



DSP 2000



Suministradora de Componentes Electrónicos

Casos de éxito

La unión hace la fuerza y esto queda demostrado en el siguiente caso de éxito, que ha sido llevado a cabo entre las tiendas NCS de Majadahonda y NCS Villaviciosa de Odón. Un ejemplo de que cualquiera de nosotros puede acceder a cualquier tipo de cliente por grande que este sea. Vosotros ponéis el cliente, NCS pone su experiencia y recursos y entre todos lo sacaremos adelante.

Escenario

Edificio del Aula de Música de la Universidad de Alcalá de Henares. Consta de una red local LAN con menos de 10 ordenadores y un servidor.

Composición del armario de datos:

ROUTER estándar de la compañía TELEFONICA con la red Wireless activada sin cifrar (se procede a cifrarlo por seguridad ante intrusiones) y switch no gestionable básico con conexiones bifurcadas en los cables UTP.

Objetivo

El objeto del proyecto es dotar de cobertura inalámbrica a las estancias tales como aulas, auditorio y zonas de oficina y proporcionarles salida a Internet. Ambas redes estarán separadas. En el caso de la oficina de administración se desarrollará una red LAN que estará totalmente separada de la red Wireless del resto del edificio.

También habrá una red Wireless dentro de la LAN para el uso de la oficina, por supuesto separada de la red Wireless pública. La red LAN podrá usar los servicios que desee a la hora de configurar el cortafuegos, tales como FTP, correo entrante y saliente, Web, etc, y la red pública sólo podrá tener acceso a los servicios básicos de Internet, tales como navegar por la Web y poco más. Esto será totalmente configurable.

Tecnología presente

Actualmente la configuración está basada en un único Router muy básico proporcionado por la compañía proveedora de acceso a Internet (ISP) y un Switch también muy básico y limitado en número de conexiones y capacidad de proceso. El hecho de ser un edificio singular y disponer de paredes muy gruesas, hace que sea difícil usar un único punto de acceso para todo el edificio, provocando:

- 1 – Zonas en sombra causadas por el alcance y la ubicación de la única antena.
- 2 – Zonas en sombra causadas por obstáculos arquitectónicos tales como muros y forjados.
- 3 – El acceso WiFi se puede congestionar ante una utilización masiva si fuese accesible por todas las aulas.

Infraestructura

Se estudia la siguiente solución mixta: cable/wireless.

- 1 – Usar los cables UTP ya instalados para llevar la señal a los puntos de acceso AP.
- 2 – Establecer puentes inalámbricos entre APs ante la dificultad de cablear las estancias

Debido a las distancias y a la cantidad de usuarios previsibles, se opta por electrónica profesional y antenas diferentes para cada requerimiento. Se usarán APs con dos antenas. Los que compondrán



esprinet®

Sage Eurowin



Auge OKI®



CONCEPTRONIC®
The Concept of Global Communication

el "bridge" inalámbrico usarán una antena direccional cada uno para establecer el enlace, obteniendo la máxima potencia en un haz de cobertura restringido para concentrar la potencia en el enlace. La otra antena será omnidireccional y se usará para dar cobertura a los diferentes ordenadores que se validen en el AP. También se usará un AP con una antena direccional que cubra el auditorio.

Por último, en la planta baja se colocará un cuarto AP para dar cobertura a la red de la oficina, que también estará cableada.

Networking

El esquema de la red está basado en sistema Switch y Firewall de gama profesional. El Firewall puede contemplar la posibilidad de controlar dos proveedores de datos por si se quiere disponer de mayor ancho de banda o redundancia, ante un acceso masivo para el ancho de banda contratado actualmente. A su vez dispondrá de puertos LAN y puertos DMZ. La zona LAN será la dedicada al tráfico de datos de la oficina, y la zona DMZ será usada para la red Wifi pública, estando totalmente separadas y con criterios de uso totalmente diferentes. También se podrá controlar el ancho de banda utilizable por cada red y por cada servicio, pudiendo incluso balancear la carga de trabajo entre los dos posibles proveedores de datos.

El Switch, que será gestionable, permitirá impedir las conexiones entre los usuarios de la zona DMZ para evitar contaminaciones por virus o cualquier tipo de ataques, para así mantener preservado cada ordenador de la red pública de los demás que estén simultáneamente conectados. Además será capaz de gestionar desahogadamente el tráfico masivo proveniente de las aulas y el auditorio. Cada punto de acceso es capaz de gestionar varias decenas de conexiones, pero el fabricante recomienda no sobrepasar 15 o 20 conexiones simultáneas al mismo AP. Esto se debe tener en cuenta dependiendo del uso futuro en cuanto a acceso simultáneo.

Tanto en el Switch como en el firewall se han configurado dos VLAN (Redes de Area Local Virtuales), de este modo es posible separar físicamente el tráfico del punto de acceso de la administración y la red cableada de la oficina.

De forma que si un ataque Wireless al punto de acceso tuviese éxito, no se vería comprometida la seguridad de la red LAN. Esto significa que se podrá usar la conexión Wifi para navegar con las condiciones de la LAN, pero sin poder acceder a ésta. Así tendríamos dos segmentos de red que serían la DMZ para los accesos públicos y la LAN, que constará de dos VLAN separadas virtualmente por la electrónica de red. Esto es posible gracias a que los elementos de la red, el Firewall, el Switch y los AP soportan la gestión de VLANs.