

SNMP

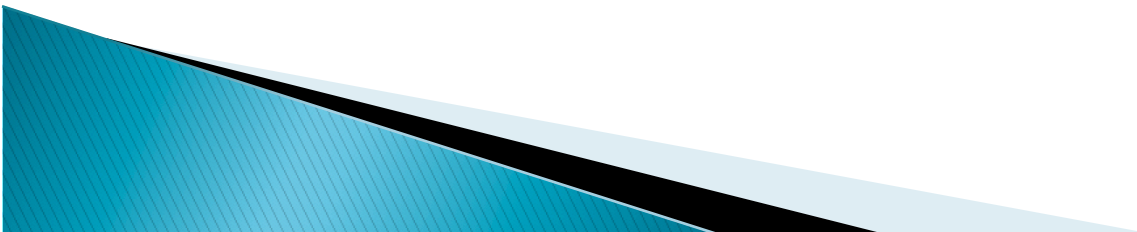
Gestión de Redes



Este documento es producto de trabajo realizado por Network Startup Resource Center (NSRC at <http://www.nsrc.org>). Este documento puede ser libremente copiado o re-utilizado con la condición de que toda re-utilización especifique a NSRC como su fuente original.

Contenido

- Qué es SNMP?
- OIDs
- MIBs
- Solicitudes
- Trampas
- SNMP version 3 (Opcional)



Qué es SNMP?

SNMP – Protocolo Simple de Gestión de Red

- Estandar reconocido, muchas herramientas disponibles
Presente en cualquier dispositivo de red (decente)

Basado en Solicitud/Respuesta: **GET / SET**

- GET se usa para monitoreo

Concepto de MIBs (Base de Informacion de Gestion)

- Jerarquía de Arbol
 - Se encuesta el estado de "Identificadores de Objeto" (OIDs)
- Existen definiciones estandard, y específicas de proveedores ("enterprise")



Qué es SNMP?

UDP protocolo UDP, puerto 161

Diferentes versiones

- v1 (1988) – RFC1155, RFC1156, RFC1157
 - Especificación original
- v2 – RFC1901 ... RFC1908 + RFC2578
 - Nuevos tipos de datos, métodos de recopilación de datos mejorados (GETBULK)
 - La versión más usada es v2c (carece de método de alta seguridad)
- v3 – RFC3411 ... RFC3418 (alta seguridad)

Típicamente se usa SNMPv2 (v2c), y a veces v3



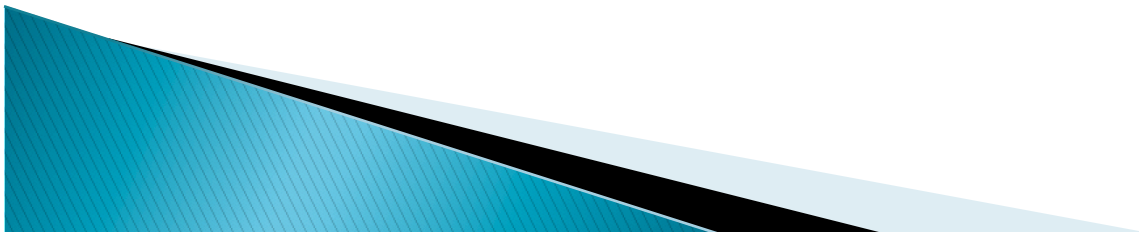
Componentes: quiénes interactúan?

■ La *entidad gestora*

- Recopila y presenta la información de dispositivos y servidores

■ El *dispositivo gestionado*

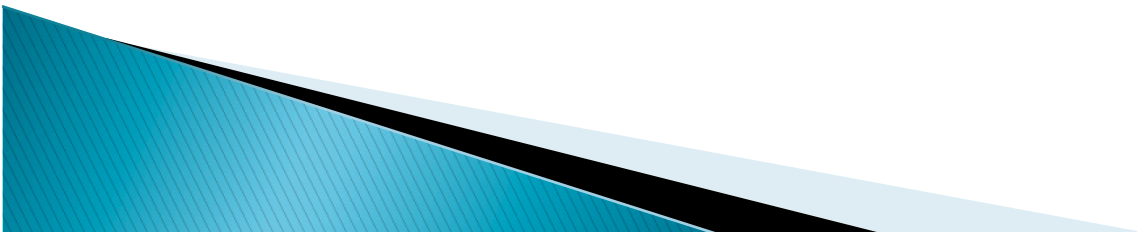
- Contiene un agente de gestión que responde a las encuestas de la entidad gestora
- Qué tipo de información?
 - Los objetos gestionados pueden ser muy variados:
 - Carga del CPU, estado de una interfaz de red, espacio en disco duro, entre muchas otras...



Componentes: como conversan?

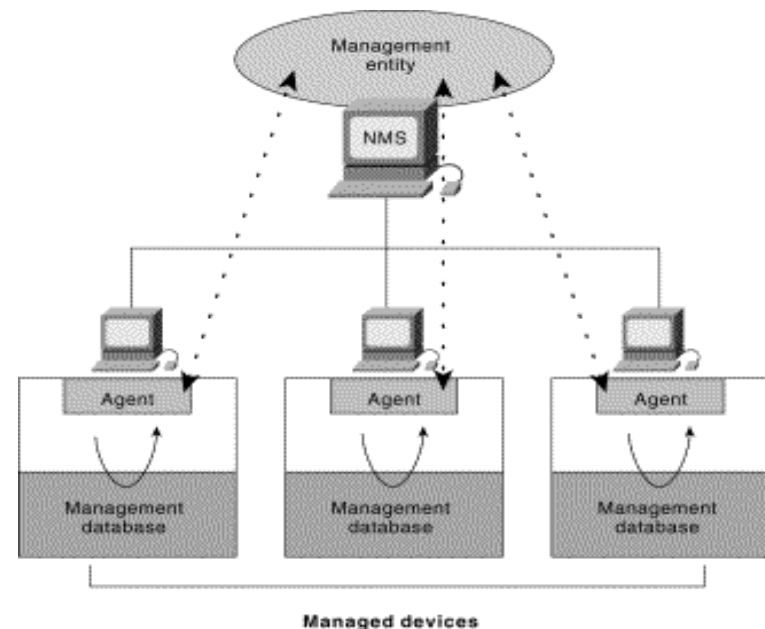
■ El *protocolo de gestión*

- Provee las reglas de comunicación entre la entidad gestora y los dispositivos gestionados
- Define entre otros:
 - Tipos de mensajes (solicitud y respuesta)
 - Seguridad de acceso, y datos (autenticación, privacidad)



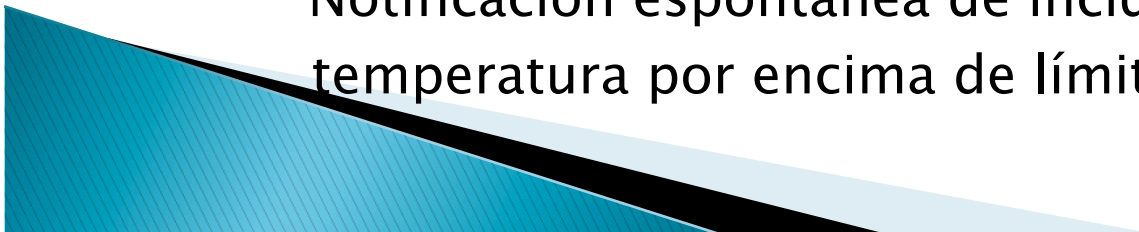
SNMP en esencia

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



SNMP: comandos

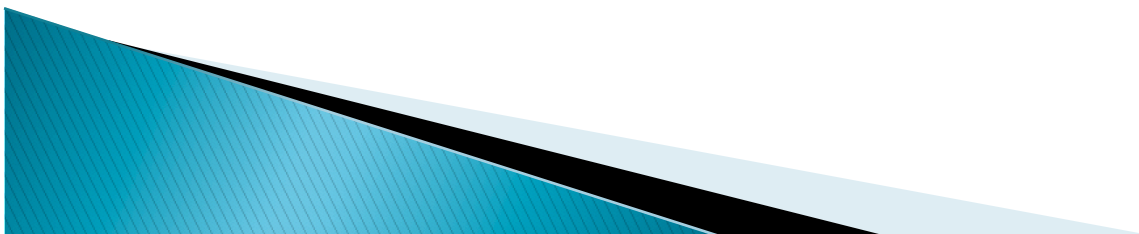
- GET (entidad gestora → agente)
 - Solicitud de valor de variable única
- GET-NEXT (entidad gestora → agente)
 - Solicitando valor siguiente (recursivo, para listas)
- GET-RESPONSE (agente → entidad gestora)
 - Respuesta a GET/SET, o error
- SET (entidad gestora → agente)
 - Configurar un valor, o ejecutar acción
- TRAP (agente → entidad gestora)
Notificación espontánea de incidente (falla de línea, temperatura por encima de límite, etc ...)



SNMP

■ Tipos de datos de respuesta:

- 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



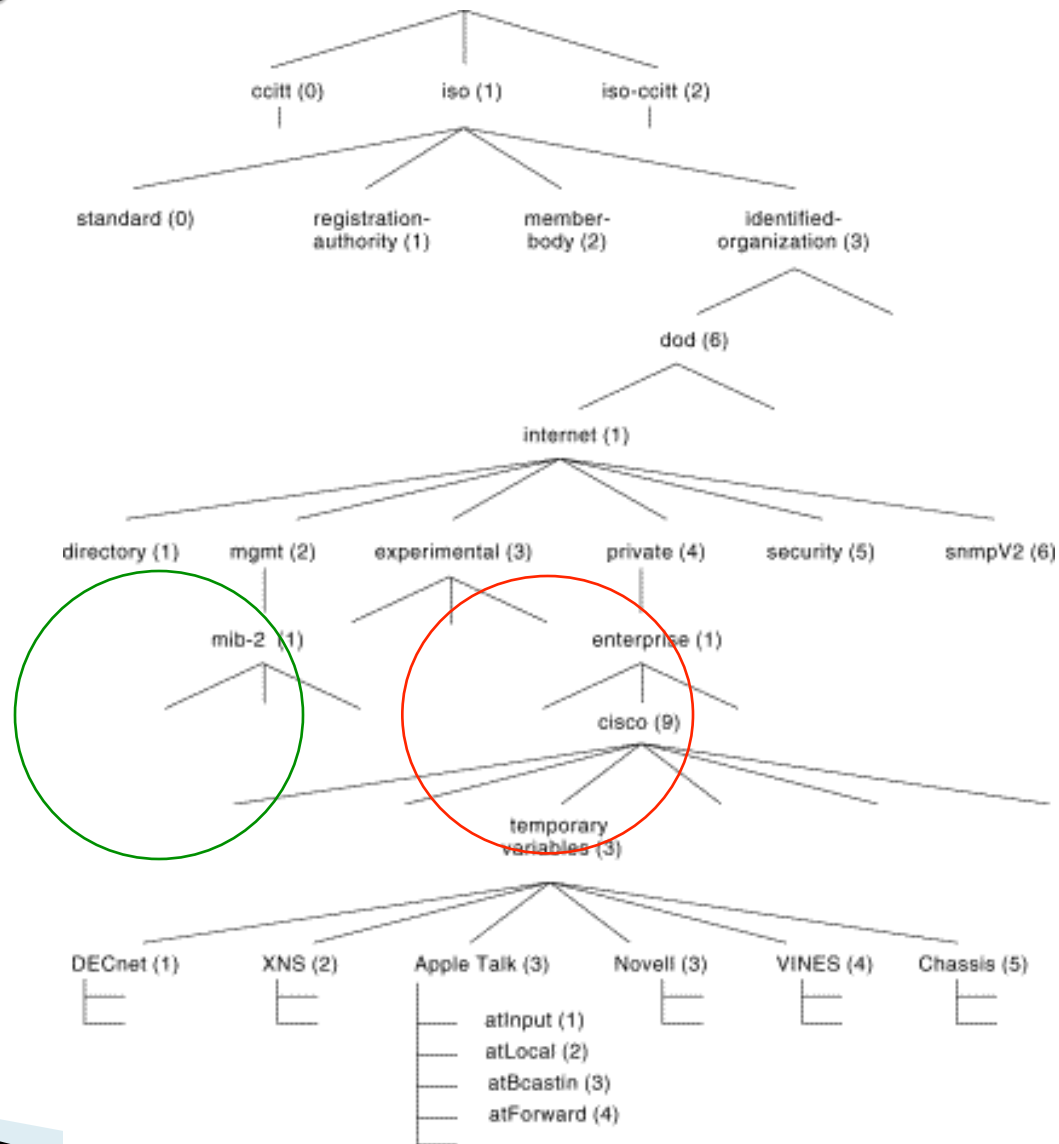
MIB: Base de Información de Gestión

(Management Information Base)

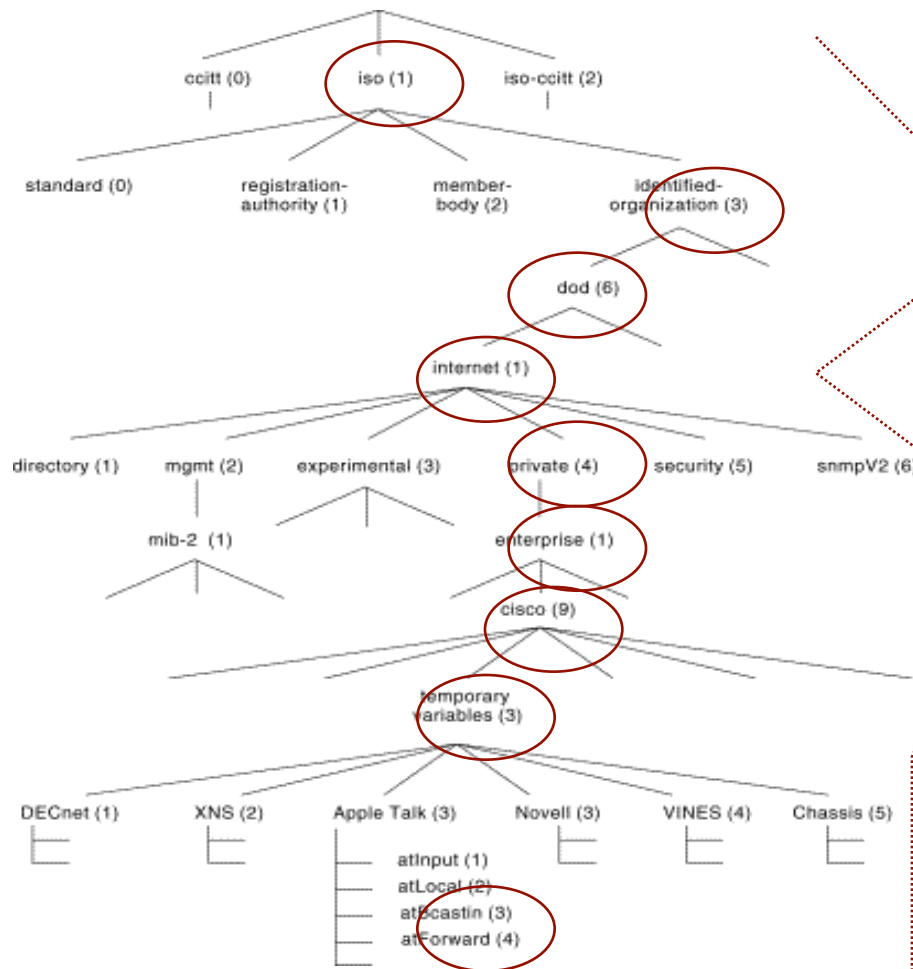
- Agrupación de objetos de gestión en módulos
- Hay cientos de módulos estándar definidos por la IETF
- Hay **miles** de módulos privados definidos y registrados por fabricantes para la gestión de sus equipos
- Muchas veces, los fabricantes indizan información estándar sólo en sus módulos privados
 -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



Arbol MIB



Arbol MIB



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

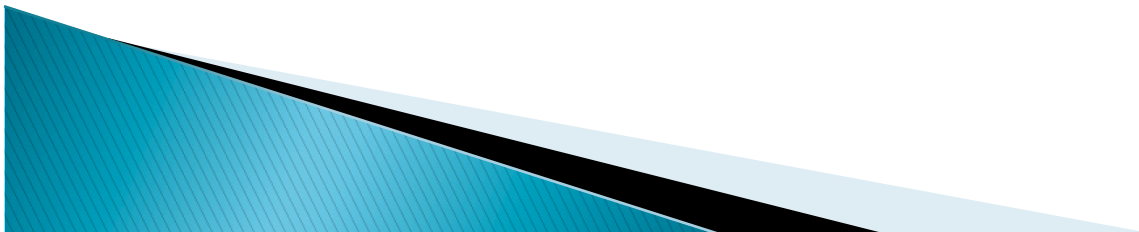
El protocolo SNMP

- 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)



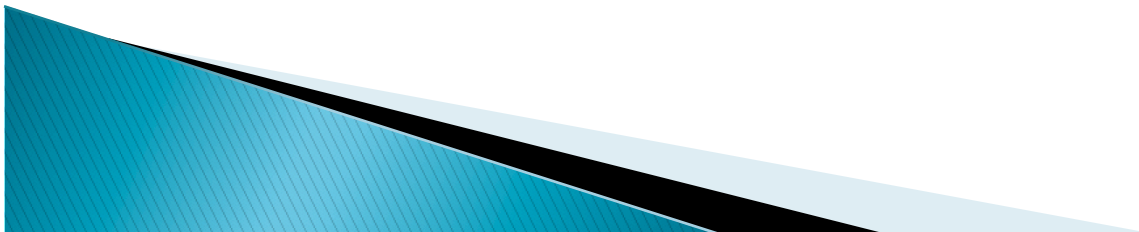
SNMP v1

■ 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

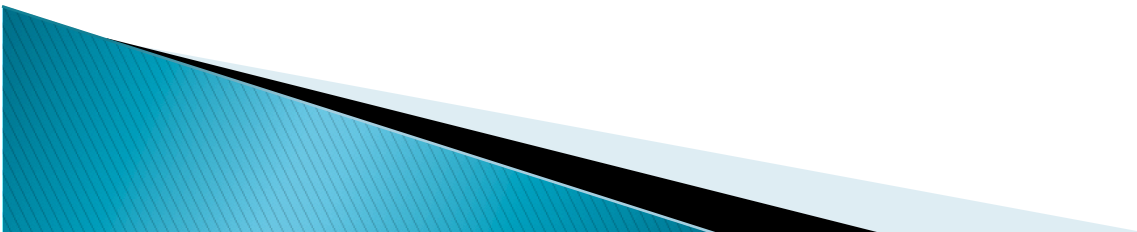
```
GetNextRequest ( ipRouteDest, ipRouteNextHop, ipRouteMetric1 )|
```

```
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 ) )|
```



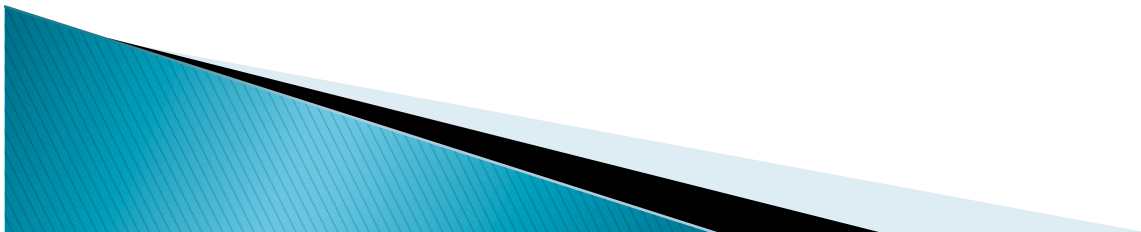
SNMP v2

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



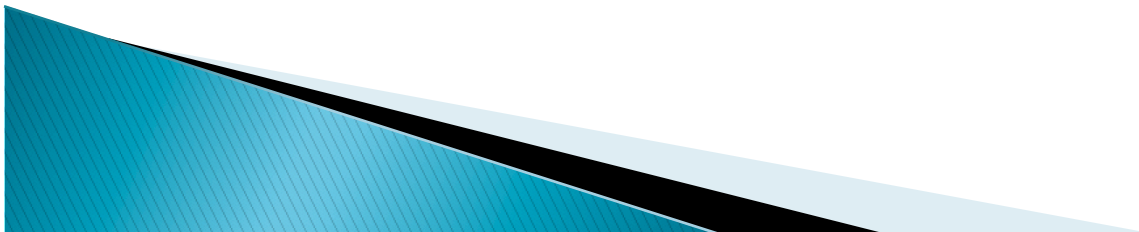
SNMP v2

- A pesar de sus mejoras, no es lo suficientemente seguro
 - Sigue utilizando el esquema de 'comunidades' como único medio de autenticación
 - La version 2c es la mas común



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 relojes 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



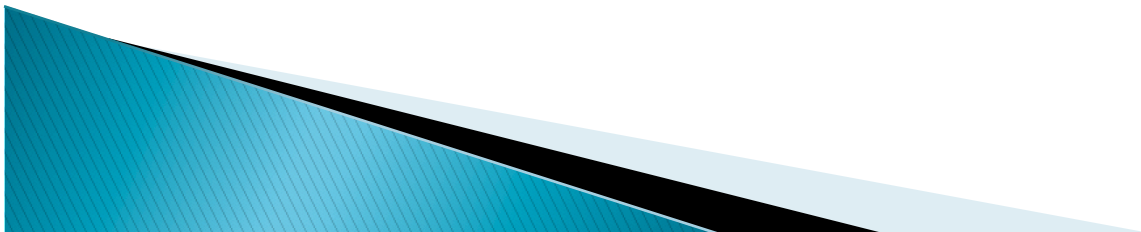
Niveles de Seguridad

- ▶ noAuthNoPriv
 - Sin autenticación, sin privacidad
- ▶ authNoPriv
 - Autenticación, sin privacidad
- ▶ authPriv
 - Autenticación y privacidad



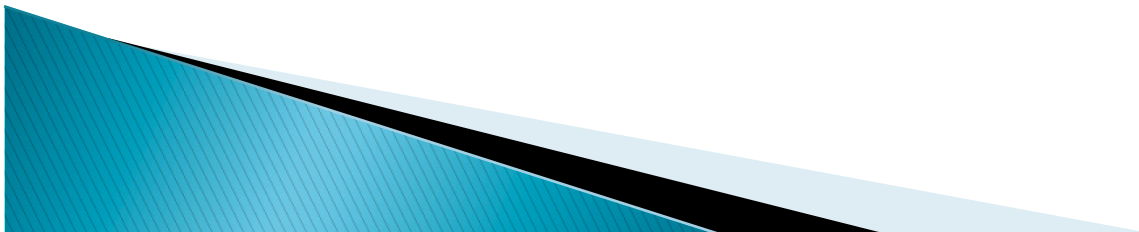
Configurar SNMP v3 en Cisco

- ▶ `snmp-server view vista-ro internet included`
- ▶ `snmp-server group ReadGroup v3 auth read vista-ro`
- ▶ `snmp-server user admin ReadGroup v3 auth md5 xk122r56`
- ▶ *O alternativamente:*
- ▶ `snmp-server user admin ReadGroup v3 auth md5 xk122r56 priv des56 D4sd#rr56`



SNMPv3 con Net-SNMP

- ▶ *apt-get install snmp*
- ▶ *apt-get install snmpd*
- ▶ *net-snmp-config --create-snmpv3-user -a "xk122r56" admin*
- ▶ */usr/sbin/snmpd*
- ▶ *snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A "xk122r56" 127.0.0.1*



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](#)

