

Integración Red Wired - Wireless

Memoria.



U.O.C.

15 de junio de 2012

Autor: Francisco Javier García Moreno.

Consultor: Antoní Morell Pérez

Integración Red Wired - Wireless

Memoria.

ÍNDICE

Contenido

ÍNDICE.....	1
ÍNDICE FIGURAS.....	3
ÍNDICE DE TABLAS	4
PRELIMINAR.....	5
DEDICATORIAS	5
1. BUSCANDO LA INTEGRACIÓN	6
1.1 INTRODUCCIÓN.....	6
1.2 JUSTIFICACIÓN Y CONTEXTO DEL PROYECTO.....	7
1.3 OBJETIVOS GENERALES	8
1.4 ENFOQUE UTILIZADO	9
1.5 PLANIFICACIÓN PROPUESTA	9
1.5 COSTE ESTIMADO	10
1.6 PRODUCTO OBTENIDO	11
1.6.1 MOBILIDAD.....	12
1.6.2 SEGURIDAD	14
2. ANALIZANDO LA SITUACIÓN	15
2.1 TECNOLOGÍA DISPONIBLE	15
2.1.1 RED CABLEADA.....	15
2.1.2 RED WIFI.....	16
2.1.3 SERVICIO DE DIRECTORIO	17
2.1.4 SERVIDOR DE RADIUS.....	18
2.1.5 NPS.....	19
2.2 IEEE 802.11X.....	20
2.3 VIRTUAL LAN.....	22
2.4 RESUMEN TECNOLÓGICO.....	22
3. ESTUDIO DE VIABILIDAD.....	24
3.1 RED CABLEADA	24
3.2 RED WIFI	28
3.3 DIRECTORIO ACTIVO.....	30
4. EJECUTANDO EL PROYECTO.....	32
4.1 TRABAJOS PREVIOS	32
4.1.1 ADAPTACIÓN DE VLAN.....	32
4.1.2 ADAPTACIÓN DEL DIRECTORIO ACTIVO	33
4.2 CONFIGURACIÓN DE DIRECTORIO ACTIVO	34
4.2.1 ACCESO A RED ADMINISTRATIVA.....	34
4.2.2 ACCESO A RED DE SALAS PÚBLICAS	36
4.2.3 ACCESO A RED DE INVITADOS.....	36

4.2.4 ACCESO A RED SIN DOMINIO	36
4.3 CONFIGURACIÓN DE ELECTRÓNICA DE RED.....	37
4.3.1 RED CABLEADA	37
4.3.2 RED INALÁMBRICA.....	39
4.4 CONFIGURACIÓN DE RADIUS	42
4.4.1 ARQUITECTURA DE RED.....	42
4.4.2 INSTALACIÓN DEL SERVICIO	43
4.4.3 AUTORIZACIÓN EN EL AD.....	44
4.4.4 CONFIGURACIÓN DE CLIENTES RADIUS.....	45
4.4.5 REDUNDANCIA.	48
4.4.6 CONFIGURACIÓN DE POLÍTICAS.....	49
5. PRESENTANDO RESULTADOS.....	60
5.1 TEST Y VALIDACIÓN	60
5.2 ANÁLISIS TÉCNICO.....	63
6. CONCLUSIONES	66
ANEXO I.....	67
GUÍA DE CONFIGURACIÓN DEL CLIENTE.....	67
GLOSARIO DE SIGLAS Y TÉRMINOS.....	69
BIBLIOGRAFÍA.....	71

ÍNDICE FIGURAS

Ilustración 1 Fenomeno BYOD	6
Ilustración 2 Diagrama de Gantt	10
Ilustración 3 Esquema conceptual.....	11
Ilustración 4 Movilidad en Red cableada	12
Ilustración 5 Movilidad sobre Wifi.....	13
Ilustración 6 Grupos de seguridad Directorio Activo	14
Ilustración 7 Arquitectura de Red.....	15
Ilustración 8 Arquitectura Wifi.....	16
Ilustración 9 Compatibilidad directorio activo.....	17
Ilustración 10 Propiedades de marcado	17
Ilustración 11 Funciones de Radius	18
Ilustración 12 Funcionamiento NPS	19
Ilustración 13 Validación 802.1X	21
Ilustración 14 Ejemplo Vlan	22
Ilustración 15 Resumen de tecnología.....	23
Ilustración 16 Topología de Red	24
Ilustración 17 Electrónica de Red en edificios	25
Ilustración 18 Cisco Feature Navigator	26
Ilustración 19 Autenticación Directorio Activo.....	30
Ilustración 20 AD, Políticas de marcado.....	34
Ilustración 21 Nuevo Grupo AD	35
Ilustración 22 Usuarios MAC	36
Ilustración 23 Proceso EAPoL.....	38
Ilustración 24 Configuración Radius Wifi	40
Ilustración 25 Perfil de seguridad Wifi	40
Ilustración 26 Perfil de ESS Wifi	41
Ilustración 27 Arquitectura de Switch.....	42
Ilustración 28 Roles Servidor	43
Ilustración 29 Registro Servidor	44
Ilustración 30 Proceso de Autenticación	45
Ilustración 31 Plantilla secreto compartido.....	46
Ilustración 32 Radius, configuración cliente	46
Ilustración 33 Comando netsh.....	47
Ilustración 34 Hoja de clientes.....	47
Ilustración 35 Propiedades conexiones Ethernet	50
Ilustración 36 Condiciones, Tipo puerto NAS	50
Ilustración 37 Condiciones, Tipo de túnel	51
Ilustración 38 Configuración, autenticación.....	51
Ilustración 39 Propiedades conexión Wifi	52
Ilustración 40 Condiciones, conexión Wifi.....	52
Ilustración 41 Diagrama de políticas.....	54
Ilustración 42 Directiva vlan50.....	55
Ilustración 43 Grupos directiva vlan50.....	55
Ilustración 44 Permisos directiva vlan50.....	56
Ilustración 45 Atributos directiva vlan50	56

Ilustración 46 Método de autenticación.....	57
Ilustración 47 Elección del certificado	58
Ilustración 48 Evento acceso vlan50	60
Ilustración 49 Evento acceso vlan26	61
Ilustración 50 Evento acceso Wifi.....	62
Ilustración 51 Solicitud de acceso eapol.....	63
Ilustración 52 Respuesta eapol.....	64
Ilustración 53 Estadísticas Radius	64
Ilustración 54 Configuración 802.1X W7	68
Ilustración 55 Configuración EAP W7	68

ÍNDICE DE TABLAS

Tabla 1 Requisitos tecnológicos.	8
Tabla 2 Coste estimado	10
Tabla 3 Perfiles de acceso	32

PRELIMINAR

DEDICATORIAS

Subir a la cima de una montaña no es posible sin la ayuda de un gran equipo, y ninguna celebración es merecida si no la podemos compartir con ellos.

Mi mayor agradecimiento va a mi equipo base: mi mujer y mi hija, que me han acompañado en los buenos y en los malos momentos de mi recorrido, dándome la fuerza que he necesitado en cada momento y ayudándome a creer en mí y en que la cima era alcanzable.

Mención especial también a mis amigos, los cuales siempre han estado presentes para darme ánimos en los malos momentos este ascenso.

A todos ellos les estaré siempre agradecido.



1. BUSCANDO LA INTEGRACIÓN

1.1 INTRODUCCIÓN

Una de las definiciones que encontramos para la palabra **integración** es: “acción y efecto de incorporar algo en un todo”. En nuestro caso, asimilamos “el todo” a nuestro concepto de Red empresarial, y nos centramos en solventar los problemas que nos plantearán **las distintas formas de acceso** a la misma.

Esta palabra, Red, engloba a su vez infinidad de conceptos: segmentación en redes virtuales (las llamadas Vlan), tipos de acceso (p.e mediante cableado estructurado o medios aéreos –Wifi-) o distintos perfiles de usuarios y sus dispositivos. Todo esto hace que el concepto de Red no sea único, ni independiente en cada situación, y que, por lo tanto, genere en muchas ocasiones confusión entre los usuarios y los propios responsables de los departamentos de Tecnologías de la Información (TI). El caso más habitual, hoy en día, se produce cuando un trabajador solicita trabajar con la aplicación empresarial mediante su propio portátil o dispositivo personal... Cubrir esta y otras situaciones es, para el departamento de TI, un gran reto ya que siempre debe adaptar y garantizar los servicios de la Red y adoptar como propios dispositivos ajenos a la empresa, en ocasiones tecnológicamente más avanzados que los que la propia compañía puede ofrecer. Bring Your Own Device (BYOD) es el nombre que define este fenómeno y al que infinidad de compañías están tratando de dar respuesta (*).



ILUSTRACIÓN 1 FENOMENO BYOD

(*) Avande (Noviembre de 2011): (<http://www.avande.com/Documents/Resources/consumerization-of-it-executive-summary.pdf>)

“Globally, 88 percent of executives report employees are using their personal computing technologies for business purposes today.

And, the majority of companies (60 percent) said they are now adapting their IT infrastructure to accommodate employee’s personal devices, rather than restricting employee use of personal devices.”

1.2 JUSTIFICACIÓN Y CONTEXTO DEL PROYECTO.

Nuestro punto de partida será la coexistencia de distintas Redes de acceso, cableada y Wifi, en el entorno de una empresa multidisciplinaria que soporta el acceso, a sus sistemas, de un n° indeterminado de usuarios que, además, deben estar categorizados por distintos niveles de seguridad en ese acceso. Este proyecto cubrirá la integración de ambas redes y, sobre todo, el control de dichos diferentes accesos con políticas aplicables en todos los posibles escenarios.

Como modelo usaremos una Red empresarial, red tipo campus (CAN), que abarca distintos departamentos, centros y edificios. En nuestro caso, una red Hospitalaria que, por su envergadura y diversidad de clientes, cubre este prototipo. La situación de partida será una segmentación a nivel de VLAN, y una configuración de los clientes y equipos, en las distintas redes, realizada de forma manual. Es decir, actualmente, tenemos que configurar, explícitamente, cada punto de red en la VLAN para cada tipo de usuario que se vaya a conectar a ellos. Este modelo de trabajo está implantado en una red cableada; sin embargo, recientemente, se empiezan a incorporar las redes Wifi a la compañía, sobre todo por las peticiones realizadas por nuestros usuarios de Red, los cuales precisan, cada vez, más soluciones de movilidad y, por lo tanto, de conexión sin cables. Añadimos, pues, el factor humano a nuestra estructura de control ya que, el usuario Wifi, debe conocer a qué tipo de Red se conecta y su nombre (SSID) y hacer la conexión, también, de manera manual.

Llegados a este punto el departamento de TI se plantea distintas opciones para facilitar la conexión de estos clientes de red: generar distintos SSID en función de la Red a la que proporcionan acceso, usar cableado de distintos colores en función de la Red a la que conectan el punto de red, etc. Con todos estos planteamientos, el usuario, fácilmente, acaba en una disyuntiva sobre dónde conectarse a la red, cómo y con qué dispositivo; y la empresa, a su vez, ve como la seguridad y la integridad de su Red se ven comprometidas continuamente.

Para solucionar este tipo de situaciones desarrollamos un proyecto que nos permita un acceso a la Red de datos de forma automática, universal, y con un gran nivel de autonomía por parte del departamento de TI.

Para ello, desarrollaremos la implementación práctica del protocolo 802.1X, y su configuración, para construir un sistema que, de forma automática e independientemente del medio de acceso usado, se encargue de situar a los distintos usuarios y equipos en la Red según su perfil de seguridad.

Ejemplos:

- Un usuario externo a la empresa, que precisa conectarse a nuestra red para salir a Internet: Le asignaremos una determinada red de trabajo, distinta a la usada por los usuarios y equipos propios de la empresa.
- Trabajador de la empresa que usa su propio dispositivo (tablet, Smartphone, portátil, etc) para conectarse a la aplicación corporativa. Debido a que la seguridad de su dispositivo (antivirus, actualizaciones de SO, etc) no está en nuestras manos, podemos desear que no comparta la misma Vlan que nuestros equipos empresariales.

Para lograr este objetivo realizamos una recopilación de las tecnologías en las cuales nos podremos apoyar:

TECNOLOGÍA	USO
Directorio Activo	Identificación y control de cuentas.
Radius	Políticas de control de acceso a la Red.
Cortafuegos	Control de las comunicaciones entre redes.
Switches y Puntos de Acceso	Asignación dinámica a VLAN (802.11X)

TABLA 1 REQUISITOS TECNOLÓGICOS.

1.3 OBJETIVOS GENERALES

Los principales objetivos, que perseguimos con una solución de este tipo, son:

- **Mejorar la seguridad:** Cualquier punto de red, o conexión Wifi, accederá a la red que le corresponda, con lo cual el control presencial a las zonas de acceso será menos importante o complementario.
- **Facilitar la conexión del usuario:** Podrá usar cualquier medio de acceso para conectarse, teniendo en cuenta que los servicios de la red los tendrá disponibles en función de sus credenciales y equipo.
- **Libertad de movimiento.** La red estará accesible en cualquier zona, y para cualquier equipo, con el único requisito de disponer de cobertura de red o una roseta de conexión cercana.
- **Minorar los costes de gestión:** ya que el sistema se auto-gestionará en función de las políticas configuradas de forma centralizada.

Debido a las limitaciones de tiempo y extensión de nuestro proyecto, sólo contemplaremos los apartados de configuración y gestión que estén directamente relacionados con el protocolo 802.1X. El resto de componentes, como la instalación y configuración de un servidor de Directorio Activo, configuración básica de la electrónica de red, servidores de certificados digitales, etc, no serán contemplados en este proyecto, aunque en determinados momentos se pueda hacer referencia a distintos aspectos de estos componentes y podamos dar indicaciones básicas de su configuración.

1.4 ENFOQUE UTILIZADO

Actualmente disponemos de una gran variedad de tecnologías y dispositivos capaces de formar parte de un proyecto de este tipo. Por lo tanto, a la hora de evaluar la implantación, nos hemos centrado en realizar un análisis exhaustivo de las opciones más comunes en el mercado y, sobre todo, en el tipo de Red en la que hemos desplegado el producto.

El mayor reto al que nos hemos enfrentado ha sido que, aunque hemos trabajado sobre un protocolo estándar, cada fabricante ha personalizado su forma de trabajar con él, por lo cual todo lo avanzado con unos equipos ha tenido que ser nuevamente investigado para los demás casos. Debido a esta circunstancia, decidimos seguir un análisis secuencial sobre cada pieza del proyecto y, finalmente, realizar una implantación de todas las piezas.

Así, dentro de la metodología usada, hemos ido analizando los siguientes componentes:

- Servicios de directorio.
- Electrónica de red.
 - o Cableada
 - o Wifi
- Radius
 - o Servidor NPS.
- Protocolo 802.1X

1.5 PLANIFICACIÓN PROPUESTA

La planificación que se ha realizado es la siguiente:

Tarea 1.: Análisis previo

Descripción: Realizar un análisis de la situación actual, y de la metodología usada, para la definición de clientes y redes virtuales.

Objetivos: Definir y delimitar los distintos escenarios para poder diseñar las reglas que manejen la asignación de equipos y usuarios a las redes que les correspondan.

Tarea 2.: Búsqueda de información.

Descripción: Recopilar documentación técnica para implementar la solución.

Objetivos: Disponer de manuales y guías que permitan diseñar y parametrizar la solución planteada.

Tarea 3.: Diseño.

Descripción: Definición diseño propuesto.

Objetivos: Realizar el diseño de la solución en el entorno propuesto.

Tarea 4.: Implementación.

Descripción: Construcción de la solución.

Objetivos: Implementar el sistema y realizar la instalación y configuración de los dispositivos mediante las herramientas estándares.

Tarea 5.: Informes.

Descripción: Confeccionar documentación.

Objetivos: Realización de informes, manuales de uso y conclusiones finales.

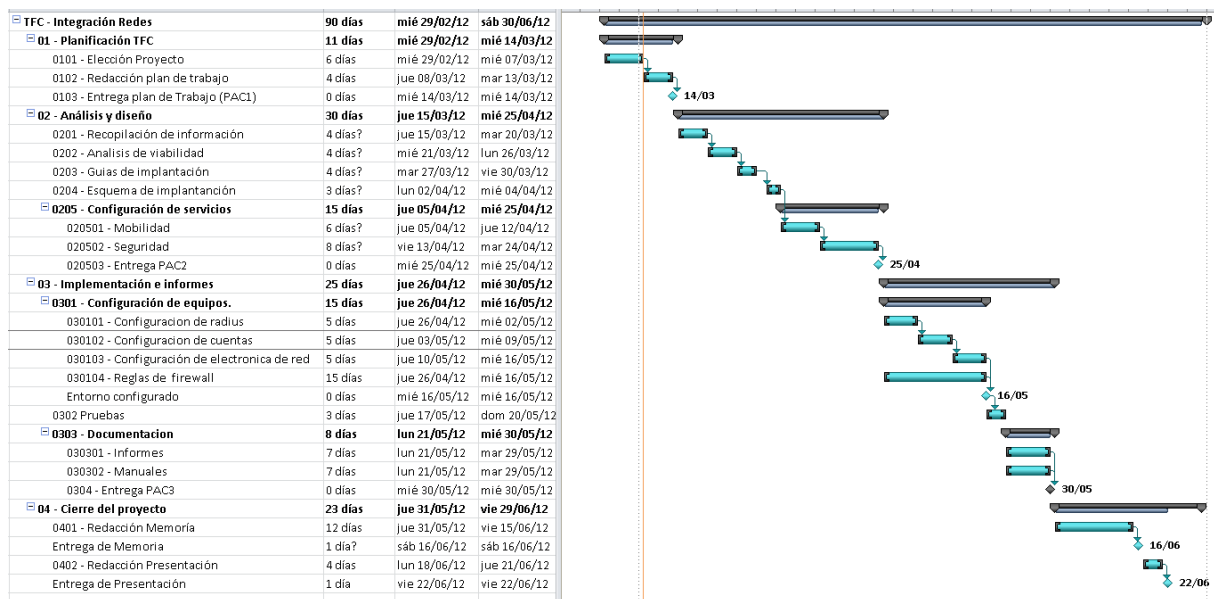


ILUSTRACIÓN 2 DIAGRAMA DE GANTT

1.5 COSTE ESTIMADO

Este proyecto se realiza sobre las bases de la arquitectura y equipos ya disponibles en la compañía. Sobre todo trabajamos la adaptación de los equipos a este nuevo entorno, partiendo de la base de que cumplirán los requisitos necesarios para ello.

Por tanto, los únicos servicios añadidos que habrá que adquirir serán las licencias del servidor Radius y las horas de implantación, que son en realidad la base del proyecto.

Producto	Unidades	Precio/u	Total
Windows Server 2008 OEM	2 licencias	120 €	240 €
Implantación.	240 horas	45 €	10.800 €
			Total: 11.040 €

TABLA 2 COSTE ESTIMADO

1.6 PRODUCTO OBTENIDO

Procedemos a realizar la configuración de todos los elementos que forman parte del proyecto:

- Servidor NPS.
- Directorio Activo.
- Clientes de Radius
 - o Switches.
 - o Controlador Wifi.

El proceso que seguirá el sistema será el siguiente:

- Un cliente de red se conecta a la red mediante un switch o un punto de acceso inalámbrico.
- La solicitud se transmite, desde la electrónica de red, hacia el servicio de NPS mediante 802.1X
- El servicio de NPS revisará el perfil de acceso, en función de las políticas y su correspondencia, con las credenciales en el directorio activo.
- Una vez autorizada la conexión se asigna la Vlan y se le indica a la electrónica de red que realizó la solicitud.
- El usuario es conectado a la red asignada y puede comenzar a usar sus servicios.

Gráficamente lo podemos describir en la siguiente imagen:

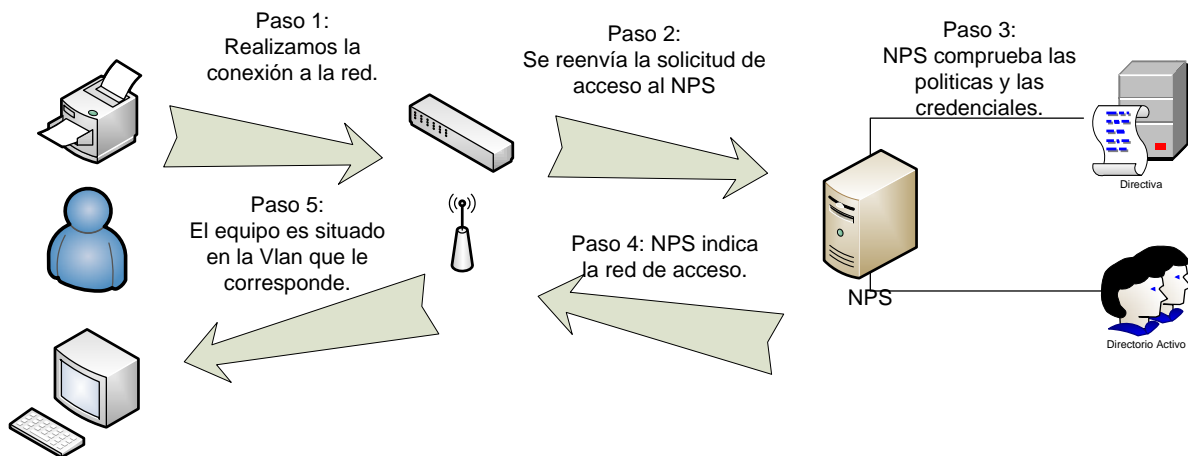


ILUSTRACIÓN 3 ESQUEMA CONCEPTUAL

Como subproductos obtenidos podemos indicar mejoras notables en los aspectos de movilidad y seguridad. Los describimos a continuación:

1.6.1 MOBILIDAD

La movilidad vendrá garantizada en todos los entornos:

En el entorno de **red cableada**, el equipo será validado junto con el usuario. Es decir, el usuario dispondrá siempre de acceso a los servicios de Red, dependiendo del equipo que use.

Por ejemplo, un trabajador de la empresa, que deba acceder a la red de administrativa de la empresa, podrá utilizar cualquier equipo corporativo siempre que se identifique correctamente con el usuario que tenga asignado dentro de la compañía.

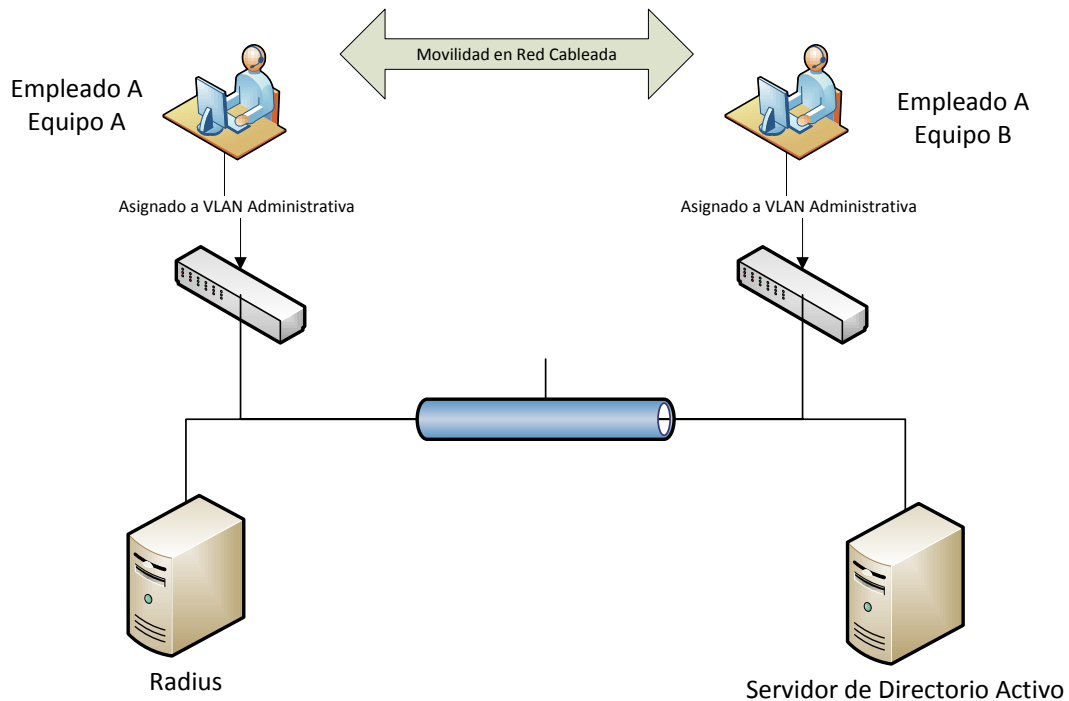


ILUSTRACIÓN 4 MOVILIDAD EN RED CABLEADA

Vemos en la anterior imagen que el usuario ha cambiado de equipo, del equipo A al equipo B y, sin embargo, la asignación de la red se ha mantenido independiente. Esta circunstancia mejora la polivalencia de nuestra red dado que, antes de la implantación de nuestro proyecto, los accesos a la red de administrativa siempre se han asegurado en función de la roseta de red a la que el equipo estaba conectado.

En el entorno **de red Wifi**, la movilidad la garantizará la cobertura de nuestra red y el propio dispositivo usado para la conexión. En este caso, no es habitual el intercambio de máquinas, sin embargo también estaría controlado por nuestro sistema, dado que las políticas de acceso las configuraremos para permitir la integración de ambas redes. Pero **el punto fuerte de nuestro proyecto, en este entorno, es que sólo existe un SSID corporativo**. De esta forma, el equipo no ha de tener distintas configuraciones, dependiendo del uso que le vayamos a dar a nuestra conexión, sino que el uso estará definido en función de nuestro tipo de usuario y la máquina usada.

Vemos un ejemplo de uso en la siguiente imagen:

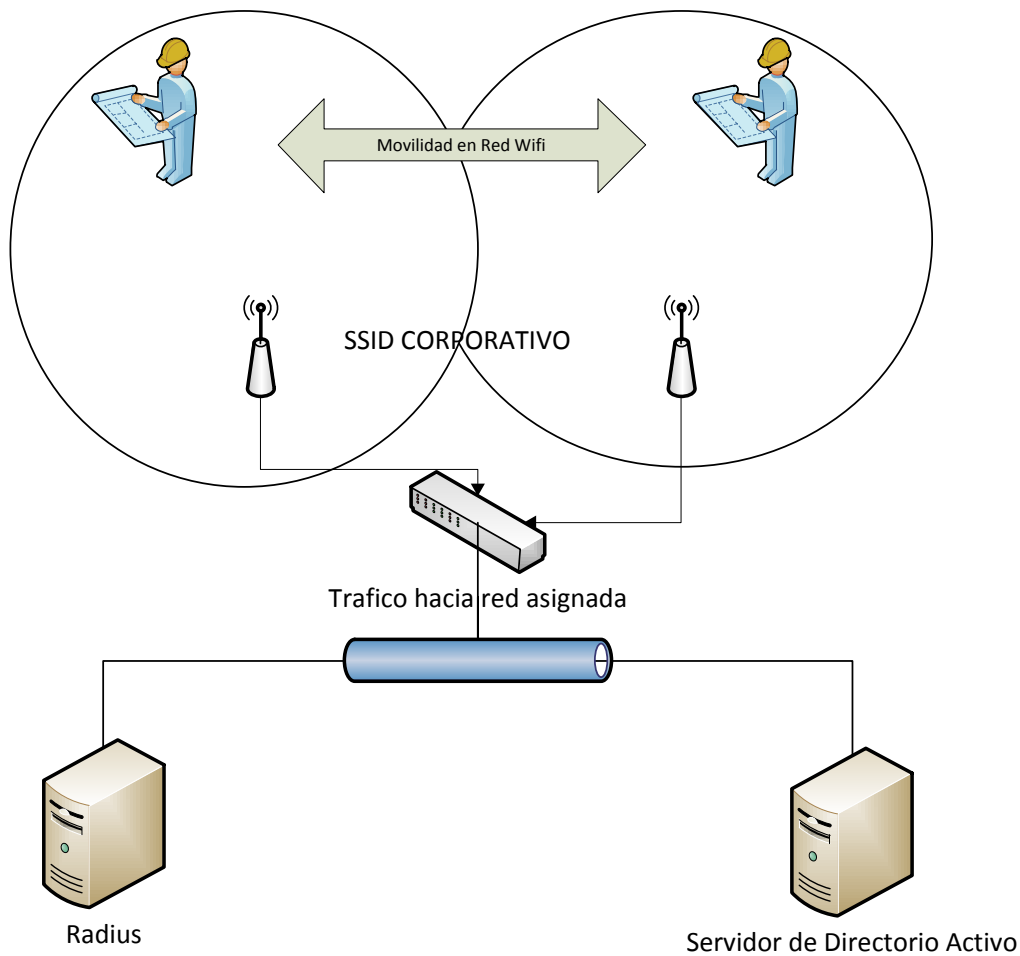


ILUSTRACIÓN 5 MOVILIDAD SOBRE WIFI

En este ejemplo, vemos que el usuario puede usar cualquier punto de acceso (AP) para realizar su conexión. Recordemos que todos los AP están gestionados por el controlador central, y que sólo configuramos un SSID de acceso. El usuario no tendrá que cambiar su configuración en la tarjeta de red, puede definir que la conexión se realice siempre que tenga alcance a la red; en ese momento se le pedirá identificación que, una vez proporcionada y validada, dará acceso a la red permitida por las políticas configuradas.

La movilidad, que aporta el sistema Wifi, se ve mejorada por la simplicidad de configuración de acceso, y la universalidad de este, desde cualquier equipo y zona de cobertura.

1.6.2 SEGURIDAD

La seguridad la diseñaremos desde el punto de vista del control del equipo, del usuario, y de la combinación de ambos. En este sentido delegaremos a la Organización la gestión de estos entes, es decir todo usuario o equipo habrá de ser controlado en algún sentido por la empresa.

Esta fase de control se escapa de nuestro proyecto, pero podemos esbozar una aproximación que sirva de base para el desarrollo de la misma.

Por una parte, todos los equipos corporativos habrán de ser dados de alta en el directorio activo. Para esta operación sólo el personal autorizado tendrá derechos, por lo cual el aprovisionamiento de equipos deberá realizarse centralizadamente, o bien de forma fuertemente regulada.

Por otra, todos los usuarios de acceso deberán ser registrados como mínimo en el directorio activo pero, además tendremos que especificar su rol de usuario. En este sentido sería interesante contar con una tercera aplicación que registre todos los datos de los usuarios y su relación con la organización.

Una vez registrados todos los equipos y usuarios, la asignación de estos a los grupos de seguridad definirá el acceso a las distintas redes. Vemos cómo quedaría la organización de grupos de seguridad en la siguiente imagen:

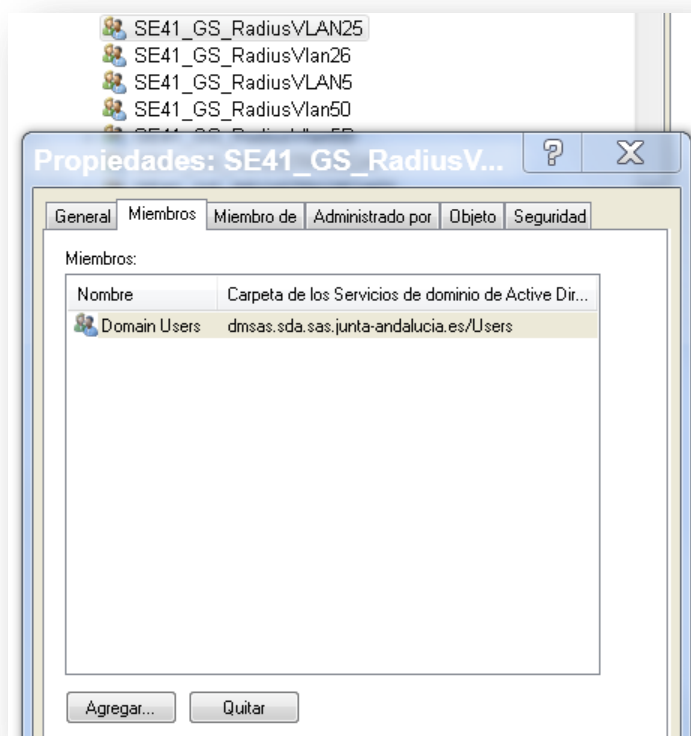


ILUSTRACIÓN 6 GRUPOS DE SEGURIDAD DIRECTORIO ACTIVO

A nivel inter-redes, delegaremos en las funciones existentes del firewall la seguridad avanzada de los equipos a nivel IP. Es decir, una vez dentro de la red virtual nuestro trabajo ha finalizado, y será el firewall quien, a determinadas IP, pueda dar un nivel de seguridad distinto para permitir la comunicación con determinadas redes y puertos de máquinas situadas en otras redes en las que se encuentre el equipo.

2. ANALIZANDO LA SITUACIÓN

2.1 TECNOLOGÍA DISPONIBLE

2.1.1 RED CABLEADA.

Dentro del equipamiento de red cableada, usaremos como base la tecnología disponible de Cisco. Nos basaremos en esta tecnología por la gran cuota de mercado que tiene actualmente, pero sobre todo porque disponen de un intérprete de comandos, llamado CLI, que otros fabricantes también han adaptado en sus equipos. Este último detalle permitirá que se puedan reutilizar los comandos de configuración que realicemos en este proyecto y los podamos escalar a otros entornos.

Dentro de la gama de equipos Cisco, utilizaremos el modelo Cisco Catalyst 2960 diseñado para dar servicio dentro de la gama de acceso (ilustración 7), y que cumple el requisito de ser compatible como cliente de Radius:

“Data Sheet Data Sheet Cisco Catalyst 2960-S and 2960 Series Switches with LAN Base Software”:

“Other Advanced Security Features

Other Advanced Security features include but are not limited to:

- *Private VLANs restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a nonbroadcast multiaccesslike segment.*
- *TACACS+ and **RADIUS** authentication facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.”*

La implementación del protocolo 802.11X la realizamos en la capa de acceso, que tal como vemos en la siguiente imagen, es donde se sitúa la conexión los equipos clientes.

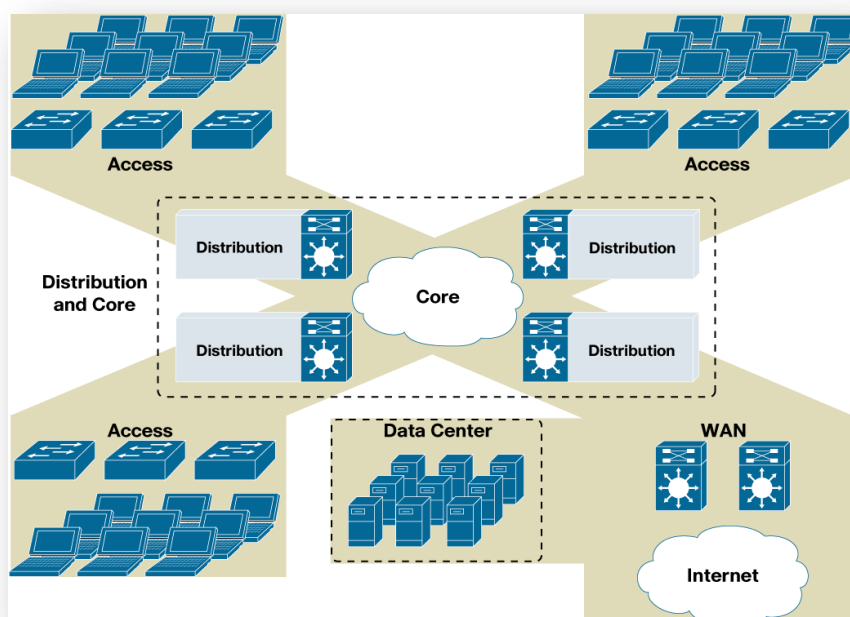


ILUSTRACIÓN 7 ARQUITECTURA DE RED

2.1.2 RED WIFI.

Actualmente, en el mercado tenemos 2 opciones, para planificar nuestra red Wifi, a nivel de cobertura y canales de radio usados. Por una parte el sistema de micro celdas, y por otra el sistema de celda única.

Con el sistema de celda única, se consigue que todos los puntos de acceso trabajen en el mismo canal sin producir interferencias entre ellos, dado que se muestran como un único punto de acceso de cara a los clientes. De esta forma el crecimiento es más rápido, no requiere de costosos estudios de cobertura y ganamos tanto en velocidad de roaming como en el número de usuarios soportado por zonas. Por tanto, nos basamos en esta opción dado que simplificará el despliegue de nuestro proyecto.

El esquema de configuración que hemos elegido, en este proyecto, estará basado en el controlador Meru Network MC4100, o superior, que permite dar soporte hasta 500 puntos de acceso. Dicho controlador se encargará de centralizar toda la configuración y distribuirla hacia todos los AP.

Los puntos de acceso se integrarán en la Red de la siguiente forma. Cuando arrancan buscan un servidor DHCP, dicho servidor les asigna una IP y les indica cuál es su controlador. En ese momento, el controlador le transfiere la configuración, que es almacenada por el AP temporalmente, de forma que en caso de hurto de nuestro equipo la seguridad no se vea comprometida al no tener ninguna información o claves. Dado que sólo se usa un canal de radiofrecuencias, cualquier punto de acceso, en el mismo momento de recibir la configuración, puede comenzar a difundir los SSID configurados y aceptar clientes.

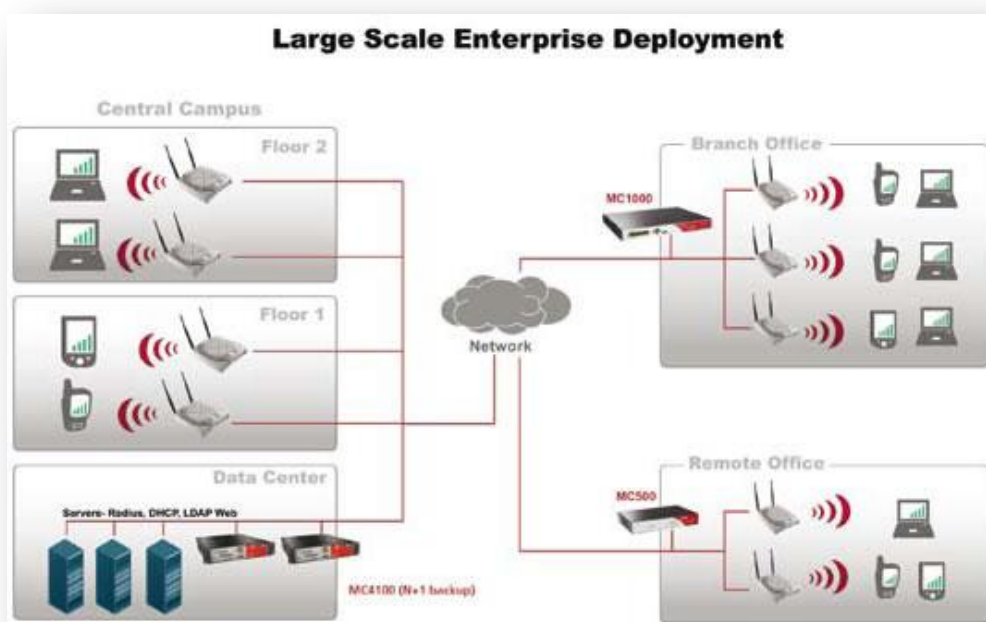


ILUSTRACIÓN 8 ARQUITECTURA WIFI

Otra ventaja de este fabricante es que la interfaz de comandos de este equipo está basada también en CLI. Además, gracias a que podemos establecer comunicación entre el controlador y los puntos de acceso a nivel 3 (nivel IP), ganamos que el AP no está limitado a estar en la misma VLAN, o segmento de red donde se encuentre el controlador; de esta forma un solo controlador puede darnos servicio a toda nuestra red CAMPUS.

2.1.3 SERVICIO DE DIRECTORIO

Respecto al servicio de cuentas de usuarios, usaremos un sistema compatible con LDAP. Evaluamos el Directorio Activo de Microsoft como solución, dado que incorpora el uso de estándares como X.500 y LDAP, para el acceso a la información, con lo cual podemos garantizar una integración con distintas tecnologías y fuentes de información que requieran una validación de cuentas de usuario centralizada.

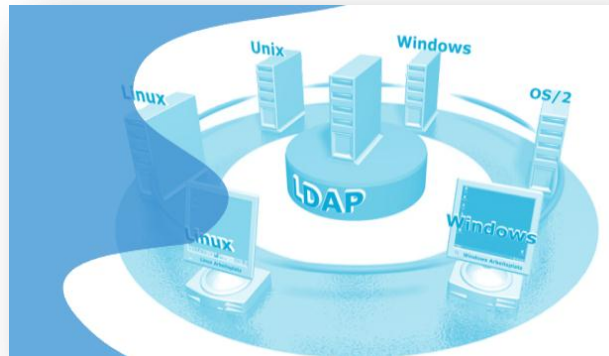


ILUSTRACIÓN 9 COMPATIBILIDAD DIRECTORIO ACTIVO

Esta faceta de estandarización del servicio de directorio de Microsoft, y su bajo coste de mantenimiento (recursos tecnológicos disponibles en el mercado), ha permitido que se sitúe como líder del mercado en el segmento de escenarios sobre el que vamos a desplegar nuestro proyecto, por lo cual lo usaremos para este desarrollo.

Dentro de sus ventajas, la principal, por la que escogemos esta tecnología, es la autorización y autenticación de usuario centralizadas.

Para autenticar una solicitud de conexión, además de validar las credenciales de conexión con cuentas de usuario y equipos de Directorio Activo, también podemos hacer uso de grupos de objetos y facilitar la segmentación de los distintos tipos de usuarios en base a perfiles comunes.

Por otra parte, para autorizar una solicitud de conexión, podemos hacer uso de las propiedades de marcado de cada cuenta de usuario. Esto nos permite hacer uso de esta configuración de permisos y poder limitar el acceso independientemente de la configuración que realicemos en nuestro servidor Radius. Podemos ver esta característica en la siguiente imagen:

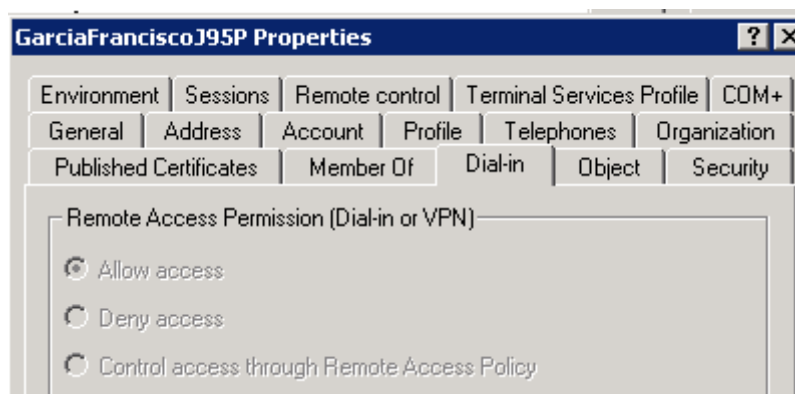


ILUSTRACIÓN 10 PROPIEDADES DE MARCADO

2.1.4 SERVIDOR DE RADIUS

Este proyecto surge de la idea de integrar el acceso a nuestra red desde los distintos medios disponibles, y por cualquier tipo de usuario que podamos llegar a tener. Para llevar a cabo este cometido decidimos basarnos en un servidor Radius, que será el núcleo de este proyecto.

Sabemos que un servidor de Radius se basa en un protocolo de autenticación y autorización, que podemos implementar en distintos escenarios; en la siguiente imagen un servidor de VPN. Pero en nuestro caso sólo lo aplicaremos en la gestión de acceso a la red, tanto a nivel cableado como Wifi.

A la vez que las funciones básicas de autenticación y autorización, también ganamos en otros servicios como la monitorización de la conexiones o en información sobre los accesos realizados: hora de acceso y fin, usuarios, redes, etc.

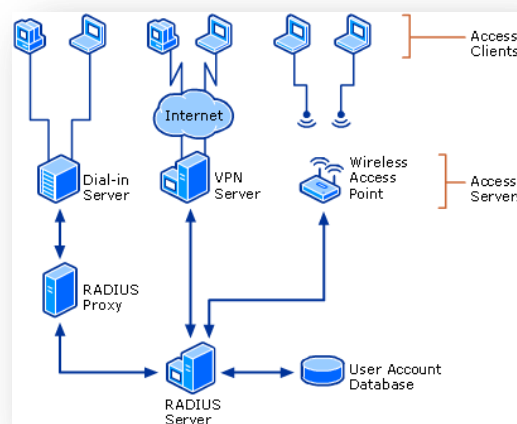


ILUSTRACIÓN 11 FUNCIONES DE RADIUS

A la hora de valorar el servidor de nuestro proyecto, tenemos tanto implementaciones Radius comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc.

Sin embargo, y dado que tenemos como punto de partida un servidor de Directorio Activo, consideramos que la integración con todo el conjunto de usuarios, perfiles y grupos definidos, pueden ser mejor integrados con la herramienta Radius de Microsoft llamada NPS. Además el coste por licencias lo podremos amortizar rápidamente al repercutir un menor número de horas en la implantación e integración y, en una ampliación futura del número de servicios ofrecidos por dicho servidor, dado que, como hemos comentado, puede ofrecer distintos roles en un mismo producto.

2.1.5 NPS.

NPS es la implementación Radius de Microsoft. Entre las distintas ventajas que puede ofrecernos podemos enumerar:

- Configurable como un proxy Radius que reenvía las solicitudes de conexión a otros servidores Radius para que estos realicen su procesamiento.
- Escalable a un sistema de NAP. Sistema de protección de acceso a la Red, basado en el cumplimiento de requisitos en el cliente, antivirus, parches de seguridad, etc., evolución futura de un proyecto de este tipo.
- Totalmente compatible con bases de datos de cuentas de usuario en Active Directory Domain Services (AD DS). **Punto fuerte en el que basaremos nuestro proyecto.**

La implementación básica nos permite usar políticas de red para redirigir el acceso a grupos específicos de directorio activo. Así, podremos crear grupos universales donde integrar todos los usuarios a los que deseemos permitir el acceso y, luego, crear una directiva de red asociada a este grupo universal. Como optimización, los usuarios no serán incluidos directamente en el grupo universal; en su lugar, se podrán crear grupos separados que sí serán miembros del grupo universal y, a continuación, agregar usuarios a esos grupos. Esta técnica es la recomendada en grandes organizaciones, como la nuestra.

Podemos ver un resumen de este procedimiento en la siguiente imagen:



ILUSTRACIÓN 12 FUNCIONAMIENTO NPS

Para poder tener un sistema estable, ante fallos o caídas del sistema, podremos tener varios servidores de NPS. Estos serán configurados en todos los equipos de acceso y realizaremos una sincronización de su configuración para replicar todas las políticas de acceso definidas.

2.2 IEEE 802.11X

Una vez situados en el extremo del acceso de nuestro cliente, la opción a la hora de comunicar con todo nuestro sistema de autenticación será un protocolo estándar que permita su implementación y configuración en todos los clientes de nuestra red. Los protocolos usados, en este sentido, nos permitirán transmitir toda la información necesaria y recibir la configuración en tiempo real en nuestros puertos de acceso. En nuestro caso, el protocolo usado para cubrir todas estas funcionalidades ha sido 802.1X; cualquier otro protocolo propietario, como por ejemplo NAC de Cisco, nos habría forzado a realizar una instalación y configuración específica en cada cliente, con lo cual habríamos perdido flexibilidad, uno de los objetivos de nuestro proyecto.

Sobre 802.1X, un estudio de Gartner indicó que el 50% de las grandes empresas planean implementar 802.1X en sus redes cableadas durante el 2011 y que este porcentaje se podría elevar al 70%. Este dato nos da una mayor seguridad en la elección del estándar IEEE 802.1X para todos nuestros dispositivos clientes, dado que goza de una gran aceptación en el mercado de productos compatibles y su popularidad va subiendo.

IEEE 802.1X define la autenticación de los clientes mediante la encapsulación del protocolo de autenticación extensible (EAP) a través de EAPOL (EAP sobre LAN). EAPOL cubre los requisitos de este proyecto dado que se puede usar en tecnologías LAN IEEE 802, a la vez que otros estándares como IEEE 802.11 inalámbrica. El protocolo EAPOL nos permitirá funciones adicionales de negociación, principalmente para las comunicaciones inalámbricas, donde debemos garantizar un nivel de seguridad mayor.

La Autenticación 802.1X consta de tres partes:

- **Suplicante:** es un dispositivo cliente (por ejemplo, un ordenador portátil) que desee conectarse a la red LAN / WLAN (el término *suplicante* también se utiliza indistintamente para referirse al software que se ejecuta en el cliente que proporciona las credenciales al autenticador).
- **Autenticador:** es un dispositivo de red, como un switch Ethernet o un punto de acceso inalámbrico. Actúa como un guardia de seguridad hacia una red protegida. Al suplicante (es decir, el dispositivo cliente) no se le permite el acceso a la red hasta que su identidad ha sido validada y autorizada. En este sentido podemos establecer distintas políticas que puedan autorizar tanto la máquina, como al usuario o una combinación de ambos.
- **Servidor de Autenticación:** es, normalmente, un host que ejecuta el software de soporte del Radius y los protocolos EAP.

Con la autenticación 802.1X, el suplicante proporciona las credenciales, como el nombre de usuario / contraseña o certificado digital, al autenticador y este reenvía las credenciales al servidor de autenticación para proceder, así, a su verificación. Si el servidor de autenticación determina que las credenciales son válidas permite que el suplicante (dispositivo cliente) acceda a los recursos configurados en la política de acceso.

Este proceso lo podemos ver detalladamente en la siguiente imagen:

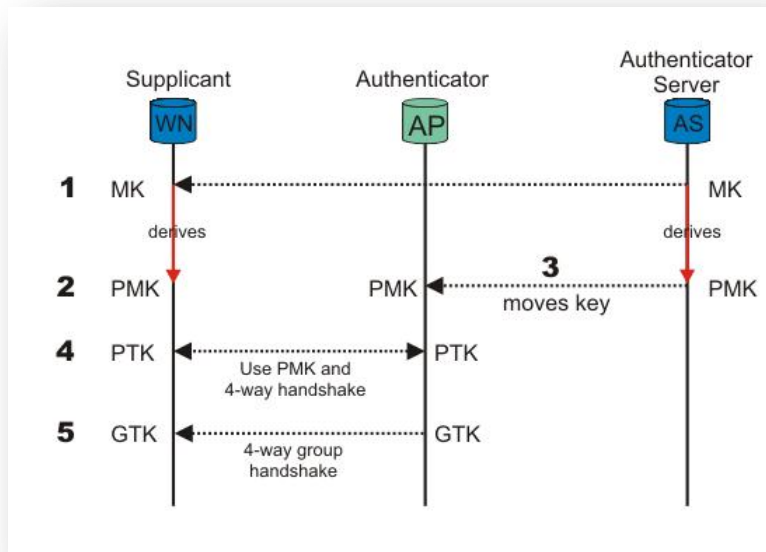


ILUSTRACIÓN 13 VALIDACIÓN 802.1X

Para la red WiFi, dado que el medio aéreo es compartido y no podemos evitar que alguien pueda interceptarlo, la elección de un tipo de protocolo seguro, en la validación de credenciales, es un aspecto importante del proyecto.

En este sentido contamos con distintas opciones:

- La implementación de EAP protegido de Microsoft (PEAP MS-CHAP) v2. Implica menos procesamiento que los otros mecanismos comunes de EAP.
- El Protocolo de autenticación extensible Transport Layer Security (EAP-TLS). Precisa de una infraestructura de clave pública (PKI) en nuestra organización y su implementación en los equipos clientes.

Optamos por PEAP MS-CHAP v2, que utiliza las credenciales de identificación de usuarios de Directorio Activo y su contraseña bajo un canal seguro y, a la vez que no requiere cambios en los PCs o clientes con Windows, es el tipo de cliente más popular de escritorio en las grandes empresas como la nuestra.

2.3 VIRTUAL LAN.

Mediante este sistema podremos dividir, a nivel lógico, nuestra red en distintos segmentos, aislados unos de otros, sin necesidad de replicar toda la configuración física y elementos de red adicionales.

Podemos ver un diseño de este concepto en la siguiente imagen:

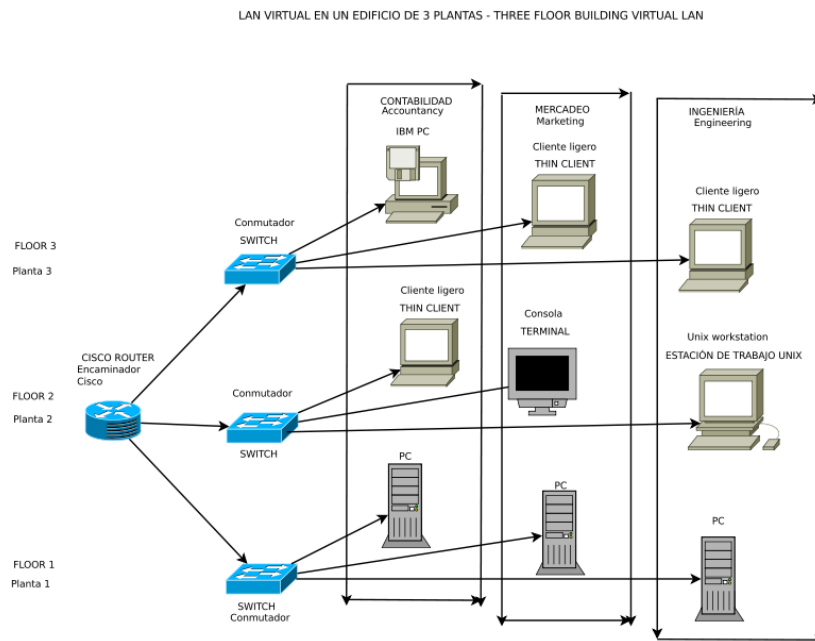


ILUSTRACIÓN 14 EJEMPLO VLAN

En el contexto de las VLAN, el término trunk (troncal) designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports ('puertos etiquetados') de dispositivos con soporte de VLANs, por lo que, a menudo, son enlaces conmutador a conmutador o conmutador a enrutador, más que enlaces a nodos.

Es decir, gracias al uso de redes virtuales, podremos segmentar la Red no en ubicaciones físicas, sino en Redes agrupadas por servicios o distintos tipos de equipos clientes.

2.4 RESUMEN TECNOLÓGICO.

Tecnológicamente, hemos visto que la autenticación 802.1X funciona bien. El proceso de inicio de sesión del usuario final no lo hemos cambiado, y 802.1X no debe añadir un retraso de inicio de sesión notable, realmente el usuario típico no debería apreciar la aplicación de 802.1X durante su conexión.

El equipo de switches del proyecto permitirá configurar la totalidad de puertos de switch con 802.1X y conectados a ellos todos los dispositivos suplicantes de 802.1X. A su vez la red Wifi dará esta función allí donde tengamos cobertura.

Todos los usuarios actuales y futuros serán integrados en un único punto de control de cuentas de usuarios, nuestro directorio activo, por lo que la gestión centralizada nos repercutirá en una mayor claridad a la hora de personalizar y asegurar los accesos individuales, a la vez que en el mismo sistema podremos tener controlados

todos los equipos usados en nuestra red. Para los equipos no compatibles con el cliente de directorio activo, podremos usar una cuenta de máquina ficticia basada en la dirección MAC del equipo cliente. Mediante este mecanismo podremos recibir y validar su dirección física y validarla, igualmente, con nuestras políticas de accesos como si de un cliente compatible se tratara.

El servidor Radius, junto con el despliegue de una segmentación de LAN virtual, será básico para hacer cumplir las políticas basadas en la identificación de roles. Con esta técnica, la red nos permitirá reconocer múltiples perfiles (los clientes, empleados, empleados con niveles superiores de acceso, invitados, etc), y dirigir el tráfico en función del usuario y su autorización basada en políticas de acceso.

El uso de la red Wifi nos complementará los tipos de clientes soportados, dado que, en la actualidad, algunos dispositivos ya no incorporan una interfaz Ethernet en su chasis.

Gracias a la inclusión de EAP podremos tener un medio seguro para validar los distintos tipos de usuarios y asociarlos a los perfiles y niveles de acceso.

Y, finalmente, podremos monitorizar el sistema y revisar los accesos mediante los registros que el sistema nos irá generando.

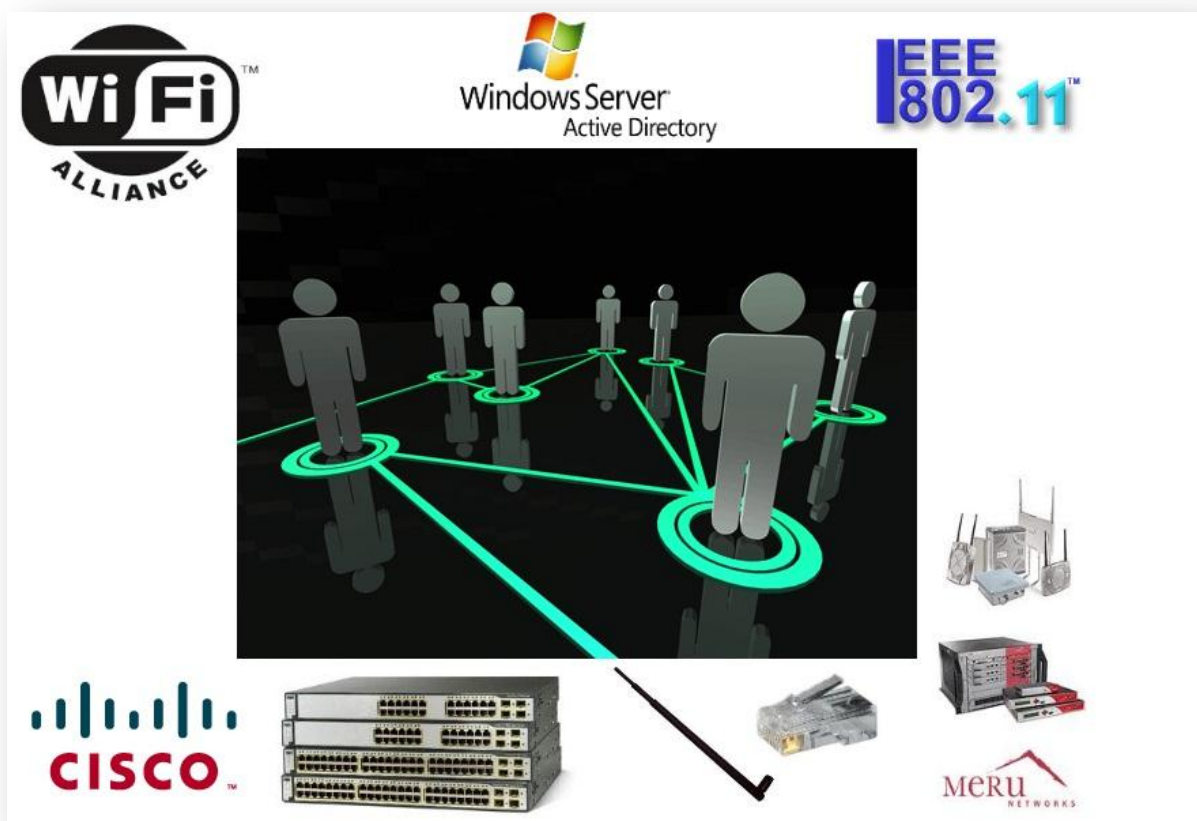


ILUSTRACIÓN 15 RESUMEN DE TECNOLOGÍA

3. ESTUDIO DE VIABILIDAD

Como ya dijimos, en la introducción, nuestro estudio está basado en una red tipo Campus, en nuestro caso hospitalario, y el análisis de viabilidad nos debe servir de guía para futuras implementaciones. La eficacia de nuestro proyecto dará solución a las futuras cuestiones que nos pueda plantear la complejidad de este tipo de red.

Analizaremos los recursos disponibles para saber si es posible abarcar un proyecto de esta envergadura con recursos propios o, por el contrario, si requiere alguna inversión en equipos o nuevos elementos. Y si es así realizaremos el estudio económico pertinente para llevarlo a cabo.

3.1 RED CABLEADA

Un esquema de red tipo campus está formado, normalmente, por una topología en estrella distribuida. Esta topología se implanta en centros o conjuntos formados por varios edificios que forman parte de una misma entidad corporativa.

Tomamos como referencia el Campus implantado en este centro de hospitales universitarios.

La topología inicial es la siguiente:

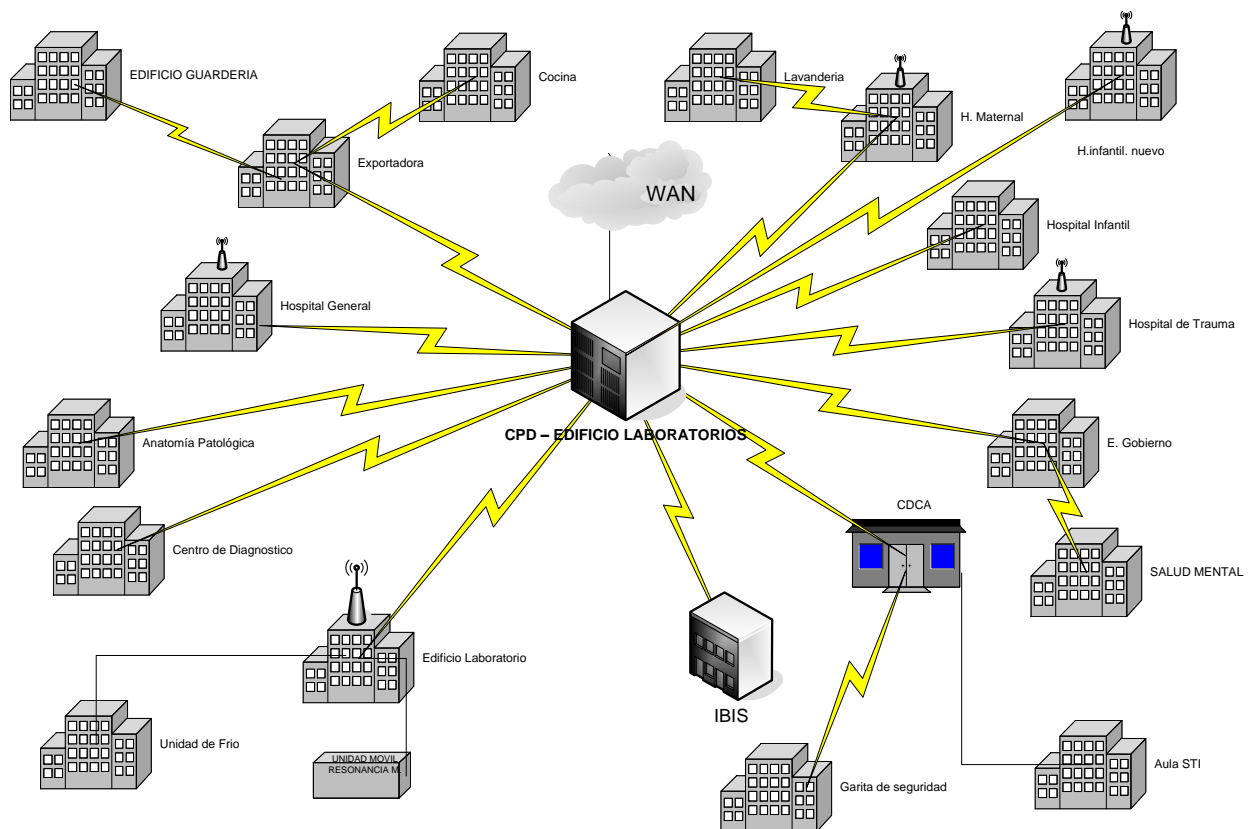


ILUSTRACIÓN 16 TOPOLOGÍA DE RED

Como vemos, siempre tenemos un punto central donde “nace” nuestra red; desde este punto repartiremos la señal a todos los centros periféricos, donde a su vez realizaremos una disgregación de la señal desde su punto de distribución a las distintas plantas donde ya se encontraran los puntos de acceso de usuario.

A nivel de los centros podemos tener una situación similar a la siguiente.

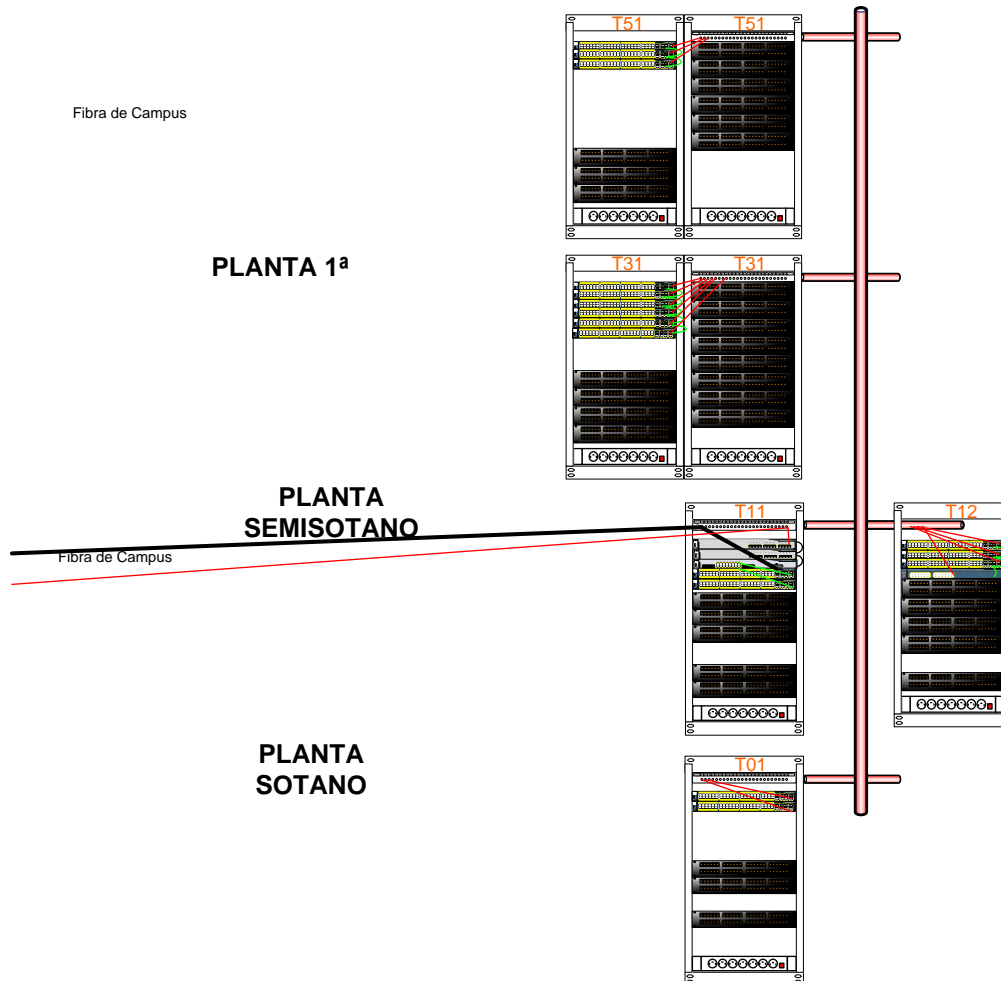


ILUSTRACIÓN 17 ELECTRÓNICA DE RED EN EDIFICIOS

Una vez analizada la topología física, podemos ver que la topología lógica se basará en una virtualización de nuestras redes, de forma que el esquema de interconexión planteado pueda ser reutilizado por todas nuestras posibles redes sin necesidad de replicar los equipos y tampoco, lo más importante, los enlaces.

A nivel de redes virtuales partimos de una situación inicial en la que tenemos distintas VLAN distribuidas, desde nuestro punto central de red, a los distintos edificios.

Estas redes dispondrán a su vez de un direccionamiento propio y podremos interconectarlas mediante un router/firewall con reglas de filtrado y de acceso entre ellas.

A nivel de equipamiento podemos definir 3 tipos de electrónica.

- Switches Core: Cisco 6513
- Switches distribución: Cisco 3750
- Switches de acceso: Cisco 2950

Sobre esta base, revisamos los requisitos para la asignación de VLAN IEEE 802.1X en los switches. Dado que la electrónica es Cisco, comprobamos que sus requisitos para este servicio es la siguiente:

Antes de que la función de asignación de VLAN se lleve a cabo, las siguientes condiciones deben cumplirse:

- IEEE 802.1X debe estar habilitado en el puerto del switch.
- El soporte de EAP deben estar habilitadas en el servidor RADIUS.
- La autorización de la AAA debe estar configurado en el puerto para todas las solicitudes de servicios relacionados con la red.
- El puerto debe ser autenticado correctamente.

Configuraremos 802.11X para que se apoye en un servidor de Radius. Esta característica es la llamada IEEE 802.1X Radius Accounting, soportada a partir de una revisión de firmware en el nivel: Cisco IOS Release 12.2(20). El resto de requisitos los cubriremos a nivel de configuración en el apartado de implementación.

También precisamos poder configurar automáticamente un puerto de red en una determinada red Vlan. Esta funcionalidad, llamada IEEE 802.1X Vlan Assignment, nos permitirá definir la red de acceso en función del usuario que se conecte a un determinado puerto. En este caso comprobamos que con una revisión de firmware en el nivel: Cisco IOS Release 12.2(22), cubrimos esta característica.

Para realizar esta revisión en detalle hemos utilizado la utilidad de Cisco: Cisco Feature Navigator (<http://tools.cisco.com/ITDIT/CFN/jsp/by-feature.jsp>). Podemos ver un ejemplo del uso de dicha herramienta en la siguiente imagen:

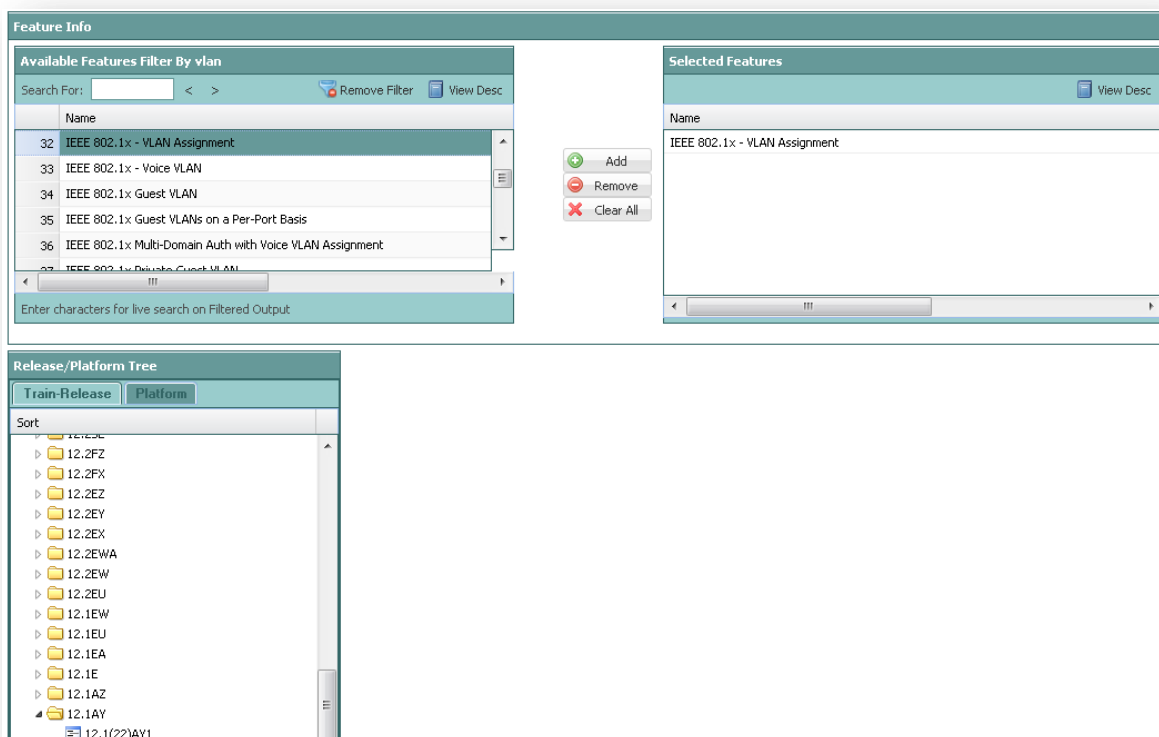


ILUSTRACIÓN 18 CISCO FEATURE NAVIGATOR

Una vez conocido el nivel de IOS necesario, realizamos una comprobación en los equipos de nuestra Red. Esto lo podemos realizar mediante el comando: "show ver" en la consola de cada switch.

Mostramos el resultado del comando sobre un switch de acceso Cisco 2960:

```
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 19-Jul-07 20:06 by nachen
Image text-base: 0x00003000, data-base: 0x00D40000

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE SOFTWARE (fc1)

273565D uptime is 3 years, 8 weeks, 1 day, 22 hours, 55 minutes
System returned to ROM by power-on
System restarted at 12:39:40 CEST Thu Feb 5 2009
System image file is "flash:c2960-lanbase-mz.122-35.SE5/c2960-lanbase-mz.122-35.SE5.bin"

cisco WS-C2960G-48TC-L (PowerPC405) processor (revision C0) with 61440K/4088K bytes of memory.
Processor board ID FOC1147Z420
Last reset from power-on
2 Virtual Ethernet interfaces
48 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:1E:79:3E:00:00
Motherboard assembly number    : 73-10300-07
Power supply part number       : 341-0098-02
Motherboard serial number      : FOC11472BU0
Power supply serial number     : AZS11441604
Model revision number          : C0
Motherboard revision number    : A0
Model number                   : WS-C2960G-48TC-L
System serial number           : FOC1147Z420
Top Assembly Part Number      : 800-27071-02
Top Assembly Revision Number  : A0
Version ID                     : V02
CLEI Code Number               : COM4A10BRB
Hardware Board Revision Number : 0x01
```

Switch	Ports	Model	SW Version	SW Image
*	1 48	WS-C2960G-48TC-L	12.2(35)SE5	C2960-LANBASE-M

Configuration register is 0xF

Hemos comprobado que los switches y la topología de red usada, cumplen los requisitos de implantación de este proyecto. Recalamos que a nivel de switch, sólo los que asuman el rol de "autenticador" (visto en apartado 802.11X) serán los que principalmente precisen de estas características. Este rol será realizado sólo en los switches de acceso Cisco 2960.

3.2 RED WIFI

La topología usada en la Red WIFI del Campus está basada en un controlador central, que gestiona y centraliza toda la configuración de los puntos de acceso.

Los puntos de acceso tienen conexión con el controlador para poder recibir toda la configuración y reportar los eventos que generen al controlador. Para ello se ha desplegado sobre una VLAN independiente, llamada “de gestión”, donde están todos los equipos WIFI. De esta forma minimizamos la complejidad de la configuración y garantizamos una conexión continua basada sólo en LAN.

Los equipos sobre los cuales determinaremos la posibilidad de implantación de este proyecto son:

- Controlador Meru MC4100
- Punto de acceso AP1020

Todos los controladores de Meru ejecutan el System Director, que es el sistema operativo de Meru que gestiona y supervisa los puntos de acceso (AP). Este software proporciona un sistema de gestión centralizada desde una interfaz web, o por línea de comandos Interface (CLI). Desde él podemos realizar la monitorización, configuración y solución de problemas del sistema. Además, incorpora un conjunto de servicios que proporcionan sistema de gestión para la seguridad, la planificación del espectro de radio frecuencia, la calidad de servicio para la convergencia de datos, redes de voz y video, la transferencia de datos durante el roaming, y aplicaciones basadas en localización.

Meru Wireless es compatible con WPA2 y WPA, protocolos que han sido presentados por la Alianza Wi-Fi como las normas de seguridad provisionales que mejoran las vulnerabilidades conocidas de WEP hasta el lanzamiento del estándar 802.11i.

Sabemos que a partir del estándar WPA, se incluye el protocolo de cifrado TKIP (ver TKIP) y se aprovechan los mecanismos de control de acceso y autenticación del sistemas 802.1X. Por tanto, la compatibilidad con WPA nos indica la garantía de poder implementar 802.1X en un sistema Wifi.

En la implementación de 802.1X un sistema Wifi, compatible con WPA, se configura un ESS que utiliza WPA/WPA2 como perfil de seguridad, se realiza la autenticación de usuarios del sitio con 802.1X y cifrado TKIP o CCMP. Una vez asociados con este perfil, podemos tener la seguridad de que el acceso se ha realizado basado en la información de la base de datos de cuentas de usuarios.

De esta forma vemos que nuestro sistema es compatible con 802.1X, mediante la configuración de un SSID, que cumpla los requisitos de configuración descritos. Aun así revisamos las especificaciones del equipamiento y la versión de firmware del mismo.

Vemos que el cumplimiento de estas capacidades es independiente del nivel de firmware, dado que en las especificaciones generales del Controlador MC4100 ya se indica como soportado 802.1X:

General

Tipo de dispositivo	Dispositivo de gestión de la red
Altura (unidades de bastidor)	2U
Dispositivos integrados	Indicador LED de estado
Anchura	43.2 cm
Profundidad	55.8 cm
Altura	8.9 cm
Peso	16.3 kg
Conexión de redes	
Factor de forma	Externo
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet

Protocolo de gestión remota	HTTP, HTTPS
Rendimiento	Capacidad: 4 Gbps
Capacidad	Número máximo de puntos de acceso: 100
Indicadores de estado	Actividad de enlace, velocidad de transmisión del puerto, alimentación, estado
Características	Protección firewall, control de tráfico SMTP, Quality of Service (QoS)
Algoritmo de cifrado	LEAP, AES, WEP de 128 bits, ncriptación de 64 bits WEP, TLS, PEAP, TTLS, TKIP, MD2
Método de autenticación	RADIUS, CHAP, Extended Service Set ID (ESSID)
Cumplimiento de normas	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1x
Telefonía IP	
Protocolos VoIP	SIP, H.323 v1
Expansión / Conectividad	
Ranura(s) de expansión	2 SFP (mini-GBIC)
Interfaces	4 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x gestión - D-Sub de 9 espigas (DB-9) 1 x USB - 4 PIN USB tipo A
Diverso	
Cumplimiento de normas	EN55022, VCCI Class A ITE, EN55024, FCC Part 15, MIC, ICES-003 Class A, IUL 60950-1, IEC 60950-1, KCC
Alimentación	
Dispositivo de alimentación	Fuente de alimentación
Potencia suministrada	300 vatios
Garantía del fabricante	
Servicio y mantenimiento	1 año de garantía
Detalles de Servicio y Mantenimiento	Garantía limitada - 1 año
Parámetros de entorno	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	0 - 95%

Los puntos de acceso tomarán la configuración del SSID, que hemos definido en el controlador, pero aun así revisamos, en las especificaciones técnicas, que cumple con el estándar 802.1X:

Ficha técnica del punto de acceso AP1020i de Meru Networks:

GENERAL	
Tipo de dispositivo: Punto de acceso inalámbrico	
Anchura: 17.1 cm	
Profundidad: 17.1 cm	
Altura: 5.7 cm	
Peso: 455 g	
CONEXIÓN DE REDES	
Factor de forma: Externo	
Tecnología de conectividad: Inalámbrico	
Velocidad de transferencia de datos: 300 Mbps	
Protocolo de interconexión de datos: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n	
Protocolo de gestión remota: SNMP, Telnet, HTTP, HTTPS, SSH, CLI	
Banda de frecuencia: 2.4 GHz, 5 GHz	
Nº de canales seleccionables: 14	
Indicadores de estado: Actividad de enlace, alimentación, inalámbrico	
Características: Soporte Wi-Fi Multimedia (WMM), admite varios SSID	
Algoritmo de cifrado: LEAP, MD5, AES, WEP de 128 bits, WEP de 40 bits, TLS, PEAP, TTLS, TKIP, WPA, WPA2	
Método de autenticación: RADIUS, EAP-FAST	
Cumplimiento de normas: IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 802.11n, IEEE 802.3at	
ANTENA	
Antena: Interna integrada	
Directividad: Omnidireccional	
Nivel de ganancia: 5 dBi	
EXPANSIÓN / CONECTIVIDAD	
Interfaces:	

1 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45
1 x US

DIVERSO

Cumplimiento de normas: UL 60950-1, IEC 60950-1, CSA C22.2 No. 60950-1

ALIMENTACIÓN

Admite Power Over Ethernet (PoE): Sí

GARANTÍA DEL FABRICANTE

Servicio y mantenimiento: Garantía limitada de por vida

Detalles de Servicio y Mantenimiento: Garantía limitada - de por vida

PARÁMETROS DE ENTORNO

Temperatura mínima de funcionamiento: 0 °C

Temperatura máxima de funcionamiento: 50 °C

Ámbito de humedad de funcionamiento: 0 - 90% (sin condensación)

3.3 DIRECTORIO ACTIVO

La base de datos utilizada en la empresa es el Directorio Activo de Microsoft. Dicha base de datos centraliza todas las cuentas de usuario, equipos, y recursos.

La idea, que hay detrás de 802.1X, es proporcionar autenticación de capa 2; es decir, autenticar a los clientes de nuestra LAN en la capa Ethernet. Esto antes de que el cliente obtenga una concesión de IP en el DHCP. Con el fin de lograr la conectividad de red, el dispositivo debe autenticarse antes de que su tráfico de red esté permitido.

El uso de esta infraestructura es configurar la autenticación 802.1X en un conmutador de red, de tal manera que pueda aprovechar los servicios de autenticación existentes, proporcionados por el Directorio Activo. Podemos ver una representación de este proceso en la siguiente imagen:

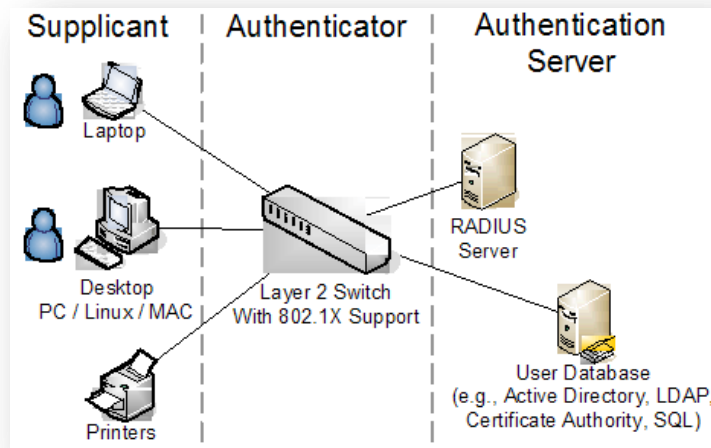


ILUSTRACIÓN 19 AUTENTICACIÓN DIRECTORIO ACTIVO

Gracias a las características avanzadas del directorio activo, podremos obtener mejoras con respecto al uso de una base de datos de cuentas de usuario simple. En nuestro caso podríamos configurar los sitios necesarios de la compañía, y en cada uno de ellos configurar las unidades organizativas que definan cada centro o perfil.

Usaremos esta característica de segmentación de usuarios y máquinas para poder generar todos los grupos de usuarios necesarios para cumplir los distintos tipos de accesos que definamos, por ejemplo un grupo para los empleados, otro para los visitantes, etc.

Además desde directorio activo podemos autorizar los distintos servicios desplegados en nuestra red, como por ejemplo servidores DHCP, DNS, y el que usaremos en este proyecto que será el servidor NPS. Gracias a esta característica mejoramos la seguridad de nuestra red, dado que no sólo es preciso configurar los servicios mencionados sino que, como administradores, los autorizaremos en cada máquina. De esta forma el control y seguimiento de nuestra red es mayor.

Con este tipo de capacidades, que van más allá de 802.1X, ganamos un control flexible posterior a la admisión o autorización, con la capacidad de diseñar las políticas que definan el acceso de los usuarios en función de su papel en la organización. Este aprovisionamiento, basado en roles, proporciona un control de acceso universal, asegurando que los derechos y los permisos se aplican universalmente también, independientemente del medio de acceso de un usuario o su ubicación.

En este punto los clientes también formarán una parte importante del sistema puesto que, para que podamos acceder al abanico completo de utilidades, que nos aporta el directorio activo, estos clientes han de ser compatibles con esta plataforma.

Los clientes compatibles por defecto con directorio activo son toda la familia de sistema operativos de Microsoft, Windows XP, Windows /, etc. Aunque hoy en día existen conectores para usar directorio activo como base centralizada de cuentas de usuarios incluso desde UNIX.

De todas formas el informe de viabilidad no lo cruzaremos con los posibles sistemas operativos usados por el cliente, dado que siempre partimos de la base que estamos usando un estándar de mercado, como es 802.1X, por lo tanto las configuraciones mínimas, desde el punto de vista de seguridad, siempre se cumplirán si el sistema operativo cliente respeta el estándar.

4. EJECUTANDO EL PROYECTO

4.1 TRABAJOS PREVIOS

4.1.1 ADAPTACIÓN DE VLAN

Realizaremos un recorrido sobre los distintos perfiles de acceso que puedan existir. A estos perfiles les tendremos que asignar una determinada red de acceso. En la mayoría de los casos su red puede estar ya creada y en algunos casos podremos definir nuevas redes para cubrir toda la casuística.

Los perfiles de acceso controlados por 802.1X son:

- Equipos de la empresa.
 - o Equipos de escritorio (PC) usados para trabajo interno. Impresoras de red. Terminales ligeros. Equipos aislados por seguridad (Equipos que no cumplen requisitos de conexión a directorio activo, antivirus, parches de seguridad, etc). Equipos de escritorio para uso externo (salas de internet, bibliotecas, etc).
- Equipos externos.
 - o Dispositivos personales de trabajadores. Equipos de proveedores usados para dar soporte.
- Personal.
 - o Trabajadores internos. Proveedores. Clientes.

A partir de estos datos vamos a confeccionar la tabla matriz de asignaciones de redes.

Perfil \ VLAN	5 – Red administrativa	25 – Salas públicas.	26 - Invitados	50 – Sin dominio
Equipos de escritorio (PC) usados para trabajo interno	✓			
Impresoras de red	✓			
Terminales ligeros	✓			
Equipos aislados por seguridad				✓
Equipos de escritorio para uso externo			✓	
Dispositivos personales de trabajadores		✓		
Equipos de proveedores usados para dar soporte		✓		
Trabajadores internos	✓	✓		
Proveedores		✓		
Clientes			✓	

TABLA 3 PERFILES DE ACCESO

Vemos que para la Vlan 5 asignaremos los PCs dados de alta en dominio con usuarios pertenecientes al dominio y dentro del grupo de trabajadores. Así mismo, todos los dispositivos como Impresoras de red, fotocopadoras, escáner y terminales ligeros serán dados de alta en esta red al ser equipos que únicamente puede la empresa proporcionar. En este último caso, el dispositivo no iniciará sesión en el directorio activo, por lo tanto usaremos una política de alta de direcciones MAC como cuentas de equipo en el dominio.

Para la Vlan 25 tendremos a usuarios conocidos, dados de alta en dominio, pero que estén usando PCs externos (portátiles personales o PCs de proveedores usados para dar soporte local de forma puntual).

La Vlan 26 se usará para equipos dados, o no, de alta en el dominio pero pensados para uso externo, por ejemplo PCs de aulas de formación, bibliotecas, etc. El Usuario validado tampoco ha de estar en el dominio.

Finalmente usaremos la Vlan 50 para equipos conocidos, y aceptados para estar en la red, pero que por algún motivo no cumplen con los requisitos de conexión a la Lan 5. Por ejemplo servidores, o equipos de red, adquiridos por la empresa, pero que por motivos de garantía o soporte no pueden contar con antivirus o con una política de actualización de parches de seguridad, ni nos permiten su inclusión en el Directorio Activo. Procederemos a realizar su alta mediante su dirección MAC en AD.

Esta configuración no es cerrada, nos permite asumir nuevos roles y con ello nuevas redes según la complejidad del entorno en el que trabajemos. Para poder comprobar toda la flexibilidad, a nivel de políticas, que nos permite el sistema, nos es suficiente con los 4 roles que hemos descrito antes.

4.1.2 ADAPTACIÓN DEL DIRECTORIO ACTIVO

En nuestro directorio activo es donde residirán todas las cuentas de usuarios y equipos; es por tanto con esta base de datos con la cual cruzaremos las políticas de seguridad implementadas en nuestro servidor de acceso (NPS).

Una vez que hemos adaptado las distintas redes virtuales según el perfil de trabajo, podremos generar en el directorio activo los distintos grupos de seguridad donde iremos colocando los objetos.

Dado que ya hemos definido las distintas VLAN de trabajo en función de los perfiles, una buena gestión en este caso será generar un grupo de seguridad por cada VLAN. El nombre del grupo de trabajo lo podemos generar en función de los distintos estándares usados en la empresa pero, por claridad, añadiremos siempre una referencia a la VLAN donde trabajarán los equipos incluidos en él.

Así, lo grupos creados serán:

- SE41_GS_VLAN5
- SE41_GS_VLAN25
- SE41_GS_VLAN26
- SE41_GS_VLAN50

De esta forma, una vez asignado un nuevo elemento a nuestro directorio, el segundo paso será asignarlo al grupo de seguridad correspondiente, según el perfil de trabajo. Nuestro mayor hándicap será el asociar estos grupos a todas las máquinas ya incluidas en nuestro dominio. Para ello nos apoyaremos en el esquema de implantación.

4.2 CONFIGURACIÓN DE DIRECTORIO ACTIVO

Procedemos a realizar la configuración de grupos de usuarios, y máquinas, en los distintos perfiles de acceso que teníamos definidos.

Independiente al tipo de perfil que vaya a tener cada equipo, o usuario, todos deben cumplir, primero, el requisito de tener permisos de conexión remota controlada por políticas de acceso.

Para situar dicha configuración, tendremos que verificar que, en las propiedades del objeto, tanto de equipos como de usuarios, tengan activo el permiso de acceso remoto controlado por políticas de marcado e indicar que no retorne la llamada al usuario (No Callback).

Este sistema también nos servirá para que, por motivos de seguridad o de otra índole, podamos denegar a un objeto, tipo maquina o usuario, el acceso a cualquiera de nuestras redes sin necesidad de limitar su acceso al nivel de capa 2 (switch).

Podemos ver estas opciones en la siguiente imagen:

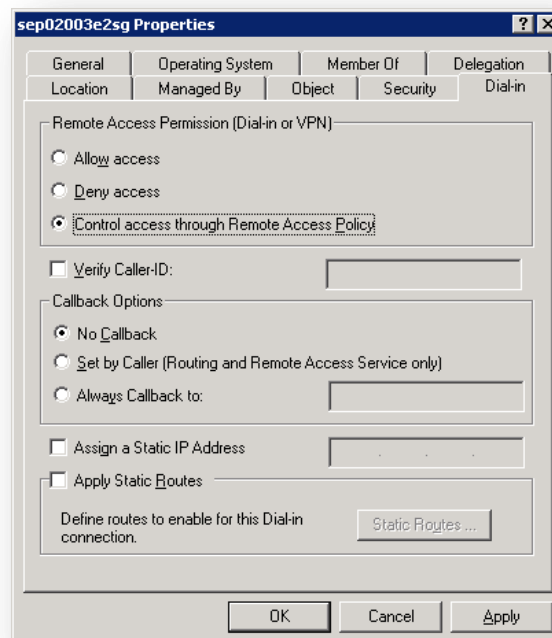


ILUSTRACIÓN 20 AD, POLÍTICAS DE MARCADO

4.2.1 ACCESO A RED ADMINISTRATIVA

El tipo de equipo, a los que autorizaremos la conexión a este sistema, son:

- PCs corporativos.
- Impresoras de red, fotocopiadoras, escáner y terminales ligeros.

Generaremos los grupos locales en el dominio para incluir en ellos los distintos clientes que se correspondan con los tipos de perfiles nombrados.

Para generar los grupos, arrancamos nuestro administrador de usuarios y equipos de Active Directory, nos situamos en la unidad organizativa de nuestra sede (en el caso de que tengamos varias) y seguimos los siguientes pasos:

1. Sobre “Grupos”, botón derecho y pulsamos en nuevo.
2. Introducimos el nombre del grupo :ejemplo: SE41_GS_RadiusVlan5
3. El ámbito habrá de ser: “Global”.
4. Tipo de grupo de “Seguridad”.

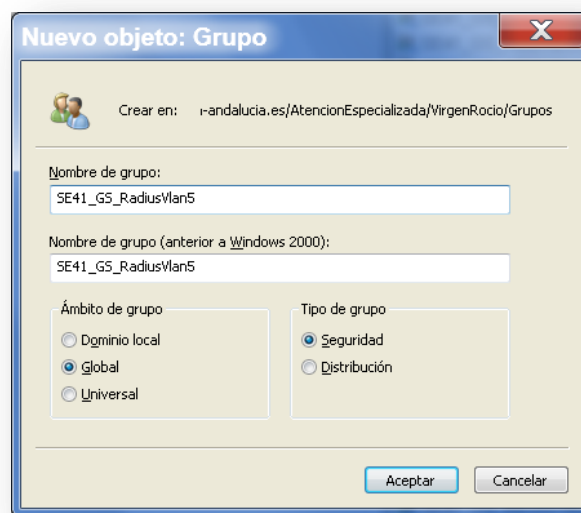


ILUSTRACIÓN 21 NUEVO GRUPO AD

Para PCs corporativos sabemos que, por diseño, todos los equipos dados de alta, en un directorio activo, forman parte del grupo de seguridad local llamado “Domain Computers”. Una vez el equipo esté validado en Radius, podemos delegar la validación del usuario corporativo en los propios controladores de dominio.

Para el segundo tipo, tenemos que seguir otro procedimiento para su control dado que no son equipos que realicen un proceso de validación en el directorio activo. Este procedimiento se basa en el control de su identificación mediante su dirección MAC; por ello debemos generar una cuenta de usuario en la cual, tanto nombre de usuario como contraseña, sean esa misma dirección. Además, por sus características, sólo usarán la interfaz de red cableada.

Una vez generado el grupo pasamos a incluir en él los objetos creados:

- Los equipos corporativos, que no permitan su inicio en el servidor de dominio (por ejemplo una impresora de red) los podremos añadir al sistema como usuario del dominio teniendo en cuenta que su nombre y contraseña (en minúsculas) habrá de ser su dirección MAC. Estos objetos son los que añadiremos al grupo SE41_GS_RadiusVlan5.

Vemos un ejemplo de usuarios de este tipo:




Nombre	Tipo	Descripción
 000ae40cadaa	Usuario	
 001cc42a56ba	Usuario	
 0026BB1AEC92	Usuario	Usuario MAC para Radius

ILUSTRACIÓN 22 USUARIOS MAC

A lo largo de este documento veremos cómo podremos manejar este tipo de elementos en conjunción con la electrónica de red y el servidor de políticas de Radius NPS.

4.2.2 ACCESO A RED DE SALAS PÚBLICAS

Esta red está pensada para pueda ser utilizada mediante dispositivos externos a la compañía, pero siempre con usuarios conocidos.

Por defecto, también le generamos un grupo de seguridad para poder incluir en dicho perfil cualquier objeto de forma independiente. El grupo se llamará SE41_GS_RadiusVlan25. Aquí concentraremos a todos nuestros usuarios; de esta forma, cuando apliquemos una política basada en este grupo, el dispositivo no será tenido en cuenta pero sí al usuario.

Para ello podemos basarnos en un grupo interno del dominio que ya los incluye:

- Domain Users.

4.2.3 ACCESO A RED DE INVITADOS

Este perfil tendrá un control total por parte del departamento de TI de la compañía. En él incluiremos todos los equipos de la compañía que situemos en salas destinadas al uso de personal externo.

Como vimos, este tipo de equipos estarán situados, por ejemplo, en salas de formación o salas de espera.

Con este criterio generaremos un grupo de seguridad donde incluirlos y lo llamaremos: SE41_GS_RadiusVlan26.

4.2.4 ACCESO A RED SIN DOMINIO

Este es último perfil de acceso que controlaremos bajo nuestro servicio de NPS. Estará formado por todos aquellos equipos que, por sus características, no pueden compartir la misma red de trabajo que el resto de máquinas. Dado que tampoco los podremos incluir en el dominio, seguiremos el procedimiento de alta en directorio activo mediante la creación de un usuario cuyo nombre y contraseña serán su dirección MAC.

Todos los usuarios generados por este sistema, para diferenciarlos del resto de perfiles de acceso, serán dados de alta en el grupo SE41_GS_RadiusVlan50.

Por el tipo de máquinas que se usarán en este entorno, el único acceso será mediante la red cableada.

Bajo esta organización de perfiles y grupos, podremos personalizar las políticas de NPS discriminando, así, el tipo de usuario que está solicitando el acceso. Procedemos ahora con la configuración del servicio de NPS.

4.3 CONFIGURACIÓN DE ELECTRÓNICA DE RED

4.3.1 RED CABLEADA

En el apartado de red cableada, mantenemos el diseño de segmentación en capas (Core, Distribución, Acceso). Sabemos que los clientes de red se encontrarán en la capa de nivel de acceso. A este nivel los dispositivos de red, que usaremos, son switches Cisco 2960.

La configuración de estos dispositivos, para actuar de clientes de Radius, pasa por las siguientes medidas:

- Configuración general para usar autenticación en el switch.
- Establecer el switch como cliente de NPS.
- Establecer en los puertos de acceso la configuración 802.1X correcta.

Configuración general para usar autenticación en el switch.

Por defecto, los switches no tienen habilitados los mecanismos de autenticación, autorización y monitorización en su configuración; comúnmente esta función se conoce como AAA: authentication, authorization, y Accounting.

Para habilitar esta función en los equipos Cisco procedemos de la siguiente forma:

- 1- Accedemos al modo de consola. Ejemplo: Telnet ip switch
- 2- Nos situamos con el rol de administrador (enable): Ejemplo: switch>enable
- 3- Activamos el modo de configuración. Ejemplo: switch# configure terminal
- 4- Configuramos la función AAA: Ejemplo: switch(config)# aaa new-model

Procedemos ahora a configurar el modo de autenticación basado en 802.1X:

- 1- Situados en el modo de configuración: switch# configure terminal
- 2- Habilitamos 802.1X: Ejemplo: switch(config)#dot1x system-auth-control

Finalmente indicamos que toda la autenticación 802.1X sea realizada sobre los servidores Radius configurados sobre este switch.:

- 1- Situados en el modo de configuración: switch# configure terminal
- 2- Habilitamos la autenticación bajo Radius: switch(config)#aaa authentication dot1x default group Radius

Establecer el switch como cliente de NPS

Una vez establecidos los mecanismos de autenticación en el switch, indicamos los servidores de Radius que serán nuestros servidores de NPS, que evaluarán las políticas de acceso. También debemos indicar los puertos que se usarán para las funciones de autorización y autenticación: los puertos estándares para este protocolo son 1812 y 1813, respectivamente.

La configuración necesaria se completará indicando, además del servidor NPS, la clave compartida entre ambos. Esta clave es una palabra de paso, que se establece entre cliente Radius y Servidor, para evitar la solicitud de acceso por clientes no autorizados.

Procedemos a configurarlos:

- 1- Situados en el modo de configuración: switch# configure terminal
- 2- Indicamos el servidor NPS, realizaremos este paso 2 veces, una por cada servidor NPS: Ejemplo:
switch(config)# Radius-server host 10.232.1.180 auth-port 1812 acct-port 1813
- 3- Indicamos la clave compartida: Ejemplo: switch(config)# Radius-server key ;ruts!b

Establecer en los puertos de acceso la configuración 802.1X correcta.

Una de las ventajas de esta implantación, es que puede ser progresiva; es decir por cada switch podemos indicar a todos, o a cada uno, los puertos de acceso que realizarán la autenticación basada en 802.1X.

Otra cuestión importante, a la hora de configurar cada puerto, es realizar las indicaciones oportunas para que, con los equipos no compatibles con 802.1X, podamos articular un mecanismo que les permita iniciar sesión.

En este sentido, Cisco incorpora un mecanismo llamado MAB que permite realizar una autenticación 802.1X basada en la dirección MAC del equipo que solicita el acceso cuando este no es capaz de realizarlo por sí mismo con unas credenciales de usuario.

Vemos en la siguiente figura el proceso descrito:

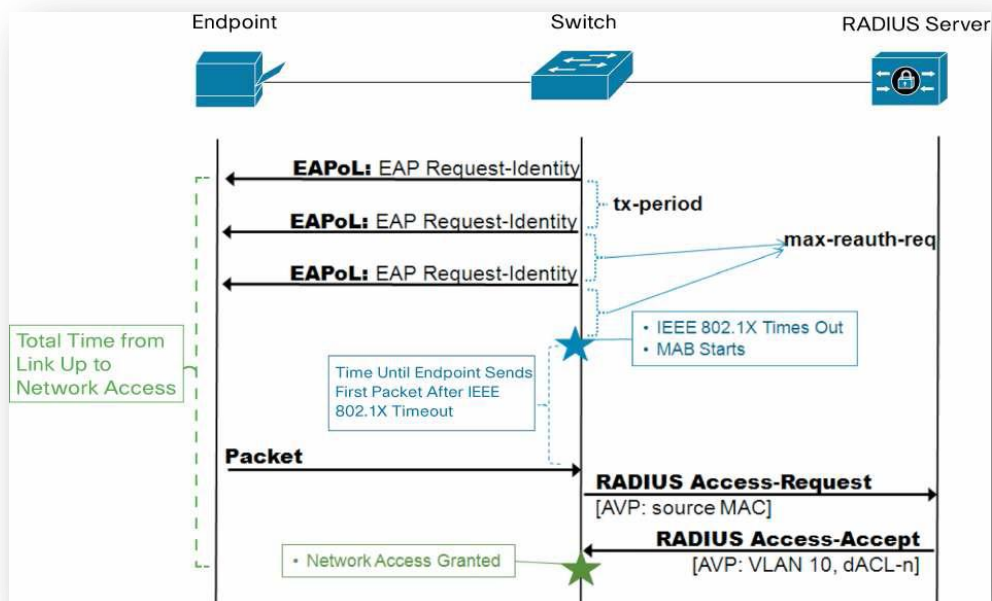


ILUSTRACIÓN 23 PROCESO EAPoL

Vemos que, en caso de que el equipo sea capaz de realizar el proceso de autenticación EAPoL, este procedimiento MAB no se realiza.

Con estas indicaciones, procedemos a configurar, en todos los puertos involucrados en este sistema, la autenticación 802.1X

- 1- Situados en el modo de configuración: `switch# configure terminal`
- 2- Entramos en la configuración del puerto en cuestión: Ejemplo: `switch(config)#interface [type/mod]`
- 3- Activamos el proceso MAB: Ejemplo: `switch(config)#dot1x mac-auth-bypass`
- 4- Activamos el control del puerto mediante 802.1X: Ejemplo: `switch(config)#dot1x port-control auto`

A estos comandos añadiremos los básicos que requiera un puerto de acceso, como es indicar que el puerto será usado por un equipo y no por otro switch (switch mode Access) y podremos establecer una Vlan por defecto, en caso de que toda la autenticación falle (se recomienda que esta Vlan no esté en uso para aislar completamente el equipo que ha tratado de realizar el acceso de forma no autorizada).

Seguiremos este proceso a lo largo de nuestra red, según la planificación de implantación que se marque.

4.3.2 RED INALÁMBRICA

Para la configuración de la red inalámbrica, tendremos un único punto de configuración, que será nuestro Controlador Wifi, según indicamos en la arquitectura elegida para el proyecto:

Todos los puntos de acceso inalámbricos recibirán las solicitudes de conexión que retransmitirán a su controlador. Este controlador será, realmente, el cliente de nuestro sistema de Radius, y es en él en el que configuraremos los parámetros tales como la clave compartida.

El procedimiento para la configuración del Controlador será muy parecido a la red cableada dado que tendremos, primero, que configurar los parámetros generales del servidor Radius y, seguidamente, configurar los SSID a los que se aplique una validación en Radius. Los pasos son:

- 1- Configuración de los parámetros generales de Radius.
- 2- Generación de un perfil de seguridad.
- 3- Configuración del ESS.

Configuración de los parámetros generales de Radius:

1. Nos conectamos al modulo de administración del controlador Wifi.
2. Nos situamos en el apartado "Configuration", subapartado Security.
3. En la opción de Radius damos de alta los servidores de NPS, usando la clave compartida asignada:
 - a. Pulsamos en "Add".
 - b. Introducimos la IP del servidor Radius y clave compartida.
 - c. Dejamos el resto por defecto.

Mostramos la configuración de este apartado en la siguiente imagen:

RADIUS Profile Table - Update

<u>Summary Selection</u> Profile Name	se41sww05			
Description	<input type="text"/> Enter 0-128 chars.			
RADIUS IP	<input type="text" value="10"/>	<input type="text" value="232"/>	<input type="text" value="1"/>	<input type="text" value="180"/>
RADIUS Secret	<input type="password" value="••••••"/>			
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-65535]		
MAC Address Delimiter	Hyphen (-) ▾			
Password Type	Shared Key ▾			

ILUSTRACIÓN 24 CONFIGURACIÓN RADIUS WIFI

Este procedimiento lo realizaremos también para agregar el segundo controlador.

Tras este proceso, ya podemos realizar la configuración de un perfil de seguridad que usará la validación en los servidores NPS.

Generación de un perfil de seguridad.

Para generar un SSID realizamos los siguientes pasos:

1. Nos conectamos al módulo de administración del controlador Wifi.
2. Nos situamos en el apartado “Configuration”, subapartado Security.
3. En la opción “Profile”, generamos un perfil de acceso para acceso a NPS.
 - a. Pulsamos en ADD y registramos los valores necesarios.
 - b. Usaremos como protocolo cifrado WPA2, que usará AES como sistema de cifrado, mucho más seguro que WEP y TKIP.
 - c. Situamos en “primary” y “secondary Radius profile name” los servidores configurados anteriormente como servidores de NPS.

Mostramos la configuración de este apartado en la siguiente imagen:

Security Profile Table - Update	
<u>Summary Selection</u> Profile Name	Corporativo
L2 Modes Allowed	<input type="checkbox"/> Clear <input type="checkbox"/> 802.1x <input type="checkbox"/> Static WEP keys <input type="checkbox"/> WPA <input type="checkbox"/> WPA PSK <input checked="" type="checkbox"/> WPA2 <input type="checkbox"/> WPA2 PSK <input type="checkbox"/> MIXED <input type="checkbox"/> MIXED_PSK
Data Encrypt	<input type="checkbox"/> WEP64 <input type="checkbox"/> WEP128 <input type="checkbox"/> TKIP <input checked="" type="checkbox"/> CCMP-AES <input type="checkbox"/> CCMP/TKIP <input type="checkbox"/> Clear
Primary RADIUS Profile Name	se41sww05 ▾
Secondary RADIUS Profile Name	se41sww10 ▾

ILUSTRACIÓN 25 PERFIL DE SEGURIDAD WIFI

Finalmente, configuramos el SSID para dar servicio a nuestra red.

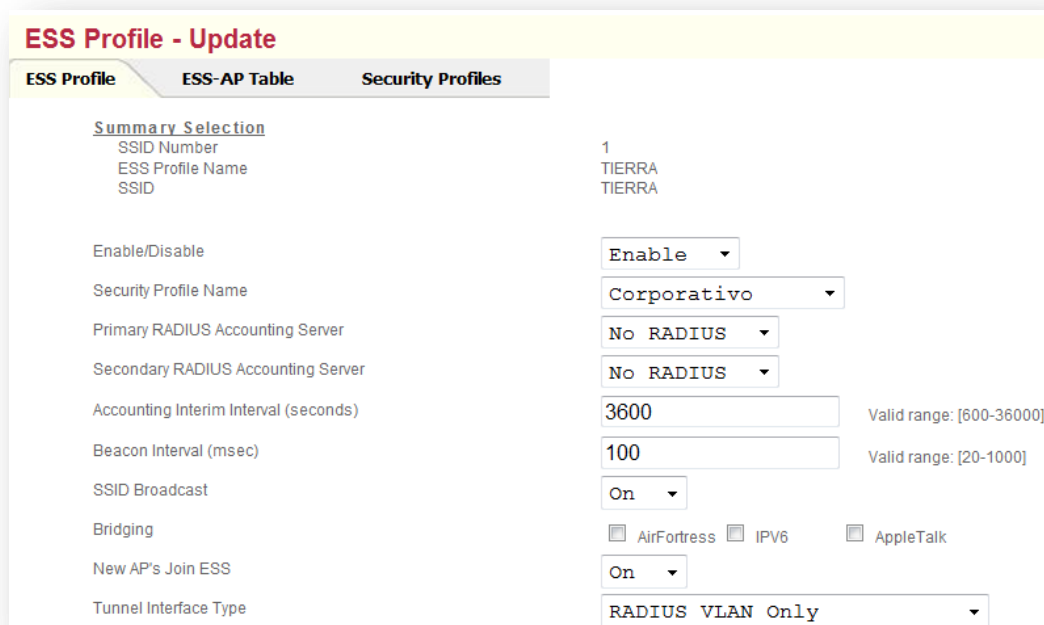
Configuración del ESS.

El tipo de arquitectura usada ha sido Extended Service Set (ESS) lo que nos garantiza que un mismo SSID será replicado por medio de todos nuestros puntos de acceso con el mismo identificador.

Para configurarlo realizamos los siguientes pasos:

1. Nos conectamos al módulo de administración del controlador Wifi.
2. Nos situamos en el apartado “Configuration”, subapartado Wireless.
3. En la opción “ESS”, generamos los SSID necesarios.
 - a. Pulsamos en ADD y registramos los valores necesarios.
 - b. Situamos como “Security Profile Name” el perfil de seguridad generado anteriormente.
 - c. En el SSID no es necesario volver a configurar los parámetros de Radius ya que usará los del perfil de seguridad.
 - d. En “Tunnel Interface Type” indicaremos que sea el servidor de Radius quien asigne la VLAN mediante la opción: “Radius VLAN Only”

Mostramos la configuración de este apartado en la siguiente imagen:



ESS Profile	ESS-AP Table	Security Profiles
Summary Selection		
SSID Number	1	
ESS Profile Name	TIERRA	
SSID	TIERRA	
Enable/Disable	Enable	
Security Profile Name	Corporativo	
Primary RADIUS Accounting Server	No RADIUS	
Secondary RADIUS Accounting Server	No RADIUS	
Accounting Interim Interval (seconds)	3600	Valid range: [600-36000]
Beacon Interval (msec)	100	Valid range: [20-1000]
SSID Broadcast	On	
Bridging	<input type="checkbox"/> AirFortress <input type="checkbox"/> IPV6 <input type="checkbox"/> AppleTalk	
New AP's Join ESS	On	
Tunnel Interface Type	RADIUS VLAN Only	

ILUSTRACIÓN 26 PERFIL DE ESS WIFI

Con la configuración realizada a nivel del Controlador, el modo de funcionamiento de los AP quedará supeditado a lo que indiquen los servidores NPS. De forma que, una vez asociado los clientes al SSID, el controlador

reenviará sus credenciales a los servidores NPS y estos, mediante sus políticas, concederán, o no, acceso e indicarán en qué VLAN hay que situarlos. Una vez en la VLAN, podremos comenzar a usar todos los servicios de Red que se permitan en dicha subred. Procedemos así con la parte final, y más importante, de la configuración: los servidores NPS.

4.4 CONFIGURACIÓN DE RADIUS

4.4.1 ARQUITECTURA DE RED

El servidor de Radius, elegido para nuestro proyecto, es el servidor NPS de Microsoft Corp. Dicho servidor lo implementaremos bajo el sistema operativo Windows Server, recomendado para esta tarea. Es decir, nuestro objetivo final de la instalación es contar con los siguientes recursos:

- Windows Server 2008 R2 Enterprise.
- Servidor de directiva de redes Microsoft NPS. Versión 6.1

Para conseguir tener redundancia en nuestro entorno, realizaremos la instalación de 2 servidores de NPS. Los conectaremos directamente a los switches centrales, que estarán redundados a su vez; así garantizaremos que la configuración de políticas esté siempre disponible mientras uno de los switches centrales esté activo.

Podemos describir la situación final con la siguiente imagen:

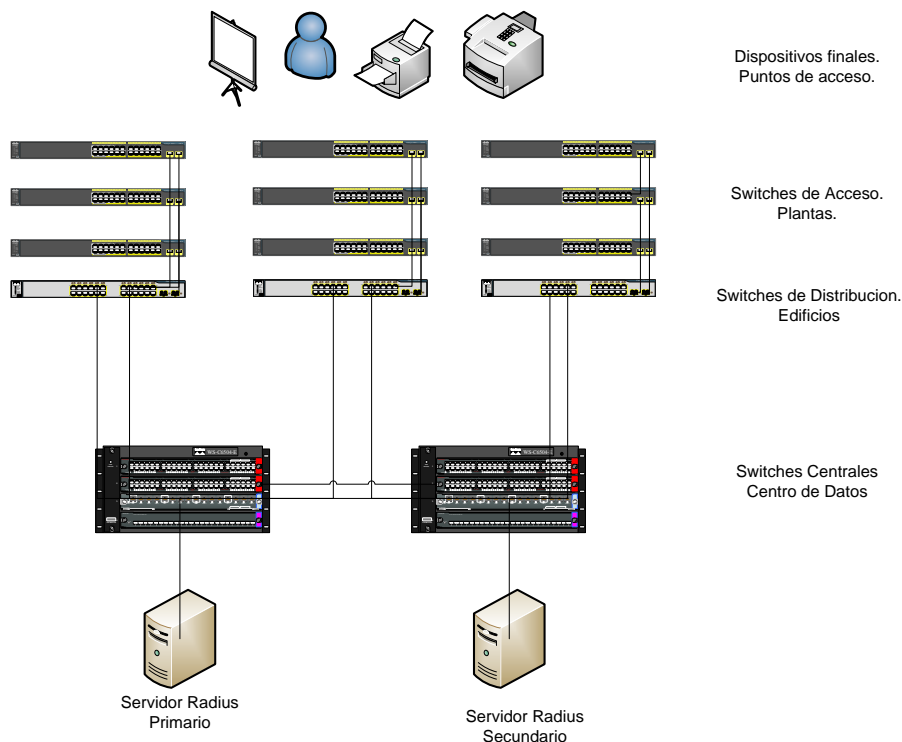


ILUSTRACIÓN 27 ARQUITECTURA DE SWITCH

Este esquema de arquitectura es el recomendado para redes tipo campus, en la cual tendremos 3 capas antes de que un dispositivo cliente se conecte a la red. De esta forma, podemos adquirir distinta tecnología en función del nivel que estemos configurando: en la capa central tendremos conmutadores de alto rendimiento y, sin embargo, en la capa de acceso podremos utilizar switches con un nivel menor de complejidad.

4.4.2 INSTALACIÓN DEL SERVICIO

Partiremos de una situación en la cual ya disponemos de un servidor con Windows Server 2008 instalado.

Una vez con el sistema operativo en línea, procederemos, primero, a instalar el servicio de NPS y después realizaremos su configuración inicial.

Para su instalación seguimos la guía de configuración que nos indica los siguientes pasos:

1. En tareas de configuración inicial, Personalizar este servidor, seleccionamos agregar funciones para iniciar el asistente de instalación del acceso y directiva de redes.
De no tener activa la configuración inicial, podemos, desde el menú de administración del servidor, revisar sus funciones o roles. En el caso de que no tengamos los servicios de acceso y directivas de redes, agregaremos esta función.
2. En Seleccionar funciones de servidor, en Funciones, seleccionamos Servicios de acceso y directivas de redes y, a continuación, clic en Siguiente.

Mostramos la configuración de este apartado en la siguiente imagen:

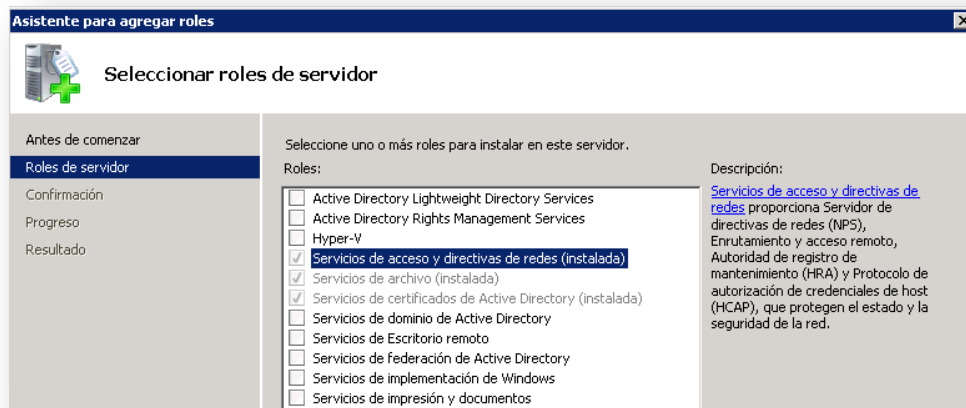


ILUSTRACIÓN 28 ROLES SERVIDOR

Esta tarea la realizaremos en ambos servidores, sin distinción de roles a usar.

Con este servidor podremos configurar 3 tipos de servicios:

- Servidor de políticas de NAP.
- Servidor RADIUS para RAS o conexiones VPN.
- Servidor RADIUS para 802.1X cableada e inalámbricas.

En nuestro caso, utilizaremos el servidor para el último tipo de servicios. Es decir, como servidor de políticas para 802.1X

4.4.3 AUTORIZACIÓN EN EL AD.

Dado que el servidor se apoyará en la base de datos de cuentas de equipos y usuarios de Microsoft, Directorio Activo, tendremos que proceder a la autorización de este servicio en nuestra red.

Para realizar esta tarea, tendremos que disponer de suficientes privilegios en el Dominio. En caso de no disponer de un usuario con estos requisitos, tendremos que solicitar que se realice esta tarea por las personas del departamento de TI encargadas de las mismas.

Existen varias formas de realizar este registro:

- Desde la consola de NPS.
- Usando el comando netsh.
- Mediante la consola de equipos y usuarios del Directorio Activo.

La forma más habitual de realizarlo es mediante la propia consola del NPS, y los pasos a seguir, en este caso, son:

- Iniciar sesión en el servidor NPS, empleando una cuenta que tenga credenciales administrativas para el dominio.
- Abrir la consola de NPS.
- Con el botón secundario en NPS (local), a continuación, seleccionamos Registrar servidor en Active Directory. Cuando aparezca el cuadro de diálogo Registrar servidor de directivas de redes en Active Directory, aceptaremos.

Mostramos la configuración de este apartado en la siguiente imagen:

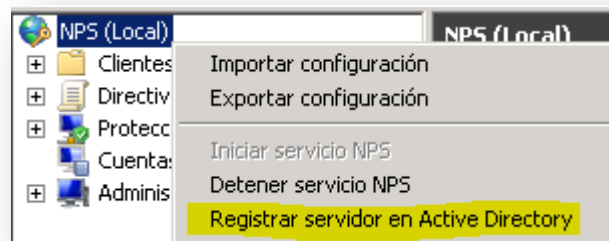


ILUSTRACIÓN 29 REGISTRO SERVIDOR

Un servidor RADIUS, registrado en AD, tiene acceso a la información de cuentas de usuario y puede comprobar las credenciales de autenticación de acceso a la red. Si las credenciales de los usuarios se autentican, y el intento de conexión se autoriza, el servidor RADIUS autoriza el acceso de los usuarios sobre la base de condiciones que se especifican y, a continuación, se registra el acceso de dicha conexión registro del servidor, de forma que podríamos auditar estos servicios. El uso de RADIUS permite a la red que pueda controlar los accesos mediante la autenticación del usuario, su autorización, y su registro en un punto central que serían nuestros servidores de Radius, en vez de mantener toda esta configuración independiente a cada switch. De esta forma, como ya vimos, la movilidad y seguridad están garantizadas por toda nuestra red.

4.4.4 CONFIGURACIÓN DE CLIENTES RADIUS.

Si recordamos la arquitectura de Radius, los clientes 802.1X no son los dispositivos finales, sino las máquinas encargadas de realizar la conexión a la red de datos, en nuestro caso los switches y controladores wifi. Lo representamos en la siguiente imagen:

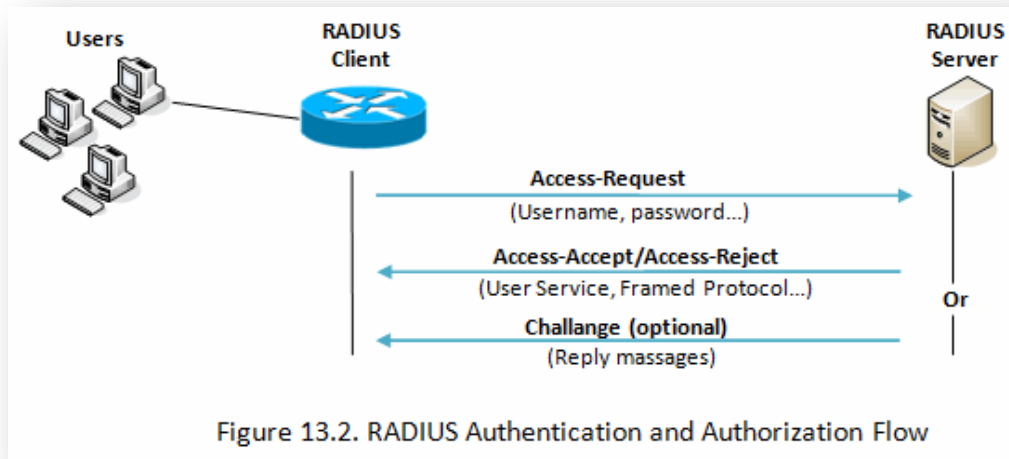


ILUSTRACIÓN 30 PROCESO DE AUTENTICACIÓN

Estos clientes autorizarán la conexión a la Red en base a la asignación de políticas establecidas en el Radius. Para evitar un uso no autorizado de estas comprobaciones, podemos establecer una palabra de paso, llamada secreto compartido, entre cliente Radius y Servidor NPS.

La filosofía de esta clave es establecer una contraseña única entre estos dos equipos, por lo tanto podemos llegar a establecer esta comunicación de forma individual por cada cliente usando siempre contraseñas distintas. Sin embargo trataremos de definir una clave común a todos nuestros clientes para facilitarnos la gestión de estos sistemas. En caso contrario deberíamos tener un repositorio donde guardar todas estas contraseñas individuales, lo cual dificultaría la gestión posterior de todo el entorno.

A la hora de generar el secreto compartido, podemos realizarlo de 2 formas:

- Manual. Se decide y se configura por medio de la consola.
- Automático. El propio servidor NPS genera una clave automática que después habrá que configurar en el cliente.

En nuestro caso, realizaremos la configuración manual, para establecer una única clave para todos los clientes. Con el fin de facilitar esta tarea, además, crearemos una plantilla de configuración de la clave compartida, de forma que, cada vez que agreguemos un cliente nuevo, podamos seleccionar esta plantilla y la configuración de la clave sea automática.

Generamos la plantilla.

Dentro de la consola de NPS, seguimos los siguientes pasos:

1. Administración de plantillas.
2. Secretos compartidos, botón derecho -> Nuevo.

Mostramos la configuración de este apartado en la siguiente imagen:

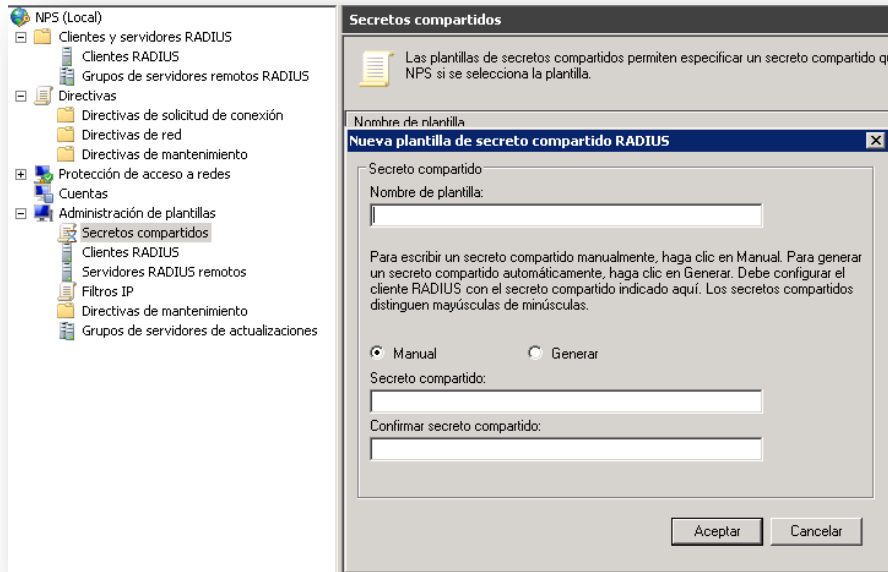


ILUSTRACIÓN 31 PLANTILLA SECRETO COMPARTIDO

Establecemos un nombre para la plantilla, y configuramos manualmente nuestro secreto compartido.

Ahora procedemos a agregar a un cliente Radius, en el cual usaremos la plantilla creada anteriormente. Dentro de la consola de NPS, seguimos los siguientes pasos:

1. Clientes y servidores RADIUS
2. Clientes RADIUS, botón derecho -> Nuevo cliente
 - a. Nombre y descripción: Nombre de equipo.
 - b. Dirección IP: Dirección del equipo.
 - c. Secreto compartido. Elegimos plantilla.
3. Opciones avanzadas
 - a. Nombre de proveedor: RADIUS standard

Mostramos la configuración de este apartado en la siguiente imagen:

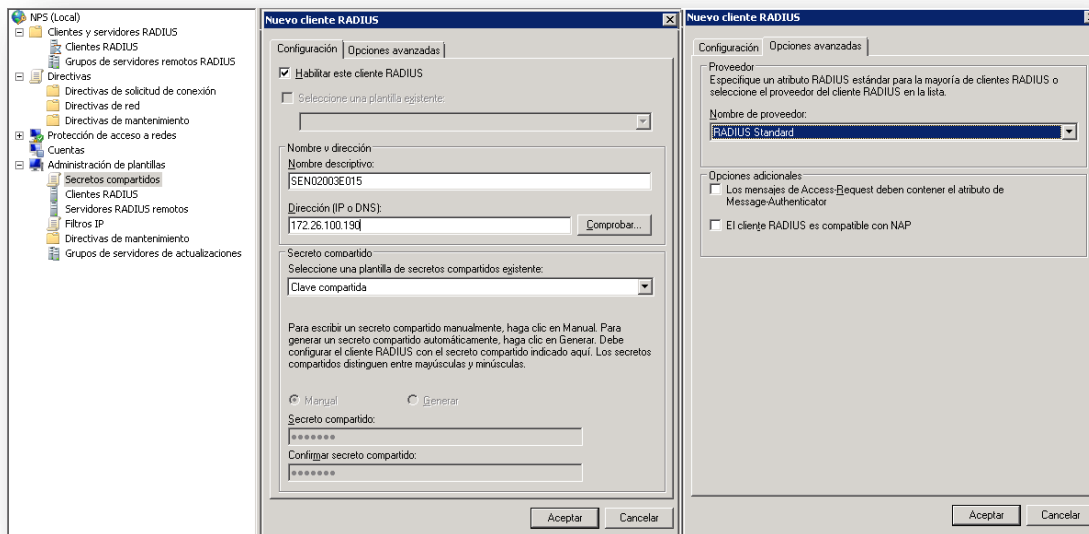


ILUSTRACIÓN 32 RADIUS, CONFIGURACIÓN CLIENTE

Los datos más importantes en esta configuración son tanto la IP del cliente como el tipo de proveedor. En este último detalle, debemos indicar “RADIUS standard”, dado que, tanto los equipos Cisco, como los controladores de Meru son totalmente compatibles con el estándar.

Esta parte de la configuración puede ser muy tediosa, por lo cual podemos combinar la configuración básica inicial de la consola grafica, con el uso del editor de comandos en modo texto con el comando “netsh”, vemos un ejemplo de su uso en la siguiente imagen:

```
C:\Windows\system32>netsh nps add client name=SEN02003E014 address=172.26.100.190 sharedsecret=¡ruts!b
Aceptar
```

ILUSTRACIÓN 33 COMANDO NETSH

El editor de comandos netsh no nos permite el uso de plantillas, pero sí podemos confeccionar un script. Para ello, podemos usar una hoja de cálculo donde pongamos todos los comandos en varias filas y anexar los nombres y direcciones ip de los equipos clientes en las restantes. Una vez confeccionada, sólo nos quedará copiar y pegar en el intérprete de comandos del servidor.

En nuestro proyecto hemos usado:

	A	B	C	D	E
1	netsh nps add client name=	212679T	address=	172.26.100.100	sharedsecret=¡ruts!b
2	netsh nps add client name=	212680A	address=	172.26.100.101	sharedsecret=¡ruts!b
3	netsh nps add client name=	273571T	address=	172.26.100.102	sharedsecret=¡ruts!b
4	netsh nps add client name=	273570M	address=	172.26.100.103	sharedsecret=¡ruts!b
5	netsh nps add client name=	273569F	address=	172.26.100.104	sharedsecret=¡ruts!b
6	netsh nps add client name=	273564w	address=	172.26.100.105	sharedsecret=¡ruts!b
7	netsh nps add client name=	273565D	address=	172.26.100.106	sharedsecret=¡ruts!b
8	netsh nps add client name=	283090O	address=	172.26.100.110	sharedsecret=¡ruts!b
9	netsh nps add client name=	283091V	address=	172.26.100.111	sharedsecret=¡ruts!b
10	netsh nps add client name=	277093Z	address=	172.26.100.112	sharedsecret=¡ruts!b
11	netsh nps add client name=	242421F	address=	172.26.100.113	sharedsecret=¡ruts!b
12	netsh nps add client name=	242420Y	address=	172.26.100.114	sharedsecret=¡ruts!b
13	netsh nps add client name=	276991N	address=	172.26.100.115	sharedsecret=¡ruts!b
14	netsh nps add client name=	283085F	address=	172.26.100.116	sharedsecret=¡ruts!b
15	netsh nps add client name=	283097L	address=	172.26.100.117	sharedsecret=¡ruts!b
16	netsh nps add client name=	249520M	address=	172.26.100.118	sharedsecret=¡ruts!b
17	netsh nps add client name=	249521T	address=	172.26.100.119	sharedsecret=¡ruts!b
18	netsh nps add client name=	296461L	address=	172.26.100.12	sharedsecret=¡ruts!b
19	netsh nps add client name=	249522A	address=	172.26.100.120	sharedsecret=¡ruts!b
20	netsh nps add client name=	249523H	address=	172.26.100.121	sharedsecret=¡ruts!b
21	netsh nps add client name=	283084Y	address=	172.26.100.122	sharedsecret=¡ruts!b
22	netsh nps add client name=	249524O	address=	172.26.100.123	sharedsecret=¡ruts!b
23	netsh nps add client name=	249525V	address=	172.26.100.124	sharedsecret=¡ruts!b
24	netsh nps add client name=	249526C	address=	172.26.100.125	sharedsecret=¡ruts!b
25	netsh nps add client name=	283082K	address=	172.26.100.126	sharedsecret=¡ruts!b
26	netsh nps add client name=	283083R	address=	172.26.100.127	sharedsecret=¡ruts!b
27	netsh nps add client name=	283081D	address=	172.26.100.128	sharedsecret=¡ruts!b
28	netsh nps add client name=	283089H	address=	172.26.100.129	sharedsecret=¡ruts!b
29	netsh nps add client name=	HUVR5298	address=	172.26.100.13	sharedsecret=¡ruts!b
30	netsh nps add client name=	283092C	address=	172.26.100.130	sharedsecret=¡ruts!b
31	netsh nps add client name=	249534G	address=	172.26.100.131	sharedsecret=¡ruts!b
32	netsh nps add client name=	2960-G14	address=	172.26.100.132	sharedsecret=¡ruts!b

ILUSTRACIÓN 34 HOJA DE CLIENTES

4.4.5 REDUNDANCIA.

La redundancia de un sistema se puede medir por muchas variables del entorno: la propia arquitectura hardware, la red, los servicios, etc. En este apartado, nos centraremos sólo en la redundancia a nivel del servicio, dado que los demás apartados se encontrarán ya supervisados y controlados por el personal de TI.

Para velar por la salvaguarda de la información, y la redundancia del sistema, indicamos en la arquitectura inicial que se instalarían 2 servidores NPS que gestionarían todas las conexiones de los clientes. Procederemos a gestionar esa sincronización entre ambos.

La forma de configuración de esta redundancia se basa en la capacidad de los clientes de poder tener configurados más de un servidor Radius. Es una forma de trabajo similar a la configuración DNS en los clientes, en la cual sólo se interroga a los equipos secundarios, en caso de que el primario deje de dar servicio. Es decir, la configuración estará siempre actualizada y sincronizada en todos los servidores NPS, de forma que ante la caída de un servidor el otro pueda dar el mismo servicio.

Previamente, seleccionaremos uno de los dos servidores NPS como principal. Este rol será asignado, por nuestra parte, en base, por ejemplo, a una mayor capacidad de proceso de uno de los dos equipos, mayor ancho de banda, etc. En caso de igualdad de todos los términos elegidos, simplemente elegiremos uno de ellos y mantendremos nuestra selección todo el proyecto.

Una vez seleccionados servidor principal y secundario, nos basaremos, una vez más en el entorno de línea de comandos, de forma que podemos acceder a la configuración, exportarla e importarla, además de poder hacer uso de la programación de tareas para esta labor.

EXPORTACIÓN.

El primer paso para la sincronización de configuraciones será la exportación de toda la configuración de NPS en el servidor principal.

El comando utilizado será del subconjunto de comandos de la interfaz netsh, y realizará un volcado a XML de toda la configuración del servicio.

Para simplificar el proceso, podemos realizar esta exportación directamente sobre el servidor secundario, donde tengamos permisos de escritura, usando por ejemplo una ruta UNC sobre un directorio.

El comando a lanzar desde el intérprete de comandos es:

```
netsh nps export filename = \\se41sww10\replica\ConfigNPS.xml exportPSK = YES
```

La ruta elegida, y el nombre del archivo, pueden variar según nuestro criterio; la opción exportPSK nos salvará también las claves entre cliente y servidor. Además, gracias a que el resultado es un fichero XML, podemos tener la posibilidad de editarlo y variar la configuración que veamos necesaria para después proceder a importarla.

IMPORTACIÓN.

El procedimiento de importación será similar al de exportación; mismo procedimiento pero distinta línea de comandos.

En este caso, si no hemos de modificar nada en el fichero XML, generado en el primer paso, procederemos a realizar la importación.

```
netsh nps import filename = "C:\Radius Script\conf_nodo1\ConfigNPS.xml"
```

De esta forma, tendremos toda la configuración del servidor NPS importada en el servidor secundario. Llegados a este punto, podemos, como añadido, programar dichas tareas para evitar su tarea manual. Para ello, en el servidor principal, programaremos la exportación y a una hora posterior la importación en el secundario.

4.4.6 CONFIGURACIÓN DE POLÍTICAS.

Antes de configurar las políticas del sistema, debemos conocer claramente el funcionamiento del motor de políticas de NPS.

Su funcionamiento está basado en un sistema similar al de colas, en la cual cada política tiene un determinado orden, que le asigna su prioridad de ejecución. Secuencialmente el sistema va revisando las políticas configuradas de forma ordenada; una vez que localiza que una determinada política se aplica a un perfil, el sistema termina la evaluación, ejecuta la política y devuelve los resultados al cliente Radius.

En caso de que ninguna política sea aplicable, se puede establecer una por defecto.

Dentro de las políticas, tenemos a su vez varios tipos de políticas:

- Directivas de solicitud de conexión.
- Directivas de red.
- Directivas de mantenimiento.

En nuestro caso sólo las dos primeras serán de aplicación, dado que la tercera sólo se usa en caso de añadir, a nuestro sistema, un sistema de NAP.

DIRECTIVAS DE SOLICITUD DE CONEXIÓN

Mediante este tipo de políticas estableceremos qué servidores Radius llevan a cabo la autenticación, autorización y administración de las solicitudes de acceso recibidas desde los clientes de NPS. Es decir, validan las solicitudes de acceso a la red y determinan dónde se realiza esta validación.

En nuestro caso, tendremos que realizar estas tareas sobre el propio servidor Radius, dado que no utilizaremos un servicio Radius ajeno a nuestra red. Para este cometido, primero tendremos que definir qué tipos de conexiones controlaremos en este proyecto que, tal como habíamos indicado a los inicios del proyecto, serán las conexiones Ethernet cableadas y Wifi. Por lo tanto será para estos dos perfiles para los que configuraremos nuestras reglas.

Procedemos a configurar la solicitud de conexión desde la red cableada:

Dentro de la consola NPS, en directivas de solicitud de conexión, generamos una nueva política, la llamaremos "Conexiones Ethernet".

En la primera ventana de configuración, tendremos que especificar “unspecified”, dado que no debemos especificar el tipo de servidor de acceso a la red, pues en nuestro caso cualquier switch podrá realizarnos solicitudes de acceso. El campo de esta opción tomar otros valores en función de que apliquemos otros servicios a nuestro NPS; por ejemplo servidor de acceso para conexiones VPN. Vemos en la siguiente imagen el acceso a estas opciones:

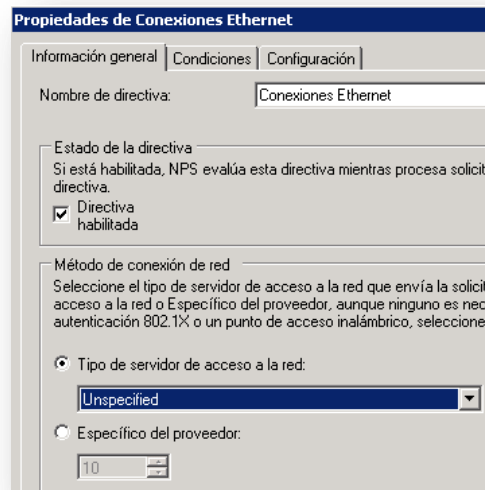


ILUSTRACIÓN 35 PROPIEDADES CONEXIONES ETHERNET

Lo siguiente a configurar es el apartado: “Condiciones”. Mediante este apartado, revisamos el mensaje recibido por nuestro servidor Radius y evaluamos si cumple los requisitos de esta directiva. En nuestro caso queremos que todas las solicitudes de conexión reenviadas por nuestros switches sean evaluadas por nuestro servidor. Para ello agregaremos la condición para que esta política atienda a todos los mensaje recibidos de este tipo.

Para ello tendremos que especificar la condición del tipo de puerto NAS, el cual evalúa el tipo de medio utilizado por el cliente de acceso. Entre los ejemplos se encuentran: líneas telefónicas analógicas (conocidas como asincrónicas), ISDN (RDSI), túneles o redes virtuales privadas (conocidas como virtuales), conexión inalámbrica IEEE 802. 11 y el que usaremos en nuestro caso:Switches Ethernet.

Para ellos agregamos una nueva condición, y elegimos: “Tipo de puerto NAS”.

Mostramos la configuración de este apartado en la siguiente imagen:

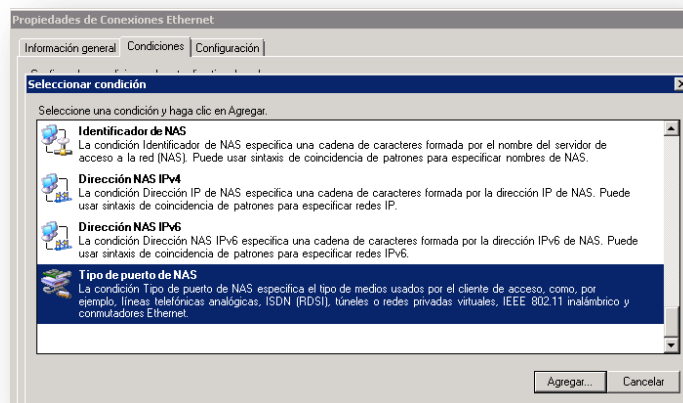


ILUSTRACIÓN 36 CONDICIONES, TIPO PUERTO NAS

En nuestro caso el tipo de conexión que nos llegará, desde este tipo de cliente, será conexión túnel 802.1X por Ethernet; elegimos esta opción.

Dado que los clientes ya los hemos limitado en el apartado de clientes, vemos que, a medida que vamos configurando las directivas, filtramos también, en los distintos niveles, todas las comunicaciones entrantes y sus condiciones.

En la siguiente imagen vemos la opción elegida para este tipo de cliente:

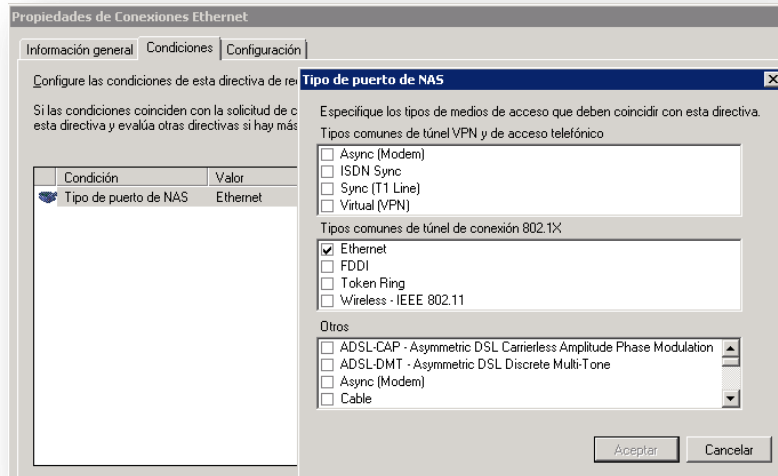


ILUSTRACIÓN 37 CONDICIONES, TIPO DE TÚNEL

El último paso de esta configuración será indicar que estas solicitudes se procesarán en este servidor. Para ello, en "Configuración" nos cercioraremos de que, en "Autenticación", indicamos que las solicitudes se procesan en este servidor. Resaltamos este detalle en la siguiente imagen:

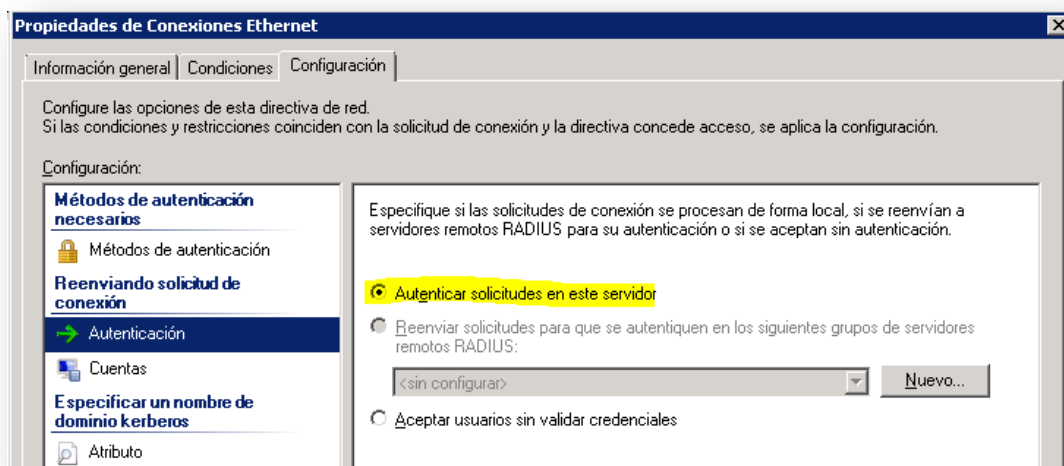


ILUSTRACIÓN 38 CONFIGURACIÓN, AUTENTICACIÓN

Con esto tendríamos finalizada la configuración de esta directiva y con ello procesaríamos todas las peticiones enviadas desde nuestros Clientes de la red cableada, es decir todos los switches configurados como clientes.

Procedemos a configurar la solicitud de conexión desde la red Wifi:

Para este tipo de conexiones tenemos que tener en cuenta, antes de configurar, un detalle de nuestra arquitectura en este apartado.

Si recordamos la arquitectura elegida en este apartado, el sistema que vamos a utilizar será un tipo de funcionamiento en el cual nuestros AP sólo tendrán comunicación con el Controlador Wifi, el cual redirigirá todo el tráfico hacia la red.

Dentro de este tráfico también incluimos toda la validación Radius, por lo tanto la configuración de la directiva de acceso no la realizaremos directamente sobre los puntos de acceso Wifi, en este caso solo intervendrá el Controlador Wifi.

Esta forma de funcionamiento la configuraremos de la siguiente forma:

Generamos nuevamente una directiva de acceso, al igual que en el anterior caso no especificamos el tipo de servidor de acceso a la red.

Mostramos la configuración de este apartado en la siguiente imagen:

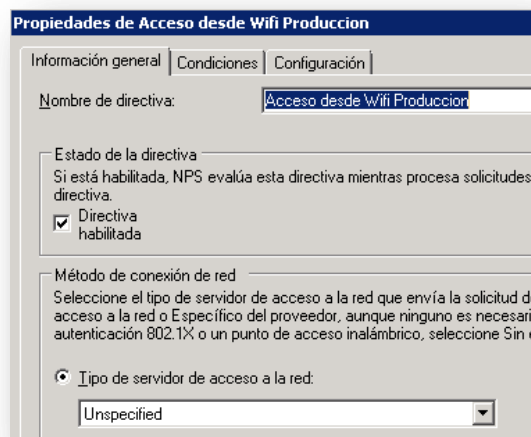


ILUSTRACIÓN 39 PROPIEDADES CONEXIÓN WIFI

Procedemos a configurar las “Condiciones”, es en este apartado donde definimos la forma de funcionar de nuestra arquitectura Wifi.

Agregamos una nueva condición y, en este caso, la definimos en función de la dirección del cliente de acceso. Esta dirección será de nuestro controlador Wifi. En nuestro caso tendremos un cluster de controladores Wifi que, de cara a la red, se publicarán con una única dirección hacia ella. Vemos en la siguiente imagen la opción a elegir:

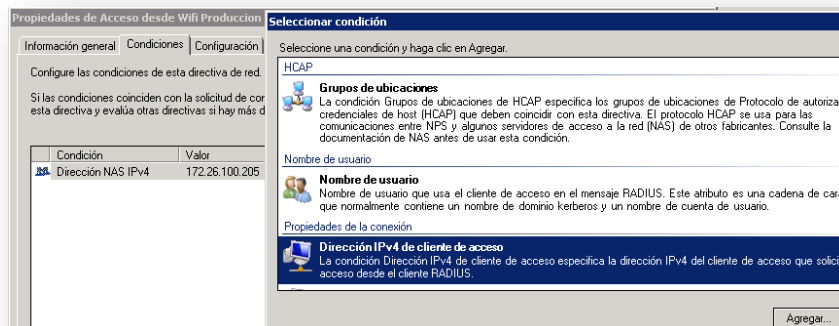


ILUSTRACIÓN 40 CONDICIONES, CONEXIÓN WIFI

De esta forma podemos fácilmente escalar hacia una solución con múltiples controladores Wifi independientes, si se diera el caso.

Finalmente, el último paso de esta configuración será indicar que estas solicitudes se procesen en este servidor. Para ello, en “Configuración”, nos cercioraremos de que, en “Autenticación”, indicamos que las solicitudes se procesan.

De esta forma ya estarían configurados tanto las conexiones de clientes Wifi, provenientes de su Controlador, como las peticiones de los switches de red, que serán analizadas en nuestros servidores Radius.

DIRECTIVAS DE RED.

Las directivas de red son la parte más importante de nuestra configuración de Radius. En este apartado, configuraremos las acciones que realizaremos frente a las solicitudes de acceso reenviadas por nuestros clientes.

Para adaptar las políticas, primero tenemos que revisar si cumplimos con todos los requisitos de los perfiles de acceso que vamos a controlar. Realizando un repaso sobre los perfiles de acceso (PAC 2 – Adaptación de Vlan), concluimos que los tipos de acceso son:

- Red Administrativa.
- Salas Públicas. Caso 1.
- Salas Públicas. Caso 2.
- Invitados.
- Sin dominio.

Tal como vimos, la información de las cuentas de usuarios estará apoyada sobre la base de datos de nuestro Directorio Activo; por tanto, estas políticas estarán apoyadas sobre las tareas de configuración de este servicio que realizamos en el apartado de configuración del Directorio Activo.

Sabemos que el modo de funcionamiento del motor de política nos limita, ya que sólo se ejecutará la primera política de acceso que cumpla los requisitos indicados. Es por ello que, previamente a la configuración de las políticas, tendremos que realizar el diagrama de flujo que deberá seguir nuestro sistema. Lo indicamos a continuación.

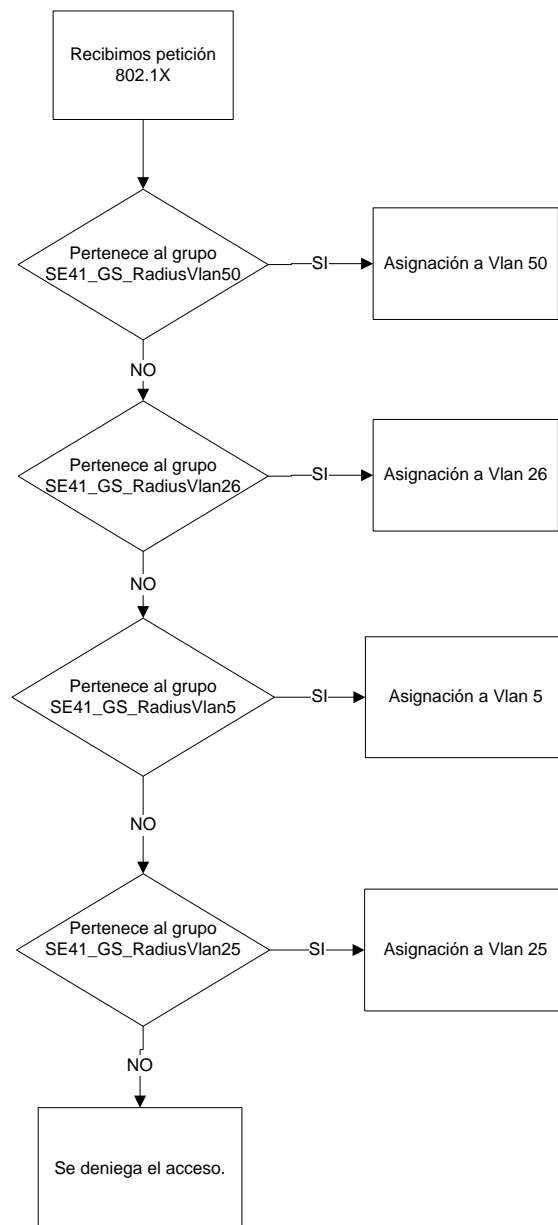


ILUSTRACIÓN 41 DIAGRAMA DE POLÍTICAS

Procedemos a realizar las configuraciones de políticas siguiendo el diagrama de flujo.

Incluiremos una descripción detallada de las 2 primeras políticas, el resto seguirán el mismo procedimiento, por lo que solo será indicado:

Vlan50

El primer perfil que nos encontramos es el de la red “Sin dominio – Vlan 50”, dicha red solo requiere que el equipo pertenezca al grupo “SE41_GS_RadiusVlan50”. Los pasos a seguir para agregar dicha política son:

1. En el administrador de NPS, sobre Directivas de Red, pulsamos botón derecho ratón -> Nuevo. Introducimos el nombre de la política; en nuestro caso: Equipos Vlan50.

Mostramos la configuración de este apartado en la siguiente imagen:

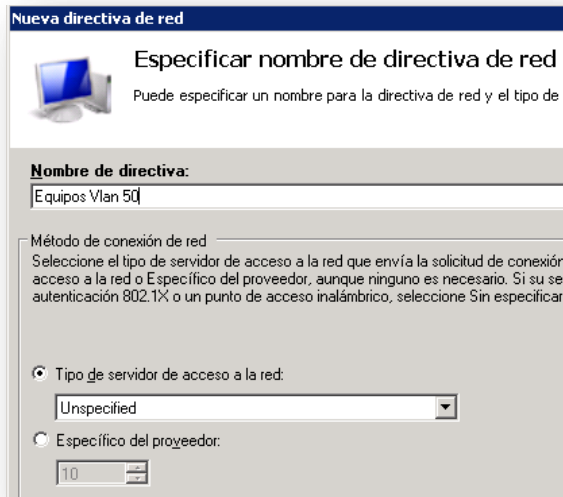


ILUSTRACIÓN 42 DIRECTIVA VLAN50

- El siguiente paso nos solicita las condiciones que ha de tener el equipo para cumplir esta política. Indicamos que ha de pertenecer al grupo: SE41_GS_RadiusVlan50. Para ello pulsamos en “Agregar” y seleccionamos “Grupos de Windows”. Localizamos el grupo en cuestión y lo agregamos. De esta forma la única condición que nos debe quedar es que pertenezca al grupo que hemos seleccionado.

Mostramos la configuración de este apartado en la siguiente imagen:

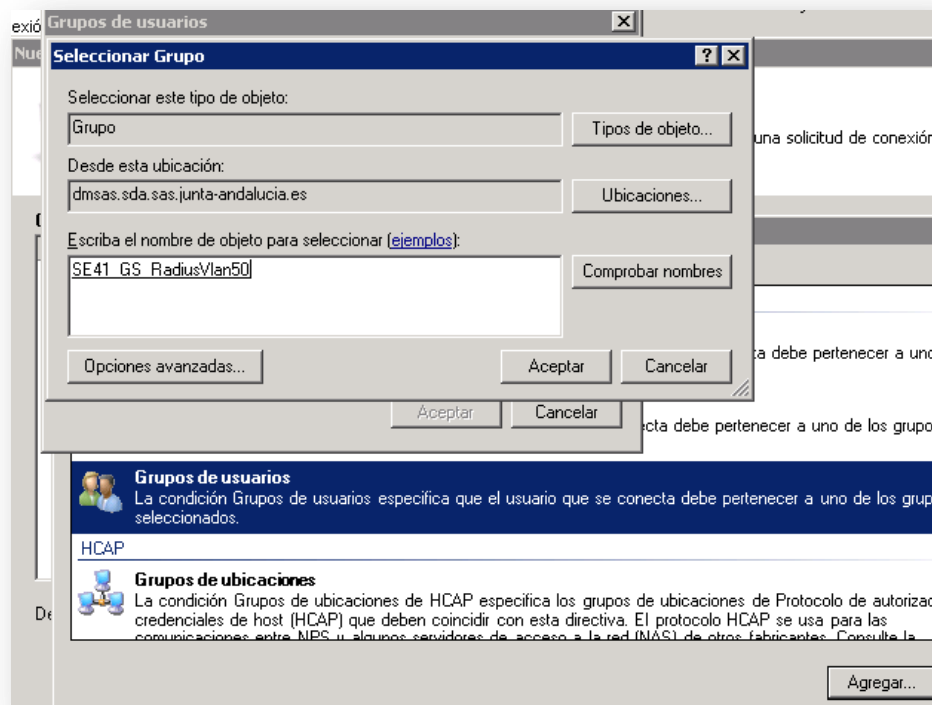


ILUSTRACIÓN 43 GRUPOS DIRECTIVA VLAN50

3. En la siguiente pantalla indicamos que concedemos el acceso a dicha petición.

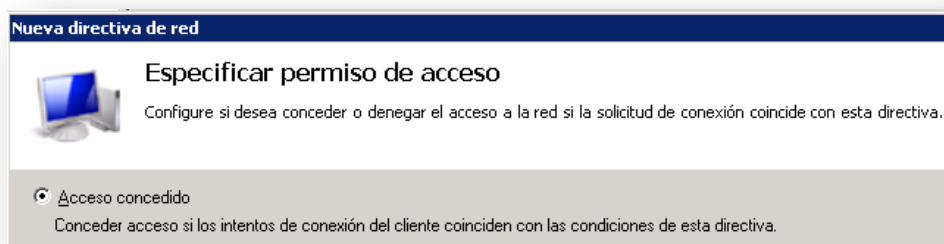


ILUSTRACIÓN 44 PERMISOS DIRECTIVA VLAN50

4. Elegimos el método de encriptación. Estas máquinas se apoyan en el servicio de los switches de MAB, el cual permite, tras un intento fallido de autenticación por 802.1X, enviar como credenciales de usuario y contraseña su dirección MAC. Por ello podemos usar un método de cifrado básico en el envío de dichos valores, ese método será PAP.
5. En el apartado de restricciones no indicamos ninguna, dado que los clientes que aceptarán las conexiones de estos equipos ya se establecieron en las políticas de “Directivas de solicitud de conexión”.
6. El paso final será situar el interfaz de red en la Vlan correspondiente.
 - a. Framed protocol: PPP
 - b. Service-Type: Framed
 - c. Tunnel-Medium-Type: 802 (includes all 802 media plus Ethernet canonical format)
 - d. Tunnel-Pvt-Group-ID: 5
 - e. Tunnel-Type: Virtual LANs

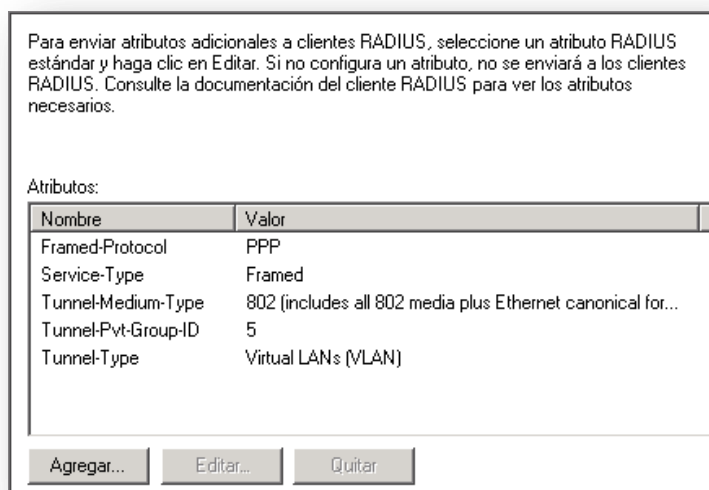


ILUSTRACIÓN 45 ATRIBUTOS DIRECTIVA VLAN50

7. Finalmente obtenemos un resumen de la configuración final que se ha realizado, revisamos los valores y finalizamos el asistente.

Vlan 26

Procedemos a realizar la configuración de la siguiente Vlan en función del diagrama de flujo, en nuestro caso la Vlan26, que pertenece al perfil de Red de Invitados.

Los pasos a seguir son similares a la configuración de la Vlan50, los enumeramos todos:

1. En el administrador de NPS, sobre Directivas de Red, pulsamos botón derecho ratón -> Nuevo. Introducimos el nombre de la política, en nuestro caso: Equipos Vlan26
2. El siguiente paso nos solicita las condiciones que ha de tener el equipo para cumplir esta política. Indicamos que ha de pertenecer al grupo: SE41_GS_RadiusVlan26. Para ello pulsamos en “Agregar” y seleccionamos “Grupos de Windows”. Localizamos el grupo en cuestión y lo agregamos. De esta forma la única condición que nos debe quedar es que pertenezca al grupo que hemos seleccionado.
3. En la siguiente pantalla indicamos que concedemos el acceso a dicha petición.
4. Elegimos el método de encriptación. Estas máquinas se apoyan en sus cuentas de equipos generadas en el servicio de directorio, y será el sistema operativo cliente el encargado de enviarlas por la red. Es por ello que usaremos un método seguro en el envío de sus credenciales; ese método será MS-CHAP y su segunda versión mejorada MS-CHAP-V2. Este tipo de comunicación los apoyaremos en el método seguro EAP-PEAP, que permite realizar una encriptación del tráfico con la opción de poder prescindir de una asignación de certificados digitales por cada cliente.

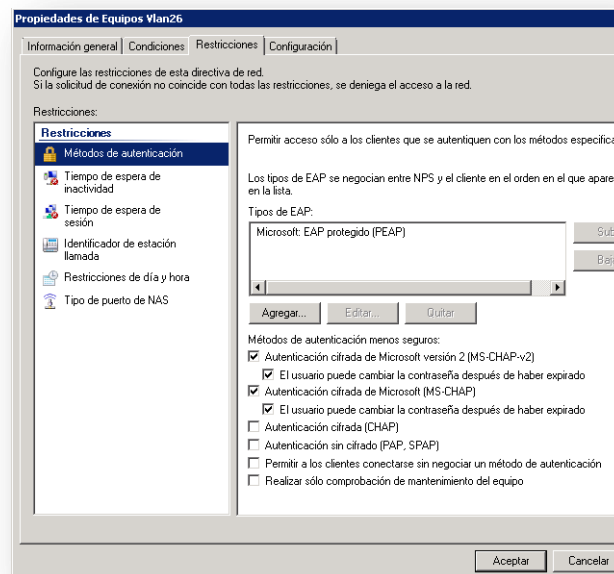


ILUSTRACIÓN 46 MÉTODO DE AUTENTICACIÓN

En este caso usaremos un certificado de servidor para configurar este nivel de seguridad. La configuración y creación del certificado no es parte del proyecto, pues hay distintas formas de conseguir este servicio y, en sí mismo, tiene entidad para formar un proyecto individual a desarrollar.

Indicamos un certificado individual generado para este servidor, tal como vemos en la siguiente imagen

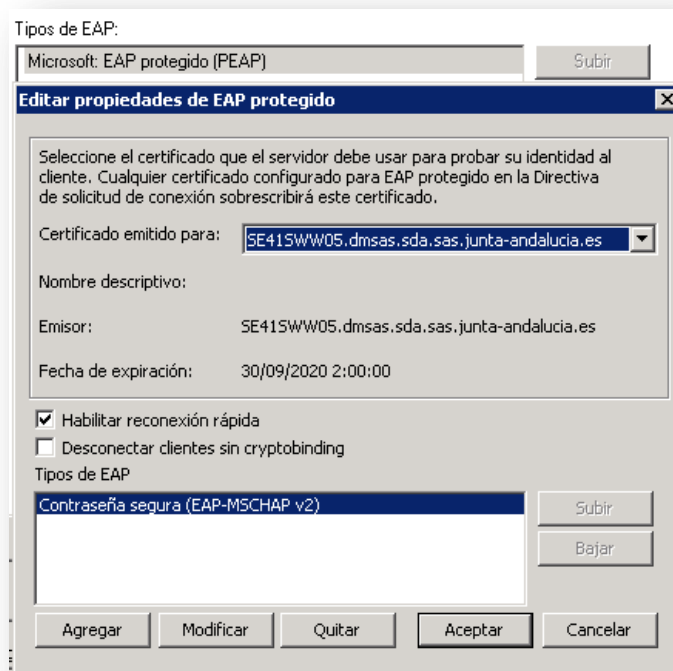


ILUSTRACIÓN 47 ELECCIÓN DEL CERTIFICADO

5. En el apartado de restricciones no indicamos ninguna, dado que los clientes que aceptarán las conexiones de estos equipos ya se establecieron en las políticas de “Directivas de solicitud de conexión”.
6. El paso final será situar el interfaz de red en la Vlan correspondiente,
 - a. Framed protocol: PPP
 - b. Service-Type: Framed
 - c. Tunnel-Medium-Type: 802 (includes all 802 media plus Ethernet canonical format)
 - d. Tunnel-Pvt-Group-ID: 26
 - e. Tunnel-Type: Virtual LANs
7. Finalmente, obtenemos un resumen de la configuración final que se ha realizado, revisamos los valores y finalizamos el asistente.

Vlan 5

Realizaremos ahora la configuración de la Vlan 5, que corresponde al perfil de Red Administrativa. Esta Red es la que dispone de un mayor número de usuarios y, además, sabemos que entre ellos tendremos 2 tipos o perfiles distintos (ver apartado 4.2.1).

Para manejarlos tendremos que generar 2 políticas de acceso distintas: una para los equipos compatibles con la autenticación 802.1X, y otra para los que no lo sean (impresoras, terminales, etc) en la que debemos usar su dirección MAC como credenciales de acceso. Ambas configuración seguirán el mismo proceso que las anteriores políticas ya configuradas.

Vlan 25

La última política a evaluar es la Red de Salas Públicas. Esta red permitirá su acceso a usuarios corporativos, es decir, registrados en nuestra base de datos de usuarios, usando dispositivos externos. Este comportamiento se consigue con el grupo creado en AD llamado SE41_GS_RadiusVlan25 donde hemos incluido todos nuestros usuarios registrados.

Procedemos a configurar la política siguiendo el mismo procedimiento que hemos realizado anteriormente.

5. PRESENTANDO RESULTADOS

5.1 TEST Y VALIDACIÓN

Una vez esté todo el entorno configurado, realizaremos una serie de pruebas sobre cada perfil de acceso.

Para la realización de las pruebas, hemos tenido que realizar unos ajustes de configuración en los equipos clientes. Estas indicaciones vienen detalladas en el anexo, donde se encuentra el “Manual” de configuración básica.

A modo de ejemplo indicamos solo los resultados sobre dos de los tipos de clientes:

Red de acceso sin dominio.

Esta red, por las características de los equipos usados, sólo tendrá una interfaz de red Ethernet, y los equipos no tienen el requisito de ser o no compatibles con 802.1X. Por lo tanto, procedemos a realizar su autenticación solo basándonos en su dirección MAC.

Realizamos el alta de la cuenta de usuario usando para ello la dirección MAC de la máquina, tanto en el nombre como en la contraseña del usuario del dominio.

Conectamos la red del equipo a un concentrador, configurado a tal efecto, y monitorizamos la conexión.

Comprobamos que el acceso se realiza correctamente y que el equipo se asigna a la Vlan indicada.

Usamos el visor de sucesos del servidor de NPS para tal efecto:

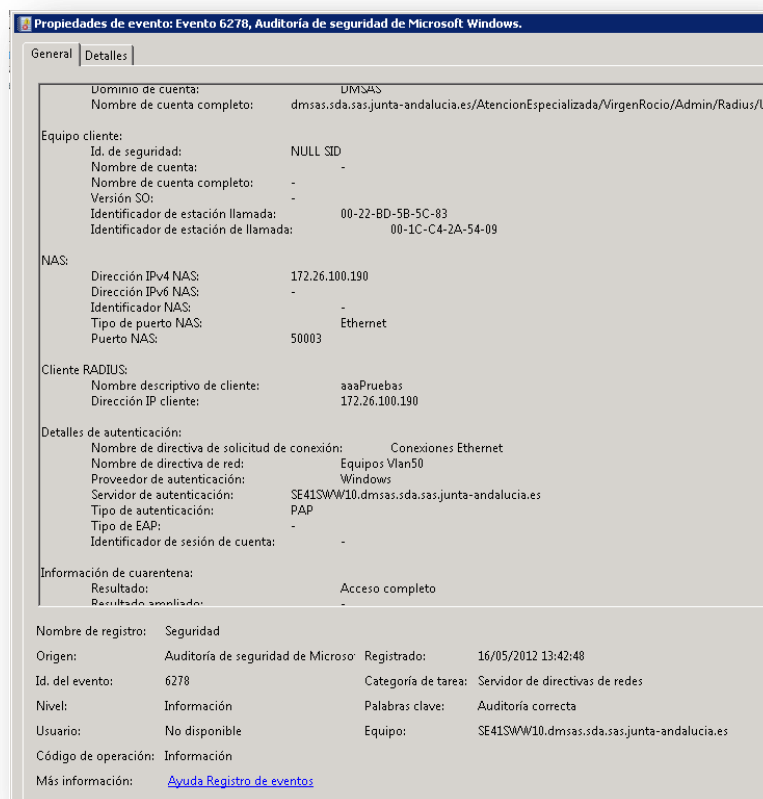


ILUSTRACIÓN 48 EVENTO ACCESO VLAN50

Red de invitados.

Esta red tendrá un control total por parte del departamento de TI. Es por ello que los equipos que formarán parte de ella estarán incluidos de forma manual en el grupo de seguridad correspondiente, SE41_GS_RadiusVlan26.

Tomamos un equipo corporativo, en nuestra prueba el nombre del equipo es SEPO2003E38W, y procedemos a asignarlo al grupo de seguridad indicado anteriormente y realizar la conexión a la red.

Realizamos, primero, la conexión mediante la red cableada.

Usamos el visor de sucesos del servidor de NPS para verificar la conexión:



ILUSTRACIÓN 49 EVENTO ACCESO VLAN26

Vemos que, tal como se esperaba, el equipo registra correctamente la conexión. Realizamos, ahora, la misma conexión mediante la red Wifi.

Vemos que igualmente el servidor NPS registra correctamente el acceso.

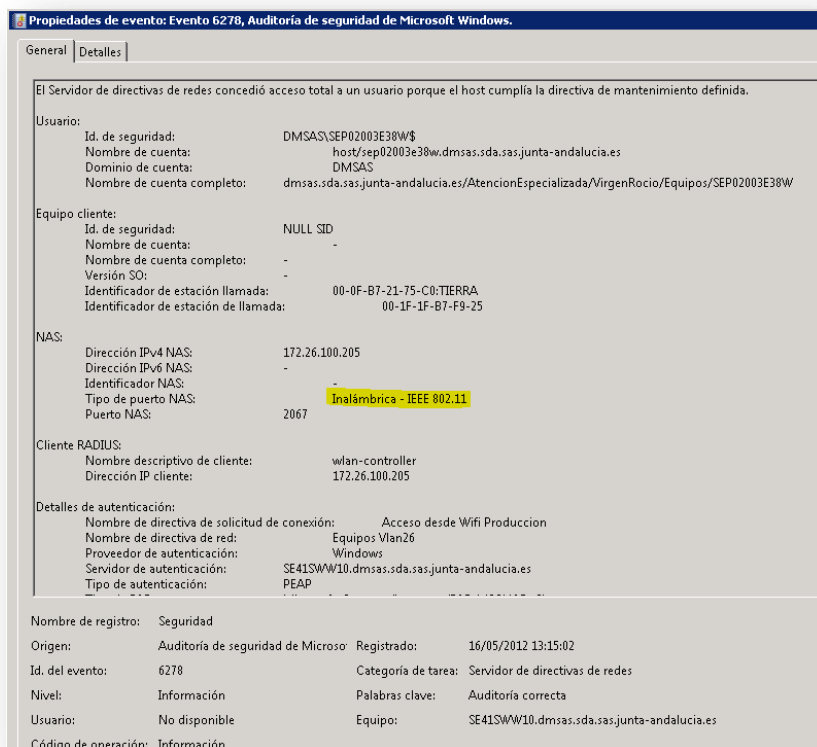


ILUSTRACIÓN 50 EVENTO ACCESO WIFI

Por tanto las pruebas también son satisfactorias.

Con este test finalizamos, satisfactoriamente, la batería de pruebas para todos los perfiles y situaciones de acceso.

5.2 ANÁLISIS TÉCNICO.

Realizaremos un análisis del funcionamiento de la solución implantada. El motivo de este trabajo es poder desgranar, a bajo nivel, el funcionamiento del producto obtenido y, de esta forma también, usar estos pasos como diagnóstico para posibles problemas futuros.

Para este análisis, hemos tomado como referencia un equipo con 2 tarjetas de red (SEP02003E38W), una en la red cableada y otra inalámbrica, analizando, así, los dos escenarios.

Para el diagnóstico en la red cableada, hemos conectado el equipo en un switch configurado para actuar como cliente Radius.

Seguidamente hemos procedido a monitorizar la puerta de enlace del switch contra el troncal de red; para ello hemos realizado un “Span” del puerto troncal contra otro puerto, donde hemos montado un equipo con un sniffer; en este caso hemos usado WireShark (antiguo Ethereal) como analizador de red.

Mediante el analizador de red comprobamos que, una vez conectado el equipo, el cliente de NPS (switch) comienza las peticiones al servidor de Radius. Vemos unas capturas de este tráfico:

Petición al servidor NPS:



```
Frame 5956: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0
Ethernet II, Src: Cisco_5b:5c:c1 (00:22:bd:5b:5c:c1), Dst: Cisco_7d:3e:00 (00:18:19:7d:3e:00)
Internet Protocol, Src: 172.26.100.190 (172.26.100.190), Dst: 10.232.0.181 (10.232.0.181)
User Datagram Protocol, Src Port: sighthline (1645), Dst Port: radius (1812)
Radius Protocol
  Code: Access-Request (1)
  Packet identifier: 0x55 (85)
  Length: 305
  Authenticator: e1942594d3e80e125b636b2bcb9e11be
  [The response to this request is in frame 5958]
  Attribute value Pairs
    AVP: l=52 t=User-Name(1): host/sep02003e38w.dmsas.sda.sas.junta-andalucia.es
    AVP: l=6 t=Service-Type(6): Framed(2)
    AVP: l=6 t=Framed-MTU(12): 1500
    AVP: l=19 t=Called-Station-Id(30): 00-22-BD-5B-5C-83
    AVP: l=19 t=Calling-Station-Id(31): 18-A9-05-20-1C-94
    AVP: l=109 t=EAP-Message(79) Last Segment[1]
      EAP fragment
        Extensible Authentication Protocol
          Code: Response (2)
          Id: 11
          Length: 107
          Type: PEAP [Palekar] (25)
          Flags(0x0):
          PEAP version 0
        Secure Socket Layer
          TLV1 Record Layer: Application Data Protocol: Application Data
            Content Type: Application Data (23)
            Version: TLS 1.0 (0x0301)
            Length: 96
            Encrypted Application Data: aeaf310e98765b9e98ac7504d19ed74278fc5c07c8ae883b...
          AVP: l=18 t=Message-Authenticator(80): dd4a0c80bf94f916aefc033ea19051fe
          AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
          AVP: l=6 t=NAS-Port(5): 50003
          AVP: l=38 t=State(24): 2d8302f100000137000102000ae800b50000000000000000...
            State: 2d8302f100000137000102000ae800b50000000000000000...
          AVP: l=6 t=NAS-IP-Address(4): 172.26.100.190
```

ILUSTRACIÓN 51 SOLICITUD DE ACCESO EAPOL

Respuesta del servidor:


```

⊞ Frame 5958: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits)
⊞ Ethernet II, Src: Cisco_7d:3e:00 (00:18:19:7d:3e:00), Dst: Cisco_5b:5c:c1 (00:22:bd:5b:5c:c1)
⊞ Internet Protocol, Src: 10.232.0.181 (10.232.0.181), Dst: 172.26.100.190 (172.26.100.190)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: sightline (1645)
⊞ RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x55 (85)
  Length: 298
  Authenticator: 934f7997960e41488cea9fc05335425d
  [This is a response to a request in frame 5956]
  [Time from request: 0.003972000 seconds]
  Attribute value Pairs
    ⊞ AVP: l=6 t=Framed-Protocol(7): PPP(1)
    ⊞ AVP: l=6 t=Service-Type(6): Framed(2)
    ⊞ AVP: l=6 t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
    ⊞ AVP: l=3 t=Tunnel-Private-Group-Id(81): 5
    ⊞ AVP: l=6 t=Tunnel-Type(64) Tag=0x00: VLAN(13)
    ⊞ AVP: l=6 t=EAP-Message(79) Last Segment[1]
      EAP fragment
      ⊞ Extensible Authentication Protocol
        Code: Success (3)
        Id: 11
        Length: 4
        ⊞ AVP: l=46 t=Class(25): 5caa052d00000137000102000ae800b50000000000000000...
        ⊞ AVP: l=14 t=Vendor-Specific(26) v=Microsoft(311)
        ⊞ AVP: l=51 t=Vendor-Specific(26) v=Microsoft(311)
        ⊞ AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
        ⊞ AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
        ⊞ AVP: l=18 t=Message-Authenticator(80): 324b34d10e8e9f9e60899dbac9bf1417

```

ILUSTRACIÓN 52 RESPUESTA EAPOL

Este tipo de comunicación se repetirá entre todos los clientes de NPS, incluido los inalámbricos. Por lo tanto, podemos tener ,para todos ellos, esta captura como muestra del tipo de tráfico que se va a producir.

A nivel de switch, una vez establecida la comunicación, también podemos comprobar cómo las estadísticas de peticiones de conexión 802.1X han aumentado.Para ello podemos usar el comando: show Radius statistics

```

sen02003e014#show radius statistics
Auth.      Acct.      Both
Maximum inQ length:      NA          NA          1
Maximum waitQ length:    NA          NA          1
Maximum doneQ length:    NA          NA          1
Total responses seen:    341         32         373
Packets with responses:  341         32         373
Packets without responses:  0           0           0
Average response delay(ms):  42          1           39
Maximum response delay(ms): 1233        17          1233
Number of Radius timeouts:  0           0           0
Duplicate ID detects:    0           0           0
Buffer Allocation Failures:  0           0           0
Maximum Buffer Size (bytes):  543         328         543
Source Port Range: (2 ports only)
1645 - 1646
Last used Source Port/Identifier:
1645/85
1646/32

Elapsed time since counters last cleared: 4d42m

```

ILUSTRACIÓN 53 ESTADÍSTICAS RADIUS

En la red inalámbrica también podemos realizar un seguimiento de este tipo de conexión. Para ello hemos procedido a realizar el mismo tipo de conexión con nuestro equipo, pero en esta ocasión a la red inalámbrica.

Para realizar una monitorización, nos conectamos al Controlador Wifi y lanzamos el comando: wlan-controller(15)# station-log show -mac=00:1f:1f:b7:f9:25. La dirección MAC la podemos variar en función del equipo a monitorizar.

Este comando nos muestra todo el tráfico que ha existido entre ambos equipos; para tener una visión, de qué tipo de tráfico se ha de recibir, tomamos sólo la parte de los mensajes donde vemos que se ha realizado correctamente la autorización del equipo:

```
2012-05-21 11:55:44.848 | 00:1f:1f:b7:f9:25 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=13> <info=relay eap-request f  
rom Radius> sent  
2012-05-21 11:55:44.860 | 00:1f:1f:b7:f9:25 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=13>  
2012-05-21 11:55:44.860 | 00:1f:1f:b7:f9:25 | 1X Authentication | Radius <msg code=access_request><msg ID=35> sent  
<ip=10.232.1.180>:<port=1812  
>  
2012-05-21 11:55:44.865 | 00:1f:1f:b7:f9:25 | 1X Authentication | Radius ACCESS-ACCEPT received : VLAN Tag :  
5, Filter id : , CUI : None  
2012-05-21 11:55:45.572 | 00:1f:1f:b7:f9:25 | 1X Authentication | <pkt type=EAP_PACKET> <EAP  
code=success><EAP ID=13> <info=relay eap-request f  
rom Radius> sent
```

6. CONCLUSIONES

Cuando me plantee realizar este proyecto, realice un análisis previo de qué tecnologías había disponibles para desarrollar una solución de este tipo. Localice muchas empresas que están ofreciendo soluciones propias que, aunque algunas pueden estar basadas en un estándar abierto, finalmente nos fuerzan a tener que instalar programas y sistemas propietarios tanto en el apartado servidor como en el lado del cliente.

Sin embargo, este tipo de soluciones propietarias también nos ofrecen una gran ventaja, y es el valor de ser instalaciones “llave en mano”, es decir, nos ofrecen una puesta en marcha del sistema muy rápida, y un control de todos los mecanismos de seguridad implicados mediante un único punto de gestión. Aun con este valor añadido, también encontré que las soluciones de este tipo nos limitan el escalado o integración con otros dispositivos o tecnologías que no estén aceptados por dichas compañías, por ejemplo algunas de ellas usan un sistema propio de cuentas de usuarios basado en una base de datos propia. Estos inconvenientes me decantaron por buscar una solución que estuviera basada en estándares y protocolos abiertos, eligiendo 802.1X como piedra angular de todo el proyecto.

Ha sido muy grato, tanto a nivel académico como profesional, conseguir integrar dentro de este proyecto todo un conjunto de herramientas independientes, como han sido: los elementos de gestión de la red cableada, los controladores Wifi, la base de datos de cuentas de usuarios y equipos del Directorio Activo y el servidor Radius de Microsoft, NPS, como la pieza principal de todo el conjunto.

Personalmente pienso que, en el momento tecnológico actual que vive nuestro sector, la idea principal que deben seguir nuestros proyectos es intentar usar siempre la filosofía de “integración” y esto, en gran parte, significa basarnos en estándares abiertos y no en productos cerrados de determinadas compañías que ofrecen soluciones cerradas y que solo funcionan siempre que cumplamos todos sus requisitos.

Finalmente quiero recalcar que uno de los mayores logros de todo el proyecto, ha sido realizar la implementación sobre uno de los entornos más exigentes respecto a seguridad y movilidad, un Hospital. Este escenario en vez de ser un inconveniente, nos ha aportado una gran una gran riqueza de elementos y casos a controlar, lo cual nos ha permitido poder desarrollar un producto muy completo, adaptable a muchas circunstancias futuras, y escalable a otros entornos similares.

El resultado de todo este trabajo lo podemos sintetizar en que con una inversión contenida, dado que hemos utilizado todos los elementos actuales, hemos obtenido una Red más segura, autónoma y por todo ello más eficiente, que ha cumplido mis expectativas para un proyecto de este tipo.

ANEXO I

GUÍA DE CONFIGURACIÓN DEL CLIENTE.

Dentro de este apartado incorporamos las bases para la configuración de acceso para cualquier tipo de cliente de Red. Dado que los sistemas operativos de nuestro cliente pueden variar, nos basaremos en el sistema operativo más desplegado en nuestra red y, sobre todo, con mayor crecimiento actual. La guía de instalación, dado que estamos tratando con un tipo de protocolo estándar, se podrá usar como indicación para los casos no contemplados aquí.

Dentro de nuestro proyecto podemos tener 2 perfiles básicos.

- Compatibles con 802.1X
- No compatibles.

Los segundos serán controlados mediante su dirección MAC, por lo que el equipo no requiere ninguna configuración adicional; es por ello que nos centramos en el primer caso.

Para los clientes compatibles de 802.1X, debemos tener en cuenta que siempre tendremos que tener activada la validación de máquina, y sólo usaremos la de usuario en la red de salas públicas.

Para poder configurar el método de acceso, tendremos que tener activo el servicio de red que gestiona este protocolo; en Windows 7 este servicio viene desactivado por defecto para las redes cableadas, por lo tanto indicamos como activarlo:

- 1- Nos dirigimos al administrador de servicios. Ejemplo: Ejecutamos services.msc
- 2- Buscamos el servicio llamado “Configuración automática de redes cableadas”, y lo iniciamos (se recomienda configurar para que siempre quede iniciado de modo automático).

Una vez sobre la configuración 802.1X del cliente (en Windows 7 la podemos encontrar en la propiedades de la conexión de red), indicamos los métodos de conexión según el perfil de red a usar.

- Para todas las redes podemos indicar autenticación de máquina, y para la red de salas publicas la autenticación de usuarios.
- En el método de autenticación elegimos EAP protegido (PEAP).

Mostramos la configuración de este apartado en la siguiente imagen:

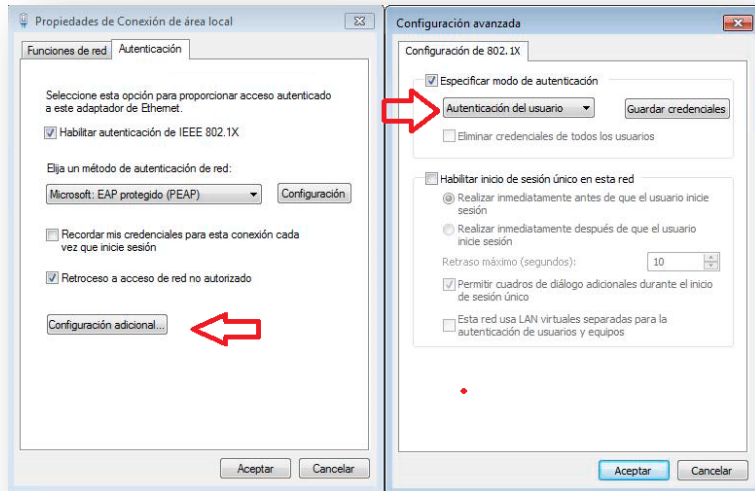


ILUSTRACIÓN 54 CONFIGURACIÓN 802.1X W7

- Podemos indicar que no use las credenciales automáticamente, y así poder indicar el usuario de red que realizará el acceso (sólo para la red de salas publicas).
- Es importante indicar que no valide el certificado de servidor. En este proyecto no hemos abarcado la implantación de un servidor de certificados autorizado en la Red, aunque podría haber incrementado la seguridad notablemente, ya que su complejidad requeriría un proyecto en sí mismo y sólo hemos generado un certificado de servidor independiente y, además, no generado por una entidad de certificación autorizada.

Mostramos la configuración de este apartado en la siguiente imagen:

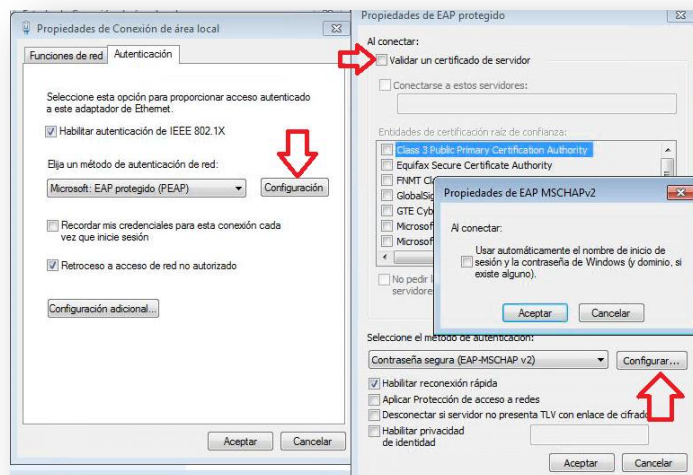


ILUSTRACIÓN 55 CONFIGURACIÓN EAP W7

Estos parámetros son también los que debemos usar en la configuración inalámbrica, dado que hemos personalizado las políticas para que funcionen con los dos tipos de conexión.

Con estos parámetros podemos realizar la configuración de todos los tipos de clientes usados en este proyecto.

GLOSARIO DE SIGLAS Y TÉRMINOS.

AAA: Autenticación, Autorización, y Archivado.

AD: Directorio Activo.

AES: Estándar avanzado de encriptación.

AP: Access Point. Punto de acceso inalámbrico.

CAN: Red de área de campus (CAN) es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar.

CHAP: Protocolo de Autenticación por desafío mutuo.

DA (Directorio Activo): Almacén de información de una organización en una base de datos central, organizada y accesible, que contiene los servicios de directorio de una red distribuida de computadores.

DNS: Servidor de nombres de dominio. Servicio que puede resolver dirección IP en nombres de dominio y viceversa.

EAP: Protocolo extensible de autenticación.

EAPoL: EAP sobre una Red LAN.

Firewall: Sistema que está diseñado para bloquear o permitir el acceso a las distintas comunicaciones entre redes.

ESS: Extended Service Set. Modo de propagación único de un SSID a lo largo de varios AP.

IEEE 802.11: Define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

MAB: Pasarela de autenticación de direcciones MAC.

MAC (Dirección). Dirección de acceso al medio. Identificador único generado en fabricación para cada tarjeta de red.

NAP: Sistema de Protección de Acceso a la Red.

NPS: Servidor de directivas de red.

PAP: Protocolo de Autenticación de Contraseñas.

PEAP: Protocolo Protegido Extendido de Autenticación.

Radius: Protocolo de autenticación y autorización para aplicaciones de acceso a la red.

RAS: Servidor de acceso remoto. Servicio que permite recibir llamadas entrantes de clientes de red y autenticarlos en la red.

RDSI: Red Digital de Servicios Integrados.

Sniffer: Analizador de Red.

Spanning Tree: Protocolo que se encarga de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes.

SSID: Service Set Identification. Identificación, en forma de código o palabra, usado para asociar una determinada red

TI: Acrónimo de tecnologías de la información.

TKIP: Protocolo de integridad de claves temporales.

UNC: Convección Universal de nombres de Red.

UTP: (Unshielded twisted pair) Cable de par trenzado que no se encuentra blindado y que se utiliza principalmente para comunicaciones.

Vlan: Red virtual LAN.

WPA: Acceso Wifi protegido.

XML: Lenguaje de marcas extendidas.

BIBLIOGRAFÍA.

<https://supportforums.cisco.com/thread/2133724>

Network Policy Server (NPS) Operations Guide, MICROSOFT CORP April 2008.

MAC Authentication Bypass Deployment Guide, CISCO SYSTEMS Inc, Mayo 2011.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/config_guide_c17-663759.pdf

Identity-Based Networking Services: IEEE 802.1X Deployment Guide, CISCO SYSTEMS.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/guide_c07-627531.html

Cisco Catalyst 2960-S and 2960 Series Switches with LAN Base Software, CISCO SYSTEMS.

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.pdf

Magic Quadrant for Wireless LAN Infrastructure (Global), GARTNER INC. G00210047.

<http://www.gartner.com/id=1572016>

MC4200 Datasheet. Meru Networks. <http://www.merunetworks.com/collateral/data-sheets/mc4200-datasheet.pdf>

Selecting the Best Network Authentication Solution, GARTNER INC. ID:G00166065.

<http://my.gartner.com/portal/server.pt?open=512&objID=249&mode=2&PageID=864059&resId=967117&ref=Browse>

Meru Controller Installation Guide, Meru Networks INC. 882-60040 Rev A Rel 4.0 Ver 7 Controller Install Guide.

<http://securityuncorked.com/2011/11/the-4-wireless-controller-architectures-you-need-to-know/>