Política de Instalación de Puntos de Acceso Inalámbricos de la Universidad Carlos III de Madrid

Introducción

De todas las tecnologías de acceso a red local, la inalámbrica (Wireless LAN) es, probablemente, la que más ha llamado la atención a los usuarios de servicios de telecomunicaciones.

El motor de su éxito, además de en los beneficios de la conectividad sin cables ó el abaratamiento de los dispositivos móviles, está en la firme apuesta de los fabricantes por garantizar la compatibilidad de los productos Wireless. Con esta finalidad, en 1999 se creó la WiFi Alliance[5], - *WiFi, Wireless Fidelity*- asociación internacional sin ánimo de lucro cuyo objetivo es certificar la interoperabilidad de los productos de Red de Área Local basados en la especificación IEEE 802.11[4].

El Servicio de Informática y Comunicaciones (SdIC), está trabajando para desplegar de forma progresiva cobertura inalámbrica en distintas zonas de la universidad. Este servicio debe coexistir con aquellos implantados por los usuarios y/o departamentos, por ello es necesario contar con una normativa que establezca las condiciones en las que un usuario o departamento concreto puede implantar o mantener un Punto de Acceso inalámbrico, de modo que no perjudique al resto de usuarios o departamentos.

Limitaciones de la tecnología

La tecnología de redes inalámbricas utiliza un conjunto de frecuencias del espectro radio-eléctrico reservado para uso libre, por lo que cualquier equipo o dispositivo puede utilizar dichas frecuencias libremente, pudiendo provocar interferencias con el resto de sistemas que utilizan esta tecnología.

Como consecuencia de ello, la potencia de emisión y la dimensión de la zona de cobertura de un Punto de Acceso deben ser limitadas, y la asignación de las frecuencias de emisión, o canales, debe hacerse de forma controlada. Además, debido al número limitado de canales disponibles, no deben coexistir más de tres Puntos de Acceso en una misma zona.

Las interferencias provocadas por los equipos que transmiten en el conjunto de frecuencias que emplean las redes inalámbricas tienen diferentes efectos, en función de la intensidad y duración de dichas interferencias, y van desde la degradación del servicio, siendo necesario ajustar la velocidad de transmisión, hasta la imposibilidad de establecer conexión.

Fundamentación de la propuesta

El Reglamento del Servicio de Informática[1] establece:

- Artículo 7: El Sistema General Informático de la Universidad:

"... Corresponde al Servicio de Informática de la Universidad la planificación, organización y mantenimiento de los sistemas, dispositivos, medios y soportes integrados en el Sistema General de Informática de la Universidad. Los sistemas informáticos no integrados en el Sistema General de Informática, podrán acceder a los servicios de la red en las condiciones que se indiquen en los correspondientes reglamentos técnicos."

- Artículo 8: Funciones del Servicio de Informática en materia de comunicaciones:

"El Servicio de Informática de la Universidad es responsable de la organización y funcionamiento de las comunicaciones informáticas en el seno de la Universidad, así como de las de ésta con terceros.

Corresponde al Servicio de Informática de la Universidad la supervisión y verificación de las redes y los dispositivos de comunicación de la Universidad, con especial atención a la compatibilidad de equipos y condiciones de seguridad de las instalaciones, así como el cumplimiento de la normativa técnica sobre homologaciones de los equipos que en cada caso sea aplicable.
A tal efecto se establecerán normas reguladoras de los servicios de comunicación informática en el seno de la Universidad y de ésta con terceros. Dichas normas deberán referirse en todo caso a: a) la definición del servicio o servicios, b) el nivel de prestación, c) los derechos y deberes de los usuarios, d) las garantías técnicas y jurídicas del servicio. Las normas generales de la Universidad o de los distintos servicios de telecomunicación podrán condicionar el acceso a prestaciones de la red en función de los niveles de compatibilidad y seguridad que se establezcan."
De lo que se deduce que el SdIC tiene las siguientes obligaciones:

- Establecer la reglamentación técnica para la conexión de sistemas a la red de la Universidad.
- Supervisar y verificar las redes y dispositivos de comunicación de la universidad, estableciendo normas reguladoras.

Ámbito de aplicación

La siguiente normativa debe aplicarse a todos aquellos equipos de comunicaciones que puedan actuar como Puntos de Acceso inalámbricos que se implanten en dependencias de la Universidad Carlos III de Madrid, estos incluyen, pero no se limitan a:

- Puntos de Acceso dedicados.
- Ordenadores dotados de tarjeta inalámbrica, que puedan ser configurados para actuar como Punto de Acceso.

Definiciones

Bluetooth: Estándar de comunicaciones inalámbricas que emplea el mismo rango de frecuencias que Wi-Fi y por lo tanto puede generar interferencias con los equipos de transmisión Wi-Fi.

Canal: En Wi-Fi, rango de frecuencias empleado por los nodos de una red inalámbrica para comunicarse.

Dirección MAC o de enlace: Identificador compuesto por 6 números, asociado a las tarjetas de conexión a la red.

ESSID: Identificador de red inalámbrica, empleado por todos aquellos equipos que pertenecen a una misma red inalámbrica.

Interferencia: Efecto producido cuando dos equipos transmiten simultáneamente empleando el mismo canal de comunicaciones.

Potencia de emisión: Parámetro de emisión de un Punto de Acceso, que determina el área de cobertura de dicho Punto de Acceso, y por lo tanto el área en la que el Punto de Acceso puede crear interferencias.

Punto de Acceso: Equipo de comunicaciones de una red inalámbrica que permite el acceso a la red cableada a los ordenadores dotados de tarjeta inalámbrica.

Red Privada Virtual: Técnica que permite, manteniendo la conexión con nuestro proveedor habitual, acceder a los servicios de la red como si el ordenador se encontrase conectado a otra red, por ejemplo la red de la universidad. En determinadas configuraciones, incorpora cifrado de la conexión.

Warchalking: Acción de realizar marcas en las superficies exteriores (paredes, aceras, edificios, etc) para indicar la existencia de Puntos de Acceso abiertos, de modo que pueden ser empleados por terceros.

WEP: Protocolo de seguridad implementado en las tarjetas y Puntos de Acceso Wi-Fi que cifra la información que se envía a través de las ondas de radio. Debido a debilidades en su diseño, su utilización no garantiza la confidencialidad de las comunicaciones.

Wi-Fi: Término empleado para referirse a los estándares de comunicaciones inalámbricas 802.11.

Despliegue de la red inalámbrica por el SdIC

Para un correcto funcionamiento del servicio de acceso inalámbrico proporcionado por el SdIC, se asignan al SdIC las siguientes atribuciones:

- Prestación del servicio de conectividad inalámbrica en espacios comunes (biblioteca, auditorio, aulas, etc.), con las medidas de seguridad que la tecnología permita en cada momento.
- Asignación de los parámetros de configuración de los Puntos de Acceso para evitar interferencias con los Puntos de Acceso instalados por usuarios y/o departamentos. Además, se ha reservado el valor de algunos parámetros de configuración, entre los que inicialmente se incluye:
- Identificador de red inalámbrica o ESSID, con valor "WiFi-UC3M"
- Mantenimiento de un registro de los Puntos de Acceso instalados, reservándose el derecho a solicitar la realización de cambios en los parámetros de configuración al administrador del Punto de Acceso.
- Elaboración de una guía con los requisitos mínimos que debe cumplir un Punto de Acceso inalámbrico conectado a la red de la Universidad, para evitar problemas de seguridad. Esta guía se actualizará en función de la evolución de la tecnología.
- Desconexión de la red corporativa a aquellos Puntos de Acceso que no cumplan las especificaciones indicadas por el SdIC o que supongan una amenaza grave a la seguridad de la red corporativa.
- El SdIC en caso de detectar algún Punto de Acceso instalado por usuarios y/o departamentos que provoque interferencias radio-eléctricas con los Puntos de Acceso de la red "WiFi-UC3M" comunicará al Vicerrector de Infraestructuras Académicas la zona en la que se produce la interferencia para que a su vez lo ponga en conocimiento del departamento en el que se encuentra el Punto de Acceso y procedan a bajar la potencia de emisión, cambiar el canal o si se diera el caso de que todos los canales se encontrasen ocupados por la red WiFi-UC3M, eliminar el Punto de Acceso.

Registro de Puntos de Acceso

Los usuarios o departamentos que deseen instalar Puntos de Acceso deberán facilitar al SdIC la siguiente información:

- Referentes al Punto de Acceso
    - Dependencia en la que se instalará el Punto de Acceso.
    - Zonas de cobertura y potencia de emisión estimada.
    - Marca, modelo y capacidades de seguridad del Punto de Acceso.
    - Dirección MAC del Punto de Acceso.
    - Segmento de red y roseta a los que se conectará el Punto de Acceso.
    - ESSID del Punto de Acceso.
- Referentes al Administrador del Punto de Acceso:
    - Nombre y Apellidos
    - Despacho
    - Teléfono de contacto
    - Dirección de correo

Tras recibir la solicitud, el SdIC, estudiará la viabilidad de la instalación del Punto de Acceso y comunicará el resultado al Administrador del Punto de Acceso. En caso afirmativo, facilitará al Administrador del Punto de Acceso los parámetros de configuración, el canal y la potencia de emisión que debe asignarse al Punto de Acceso.

Debilidades de la tecnología inalámbrica

La diferencia entre las redes de cable y las inalámbricas estriba en que en estas últimas no es necesario tener una roseta de conexión para tener acceso y por lo tanto no es necesario acceder a una dependencia para poder emplear el Punto de Acceso. A día de hoy, se están extendiendo prácticas como warchalking [2], que consiste en dibujar en vallas, paredes o aceras, signos que indican la presencia de Puntos de Acceso con referencia a si emplean WEP o no. Además, la tecnología inalámbrica es en estos momentos bastante insegura, de hecho algunos fabricantes han publicado dossiers[3] con información sobre los ataques y las posibles soluciones a algunos de estos ataques (determinados ataques, sobre todo aquellos basados en negación de servicio no tienen solución, debido al diseño del protocolo). Prueba de esta inseguridad está en el número de aplicaciones y herramientas disponibles para vulnerar las medidas de protección[9].

Descripción de las medidas de seguridad del servicio de conexión inalámbrica prestado por el SdIC

Se han propuesto varias soluciones que permiten solventar la mayoría de los problemas de seguridad. El SdIC ha optado para utilización de redes privadas virtuales cifradas, tal y como sugiere Wi-Fi Alliance[6] y algunos fabricantes[7]. Esta solución permite emplear técnicas de cifrado robustas, sin necesidad de emplear WEP, lo que garantiza que cualquier tarjeta Wi-Fi puede ser empleada. Además, se encuentra en explotación para sistemas Windows y Linux[8].

Nota importante:

Con posterioridad a su aprobación en el Consejo Informático, se ha migrado a la tecnología 802.1X, empleada en la red *eduroam*. Puede ampliarse la información aquí.

Requisitos de seguridad de los Puntos de Acceso conectados a la red de la Universidad

Debido a los problemas de seguridad que plantea la implantación de Puntos de Acceso, es recomendable la utilización del servicio prestado por SdIC, y en caso de que un usuario o departamento necesite implantar un Punto de Acceso inalámbrico, deben cumplirse los siguientes requisitos:

- El Punto de Acceso debe:
  - Mantener registro de las direcciones MAC de los equipos que lo utilicen, indicando los períodos de utilización.
  - Control de acceso por dirección MAC o usuario.

- Cifrado de la conexión. Este aspecto puede cubrirse mediante:
  - Utilización de la red privada virtual (VPN) que presta el SdIC. Esta es la opción recomendable y la única que garantiza la confidencialidad de los datos transmitidos a través de la red inalámbrica.
  - Utilización de cifrado WEP con claves de 128 bits. Opción alternativa, no recomendada, ya que no garantiza la confidencialidad de las comunicaciones.

Referencias

[1] Reglamento del Servicio de Informática, http://www.uc3m.es/uc3m/gral/IG/NOR/norm502.html, 17 de junio de 1.997.
[2] http://www.warchalking.org
[3] http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf
[4] http://standards.ieee.org/getieee802/download/802.11-1999.pdf
[5] http://www.wi-fi.com
[6] http://www.wi-fi.com/OpenSection/secure.asp?TID=2#vpn
[7] http://www.cisco.com/warp/public/759/ipj_5-3/ipj_5-3_wireless_security.html
[8] https://asyc.uc3m.es/index.php?Id=48
[9] http://downloads.wireless-kit.com/