Transparencias

de

Redes de Ordenadores

Tema 13

SNMP

Uploaded by

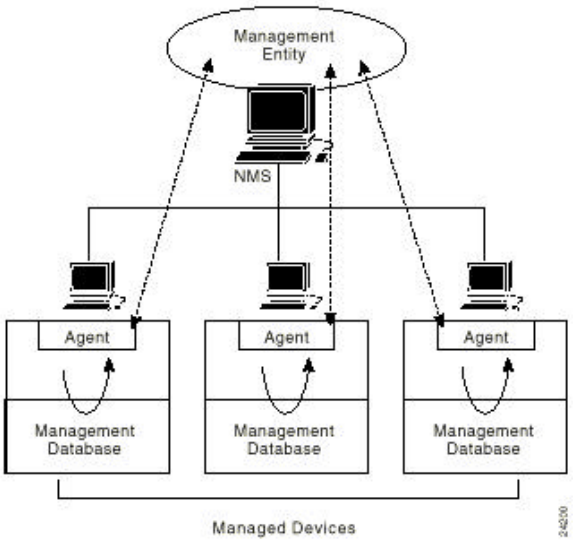
IngTeleco

http://ingteleco.iespana.es
ingtelecoweb@hotmail.com

Gestión de Red: SNMP

- Protocolo del nivel de aplicación que facilita el intercambio de información de gestión entre dispositivos de red.
- Existen varias versiónes, SNMP v1, SNMP v2 y SNMP v3
- Componentes básicos:
  - Dispositivos o nodos gestionados (NE)
    - Nodo de una red que contiene un agente SNMP.
    - Recopila información y almacena información de gestión haciéndola accesible a los NMS mediante el uso de SNMP
    - Estaciones, servidores, routers, switches, hubs, impresoras, …
  - Agentes de gestión (MA)
    - Módulo software de gestión de red que reside en un nodo gestionado.
    - Tiene conocimiento local de la información de gestión y la traduce a un formato compatible a SNMP.
  - Sistemas de gestión de red (NMS)
    - Ejecuta aplicaciones que monitorizan y contolan dispositivos.
    - Puede haber uno o varios por red

Red Gestionada con SNMP



Comandos básicos SNMP

- Los nodos gestionados se monitorizan y controlan mediante tres comandos básicos SNMP:
  - Read
    - Utilizado por los NMS para monitorizar los nodos gestionados.
    - Examinan variables mantenidas por los nodos gestionados
  - Write
    - Utilizado por los NMS para controlar los nodos gestionados.
    - Cambian los valores de las variables almacenadas en los dispositivos
  - Trap
    - Utilizado por los nodos gestionados para notificar eventos asíncronamente al NMS.
    - Cuando se producen ciertos tipos de eventos se notifican al NMS mediante el envío de un trap.

Gestión TCP/IP

- Tres elementos :
  - La Base de Información de Gestión (MIB)
    - Especifica qué objetos (o variables) deben mantener los NE relacionados con su configuración y operación.
    - MIB-II definida en RFC 1213.
  - La Estructura de Gestión de Informacion (SMI)
    - Conjunto de estructuras y esquema de identificación para la definición de los objetos MIB
  - El Protocolo de Gestión de Red Simple (SNMP)
    - Protocolo para la comunicación entre NMS y NE.

MIB

- Definición de los objetos que debe proporcionar cada MA.
  - Las MIBs son accedidas mediante el uso de SNMP.
  - Están compuestas por objetos gestionados e identificadas por identificadores de objetos
- Objeto gestionado
  - Característica específica de un NE, organizados en grupos relacionados con los niveles TCP/IP (muchos son contadores).
  - MIB-II (RFC 1213), MIB-I (RFC 1156)
  - Los objetos gestionados están compuestos de una o más instancias de objeto, que son esencialmente variables.
  - Tipos de objetos gestionados:
    - Escalares
      - Definen una instancia de objeto simple
    - Tabulares
      - Definen instancias múltiples relacionadas, agrupadas en tablas MIB.
- Dividida en grupos:
  - System, Interfaces, at, ip, icmp, tcp, udp, egp, transmiss, snmp
  - Cada NE soporta sólo aquellos grupos que son apropiados.

MIB (II)

- System Group
  - sysDescr - Full description of the system (version, HW, OS)
  - sysObjectID - Vendor's object identification
  - sysUpTime - Time since last re-initialization
  - sysContact - Name of contact person
  - sysServices - Services offered by device
- Interfaces Group
  - ifIndex - Interface number
  - ifDescr - Interface description
  - ifType - Interface type
  - ifMtu - Size of the largest IP datagram
  - ifAdminisStatus - Status of the interface
  - ifLastChange - Time the interface entered in the current status
  - ifINErrors - Number of inbound packets that contained errors
  - ifOutDiscards - Number of outbound packets discarded

MIB (III)

- Address Translation Group
  - atTable - Table of address translation
  - atEntry - Each entry containing one network address to physical address equivalence
  - atPhysAddress - The media-dependent physical address
  - atNetAddress - The network address corresponding to the media-dependent physical address
- IP Group
  - ipForwarding - Indication of whether this entity is an IP gateway
  - ipInHdrErrors - Nº of input datagrams discarded due to errors in their IP headers
  - ipInAddrErrors - Nº of input datagrams discarded due to errors in their IP address
  - ipInUnknownProtos - Nº of input datagrams discarded due to unknown or unsupported protocol
  - ipReasmOKs - Number of IP datagrams successfully re-assembled
  - ipRouteMask - Subnet-mask for route

MIB (III)

- ICMP Group
  - icmpInMsgs - Nº of ICMP messages received
  - icmpInDestUnreachs - Nº of ICMP destination-unreachable received
  - icmpInTimeExcds - Nº of ICMP time-exceeded messages received
  - icmpInSrcQuenchs - Nº of ICMP source-quench messages received
  - icmpOutErrors - Nº of ICMP messages not sent due to ICMP problems
- TCP Group
  - tcpRtoAlgorithm - Algorithm to determine the timeout for retransmitting unacknowledged octets
  - tcpMaxConn - Limit on the nº of TCP connections supported
  - tcpActiveOpens - Nº of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state
  - tcpInSegs - Nº of segments received, including those received in error
  - tcpConnRemAddress - The remote IP address for this TCP connection
  - tcpInErrs - Nº of segments discarded due to format error
  - tcpOutRsts - Nº of resets generated

MIB (IV)

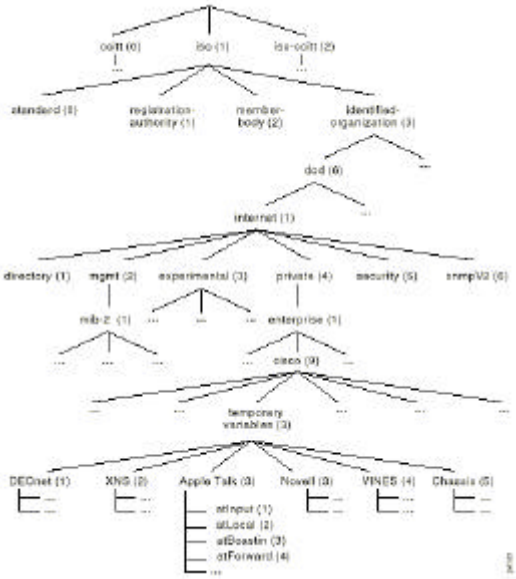
- UDP Group
  - udpInDatagrams - Nº of UDP datagrams delivered to UDP users
  - udpNoPorts - Nº of received UDP datagrams for which there was no application at the destination port
  - udpInErrors - Nº of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port
  - udpOutDatagrams - Nº of UDP datagrams sent from this entity

Representación de datos (SMI)

- Define reglas para describir información de gestión
  - Define la estructura de una MIB particular.
  - Define cada objeto, la sintaxis y valor.
  - Codifica el valor de los objetos.
- La definición se realiza en una plantilla :
  - Object (object descriptor):
    - Un nombre textual junto con su correspondiente "object identifier".
  - Syntax:
    - La sintaxis abstracta de ASN.1 del tipo objeto. Tipos de datos SMI
      - Tipos simples: Integer, octect string, object ID, Null, Sequence y Sequence of.
      - Tipos de datos de aplicación: networks addresses, counters, gauges, time ticks, opaques, integers, unsigned integers.
  - Definition:
    - Una descripción textual de la semántica del tipo objeto.
  - Access:
    - Restricciones de acceso al objeto (R, RW, W, NA).
  - Status:
    - Indica si el objeto es obligatorio, opcional o bien si está obsoleto.

SMI: Identificadores de objeto

- Un objeto debe identificarse unívocamente.
  - Cada identificador es único, y su valor consiste en una secuencia de enteros separados por puntos decimales
  - El grupo de objetos definidos formará una estructura en árbol.
  - Los objetos particulares estarán en las hojas de las ramas del árbol.



SNMP

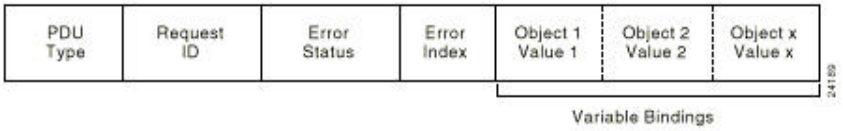
- Mecanismo de comunicación entre NMS y NE
  - Acceso del NMA a los objetos MIB mantenidos por el MA, para consultarlos y modificarlos.
  - Envío de mensajes no solicitados desde el MA al NMS para indicar que se ha producido un evento.
- Protocolo muy simple:
  - Dos funciones esenciales: alteraciones (set) o inspecciones (get) de variables
  - Nº limitado de mensajes no solicitados (traps) desde el MA para informar de eventos asíncronos.
  - Precisa un servicio de datagramas no fiable: UDP

Operación del protocolo SNMP

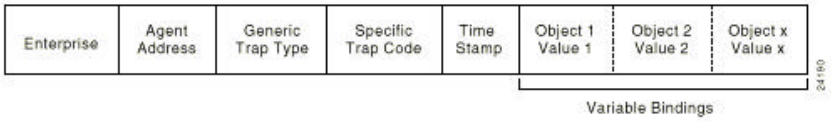
- Es un protocolo simple de petición-respuesta
  - El NMS envía una petición y el NE devuelve una respuesta.
- Operaciones:
  - GET-REQUEST
    - Usado por el NMS para recuperar el valor de una o más instancias de un objeto desde un agente.
    - El agente devuelve todos los valores consultados o ninguno.
  - GET-NEXT-REQUEST
    - Utilizado por el NMS para recuperar el valor de la instancia del siguiente objeto de la tabla o lista dentro de un agente.
  - RESPONSE
    - Utilizado por el NE para devolver el valor de una o más instancias de un objeto hacia el NMS, como respuesta a una petición de aquel.
  - SET-REQUEST
    - Utilizado por el NMS para establecer los valores de una o más instancias de un objeto dentro de un agente.
  - TRAP
    - Utilizado por un nodo gestionado para informar al NMS de un evento.

Formato de los mensajes SNMP v1

- Cabecera
  - Número de versión
  - Nombre de comunidad
    - Define un entorno de acceso para un grupo de NMSs (autenticación)
- PDU
  - Contienen un comando específico y operandos que indican las instancias de objetos involucrados en la operación.
  - Formato de las tramas GET, GETNEXT, RESPONSE y SET



  - Formato de las tramas TRAP



Entidad SNMP v2

- Proceso que desarrolla operaciones de gestión de red generando y/o respondiendo a mensajes SNMPv2.
- Las operaciones posibles pueden restringirse a un subconjunto de todas las operaciones de un "Party"
  - Una entidad puede ser miembre de varios Parties.
- Una entidad SNMPv2 mantiene las siguientes Bases de Datos locales:
  - Una Base de Datos para todos los Parties conocidos por la entidad SNMPv2 que podrían ser:
  - Al menos una Base de Datos que representa una política de control de acceso.

Party SNMP v2

- Entorno de ejecución virtual, cuya operación está restringida a un subconjunto administrativamente definido de todas las operaciones posibles de una entidad SNMPv2.
- Arquitectura de un Party :
  - Una identidad de party única
  - Una ubicación de red lógica en la que se ejecuta el party.
  - Protocolo de autenticación único: todos los mensajes originados por el party son autenticados en origen e integridad.
  - Protocolo de privacidad único para proteger todos los mensajes recibidos por el party.

SNMPv2 GetBulkRequest

- Pedir la transferencia de una cantidad de datos potencialmente grande, incluyendo la recuperación de tablas de grandes dimensiones.
- Más eficiente que GetNextRequest en el caso de recuperación de la MIB de objetos tablas de gran dimensión.
  - Con el comando GetBulkRequest se puede recuperar de manera eficiente el contenido de la siguiente variable o de los siguientes M variables en una sola petición.
- Sintaxis :

```
GetBulkRequest [ non-repeaters = N, max-repetitions = M ]
                    ( RequestedObjectName1,
                      RequestedObjectName2,
                      RequestedObjectName3 )
```


SNMPv2 GetBulkRequest

```
Interface-Number  Network-Address  Physical-Address  Type
      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
GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]
            ( sysUpTime, ipNetToMediaPhysAddress, ipNetToMediaType )
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" ))
GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]
    (sysUpTime, ipNetToMediaPhysAddress.1.10.0.0.51, ipNetToMediaType.1.10.0.0.51)
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" ))
```

SNMPv2 InformRequest

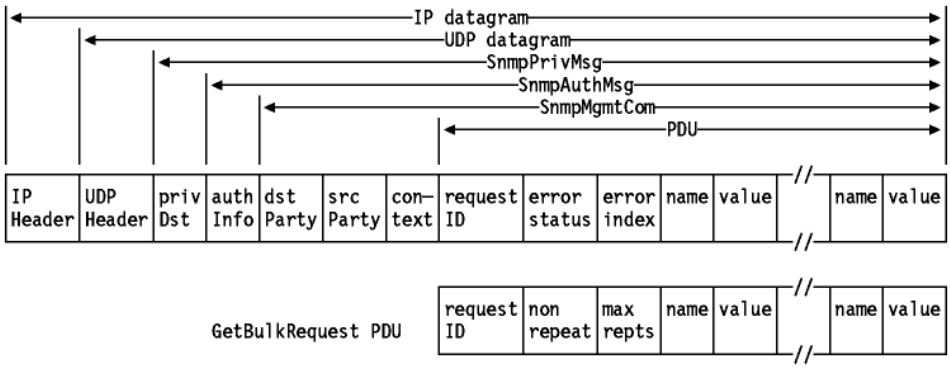
- Se genera como petición de un NMS que desea notificar a otra NMS información en la vista MIB de un party local a la aplicación emisora.
- El paquete se utiliza como una indicación al gestor del otro party de la información accesible en el party emisor (comunicación gestor-a-gestor a través de límites de party).
- Las primeras dos variables en la lista de asignación de variables de un InformRequest son sysUpTime.0 y snmpEventID.i respectivamente, pudiendo seguir otras variables.

SNMPv2: Autenticación y privacidad

- Protocolo de autenticación:
  - Mecanismo para identificar las comunicaciones de gestión SNMPv2 transmitidas por un party como originadas por dicho party.
- Protocolo de privacidad:
  - Mecanismo por el que las comunicaciones de gestión SNMPv2 transmitidas a un party son protegidas frente a consultas no deseadas.
- Servicios de seguridad :
  - Integridad de datos
    - Algoritmo de cifrado MD5.
  - Autenticación del origen de los datos
    - Prefijo secreto en cada mensaje compartido por origen y destinatario.
  - Retraso de los mensajes o repetición de los mismos
    - Se añade un valor de timestamp en cada mensaje.
  - Confidencialidad de los datos
    - Protocolo de privacidad simétrico con encriptación (clave secreta).
    - Data Encryption Standard (DES).

SNMPv2: Nuevo modelo admin.

- Distintas identidades para parejas que intercambian mensajes SNMPv2.
- Al indentificar unívocamente el emisor y el destinatario, el modelo de control de acceso permite un uso efectivo de protocolos de seguridad asimétricos (clave pública).
- Formato de la trama



RMON

- Define una MIB de monitorización remota
  - El efecto es la definición de funciones e interfaces entre consolas de gestión basadas en SNMP y monitores remotos.
- Objetivos:
  - Operación Off-line
  - Monitorización Apropiativa
  - Detección y notificación de problemas
  - Datos de valor añadido
  - Gestores múltiples
- Control de monitores remotos
  - Aparatos dedicados o una función disponible en un sistema
  - El monitor remoto debe ser configurado para la captura de datos, especificando el tipo de datos y la forma en que van a ser recogidos.
    - Tabla de control: describe la configuración del monitor RMON especificando la información que captura
    - Tabla de datos: almacena la información recogida.

RMON (II)

- Invocación de una acción
  - Mediante operaciones SNMP puede enviarse un mandato, empleando un objeto para representar un estado de modo que se realice una determinada acción cuando dicho objeto cambia de estado.
- La MIB RMON
  - Se divide en nueve grupos:
    - Estadísticas: Estadísticas de error y bajo nivel de utilización para cada subred.
    - Historia: Estadísticas periódicas de la información disponible.
    - Alarma: Intervalo de muestreo y umbral de alarma para cualquier dato grabado por el agente RMON.
    - Host: Datos sobre tipos de tráfico de y hacia nodos conectados a la subred.
    - HostTopN: Estadísticas agrupadas en una lista basadas en la tabla "host".
    - Matriz: Información sobre errores y utilizaciones en forma de matriz, para cualquier par de direcciones de la red.
    - Filtro: Observar paquetes que casan con el filtro.
    - Captura de paquetes: Modo de envío de los datos a la consola de gestión.
    - Evento: Una tabla con todos los eventos generados por el agente RMON.