Universidad Técnica Federico Santa María
Departamento de Electrónica

Proyecto Redes de Computadores Elo322
Routers, Servidor Virtual y Seguridad

Integrantes: Edson Contreras C.
Luis Marcel Barraza M.
Fecha: 18/07/2010

1. Resumen Ejecutivo:

La necesidad de poseer acceso a internet localmente en una empresa o en el hogar hace que cada día se requieran mas direcciones IP para uso de servidores Web y uso doméstico. Como IPv4 no posee tal cantidad surge la necesidad de desarrollar servidores virtuales, los cuales dejen acceso a una máquina presente en una LAN, tenga acceso a la WAN como un servidor con la IP del router que está de por medio (como un puerto (socket) de este) y de esta forma "utilizar menos IPs".

Hoy en día tener acceso a internet va de la mano con tener WIFI (o internet inalámbrico) y uno paga por un servicio que uno desea utilizar. ¿Qué tan seguro es? ¿Como saber si hay alguien que me está robando internet?

2. Introducción:

Los ISP en Chile (y por lo general en el mundo funciona así) venden internet principalmente de 2 formas:

- PPPoE, con IP dinámica (Telefónica Movistar)
- DHCP, con IP estática (VTR)

Para configurar un Servidor Virtual, asumiremos que disponemos de un router y un switch que realizaran la LAN. Para el resto de la configuracion dependeremos del ISP y el tipo de servicio como IP estática o dinámica, explicaremos ambas.

La seguridad en una red inalámbrica (en la actualidad) se basa principalmente en 2 tipos de algoritmos:

- WEP
- WPA y WPA2

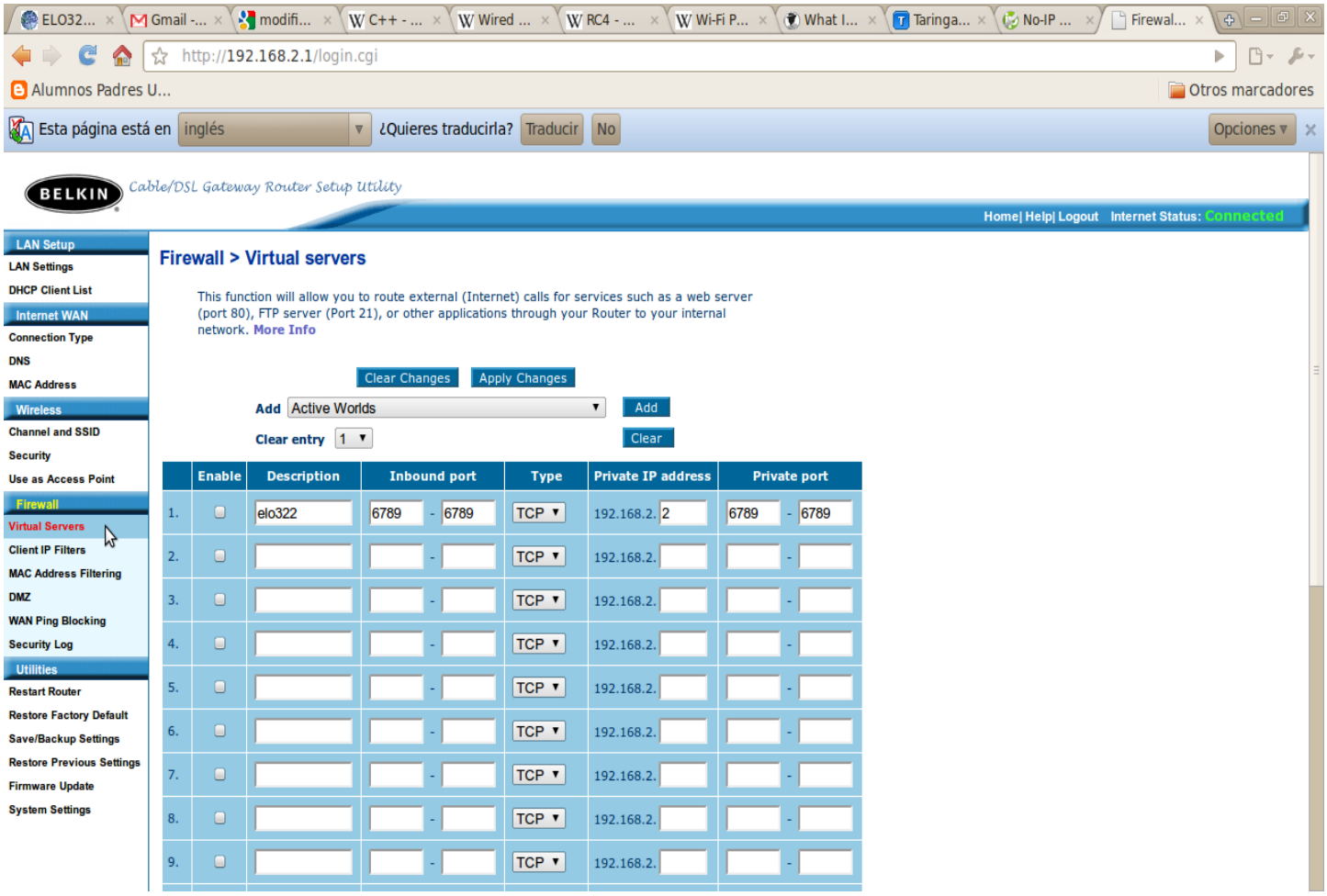
El primer algoritmo, que es el mas común, encripta la contraseña y la envía en el mismo encabezado, lo cual lo hace muy vulnerable.

Los segundos tipos de algoritmos, aunque su forma de operación no se conoce con exactitud por motivos de seguridad, se puede vulnerar su seguridad y sera explicado como.

3. Desarrollo:

<u>Montar un Servidor Virtual con ISP del tipo DHCP con IP estática:</u>

El hecho de tener una IP estática facilita bastante la forma de configurar el router. Para configurar el router explicaremos la siguiente lámina puesta a continuación.



En la lámina anterior estamos configurando un router Belkin para la demostración. Lo correspondiente al lado izquierdo de la ventana de configuración, corresponde a la descripción del servicio (para los logs y el registro de eventos que van ocurriendo).

- Inbound port: Corresponde a que puertos se van a intentar conectar las conexiones externas, es un rango y no necesariamente deben coincidir con los puertos específicos corriendo en el servidor.
- Type: Corresponde a que si la conexión esperada es del tipo TCP o UDP.
- Private IP address: Aquí va la dirección del equipo dentro de la LAN que está funcionando realmente como un servidor, por lo que es una IP local.
- Private port: Asociado al puerto en el cual efectivamente está escuchando el servidor.

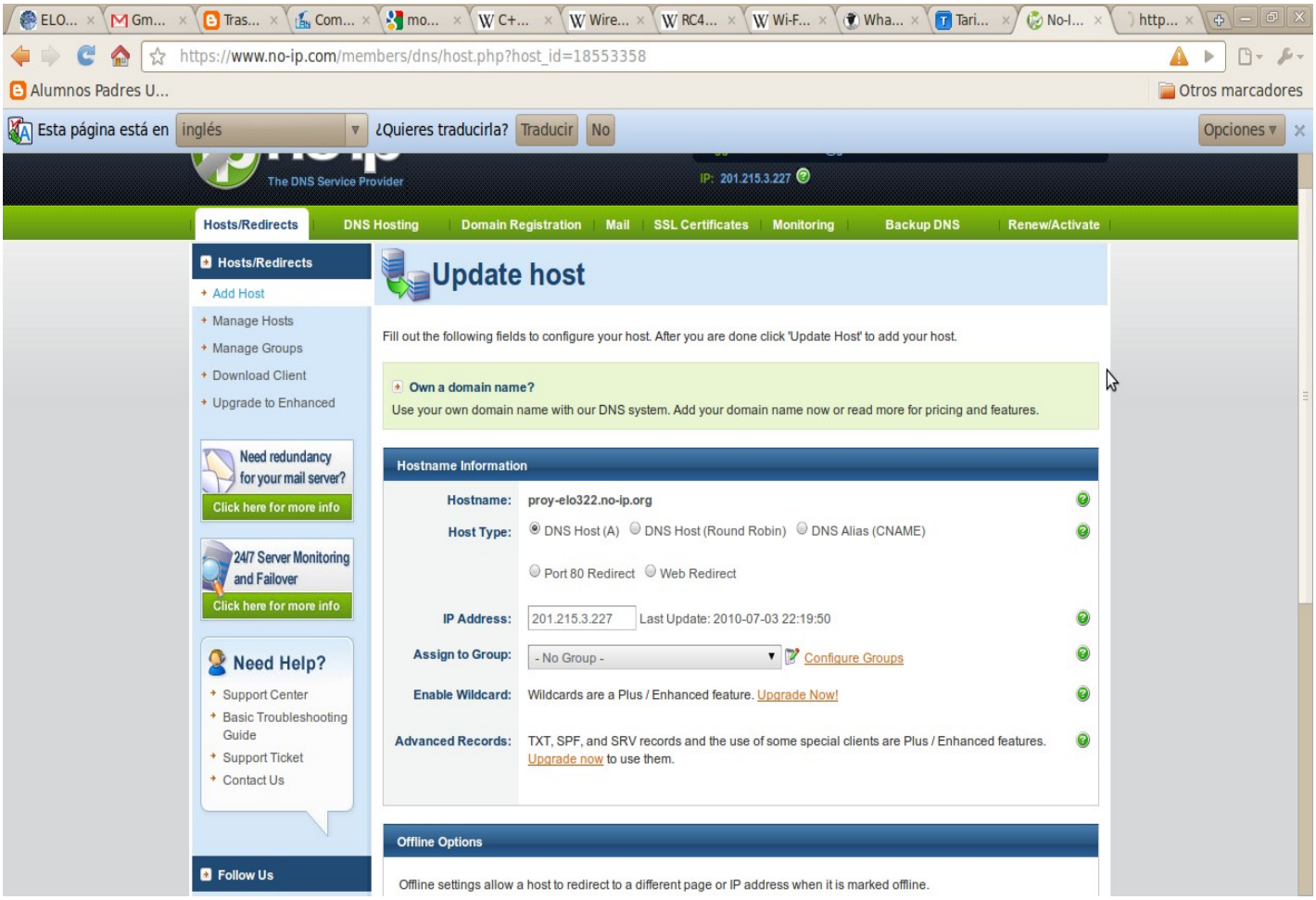
El usuario que desea conectarse al servidor virtual, solamente accede a la IP que tiene asociado el router que el ISP DHCP le asignó, como esta no varía en el tiempo no hace falta más que eso ya que este último hace la redirección localmente.

Montar un Servidor Virtual con ISP del tipo PPPoE con IP dinámica:

Aquí es donde comienzan a complicarse un poco las cosas ya que en el tema de seguridad es muy bueno tener asociada una IP que vaya cambiando cada vez que me conecto, pero para efectos de tener un servidor, comienza a generar problemas. La configuración interna del router y la LAN es la misma que el caso anterior, lo que cambia es la forma de REFERENCIAR a mi servidor.

¿Como doy referencia de una IP que es cambiante en el tiempo?

Hay sitios web que ayudan a solucionar problemas de este tipo, básicamente actúan como DNS, y poseen una lista de IP que están asociadas al servidor hosteado en la LAN. Veremos una explicación mas gráfica a continuación.



La lámina anterior muestra como funciona la configuración como DNS de la página web www.no-ip.org la cual permite crear una pagina web que basicamente redirige la conexión a una IP que uno configure.

- Hostname: Nombre de la pagina web que será referenciada por los clientes.
- Host type: Tipo de host que será nuestra página. Para efectos de un servidor virtual estándar seleccionamos DNS Host (A)
- IP Address: Aquí va la IP de nuestro router, como esta va cambiando dinámicamente basta que el administrador de la web coloque aquí la nueva IP y los clientes seguirán conectandose a: proy-elo322.no-ip.org, aunque la IP a la que es redirigido haya cambiado en el tiempo. Esta página web posee tambien un software (que corre en windows, linux y mac) que corre “eternamente” en el servidor y analiza si la IP ha cambiado. De haber cambiado, automáticamente modifica la IP y la actualiza en el servidor.

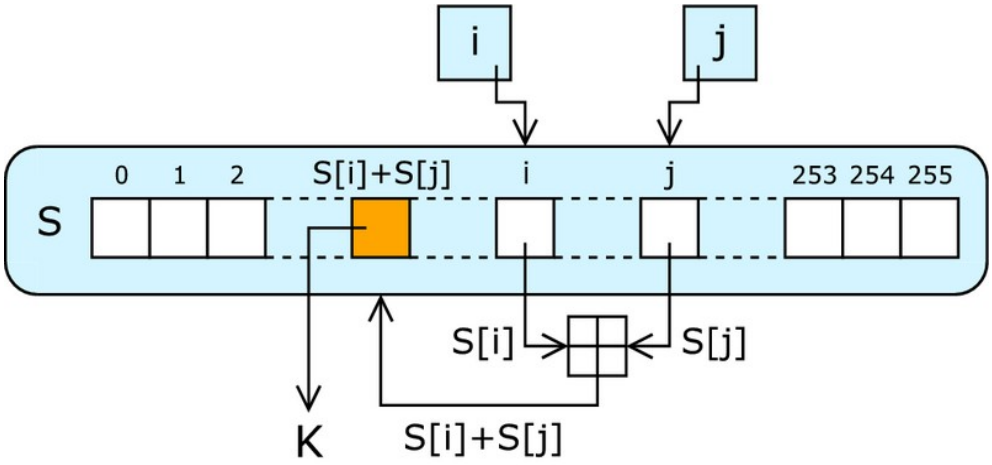
Con esto podemos notar que independiente de tener una IP estática o dinámica, podemos realizar un servidor virtual para así poder tener un servidor web o de lo que uno quisiese detrás de una LAN.

Seguridad de una red inalámbrica:

Una red inalámbrica como la que poseemos en nuestra casa envía cada paquete que nosotros solicitamos a internet o dentro de la propia LAN hasta lo más lejano que de su alcance y en todas direcciones, ya que el router no sabe si nosotros nos encontramos en un lugar fijo de la casa o a cuanta distancia exacta nos encontramos. Como cada paquete lleva en su encabezado la dirección física (MAC address) de la tarjeta de red inalámbrica que solicitó el paquete, cualquier otro computador que esté en el camino simplemente descarta dicho paquete ya que no es para el. Hay una forma de habilitar la tarjeta de red inalámbrica como modo promiscuo y así capturar paquetes que estén rondando cerca del lugar donde me encuentro. Dependiendo de la seguridad de la red y el tráfico de esta se pueden realizar diversas acciones y ataques para acceder a las contraseñas de la conexión y así acceder a internet a través de dicho punto de acceso.

Seguridad del tipo WEP:

Es el tipo de seguridad mas antiguo, pero por su facilidad de implementación a nivel de hardware hace que sea utilizado hasta el día de hoy. Se hace una tabla hash con los datos que uno ingresa y estos se van encriptando y re-encriptando cuantas veces requiera el router, pero como es el mismo algoritmo, si yo realizo esta misma operación con un gran numero de paquetes eventualmente llegaré a un patrón que se repite en todos independientemente de cuantas veces desencripte, esto último mencionado es la base del ataque WEP, lo cual hace que solamente se necesite un gran numero de datos (con 20000 es un 95% exitoso el ataque) que es perfectamente posible obtener si una red objetivo se ecuentra cargando videos por internet o escucha música por internet. La encriptación hash es de la siguiente forma:



En el dibujo anterior, podemos contemplar una de las formas en las cuales se encriptan los paquetes donde en el bloque con la + en su interior, suma los contenidos y lo va haciendo periódicamente cuantas veces el router esté programado para hacerlo.

Seguridad del tipo WPA y WPA2:

Era el tipo de seguridad “mas seguro” hasta hace poco, tanto que su funcionamiento en si no es público para asi evitar ataques al algoritmo. Se descubrió que si yo quiero atacar una red de este tipo y hay alguien ya conectado a esta red, puedo “suplantar” su identidad y así desconectarlo del router con un ataque del tipo chop-chop. Luego de haberlo desconectado el usuario intentara reconectarse, pero como estoy suplantando su identidad me conecto JUNTO con él (cabe destacar que WPA tiene un sistema de contraseñas locales y globales, unas dejan acceder a ciertos sectores, en los cuales se intercambia la contraseña real, es a este lugar donde se tiene el acceso). Como se está reconectando, va mandar toda la información de conexión. Ahí es donde capturaremos un paquete del tipo ARP (Address Request Protocol, Protocolo de resolución de direcciones) donde el router le asigna una IP válida (LAN) si se ha ingresado la contraseña correcta. Al atrapar ese paquete en particular, se puede atacar exitosamente una red WPA, aunque es mucho más engorroso y complejo.

4. Conclusión:

En el ámbito de los servidores virtuales, con el fuerte surgimiento de IPv6 será un tema del pasado, hasta que la masificación de IPv6 sea un hecho, es la mejor forma de levantar servidores u ofrecer servicios desde mi casa o la oficina y de esta forma tener un control mas seguro de lo que llega hasta el servidor, ya que el router que está en el camino actúa tambien como un firewall.

La seguridad de las redes inalámbricas siempre será un problema ya que de una u otra forma debe ir la información de autentificación en todos los paquetes que van hacia el router, de no ser asi no se podría discriminar de una persona que hace uso bueno o malo del router que está de por medio. Y el hecho de utilizar una única contraseña, le da mucha desventaja contra la cantidad de paquetes que son enviados por segundo. ¿Una evolución al momento de construir físicamente?, ¿Utilizar más de una contraseña? ¿Restringir más el acceso de los usuarios al área inalámbrica?. Ciertamente estas preguntas no tienen respuesta en el corto plazo, pero quizás sean las mejores formas de optimizar la seguridad de las personas y las empresas, ya que cada día mas tipos de transacciones se realizan por internet y estamos cada vez más expuestos.