

DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN INTEGRAL DE TELECOMUNICACIONES Y RED PARA LA COOPERATIVA ORDEN Y SEGURIDAD Y LA COOPERATIVA SAN GREGORIO DE LA POLICÍA NACIONAL

Lenin Eduardo Villagómez Morillo, movi_len@hotmail.com

Abstracto — El presente trabajo muestra el diseño e implementación de una solución integral de telecomunicaciones y red para la Cooperativa Orden y Seguridad y la Cooperativa San Gregorio de la Policía Nacional, pasando por el análisis de la situación de la red, diseño e implementación de mejoras y solución de problemas, además pruebas de conexión y comunicación en la red de datos de las Cooperativas comparando y analizando resultados.

Keywords: Redes de Datos, IPCOP, Comunicaciones, Seguridad en Redes, VPN

I. INTRODUCCIÓN

Con el desarrollo de nuevos equipos y sistemas, la tecnología permite optimizar y mejorar la administración, la comunicación y los servicios de las redes de datos, facilitando a los usuarios el manejo y procesamiento de información.

Por esta razón, las empresas auspiciantes del presente proyecto, Cooperativas Orden y Seguridad y Cooperativa San Gregorio de la Policía Nacional, decidieron realizar las modificaciones necesarias para mejorar en todo aspecto las características de la red de datos y las comunicaciones del edificio principal de las Cooperativas, ya que la red ha presentado varios conflictos.

Además, decidieron establecer un medio de comunicación entre Quito y Guayaquil con el fin

de que las dos ciudades tengan acceso a los mismos servicios informáticos, logrando con esto efectivizar el trabajo de los funcionarios de las Cooperativas.

II. ANÁLISIS DEL ESTADO ACTUAL DE LA RED DE DATOS

Se realizó un estudio de la estructura de la red de datos del edificio principal de las Cooperativas, para determinar cómo es el funcionamiento de la red y establecer los conflictos y las necesidades que tiene la misma.

Básicamente la estructura de la red de datos, consta de un ISP proporcionado por CNT para facilitar el acceso a internet a todas las computadoras del edificio principal de las Cooperativas, el ISP está conectado directamente a un firewall CISCO ASA 5505 que controla el acceso a los servicios y protege la red de datos, el mismo está conectado a un switch TP – LINK capa dos no configurable de 24 puertos, el cual tiene una conexión en cascada con otro switch de las mismas características los cuales vinculan a todas las computadoras y servidores a la red 192.168.100.0 /25 y al dominio “sangregorio.int”.

Para tener un panorama claro de los problemas que puede tener la red de datos se establecen posibles puntos de falla (PPF). La Figura 1 muestra la estructura actual de la red de datos y los PPF establecidos.

El autor agradece a la Cooperativa Orden y Seguridad ya a la Cooperativa San Gregorio de la Policía Nacional por el auspicio y apoyo incondicional en el desarrollo del proyecto. Además, agradece al Departamento de Eléctrica y Electrónica por la colaboración brindada en el proceso de diseño e implementación del proyecto.

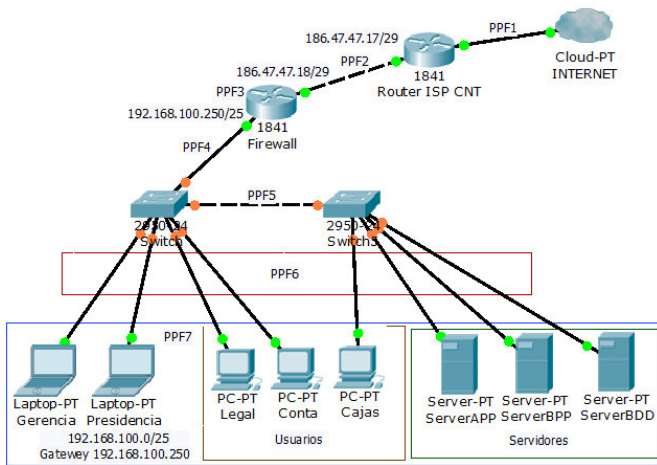


Figura 1: Estructura actual de la red de datos y los PPF establecidos

PPF1: Enlace y conexión de CNT, las Cooperativas realizaron la contratación del servicio sin asesoramiento técnico por lo que en ningún momento se confirmó el correcto funcionamiento del mismo, ni que los equipos estén configurados adecuadamente.

PPF2: Configuraciones y conexión del firewall con router de CNT, es posible que el router proporcionado por CNT no este configurado correctamente y no se establezca una conexión confiable a internet.

Por otro lado se puede tener fallas con el cableado que comunica el router con el firewall o a su vez el firewall no se encuentra configurado correctamente y niega el acceso a internet.

PPF3: Firewall Cisco ASA 5505, la configuración completa del mismo para gestionar el control de la red de datos puede estar mal realizada o a su vez el equipo no soporta el número de usuarios conectados simultáneamente para tener acceso a los servicios integrados en la red y a internet.

PPF4: Conexión Switch – firewall, se puede tener problemas con el cableado que comunica los equipos, y con la configuración del firewall para gestionar la red LAN conformada por computadores, servidores, impresoras, entre otras; o a su vez el switch no está funcionando correctamente.

PPF5: Conexión en cascada de switch, para integrar a todos los usuarios en la misma red, están conectados dos switch en cascada, se puede tener problemas con el cable que une los dos equipos o con los puertos de los mismos, los equipos no son configurables por lo que no se tiene problemas de configuración.

PPF6: Cableado estructurado, es posible que los cables de red o los conectores de los mismos

hayan sufrido alguna avería a partir de la construcción del edificio o estén conectados inadecuadamente, hay que verificar la categoría de los cables para garantizar la calidad de los mismos.

PPF7: Configuración de computadoras y servidores, Los equipos que pertenecen a la red de datos deberían estar configurados correctamente para que los usuarios tengan acceso a servicios internos y a internet, dependiendo de las necesidades de cada funcionario.

El firewall CISCO ASA 5505, genera varios reportes relacionados a la situación de la red como: tráfico en la LAN, velocidad en la LAN, Tasa de paquetes perdidos, entre otros; permitiendo realizar un análisis detallado del estado de la red, tomando en cuenta gráficos y tablas de datos proporcionados por el equipo.

A. Tráfico en la Red de Área Local (LAN)

El firewall muestra gráficamente la cantidad de información que se maneja a través de la interface de entrada del equipo asociada a la red LAN de las Cooperativas, los datos se presentan en kbytes. La figura 2 muestra la cantidad de información que circula a través de la red LAN de las Cooperativas.

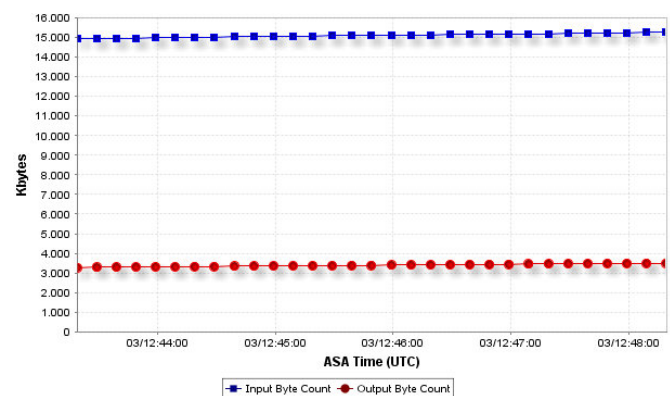


Figura 2: Cantidad de información que circula a través de la red LAN de las Cooperativas.

El firewall registra con fecha y hora la cantidad de kbytes que circulan por el equipo, detallando el total de kbytes que ingresan y salen por el puerto de entrada; de acuerdo a los datos obtenidos la cantidad de kbytes que ingresan es aproximadamente 15000 KB y los que salen 3500 KB, esta es la cantidad de información que se maneja en la red de datos, cabe destacar que la mayoría de equipos no tienen conexión y no pueden acceder a los servicios informáticos de las

Cooperativas lo que influye en la cantidad de información que se maneja en la red de datos.

B. Velocidad en la Red de Área Local (LAN)

El firewall Cisco ASA registra con hora y fecha la velocidad de transmisión de la información que circula a través del puerto de entrada del equipo, es la velocidad de entrada y salida promedio que se maneja en la red de datos de las Cooperativas.

La figura 3 muestra la tasa de velocidad promedio en la red de datos de las Cooperativas.

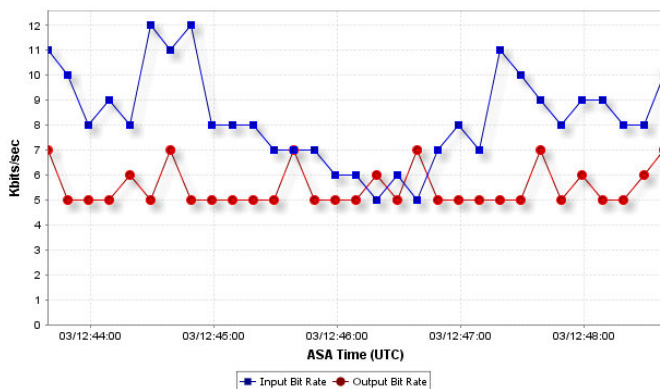


Figura 3: Tasa de velocidad promedio en la red de datos de las Cooperativas

De acuerdo con los datos obtenidos por el firewall, en la red de las Cooperativas circula una tasa de velocidad promedio en la entrada del puerto de 12 kbps y en la salida de 6 kbps, hay que tomar en cuenta que el equipo no está trabajando correctamente y no permite gestionar toda la información que se maneja en la red de datos de las Cooperativas.

C. Paquetes perdidos en la LAN

Los paquetes perdidos, son los que no encuentran la ruta para llegar a su destino y se quedan circulando por la red de datos, el firewall registra gráficamente el total de paquetes perdidos en un determinado tiempo, como muestra la figura 4, el promedio de paquetes perdidos es de 135 kpackets, lo que indica que hay un alto porcentaje de pérdida de paquetes en la red de datos de las Cooperativas, posiblemente porque no se resuelven correctamente las direcciones IP y los paquetes no encuentran su destino.

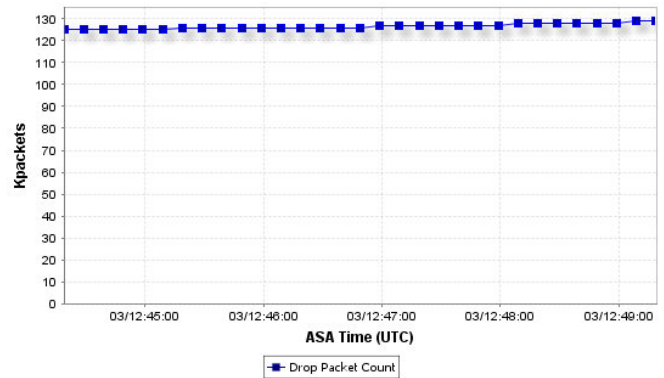


Figura 4: Cantidad de paquetes perdidos.

III. REDISEÑO E INCORPORACIÓN DE NUEVOS SERVICIOS PARA LA RED DE DATOS

En la sección anterior se establecieron posibles puntos de falla, lo que facilita determinar los requerimientos de la red y los problemas que se presentan.

PPF1: Enlace y conexión de CNT, Conexión de fibra óptica con un ancho de banda de dos megas, compartición de 1:1 *clear chanel*, disponibilidad del 99,80%, con una dirección IP fija publica, se encuentra instalados dos equipos, un router cisco 881 y un conversor de fibra óptica.

Para descartar el posible punto de falla 1 se conectó directamente una computadora al router cisco, con cable cruzado y asociando los equipos a la misma red se comprobó que el acceso a internet no tenía inconvenientes.

Por otra parte, CNT ofrece atención a primer nivel 7x24 y asistencia técnica 5x8, lo que permitió valorar y coordinar varias pruebas vía telefónica de conexión y la calidad del servicio de internet, las cuales no presentaron ningún problema a nivel de configuraciones ni de cableado.

PPF2: Configuraciones y conexión del firewall con router de CNT, los equipos están asociados a la misma red y se encuentran conectados directamente, no se encontraron problemas en los puertos ethernet ni en el cableado que influye en su conexión.

En la configuración de los equipos, CNT comprobó remotamente que los puertos ethernet del router estén levantados y habilitados, lo que permite asociar directamente al router con el firewall para tener conexión y comunicación entre los equipos. Luego se realizó la verificación de las configuraciones en el puerto ethernet del firewall

que se conecta con el router, la cual no presento ningún problema.

PPF3: Firewall Cisco ASA 5505, el equipo presento problemas al momento de resolver las direcciones IP de la red LAN por lo que se realizó algunos cambios en la configuración asignando puertos de entrada y salida con diferentes niveles de seguridad y NAT por sobrecarga para resolver las direcciones IP automáticamente, pero los usuarios seguían teniendo inconvenientes con el acceso a internet y a los servicios informáticos, por lo que se vio la necesidad de analizar más detenidamente el equipo, tomando en cuenta listas de acceso y licencias del mismo.

Las listas de acceso y la configuración del equipo eran correctos, por lo que se descartó la posibilidad de que el problema fuera por configuración, la licencia del equipo es básica y no soporta más de diez usuarios conectados simultáneamente, por lo que los demás tenían conexión pero no acceso a los servicios; el equipo presentaba problemas al momento de resolver las direcciones IP, no ejecutaba correctamente el NAT por sobrecarga.

PPF4: Conexión Switch – firewall, como se vio anteriormente el firewall no permitía realizar una administración adecuada de la red de datos, lo que producía errores y conflictos con los servicios de la red.

Se realizaron pruebas de los cables que comunican los equipos al igual que de los puertos y no se encontraron problemas.

PPF5: Conexión en cascada de switch, los dos equipos no son administrables por lo que no es necesario revisar ninguna configuración de los mismos, se verificó el estado de las conexiones y de los cables que utilizan y no se encontró ningún inconveniente, solo están conectados dos switch en cascada por lo que no hay problemas de latencia ni del estado de conexión.

PPF6: Cableado estructurado, luego de realizar pruebas en el cableado estructurado del edificio y verificar la categoría de los cables, utilizando testadores y pruebas de conectividad, no se encontró ningún problema, por lo que se puede afirmar, que el cableado estructurado, si está diseñado para proporcionar una conexión física entre todas las zonas de trabajo del edificio principal de las Cooperativas. El único inconveniente que se encontró es la desorganización del cableado en el rack de

comunicaciones, para lo cual se realizarán las respectivas correcciones.

PPF7: Configuración de computadoras y servidores, Todas las computadoras tienen que estar asociadas a una misma red para acceder a diferentes servicios dependiendo de las necesidades y funciones de cada usuario de la Cooperativa, se cambió dos tarjetas de red que no estaban funcionando correctamente, ya que se verificó la correcta configuración de cada una de las tarjetas de red realizando pruebas de conectividad.

Es necesario optimizar el servicio de correos corporativos, para garantizar una comunicación directa entre los funcionarios de las Cooperativas y los socios.

Implementar los equipos necesarios para mejorar la página web de la Cooperativa Orden y Seguridad con la ayuda de QUITOUNO e incrementar el servicio de consultas del estado de cuentas y saldos para los socios de la Cooperativa con la ayuda de GREENSOFTH.

Generar y establecer la comunicación entre el edificio principal de las Cooperativas ubicado en la ciudad de Quito en las calles Italia 222 y Vancouver, y la oficina en Guayaquil conjuntamente con los funcionarios que necesitan acceso remoto a los servicios de la red de datos de las Cooperativas.

A. Rediseño de la estructura de la red de datos

Luego de analizar y comprender la situación actual de la red de datos de las Cooperativas se decidió sustituir el firewall Cisco ASA, debido a los problemas que estaba generando, el NAT por sobrecarga PAT, no gestiona correctamente las direcciones IP, además las licencias que fueron adquiridas para el equipo solo soportan 10 usuarios según el detalle de la licencia, por lo que, los demás usuarios aparecían conectados, pero no tenían acceso a los servicios.

Para optimizar la administración de la red y abaratar costos, se decidió cambiar el firewall y utilizar un servidor que se encontraba inhabilitado en el edificio principal de las Cooperativas, el servidor Linux es un hp ml 110 Proliant, con un procesador Intel (R) Pentium (R) 4 de 3.20 GHZ, RAM 1.5 GB, y 80 GB en disco.

Las características del equipo son adecuadas para la instalación del software llamado IPCOP.

lo que facilita la asociación de la misma a la red principal de las Cooperativas ubicada en la ciudad de Quito.

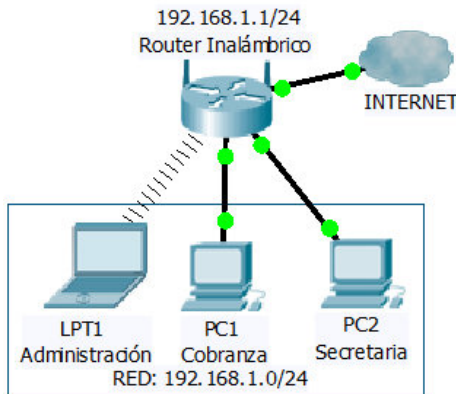


Figura 8: Red de datos Guayaquil

Tomando en cuenta las características de las dos redes y las necesidades de la Cooperativa, es recomendable establecer y configurar VPN cliente-servidor para que los 3 usuarios de la red en Guayaquil tengan acceso a los servicios informáticos levantados en la red principal de las Cooperativas ubicada en la ciudad de Quito.

IPCOP incluye un servidor VPN que permite establecer conexiones de red a red o de cliente a red mediante certificados (raíz / anfitrión), esto quiere decir que el servidor genera certificados de conexión para él y para el cliente, con lo que se garantiza la seguridad de la información que se maneja en la transmisión.

La figura 9 muestra la estructura general de la conexión VPN cliente-servidor que permite la comunicación entre Quito y Guayaquil, en la que los clientes se conectan con el servidor VPN para tener acceso a los servicios informáticos levantados en la red principal de las Cooperativas ubicada en la ciudad de Quito.

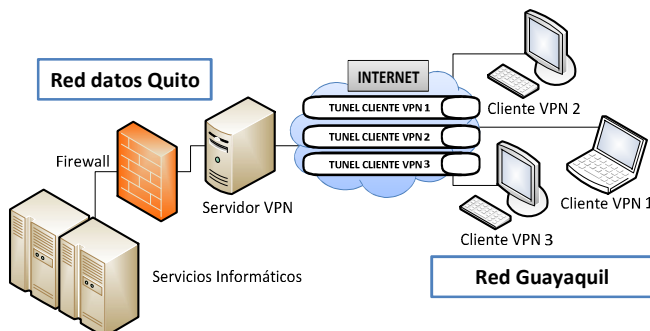


Figura 9: Conexión VPN cliente-servidor (Quito-Guayaquil)

Se debe tomar en cuenta la seguridad de la

conexión y de la información que manejan las Cooperativas, IPCOP valida el acceso a la red mediante certificados y posee diferentes métodos de encriptación para proteger los datos; más adelante se explicará la configuración del servidor y cliente VPN detallando los parámetros necesarios para establecer una conexión eficiente y segura.

C. Diseño de la estructura de red para integrar los servicios

Considerando otro aspecto, el servicio de consultas y estados de cuentas para los socios de la Cooperativa, se tiene que integrar a la página web de la Cooperativa, con el vínculo "Cooperativa en línea", para lo cual es necesario realizar modificaciones e integrar nuevos equipos en la red.

IPCOP, permite establecer una red específica para levantar servicios web, diferente de la red principal, donde se manejan todas las bases e información de la Cooperativa, por esta razón, IPCOP se encargará de gestionar el acceso y re direccionamiento a la página web.

El ISP de CNT, se conecta directamente con el equipo de IPCOP, el cual protege la red de datos y gestiona el acceso al servidor web como lo muestra la figura 10.

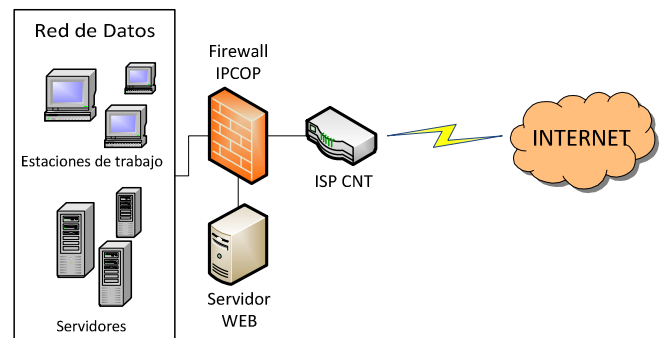


Figura 10: Conexión servidor web

El diseño completo de la red de datos del edificio, conjuntamente con la conexión y comunicación de Guayaquil y el servidor web para consultas de saldos y estados de cuenta, se puede apreciar en la figura 11.

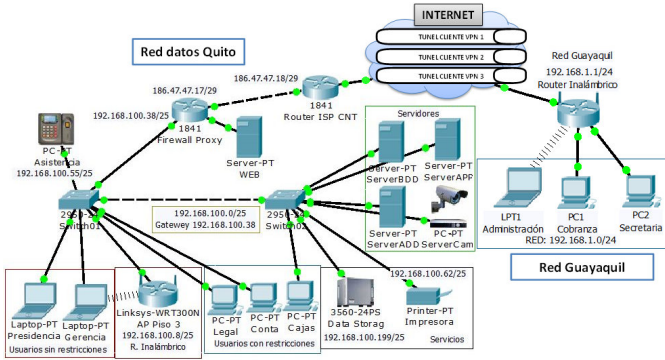


Figura 11: Red de datos completa con servicios informáticos

IV. PRUEBAS DE CONEXIÓN Y COMUNICACIÓN

A. Pruebas de Conexión

Desde cualquier máquina de la red, usando el comando “ping”, se puede verificar la conexión a servidores, equipos e internet.

```
C:\Users>ping serverapp
Haciendo ping a serverapp [192.168.100.200] con 32 bytes de datos:
Respuesta desde 192.168.100.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.200: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.100.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users>ping www.google.com
Haciendo ping a www.google.com [74.125.26.103] con 32 bytes de datos:
Respuesta desde 74.125.26.103: bytes=32 tiempo=116ms TTL=34
Respuesta desde 74.125.26.103: bytes=32 tiempo=116ms TTL=34
Respuesta desde 74.125.26.103: bytes=32 tiempo=117ms TTL=34
Respuesta desde 74.125.26.103: bytes=32 tiempo=117ms TTL=34

Estadísticas de ping para 74.125.26.103:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 116ms, Máximo = 117ms, Media = 116ms
```

Figura 12: Red de datos

La máquina del administrador que pertenece a la red de datos, tiene conexión al *serverapp* y a internet, como se puede apreciar en la figura 12, con lo que se demuestra la conexión a los servicios informáticos, las mismas pruebas se realizaron en todas las computadoras logrando verificar que todas las máquinas que pertenecen a la red de datos de las Cooperativas, tengan conexión.

Una vez comprobado que todos los funcionarios de las Cooperativas San Gregorio y Orden y Seguridad tengan conexión a la red de datos, se vio la necesidad de llevar un registro de todos los inconvenientes de conexión que se pueden presentar durante un mes, en función de los requerimientos de cada funcionario, con lo que se generó la Tabla 1 y la figura 13.

Tabla 1: Problemas de conexión en un mes

Problemas de conexión Octubre 2012				
Día	Primera Semana	Segunda Semana	Tercera Semana	Cuarta Semana
Lunes	3	2	2	1
Martes	1	1	0	0
Miércoles	1	1	3	0
Jueves	2	0	0	2
Viernes	1	1	1	0
Total problemas conexión semana	8	5	6	3
Numero de total de Usuarios: 30				

Problemas de conexión Octubre 2012

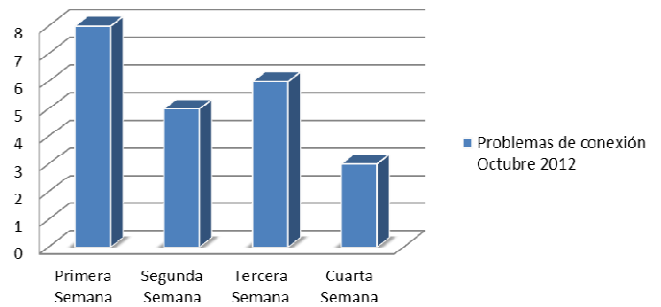


Figura 13: Problemas de conexión en un mes

Tomando en cuenta el total de funcionarios de las Cooperativas, los problemas que se presentan son reducidos, paulatinamente los inconvenientes de conexión se depurarán; La primera semana del mes fue la más crítica con un 5,3% en problemas de conexión, esto se puede dar por la cantidad de información que se procesa a inicio de cada mes en cada una de las Cooperativas.

B. Pruebas de Comunicación

Para validar la comunicación entre computadoras y servidores de las Cooperativas, se ingresa a cada uno de los servicios informáticos levantados en la red de datos, desde todos los equipos que pertenecen a la misma, descartando la posibilidad de que algún computador no tenga comunicación. Si la comunicación no tiene inconvenientes, las aplicaciones contables de las Cooperativas abren la página principal de las aplicaciones como muestra la figura 14.

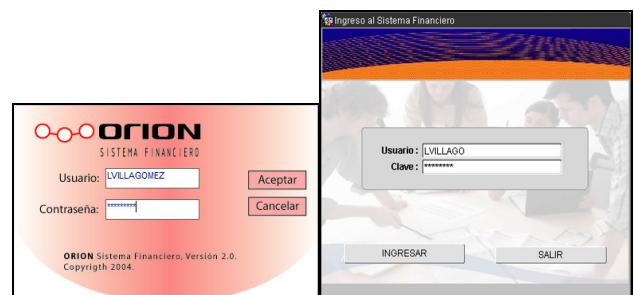


Figura 14: Pantallas principales de aplicaciones contables, Cooperativa Orden y Seguridad, Cooperativa San Gregorio

Una vez comprobado que todos los funcionarios de las Cooperativas San Gregorio y Orden y Seguridad tengan comunicación con los servicios informáticos de las Cooperativas e internet, se vio la necesidad de llevar un registro de todos los inconvenientes de comunicación que se pueden presentar durante un mes, en función de los requerimientos de cada funcionario, con lo que se generó la Tabla 2 y la figura 15.

Tabla 2: Problemas de comunicación en un mes

Problemas de comunicación Octubre 2012				
Día	Primera Semana	Segunda Semana	Tercera Semana	Cuarta Semana
Lunes	4	2	2	1
Martes	1	1	1	0
Miércoles	2	2	3	1
Jueves	2	0	0	2
Viernes	1	1	2	1
Total problemas comunicación semana	10	6	8	5
Numero de total de Usuarios: 30				

Al momento de tener problemas de conexión, también se generaban inconvenientes con la comunicación, los servidores solicitaban clave de administrador para ingresar al servicio, lo que no era normal, además los funcionarios no lograban acceder al sistema, por no tener claro cómo hacerlo o el sistema no se encontraba instalado correctamente; La primera semana del mes fue la más crítica con 6,67% en problemas de comunicación, pero los inconvenientes que se presentan son reducidos y paulatinamente fueron depurados.

Problemas de comunicación Octubre 2012

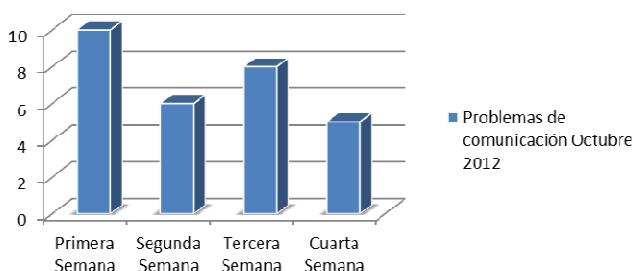


Figura 15: Problemas de comunicación en un mes

C. Tráfico en LAN

IPCOP lleva un registro diario, semanal, mensual y anual del tráfico de entrada y salida que maneja la red LAN de las Cooperativas por el puerto ethernet (GREEN) del equipo IPCOP, con el fin de evaluar el estado de la red, controlar la

misma y dimensionar los recursos para aprovechar al máximo las características de la red.

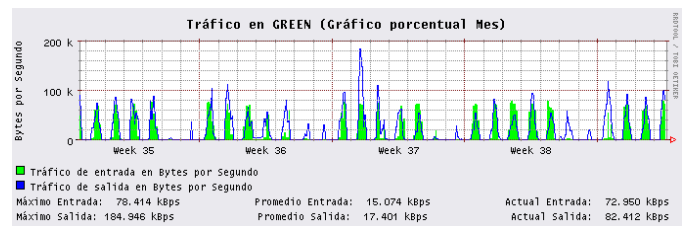


Figura 16: Tráfico en LAN mensual

En el gráfico porcentual mensual, del tráfico en la LAN que se muestra en la figura 16, se puede apreciar que en la primera semana del mes (semana 37), circula mayor cantidad de tráfico en la red, debido a que las Cooperativas realizan todos los pagos, descuentos, declaraciones, entre otros procesos, por lo que circula gran cantidad de información por la red, aumentando el tráfico de la misma.

- Tráfico máximo de entrada 78,414 kbps y promedio mensual de 15,074 kbps.
- Tráfico máximo de salida 184,946 kbps y promedio mensual de 17,401 kbps.

El tráfico mensual generado en la red LAN, según los registros de IPCOP, no presenta ninguna complicación durante todo el mes, ya que los valores promedio del tráfico no son elevados y los valores máximos que se muestran en la semana crítica, son controlables, con restricciones a los funcionarios.

D. Tráfico en WAN

Para establecer el tráfico que circula a través del puerto de IPCOP asociado a la WAN de las Cooperativas, se registra datos manuales y semanales.

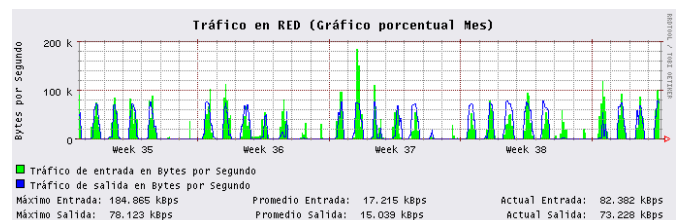


Figura 17: Tráfico en WAN mensual

En el gráfico porcentual mensual, del tráfico en el puerto asociado a la WAN que se muestra en la figura 17, se puede apreciar que en la primera semana del mes (semana 37), circula mayor cantidad de tráfico en la red, debido a que las Cooperativas realizan todos los pagos, descuentos,

declaraciones, entre otros procesos, por lo que circula gran cantidad de información por la red, aumentando el tráfico de la misma.

- Tráfico máximo de entrada 184,865 kbps y promedio mensual de 17,215 kbps.
- Tráfico máximo de salida 78,123 kbps y promedio mensual de 15,039 kbps.

El tráfico mensual generado en la red WAN, según los registros de IPCOP, no presenta ninguna complicación durante todo el mes, ya que los valores promedio del tráfico no son elevados y los valores máximos que se muestran en la semana crítica, son controlables, con restricciones a los funcionarios.

V. ANÁLISIS DE LAS PRUEBAS DE CONEXIÓN, COMUNICACIÓN

Una vez realizadas las modificaciones necesarias, reestructuración de la red para mejorar el rendimiento de la misma y añadir nuevos servicios informáticos; de acuerdo a las pruebas realizadas en toda la red de datos de las Cooperativas tanto LAN como WAN, el actual dimensionamiento y volumen de la red soporta los requerimientos de todos los servicios informáticos levantados en la misma.

A. Análisis de las pruebas de conexión

Los problemas que se generan en conexiones, son mínimos, normalmente la primera semana de cada mes presenta el mayor porcentaje de problemas en conexión, en el mes de octubre del 2012, la primera semana registró el 5,3% de inconvenientes con las conexiones.

Varios cables de red deteriorados y desconectados, conflicto con las direcciones IP, falta de conocimiento de los usuarios, fueron las principales causas de inconvenientes con la conexión, pero todos los problemas fueron solucionados de acuerdo a las necesidades de conexión y en la actualidad se puede afirmar que los problemas de conexión se han reducido a un 1% semanal como máximo.

B. Análisis de las pruebas comunicación

En la primera semana del mes de octubre del 2012 se presentó un 6,67% de inconvenientes en la comunicación de la red de datos LAN y WAN de las Cooperativas, los usuarios internos y externos no podían establecer comunicación cliente servidor y viceversa.

La configuración inicial del sistema no era la correcta o los usuarios no tenían claro el procedimiento y la forma adecuada de acceder a los servicios informáticos de la red de datos de las Cooperativas, gradualmente se fueron depurando los errores y se ha logrado reducir a un 3% en problemas de comunicación por semana, es un porcentaje mínimo con respecto a la cantidad de usuarios que pertenecen a la red.

VI. CONCLUSIONES Y RECOMENDACIONES

- Se realizó un análisis detallado de las necesidades tecnológicas y de servicios informáticos de las Cooperativas, enfocado a prestar una solución eficiente a los problemas de la red.
- Se logró determinar: cada uno de los inconvenientes, las necesidades, el diseño, la estructura de la red de datos de la Cooperativa San Gregorio y de la Cooperativa Orden y Seguridad, así como varios problemas en conexión, comunicación, administración y servicios informáticos.
- Luego de analizar el estado de todos los equipos que forman parte de la red de datos de las Cooperativas, se determinó que el firewall no cumplía correctamente con sus funciones al momento de controlar, proteger y gestionar las conexiones y comunicaciones en la red de datos de las Cooperativas.
- Se consiguió rediseñar la estructura de la red de datos e incorporar nuevos equipos, con el fin de mejorar la calidad de conexión, comunicación, administración y seguridad en la red.
- Se establecieron conexiones y comunicaciones remotas (VPN) considerando varias medidas de seguridad como certificados cliente - servidor y la encriptación de información, con el fin de que los funcionarios de otra ciudad puedan acceder a los servicios informáticos levantados en la red principal de las Cooperativas.
- Se logró incorporar a la red el servidor web de la Cooperativa Orden y Seguridad para que los socios puedan realizar consultas de forma remota, de saldos y estados de cuenta, IPCOP permite redireccionar las solicitudes de la web hacia el servidor con las respectivas seguridades.
- Se logró depurar en gran parte los

inconvenientes que se presentaban en: seguridad, comunicación, conexión y administración de la red.

- Se recomienda incrementar las características del hardware de IPCOP para que el servidor resuelva los requerimientos de los usuarios terminales con mayor eficacia y mejore la calidad de los servicios que brinda.
- Realizar el mantenimiento preventivo y correctivo de todos los equipos que pertenecen a la red de datos de las Cooperativas cada 6 meses si es posible, con la finalidad de evitar daños en los mismos o pérdida de información.
- Se recomienda establecer a futuro una conexión VPN punto a punto, con el fin de mejorar la calidad de la conexión virtual y la seguridad de la información que se trasmite a través del túnel VPN.
- Monitorear y evaluar regularmente el rendimiento de la red de datos de las Cooperativas y el estado de todos los servicios informáticos levantados dentro y fuera de la misma.

REFERENCIAS

- [1] Villagómez, L. (2013). Diseño e implementación de una solución integral de redes y telecomunicaciones para la Cooperativa Orden y Seguridad y Cooperativa San Gregorio de la Policía Nacional. Quito.
- [2] Stallings, W. (2000). Comunicaciones y redes de computadores 6ta edición. Madrid, México, Santafé de Bogotá, Buenos Aires, Caracas, Lima, Montevideo, San Juan, San José, Santiago, Sao Paulo, White Plains: Prentice Hall.
- [3] Huidobro, J. M., Millán Tejedor, R. J., & Roldán Martínez, D. (2006). Tecnologías de TELECOMUNICACIONES. México, D.F: Alfaomega.
- [4] Miller, S. S. (2004). Seguridad en WiFi. Madrid: McGraw-Hill Profesional.
- [5] Nieto, Á. T. (2002). TELECOMUNICACIONES Y TELEMÁTICA, segunda edición. Bogotá: Escuela Colombiana de Ingeniería.
- [6] Hallberg, B. (2007). Fundamentos de redes 4ta Edición. México: McGrawHill.
- [7] [G] Sugano, A. (2005). Solución de problemas en redes. Madrid: Anaya Multimedia.

- [8] Dye, M. A., McDonald, R., & Rufi, A. W. (2008). Aspectos básicos fr networking Guía de estudio de CCNA Exploration. Madrid: PEARSON EDUCATION.
- [9] S. (s.f.). Universidad del Azuay. Recuperado el 06 de Octubre de 2012, de Universidad del Azuay: http://uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan.pdf
- [10] Feregrino, C. (Diciembre de 2003). Recuperado el 10 de Octubre de 2012, de http://www.weblapaz.com.mx/cursos/admonredes/3-Riesgos_de_Seguridad_y_tecnicas_de_ataque.pdf
- [11] Lerch, D. (22 de Julio de 2007). Recuperado el 19 de Diciembre de 2012, de <http://dlerch.blogspot.com/2007/07/modos-de-cifrado-ecb-cbc-ctr-ofb-y-cfb.html>
- [12] I. (s.f.). IPCOP. Recuperado el 27 de Octubre de 2012, de IPCOP: <http://www.ipcop.org/1.4.0/en/admin/html/>
- [13] Cisco Systems, I. (s.f.). CISCO. Recuperado el 10 de Diciembre de 2012, de CISCO: http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html

Autor



Lenin Eduardo Villagómez Morillo, nace el 9 de Enero de 1989 en la ciudad de Quito, realizó sus estudios primarios en La Academia Naval Almirante Nelson, continuo sus estudios secundarios en el Colegio Técnico Experimental Salesiano Don Bosco, donde obtiene el título de Bachiller Técnico en Electricidad y Electrónica. En la actualidad es egresado del Departamento de Ingeniería Eléctrica y Electrónica de la Escuela Politécnica del Ejercito, Sangolquí – Ecuador. Completo los cursos de certificación CCNA y trabaja en el Ministerio del Interior en la Dirección Tecnológica área de Monitoreo.