Redes Inalámbricas en la Universidad Simón Bolívar:
Posición de la DST
Director de Servicios Telemáticos
9 de noviembre de 2005

Antecedentes

La tecnología de conexión a redes locales por medios inalámbricos (conocida como *WiFi*) está experimentando un auge, en gran parte por una combinación de costos bajos, reducción o eliminación de la necesidad de hacer obras civiles o tender cables, y portabilidad de las computadoras, con la consecuente mayor autonomía para el usuario. Ante el aumento en solicitudes de instalación de esta tecnología que están llegando a la DST, se hace necesario definir una posición clara al respecto.

Consideraciones Tecnológicas

Hay varias tecnologías agrupadas bajo el término WiFi, y no es el propósito de este documento profundizar en sus diferencias, excepto notar que han pasado por varias generaciones de distintos niveles de desempeño y costo, y que no son todas compatibles entre sí. Lo que tienen en común es que están basadas en comunicación por radio de alta frecuencia y relativamente baja potencia. La alta frecuencia permite una tasa de transmisión teórica que es comparable con las redes locales (pero véase más abajo), y la baja potencia implica que el alcance es relativamente corto, lo cual reduce la interferencia entre estaciones, aunque no la elimina. La banda de frecuencias usada es una que se ha designado como “libre de licencias”, lo que quiere decir que el usuario no requiere permisología de las autoridades competentes como sería el caso de una radiotransmisora normal.

Aunque los equipos terminales (PCs, laptops, PDAs, etc.) pueden intercomunicarse directamente, generalmente se asume que grupos de ellos lo hacen a través de una *estación base*, y que ésta a su vez tiene una conexión por cable al resto de la infraestructura de red corporativa. En algunos casos, las estaciones base también pueden conectarse entre sí por radio.

La tecnología WiFi tiene varias implicaciones tanto positivas como negativas. Las positivas ya se mencionaron anteriormente. Las negativas son de varios tipos:

- Si bien la tasa de transmisión física puede ser de varios Mbps (megabits por segundo) – típicamente 11Mbps o 54Mbps en las versiones más comúnes – hay varios factores que conspiran en contra de un ancho de banda efectivo en estos niveles:
    - Distancia entre el equipo y la base y la consecuente atenuación de la señal. El máximo rango anunciado por los fabricantes (típicamente 45 metros)raras veces se obtiene en la práctica.
    - Interferencia de objetos (edificios, árboles, muebles, ...) en el camino entre el equipo y la base, resultando en reflejos (señales multicamino), reducción de potencia y hasta bloqueo total.
    - nterferencia de otros equipos que operan en la misma banda “libre de licencias”, incluyendo teléfonos inalámbricos, hornos de microondas, etc.
    - Efectos de congestión producidos por una sobredemanda del espectro en el vecindario, generalmente porque demasiados equipos intentan comunicarse con la misma base, o porque varias bases cercanas solapan señales entre sí. La capacidad total se comparte entre los equipos activos, pero no en forma lineal. Por ejemplo si dos PCs intentan transmitir archivos a través de la misma base al mismo tiempo, cada uno recibirá menos de la mitad del ancho de banda teóricamente disponible.

- La transmisión por radio es por su naturaleza vulnerable a dos clases de ataque:
    - *Pasivo*: un intruso puede monitorear las transmisiones con un equipo de relativamente bajo costo, sin ser detectado.Se hace necesario utilizar medidas de seguridad criptográfica para evitar la fuga de información confidencial (por ejemplo, la contraseña de un usuario). Aunque hay prácticas bien establecidas para permitir la comunicación privada, estas requieren conocimiento, concientización de los usuarios y administración experta para que sean efectivas. (Es por estas razones que la mayoría de las redes WiFi instaladas actualmente no tienen protección alguna.)
    - *Activo*: un intruso inescrupuloso puede intentar inyectar datos en una comunicación. Una buena infraestructura de seguridad criptográfica puede eliminar este problema. Sin embargo, potencialmente mucho más grave es que un adversario puede bloquear la comunicación totalmente, transmitiendo ruido electrónico en la banda usada. Es imposible protegerse del todo contra esto, y en general es impráctico detectar al responsable después del hecho cumplido.

Es de notar que estas clases de ataque son factibles con las redes tradicionales también. La diferencia en el caso de las redes WiFi es que es mucho más dificil detectar al responsable durante y después de un incidente (podría estar sentado en un automóvil en el estacionamiento, o caminando por el pasillo).

- Otra consecuencia de la naturaleza física de WiFi es que si no se toman medidas en contra, el acceso a la red corporativa queda expuesta a personas que no necesariamente tengan derecho a tenerlo (visitantes, personas en las zonas aledañas al campus, etc.). Esto produce múltiples complicaciones, entre ellas el uso inapropiado de nuestra ancho de banda de Internet y el aumento en riesgo de ataques informáticos a nuestra infraestructura, dado que el tráfico de los equipos en cuestión no tendrían que pasar por el *firewall* de USBnet. Si bién parte de este peligro ya está presente (por ejemplo, cada vez que alguien trae un laptop desde afuera y lo conecta a la red), las redes inalámbricas sin duda aumentarían la frecuencia de estos eventos y en consecuencia el grado de molestias causadas a la comunidad. Para paliar esta situación sería necesario diseñar, establecer y administrar un mecanismo de control de acceso. Dada la estructura actual de USBnet, y frente a la escasez crónica de personal calificado, la DST no está en condiciones para asumir esta responsabilidad a corto plazo.
- La presencia de múltiples estaciones base en una misma zona, todas bajo el control de personas o unidades distintas, invita a problemas de configuración y consistencia en acceso a la red, y potencialmente puede producir el colapso del servicio localmente. Es dificil estimar el riesgo real de esta situación porque no tenemos la debida experiencia, pero sería prudente proceder con cautela.

Alternativas

Las siguientes son las opciones que tiene la DST en cuanto a las redes WiFi en la USB:

1.Prohibirlas, porque pueden tener problemas y no contamos con suficientes recursos humanos para dar el soporte adecuado. *Objección*: ya existen algunas instalaciones (no soportadas) y en la práctica puede ser difícil o imposible hacer valer una prohibición de este tipo.

2. Asumir el problema como nuestro y estandarizar en una tecnología, la cual sería soportada completamente por la DST. *Objección*: aparte de la insuficiencia de recursos humanos ya mencionada, el proceso de avance tecnológico no se ha detenido. Por ejemplo, en el horizonte hay una nueva generación llamada *WiMax*, que no está soportada por casi ninguno de los proveedores actuales y que tampoco es compatible con la generación actual de equipos. Sin embargo, *WiMax* puede ofrecer ventajas importantes a futuro en el contexto de una red de campus. Otra alternativa en desarrollo muy activo es el concepto de *mesh networks*, que buscan interconectar múltiples bases inalámbricas para dar cobertura económicamente a una área extendida. Frente a esta situación, una inversión grande de esfuerzo y dinero en la generación actual de WiFi podría resultar en pérdidas si el panorama tecnológico cambia a corto plazo (lo cual es bastante probable).

3. Ni soportar ni prohibir la instalación y uso de WiFi, en otras palabras dejar el problema al usuario. *Objección*: aunque esto es factible a corto plazo, es muy probable que no sea una política práctica a largo

plazo. Si el número de instalaciones WiFi crece sustancialmente, la comunidad reclamará el soporte Institucional y habrá que re-evaluar la posición.

Conclusiones

En las condiciones actuales en las que se encuentra la DST, la única alternativa viable es la tercera, pero ésta debe mantenerse bajo revisión permanente. Por las razones expuestas, se define la siguiente política hasta nuevo aviso:

1. *La DST no dará soporte para redes inalámbricas, con excepción de las que pueda requerir para sus propios fines (por ejemplo, para conectar lugares remotos o de poco uso a la red USBnet).*
2. *Las unidades o personas que adquieran tecnología inalámbrica lo hacen bajo su propia cuenta y riesgo. Si se tramita dicha adquisición a través de los procesos de compra de la DST, el solicitante de la adquisición deberá firmar una declaración que explícitamente libera a la DST de la responsabilidad de soporte. En particular, no se garantiza compatibilidad "hacia adelante" con ninguna tecnología inalámbrica que pudiese tener soporte de la DST en el futuro.*
3. *Como unidad designada por el Consejo Directivo para la administración y custodia de la red universitaria, la DST reserva su potestad reglamentaria de bloquear el acceso a USBnet a las bases inalámbricas cuando determine que están causando problemas para el resto de la red, de la misma manera que en ocasiones hace con otros equipos.*