SNMP: Conceptos

Carlos Armas
Roundtrip Networks

Hervey Allen
NSRC

Preparado con materiales de:

Carlos Vicente
Servicios de Red/Universidad de Oregon

Necesidad de una arquitectura

- En una red heterogénea, es necesario definir (y estandarizar) una serie de elementos para su fácil gestión:
  - Las entidades que participan en la gestión
  - Las estructuras de datos que se van a utilizar
  - Los protocolos de comunicación

Componentes de la Infraestructura

- La *entidad gestora*
  - Hardware y software que reune, procesa, analiza y presenta la información de red
  - Interactúa con el administrador de red
  - Punto central de control de los dispositivos

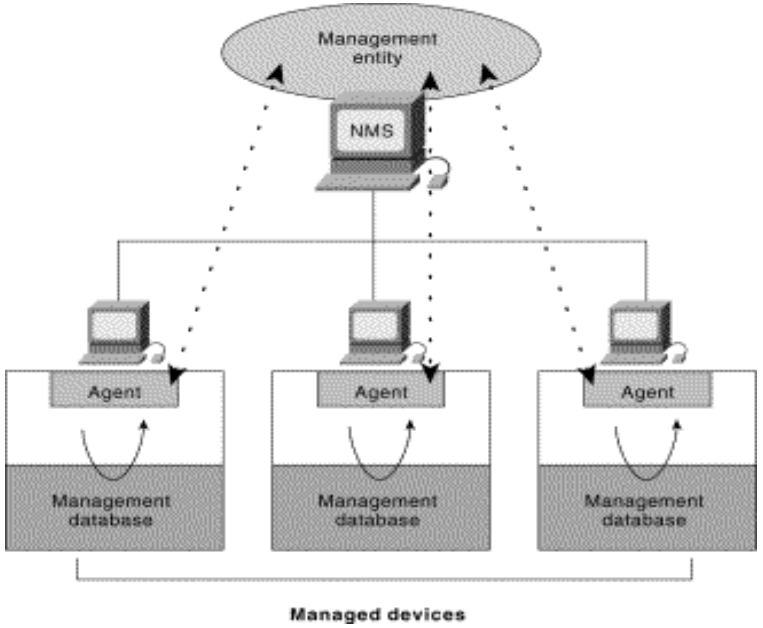
Componentes de la infraestructura

- El *dispositivo gestionado*
  - Contiene uno o más objetos gestionados
    - Una tarjeta de red, el CPU, la pila de protocolos IP, el ventilador...
  - Estos objetos contienen información que puede ser recogida (y a también cambiada) por la entidad gestora
  - Contiene un agente de gestión cuya función es comunicarse con la entidad gestora y ejecutar acciones localmente (leer, escribir un dato)

Componentes de la infraestructura

- El *protocolo de gestión*
  - Provee las reglas de comunicación entre la entidad gestora y los agentes de gestión
  - Define cosas como:
    - Tipos de mensajes y operaciones
    - Seguridad (autenticación, privacidad)
    - Manejo de secuencias

"Los *agentes de gestión*, localizados en los *dispositivos gestionados*, son sondeados periódicamente por la *entidad gestora*, utilizando un *protocolo de gestión*"



Diferentes estándares

- Dos grupos principales:
  - Definidos por OSI (Open Systems Interconnection)
    - CMISE/CMIP (Commmon Management Information Services Element/Common Management Information Protocol)
  - DoD – TCP/IP (actual Internet)
    - SNMP (Simple Network Management Protocol)
    - Terminó siendo el más utilizado

Marco de Referencia Estándar de Gestión en Internet

- Se define un marco de referencia y no sólo un protocolo (SNMP)
  - SNMP no es tan “simple” si se tiene en cuenta esto.
- Resuelve los siguientes problemas:
  - Qué se va a gestionar y qué tipo de control se va a ejercer?
  - En qué formatos se va a transmitir la información?
  - Qué reglas se van a seguir durante la transmisión de esta información?

SMI: Estructura de Información de Gestión
(Structure of Management Information)

- Es un lenguaje de definición de datos (DDL)
- Elimina la ambigüedad en la sintaxis y semántica de los datos
  - Por ejemplo, cómo se han de representar los números enteros (big-endian, little-endian)
- Basado en ASN.1 (estándar de la ISO), pero extendido
- Define lo siguiente:
  - Tipos de datos
  - Modelo de objetos
  - Reglas para revisar y cambiar los datos
- RFCs 2578, 2579, 2580

SMI: Estructura de Información de Gestión
(Structure of Management Information)

- Algunos tipos de datos relevantes:
  - Integer: Entero de 32 bits
  - Octet String: Cadena de bytes (2^16)
  - Counter32: Entero de 32 bits que se incrementa
  - Counter64: Entero de 64 bits que se incrementa
  - Gauge32: Entero de 32 bits que no se incrementa
  - TimeTicks: Tiempo medido en centésimas de segundo desde algún momento determinado

SMI: Estructura de Información de Gestión
(Structure of Management Information)

```
ipForwarding OBJECT-TYPE
   SYNTAX      INTEGER {
                  forwarding(1),    -- acting as a router
                  notForwarding(2)  -- NOT acting as a router
               }
   MAX-ACCESS  read-write
   STATUS      current
   DESCRIPTION
         "The indication of whether this entity is acting as an IP
         router in respect to the forwarding of datagrams received
         by, but not addressed to, this entity.  IP routers forward
         datagrams.  IP hosts do not (except those source-routed via
         the host)."
   ::= { ip 1 }
```

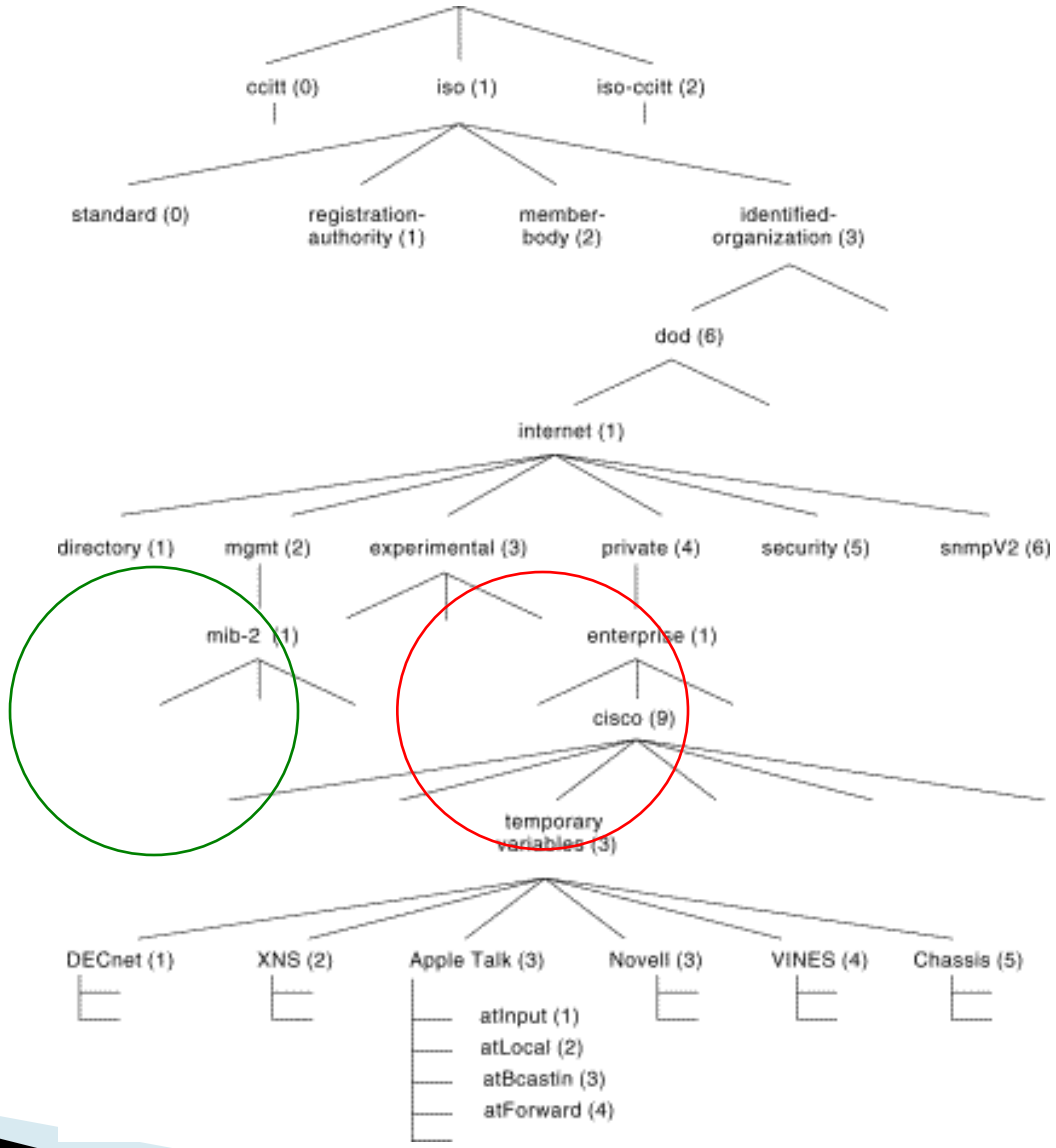
SMI: Estructura de Información de Gestión
(Structure of Management Information)

```
ipMIB MODULE-IDENTITY
   LAST-UPDATED "9411010000Z"
   ORGANIZATION "IETF SNMPv2 Working Group"
   CONTACT-INFO
          "       Keith McCloghrie

          Postal: Cisco Systems, Inc.
                  170 West Tasman Drive
                  San Jose, CA  95134-1706
                  US

          Phone:  +1 408 526 5260
          Email:  kzm@cisco.com"
   DESCRIPTION
          "The MIB module for managing IP and ICMP implementations,
          but excluding their management of IP routes."
   REVISION      "9103310000Z"
   DESCRIPTION
          "The initial revision of this MIB module was part of MIB-II."
   ::= { mib-2 48}
```

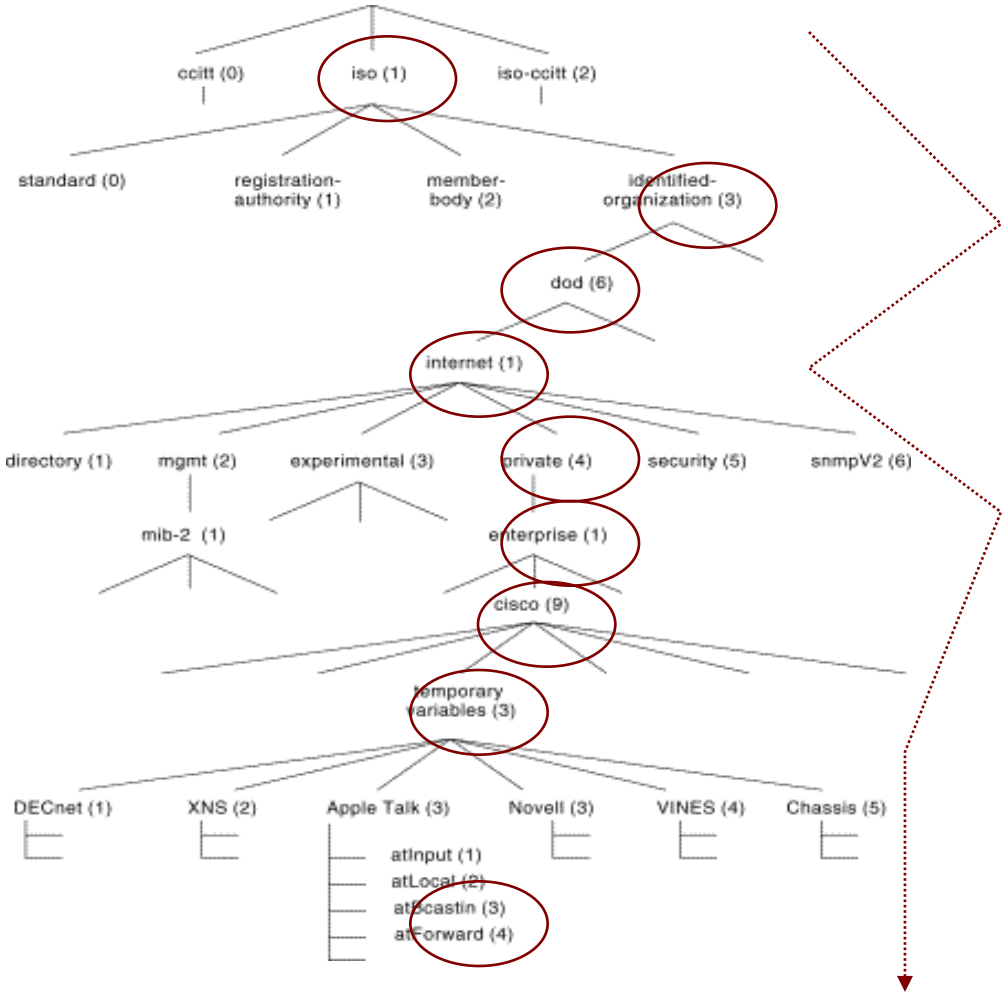
MIB: Base de Información de Gestion (Management Information Base)

- Agrupación de objetos de gestión en módulos
- Hay cientos de módulos estándar definidos por la IETF
- Hay **miles** de módulos privados definidos y registrados por fabricantes para la gestión de sus equipos
- Muchas veces, los fabricantes indizan información estándar sólo en sus módulos privados
  - Hace muy difícil la utilización de herramientas comunes para gestionar redes heterogéneas :-(

Arbol de identificación de objetos de ISO



Arbol de identificación de objetos de ISO



Equivale a: .iso.org.dod.internet.private.enterprise.cisco.temporary.tmpappletalk.atForward
O tambien: .1.3.6.1.4.1.9.3.3.4

El protocolo SNMP

- Generalmente utilizado en modo pregunta-respuesta
  - Ya sea para leer (get) o escribir un dato (set)
  - Minimalista
- También puede enviar mensajes (no-solicitados) a la entidad gestora para notificar acerca de algún estado anormal.
  - Ejemplos:
    - Cuando una interfaz se “cae”
    - La utilización del CPU sobrepasa el 85%
- Estos mensajes se conocen como “traps”
- Cada tipo de mensaje tiene un correspondiente PDU (Protocol Data Unit)

El protocolo SNMP

- Tres versiones
- Fácil implementación gracias a la modularidad del diseño:
  - El lenguaje de definición de datos (SMI) es independiente de las bases de datos de objetos (MIBs), que a la vez son independientes del protocolo de comunicación (SNMP)

SNMP v1

- Utiliza un método muy simple de autenticación, basado en 'comunidades'
- Provee los siguientes tipos de operaciones
  - **GET** (petición de un valor)
  - **GET-NEXT** (petición del valor siguiente en la tabla)
  - **GET-RESPONSE** (respuesta al get o set)
  - **SET-REQUEST** (petición de escritura)
  - **TRAP** (alarma espontánea enviada por el agente)

SNMP v1

- Información Tabular:

Destination	NextHop	Metric
10.0.0.99	89.1.1.42	5
9.1.2.3	99.0.0.3	3
10.0.0.51	89.1.1.42	5

```
GetNextRequest ( ipRouteDest, ipRouteNextHop, ipRouteMetric1 )
```

```
GetResponse (( ipRouteDest.9.1.2.3 =  "9.1.2.3" ),
             ( ipRouteNextHop.9.1.2.3 = "99.0.0.3" ),
             ( ipRouteMetric1.9.1.2.3 = 3 ))
```

SNMP v2

- Contiene una serie de mejoras
  - Tipos de datos
    - Counter64
    - Cadenas de bits
    - Direcciones de red (además de IP)
  - Operaciones
    - GetBulk
    - Inform

SNMP v2

- A pesar de sus mejoras, no es lo suficientemente seguro
  - Sigue utilizando el esquema de 'comunidades' como medio de identificación

SNMP v3

- Principalmente, resuelve los problemas de seguridad de versiones anteriores:
  - ¿El mensaje solicitando una operación ha sido alterado? ¿Ha llegado en el momento adecuado?
  - ¿Quién solicitó la operación?
  - ¿A qué objetos se accederá en esta operación?
  - ¿Qué privilegios tiene el solicitante sobre los objetos en cuestión?

SNMP v3

- La arquitectura de seguridad se diseñó para adaptar diferentes modelos de seguridad
- El modelo más común es basado en usuarios (User-based Security Model, o USM)
  - **Autenticidad e Integridad**: Se utilizan claves por usuario, y los mensajes van acompañados de "huellas digitales" generadas con una función hash (MD5 o SHA)
  - **Privacidad**: Los mensajes pueden ser cifrados con algoritmos de clave secreta (CBC-DES)
  - **Validez temporal**: Utiliza reloj sincronizados, y una ventana de 150 segundos con chequeo de secuencia

SNMP: Estado actual de la implementación

- Prácticamente todos los equipos de red soportan SNMPv1
- La mayoría de los equipos actualmente soportan SNMPv2
- Actualmente muchos fabricantes aún no han implementado SNMPv3

Referencias

- RFCs 1157, 1901, 1905, 2570, 2574
- Computer Networking: A Top-Down Approach Featuring the Internet. James F. Kurose.
- Internetworking with TCP/IP, Vol 1: Principles, Protocols and Architectures. Douglas Comer.
- The Simple Times www.simple-times.org
  - Essential SNMP (O'Reilly Books) Douglas Mauro, Kevin Schmi