INFORMATICA A BORDO

CAPITULO 26

CONECTIVIDAD WiFi (II)

Vamos a segur aprendiendo sobre las conexiones inalámbricas. Esta vez vamos a ver las opciones del usuario y las opciones de implementación del puerto. Analizaremos las decisiones que deben tomar ambas partes para conseguir el mejor servicio, según vayamos afrontando temas y dudas.

¿Cómo establecemos la primera conexión?

Lo primero que debemos hacer es informarnos en capitanía del puerto sobre las condiciones de conexión. Cada puerto es un "mundo" y nos podemos encontrar muchos escenarios diferentes. Luego analizaremos cual es la mejor opción.

A primera vista seguro que queremos que nos las ofrezcan gratuita y sin condiciones, pero … ¿es la mejor? Sin duda no lo es. Estas conexiones libres de pago no tienen habitualmente ningún control y podemos correr varios peligros.

1. No hay reserva de ancho de banda. El que primero llega se lleva todo el caudal. Si tenemos un vecino que se el dia bajándose películas y canciones nos encontraremos con una calidad bajísima, ya que el caudal que nos queda es mínimo. Los usuarios que utilizan programas P2P para bajarse contenidos (Kazaa, Emule, Ares, BitTorrent …), utilizan todo el caudal de bajada y subida de internet que se encuentran, "sin piedad", de forma que el resto de usuarios se encontrarán con un caudal mínimo o bajo mínimos para navegar o ver su correo.
   Lo veremos fácilmente con un ejemplo:
   Imaginemos que el caudal que nos ofrecen en nuestro puerto es como una autopista de 4 u 8 carriles, dependiendo de la ADSL que tengan. En condiciones normales, con seguridad "anti-P2P", tenemos carriles de sobras para más de 50 usuarios trabajando. No tendríamos problemas de "tráfico", ya que las peticiones a Internet no son continuas y los "carriles" las van absorbiendo.

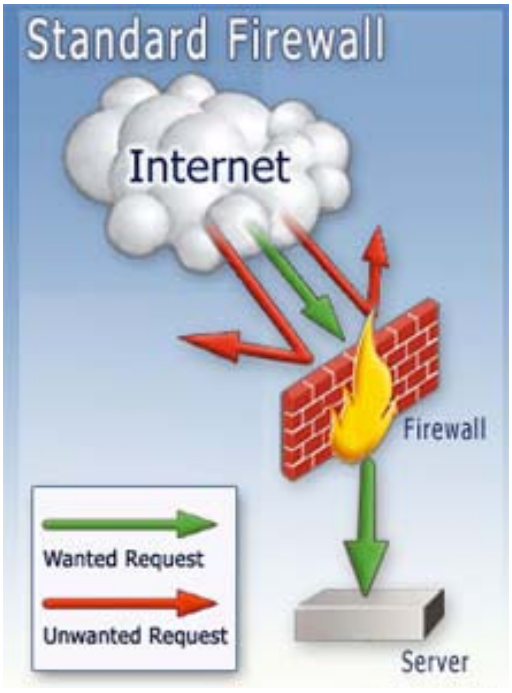
Si uno o varios usuarios tienen en marcha sus programas P2P, nos encontraremos que sus peticiones de entrada y salida son continuas. Es lo mismo que encontrarnos con una autopista llena de coches hasta saturarla, de forma que si se sale un coche por una salida, al momento entra otro a ocupar su lugar. ¿Qué espacio de circulación nos queda?. Ninguno. Nos encontraríamos con esta foto:

2. La información que movemos está al alcance de todos. Si no tenemos clave de encriptación y seguridad en el sistema, podemos encontrarnos que el mismo vecino que se está bajando canciones, tiene un "programilla" que captura todo lo que se mueve por las ondas, y le va a llegar toda la información en enviamos y recibimos. Realmente peligroso. Y no pensemos eso de "¿a quién le importa mi información?, no me preocupa …". Acuérdense de una norma: En informática siempre hay gente aburrida que su objetivo es robar la información del vecino, aunque no le sirva de nada. Y uno de esos "aburridos" estará seguro acechando nuestra red de forma continua para ver si nos caza algo. ¿No se lo creen? Pónganse un Firewall en la red y activen los LOGS una semana. Cuando vean los informes de intentos de ataques al sistema ya

no dormirán tranquilos pensando qué hacían hasta entonces sin un Firewalll. Parta de la idea que tiene un vecino hacker, no lo dude …

3. Si nuestro PC está compartido los tendremos a todos dentro. Si la red no tiene sistemas de aislamiento de usuarios, nos encontraremos que nuestros recursos compartidos del portátil, por necesidades de trabajo en nuestra ubicación habitual, pasan a estar a disposición de todos los usuarios conectados a nuestra misma red inalámbrica. Esto empieza a dar miedo ¿verdad?

4. Estaremos desprotegidos ante la entrada de virus y spywares. Si el punto de acceso no bloquea todo el tráfico entre las conexiones, estaremos expuestos a recibir virus y spywares desde el resto de usuarios. Es muy importante tener la tranquilidad de saber que nuestra conexión está aislada y blindada. Para eso los sistemas del puerto deben tener buenos sistemas de seguridad perimetral con Firewalls (cortafuegos) que bloqueen todo el tráfico de entrada con contenidos peligrosos.



5. No hay garantía de conexión. En la mayoría de estos escenarios de trabajo no hay garantía de conexión. En caso de fallo nos podemos encontrar en muchos casos con la respuesta de "Es gratis, no podemos ofrecerle ninguna garantía".

Conclusión:

¿Y si resulta que lo que necesitamos nosotros es una conexión con garantías, segura y con un buen ancho de banda?

Si vamos a trabajar y mover información de trabajo ¿Nos interesa estar protegidos de ataques externos o vamos a dejar nuestra información expuesta al primero que pase?

¿Podríamos, en este caso de conexión gratuita, implementar los escenarios que hemos visto en entregas anteriores de Voz IP o Vigilancia IP? Con toda seguridad ya les digo que NO será posible.

Rechacen las conexiones gratuitas, sobre todo si no les garantizan toda las seguridad que les he citado.

¿Y cual es la mejor opción?

Esta es una decisión importante para el club. Vamos a analizar todos los escenarios posibles:

OPCION A: Conexión Gratuita.

Es la opción que se encontrará el usuario con lo que hemos hablado hasta ahora. Es la peor opción, pero veamos como tiene que implementarla el puerto. Para ponerla en marcha basta con instalar una línea ADSL y conectarle un punto de acceso WiFi abierto a todo el mundo. La forma más abierta es establecer un nombre de SSID a la red y asignar a las conexiones una IP dinámica a través de DHCP, de forma que los usuarios no deberán hacer nada más que encontrar nuestra red inalámbrica y conectarse sin ningún dato adicional.

OPCION B: Conexión Gratuita pero con seguridad.

Esta opción es la que va destinada a aquellos puertos que quieran ofrecer un servicio de calidad gratuito.

En este caso deberán instalar un buen punto de acceso, con cobertura en todos los puntos del puerto.

Como seguridad, recomiendo estas acciones:

- Deshabilitar el broadcast del SSID. Se trata de esconder la propagación de su nombre. Cuando los usuarios busquen redes inalámbricas, esta conexión no saldrá. Para podernos conectar deberemos pedir los datos a Capitanía y establecer la conexión manualmente.
- Instalar un DHCP falso en el punto de acceso y asignar a cada usuario una dirección IP personal. De esta forma los usuarios que se conecten a al red y no hayan pasado por capitanía se encontrarán que se conectan a la red, pero no pueden hacer nada ya que los datos recibidos no son correctos. Existen puntos de acceso WiFi que obligan a asociar una dirección IP a una determinada dirección MAC. Esta sería la mejor opción.
- Establecer un código de encriptación WEP, de 64 ó 128 bits, de forma que los interesados en la conexión deban solicitarlo en capitanía. Esta clave WEP debería cambiarse con periodicidad, y notificarlo vía mail a los usuarios conectados.
- Bloquear los programas P2P. Para esto hace falta un Firewall avanzado, y la ayuda de un buen informático, pero es sin duda algo imprescindible si queremos dar buen servicio.
- Establecer una reserva máxima de caudal por usuario. Podríamos asignar un máximo de 128Kb por usuario, de forma que limitemos a nuestro vecino el uso excesivo que hace del caudal y tengamos

garantizado unos “carriles de la autopista” para nosotros. De esta forma garantizamos un mínimo de calidad para cada conexión.

Vemos que significan los tecnicismos que hemos ido viendo (SSID, DHCP, MAC …).

Una red P2P es una red de igual a igual (en inglés “peer-to-peer”, que se traduciría de par a par- o de punto a punto) Es una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red. Las redes de ordenadores Peer-to-peer (o "P2P") son redes que aprovechan del uso de banda ancha de cada uno de los usuarios que se conectan a su red.
Dichas redes, se usan para muchas aplicaciones, pero son realmente conocidas por usarse para peliculas, música y todo tipo de archivos. Tienen la capacidad de hacerse con todo el caudal de internet que “pillan” por el camino.

El SSID (Service Set IDentifier) es el nombre que se le asigna al dispositivo Wifi llamado Punto de Acceso que dará señal a los usuarios de su red. Se establece un nombre identificativo (SSID) para ayudar a los usuarios a identificar la red a la que se van a conectar.

Como consejo de seguridad, el SSID puede esconderse y no propagarse por la red, de forma que para saber cual es la red debamos solicitarlo en Capitanía y establecer la conexión a mano .Es una de las formas más sencillas de proteger la red inalámbrica.

DHCP (Dynamic Host Control Protocol) es un protocolo de red que permite a los usuarios de una red obtener los datos de la red en el momento de establecer la conexión. Para ello hace falta que en la red exista un servidor DHCP que haga esta función. Habitualmente los Puntos de Acceso WiFi tienen esta función.

Otro consejo se seguridad es no proveer de este servidor en la red, ya que facilitamos un dato primordial para una conexión de red. En algunos casos incluso recomiendo establecer el servidor DHCP entregando información errónea, e decir, datos IP que no pertenecen a nuestra red y que despintaran totalmente al usuario conectado.

Dirección MAC *(Media Access Control address) es la matrícula que tiene cada dispositivo de red. Es la* dirección de control de acceso al medio. Consiste en un identificador hexadecimal de 48 bits que se otorga a cada dispositivo de red cuando sale de fábrica, controlado por una norma internacional que asigna a cada fabricante un rango de direcciones.

Esta matrícula es la que nos puede permitir identificar al usuario conectado, o más que al usuario, al equipo que se conecta.

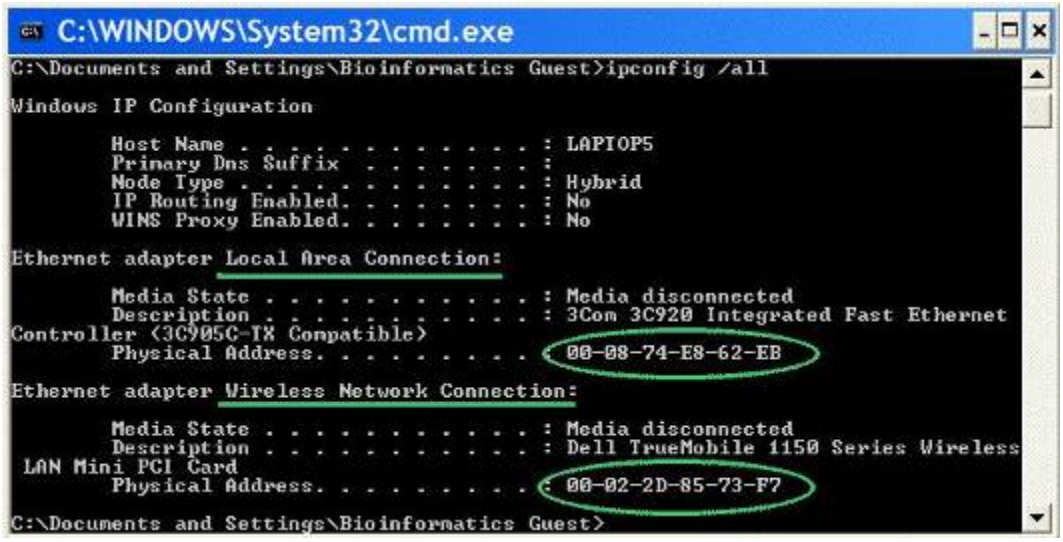
Una forma adicional de aumentar la seguridad es establecer una lista de dispositivos autorizados, de forma que los que no es ten en la lista del Punto de Acceso no podrán acceder a la red inalámbrica.

¿Cómo averiguamos nuestra dirección MAC?

Si se trata de un dispositivo externos (USB o PCMCIA, por ejemplo), basta con ver su parte posterior. Veremos con toda seguridad una etqiueta con la "matrícula" Hexadecimal".

Si se trata de un dispositivo interno, podemos averiguarlo desde el interprete de comandos. Para ello debemos seguir los siguientes pasos:

1. Situarse en MSDOS: Inicio – Ejecutar- CMD
2. Escribir IPCONFIG ALL y darle al INTRO
3. Tomar nota de los datos que vemos por pantalla, anotando la MAC ADDRESS del dispositivo que nos interesa. Hay que tener en cuenta que si el equipo tiene una tarjeta de red normal y otra inalámbrica, cada dispositivo tiene su propia matrícula. Es importante, cuando demos dicha matrícula al informativo del puerto, en caso de disponer de seguridad por MAC, que no le demos la "matrícula" de otra tarjeta de red.



WEP (Wired Equivalent Privacy) es el sistema de encriptación para la información que viaja a través del WiFi. Utiliza claves de 64 o de 128 bit. Aumenta considerablemente el tamaño de los paquetes de información que circulan por lo que ralentiza el trafico de la red, pero es la mejor opción combinada por la autorización de listas de MAC.

OPCION C. Escenario óptimo. Dos conexiones. Conexión de pago y conexión gratuita con seguridad.

En esta opción mezclamos los anteriores escenarios A y B. Necesitamos dos líneas ADSL. La primera es la más básica y va conectada directamente a un punto de acceso básico. Es una conexión gratuita sin control alguno para todos aquellos que quieran conectarse. Podemos dar una clave Wep gratuita en Capitanía para que no se nos conecten usuarios de fuera del puerto.
La segunda ADSL debe ser de más capacidad, conectado a un buen punto de acceso con servicios de seguridad, clave WEP, separación de usuarios, protección Firewall, protección P2P, reserva de caudal por usuario, acceso por lista de MAC ADDRESS y asociación de IP por MAC.
Los usuarios que necesiten conectarse para "jugar", sin calidad ni seguridad, pueden tener suficiente con la línea gratuita. Y aquellos usuarios que necesiten calidad y seguridad en su conexión para poder conectarse a sus sistemas de trabajo, sistemas de vigilancia IP o Telefonía IP, por ejemplo, se abonarán al servicio "Premium" de pago.

En la próxima entrega configurarnos este último escenario "C" con detalle, de forma que nuestro puerto no tenga excusa para ofrecernos el mejor servicio. Si nos dice que no puede ofrecernos dicho servicio, le llevamos un ejemplar de de esta revista y ya no tendrán excusa.

José María Serra Cabrera
Capitán de Yate
Licenciado en Informática
Gerente DEINFO Servicios Informáticos.