**ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN**

**UNIVERSIDAD DE CANTABRIA**

*Proyecto Fin de Carrera*

# TELECOMUNICACIONES EN PARQUES EÓLICOS
# (Telecommunications at wind farms)

**Para acceder al Titulo de**

## INGENIERO DE TELECOMUNICACIÓN

**Autor: Luis Carrión Echevarría**

**Junio - 2010**

E.T.S. DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACION

# INGENIERÍA DE TELECOMUNICACIÓN

CALIFICACIÓN DEL PROYECTO FIN DE CARRERA

**Realizado por: Luis Carrión Echevarría**
**Director del PFC: Adolfo Cobo García**
**Título: "Telecomunicaciones en parques eólicos"**
**Title: "Telecommunications at wind farms"**

**Presentado a examen el día: 29 de junio de 2010**

para acceder al Título de

## INGENIERO DE TELECOMUNICACIÓN

Composición del Tribunal:
Presidente (Apellidos, Nombre): Mañana Canteli, Mario
Secretario (Apellidos, Nombre): Cobo García, Adolfo
Vocal (Apellidos, Nombre): Fernández García, Tomás

Este Tribunal ha resuelto otorgar la calificación de: .....

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: El Vocal

Fdo.: El Director del PFC
(sólo si es distinto del Secretario)

Vº Bº del Subdirector

Proyecto Fin de Carrera Nº
(a asignar por Secretaría)

Quiero agradecer a mi familia el apoyo que he encontrado en ellos no sólo durante la realización del proyecto si no durante todo este ciclo que hoy se cierra. Y especialmente a mi madre, mi hermano y mi novia que son lo más importante de mi vida.

No me quiero olvidar de Adolfo, ha sido fantástico contar contigo como director de mi proyecto.

Dedicado con todo mí cariño a mi novia.
Eres la mejor. No cambies nunca.

Índice de contenidos

# 1. Introducción

## 1.1. La energía eólica

La energía eólica es la energía obtenida del viento, es decir, la energía cinética de las corrientes de aire, y que es transformada en otros tipos de energía. La energía eólica ha sido aprovechada desde la antigüedad para mover los barcos impulsados por velas o hacer funcionar la maquinaria de molinos al mover sus aspas. En la actualidad, la energía eólica es utilizada principalmente para producir energía eléctrica mediante aerogeneradores.

La energía eólica es un recurso abundante, renovable, limpio y ayuda a disminuir las emisiones de gases de efecto invernadero. Reemplaza a las centrales termoeléctricas a base de combustibles fósiles, lo que la convierte en un tipo de energía verde. Sin embargo, el principal inconveniente es su intermitencia. Es un tipo de energía renovable ya que tiene su origen en procesos atmosféricos debidos a la energía que llega a la Tierra procedente del Sol.

Son varias las ventajas que aporta la energía eólica (y las energías renovables en general):

- Es una energía limpia ya que no produce emisiones atmosféricas ni residuos contaminantes.
- No requiere una combustión que produzca dióxido de carbono (CO2), por lo que no contribuye al incremento del efecto invernadero ni al cambio climático.
- Puede instalarse en espacios no aptos para otros fines, por ejemplo en zonas desérticas, próximas a la costa, en laderas áridas y muy empinadas para ser cultivables.
- Crea un elevado número de puestos de trabajo en las plantas de ensamblaje y las zonas de instalación.
- Su instalación es rápida, entre 6 meses y un año.
- Su utilización combinada con otros tipos de energía, habitualmente la solar, permite la autoalimentación de viviendas, terminando así con la necesidad de conectarse a redes de suministro.
- La situación actual permite cubrir la demanda de energía en España un 30% debido a multitud de parques eólicos que hay repartidos por nuestro territorio, compensando la baja producción de unos por falta de viento con la alta producción en las zonas de viento.
- Posibilidad de construir parques eólicos en el mar, donde el viento es más fuerte, más constante y el impacto social es menor, aunque aumentan los costes de instalación y mantenimiento. Los parques *offshore* son una realidad en los países del norte de Europa, donde la generación eólica empieza a ser un factor bastante importante.

Por contra, debido a la falta de seguridad en la existencia de viento, la energía eólica no puede ser utilizada como única fuente de energía eléctrica. Por lo

tanto, para salvar los "valles" en la producción de energía eólica, es indispensable un respaldo de las energías convencionales (centrales de carbón o de ciclo combinado, por ejemplo, y más recientemente, de carbón limpio). Sin embargo, cuando respaldan la eólica, las centrales de carbón no pueden funcionar a su rendimiento óptimo, que se sitúa cerca del 90% de su potencia. Tienen que quedarse muy por debajo de este porcentaje, para poder subir sustancialmente su producción en el momento en que afloje el viento. Por tanto, en el modo "respaldo", las centrales térmicas consumen más combustible por kW/h producido. También, al subir y bajar su producción cada vez que cambia la velocidad del viento, se desgasta más la maquinaría. Este problema del respaldo en España se va a tratar de solucionar mediante una interconexión con Francia que permita emplear el sistema europeo como colchón de la variabilidad eólica.

Para evacuar la electricidad producida por cada parque eólico (que suelen estar situados además en parajes naturales apartados) es necesario construir unas líneas de alta tensión que sean capaces de conducir el máximo de electricidad que sea capaz de producir la instalación. Sin embargo, la media de tensión a conducir será mucho más baja. Esto significa poner cables cuatro veces más gruesos, y a menudo torres más altas, para acomodar correctamente los picos de viento. Es necesario suplir las bajadas de tensión eólicas "instantáneamente" (aumentando la producción de las centrales térmicas), pues sino se hace así se producirían, y de hecho se producen, apagones generalizados por bajada de tensión. Este problema podría solucionarse mediante dispositivos de almacenamiento de energía eléctrica. Pero la energía eléctrica producida no es almacenable: es instantáneamente consumida o perdida.

Uno de los grandes inconvenientes de este tipo de generación, es la dificultad intrínseca de prever la generación con antelación. Dado que los sistemas eléctricos son operados calculando la generación con un día de antelación en vista del consumo previsto, la aleatoriedad del viento plantea serios problemas. Los últimos avances en previsión del viento han mejorado muchísimo la situación, pero sigue siendo un problema.

Además de la evidente necesidad de una velocidad mínima en el viento para poder mover las aspas, existe también una limitación superior: una máquina puede estar generando al máximo de su potencia, pero si el viento aumenta lo justo para sobrepasar las especificaciones del aerogenerador, es obligatorio desconectar ese circuito de la red o cambiar la inclinación de las aspas para que dejen de girar, puesto que con viento de altas velocidades la estructura puede resultar dañada por los esfuerzos que aparecen en el eje. La consecuencia inmediata es un descenso evidente de la producción eléctrica, a pesar de haber viento en abundancia, y otro factor más de incertidumbre a la hora de contar con esta energía en la red eléctrica de consumo.

El impacto paisajístico es una nota importante debido a la disposición de los elementos horizontales que lo componen y la aparición de un elemento vertical como es el aerogenerador. Esto, unido al ruido, puede llevar a la gente hasta un alto nivel de estrés, con efectos de consideración para la salud. No

obstante, la mejora del diseño de los aerogeneradores ha permitido ir reduciendo el ruido que producen.

## 1.2. ¿Qué relación tienen los parques eólicos y las telecomunicaciones?

Este proyecto fin de carrera trata de explicar de manera sencilla el uso y necesidad de las telecomunicaciones en un parque eólico. Aunque parezca a priori que un parque eólico no precise de instalación de telecomunicaciones, en la práctica se hace necesario. De hecho, todo parque eólico (y centro de producción de energía en general) tiene asociado mucho trabajo en cuanto a la instalación de telecomunicaciones. Tanto es así que las empresas del sector disponen incluso de varios departamentos dedicados a las telecomunicaciones.

Para entrar en materia quizá lo mejor sea hablar sobre el funcionamiento de un parque eólico a grandes rasgos. Un parque eólico se compone de varios, desde unos pocos hasta centenares, molinos. Cada uno de ellos transforma la energía eólica en energía eléctrica que se inyecta “directamente” a la red eléctrica. Ese es el negocio que persigue quien explota un parque eólico: vender electricidad. Es obvio que para tener los mayores beneficios es necesario aprovechar el viento de la manera más eficiente. Esto es: que las palas aprovechen cuanto mejor el viento y que en ningún caso un molino esté parado cuando el viento sopla.

Por otro lado, la administración reguladora pertinente del país (en España R.E.E.) obliga a que esa electricidad que se inyecta a la red esté en todo momento bajo monitorización y control. Y es aquí donde entran en juego las telecomunicaciones. Las empresas, que típicamente tienen más de un parque eólico, lejos de tener un operario en cada parque, montan auténticos “centros de control” donde, de forma centralizada monitorizan y telecontrolan miles y miles de variables de cientos de molinos. Evidentemente esto es así porque el coste es menor.

Para que esas cientos de variables lleguen hasta el personal que lo monitoriza y controla, es necesario que exista una conexión entre cada molino y el “telemando”.

Es de destacar la importancia que cobran las telecomunicaciones para que el parque pueda ser “visto” desde el centro de control. Ante la caída del servicio (la no habilidad de telemandar el parque por causas referentes a las telecomunicaciones) es necesario desplazar a personal de guardia al parque para que monitorice de forma local el parque eólico o incluso detenga todos los molinos desde la propia subestación o sala de control del parque. Es realmente peligroso que un parque eólico inyecte electricidad a la red sin ningún tipo de control ni monitorización. Evidentemente esto puede afectar mucho a la rentabilidad de un parque. Y por ello, merece la pena realizar una buena inversión tanto en equipos de red interna como en las comunicaciones hacia el exterior.

## 1.3. Estructura del proyecto

A lo largo de la memoria de este proyecto fin de carrera se trata de explicar todo lo relacionado con las telecomunicaciones en un parque eólico. El documento se ha organizado de la siguiente manera:

- Explicación general
- Comunicaciones externas
- Equipamiento de red
- Comunicaciones internas
- Caso real de implementación
- Costes asociados a las comunicaciones

# 2. Visión general de las telecomunicaciones en un parque eólico.

Los departamentos de comunicaciones en las empresas energéticas que construyen parques eólicos son los responsables de que el centro de producción esté comunicado con el centro de control. Para ello desarrollan varias tareas.

Por un lado es necesario realizar la conexión del parque eólico a Internet. Se necesita contratar al menos un proveedor de servicios de Internet de la zona. Esta tarea tiene alta dificultad, pues los parques eólicos se sitúan en lugares alejados de núcleos urbanos con las desventajas que ello conlleva. La red del proveedor de Internet suele llegar hasta lo conocido con “sala de control” o Control Room. Típicamente esta sala se encuentra en las inmediaciones de la subestación eléctrica. Es decir, el punto desde el que se evacua o inyecta hacia la red la electricidad “generada” por los molinos. También es conocida como subestación eléctrica elevadora ya que ella se eleva la tensión eléctrica de salida de los generadores.

Esta sala, que puede ser desde un pequeño container de obra hasta un auténtico edificio de varias plantas, alberga todo los equipos de gestión y monitorización que son necesarios para la operación del parque cuando el personal de operación y mantenimiento se encuentra en el parque. Típicamente es en las inmediaciones de la sala donde se colocan todos los armarios de comunicaciones.

Por otro lado se encuentra la red que hay que desplegar entre los routers de los ISPs y cada uno de los molinos. Esta red se divide en dos segmentos

- La red de parque: en la que todos los molinos están conectados hasta un punto, típicamente en la “subestación”. También recibe el nombre de red de producción o red SCADA
- La red exterior de comunicaciones: se trata de la red que hace de unión entre Internet (brindado por los ISPs) y la red de parque. Es en esta red donde reside o se ponen todos los medios para que las comunicaciones que, no olvidemos, van a viajar a través de Internet, lo hagan de forma lo más segura posible. Switches, routers, conversores de medio optoelectrónicos y firewalls son los elementos que conforman esta red

En algunas ocasiones, dentro de parque eólico también se disponen puestos informáticos para los trabajadores o investigadores, con lo que es necesario desplegar una red de ofimática en la que se encuentran los PC de los usuarios, fotocopiadoras en red, teléfonos IP o impresoras. Es necesario aislar esta red de la red de producción a todos niveles, para que un bucle de red, un virus o algún otro peligro no pueda afectar a la red SCADA, que es la red realmente importante.

# 3. Comunicaciones exteriores

## 3.1. Introducción

Como bien se ha dicho en anteriores apartados, los parques eólicos están comunicados con los centros de control. Realmente, cada parque está conectado al menos con un centro de control. Típicamente los parques eólicos son construidos por una empresa (vendedora) y explotados por otra diferente (compradora). Por ello, lo normal es que el parque eólico esté conectado a los centros de control o monitorización de ambos.

Desde el centro de control de la empresa que explota el parque, se puede decir que el parque se “telemanda” para sacarle el máximo rendimiento. Por otro lado, la empresa que fabrica y vende los molinos, generalmente vende las máquinas con una garantía de unos años. Durante este tiempo, es muy recomendable que se monitoricen las máquinas para comprobar que el uso que se hace de ellas es el debido. Incluso se puede añadir una tercera conexión al parque eólico. Generalmente se crea un acceso exclusivo para los “grandes cargos” de la empresa que explota el parque, para que de manera sencilla, desde cualquier lugar y en cualquier momento, puedan comprobar el rendimiento de cada una de las máquinas del parque.

Típicamente los parques eólicos están situados en zonas de media o alta montaña, pues las condiciones de viento son idóneas para la implantación de los molinos. Antes de la construcción del parque se realizan estudios incluso del emplazamiento óptimo de los molinos. Es una razón lógica y fácilmente entendible. Además los parques eólicos ocupan grandes extensiones, con lo que se encuentran lejos de núcleos urbanos. Se trata de lugares con condiciones climatológicas adversas: hielo y frío en invierno y altas temperaturas en verano. Es tanto así, que todo lo bueno que tienen en cuanto a lugar estratégico desde el punto de vista del aprovechamiento del viento lo tienen de negativo o lo hacen complicado en cuanto a comunicaciones.

Empezando por el hardware y siguiendo por las líneas acceso a Internet, casi todo se vuelve más complicado de lo que en un principio pudiera pensarse. Además es altamente recomendable que las comunicaciones estén redundadas casi de extremo a extremo. De esta manera, si las comunicaciones no fallan el “cliente” estará satisfecho pero por el contrario si algún elemento de la red o operador de Internet falla, se puede estar orgulloso de que gracias a la redundancia, no ha existido pérdida de comunicación ni de servicio.

## 3.2. Tecnologías de acceso a Internet

Cuando se construye un parque eólico, se suele hablar de que se realiza un proyecto “llave en mano”. Esto quiere decir que el cliente o comprador no se tiene que preocupar ni ocupar en ningún sentido sobre la construcción y puesta en marcha del parque eólico.
Los departamentos de comunicaciones son los encargados de a cabo la tarea de comunicar el parque eólico con el centro de control.

La conexión entre ambas sedes (centro de producción y centro de control) se podría realizar contratando un enlace dedicado punto a punto. Pero hoy en día esto no se hace así por dos motivos: se trata de una solución muy cara. Pensemos en que las dos sedes no tienen por qué estar en el mismo país. Ni siquiera en el mismo continente. El otro motivo es que esa conexión ya la tenemos (casi) gracias a Internet. Es una muy buena idea aprovechar que existen empresas (ISP) que se dedican justamente a estos menesteres. Con lo cual, el trabajo se “limita” encontrar un proveedor de servicios de Internet en la zona.

Antes de continuar, incluir un apunte en cuanto al acceso a Internet empresarial. Puede parecer que el acceso a Internet que contratan las empresas es de igual o muy parecida velocidad al que cualquier persona puede contratar (acceso residencial se le suele llamar). Pero no es sólo cuestión de velocidad (que también lo es) lo que más preocupa y más interés tiene. Es la disponibilidad del servicio y el ancho de banda garantizado y simetría de velocidades (downstream/ upstream) lo que más se busca en estos contratos. Hay proveedores de Internet que cobran grandes cantidades por líneas de 4 mbps simétricos en las que están garantizados el 50% del ancho de banda además de una disponibilidad del 99.99% del tiempo (que son aproximadamente 5 minutos al año sin servicio). Estos números distan mucho de la simetría de la línea, el ancho de banda garantizado y disponibilidad anual de los accesos a Internet residenciales.

Dada la importancia que tienen las comunicaciones en los parque eólicos, muchas empresas energéticas tienen definido un estándar en para ellas. En él, se ponen de manifiesto los criterios a seguir en cada uno de las tareas a desarrollar. Además, de esta forma se guarda una cierta uniformidad en la creación de lo que a largo plazo puede llegar a ser un sistema que maneja grandes cifras. Uno de los criterios más comunes hace referencia a las especificaciones de las líneas de Internet que se contratan en los parques eólicos.

Aún así, la tarea de encontrar un proveedor de Internet para el parque eólico no es una tarea fácil y puede que se trate de la tarea en la que hay que hacer un ejercicio de imaginación mayor. Es necesario conocer muy bien las necesidades y así poder realizar un buen trabajo para que el centro de control opere el parque de manera cómoda. En la actualidad hay muchas empresas que se dedican a fabricar molinos para parques eólicos. Cada fabricante de molinos, obviamente, se ocupa de diseñar las turbinas, palas y torre que

componen cada molino. Lo normal es que dispongan de varios modelos y según las características de la zona donde se vaya a construir el parque eólico, se elige un tipo de pala y un tipo de turbina. De hecho la construcción de parque eólicos se demora bastante tiempo porque antes de instalar el primer molino, es necesario haber recogido los datos climatológicos de al menos un año entero para valorar la viabilidad del proyecto y poder elegir de forma correcta el tipo de turbina y palas más adecuado.

Además de la parte más industrial del proyecto, los fabricantes de molinos desarrollan su propio sistema SCADA. O al menos disponen de alguna empresa a la que subcontratan el desarrollo. El término SCADA usualmente se refiere a un sistema central que monitoriza y controla un sitio completo o una parte de un sitio. Se trata de software, de una aplicación informática muy completa que recoge información típicamente metrológica y del estado de los molinos y que a su vez es capaz de controlar las máquinas. La mayor parte del control del sitio es en realidad realizada de forma automática pero siempre con la supervisión de personal. Para la monitorización, en cada uno de los molinos se instalan dispositivos que pueden dar información muy precisa de varios cientos de variables (se montan auténticas estaciones meteorológicas). Del mismo modo, el sistema SCADA se utiliza para enviar las órdenes desde el centro de control al parque.

Como se comentó al comienzo del apartado, estos datos llegan hasta el centro de control a través de Internet. Por ello, es necesario tener en cuenta los requerimientos de anchos de banda mínimo y latencia máxima para el correcto funcionamiento de la red SCADA.

Uno de los requisitos más recomendables en cuanto a las telecomunicaciones es que exista una redundancia en cuanto a líneas de Internet. La disponibilidad de dos líneas de Internet hace que las probabilidades de que ambas fallen al mismo tiempo sean realmente bajas. Lo óptimo en estos casos es disponer de dos líneas de Internet de dos proveedores distintos. Esto es así por la sencilla razón de que si existe un problema en red de acceso y ambos líneas son del mismo proveedor, se dará una situación en la que la redundancia de las líneas no tiene sentido.

Hoy por hoy, existen varias tecnologías usadas en las redes de acceso a Internet. Son por todos conocidas las RDSI, Frame Relay, xDSL, HFC, FTTx, vSAT, WiFi, WiMAX, GSM, GPRS UMTS, HSDPA o HSPA.

Por comentar brevemente, los servicios de acceso a Internet a través medios guiados en cable como fibra, cable coaxial o par de cobre son conexiones más estables, con tecnología muy madura y estudiada. Además, suelen prestar servicio de mayor ancho de banda, con menores latencias y variación de esta que los accesos radio. En contraposición, los accesos radio tienen como mayor ventaja un despliegue rápido y “barato” comparados con los accesos vía cable. Por el contrario, se trata de tecnología mucho más nueva, menos probada. Por último, la ventaja entre las ventajas de estos accesos es que suelen ser de tipo móvil o al menos nómada, aunque esto no es propiamente una ventaja en el caso de parques eólicos, pues la movilidad no es una necesidad.

Evidentemente y en la medida de lo posible, siempre se intenta contratar un acceso a Internet de cable. La razón no es otra que la fiabilidad que dan las comunicaciones a través de fibra óptica, coaxial o par de cobre, pues no hay que olvidar que los parque eólicos se construyen en zonas altas, con condiciones meteorológicas adversas que influyen mucho más en, por ejemplo, los radio-enlaces de microondas, que en la señal de un cable soterrado un metro bajo la tierra.

El departamento de comunicaciones afronta esta tarea es consciente de que no es fácil que el acceso por cable esté disponible. En ocasiones se puede llegar a contactar con empresas que están dispuestas a realizar una tirada de cable hasta el parque eólico, con la consecuente obra civil que hay que realizar. Estas obras suelen ser aprovechadas por el ISP para ofrecer servicio a la zona que hasta el momento no estaba contemplada.

Los ISP rápidamente echan sus cálculos, sabiendo que el servicio de Internet que van a prestar al parque eólico va a durar varios años y por ello la instalación y despliegue inicial van a tener un retorno de la inversión asegurado.

Lo anterior no quiere decir que nunca exista un proveedor de Internet con cableado en la zona. Dependiendo del país y la orografía de la zona, hay parque eólicos que pueden contratar líneas ADSL o HDSL sin que el ISP tenga que realizar obra de ampliación en su red. Esto se traduce en tiempos de puesta en servicio de las comunicaciones mucho menores que cuando es necesaria la realización de obra civil.

Lo cierto es que la imaginación y el dinero son los únicos límites en cuanto a las formas o posibilidades que existen para contratar un acceso a Internet en parques eólicos.

Por lo general, insistiendo en ello dada la importancia que tiene, es necesario contratar dos líneas de Internet totalmente independientes, para disfrutar de redundancia real. Por ello, a partir de ahora se utilizarán los términos línea principal y línea de backup.

Como línea principal se emplea la que mejores características presente. Generalmente un ADSL o T1, dependiendo del continente en el que nos encontremos. Los accesos vía radio para línea principal cada vez son más típicos debido a su cada vez mejor relación calidad/precio y estabilidad. Conexiones WiMAX no se suelen barajar como línea principal ya que su fiabilidad no es muy alta. Si es común la utilización de radio-enlaces de tecnologías propietarias en la última milla, típicamente IP aunque en ocasiones se utilizan enlaces profesionales en los que solo se maneja la capa 2 del modelo OSI.

En muchas ocasiones es necesario realizar un ejercicio de imaginación y lograr el acceso a Internet a base de varias tecnologías. Se puede llegar a algún tipo de acuerdo con una empresa local que, fuera del parque eólico contrate el

servicio ADSL con proveedor de Internet y desde sus instalaciones se realice un radio-enlace hasta el parque, a modo de bridge. No es el mejor escenario pues las responsabilidades en cuanto a la gestión del servicio no queda totalmente clara pero suele tratarse de soluciones que satisfacen las necesidades.

En cuanto a las líneas de Internet sobre Frame Relay, la verdad es que no es una tecnología que se use ampliamente en la actualidad, aunque aún hay operadores, por ejemplo en los Estados Unidos, que ofrecen el servicio con Frame Relay.

Como soluciones para la línea secundaria o de backup se suelen barajar varias tecnologías. Si es posible y asequible, se contrata otro servicio de ADSL de otro proveedor (por aquello de la redundancia "efectiva"). SI no es posible, se piensa en soluciones WiMAX. También hay que estudiar la cobertura UMTS de los operadores móviles del país. Es espectacular el rendimiento que están demostrando las últimas revisiones de UMTS: en HSUPA, los anchos de banda se asemejan a las líneas ADSL y las latencias son poco mayores. Su problema es la gran inestabilidad y variabilidad que presentan de un día para otro.

Como último recurso, se puede contratar servicios de Internet por satélite VSAT (Very Small Aperture Terminals). El ancho de banda suele ser bastante limitado, debido a la gran concurrencia de usuarios con los que se comparte el servicio. A pesar de esto, el gran problema de esta solución es la latencia en las comunicaciones. Hay que tener en cuenta que un satélite geoestacionario se encuentra aproximadamente a 36000 Km. de la Tierra con lo que una conexión satelital tiene un mínimo de 240 ms. de retardo por el simple hecho de propagarse la señal (la comunicación en un sentido tiene que ir desde la Tierra al satélite y vuelta) y normalmente se obtienen unos retardos de 800 ms. llegando incluso en muchas ocasiones a los 2 segundos. Esto hace que el refresco de los datos obtenidos desde el centro de control no sea cómodo para su visualización.

Tanto en el caso de la línea primaria como en la línea secundaria es necesario negociar con el proveedor una serie de requisitos antes de firmar el contrato.

Es necesario el ISP nos entregue el servicio de Internet en una conexión Ethernet. No debe existir ningún tipo de negación de servicios o conexiones en los firewalls del proveedor, pues esto puede causar que las comunicaciones no se puedan establecer de forma correcta o estable sobre la línea de Internet.

Además es muy aconsejable la obtención varias IP públicas, pero sobre todo que las direcciones asignadas sean estáticas. Esto tiene una razón que en los siguientes capítulos será explicada con detalle. Si el proveedor no puede arrendarnos un rango de direcciones IP públicas y solo se va a disponer de una única dirección IP pública, será necesario exigir que su router esté configurado en modo transparente, ya que si la única IP pública se la cedemos al router del proveedor, será necesario hacer NAT para nuestra red, situación no deseable en ningún caso dadas las limitaciones que impone.

Dependiendo de la ocasión, la configuración del router del ISP puede correr a cargo del propio ISP o puede ser realizada por parte del cliente. Como no podía ser de otra manera, cada una de las posibilidades tiene sus pros y sus contras...

La mayor ventaja de que la configuración sea realizada por parte del personal del departamento de comunicaciones es que seguramente se realice una instalación más ajustada a las necesidades específicas. Además, facilita el acceso para la gestión y monitorización del equipo de forma remota. La desventaja que existe por este lado es que ante un fallo del servicio, que no sea debido al hardware, el proveedor puede argumentar que la causa del problema tiene relación con la configuración o desconfiguración del equipo, siendo el cliente (en este caso el personal de comunicaciones), responsable de la reconfiguración del mismo.

Lo anterior no sucede si es el propio ISP el que realiza la configuración del equipo, pues es su responsabilidad que el servicio de Internet funcione de extremo a extremo. En este caso, es extraño que se facilite la monitorización del mismo más allá de la respuesta al ping.

Además, es necesario comentar que el equipo puede ser adquirido en términos de alquiler o compra. Cuando se alquila el equipo existe la ventaja de que cualquier fallo del hardware será cubierto por el ISP, con lo que seguramente será sustituido por el proveedor sin ningún problema. Por otro lado, si se compra el equipo, este está cubierto solo por la garantía del fabricante y será el departamento de comunicaciones el encargado de realizar todas las gestiones de logística y transporte del mismo, con el trabajo adicional que esto supone.

Antes de explicar más detalles sobre la configuración del router del ISP quizá sea conveniente explicar dónde se instalan estos dispositivos. Cuando se realiza el proyecto del parque eólico, es necesario dejar un espacio físico dedicado a las comunicaciones. Como se comentó anteriormente, la línea del proveedor de Internet suele llegar hasta la subestación. Es en ella, donde se habilita un lugar para el armario o armarios de comunicaciones. Los armarios de comunicaciones tipo rack son los que se usan comúnmente. Se trata de estructuras que protegen a los equipos de comunicaciones del polvo, humedad que incluso disponen de ventilación propia. Suelen tener la posibilidad de cerradura bajo llave para evitar que cualquier persona no autorizada pueda acceder a los equipos. Los armarios de tipo rack, permiten disponer los equipos de comunicaciones de una forma ordenada y sencilla para su manejo, cableado y conservación. De este modo, el router del ISP se instala dentro del rack de comunicaciones junto a los demás equipos de comunicaciones.

El router del ISP, ya sea configurado por el propio ISP o no y sea alquilado o comprado, tiene que ser altamente fiable, capaz de trabajar durante meses o incluso años sin fallos.

# 4. Red comunicaciones o electrónica de red

## 4.1. Introducción

En el capítulo anterior se ha explicado cómo el acceso a Internet llega hasta el parque eólico. Además se ha descrito de forma breve cómo el proveedor de Internet ha de prestar un servicio con al menos una IP pública estática.

En los casos en que el proveedor se encargue de la configuración del router, el trabajo realizado por parte del personal de comunicaciones se limita al trato con el ISP y las correspondientes labores de gestión.

En este capítulo se trata de explicar cómo se realiza la conexión de la red SCADA con Internet, que no olvidemos su objetivo real no es el acceso a Internet, sino el uso de esta para alcanzar el centro de control. La red que se despliega tras el router del ISP es la que provee a las comunicaciones de parque la fiabilidad y la seguridad. En ella se encuentra la electrónica de red redundada que hace posible la continuidad en la teleoperación del parque desde el centro de control ante el fallo de algún equipo.

Por norma se intenta seguir una topología de la red previamente definida por la empresa constructora para alcanzar unos altos niveles de calidad en cuanto a disponibilidad, aunque en ocasiones por requisitos específicos o circunstancias ajenas, la topología de red sufre cambios y exige un mayor grado de estudio para que estos sean lo más transparente posible a las comunicaciones y el resultado final se asemeje cuanto más al estándar.

Hasta ahora no se ha hecho referencia la seguridad de los datos que se transmiten entre el centro de control y el parque eólico. La utilización de Internet para la conexión del centro de control y de producción tiene enormes ventajas, sobre todo económicas. Pero también tiene sus contras. Cuando conectamos a Internet la red del parque eólico es necesario ser consciente de que Internet es una gran red de por si bastante insegura. Para explicarlo de forma breve, es necesario proteger en dos aspectos nuestra red de parque. Por un lado, es necesario evitar accesos no deseados a nuestra red. Esto se consigue con la instalación de firewalls o cortafuegos. Por otra parte, es necesario proveer de una seguridad (tanto en modo de autenticación como de cifrado) a la información que viaja o se intercambia entre el parque eólico y el centro de control. Para ello se realiza una conexión de red privada virtual, más conocidas como VPN.

La realización de la VPN es uno de los puntos sobre los que hay que prestar mayor atención. Las redes privadas virtuales hacen posible la interconexión de ambas sedes de forma totalmente transparente a los operarios que telecontrolan el parque eólico a cientos o miles de kilómetros. Son muchos los parámetros a definir y controlar para que la VPN se realice con éxito.

Todo el sistema de comunicaciones se basa en la idea de las VPN. Sin ellas no sería posible utilizar Internet como medio para comunicar el parque eólico y el centro de control, ya que como se apuntó antes, es inviable que los datos viajen a través de Internet sin ninguna seguridad añadida.

Además de los firewalls, dentro de la electrónica de red nos encontramos con más equipos como son los switches, PCs de monitorización local, PCs de troubleshoting, dispositivos de VoIP, etc.

A continuación se explica de forma resumida algunos conceptos teóricos. Estos son de alguna manera imprescindibles si se quiere entender el funcionamiento de las comunicaciones y seguramente que refuercen la propia explicación.

## 4.2. Conceptos teóricos previos

### 4.2.1. VPN

Una VPN (Virtual Private Network o red privada virtual) es una interconexión (red) que se extiende, mediante un proceso de encapsulación, y en su caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

Existen dos tipos comunes de VPN

Remote-Access: también llamada Virtual Private Dial-up Network (VPDN); es una conexión usuario-LAN usada por empresas que tienen empleados móviles que se conectan desde localidades remotas. Usualmente, las empresas que trabajan este esquema, también contratan un ISP que provea el servicio de Dial-up a sus empleados móviles, y podría incluso ser a través de un número gratuito para conectarse a Internet y comunicarse con la red corporativa a través de un cliente de VPN. Las redes VPN de Remote-Access permiten conexiones seguras y encriptadas entre la red privada de una empresa y los usuarios remotos a través de un proveedor de servicios.

Site-to-Site: A través del uso de equipo dedicado y encriptación a gran escala, una empresa puede conectar múltiples sitios fijos sobre una red pública como Internet. Cada sitio requiere sólo una conexión local a la misma red pública; de ahí proviene el ahorro comparado con líneas privadas dedicadas. Las VPNs Site-to-Site se pueden clasificar como intranets (entre dos oficinas remotas de la misma compañía) o extranets (si se construye la VPN entre oficinas de compañías distintas, ya sea un socio, cliente, proveedor, etc.)

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet publico.

En ocasiones puede ser interesante que la comunicación que viaja por el túnel establecido en la red pública vaya encriptada para permitir una mayor confidencialidad. El éxito de las VPN durante los últimos años ha sido enorme. La causa de ello es que cuando se desea enlazar las oficinas centrales con alguna sucursal u oficina remota existen tres opciones:

La utilización de un MODEM. Se trata de una mala opción ya que tiene diversas desventajas como son el precio de la llamada, el coste de esta llamada sería por minuto conectado, además sería en muchos de los casos una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

Línea Privada: sería necesario tender un cable ya sea de cobre o fibra óptica de un punto a otro. En esta opción el coste es muy elevado porque si por ejemplo se necesita enlazar la oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el precio se dispara.

VPN: Los costes son bajos porque simplemente es necesario el acceso a Internet. Además se tiene la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

Dada esta explicación se entiende que el uso de las VPN es la forma más correcta de realizar la comunicación. Son varios los componentes y aspectos importantes en la realización de una VPN. Estos componentes son simples requisitos pero garantizan que la red sea segura, este disponible y sea fácil de mantener.

A continuación se explica cada uno de los aspectos sobre los que hay que prestar atención para la consecución de una VPN:

Control: el plano de control presta la supervisión meticulosa y funciones de alerta que ofrece algunos proveedores de servicios administrados. Una consideración significativa es que sin importar lo grande que sea la organización, es probable que cuente con varias VPN corporativas y un control exhaustivo sobre el par de extremos que posee la VPN es necesario.

Compatibilidad: para utilizar tecnología VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet.

Escalabilidad y flexibilidad: el mismo equipo puede establecer múltiples VPN contra sucursales remotas sin necesidad de una nueva inversión en hardware. Además pueden ser fácilmente reconfiguradas para la conexión de nuevos equipos o redes completas.

Confianza: cuando una compañía decide utilizar VPNs gestionadas por un proveedor de Internet o un gestor de VPN, está a merced de este.

Autenticación de datos y usuarios: cuando se habla de la autenticación de datos se refiere a que hay que asegurar que el mensaje ha sido enviado

completamente y que no ha sido alterado de ninguna forma. La autenticación de los usuarios es el proceso que permite que el usuario que acceda a la red tenga permiso y además sea quien dice ser.

Sobrecarga de tráfico: En todo tipo de tecnologías existen compromisos, sacrificando algunas características por otras: velocidad contra desempeño, seguridad contra flexibilidad. En el caso de las VPN ocurre exactamente lo mismo. El cifrado de paquetes conlleva un incremento ineludible de la información a enviar, con lo que se compromete la velocidad de traspaso de la información útil.

Sin repudio: se trata de una característica en el proceso de identificación del emisor, de tal manera que no pueda negarlo.

Seguridad: lo es todo en una VPN, desde el proceso de cifrado que implementa y los servicios de autenticación que se eligen hasta las firmas digitales y las autoridades emisoras de certificados que utilizan. Abarca el software que implementa los algoritmos de cifrado en el dispositivo de la VPN.

Son numerosos los protocolos de encriptación que existen en la actualidad pero la mayoría de las VPN usan uno de los siguientes:

PPTP/MPPE- PPTP fue creado en el foro PPTP, un consorcio que incluye a US Robotics, Microsoft, 3COM, Ascend y ECI Telematics. PPTP soporta VPNs multiprotocolo, con encriptación de 40 y 128 bits usando un protocolo llamado Microsoft Point-to-Point Encryption (MPPE). Es importante notar que PPTP por si mismos no provee encriptación.

L2TP**:** conocido como túnel de Layer 2 Tunneling Protocol. L2TP es el producto de la alianza entre miembros del foro PPTP, Cisco y la Internet Engineering Task Force (IETF). Usado principalmente para VPNs de acceso remoto con sistemas operativos Windows 2000, ya que Windows 2000 trae incorporado un cliente nativo de IPsec y L2TP. Los proveedores de Internet también pueden ofrecer conexiones L2TP para usuarios de dial-up (conexión por módem analógico) y encriptar el tráfico entre sus puntos de acceso y los servidores de red de las oficinas remotas.

IPsec**:** es el protocolo de encriptación que se utiliza de forma predominante en las VPN hoy en día, por lo que se realiza un mayor estudio del mismo.

Realmente no se trata de un protocolo, sino de un conjunto de ellos. IPsec fue diseñado por un grupo de trabajo dedicado del Internet Engineering Task Force (IETF). El objetivo para el cuál fue creado IPsec era el desarrollo de un único estándar de seguridad que brindase alta calidad, interoperabilidad y flexibilidad tanto en redes IPv4 como en IPv6. El desarrollo fue iniciado desde la necesidad de interconexión de forma segura de equipos de fabricantes, para una posterior conexión de usuarios también segura.

El grupo de trabajo de IPsec desarrolló mecanismos para la protección del tráfico IP y definió estructura de los paquetes IP protegidos, así como la

implementación de asociaciones de seguridad usadas para las comunicaciones a través de VPN. A pesar de que el protocolo no esté finalizado en cuanto a cuestiones relativas a su gestión de claves, sí que se definen los protocolos específicos para la autenticación, confidencialidad e integridad de datos.

IPsec consiste se asienta sobre tres bases que definen sus dos modos de operación.

- AH (authentication header o Cabecera de Autentificación): Proporciona integridad sin conexión, autentificación del origen de datos, y un servicio opcional de protección antireplay.

- ESP (encapsulated security payload o Carga de Seguridad Encapsulada), puede proporcionar confidencialidad (encriptación), y confidencialidad limitada al flujo de tráfico. También puede proporcionar integridad sin conexión, autenticación del origen de datos, y un servicio de protección antireplay. Uno u otro de estos servicios de seguridad debe ser aplicado siempre que se use ESP.

- IKE (Internet key Exchange) que proporciona el algoritmo de negociación criptográfico y distribuye las claves utilizadas por AH y ESP

Tanto AH como ESP confían en las Security associations (SA o asociaciones de seguridad) negociando las propiedades de una conexión segura utilizando IKE. SA se encarga de la administración de la información negociada entre las dos partes participantes en una VPN. Dicha información incluye las claves criptográficas, sus tiempos de vida, los algoritmos criptográficos usados y el modo de operación utilizado de IPsec.

Para cada modo de funcionamiento se requieren dos SA, una para el tráfico saliente y otra para el entrante. Si los dos modos de funcionamiento (AH y ESP) se utilizan, sería necesaria la negociación de cuatro asociaciones de seguridad. Cada SA está específicamente identificado por un protocolo AH o ESP, IP de destino para una salida o IP de origen de una conexión entrante, y un número entero de 32 bits, utilizado como identificador único (SPI). Otra característica importante de cada SA es su tiempo de vida. El parámetro de tiempo de vida especifica el intervalo de tiempo tras el cual el SA deberá ser renegociado o terminado.

Cada host o Security Gateway que participa posee una información de su SA en lo que se conoce como la Security Assotiation Database (SAD o base de datos de asociación de seguridad). En realidad, una segunda base de datos es necesaria para el funcionamiento de IPsec, que se conoce como Security Policy Database (SPD o base de datos de la política de seguridad), la cual recoge la información de las políticas que serán aplicadas sobre el tráfico. SPD consiste en un conjunto de reglas que llevan la información sobre el tipo de acción que debe realizarse. Una vez que un paquete llega, éste se comprueba contra la base de datos del SPD y así poder tomar la decisión de qué hacer con él. Éste puede ser descartado, distribuido o ser objeto de manipulación por

parte de IPsec. No hay que confundir el la SPD con la SAD, siendo esta última la que suministra los parámetros necesarios para la conexión.

Para decidir qué hacer con un paquete, tres campos se extraen de la cabecera del paquete y se comparan con los respectivos SAD (protocolo IPsec, dirección IP, y SPI). Si se encuentra una coincidencia, los parámetros se comparan con los más campos de AH o ESP. Si no hay coincidencias, el paquete se descarta

AH es uno de los protocolos IPsec que permite comprobar la autenticidad de los datos y el encabezado del paquete IP. No provee un mecanismo para el cifrado de datos, sino que proporciona un valor hash que permite comprobar si el paquete fue manipulado por el camino. Esta forma de encapsulación solo ha ganado un uso bastante limitado, ya que mayoritariamente se tiende a usar ESP solo o una combinación de ESP y AH.

AH también es responsable de la protección del ataque de respuesta mediante el uso de números de secuencia en los paquetes que envía y la aplicación de una ventana deslizante en cada nodo IPsec. Una vez que el paquete IP se recibe, la ventana se adelanta, de modo que los paquetes que llegan fuera de esta ventana se descartan. Lo mismo se aplica a los paquetes con números de secuencia que se repiten.

La autenticación de un paquete se comunicará mediante HMAC. Si cualquier parte del campo de la cabecera IP o datos de campo se ha modificado, el mensaje HMAC calculado en el host receptor sería distinto del original, lo que significa que el paquete fue modificado en tránsito. Por lo tanto, la integridad de los datos transmitidos se comprueba de una manera inequívoca.
IPsec utiliza HMAC empleando varias funciones de hash de un solo sentido como MD5, SHA-1 / 2 y RIPEMD-160.
AH puede operar en el túnel y los modos de transporte y se clasifica en el RFC 2402 como el tipo de protocolo 51.

ESP ofrece encriptación y autenticación de los paquetes IP sin protección a través de una encapsulación.
Tradicionalmente, IPsec utiliza cifrado DES o 3DES. DES se considera débil y puede romperse en cuestión de días o incluso horas si es necesario, por lo que su uso no está recomendado. 3DES, a veces denominado " el DES con esteroides", proporciona un cifrado mucho más fuerte, pero el algoritmo requiere un cálculo matemático intensivo con lo que esto supone un proceso bastante lento en dispositivos con capacidad de procesamiento limitada, como puntos de acceso, equipos antiguos.

Para la protección de la integridad de datos, MD5 o SHA-1 son de uso común para calcular los hashes de los datos incluidos en un paquete. La detección del ataque tipo replay funciona de manera similar a la detección en AH.

ESP se clasifica como protocolo 50 y se encuentra ampliamente definido en el RFC 2402.

Compresión IP

La adición de cabeceras adicionales al paquete IP tras la encapsulación da como resultado un aumento de tamaño del paquete, creando una sobrecarga. La adición puede ser de hasta 300 bytes para el tráfico ESP encapsulados. Si AH se utiliza junto con el ESP, la sobrecarga resultante se incrementa aún más. Esto afecta negativamente al rendimiento de la comunicación, ya que el rendimiento real de las disminuciones de la red. En comparación a las modernas redes cableadas, redes inalámbricas tienen un menor ancho de banda y rendimiento, lo que sobrecarga adicional altamente indeseables.

IPsec intenta combatir este problema con una compresión incorporada IP (IPComp) protocolo que generalmente utiliza los algoritmos de compresión conocidos LZS (*Algoritmos* de compresión Van Jacobson). Estos consisten en que se aplica una compresión antes de cualquier modificación o fragmentación realizada por IPsec. A menudo es inútil para comprimir datos aleatorios o ya comprimidos (por ejemplo, Mp3 o archivos rar.), Puede parecer increíble pero incluso, una vez aplicada la compresión a veces resulta en un aumento del tamaño del paquete IP. Además, si se está usando un túnel IPsec sobre PPP o SLIP, puede ser que ya se realice una compresión de los datos en la capa inferior, por lo que si la compresión que incorpora IPsec se está realizando también, el rendimiento global de la comunicación se verá afectado, ya que los datos se pasan por dos procesos de compresión.

El protocolo IPComp introduce en la negociación un componente adicional. Antes de que los extremos sean capaces de comunicarse, la Asociación IPComp (IPCA) se debe establecer mediante el mecanismo de IKE. Hay que mencionar que IPComp es flexible y se puede aplicar de manera selectiva y utilizarse solo compresión de un protocolo de capa de transporte específico o en un extremo de la conexión establecida.

Existen alternativas a IPsec que utilizan sistemas de cifrado mucho más fuerte, como Rijndael. Funciones de hash criptográficas más seguras son también soportadas, como son el caso de SHA-2 y RIPEMD.

Intercambio de claves y protocolo de gestión.

El IPsec key Exchange y el protocolo de administración (ISAKMP) es una parte del conjunto de protocolos IPsec que definen los procedimientos para la negociación, el establecimiento, modificación y cierre de la SA, así como el formato del paquete utilizado. Fue diseñado para ser independiente de cualquier intercambio de claves específico o técnicas de generación de claves. ISAKMP define lo que se puede entender como el marco general y es más bien abstracto en su aplicación.

Tras la explicación de AH y ESP es necesario abordar el funcionamiento del IKE.

IKE (Internet Key Exchange o Intercambio de las claves de conexión) es un protocolo de de seguridad de intercambio de claves de propósito general que utiliza IPsec para la autenticación de los extremos, negociación de las SAs y el

acuerdo de los algoritmos de encriptación. La RFC 2407 recoge de forma amplia el dominio de operación y el uso que se puede dar al protocolo.

IKE se compone de dos modos diferentes que operan en una o dos fases ISAKMP. Fase 1 se utiliza para la creación de un canal seguro utilizado más adelante para proteger a todas las negociaciones que se dan en la Fase 2.

Las funciones siguientes se realizan durante la Fase 1 de IKE:

- Autenticación y protección de cada uno de los nodo extremo IPsec
- Negociación y comprobación de la coincidencia de la política IKE SA para proteger el intercambio de los IKEs
- Intercambio de claves Diffie-Hellman para establecer un acuerdo en la clave secreta compartida
- Establecimiento del túnel para la negociación de la fase 2 de IKE

Existen tres maneras posibles de negociar la SA en la Fase 1:

- Main Mode: Este modo fue diseñado para separar la información de intercambio de claves de la identidad y de la información de autenticación para proteger la información de identidad en el marco de la clave anteriormente compartida. Este modo de intercambio requiere seis datagramas UDP

- Modo agresivo. Este modo de intercambio permite la transmisión de intercambio de claves, la identidad y autenticación juntos. A menudo se utiliza cuando la protección de la información de identidad no es importante. Se intercambian tres datagramas UDP. Una vez recibido el mensaje de la primera propuesta, se necesitan muchos recursos para generar el mensaje de respuesta. Es posible que se llegue a una denegación del servicio si se envían demasiados mensajes de propuesta sin éxito, como medida de autoprotección.

- Modo base. Cuatro datagramas UDP se intercambian. Este modo se evita la parte de cómputo intensivo del modo agresivo hasta que la parte que inicia la negociación confirma su existencia. Se supone que se acumulan las ventajas del modo agresivo, pero como desventaja presenta que la identidad no se envía protegida a no ser que ambas partes encripten sus claves públicas.

La Fase 2 se utiliza para negociar las SA de IPsec empleadas para establecer un túnel IPsec y así poder establecer la VPN y proteger el tráfico IP.

Las funciones siguientes se realizan durante la Fase 2 de IKE:

- Negociaciones de los parámetros de la SA IPsec

- Establecimiento de la SA IPsec

- Establecimiento del período de renegociación de la SA IPsec.

Por su parte, la fase 2 solo posee un modo de negociación, el conocido como Quick Mode (modo rápido). Se produce después de que el IKE haya establecido con éxito un túnel seguro en el modo 1, por lo tanto, todos los datos utilizados en las negociaciones están encriptados. La conexión puede ser iniciada por cualquiera de los extremos y una o más asociaciones de seguridad IPsec que se negocian en el intercambio de tres mensajes Para que cada uno de los extremos sea capaz de establecer una forma de comunicación segura con el otro, es necesario cumplir un requerimiento de autenticación inicial. La implementación típica de IPsec se basa en los siguientes métodos:

- PSK (Pre-Shared Key o clave precompartida). Este método de autenticación se basa en la posesión de una clave que es conocida por ambas partes. El mayor inconveniente y que compromete seriamente la seguridad es la distribución de la clave al otro extremo.

- Algoritmo de clave pública. Este método de autenticación se basa en la generación de un par de claves pública y privada. Las claves públicas pueden ser intercambiadas de forma segura sobre medios de comunicación insegura, pero también tiene desventajas como la validación del otro extremo (ser quien realmente dice ser).

- Certificados digitales. El sistema público de distribución de claves requiere cierto nivel de confianza. En redes como Internet, donde el control es muy cuestionable y la infraestructura no es de confianza, la distribución de claves puede ser problemático. Lo mismo se aplica a las redes inalámbricas, que son, además, susceptibles a ataques de nivel 2 "man-in-the-middle". Con la introducción de una tercera parte, reconocida como la CA (Certification Authority o Autoridad Certificadora) los certificados digitales se emiten con la identidad del portador del certificado, el nombre o la dirección IP, número de serie, fecha de vencimiento, y una clave pública. El formato estándar de certificado digital se define como X.509.

Otra de las características de IPsec que mejora enormemente la seguridad es Perfect Forward Secrecy (PFS). Cuando está activada, un nuevo intercambio Diffie-Hellman se realiza para cada Quick mode. Por lo tanto, si una de las asociaciones de seguridad ISAKMP se ve comprometida, no afectará a otras asociaciones de seguridad. El inconveniente es que el uso de CPU se incrementa, afectando negativamente el rendimiento de dicho sistema.

### 4.2.2. NAT

El proceso de la traducción de direcciones de red (NAT, por sus siglas en inglés) se desarrolló en respuesta a la falta de direcciones de IP con el protocolo IPv4 (el protocolo IPv6 propondrá una solución a este problema).
En efecto: en la asignación de direcciones IPv4, no hay suficientes direcciones IP enrutables (es decir, únicas en el mundo) para permitir que todas las máquinas que necesiten conectarse a Internet puedan hacerlo.

El concepto de NAT consiste en utilizar una dirección IP enrutable (o un número limitado de direcciones IP) para conectar todas las máquinas a través de la traducción, en la pasarela de Internet, entre la dirección interna (no enrutable) de la máquina que se desea conectar y la dirección IP de la pasarela.

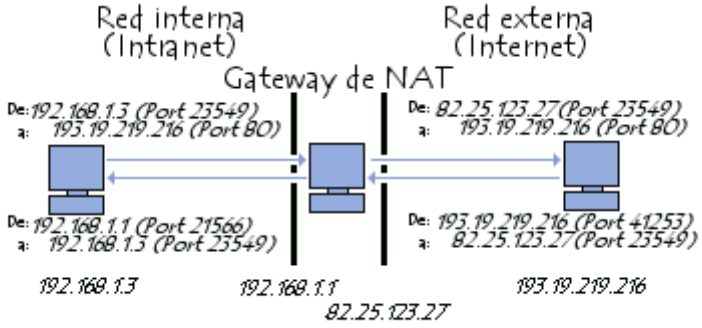



**Figura 1**

Además, el proceso de traducción de direcciones permite a las empresas asegurar la red interna siempre y cuando oculte la asignación de direcciones internas. Para un observador que se ubica fuera de la red, todos los pedidos parecen provenir de la misma dirección IP.

El concepto de NAT estático o NAT 1:1 consiste en hacer coincidir una dirección IP pública con una dirección IP de red privada interna. Un router (o, más precisamente, la pasarela) hace coincidir una dirección IP privada (por ejemplo, 192.168.0.1) con una dirección IP pública enrutable en Internet y, en cierto sentido, realiza la traducción mediante la modificación de la dirección en el paquete IP.

La traducción de las direcciones estáticas permite conectar máquinas de red interna a Internet de manera transparente, aunque no resuelve el problema de escasez de direcciones debido a que se necesitan n direcciones IP enrutables para conectar n máquinas de la red interna.

El NAT dinámico permite compartir una dirección IP enrutable (o una cantidad reducida de direcciones IP enrutables) entre varias máquinas con direcciones privadas. Así, todas las máquinas de la red interna poseen la misma dirección IP virtual en forma externa. Por esta razón, el término "enmascaramiento de IP" se usa en ciertos casos para procesar la NAT dinámica.

Para poder compartir diferentes direcciones IP con una o más direcciones IP enrutables, la NAT dinámica utiliza la traducción de direcciones de puerto, es decir, la asignación de un puerto de origen diferente para cada solicitud, de modo que se pueda mantener una correspondencia entre los pedidos que provienen de la red interna y las respuestas de las máquinas en Internet, las cuales están dirigidas a la dirección IP del router.

NAT supone la manipulación y por ende modificación del paquete IP original para resolver el problema del direccionamiento IP (público/privado).

En cuanto a NAT en entornos VPN, IPsec considera la acción de NAT como un ataque a la integridad del paquete y la conexión no se realiza. Nat-Trasversal es la solución propuesta definida en RFCs 3947 y 3948 en base a los requerimientos definidos en RFC 3475.

Consiste en encapsular la trama cifrada por IPsec (antes de añadirle la cabecera IP final) con un campo UDP y sobre esta cabecera extra se realizan las operaciones de NAT.

### 4.2.3. SNMP

SNMP o Protocolo simple de administración de red es un protocolo que permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red.

El sistema de administración de red se basa en dos elementos principales: un supervisor y agentes. El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

Los switches, routers y servidores son ejemplos de hardware que contienen objetos administrados. Estos objetos administrados pueden ser información de hardware, parámetros de configuración, estadísticas de rendimiento y demás elementos que estén directamente relacionados con el comportamiento en progreso del hardware en cuestión. Estos elementos se encuentran clasificados en algo similar a una base de datos denominada MIB ("Base de datos de información de administración"). SNMP permite el diálogo entre el supervisor y los agentes para recolectar los objetos requeridos en la MIB.

La arquitectura de administración de la red propuesta por el protocolo SNMP se basa en tres elementos principales:

- los dispositivos administrados son los elementos de red (puentes, concentradores, routers o servidores) que contienen "objetos administrados" que pueden ser información de hardware, elementos de configuración o información estadística;

- los agentes, es decir, una aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local desde el periférico en formato SNMP;
- el sistema de administración de red (NMS), esto es, un terminal a través del cual los administradores pueden llevar a cabo tareas de administración.

Si es necesario, se puede obtener toda la información del protocolo SNMP la RFC 1157.

### 4.2.4. VLAN

Una VLAN (Virtual Local Area Network o Red de área local virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

La comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

- VLAN de nivel 1 (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador.

- VLAN de nivel 2 (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación.

- VLAN de nivel 3: existen diferentes tipos de VLAN de nivel 3:

    - VLAN basada en la dirección de red conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

    - VLAN basada en protocolo permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

La utilización de VLANs permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

- mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores.

- aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza.

- disminución en la transmisión de tráfico en la red.

Las VLAN están definidas por los estándares IEEE 802.1D, 802.1p, 802.1Q y 802.10-

## 4.3. Electrónica de red

La electrónica de red que se instala tras el router del operador trata de dotar de seguridad a las comunicaciones del parque así como proteger a los propios equipos de la red de producción. Estos equipos se disponen en lo que se conoce rack o armario de comunicaciones. Normalmente, el router del operador también se encuentra en el rack de comunicaciones del parque eólico. Realmente no se dispone de un solo router si no de dos routers, ya que siempre se dispondrá de dos líneas de Internet.

Para poder lograr una alta disponibilidad de las comunicaciones se utiliza la redundancia como norma. De esta manera todo equipo de red imprescindible para las comunicaciones con el centro de control esta duplicado.

Introduciendo cada uno de los equipos que típicamente se instalan en el rack, ordenándolos en sentido desde el router del operador hacia el interior de la red de parque nos encontramos con:

- Switches WAN
- Firewalls
- Switches LAN
- SAI (Sistema de alimentación ininterrumpida)

Switches WAN

Los routers de los ISP suelen proporcionar un solo cable Ethernet para su conexión a nuestra red. Típicamente, este cable debería ir conectado al Firewall, pues todo el equipamiento que se encuentre tras él ya se encuentra protegido. El problema que existe en este punto es que se necesitan dos cables, pues también se instalan dos firewalls. Por ello es necesario introducir un switch entre el router del proveedor de Internet y el firewall. Destacar que existen dos proveedores y dos firewalls, con lo que también es necesario disponer de dos switches.

A estos switches se les denomina switches WAN, ya que se encuentran en la parte externa del firewall, en su interface WAN (Wide Área Network).

Como toda la electrónica de red que se instala en la red externa de comunicaciones, los switches WAN han de ser gestionables. Es decir, es necesario que dispongan de mecanismos por los cuales puedan ser configurados.

La función básica e imprescindible de los switches WAN es la de replicador del puerto disponible en router hacia ambos firewalls. Esta función también es cumplida por parte de los switches sin gestión, pero en absoluto son los más recomendados

Es cierto que la instalación de switches gestionables encarece de una forma abultada el precio de los mismos, pero es un requerimiento fundamental para la monitorización del estado de los equipos, pues la identificación y resolución de futuros problemas se hace más compleja sin esa capacidad de gestión.

La gestión en estos equipos aporta unas funcionalidades dependiendo de la gama y del fabricante en cuestión. Los switches gestionables con una cierta calidad permiten realizar configuraciones muy diversas, agregan un plus de seguridad y suelen gozar además de mayor fiabilidad.

Los switches gestionables suelen implementar los protocolos HTTP, Telnet y SSH para su configuración, así como SNMP para su monitorización.

Los swtiches Ethernet han sido desde siempre dispositivos de capa 2 del modelo OSI. Es decir, trabajan con tramas Ethernet. Tienen la gran ventaja respecto a sus antecesores los hubs en que cada una de sus interfaces representa un dominio de colisión independiente, con lo que las prestaciones en cuanto a velocidad se disparan. Últimamente se tiende a utilizar switches de capa 3. Esto a priori parece una contradicción, ya que los equipos de capa 3 del modelo OSI son los routers. Los switches de capa 3 no son capaces de realizar las mismas tareas que los routers (ni lo pretenden), pero si que son capaces de conmutar paquetes entre diferentes VLANs, que tanto se utilizan hoy en día. Realmente se diferencian en que las tareas de routing se realizan por hardware en el caso de los routers y por software en el caso de los switches de capa 3.

La configuración que se aplica a los switches WAN (y de todos los equipos de la red de comunicaciones) depende por completo de las características del servicio de Internet que preste el ISP. En capítulos anteriores se comentó la recomendación de contratar varias direcciones IP públicas (un rango, haciendo subnetting) al proveedor de Internet, pero esto no es siempre posible. Es conveniente explicar los tres escenarios en los que la configuración varía de forma significativa.

- Concesión por parte del ISP de una dirección IP pública (arrendada al router). En esta situación, la única dirección IP pública que el ISP nos asigna es utilizada por el router que nos proporciona el ISP. De esta manera, es necesario el uso de NAT y de una asignación de direcciones IP privadas a cada uno de los equipos que componen la red exterior de comunicaciones.

- Se trata de una situación nada recomendable, pues para la realización de la VPN contra el centro de control es necesario que el router del operador disponga de la opción NAT Passtrough o NAT transversal, aunque con esta característica tampoco está garantizado el

funcionamiento correcto de la misma. Estos casos se dan cuando el servicio de Internet que se contrata tiene un perfil más parecido al residencial que al empresarial. Evidentemente el switch WAN también tendrá una dirección IP privada, pero es importante remarcar, que esta no será del rango de direcciones IP existente en el segmento de red comprendido por el interface "LAN" del router del ISP y el interface WAN del firewall a instalar. Es necesario poder llevar a cabo la gestión de los switches WAN remotamente, con lo que la dirección IP a asignar debe ser del segmento de red conectado a alguna de las interfaces LAN del firewall. Es decir, una dirección de una de las redes del parque eólico, que será alcanzable solo bien desde la propia red interna o bien a través de la VPN desde un sitio remoto. Por ello, será recomendable crear dos VLANs en el switch: una dedicada a su función como duplicador de puertos hacia los firewalls y otra con, al menos un interface físico en ella, para su gestión. Se trata de un switch WAN con la gestión en la parte LAN.

- Concesión por parte del ISP una dirección IP pública (para su uso). En este caso, como en el anterior, tan solo se dispone de una dirección IP pública, aunque esta es posible asignársela a uno de los equipos de la red de comunicaciones. Obviamente, la dirección IP pública de la que disponemos está destinada para el interface WAN del firewall. Esto facilita mucho el establecimiento de la VPN. En este caso, como ocurre en el anterior, la gestión del switch WAN se realizará a través de una VLAN de gestión a la cual pertenezca una interface física conectada a alguno de los interfaces LAN del firewall.

- Concesión por parte del ISP de un rango de direcciones IP públicas. Disponer de varias direcciones de IP públicas es la mejor idónea. Se asignará una al firewall, otra al switch WAN y otras se pueden utilizar para otros fines, tal como algún servidor cuyo acceso desde Internet no consienta hacer NAT. Para esto es necesario que el ISP nos ceda una subred con una máscara de subred /29 (255.255.255.248) o menor, ya que no hay que olvidar que el router del proveedor utiliza también una dirección IP en su interface hacia nuestra red.

  Dado que la dirección IP del switch WAN es pública, se podrá acceder a su gestión cualquier ordenador con Internet. Además no será necesario el cable adicional hacia la parte LAN del firewall como ocurría en los dos casos anteriores. Esta situación parece que sólo tiene ventajas pero no es así. No hay que olvidarse que el firewall es el equipo que protege a todos los demás equipos de accesos indeseados desde Internet, pero solo en el caso en que estos se sitúen tras el firewall.

  En cambio, ahora este switch está situado justo antes del firewall, por lo que carece de su protección. Dada la importancia que tienen la seguridad de las comunicaciones de los parques eólicos, no sería nada recomendable dejar un dispositivo "expuesto" a Internet tan solo protegido con una clave.

Por todo ello y si el presupuesto lo permite, lo más recomendable es la utilización de switches con ACL (Access lists). Las access lists no son otra cosa que una funcionalidad en el plano de gestión cuya función es permitir acceso a la gestión desde unas direcciones IP que se han preestablecido. Por ello, con añadir las IPs públicas que se tengan desde las oficinas del departamento de comunicaciones a las TRUST IPs (IPs de confianza) bastará para que el switch WAN quede con una protección casi total.

Firewalls

El firewall o cortafuegos, es el corazón, el núcleo de toda la electrónica de red. Se trata de una pieza muy valiosa dentro del conjunto, pero evidentemente es necesario que existan los demás componentes para que el firewall pueda llevar a cabo sus funciones.

Al igual que la demás electrónica de red, el firewall también se encuentra redundado. Por lo general, se suelen denominar Main firewall (firewall principal) y firewall de backup (firewall de respaldo). En este caso no se trata de una redundancia física como era el caso de los routers de los proveedores o los switches WAN. Hace falta algo más.

Cuando se dispone de una pareja de firewalls con los cuales se quiere obtener una redundancia es necesario configurarlos en lo que se conoce como alta disponibilidad (high availability). Esta técnica, que es necesario que la marca y modelo de firewall permita su uso, dota de una inteligencia extra a los dispositivos.

La disposición de alta disponibilidad se basa en lo siguiente: ambos firewall están encendidos y configurados de la misma manera a excepción de que uno de ellos se ha designado como Main (firewall principal) y el otro como backup (de respaldo). Los firewalls están interconectados directamente por un cable Ethernet a través de una interface exclusivamente designada para ello. Cada uno de los firewalls conoce su pareja porque a cada uno se ha introducido la dirección MAC del otro en la configuración. Además, solo uno de los firewalls está activo (por lo general el Main) y el de backup está en modo idle (reposo). Cuando el firewall principal falla, debido por ejemplo a un fallo eléctrico, o que un interface deja de funcionar, el firewall de backup toma el control y pasa a estado activo. Dado que ambos firewalls están todo el rato sincronizados, el cambio se realiza de forma casi instantánea, permitiendo una conmutación que apenas será apreciada por los usuarios.

Otra de las características a destacar en cuanto a los firewall que se instalan en los parques eólicos es la necesidad de tener al menos dos interfaces WAN. Es la única manera de aprovechar la redundancia de líneas de Internet. La redundancia de líneas de Internet se puede utilizar rasgos de dos maneras: mediante un balanceo de la carga o bien utilizando una de las líneas y solo conmutar a la secundaría cuando la primaria falle.

El firewall es también el encargado de conmutar, de realizar esta operación. Esto es conocido con el WAN FailOver. Que funcione el sistema de WAN FailOver significa que el firewall ha conseguido “darse cuenta” de que la línea en funcionamiento ha fallado y es necesario que las comunicaciones sean encaminadas a través de la otra línea. La monitorización del estado de las líneas de Internet es realmente sencilla. Se suele disponer de un lugar en la configuración del firewall en el que se introducen unas direcciones IP de Internet. El firewall realizará un ping continuo a estas direcciones IP. En el caso de que no se obtenga respuesta, entenderá que la línea se encuentra caída y conmutará automáticamente hacia la otra línea. En este caso se está confiando en que las direcciones públicas a las que el firewall hace ping no fallen y lleven a engaño al firewall. Por eso se pueden configurar varias direcciones IP de prueba e incluso configurar el sistema en una lógica en la que si alguna de ellas contesta, es que el servicio sobre esa línea se encuentra levantado.

En ocasiones se da la circunstancia de que el proveedor de Internet se ofrece y pone a nuestra disposición la posibilidad de que su router sea el encargado de utilizar una u otra línea. Esto no es aconsejable por varios motivos: es mejor tener cuanto más control de la situación; si el WAN FailOver puede ser implementado por el interesado ha de hacerse así. La otra razón es que si el proveedor de Internet ofrece este servicio, significa que ambas líneas están contratadas al mismo proveedor, con lo que si existe un corte del servicio generalizado en la red del operador en la zona, el parque quedará totalmente incomunicado. Aunque pueda trazar rutas diferentes para cada línea, es más que probable que la última milla esté compartida físicamente.

Evidentemente el firewall realiza las tareas de cortafuegos. Esta es una función realmente importante, ya que la seguridad de la información que se encuentra en los servidores de la red SCADA está totalmente confiada a los firewalls. Es cierto que el coste de un firewall está muy asociado a la versatilidad, la flexibilidad y posibilidades que brinde pero también es cierto que el gasto en estos dispositivos está más que justificado en le caso de los parque eólicos.

Un dispositivo conectado a Internet es, de por sí, altamente vulnerable. Y no sólo es necesaria la protección desde fuera (desde Internet) hacia la red de parque, también es interesante tener la capacidad de regular (denegando o permitiendo) el acceso desde unas de las redes a otras, internamente.

Lo más común es que se instalen firewalls con dos interfaces WAN, al menos dos interfaces LAN y el interface dedicado a la interconexión con el firewall de backup en configuración de alta disponibilidad. La razón por la que es aconsejable disponer de los interfaces LAN no es otra que la de separar la red SCADA de la red de ofimática. La red SCADA ha de estar muy controlada. En ningún caso se tendrá un libre acceso a Internet ni entrante ni saliente desde la red SCADA. En contraposición, si que puede ser necesario que la red de ofimática, prevista para el trabajo diario de los operarios de parque, tenga acceso a Internet. Por ello, también los firewalls de gama alta también permiten la implementación de políticas de QOS (quality of service, calidad de servicio) a través de las cuales se puede reservar un ancho de banda a la conexión de la red SCADA y limitar al sobrante la red de ofimática. El ancho de banda de las

conexiones es un bien preciado, por lo que hay que gestionarlo de la mejor manera.

Todas las características que hasta ahora se han explicado acerca de los firewall que se instalan en los parque eólicos son bastantes importantes, de hecho son imprescindibles. Una vez configurado el cortafuegos del parque su red goza de una alta seguridad. Además se da por hecho que en el centro de control también se dispone de una red debidamente protegida, utilizando para ello habitualmente, la misma marca de firewall que en los parques eólicos. Queda pues, proteger la información que se intercambian centro de control y centro de producción (parque eólico en este caso). La manera en la que se realiza esto es a través de VPN. Los firewalls tanto del centro de control como del parque eólico son los encargados de realizar la VPN. El establecimiento de una VPN hace seguro el intercambio de información de dos redes seguras a través de una red insegura o al menos incontrolada como es el caso de Internet.

Existen muchos tipos de VPN, pero sin duda las más extendidas son las de tipo IPsec y gracias a la versatilidad que ofrecen son las que se utilizan para el establecimiento de una comunicación segura entre el centro de control y el parque eólico.

Existe la posibilidad de que la VPN se pueda realizar entre los routers de los operadores, pero no es la mejor opción pues es necesario tener un control absoluto de los dispositivos que realizan las VPN por si fuera necesario realizar cambios o mejoras.

Los centros de control monitorizan un alto número de parques eólicos. Cada parque está aislado del resto de parques y solo se comunica con el centro de control. Es decir, con las VPN se construye una red con topología en estrella cuyo punto común es el centro de control. Para que todo funcione correctamente, es necesario asignar a cada parque eólico un direccionamiento IP privado único. Es más, lo más normal es destinar un par de direccionamientos IP por parque: uno para la red SCADA (típicamente una clase C, 254 direcciones disponibles) y otro para la red de ofimática de parque (típicamente media clase C, 127 direcciones, aunque depende mucho de las necesidades de la propia red). La gestión y asignación de las direcciones IP es un tema al que hay que prestar bastante atención y mantener un listado actualizado del direccionamiento IP que se usa para evitar problemas.

Para el establecimiento de la VPN es necesario realizar la configuración en el firewall de ambos extremos. Para el establecimiento de la comunicación lo imprescindible es conocer la IP del centro remoto contra el que se quiere realizar la VPN. Esta es la razón de que la dirección IP pública que nos asigne el ISP del parque eólico sea estática.

Es necesario introducir en cada uno de los firewalls las redes locales que se desea sean accesibles desde el otro extremo y además han de coincidir las subredes. Puede que se necesite que solo ciertos equipos del parque eólicos sean accesibles desde el centro de producción o que solo sean accesibles

desde unas ciertas direcciones del centro de control. En general, se interconectan todas las subredes contra todas las del otro extremo y más tarde con políticas de firewall se permite o deniega el acceso según interese.

Una vez establecida la VPN es toda una ventaja el acceso a la configuración del firewall del parque eólico sin tener desplazarse al mismo. De esta manera se pueden realizar cambios, incluso sobre la VPN. De todos modos, siempre dependiendo de las limitaciones del firewall, se puede acceder a la configuración del firewall tanto a través de la VPN, como a través de la dirección IP pública asignada a cualquiera de las interfaces WAN.

Switch LAN

Dado que los firewalls que se instalan en los parque eólicos disponen de interfaces LAN a modo de router (cada interface pertenece a un segmento de red diferente y no está permitido lo contrario) es necesaria la utilización de un switch si se quieren conectar más de un dispositivo en cada red.

Al dispositivo se le conoce como switch LAN para poder diferenciarlo de los que se instalan entre el router del operador y el firewall. Su uso está totalmente dedicado a la red de ofimática. Se utilizan switches gestionables que puedan ser enracables para su instalación dentro del armario de comunicaciones. Según el escenario, puede ser interesante la realización de VLANs. A los switches LAN suelen conectarse los PC de operarios, impresoras de red, escáneres o incluso teléfonos IP.

Para la red SCADA no se instala ningún otro dispositivo de comunicaciones, sino que el interface LAN SCADA del firewall se conecta directamente con equipos de la red SCADA. Estos equipos suelen instalarse en un armario aparte, dado que ya se trata de las comunicaciones internas del parque eólico y suele ser gestionado por personal de diferente departamento.

SAI

Los sistemas de alimentación ininterrumpidos (SAI) son otro de los dispositivos de red que se instalan en los armarios de comunicaciones. Los parques eólicos, por paradójico que parezca no gozan de una buena calidad en cuanto al suministro eléctrico e incluso los cortes eléctricos son habituales por disparos en la subestación. Contando con un SAI que alimente a la electrónica de red proporcionamos una mejor electricidad, ya que la salida de electricidad de los SAI está rectificada. Además se previene de cortes que pueden provocar daños en los dispositivos. Con una pequeña inversión se protege a equipos que tienen mayor valor, no solo económico, sino por las pérdidas que puede acarrear si dejan de funcionar.

Además, se puede instalar una tarjeta de red en el dispositivo que permita su gestión. El SAI pertenece a la red de ofimática, con lo que se le asigna una dirección IP del rango y se conecta a la red a través del switch LAN. De esta manera, se saca un rendimiento extra al SAI.

En la mayoría de marcas se pueden configurar alarmas que avisen por medio de email del paso a modo baterías de la unidad. Con esto se puede actuar de manera proactiva y por ejemplo, se puede poner en conocimiento del personal de guardia que la subestación (o al menos el magnetotérmico del que el SAI toma la alimentación) está desarmada y que si no se actúa antes de que se acaben las baterías, se perderá todo contacto remoto con el parque eólico.

# 5. Comunicaciones internas de parque: Red SCADA

## 5.1. Introducción al sistema

El término SCADA (Supervisory Control and Data Acquisition, Control supervisado y adquisición de datos) hace referencia a la tecnología que permite que un usuario tenga acceso a datos sobre el estado de un sistema remoto a la vez que tenga la posibilidad de enviar instrucciones de control.

Los sistemas SCADA se utilizan en aquellas instalaciones que requieren unos niveles de seguridad elevados, como es el caso de los parques eólicos, donde cualquier avería puede acarrear un resigo inaceptable. Es necesario ser consciente de que un parque eólico no es un sistema aislado, sino que forma parte de la red eléctrica y por ello ha de estar en todo momento monitorizado.

Debe de existir un operario humano supervisando el funcionamiento de los sistemas críticos, con capacidad para enviar órdenes de control. El operador puede detectar gracias a estos sistemas, condiciones de funcionamiento anómalas, y realizar una intervención manual sobre el sistema para evitar males mayores.

Hoy en día los sistemas SCADA que vienen implementados en los aerogeneradores se encuentran en tales niveles integración que toda acción puede ser ejecutada remotamente, a excepción de los trabajos propios de mantenimiento.

De esta manera, con el uso de la tecnología SCADA como sistema de monitorización remoto permite una rápida identificación de los elementos problemáticos, haciendo más ágil su sustitución. En las zonas de difícil acceso puede que el personal de mantenimiento sólo pueda desplazarse una o dos veces al año. Si hay que sustituir un equipo averiado, es importante saber qué equipo hay que reemplazar para llevar todo el material necesario y así ahorrar viajes innecesarios y costosos.

Un aspecto muy importante de un sistema SCADA es que debe permitir el envío de órdenes de control más o menos complejas hacia el sistema remoto. Esto diferencia un sistema SCADA de un sistema de telemetría, ya que normalmente estos sólo permiten una comunicación unidireccional de los datos desde los elementos remotos hacia la estación de visualización.

No hay que olvidar que todo lo que se ha explicado en capítulos anteriores sobre la conexión a Internet del parque eólico, la electrónica de red, las VPN con el centro de control, etc. no son más que herramientas para conseguir que este sistema SCADA sea llevado más allá del recinto del parque eólico

## 5.2. Componentes del sistema de telecontrol

El puesto de operación local, el interface del operador, los sistemas de control local y los sensores y actuadores son los elementos que gobiernan el funcionamiento de un parque eólico, todos ellos conectados a través de un sistema o red de comunicaciones.

A continuación se describe cada uno de ellos.

Puesto de operador local

El ordenador central de la instalación (Master Terminal Unit) se encuentra localizado en el edificio de la subestación transformadora del parque eólico, constituyendo lo que se denomina Puesto de Operación Local (POL). En este puesto se reciben los datos provenientes de los aerogeneradores que componen el parque y habitualmente de las torres meteorológicas ubicadas en el emplazamiento. En algunos casos el sistema de control de la subestación se integra en el POL permitiendo realizar determinadas maniobras de operación de la instalación como descargos de las líneas, rearme de interruptores, etc.

Este puesto proporciona acceso a toda la información del parque eólico en tiempo real. Por este motivo es fundamental garantizar, por un lado, el funcionamiento continuado del puesto, lo que justifica una vez más, al igual que para la electrónica de red, la utilización de SAIs y por otro, unas comunicaciones de calidad que enlace el sistema de control del parque eólico con el sistema de gestión remoto situado en el telemando. Esto es debido a que la información que llega a los operadores del centro de control remoto no llega directamente de las turbinas o estaciones meteorológicas, sino que todas esas miles de variables se vuelcan en este ordenador y este hace de servidor a los clientes remotos instalados en el centro de control.

Además es habitual implementar un terminal duplicado de este puesto de control en las oficinas del promotor o cliente final. A través de la VPN establecida con sus oficinas, el cliente tiene acceso directo y en tiempo real a toda la información relevante relacionada con la explotación del parque eólico (datos meteorológicos, producción de energía, alarmas...)

Interface del Operador

Es el software de telecontrol instalado en el puesto de operación local del parque eólico. Engloba diferentes módulos de programación, básicamente orientados a realizar las tareas de control de determinados parámetros de la instalación, a la vez que a emitir informes de tipo estadístico de dichos parámetros.

En el POL se almacena en una base de datos y en tiempo real información relativa a los aerogeneradores, subestación y torres meteorológicas. Con esta información es posible realizar informes de explotación donde se recogen las producciones individuales de cada máquina, seguimiento del tipo y duración de

fallos en el parque, comparación entre las previsiones de producción realizadas en el estudio de viabilidad y los datos reales medidos.

Sistemas de Control Local

Generalmente, un autómata programable situado en la base del aerogenerador es el encargado de recoger, almacenar y transmitir la información de las señales tanto analógicas como digitales que gobiernan el funcionamiento del mismo. Estos equipos integran los diferentes sistemas de regulación y control de un aerogenerador, cuyas funcionalidades son muy diversas.

Debido a la caída progresiva de los precios de los ordenadores, estos sistemas ubicados en cada aerogenerador se han convertido en sistemas complejos capaces de gobernar por sí mismas el funcionamiento completo de la turbina. Normalmente, un PLC que integra diferentes reguladores, procesa la información recogida por los diferentes sensores ubicados en el aerogenerador y envía señales de control a los diferentes subsistemas que optimizan el funcionamiento global para las infinitas condiciones de viento existentes. En aerogeneradores de última generación, el control del sistema se ha distribuido entre la unidad central ubicada en la base y una unidad de control auxiliar o de apoyo localizada en la góndola, la cual se encarga fundamentalmente de la comunicación de los distintos componentes de la turbina con la unidad principal, enviando la información recogida por los diferentes sensores.

Por oto lado,  casi la totalidad de los fabricantes, permiten una parametrización manual del sistema del aerogenerador de forma local, es decir, que un operario ubicado físicamente dentro del aerogenerador puede configurar manualmente los valores de consigna que controlen el funcionamiento del mismo. Los sistemas de control local han de incorporar funcionalidades a las que se acceda de forma manual, que resultan imprescindibles durante las tareas de pruebas y puesta en marcha del aerogenerador y que serán también necesarias durante la vida útil del mismo, para realizar las tareas de operación y mantenimiento. Sin embargo, debido a los exigentes criterios de integración en la red que tienden a imponerse en los sistemas de generación eléctrica proveniente del viento, es más que deseable poder acceder a la parametrización de los PLCs de cada aerogenerador de forma remota. De esta manera, resulta posible implementar sistemas de control automáticos. Hoy por hoy, la implantación es masiva y en un breve período de tiempo dejará de ser una opción para convertirse en un requisito si se quiere mantener en un mercado eólico cada vez más exigente y competitivo.

Sensores y actuadores

El sensor es el dispositivo capaz de producir información sobre el estado de determinadas variables que se pretenden regular, convirtiendo las viables a medir en señales eléctricas al igual que hacen los transductores. Por otra parte, el actuador es un dispositivo que, en función de la señal generada por una unidad de control, modifica un parámetro de un determinado proceso con el objetivo de que el valor real de la variable en cuestión se acerque lo máximo a los de la consigna, como buen sistema de control.

En un aerogenerador existen gran variedad de sensores que recogen los datos necesarios para la optimización del funcionamiento del mismo. Al subsistema de control le pueden llegar datos de sensores de temperatura, tacómetros, encoders (posición) anemómetros o medidores de presión del circuito hidráulico. Las señales generadas por todos estos sensores pueden ser tanto digitales como analógicas, por lo que estas deben ser adaptadas antes de poder ser utilizadas de manera conjunta por el regulador correspondiente. Al igual que en el caso de la electrónica de red, los sensores que se utilizan en un aerogenerador deben estar preparados para funcionar en condiciones adversas, que van desde elevadas temperaturas en verano hasta temperaturas extremadamente bajas en invierno.

Cada subsistema del generador está convenientemente equipado de sensores que recogen la información relevante y la envían por medio de buses de campo a la unidad central o auxiliar. Estas unidades aportan las medidas físicas del aerogenerador, en función de las cuales el sistema de supervisión envía consignas de control a los diferentes actuadores que forman parte de los elementos que intervienen en las maniobras propias del funcionamiento del aerogenerador.

Medio de transmisión

La fibra óptica es utilizada en la mayoría de los casos como medio de transmisión entre molinos y los molinos en la subestación, es decir, en toda la red interna de parque. Se evitan en todo momento medios de cobre para la transmisión de datos, consiguiendo así un aislamiento eléctrico en la red de comunicación del parque eólico, además de una óptima respuesta frente a ruidos e interferencias electromagnéticas (EMI).

La fibra óptica se sitúa en zanjas de media tensión de los circuitos interiores del parque eólico. Independientemente del tipo de zanja, la fibra se sitúa directamente sobreterrada junto a los cables de potencia y preferiblemente junto a la pared de la zanja, totalmente horizontal y minimizando el uso de arquetas.

La manguera de fibra óptica es típicamente de 8 fibras mínimo, contemplando 2 tipos en función de la distancia del tendido. La fibra empleada entre turbinas será usualmente multimodo mientras que tendidos de fibra en largas distancias como entre la subestación y grupos de aerogeneradores o edificios lejanos, etc. será realizado utilizando fibra monomodo. De forma general:

- Monomodo para tendido superior a 2 Km. Núcleo E9/125.
- Multimodo para distancias inferiores. Núcleo G50/125.

En cada aerogenerador la fibra penetra físicamente hasta 10 metros para permitir conexiones de forma holgada.

Por causas de rendimiento, los aerogeneradores de los parques eólicos se disponen en enfilaciones, pudiendo tener un parque un número variable de

generadores por enfilación y enfilaciones. Debido a esto, la fibra óptica que conecta cada enfilación con la subestación crea una topología en anillos, todos ellos con la subestación como punto en común. Además, la fibra óptica se distribuye en cada enfilación alternando los aerogeneradores para realizar la "vuelta" sobre los que no se conectaron en la "ida". Esto se puede observar en la siguiente figura.

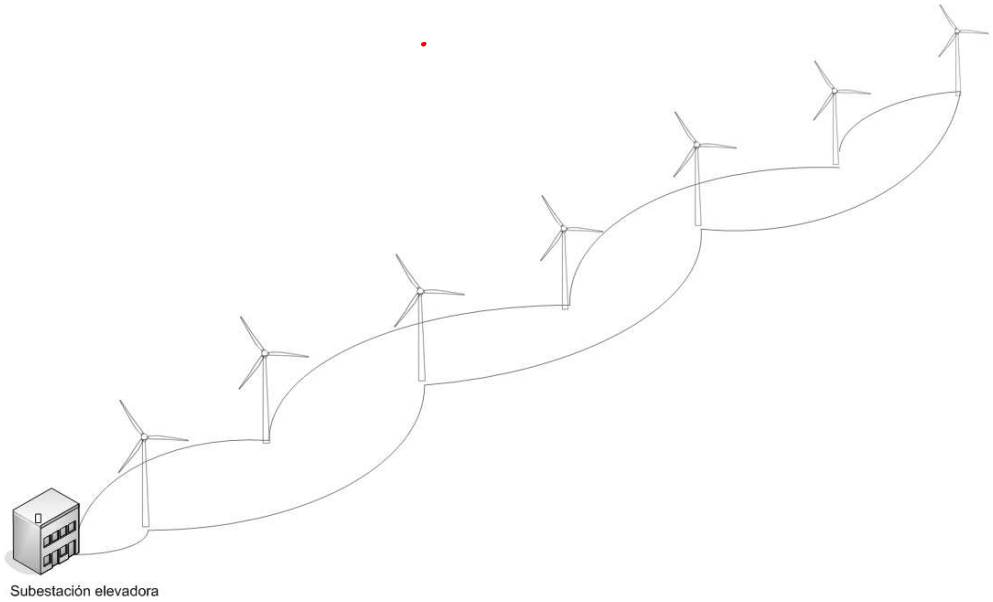



**Figura 2**

Con esta técnica se obtiene la mencionada topología en anillo sobre cada enfilación, con la ventaja de que se libra la gran distancia entre el último molino y la subestación.

Protocolo de aplicación

El nivel de aplicación (nivel 5 TCP/IP) se implementa mediante un protocolo estándar abierto como es Modbus. (MODBUS sobre TCP). El controlador de la turbina es un esclavo (Servidor de datos) que envía datos en respuesta a las peticiones del puesto de parque, maestro (Cliente de datos). Las direcciones MODBUS en las que aerogenerador vuelca la información corresponden a unos determinados registros de la pila de memoria del controlador PLC. El maestro utiliza las funciones MODBUS para leer en bloques todos los datos necesarios.

La información digital (alarmas y estados) es compactada en los mismos bloques que los datos analógicos, de manera que todos los datos de la turbina (analógicos y digitales) son enviados con las mínimas peticiones posibles.

# 6. Caso real

## 6.1. Introducción

La explicación que se ha realizado hasta ahora tanto de las comunicaciones externas como la propia red de parque ha sido puramente desde un punto de vista teórico. Como complemento a ello, se ha visto oportuno destinar un capítulo a la implementación de un caso real en el que se pretende instalar y configurar todos y cada uno de los dispositivos con el fin de comunicar un parque eólico con su Centro de Control.

Es necesario advertir que las marcas y modelos de los dispositivos que se han utilizado son una de las múltiples opciones o posibilidades que existen en el mercado. No se trata ni de los mejores equipos ni de los únicos que se pueden utilizar. Sencillamente se trata de unas marcas comerciales que cumplen las funciones para las que se van a destinar. En el anexo final se pueden encontrar las hojas de características de cada uno de los equipos que se han utilizado.

En la explicación se detalla la implementación y configuración de los equipos que se instalan en el parque eólico, dando por hecho que los equipos del Centro de Control se encuentran totalmente configurados.

En el caso que se va a tratar, la red que se despliega tiene las siguientes características:

- El proveedor de Internet principal (ISP1) ofrece un servicio ADSL con un router Cisco 1841 a cuya configuración se ha tenido acceso pero tan solo en modo lectura.

- El proveedor de Internet secundario (ISP2) ofrece un servicio ADSL aunque el MODEM/router ADSL se encuentra fuera del parque eólico. A través de un radio enlace con dispositivos Mikrotik se consigue hacer llegar la conexión a Internet secundaria a la subestación del parque eólico.

- Switches WAN: se han utilizado dos switches Cisco 3560 8 puertos. El que distribuye la conexión del ISP1 posee una IP pública para su gestión; el switch WAN del ISP2 posee una IP privada. La IP de gestión pertenece a la red de ofimática.

- Firewall: se utilizan 2 appliances SonicWALL, de la gama NSA, modelo 2400, en alta disponibilidad. Estos equipos disponen de dos interfaces WAN y 4 interfaces LAN.

- Switch LAN: switch Cisco 2960 de 24 puertos para uso en la red de ofimática.

- SAI: UPS de la marca APC, de 1500 VA, con tarjeta de red para su gestión. Se configura con una IP de la red de ofimática.

- Conversor optoelectrónico: dado que en el caso en estudio la subestación y la sala de control se encuentran separadas por varios kilómetros, se utiliza fibra óptica para su comunicación. En este caso se ha utilizado un Moxa de la gama EDS, con 6 puertos de cobre y dos pares de fibra óptica, todos ellos Ethernet.

- Switch SCADA: se trata de un switch de la casa HirschMan, (Belden) modular y de gran robustez.

- Servidor y cliente SCADA. Es necesaria la inclusión de un servidor en la red donde se vuelvan todos los datos desde los molinos y de un cliente que sirve como equipo de monitorización local del parque eólico. Ambos equipos son PCs con sistema operativo Windows en los cuales se instala el software SCADA pertinente.

El segmento de subred de IPs públicas ofrecidas por el ISP1 es 12.144.25.104/29 con lo que se dispone de 6 direcciones IP públicas.

En el caso del ISP2, tan sólo se dispone de una dirección IP pública (91.188.12.226). Por este motivo es necesario realizar NAT en el MODEM/router ADSL y por consiguiente, una interface WAN del SonicWALL y la IP de gestión del switch LAN 2 tendrán IP privadas.

La red de ofimática tiene asignado el rango de IPs 192.168.52.0/25, con lo que se dispone de media clase C (126 direcciones utilizables).

La red SCADA tiene asignado el rango de IPs 192.168.51.0/24, con lo que se dispone de una clase C completa (254 direcciones utilizables)

A continuación, en la figura 3, se muestra el esquema a nivel físico de la red de comunicaciones.

En la figura se puede apreciar cómo a través de Internet se conecta el centro de control con los routers de los proveedores de Internet. Estos son conectados a los Switches WAN, que a su vez “cruzan” la conexión a cada uno de los firewalls.

Los firewalls se encuentran también interconectados directamente para disponer de un canal de comunicación para su sincronización. De los interfaces de los firewalls se crean dos redes de área local: la red SCADA y la red de ofimática.

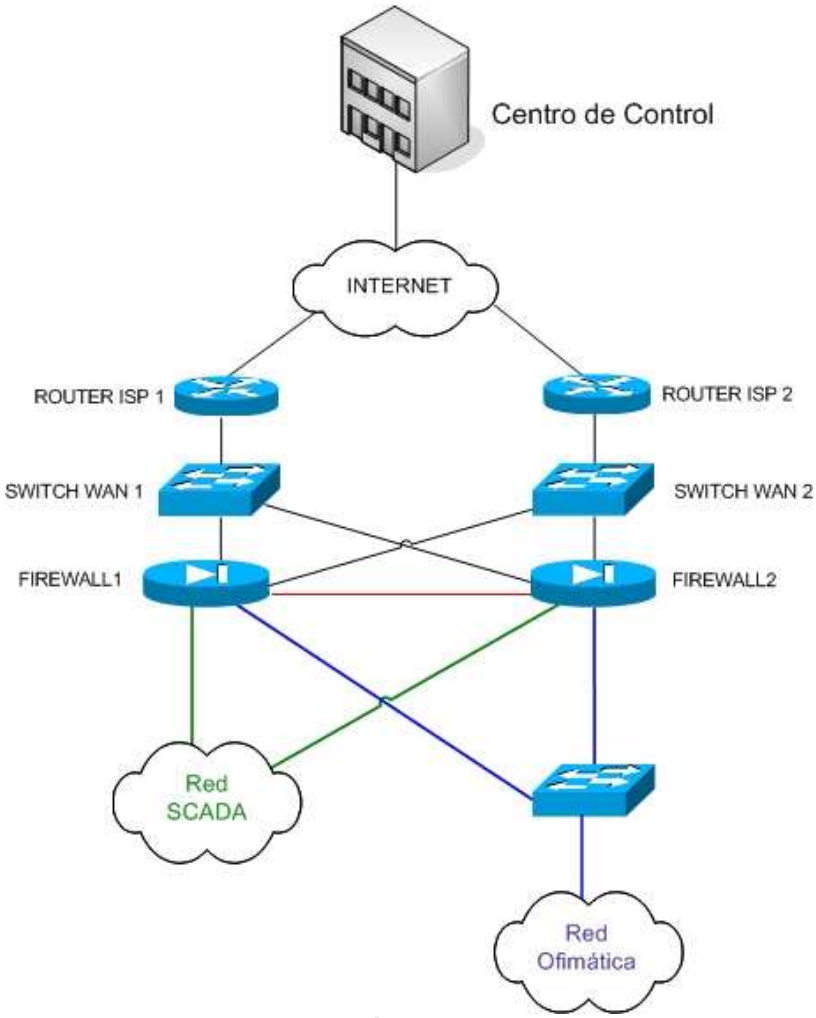



**Figura 3**

## 6.2. Comunicaciones exteriores

De la misma manera que en el tercer capítulo se explican las funciones de cada uno de los dispositivos que se utilizan en la red externa o red de comunicaciones, en este apartado se detalla la configuración de los equipos que la componen.

En el ejemplo mostrado, el router Cisco 1841 del ISP1 está configurado por los propios técnicos del ISP. De cualquier manera y sin que sea lo habitual, se tiene acceso a la línea de comandos del equipo. Para acceder a la configuración del router, así como de cualquier equipo Cisco, tan solo es necesario ejecutar la orden show running-config en modo EXEC privilegiado. A continuación se puede observar la salida del mismo:

*version 12.2*
*service timestamps debug uptime*
*service timestamps log uptime*
*service password-encryption*
*!*

```
hostname Cisco1841
!
!
logging rate-limit console 10 except errors
enable secret 5 ES049DNRKIS]
!
ip subnet-zero
!
interface Ethernet0
 ip address 12.144.25.105 255.255.255.248
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 bundle-enable
 dsl operating-mode auto
 hold-queue 224 in
!
!
interface ATM0.1 point-to-point
 bandwidth 256
 ip address 10.0.0.1 255.0.0.0
 pvc 8/32
  protocol ip inarp
  encapsulation aal5snap
 !
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 ATM0.1
no ip http server
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 access-class 23 in
 exec-timeout 120 0
 login local
 length 0
!
!
end
```

Como solución para la línea secundaria, se ha contratado un servicio de adsl. El ISP no puede prestar este servicio directamente en la subestación, por lo que se opta por un radio enlace para salvar la distancia.

EL ISP tan solo puede prestar el servicio con una IP pública con lo que es necesario realizar NAT en el MODEM/router ADSL. Por ello, es necesario asignar direcciones IP de la red de ofimática para gestión de los equipos en ambos extremos del radio enlace. Los equipos que se utilizan son dos RB411 de la marca Mikrotik.

Para la configuración y monitorización de los equipos Mikrotik, existe una herramienta llamada WinBox la cual puede ser descargada directamente desde la página Web del fabricante.

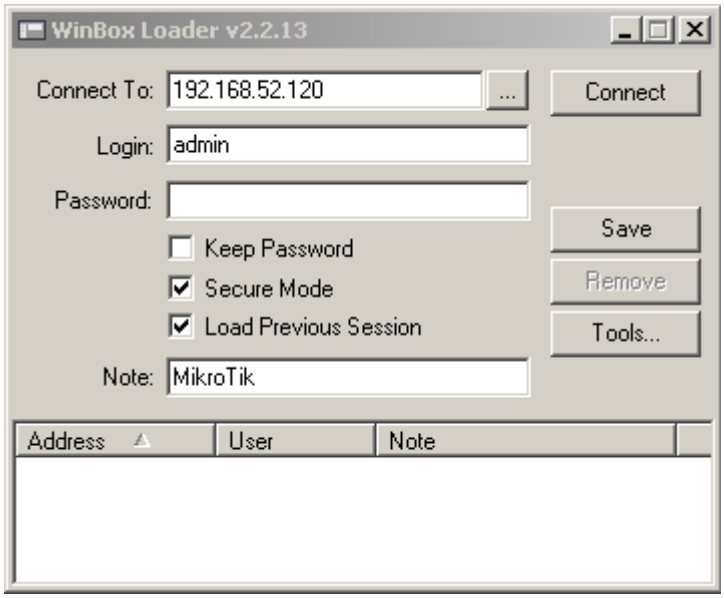



**Figura 4**

Una vez introducidas las credenciales, se puede acceder a la configuración del equipo.

Esta se puede realizar por medio de órdenes o bien a través del menú que aparece en la parte izquierda del WinBox como se puede apreciar en la siguiente figura:

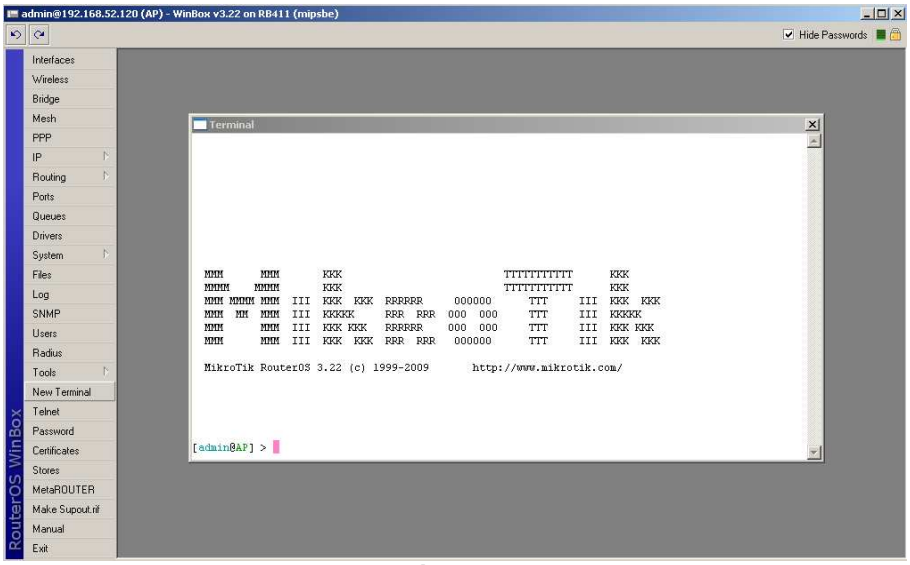



**Figura 5**

En ambos equipos se aplica la misma configuración: modo AP-bridge, activado el modo WDS (Wireless Distribuition System) y configurada una ruta por defecto hacia el firewall.

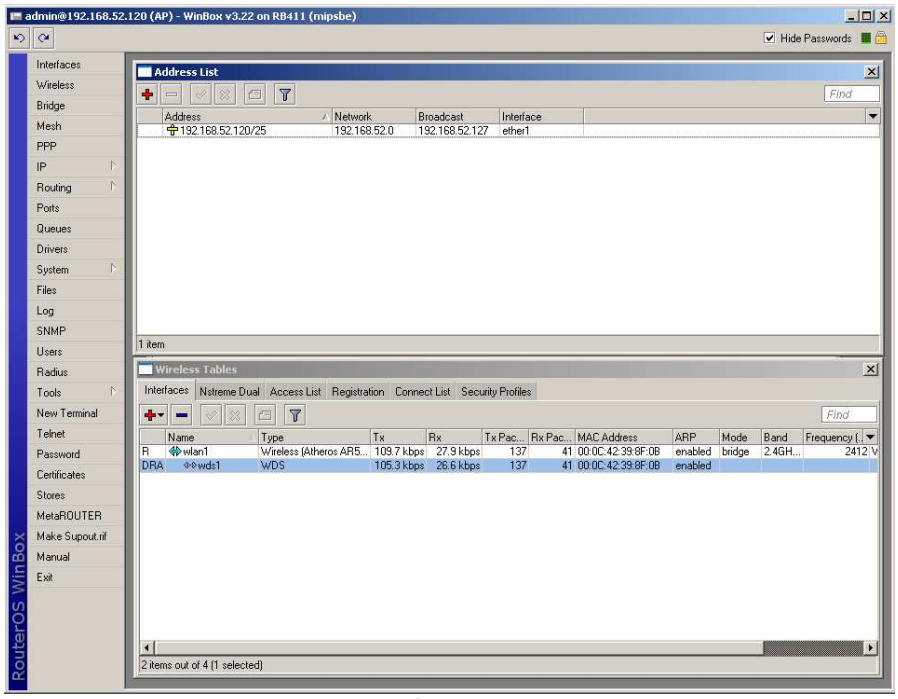



**Figura 6**

## 6.3. Red de comunicaciones

Switches WAN

A pesar de que se instalan dos switches de la misma marca y modelo (se trata de un Cisco 2560 de 8 puertos), existe una diferencia remarcable en cuanto a la conexión física y configuración de ambos. En el caso del Switch WAN 1, la configuración se realiza a través del cable de consola. Una vez configurado el equipo, se muestra la misma a través de la salida de la orden *show running-config:*

```
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname WAN_SW1
!
enable secret 5 $1$v17P$2/IeDsyQlg19c.wVNc3xm1
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
ip tcp synwait-time 5
ip tcp path-mtu-discovery
no ip domain-lookup
!
!
!
!
no file verify auto
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface GigabitEthernet0/1
!
interface Vlan1
 description Conexion Internet Principal
 ip address 12.144.25.110  255.255.255.248
 no ip proxy-arp
 no ip route-cache
!
ip default-gateway 12.144.25.105

ip classless
ip http server
!
ip access-list standard IPS_CONFIANZA
 permit 80.39.119.122
 permit 79.148.122.125
 permit 195.76.213.120 0.0.0.7
!
snmp-server community TRAVIATTA  RO IPS_CONFIANZA
!
control-plane
!
!
line con 0
line vty 0 4
 access-class IPS_CONFIANZA  in
 exec-timeout 5 0
 password 7 020E2555033619725E
 login
 transport input telnet
line vty 5 15
 login
!
end
```

En la configuración se puede apreciar que se ha dado el nombre de WAN_Switch 1 al equipo. Se ha asignado la IP 12.144.25.110 a la Vlan1, que por defecto es la VLAN de gestión. Además se ha configurado como puerta de enlace 12.144.25.105, que es la dirección IP del router del ISP1. Se ha habilitado el interface Web para su posterior gestión. Se ha habilitado el acceso Telnet al equipo, pues se trata de la mejor forma de gestión remota del equipo en los equipos Cisco. Se ha configurado una lista ACL (Access list, lista de acceso) con nombre IPS_CONFIANZA en la que sólo se encuentran las direcciones IP públicas del centro de control y se aplica al acceso por Telnet al equipo.

Con la utilización de ACL se consigue que tan solo desde las direcciones IP autorizadas, se pueda tomar control remoto del equipo. Es un método muy

fiable, pues por el simple hecho de haberse establecido una contraseña en el equipo no se puede asegurar que el equipo esté a salvo de accesos no deseados. También se ha activado el servicio SNMP para la monitorización remota.

Uno de los aspectos a los que hay que prestar mayor atención es la seguridad ya que el este equipo está configurado con una IP pública, con lo que es accesible Internet. Además se encuentra conectado físicamente antes del firewall, por lo que no se encuentra bajo la protección que podría proveer el mismo.

Posiblemente el hecho de tener acceso al switch no sea un peligro para la propia red, pero si que puede utilizarse este acceso como puente y acceso al firewall. Es decir, una vez logeado en el switch, realizar una nueva conexión vía Telnet o SSH contra el firewall).

Por todo ello, es altamente recomendable utilizar como Switches WAN con IP pública sólo aquellos en los que se pueda aplicar listas de acceso.

Por último se puede comprobar en la siguiente figura cómo en el switch tan solo se encuentran levantados los puertos 1 (conectado al router del ISP1), 2 (conectado a un interface WAN del Firewall primario) y el 3 (conectado a un interface WAN del firewall secundario).

| Port | Name | Status | Vlan | Duplex | Speed | Type |
|---|---|---|---|---|---|---|
| Fa0/1 | | connected | 1 | a-full | a-100 | 10/100BaseT |
| Fa0/2 | | connected | 1 | a-half | a-100 | 10/100BaseT |
| Fa0/3 | | connected | 1 | a-half | a-100 | 10/100BaseT |
| Fa0/4 | | notconnect | 1 | auto | auto | 10/100BaseT |
| Fa0/5 | | notconnect | 1 | auto | auto | 10/100BaseT |
| Fa0/6 | | notconnect | 1 | auto | auto | 10/100BaseT |
| Fa0/7 | | notconnect | 1 | auto | auto | 10/100BaseT |
| Fa0/8 | | notconnect | 1 | auto | auto | 10/100BaseT |
| Gi0/1 | | notconnect | 1 | auto | auto | Not Present |

El WAN switch 2 a pesar de que es exactamente el mismo dispositivo, posee una configuración diferente. Se trata de un switch que realiza la misma tarea que el WAN switch 1 pero en este caso el ISP2 tan solo concede una dirección IP pública, utilizada por el propio router del operador. Por ello, para la gestión del equipo se asigna una IP de la red interna del parque. Para la electrónica de red en general, es preferible utilizar direcciones IP de la red de ofimática para tener totalmente aislada la red de producción del resto de los equipos.

En este caso se ha realizado una configuración en cuanto a VLAN. Los puertos 1, 2 y 3 se han configurado en la VLAN2, mientras que los demás puertos permanecen en la VLAN1 (por defecto) y con ellos la gestión del switch. No ha sido necesario configurar ningún tipo de ACL en el switch, ya que la dirección IP a través de la que se puede gestionar el switch es de la red interna (dirección IP privada) y por ello la seguridad se confía al firewall.

A continuación se muestra la configuración del WAN switch 2 (a través de la orden *show running-config* una vez logeado en el equipo en modo EXEC privilegiado):

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname WanSw_2
!
enable secret 5 $1$YhIt$EqomYDdvOJHwOgEvpNOgE0
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface GigabitEthernet0/1
!
interface Vlan1
description Conexion Internet Secundaria
ip address 192.168.52.253 255.255.255.128
!
ip default-gateway 192.168.52.126
ip classless
ip http server
!
snmp-server community TRAVIATTA  RO
 control-plane
!
!
line con 0
line vty 0 4
 password 7 04295814227042
 login
 length 0
line vty 5 15
 password 7 04295814227042
 login
!
end
```

Del mismo modo que en el caso del WAN switch 1, se muestra la salida de la orden show interface status en la que se puede comprobar cómo están levantados los puertos 1, 2, 3 y 8.

| Port | Name | Status | Vlan | Duplex | Speed | Type |
|---|---|---|---|---|---|---|
| Fa0/1 | | connected | 2 | a-full | a-100 | 10/100BaseTX |
| Fa0/2 | | connected | 2 | a-full | a-100 | 10/100BaseTX |
| Fa0/3 | | connected | 2 | a-full | a-100 | 10/100BaseTX |
| Fa0/4 | | notconnect | 1 | auto | auto | 10/100BaseTX |
| Fa0/5 | | notconnect | 1 | auto | auto | 10/100BaseTX |
| Fa0/6 | | notconnect | 1 | auto | auto | 10/100BaseTX |
| Fa0/7 | | notconnect | 1 | auto | auto | 10/100BaseTX |
| Fa0/8 | | connected | 1 | a-full | a-100 | 10/100BaseTX |
| Gi0/1 | | notconnect | 1 | auto | auto | Not Present |

## Firewall

El firewall es el dispositivo al que más atención hay que prestar pues en su configuración radica el buen funcionamiento de todas las comunicaciones. Hay que destacar que este equipo realiza las tareas para la creación de la VPN contra el centro de control, realiza la tarea de routing, NAT, servidor DHCP además de, como su propio nombre indica, las funciones de firewall.

El firewall que se utiliza en este caso es un NSA 2400 de la casa SonicWALL en alta disponibilidad. Se trata de un dispositivo enracable y cuyo interface gráfico facilita enormemente la configuración.

El SonicWALL NSA 2400 dispone de 6 interfaces de red. La gestión del dispositivo se basa en la creación de zonas y objetos red. Cada uno de los interfaces del SonicWALL tiene que pertenecer a una y solo una zona y a cada zona es natural que pertenezcan varias interfaces. Las zonas LAN, WAN, DMZ, VPN ya vienen preconfiguradas y en la mayoría de los casos con ellas es más que suficiente para las tareas que el firewall realiza. Las diferencias entre ellas se ciñen a aspectos como la confianza de los datos que entran al dispositivo a través de ellas así como la inspección de paquetes. Los objetos de red son entidades tales como direcciones IP, rangos de direcciones IP, segmentos de direcciones IP, etc. Una vez creadas las zonas y los objetos de red, se pueden aplicar sobre ellos las políticas que se desee.

De los 6 interfaces que se disponen (nombrados como X0, X1, X2, X3, X4 y X5) todos son totalmente configurables a excepción del X0 que, siendo configurable, siempre pertenece a la zona LAN y el X5, que sirve para la interconexión y sincronización de los dos SonicWALL configurados en alta disponibilidad.

Para acceder a la configuración del SonicWALL por primera vez es necesario conectarse con un cable de red a su interface X0. Si dirección IP por defecto es la 192.168.168.168/24. Su interface http se encuentra habilitada con lo que a través del navegador podemos acceder al mismo. El aspecto que muestra es el siguiente:

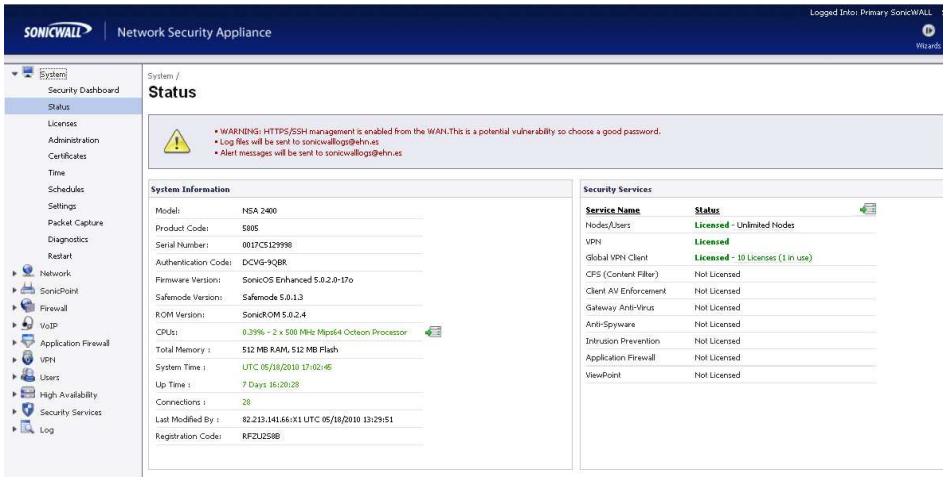



**Figura 7**

Se comienza con la configuración de los interfaces de red. En el menú desplegable de la parte izquierda se puede encontrar la pestaña *Network* y en ella el apartado *Interfaces.* Es necesario configurar cada uno de los interfaces a través del cuadro de diálogo que aparece tras hacer clic en el correspondiente *Configure.*

Es necesario asignar a cada interface la zona, la dirección IP al ser siempre estáticas, la máscara de red, el Gateway y los servidores DNS que se utilizarán. Además se puede verificar el acceso a la gestión del equipo a través del interface por medio de HTTP, HTTPS, SNMP, SSH así como permitir la respuesta al ping (ICMP).

En la siguiente figura se puede observar el cuadro de diálogo en el que se configura la conexión del proveedor de Internet principal en el interface X1 en la zona WAN:

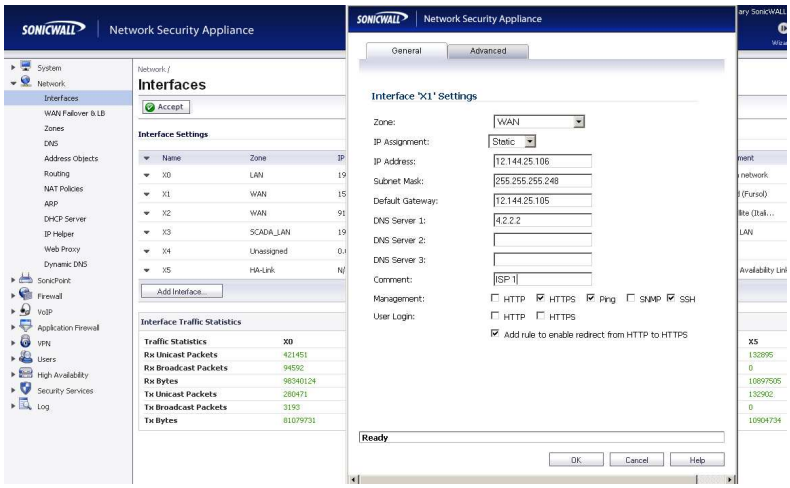



**Figura 8**

De la misma manera sería necesario realizar la configuración para el interface X2, también perteneciente a la zona WAN. No se muestra figura alguna sobre la configuración de la interface X2 ya que esta es similar al caso de la X1.

Por restricciones propias del firewall, la interface X0 siempre se sitúa en la zona LAN, con lo que no puede ser asignada a ninguno de los proveedores de Internet. Por ello esta interface puede ser destinada tanto para la red de ofimática como para la red SCADA o de producción.

En la siguiente figura se puede observar cómo se configura la interface X0 incluyéndola en la zona LAN y a la cual se le asigna una dirección IP estática de la red de ofimática.

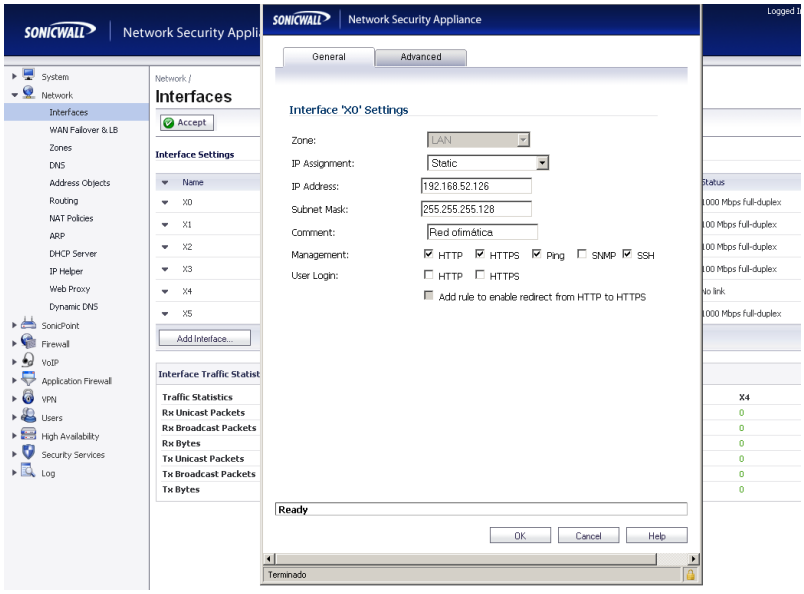



**Figura 9**

Como se puede apreciar en la figura anterior, en este interface no se permite configuración alguna de gateway, ya que se trata de un interface de la zona LAN. La interface X3 se destina para la red SCADA, a continuación se muestra la figura detallando su configuración:

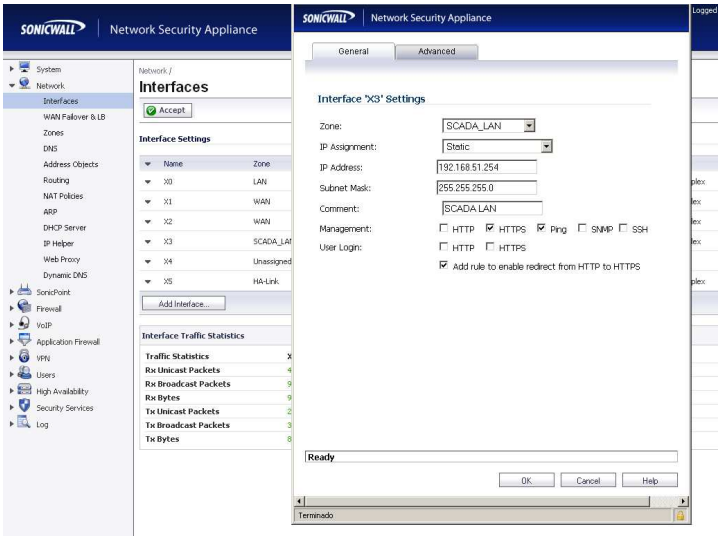



**Figura 10**

Hay que destacar que la red SCADA se sitúa en una zona diferente que la LAN de ofimática. Esto será de gran utilidad cuando se configuren las reglas de firewall del SonicWALL. Con esto quedan configuradas las interfaces del firewall que se utiliza en el parque eólico.

El WAN FailOver se puede habilitar una vez que se han configurado las interfaces WAN. Sin abandonar la pestaña *Network,* en el apartado WAN FailOver & LB se puede configurar como se puede observar en la siguiente figura:

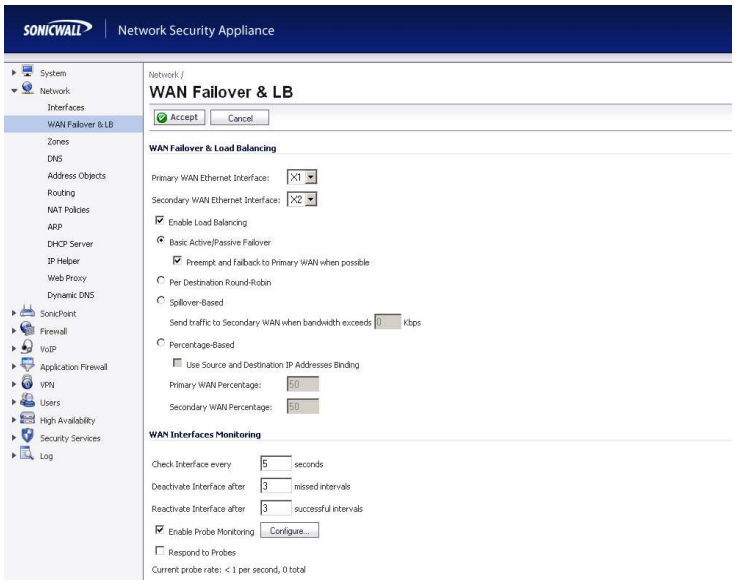



**Figura 11**

SonicWALL ofrece la posibilidad de escoger cuál es el interface principal y cuál el interface secundario. Por simplicidad se define el X1 como interface WAN principal y como secundario el X2. Esto sirve para decidir cual de los proveedores de Internet se toma por defecto desde que entre las opciones de *Load Balancing* se escoge *Basic Active/Pasive FailOver.* Con esto se configura el firewall de tal manera que por defecto utilice la conexión del proveedor de Internet principal y en el caso de que este falle, toda comunicación se reencamine a través del ISP 2.

En cuanto a la configuración de los demás apartados de la pestaña Network no es necesario realizar cambios, ya que los DNS se han configurado en las interfaces WAN, no es necesario ningún protocolo de routing, el NAT está configurado por defecto para que se realice en cuanto cualquier acceso desde un equipo de la zona LAN envíe tráfico a Internet y el servidor DHCP se mantendrá inhabilitado pues todas las IP se asignan manualmente como política de seguridad.

Se puede verificar cómo tras la configuración de las interfaces de red se han creado los pertinentes objetos de red. En el caso que nos ocupa se han creado de forma automática los objetos de red tipo host que implementan las interfaces de red así como las subredes a las que pertenecen.

La siguiente tarea a realizar es la configuración y establecimiento de la VPN contra el centro de control. Se asume que la configuración en el centro de control ya se ha realizado y se está a la espera de la configuración del extremo del parque eólico para el establecimiento del túnel.

En la pestaña VPN, tras verificar la casilla *Enable VPN* , se pulsa el botón *add* surgiendo un cuadro de diálogo para la configuración del nuevo túnel.

A continuación se muestran las figuras en las que se puede apreciar la configuración de la VPN a establecer:

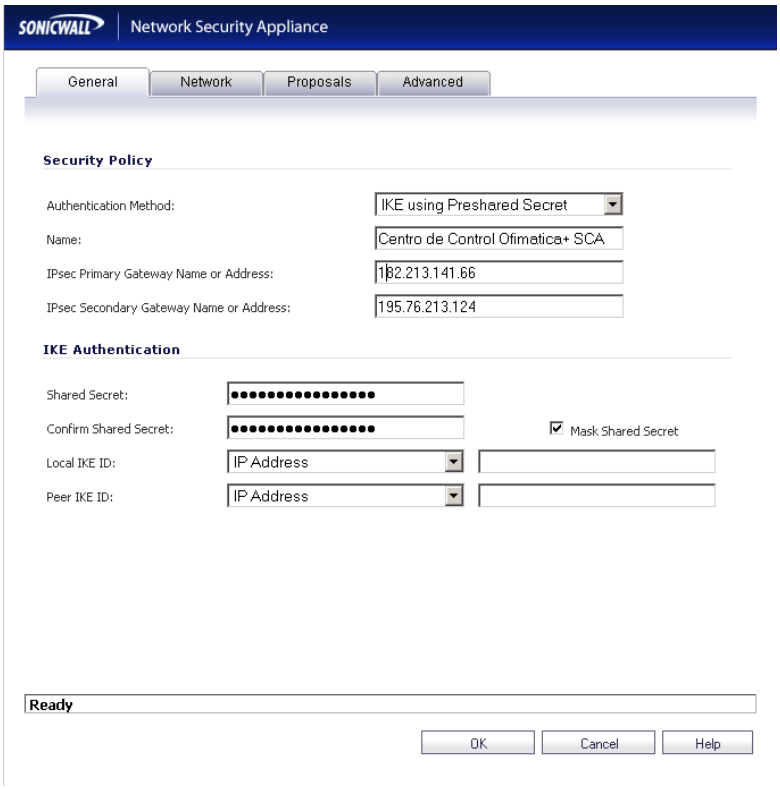



**Figura 12**

En la anterior figura se puede apreciar cómo el método de autenticación escogido es IKE con clave precompartida.

De la misma manera, observar cuales son las redes que la nueva VPN va a comunicar. Por parte del parque eólico (red local) se ha incluido tanto la red de ofimática como la red SCADA. En el extremo remoto se ha incluido el objeto de red que representa la red local del centro de control, donde se encuentran los ordenadores con los que los operarios monitorizan el parque eólico.

Como se imagina, en principio se crea un túnel en el que la accesibilidad y comunicación es total entre las redes LAN de los extremos. Para implementar las limitaciones (denegación) de acceso según convenga se hace uso de las técnicas del propio firewall como más adelante se detalla.

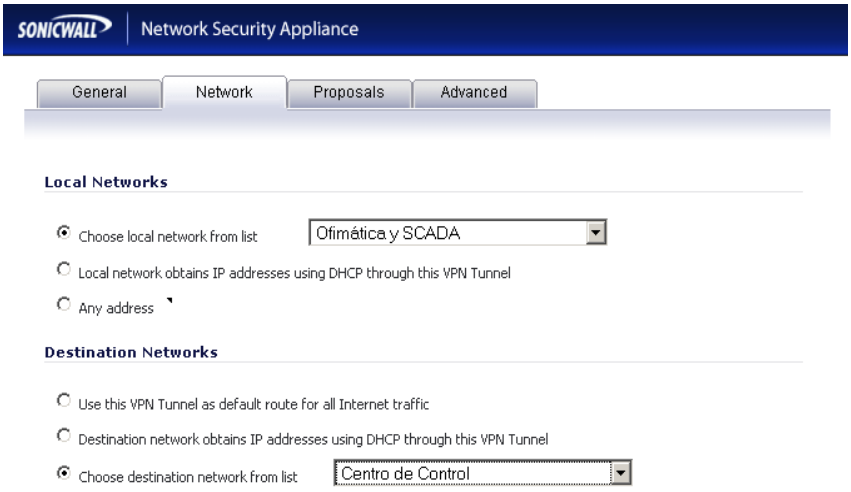



**Figura 13**

En la siguiente figura se detalla la configuración más técnica de la VPN. Es imprescindible que todos y cada uno de los campos coincidan con el otro extremo del túnel situado en el firewall del centro de control.

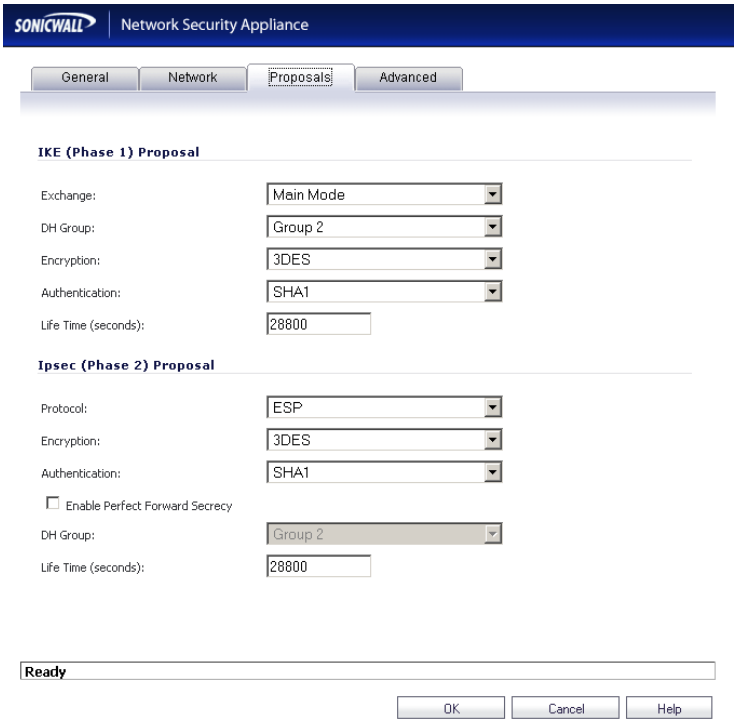



**Figura 14**

Se puede verificar que el cifrado se confía al 3DES, la autenticación modo SHA1 y ESP como protocolo de encapsulación.

Por último en cuanto a la configuración de la VPN, es importante marcar la opción *Enable Keep Alive* ya que de lo contrario el túnel solo se establecería cuando existan nuevas conexiones entre los extremos. Esto puede ser causa de interrupción en la comunicación si por ejemplo se abre una conexión tcp que dura un largo tiempo.

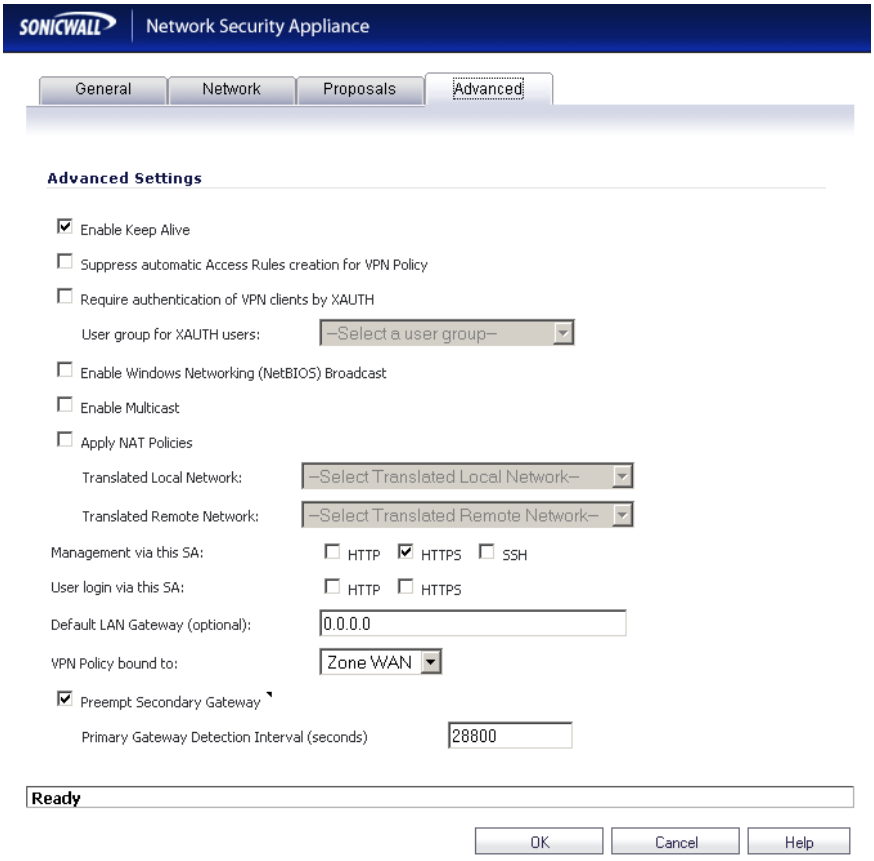



**Figura 15**

Además es necesario escoger la opción *Zone WAN* de *VPN Policy bound to* ya que con esto se permite que el establecimiento de la VPN utilice cualquiera de las interfaces WAN de las que se dispone.

Tras la configuración y unos pocos segundos de espera se puede comprobar el establecimiento con éxito de la VPN en la propia pestaña Settings de VPN:

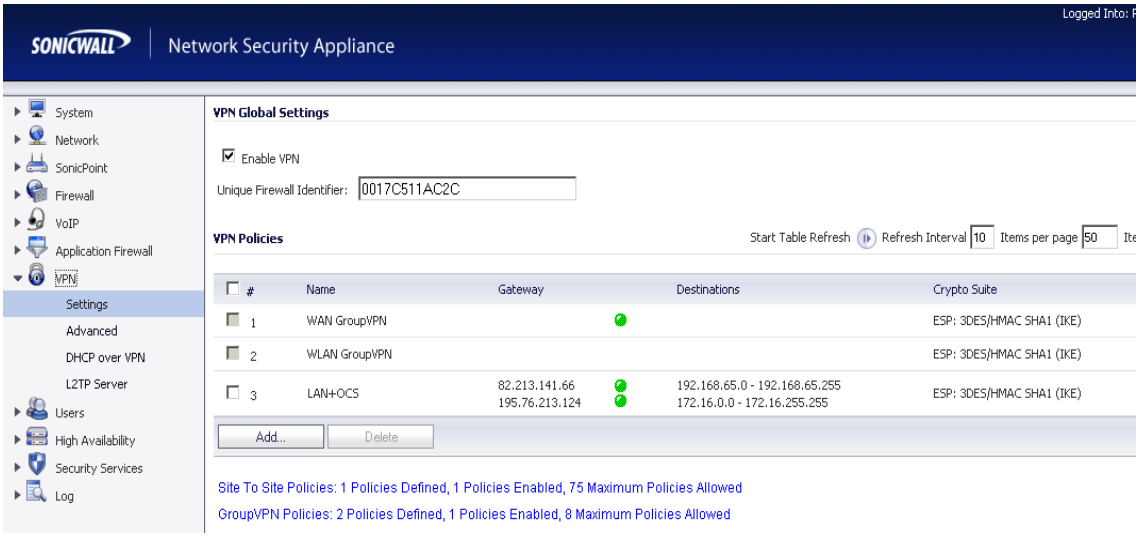



**Figura 16**

A continuación se configura la redundancia de los SonicWALL. Se dispone de dos dispositivos similares. Hasta el momento se ha configurado uno, el que se considera sea el primario. SonicWALL dispone de una automatización del proceso por el que se copia la configuración al firewall secundario. Esto se realiza a través del interface X5 y un proceso de sincronización basado en las direcciones MAC de ambos dispositivos.

Se puede contemplar en la figura cómo se realiza esta tarea en la pestaña *High Availability* apartado *Settings*.

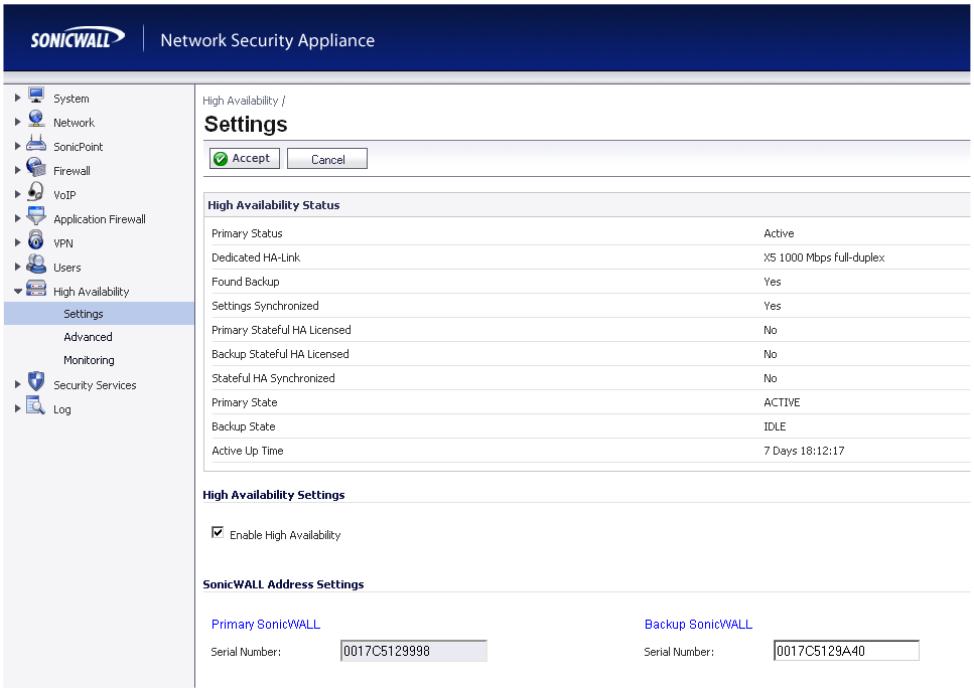



**Figura 17**

En la parte inferior se habilitado la función de alta disponibilidad y se ha introducido la dirección MAC del SonicWALL de Backup.

Con esta redundancia física se consigue que aún fallando el dispositivo principal, las comunicaciones se mantengan intactas, ya que ambos dispositivos están en todo momento sincronizados y cuando el SonicWALL de Backup detecta algún problema en el su pareja, toma el control de manera automática, renegociando incluso las VPN activas en el momento. Este proceso es realmente rápido y puede ser incluso imperceptible por los usuarios.

A continuación se describen las opciones que posee el SonicWALL como firewall. Se pueden aplicar reglas de firewall que permiten habilitar o denegar la comunicación entre dos objetos de red.

Es este apartado el que aprovecha en gran parte las ventajas de una configuración basada en objetos. En la pestaña *Firewall* se presentan las combinaciones posibles de accesos entre zonas en modo matriz. De esta manera se filtran gran cantidad de reglas que puedan existir y se encamina al usuario a una configuración más cómoda. Si se trata de tráfico entre la sede de control y el centro de producción, las reglas de firewall se pueden aplicar tanto en el SonicWALL del parque eólico como en el del centro de control. En ambos SonicWALL ha de estar permitido el tráfico concreto para habilitar la comunicación pero por el contrario con uno de los dos que no permita el tráfico será suficiente para cortar el mismo.

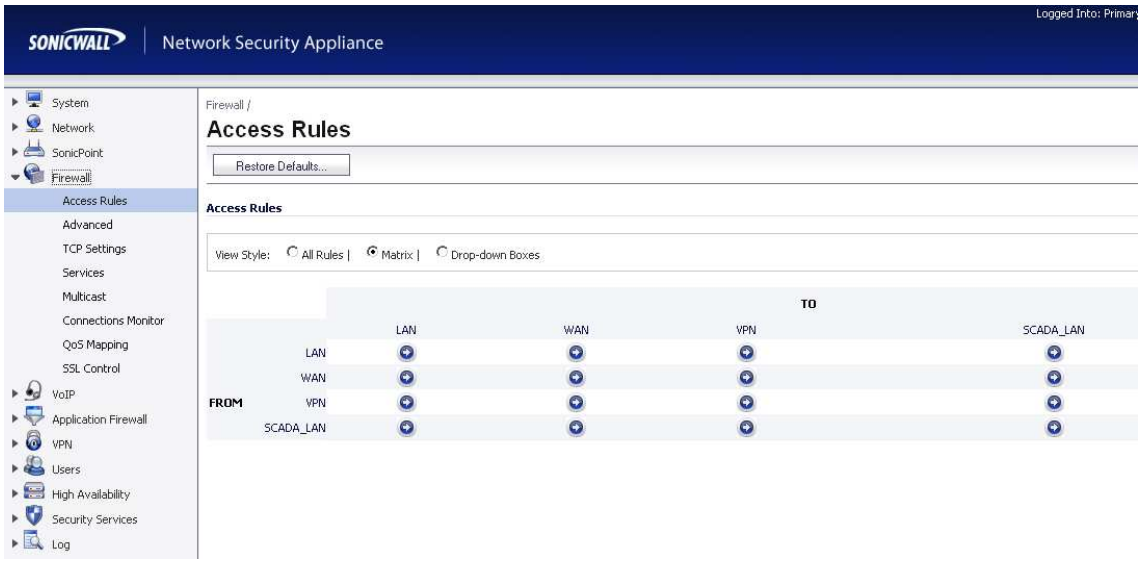



**Figura 18**

Comúnmente se permite todo el tráfico entre la red SCADA del parque eólico y la red local del centro de control. Por motivos de seguridad se niega cualquier acceso desde la red de ofimática del parque a la red SCADA. También se niega el tráfico hacia Internet desde cualquiera de las redes locales. Por seguridad en el caso de la red SCADA y porque la red de ofimática no debe de

malgastar ancho de banda de las conexiones a Internet ya que el mismo suele ser bastante limitado.

En la anterior figura también se puede observar que las reglas de firewall se pueden aplicar en un sentido u otro de la comunicación entre dos zonas. Esto obedece quién comienza la comunicación.

Como ejemplo se configura una regla de firewall a través de la cual se deniega la comunicación entre cualquier dispositivo de la red SCADA con cualquier dispositivo de la red de ofimática y viceversa. Para ello será necesario realizar dos reglas de firewall: Una en sentido LAN→ SCADA LAN y otra en sentido SCADA LAN→ LAN

A continuación se muestra el cuadro de diálogo para la creación de la regla de firewall:

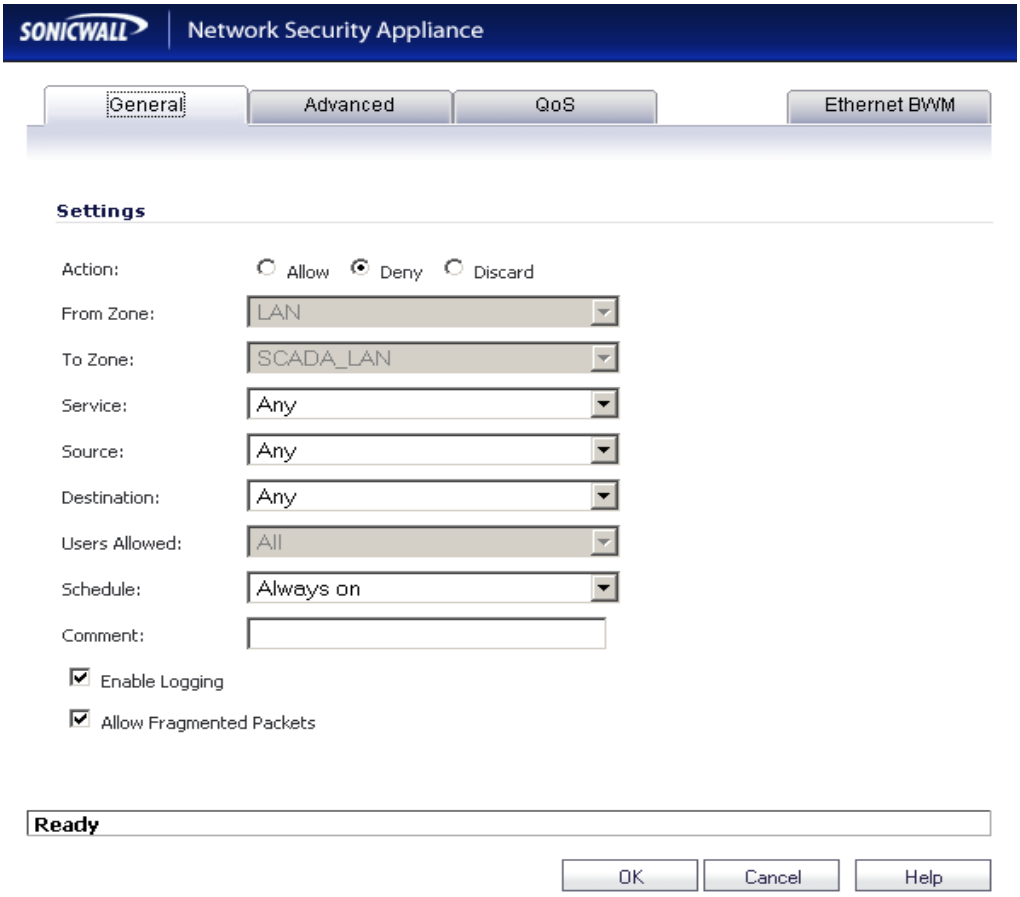



**Figura 19**

La acción a realizar es *Deny*, como no se desea que ningún tipo de tráfico pueda pasar el servicio se configura como *Any* así como la fuente y destino *Any*.

La regla aplicada se muestra a continuación:

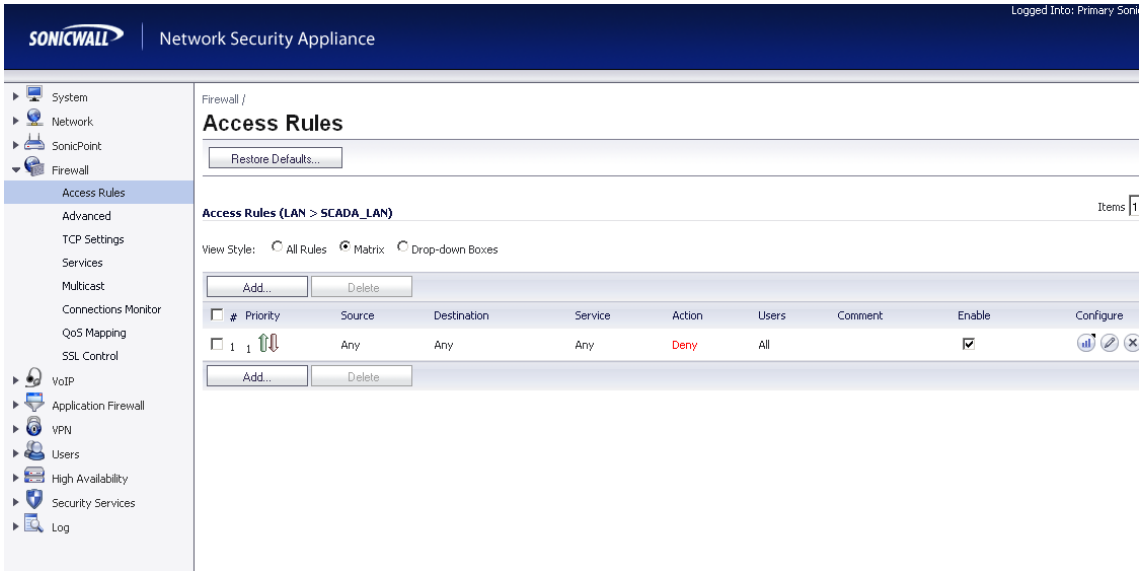



**Figura 20**

Sería necesario realizar la misma configuración en sentido SCADA LAN→ LAN como a continuación se observa:

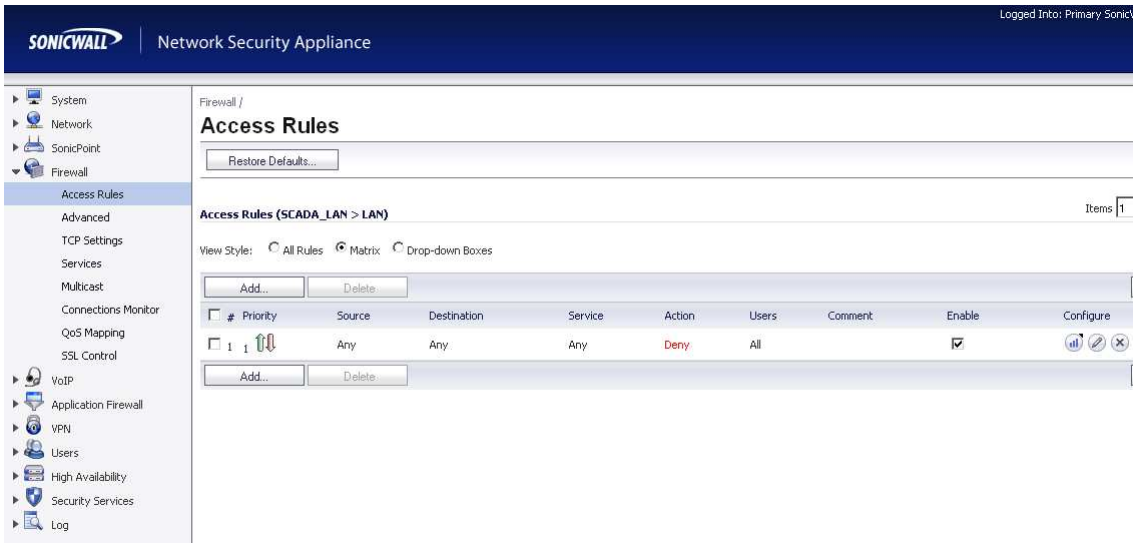



**Figura 21**

Además de la propia herramienta de firewall, el SonicWALL NSA 2400 dispone también de un firewall de aplicación, es decir de capa 7. La utilización de la misma es realmente potente ya que permite la creación de reglas de firewall que se aplican no solo a dispositivos o zonas, sino más específicamente a la utilización de ciertas aplicaciones desde los dispositivos de red. En los parques eólicos no se utiliza ya que hasta la fecha no se ha visto la necesidad de ello (con una configuración todo-nada a nivel de firewall es suficiente) además de que SonicWALL funciona con un modelo de licencias y la licencia de esta opción supone un alto coste.

LAN Switch

El switch que se utiliza como switch LAN en el parque eólico es de la marca HP, serie Procurve 1700. Se trata de un switch gestionable con 24 puertos. El switch se conecta al SonicWALL a través de las interfaces X0. Dado que se dispone de dos SonicWALL en alta disponibilidad, en el switch se ocupan dos puertos igualmente.

En este caso se ha optado por este equipo de un coste menor que los equipos Cisco porque cumple con los requisitos de forma notable.

Una de las grandes diferencias con las características que implementan los switches WAN que se han utilizado en este caso es que los equipos Cisco son capaces de manejar ACL al contrario que la serie Procurve de HP. En el caso del switch LAN no es necesario el uso de ACL desde que este equipo queda protegido por el firewall y no es accesible directamente desde Internet.

La configuración del switch se realiza por medio de su interface Web. El aspecto que presenta el mismo es el siguiente:

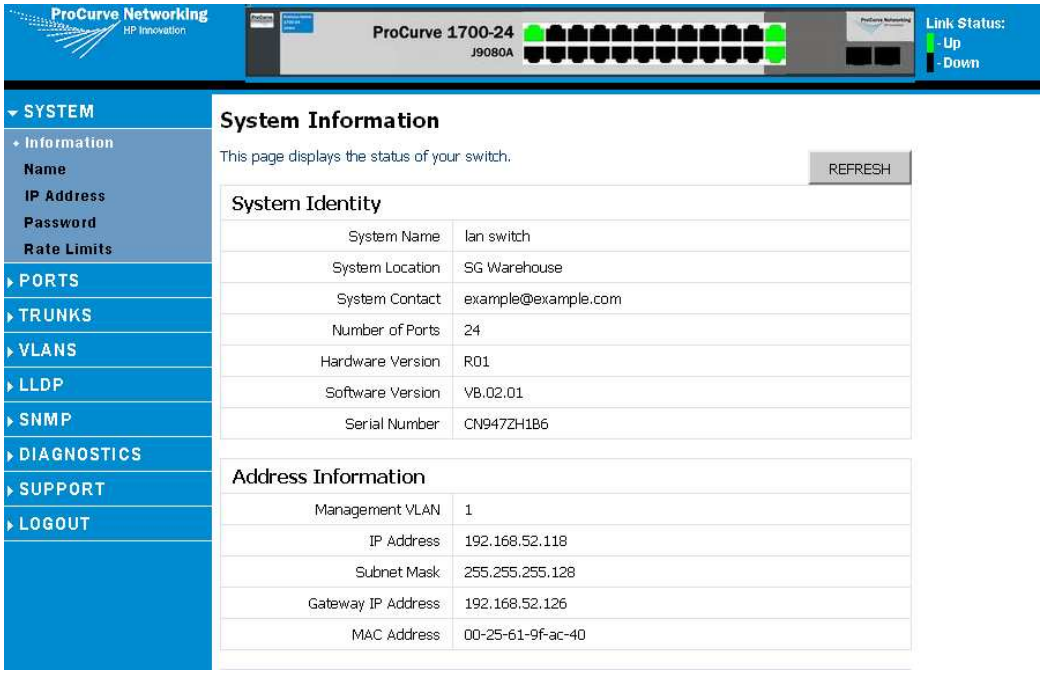



**Figura 22**

Lo primera tarea en la configuración del switch es dotarle de una IP estática perteneciente a la red de ofimática. En el menú de la parte izquierda, en el apartado SYSTEM > IP Address se puede configurar el direccionamiento IP:

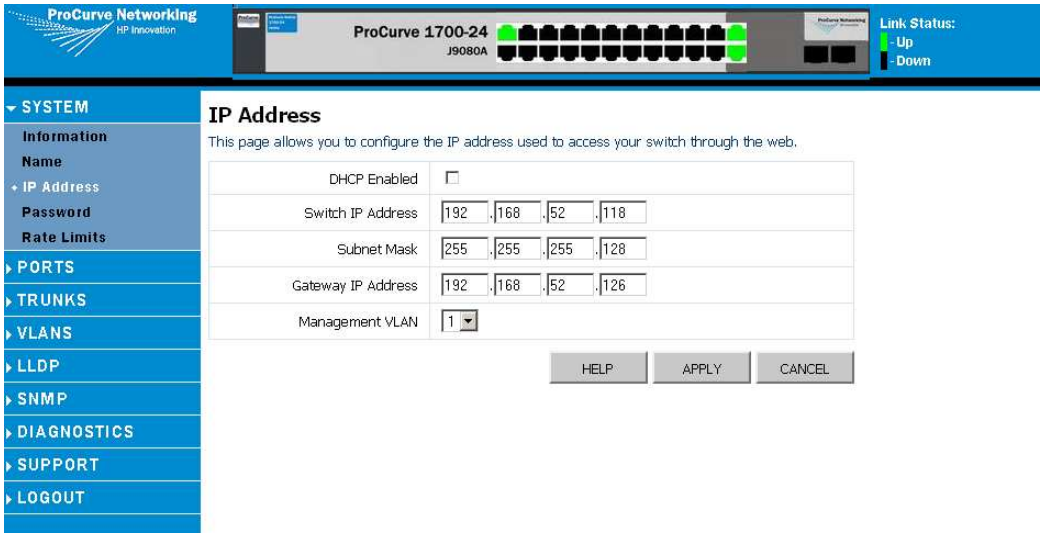



**Figura 23**

Esta configuración permite el acceso a la interface Web el dispositivo, pero es importante remarcar que el hecho de configurar en este punto un Gateway no aplica en la función como switch que desarrolla. Es decir, aunque no se configurara la dirección IP del switch, el equipo realizaría sus funciones de la misma forma. Esta configuración tan solo sirve en el plano de gestión. Como se puede observar en la figura anterior, los puertos 23 y 24 se encuentran levantados, conectados respectivamente a la interface X0 del SonicWALL primario y SonicWALL de Backup.

Otra de las características de gestión que conviene aprovechar es el agente SNMP que implementa HP en su serie Procurve. En el apartado SNMP tan solo es necesario activar el servicio del mismo y dar un nombre de comunidad de lectura (*public* en este caso). Es conveniente resaltar que se echa en falta la posibilidad de configurar el envío de traps SNMP a alguna dirección IP para poder realizar una mejor monitorización del equipo.

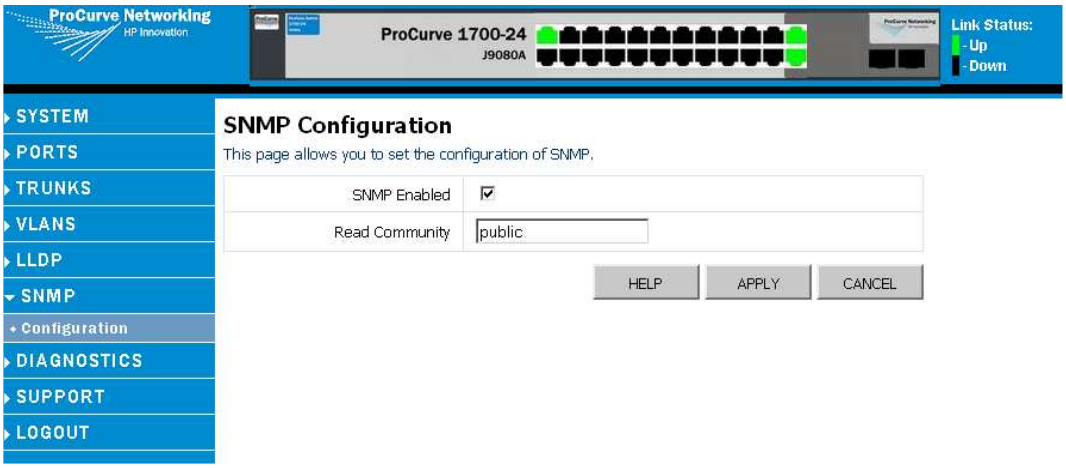



**Figura 24**

En algunas situaciones es conveniente la utilización de VLAN para reducir el dominio de broadcast. En este caso, al tratarse de una subred pequeña, no se ve conveniente el uso de VLANs por lo que tanto la VLAN de gestión como todos los puertos del switch permanecen en la VLAN1. Como medida de protección se procede también a cambiar la clave de acceso al equipo.

UPS

EN el caso real que se describe en el documento se utiliza una UPS de la marca APC. El consumo de la electrónica de red no es elevado por lo que se decide instalar un modelo que provee 1500 VA. Además se instala una tarjeta de red para la gestión del equipo. Se trata de un extra que si bien no es imprescindible para el uso normal de la UPS como respaldo en casos de fallo eléctrico, si que es altamente recomendable para su posterior mantenimiento, gestión y monitorización de la salud de la electricidad de la subestación.

La configuración se realiza bien a través de un cable serie y la ayuda del hyperterminal o bien con la aplicación que contiene el CD-ROM que acompaña a la tarjeta de red de la UPS. Esto se hace imprescindible debido a que a pesar de que puede disponerse en modo cliente DHCP, la unidad no viene configurada así de serie.

En ambos casos se realiza una mínima configuración de la dirección IP de la tarjeta de red para que esta pueda ser configurada a través de su interface Web o a través de Telnet.


**Figura 25**

Como a toda la electrónica de red, se asigna una dirección IP de la red de ofimática y se conecta a un puerto del switch LAN.

Una vez que la UPS disponga de dirección IP, lo más eficiente es configurar todas las opciones a través de su interface Web.

A través de ella se puede conocer el estado de la unidad (batería o por entrada de corriente alterna), el tiempo que podría mantener en modo batería a los equipos que están conectados eléctricamente a ella así como un log de los eventos que han sucedido como se puede observar en la siguiente figura.

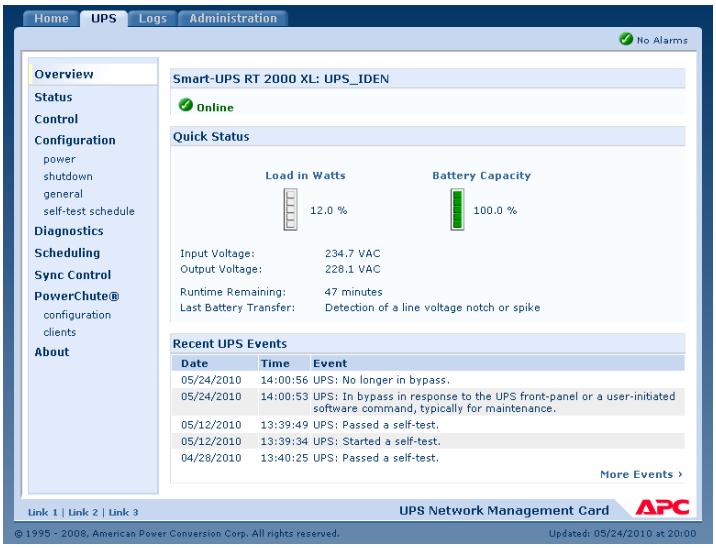



**Figura 26**

Una de las funciones que más información aportan es la capacidad de enviar un e-mail (previa configuración) en forma de aviso ante cualquier tipo de evento.

En la pestaña Administration > Notification se configura el servidor y cuenta de correo así como los destinatarios a los que hay que informar sobre lo sucedido en la UPS. Incluso se pueden programar test cuyos resultados sean enviados de forma automática a los destinatarios de los eventos, para conocer si por ejemplo, la batería de la UPS goza de capacidad sin necesidad de acceder su interface Web.

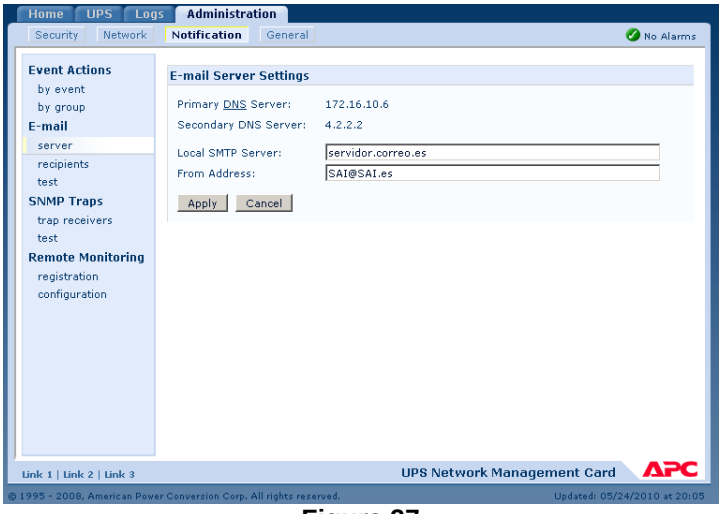



**Figura 27**

Así mismo, la gestión SNMP es necesaria configurar para poder monitorizar la unidad de forma remota. A esto se accede a través del menú Administration > Network

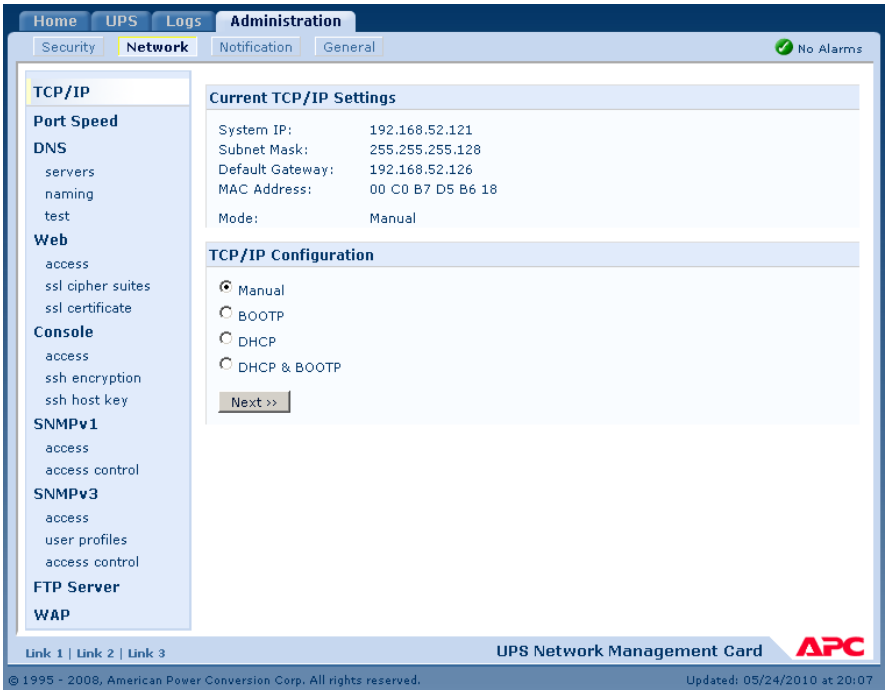



**Figura 28**

## 6.4. Comunicaciones internas

Conversor optoelectrónico

Como se adelantó al comienzo del capítulo, en el caso que ocupa esta explicación, la sala de control (donde se encuentra la electrónica de red) y la subestación (donde se encuentran los servidores SCADA) están separadas por una distancia cercana a los dos kilómetros. Por este motivo se decide emplear fibra óptica para su comunicación.

Debido a que el SonicWALL no posee ningún interface de fibra ni la posibilidad de instalar un módulo de fibra adicional, se utiliza un par de conversores optoelectrónicos MOXA. Estos están conectados a los interfaces X3 de los SonicWALL a través de sus interfaces de pares de cobre trenzado (del dominio eléctrico) a 100mbps y a través de fibra (los Moxa disponen de conectores SC) directamente a los Switches SCADA. No es necesaria la instalación de otro par de conversores optoelectrónicos en la subestación ya que los propios switches SCADA disponen de módulos con interfaces de fibra.

La fibra que se utiliza es de 50/125 µm, lo que según la hoja de características del fabricante será suficiente para que en 2ª ventana, la velocidad de la red no se vea mermada.

Su configuración es realmente sencilla ya que se trata de un dispositivo de capa 2 con gestión. Su interface web se muestra a continuación:

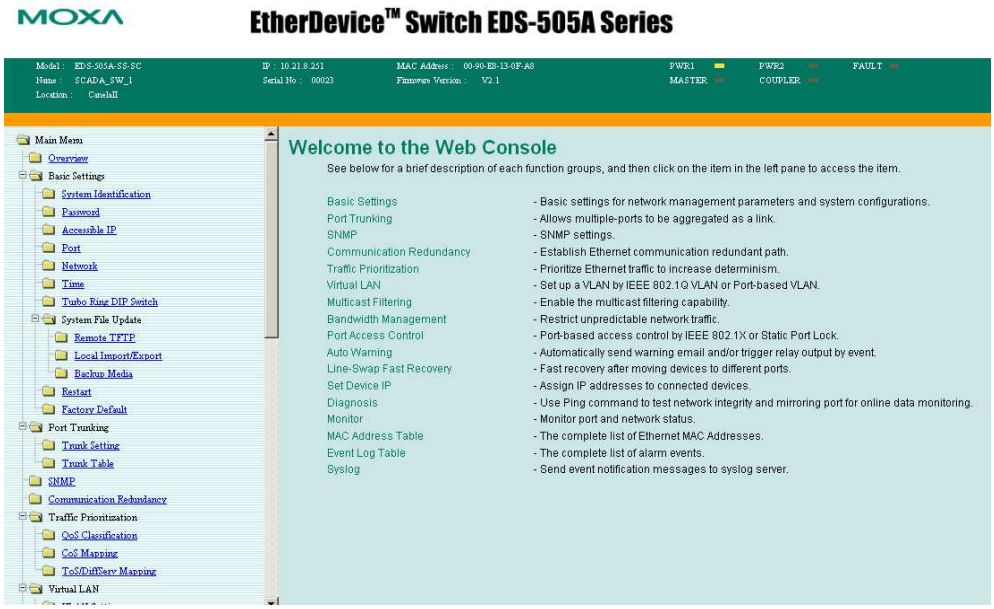



**Figura 29**

Como en el resto de los dispositivos, se configura su dirección IP de gestión y se activa la gestión SNMP para poder realizar su monitorización remota.

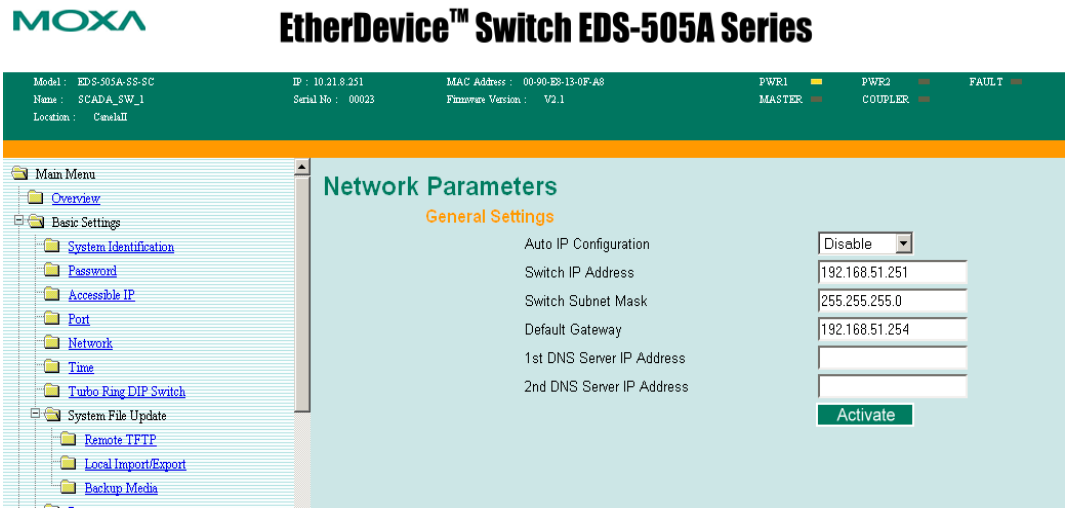



**Figura 30**

Dado que desde la sala de control a la subestación tan sólo se necesita comunicar la red SCADA, no se realiza ningún tipo de manipulación sobre VLANs.

Como comentario, se puede destacar que el dispositivo no cuenta en su interface Web con un monitor de nivel de señal óptica recibida ni emitida. Su monitorización se encamina más hacia la parte telemática ya que sí que es posible comprobar el estado de sus interfaces a través de la pestaña *Monitor* como a continuación se muestra:

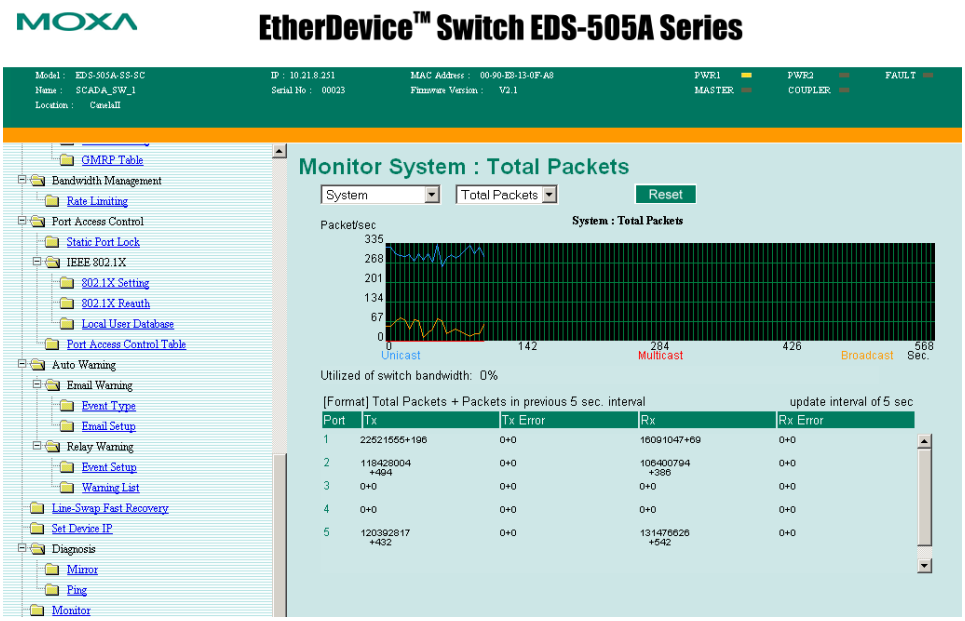



**Figura 31**

Switch SCADA

Como todo equipamiento SCADA, se trata de dispositivos industrial con múltiples inveraces Ethernet, tanto de fibra como de cobre.

En este caso se utiliza un switch de la marca HirschMann, en concreto la serie MICE (modular industrial Ethernet switch) L2E con capacidad POE (Power Over Ethernet).

El equipo sirve de interface de conexión entre la electrónica de red y la red SCADA. Dentro de la red SCADA conecta los autómatas y estaciones meteorológicas con los servidores OCS locales que recogen los datos de los primeros.

Una vez más, se instalan los equipos de forma redundada, con lo que un puerto Ethernet de cada MICE se conecta a un interface de fibra de cada uno de los conversores optoelectrónicos que se han instalado en la sala de control.

Su configuración se realiza a través del interface Web continuación se puede observar el aspecto de la misma.

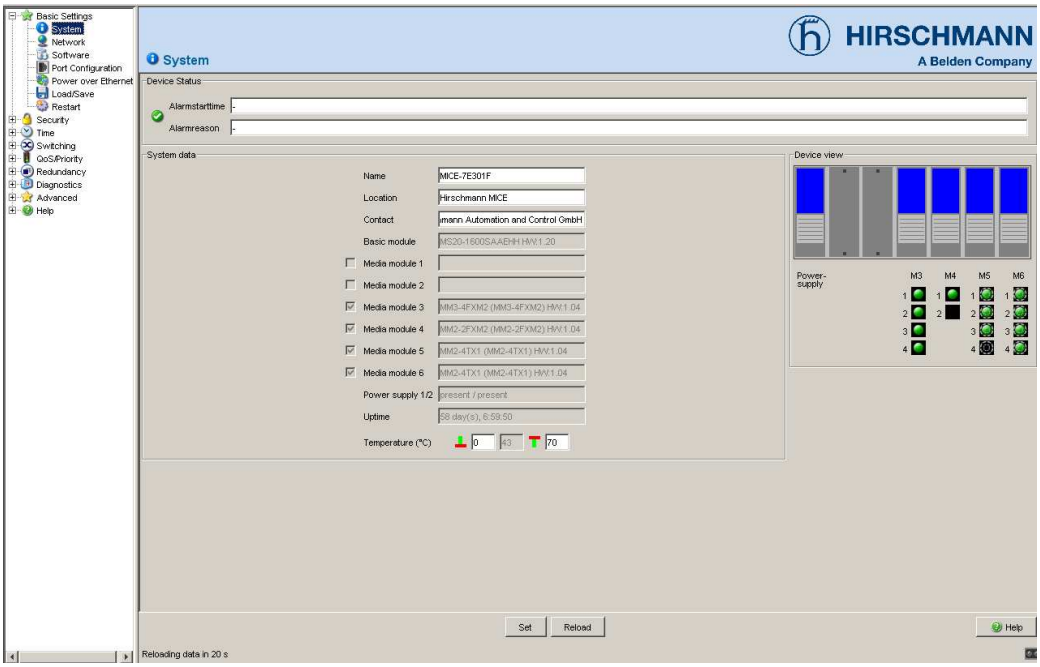



**Figura 32**

Se puede consultar el estado de los puertos del MICE, En la siguiente figura se pueden reconocer los módulos instalados en el dispositivo, siendo interfaces de cobre los que tienen la posibilidad de auto-MDIX (Manual cable crossing). En los interfaces de fibra esta opción se encuentra deshabilitada.

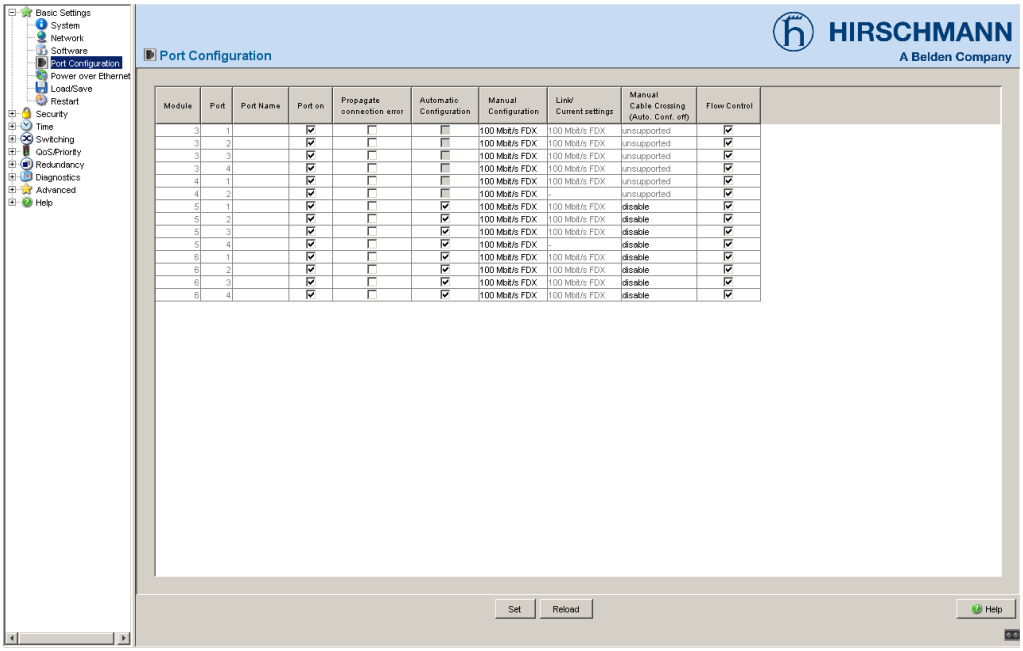



**Figura 33**

Por último quedaría añadir los PLCs y switches de los molinos (a los que llega la fibra bien desde otra máquina o desde el MICE de la sala de control en el caso de los últimos molinos de cada enfilación) pero no ha sido posible acceder

a su configuración aunque sí se incluye en los anexos la hoja de características de un modelo que es instalado por numerosos fabricantes de molinos

# 7. Valoración económica

La realización de un presupuesto económico sobre lo que puede suponer el conjunto de tareas que rodean a el proyecto de telecomunicaciones de un parque eólico, tales como el estudio de ingeniería previa, la gestión de contratación de las líneas de acceso a Internet, los trabajos de instalación, compra del material y su puesta en servicio es considerablemente variable y no tiene sentido si no se aplica a un caso concreto.

Si nos referimos a los dispositivos de la red de parque, no es el mismo caso si se trata de un parque eólico de unos pocos molinos a casi un centenar, ya que el número de PLCs y la fibra óptica necesaria varía de forma proporcional al número de máquinas que se van a instalar.

Por el contrario, los equipos que componen la electrónica de red tales como switches, firewalls y SAIs sí que mantienen un precio independiente de la magnitud del parque eólico. Sí que es verdad que dependiendo de también del número de máquinas se puede optar por una gama superior o inferior dentro de una marca.

Por último, el coste del servicio de Internet es posiblemente lo que más puede variar. Una vez más se aplica la ley de la oferta y la demanda y si en el lugar donde se encuentra el parque eólico se dispone de un solo ISP, el precio será alto. Incluso si no existe a priori ninguno en la zona y tras negociaciones se llega un acuerdo para que un ISP preste servicio el cual incurre en obra civil, el coste puede dispararse.

A continuación se muestran los costes que supone el caso en concreto que se ha desarrollado en el apartado anterior.

El desglose de la inversión inicial es el siguiente:

- Estudio previo, de ingeniería, con las visitas pertinentes de replanteo y puesta en servicio para la certificación de la instalación ascienden a 15.000 €

- Suministro de la electrónica de red y su instalación llevada a cabo por una empresa de IT local asciende a 10.000 €

- Suministro de la electrónica de la red interna, para el parque eólico que cuenta con 30 molinos, incluyendo los servidores y clientes SCADA con sus respectivas licencias asciende a 20.000

- Instalación y alta de los servicios de Internet, teniendo en cuenta que fue necesaria obra civil para el despliegue de la red del operador asciende a 8.000 €

Esto supone en su conjunto una inversión inicial de 53.000 €.

A continuación se detallan los gastos anuales que suponen las comunicaciones del parque eólico:

- El servicio de Internet prestado por ambos ISP tiene un coste de 9.500 €

- El compromiso por parte de la empresa de IT local para dar un servicio de asistencia NBD (Next Businness Day) sin incluir material y con una visita anual preventiva para el chequeo de la electrónica de red tiene un coste asociado de 600 €

- El servicio de soporte 24x7 que se encarga de monitorizar las comunicaciones del parque eólico y gestionar incidencias con operadores ante cualquier alarma asciende a 4000 €

- El soporte a la garantía de los equipos cisco hp y SonicWALL así como la actualización de las licencias de este último asciende a 500 €

Lo anterior se traduce en unos gastos recurrentes anuales de 14.600 €

En cualquier caso, el precio de las comunicaciones no representa una partida importante teniendo en cuenta las cifras que se barajan en los parques eólicos.

# 8. Mejoras y líneas futuras

Se puede afirmar que las comunicaciones de un parque eólico, tal como se ha explicado a lo largo del documento, son dignas de atención. Su importancia es muy alta y por ello son objeto de estudio. No siendo un dato de ámbito público, unas comunicaciones tales como las planteadas en el caso real descrito, puedo asegurar que gozan de una buena salud. Es una excelente idea la introducción de redundancia de equipos, de proveedores de Internet, de comunicación interna con topología de fibra en anillo, etc. Y los departamentos de comunicaciones de las empresas productoras de energía realizan un trabajo más que sobresaliente.

Después de mi corta experiencia en temas de comunicaciones de parques eólicos sí que se me ocurren algunas mejoras (pocas y pequeñas, la verdad sea dicha) que se pueden introducir.

Por un lado, la existencia de software libre es nula hasta donde yo conozco. Es una verdadera lástima. Por poner un ejemplo, existen en Internet multitud de firewalls que sin llegar a la simplicidad que proporciona SonicWALL, posee el 99% de las características de este. Un sistema basado en GNU/Linux configurado adecuadamente con IPtables puede ser tan robusto como el mejor de los firewalls comerciales (ya que muchos de ellos se basan en IPtables).

El uso de la electrónica de red simplemente tiene sentido para proporcionar seguridad y fiabilidad a la información que tiene que transportarse entre el centro de producción y el centro de control y viceversa. Dejando de un lado la redundancia física, una regla muy importante a seguir es que los dispositivos que se instalan han de ser los imprescindibles debido a que su conexión es en “serie” y un fallo en cualquiera de ellos imposibilita a los demás. Con esto me refiero concretamente a los switches WAN que se utilizan para “replicar” el acceso a Internet a los dos firewalls. Si se consiguiera que el router del ISP tuviera embebido un switch, se eliminaría el WAN switch y con ello un equipo que pueda fallar.

Otra de las mejoras o características que se echan en falta es el uso de VoIP en cada uno de los parques eólicos para su comunicación telefónica con el centro de control. La comunicación entre ambas sedes es constante y si se trata de llamadas de larga distancia, el ahorro que supone el uso de VoIP es superior al desembolso que habría que realizar para la instalación de teléfonos VoIP. Hay que destacar que ambas sedes ya se encuentran conectadas “directamente” a través de la VPN IPsec y la comunicación por voz sobre datos entre la red ofimática del parque y el centro de control es un simple paso más.

# 9. Bibliografía

**SonicWALL NSA2400 series**
http://www.sonicwall.com/es/8992.html

**Mikrotik routers & Wireless**
www.mikrotik.com

**Cisco Systems Inc.**
http://www.cisco.com/web/ES/index.html

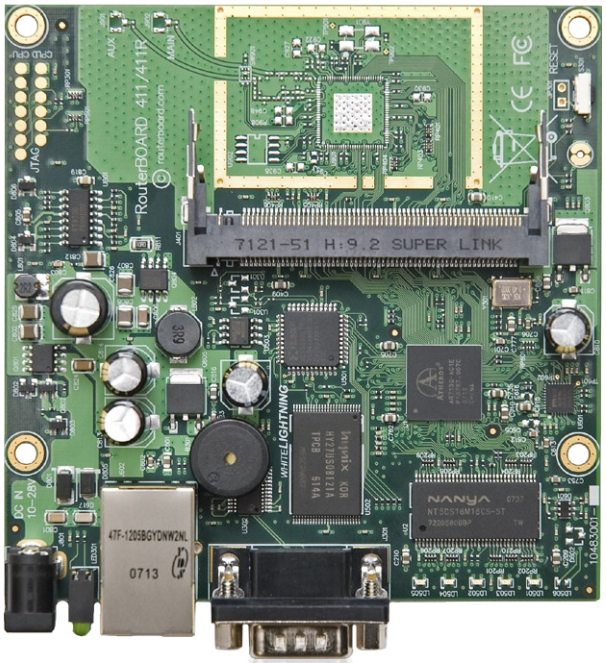
**HP Procurve 1700 series switches**
http://h10010.www1.hp.com/wwpc/es/es/sm/WF05a/12883-12883-3445275-3445282-3445282-3411648.html

**Danish Wind Industry association**
http://guidedtour.windpower.org/es/tour/wres/index.htm

**Sistemas eólicos de producción de energía eléctrica**
J.L. Rodriguez Amenedo, J.C. Burgos Díaz, S.Arnalte Gómez (Ed Rueda)

# 10. Anexos

# RouterBOARD 411/A




The heart of RB411 is the new Atheros CPU which makes this tiny device a quick one. Tests show that it is up to three times more powerful than our previous model.

Comparing to RB411, the RB411A adds more memory and a Level4 license.

RB411/A includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router/firewall or bandwidth manager.

One small device - with all the power of RouterOS. At a very special price.

| | |
|---|---|
| CPU | Atheros AR7130 300MHz network processor |
| Memory | 32/64MB DDR SDRAM onboard memory |
| Boot loader | RouterBOOT |
| Data storage | 64MB onboard NAND memory chip |
| Ethernet | One 10/100 Mbit/s Fast Ethernet port with Auto-MDI/X |
| miniPCI | One MiniPCI Type IIIA/IIIB slot |
| Extras | Reset switch, Beeper |
| Serial port | One DB9 RS232C asynchronous serial port |
| LEDs | Power, NAND activity, 5 user LEDs |
| Power options | Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC |
| Dimensions | 10.5 cm x 10.5 cm (4.13 in x 4.13 in) Weight: 82 g (2.9 oz) |
| Power consumption | ~3W without extension cards, maximum – 12 W |
| Operating System | MikroTik RouterOS v3, Level3 license (RB411A: Level4) |

routerboard.com

# Cisco Catalyst 3560 Series Switches

## Foundation for Innovation-Powered by Cisco

**Figure 1.** Catalyst 3560 Series Switches

The Cisco® Catalyst® 3560 Series (Figure 1) is a line of fixed-configuration, enterprise-class switches that includes IEEE 802.3af and Cisco prestandard Power over Ethernet (PoE) capability in Fast Ethernet and Gigabit Ethernet configurations. The Cisco Catalyst 3560 is an ideal access-layer switch for small enterprise LAN access or branch-office environments, combining both 10/100/1000 and PoE configurations for maximum productivity and investment protection while facilitating the deployment of new applications such as IP telephony, wireless access, video surveillance, building management systems, and remote video kiosks. Customers can deploy networkwide intelligent services-such as advanced quality of service (QoS), rate limiting, access control lists (ACLs), multicast management, and high-performance IP routing-while maintaining the simplicity of traditional LAN switching.

## PRODUCT BENEFITS

### IEEE 802.3af and Cisco Prestandard Power over Ethernet

The Cisco Catalyst 3560 Series can provide a lower total cost of ownership (TCO) for deployments that incorporate Cisco IP phones, Cisco Aironet® wireless LAN (WLAN) access points, or any IEEE 802.3af-compliant end device. PoE removes the need for wall power to each PoE-enabled device and eliminates the cost for additional electrical cabling that would otherwise be necessary in IP phone and WLAN deployments.

The Cisco Catalyst 3560 24-port PoE configurations can support 24 simultaneous full-powered PoE ports at 15.4 watts (W) for maximum powered-device support. Taking advantage of Cisco Catalyst Intelligent Power Management, the 48-port PoE configurations can deliver the necessary power to support 24 ports at 15.4W, 48 ports at 7.7W, or any combination in between through the sophisticated power-management features in Cisco IOS® Software.

Maximum power availability for a converged voice and data network is attainable when a Cisco Catalyst 3560 Series switch is combined with the Cisco RPS 675 Redundant Power System for transparent protection against internal power supply failures and an uninterruptible power supply (UPS) system to safeguard against power outages.

**Gigabit Ethernet**

At speeds of 1000 Mbps, Gigabit Ethernet provides the bandwidth to meet new and evolving network demands, alleviate bottlenecks, and boost performance while increasing the return on existing and new infrastructure investments. Today's workers are placing higher demands on networks, running multiple, concurrent applications. For example, a worker joins a team conference call through an IP videoconference, sends a 10-MB spreadsheet to meeting participants, broadcasts the latest marketing video for the team to evaluate, and queries the customer relationship management (CRM) database for the latest real-time feedback. Meanwhile, a multiple-gigabyte system backup starts in the background, taking advantage of simple and affordable network attached storage (NAS) to comply with regulatory record keeping requirements such as Sarbanes-Oxley.

The Cisco Catalyst 3560 Series can scale the access network to 1 Gbps over existing Category 5 copper cabling and make the most of the desktops and notebooks that are now shipping with Gigabit Ethernet network interface cards (NICs) and higher PC bus speeds for full bandwidth utilization. In addition to being easy to deploy, Gigabit Ethernet networks are simpler to maintain with the new Cisco Time Domain Reflectometry (TDR) that helps verify existing cabling.

The Gigabit Ethernet models of the Cisco Catalyst 3560 Series also facilitate high-performance Grid and distributed computing in addition to preparing your network to deploy software applications such as Microsoft Exchange, as well as Microsoft Vista's remote imaging, data synchronization, and computer-to-computer search capabilities.

**Enhanced Security**

With the wide range of security features that the Cisco Catalyst 3560 Series offers, businesses can protect important information, keep unauthorized people off the network, guard privacy, and maintain uninterrupted operation. The Cisco Catalyst 3560 Series supports a comprehensive set of security features for connectivity and access control, including network admission control (NAC), ACLs, Dynamic ARP Inspection, IP Source Guard, VPN Routing/Forwarding Lite (VRF Lite), port-level security, and identity-based network services with 802.1x and extensions. These features increase LAN security; protect passwords and configuration information; offer options for network security based on users, ports, or MAC addresses; and help quicken responses to intruder and hacker detection. NAC helps organizations to limit damage from viruses and worms by enforcing security-policy compliance on endpoint devices.

**Availability and Scalability**

The Cisco Catalyst 3560 Series is equipped with a robust set of features that allow for network scalability and higher availability through IP routing as well as a complete suite of Spanning Tree Protocol enhancements aimed to maximize availability in a Layer 2 network. Enhancements to the standard Spanning Tree Protocol, such as Per-VLAN Spanning Tree Plus (PVST+), Uplink Fast, and Port Fast, as well as innovations such as Flex Links, maximize network uptime. PVST+ allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. Uplink Fast, Port Fast, and Backbone Fast all greatly reduce the standard 30- to 60-second Spanning Tree Protocol convergence time.

The Cisco Catalyst 3560 Series also delivers high-performance, hardware-based IP routing for either unicast or multicast traffic. The Cisco Express Forwarding-based routing architecture allows for very high-speed lookups while delivering the stability, performance, and scalability necessary to meet the needs of future requirements. Implementing routed uplinks to the core will improve network availability by enabling faster failover protection and simplifying the Spanning Tree Protocol algorithm by terminating all Spanning Tree Protocol instances at the aggregator switch. Additionally, routed uplinks allow better bandwidth utilization by implementing equal cost routing (ECR) on the uplinks to perform load balancing. Routed uplinks optimize the utility of uplinks out of the wiring closet by eliminating unnecessary broadcast data flows into the network backbone. Private VLANs improve scalability and provide IP address management benefits and Layer 2 security by partitioning a regular VLAN domain into subdomains. Support for the IPv6 industry standard in the Cisco Catalyst 3560 Series also alleviates address space problems.

**Advanced Quality of Service**

The Cisco Catalyst 3560 Series provides intelligent services to keep everything flowing smoothly. Industry-leading mechanisms for marking, classifying, and scheduling deliver best-in-class performance for data, voice, and video traffic-all at wire speed. Important features include Shaped Round Robin scheduling and policing/rate limiting as well as innovations like Scavenger Traffic Queuing functions. The IP Services license (formerly called the Enhanced Multilayer Image, or EMI) provides a richer set of enterprise-class features, including advanced hardware-based IP Unicast and IP Multicast routing as well as policy-based routing (PBR).

**Enhanced Security**

The Cisco Catalyst 3560 Series uses the following capabilities to protect sensitive data and network resources from internal and external threats:

- The Cisco Catalyst 3560 Series supports Network Admission Control (NAC), an industry initiative sponsored by Cisco Systems® that uses the network infrastructure to enforce security-policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms. Using NAC, organizations can provide network access to endpoint devices such as PCs, personal digital assistants (PDAs), and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.
- Dynamic ARP Inspection and IP Source Guard are security features in the Cisco Catalyst 3560 Series that protect the network from certain man-in-the-middle attacks. Dynamic ARP Inspection validates Address Resolution Protocol (ARP) packets in a network and ensures that only valid ARP requests and responses are relayed. IP Source Guard restricts IP traffic from untrusted sources.
- VPN Routing/Forwarding Lite (VRF Lite) in the Cisco Catalyst 3560 Series helps enable unique VPNs without additional equipment at the customer site.
- The IEEE 802.1x standard supported by the Cisco Catalyst 3560 Series prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated.
- Cisco Identity Based Networking Services (IBNS) in the Catalyst 3560 Series prevents unauthorized access and helps ensure that users receive only their designated privileges. It provides the ability to dynamically administer granular levels of network access.

- Secure Shell Protocol Version 2 (SSHv2) and Simple Network Management Protocol Version 3 (SNMPv3) provide network security by encrypting administrator traffic-preventing unauthorized users from accessing passwords or configuration information.
- Access control lists (ACLs) can be used to restrict access to sensitive portions of the network by denying packets based on source and destination MAC addresses, IP addresses, or TCP/UDP ports. ACLs can be used to guard against denial-of-service (DoS) and other attacks, and because ACL processing is done in hardware, forwarding performance of the switch is not compromised when implementing ACL-based security.
- Private VLAN edge provides security and isolation between ports on a switch, helping ensure that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port.
- Port security can be used to limit access on an Ethernet port based on the MAC address of the device that is connected to it. It also can be used to limit the total number of devices plugged into a switch port, thereby reducing the risks of rogue wireless access points or hubs.
- MAC Address Notification can be used to monitor the network and track users by sending an alert to a management station so that network administrators know when and where users entered the network. The Dynamic Host Configuration Protocol (DHCP) Interface Tracker (Option 82) feature tracks where a user is physically connected on a network by providing both switch and port ID to a DHCP server. Additionally, the DHCP Snooping Option 82 feature enables granular control over IP address assignment by a DHCP server by augmenting a host IP address request so that the DHCP server can make a more sophisticated address assignment.
- TACACS+ or RADIUS authentication facilitates centralized access control of switches and restricts unauthorized users from altering the configurations. Alternatively, a local username and password database can be configured on the switch itself. Fifteen levels of authorization on the switch console and two levels on the Web-based management interface provide the ability to give different levels of configuration capabilities to different administrators.

**Redundancy**

The Cisco Catalyst 3560 Series supports the following capabilities to optimize network availability, so that users can access data at all times, locally and remotely:

- Per VLAN Rapid Spanning Tree Plus (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances.
- Flex Links are a pair of Layer 2 interfaces (switch ports or port channels), where one interface is configured to act as a backup to the other. This feature provides an alternative solution to the Spanning Tree Protocol, allowing users to turn off Spanning Tree Protocol and still provide basic link redundancy.
- 802.1s Multiple Spanning Tree Protocol facilitates load balancing and improves network fault tolerance by providing multiple forwarding paths for data traffic. 802.1w Rapid Spanning Tree Protocol provides rapid recovery of uplink connectivity following failure.
- Cisco Hot Standby Router Protocol (HSRP) is supported to create redundant, failsafe routing topologies.

- Equal cost routing (ECR) provides load balancing and redundancy. Basic IP Unicast routing protocols (static, RIPv1, and RIPv2) are supported for small-network routing applications. Advanced IP Unicast routing protocols (OSPF, Interior Gateway Routing Protocol [IGRP], Enhanced IGRP [EIGRP], and Border Gateway Protocol Version 4 [BGPv4]) are supported for load balancing and constructing scalable LANs. IP Services is required.
- Switch port auto-recovery (errdisable) automatically attempts to re-enable a link that is disabled because of a network error.
- The optional Cisco RPS 675 Redundant Power System protects against internal power supply failures.

**Management**

The Cisco Catalyst 3560 Series supports the following management capabilities:

- IEEE 802.3af and Cisco prestandard PoE support come with automatic discovery to detect a Cisco prestandard or IEEE 802.3af endpoint, negotiate the power to be budgeted for that device, and provide the necessary power-all done by the Cisco Catalyst 3560 Series switch without any user configuration.
- Cisco Smartport macros offer a set of verified feature templates per connection type in an easy-to-apply manner. With these templates, users can consistently and reliably configure essential security, IP telephony, availability, QoS, and manageability features with minimal effort and expertise. Smartport macros simplify the configuration of critical features for Ethernet networks.
- All Cisco Catalyst 3560 Series switches can be managed by the CiscoWorks LAN Management Solution (LMS) applications such as Resource Manager Essentials, Campus Manager, Device Fault Manager, and CiscoView. CiscoWorks LMS is a suite of powerful management tools that simplify the configuration, administration, monitoring, and troubleshooting of large Cisco networks. It integrates these capabilities into a world-class solution for improving the accuracy and efficiency of operations staff, increasing the overall availability of networks through proactive planning, and maximizing network security.
- Cisco Network Assistant software can manage a small network consisting of a diverse array of network devices, such as Cisco routers and Cisco Aironet wireless access points. A few mouse clicks enable the security, availability, and QoS features recommended by Cisco, without the need to consult a detailed design guide. The Security wizard automatically restricts unauthorized access to servers with sensitive data. Cisco Smartports and wizards save hours of time for network administrators, reduce human errors, and help ensure that the configuration of the switch is optimized for these applications. Available at no cost, Cisco Network Assistant can be downloaded from http://www.cisco.com/go/cna.
- The Cisco Express Setup feature simplifies initial configuration, eliminating the need for more complex terminal emulation programs and knowledge of CLI. This reduces the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches.
- The DHCP Server feature enables a convenient deployment option for the assignment of IP addresses in networks that do not have a dedicated DHCP server.

**Bandwidth Optimization**

- Voice VLAN allows network administrators to assign voice traffic to a VLAN dedicated to IP telephony, simplifying phone installations and providing easier network traffic administration and troubleshooting.

- Cisco Fast EtherChannel® and Gigabit EtherChannel technology allows for aggregating ports for up to 2 Gbps full duplex on network or server connections. Use Port Aggregation Protocol (PAgP) for automatic configuration. Similarly, Link Aggregation Group Protocol (LACP) allows creation of Ethernet channeling with devices that conform to IEEE 802.3ad standard.
- Internet Group Management Protocol (IGMP) facilitates monitoring and management of multicast applications (such as e-learning and videoconferencing) while minimizing the performance impact of managing group membership information.

**IPv6**

- The Cisco Catalyst 3560 Series supports the IPv6 standard, which increases Internet global address space to accommodate the rapidly increasing number of users and applications that require unique global IP addresses.
- In addition to the larger address space, the Cisco Catalyst 3560 Series switches also make the most of other IPv6 features such as address autoconfiguration, embedded IP Security (IPSec), routing optimized for mobile devices, and Duplicate Address Detection.

**Advanced Quality of Service**

Cisco Catalyst intelligent switches offer industry-leading QoS features to prioritize critical traffic and applications thereby avoid bottlenecks. These features bring new levels of control, predictability, and adaptability to networks of all sizes:

- The Cisco Catalyst 3560 Series can identify traffic flows or traffic groups, and classify or reclassify these groups using Differentiated Services Code Point (DSCP) in the IP packet and the 802.1p class of service (CoS) field in the Ethernet packet.
- Users can mitigate DoS attacks by assigning a minimal bandwidth queue to “scavenger traffic” or unimportant traffic used for peer-to-peer media sharing, gaming, or any entertainment video applications. This reduces scavenger traffic during periods of congestion, but allows it to be available if bandwidth is not being used for business purposes, for example during off-peak hours.
- Rate limiting gives control over the amount of bandwidth across any configured interface, for appropriate distribution of available bandwidth.
- Four egress queues help network administrators to be more discriminating and specific in assigning priorities for the various applications on the LAN. Scheduling is performed in egress to assign the appropriate queues to the outgoing packets.
- Shaped Round Robin (SRR) scheduling helps ensure differential prioritization of packet flows by intelligently servicing the ingress queues and egress queues.
- Weighted Tail Drop (WTD) provides congestion avoidance at the ingress and egress queues before a disruption occurs.
- 64 policers per 10/100 or Gigabit Ethernet port used to allocate bandwidth based on source/destination (IP address, MAC address) or TCP/UDP port numbers.

## CISCO CATALYST 3560 SERIES SWITCHES

Each model is available with the IP Base or the IP Services software loaded on it.

Table 1 lists the switches currently available in the Cisco Catalyst 3560 Series.

**Table 1.** Cisco Catalyst 3560 Series Switches

| Product | Port Speed | Number of Ports | Uplinks | When to Buy |
|---|---|---|---|---|
| **Cisco Catalyst 3560-8PC** | 10/100 with IEEE 802.3af and Cisco prestandard PoE | 8 | 1 dual-purpose 10/100/1000 and Small Form-Factor Pluggable (SFP) port | For deployments outside the wiring closet requiring low-density access with PoE |
| **Cisco Catalyst 3560-24TS** | 10/100 | 24 | 2 SFP-based ports | For networks requiring low-density access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |
| **Cisco Catalyst 3560-48TS** | 10/100 | 48 | 4 SFP-based ports | For networks requiring medium-density access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |
| **Cisco Catalyst 3560-24PS** | 10/100 with IEEE 802.3af and Cisco prestandard PoE | 24 | 2 SFP-based ports | For networks requiring low-density access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |
| **Cisco Catalyst 3560-48PS** | 10/100 with IEEE 802.3af and Cisco pre-standard PoE | 48 | 4 SFP-based ports | For networks requiring medium-density access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |
| **Cisco Catalyst 3560G-24TS** | 10/100/1000 | 24 | 4 SFP-based ports | For networks requiring low-density 10/100/1000 access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |
| **Cisco Catalyst 3560G-24PS** | 10/100/1000 with IEEE 802.3af and Cisco prestandard PoE | 24 | 4 SFP-based ports | For networks requiring low-density 10/100/1000 access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |
| **Cisco Catalyst 3560G-48TS** | 10/100/1000 | 48 | 4 SFP-based ports | For networks requiring medium-density 10/100/1000 access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |
| **Cisco Catalyst 3560G-48PS** | 10/100/1000 with IEEE 802.3af and Cisco prestandard PoE | 48 | 4 SFP-based ports | For networks requiring medium-density 10/100/1000 access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks |

## FOR MORE INFORMATION

For more information, please visit http://www.cisco.com/go/catalyst3560.

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



Printed in USA

C02-379065-01 03/09

# The SonicWALL Network Security Appliance Series

NETWORK SECURITY

## Next Generation Unified Threat Management Protection

- **SonicWALL's next generation security**
- **Scalable multi-core hardware and Reassembly-Free Deep Packet Inspection**
- **Stateful High Availability and load balancing features**
- **High performance and lowered TCO**
- **Advanced routing services and networking features**
- **Standards-based Voice over IP (VoIP)**
- **Secure distributed wireless LAN services**
- **Onboard Quality of Service (QoS)**

Organizations of all sizes depend on their networks to access internal and external mission-critical applications. As advances in networking continue to provide tremendous benefit to organizations, they are increasingly challenged by sophisticated and financially-motivated attacks designed to disrupt communication, degrade performance and compromise data.

Malicious attacks penetrate outdated stateful packet inspection firewalls by exploiting higher network levels. Point products add layers of security, but are costly, difficult to manage, limited in controlling network misuse and ineffective against the latest multipronged attacks. The SonicWALL® Network Security Appliance (NSA) Series revolutionizes network security, utilizing a breakthrough multi-core design and patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology* offering complete protection without compromising network performance. This platform was first made available on the SonicWALL E-Class NSA Series, and it is now available for mid-sized organizations.

The NSA Series overcomes the limitations of existing security solutions by scanning the entirety of each packet for current internal and external threats in real time. Built on a high-speed multi-core processing platform, the NSA Series enables deep packet inspection without adversely impacting the performance of mission-critical networks and applications.

**The NSA Series applies next-generation Unified Threat Management (UTM) against a comprehensive array of attacks, combining intrusion prevention, anti-virus and anti-spyware with the application-level control of SonicWALL Application Intelligence Service.** With advanced routing, stateful high-availability and high-speed IPSec and SSL VPN technology, the NSA Series adds security, reliability, functionality and productivity to branch offices, central sites and distributed mid-enterprise networks, while minimizing cost and complexity.

Comprised of the **SonicWALL NSA 240, 2400, NSA 3500 and NSA 4500**, the NSA Series offers a scalable range of solutions designed to meet the network security needs of any organization.

### Features and Benefits

**SonicWALL's next generation security** incorporates a new level of UTM that integrates intrusion prevention, gateway anti-virus and anti-spyware and features the Application Intelligence Service suite of configurable tools to prevent data leakage and offer granular application control.

**Scalable multi-core hardware and Reassembly-Free Deep Packet Inspection** scans and eliminates threats of unlimited file sizes, and provides virtually unrestricted concurrent connections with uncompromising speed. The NSA 240 can be configured using primary or secondary modem or 3G wireless interfaces for future-proofed extensibility.

**Stateful High Availability and load balancing features** in SonicOS 5.5 Enhanced maximize total network bandwidth and maintain seamless network uptime, delivering uninterrupted access to mission-critical resources, and ensuring that VPN tunnels and other network traffic will not be interrupted in the event of a failover.

**High performance and lowered TCO** are achieved by using the processing power of multiple cores in unison to dramatically increase throughput and provide simultaneous inspection capabilities, while lowering power consumption.

**Advanced routing services and networking features** incorporate advanced networking and security technology including 802.1q VLANs, Multi-WAN failover, zone and object-based management, load balancing, advanced NAT modes and more, providing granular configuration flexibility and comprehensive protection at the administrator's discretion.

**Standards-based Voice over IP (VoIP)** capabilities provide the highest levels of security for every element of the VoIP infrastructure, from communications equipment to VoIP-ready devices such as SIP Proxies, H.323 Gatekeepers and Call Servers.

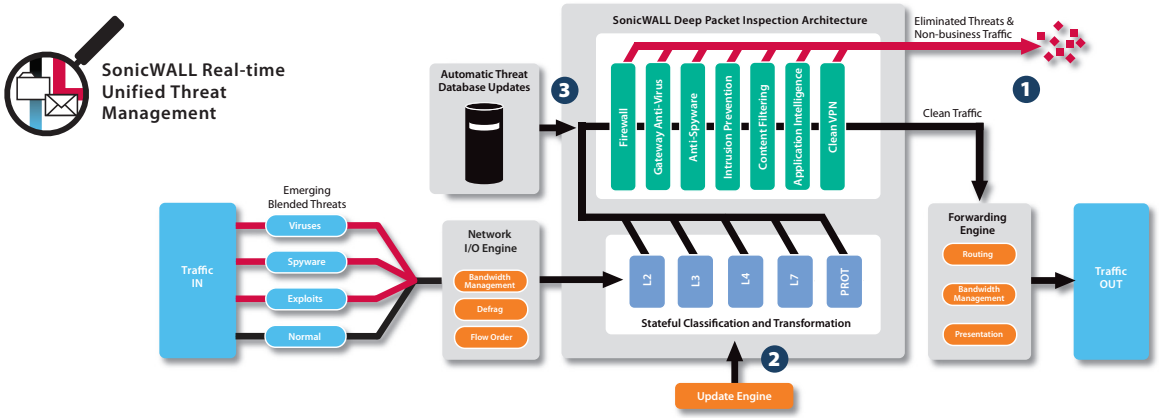
**Secure distributed wireless LAN services** enable the appliance to function as a secure wireless switch and controller that automatically detects and configures SonicPoints,™ SonicWALL wireless access points, for secure remote access in distributed network environments.

**Onboard Quality of Service (QoS)** features use industry standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators to provide powerful and flexible bandwidth management that is vital for VoIP, multimedia content and business-critical applications.

*U.S. Patent 7,310,815–A method and apparatus for data stream analysis and blocking.

SONICWALL®

## Dynamic Security Architecture and Management

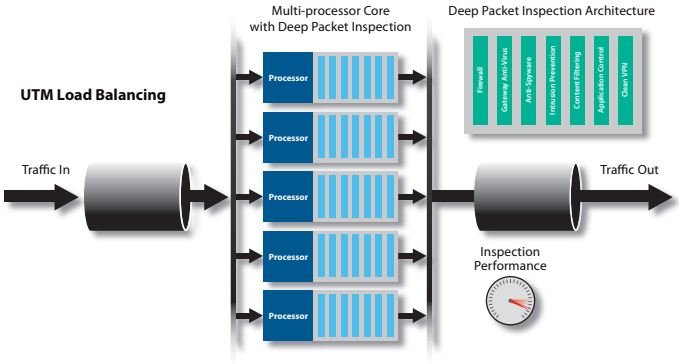


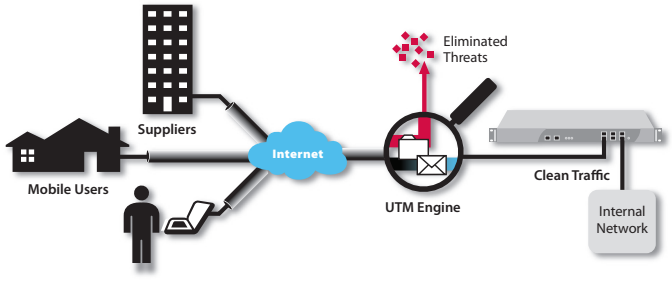

### Best-in-Class Threat Protection

1. SonicWALL deep packet inspection protects against network risks such as viruses, worms, Trojans, spyware, phishing attacks, emerging threats and Internet misuse. Application Application Intelligence adds highly-configurable controls to prevent data leakage and manage bandwidth at the application level.
2. The SonicWALL Reaseembly-Free Deep Packet Inspection (RFDPI) technology utilizes SonicWALL's multi-core architecture to scan packets in real time without stalling traffic in memory. This functionality allows threats to be identified and eliminated over unlimited file sizes and unrestricted concurrent connections, without interruption.
3. The Network Security Appliance Series provides dynamic network protection through continuous, automated security updates, protecting against emerging and evolving threats, without requiring any administrator intervention.

### Unified Threat Management Load Balancing

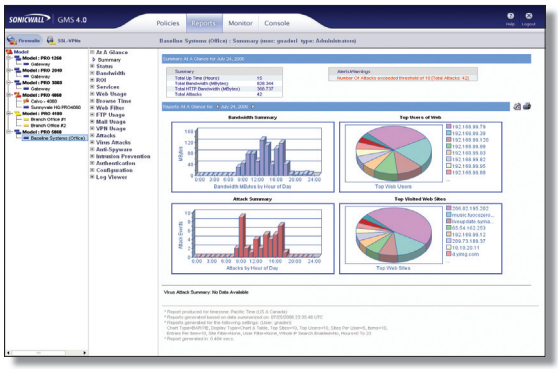
Single processor designs that include multiple protection technologies are severely limited by a single centralized processor. SonicWALL UTM load balancing integrates a high-speed deep packet inspection and traffic classification engine onto multiple security cores inspecting applications, files and content-based traffic in real time without significantly impacting performance or scalability. This enables the scanning and control of threats for networks that carry bandwidth intensive and latency sensitive applications.




### SonicWALL Clean VPN

The Network Security Appliance Series includes innovative SonicWALL Clean VPN™ technology which decontaminates vulnerabilities and malicious code from remote mobile users and branch offices traffic before it enters the corporate network, and without user intervention.



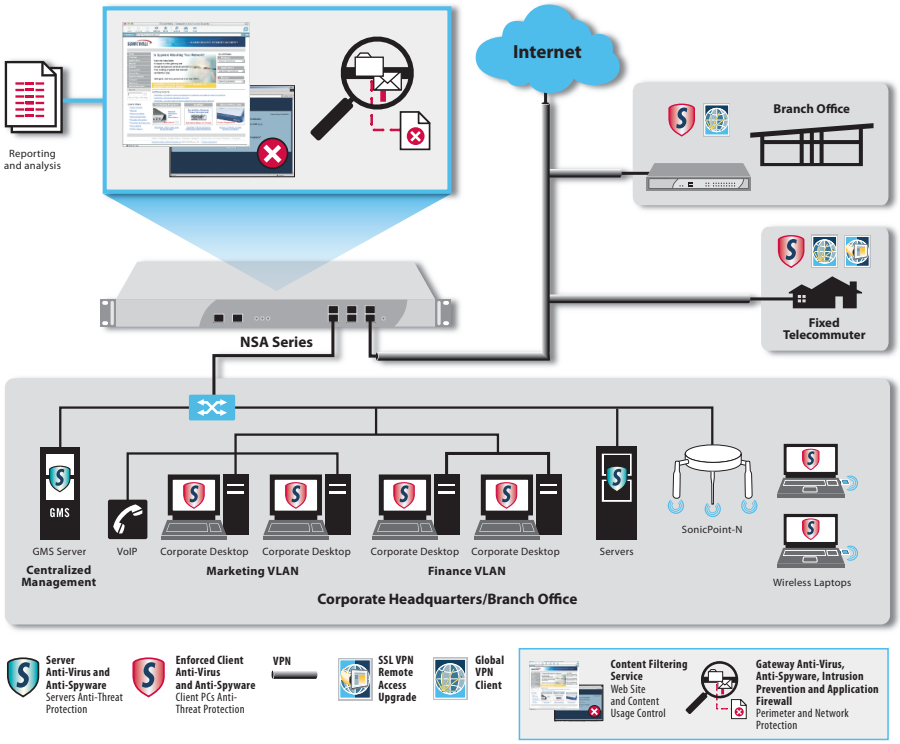
### Centralized Policy Management

The Network Security Appliance Series can be managed using the SonicWALL Global Management System (GMS), which provides flexible, powerful and intuitive tools to centrally manage configurations, view real-time monitoring metrics and integrate policy and compliance reporting.

## Flexible, Customizable Deployment Options – NSA Series At-A-Glance

Every SonicWALL Network Security Appliance solution delivers next generation Unified Threat Management protection, utilizing a breakthrough multi-core hardware design and Reassembly-Free Deep Packet Inspection for internal and external network protection without compromising network performance. Each NSA Series product combines high-speed intrusion prevention, file and content inspection, and powerful Application Intelligence Service controls with an extensive array of advanced networking and flexible configuration features. The NSA Series offers an accessible, affordable platform that is easy to deploy and manage in a wide variety of corporate, branch office and distributed network environments.

- The SonicWALL **NSA 4500** is ideal for corporate central-site and large distributed environments requiring high throughput capacity and performance
- The SonicWALL **NSA 3500** is ideal for corporate, branch office and distributed environments needing significant throughput capacity and performance
- The SonicWALL **NSA 2400** is ideal for small- to medium-sized corporate and branch office environments concerned about throughput capacity and performance
- The SonicWALL **NSA 240** is ideal for small- to medium-sized businesses and branch office sites




## Security Services and Upgrades

**Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service and Application Intelligence Service** delivers intelligent, real-time network security protection against sophisticated application layer and content-based attacks including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows. Application Intelligence Service delivers a suite of configurable tools designed to prevent data leakage while providing granular application-level controls.

**Enforced Client and Server Anti-Virus and Anti-Spyware** delivers comprehensive virus and spyware protection for laptops, desktops and servers using a single integrated client and offers automated network-wide enforcement of anti-virus and anti-spyware policies, definitions and software updates.

**Content Filtering Service** enforces protection and productivity policies by employing an innovative rating architecture, utilizing a dynamic database to block up to 56 categories of objectionable Web content.

**ViewPoint Reporting** delivers easy-to-use, Web-based capabilities that provide administrators with instant comprehensive insight into network performance and security. Delivered through a series of historical reports using dashboards and detailed summaries, ViewPoint helps organizations of all sizes track Internet usage, fulfill regulatory compliance requirements and monitor the security status of their network.

**SonicWALL® Virtual Assist** is a remote support tool that enables a technician to assume control of a PC or laptop for the purpose of providing remote technical assistance. With permission, the technician can gain instant access to a computer using a Web browser, making it easy to diagnose and fix a problem remotely without the need for a pre-installed "fat" client.

**Dynamic Support Services** are available 8x5 or 24x7 depending on customer needs. Features include world-class technical support, crucial firmware updates and upgrades, access to extensive electronic tools and timely hardware replacement to help organizations get the greatest return on their SonicWALL investment.

**Global VPN Client Upgrades** utilize a software client that is installed on Windows-based computers and increase workforce productivity by providing secure access to email, files, intranets, and applications for remote users. Upgrade licenses are available in a variety of user counts allowing this solution to scale as the organization grows.

**SSL VPN Remote Access Upgrades** provide clientless remote network level access for PC, Mac and Linux-based systems. With integrated SSL VPN technology, SonicWALL UTM appliances enable seamless and secure remote access to email, files, intranets, and applications from a variety of client platforms via NetExtender, a lightweight client that is pushed onto the user's machine. NetExtender is installed and configured automatically, requiring no user interaction.

**SonicWALL Comprehensive Anti-Spam Service** blocks spam phishing and virus-laden emails at the gateway. There is no need to redirect an MX Record or send email to another vendor, with one click the service is activated and immediately starts blocking junk email and saving valuable network bandwidth.

# Specifications

Network Security Appliance 4500
01-SSC-7012
NSA 4500 TotalSecure* (1-year)
01-SC-7032

Network Security Appliance 3500
01-SSC-7016
NSA 3500 TotalSecure* (1-year)
01-SC-7033

Network Security Appliance 2400
01-SSC-7020
NSA 2400 TotalSecure* (1-year)
01-SC-7035

Network Security Appliance 240
TotalSecure* (1-year)
01-SSC-8760

SonicWALL PC Card to
ExpressCard Adapter
(for NSA 240)
01-SSC-2887

For more information on SonicWALL network security solutions, please visit **www.sonicwall.com**.

*Includes one-year of Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence Service, Content Filtering Service, Dynamic Support 24x7 and ViewPoint Reporting.

| Firewall | NSA 240 | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|
| SonicOS Version | SonicOS Enhanced 5.6 (or higher) | | | |
| Stateful Throughput[1] | 600 Mbps | 775 Mbps | 1.5 Gbps | 2.75 Gbps |
| GAV Performance[2] | 115 Mbps | 160 Mbps | 350 Mbps | 690 MBps |
| IPS Performance[2] | 195 Mbps | 275 Mbps | 750 Mbps | 1.4 Gbps |
| UTM Performance[2] | 110 Mbps | 150 Mbps | 240 Mbps | 600 Mbps |
| IMIX Performance[2] | 195 Mbps | 235 Mbps | 580 Mbps | 700 Mbps |
| Maximum Connections[3] | 85,000/110,000[4] | 225,000 | 325,000 | 500,000 |
| Maximum UTM Connections | 32,000/50,000[4] | 125,000 | 175,000 | 250,000 |
| New Connections/Sec | 2,000 | 4,000 | 7,000 | 10,000 |
| Nodes Supported | Unrestricted | | | |
| Denial of Service Attack Prevention | 22 classes of DoS, DDoS and scanning attacks | | | |
| SonicPoints Supported (Maximum) | 16 | 32 | 32 | 64 |

| VPN | NSA 240 | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|
| 3DES/AES Throughput[5] | 150 Mbps | 300 Mbps | 625 Mbps | 1.0 Gbps |
| Site-to-Site VPN Tunnels | 25/50[4] | 75 | 800 | 1,500 |
| Bundled Global VPN Client Licenses (Maximum) | 2 (25) | 10 (250) | 50 (1,000) | 500 (3,000) |
| Bundled SSL VPN Licenses (Maximum) | 2 (15) | 2 (25) | 2 (30) | 2 (30) |
| Virtual Assist Bundled (Maximum) | 1 30-day trial (5) | 1 (5) | 2 (10) | 2 (10) |
| Encryption/Authentication/DH Group | DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1/DH Groups 1, 2, 5, 14 | | | |
| Key Exchange | Key Exchange IKE, IKEv2, Manual Key, PKI (X.509), L2TP over IPSec | | | |
| Route-Based VPN | Yes (OSPF, RIP) | | | |
| Certificate Support | Verisign, Thawte, Cybertrust, RSA Keon, Entrust, and Microsoft CA for SonicWALL-to-SonicWALL VPN, SCEP | | | |
| Dead Peer Detection | Yes | | | |
| DHCP Over VPN | Yes | | | |
| IPSec NAT Traversal | Yes | | | |
| Redundant VPN Gateway | Yes | | | |
| Global VPN Client Platforms Supported | Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-bit/64 bit, Windows 7 | | | |
| SSL VPN Platforms Supported | Microsoft® Windows 2000 / XP / Vista 32/64-bit / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE | | | |

| Security Services | NSA 240 | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|
| Deep Packet Inspection Service | Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence | | | |
| Content Filtering Service Premium Edition | (CFS) HTTP URL,HTTPS IP, keyword and content scanning ActiveX, Java Applet, and cookie blocking | | | |
| Gateway-enforced Client Anti-Virus and Anti-Spyware | HTTP/S, SMTP, POP3, IMAP and FTP, Enforced McAfee™ Clients Email attachment blocking | | | |
| Comprehensive Anti-Spam Service | Yes | | | |
| Application Intelligence | Provides application level enforcement and bandwidth control, regulate Web traffic, email, email attaches and file transfers, scan and restrict documents and files for key words and phrases | | | |
| DPI-SSL[6] | Provides the ability to decrypt HTTPS traffic transparently, scan this traffic for threats using SonicWALL's Deep Packet Inspection technology (GAV/AS/IPS/Application Intelligence/CFS),then re-encrypt the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both clients and servers. | | | |

| Networking | NSA 240 | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|
| IP Address Assignment | Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay | | | |
| NAT Modes | 1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode | | | |
| VLAN Interfaces (802.1q) | 10/25[4] | 25 | 50 | 200 |
| Routing | OSPF, RIPv1/v2, static routes, policy-based routing, Multicast | | | |
| QoS | Bandwidth priority, maximum bandwidth, guaranteed bandwidth, DSCP marking, 802.1p | | | |
| IPv6 | IPv6 Ready | | | |
| Authentication | XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix | | | |
| Internal Database/Single Sign-on Users | 100/100 Users | 250/250 Users | 300/500 Users | 1,000/1,000 Users |
| VoIP | Full H.323v1-5, SIP, gatekeeper support, outbound bandwidth management, VoIP over WLAN, deep inspection security, full interoperability with most VoIP gateway and communications devices | | | |

| System | NSA 240 | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|
| Zone Security | Yes | | | |
| Schedules | One Time, Recurring | | | |
| Object-based/Group-based Management | Yes | | | |
| DDNS | Yes | | | |
| Management and Monitoring | Web GUI (HTTP, HTTPS), Command Line (SSH, Console), SNMP v2: Global management with SonicWALL GMS | | | |
| Logging and Reporting | ViewPoint® Local Log, Syslog, Solera Networks | | | |
| High Availability | Optional Active/Passive with State Sync[4] | Optional Active/Passive with State Sync | | Active/Passive with State Sync |
| Load Balancing | Yes, (Outgoing with percent-based, round robin and spill-over); (Incoming with round robin, random distribution, sticky IP, block remap and symmetrical remap) | | | |
| Standards | TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | | | |
| Wireless Standards | 802.11 a/b/g/n, WPA2, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS | | | |

| Hardware | NSA 240 | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|
| Interfaces | (3) GE Gigabit Ports+ (6) 10/100, 2 USB, PC Card Slot (Optional 3G/Analog Modem), 1 Console Interface | (6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB | | |
| Memory (RAM) | 256 MB | 512 MB | 512 MB | 512 MB |
| Flash Memory | 32 MB Compact Flash | 512 MB Compact Flash | | |
| 3G Wireless/Modem[7]* | With 3G USB Adapter Modem | | | |
| Power Supply | 36W External | Single 180W ATX Power Supply | | |
| Fans | No Fan | 2 Fans | | |
| Power Input | 10-240V, 50-60Hz | 100-240Vac, 60-50Hz | | |
| Max Power Consumption | 15W | 42W | 64W | 66W |
| Total Heat Dissipation | 51.1BTU | 144BTU | 219BTU | 225BTU |
| Certifications | VPNC, ICSA Firewall 4.1 | | EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1 | |
| Certifications Pending | EAL-4+, FIPS 140-2 | | – | – |
| Form Factor and Dimensions | 7.125 x 1.5 x 10.5 in/ 18.10 x 3.81 x 26.67 cm | 1U rack-mountable/ 17 x 10.25 x 1.75 in/ 43.18 x 26 x 4.44 cm | | 1U rack-mountable/ 17 x 13.25 x 1.75 in/ 43.18 x 33.65 x 4.44 cm |
| Weight | 2.55Lb/1.16Kg | 8.05 lbs/ 3.65 kg | | 11.30 lbs/ 5.14 kg |
| WEEE Weight | 3.15Lb/1.43Kg | 8.05 lbs/ 3.65 kg | | 11.30 lbs/ 5.14 kg |
| Major Regulatory | FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE | | | |
| Environment | 32-105° F, 0-40° C | 40-105° F, 5-40° C | | |
| MTBF | 9.5 years | 16.0 years | 14.3 years | 14.1 years |
| Humidity | 0-95% non-condensing | | 10-90% non-condensing | |

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. [2] UTM/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. [3] Actual maximum connection counts are lower when UTM services are enabled. [4] Only with the NSA 240 Stateful HA and Expansion Upgrade. [5] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. [6] Supported on the NSA 3500 and higher. [7] Not available on NSA 2400. *USB 3G card and modem are not included. See http://www.sonicwall.com/us/products/cardsupport.html for supported USB devices.

**Certifications**

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

**SonicWALL's line-up of comprehensive protection**

NETWORK SECURITY | SECURE REMOTE ACCESS | WEB AND E-MAIL SECURITY | BACKUP AND RECOVERY | POLICY AND MANAGEMENT

**SonicWALL, Inc.**
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

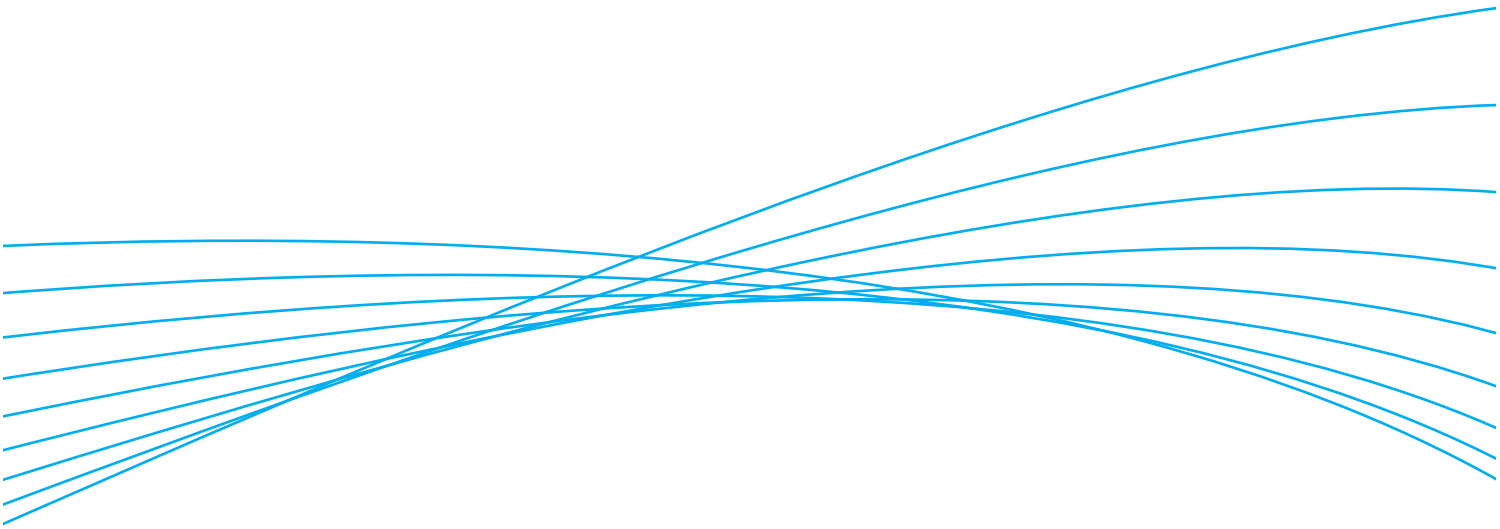
ProCurve Networking
HP Innovation

# NEW ProCurve Switch 1700 Series

The ProCurve Switch 1700 series complements the ProCurve Switch 1800 series as the newest addition to the ProCurve Web Managed portfolio. Ideal for businesses making the transition from unmanaged to managed networks, the ProCurve Switch 1700 series consists of two Web Managed switches. The ProCurve Switch 1700-24 is a 24-port switch with 22 10/100 ports plus 2 dual-personality ports. The ProCurve Switch 1700-8 is a small-form-factor switch with 7 10/100 ports and 1 10/100/1000 port. Ideal for deployment in open spaces, both switches feature silent operation via a fanless design. The ProCurve Switch 1700 series enables increased network capabilities without added complexity.

NEW ProCurve Switch 1700-24 (J9080A)

NEW ProCurve Switch 1700-8 (J9079A)



hp invent

## Features and benefits

**Deployment flexibility**

- **Small form factor**: ideal for desktop use; space-efficient for deployment flexibility (1700-8 only)
- **Designed with no fan**: enables quiet operation for deployment in open spaces

**Manageability**

- **Intuitive Web interface**: enables simple management via an easy-to-use Web browser interface for switch configuration, monitoring, and administration
- **Integration with ProCurve Manager**: enables discovery and mapping via ProCurve Manager, available as a free download from the Web
- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP)**: automated device discovery protocol for easy mapping by network management applications

**Ease of use**

- **Comprehensive LED display with per-port indicators**: provides an at-a-glance view of status, activity, speed, and full-duplex operation
- **ProCurve/IEEE Auto-MDIX**: automatically adjusts for straight-through or crossover cables on all RJ-45 ports

**Security**

- **Management password**: provides security so that only authorized access to the Web browser interface is allowed

**Layer 2 switching**

- **VLAN support and tagging**: support up to 64 port-based VLANs and dynamic configuration of IEEE 802.1Q VLAN tagging, providing security between workgroups

**Resiliency and high availability**

- **IEEE 802.3ad Link Aggregation Control Protocol (LACP)**: provides link-level redundancy; support for up to 4 trunks, with up to 7 links (ports) per trunk on the Switch 1700-8, and support for 12 trunks, with up to 8 links (ports) per trunk on the Switch 1700-24

**Quality of Service (QoS)**

- **IEEE 802.1p prioritization**: delivers data to devices by honoring the priority and type of traffic
- **Broadcast control**: allows limitation of broadcast traffic rate to cut down on unwanted broadcast traffic on the network

**Monitoring and diagnostics**

- **Port mirroring**: enables traffic on a port to be simultaneously sent to a network analyzer for monitoring

**Industry-leading warranty**

- **Lifetime warranty**: for as long as you own the product, with next-business-day advance replacement (available in most countries)

## Services

Check **www.hp.com/go/procurveservices** for part numbers and service-level descriptions. For details about services and response times in your area, please contact your local HP sales office.

## Accessories

**ProCurve Gigabit-SX-LC Mini-GBIC (J4858B)**
(1700-24 only)

**ProCurve Gigabit-LX-LC Mini-GBIC (J4859B)**
(1700-24 only)

**ProCurve Gigabit-LH-LC Mini-GBIC (J4860B)**
(1700-24 only)

**ProCurve Manager 2.1**

**ProCurve Manager Plus 2.1 100-device limited version (J8778A)**

**ProCurve Manager Plus 2.1 upgrade to unlimited license (J8779A)**

**ProCurve Manager Plus 2.1 100 device Upgrade (J8991A)**

**ProCurve Manager Plus 2.1 unlimited license (J9009A)**

# ProCurve Switch 1700 Series

## Specifications

| | ProCurve Switch 1700-24 (J9080A) | ProCurve Switch 1700-8 (J9079A) |
|---|---|---|
| **Ports** | 22 10/100 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX) | 7 10/100 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX) |
| **Transceiver** | 2 dual-personality ports—each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) | 1 10/100/1000 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab 1000Base-T Gigabit Ethernet) |
| **Physical characteristics** | | |
| Dimensions (D x W x H) | 17.12 x 44.25 x 4.39 cm (6.74 x 17.42 x 1.73 in.) (1U height) | 11.63 x 19.63 x 4.39 cm (4.58 x 7.73 x 1.73 in.) (1U height) |
| Weight | 1.99 kg (4.38 lb.) | 0.54 kg (1.19 lb.) |
| **Memory and processor** | | |
| Packet buffer size | 500 KB | 144 KB |
| RAM/ROM capacity | 2 MB | 1 MB |
| Flash capacity | 2 MB | 1 MB |
| **Mounting** | Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included) | Horizontal surface mounting only |
| **Performance** | | |
| Latency | | |
| 100 Mb latency | <4.7 µs (64-byte packets) | <3.9 µs (64-byte packets) |
| 1000 Mb latency | <3.0 µs (64-byte packets) | <2.1 µs (64-byte packets) |
| Throughput | Up to 6.25 million pps (64-byte packets) | Up to 2.08 million pps (64-byte packets) |
| Switching capacity | 8.4 Gbps | 3.4 Gbps |
| MAC address table size | 8,000 entries | 8,000 entries |
| **Environment** | | |
| Operating temperature | 0°C to 40°C (32°F to 104°F) | 0°C to 40°C (32°F to 104°F) |
| Operating relative humidity | 15% to 95% @ 40°C (104°F), non-condensing | 15% to 95% @ 40°C (104°F), non-condensing |
| Non-operating/Storage temperature | –40°C to 70°C (–40°F to 158°F) | –40°C to 70°C (–40°F to 158°F) |
| Non-operating/Storage relative humidity | 10% to 90% @ 65°C (149°F), non-condensing | 10% to 90% @ 65°C (149°F), non-condensing |
| Altitude | Up to 3 km (10,000 ft.) | Up to 3 km (10,000 ft.) |
| Acoustic | Power: 0 dB, no fan | Power: 0 dB, no fan |
| **Electrical characteristics** | | |
| Maximum heat dissipation | 86.51 kJ/hr (82 BTU/hr) | 64.35 kJ/hr (61 BTU/hr) |
| Voltage | 100–127 VAC/200–240 VAC | 100–127 VAC/200–240 VAC |
| Current | 0.75 A/0.4 A | 1.0 A/0.8 A |
| Power consumption | 24 W | 18 W |
| Frequency | 50/60 Hz | 50/60 Hz |
| Notes | N/A | The exact input voltage and frequency rating are determined by the specific power adapter part number ordered. Please select the correct power adapter country option. |
| **Safety** | CSA 22.2 No. 60950; EN 60950/IEC 60950; UL 60950 | |
| **Emissions** | FCC Rules Part 15, Subpart B Class A; EN55022; VCCI; ICES-003 (Canada) | |
| **Immunity** | | |
| EN | EN55024, CISPR 24 | EN55024, CISPR 24 |
| ESD | IEC 61000-4-2 | IEC 61000-4-2 |
| Radiated | IEC 61000-4-3 | IEC 61000-4-3 |
| EFT/Burst | IEC 61000-4-4 | IEC 61000-4-4 |
| Surge | IEC 61000-4-5 | IEC 61000-4-5 |
| Conducted | IEC 61000-4-6 | IEC 61000-4-6 |
| Power frequency magnetic field | IEC 61000-4-8 | IEC 61000-4-8 |
| Voltage dips and interruptions | IEC 61000-4-11 | IEC 61000-4-11 |
| Harmonics | IEC61000-3-2 | IEC61000-3-2 |
| Flicker | IEC61000-3-3 | IEC61000-3-3 |
| **Management** | ProCurve Manager; Web browser | ProCurve Manager; Web browser |
| **Standards and protocols** | IEEE 802.3x Flow Control; IEEE 802.3ad Link Aggregation Control Protocol; IEEE 802.1AB Link Layer Discovery Protocol; IEEE 802.1Q VLANs; IEEE 802.1p Priority; RFC 1534 DHCP/BootP | |
| **Notes** | Use only supported genuine ProCurve mini-GBICs with your switch. | |

## For more information

To learn more about ProCurve Networking, please visit
**www.hp.com/eur/procurve**



4AA1-0121EEE, 03/2007

ProCurve Networking
HP Innovation

## APC Smart-UPS 1500VA USB & Serial RM 2U 230V

APC Smart-UPS, 1500VA/980W,
Input 230V/Output 230V, Interface Port DB-9 RS-232, SmartSlot, USB, Rack Height 2 U
Includes: CD with software, Rack Mounting Brackets, Rack Mounting support rails, Smart UPS signalling RS-232 cable, USB cable, User Manual

Part Number : **SUA1500RMI2U**

**Over 10 million currently installed - the one you can trust**

APC Smart-UPS® XL protects your data by supplying reliable, network-grade power with scalable run-time in tower and rack mount form factors. With optional, matching battery packs, run-time can be easily extended and optimized for the application. APC understands long run-time requirements so; Smart-UPS® XL's can be configured with up to 10 additional battery packs - for run-times exceeding 24 hours, if necessary. The convergence of voice and data networks is placing higher demands on availability expectations - and the Smart-UPS® XL delivers. Voice over Internet Protocol (VoIP), e-commerce, WiFi ("hotspots", WLAN/ WWAN, and mixed wireless), and data enabled PBX's are a few of the applications driving the need for Smart-UPS® XL. APC Smart-UPS® XL is also the perfect UPS for fileservers (Intel or UNIX based), minicomputers, Network switches and hubs, ATM's, telecommunications systems and other mission-critical applications requiring longer runtime.

With included PowerChute® management software for servers and workstations, IT administrators can provide safe system shutdown and advanced UPS management (All major operating systems supported). Connectivity is through a serial or USB port (USB not standard on all models, see specific models for details). Additional manageability is available through the SmartSlot, an internal accessory slot that allows you to install optional accessories to enhance the performance of your UPS. Network connection with Web browser management and/or environmental monitoring, serial port expansion, and out-of-band management options are available. With pure sine-wave output ensuring compatibility with all connected devices, Intelligent Battery Management ensuring a highly available UPS and an advanced 16 segment bar graph display ensuring information and management, the Smart-UPS® XL is a UPS you can count on.

## Features & Benefits

| Availability | |
|---|---|
| Power conditioning | Protects connected loads from surges, spikes, lightning, and other power disturbances. |
| Temperature-compensated battery charging | Prolongs battery life by regulating the charge voltage according to actual battery temperature. |
| Intelligent battery management | Provides higher availability through intelligent precision-charging that maximizes battery performance, life, and reliability. |
| Automatic restart of loads after UPS shutdown | Automatically starts up the connected equipment upon the return of utility power. |
| Automatic self-test | Ensures early detection of potential problems by periodic testing of UPS components. |
| Boost and Trim Automatic Voltage Regulation (AVR) | Preserves battery life and maximizes run time by correcting low and high voltage conditions without discharging the battery. |
| Cold-start capable | Provides temporary battery power when the utility power is out. |
| Generator compatible | Ensures clean, uninterrupted power to protected equipment when generator power is used. |

| Manageability | |
|---|---|
| SmartSlot | Customize UPS capabilities with management cards. |
| Audible alarms | Actively let you know if the unit is on battery, if the battery is low or if there is an overload condition. |
| LED status indicators | Quickly understand UPS status with indicators. |
| Network manageable | Provides remote management of the UPS over the network. |
| Serial Connectivity | Provides management of the UPS via a serial port. |

| Serviceability | |
|---|---|
| Hot-swappable batteries | Ensures clean, uninterrupted power to protected equipment throughout battery replacement. |
| Predictive failure notification | Provides early-warning fault analysis ensuring proactive component replacement. |
| Resettable circuit breakers | Enables quick recovery from UPS overload events. |

| Adaptability | |
|---|---|
| Adjustable voltage-transfer points | Saves battery power and helps extend battery life. |
| Adjustable voltage sensitivity | Provides the ability to adapt the UPS for optimal performance in specific power environments or generator applications. |

| Safety | |
|---|---|
| Safety-agency approved | Ensures product testing and approval to work safely with the connected loads and within the environment. |

# Technical Specifications

## Output

| | |
|---|---|
| Output power capacity | 1500 VA |
| Output power capacity | 980 watts |
| Max Configurable Power | 1500 VA |
| Max Configurable Power | 980 watts |
| Nominal output voltage | 230V |
| Output Voltage Note | Configurable for 220 : 230 or 240 nominal output voltage |
| Output Voltage Distortion | less than 5% at full load |
| Output Frequency (sync to mains) | 47-53Hz for 50Hz nominal , 57-63Hz for 60Hz nominal |
| Crest Factor | up to 5 : 1 |
| Waveform type | Sinewave |
| Output Connections | (4) IEC 320 C13  (2) IEC Jumpers |

## Input

| | |
|---|---|
| Nominal input voltage | 230V |
| Input frequency | 50/60 Hz +/- 3 Hz (auto sensing) Hz |
| Input Connection Type | IEC-320 C14 |
| Input voltage range for main operations | 160 - 286 V |
| Input voltage adjustable range for mains operation | 151 - 302 V |

## Batteries & Runtime

| | |
|---|---|
| Battery type | Maintenance-free sealed Lead-Acid battery with suspended electrolyte : leakproof |
| Replacement battery cartridge | RBC24 |
| RBC™ Quantity | 1 |
| Typical backup time at half load | 26.5 minutes (490 Watts) |
| Typical backup time at full load | 7.4 minutes (980 Watts) |
| Runtime Chart | Smart-UPS |

## Surge Protection and Filtering

| | |
|---|---|
| Surge energy rating | 480 Joules |
| Filtering | Full time multi-pole noise filtering : 0.3% IEEE surge let-through : zero clamping response time : meets UL 1449 |

## Communications & Management

| | |
|---|---|
| Interface port | DB-9 RS-232 , SmartSlot , USB |
| Available Smart Slot Interface Quantity | 1 |
| Control panel | LED status display with load and battery bar-graphs and On Line : On Battery : Replace Battery : and Overload Indicators |
| Audible alarm | Alarm when on battery : distinctive low battery alarm : configurable delays |
| Emergency Power Off (EPO) | Optional |

## Physical

| | |
|---|---|
| Maximum height | 3.50 inches ( 89 mm ) |
| Maximum width | 19.00 inches ( 483 mm ) |
| Maximum depth | 18.00 inches ( 457 mm ) |
| Rack Height | 2 U |
| Net weight | 63.00 lbs. ( 28.64 kg ) |
| Shipping Weight | 70.20 lbs. ( 31.91 kg ) |
| Shipping Height | 10.00 inches ( 254 mm ) |
| Shipping Width | 23.38 inches ( 594 mm ) |
| Shipping Depth | 23.75 inches ( 603 mm ) |
| Color | Black |
| Units per Pallet | 16.00 |

## Environmental

| | |
|---|---|
| Operating Environment | 0 - 40 °C ( 32 - 104 °F ) |
| Operating Relative Humidity | 0 - 95 % |
| Operating Elevation | 0-10000 feet ( 0-3000 meters ) |
| Storage Temperature | -15 - 45 °C ( 5 - 113 °F ) |
| Storage Relative Humidity | 0 - 95 % |
| Storage Elevation | 0-50000 feet ( 0-15000 meters ) |
| Online thermal dissipation | 171 BTU/hr |

## Conformance

| | |
|---|---|
| Approvals | C-tick , CE , EN 50091-1 , EN 50091-2 , TUV , VDE |
| Standard warranty | 2 years repair or replace , optional on-site warranties available , optional extended warranties available |

Hirschmann.
Simply a good Connection.

WWW.HIRSCHMANN.COM

HIRSCHMANN

OpenRail System

# 12 parameters, 1000 versions: The Hirschmann managed switch range for maximum individuality.

# 12 Parameter, 1000 Varianten: Das Hirschmann Managed Switch Programm für maximale Individualität.

## The core of your order:
## Das Herzstück Ihrer Order:

*The order code that contains all the important options for us and using which you can track your order at any time (online tracking).*
*Der Bestellcode, der alle für uns wichtigen Optionen beinhaltet und über den Sie Ihre Bestellung jederzeit nachverfolgen können (Online-Tracking).*

| RS 30 | 24 | 02 | T1 | O6 | S | D | B | P | H | H | 01.0 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Design | FE ports | GE ports | Type 1 uplink port | Type 2 uplink port | Temperature | Power supply | Approvals | Software | Configuration | OEM type | Software release |

**Compact switch (Rail)**
- RS 20 Fast-ETHERNET uplinks
- RS 30 Gigabit-ETHERNET uplinks

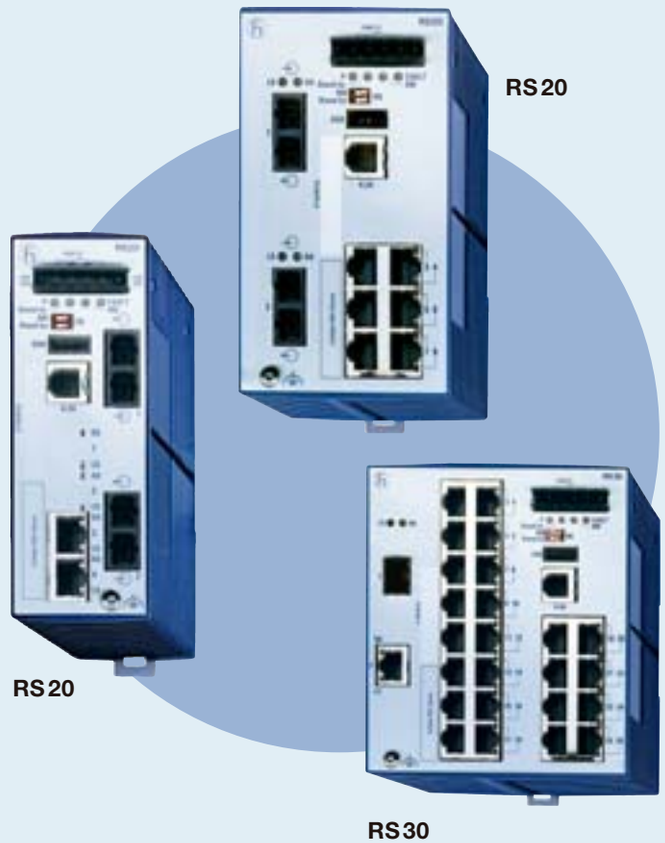
**Modular switch (MICE)**
- MS 20 Fast-ETHERNET uplinks
- MS 30 Gigabit-ETHERNET uplinks

**Number of Fast-ETHERNET ports**
- 04 4 x 100 Mbit
- 08 8 x 100 Mbit
- 16 16 x 100 Mbit
- 24 24 x 100 Mbit

**Number of Gigabit-ETHERNET ports**
- 00 0 x 1000 Mbit
- 02 2 x 1000 Mbit

**Type 1 uplink port**
- T1 Twisted Pair / RJ45
- T5 Twisted Pair / M12 (100 Mbit)
- M2 Multimode / SC (100 Mbit)
- M4 Multimode / ST (100 Mbit)
- S2 Singlemode / SC (100 Mbit)
- L2 Singlemode LH / SC (100 Mbit)
- O6 SFP slot (1000 Mbit)

**Type 2 uplink port**
- T1 Twisted Pair / RJ45
- T5 Twisted Pair / M12 (100 Mbit)
- M2 Multimode / SC (100 Mbit)
- M4 Multimode / ST (100 Mbit)
- S2 Singlemode / SC (100 Mbit)
- L2 Singlemode LH / SC (100 Mbit)
- O6 SFP slot (1000 Mbit)




**Software release**
- 01.0 Software release 1.0

**OEM type**
- H Standard
- X Customer specific

**Configuration**
- H Standard
- X Customer specific

**Software version**
- E Enhanced:
  Remote access, diagnosis, filters, redundancy
- P Professional:
  Enhanced software plus security, extended diagnosis and redundancy

**Approvals**
- A cUL508, cUL1604 Class1 Div.2
- B cUL508, cUL1604 Class1 Div.2, GL
  Substation IEC61850,
  Railway standard EN 50121-4/EN 50155
  ATEX 100a Zone 2

**Power supply**
- A 18 – 32 V DC MICE
- C 32 – 60 V DC MICE
- D 9.6 – 60 V DC and 18 – 30 V AC Rail

**Temperature range**
- S Standard 0 °C up to +60 °C
- E Extended – 40 °C up to +70 °C
  inclusive Conformal Coating

= Compulsory
= Pflichtfeld

= Optional
= Optional

# EDS-508A/505A Series

## *8- and 5-Port Managed Ethernet Switch*

### Highlights

- Plug-n-play Turbo Ring (recovery time < 20 ms), RSTP/STP (IEEE802.1W/D) for Ethernet redundancy
- QoS, IGMP snooping/GMRP, VLAN, LACP, SNMP V1/V2c/V3, RMON supported
- Customer configured e-mail notification by exception
- User-friendly web-based configuration and management
- -40 to 75˚C operating temperature (T models)
- ABC-01 (Automatic Backup Configurator) for system configuration backup

### Features

#### Advanced Industrial Networking Capability

- Plug-n-Play, Turbo Ring (recovery time < 20 ms at full load) and RSTP/STP (IEEE802.1W/D)
- IGMP Snooping and GMRP for filtering multicast traffic from industrial Ethernet
- Port-based VLAN, IEEE802.1Q VLAN and GVRP protocol to ease network planning
- QoS-IEEE802.1p/1Q and TOS/DiffServ to increase determinism
- 802.3ad, LACP for optimum bandwidth utilization
- Port Trunking for optimum bandwidth utilization
- RMON for efficient network monitoring and proactive capability
- SNMP V1/V2c/V3 for different levels of network management security
- IEEE802.1X and https/SSL to enhance network security

#### Designed for Industrial Applications

- Bandwidth management prevents unpredictable network status
- ABC-01 (Automatic Backup Configurator) for system configuration backup
- Port lock for access from unauthorized MAC address
- Port mirroring for online debugging
- Automatic warning by exception through e-mail and relay output
- Digital inputs to integrate sensors and alarms with IP networks
- Automatic recovery of connected device's IP addresses
- Line-swap fast recovery (Patented)
- Redundant, dual DC power inputs
- Regular (0 to 60°C) and extended (-40 to 75°C) operating temperature models available
- IP30, rugged high-strength case
- Long-haul transmit distance of 40 km or 80 km
- DIN-Rail or panel mounting ability
- Configurable by Web browser, Telnet/Serial console, Windows utility
- Ping commands to identify network segment integrity

#### Recommended Software and Accessories

- ABC-01 RS-232 RJ45-based Automatic Backup Configurator
- EDS-SNMP OPC Server Pro
- DR series DIN-Rail 24 VDC power supplies

### Introduction

EDS-508A/505A is a plug-and-play managed redundant Ethernet switch. A set of Turbo Ring DIP switches makes it easy to set up Turbo Ring (recovery time < 20 ms) to increase system reliability. In addition, EDS-508A/505A supports many advanced managed features, such as QoS, 802.1Q VLAN, port-based VLAN, IEEE802.1X, SSL, SNMP V1/V2c/V3, IGMP Snooping, Port Trunking, and RMON for network management. The extended operating temperature range of -40 to 75°C is also available.

## Specifications

### Technology

**Standards:** IEEE802.3, 802.3u, 802.3x, 802.1D, 802.1W, 802.1Q, 802.1p , 802.1X, 802.3ad

**Protocols:** IGMP V1/V2/V3 device, GVRP, SNMP V1/V2c/V3, DHCP Server/Client, DHCP Option 82, BootP, TFTP, SNTP, SMTP, RARP, GMRP, LACP, RMON

**MIB:** MIB-II, Ethernet-Like MIB, P-BRIDGE MIB, Q-BRIDGE MIB, Bridge MIB, RSTP MIB, RMON Group 1, 2, 3, 9

**Flow Control:** IEEE802.3x flow control, back pressure flow control

### Interface

**RJ45 Ports:** 10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection

**Fiber Ports:** 100BaseFX ports (SC/ST connector)

**Console:** RS-232 (RJ45)

**LED Indicators:** PWR1, PWR2, FAULT, MASTER, COUPLER, 10/100M

**DIP Switch:** Turbo Ring, Master, Coupler, Reserve

**Alarm Contact:** Two relay outputs with current carrying capacity of 1A @ 24 VDC

**Digital Input:** Two inputs with the same ground, but electrically isolated from the electronics

- +13 to +30V for state "1"
- -30 to +3V for state "0"
- Max. input current: 8 mA

### Optical Fiber

**Distance:**

Multi mode: 0 to 5 km, 1300 nm (50/125 µm, 800 MHz*km)
0 to 4 km, 1300 nm (62.5/125 µm, 500 MHz*km)

Single mode: 0 to 40 km, 1310 nm (9/125 µm, 3.5 PS/(nm*km))
0 to 80 km, 1550 nm (9/125 µm, 19 PS/(nm*km))

**Min. TX Output:**
Multi mode : -20 dBm

Single mode: 0 to 40 km, -5 dBm
0 to 80 km, -5 dBm

**Max. TX Output:**
Multi mode : -14 dBm

Single mode: 0 to 40 km, 0 dBm
0 to 80 km, 0 dBm

**RX Sensitivity:** -34 to -30 dBm (Multi), -36 to -32 dBm (Single)

### Power

**Input Voltage:** 24 VDC (12 to 45 VDC), redundant dual inputs

**Connection:** Two removable 6-pin terminal blocks

**Overload Current Protection:** Present

**Reverse Polarity Protection:** Present

### Mechanical

**Casing:** IP30 protection, aluminum case

**Dimensions (W x H x D):** 80.5 x 135 x 105 mm
3.17 x 5.31 x 4.13 in.

**Weight:** 1040 g

**Installation:** DIN-Rail, Wall Mounting (optional kit)

### Environmental

**Operating Temperature:** 0 to 60°C (32 to 140°F)
-40 to 75°C (-40 to 167°F) for T models

**Storage Temperature:** -40 to 85°C (-40 to 185°F)

**Ambient Relative Humidity:** 5 to 95% (non-condensing)

### Regulatory Approvals

**Safety:** UL508, UL60950-1, CSA C22.2 No. 60950-1, EN60950-1

**Hazardous location:**
UL/cUL Class I, Division 2, Groups A, B, C, and D (Pending)
ATEX Class I, Zone 2, EEx nC IIC (Pending)

**Maritime:** DNV, GL

**EMI:** FCC Part 15, CISPR (EN55022) class A

**EMS:** EN61000-4-2 (ESD), level 3
EN61000-4-3 (RS), level 3
EN61000-4-4 (EFT), level 4
EN61000-4-5 (Surge), level 3
EN61000-4-6 (CS), level 3
EN61000-4-8
EN61000-4-11

**Shock:** IEC60068-2-27

**Freefall:** IEC60068-2-32

**Vibration:** IEC60068-2-6

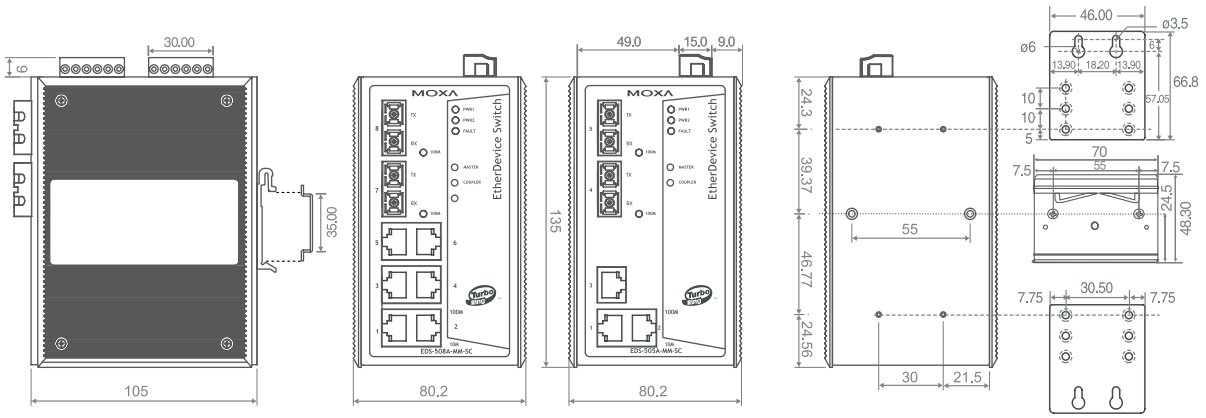
**MTBF:** EDS-508A series: 339,000 hrs
EDS-505A series: 352,000 hrs
Database: Telcordia (Bellcore), GB

*Please check MOXA's website for the most up-to-date certification status.

### Warranty

5 years

## Dimensions (unit = mm)




Side View | DIN-Rail Kit | Front View | Rear View | Panel Mounting Kit

## Ordering Information

**EDS-508A/505A-AA-BB-CC-D**

| Ordering Code Definition | Fiber Port | FO Connector | Single Mode Distance | Operating Temperature |
|---|---|---|---|---|
| | **MM:** Two Multi Mode<br>**SS:** Two Single Mode | **SC:** SC Connector<br>**ST:** ST Connector | **80:** 80 km | **T:** Operating Temp. -40 to 75°C (Standard Models: 0 to 60°C) |

**Available Models**

**EDS-508A Series**

| Standard: | Long-Haul: | Wide Temperature: |
|---|---|---|
| • EDS-508A | • EDS-508A-SS-SC-80 | • EDS-508A-T |
| • EDS-508A-MM-SC | | • EDS-508A-MM-SC-T |
| • EDS-508A-MM-ST | | • EDS-508A-MM-ST-T |
| • EDS-508A-SS-SC | | • EDS-508A-SS-SC-T |
| | | • EDS-508A-SS-SC-80-T |

**EDS-505A Series**

| Standard: | Long-Haul: | Wide Temperature: |
|---|---|---|
| • EDS-505A | • EDS-505A-SS-SC-80 | • EDS-505A-T |
| • EDS-505A-MM-SC | | • EDS-505A-MM-SC-T |
| • EDS-505A-MM-ST | | • EDS-505A-MM-ST-T |
| • EDS-505A-SS-SC | | • EDS-505A-SS-SC-T |
| | | • EDS-505A-SS-SC-80-T |

**Optional Accessories**

- **ABC-01:** Industrial RS-232, RJ45-based, Automatic Backup Configurator
- **DR-4524:** 45W/2A DIN-Rail 24 VDC Power Supply, 85 to 264 VAC input
- **DR-75-24:** 75W/3.2A DIN-Rail 24 VDC Power Supply, 85 to 264 VAC input
- **DR-120-24:** 120W/5A DIN-Rail 24 VDC Power Supply, 88 to 132 VAC/176 to 264 VAC input by switch
- **WK-46:** Wall Mounting Kit