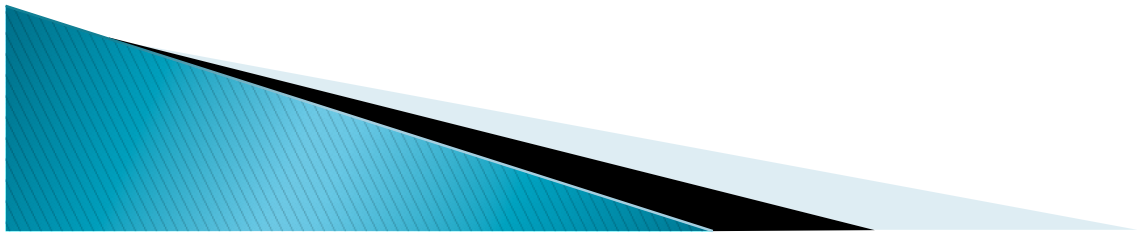
SNMPv3

Carlos Armas
Roundtrip Networks

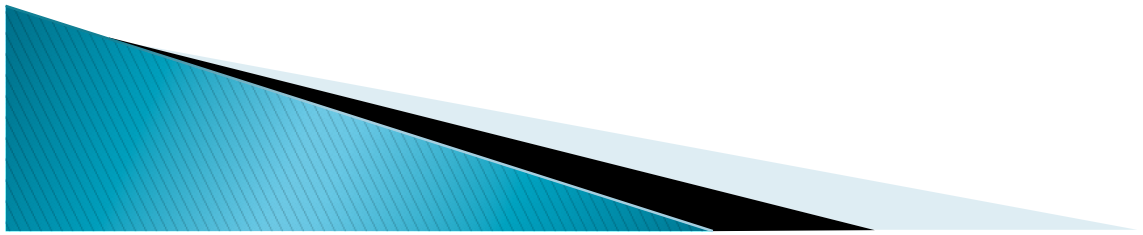
Hervey Allen
NSRC



Necesidad:

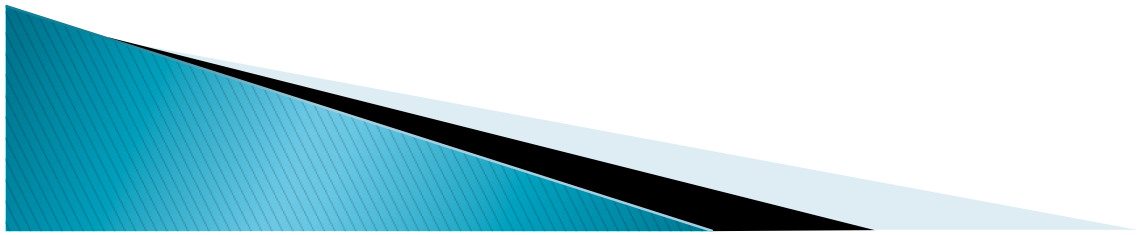
- SNMPversion 1 y 2c son protocols inseguros
- SNMPv3 creado para corregir:

- Componentes:
  - Despachador,
  - Subsistema de Procesamiento de Mensajes
  - Subsistema de Seguridad
  - Subsistema de Control de Acceso



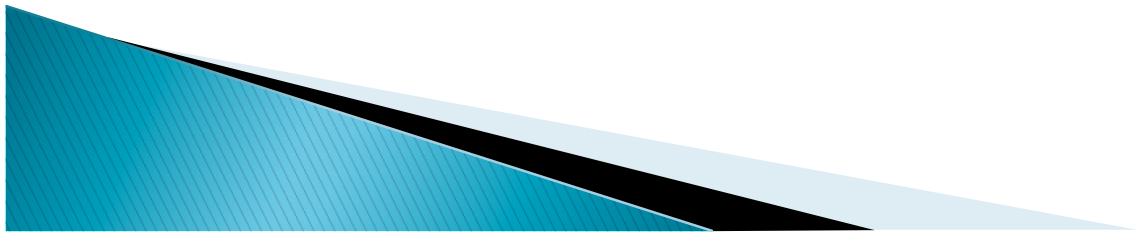
SNMP v3

- El modelo más común es basado en usuarios (User-based Security Model)
  - **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 (solo DES)
  - **Validez temporal**: Utiliza reloj sincronizados, y una ventana de 150 segundos con chequeo de secuencia



Niveles de Seguridad

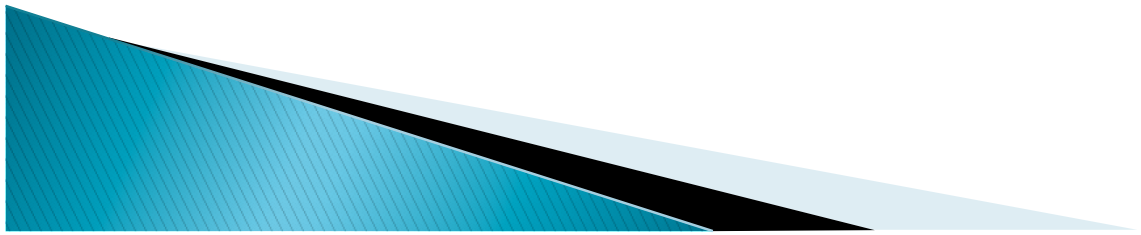
- noAuthNoPriv
  - No autentificación, no privacidad
- authNoPriv
  - Atentificación, no privacidad
- authPriv
  - Autentificación, y privacidad



Cisco SNMPv3 config

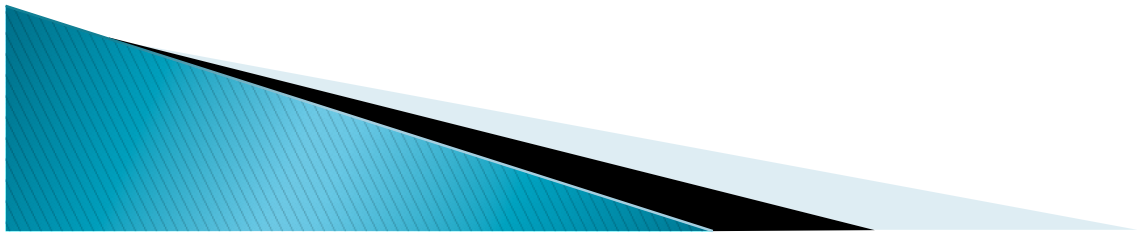
- snmp-server view *vista-ro* internet included
- snmp-server group *ReadGroup* v3 auth read *vista-ro*
- snmp-server user *admin ReadGroup* v3 auth md5 *xk122r56*

- *O alternativamente:*
- snmp-server user *admin ReadGroup* v3 auth *md5 xk122r56* priv des56 *D4sd#rr56*



Net-SNMP SNMPv3 config

- *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

- Essential SNMP (O'Reilly Books) Douglas Mauro, Kevin Schmi