (ipNetToMediaPhysAddress.2.10.0.0.15 = "000010987654"), (ipNetToMediaType.2.10.0.0.15 = "dynamic"), (ipNetToMediaNetAddress.1.9.2.3.4 = "9.2.3.4"), (ipRoutingDiscards.0 = "2"))

Esta respuesta señala el final de la tabla al manager. Con GetNextRequest se hubieran necesitado cuatro solicitudes para conseguir la misma información. Si se hubiera fijado el valor *max-repetition* de GetBulkRequest a tres, en este ejemplo sólo se hubiera necesitado una solicitud.

SNMPv2

Compatibilidad con SNMP



Proxy SNMP-SNMPv2

La forma más sencilla de asegurar la compatibilidad con SNMP es mantener los agentes SNMP existentes, y agregar la función de proxy para traducir a SNMPv2.

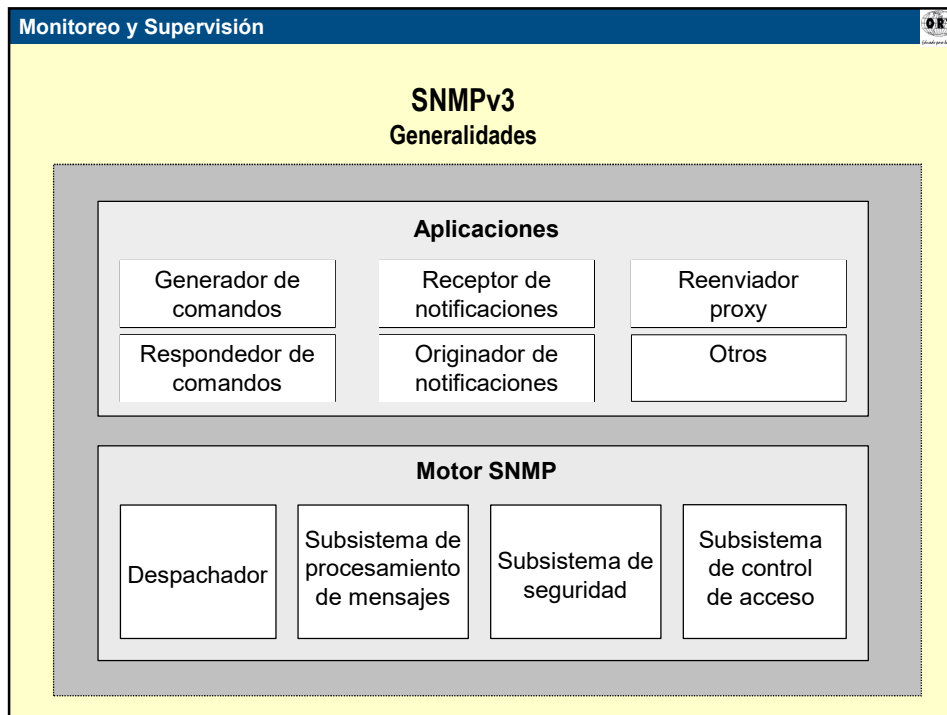
Gestor de doble stack

Una alternativa es emplear gestores que utilicen tanto SNMP como SNMPv2.

SNMPv3

Temas

- Generalidades de SNMPv3
- Generalidades de seguridad
- Objetivos de SNMPv3
- Entidades
- Referencias
- Mensajes
- Estandares
- Seguridad en SNMPv3



Seguridad y Marco de Funcionamiento

A partir de SNMPv2u y SNMPv2* surge SNMPv3 en 1998.

Mantiene las PDU de SNMPv2, pero define una serie de funciones de seguridad y un marco de trabajo para su uso.

Dichas funciones incluyen protecciones a fin de garantizar la **autenticidad**, la **privacidad** y la **integridad** de los mensajes.

El marco de funcionamiento es una arquitectura modular para cada entidad (gestor y agentes), que permite actualizar cada módulo sin afectar al resto.

Arquitectura de gestión de red: colección de entidades SNMP que interaccionan entre sí. Cada entidad implementa una parte de las capacidades de SNMP y puede actuar como agente, gestor o una combinación de ambos. Cada entidad consiste en una colección de módulos que interaccionan entre sí para proporcionar servicios. Una entidad incluye un motor SNMP que implementa funciones para enviar y recibir mensajes, autenticar y encriptar mensajes, y controlar el acceso a los objetos gestionados.

SNMPv3 Objetivos

- **Objetivos de SNMPv3**
 - Resolver finalmente el problema de la seguridad.
 - Asegurar la extensibilidad del protocolo y de los agentes.
 - Reciclar lo que ya tenemos implementado para v1 y v2.
 - Permitir las implementaciones mas simples y las mas complejas, bajo el mismo protocolo marco (*framework*).

SNMP Entity (2571):

El marco de SNMP define el universo de gestión como una colección de “*entidades SNMP*”

Estas se comunican entre sí por medio de mensajes SNMP

Pueden actuar en roles de agente, gestor o una combinación de ambos.

Cada entidad tiene una estructura interna modular.

Los módulos se comunican entre si mediante una serie de “servicios” que se prestan entre si.

Cada SNMP Entity tiene un “**SNMP Engine**”

El motor (engine) se ocupa de las funciones de:

Envío y recepción de mensajes

Encriptación y desencriptación

Autenticación de mensajes

Control de acceso

Módulos del motor SNMP

Dispatcher (RFC 2572):

Recibe PDU's de la red para entregar a las aplicaciones y viceversa.

Message Processing Subsystem (RFC 2572):

Prepara mensajes para enviar y decodifica mensajes entrantes.

Security Subsystem (RFC 2574):

Provee servicios de seguridad, encriptación y autenticación (MAC).

Puede soportar diferentes “*Security Models*”

Access Control Subsystem (RFC 2575):

Provee servicios de autorización a las aplicaciones que estas pueden chequear para controlar derechos, etc.

SNMPv3

Entidades

- **SNMP Entity, Aplicaciones (RFC 2573):**
 - *Command Generator:*
 - Inicia los Get/GetNext y demás primitivas y se encarga de recibir las respuestas a las mismas.
 - *Command Responder:*
 - Se encarga de recibir y procesar (generar respuestas) a los Get/GetNext/Set que son dirigidos al sistema local desde otros.
 - *Notification Originator:*
 - Genera los traps a partir de eventos en el sistema local, debe definir a quien enviárselo y que parámetros usar.
 - *Notification Receiver:*
 - Escucha Traps dirigidas al sistema local y genera respuestas eventualmente llegue un “inform”.
 - *Proxy Forwarder:*
 - Implementa un proxy de SNMP, es un módulo opcional.
 - *Other:*

Aplicaciones:

Las aplicaciones implementadas en cada entity son opcionales.

Un “**agente**” en el sentido tradicional necesita solo:

Command Responder

Notification Originator

Opcionalmente, puede tener también proxy forwarder

Un “**gestor**” tradicional necesita:

Command Generator

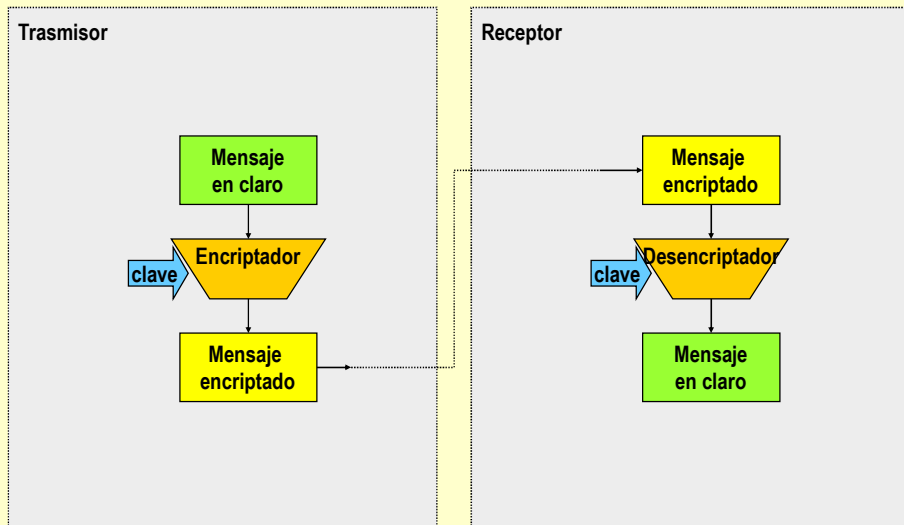
Notification Originator

Notification Receiver

SNMPv3

Generalidades de seguridad

- Encriptación:



Encriptación:

¿Cómo ocultar un mensaje para que otros no puedan leerlo?

Tipos de encriptación:

Simétrica

La misma clave se usa tanto para encriptar como para desencriptar.

Asimétrica o Clave Pública

La clave de desencriptar es diferente de la de encriptar

Elementos:

Texto plano (*plaintext*)

Es el mensaje que quiero enviar en forma comprensible por el receptor y el remitente.

Texto cifrado (*ciphertext*)

Es el mensaje a enviar en forma no comprensible, oculta.

Clave

Bloque de información (string, número) que parametriza el algoritmo de encriptación.

Algoritmo de encriptación

Algoritmo que transforma el texto plano en texto cifrado.

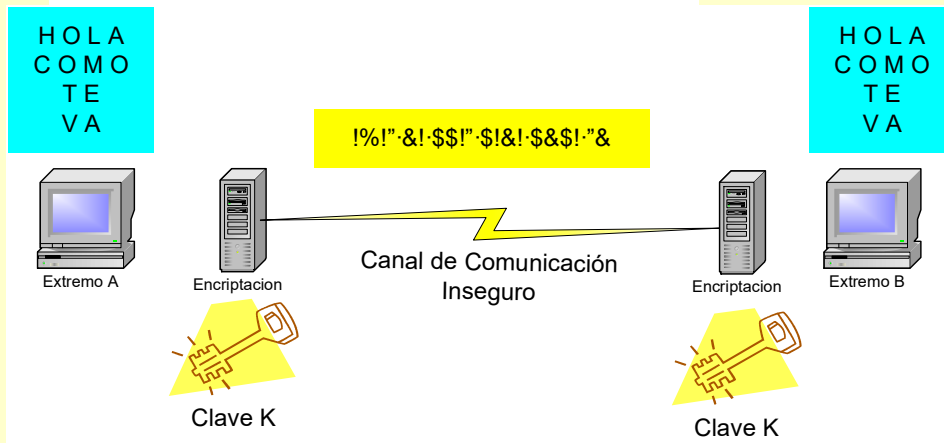
Canal de comunicación

Medio a través del cual se envía el mensaje, considerado siempre inseguro desde el punto de vista de la privacidad

SNMPv3

Generalidades de seguridad

- Encriptación:
 - ¿Cómo se combinan estas partes?



DES: Data Encryption Standard

Definido como standard del gobierno de USA en 1977

Es un "block cypher", procesa el texto plano en bloques de 64 bits.

Usa claves de 56 bits

Texto plano debe dividirse en bloques de 64 bits:

ECB y CBC

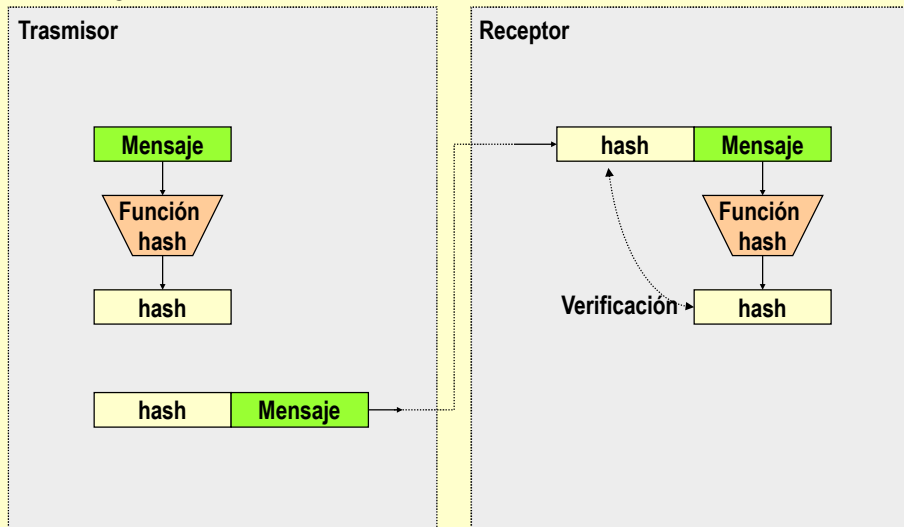
DES fue atacado con éxito por fuerza bruta a principios de los 90.

Se recomienda el uso de 3DES, pero para muchas aplicaciones DES sigue siendo suficiente.

SNMPv3

Generalidades de seguridad

- Integridad:



Funciones de Hash:

Una función de hash transforma un mensaje de largo variable, en un bloque de bits de tamaño fijo.

No son funciones 1 a 1 obviamente

Las usamos para generar firmas digitales de mensajes y autenticar las mismas.

MD5:

Definida en RFC 1321 en 1992

Genera hashes de 128 bits

Procesa la información en bloques de 512 bits

Era el hash por defecto en casi todas las aplicaciones hasta que recientemente se han encontrado algunas formas de generar "colisiones" en los mismos.

SHA-1

Estándar del gobierno de USA en 1995

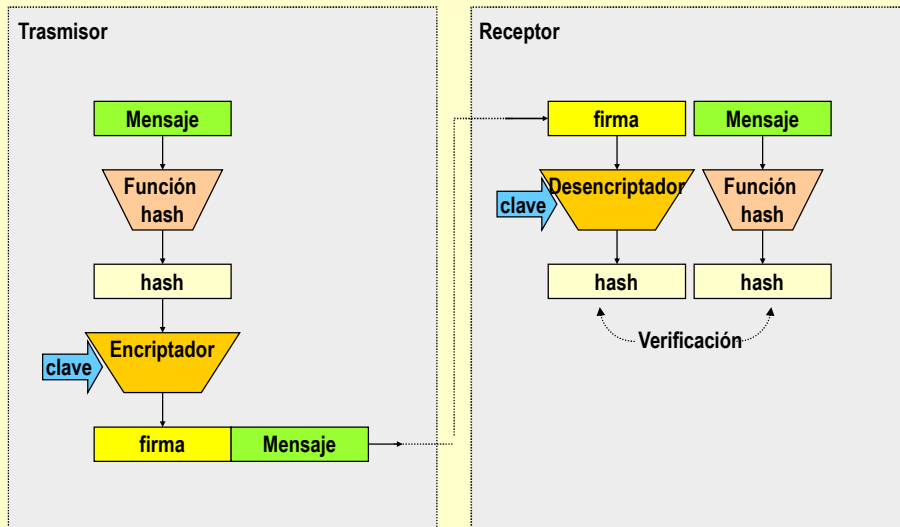
Genera hashes de 160 bits

Mas seguro que MD5, genera un digest mas largo.

SNMPv3

Generalidades de seguridad

- Autenticación:



Autenticación de mensajes (MAC)

Cuando nos comunicamos por un canal inseguro, necesitamos:

Saber que los mensajes no han sido alterados.

Saber que los mensajes provienen de quien dice enviarlos

MAC: Message Authentication Code

Familia de algoritmos que nos permiten lograr los dos objetivos anteriores.

Agrega a cada mensaje una pequeña información adicional, calculada como función del mensaje y de una clave K

El receptor comparte la clave K, a la llegada el receptor recalcula el MAC y lo compara.

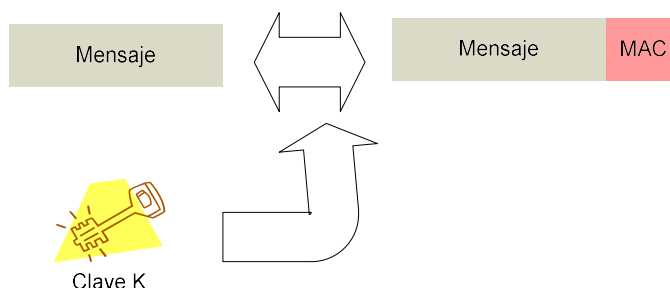
Formas de generar MAC:

Usando DES u otro algoritmo simétrico.

Usando algoritmos de hash.

Incorporando una "clave": HMAC

Se puede elegir el algoritmo de hash a utilizar, pudiendo ser MD5 o SHA-1 u otros.



SNMPv3

Objetivos

- Objetivos de SNMPv3
 - Atacar finalmente el problema de la seguridad.
 - Asegurar la extensibilidad del protocolo y de los agentes.
 - Reciclar lo que ya tenemos implementado para v1 y v2.
 - Permitir las implementaciones más simples y las más complejas, bajo el mismo protocolo marco (*framework*).

SNMP Entity:

El marco de SNMP define los elementos a gestionar como una colección de “*entidades SNMP*”

Estas se comunican entre sí por medio de mensajes SNMP

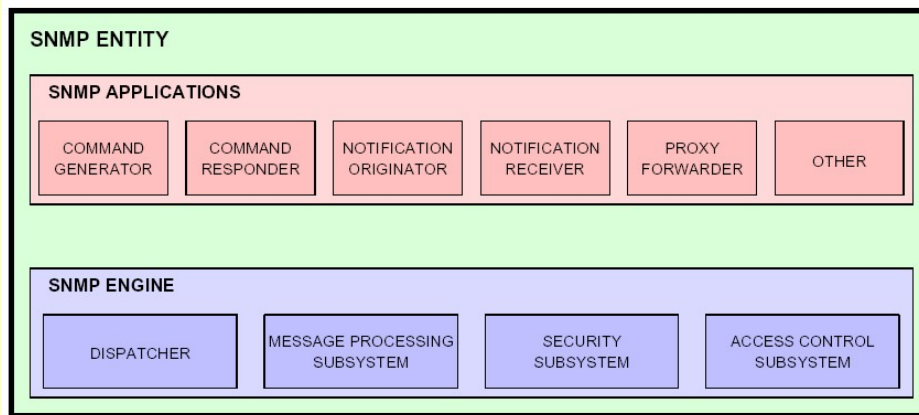
Pueden actuar en roles de agente, gestor o una combinación de ambos.

Cada entidad tiene una estructura interna modular.

Los módulos se comunican entre sí mediante una serie de “servicios” que se prestan entre sí.

SNMPv3 Entidades

- SNMP Entity



SNMP Entity:

Cada SNMP Entity tiene una “**SNMP Engine**”

La engine se ocupa de las funciones de:

- Envío y recepción de mensajes
- Encriptación y desencriptación
- Autenticación de mensajes
- Control de acceso

Módulos del SNMP Engine

Dispatcher:

Recibe PDU's de la red para entregar a las aplicaciones y viceversa.

Message Processing Subsystem:

Prepara mensajes para enviar y decodifica mensajes entrantes.

Security Subsystem:

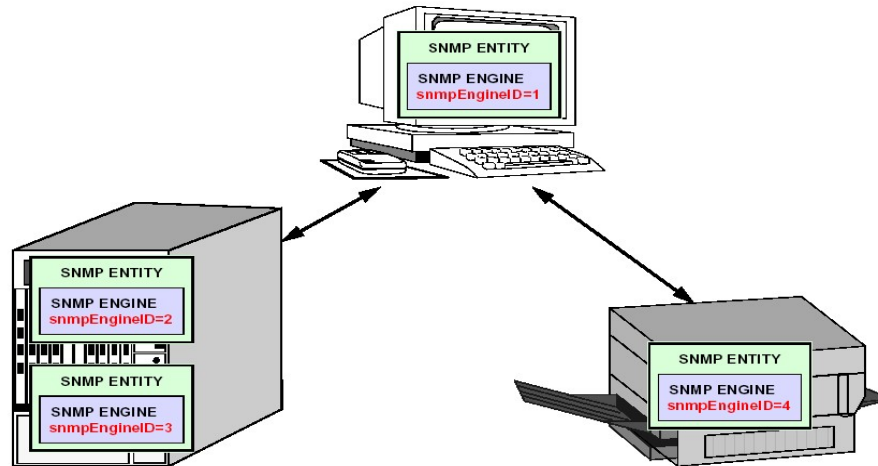
Provee servicios de seguridad, encriptación y autenticación (MAC).
Puede soportar diferentes “*Security Models*”

Access Control Subsystem:

Provee servicios de autorización a las aplicaciones que estas pueden chequear para controlar derechos, etc.

SNMPv3 Entidades

- SNMP `snmpEngineID`:



SNMP `snmpEngineID`:

First bit cleared, vendor supplied

- First four octets is the enterprise private number
- Next eight octets enterprise specific scheme

First bit set, "standard" format

- First four octets is the enterprise private number
- Fifth indicates how the subsequent octets are used
 - 1: IPv4 address
 - 2: IPv6 address
 - 3: MAC address
 - 4: admin text
 - 5: admin hex values
 - 6-127: reserved
 - 128-255: enterprise specific

1st
bit

SNMPv1 SNMPv2	0	Enterprise ID (1-4 octets)	Enterprise method (5th octet)	Function of the method (6-12 octets)
SNMPv3	1	Enterprise ID (1-4 octets)	Format indicator (5th octet)	Format (variable number of octets)

- Cada SNMP engine tiene un unico ID: *snmpEngineID*
- Acme Networks {enterprises 696}
- SNMPv1 `snmpEngineID` '000002b8'H
- SNMPv3 `snmpEngineID` '800002b8'H
(the 1st octet is 1000 0000)

SNMPv3

Entidades

- SNMP Entity, Aplicaciones:
 - *Command Generator*:
 - Inicia los Get/GetNext y demás primitivas y se encarga de recibir las respuestas a las mismas.
 - *Command Responder*:
 - Se encarga de recibir y procesar (generar respuestas) a los Get/GetNext/Set que son dirigidos al sistema local desde otros.
 - *Notification Originator*:
 - Genera los traps a partir de eventos en el sistema local, debe definir a quien enviárselo y que parámetros usar.
 - *Notification Receiver*:
 - Escucha Traps dirigidas al sistema local y genera respuestas eventualmente llegue un "inform".
 - *Proxy Forwarder*:
 - Implementa un proxy de SNMP, es un módulo opcional.
 - *Other*.

Aplicaciones:

Las aplicaciones implementadas en cada entity son opcionales.

Un **"agente"** en el sentido tradicional necesita solo:

Command Responder

Notification Originator

Opcionalmente, puede tener también proxy forwarder

Un **"gestor"** tradicional necesita:

Command Generator

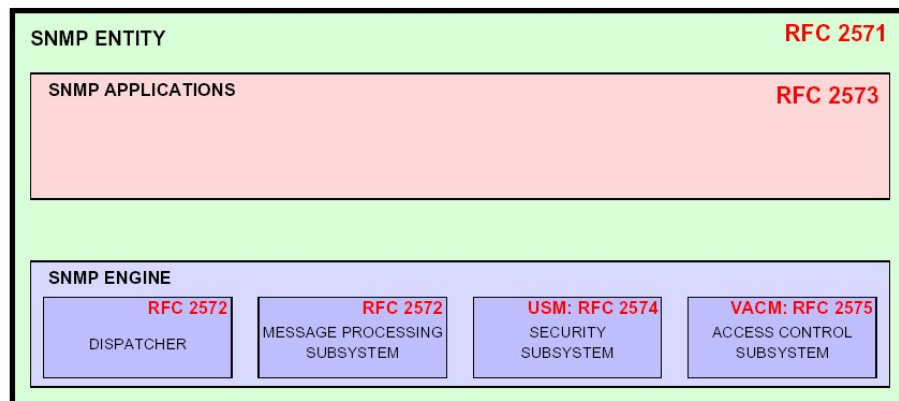
Notification Originator

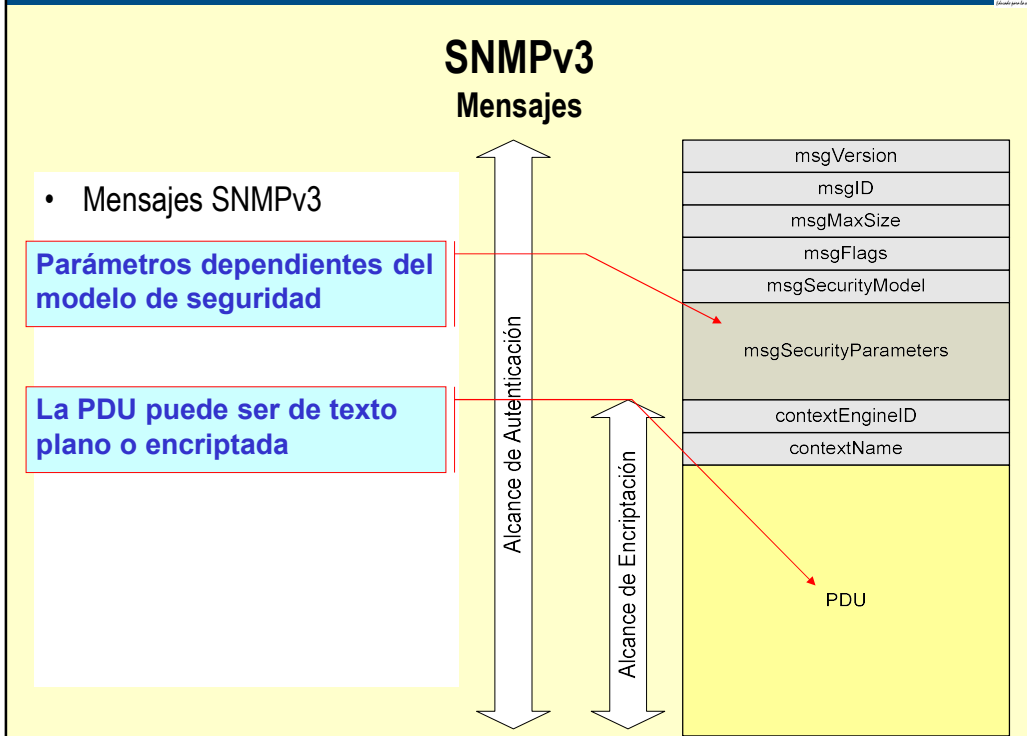
Notification Receiver

SNMPv3

Estándares

- SNMPv3, referencia de RFCs

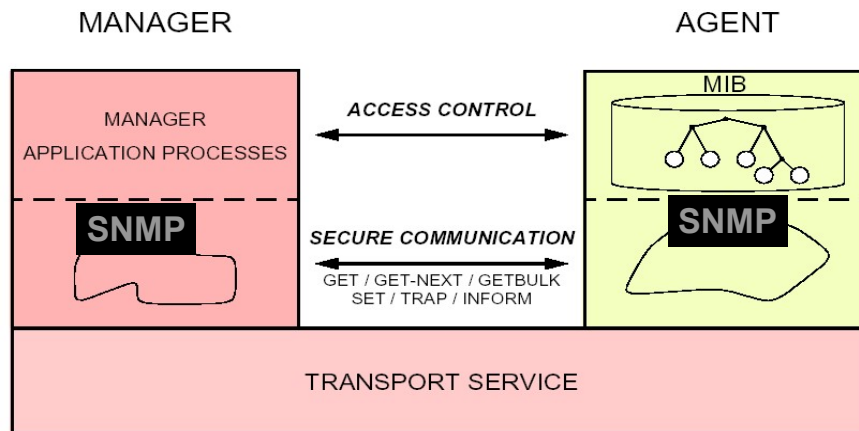




SNMPv3

Seguridad en SNMPv3

- Seguridad en SNMPv3



Seguridad en SNMPv3:

Control de acceso:

User-based Security Model (USM)

View-based Access Control Model (VACM)

Validación de mensajes

Encriptación (confidencialidad)

Engine Autoritativo:

Cuando un mensaje lleva una PDU que espera una respuesta (Gets, Set o Inform), entonces quien recibe se dice "autoritativo"

Cuando un mensaje lleva una PDU que no espera una respuesta (Trap, Report), entonces quien envía es autoritativo.

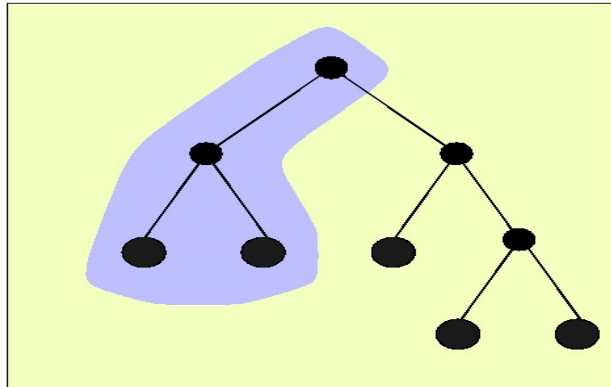
Evitar ataques de "replay"

Localización e intercambio de claves de encriptación

SNMPv3

Seguridad en SNMPv3

- Seguridad en SNMPv3 :
 - View-based Access Control:



Seguridad en SNMPv3:

User-based Security Model:

Hay una asociación entre “usuarios” y parámetros de seguridad.

Security Name:

Nombre de usuario

Authentication Protocol

MAC, MD5 o SHA-1

Authentication Passphrase

Clave para el anterior

Privacy Protocol

Plano o DES

Privacy Passphrase

Clave para el anterior

SNMPv3

Seguridad en SNMPv3

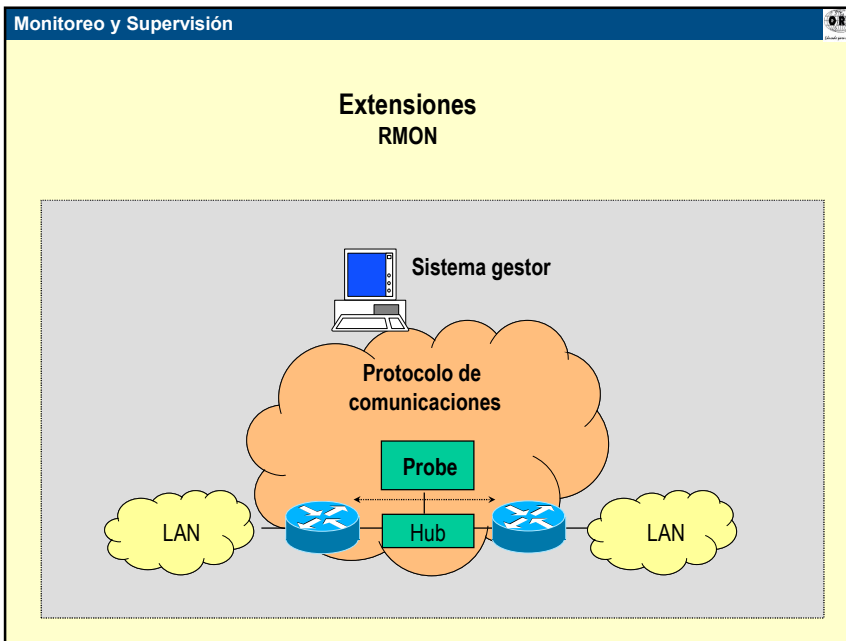
- Seguridad en SNMPv3:
 - Tablas de Control de Acceso

MIB VIEW	ALLOWED OPERATIONS	ALLOWED MANAGERS	REQUIRED LEVEL OF SECURITY
Interface Table	SET	John	Authentication Encryption
Interface Table	GET / GETNEXT	John, Paul	Authentication
Systems Group	GET / GETNEXT	George	None
...

Extensiones

Temas

- RMON
- RMON2



Remote network MONitoring (RMON)

RMON se basa en el modelo cliente-servidor y es una extensión de MIB definida en RFC 1271 y actualizada en RFC 1757. El propósito es extender el standard MIB-II de modo de proveer un mecanismo para capturar datos detalladamente en dispositivos no atendidos en forma centralizada.

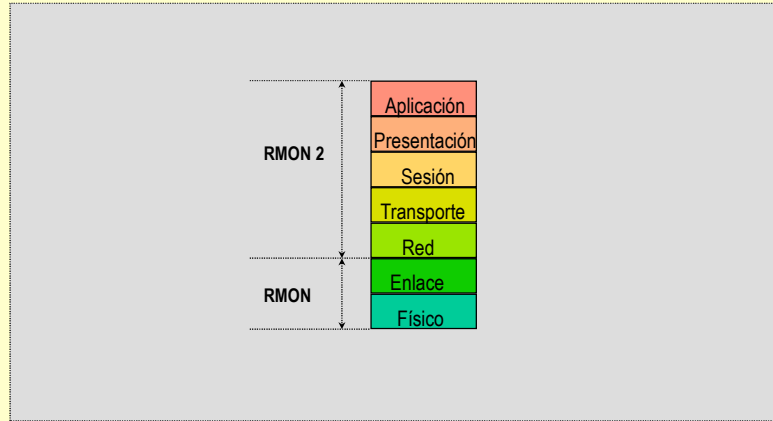
Para ello se instalan agentes basados en software o “probes” basados en hardware en varios puntos de interés de la red. Esos probes o agentes recolectan datos de ciertos tipos o grupos y los guardan en las tablas RMON. Luego, las estaciones de monitoreo de red podrán acceder a los probes a fin de obtener datos estadísticos, generar gráficas o hacer análisis de tendencias. Los probes pueden correr todo el tiempo, por lo cual recogen datos útiles para la resolución de problemas. Un probe puede consistir en una NIC y mucha memoria.

Con lo anterior, se elimina la necesidad de interrogación cíclica a los agentes remotos con lo cual disminuye el tráfico de gestión, (especialmente importante en enlaces WAN).

Grupos de RMON

RMON provee nueve grupos diferentes de datos: Estadísticas, Historia (muestras periódicas), Alarmas (superación de un umbral), Hosts (sigue la pista de las direcciones MAC a los efectos de registrar quién habla con quién), HostTopN (registro de los hosts más “habladores”), Matriz (define pares de hosts que dialogan), Filtro (criterios de selección de paquetes que se emplea en conjunto con el grupo de captura), Paquetes a Capturar (mecanismo de captura de paquetes de acuerdo con los filtros), Eventos (registro de eventos generados a partir de configuraciones o de excepciones ocurridas).

Extensiones RMON2



RMON 2

Así como RMON permite un monitoreo de las capas física y enlace, no provee mecanismos para el análisis de las direcciones de red involucradas en el tráfico ni de los protocolos empleados. RMON 2 extiende las funciones a las capas 3 a 7. De ese modo, permite detectar los orígenes y destinos finales de los paquetes así como los protocolos y aplicaciones utilizados (qué clientes acceden a qué servidores y por qué servicios). Provee información de la capacidad de red consumida por cada aplicación.

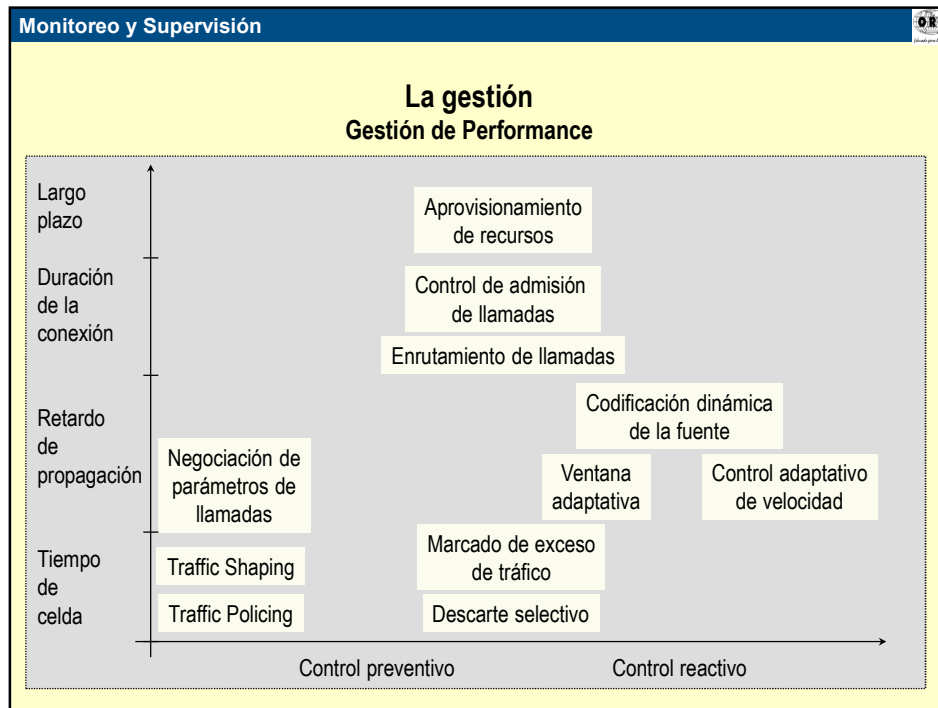
Genera tablas de Estadísticas, Host, Matrices y TopN para las capas red y aplicación. Permite guardar información de pares cliente-servidor. Permite filtros más eficientes y flexibles porque se definen en capas altas. Permite traducción de direcciones MAC-Red (Binding), especialmente útil para el descubrimiento de nodos, su identificación, y para las aplicaciones de gestión que generan mapas topológicos de red. Facilita la interoperabilidad al definir un standard por la cual una aplicación de gestión de un proveedor puede configurar un probe remoto de otro proveedor.

Cuestionario

- 1- Cuáles son las áreas funcionales definidas por ISO para la gestión y qué tareas incluyen?
- 2- Qué tareas incluyen el control y el monitoreo de dispositivos, y en qué áreas funcionales predomina cada uno de ellos?
- 3- Qué mecanismos de gestión de tráfico se pueden emplear, y en qué escala de tiempo?
- 4- Qué comprende el aprovisionamiento de recursos?
- 5- En qué casos se justifica el empleo de multiplexado estadístico y la correspondiente reserva de recursos?
- 6- Qué acciones pueden tomarse para asegurar la calidad de servicio en IP?
- 7- Cuales son los protocolos previstos para gestionar las redes de telecomunicaciones?
- 8- Cuáles son las funciones del protocolo de comunicación entre manager y agent?
- 9- Qué diferencia tienen el sondeo cíclico y la notificación asincrónica?
- 10- Cuáles son los elementos y sus respectivas funciones en SNMP?
- 11- Qué es SMI?
- 12- Cómo está organizada la información en una MIB?
- 13- Cuáles son las características y las diferencias de RMON y RMON2?
- 14- Qué operaciones pueden ejecutarse sobre las variables MIB?
- 15- Qué tipos de PDU se prevén en SNMP y para qué sirven los “variable bindings”?
- 16- Qué es una política de acceso en SNMP?
- 17- Qué son y para qué se emplean las comunidades en SNMP?
- 18- Qué operaciones se agregan en SNMPv2?
- 19- Qué novedades incorpora SNMPv3?
- 20- Qué diferencias presentan RMON y RMNO2?

Anexo

Gestión de performance



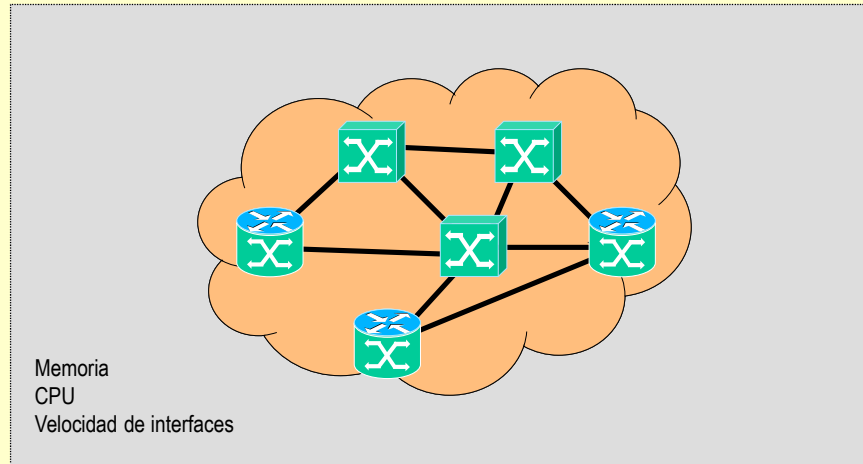
Exigencias de las redes de paquetes

Las redes de datos se basan en el multiplexado estadístico de paquetes. El control de tráfico es mucho más complejo que en las redes de conmutación de circuitos, debido al carácter aleatorio del arribo de paquetes a los nodos. Algunas características adicionales:

- el tráfico recibido es de tasas muy diferentes
- una fuente puede producir simultáneamente varios diferentes tipos de tráfico
- las redes IP deben gestionar el retardo máximo y la variación del retardo
- los requerimientos de calidad de servicio son muy diversos
- las velocidades crecientes hacen que existan varios paquetes en tránsito en el medio en cierto instante, por lo cual los embotellamientos se producen a una escala de tiempo reducida respecto a los tiempos que demanda la detección de la situación y la toma de medidas correctivas en los terminales
- las velocidades crecientes limitan los tiempos disponibles en los nodos para procesar la información

La gestión

Gestión de Performance – Aprovisionamiento de recursos

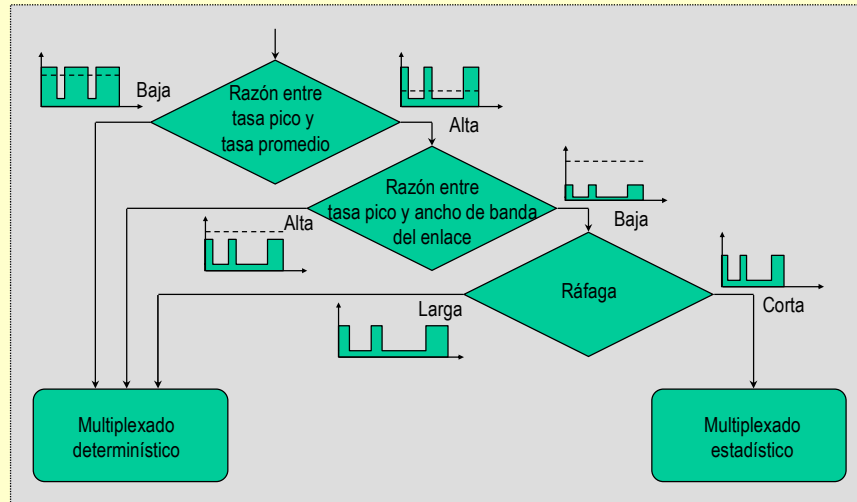


Aprovisionamiento de recursos

En las redes se requieren recursos de enlaces y nodos de red, que se van ampliando a medida que se detectan nuevas o mayores necesidades de tráfico. Las acciones son de mediano o largo plazo si las comparamos con las escalas de tiempo de la transmisión de paquetes o la duración de una llamada.

La gestión

Gestión de Performance – Control de admisión de llamadas



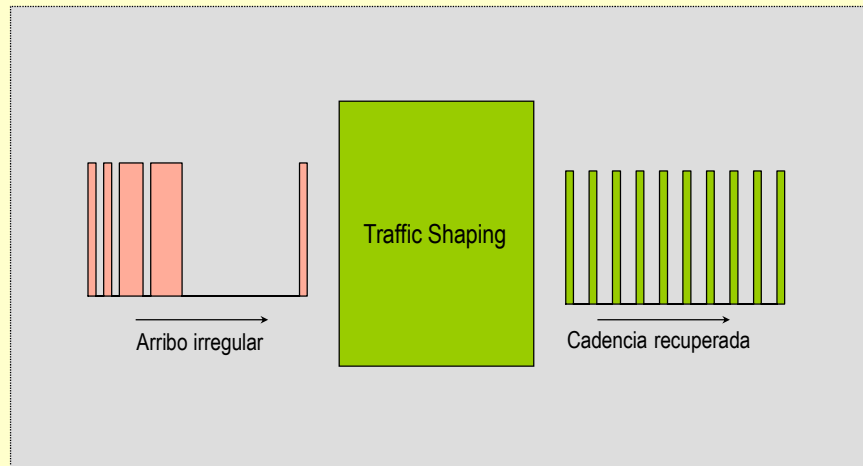
Reserva del ancho de banda

Existen dos modos de asignar ancho de banda: mediante multiplexado determinístico y mediante multiplexado estadístico. Los primeros garantizan que la probabilidad de congestión será casi cero, y lo mismo ocurrirá con la probabilidad de perder paquetes por saturación de los buffers.

Los servicios de multiplexado estadístico obtienen una alta eficiencia de los medios físicos, por lo cual reducen los costos. Pero se debe tener en cuenta que brindan calidades aceptables cuando el perfil del tráfico reúne ciertas características. El tráfico debe ser esencialmente de picos, con una ocupación reducida del total del ancho de banda del enlace. Además las ráfagas deben ser cortas a los efectos de no saturar los buffers. El cálculo de los valores de ancho de banda presenta dos aspectos: garantizar QOS de la conexión individual, asegurar que la QOS de las demás conexiones no degradan la QOS de la nueva, al multiplexarlas juntas.

La gestión

Gestión de Performance – Traffic Shaping



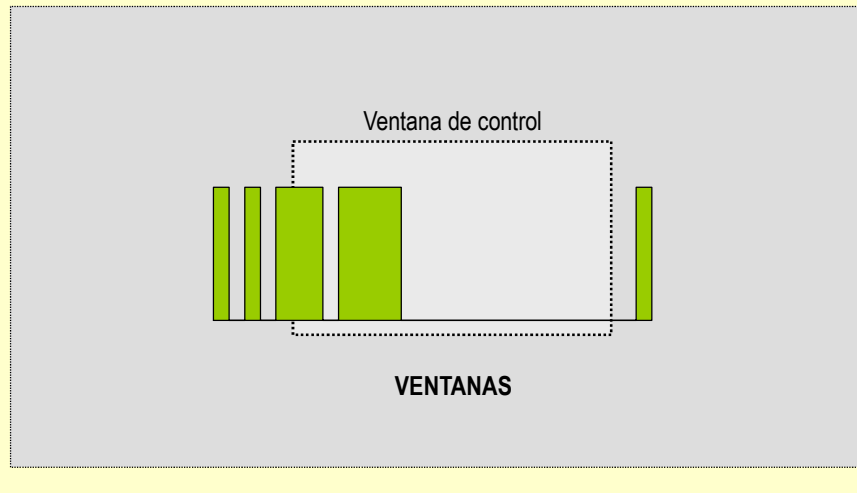
Traffic Shaping

La función de traffic shaping, implementada en el terminal que se conecta a la red, permite adaptar el tráfico ofrecido a ésta de modo de cumplir con los parámetros del contrato del servicio.

Mediante el almacenamiento en buffer de las ráfagas producidas, se puede dosificar el tráfico que se entrega a la red, reduciendo las ráfagas largas (durante las cuales se almacena más de lo que se transmite), aprovechando los lapsos de silencio para descargar el buffer. El tráfico entregado es entonces más uniforme y se garantiza el cumplimiento de los valores de ráfaga máxima admisible, tasa de pico, etc.

La gestión

Gestión de Performance – Traffic Policing



Ventanas

Existen cuatro variantes de este método:

Jumping Window (JW) - Durante un tiempo fijo T se controla la cantidad de celdas que llegan, la cual no debe superar un máximo establecido llamado ventana. Las celdas que lleguen en ese intervalo luego de alcanzarse el valor de ventana, serán descartadas. Para valores de T grandes se vuelve a llevar más tiempo detectar celdas que no cumplen, y la red admite ráfagas más largas. Si T disminuye, le resultará más difícil al terminal mantenerse dentro de los valores de cumplimiento.

Triggered Jumping Window (TJW) - En el caso anterior, la ventana comienza en los instantes que la red determina, y no necesariamente cuando el usuario inicia su actividad. En el TJW, el funcionamiento es más equitativo para el usuario: el control de ventana se inicia cuando se detecta actividad del terminal.

Moving Window (MW) - En esta variante, la ventana no está fija en el tiempo. Para cada celda que llega, se verifica su cumplimiento de contrato analizando el tráfico total recibido en un tiempo T medido desde el instante actual hacia atrás.

Exponentially Weighted Moving Average (EWMA) - Funciona con el principio del JW, pero el máximo de celdas aceptadas en cierta ventana varía de una ventana a la siguiente. La cantidad de celdas m_i aceptadas en la ventana i es la suma ponderada exponencialmente de las cantidades x_{i-1} de celdas aceptadas anteriormente, y el promedio m de celdas (valor fijo):

$$m_i = (m - d S_{i-1}) / (1 - d) \quad \text{con } S_{i-1} = (1 - d) x_{i-1} + S_{i-2}$$

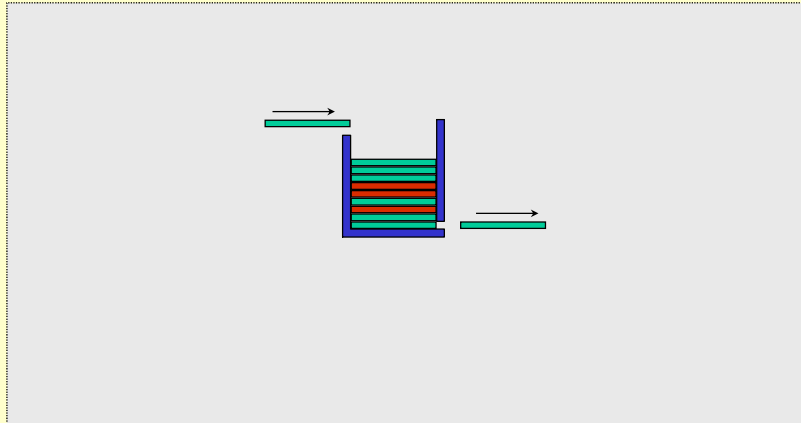
lo cual es equivalente a:

$$m_i = [m - (1 - d) (d x_{i-1} + \dots + d^{i-1} x_1) - d^{i+1} S_0] / (1 - d)$$

So es el valor inicial de EWMA. El parámetro d puede tomar valores entre 0 y 1, para $d = 0$ se tiene el caso de JW, para valores mayores se tiene un mecanismo más flexible.

La gestión

Gestión de Performance – Descarte selectivo



Descarte Selectivo

Debido al comportamiento estadístico del tráfico, existen periodos de baja actividad durante los cuales pueden encaminarse celdas aún cuando no cumplan el contrato de tráfico. Las mismas deberán ser marcadas para un tratamiento no preferencial en caso de congestión, y ese tráfico deberá tarifarse también diferencialmente (más económico).

Las técnicas para descarte de ese tipo de celdas se clasifican en:

Push-Out - Las celdas de alta y de baja prioridad son aceptadas cuando hay espacio en el buffer del nodo. Si el mismo se llena, las celdas de baja prioridad que lleguen serán descartadas, mientras que las de alta prioridad podrán desplazar a las de baja almacenadas en buffer, y sólo serán descartadas si no hay celdas de baja prioridad en espera (la excepción es que una celda de baja prioridad esté siendo transmitida). Es un mecanismo muy complejo para implementar.

Threshold - A diferencia del caso anterior, no se emplea la capacidad del buffer como referencia, sino un cierto nivel de ocupación (threshold). Si no se supera dicho nivel, ambos tipos de celdas son aceptados. Si se supera ese nivel, las celdas de baja prioridad serán descartadas hasta lograr descender por debajo del nivel. Las celdas de alta prioridad serán aceptadas mientras haya capacidad disponible en buffer.

Anexo

Structure of Management Information

Ejemplo de especificación de una tabla

Structure of Management Information

SMI – Especificación de objetos.

Veamos como ejemplo de tabla, cómo se especifica el contenido de una tabla de enrutamiento. Para obtener su contenido deberá emplearse la función get-next-request (http://www.unix.org.ua/orelly/perl/sysadmin/appe_01.htm).

-- The IP routing table contains an entry for each route

-- presently known to this entity.

ipRouteTable OBJECT-TYPE *El nombre del objeto*

SYNTAX SEQUENCE OF IpRouteEntry *El tipo*

ACCESS not-accessible *El modo de acceso*

STATUS mandatory *El grado de obligatoriedad*

DESCRIPTION

"This entity's IP Routing table."

::= { ip 21 }

En la figura de arriba, vemos que en SYNTAX se tiene la indicación de una secuencia de objetos IpRouteEntry. En ACCESS se indica "not-accesible", lo cual significa que no se trata de una variable que pueda interrogarse. Se trata de una ubicación en el árbol, debajo de la cual se acomodarán otros objetos que se describirán a continuación.

Structure of Management Information

En la figura anterior, vemos que en SYNTAX se tiene la indicación de una secuencia de objetos IpRouteEntry. En ACCESS se indica "not-accessible", lo cual significa que no se trata de una variable que pueda interrogarse. Se trata de una ubicación en el árbol, debajo de la cual se acomodarán otros objetos que se describirán a continuación.

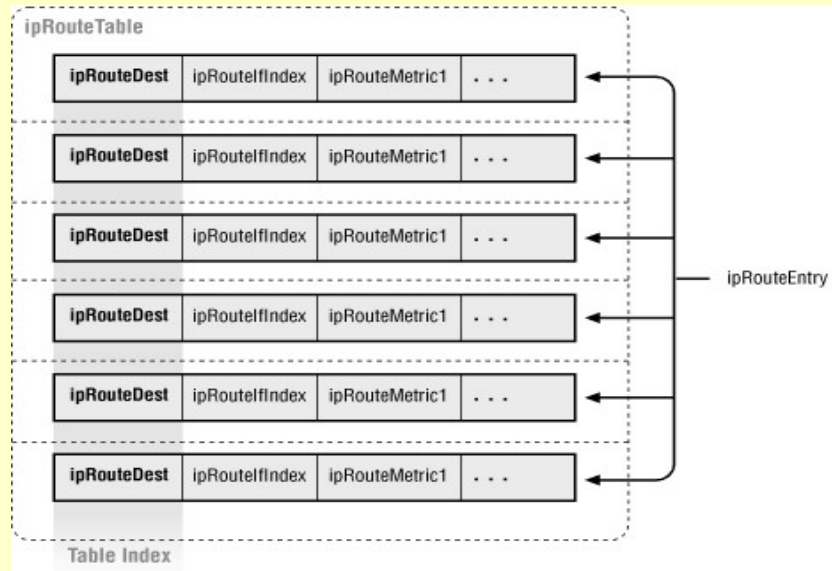
A su vez IpRouteEntry se define del siguiente modo:

```
ipRouteEntry OBJECT-TYPE
SYNTAX IpRouteEntry
ACCESS not-accessible
STATUS mandatory
DESCRIPTION
"A route to a particular destination."
INDEX { ipRouteDest }
 ::= { ipRouteTable 1 }
```

Como vemos, se trata nuevamente de una ubicación en el árbol, y no de una variable interrogable. Esta vez se define un índice: "IpRouteDest", con lo cual se indica que se trata de columnas que serán accesibles a través del mismo.

La figura de la página siguiente muestra gráficamente la organización de la tabla.

Structure of Management Information



Structure of Management Information

La definición de IpRouteEntry continúa:

```
ipRouteEntry ::=  
SEQUENCE {  
  ipRouteDest  
    IpAddress,  
  ipRouteIfIndex  
    INTEGER,  
  ipRouteMetric1  
    INTEGER,  
  ipRouteMetric2  
    INTEGER,  
  ipRouteMetric3  
    INTEGER,  
  ipRouteMetric4  
    INTEGER,  
  ipRouteNextHop  
    IpAddress,  
  ipRouteType  
    INTEGER,  
  ipRouteProto  
    INTEGER,  
  ipRouteAge  
    INTEGER,  
  ipRouteMask IpAddress,  
  ipRouteMetric5  
    INTEGER,  
  ipRouteInfo  
    OBJECT IDENTIFIER  
}
```

Structure of Management Information

ipRouteDest OBJECT-TYPE

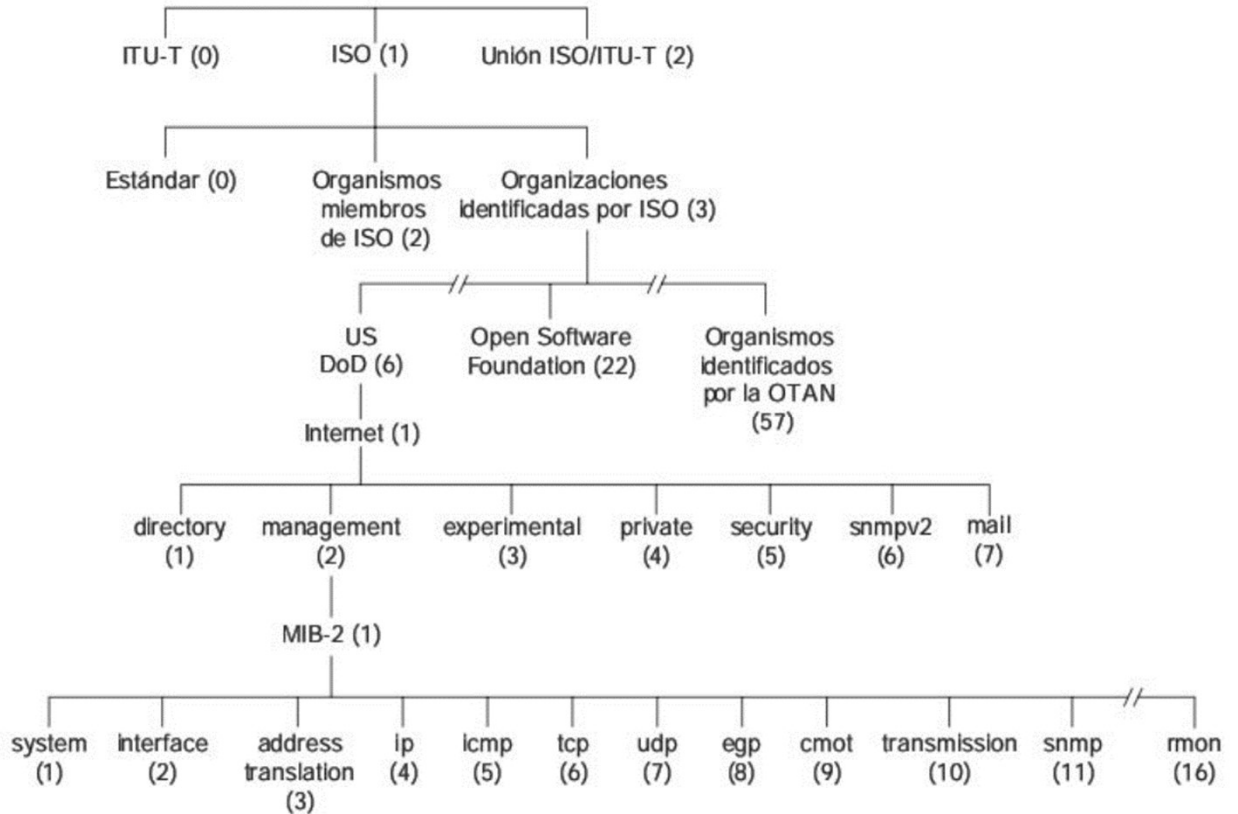
SYNTAX IpAddress

ACCESS read-write

STATUS mandatory

DESCRIPTION

"The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a



Seguridad

Virtual Private Networks - Autoridad Certificadora (CA)

Problema de autenticidad

- Cómo asegurar que la clave pública que aparece en un sitio público es auténtica?
- Emplear una autoridad certificadora que dé garantías

Implicado

Firma de
autoridad
certificadora

Clave
pública

- Cómo se asegura la autoridad certificadora de la autenticidad?
- Acuerda un encuentro en el cual se identifican los interesados y la autoridad les valida la clave pública. Los interesados podrán luego certificar a otros actores. De ese modo se puede implementar una cadena de confianza que se inicia en la autoridad certificadora.

Seguridad

Virtual Private Networks - Certificado

Formato de certificado UIT-T X.509

Field	Meaning
Version	Which version of X.509
Serial number	This number plus the CA's name uniquely identifies the certificate
Signature algorithm	The algorithm used to sign the certificate
Issuer	X.500 name of the CA
Validity period	The starting and ending times of the validity period
Subject name	The entity whose key is being certified
Public key	The subject's public key and the ID of the algorithm using it
Issuer ID	An optional ID uniquely identifying the certificate's issuer
Subject ID	An optional ID uniquely identifying the certificate's subject
Extensions	Many extensions have been defined
Signature	The certificate's signature (signed by the CA's private key)

Extraído de Tanenbaum, Computer Networks

Ejemplo de certificado UIT-T X.509

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 7829 (0x1e95)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,

OU=Certification Services Division,

CN=Thawte Server CA/Email=server-certs@thawte.com

Validity

Not Before: Jul 9 16:04:02 1998 GMT

Not After : Jul 9 16:04:02 1999 GMT

Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,

OU=FreeSoft, CN=www.freesoft.org/Email=baccala@freesoft.org

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

```
00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:66:3
6:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:16:94:6
e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:8f:a0:21:c7:4
c:d0:16:65:00:c1:0f:d7:b8:80:e3:d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:e8:35:1c:9e:27:5
2:7e:41:8f
```

Exponent: 65537 (0x10001)

Signature Algorithm: md5WithRSAEncryption

```
93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:ab:
2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:0d:
19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:8f:
0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22: 68:9f
```


Seguridad

Virtual Private Networks - Centro de Distribución de Claves (KDC)

Problema de distribución de claves simétricas

- Cómo intercambian claves compartidas A y B a través de la red?
- Emplean un Centro de Distribución de Claves que tenga una clave compartida previamente con cada uno de los actores y que pueda generar firmas iguales a las que generan A y B.
- A solicita una clave al KDC. Éste le envía una clave K y además el resultado de encriptar K y la firma de A con la clave de B. A envía dicho resultado a B. B lo descripta con su clave simétrica y obtiene la firma de A para comprobar luego la identidad de A y obtener la clave simétrica.

