Un poco más acerca de SNMP

- Management Information Base (MIB):
  - Todo recurso de red gestionable debe ser representado a través de un objeto
  - El conjunto de todas las variables conocidas por un agente es la MIB de este agente
- Structure of Management Information (SMI):
  - Lenguaje que define la sintaxis y semántica (tipo de datos) de los objetos de la MIB.
- Protocolo SNMP (gestor <-> agente), (UDP, puerto 161 y para snmp trap 162)
- Consideraciones de seguridad (SNMP v3)

SNMP – SMI

- Tipos de datos de un objeto
- OBJECT-TYPE
  - Tipo de dato, estatus y semántica del objeto
- MODULE-IDENTITY:
  - Objetos que se agrupan en una MIB

Tipos de datos

INTEGER
Integer32
Unsigned32
OCTET STRING
OBJECT IDENTIFIED
IPaddress
Counter32
Counter64
Guage32
Time Ticks
Opaque

SNMP – SMI: Ejemplo

OBJECT-TYPE: ipInDelivers

```
ipInDelivers OBJECT TYPE
  SYNTAX       Counter32
  MAX-ACCESS   read-only
  STATUS   current
  DESCRIPTION
    "The total number of input
     datagrams successfully
     delivered to IP user-
     protocols (including ICMP)"
::= { ip   9}
```

MODULE-IDENTITY: ipMIB

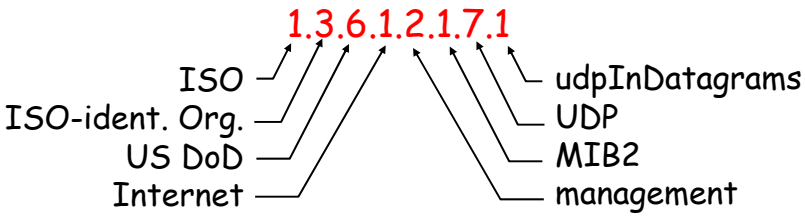
```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANZATION "IETF SNPv2
          Working Group"
  CONTACT-INFO
    " Keith McCloghrie
    ……"
  DESCRIPTION
    "The MIB module for managing IP
    and ICMP implementations, but
    excluding their management of
    IP routes."
  REVISION "019331000Z"
 ……
::= {mib-2 48}
```


SNMP – Ejemplo de MIB: Módulo UDP

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams no app at portl
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

SNMP - OID

- Cómo identificar todo posible objeto estándar para cada estándar de red?
- La respuesta es ISO Object Identifier tree:
  - Estructura jerárquica.
  - Cada rama y hoja tiene un nombre y número

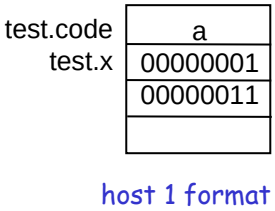


SNMP – presentación de los datos(1/2)

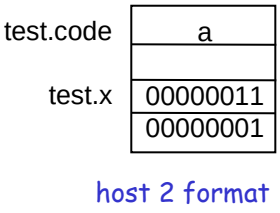
Pregunta: La copia exacta de los datos de la memoria del origen a la memoria del destino soluciona "el problema de la comunicación"

Respuesta: No siempre!

```
struct {
   char code;
    int x;
    } test;
test.x = 256;
test.code='a'
```



host 1 format



host 2 format

SNMP – presentación de los datos(2/3)

- ASN.1: Abstract Syntax Notation 1:
  - Estándar de ISO, X.680.
  - Define tipos de datos y constructores de objetos (como SMI)
  - BER: Basic Encoding Rules:
    - Especifica como los objetos deben ser transmitidos
    - Cada objeto transmitido tiene una codificación del tipo TLV (Type, Length, Value)

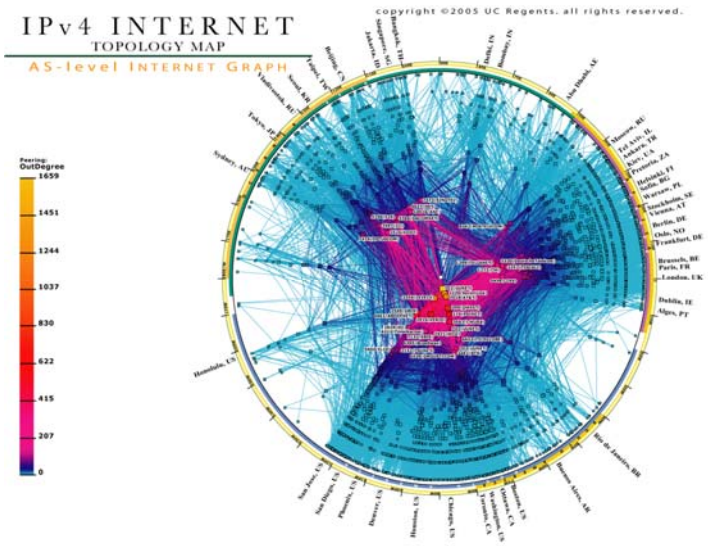
SNMP – presentación de los datos(3/3)

- TLV Encoding:
  - Idea: Los datos transmitidos están identificados en el propio paquete:
    - T: Tipo de datos, uno de los definidos en ASN.1
    - L: Largo en bytes de los datos transmitidos del objeto
    - V: Valor de los datos codificados según el estándar ASN.1.

SNMPv3 – Seguridad

- Encriptación de los mensajes.
- Autenticación
- Protección contra ataques de playback.
- Control de acceso por usuario y con perfiles.

Metrología: CAIDA



Metrología: CAIDA, IPPM...

- Cooperative Association for Internet Data Analysis
  - http://www.caida.org
  - cflowd: análisis de información de NetFlow
    - Colección y análisis de datos
      - Soporte de planificación de capacidad, análisis de tendencias, caracterización de la carga
      - Accountig&billing, data warehousing…
  - NeTraMet: implementación open-source (GPL), Network Traffic Flow Measurement
  - skitter: probe activo para analizar topología y performance en Internet
- IP Performance Metrics (ippm) WG del IETF
  - Métrica para caracterización cuantitativa de Internet
  - http://www.ietf.org/html.charters/ippm-charter.html

Metrología: Brevemente – Netflow(1/3)

- NetFlow (RFC 3954), proviene de Cisco.
- Por qué usarlo:
  - Conocer la distribución del uso de los protoclos.
  - Monitorear usuarios y aplicaciones.
  - Identificar tráfico mailicioso.
  - Peering entre ISP.
  - Planificación.
  - Ingeniería de tráfico.
  - Accounting/billing.

Metrología: Brevemente – Netflow(2/3)

- Inspecciona paquetes de capa 2-4, no aplicación y los clasifica en "flujos" que se examinan durante cierto tiempo:
  - Dirección IP de destino
  - Dirección IP de origen
  - Protocolo de capa 4
  - Puerto de origen
  - Puerto de destino
  - TOS byte
  - Interfaz de entrada al equipo de red
  - Nuevas versiones agregan más datos.
- En el equipo de red se guarda en el NetFlow cache la información del flujo junto con por ejemplo la cantidad de bytes asociados al flujo y bytes/paquete.

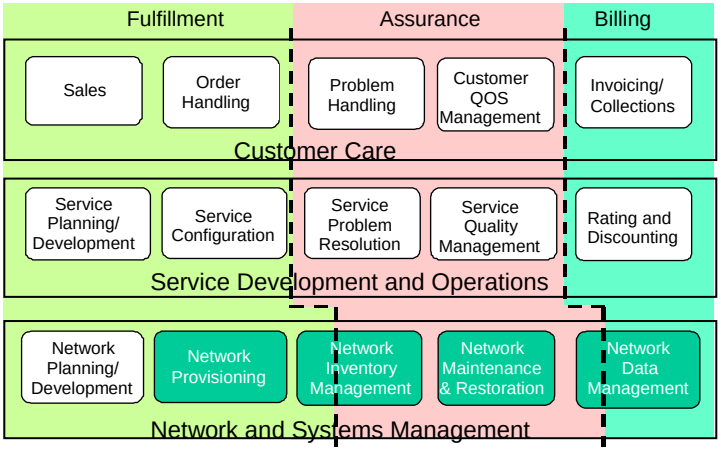
Metrología: Brevemente – Netflow(3/3)

- Consume recursos:CPU y memoria:
  - Para reducirlo se puede elegir no procesar todos los paquetes para netflow, muestras de 1 cada 100 o 1000 paquetes, no teniendo toda la información.
- La información de netflow generalmente es exportada por el nodo de red hacia otro equipo dedicado a procesar la información obtenida:
  - Un ejemplo es la biblioteca flow-tools:
    - Colecta, envía y genera reportes a partir de información de netflow.

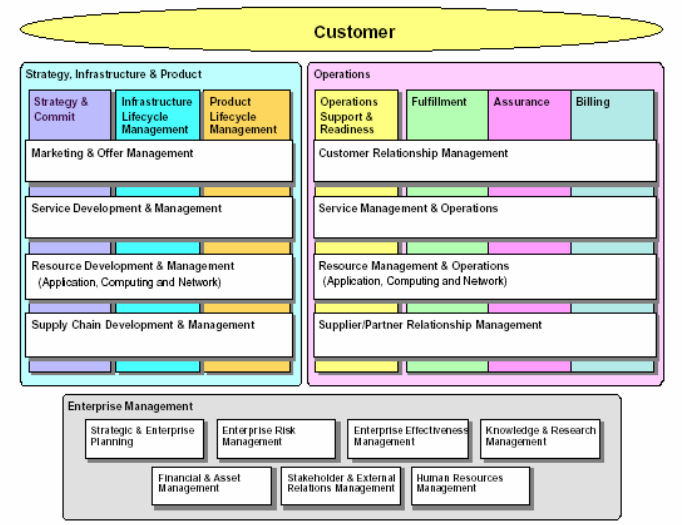
Solución completa?

- Hemos visto algunas aplicaciones que resuelven parte del problema
  - Monitorización de variables de comportamiento
  - Alarmas
  - Metrología, caracterización del tráfico…
  - Performance y Fallos
  - A nivel de red y elemento….
- Gestión del Negocio, Clientes, Servicios?

Telecom Operation Map (TOM)



eTOM



A manera de conclusión

- Gestión de redes y servicios: problema complejo
- Se necesitan modelos
- Pero...
  - Deben ser implementables
  - Énfasis en interoperabilidad