Configuración de dispositivos Cisco

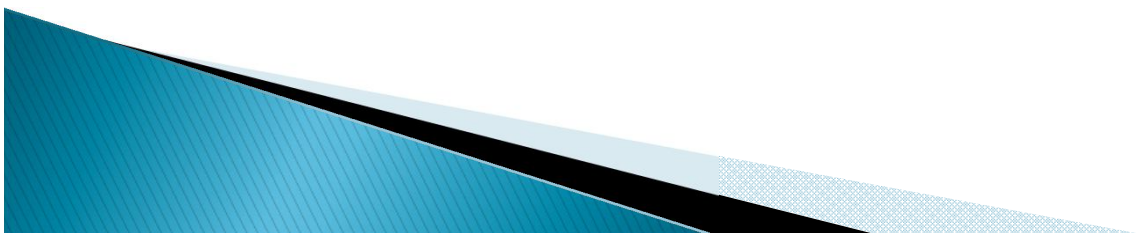
(Para facilitar gerencia de redes)

Carlos Armas
Roundtrip Networks

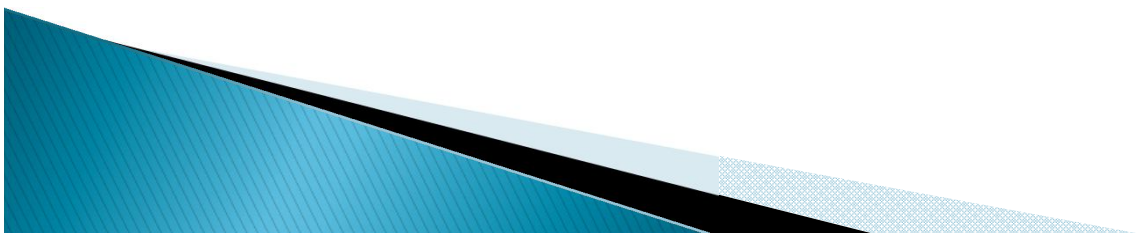
Hervey Allen
NSRC

Areas

- Configuración básica (hostname and DNS)
- Autentificación y autorización (AAA)
- Recolección de logs
- Sincronización (fecha/hora/zona horaria)
- Configuración de SNMP
- Cisco Discovery Protocol



- Configuración básica (hostname and DNS)
  - Asignar nombre
    - rtr(config)# hostname pcx-pc1-rtr.noc.com
  - Asignar dominio
    - rtr(config)# ip domain-name noc.com
  - Asignar server de DNS
    - rtr(config)# ip name-server 192.168.2.20



Autentificación y Autorización

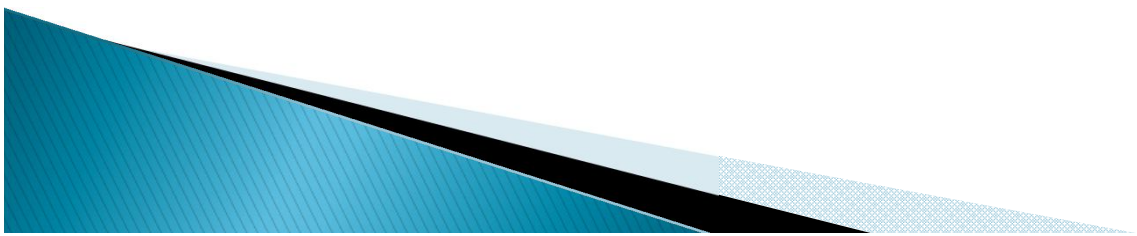
- Configurar passwords de la forma más segura
  - Utilice método mejorado en lugar del tradicional
  - Método mejorado utiliza función hash (MD5)
  - Tradicional:

    enable password 0 wer56$21

    user admin password 0 sdf!231
  - Mejorado

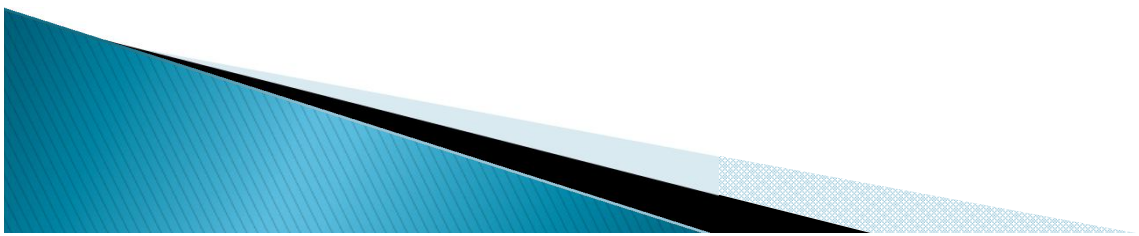
    enable secret 0 wer56$21

    user admin secret 0 sdf!231



Autentificación y Autorización

- Utilice *SSH,* deshabilite *telnet* a menos que no haya opción
- Configuración, con llave de 2048 bytes:
  - *aaa new-model*
  - *ip domain name poneloya.com*
  - *crypto key generate rsa modulus 2048 label router1.poneloya.com*
- Verificar creación de la llave:
  - *show crypto key mypubkey rsa*
- Asignar la llave que SSH va a utilizar:
  - *ip ssh rsa keypair-name router1.poneloya.com*
- Restringir a SSH version 2, y (opcional) registrar eventos:
  - *ip ssh logging events*
  - *ip ssh version 2*



Recolección de trazas (syslog)

- Envie logs al servidor de *syslog:*

  logging host 10.0.0.5

- Identificar que “canal” va a ser utilizado (local0 a local7):

  logging facility local5

  logging userinfo

- Hasta que nivel de prioridad se quiere registrar?

  logging trap <nivel_de_logging>

- **<0-7> nivel de urgencia (mas urgente mientras menor sea el numero)**
-
- debugging Debugging messages (severity=7)
- informational Informational messages (severity=6)
- notifications Normal but significant conditions (severity=5)
- warnings Warning conditions (severity=4)
- errors Error conditions (severity=3)
- critical Critical conditions (severity=2)
- alerts Immediate action needed (severity=1)
- emergencies System is unusable (severity=0)

Sincronización

Es esencial que todos los elementos de la red estén sincronizados en tiempo!

En modo config:

ntp server pool.ntp.org
clock timezone PST -8

Si se observa horario de verano, se puede:

clock summer-time recurring last Sun Mar 2:00 last Sun Oct 3:00

Verificar:

show clock

```
11:20:44.470 CMT Tue Aug 3 2010
```

Show ntp status

```
Clock is synchronized, stratum 3, reference is 4.79.132.217
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**18
reference time is D002CE85.D35E87B9 (11:21:09.825 CMT Tue Aug 3 2010)
clock offset is 2.5939 msec, root delay is 109.73 msec
root dispersion is 39.40 msec, peer dispersion is 2.20 msec
```

Configuración de SNMP

Se recomienda utilizar SNMP version 3:

- Iguales facilidades que la version 2
- pero con protección de acceso y encriptamiento

- Configurar SNMP v3:
  - *snmp-server view <view> <alcance> included*
  - *snmp-server group <group> v3 auth read <view>*
  - *snmp-server user <user> <group> v3 auth <hash> <password> [priv des56 <key>]*

  - Ejemplo:

    Configurar un usuario con acceso total al árbol de SNMP, de solo lectura.

    Password hashed via MD5, (Auth) y sin encriptar la respuesta de SNMP:

    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

Configurar Protocolo de Descubrimiento de Cisco (CDP)

- Habilitado por defecto en estos dias
- Use solamente si se necesita, para habilitar:
  - *cdp enable*
  - O *cdp run* en versiones mas antiguas

- Herramientas para visualizar anuncios de CDP:
  - tcpdump
  - cdpr
  - Wireshark
- Para visualizar en IOS:
  - *show cdp neighbors*