

**INFORME FINAL
INCLUSIÓN DIGITAL DE COMUNIDADES RURALES
APLICACIÓN LTSPEN EQUIPOS OBSOLETOS PARA ENFRENTAR LA
BRECHA DIGITAL**

**JHONATAN CAMILO BERMÚDEZ PARRA
JUAN DAVID SALAZAR LÓPEZ**



**UNIVERSIDAD DE MANIZALES
FACULTAD DE CIENCIAS E INGENIERÍAS
INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
MANIZALES
17/09/2013**

INFORME FINAL
INCLUSION DIGITAL DE COMUNIDADES RURALES
APLICACIÓN LTSP EN EQUIPOS OBSOLETOS PARA ENFRENTAR LA
BRECHA DIGITAL

JHONATAN CAMILO BERMÚDEZ PARRA
JUAN DAVID SALAZAR LÓPEZ

Proyecto de investigación con coinvestigadores, presentado como requisito parcial para optar al título de Ingeniero de Sistemas y Telecomunicaciones

Asesor temático
Néstor Jaime Castaño Pérez
Docente Universidad de Manizales

UNIVERSIDAD DE MANIZALES
FACULTAD DE CIENCIAS E INGENIERÍA
INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
MANIZALES
17/09/2013

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN.....	5
1. VENTAJAS QUE OFRECE LTSP.....	6
1.1 SEGURO.....	6
1.2 USABILIDAD	6
1.3 AMIGABLE CON EL MEDIO AMBIENTE	6
1.4 ECONÓMICO.....	7
2. CONCEPTUALIZACIÓN DE LA APLICACIÓN LTSP.....	7
2.1 HARDWARE	7
2.2 SOFTWARE	8
3. FUNCIONAMIENTO DE LA APLICACIÓN LTSP.....	9
3.1 Funcionamiento de LTSP	9
3.2 Modo de arranque o puesta en marcha de un cliente ligero.	9
4. HARDWARE UTILIZADO EN LA IMPLEMENTACIÓN DE LTSP EN CASA ...	11
4.1 El servidor: Computador Portátil marca TOSHIBA modelo SATELLITE L745. .	11
4.1.1 Memoria.RAM de 4 GB	11
4.1.2 Procesador y velocidad.I5DualCore, 2.8 MHz.....	11
4.1.3 Discos. 1 Disco físico de 500 G con 2 particiones lógicas	11
4.2 Clientes Ligeros.	11
4.2.1 Hardware utilizado (equipos portátiles).	11
4.3 Método de arranque de los clientes ligeros.....	11
5. PRUEBA PILOTO EN ARANZAZU	11
5.1 Características de los equipos.....	12
5.1.1 Servidor: Procesador: Intel core Ii5-2430M, 2.40GHz, 4 núcleos	12
5.1.2 Clientes livianos:.....	12
5.2 Análisis Del Tráfico De La Prueba Piloto	13
6. VIDEO VISTO POR EL SERVIDOR VS VIDEO VISTO POR CLIENTE LIGERO	18
.....	18

7. CONCLUSIONES DE FUNCIONAMIENTO DELA APLICACIÓN LTSP EN LA PRUEBA PILOTO.....	19
8. UDP Vs TCP.....	20
8.1 El Protocolo Udp	20
8.1.1 Transmisión de Video y Voz:.....	21
8.2 EL PROTOCOLO TCP	22
7.2.1 Negociación en tres pasos o Three-way handshake.....	22
8.2.2 Transferencia de datos:.....	23
9. CONCLUSIONES.....	25
BIBLIOGRAFIA.....	26

INTRODUCCIÓN

La masificación de equipos de cómputo o de informática utilizados para la educación, la gran mayoría de estos usados bajo licencias educativas o licencias pagas, hacen a un lado tecnologías como las que ofrecen los sistemas operativos GNU/Linux, los cuales en sus versiones más modernas traen incorporadas aplicaciones prácticas, confiables y fáciles de utilizar, no solo en instituciones de educación sino también a empresas que no cuenten con los recursos necesarios para la compra de costosas licencias para el óptimo funcionamiento de su entorno tecnológico, es de esta manera que LTSP se convierte en una gran alternativa para la mayoría de las instituciones educativas rezagadas por falta de recursos económicos para la compra de tecnología, así como para las empresas anteriormente mencionadas, ya que LTSP disminuye los costos de hardware al permitir el uso de computadores más antiguos y con menos capacidad o potencia utilizarlos como clientes ligeros o terminales brutas, también se genera una economía al momento de reducir la instalación, soporte y administración de los equipos, ya que todo se centraliza en un servidor.

Los clientes ligeros pueden llegar a tener una vida útil de casi el doble de lo que pueden llegar a tener equipos modernos. Otra de las grandes ventajas que este sistema ofrece es, que al momento de que un equipo ligero o terminal bruta falla, puede ser reemplazado fácilmente, sin que esto genere traumatismos por la pérdida de información ya que esta se encuentra en el servidor, el encargado de proveer el sistema operativo.

1. VENTAJAS QUE OFRECE LTSP

Son muchas las ventajas que ofrece LTSP, de las cuales las más importantes son seguridad, amigable con el medio ambiente, económico, la usabilidad, está diseñado para la educación y los negocios.

1.1 SEGURIDAD

La seguridad es de los factores más importantes que debe tener un sistema, la integridad de los datos que por este circulan es de esta manera que se convierte en un reto clave para los administradores de los servidores donde se captura, circula y entrega la información. La mayoría de las instituciones educativas y pequeñas empresas no cuentan con los suficientes recursos económicos para la contratación de personal capacitado para este tema, es esta una de las ventajas de la implementación de LTSP, pues los sistemas operativos con esta aplicación incluida, siendo sistemas basados en GNU/Linux, disfrutan de ventajas de seguridad que traen los sistemas tipo Unix y de código abierto, esto se refleja en un código de mayor calidad y los virus y spyware no se convierten en una preocupación. Además, estos sistemas poseen estrictas políticas de seguridad, lo que significa que la mayoría de los problemas comunes, como los son, puertos abiertos y software mal configurado. En pocas palabras los sistemas basados en LTSP son sistemas multiusuario, que facilitan a los usuarios completar sus tareas, más comunes y complejas sin tener un nivel de acceso que pueda poner en riesgo el sistema.

1.2 USABILIDAD

La gran mayoría de las instituciones educativas no cuentan con los recursos necesarios, para tener una persona encargada de tiempo completo del departamento de TI, esto también sucede en la mayoría de las pequeñas empresas, es por esto que con la utilización de LTSP, se hace más fácil el manejo de estos departamentos, pues los administradores o personas encargadas de estas áreas no deben estar pendientes de cierta cantidad de equipos, de que si uno de estos falla, encontrar en cuál de todos está el problema, por el contrario, solo se deben enfocar en el correcto funcionamiento del servidor, este sistema de clientes ligeros fue diseñado para tal función, para centralizar todo en un servidor y administrar la red que distribuye el sistema operativo.

1.3 AMIGABLE CON EL MEDIO AMBIENTE

La utilización de LTSP, permite la reutilización de equipos obsoletos como una salida para disminuir los desechos eléctricos y electrónicos para adquirir, almacenar, procesar y dar acceso a nuevos computadores por medio del LTSP (Linux Terminal Server Project). En la era actual, donde la tecnología y comunicaciones van cada vez más rápido, se busca sacar a las personas de un consumismo en el cual están; a pesar de los beneficios innegables que posee la tecnología no se debe olvidar la contaminación medioambiental que pueden causar las mismas al final de su ciclo de vida. En la práctica los equipos ligeros

utilizan la mitad de energía que los computadores tradicionales, lo cual genera un ahorro significativo a nivel económico, sino también se convierte en un medio para reducir la emisión de CO₂.

1.4 ECONÓMICO

Es común ver que las instituciones educativas y las pequeñas empresas dejen rezagado el presupuesto para el área de TI y sea lo último en considerar. LTSP ayuda a ofrecer a los estudiantes lo que requieren en temas de informática, y más precisamente en ofimática. Las licencias de funcionamiento de una suite de Office son altamente costosas, por lo que con la adquisición de una de estas licencias se puede estar consumiendo gran parte del presupuesto en un solo equipo. LTSP trae por defecto instalada una suite de ofimática, la cual funciona perfectamente igual o mejor que una con licencia paga. Es este un solo ejemplo de las muchas ventajas económicas que puede brindar la implementación de esta herramienta en los planteles educativos y en pequeñas empresas, donde solo es necesario contar con un equipo en óptimas condiciones y los demás clientes ligeros con especificaciones básicas se puede llegar a montar un centro de informática de buena calidad para reducir la brecha digital.

2. CONCEPTUALIZACIÓN DE LA APLICACIÓN LTSP

Para la implementación de del servidor bajo LTSP se hace necesario la utilización de diferentes componentes que conforman una red, como lo son el hardware y el software, a continuación se describe el funcionamiento de la red bajo estos dos componentes.

2.1 HARDWARE

La red funciona fraccionando los ficheros y paquetes de datos de información, esto es lo que se transfiere por dicha red, para este desarrollo se utilizó una red cableada. Esta red transfiere paquetes a través de un cable de red UTP cat 5E, que permite la transferencia a velocidades de 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s. En algunas ocasiones es pertinente aclarar que una red solo sirve si se puede conectar con varios computadores. Actualmente se pueden encontrar diferentes partes físicas, es decir hardware para interconectar computadores, pero no son tan útiles y funcionales como las que brinda una conexión Ethernet.

Para la creación e interconexión de una red existen diferentes dispositivos que permiten esta función entre los cuales se encuentran los siguientes:

- **Switch:** Es similar a un hub, tiene cierta cantidad de puertos e igualmente cierta cantidad de luces que corresponde a cada puerto. El Switch puede tener múltiples conexiones al mismo tiempo y se hace más factible la utilización del Switch por su velocidad de transmisión, lo que permite un óptimo funcionamiento de los equipos livianos.

- **Router:** Se utiliza para realizar conexiones entre dos redes. Estos también son utilizados para conectar la red LAN a Internet.

2.2 SOFTWARE

La infraestructura de red más común para la implementación de LTSP incluye lo siguiente:

- **DHCP:** Servicio implementado en el servidor, el cual proporciona a cada equipo interconectado a la red una dirección IP para el direccionamiento de los paquetes que circulan por la misma, para ello el DHCP proporciona al equipo de forma automática la configuración de red, en el presente caso el servidor está configurado para que el cliente liviano en su inicio pueda hacer las peticiones pertinentes al servidor para su arranque desde la tarjeta de red Ethernet.
- **DNS:** Servicio que se ejecuta en un servidor externo que guarda nombres de dominio y los enlaza directamente a una dirección IP. El cliente ligero se comunica con el servidor LTSP y este a su vez se conecta con el servidor que ofrece el servicio DNS cada vez que se refiere a un nombre de dominio.
- **NTP:** Servicio implementado en el servidor, permite la sincronización de los relojes de los clientes ligeros y el reloj atómico exacto que el servidor posee para que el aplicativo funcione sincrónicamente.
- **Proxy web:** Servicio que se ejecuta en el servidor, responde a las peticiones de los clientes ligeros hacia un portal web. el cual puede almacenar, de acuerdo a su configuración, datos de navegación y permitir accesos exitosos guardados en la memoria flotante. Esto no es realmente necesario en esencia para los clientes ligeros LTSP, ya que no se ejecuta nada en ellos, todo se ejecuta en el servidor, pero es bueno para filtrar o prohibir accesos a ciertos portales web.
- **Filtro de contenido:** Si por requerimientos se debe implementar una política de filtrado la cual permite bloquear y controlar tráfico malicioso o no deseado.
- **Firewall y bloqueo de puertos:** Un firewall se define inicialmente como un servicio en el servidor o Router para proteger el servidor o clientes ligeros restringiendo o permitiendo accesos desde una dirección ajena a la red LAN ejecutada desde el medio a puertos abiertos o vulnerables.

3. FUNCIONAMIENTO DE LA APLICACIÓN LTSP

Anteriormente se ha descrito los requerimientos físicos y de software para el correcto funcionamiento de la aplicación LTSP, ahora se debe realizar el porqué de la aplicación y como es su funcionamiento.

3.1 Funcionamiento de LTSP

El aplicativo LTSP se define principalmente como un conjunto de paquetes que configurados de una manera óptima convierte un entorno de Linux a un equipo servidor de terminales, prestando los servicios de sistema operativo, aplicaciones y administración de almacenamiento. Con ello permite que los clientes ligeros, los cuales son aquellos faltantes de disco duro o simplemente obsoletos para la actualidad, se encuentren como terminales interconectados en red con el servidor y puedan ser usados como un equipo de excelentes condiciones. LTSP a comparación de otros aplicativos como Microsoft Terminal Services se toma como el más fácil de tener siempre arriba y sin pago ya que no requiere que cada cliente ligero posea ninguna clase de programa instalado ni alguna licencia paga, sino que simplemente debe tener una tarjeta de red en buenas condiciones y que pueda hacer capaz de realizar PXE para la intercomunicación con el servidor.

3.2 Modo de arranque o puesta en marcha de un cliente ligero.

Primero se carga el kernel Linux en la memoria del cliente por medio del protocolo PXE, ya que muchas tarjetas de red, y casi cualquier placa base actual con tarjeta de red integrada lo posee. Al ser cargado en la memoria, empieza a ejecutarse.

El kernel arranca cualquier dispositivo de bajo nivel que necesite, tales como memoria ram, junto al kernel se descarga el initialramfilesystem (initramfs), el cual contiene varias utilidades y scripts de shell necesarios para el arranque del equipo. El kernel empieza su trabajo ejecutando el script de Shell llamado /init el cual se encuentra en la raíz del initramfs dando inicio al sistema.

El script /init monta /proc y /sys, inicia udev para conocer y dar inicio al hardware, especialmente la tarjeta de red, la cual se necesita para cada aspecto del inicio a partir de ese momento. También, crea un pequeño disco ram, donde cualquier almacenamiento local se puede crear o modificar. Este proceso se da mientras se genera la interfaz de red loopback que es 127.0.0.1

Ejecuta el archivo ipconfig para hacer la petición al servidor DHCP y obtiene la información proporcionada en el fichero dhcpd.conf, como la puerta de enlace por defecto entre otros parámetros importantes para configurar la tarjeta de red Ethernet, y determinar el servidor donde se va a montar root, ahora el sistema de ficheros root mediante el script /init monta un nuevo sistema de ficheros root a través de NBD o NFS. En el caso de NBD, la imagen que normalmente se carga en /opt/ltsp/images/i386.img.

Nota: Si root se monta a través de NFS, entonces el directorio que se exporta del servidor es normalmente /opt/ltsp/i386.

Se debe montar en un directorio por separado y así realizar un run-init mediante el cual cambia el sistema de ficheros. Cuando se complete, el sistema de ficheros se montará en /.cabe aclarar que todos los directorios que necesitan permisos de escritura para que se produzca el inicio normalmente son montados desde el disco ram (/tmp o /var).

Se da por terminado el script de shell /init y se ejecuta /sbin/init real el cual empieza estableciendo el entorno de cliente ligero, y lee los comandos de arranque en /etc/rcS.d. Que ejecuta el comando ltsp-client-setup configurando así varios aspectos del entorno del cliente ligero, entre ellos la habilitación del swap de NBD, configuración del syslog remoto o cargar cualquier archivo necesario en el kernel, mientras el programa init ejecuta comandos en el directorio /etc/rc2.d.

Uno de los comandos es el comando ltsp-client-core que se ejecutará mientras el cliente se está en su proceso de arranque.

Mientras se ejecuta el fichero lts.conf los parámetros en el fichero que pertenecen a este cliente ligero serán establecidos como variables de entorno para manejar el script S20ltsp-client-core. El demonio pulseaudio se inicia, para permitir conexiones remotas de audio para conectar y reproducirse en el cliente ligero. Como el cliente ligero puede soportar discos externos, el programa ltspfsd se inicia para permitir que el servidor lea desde tales dispositivos tales como memorias USB, o cd's conectados al cliente ligero.

En este punto, cualquier sesión de pantalla que se haya definido en su lts.conf se ejecutará.

Especificando en el fichero lts.conf, un script de pantalla ldm se ejecuta en SCREEN_07. El LTSP Display Manager (ldm) es el encargado de inicio de sesión del aplicativo LTSP, establece a un valor de ldm, o startx, entonces el X WindowSystem será iniciado, proporcionándole una interfaz de usuario gráfica.

Por defecto, el servidor Xorgautocomprobará la tarjeta, creará un fichero /etc/X11/xorg.conf por defecto en el disco ram en el terminal, e iniciará xorg con esa configuración personalizada.

El servidor iniciará un tunelssh encriptado hacia el servidor, en el caso de ldm o una petición XDMCP al servidor LTSP, en el caso de startx. De cualquier forma, una pantalla de registro aparecerá en el terminal.

En este punto, el usuario se identifica y establece una sesión con el servidor, ejecutando una sesión en el servidor ya que todos los comandos que ejecuta se dan en el servidor, pero la salida visual se da en el cliente ligero.

4. HARDWARE UTILIZADO EN LA IMPLEMENTACIÓN DE LTSP EN CASA

4.1 El servidor: Computador Portátil marca TOSHIBA modelo SATELLITE L745.

4.1.1 Memoria.RAM de 4 GB

4.1.2 Procesador y velocidad.I5DualCore, 2.8 MHz

4.1.3 Discos. 1 Disco físico de 500 G con 2 particiones lógicas

4.2 Clientes Ligeros.

- Samsung rb410
- SonyVaio vpcea40el
- Compaq pesario cq40
- Aceraspireone

4.2.1 Hardware utilizado (equipos portátiles).

- Samsung rb410 con 3 en ram y un procesador de 1.8 hz
- Sonyvaio vpcea40el con 3 en ram y un procesador i3 de 1.8 hz
- Compaq pesario cq40 con 1 en ram y un procesador de 1.5 hz
- Aceraspireone de 1 en ram y un procesador de 1.3 hz

4.3 Método de arranque de los clientes ligeros.

PXE: Permite a una estación de trabajo para iniciar desde un servidor en una red antes de iniciar el sistema operativo en el disco duro local. Una estación de trabajo PXE habilitado conecta su tarjeta a la LAN a través de un puente, lo que la mantiene conectada a la red, incluso cuando el equipo está apagado. Debido a que un administrador de red no tiene que desplazarse físicamente a la estación de trabajo específica y arrancar manualmente, sistemas operativos y otros programas, como los programas de diagnóstico, pueden ser cargados en el dispositivo desde un servidor en la red.

5. PRUEBA PILOTO EN ARANZAZU

La prueba inicia el 31 de agosto de 2013 a las 9:00 am.

Se hace la instalación y configuración de los equipos utilizados para la prueba fueron cinco (5) en total, uno (1) de propiedad de uno de los coinvestigadores y cuatro (4) en préstamo a la Universidad de Manizales con características definidas de la siguiente manera:

5.1 Características de los equipos

5.1.1 Servidor: Procesador: Intel core i5-2430M, 2.40GHz, 4 núcleos

RAM: 4096 MB.

Configurado con el aplicativo LTSP live para la puesta en marcha.

Conectado a internet por medio de un anclaje de red brindado por un celular de los coinvestigadores a una velocidad de bajada de 2318 Kbps y una velocidad de subida de 963 Kbps por medio del cual los clientes ligeros pueden salir al medio y navegar.

5.1.2 Clientes livianos:

1-Procesador: Intel core i3 540M, 2.07 GHz

RAM: 4096M

2- Procesador: Intel core 640M, 2.13 GHz

RAM: 2048 MB

3- Procesador: Intel core 2 dúo, E6550, 2.33 GHz

RAM: 2048 MB

4- Procesador: Pentium dual core, E5400, 2.70 GHz

RAM: 2048 MB

Nota: Todos con sus respectivos accesorios modernos, Pantalla LCD, mouse óptico USB (a excepción de uno que era de conexión P2P), teclado multifuncional.

Se interconectaron por medio de su tarjeta Ethernet configurada a PXE, es decir, que permita el arranque desde una conexión local a un switch encoire de 8 puertos con una velocidad de 10/100 MBPS por medio de cable UTP categoría 5e a la misma velocidad de transmisión.

La alimentación de energía se dio por medio de 2 tomacorrientes de 110v en donde se conectó un estabilizador a cada uno y de allí se dio energía a cada equipo, el consumo por hora de cada equipo es de 70w al servidor aproximadamente y 160w para cada uno de los clientes ligeros aproximadamente.

Nota: es de aclarar que por el amperaje se produjo un aumento de temperatura en el cable de energía sin sufrir daño alguno para este y mucho menos para los equipos.

La primera sesión inicia a las 10:30 am con la presentación de los coinvestigadores y de la prueba piloto en donde el módulo de ofimática estipulado para la prueba se muestra para la población campesina del municipio de Aranzazu, mientras los coinvestigadores guían el modulo, también se hace el constante monitoreo tanto del wireshark para la captura del tráfico que pasa por la tarjeta Ethernet del servidor, como el comportamiento de los cinco (5) equipos durante el tiempo que dura el modulo.

A las 11:50 am se da por terminada la primera sesión en donde se agradece a los asistentes por su participación en la prueba y se inspecciona cada equipo y sus

respectivas conexiones para dar un parte satisfactorio a la primera sesión de la prueba piloto, se detienen la captura de tráfico y se guarda para su utilización posterior

De 12:00 m a 2:00 pm se apagan los equipos.

A la 1:50 pm se encienden el servidor y los equipos para dar inicio a la segunda sesión de la prueba piloto.

A las 2:00 pm se da inicio a la segunda sesión y como ocurrió en la primera sesión se da la presentación de los integrantes y de la prueba piloto basada en el módulo de ofimática, mientras se da arranque a la captura del tráfico, esta sesión se alarga hasta las 3:20 pm en donde se finaliza con el agradecimiento a los participantes, guardar la captura y desinstalación del aplicativo y la desconexión de los equipos para su embalaje.

Terminado el modulo los integrantes debaten sobre la prueba realizada y se toman las siguientes conclusiones:

En cuanto a lo técnico se debe decir que pudieron ser más equipos conectados y colocados a nivel del aplicativo sin perder así el servicio LTSP, de acuerdo a mediciones al procesador del servidor.

El cable que conducía la energía de los tomacorrientes a los estabilizadores se vio con un aumento de temperatura, pero se debió a la conexión precaria que se tenía y no por el calibre del cable o por el amperaje, pero aun así no se observa imprevistos negativos.

En cuanto a lo teórico se pudo observar que aunque la institución fue una buena selección, el desarrollo del módulo y capturar la atención de los participantes fue complicado ya que se hizo en un lugar abierto, con mala acústica y con el paso continuo de gente ajena a la prueba.

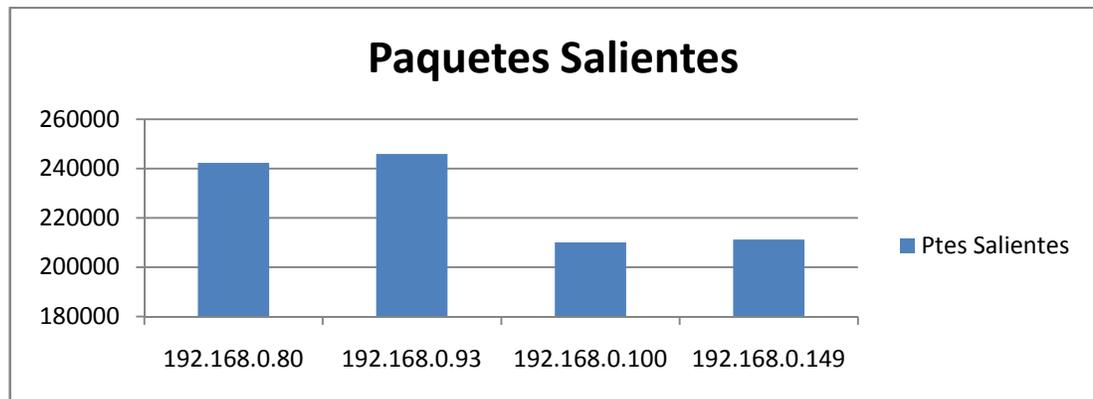
se implementó un módulo teniendo como vistos algunos conceptos de un equipo de cómputo o el simple uso continuo que el 35 o 40 % de la población activa en la prueba no tenían. Es así como se llevó a cabo un acompañamiento a dichas personas para que pudieran ir a la par con el resto de la gente.

El idioma nativo del aplicativo es el inglés, gran obstáculo en las personas que no lo conocen o están familiarizados y que fue en un 100% de los participantes, por ello se debió tomar un plan alternativo para el manejo de las funciones mostrando a cada uno donde se mostraba cada una de las mismas.

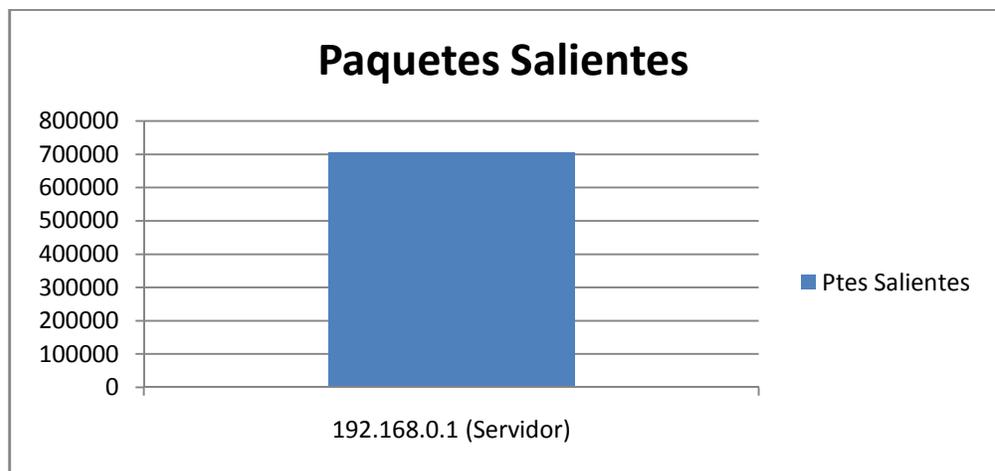
5.2 Análisis Del Tráfico De La Prueba Piloto

Con un promedio de velocidad de transmisión de 2,226 MBPS se capturaron 1616699 paquetes en 4174 segundos (1,15 hr) cada paquete tiene un tamaño de 387.333 y va a una tasa de transferencia de 278220 bytes / segundo.

De este tráfico solo se analizaran 707045 que son los generados por el servidor y sus cuatro (4) estaciones livianas y así llegar a posibles conclusiones de acuerdo a las gráficas obtenidas de la tabulación de los datos.

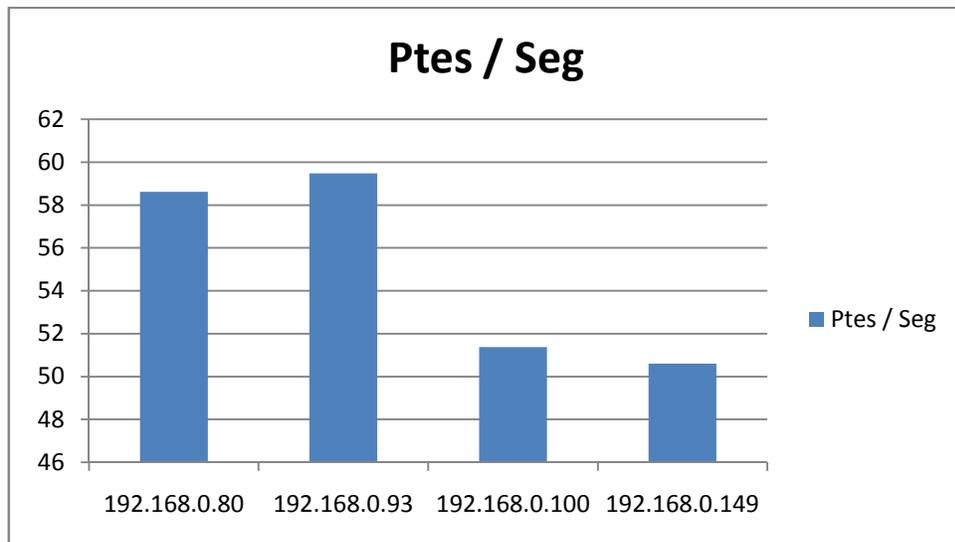


Grafica 1. Paquetes de cada cliente liviano.

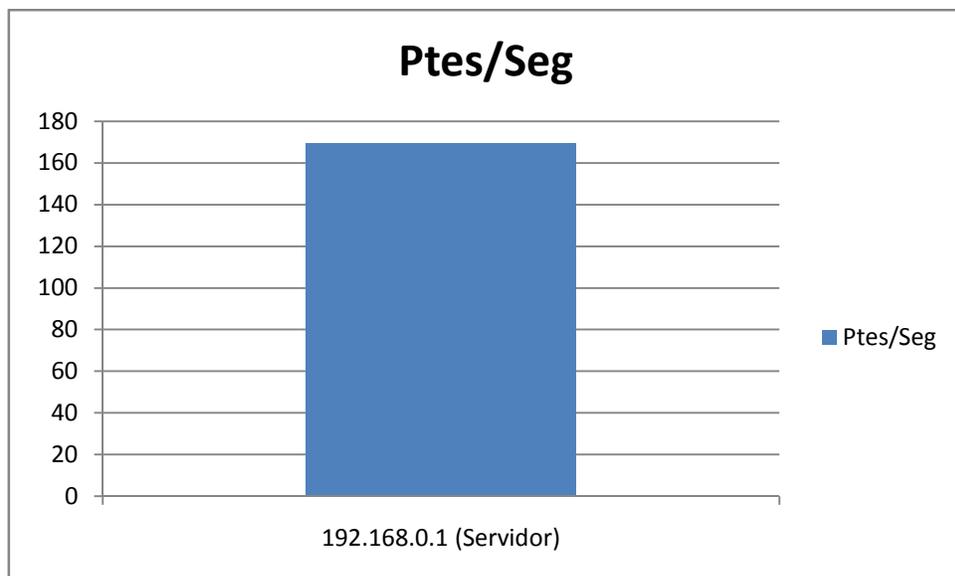


Grafica 2. Paquetes generados por el servidor.

En la gráficas 1 y 2 se puede evidenciar la cantidad de paquetes generados en cada estación y la diferencia en el tráfico, esto se debe a la causa de que los equipos no van a tener una misma carga de trabajo ya que son diferentes usuarios sentados frente a ellos y el servidor posee la mayor carga de trabajo y por ello es el que más paquetes genera. Dichos paquetes son analizados de acuerdo a su velocidad de Tx (MBPS), tasa de cantidad de paquetes en un segundo (Pte/Seg) y la tasa de bytes generada en un segundo (Byte/Seg).

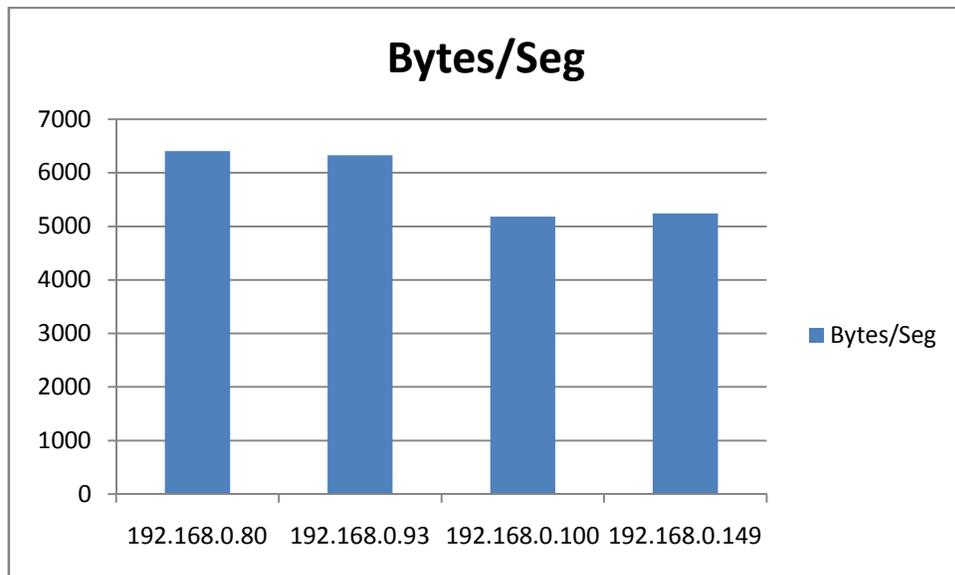


Grafica 3. Tasa de paquetes por segundo de los clientes livianos.

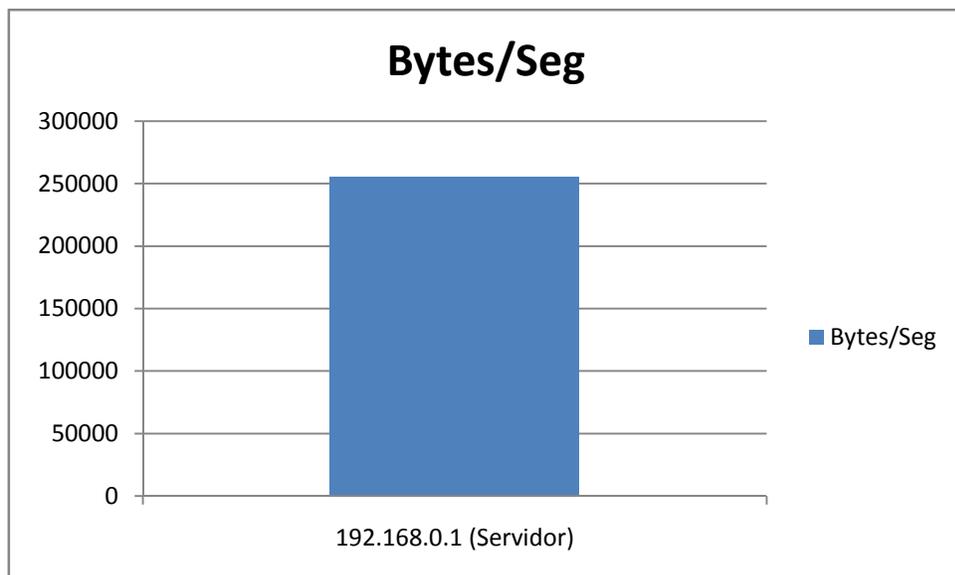


Grafica 4. Tasa de paquetes por segundo del servidor.

En las gráficas 3 y 4 se ve claramente la medición de los paquetes en un segundo tanto en los clientes ligeros como en el servidor, esto con el fin de observar la intinerancia en la red local.

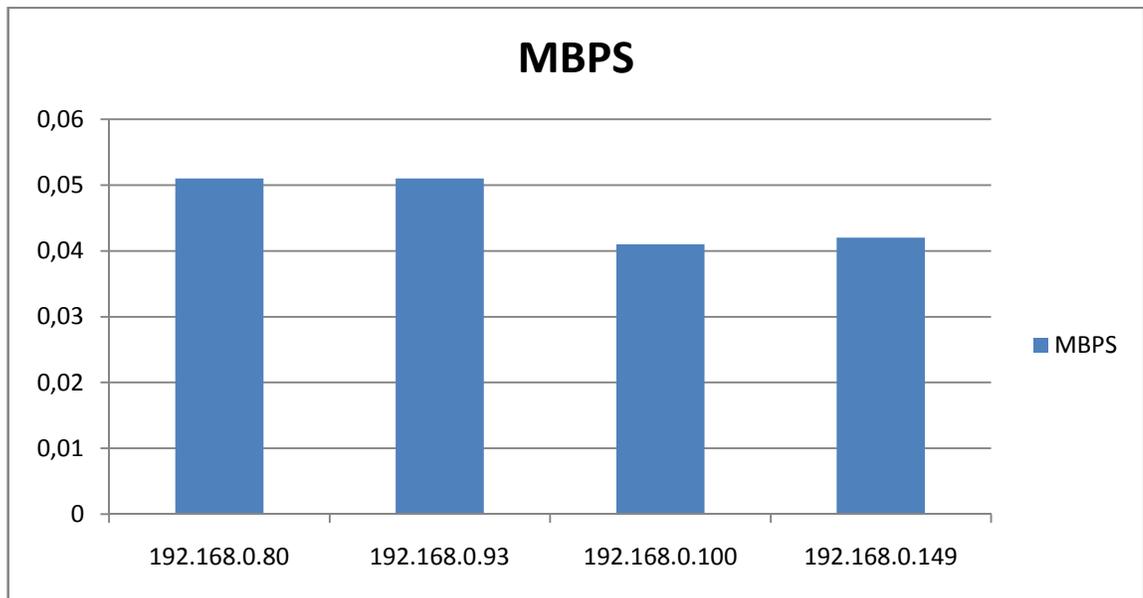


Grafica 5. Tasa de Bytes por segundo de los clientes livianos.

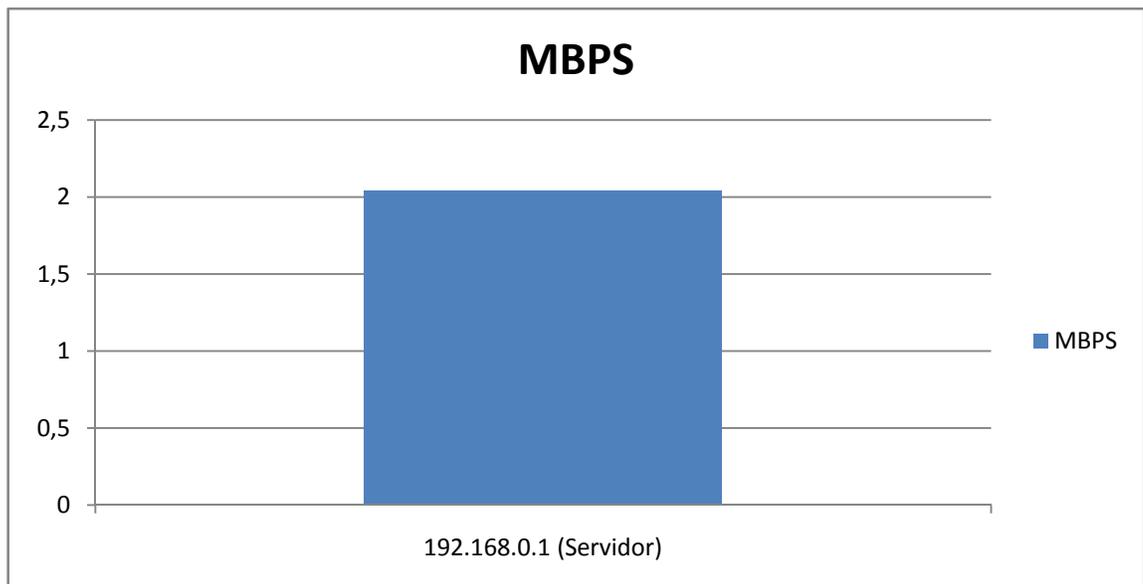


Grafica 6. Tasa de bytes generada por el servidor.

En las gráficas 5 y 6 se muestra la cantidad de bytes generada tanto por los clientes ligeros como el servidor, con ello, se podrá medir la cantidad de datos transmitidos entre dos puntos.



Gráfica 7. Consumo en MBPS de clientes ligeros.



Gráfica 8. Consumo en MBPS del servidor.

En la gráfica 7 y 8 se observa el consumo de la red en un segundo por parte de los clientes y el servidor, con base a esto se da la siguiente ecuación hipotética: Capacidad de transmisión del switch - porcentaje de expansión- porcentaje de reducción de picos = cantidad de clientes ligeros soportados sin perder el servicio por denegación del servidor.

Para una tarea de solo ofimática se podría decir que, de acuerdo con la gráfica 7 y 8 se podrían tener una cantidad considerable de equipos, pero también se observa que para transmisión de paquetes multimedia como es el caso del video, se dificulta al tener mucho más uso del ancho de banda por consiguiente menos espacio para equipos livianos a continuación se hace la descripción del laboratorio para llegar a esta conclusión.

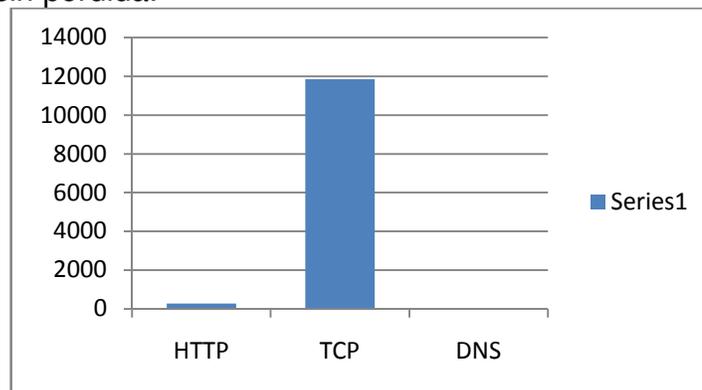
6. VIDEO VISTO POR EL SERVIDOR VS VIDEO VISTO POR CLIENTE LIGERO

Se hace la captura del tráfico de un video de la misma duración en dos (2) situaciones:

- 1- La primera es el video subido a youtube.com con el enlace <http://youtu.be/IU5QqkMFBA>, se captura el tráfico en el momento en el cual sale al medio por anclaje de red de un celular, propiedad de uno de los coinvestigadores y posteriormente se reproduce desde este portal.

En este proceso se hace una captura de 11928 paquetes, un total de 11416479 bytes en total en 162.042 segundos, con una velocidad de 73.6 paquetes / segundo y un consumo de transmisión de 0.6 MBPS aproximadamente.

Se observan los protocolos HTTP, DNS pero aquel que más se repite es el protocolo TCP el cual permite el envío de paquetes entre un punto A y un punto B sin perdida.

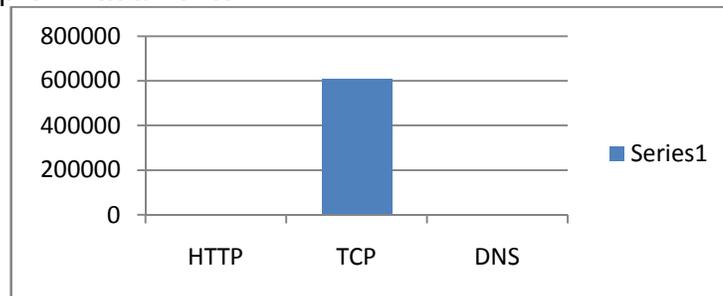


Grafica 9. Protocolos usados en internet

En la gráfica 9 se observa el uso del protocolo HTTP para transferir texto con atributos propios de Internet, es decir, la comunicación del ordenador o cliente con el medio, se observa también el protocolo DNS para la asociación de el nombre del dominio con su dirección IP, pero el protocolo de transferencia TCP se ve que supera notoriamente a los demás protocolos presentes en el laboratorio.

- 2- El mismo video se coloca en el servidor y se le dan los permisos para ser reproducidos en los clientes livianos, dando captura a su tráfico sin necesidad de salir al medio, dando así un ahorro de dinero al no salir al medio.

Se capturan 609062 paquetes en 162.973 segundos con una velocidad de 3737.206 paquetes / segundo y un consumo de transmisión de 82.373 MBPS aproximadamente.



Grafica 10. Protocolos usados LTSP

En la captura que se muestra de acuerdo a la grafica10 fácilmente se observa que el 100% de los paquetes capturados poseen protocolo TCP, esto se debe a que el video no se encuentra en la nube sino alojado en el servidor, por lo cual solo se hace una transferencia entre el servidor y el cliente.

Es de aclarar que el tráfico del video en youtube.com se captura desde la tarjeta inalámbrica y el del servidor se toma desde la tarjeta de red Ethernet.

7. CONCLUSIONES DE FUNCIONAMIENTO DE LA APLICACIÓN LTSP EN LA PRUEBA PILOTO

La aplicación LTSP tiene una velocidad de transmisión de 100 Mb/s que es el máximo que permite el switch que se utilizó para esta prueba piloto, de este 100% se utiliza un 25% para cargar y descargar archivos, el 75% restante de la transmisión se utiliza para la comunicación y transmisión entre los clientes ligeros. Como en comunicaciones y en transmisión de información no es recomendable trabajar sobre picos, es decir sobre puntos máximos o mínimos se utiliza solo el 60% para la comunicación de los clientes ligeros que es una medición recomendable para evitar que colapse dicha comunicación. Si se parte de la base por hipótesis y mediciones realizadas durante la prueba piloto que cada equipo o cliente ligero consume 2,24 Mbps se puede tener la probabilidad de que con esta velocidad pueden trabajar entre 25 y 30 equipos, posterior a esto el servidor y el resto de los servicios pueden caducar y dejar de funcionar. Esta Hipótesis o

probabilidad que se ha propuesto se deja a consideración, estudio o corroboración de futuras investigaciones

8. UDP Vs TCP

8.1 El Protocolo UDP

“UDP es un protocolo no orientado a conexión. Es decir cuando una maquina A envía paquetes a una maquina B, el flujo es unidireccional. La transferencia de datos se realiza sin haber realizado previamente una conexión a la máquina de destino (máquina B) y el destinatario recibirá los datos sin enviar una confirmación al emisor (la máquina A). Esto debido a que la encapsulación de datos enviada por el protocolo UDP no permite transmitir la información relacionada al emisor. Por el destinatario no conocerá al emisor de los datos excepto su IP.

El protocolo UDP es un protocolo mínimo de nivel de transporte orientado a mensaje documentado en el RFC 768 de la IETF. En los protocolos de internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP no otorga garantías para la entrega de sus mensajes y el origen UDP no retiene estados de los mensajes UDP que han sido enviados a la red. UDP solo añade multiplexado de aplicación y suma de verificación de la cabecera y la carga útil. Cualquier tipo de garantías para la transmisión de la información deben ser implementadas en capas superiores.

+	Bits 0 - 15	16 - 31
0	<i>Puerto origen</i>	<i>Puerto destino</i>
32	<i>Longitud del Mensaje</i>	<i>Suma de verificación</i>
64	<i>Datos</i>	

Grafica 11. Muestra la cabecera UDP que consta de 4 campos de los cuales 2 son opcionales.

La cabecera UDP consta de 4 campos de los cuales 2 son opcionales. Los campos de los puertos fuente y destino son campos de 16 bits que identifican el proceso de origen y recepción. Ya que UDP carece de un servidor de estado y el origen UDP no solicita respuestas, el puerto origen es opcional. En caso de no ser utilizado, el puerto origen debe ser puesto a cero. A los campos del puerto destino le sigue un campo obligatorio que indica el tamaño en bytes del datagrama UDP incluidos los datos. El valor mínimo es de 8 bytes.

El campo de la cabecera restante es una suma de comprobación de 16 bits que abarca una pseudo-cabecera IP (con las IP origen y destino, el protocolo y la longitud del paquete UDP), la cabecera UDP, los datos y 0's hasta completar un múltiplo de 16. El checksum también es opcional en IPv4, aunque generalmente se utiliza en la práctica (en IPv6 su uso es obligatorio). A continuación se muestra los campos para el cálculo del checksum en IPv4.

bits	0 – 7	8 – 15	16 – 23	24 – 31
0	<i>Dirección Origen</i>			
32	<i>Dirección Destino</i>			
64	<i>Ceros</i>	<i>Protocolo</i>	<i>Longitud UDP</i>	
96	<i>Puerto Origen</i>		<i>Puerto Destino</i>	
128	<i>Longitud del Mensaje</i>		<i>Suma de verificación</i>	
160	<i>Datos</i>			

Grafica 12. Tabla con los campos para el cálculo del checksum en IPv4.

*El protocolo UDP se utiliza por ejemplo cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes”.*¹

8.1.1 Transmisión de Video y Voz:

“UDP es generalmente el protocolo usado en la transmisión de vídeo y voz a través de una red. Esto es porque no hay tiempo para enviar de nuevo paquetes perdidos cuando se está escuchando a alguien o viendo un vídeo en tiempo real.

Ya que tanto TCP como UDP circulan por la misma red, en muchos casos ocurre que el aumento del tráfico UDP daña el correcto funcionamiento de las aplicaciones TCP. Por defecto, TCP pasa a un segundo lugar para dejar a los datos en tiempo real usar la mayor parte del ancho de banda. El problema es que ambos son importantes para la mayor parte de las aplicaciones, por lo que encontrar el equilibrio entre ambos es crucial.

¹<http://www.rfc-es.org>_Gonzalo Paniagua Javier, dom 14 abr 2013 15:14:37 EDT, España

*Todo este tipo de protocolos son usados en telemática*².

8.2 EL PROTOCOLO TCP

Contrariamente a UDP, el protocolo TCP está orientado a conexión. Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de datos y confirma su buena recepción. Aquí interviene el control CRC de datos que se basa en una ecuación matemática que permite verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que vuelvan a enviar los datos corruptos.

Establecimiento de la conexión (negociación en tres pasos).³

7.2.1 Negociación en tres pasos o Three-way handshake

“Aunque es posible que un par de entidades finales comiencen una conexión entre ellas simultáneamente, normalmente una de ellas abre un socket en un determinado puerto TCP y se queda a la escucha de nuevas conexiones. Es común referirse a esto como apertura pasiva, y determina el lado servidor de una conexión. El lado cliente de una conexión realiza una apertura activa de un puerto enviando un paquete SYN inicial al servidor como parte de la negociación en tres pasos. En el lado del servidor (este receptor también puede ser una PC o alguna estación terminal) se comprueba si el puerto está abierto, es decir, si existe algún proceso escuchando en ese puerto, pues se debe verificar que el dispositivo de destino tenga este servicio activo y esté aceptando peticiones en el número de puerto que el cliente intenta usar para la sesión. En caso de no estarlo, se envía al cliente un paquete de respuesta con el bit RST activado, lo que significa el rechazo del intento de conexión. En caso de que sí se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un ACK, completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión. Es interesante notar que existe un número de secuencia generado por cada lado, ayudando de este modo a que no se puedan establecer conexiones falseadas (spoofing)”.⁴

²<http://www.ietf.org>, Association Management Solutions, LLC (AMS).Fremont, California 94538

³ <http://es.kioskea.net/faq/1559-diferencias-entre-los-protocolos-tcp-y-udp>, [Jeff PILLOU](#)
[Director de la publicación](#)

⁴ http://www.linux-magazine.es/issue/35/031-035_LTSP35.crop.pdf. Cristian Kroll.
Linux Magazine.net

8.2.2 Transferencia de datos:

“Durante la etapa de transferencia de datos, una serie de mecanismos claves determinan la fiabilidad y el tamaño del protocolo. Entre ellos está incluido el uso del número de secuencia para ordenar los segmentos TCP recibidos y detectar paquetes duplicados, checksums para detectar errores, y asentimientos y temporizadores para detectar pérdidas y retrasos.

Durante el establecimiento de conexión TCP, los números iniciales de secuencia son intercambiados entre las dos entidades TCP. Estos números de secuencia son usados para identificar los datos dentro del flujo de bytes, y poder identificar (y contar) los bytes de los datos de la aplicación. Siempre hay un par de números de secuencia incluidos en todo segmento TCP, referidos al número de secuencia y al número de asentimiento. Un emisor TCP se refiere a su propio número de secuencia cuando habla de número de secuencia, mientras que con el número de asentimiento se refiere al número de secuencia del receptor. Para mantener la fiabilidad, un receptor asiente los segmentos TCP indicando que ha recibido una parte del flujo continuo de bytes. Una mejora de TCP, llamada asentimiento selectivo (SACK, Selective Acknowledgement) permite a un receptor TCP asentir los datos que se han recibido de tal forma que el remitente solo retransmita los segmentos de datos que faltan.

A través del uso de números de secuencia y asentimiento, TCP puede pasar los segmentos recibidos en el orden correcto dentro del flujo de bytes a la aplicación receptora. Los números de secuencia son de 32 bits (sin signo), que vuelve a cero tras el siguiente byte después del 232-1. Una de las claves para mantener la robustez y la seguridad de las conexiones TCP es la selección del número inicial de secuencia (ISN, Initial Sequence Number).

Un checksum de 16 bits, consistente en el complemento a uno de la suma en complemento a uno del contenido de la cabecera y datos del segmento TCP, es calculado por el emisor, e incluido en la transmisión del segmento. Se usa la suma en complemento a uno porque el acarreo final de ese método puede ser calculado en cualquier múltiplo de su tamaño (16-bit, 32-bit, 64-bit...) y el resultado, una vez plegado, será el mismo. El receptor TCP recalcula el checksum sobre las cabeceras y datos recibidos. El complemento es usado para que el receptor no tenga que poner a cero el campo del checksum de la cabecera antes de hacer los cálculos, salvando en algún lugar el valor del checksum recibido; en vez de eso, el receptor simplemente calcula la suma en complemento a uno con el checksum incluido, y el resultado debe ser igual a 0. Si es así, se asume que el segmento ha llegado intacto y sin errores.

Hay que fijarse en que el checksum de TCP también cubre los 96 bit de la cabecera que contiene la dirección origen, la dirección destino, el protocolo y el tamaño TCP. Esto proporciona protección contra paquetes mal dirigidos por errores en las direcciones.

El checksum de TCP es una comprobación bastante débil. En niveles de enlace con una alta probabilidad de error de bit quizá requiera una capacidad adicional de corrección/detección de errores de enlace. Si TCP fuese rediseñado hoy, muy probablemente tendría un código de redundancia cíclica (CRC) para control de errores en vez del actual checksum. La debilidad del checksum está parcialmente compensada por el extendido uso de un CRC en el nivel de enlace, bajo TCP e IP, como el usado en el PPP o en Ethernet. Sin embargo, esto no significa que el checksum de 16 bits es redundante: sorprendentemente, inspecciones sobre el tráfico de Internet han mostrado que son comunes los errores de software y hardware[cita requerida] que introducen errores en los paquetes protegidos con un CRC, y que el checksum de 16 bits de TCP detecta la mayoría de estos errores simples.

Los asentimientos (ACKs o Acknowledgments) de los datos enviados o la falta de ellos, son usados por los emisores para interpretar las condiciones de la red entre el emisor y receptor TCP. Unido a los temporizadores, los emisores y receptores TCP pueden alterar el comportamiento del movimiento de datos. TCP usa una serie de mecanismos para conseguir un alto rendimiento y evitar la congestión de la red (la idea es enviar tan rápido como el receptor pueda recibir). Estos mecanismos incluyen el uso de ventana deslizante, que controla que el transmisor mande información dentro de los límites del buffer del receptor, y algoritmos de control de flujo, tales como el algoritmo de Evitación de la Congestión (congestión avoidance), el de comienzo lento (Slow-start), el de retransmisión rápida, el de recuperación rápida (Fast Recovery), y otros”⁵

⁵<http://www.manolodominguez.com/content/common/pdf/cv/publications/AdministracionAvanzadaDeRedesTCPIP.pdf>. Administración Avanzada de Redes. TCP / IP. Javier Carmona Murillo, David Cortés Polo, Manuel Domínguez Dorado, Alfonso Gazo Cervero, José Luis González Sánchez, Francisco Javier Rodríguez Pérez. Primera Edición. Enero de 2012.

9. CONCLUSIONES

- El funcionamiento de la aplicación LTSP se muestra que va encaminado por la dirección correcta ya que está consiguiendo que los servicios de terminales ligeros basados en Linux sean más populares gracias a la facilidad de su mantenimiento y a su gran cantidad de funcionalidades, adicionalmente a su bajo costo de implementación.
- Con la implementación de la aplicación LTSP se está demostrando que la obsolescencia no es una disculpa para disminuir la brecha digital ya que la reutilización de estos equipos y una buena implementación de aplicaciones con clientes ligeros permiten un funcionamiento más adecuado y prolongado de las maquinas.
- Actualmente las grandes y medianas empresas están migrando a la virtualización de sus escritorios, todo esto con el fin de reducir costos relacionados a licencias de herramientas de ofimática y sistemas operativos, una muestra clara es la nueva versión de Microsoft Office 365, el cual está enfocado su funcionamiento en la nube es decir virtualizado, cuyo funcionamiento es enfocado a clientes brutos o clientes ligeros, pues sus servicios los ofrecen promocionando la virtualización de los escritorios.

BIBLIOGRAFIA

- Disponible en “<http://www.rfc-es.org>” Gonzalo Paniagua Javier, Última Actualización Domingo 14 Abril 2013 15:14:37 EDT, España
- Disponible en “<http://www.ietf.org>”, Association Management Solutions, LLC (AMS). Fremont, California 94538 USA
- Disponible en “<http://es.kioskea.net/faq/1559-diferencias-entre-los-protocolos-tcp-y-udp>”, Jeff PILLOU Director de la publicación
- Disponible en “http://www.linux-magazine.es/issue/35/031-035_LTSP35.crop.pdf”. Cristian Kroll. Linux Magazine.net
- Disponible en “<http://www.manolodominguez.com/content/common/pdf/cv/publications/AdministracionAvanzadaDeRedesTCPIP.pdf>”. Administración Avanzada de Redes. TCP / IP. Javier Carmona Murillo, David Cortés Polo, Manuel Domínguez Dorado, Alfonso Gazo Cervero, José Luis González Sánchez, Francisco Javier Rodríguez Pérez. Primera Edición. Enero de 2012.