


| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-27 |

DISEÑO E IMPLEMENTACIÓN DE RED GESTION OTM

Johana Quintana Parias

Programa Académico:

Ingeniería en Telecomunicaciones

Pedro Enrique Guerrero

INSTITUTO TECNOLÓGICO METROPOLITANO

Noviembre 2016

| | | | |
|---|--------------------------------------|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

RESUMEN

Hoy en día el mundo de la gestión de red es muy importante ya que se ha generado la necesidad de saber que está pasando con los equipos que componen una red. Gestionar una red permite al administrador anticiparse a posibles fallos en la red y detectar su impacto en la prestación de un servicio.

Es por esto que durante la realización de este proyecto se diseñó e implementó una red de gestión para el monitoreo de los equipos que componen la red OTM de la sede fraternidad del ITM.

En este proyecto también se implementó una mejora en la red Wifi que brinda servicio inalámbrico a los estudiantes del semillero de telecomunicaciones.

Para la seguridad de la red OTM y proteger los equipos que la componen, se crearon reglas de Firewall en el Router de borde de la red.

Palabras clave: firewall, Wifi, Vlans, dhcp

| | | | |
|---|--------------------------------------|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

RECONOCIMIENTOS

Quisiera dirigir mis agradecimientos a mi familia, especialmente a mi padre quien me enseñó que los sueños solo se cumplen trabajando duro por ellos, a mi madre por su infinito amor y paciencia, adicionalmente agradezco a mi asesor Pedro Guerrero por guiar mis pasos durante la realización de este trabajo y por sus grandes enseñanzas y finalmente agradezco a dios por permitirme llegar a este punto de mi vida llena de conocimiento y personas tan aportantes.

| | | | |
|---|--------------------------------------|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

ACRÓNIMOS

AP Punto de Acceso

DHCP protocolo de configuración dinámica de host.

DoS Denegación de Servicio

DNS Sistema de Dominio de Nombres

IP Protocolo de Internet

LAN Red de Área Local

MPLS Protocolo de Conmutación de Etiquetas

QoS Calidad de Servicio

SSH Secure Shell

VLAN red de área local virtual

WAN Red de Área Amplia

WPA Acceso WiFi Protegido

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

TABLA DE CONTENIDO

| | |
|---|--------------------------------------|
| 1. INTRODUCCIÓN..... | 6 |
| 2. MARCO TEÓRICO | 10 |
| 3. METODOLOGÍA..... | 12 |
| 4. RESULTADOS Y DISCUSIÓN | 28 |
| 5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO ... | 34 |
| REFERENCIAS..... | 52 |
| APÉNDICE..... | ¡Error! Marcador no definido. |

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

1. INTRODUCCIÓN

En el Instituto Tecnológico Metropolitano (ITM) se tiene una red alterna a la institucional llamada OTM, esta red es utilizada por el semillero de redes de la institución. Dicha red cuenta con Router, APs y switches ubicados en las aulas N101, N601 y bloque O; en las aulas K105 y N102 no se cuentan con router, allí se tiene switches que conectan los dispositivos de cada Lan.

Realizando el respectivo análisis de la red, a nivel físico se encuentra desorden en el cableado del aula N601 pues este no cuenta con etiquetado para identificar las conexiones de cada puerto. Los Rj45 en su mayoría están en mal estado lo cual afecta su correcta conexión.

A nivel lógico todos los equipos son gestionados con la única red la cual se configura sobre una interfaz lógica y dentro de esta interfaz lógica se agregan todos los puertos Ethernet de los Router, la anterior configuración deja los puertos Ethernet en acceso sin posibilidad de crecimiento a futuro por medio de configuraciones de Vlans. Esta red es utilizada para la gestión y propagación del servicios de internet, al estar los puestos Ethernet en bridge se presenta una falencia y es que, en caso de presentarse un ataque de red tales como DoS, virus en la Lan, etc, este ataque se extendería por toda la red teniendo en cuenta que todo está unido bajo una misma interfaz lógica y por ello una misma red, el dominio de Broadcast se extendería por todos los equipos que componen la red.

Se adjunta un diagrama de cómo se encuentra la red al inicial este trabajo:

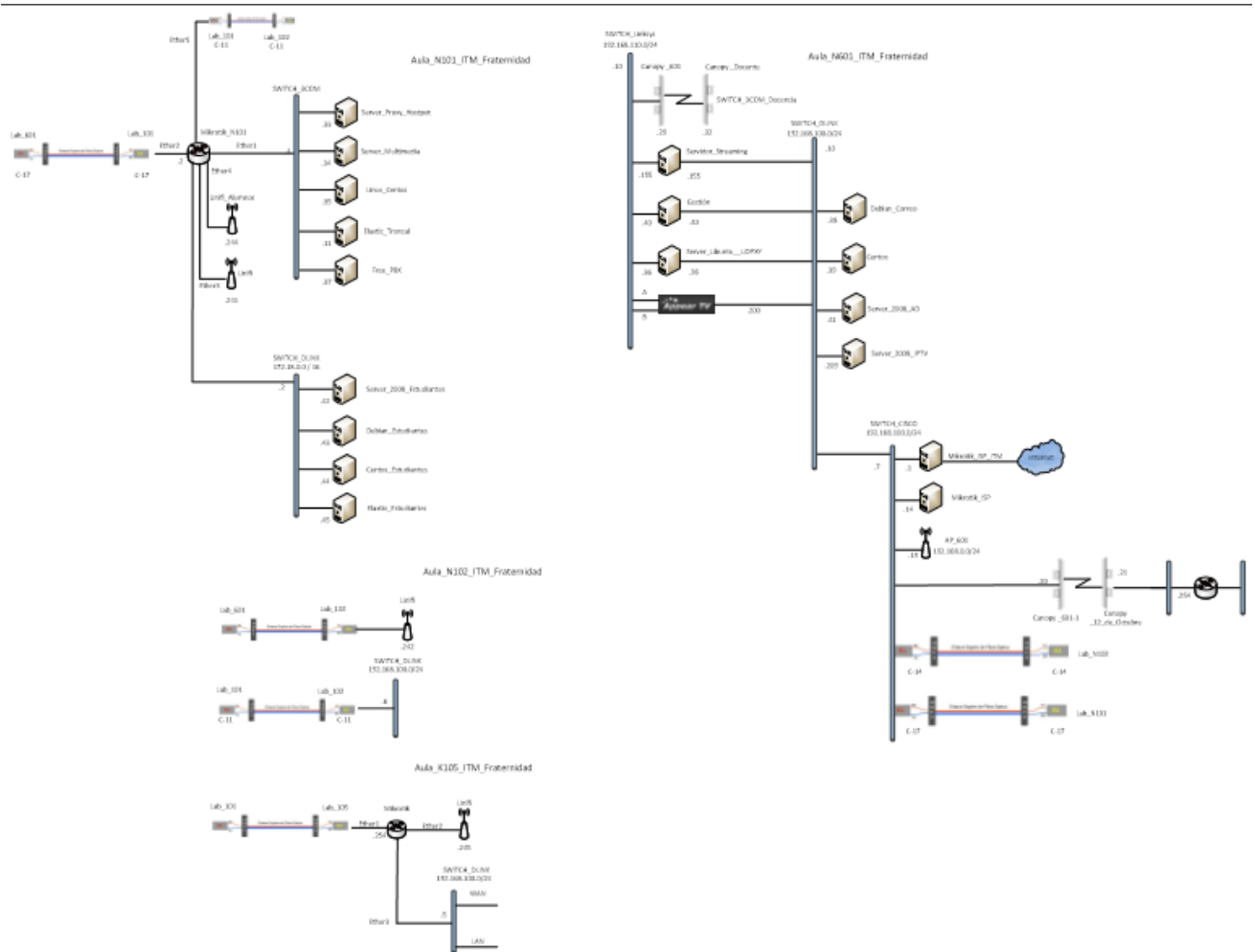


Imagen 1. Diagrama de solución general de la red.

Para mejorar la red actual OTM se realiza el diseño e implementación de una red de gestión para el monitoreo y control de los equipos que la componen. Se realiza la configuración de una Vlan que conecta a nivel lógico los equipos de la red OTM, lo anterior con el fin de segmentar el

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

Tráfico de gestión de otro tipo de tráfico (tráfico internet, datos, etc). Se asignó y configuro la red 172.16.20.0/23. Esta red alcanza a gestionar hasta 510 dispositivos.

Ahora bien, para el servicio de internet inalámbrico se cuenta con radios AP marca Ubiquiti los cuales necesitan una controladora para su gestión, configuración y administración. Esta controladora se instaló en una máquina virtual ubicada en los servidores de bloque O.

En la controladora unifi se crean los perfiles que varían según los privilegios de cada usuario, para este caso se crearon 2 Vlan que soportan estos perfiles:

Vlan 10 SSID Semillero

Vlan 11 SSID Soporte

Para la seguridad de la red OTM y proteger los equipos que la componen, se crearon reglas de Firewall para que el Router de borde N601 esté protegido de ataques de entrada.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

1.1. Objetivo

Diseñar e Implementar red de gestión que permita el monitoreo de los equipos de la red OTM.

1.2. Objetivos Específicos

- Implementar una red de gestión para el monitoreo de los equipos de la red OTM que permita segmentar el tráfico de gestión del tráfico de otros servicios, lo anterior basados en el estándar 802.1Q de la IEEE.
- Rediseñar la zona Wifi de la red OTM segmentando el tráfico de los SSID creados para los usuarios que utilizan la red.
- Aplicar políticas de firewall que protejan el Router de borde de ataques externos.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

1. MARCO TEÓRICO

Inicialmente en el desarrollo de este trabajo se realiza la asignación y configuración de la red de gestión segmentada por Vlans siguiendo el estándar 802.1Q de la IEEE. Este estándar cuenta con una estructura de trama que tiene el campo vlan ID el cual permite generar etiquetas diferenciando el tráfico y optimizando el ancho de banda disponible.

Inicio como un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

En este trabajo se implementó Vlans para segmentar el tráfico de gestión del tráfico de servicios.

2.1 SEGURIDAD EN LA RED

Desde su existencia las redes IP ayudan a aumentar y facilitar las comunicaciones a nivel mundial, posibilitan que la información sensible de diferentes empresas sea encaminada a través de la red. Es por ello que la seguridad de la información se enfatiza por la confiabilidad, integridad y disponibilidad de la información que es canalizada a través de la red. Existen

| | | | |
|---|--------------------------------------|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

Herramientas con algoritmos especializados de encriptación que ayudan a mitigar la pérdida de información porque algún intruso quiera irrumpir en la red.

2.2 QoS

La QoS permite establecer estrategias para implementar prioridades que clasifican los diferentes tipos de tráfico para darle a cada uno un tratamiento especial (dependiendo de las características). Sin el diseño y la implementación correctos de los mecanismos de QoS, los paquetes de datos se descartan sin considerar las características de la aplicación ni la prioridad.

Algunas de las decisiones prioritarias para una organización pueden ser:

Comunicaciones sensibles al tiempo: aumentan la prioridad por servicios como el teléfono o la distribución de videos. Comunicaciones no sensibles al tiempo: disminuyen la prioridad de recuperación de páginas Web o de correos electrónicos. Alta importancia para la empresa: aumenta la prioridad del control de producción o de datos de transacciones comerciales.

Comunicación no deseada: disminuye la prioridad o bloquea la actividad no deseada, como el intercambio de archivos punto a punto o el entretenimiento en vivo. *Cisco, Troubleshooting Input Queue Drops and Output Queue Drops, May 03, (2016)*

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

2. METODOLOGÍA

El principal aporte de la este trabajo es la metodología de diseño de redes Top-Down tomando el tipo re-ingeniería de un diseño existente ya que el enfoque de este trabajo fue modificar la red para compensar los problemas del diseño anterior.

3.1 Fase 1. Analizar requisitos:


Inicialmente se realizó un estudio de sitio con el fin de identificar las falencias y necesidades que se tenían en la red anterior encontrando:

- A nivel físico se encuentra desorden en el cableado del aula N601 ya que este no cuenta con etiquetado que identifique las conexiones de cada puerto. Los Rj45 en su mayoría están averiados lo cual afecta su correcta conexión en cada puerto.
- Al iniciar este trabajo de grado se realizó un estudio de sitio con el fin de identificar los componentes, falencias y necesidades que sería solventada con la res a diseñar. Se encuentra el aula N601, donde está ubicado los bordes Backbone que componen la red MPLS con fallas en la organización y cableado de datos. Este no se encuentra debidamente etiquetado y no cuenta con conectores adecuados para brindar una calidad de servicios. Los equipos Switches y router no cuentan con descripción que ayude a la debida identificación de los servicios.



| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

Se anexan las fotos de cómo se encuentra a nivel físico los equipos y cableado del aula N601:

3.2 Fotos de estructura N601 Inicialmente

| Figura | Descripción |
|--|---|
|  <p data-bbox="389 1528 941 1562" style="text-align: center;">Figura 1. Cableado del rack 1 en aula N601</p> | <p data-bbox="1159 982 1354 1381">En el aula N601 el cableado que conecta los servidores están de manera desordenada y no cuentan con etiquetado.</p> |
| | |

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

| | |
|--|--|
|  | <p>El cableado del rack donde está ubicado el equipo de Backbone y el switch de acceso de los servidores se encuentra desorganizado y sin etiquetar.</p> |
| <p style="text-align: center;">Figura 2. Cableado de la parte de atrás rack 2 en el aula N602</p> | |
|  | |
| <p style="text-align: center;">Figura 3. Cableado de la parte frontal del rack 2 en el aula N602</p> | |

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

| | | |
|---|--|--|
|  | | |
| <p>Figura 4. Cableado del rack 2 en el aula N602</p> | | |
| | | |

- A nivel lógico todos los equipos son gestionados con la red 192.168.100.0/24, en los Router Mikrotik cada Ip de esta red se configura sobre una interfaz lógica llamada bridge y dentro de estas interfaz lógica se agregan todos los 8 puertos Ethernet de los Router, la anterior configuración deja los puertos Ethernet en acceso sin posibilidad de crecimiento a futuro con configuraciones de Vlans. Esta red es utilizada para la gestión y propagación del servicios de internet, al estar los puestos Ethernet en bridge se presenta una falencia y es que, en caso de presentarse un ataque de red tales como DoS, virus en la Lan, etc, este ataque se extendería por toda la red teniendo en cuenta que todo está unido bajo una misma interfaz lógica y por ello una misma red, el dominio de Broadcast se extendería por todos los equipos que componen la red.

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

- El diagrama de red:

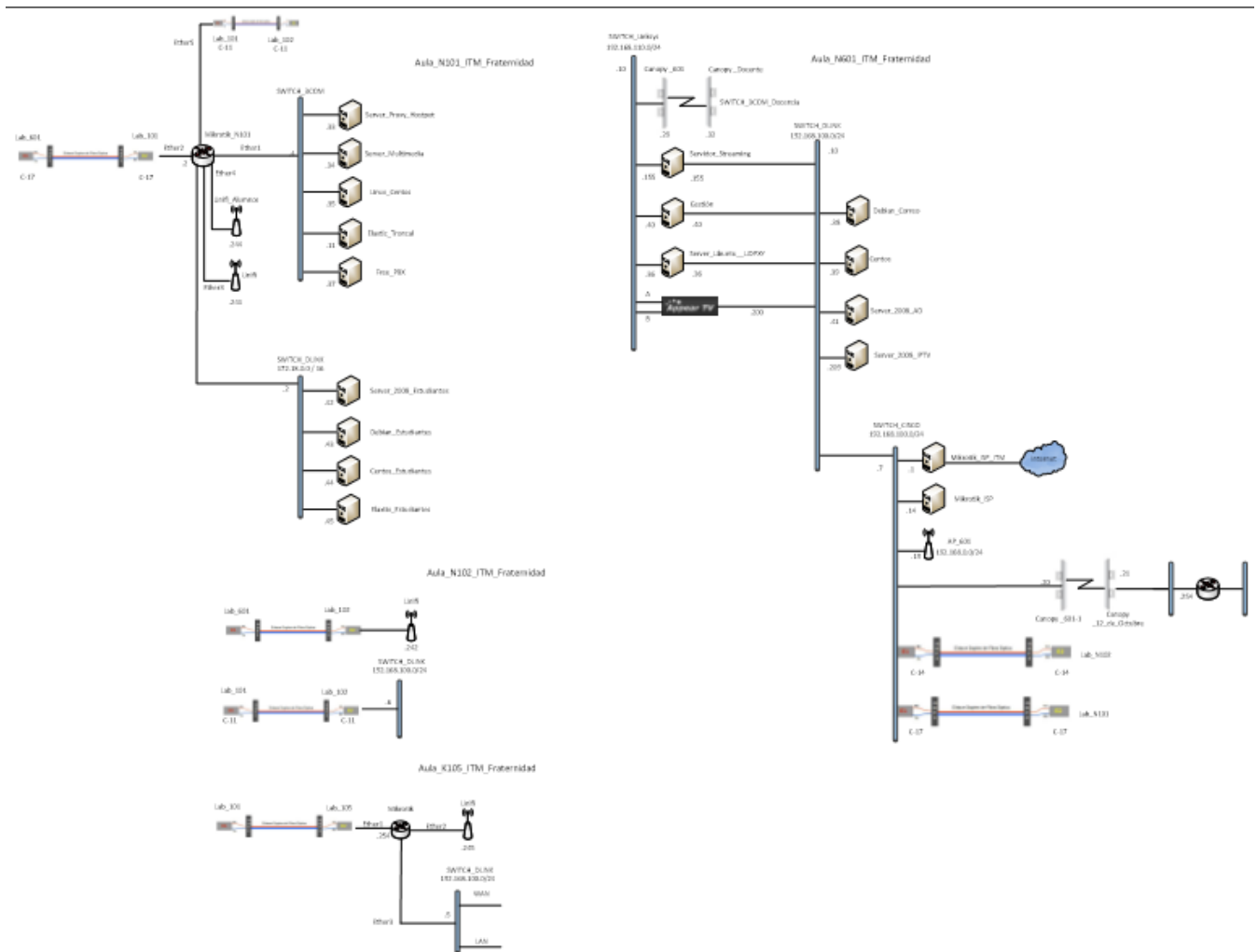


Imagen 2. Diagrama de red de la solución anterior.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

3.3 Fase 2. Diseño físico de la red:

En esta fase se realizó el movimiento de rack del piso N601 y organización del cableado. Los cables se encuentran totalmente etiquetados al igual que los puertos de cada Router nombrados según el enlace que está conectado:



Figura 5. Rack donde está ubicado N601

3.4 Fase 3. Diseño lógico de la red:

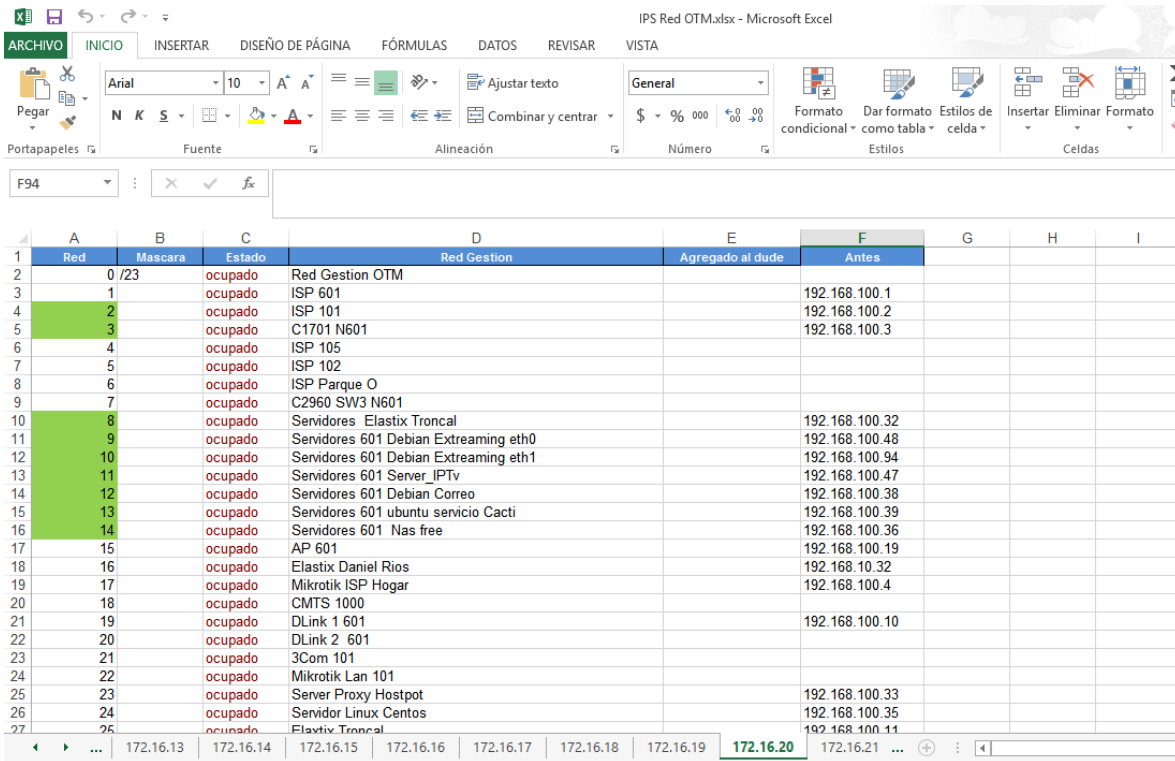
Para solucionar los inconvenientes encontrados en el ítem anterior, se realiza el siguiente diseño lógico:

- . Se realiza la configuración de una Vlan de id 100 que conecta a nivel lógico los equipos de la red OTM, lo anterior con el fin de segmentar el tráfico de gestión de otro tipo de tráfico (tráfico internet, datos, etc).

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

- Se asignó y configuro la red 172.16.20.0/23. Esta red alcanza a gestionar hasta 510 dispositivos.

Con el fin de mantener un control para la asignación de Ips de gestión para nuevos equipos se anexa en este trabajo de grado un archivo en Excel donde se encuentra el detalle de las IPs asignadas a cada equipo y las libres para asignar:



| | A | B | C | D | E | F | G | H | I |
|----|-----|---------|---------|---------------------------------------|-------------------|----------------|---|---|---|
| | Red | Mascara | Estado | Red Gestion | Agregado al dunde | Antes | | | |
| 2 | 0 | /23 | ocupado | Red Gestion OTM | | | | | |
| 3 | 1 | | ocupado | ISP 601 | | 192.168.100.1 | | | |
| 4 | 2 | | ocupado | ISP 101 | | 192.168.100.2 | | | |
| 5 | 3 | | ocupado | C1701 N601 | | 192.168.100.3 | | | |
| 6 | 4 | | ocupado | ISP 105 | | | | | |
| 7 | 5 | | ocupado | ISP 102 | | | | | |
| 8 | 6 | | ocupado | ISP Parque O | | | | | |
| 9 | 7 | | ocupado | C2960 SW3 N601 | | | | | |
| 10 | 8 | | ocupado | Servidores Elastix Troncal | | 192.168.100.32 | | | |
| 11 | 9 | | ocupado | Servidores 601 Debian Extreaming eth0 | | 192.168.100.48 | | | |
| 12 | 10 | | ocupado | Servidores 601 Debian Extreaming eth1 | | 192.168.100.94 | | | |
| 13 | 11 | | ocupado | Servidores 601 Server IPTV | | 192.168.100.47 | | | |
| 14 | 12 | | ocupado | Servidores 601 Debian Correo | | 192.168.100.38 | | | |
| 15 | 13 | | ocupado | Servidores 601 ubuntu servicio Cacti | | 192.168.100.39 | | | |
| 16 | 14 | | ocupado | Servidores 601 Nas free | | 192.168.100.36 | | | |
| 17 | 15 | | ocupado | AP 601 | | 192.168.100.19 | | | |
| 18 | 16 | | ocupado | Elastix Daniel Rios | | 192.168.10.32 | | | |
| 19 | 17 | | ocupado | Mikrotik ISP Hogar | | 192.168.100.4 | | | |
| 20 | 18 | | ocupado | CMTS 1000 | | | | | |
| 21 | 19 | | ocupado | DLink 1 601 | | 192.168.100.10 | | | |
| 22 | 20 | | ocupado | DLink 2 601 | | | | | |
| 23 | 21 | | ocupado | 3Com 101 | | | | | |
| 24 | 22 | | ocupado | Mikrotik Lan 101 | | | | | |
| 25 | 23 | | ocupado | Server Proxy Hostpot | | 192.168.100.33 | | | |
| 26 | 24 | | ocupado | Servidor Linux Centos | | 192.168.100.35 | | | |
| 27 | 25 | | ocupado | Elastix Troncal | | 192.168.100.11 | | | |

Imagen 3. Archivo para control de IPs de Gestión.

- Se realizan diagramas de solución de cada diseño los cuales se pueden observar en los resultados de este trabajo de grado.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

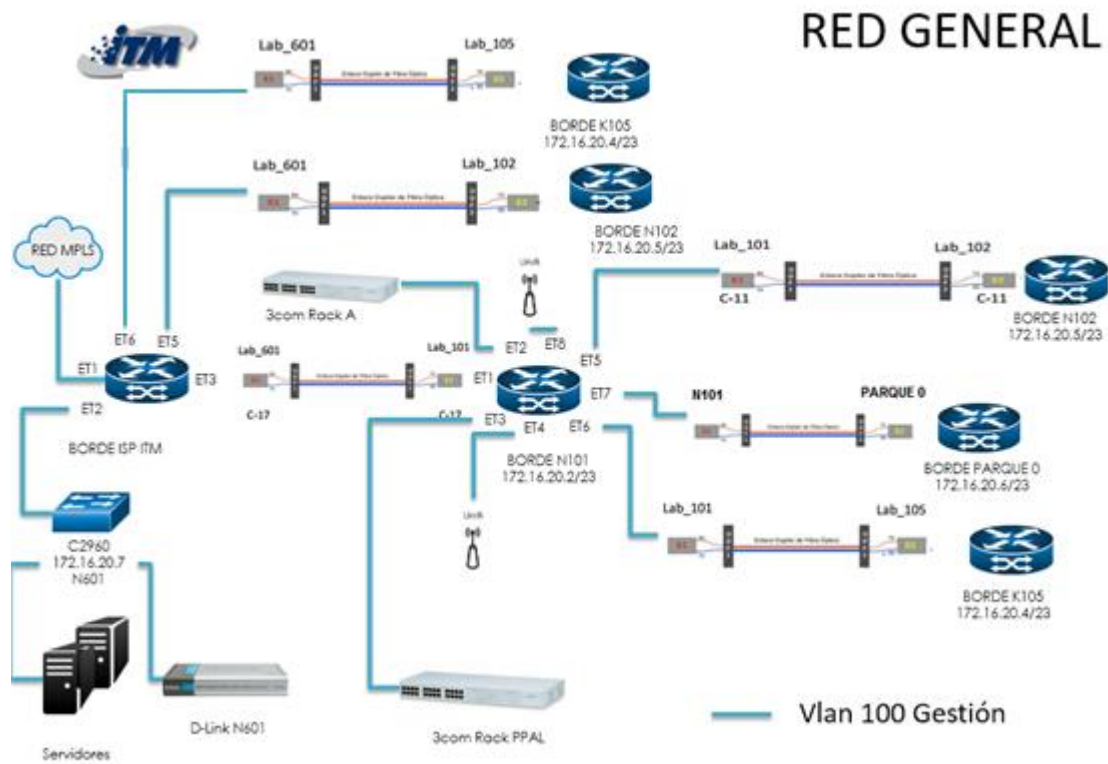


Imagen 4. Diagrama general de la red de gestión.

En el diagrama anterior, se puede observar la conexión por medio de fibra de cada Router de borde de cada aula con el Borde ISP y la conexión de los servidores del aula N601.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |



DISEÑO RED ISP 601

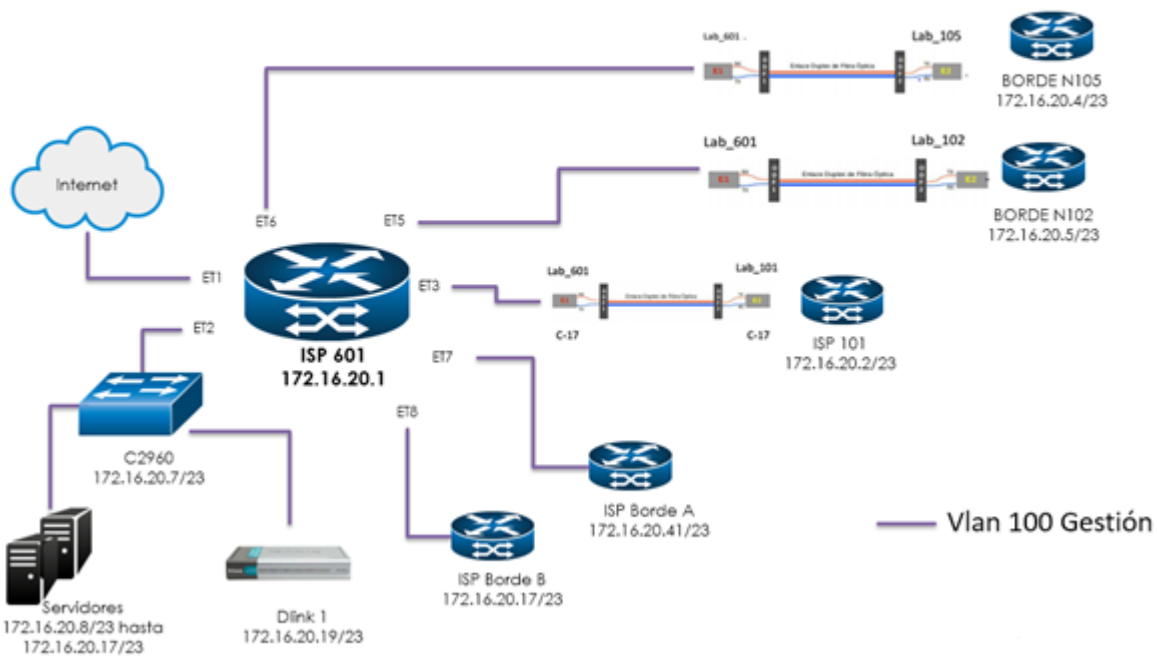


Imagen 5. Diagrama de la red de gestión aula N601.

En el diagrama anterior se puede observar un Router Borde ISP el cual recibe los servicios de la red MPLS entre ellos internet y se encarga de distribuirlo a los demás dispositivos de red. A este equipo de borde se conectan por medio de fibra oscura los Router de borde de las aulas K105, N102 y N101. De igual forma, a este Router de borde también se conecta un switch cisco C2960 que brinda servicio a los servidores del aula N601.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |



DISEÑO RED ISP 101

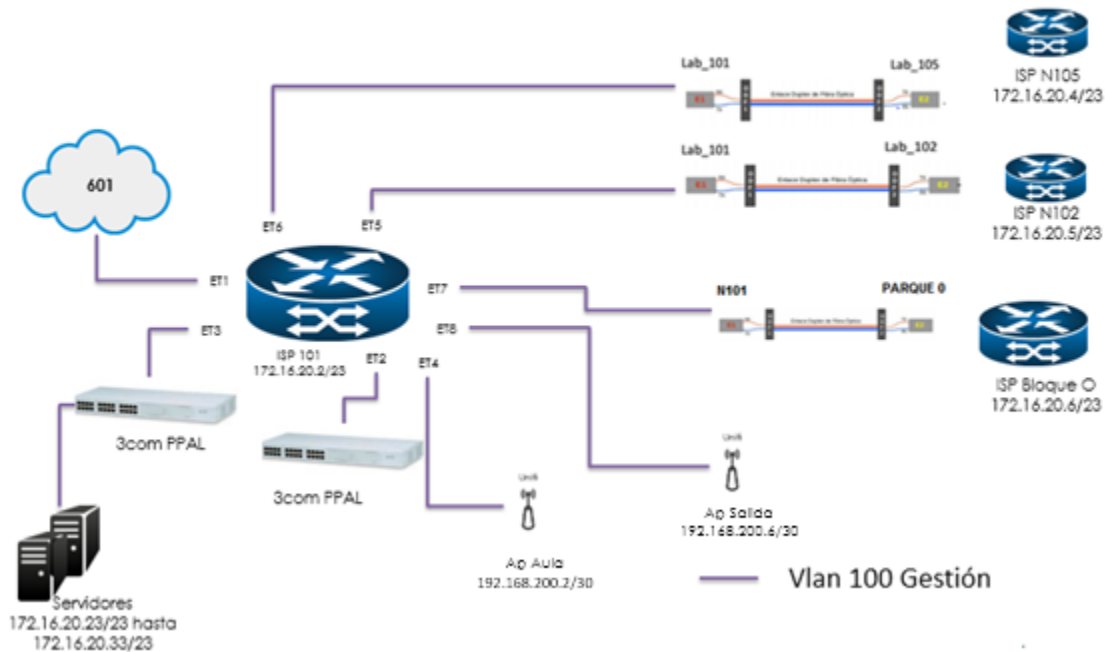


Imagen 6. Diagrama de la red de gestión aula N101.

En el diagrama anterior Allí se observa el Router de borde de esta aula el cual es el encargado canalizar el tráfico del aula N601 hasta la zona de bloque O como a los APs y servidores del aula. En esta aula también se cuenta con conexión en fibra hasta los Router de borde de las aulas N102 y K105 como respaldo.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

ISP PARQUE 0

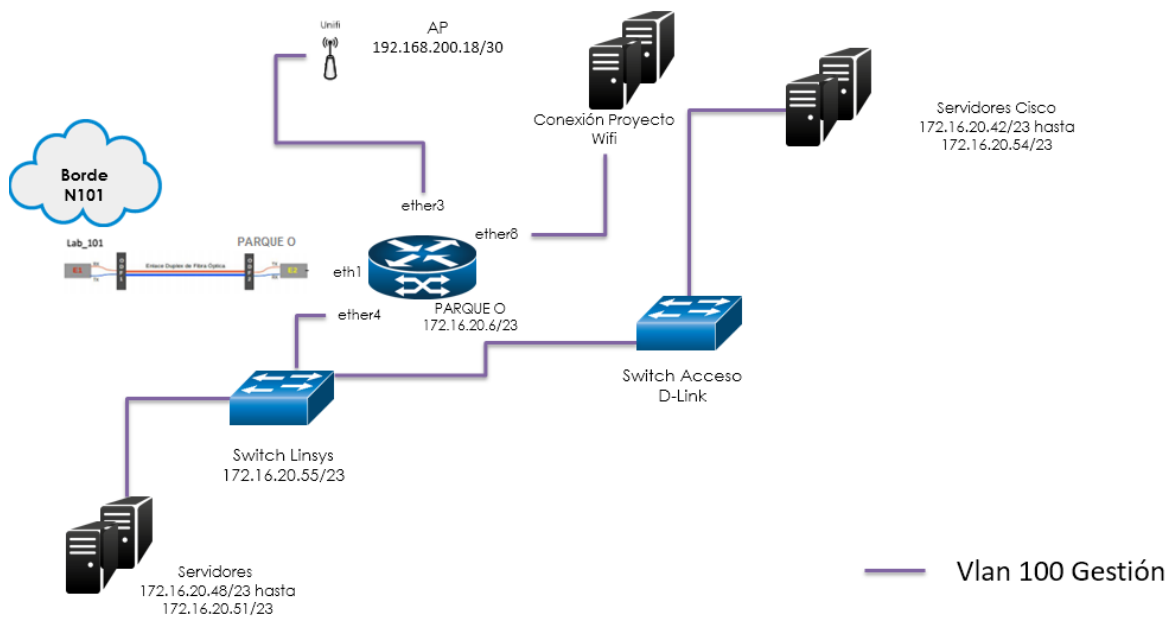


Imagen 7. Diagrama de la red de gestión aula Parque O.

En el diagrama anterior se observa la conexión del Router de borde de esa aula con el AP que brinda acceso inalámbrico a los usuarios y conexión a los servidores en sitio.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

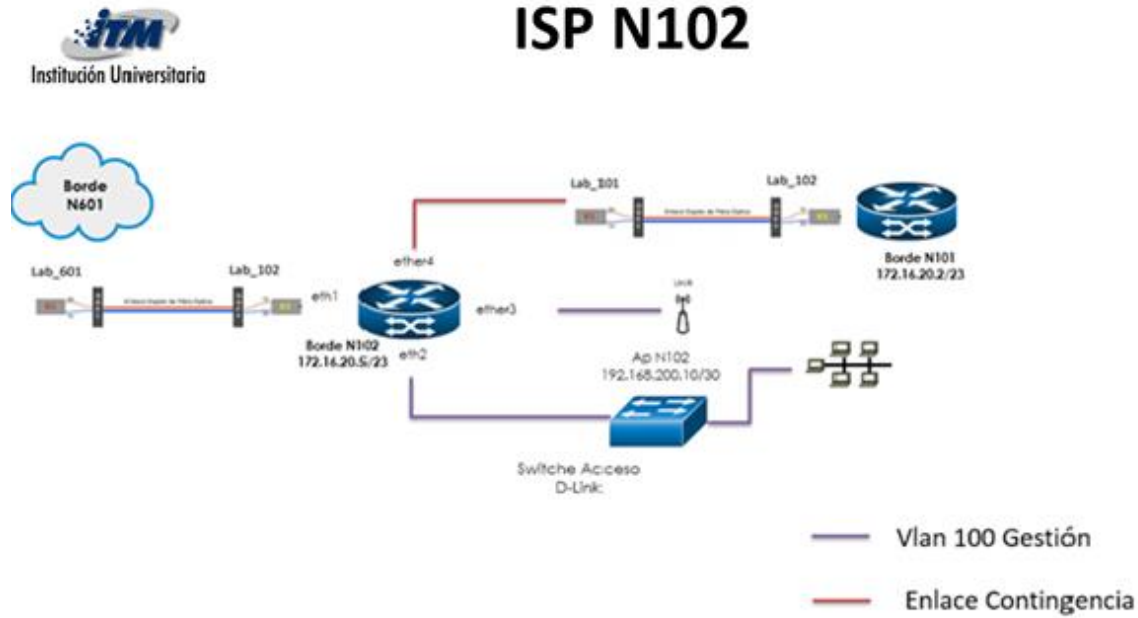


Imagen 8. Diagrama de la red de gestión aula N102.

En el diagrama anterior se observa la conexión del Router de borde de esa aula con el AP que brinda acceso inalámbrico a los usuarios y conexión a el switch al cual se conectan lo usuarios lan alámbricos. En esta aula se cuenta con un enlace de respaldo hacia el Borde N101.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

ISP N105

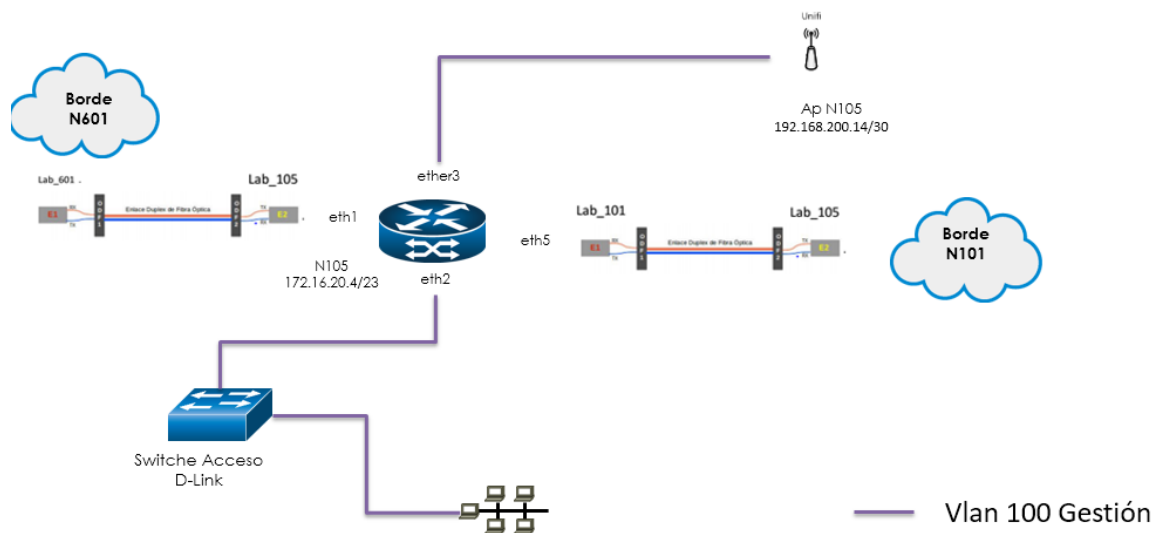


Imagen 9. Diagrama de la red de gestión aula N105.

En el diagrama anterior se observa la conexión del Router de borde de esa aula con el AP que brinda acceso inalámbrico a los usuarios y conexión a el Switches al cual se conectan lo usuarios lan alámbricos. En esta aula se cuenta con un enlace de respaldo hacia el Borde N101.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

RED WIFI

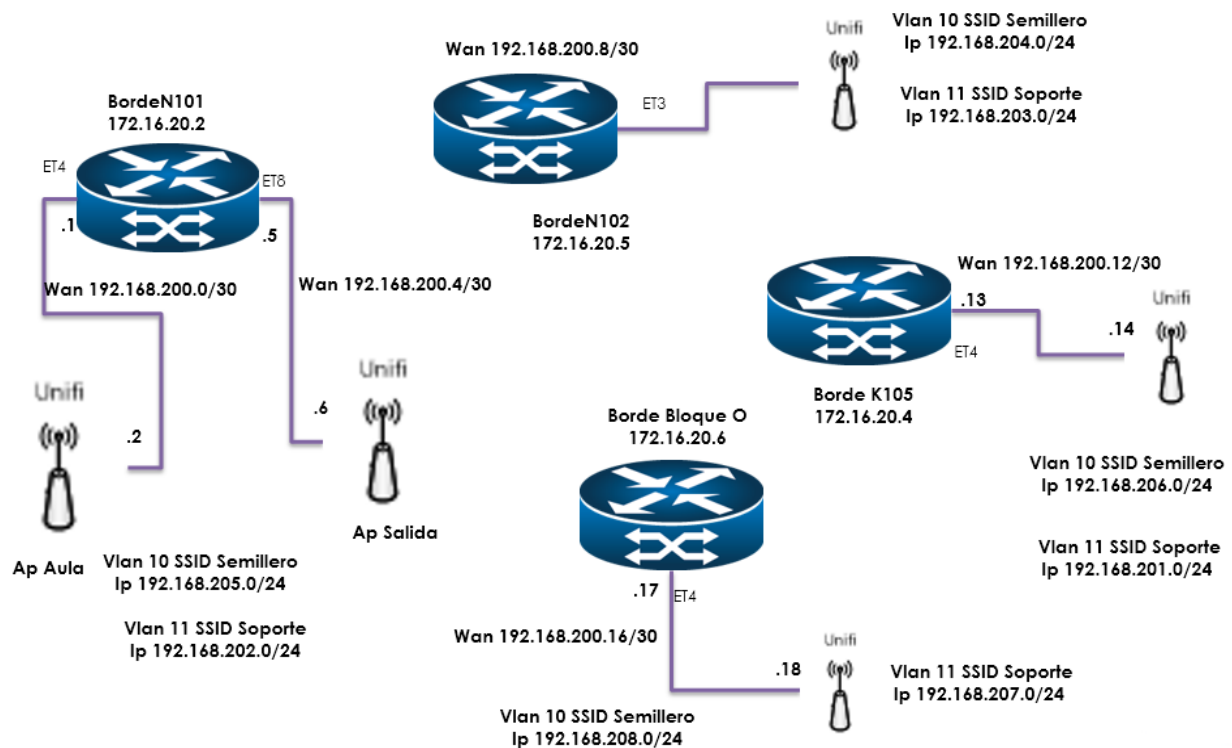


Imagen 10. Diagrama de conexión de la zona Wifi de la red OTM

En el diagrama anterior se puede observar la conexión a nivel lógico y cableado de cada AP Unifi a cada Router de borde de la red. Cada dispositivo está gestionado por Wan mascara 30 entre el Router y el AP, por medio de esta Wan se brinda internet al AP u con ello acceso a la controladora. Para la distribución de SSID, se crearon las vlans 10 y 11 para segmentar el tráfico

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

de SSID Semillero y SSID soporte. Los Router distribuyen DHCP con red mascara 24 por medio de la Vlan 10 y Vlan 11 de cada SSID.

A continuación se anexa una tabla resumen del direccionamiento utilizado en la zona Wifi

| Router | SSID | Red Wan | Red Lan |
|-----------------|-----------|--|------------------|
| N101 | Soporte | 192.168.200.0/30 AP Aula 192.168.200.4/30 Ap Salida | 192.168.202.0/24 |
| | Semillero | | 192.168.202.0/24 |
| K105 | Soporte | 192.168.200.12/30 | 192.168.201.0/24 |
| | Semillero | | 192.168.206.0/24 |
| N102 | Soporte | 192.168.200.8/30 | 192.168.203.0/24 |
| | Semillero | | 192.168.204.0/24 |
| BLOQUE O | Soporte | 192.168.200.16/30 | 192.168.207.0/24 |
| | Semillero | | 192.168.208.0/24 |

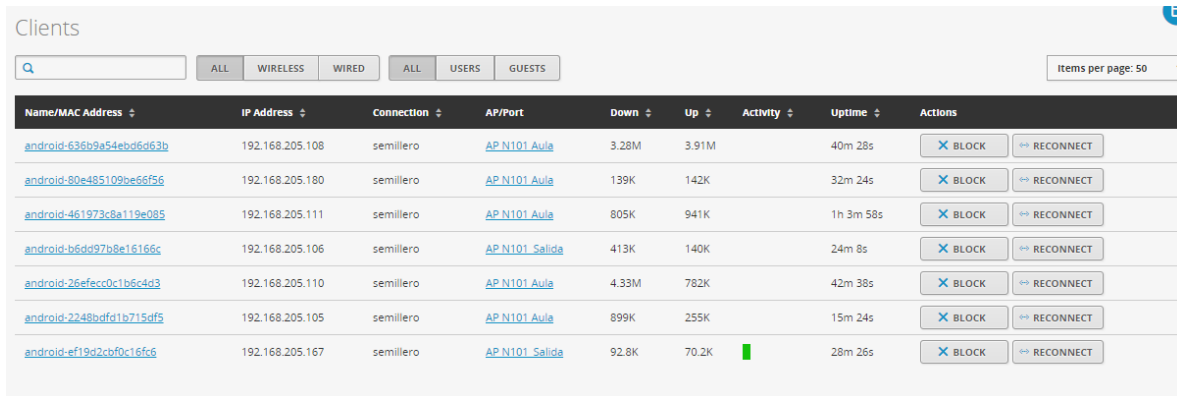
Tabla 1. Direccionamiento red Wifi OTM

En la anterior tabla se especificaron las direcciones IP utilizadas para la gestión de los AP y para la conectividad inalámbrica de los usuarios que utilizan la red OTM.

| | | | |
|---|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

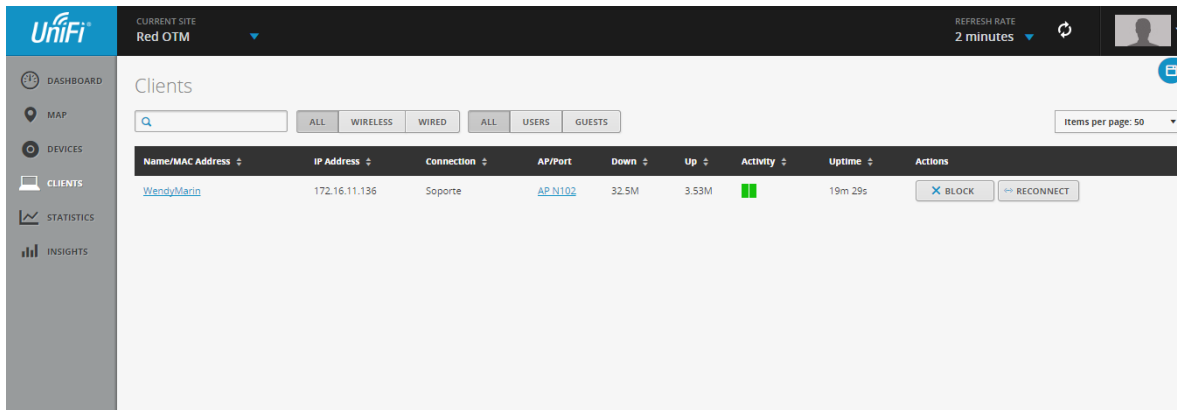
3.5 Fase 4. Pruebas de conectividad usuarios Wifi:

Para la red Wifi se realizaron pruebas de conectividad de usuarios:



| Name/MAC Address | IP Address | Connection | AP/Port | Down | Up | Activity | Uptime | Actions |
|---|-----------------|------------|--------------------------------|-------|-------|--------------------------------------|-----------|---|
| androidid-636b9a54ebd6d63b | 192.168.205.108 | semillero | AP N101 Aula | 3.28M | 3.91M | | 40m 28s | BLOCK RECONNECT |
| androidid-80e485109be66f56 | 192.168.205.180 | semillero | AP N101 Aula | 139K | 142K | | 32m 24s | BLOCK RECONNECT |
| androidid-461973c8a119e085 | 192.168.205.111 | semillero | AP N101 Aula | 805K | 941K | | 1h 3m 58s | BLOCK RECONNECT |
| androidid-b6d997b8e16166c | 192.168.205.106 | semillero | AP N101 Salida | 413K | 140K | | 24m 8s | BLOCK RECONNECT |
| androidid-26efec0c1b6c4d3 | 192.168.205.110 | semillero | AP N101 Aula | 4.33M | 782K | | 42m 38s | BLOCK RECONNECT |
| androidid-2248bdfc1b715df5 | 192.168.205.105 | semillero | AP N101 Aula | 899K | 255K | | 15m 24s | BLOCK RECONNECT |
| androidid-ef19a2cbfd0c16fc6 | 192.168.205.167 | semillero | AP N101 Salida | 92.8K | 70.2K | ■ | 28m 26s | BLOCK RECONNECT |

Imagen 11. Usuarios conectados al SSID Semillero



| Name/MAC Address | IP Address | Connection | AP/Port | Down | Up | Activity | Uptime | Actions |
|----------------------------|---------------|------------|-------------------------|-------|-------|--------------------------------------|---------|---|
| WendyMarin | 172.16.11.136 | Soporte | AP N102 | 32.5M | 3.53M | ■ | 19m 29s | BLOCK RECONNECT |

Imagen 12. Usuarios conectados al SSID Soporte

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

3. RESULTADOS Y DISCUSIÓN

En sede fraternidad de la universidad ITM se tiene una red alterna a la institucional llamada OTM, esta red es utilizada por el semillero de redes de la institución. Esta red cuenta con 3 Router marca Mikrotik modelo CCR1009-8G-1S-1S cada uno con 8 puertos ethernet en los cuales se conectan los APs marca unifi, switches marca cisco, 3Com y D-Link. Estos 3 Router están ubicados en las aulas N101, N601 y bloque O; en las aulas K105 y N102 no se cuentan con router mikrotik, allí se tiene switches que conectan los dispositivos de cada Lan.

Durante el levantamiento de información acerca de la red OTM se encuentra a nivel físico que los cables UTP conectados a cada puerto de los equipos no se encuentran debidamente etiquetados. Se observa algunos cables con falla en los conectores ya que al mínimo contacto el cable se desconecta de los puertos ocasionando falla en el servicio.

Para solucionar lo anterior, se realiza acompañamiento y ejecución en los trabajos de organización de los rack, cambio de cables UTP y reponchado de cables en el aula N601 en donde están ubicados los servidores y equipo borde la red.

A nivel lógico se encuentran todos los puertos ethernet de las routerboard Mikrotik de cada aula agregados a una interfaz virtual llamada bridge, esta configuración limita la creación de vlans porque automáticamente todos los puertos que están dentro del bridge quedan en modo acceso (cuando se configura más de una Vlan en un mismo puerto, este debe estar en modo troncal), de esta forma no se puede segmentar el tráfico de los servicios.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

Para solucionar la limitación anterior, se configura y se propaga una Vlan de id 100 que es la encargada de transportar el tráfico de gestión en todos los equipos administrables que componen la red OTM (APs, Mikrotik, cisco, linksys, servidores, etc). A continuación se indica cómo se realizó dicha configuración

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

3.1 Configuración Vlan ISP 601:

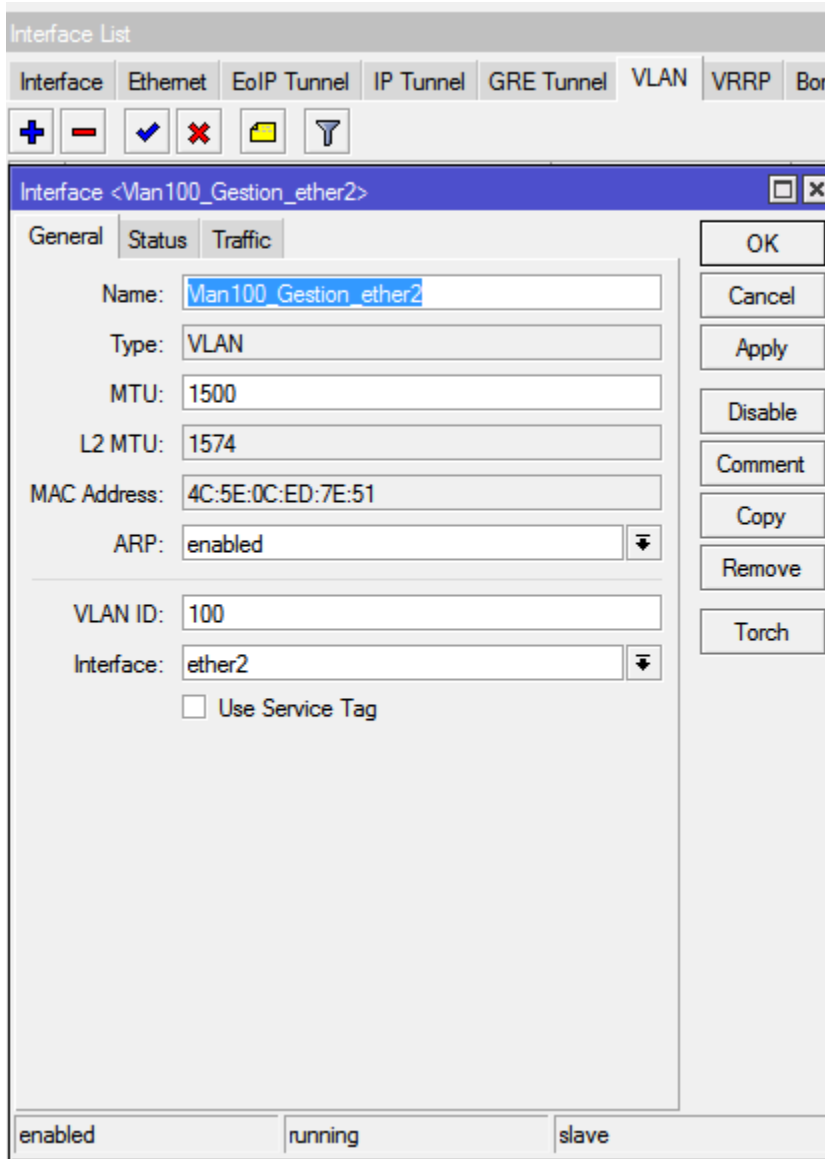


Imagen 13. Configuración de la Vlan 100 por Winbox. El procedimiento se realiza de la siguiente manera: Se da click en el icono (+) para agregar la interfaz vlan, solo es necesario colocar un nombre para identificar la interfaz y el ID que identifica la vlan. Se agrega la vlan a la interfaz Ethernet por donde se va a propagar la red de gestión.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

```
[johana@BORDE ISP ITM] > interface vlan add name=Vlan100_Gestion_ether2 vlan-id=100 interface=ether2
```

Imagen 6. Configuración de la Vlan 100 por consola

Para unificar la Vlan 100 agregadas en cada puerto Ethernet, se crea un interfaz virtual (bridge):

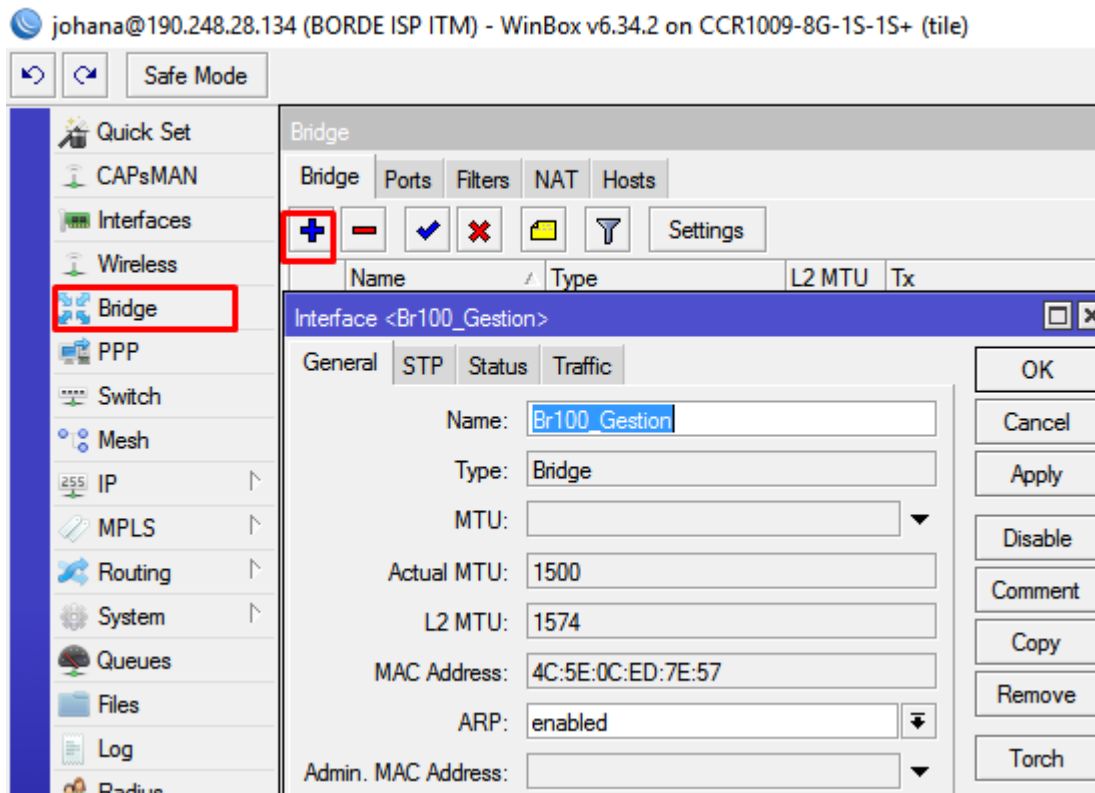


Imagen 14. Configuración del bridge 100 por Winbox. En la opción Bridge se agrega una nueva interfaz. Solo es necesario colocar un nombre para la identificación.

```
[johana@BORDE ISP ITM] > interface bridge add name=Br100_Gestion
```

Imagen 15. Configuración del bridge 100 por consola.

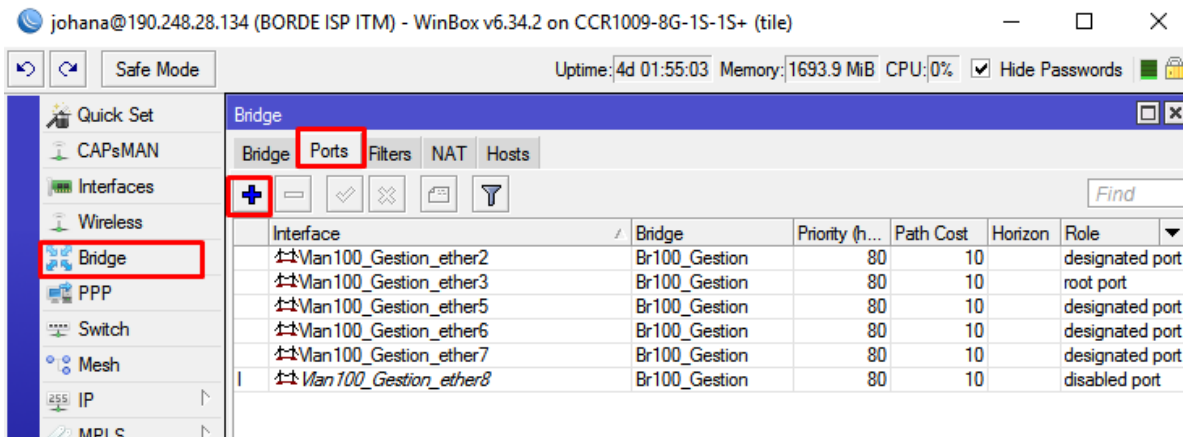


Imagen 16. Se agregan los puertos al bridge 100 por winbox. En el símbolo + se adicionan las vlans creadas en cada puerto Ethernet.

```
[johana@BORDE ISP ITM] > interface bridge port add interface=Vlan100_Gestion_ether2 bridge=Br100_Gestion
```

Imagen 10. Se agregan los puertos al bridge 100 por consola.

Para el monitoreo y gestión de los equipos se elimina la red 192.168.100.0/24, en su lugar se asigna y se configura la red 172.16.20.0/23 teniendo en cuenta que esta red puede soportar hasta 510 host. Cada Ip perteneciente a la red anterior se asigna a cada equipo Mikrotik o cisco administrable y se configura sobre el bridge al cuál se le agregaron todas las vlans de id 100 Br100_Gestión:

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

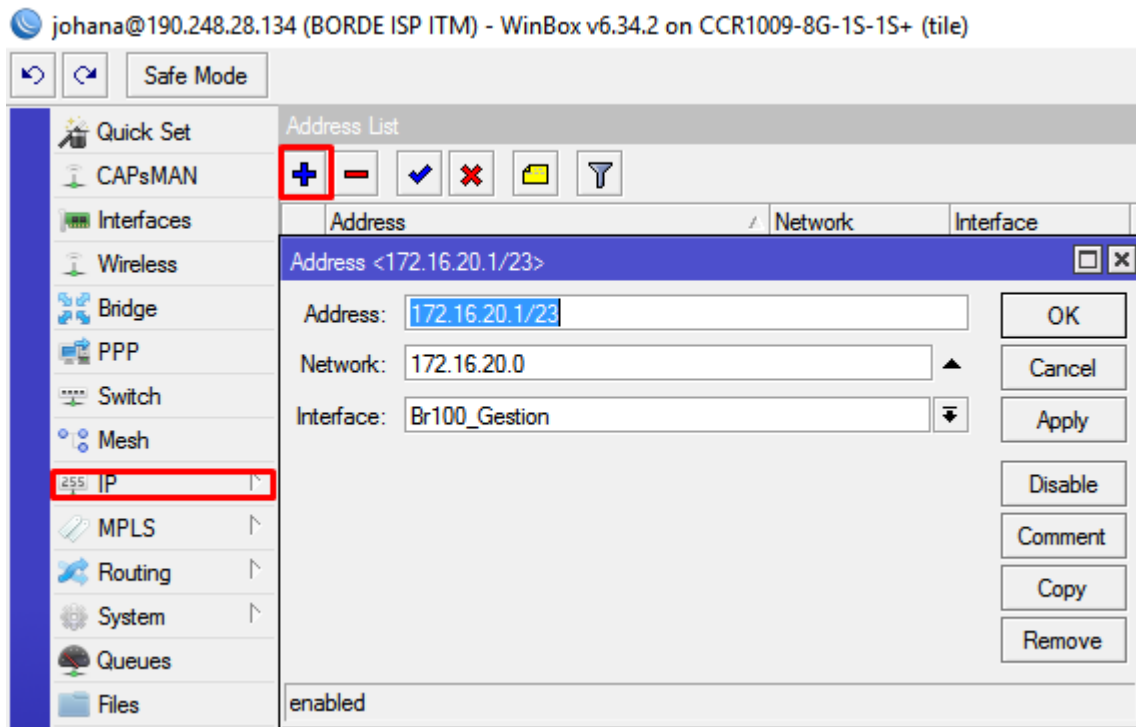


Imagen 17. Configuración de la IP de gestión sobre el bridge 100 por Winbox

```
[johana@BORDE ISP ITM] > ip address add address=172.16.20.1/23 interface=Br100_Gestion
```

Imagen 18. Configuración de la IP de gestión sobre el bridge 100 por consola

Los equipos que no son administrables y no se puede configurar la Vlan 100 están conectados directamente a los switches de acceso dentro de un bridge exclusivos para ellos.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

3.2 MEJORA ZONA WIFI

La zona Wifi de la red OTM está compuesta de equipos APs marca Unifi los cuales son gestionados por una controladora. Es por ello que para el control y configuración de los equipos se debe descargar el software libre propietario de Unifi: <https://www.ubnt.com/download/unifi>

Inicialmente se virtualiza una controladora general para administración y gestión de la zona Wifi para esta red, en una máquina Ubuntu virtual ubicada en los servidores del bloque O en donde se montó el paquete Ubuntu de la controladora de versión 4.8.18.

A la controladora se le asigna la IP 172.16.20.59 quedando con el siguiente acceso: <https://172.16.20.59:8443/>

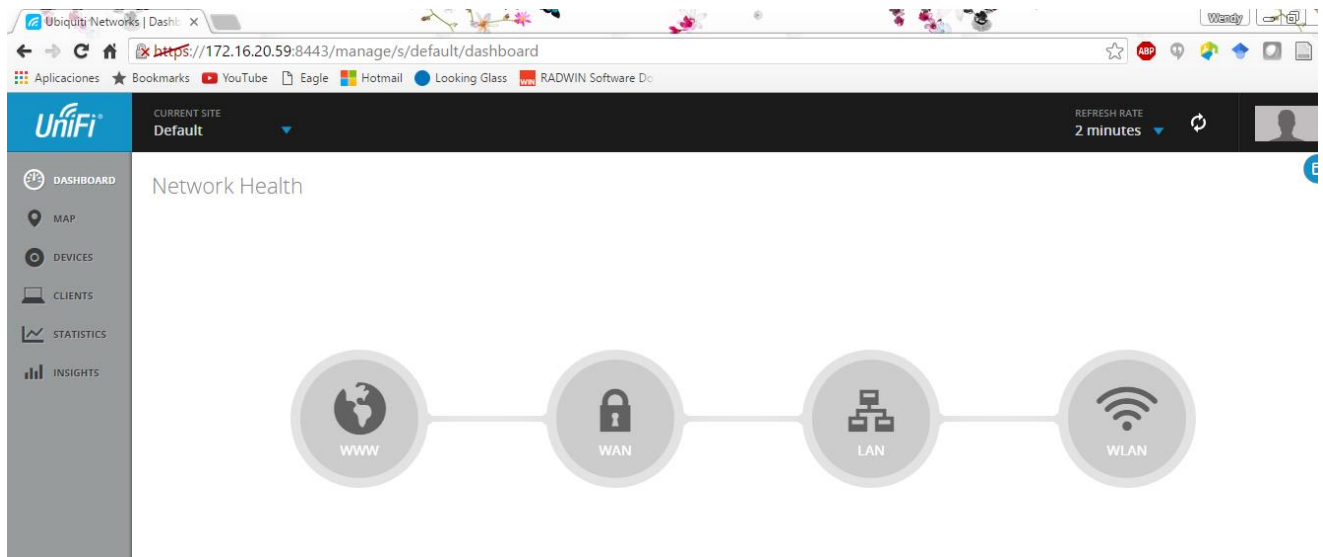


Imagen 19. Controladora Unifi después del logout

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

Allí se crean los SSID asignados para esta red:

SSID Semillero al cuál se le configura la vlan 10 para la asignacion de direccionamiento a los usuarios logueados en este SSID.

SSID Soporte al cuál se le configura la vlan 11 para la asignación de direccionamiento a los usuarios logueados en este SSID.

Se ingresa a la controladora con usuario admin/m1kr0flw, en el ítem settings-wireless network se agregan los SSID:

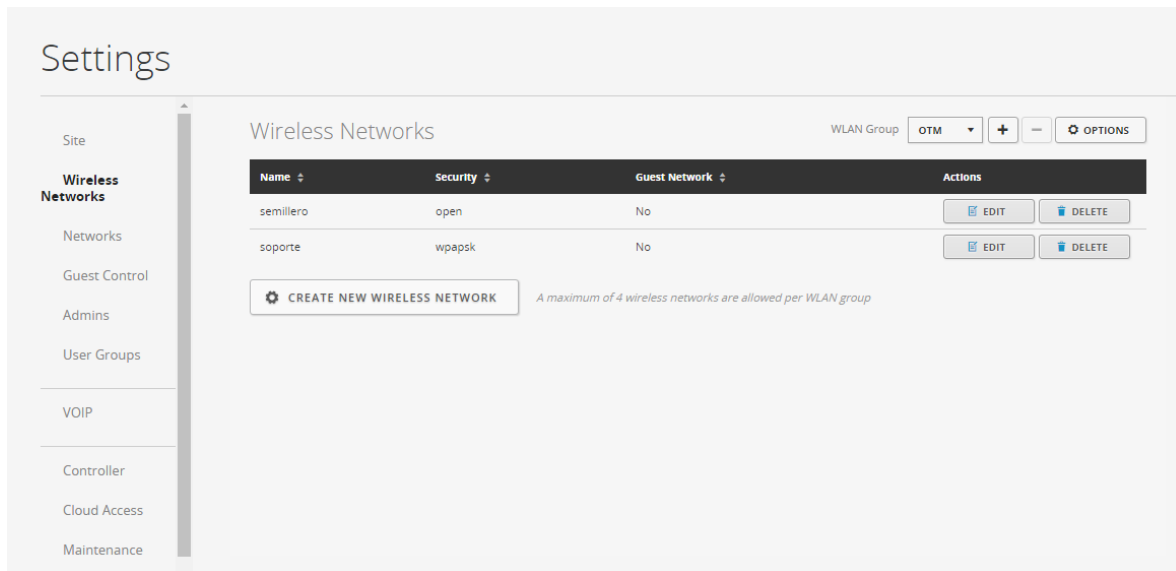


Imagen 20. Configuración del SSID en la controladora

| | | | |
|---|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

El SSID Semillero se le asigna la Vlan 10. Se deja el SSID abierto para que los estudiantes del ITM utilicen la red libremente:

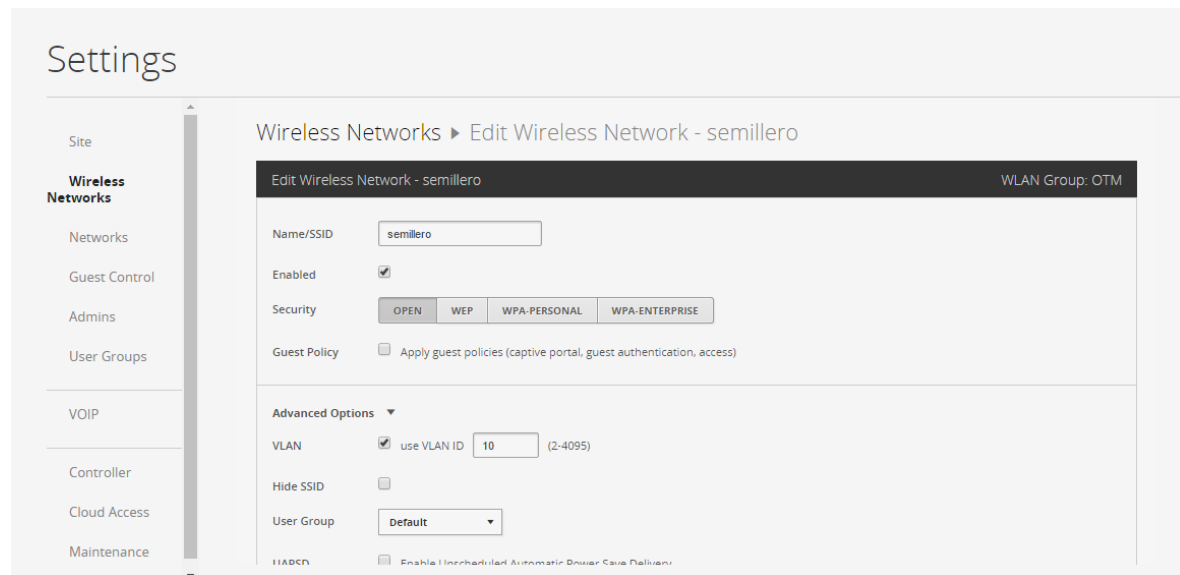


Imagen 21. Configuración del SSID Semillero en la controladora

El SSID Soporte se le asigna la Vlan 11. Se configura el protocolo WPA Personal con password sh0m4w1f1. Este SSID es solo para el uso de los administradores de la red OTM:

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

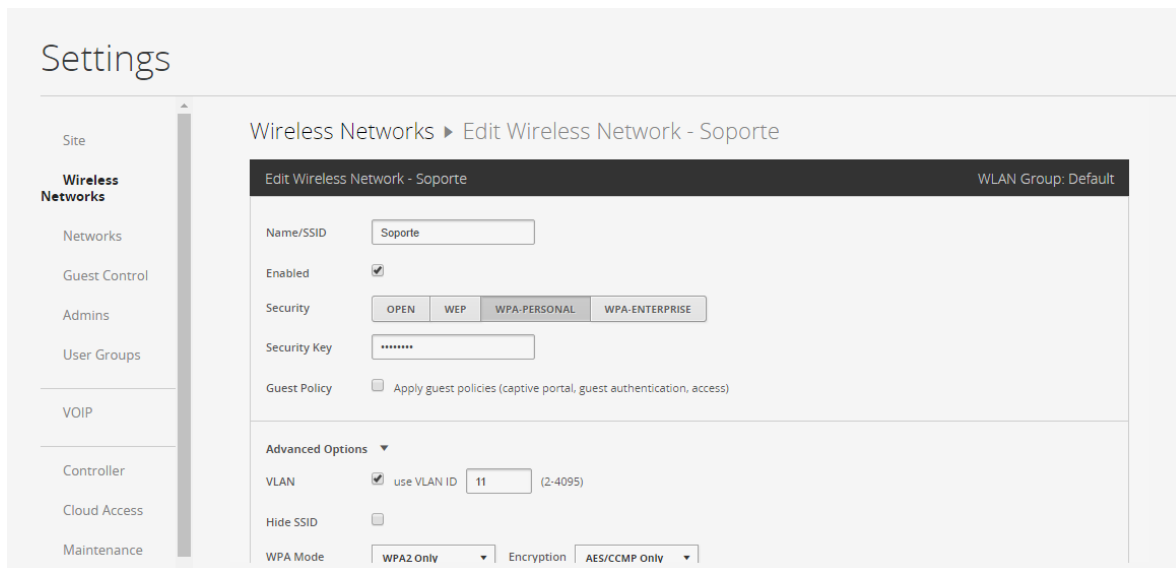


Imagen 22. Configuración del SSID Soporte en la controladora.

Teniendo en cuenta que los APs estaban en una controladora local, se realiza reset a cada dispositivo para ingresarlo así a la nueva controladora:

Se accede al AP por SSH y se ingresa el comando `syswrapper.sh restore-default`, después de esto el AP se reinicia:

```

BusyBox v1.11.2 (2015-05-31 16:46:25 PDT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

BZ.v3.2.12# syswrapper.sh restore-default
Found Backup1 on[1] ...
Found Active on[2] ...
Storing Active[1] ... [100]
Active->Backup[2] ... [100]
BZ.v3.2.12# █

```

Imagen 23. Reset a un AP unifi por consola.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

Con el programa Unifi Discovery instalado con anterioridad se escanea los APS recién reseteados:



Imagen 24. Escáner de los APs con Unifi Discovery.

En la opción manage se ingresa la IP de la controladora para que el AP se autentique, en la URL se escribe `http://172.16.20.59:8080/inform:`

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

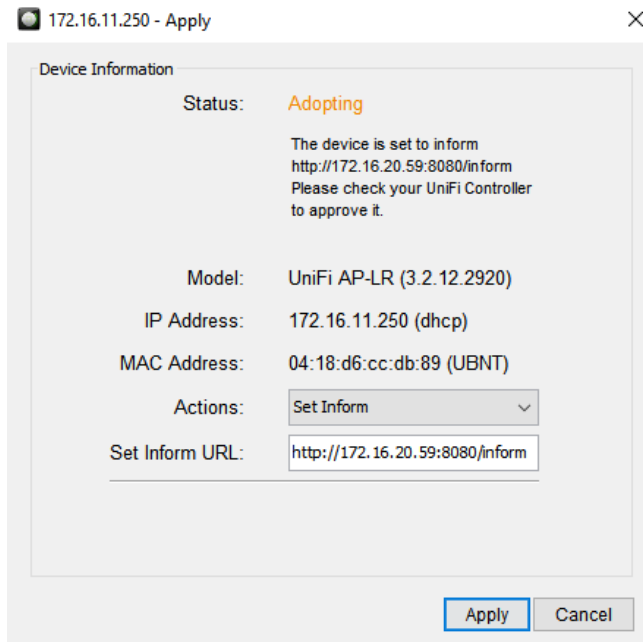


Imagen 25. Configuración de controladora en el AP.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

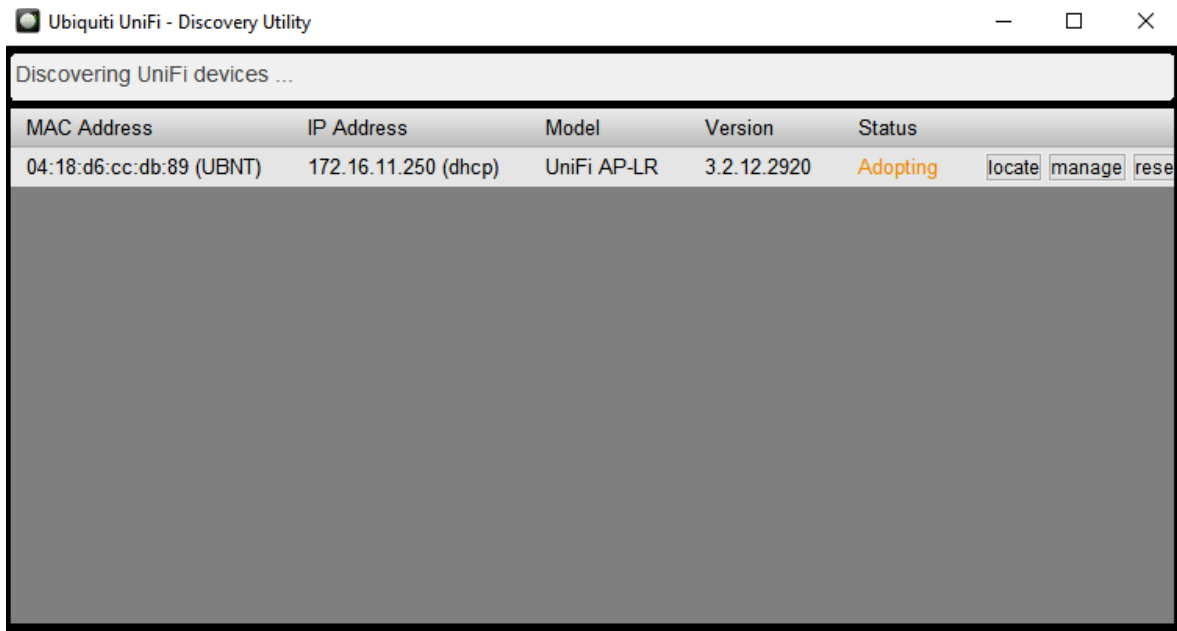


Imagen 26. Estado del Ap antes de que la controladora lo adopte.

En la controladora ya aparece el AP que se acabó de configurar, se debe adoptar:

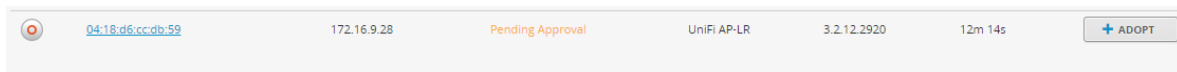


Imagen 27. Ap pendiente de que la controladora lo adopte.

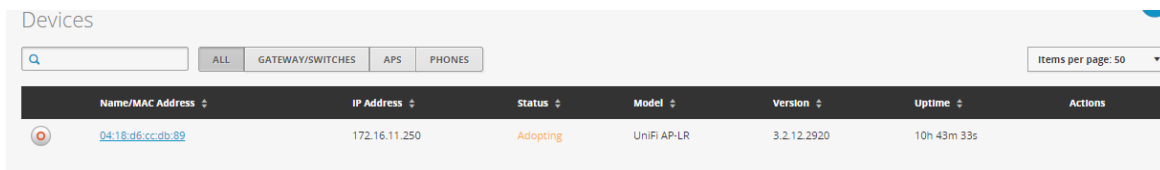


Imagen 28. Estado del AP en la controladora después de adoptarlo.

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

Después de que el AP se ha autenticado con la controladora, su estado es conectado. En caso de que el AP tenga una versión menor a la de la controladora, esta habilitará la opción para que se actualice:

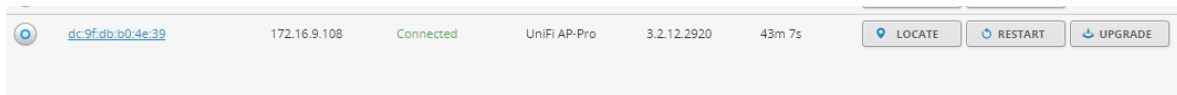


Imagen 29. Ap en la controladora listo para actualización.

Después de realizar la actualización el AP queda en conectado. Se realiza el anterior procedimiento con todos los APs:

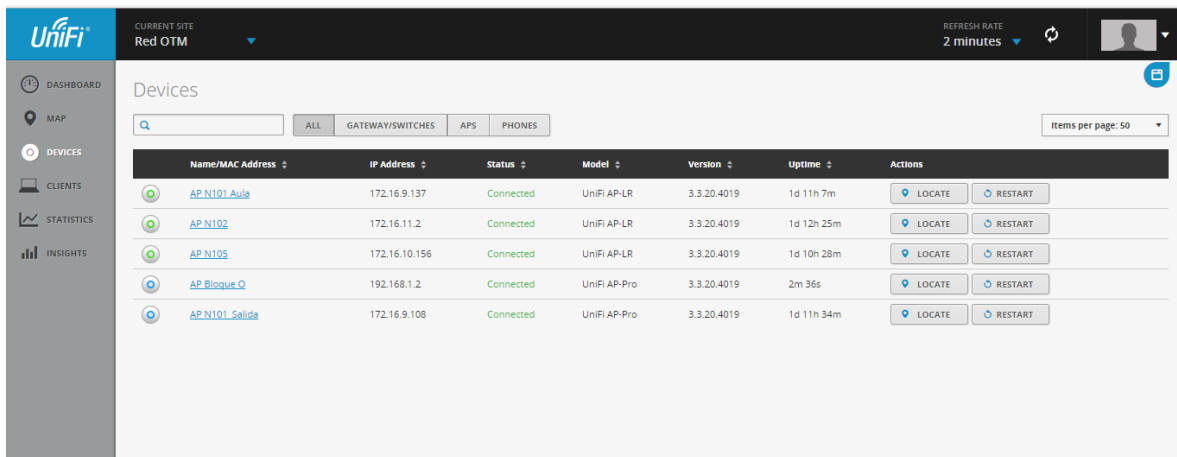


Imagen 30. AP en la controladora listo para actualización.

Después de que los APs estén operativos, los usuarios se empiezan a conectar:

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

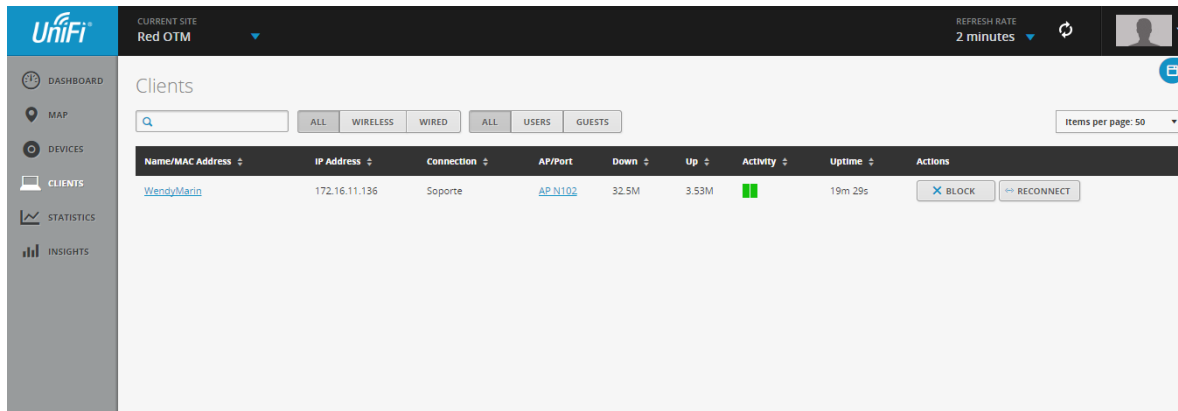


Imagen 31. Usuario operando en la controladora.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

3.3 IMPLEMENTACIÓN DE SEGURIDAD BÁSICA EN LA RED

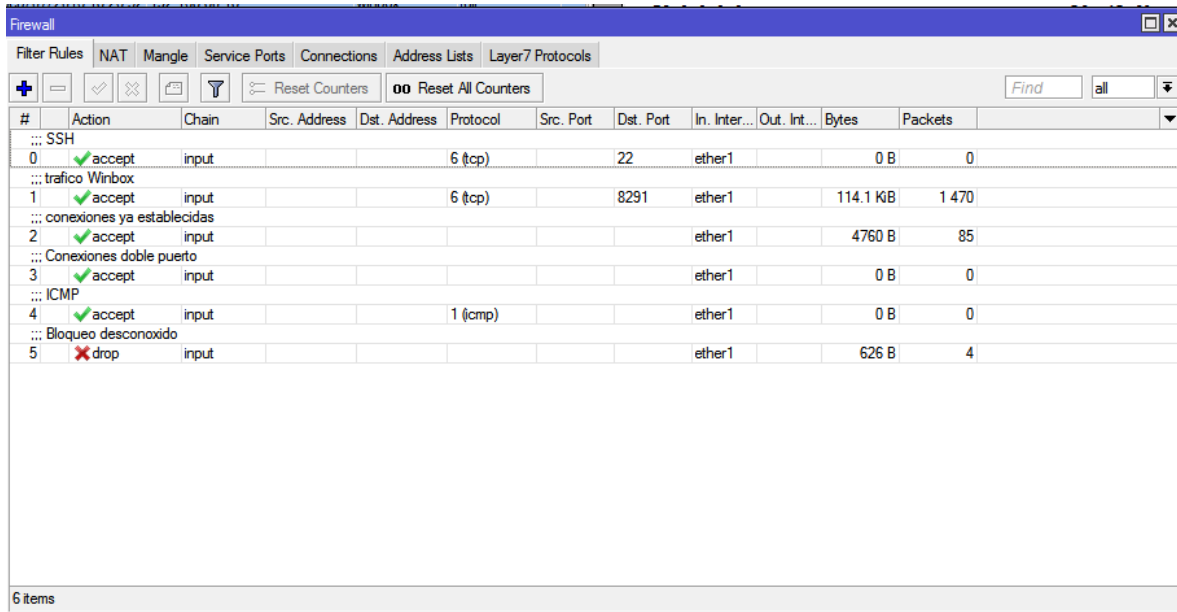
En el equipo de borde N601 se implementó una política de seguridad para que el Router esté protegido de ataques de entrada:

Se ejecutó la siguiente serie de comandos en la consola del Router N601:

- `/ip firewall filter add chain=input comment=SSH dst-port=22 in-interface=ether1 protocol=tcp`: con esta regla se está permitiendo el acceso por SSH al Router.
- `/ip firewall filter add action=accept chain=input comment="trafico Winbox" disabled=no dst-port=8291 in-interface=ether1 protocol=tcp`: con esta regla se está permitiendo el acceso por winbox al Router.
- `/ip firewall filter add action=accept chain=input comment="conexiones ya establecidas" connection-state=established disabled=no in-interface=ether1`: con esta regla se está permitiendo las conexiones que ya se había establecido con anterioridad en el Router.
- `/ip firewall filter add action=accept chain=input comment="Conexiones doble puerto" connection-state=related disabled=no in-interface=ether1`: con esta regla se está permitiendo las conexiones que las conexiones de tengan un nat con doble puerto.
- `add action=drop chain=input comment="Bloqueo desconocido" disabled=no in-interface=ether`: con esta regla se está bloqueando todo el tráfico desconocido que no cumpla con el perfil de las reglas creadas anteriormente.

```
[johana@BORDE ISP ITM] > /ip firewall filter
[johana@BORDE ISP ITM] /ip firewall filter> add chain=input comment=SSH dst-port=22 in-interface=ether1 protocol=tcp
[johana@BORDE ISP ITM] /ip firewall filter> add action=accept chain=input comment="trafico Winbox" disabled=no dst-port=8291 in-interface=ether1 protocol=tcp
[johana@BORDE ISP ITM] /ip firewall filter> add action=accept chain=input comment="conexiones ya establecidas" connection-state=established disabled=no in-interface=ether1
[johana@BORDE ISP ITM] /ip firewall filter> add action=accept chain=input comment="Conexiones doble puerto" connection-state=related disabled=no in-interface=ether1
[johana@BORDE ISP ITM] /ip firewall filter> add chain=input comment=ICMP in-interface=ether1 protocol=icmp
[johana@BORDE ISP ITM] /ip firewall filter> add action=drop chain=input comment="Bloqueo desconocido" disabled=no in-interface=ether1
```

Imagen 32. Reglas de firewall creadas para proteger el borde N601 de ataques.



| # | Action | Chain | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Port | In. Inter... | Out. Int... | Bytes | Packets |
|---|----------|-------|--------------|--------------|----------|-----------|-----------|--------------|-------------|----------|---------|
| 0 | ✓ accept | input | | | 6 (tcp) | | 22 | ether1 | | 0 B | 0 |
| 1 | ✓ accept | input | | | 6 (tcp) | | 8291 | ether1 | | 114.1 KB | 1 470 |
| 2 | ✓ accept | input | | | | | | ether1 | | 4760 B | 85 |
| 3 | ✓ accept | input | | | | | | ether1 | | 0 B | 0 |
| 4 | ✓ accept | input | | | 1 (icmp) | | | ether1 | | 0 B | 0 |
| 5 | ✗ drop | input | | | | | | ether1 | | 626 B | 4 |

Imagen 33. Reglas de firewall creadas para proteger el borde N601 de ataques.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

3.4 IMPLEMENTACIÓN DE QoS

En una red es muy importante implementar políticas para aplicar calidad de servicio ya que son las que garantizan un correcto rendimiento de la red para el tráfico especial tal como VoIP. Para esta red se configuraron reglas simples en los bordes de cada aula.

En el ISP N601, por ser el borde de la red se crearon 2 reglas de QoS. La primera limita el ancho de banda de toda la red OTM con un máximo de 40M (ancho de banda asignado por la institución para esta red). En esta misma regla se configura el límite para que la red tenga un ancho de banda garantizado de 10M. La segunda limita el ancho de banda de cada ISP:

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

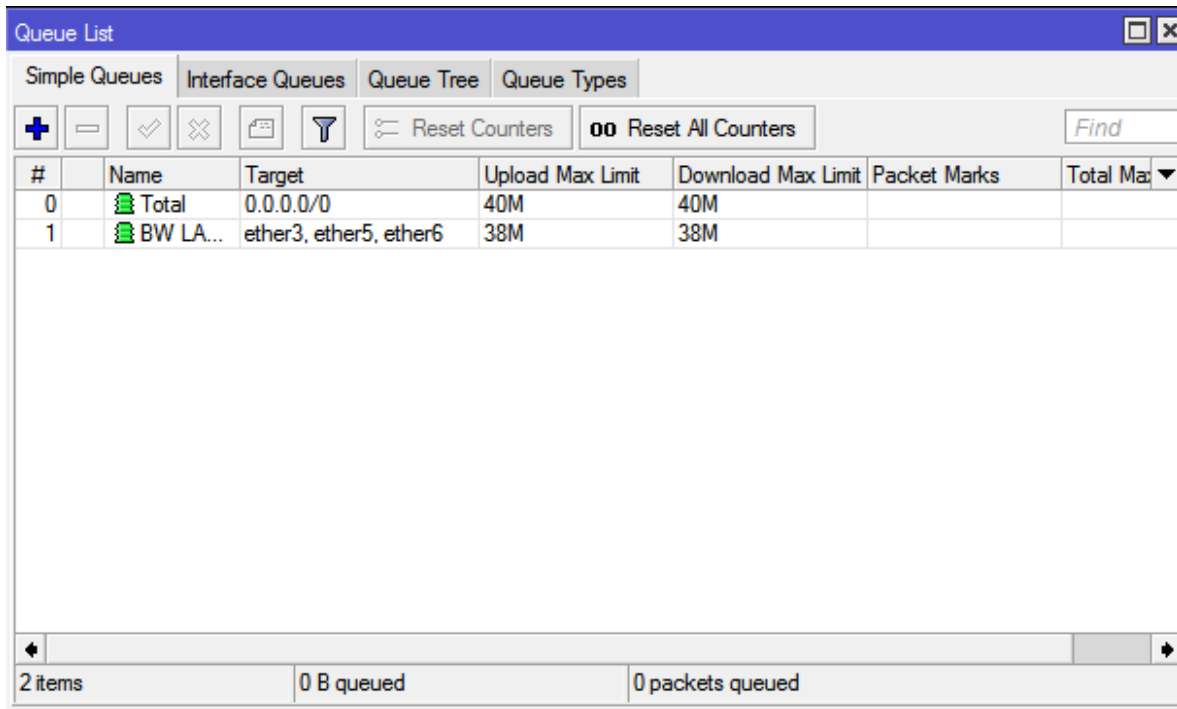


Imagen 34. Regla de QoS creada para los ISP N101, N102 y K105 en el borde N601. Se limita el BW total a 40M.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

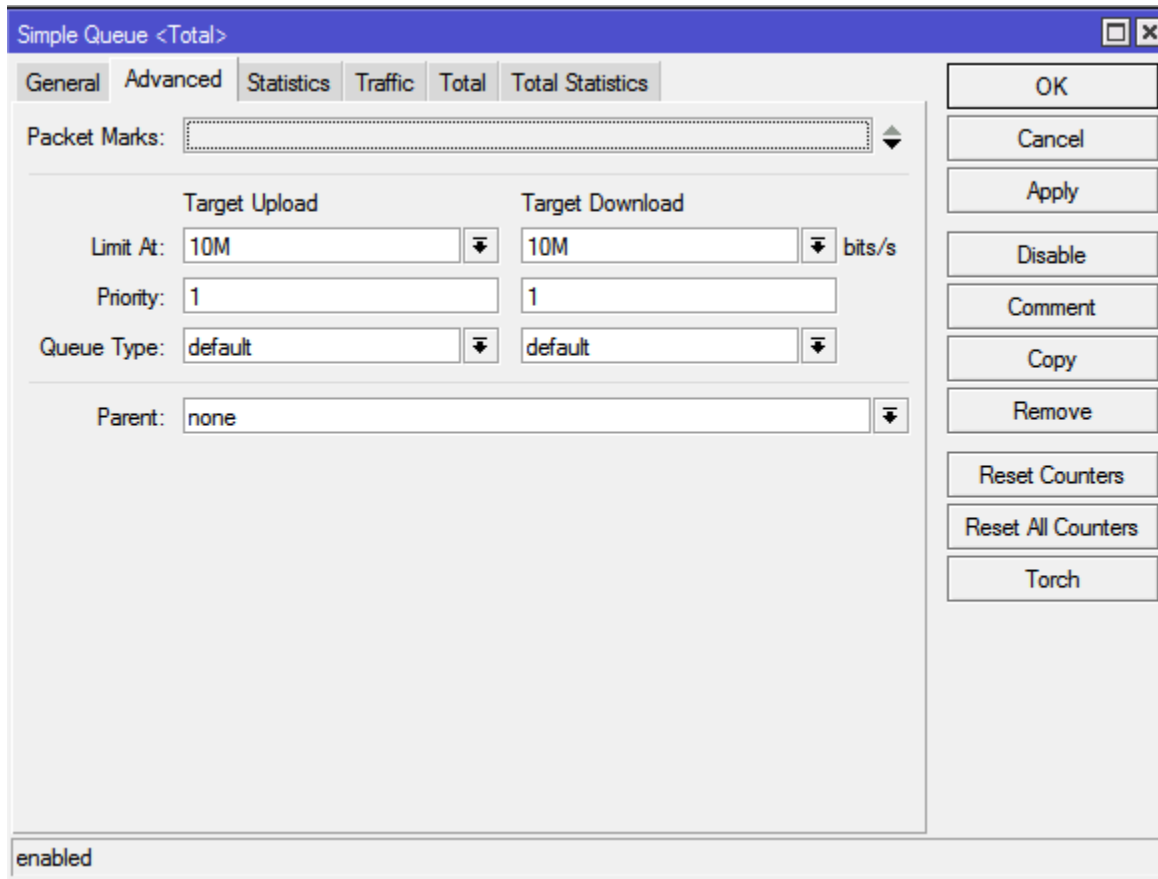


Imagen 35. Regla de QoS creada para los ISP N101, N102 y K105 en el borde N601. Se garantiza un ancho de banda para cada ISP de 10M.

En los Router ISP de las aulas N101, K105, N102 y bloque O se crearon reglas adicionales para garantizar el ancho de banda de las zonas Wifi. Para la red de soporte la cuál es utilizada por el personal que administra la red

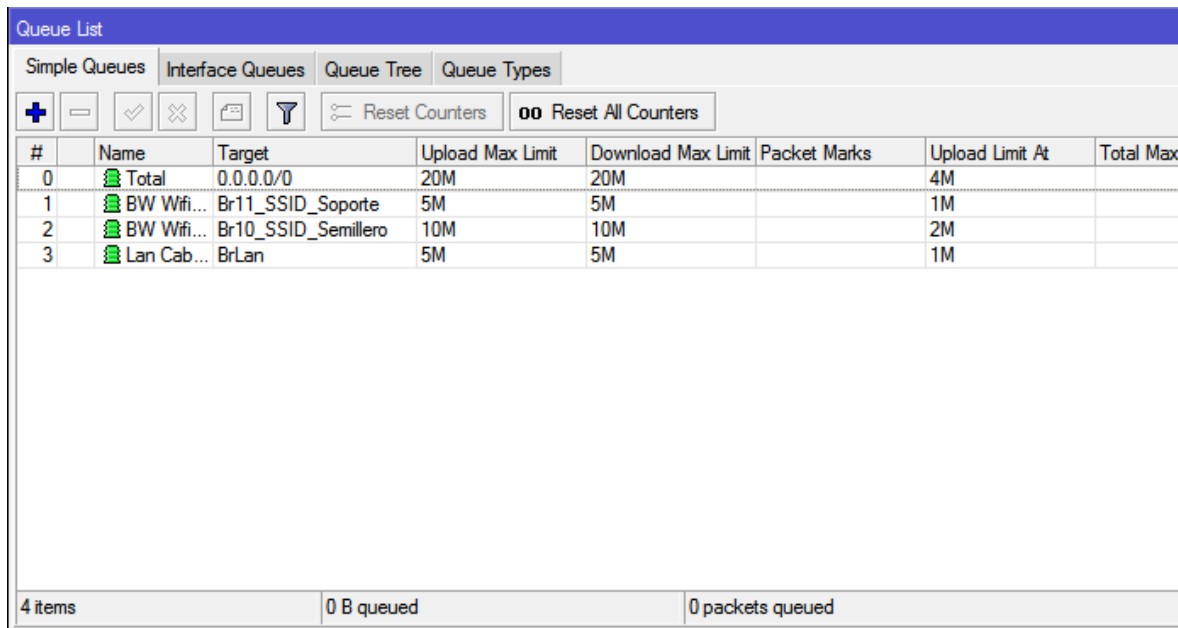
```
[johana@BORDE N101] > queue simple pr
Flags: X - disabled, I - invalid, D - dynamic
0 name="Total" target="" dst=ether1 parent=none packet-marks="" priority=1/1 queue=default-small/default-small limit-at=4M/4M max-limit=20M/20M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s

1 name="BW Wifi Soporte" target=Br11_SSID_Soporte dst=ether1 parent=Total packet-marks="" priority=8/8 queue=default-small/default-small limit-at=1M/1M max-limit=5M/5M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s

2 name="BW Wifi Semillero" target=Br10_SSID_Semillero parent=Total packet-marks="" priority=4/4 queue=default-small/default-small limit-at=2M/2M max-limit=10M/10M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s

3 name="Lan Cableada" target=BrLan parent=Total packet-marks="" priority=8/8 queue=default-small/default-small limit-at=1M/1M max-limit=5M/5M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s
```

Imagen 36. Regla de QoS creada para el ISP N101. Se garantiza un ancho de banda para cada ISP de 4M.



| # | Name | Target | Upload Max Limit | Download Max Limit | Packet Marks | Upload Limit At | Total Max |
|---|------------|---------------------|------------------|--------------------|--------------|-----------------|-----------|
| 0 | Total | 0.0.0.0/0 | 20M | 20M | | 4M | |
| 1 | BW Wifi... | Br11_SSID_Soporte | 5M | 5M | | 1M | |
| 2 | BW Wifi... | Br10_SSID_Semillero | 10M | 10M | | 2M | |
| 3 | Lan Cab... | BrLan | 5M | 5M | | 1M | |

4 items 0 B queued 0 packets queued

Imagen 37. De calidad de servicio aplicada para el salón N101

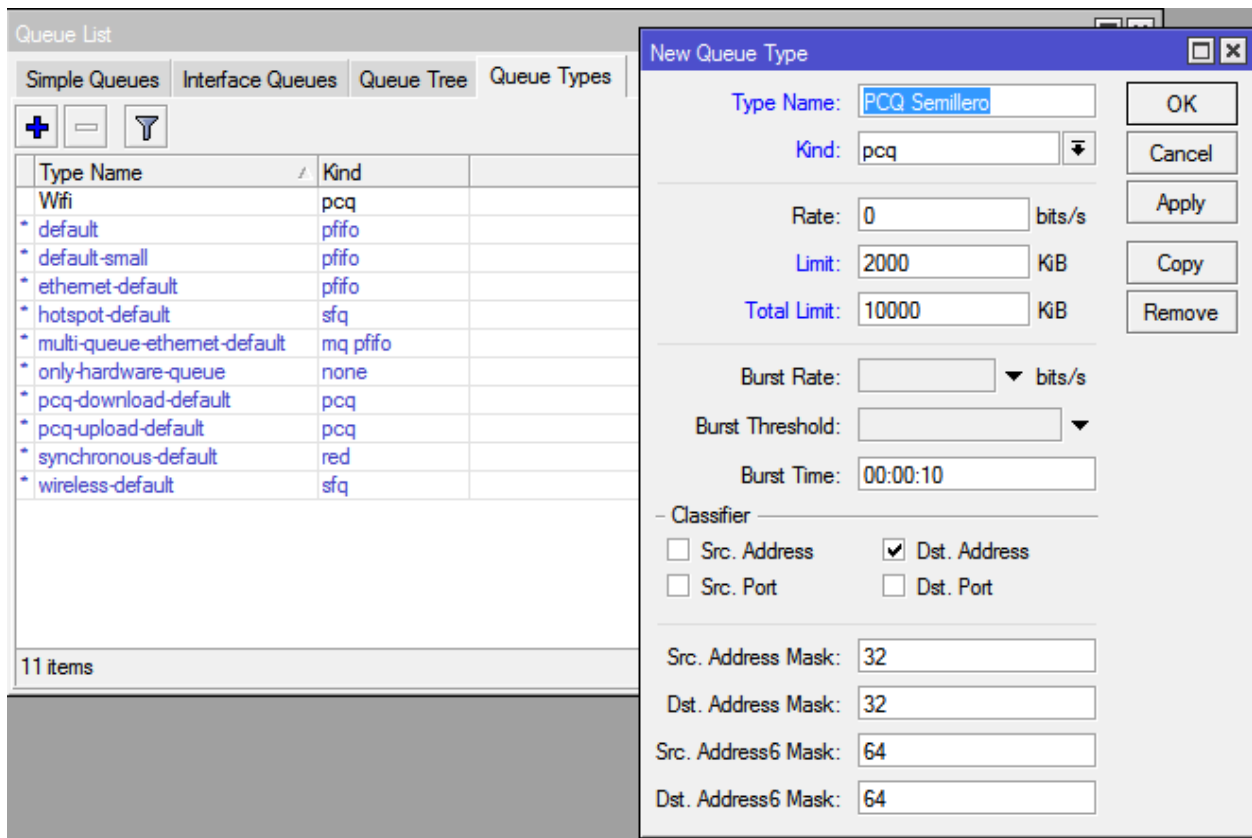


Imagen 38. Configuración de los Qos tipo PCQ

En la imagen anterior se observa el tipo de cola que se utilizó para distribuir el ancho de banda disponible entre los usuarios que se conecten a cada tipo de red alámbrica o inalámbrica de manera que se pueda optimizar al flujo de paquetes canalizados en la red.

Este procedimiento se realiza de la siguiente manera:

Al seleccionar la opción Queues tendremos acceso a la ventana de lista de colas, allí damos clic a la opción Queue Type, posterior a esto damos click en (+), es allí donde creamos el tipo de cola que deseamos utilizar. Nombramos la cola para identificar el tipo de red en la que se va a aplicar, en la parte de Kind se selecciona el tipo de cola, en este caso (pcq), posteriormente se despliega una lista de condiciones que definen los límites de ancho de banda a los que tendrán acceso los usuarios de la red. Ahora se aplica el tipo de cola en la ventana general:

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

```
[johana@BORDE N101] > queue simple prin
Flags: X - disabled, I - invalid, D - dynamic
0  name="Total" dst=ether1 parent=none packet-marks="" priority=1/1 queue=default-small/default-small limit-at=4M/4M
   max-limit=20M/20M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s

1  name="BW Wifi Soporte" target=Br11_SSID_Soporte dst=ether1 parent=Total packet-marks="" priority=8/8
   queue=PCQ Soporte/PCQ Soporte limit-at=1M/1M max-limit=5M/5M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s

2  name="BW Wifi Semillero" target=Br10_SSID_Semillero parent=Total packet-marks="" priority=4/4
   queue=PCQ Semillero/PCQ Semillero limit-at=2M/2M max-limit=10M/10M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s

3  name="Lan Cableada" target=BrLan parent=Total packet-marks="" priority=8/8 queue=PCQ Lan Cableada/PCQ Lan Cableada
   limit-at=1M/1M max-limit=5M/5M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s
[johana@BORDE N101] > █
```

Imagen 39. Creación de colas PCQ por consola.

| | | | |
|---|--|---------|------------|
|  | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

4. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

- Se realiza una mejora en la red OTM diseñando e implementando una red de gestión para el monitoreo y control de los equipos que la componen. En este diseño se propago una vlan de id 100 que es la encargada de transportar el tráfico de gestión. A nivel de capa 3 (según el modelo OSI) se configura la red 172.16.20.0/23 la cual soporta gestión de hasta 510 host. Para la red inalámbrica se implementa por SSID Vlans que aísle el tráfico de cada usuario. El SSID Soporte es utilizado solo por los usuarios que administran la red OTM, el SSID Semillero es utilizado para invitados y estudiantes que pertenezcan a un semillero de Telecomunicaciones.
- Durante el desarrollo de este trabajo se encontró falencias en los usuarios que administran la red, constantemente el cableado presenta fallas en los conectores, los Jack de los patch panel se deterioran por la constante manipulación, los equipos en los rack son reubicados y manipulados por el personal sin control alguno. Para lo anterior se recomienda la realización constante de capacitaciones sobre cableado estructurado y manipulación de equipos de red con el fin de mantener operatividad constante de la red.

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

REFERENCIAS

- Academia de cisco-CCNA-capitulo1-introducción a las redes.
- H. Li and Guangjing Chen, "Wireless LAN network management system," *Industrial Electronics, 2004 IEEE International Symposium on*, 2004, pp. 615-620 vol. 1.
doi: 10.1109/ISIE.2004.1571877
keywords: {computer network management;media streaming;mobile communication;protocols;wireless LAN;access point;mobile devices;simple network management protocol;wireless LAN network management system;wireless media streaming;wireless network performance;Access protocols;Automatic control;Computerized monitoring;Environmental management;Standards development;Streaming media;Technology management;Wireless LAN;Wireless application protocol;Wireless networks}, URL:
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1571877&isnumber=33258>
- D. Xiao, H. Li and Wendong Wang, "QoS management network," *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, 2003, pp. 320-323 vol.1.
doi: 10.1109/ICCT.2003.1209093
keywords: {IP networks;SONET;asynchronous transfer mode;computer network management;quality of service;telecommunication congestion control;telecommunication traffic;ATM;IP;Internet protocol;QoS management network;SONET;asynchronous transfer mode;frame relay;heterogeneous network;network traffic;quality of service;synchronous optical network;traffic control;Asynchronous transfer mode;Environmental management;Frame relay;Integrated circuit

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

technology;Laboratories;Quality of service;Resource management;SONET;Technology management;Telecommunication switching},

URL:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1209093&isnumber=272>

- K. Rojanakul and Hu Liang, "Network security infrastructure management," Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, Beijing, 2009, pp. 417-420.

doi: 10.1109/ICCSIT.2009.5234673

keywords: {Internet;computer network management;telecommunication security;IT infrastructure;Internet;network security infrastructure management;network stability;resources protection;security policy;Communication system security;Global communication;Internet;Protection;Stability;Network management;Strategic network plan},

URL:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5234673&isnumber=5234374>

- G. Di and G. Libin, "The Study of Security of Network Management Information System Based on Logistics Information Platform," Multimedia and Information Technology (MMIT), 2010 Second International Conference on, Kaifeng, 2010, pp. 227-230.

doi: 10.1109/MMIT.2010.87

keywords: {logistics data processing;management information systems;security of data;enterprise information management technology;logistics commerce;logistics information platform;network management information system security;server security control;transmit control;visit control;Authorization;Business;Computer hacking;Control systems;Information security;Internet;Logistics;Management information systems;Protection;Viruses (medical)},

URL:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5474367&isnumber=5474300>

| | | | |
|--|--------------------------------------|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

- *Cisco, Troubleshooting Input Queue Drops and Output Queue Drops, May 03, (2016)*

URL:

<http://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/6343-queue-drops.html>

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

ANEXOS

FDE146 Registro Actividades

| ITM | | MODALIDAD TRABAJO DE GRADO | | | | PRODUCTO OBTENIDO EN TALLERES O LABORATORIOS DEL ITM | |
|---|--|---|-------------|--|--------------------|--|------------|
| Institución Universitaria | | Registro de actividades y cumplimiento de horas / Talleres o Laboratorios de DOCENCIA | | | | Código | FDE 089 |
| | | | | | | Versión | 03 |
| | | | | | | Fecha | 2015-01-22 |
| Documento de identificación | | T. 156.1153.330 | | | | | |
| Número completo del estudiante | | Adrián Quiroga Torres | | | | | |
| Programa académico ITM | | Ing. Mecatrónica | | | | | |
| Número completo del Docente Asesor | | Prof. Dr. Juan Carlos | | | | | |
| Fecha de inicio del producto (semestre) | | 2014-01-20 | | Fecha de terminación del producto (semestre) | | | |
| Módulo Taller o Laboratorio | | Ejemplar | | | | | |
| Fecha | Actividad desarrollada por el estudiante | Hora ingreso | Hora salida | Tiempo horas | Firma Laboratorial | Firma Estudiantil | |
| 2015-01-24 | Spiga - estudiantes en creación de cables | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-01-25 | Suministro del hardware o software | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-01-26 | Planificación del diseño de la red (wired - wlan) | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-01-27 | Configuración de redes (wired - wlan) | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-01-28 | Planificación y diseño de firewall básico para la red (wired - wlan) | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-01-29 | Planificación y diseño de DNS para la red (wired - wlan) | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-01-30 | Revisión de los documentos de la clase del docente | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-01-31 | Pruebas y resultados de configuración de la red (wired - wlan) | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-02-01 | Pruebas y resultados de configuración de la red (wired - wlan) | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |
| 2015-02-02 | Pruebas y resultados de configuración de la red (wired - wlan) | 6:00 pm | 07:00 pm | 1 hora | | Adrián Quiroga Torres | |


| Fecha | Actividad | Inicio | Fin | Horas | Firma | Nombre |
|--------------------|---|----------|----------|--------|---------|--------------------|
| 2015-01-22 | Revisión y aprobación de contenido final en laboratorio | 08:00 am | 09:00 am | 1 hora | [Firma] | Juan Carlos Rivera |
| 2015-01-22 | Configuración de S3 | 08:00 am | 09:00 am | 1 hora | [Firma] | Juan Carlos Rivera |
| 2015-01-22 | Configuración Firewall | 08:00 am | 09:00 am | 1 hora | [Firma] | Juan Carlos Rivera |
| 2015-01-22 | Desconexión del laboratorio virtualizado | 08:00 am | 09:00 am | 1 hora | [Firma] | Juan Carlos Rivera |
| 2015-01-22 | Desconexión del laboratorio virtualizado | 08:00 am | 09:00 am | 1 hora | [Firma] | Juan Carlos Rivera |
| TOTAL HORAS | | | | | | |

Firma Estudiante
[Firma]
Nombre y firma Laborantista

Nombre y firma Profesional Universitario - Centro de Laboratorios

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

FDE90 Evaluación de Modalidad

| | | | | |
|--|---|--|---------|------------|
|  Institución Universitaria | EVALUACIÓN DE MODALIDAD TRABAJO DE GRADO Y PRÁCTICAS PROFESIONALES | | Código | FDE 090 |
| | | | Versión | 04 |
| | | | Fecha | 2015-10-05 |

INFORMACIÓN DEL TRABAJO DE GRADO

1. Título:

| | | | |
|---|--------------------|------------|--|
| DISEÑO E IMPLEMENTACIÓN DE RED DE GESTION | | | |
| Programa Académico: | Telecomunicaciones | Tecnología | Ingeniería <input checked="" type="checkbox"/> |

2. Modalidad Trabajo de Grado:

| | | | |
|---------------------------|--|---|--|
| Proyecto de Grado | Práctica Profesional | Emprendimiento | |
| Producto de Investigación | Producto obtenido en Talleres o Laboratorios ITM | <input checked="" type="checkbox"/> Pasantías | |
| Certificación | Reconocimiento Laboral | Cursos de Posgrado | |
| Ingeniería para la Gente | | | |
| Grupo de investigación: | | Código proyecto | |
| Tipo de Informe | Propuesta de Proyecto de Grado | Informe Final de Proyecto de Grado | |

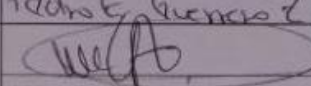
3. Información estudiante(s):

| | | |
|------------------------|------------|---------------------------------------|
| Nombre | Cédula | Correo electrónico |
| Johana Quintana Parias | 1128473550 | johanaquintana78723@correo.itm.edu.co |


4. Información asesor:

| | | |
|------------------------|-------------|--------------------------|
| Nombre | Institución | Correo electrónico |
| Pedro Enrique Guerrero | ITM | pedroguerrero@itm.edu.co |

CONCEPTO DEL JURADO EVALUADOR

| | | |
|---|---|--------------------|
| Concepto inicial sobre el trabajo de grado | | |
| Aprobado sin modificaciones | Se requieren modificaciones | Mención honorífica |
| Observaciones | | |
| Se puede anexar hojas adicionales para una descripción más amplia de las observaciones. Justificar en esta parte porqué otorgar mención honorífica. | | |
| | | |
| Nombre jurados evaluadores | Pedro E. Guerrero | |
| Firma |  | |
| | FECHA: 22/11/2016 | |

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

| | | | |
|--|--|---------|------------|
|  Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código | FDE 089 |
| | | Versión | 03 |
| | | Fecha | 2015-01-22 |

FIRMA ESTUDIANTES Johann Antonio Pavaas

FIRMA ASESOR Pedro Enrique Guerrero Zuluaga

FECHA ENTREGA: 22/11/2016

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO ___ ACEPTADO ___ ACEPTADO CON MODIFICACIONES ___

ACTA NO. _____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD _____

ACTA NO. _____

FECHA ENTREGA: _____