TITANIA®

NETWORKS LTD

QoS OtA

Quality of Service Over the Air

Introducción a la Calidad de Servicio sobre el aire

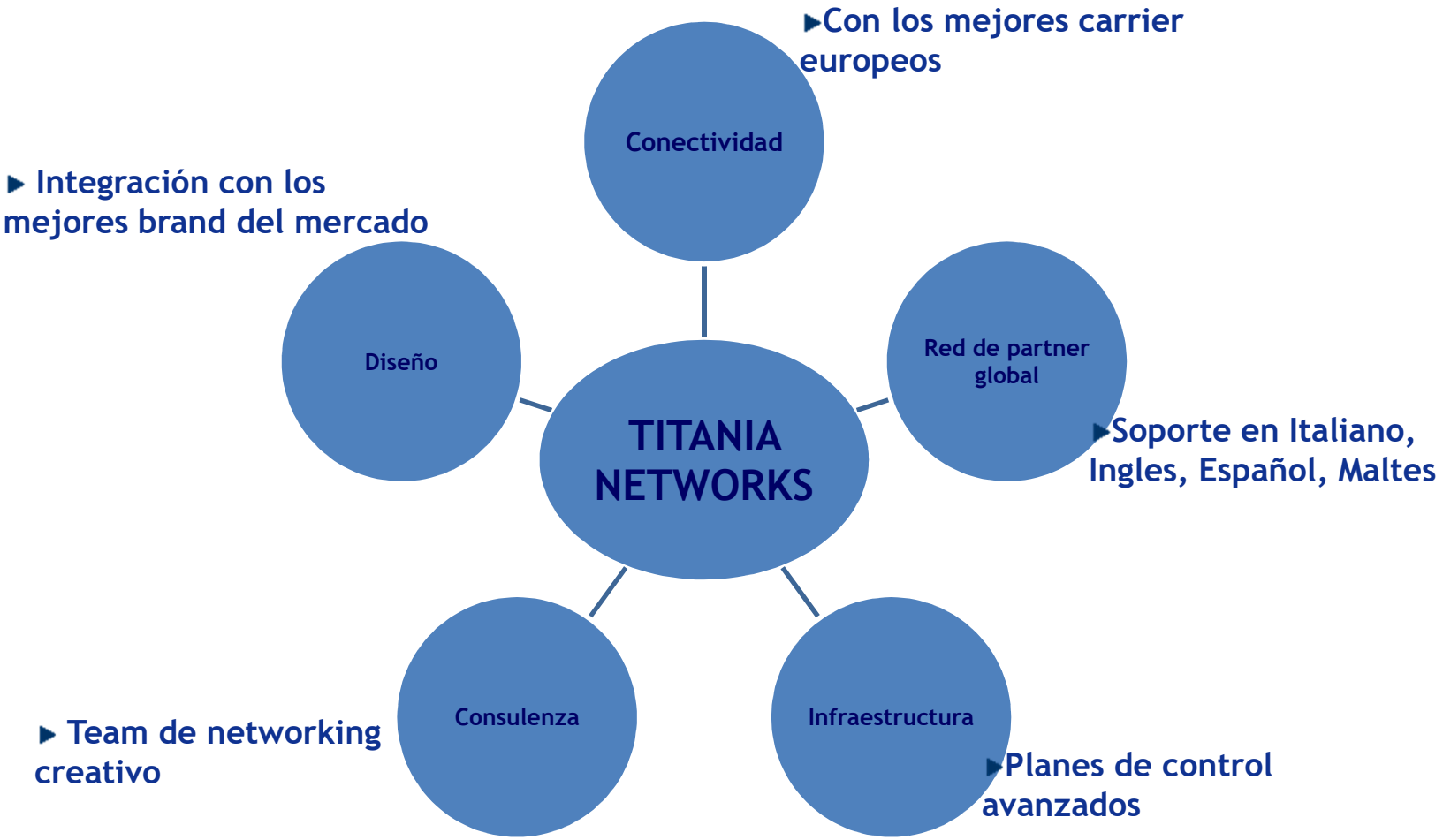
Alfredo Giordano

- Trainer Certificado MikroTik.
- Consulente certificado para MikroTik, Cisco, Ubi*** especializado en el desarollo de ISP y WISP.
- Proporcionando soluciones con MikroTik desde el 2006.
- Trabajando en telecomunicaciones desde el 2001.
- Administrador de varios LIR
- Graduado en Ingenieria Electronica en el Politecnico de Torino, ITA y universidad de Illinois en Chicago, USA.

Titania Networks

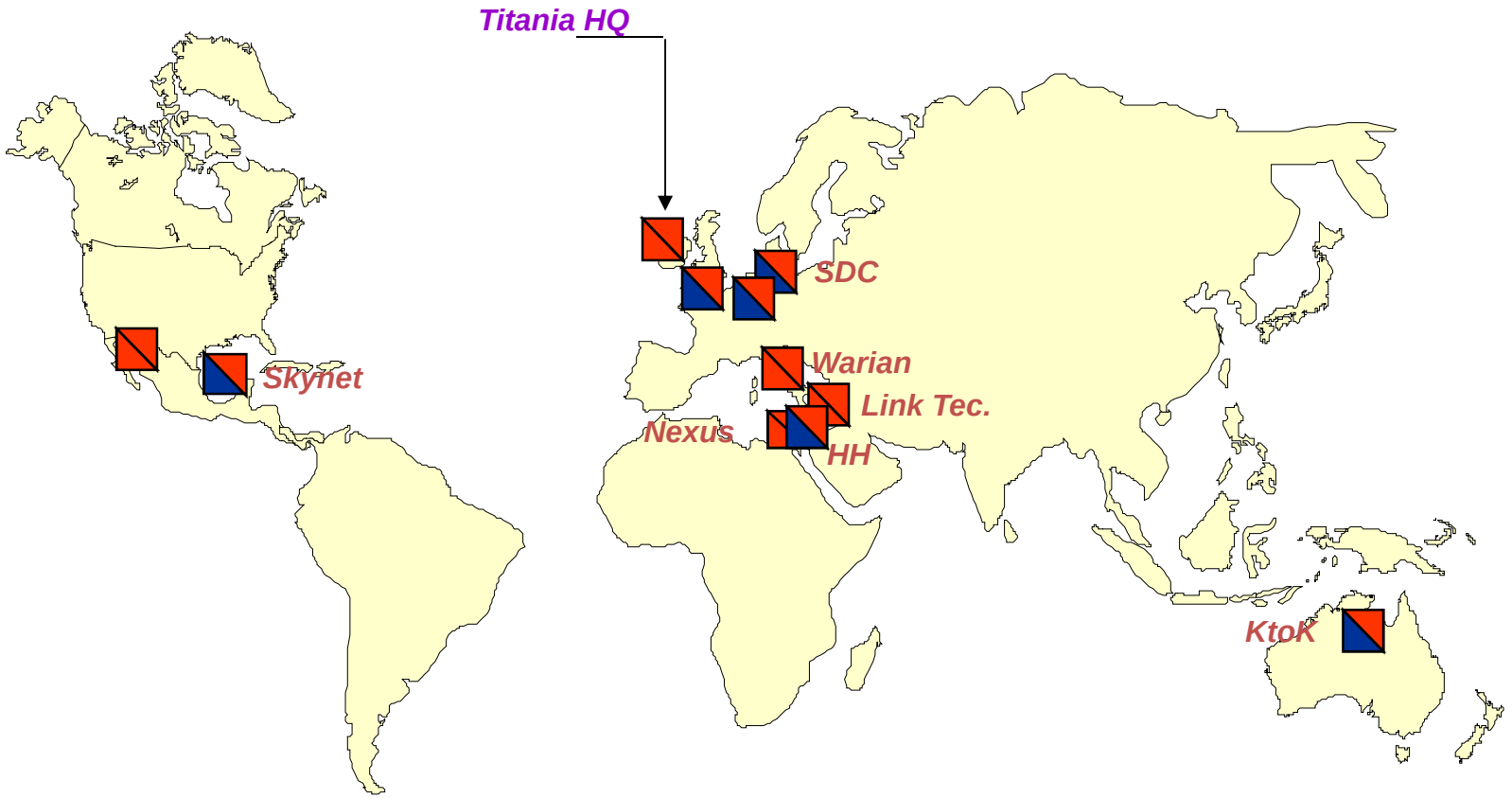
- Fundada en el 2015 en Dublín, Irlanda
- Responde a necesidades de negocios con criticidad en redes.
- Principales servicios:
  - Consultoría de red misión critica
  - Diseño de ISP
  - Network Training
- Áreas de operación:
  - Europa
  - América Latina

Operaciones



- Con un solo punto de contacto.

Clientes



Consulting Customer

Partner with Infrastructure facility

Objetivos

- Entender los beneficios y limitaciones del uso de QoS en el Wireless
- Familiarizar con las características hardware y software de MikroTik relacionadas con el QoS OtA
- Obtener los conocimientos básicos de RouterOS relacionados con las configuraciones presentadas
- Reproducir un escenario del mundo real con las habilidades de red obtenidas.

Requerimientos

- MikroTik Routerboard con una (o más) interfaz wireless
- Conocimientos básicos de RouterOS
- Conocimientos del nivel PHY de 802.11 deseable pero no requerido
- Capacidades básicas de uso de firewall
- Fundamentos de Bridging y Vlan.

Resumen

- Introducción
  - La raíz del problema
  - Que significa QoS OtA y que puede hacer por nuestra red
  - LAB: Un simple entorno de simulación (Nv2 + Vlan)
- Background
  - Linux, Atheros driver & C.
  - WMM y Nv2
- Configuración de RouterOS
  - WMM
  - Nv2
  - Configuración de prioridad en bridge y firewall
  - LAB: Configuración del gateway
- Resolución de problemas
  - Uso de Log
  - LAB: Pruebas y conclusiones

La raíz del problema

- Las trasmisiones Wireless (basadas en 802.11) son half-duplex. Es decir que la interfaz aire solo se puede utilizar para trasmitir o recibir información. (iso-frequencia)
- Cuando un punto de acceso sirve a varios clientes el aire se vuelve un medio compartido y el tiempo aire se divide entre todas las estaciones conectadas y activas.
- Originalmente las WLANs fueron pensadas para trasportar trafico con poco ancho de banda. Ahora en día la demanda de banda ha crecido exponencialmente y es muy fácil que una red inalámbrica se vuelva congestionada.
- Como si no fuera suficiente no todos los clientes cuentan con unas condiciones radios optímales…

La raíz del problema

- Hay necesidad de mantener la calidad de servicio en las redes inalámbricas para optimizar el ancho de banda disponible y proteger aplicaciones sensibles.

QoS Over the Air

- Hoy en día, con la expansión de las redes WLAN in mercados verticales (como as ventas, financia, y educación) y entornos enterprise, las WLANs se usan muy seguido para aplicaciones de gran ancho de banda high-bandwidth en conjunto con aplicaciones multimedia sensibles a la latencia.
- Este requerimiento implica la necesidad de QoS en wireless especialmente en un entorno ISP.
- QoS Over the Air se refiere a la capacidad de una red inalámbrica de proporcionar un servicio diferente por algunas tipologías de trafico.

QoS en general–para que es?

En general el uso de QoS proporciona los siguientes beneficios:

- Permite de acordar niveles de servicio (SLAs) con usuarios
- Permite a los recursos de red de ser compartidos mas eficientemente y de manejar aplicaciones criticas.
- Habilitar aplicaciones multimedia y voz asegurándose que su trafico reciba una prioridad mas alta y menos latencia con respecto a los demás flujos de trafico.

Podemos afirmar que por medio del QoS, el ancho de banda puede ser manejado mas eficientemente en redes WAN y LAN e incluso en WLANs.

QoS Over the Air – para que es?

Habilitando el QoS OtA en RouterOs, los usuarios MikroTik pueden introducir las siguientes mejoras en una red inalámbrica:

- Soportar ancho de banda dedicado para usuarios y aplicaciones criticas
- Controlar el jitter y la latencia (trafico real time)
- Manejar la congestión del medio inalámbrico
- Configurar prioridades por trafico de red

QoS over the Air – para que NO es?

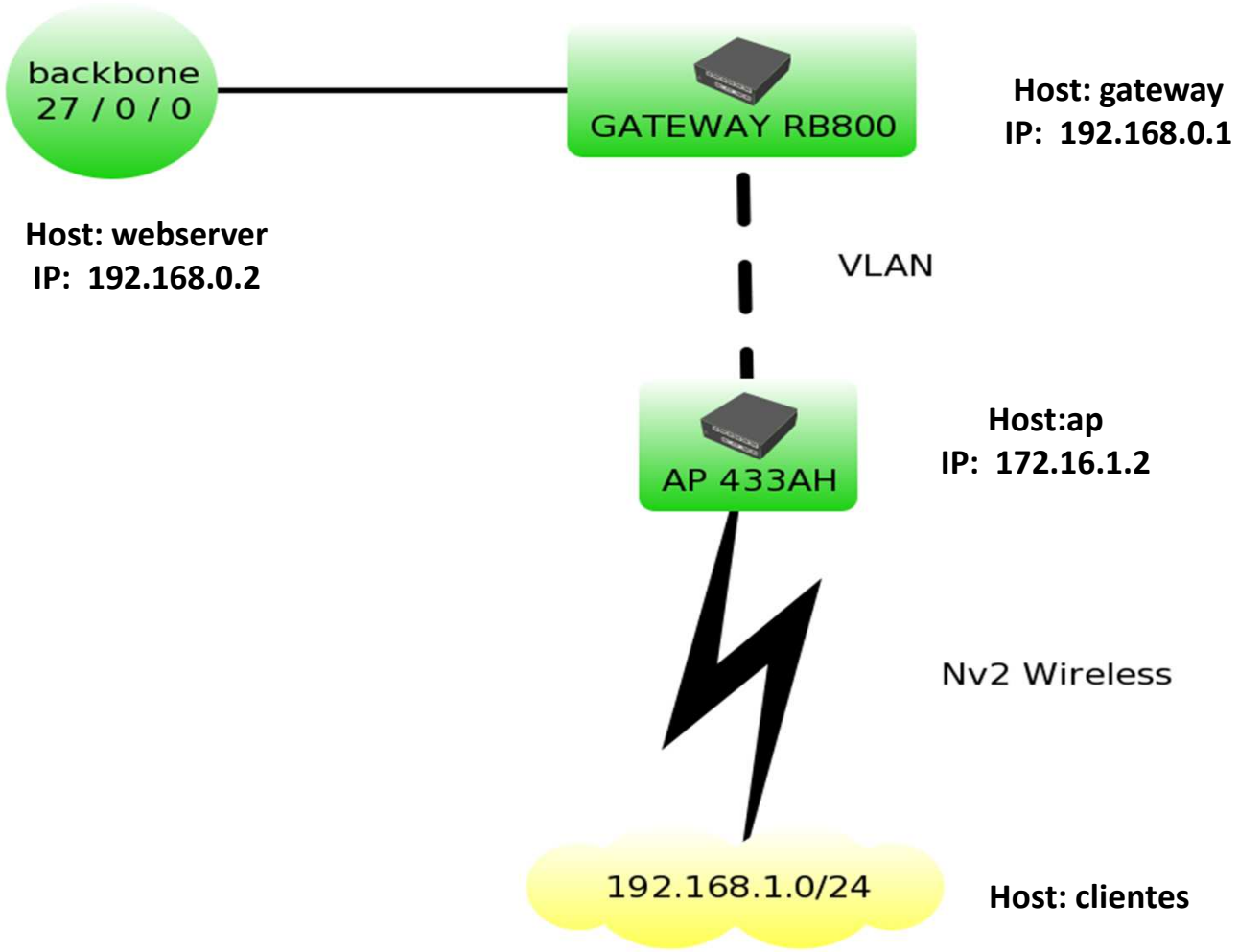
- El QoS !no es una barita mágica!
- Antes de implementar QoS en una red Wireless la red tiene que estar funcionando correctamente.
- QoS Over the Air puede ayudar en proporcionar prioridad a servicios diferentes (voz, gaming, etc..)
- QoS NO puede ayudar con malas instalaciones, baja señal interferencia, etc…
- Si una red inalámbrica no funciona bien con un trafico ligero sin QoS tampoco va a funcionar bien con QoS!

Estándares de referencia

- Para seguir investigando:

- Atk5, Atk9, Atk10 Linux Kernel drivers
- WMM aka WME (Wifi Alliance)
- IEEE 802.11e (IEEE)
- 802.1D-2004 (bridging)

LAB – una simple simulación



LAB – configuración de clientes

- Reset RB:

```
/system reset-configuration no-defaults=yes
```

- Configuración clientes

```
/system identity set name=CLI01
/interface wireless set [ find default-name=wlan1 ] ssid=LAB\
  wireless-protocol=nv2 radio-name=CLI01 \
  tx-power-mode=all-rate-fixed tx-power=10
/interface vlan add interface=wlan1 name=wlan1-vlan100 \
  vlan-id=100
/ip dhcp-client add default-route-distance=0 \
  dhcp-options=hostname,clientid disabled=no \
  interface=wlan1-vlan100
```

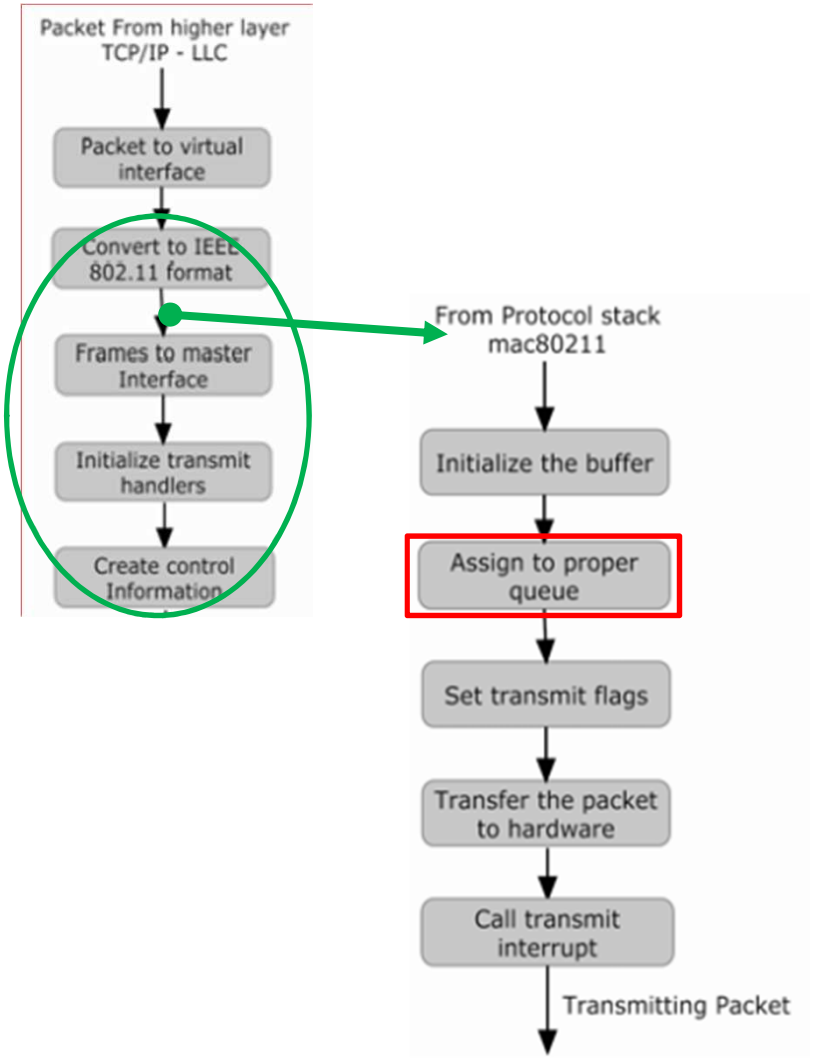
LAB – pasos a seguir

- Al configurar la red inalámbrica tomaremos nota de los tiempos de respuesta de ICMP.

- Haremos dos tareas muy básicas para habilitar el QoS OtA:
  - Configurar un protocolo que soporte Wireless QoS .
  - Configurar la prioridad en el frame que se trasmitirá por la interfaz wireless.

Linux Kernel

- El nivel mas alto de la capa (L3) transfiere la estructura del paquete a la capa MAC por medio de llamadas a las funciones de tx del kernel
- El driver Atheros recibe la estructura del frame por medio del controlador de protocolo mac80211.
- Es precisamente en este punto que el frame puede ser ingresado en una diferente cola.



Atheros source driver (código fuente)

- Un vistazo al código nos permite de entender mejor las próximas diapositivas.

txrx.c

```
/*
 * We may have to search for the next active stream
 * that is the highest priority.
 */
if (ar->hiac_stream_active_pri ==
          ar->ac_stream_pri_map[traffic_class]) {
          /*
           * The highest priority stream just went inactive
           * reset and search for the "next" highest "active"
           * priority stream.
           */
          ar->hiac_stream_active_pri = 0;

          for (i = 0; i < WMM_NUM_AC; i++) {
                    if (ar->ac_stream_active[i] &&
                        (ar->ac_stream_pri_map[i] >
                         ar->hiac_stream_active_pri))
                              /*
                               * Set the new highest active
                               * priority.
                               */
                              ar->hiac_stream_active_pri =
                                        ar->ac_stream_pri_map[i];
```

core.c

```
/* setup access class priority mappings */
ar->ac_stream_pri_map[WMM_AC_BK] = 0; /* lowest  */
ar->ac_stream_pri_map[WMM_AC_BE] = 1;
ar->ac_stream_pri_map[WMM_AC_VI] = 2;
ar->ac_stream_pri_map[WMM_AC_VO] = 3; /* highest */
```

WMM

- WMM trabaja dividiendo el trafico en 4 categorías de acceso: background, best effort, video, voice
- Prioridades de acuerdo a la siguiente tabla:

Priority	Layer 2 COS	WMM Access Category
Lowest	1	AC_BK (background)
	2	AC_BK (background)
	0	AC_BE (best effort)
	3	AC_BE (best effort)
	4	AC_VI (video)
	5	AC_VI (video)
	6	AC_VO (voice)
Highest	7	AC_VO (voice)

- Las políticas se aplican únicamente en el lado TX, eso significa que el AP no tiene control de como los clientes transmiten los frames y los clientes de como los transmite el AP.
- Prioridades mas altas tienen mayor probabilidad de acceso al medio. En todo efecto los clientes WMM se pueden considerar como cuatro, uno por cada categoría de acceso los que tienen mayor prioridad tienen mas posibilidad de trasmitir.

Nv2

- Nv2 (Nestreme Versión 2) es un protocolo propietario de RouterOS que se introdujo a partir de las versiones 5.x
- Funciona en hardware reciente (Atheros N chips and >= AR5212)
- Nv2 se basa en TDMA (Time Division Multiple Access)
- Nv2 NO es compatible con 802.11 y otros estándares así que todos los nodos que participan tiene que usar RouterOS

Nv2

- Las políticas de QoS en una red Nv2 está controlada por el AP todos los clientes usan la misma configuración del AP
- NV2 tiene un mecanismo de QoS con una cantidad de colas libremente configurable.
- Así como por WMM también Nv2 usa el esquema de prioridades de IEEE 802.1D-2004.
- Nv2 sigue la siguiente regla para trasmitir:
  - Una cola se considera para trasmitir únicamente si las colas con mayor prioridad están vacías
  - Primero se trasmiten todos los frames con prioridad mas alta y solamente entonces se pasa a trasmitir frames con prioridad inferior.
- **Eso tiene como resultado que hay que diseñar con cuidado los sistemas de QoS para dejar algo de espacio a las colas con menor prioridad.**

Frame priority

- Para poder enviar un frame en alguna cola especifica de Nv2 o WMM hay que utilizar un campo especifico llamado prioridad del frame (L2).
- El campo prioridad no es lo mismo de DSCP! Ya que DSCP se encuentra en el encabezado IP (L3) La información de prioridad que configuremos solo importa en el proceso local.
- También cuando hay tipos de frame que pueden transportar información de prioridad (VLAN, WMM) SIEMPRE hay que leer la información en la interfaz que recibe y escribirla en la interfaz de salida. NO AUTOMAGIC!

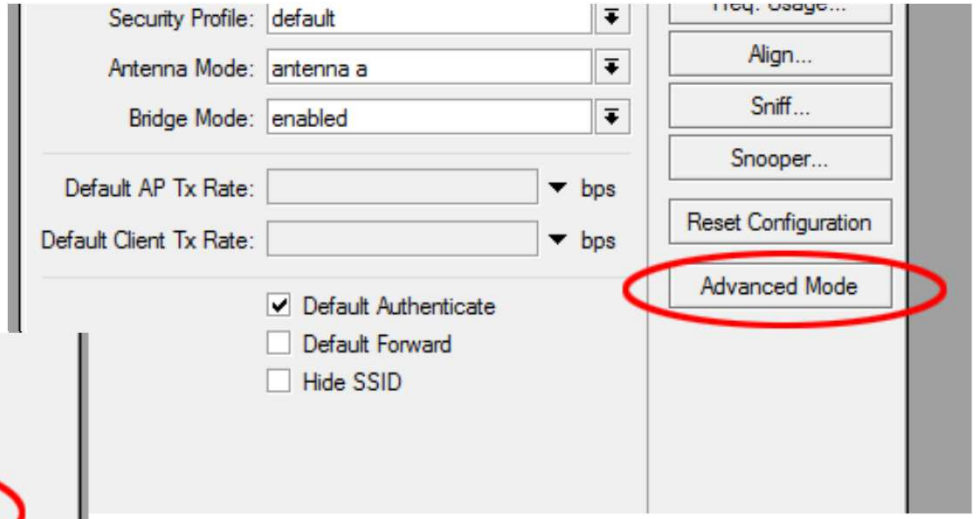
Frame priority

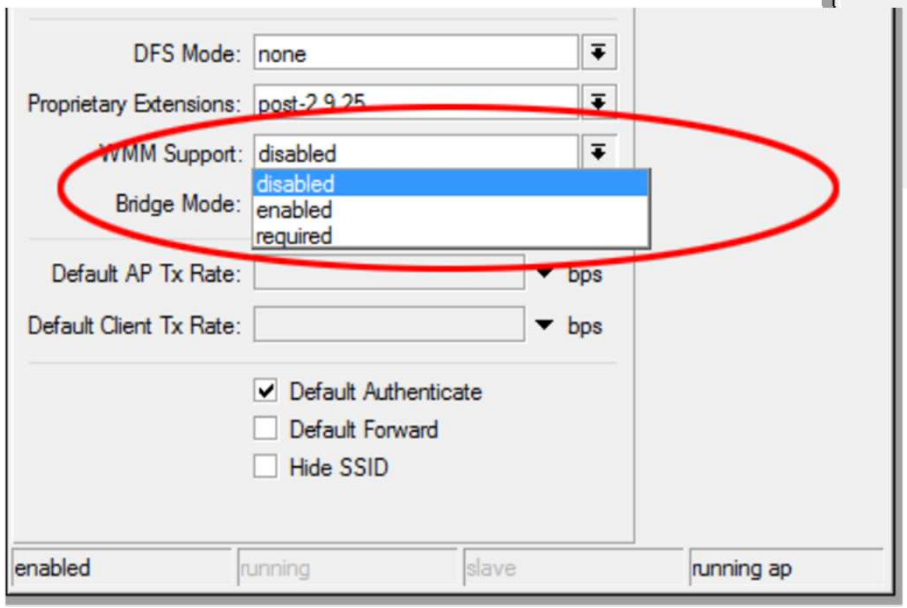
- El concepto clave que hay que entender para manejar la prioridad es el siguiente: “la interfaz que trasmite el frame tiene que recibir los paquetes con la información de prioridad ya configurada” (mas en un momento)

Configuración - WMM

```
/interface wireless set wlan1 wmm-support=enable
```

- Puede ser habilitado en el modo “advanced”



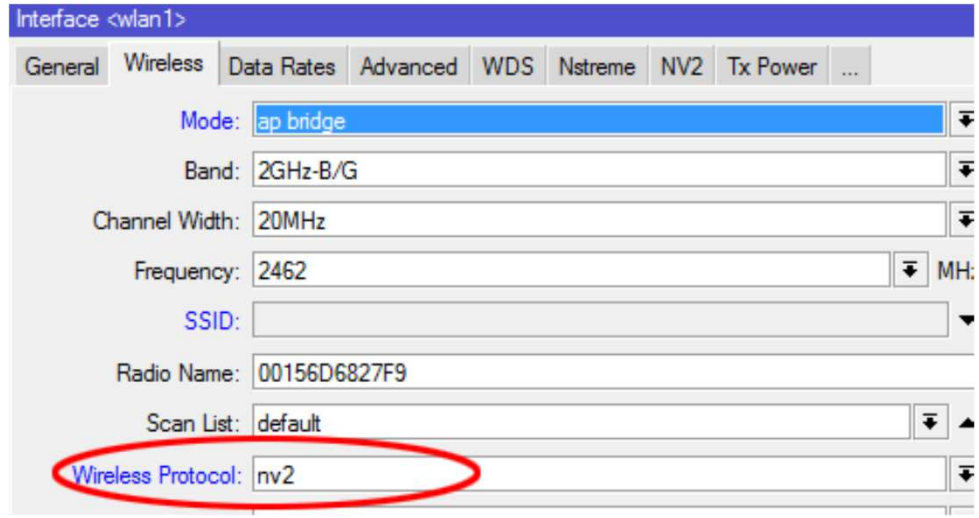


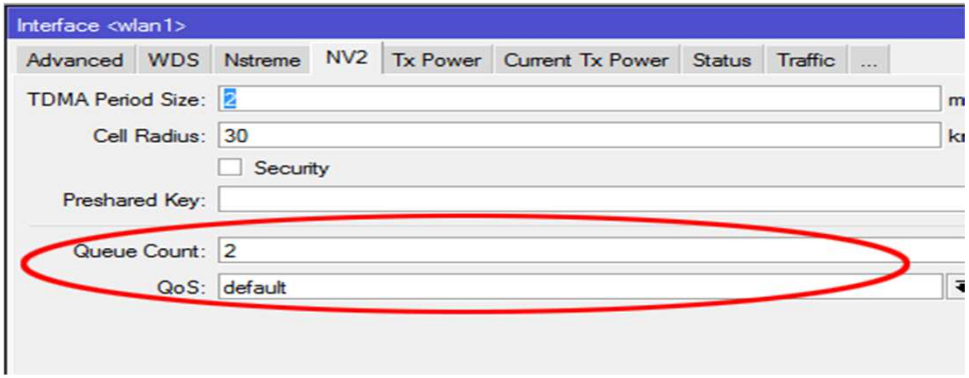
- Hay que habilitarlo en el AP y en todos los clientes

Configuración - Nv2

```
/interface wireless set wlan1 wireless-protocol=nv2
```

- Hay que configurar el modo del AP en Nv2. Hay que configurar los clientes para acceso a la red Nv2.
- La configuración del QoS se encuentra en la pestaña Nv2 del AP (no se requiere otra configuración en los clientes)





Configuración- Nv2

```
/interface wireless set wlan1 nv2-qos=default | frame-priority
```

- nv2-qos=default
  - El frame a trasmitir se va a inspeccionar antes por el algoritmo QoS built-in que seleccionará una cola en base al tipo y tamaño del frame.
  - Si el frame no encaja ninguna regla del algoritmo se checará la prioridad del frame (si esta presente) como por “frame-priority”.
- nv2-qos=frame-priority
  - La cola de QoS se seleccionara basándose únicamente sobre la información de prioridad del frame.

Configuración - Nv2

```
/interface wireless set wlan1 nv2-queue-count=2
```

- nv2-queue-count
  - Especifica cuantas colas serán utilizadas en la red Nv2.
  - El mapeo se basa en la prioridad de usuario como por 802.1D-2004.
- Por defecto queues-count es 2, otros valores comunes de queue-count son:

2 queues	
priority	queue
0,1,2,3	0
4,5,6,7	1

4 queues	
priority	queue
1,2	0
0,3	1
4,5	2
6,7	3

8 queues	
priority	queue
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

****Poner atención en el esquema a 4 (como WMM) y 8 colas****

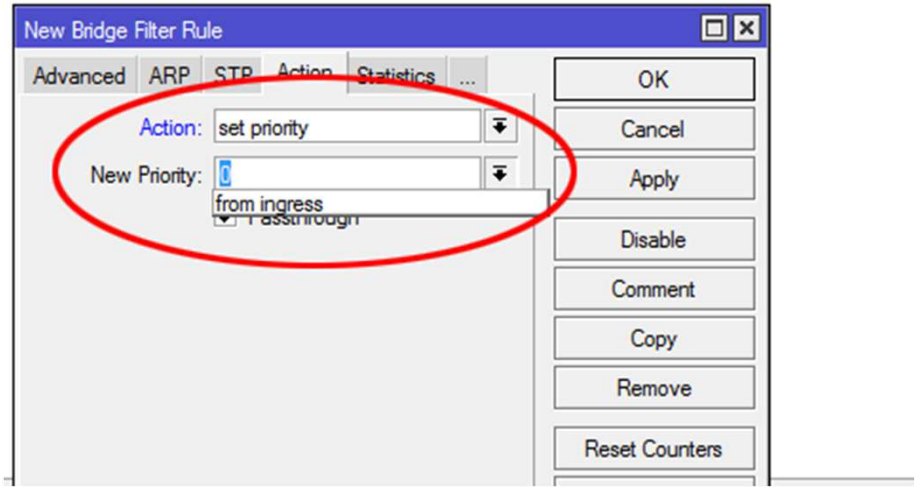
Configurar las prioridades

- Para asignar correctamente las prioridades hay que considerar lo siguiente:
  - Por defecto todos los frames se consideran prioridad 0.
  - Eso implica que en los esquemas anteriores prioridad 1 y 2 penalizan el trafico con respecto a todo los de mas tipos (incluyendo el trafico no clasificado)
  - Los Frames VLAN y WMM (y MPLS Exp bit) PUEDEN trasportar información de prioridad a fuera del equipo.
  - Por defecto las prioridades recibidas en una interfaz se REMUEVEN antes que el frame (o paquete) sea trasmitido (o ruteado) por la interfaz de salida.
  - Hay dos posibilidades para configurar la prioridad el firewall L3 (/ip firewall mangle) y el firewall L2 (/interface bridge filter)

Bridge Firewall

```
/interface bridge filter add action=set-priority \
  chain=forward new-priority= from-ingress | value
```

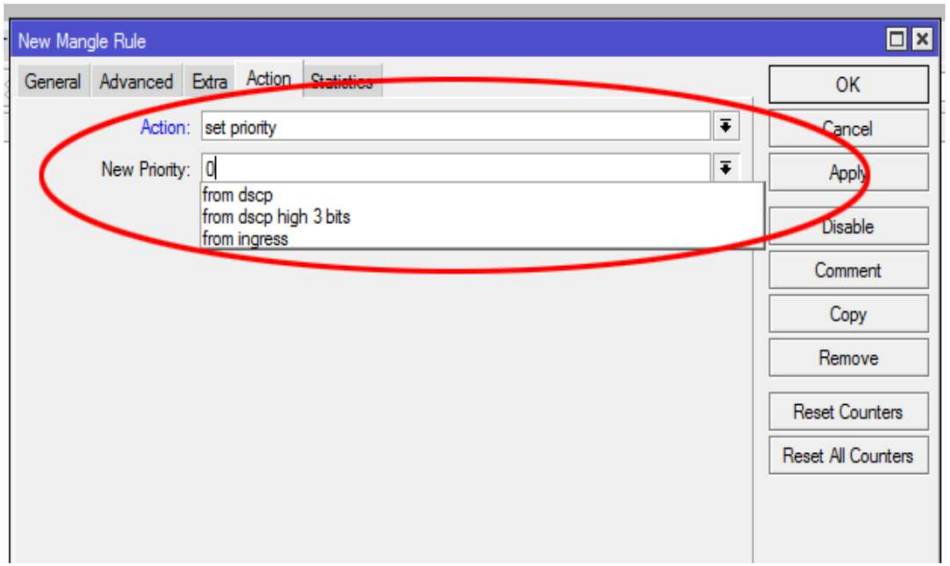
- new-priority=value
  - Los valores de prioridad indicados se usarán en la interfaz de salida.
  - Asegurarse que la interfaz de SALIDA tenga capacidad ara utilizar la información de prioridad de otras formas esa no tendrá efecto.
- new-priority=from-ingress
  - Los valores de prioridad se copiarán desde la interfaz de ENTRADA.
  - Como antes.



Firewall Mangle

```
/ip firewall mangle add action=set-priority chain=postrouting \
  new-priority= value | from-dscp | from-dscp-high-3-bits | from-ingress
```

- new-priority = value
  - El valor seleccionado se usará en la interfaz de SALIDA del router.
- new-priority=from-ingress
  - El valor se copiará desde la interfaz de entrada del paquete.
- new-priority = from-dscp
  - El valor de prioridad se copiará desde el encabezado IP DSCP. La prioridad efectiva será el valor de DSCP dividido por 8. ej (56->0)



- new-priority = from-dscp-high-3-bits
  - Como antes pero solo se consideran los bit mas significativos de DSCP. ej (56->7)

LAB – gateway setup

Referencias en slide 12

```
/interface vlan add interface=ether1 name=ether1-vlan1 vlan-id=100
/ip pool add name=pool1 ranges=192.168.1.100-192.168.1.200
/ip dhcp-server add address-pool=pool1 disabled=no interface=ether1-
vlan1 name=server1
/ip address add address=192.168.0.1/24 interface=ether3
network=192.168.0.0
/ip address add address=172.16.1.1/24 interface=ether1
network=172.16.1.0
/ip address add address=192.168.1.1/24 interface=ether1-vlan1
network=192.168.1.0
/ip dhcp-server network add address=192.168.1.0/24 dns-
server=192.168.1.1 gateway=192.168.1.1 netmask=24
/ip dns set allow-remote-requests=yes servers=8.8.8.8
/ip firewall mangle add action=set-priority chain=postrouting \
   new-priority=3 protocol=icmp
/ip firewall mangle add action=log chain=postrouting protocol=icmp
```

LAB - AP Setup

```
/interface bridge add name=bridge1
/interface wireless set [ find default-name=wlan1 ]
mode=ap-bridge \
    nv2-qos=frame-priority nv2-queue-count=8 ssid=LAB \
    wireless-protocol=nv2

/interface vlan
add interface=ether1 name=ether1-vlan100 vlan-id=100
add interface=wlan1 name=wlan1-vlan100 vlan-id=100

/interface bridge port
add bridge=bridge1 interface=wlan1-vlan100
add bridge=bridge1 interface=ether1-vlan100

/ip address add address=172.16.1.2/24 interface=ether1
/ip route add distance=1 gateway=172.16.1.1
```

Resolución de problemas – Log

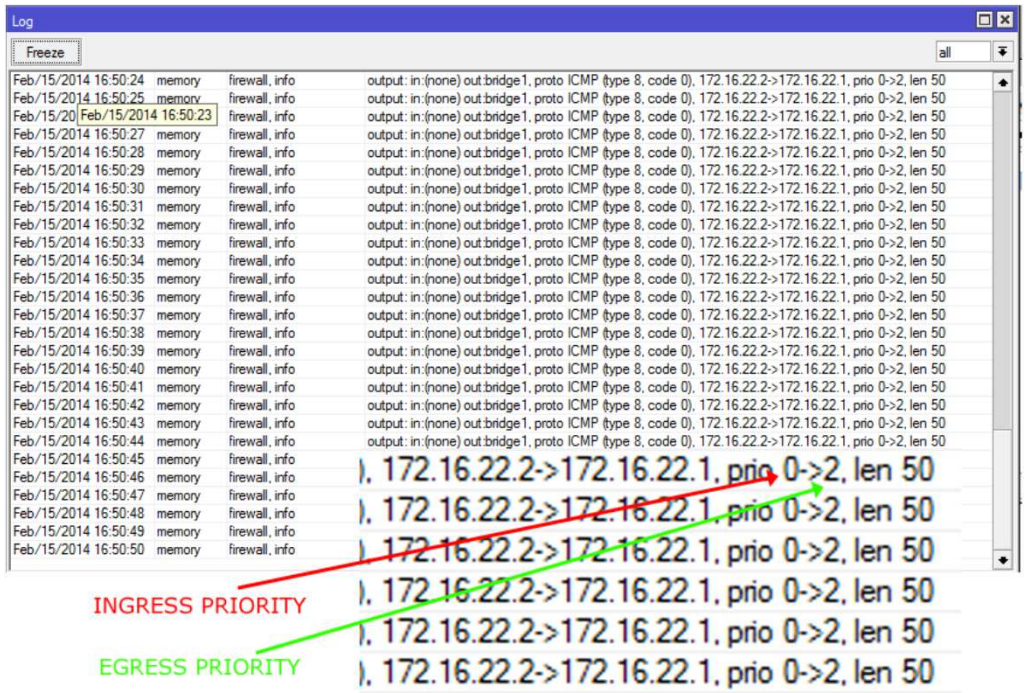
- La acción log en el firewall L3 permite una rápida inspección para verificar que nuestra configuración este aplicando correctamente las prioridades.
- Podemos utilizar toda la potencia del firewall para refinar los paquetes a inspeccionar
- Para una inspección mas profunda del flujo podemos utilizar el packet sniffer en conjunto con un programa separado como Wireshark

Resolución de problemas – Log

- Por ejemplo para icmp podríamos utilizar

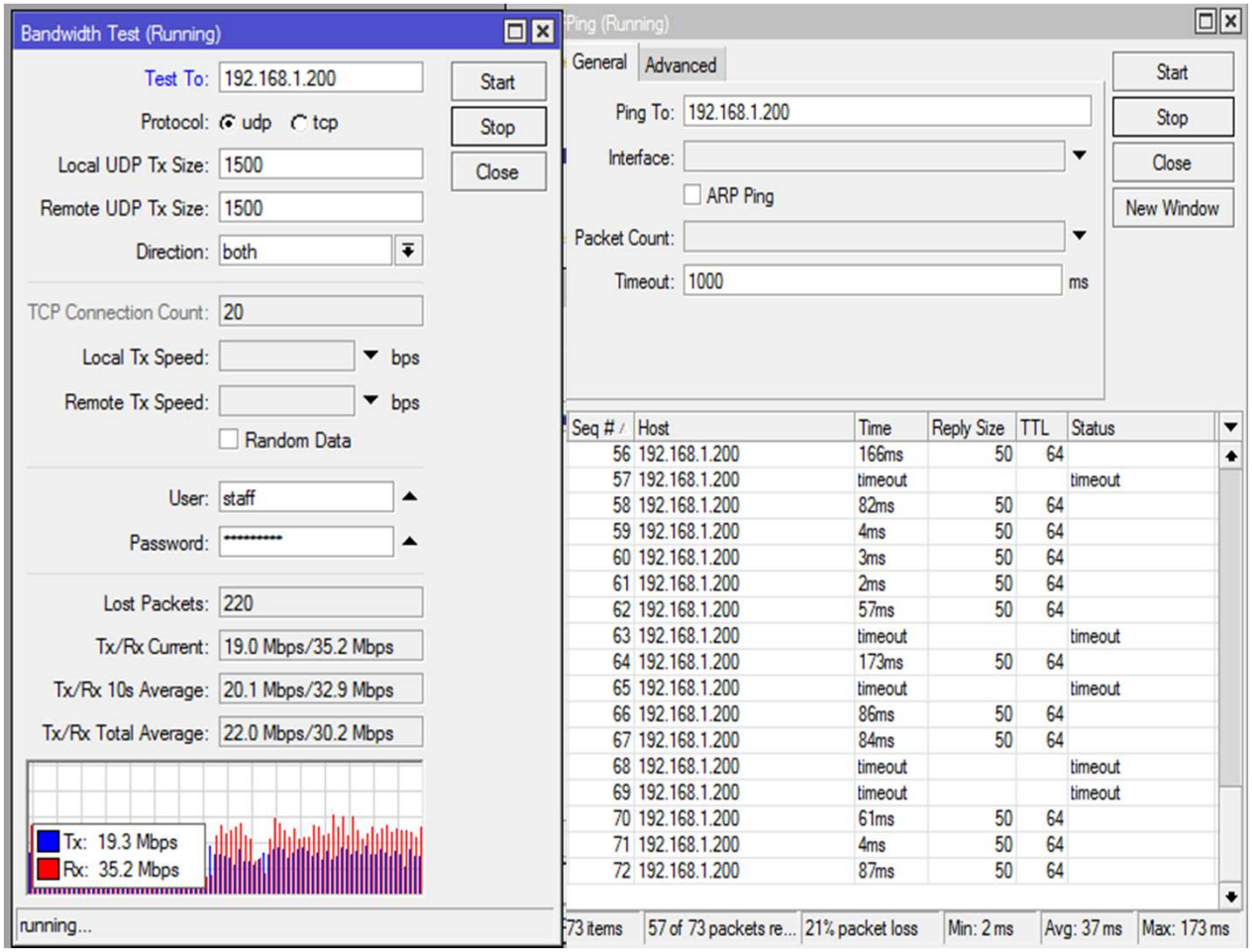
```
/ip firewall filter add action=log chain=output protocol=icmp
/ip firewall mangle add action=set-priority chain=output new-priority=2
protocol=icmp
```

- Ingress priority es 0 porque es un paquete generado localmente (chain output)
- Prestar atención para equipos en producción por la cantidad de paquetes que se manejan.



LAB - tests

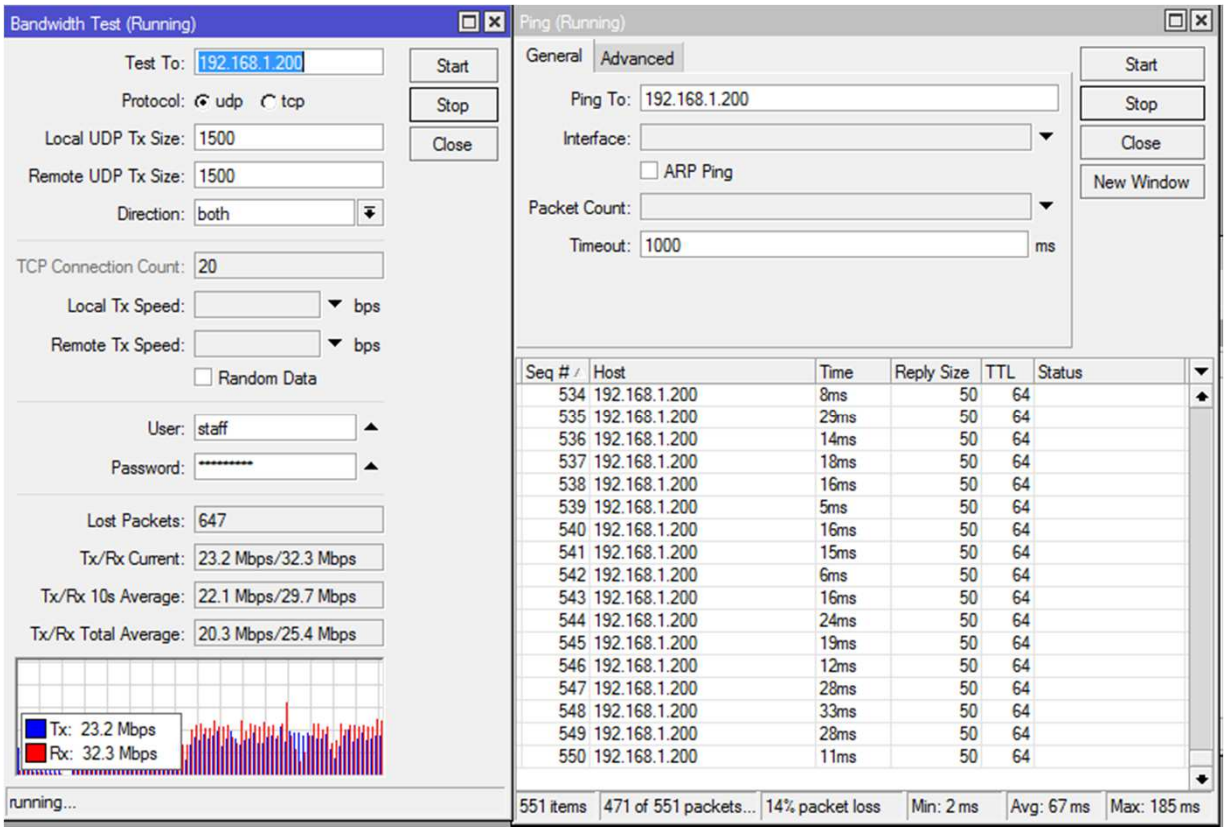
- Con el objetivo de simular un enlace congestionado se puede lanzar un Bandwidth test gateway -> cliente.
- El tiempo de latencia, como estamos acostumbrados a ver, se dispara erráticamente.



LAB - tests

- Después de añadir en el AP

```
/interface bridge filter add action=set-priority
 chain=forward new-priority=from-ingress
```



LAB - tests

- Que sucedería si pusiera:

```
/ip firewall mangle add action=set-priority chain=forward \
  new-priority=0 protocol=icmp
```

- O bien

```
/ip firewall mangle add action=set-priority chain=forward \
  new-priority=2 protocol=icmp
```

Conclusiones

- Para habilitar QoS en Aire necesitamos:
  - Un protocolo que maneje prioridades
  - Configurar las prioridades en el modulo correcto
- Con los mismos bloques funcionales podemos implementar configuraciones mas complejas como por ejemplo con PPPoE (sobre VLAN)
- También el bit EXP de MPLS puede transportar la información de prioridad en las redes basadas en label switching.
- Si algo no funciona contamos con el Log para depurar nuestra configuración.

Conclusiones

Con la tecnología presentada se pueden armar complejas configuraciones cross-layers utilizando packet marking y priority en IP firewall (L3) y priority en Bridge Filters (L2)

Sugerencias:

- Usar DSCP cuando posible (no hay overhead!)
- Usar la cantidad mínima de filtros porque consumen recursos.
- usar VLANs cuando necesario, asegurándose que la prioridad no sea cancelada en alguna parte de la red.
- Recordarse que QoS no mejora el throughput de los enlaces.

Créditos

- http://linuxwireless.org/en/users/Drivers/ath9k
- http://linuxwireless.org/en/developers/Documentation/mac80211
- http://mum.mikrotik.com/presentations/US13/lutz.pdf
- https://www.researchgate.net/publication/224116216_Analysis_of_open_source_drivers_for_IEEE_80211_WLANs

Por su atención

¡GRACIAS!

Bienvenidas preguntas y sugerencias

ag@tnxe.net