3. Desarrollo y configuración de los sistemas de red

En este capitulo se muestra la configuración de las distintas aplicaciones que serán implementadas en la red Willay Cusco, específicamente en cada RouterBoard 333 y RouterBoard 433. La configuración de estas computadoras embebidas en la red Willay Cusco se puede agrupar según los siguientes grupos,

- Nombre del sistema
- Seguridad WPA/2
- Interfaz inalámbrica
- Nstreme
- VLAN
- Direcciones IP
- Mangle
- NAT
- Tabla de rutas
- OSPF
- MikroTik Neighbour Discovery Protocol
- Network Time Protocol
- SNMP
- Watchdog
- Servicios, Protocolos y Puertos
- Seguridad IP
- QoS
- Adquisición de parámetros en la MikroTik

Nombre del sistema

Aquí se muestra el ejemplo de configuración del nombre del sistema:

```
[admin@MikroTik] /system identity> set name="UGEL Acomayo - Acomayo - Cusco"
```

Para identificar cada computadora embebida con un nombre, se indica el nombre del punto de la red y el municipio donde pertenece (en el ejemplo UGEL Acomayo), seguido por la provincia donde se encuentro el punto, y seguido por el departamento donde se encuentra el punto. En el caso de la red Willay Cusco, la provincia en todos los puntos es Acomayo y el departamento Cusco.

Seguridad WPA/2

Aquí se muestra el ejemplo de configuración de la seguridad WPA/2:

```
[admin@MikroTik] /interface wireless security-profiles> add
name=willay authentication-types=wpa2-psk,wpa-psk eap-
methods=passthrough group-ciphers=aes-ccm mode=dynamic-keys
unicast-ciphers=aes-ccm wpa2-pre-shared-key=XXXXXXXXXXXX wpa-
pre-shared-key=XXXXXXXXXXXX
```

En cada punto de la red se configura la seguridad en la capa de enlace WPA y WPA2. Como no se usan certificaciones TLS para la autentificación, el eap-method se configura como passthrough, lo que significa que se confía el proceso de autentificación en el servidor RADIUS si éste existe. Tanto los datos unicast como broadcast usan el protocolo aes-ccm para encriptar, el cual es mucho más seguro que tkip. El modo en dynamic-keys significa que las claves de encriptación se generan de forma dinámica.

Interfaz inalámbrica

Aquí se muestra el ejemplo de configuración de la interfaz inalámbrica:

```
[admin@MikroTik] /interface wireless> set wlan1 ack-
timeout=dynamic antenna-mode=ant-a band=5ghz basic-rates-
a/g=6Mbps disabled=no disable-running-check=yes frequency=5745
mode=station rate-set=configured security-profile=willay
ssid=WILLAY15 supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps tx-
power=25 tx-power-mode=card-rates
```

La configuración de la interfaz inalámbrica presenta distintos parámetros, uno de ellos el ack-timeout se configura como dynamic, lo que quiere decir que el ack-timeout se calcula de forma dinámica con la distancia. Aunque si se configura Nstreme este parámetro no tiene sentido, es bueno tenerlo como base. El modo de antena se configura como ant-a para anular la diversidad y para que los datos se transmitan y reciban exclusivamente por la salida main de la tarjeta inalámbrica. La banda de frecuencia se configura sólo en 5.8 GHz, puesto que toda la red opera con el estándar IEEE 802.11a. La velocidad de transmisión básica a la que se configuran todos los puntos de la red mediante el parámetro basic-rates-a/g es la mínima de 6 Mbps, eso permite un comportamiento de enganche a velocidades de transmisión más estable. El modo disabled no se activa para que la interfaz inalámbrica esté operativa y sea reconocida por el RouterOS. Activar el parámetro disable-running-check permite que la interfaz inalámbrica siempre se muestre en funcionamiento aunque realmente no lo

esté, esto evita cambios automáticos en la tabla de rutas. La frecuencia asignada a la interfaz inalámbrica es la asociada con uno de los 5 canales distintos usados en 5.8 GHz (149, 153, 157, 161 y 165) según el diseño de cada enlace. En el mode se indica si el punto se trata de un cliente (station) o de un AP (ap-bridge). El rate-set determina qué velocidades de transmisión usar, si está configurado como configured las velocidades de transmisión se obtienen de las basic-rates-a/g y de las supported-rates-a/g. El parámetro security-profile indica qué clase de seguridad se implementa en la capa de enlace, en todos los puntos de la red Willay Cusco se pone el willay que es el nombre de la configuración que se estableció en el apartado anterior. En el ssid se indica el nombre identificador del enlace inalámbrico según los asignados en el diseño de la red, esos toman la forma WILLAY[Número]. El parámetro supported-rates-a/g determina las velocidades de transmisión soportadas en cada uno de los puntos de la red, teniendo como velocidad máxima 18 Mbps. El valor de tx-power sólo tiene sentido si el tx-power-mode es configurado como card-rates o all-rates-fixed, el valor de tx-power es de 25 dBm para todos los puntos de la red excepto los clientes finales y repetidor local dentro de cada municipio, en ellos hay que reducir la potencia de transmisión entre 15 dBm y 20 dBm dada su proximidad. El tx-power-mode se configura en card-rates, eso significa que la potencia asociada a las velocidades de transmisión configuradas es el valor del parámetro tx-power, para el resto de velocidades la potencia de transmisión se calcula mediante un algoritmo propio del RouterOS que toma como parámetro el valor de tx-power.

Nstreme

Aquí se muestra el ejemplo de configuración del protocolo Nstreme:

```
[admin@MikroTik] /interface wireless nstreme> set wlan1 enable-
nstreme=yes enable-polling=no framer-policy=best-fit
```

El protocolo propietario de MikroTik Nstreme se va a activar en todos los enlaces de la red Willay Cusco, tanto los de larga distancia como los de corta distancia. Los de larga distancia para superar las limitaciones que supone el estándar IEEE 802.11 para tales enlaces, y los de corta distancia como los clientes finales dentro de un municipio, porque con Nstreme activado es la única manera que tiene el RouterOS para poder realizar polling (sondeo) y de esta forma superar el problema del nodo oculto, aunque teóricamente el estándar IEEE 802.11 lo soporta intrínsicamente. La configuración que se presenta es la asociada a un AP, cuando se configura un punto en modo cliente

sólo es necesario tener los dos primeros parámetros “set wlanX enable-nstreme=yes”, puesto que el cliente se adapta de forma automática a la configuración del AP. En todos los enlaces punto a punto de la red Willay Cusco no se va a activar el parámetro enable-polling, sólo en el repetidor local de cada municipio sí se va a activar. En los casos que el enable-polling esté activado, es recomendable a la vez desactivar el acceso al medio CSMA/CA mediante el parámetro disable-csma. Se configura como framer-policy el best-fit, aunque teóricamente el modo más óptimo de todos es el exact-size, también es cierto que cuando se fragmentan paquetes y uno de ellos se pierde, el número de paquetes que tienen que ser retransmitidos son todos aquellos que había en la trama, por lo que si hay pérdidas de paquetes el caudal efectivo puede no ser tan óptimo. En cualquier caso, el framer-policy óptimo para la red Willay Cusco tendrá que ser validado mediante pruebas de campo, pudiendo cambiar la configuración de dicho parámetro por defecto aquí expresada.

VLAN

Aquí se muestra el ejemplo de configuración de las VLAN’s:

```
[admin@MikroTik] /interface vlan> add name=public-acomayo vlan-id=1
interface=ether1
[admin@MikroTik] /interface vlan> add name=public-sangarara vlan-id=2
interface=ether1
[admin@MikroTik] /interface vlan> add name=public-pomacanchi vlan-id=3
interface=ether1
```

Las VLAN’s sólo se configuran en el repetidor de la UNSAAC situado en la ciudad de Cusco. Son necesarias para trabajar conjuntamente con el switch y crear dominios de colisión separados dentro del mismo medio físico. Básicamente lo que se indica es el nombre de la VLAN, el identificador lógico mediante el parámetro vlan-id, y la interfaz en la cual se crea. Las tres VLAN’s se crean con identificadores distintos pero compartiendo la misma interfaz.

Direcciones IP

Aquí se muestra el ejemplo de configuración de las direcciones IP:

```
[admin@MikroTik] /ip address> add address=10.10.1.1/24 interface=wlan1
[admin@MikroTik] /ip address> add address=10.10.2.1/24 interface=wlan2
[admin@MikroTik] /interface bridge> add name=br1
[admin@MikroTik] /interface bridge port> add interface=ether2
bridge=br1
```

```
[admin@MikroTik] /interface bridge port> add interface=ether3
bridge=br1
[admin@MikroTik] /ip address> add address=10.10.0.1/24 interface=br1
[admin@MikroTik] /ip address> add address=IP_PUBLIC_ACOMAYO/NETMASK
interface=public-acomayo
[admin@MikroTik] /ip address> add address=IP_PUBLIC_SANGARARA/NETMASK
interface=public-sangarara
[admin@MikroTik] /ip address> add address=IP_PUBLIC_POMACANCHI/NETMASK
interface=public-pomacanchi
```

Siguiendo el apartado VLAN, se comenta la configuración más general posible de las direcciones IP's que corresponde de nuevo al repetidor de la UNSAAC. En el resto de los puntos de la red la configuración es idéntica con sus respectivas IP's y sin hacer uso de las interfaces VLAN's. Para añadir una dirección IP sólo hace falta introducirla según el parámetro address e indicar a qué interfaz está asociada, también es necesario indicar qué máscara de red se usa. Los puertos ethernet que no se usan de forma activa, se agrupan mediante una interfaz puente (bridge). Para ello primero se añaden las interfaces físicas a la interfaz bridge, y posteriormente se añade una IP de la misma manera que se ha comentado anteriormente pero asociada a la interfaz bridge. Para añadir las IP's a las interfaces VLAN's creadas en el apartado anterior, se sigue el mismo procedimiento de forma equivalente.

Mangle

Aquí se muestra el ejemplo de configuración de mangle:

```
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 action=accept chain=prerouting

[admin@MikroTik] /ip firewall mangle> add src-address=10.11.0.0/20
action=mark-routing new-routing-mark=internet-upload-acomayo
chain=prerouting passthrough=no
[admin@MikroTik] /ip firewall mangle> add src-address=10.11.16.0/20
action=mark-routing new-routing-mark=internet-upload-sangarara
chain=prerouting passthrough=no
[admin@MikroTik] /ip firewall mangle> add src-address=10.11.32.0/20
action=mark-routing new-routing-mark=internet-upload-pomacanchi
chain=prerouting passthrough=no

[admin@MikroTik] /ip firewall mangle> add dst-address=10.11.0.0/20
protocol=ipsec-esp action=mark-packet new-packet-mark=internet-
download-acomayo chain=postrouting passthrough=no
[admin@MikroTik] /ip firewall mangle> add dst-address=10.11.16.0/20
protocol=ipsec-esp action=mark-packet new-packet-mark=internet-
download-sangarara chain=postrouting passthrough=no
[admin@MikroTik] /ip firewall mangle> add dst-address=10.11.32.0/20
protocol=ipsec-esp action=mark-packet new-packet-mark=internet-
download-pomacanchi chain=postrouting passthrough=no
```

```
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dscp=46 action=mark-connection new-connection-
mark=voice-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add connection-mark=voice-con
action=mark-packet new-packet-mark=voice chain=postrouting
passthrough=no

[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=22 protocol=tcp action=mark-connection
new-connection-mark=ssh-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=22 protocol=udp action=mark-connection
new-connection-mark=ssh-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add connection-mark=ssh-con
action=mark-packet new-packet-mark=dedicated-traffic chain=postrouting
passthrough=no
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=21 protocol=tcp action=mark-connection
new-connection-mark=ftp-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=21 protocol=udp action=mark-connection
new-connection-mark=ftp-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=20 protocol=tcp action=mark-connection
new-connection-mark=ftp-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=20 protocol=udp action=mark-connection
new-connection-mark=ftp-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add connection-mark=ftp-con
action=mark-packet new-packet-mark=dedicated-traffic chain=postrouting
passthrough=no
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=25 protocol=tcp action=mark-connection
new-connection-mark=mail-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 dst-port=25 protocol=udp action=mark-connection
new-connection-mark=mail-con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add connection-mark=mail-con
action=mark-packet new-packet-mark=dedicated-traffic chain=postrouting
passthrough=no

[admin@MikroTik] /ip firewall mangle> add src-address=10.0.0.0/8 dst-
address=10.0.0.0/8 action=mark-connection new-connection-mark=traffic-
con chain=postrouting
[admin@MikroTik] /ip firewall mangle> add connection-mark=traffic-con
action=mark-packet new-packet-mark=other-traffic chain=postrouting
passthrough=no
```

Todos los puntos de la red excepto los clientes finales en cada municipio tienen configurado el marcado de paquetes. De ellos, el repetidor de la UNSAAC tiene toda la configuración completa (configuración marcada en gris inclusive), y el resto de puntos comparten la misma configuración (configuración no marcada en gris).

El repetidor de la UNSAAC añade unas reglas para diferenciar el tráfico con origen y destino dentro de la misma red Willay Cusco, del tráfico originado en cada uno de los distintos municipios pero con destino fuera de dicha red para poder enrutarlo al enrutador comercial correspondiente. Ello se consigue mediante la asignación de la

etiqueta routing-mark, para su uso en el enrutamiento a través del uso de múltiples tablas de rutas. Como todo ese proceso de diferenciación de paquetes está orientado al enrutamiento, la cadena donde toma lugar es la prerouting.
El resto de configuración común a todos los puntos con mangle, asigna etiquetas a los paquetes para diferenciarlos entre el tipo de tráfico de voz, internet, tráfico dedicado (ftp, correo electrónico, ssh) y otro tráfico para el filtrado que se da en la QoS. Todo este proceso se da en la cadena postrouting para etiquetar tanto los paquetes que están de paso por el punto de red, como los que origina el mismo punto de red. En los tráficos donde se pueden identificar nuevas conexiones TCP, se usa dos tipos de marcado de paquetes, primero se identifica cuando existe una conexión nueva mediante el connection-mark, y todos los paquetes dentro de la misma conexión se marcan con el packet-mark, de esta forma se ahorra bastante carga de procesamiento de la CPU. El packet-mark es la etiqueta que se usa en la QoS para filtrar los distintos tráficos. En el caso del uso de IPSec, como la trama TCP queda encapsulada es imposible determinar si existe o no una nueva conexión en un paquete hasta que éste no es desencriptado, por lo que directamente se marca con la etiqueta packet-mark.

NAT

Aquí se muestra el ejemplo de configuración de NAT:

```
[admin@MikroTik] /ip firewall nat> add action=masquerade out-
interface=public-acomayo chain=srcnat
[admin@MikroTik] /ip firewall nat> add action=masquerade out-
interface=public-sangarara chain=srcnat
[admin@MikroTik] /ip firewall nat> add action=masquerade out-
interface=public-pomacanchi chain=srcnat
```

El NAT sólo se configura en el repetidor de la UNSAAC. La acción masquerade indica que sólo se traduce la IP del paquete por la IP de la interfaz por donde se ha decidido en la tabla de rutas que va a salir. La cadena donde se da el proceso es la srcnat. En el caso de la red Willay Cusco al haber tres conexiones de acceso a Internet independientes, hay que realizar un NAT por cada municipio distinto.

Tabla de rutas

Aquí se muestra el ejemplo de configuración de tabla de rutas:

```
[admin@MikroTik] /ip route> add dst-address=10.10.21.0/24
gateway=10.10.0.2
```

```
[admin@MikroTik] /ip route> add dst-address=10.10.22.0/24
gateway=10.10.0.2
[admin@MikroTik] /ip route> add dst-address=10.10.23.0/24
gateway=10.10.0.2
[admin@MikroTik] /ip route> add gateway=IP_PUBLIC_ROUTER_ACOMAYO
routing-mark=internet-upload-acomayo
[admin@MikroTik] /ip route> add gateway=IP_PUBLIC_ROUTER_SANGARARA
routing-mark=internet-upload-sangarara
[admin@MikroTik] /ip route> add gateway=IP_PUBLIC_ROUTER_POMACANCHI
routing-mark=internet-upload-pomacanchi
```

Para introducir la dirección de red en la tabla de rutas se realiza mediante el parámetro dst-address con su respectiva máscara de red e indicando el gateway hacia donde se va a mandar el paquete con el parámetro gateway. En el caso del repetidor de la UNSAAC, se usan múltiples tablas de rutas con la etiqueta routing-mark para enrutar hacia el correspondiente enrutador comercial los paquetes destinados fuera de la red Willay Cusco y provenientes de cada municipio distinto. En el resto de puntos de la red para configurar el gateway por defecto, sólo hace falta introducir su dirección IP con el parámetro gateway.

OSPF

Aquí se muestra el ejemplo de configuración del OSPF:

```
[admin@MikroTik] /routing ospf> set router-id=1.1.1.1
[admin@MikroTik] /routing ospf> set redistribute-static=as-type-1
[admin@MikroTik] /routing ospf> set distribute-default=if-installed-
as-type-1
[admin@MikroTik] /routing ospf network> add network=10.10.1.0/24
area=backbone
[admin@MikroTik] /routing ospf network> add network=10.10.2.0/24
area=backbone
[admin@MikroTik] /routing ospf network> add network=10.10.0.0/24
area=backbone
[admin@MikroTik] /routing ospf interface> add interface=wlan1 cost=100
authentication=md5 authentication-key=XXXXXXXXXXXXXX authentication-
key-id=0
[admin@MikroTik] /routing ospf interface> add interface=wlan2
authentication=md5 authentication-key= XXXXXXXXXXXXXX authentication-
key-id=0
```

En la configuración del protocolo de enrutamiento dinámico OSPF, a cada punto de la red se le asigna una prioridad mediante el parámetro router-id para poder crear adyacencias correctamente. La siguiente es la lista de equivalencias entre router-id y puntos de la red,

Punto de la red	Router-id
Repetidor de la UNSAAC	1.1.1.1
Repetidor Josjojahuarina 1 (1)	1.1.1.2
Repetidor Josjojahuarina 1 (2)	1.1.1.3
Repetidor Don Juan (1)	1.1.1.4
Repetidor Don Juan (2)	1.1.1.5
Repetidor Pomacanchi	1.1.1.6
Repetidor Laykatuyoc (1)	1.1.1.7
Repetidor Laykatuyoc (2)	1.1.1.8
Repetidor Huáscar	1.1.1.9

Tabla 3.1: Asignación del router-id a los repetidores de la red troncal

Todas las rutas estáticas se redistribuyen como “tipo 1”, y en el caso del repetidor de la UNSAAC los gateways por defecto se configuran como “tipo 1 si instalado”. En todos los segmentos de red donde corre OSPF hay que añadir sus direcciones de red al área backbone. Para añadir autentificación en los mensajes se usa md5, y mediante el parámetro authentication-key-id se indica con qué entero está asociada la clave usada, facilitando de esta forma la posible migración de claves. Con el parámetro cost se le asigna un coste determinado (100 puesto que el coste asignado por defecto es 10), para determinar por donde se van a recibir los datos en los dobles enlaces.

MikroTik Neighbour Discovery Protocol

Aquí se muestra el ejemplo de configuración del MNDP:

```
[admin@MikroTik] /ip neighbor discovery> set ether1 discover=no
[admin@MikroTik] /ip neighbor discovery> set ether2 discover=no
[admin@MikroTik] /ip neighbor discovery> set ether3 discover=no
[admin@MikroTik] /ip neighbor discovery> set br1 discover=no
[admin@MikroTik] /ip neighbor discovery> set wlan1 discover=yes
[admin@MikroTik] /ip neighbor discovery> set wlan2 discover=yes
```

Para la gestión de red, la información necesaria de los vecinos dentro del mismo segmento de red es únicamente la de las interfaces inalámbricas, por lo que mediante el parámetro discover se activan dichas interfaces y se desactivan el resto.

Network Time Protocol

Aquí se muestra el ejemplo de configuración del NTP:

```
[admin@MikroTik] /system clock> set time-zone-name=America/Lima
[admin@MikroTik] /system ntp server> set enabled=yes manycast=no
[admin@MikroTik] /system ntp client> set enabled=yes primary-
ntp=IP_PUBLIC_NTP_SERVER1 secondary-ntp=IP_PUBLIC_NTP_SERVER2
```

La sincronización de todos los puntos de la red se realiza a través de servidores públicos NTP. Se configura el parámetro time-zone-name en donde se encuentran los puntos para tener asignada la diferencia horaria adecuada según el GMT. El repetidor de la UNSAAC hace a la vez de cliente de los servidores públicos primarios y secundarios NTP, y de servidor primario para el resto de puntos de la red Willay Cusco con la IP asociada a la interfaz bridge. El repetidor local dentro de cada municipio también realiza a la vez el papel de cliente y servidor primario, cliente del servidor repetidor de la UNSAAC y servidor primario con la IP asociada a la interfaz bridge para los clientes finales dentro del municipio. En los clientes finales dentro de cada municipio, sólo se configura como cliente del repetidor local del mismo municipio. En los puntos de la red que hacen el papel de servidor, sólo se aceptan tramas unicast por lo que mediante el parámetro manycast se desactivan esos mismos tipos de trama, y por lo tanto también hay que comprobar que en cada cliente el modo de funcionamiento sea unicast.

SNMP

Aquí se muestra el ejemplo de configuración del SNMP:

```
[admin@MikroTik] /snmp> set enabled=yes
[admin@MikroTik] /snmp community> set public name=willay-cusco
address=10.0.0.0/8
```

En todos los puntos de la red Willay Cusco se activa el protocolo SNMP para que el RouterOS funcione como agente para obtener los datos solicitados, ello se configura activando el parámetro enabled. A la vez se cambia el nombre de la comunidad que viene por defecto (public) por el nombre willay-cusco, y se restringe la obtención de datos a puntos que tengan su IP dentro de la dirección de red 10.0.0.0/8.

Watchdog

Aquí se muestra el ejemplo de configuración del watchdog:

```
[admin@MikroTik] /system watchdog> set automatic-supout=no
```

Cada vez que el RouterOS de MikroTik realiza un reinicio inesperado, se guarda un archivo de soporte como medida de seguridad. Para evitar que el disco duro se pueda

llegar a llenar innecesariamente de estos archivos, se desactiva la opción mediante el parámetro automatic-supout.

Servicios, Protocolos y Puertos

Aquí se muestra el ejemplo de configuración de los servicios, protocolos y puertos:

```
[admin@MikroTik] /ip service> disable telnet
[admin@MikroTik] /ip service> disable ftp
[admin@MikroTik] /ip service> disable www
[admin@MikroTik] /ip service> set ftp address=10.0.0.0/8
[admin@MikroTik] /ip service> set ssh address=10.0.0.0/8
[admin@MikroTik] /ip service> set winbox address=10.0.0.0/8
```

Existen ciertos servicios que por seguridad es conveniente desactivar en la red Willay Cusco, por ejemplo telnet, ftp y www. En el caso del ftp, normalmente no se hará uso de este servicio, pero cuando se deba actualizar la versión del RouterOS primero se deberá acceder como root en la máquina y activar el servicio. También se restringe el acceso a los servicios ftp, ssh y winbox a puntos que tengan su IP dentro de la dirección de red 10.0.0.0/8.

Seguridad IP

Aquí se muestra el ejemplo de configuración de seguridad IP:

```
[admin@MikroTik] /ip ipsec proposal> set default enc-algorithms=aes-
128

[admin@MikroTik] /ip ipsec policy> add action=none src-
address=10.11.2.3/32:any dst-address=10.0.0.0/8:any
[admin@MikroTik] /ip ipsec policy> add action=encrypt src-
address=10.11.2.3/32:any sa-src-address=10.11.2.1 sa-dst-
address=10.10.0.1 tunnel=yes
[admin@MikroTik] /ip ipsec peer> add address=10.10.0.1/32:500
secret=XXXXXXXXXXXXXX enc-algorithm=aes-128 hash-algorithm=sha1
```

En los clientes finales dentro de cada municipio con acceso a Internet, se crea un túnel IPSec hasta el repetidor de la UNSAAC. Para ello el cliente final usa como nueva IP de origen la de la interfaz bridge de su placa MikroTik, y como nueva IP de destino la de la interfaz bridge de la placa MikroTik en el repetidor de la UNSAAC. Primeramente se configura el algoritmo de encriptación usado en la fase 1, se elige AES-128 que es mucho más rápido que el 3DES y aunque no es tan fuerte como el AES-192 y AES-256 sí es mucho más rápido que ellos también. Sólo se encriptan los datos hacia

Internet, por lo que los datos con destino hacia la dirección de red de la red Willay Cusco no se toma ninguna acción. El resto de datos sí se encriptan con las nuevas IP's de origen y destino comentadas con anterioridad en cada caso, y las nuevas IP's asignadas del nuevo datagrama IP quedan identificadas bajo el parámetro sa-src-address y sa-dst-address en la "policy". Como el modo de funcionamiento IPSec utilizado es en modo túnel, debe activarse el parámetro tunnel. En el "peer", se configura la IP del otro lado del túnel y el puerto que se va a usar para la negociación de las asociaciones de seguridad (SA's) que en todos los casos es el 500, se introduce la clave usada mediante el parámetro secret, y para la fase 2 se establece el uso del algoritmo de encriptación AES-128 y el uso del algoritmo de hash sha1 que es más fuerte que el md5.

QoS

Aquí se muestra el ejemplo de configuración de QoS:

```
[admin@MikroTik] /queue type> add name=pcq-internet-download-acomayo
kind=pcq pcq-classifier=dst-address
[admin@MikroTik] /queue tree> add name=queue-internet-download-acomayo
parent=wlan2 queue=pcq-internet-download-acomayo packet-mark=internet-
download-acomayo limit-at=524288 max-limit=524288 priority=2
[admin@MikroTik] /queue tree> add name=queue-internet-download-acomayo
parent=wlan1 queue=pcq-internet-download-acomayo packet-mark=internet-
download-acomayo-backup limit-at=524288 max-limit=524288 priority=2

[admin@MikroTik] /queue type> add name=sfq-voice kind=sfq
[admin@MikroTik] /queue tree> add name=queue-voice-download
parent=wlan2 queue=sfq-voice packet-mark=voice limit-at=655360 max-
limit=655360 priority=1
[admin@MikroTik] /queue tree> add name=queue-voice-download-backup
parent=wlan1 queue=sfq-voice packet-mark=voice limit-at=655360 max-
limit=655360 priority=1

[admin@MikroTik] /queue type> add name=sfq-dedicated-traffic kind=sfq
[admin@MikroTik] /queue tree> add name=queue-dedicated-traffic-
download parent=wlan2 queue=sfq-dedicated-traffic packet-
mark=dedicated-traffic limit-at=393216 max-limit=393216 priority=2
[admin@MikroTik] /queue tree> add name=queue-dedicated-traffic-
download-backup parent=wlan1 queue=sfq-dedicated-traffic packet-
mark=dedicated-traffic limit-at=393216 max-limit=393216 priority=2

[admin@MikroTik] /queue type> add name=sfq-other-traffic kind=sfq
[admin@MikroTik] /queue tree> add name=queue-other-traffic-download
parent=wlan2 queue=sfq-other-traffic packet-mark=other-traffic limit-
at=393216 max-limit=4294967295 priority=3
[admin@MikroTik] /queue tree> add name=queue-other-traffic-download-
backup parent=wlan1 queue=sfq-other-traffic packet-mark=other-traffic
limit-at=393216 max-limit=4294967295 priority=3
```

Todos los puntos de la red excepto los clientes finales en cada municipio tienen configurado la QoS. Tantos los tráficos de bajada (download) como de súbida (upload)

de Internet usan un tipo de cola pcq que se define mediante el parámetro kind, y según el pcq-classifier se decide según qué criterio se clasifican las subcolas dentro de la cola pcq, en el caso del tráfico upload es mediante src-address y en el tráfico download es mediante dst-address para ecualizar el uso del ancho de banda. En el apartado “tree” se elige con el parámetro parent, la cola padre a la que va asociada la cola previamente creada y elegida mediante el parámetro queue. También se configura la prioridad de dicho tráfico mediante el parámetro priority, siendo la máxima prioridad 1 y la mínima 8. El ancho de banda asignado a cada tráfico se configura mediante el parámetro limit-at, que coincide por las razones que se comentaron en el diseño con el parámetro max-limit, la unidad que se toma para el tráfico de bajada de Internet es 512 Kbps, lo que en realidad es 512 bps x 1024 = 524288 bps. Lo mismo pasa para el tráfico de subida de Internet, 128 Kbps = 128 bps x 1024 = 131072 bps. En el resto de tráficos la configuración es similar, con la única diferencia que en todos ellos se usa el tipo de cola sfq y distintas prioridades. Todos los valores que aparecen de asignación de ancho de banda son múltiples de los 128 Kbps = 131072 bps, puesto que tanto el tráfico de voz, tráfico dedicado y otro tráfico se ha asignado dicho valor. Para asignar el ancho de banda necesario a un punto de la red, se necesita ver cuantos flujos distintos del mismo tráfico pasan a través, y multiplicar por el valor anterior. El hecho que en el otro tráfico los valores de los parámetros limit-at y max-limit sean distintos, también está comentado en el diseño de la red Willay Cusco.

Scripts en la MikroTik

Aquí se muestran los scripts implementados dentro del RouterOS de cada computadora embebida RouterBOARD 333 y 433 de la red Willay Cusco, para recopilar ciertos parámetros necesarios para el sistema de monitoreo de datos de la red.

```
[admin@MikroTik] /user group> add name=ssh-login
policy=read,write,ssh,test,policy
[admin@MikroTik] /user> add name=admin-ssh group=ssh-login
[admin@MikroTik] /user ssh-keys> import file=id_dsa.pub user=admin-ssh
[admin@MikroTik] /user group> add name=bwtest-login policy=test,winbox
[admin@MikroTik] /user> add name=admin-bwtest group=bwtest-login

[admin-bwtest@MikroTik] > password

sshtest

[admin-bwtest@MikroTik] > password

bwtest
```

Script reinicio automático

```
[admin@MikroTik] /system script> add name=reboot source={:if ([/system
resource get uptime] >= 1w) do={/system reboot}}

[admin@MikroTik] /system scheduler> add name=automatic-reboot on-
event=reboot start-time=01:30:00 interval=24h
```

Script carga de procesamiento de la CPU

```
[admin@MikroTik] /system script> add name=cpuload source={
:global cpuarray;
:global highavgcpuload;
:global avgcpuload 0;
:local cpuload 0;
:local arraylen 0;
:local arraypos 0;
:local arraytot 0;
:local arraysize 20;

:set cpuload [/system resource get cpu-load];
:set cpuarray ([:toarray $cpuload] + $cpuarray);
:set cpuarray [:pick $cpuarray 0 $arraysize];

:set arraypos 0;
:set arraylen [:len $cpuarray];
:while ($arraypos < $arraylen) do={
:set arraytot ($arraytot + [:pick $cpuarray $arraypos]);
:set arraypos ($arraypos +1 )};

:set avgcpuload ($arraytot / [:len $cpuarray]);
:if ([:len $highavgcpuload] = 0) do={:set highavgcpuload $avgcpuload};
:if ($avgcpuload > $highavgcpuload) do={:set highavgcpuload
$avgcpuload}}

[admin@MikroTik] /system scheduler> add name=automatic-cpuload on-
event=cpuload start-time=startup interval=1s
```

Script testeo automático de ancho de banda

```
[admin@MikroTik] /system script> add name=bwtest source={
:global ipserver1 "";
:global ipserver2 "";
:global ipserver3 "";
:global ipclient1 "";
:global ipclient2 "";
:global ipclient3 "";
:global rxtotalavg1 0;
:global txtotalavg1 0;
:global rxtotalavg2 0;
:global txtotalavg2 0;
:global rxtotalavg3 0;
:global txtotalavg3 0;
:global rx10secondavg1 0;
:global tx10secondavg1 0;
```

```
:global rx10secondavg2 0;
:global tx10secondavg2 0;
:global rx10secondavg3 0;
:global tx10secondavg3 0;
:local durationtest 60;
:local remoteudptxsize 1500;
:local localudptxsize 1500;
:local loginuser admin-bwtest;
:local loginpass bwtest;

:foreach j in=[/ip address find] do={
      :local ipadd [/ip address get $j address];
      :local posadd [:find $ipadd /];
      :set ipadd [:pick $ipadd 0 $posadd];

      :set posadd [:find $ipadd .];
      :local firstadd [:pick $ipadd 0 $posadd];

      :local substradd [:pick $ipadd ($posadd + 1) [:len $ipadd]];
      :set posadd [:find $substradd .];
      :local secondadd [:pick $substradd 0 $posadd];

      :set substradd [:pick $substradd ($posadd + 1) [:len
$substradd]];
      :set posadd [:find $substradd .];
      :local thirdadd [:pick $substradd 0 $posadd];

      :set substradd [:pick $substradd ($posadd + 1) [:len
$substradd]];
      :local fouradd $substradd;

      :local minfourneigh 255;
      :local minipneigh;

      :foreach i in=[/ip neighbor find] do={
            :local ipneigh [/ip neighbor get $i address];
            :local posneigh [:find $ipneigh .];
            :local firstneigh [:pick $ipneigh 0 $posneigh];

            :local substrneigh [:pick $ipneigh ($posneigh + 1) [:len
$ipneigh]];
            :set posneigh [:find $substrneigh .];
            :local secondneigh [:pick $substrneigh 0 $posneigh];

            :set substrneigh [:pick $substrneigh ($posneigh + 1) [:len
$substrneigh]];
            :set posneigh [:find $substrneigh .];
            :local thirdneigh [:pick $substrneigh 0 $posneigh];

            :set substrneigh [:pick $substrneigh ($posneigh + 1) [:len
$substrneigh]];
            :local fourneigh $substrneigh;

            :if (($firstneigh = $firstadd) && ($secondneigh =
$secondadd) &&
            ($thirdneigh = $thirdadd)) do={
                  :if ($fourneigh < $minfourneigh) do={
                        :set minfourneigh $fourneigh;
                        :set minipneigh $ipneigh;
                  }
            }
```

```
      };

      :if ($fouradd > $minfourneigh) do={
            :if (($ipserver1 = "") && ($ipserver2 = "") && ($ipserver3
= "")) do={
                  :set ipserver1 $minipneigh;
                  :set ipclient1 $ipadd;
            };
            :if (($ipserver1 != $minipneigh) && ($ipserver2 = "") &&
($ipserver3 = ""))
            do={
                  :set ipserver2 $minipneigh;
                  :set ipclient2 $ipadd;
            };
            :if (($ipserver1 != $minipneigh) && ($ipserver2 !=
$minipneigh) &&
            ($ipserver3 = "")) do={
                  :set ipserver3 $minipneigh;
                  :set ipclient3 $ipadd;
            }
      }
};

:if ($ipserver1 != "") do={
/tool bandwidth-test $ipserver1 direction=both user=$loginuser
password=$loginpass local-udp-tx-size=$localudptxsize remote-udp-tx-
size=$remoteudptxsize duration=$durationtest do={:set rxtotalavg1
$"rx-total-average"; :set rx10secondavg1 $"rx-10-second-average"; :set
txtotalavg1 $"tx-total-average"; :set tx10secondavg1 $"tx-10-second-
average"}};

:if ($ipserver2 != "") do={
/tool bandwidth-test $ipserver2 direction=both user=$loginuser
password=$loginpass local-udp-tx-size=$localudptxsize remote-udp-tx-
size=$remoteudptxsize duration=$durationtest do={:set rxtotalavg2
$"rx-total-average"; :set rx10secondavg2 $"rx-10-second-average"; :set
txtotalavg2 $"tx-total-average"; :set tx10secondavg2 $"tx-10-second-
average"}};

:if ($ipserver3 != "") do={
/tool bandwidth-test $ipserver3 direction=both user=$loginuser
password=$loginpass local-udp-tx-size=$localudptxsize remote-udp-tx-
size=$remoteudptxsize duration=$durationtest do={:set rxtotalavg3
$"rx-total-average"; :set rx10secondavg3 $"rx-10-second-average"; :set
txtotalavg3 $"tx-total-average"; :set tx10secondavg3 $"tx-10-second-
average"}}

[admin@MikroTik] /system scheduler> add name=automatic-bwtest on-
event=bwtest start-time=03:30:00 interval=24h
```

En todos los puntos de la red, aparte del usuario root se crean dos usuarios adicionales llamados admin-ssh y admin-bwtest para la gestión de la red Willay Cusco. Ambos usuarios tienen privilegios limitados para aumentar la seguridad cuando accedan al RouterOS, el usuario admin-ssh ingresa al sistema con una clave privada dsa, sólo tiene privilegios de lectura (read), ssh, testeo (test), escritura (write), política

(policy), y se le cambia la clave de usuario a “sshtest”; el usuario admin-bwtest sólo tiene privilegios de test, winbox y se le cambia la clave de usuario a “bwtest”.

Se configuran tres scripts propios del RouterOS a cada punto de la red, el primero tiene la función de reiniciar la placa MikroTik si ésta lleva más de una semana funcionando, y se programa para que se ejecute a las 01:30 h exactamente mediante el programador de tareas.

El segundo script lo que hace es obtener la media y el valor máximo de todas las medias de la carga de procesamiento del CPU. Los valores son muestreados mediante el programador de tareas cada 1 s, y se guardan en un vector de tamaño 20 unidades.

El tercer script realiza de forma automática los testeos de ancho de banda mediante la herramienta testeo de ancho de banda del RouterOS. A través de las IP’s de los vecinos en un segmento de red obtenidas mediante el MNDP, se comparan con las locales estableciendo que el de la IP mayor (192.168.1.2 es mayor que 192.168.1.1) hace el papel de cliente y el de la menor de servidor. Por defecto la herramienta usa una arquitectura cliente – servidor, en la que el servidor acepta conexiones con autentificación previa mediante el terminal propio del RouterOS winbox. El testeo que se realiza es mediante tráfico UDP, en ambos sentidos (transmisión y recepción), y su duración es de 60 segundos. Al finalizar se actualizan unas variables globales dentro del RouterOS que determinan para cada enlace inalámbrico el ancho de banda total medido y el ancho de banda total medido en los 10 últimos segundos de prueba. Esas variables son accedidas mediante el usuario ssh ubicado en el script willay.sh para obtener sus valores, lo mismo que ocurre en el segundo script comentado anteriormente. Con el programador de tareas se programa para que el script se ejecute de forma diaria a las 03:30 h.

Como apunte adicional comentar que por defecto el servidor acepta un máximo de 10 conexiones para el testeo de ancho de banda, y esa es la configuración que se implementa, por lo que hay que tener en cuenta si en un futuro algún municipio llegara a tener más de 10 clientes finales se tendría que cambiar la configuración por defecto.