



**UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO**

---

---

**FACULTAD DE ESTUDIOS SUPERIORES  
ARAGÓN**

**“DISEÑO E IMPLEMENTACIÓN DE UNA RED VIRTUAL PARA  
USO ACADÉMICO (VLAN INALÁMBRICA)”**

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE  
INGENIERO MECÁNICO ELÉCTRICO  
P R E S E N T A :**

**MORALES LUNA JOSÉ LUIS.  
VELÁZQUEZ JIMÉNEZ DANIEL.**

**ASESOR: ING. BENITO BARRANCO CASTELLANOS**



**2010.**



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

<b>Indice</b>	<b>I</b>
<b>Introducción</b>	<b>II</b>
<b>Capítulo 1. Redes y equipos de interconexión</b>	
1.1 Uso de las redes de computadoras	1
1.2 Hardware de red	2
1.3 Software de red	7
1.4 Puentes y los switches	18
1.5 Los ruteadores	19
1.6 Componentes de redes inalámbricas	23
1.7 Modos de operación de redes inalámbricas	27
1.8 Ejemplos reales de infraestructura inalámbrica	28
1.9 Consideraciones	29
<b>Capítulo 2. Estado inicial de la red</b>	<b>30</b>
2.1 Situación inicial	31
2.2 Equipos usados para la WLAN	26
2.3 Inconvenientes	39
2.4 Inseguridad	40
<b>Capítulo 3. Diseño y configuración de la VLAN inalámbrica</b>	<b>43</b>
3.1 Visión general para el diseño del sistema.	43
3.2 Conexión de equipos inalámbricos más robustos	57
3.3 Ubicación de antenas	58
3.4 DHCP por servidor	59
3.5 Proceso de registro para usuarios	63
3.6 Implementación de VLAN para la red inalámbrica	66
3.7 Pruebas en Campo	71
3.8 Situación actual	72
<b>Conclusiones</b>	<b>74</b>
<b>Glosario de términos</b>	<b>76</b>
<b>Bibliografía</b>	<b>88</b>

## Objetivo

Rediseñar la parte inalámbrica de una red de uso académico, haciendo uso de los recursos que ya se tienen, aprovechando al máximo sus capacidades, como las antenas omnidireccional y sectorial con las que ya se cuenta, además de los equipos inalámbricos enterasys propuestos para la realización del proyecto, valiéndonos también de las bondades de los equipos de Switchero para poder separar el tráfico de la red inalámbrica y de esta forma segmentar el broadcast de la misma, para poder implementar métodos de seguridad más eficientes y robustos que den confiabilidad a la red inalámbrica como a la alámbrica.

## Introducción

La aplicación como caso real, hace caso a las necesidades por parte del departamento de computo para solucionar un problema latente, al hacer la propuesta de VLANs pretendemos dar solución a la administración de la red, específicamente la administración de direcciones IP.

Además, como segunda instancia e independientemente de la red inalámbrica, ponemos en práctica los conocimientos adquiridos en el campo de trabajo para comenzar a realizar la segmentación en toda la unidad, trabajo que realizaremos como proyecto a corto plazo, para mejorar la calidad del servicio en cualquier unidad académica.

**El capítulo 1** hace referencia a las redes de computadoras, a lo largo del desarrollo encontraremos, uso de las computadoras, *software* (equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas) y *hardware* (corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado) de red, modelos de referencia, switches y routers, y ejemplos de tecnologías, Ethernet y Token ring, que son los percursores de todas las tecnologías actuales, con esto se pretende adentrar a lector en el marco teórico.

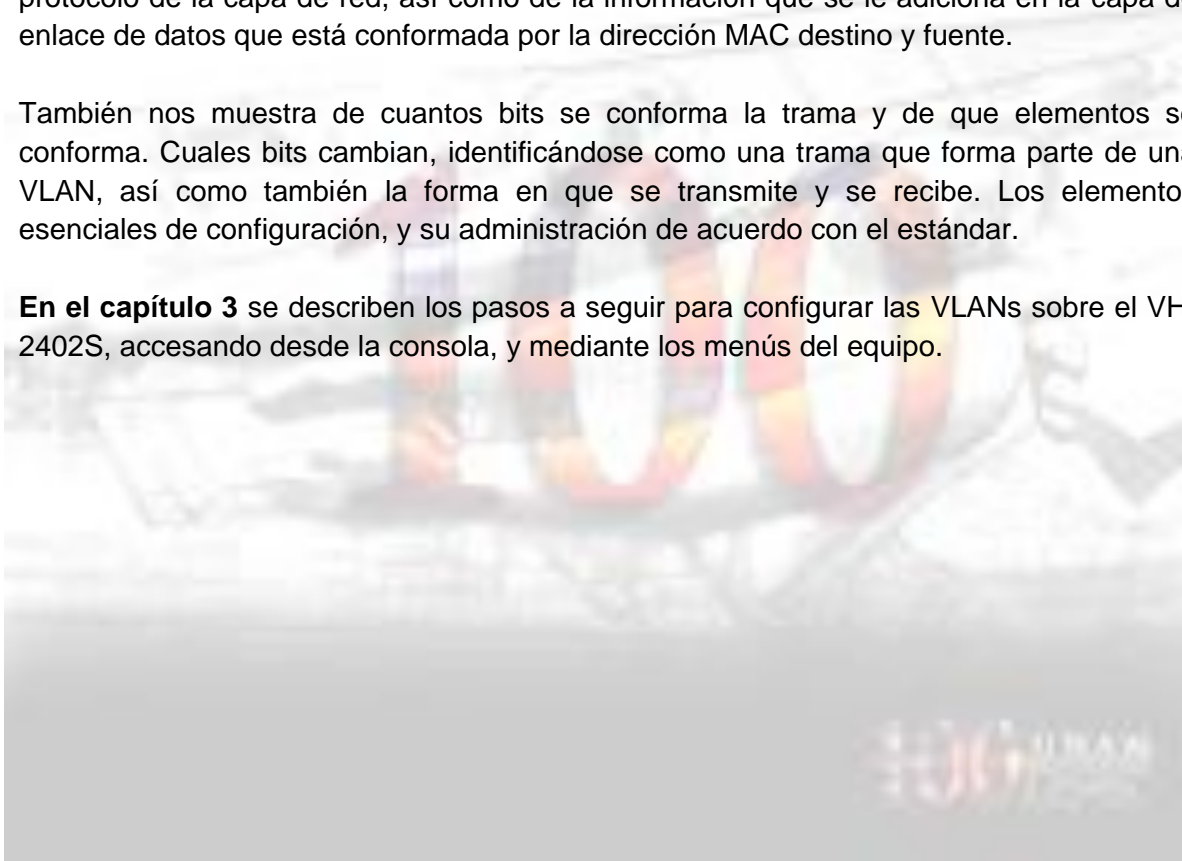
El tema principal y al que está enfocado el trabajo presentado son las VLANs que son Redes Virtuales de Área Local, son agrupamientos lógicos de dispositivos o usuarios que se pueden agrupar por función, departamento, aplicación, etc., independientemente de su ubicación física en un segmento de la red. El punto más importante de este tipo de agrupación ya sea de manera estática y/o dinámica; es que esto se hace directamente en un Switch Administrable de Capa 2 del Modelo de referencia OSI (Capa de Enlace de Datos) realizando segmentación de dominios de colisión, por lo que la comunicación será más eficiente debido a que la carga en el Router (capa 3 del modelo de referencia OSI), es menor y más rápida.

Además permite una fácil escalabilidad debido a su fácil administración que permite adicionar puertos como miembros a una VLAN dada.

**El capítulo 2** se refiere básicamente a cómo están compuestas las tramas basadas en el estándar IEEE 802.1Q, referente a la conformación de VLANs desde su forma de identificarse y diferenciarse de otros tipos de tramas, debido al filtro de la base de datos, al agrupado de los usuarios y en base a las direcciones MAC del Switch, o el tipo de protocolo de la capa de red, así como de la información que se le adiciona en la capa de enlace de datos que está conformada por la dirección MAC destino y fuente.

También nos muestra de cuantos bits se conforma la trama y de que elementos se conforma. Cuales bits cambian, identificándose como una trama que forma parte de una VLAN, así como también la forma en que se transmite y se recibe. Los elementos esenciales de configuración, y su administración de acuerdo con el estándar.

**En el capítulo 3** se describen los pasos a seguir para configurar las VLANs sobre el VH-2402S, accedendo desde la consola, y mediante los menús del equipo.



# Capítulo 1

## Redes y equipos de interconexión

El uso de las redes de computadoras en la actualidad, es tan difundido que se encuentran en los sistemas centrales que controlan casi todas las funciones de las ciudades,

### 1.1 Hardware de red

Para la clasificación del hardware de red no existe una clasificación específica, pero dos puntos sobresalen como importantes: la tecnología de transmisión y la escala. Por eso se examinarán cada una de ellas, en términos generales hay dos tipos de tecnologías de transmisión:

- Redes de difusión
- Redes punto a punto

Las redes de difusión tienen un solo canal de comunicación compartido por todas las computadoras de la red. Los mensajes cortos (llamados paquetes) que envía una computadora son recibidos por otras. Un campo de dirección dentro del paquete especifica a quien se dirige. Al recibir un paquete, una computadora verifica el campo de dirección. Si el paquete está dirigido a ella, lo procesa; si está dirigido a alguna otra computadora, lo ignora.



Fig. 1 .1 Tarjeta de red para puerto PCI

Los sistemas de difusión generalmente ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando un paquete con este código, cada computadora en la red lo recibe y lo procesa. Este modo de operación se llama difusión (broadcast) Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las computadoras, algo conocido como multidifusión. Un esquema posible consiste en reservar un bit para indicar multidifusión. Los restantes  $n-1$  bits de dirección pueden contener un número de grupo. Cada computadora se puede suscribir a cualquier grupo o a todos. Cuando se envía un paquete a cierto grupo, se entrega a todas las computadoras que se suscribieron a ese grupo.

En contraste las redes punto a punto consisten en varias conexiones entre pares individuales de computadoras. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más computadoras intermedias. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo desempeñan un papel importante



- Gran variedad y número de dispositivos conectados.
- Posibilidad de conexión con otras redes.
- Limitante de 100 m, puede llegar a más si se usan repetidores.

**1.2.1. Topologías**

Las LAN de transmisión pueden tener diversas topologías:

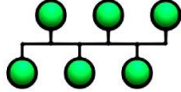
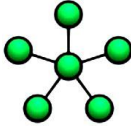
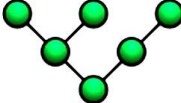
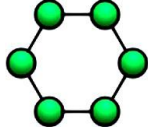
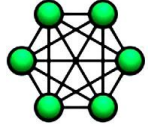
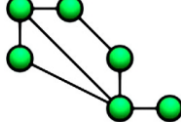
<p><b>Bus.</b> Todos los nodos están conectados a un cable común o compartido.</p>	
<p><b>Estrella.</b> Cada nodo se conecta directamente a un concentrador central. En una topología de estrella todos los datos pasan a través del concentrador antes de alcanzar su destino. Esta es una topología común tanto en redes Ethernet como inalámbricas.</p>	
<p><b>Árbol.</b> Una combinación de las topologías de bus y estrella. Es un conjunto de nodos configurados como estrella que se conectan a una dorsal (backbone).</p>	
<p><b>Anillo.</b> Todos los nodos se conectan entre sí formando un lazo cerrado, de manera que cada nodo se conecta directamente a otros dispositivos. Típicamente la infraestructura es una dorsal (backbone) con fibra óptica.</p>	
<p><b>Malla completa.</b> Existe enlace directo entre todos los pares de nodos de la red. Una malla completa con n nodos requiere de <math>\frac{n(n-1)}{2}</math> enlaces directos. Debido a esta característica, es una tecnología costosa pero muy confiable. Se usa principalmente para aplicaciones militares.</p>	
<p><b>Malla parcial.</b> Algunos nodos están organizados en una malla completa, mientras otros se conectan solamente a uno o dos nodos de la red. Esta topología es menos costosa que la malla completa pero por supuesto, no es tan confiable ya que el número de enlaces redundantes se reduce.</p>	

Tabla 1.1 Topologías.

El otro tipo de LAN se construye con líneas punto a punto. Las líneas individuales conectan una computadora específica a otra. Una LAN así es realmente una red de área amplia en miniatura.



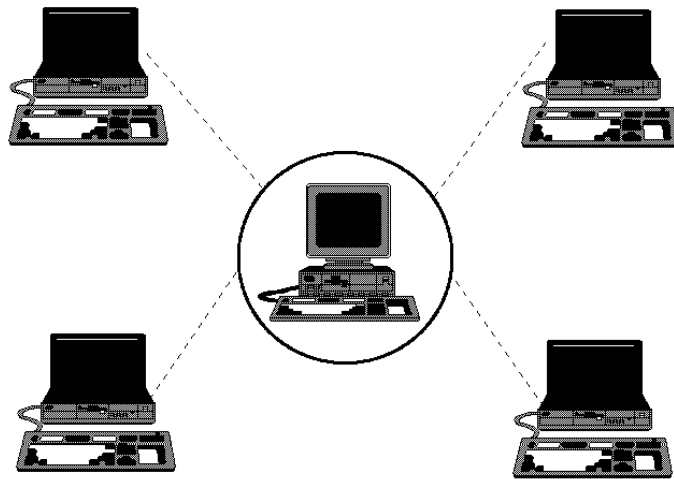


Fig. 1.3 red de área amplia en miniatura.

### 1.2.2 Redes de área metropolitana

Una red de área metropolitana, o MAN (Metropolitan area network) es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. Podría abarcar un grupo de oficinas corporativas cercanas o una ciudad y podría ser privada o pública. Una MAN puede manejar datos y voz, e incluso podría estar relacionada con la red de televisión por cable local. Una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Al no tener que conmutar, se simplifica el diseño.



Fig. 1.4 Red de área metropolitana.

La principal razón para distinguir las MAN como una categoría especial es que se ha adoptado un estándar para ellas, y este estándar ya se está implementando: se llama DQDB (Distributed Queue Dual Bus, o bus dual de cola distribuida), o para la gente que prefiere números a letras, se define como la norma IEEE 802.6. El DQDB consiste en dos buses (cables) unidireccionales, a los cuales están conectadas todas las computadoras. Cada bus tiene una cabeza terminal (head-end), un dispositivo que inicia la actividad de transmisión. El tráfico

destinado a una computadora situada a la derecha del emisor usa el bus superior. El tráfico hacia la izquierda usa el de abajo.

Un aspecto clave de las MAN es que hay un medio de difusión (dos cables, en el caso de la 802.6) al cual se conectan todas las computadoras. Esto simplifica mucho el diseño comparado con otros tipos de redes.

### 1.2.3 Redes de área amplia

Una red de área amplia, o WAN (Wide Area Network), se extiende sobre un área geográfica extensa, a veces un país o un continente; contiene una colección de computadoras dedicadas a ejecutar programas de usuario (es decir, de aplicación). Seguiremos el uso tradicional y llamaremos a estas computadoras "hosts". El término sistema terminal (End system) se utiliza también ocasionalmente en la literatura. Las hosts están conectadas por una subred de comunicación, o simplemente subred (En redes de computadoras, una subred es un rango de direcciones lógicas. Cuando una red de computadoras se vuelve muy grande, conviene dividirla en subredes). El trabajo de la subred es conducir mensajes de una host a otra, así como el sistema telefónico conduce palabras del que habla al que escucha. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (las hosts), simplifica enormemente el diseño total de la red.

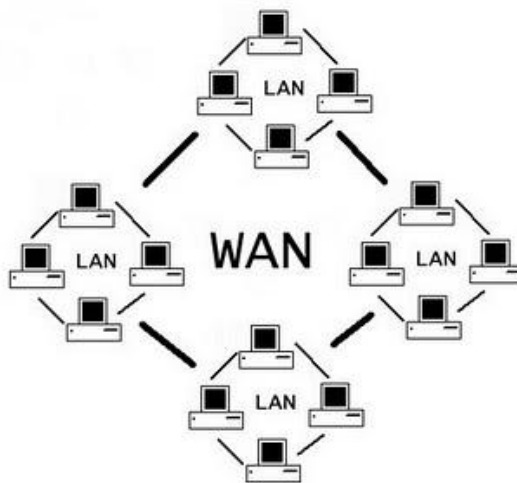


Fig. 1.5 Red de área amplia, o WAN (Wide Area Network).

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos, canales o troncales) mueven bits de una computadora a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para reenviarlos. Desafortunadamente, no hay una terminología estándar para designar estas computadoras; se les denomina nodos conmutadores de paquetes, sistemas intermedios y centrales de conmutación de datos, entre otras cosas. Como término genérico para las computadoras de conmutación, usaremos la palabra router, pero conviene que el lector quede advertido de que no hay consenso sobre la terminología. En este modelo, cada host generalmente está conectada a una LAN en la cual está presente un router,

aunque en algunos casos una host puede estar conectada directamente a un router. La colección de líneas de comunicación y routers (pero no las hosts) forman la subred.

En casi todas las WAN, la red contiene numerosos cables o líneas telefónicas (fig.1.6), cada una conectada a un par de routers. Si dos routers que no comparten un cable desean comunicarse, deberán hacerlo indirectamente, por medio de otros routers. Cuando se envía un paquete de un router a otro a través de uno o más routers intermedios, el paquete se recibe completo en cada router intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía. Una subred basada en este principio se llama, de punto a punto, de almacenar y reenviar, o de paquete conmutado. Casi todas las redes de área amplia (excepto aquellas que usan satélites) tienen subredes de almacenar y reenviar. Cuando los paquetes son pequeños y el tamaño de todos es el mismo, suelen llamarse celdas.

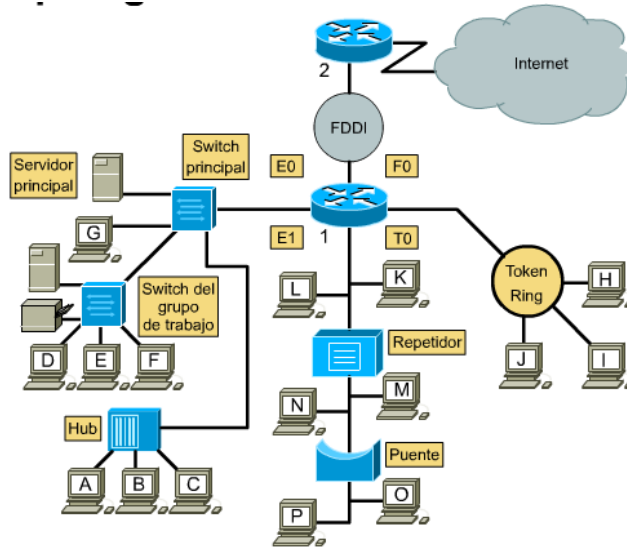


Fig. 1.6 Configuración de una red WAN

Cuando se usa una subred punto a punto, una consideración de diseño importante es la topología de interconexión del router. Las redes locales que fueron diseñadas como tales usualmente tienen una topología simétrica. En contraste, las redes de área amplia típicamente tienen topologías irregulares.

Una segunda posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada router tiene una antena por medio de la cual puede enviar y recibir paquetes de datos. Todos los routers pueden captar las salidas enviadas desde el satélite y en algunos casos pueden también captar la transmisión ascendente de los otros routers hacia el satélite. Algunas veces los routers están conectados a una subred punto a punto de gran tamaño, y únicamente algunos de ellos tienen una antena de satélite. Por su naturaleza, las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es importante.

### 1.3 Software de red

#### 1.3.1. Modelo OSI

La Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) elaborando así el modelo de referencia OSI en 1984.

Para enfrentar el problema de incompatibilidad de las redes y su imposibilidad de comunicarse entre sí, la *Organización Internacional para la Normalización (ISO)* estudió esquemas de red como DECNET, SNA y TCP/IP a fin de encontrar un conjunto de reglas. Como resultado de esta investigación, la ISO desarrolló un modelo de red que ayudaría a los fabricantes a crear redes que fueran compatibles y que pudieran operar con otras redes.

El proceso de dividir comunicaciones complejas en tareas más pequeñas y separadas se podría comparar con el proceso de ensamble de un automóvil. Visto globalmente, el diseño, la fabricación y el ensamblaje de un automóvil es un proceso de gran complejidad. Es poco probable que una sola persona sepa cómo realizar todas las tareas requeridas para la manufactura de un automóvil desde cero. Es por ello que los ingenieros mecánicos diseñan el automóvil, los ingenieros de fabricación diseñan los moldes para fabricar las partes y los técnicos especializados ensamblan cada uno una parte del auto.

El *modelo de referencia OSI* (No debe confundirse con ISO.), Adoptado en 1984, fue el esquema descriptivo que crearon. Este modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.



Fig. 1.7 Las siete capas del Modelo OSI

El modelo de referencia OSI es la aplicación principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia (OSI), especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.

- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje

La información que viaja a través de una red se conoce como *paquete*, *datos* o *paquete de datos*. Un paquete de datos es una unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación. Incluye la información de origen junto con otros elementos necesarios para hacer que la comunicación sea factible y confiable en relación con los dispositivos de destino. La dirección origen de un paquete especifica la identidad del computador que envía el paquete. La dirección destino especifica la identidad del computador que finalmente recibe el paquete.

En Networking, es el medio a través del cual viajan los paquetes de datos. Puede ser cualquiera de los siguientes materiales:

- Cables telefónicos
- UTP (*Unshielded Twisted Pair, par trenzado no apantallado*) es un tipo de cable de par trenzado que no se encuentra apantallado y que se utiliza principalmente para comunicaciones. Se encuentra normalizado de acuerdo a la norma estadounidense TIA/EIA-568-B y a la internacional ISO/IEC 11801. ) de categoría 5 se utiliza para Ethernet 10BASE-T
- Cable coaxial (se utiliza para la TV por cable)
- Fibra óptica (delgadas fibras de vidrio que transportan luz)

Existen otros dos tipos de medios que son menos evidentes, pero que no obstante se deben tener en cuenta en la comunicación por redes. En primer lugar, está la atmósfera (en su mayor parte formada por oxígeno, nitrógeno y agua) que transporta ondas de radio, microondas y luz. )

La comunicación sin ningún tipo de alambres o cables se denomina inalámbrica o comunicación de espacio abierto, usando ondas electromagnéticas (EM); Entre las ondas EM, que en el vacío viajan a velocidad de la luz, se incluyen las ondas de energía, ondas de radio, microondas, luz infrarroja, luz visible, luz ultravioleta, rayos x y rayos gama. Viajan a través de la atmósfera (principalmente compuesta de oxígeno, nitrógeno y agua), pero también viajan a través del vacío del espacio exterior (donde no existe prácticamente materia, ni moléculas ni átomos).

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red entiendan el mismo lenguaje o *protocolo*. Un *protocolo* es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente.

Las siete capas del modelo de referencia *OSI* son:

### **Capa 7: Aplicación**

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la

disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.



Fig. 1.8 Capa de Aplicación.

### Capa 6: Presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.



Fig. 1.9 Capa de Presentación.

### Capa 5: Sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.



Fig. 1.10 Capa de Sesión

### Capa 4: Transporte

La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.



Fig. 1.11 Capa de Transporte.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

**Capa 3: Red**

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Se encarga más que nada de selección de ruta, direccionamiento y enrutamiento.



Fig. 1.12 Capa de Red.

**Capa 2: Enlace de datos**

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Se basa en tramas y control de acceso al medio.



Fig. 1.13 Enlace de Datos



## Capa 1: La capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física.



Fig. 1.14 Capa Física.

Las capas del modelo OSI pueden ser divididas en dos categorías: capas superiores y capas inferiores. Las capas superiores se implementan únicamente para las aplicaciones en software y son las que se encuentran más cerca del usuario, por lo que respecta de las capas inferiores es que la capa física y la de enlace, se aplican principalmente en hardware y software, las demás capas se implementan únicamente en software, la capa más baja, la capa física, se enfoca principalmente en el medio de transmisión, como el cable por ejemplo, y es responsable de colocar la información en el medio.

### 1.3.2. Interacción entre las capas e Intercambio de información

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicaciones de par-a-par. Durante este proceso, cada protocolo de capa intercambia información, que se conoce como unidades de datos de protocolo (PDU), entre capas iguales. Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función. Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final

adicionales. Después de que las Capas 7, 6 y 5 han agregado la información, la Capa 4 agrega más información. Este agrupamiento de datos, la PDU de Capa 4, se denomina segmento.

Por ejemplo, la capa de red presta un servicio a la capa de transporte y la capa de transporte presenta datos al subsistema de Internetwork. La tarea de la capa de red consiste en trasladar esos datos a través de la Internetwork. Ejecuta esta tarea encapsulando los datos y agregando un encabezado, con lo que crea un paquete (PDU de Capa 3). Este encabezado contiene la información necesaria para completar la transferencia, como por ejemplo, las direcciones lógicas origen y destino.

La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red en una trama (la PDU de Capa 2); el encabezado de la trama contiene información (por Ej., direcciones físicas) que es necesaria para completar las funciones de enlace de datos. La capa de enlace de datos suministra un servicio a la capa de red encapsulando la información de la capa de red en una trama.

La capa física también suministra un servicio a la capa de enlace de datos. La capa física codifica los datos de la trama de enlace de datos en un patrón de unos y ceros (bits) para su transmisión a través del medio (generalmente un cable) en la Capa 1 Fig. 1.15.

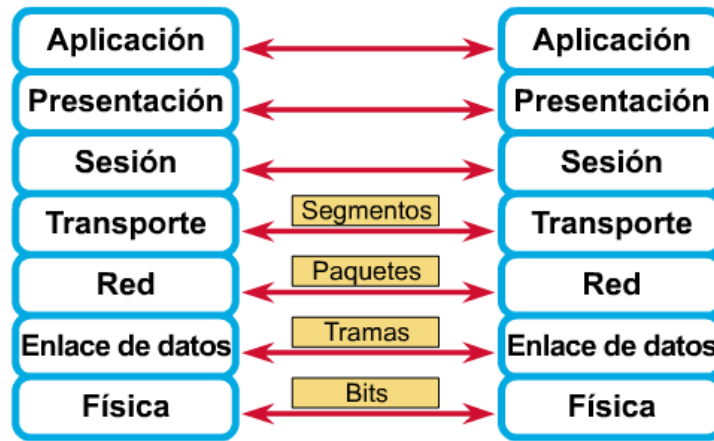


Fig. 1.15 Comunicación par a par.

### 1.3.3 El modelo de referencia TCP/IP

Pasemos ahora del modelo de referencia OSI al modelo que se usaba en las redes de computadoras, la ARPANET, y su sucesora, la Internet mundial. Aunque más adelante presentaremos una breve historia de la ARPANET, es de utilidad mencionar ahora algunos de sus aspectos.



Fig. 1.16 Modelos de Referencia TCP/IP

La ARPANET era una red de investigación patrocinada por el DoD (Departamento de Defensa de Estados Unidos de América). Al final conectó a cientos de universidades e instalaciones del gobierno usando líneas telefónicas rentadas. Cuando más tarde se añadieron redes de satélite y radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitó una arquitectura de referencia nueva. Así, la capacidad de conectar entre sí múltiples redes de manera útil fue uno de los principales objetivos de diseño desde el principio. Esta arquitectura se popularizó después como el modelo de referencia TCP/IP<sup>1</sup>, por las iniciales de sus dos protocolos primarios.

Debido a la preocupación del DoD por que alguno de sus costosos nodos, enrutadores o pasarelas de interredes pudiera ser objeto de un atentado en cualquier momento, otro de los objetivos principales fue que la red fuera capaz de sobrevivir a la pérdida del *hardware* de subred sin que las conversaciones existentes se interrumpieran. En otras palabras, el DoD quería que las conexiones permanecieran intactas mientras las computadoras de origen y destino estuvieran funcionando, aun si alguna de las computadoras o de las líneas de transmisión en el trayecto dejara de funcionar en forma repentina. Es más, se necesitaba una arquitectura flexible, pues se tenía la visión de aplicaciones con requerimientos divergentes, abarcando desde la transferencia de archivos hasta la transmisión de discursos en tiempo real.

### 1.3.3.1. La capa de interred

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred carente de conexiones. Esta capa, llamada capa de interred, es el eje que mantiene unida toda la arquitectura. La misión de esta capa es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino (que podría estar en una red diferente). Los paquetes pueden llegar incluso en un orden diferente a aquel en que se enviaron, en cuyo caso corresponde a las capas superiores recomodarlos, si se desea la entrega ordenada. Nótese que aquí se usa "interred" en un sentido genérico, aunque esta capa esté presente en la Internet.

Aquí la analogía es con el sistema de correos (lento). Una persona puede depositar una secuencia de cartas internacionales en un buzón en un país, y con un poco de suerte, casi todas se entregarán en la dirección correcta en el país de destino. Es probable que las cartas viajen a

---

<sup>1</sup> Es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina *conjunto de protocolos TCP/IP*, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa de dicho departamento.

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI (*Open System Interconnection*), que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables. **D. Weitzmann (April de 1990).** «[<http://www.isi.edu/in-notes/rfc1149.txt> A Standard for the Transmission of IP Datagrams on Avian Carriers]». **Internet Engineering Task Force. Consultado el 20-11-2007.**

través de una o más pasarelas internacionales de correo en el camino, pero esto es transparente para los usuarios. Más aún, los usuarios no necesitan saber que cada país (esto es, cada red), tiene sus propias estampillas, tamaños preferidos de sobres y reglas de entrega.

La capa de interred define un formato de paquete y protocolo oficial llamado IP (*Internet protocol*, protocolo de interred). El trabajo de la capa de interred es entregar paquetes IP a donde se supone que deben ir. Aquí la consideración más importante es claramente el ruteo de los paquetes, y también evitar la congestión. Por lo anterior es razonable decir que la capa de interred TCP/IP es muy parecida en funcionalidad a la capa de red OSI

### 1.3.3.2 La capa de transporte

La capa que está sobre la capa de interredes en el modelo TCP/IP se llama usualmente ahora capa de transporte. Esta capa se diseñó para permitir que las entidades pares en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definieron dos protocolos de extremo a extremo. El primero, TCP (*transmission control protocol*: protocolo de control de la transmisión) es un protocolo confiable orientado a la conexión que permite que una corriente de bytes originada en una computadora se entregue sin errores en cualquier otra computadora de la interred. Este protocolo fragmenta el flujo entrante de bytes en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar la corriente de salida. El TCP también se encarga del control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo de esta capa, el **UDP** (*user datagram protocol*: protocolo de datagrama de usuario), es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo también se usa ampliamente para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor, y en aplicaciones en las que la entrega pronta es más importante que la entrega precisa, como las transmisiones de voz o vídeo.

### 1.3.3.3 La capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se pensó que fueran necesarias, así que no se incluyeron. La experiencia con el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayor parte de las aplicaciones.

Encima de la capa de transporte está la capa de aplicación, que contiene todos los protocolos de alto nivel. Entre los protocolos más antiguos están el de terminal virtual (TELNET), el de transferencia de archivos (FTP) y el de correo electrónico (SIP). El protocolo de terminal virtual permite que un usuario en una computadora ingrese en una computadora distante y trabaje ahí. El protocolo de transferencia de archivos ofrece un mecanismo para mover datos de una computadora a otra en forma eficiente. El correo electrónico fue en sus orígenes sólo una clase de transferencia de archivos, pero más adelante se desarrolló para él un protocolo especializado; con los años, se le han añadido muchos otros protocolos, como el servicio de nombres de dominio (DNS) para relacionar los nombres de los nodos con sus direcciones de la red; NNTP, el protocolo que se usa para transferir artículos noticiosos; HTTP, el protocolo que se usa para recuperar páginas en la *World Wide Web* y muchos otros.

### 1.3.3.4 La capa del nodo a la red

Bajo la capa de interred está un gran vacío. El modelo de referencia TCP/IP realmente no dice mucho de lo que aquí sucede, fuera de indicar que el nodo se ha de conectar a la red haciendo uso de algún protocolo de modo que pueda enviar por ella paquetes de IP. Este protocolo no está definido y varía de un nodo a otro y de red a red. Los libros y artículos sobre el modelo TCP/IP rara vez hablan de él.

#### 1.3.3.4.1 Comparación de los modelos de referencia OSI y TCP/IP

Los modelos de referencia OSI y TCP/IP tienen mucho en común. Ambos se basan en el concepto de un gran número de protocolos independientes. También la funcionalidad de las capas es muy similar. Por ejemplo, en ambos modelos las capas por encima de la de transporte, incluida ésta, están ahí para prestar un servicio de transporte de extremo a extremo, independiente de la red, a los procesos que deseen comunicarse. Estas capas forman el proveedor de transporte. También en ambos modelos, las capas encima de la de transporte son usuarios del servicio de transporte orientados a aplicaciones.

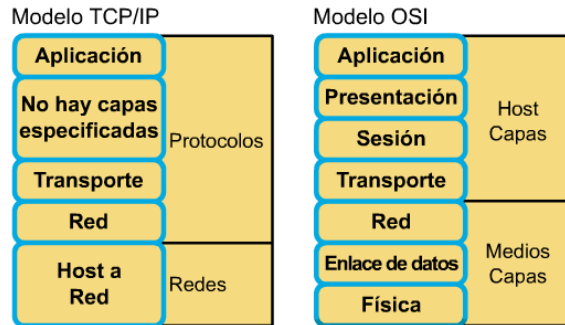


Fig. 1.17 Comparación entre OSI y TCP/IP

A pesar de estas similitudes fundamentales, los dos modelos tienen también muchas diferencias. Es importante notar que aquí estamos comparando los *modelos de referencia*, no las *pilas de protocolos* correspondientes. En el modelo OSI, tres conceptos son fundamentales:

1. Servicios.
2. Interfaces.
3. Protocolos.

Es probable que la contribución más importante del modelo OSI sea hacer explícita la distinción entre estos tres conceptos. Cada capa presta algunos servicios a la capa que se encuentra sobre ella. La definición de *servicio* dice lo que la capa hace, no cómo es que las entidades superiores tienen acceso a ella o cómo funciona la capa.

La *interfaz* de una capa les dice a los procesos de arriba cómo acceder a ella; especifica cuáles son los parámetros y qué resultados esperar; nada dice tampoco sobre cómo trabaja la capa por dentro.

Finalmente, los *protocolos* pares que se usan en una capa son asunto de la capa. Ésta puede usar los protocolos que quiera, siempre que consiga que se realice el trabajo (esto es, que provea los servicios que ofrece). La capa también puede cambiar los protocolos a voluntad sin afectar el *software* de las capas superiores.

Estas ideas ajustan muy bien con las ideas modernas acerca de la programación orientada a objetos. Al igual que una capa, un objeto tiene un conjunto de métodos (operaciones) que los

procesos pueden invocar desde fuera del objeto. La semántica de estos métodos define el conjunto de servicios que ofrece el objeto. Los parámetros y resultados de los métodos forman la interfaz del objeto. El código interno del objeto es su protocolo y no está visible ni es de la incumbencia de las entidades externas al objeto.

El modelo TCP/IP originalmente no distinguía en forma clara entre servicio, interfaz y protocolo, aunque se ha tratado de reajustarlo después a fin de hacerlo más parecido a OSI. Por ejemplo, los únicos servicios reales que ofrece la capa de Interred son SENT IP PACKET Y RECIVE IP PACKET para enviar y recibir paquetes de IP, respectivamente.

Como consecuencia, en el modelo OSI se ocultan mejor los protocolos que en el modelo TCP/IP y se pueden reemplazar con relativa facilidad al cambiar la tecnología. La capacidad de efectuar tales cambios es uno de los principales propósitos de tener protocolos por capas en primer lugar.

El modelo de referencia OSI, se desarrolló antes de que se inventaran los protocolos. Este orden significa que el modelo no se orientó hacia un conjunto específico de protocolos, lo cual lo convirtió en algo muy general. El lado malo de este orden es que los diseñadores no tenían mucha experiencia con el asunto y no supieron bien cuál funcionalidad poner en cuál capa.

Por ejemplo, la capa de enlace de datos originalmente tenía que ver sólo con redes de punto a punto. Cuando llegaron las redes de difusión, se tuvo que insertar una nueva subcapa en el modelo. Cuando la gente empezó a construir redes reales haciendo uso del modelo OSI y de los protocolos existentes, descubrió que no coincidían con las especificaciones de servicio requeridas, de modo que se tuvieron que injertar en el modelo subcapas de convergencia que permitieran "tapar" las diferencias. Por último, el comité (Organización Internacional para la Estandarización o ISO) esperaba originalmente que cada país tuviera una red controlada por el gobierno que usara los protocolos OSI, de manera que no se pensó en la interconexión de redes.

Lo contrario sucedió con TCP/IP: primero llegaron los protocolos, y el modelo fue en realidad sólo una descripción de los protocolos existentes. No hubo el problema de ajustar los protocolos al modelo; se ajustaban a la perfección. El único problema fue que el *modelo* no se ajustaba a ninguna otra pila de protocolos; en consecuencia, no fue de mucha utilidad para describir otras redes que no fueran del tipo TCP/IP.

Una diferencia obvia entre los dos modelos es la cantidad de capas: el modelo OSI tiene siete capas y el TCP/IP cuatro. Ambos tienen capas de (inter)red, de transporte y de aplicación, pero las otras capas son diferentes.

Otra diferencia se tiene en el área de la comunicación sin conexión frente a la orientada a la conexión. El modelo OSI apoya la comunicación tanto sin conexión como la orientada a la conexión en la capa de red, pero en la capa de transporte donde es más importante (porque el servicio de transporte es visible a los usuarios) lo hace únicamente con la comunicación orientada a la conexión. El modelo TCP/IP sólo tiene un modo en la capa de red (sin conexión) pero apoya ambos modos en la capa de transporte, con lo que ofrece una alternativa a los usuarios. Esta elección es importante sobre todo para los protocolos simples de petición y respuesta.

## 1.4. Puentes & Switches

Los puentes y los switches son dispositivos de comunicación de datos que operan principalmente en la capa dos del modelo OSI, son ampliamente conocidos como dispositivos de la capa de enlace. Los puentes se encontraron disponible por primera vez en los años 80's, al inicio los puentes conectaban y enviaban paquetes a través de dos redes homogéneas, actualmente los puentes entre diferentes redes se han definido y estandarizado. Hoy en día surge una nueva tecnología switches basado principalmente en soluciones de Internetworking, con mayor flexibilidad a menor costo por puerto.

### 1.4.1. Dispositivos de la capa de enlace

Los puentes y switches funcionan en la capa de enlace, los cuales controlan el flujo de información, provee direccionamientos físicos y administran los accesos al medio físico. Los puentes proveen estas funciones por medio de los protocolos de enlace que especifican algoritmos de flujo de información, de direccionamiento y de acceso al medio ejemplos de protocolos populares incluye que Ethernet, FDDI, y Token Ring.



Fig. 1.18 Switch de 8 puertos

La transparencia de los protocolos de las capas superiores es una ventaja principal tanto de los puentes como de los switches. Porque ambos dispositivos funcionan en la capa de enlace, no necesitan examinar la información de las capas superiores. Esto quiere decir que estos dispositivos pueden enviar rápidamente el tráfico representado por un protocolo de red.

**Puente:** Es dispositivo de capa 2, diseñado para conectar dos segmentos LAN. El propósito de un puente es filtrar el tráfico de una LAN, para que el tráfico local siga siendo local, pero permitiendo la conectividad a otras partes (segmentos) de la LAN para enviar el tráfico dirigido a esas otras partes. La forma en que se verifica la dirección local. Cada dispositivo de networking tiene una dirección MAC exclusiva en la NIC. el puente rastrea cuáles son las direcciones MAC que están ubicadas a cada lado del puente y toma sus decisiones basándose en esta lista de direcciones MAC.

Los puentes no son dispositivos complejos. Analizan las tramas entrantes, toman decisiones de envío basándose en la información que contienen las tramas y envían las tramas a su destino. Los puentes sólo se ocupan de pasar los paquetes, o de no pasarlos, basándose en las direcciones de MAC. Los puentes a menudo pasan paquetes entre redes que operan bajo distintos protocolos de capa 2.

### 1.4.2. Los switches

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían y saturan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto de switch como un micropuerto; este proceso se denomina *microsegmentación*. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host.

Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 de dirección MAC destino.

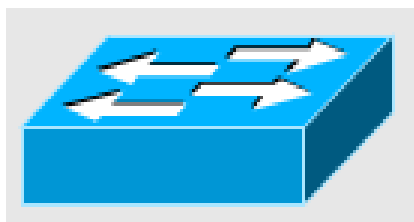


Fig. 1.19 Switch.

Los switches pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

La conmutación Ethernet aumenta el ancho de banda disponible en una red. Esto se hace creando segmentos de red dedicada, o conexiones punto a punto, y conectando estos segmentos en una red virtual dentro del switch. Este circuito de red virtual existe sólo cuando se deben comunicar dos nodos. Esto se denomina *circuito virtual* ya que existe sólo cuando es necesario y se establece dentro del switch.

Aunque el switch de LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch se encuentran todavía en el mismo dominio de broadcast, por lo tanto, un broadcast desde un nodo será visto por todos los demás nodos conectados a través del switch de LAN.

### 1.5. Los ruteadores

Los routers están diseñados para interconectar múltiples redes. Esta interconexión permite que las computadoras de diferentes redes se comuniquen entre sí. Las redes interconectadas pueden estar colocadas o dispersas geográficamente.



Fig. 1.20 Ruteador.



Las redes WAN están formadas por muchas tecnologías distintas, incluyendo los routers, los servicios de transmisión y los controladores de línea. Lo que hace indispensable al router es su capacidad para interconectar redes en una WAN.

Un router es un dispositivo de red inteligente que funciona predominantemente en las tres primeras capas del modelo de referencia OSI. Los routers, al igual que los hosts, son en realidad capaces de actuar en las siete capas del modelo de referencia OSI. Dependiendo de su configuración particular, puede utilizar o no las siete capas de funcionalidad. Sin embargo, las necesidades de las tres primeras capas es virtualmente universal. La comunicación a través de las dos primeras capas permite que los routers se comuniquen directamente con las LAN (construcción de la capa de enlace de datos). Más importante aún es que los routers pueden identificar rutas a través de redes basándose en las direcciones de la capa 3. Esto permite que los routers interconecten múltiples redes utilizando el direccionamiento de la capa de red, sin tener en cuenta lo cerca o lejos que puedan estar unos de otros.

Entender los routers y el enrutamiento necesita examinar un router desde dos perspectivas distintas: la física y la lógica. Desde una perspectiva física, los routers contienen miríadas de partes, cada una de las cuales tiene una función específica. Desde una perspectiva lógica, los routers realizan muchas funciones, incluyendo encontrar otros routers en la red, conocer las redes de destino potenciales y los hosts, descubrir y seguir rutas potenciales y enviar datagramas hacia un destino especificado. Juntos, estos componentes físicos y funciones lógicas le permiten construir y utilizar internetworks, incluidas las WAN.

### 1.5.1. Componentes físicos

Un router es un dispositivo extraordinariamente complejo. Su complejidad yace en su computadora de enrutamiento (la lógica que permite que el dispositivo físico realice varias funciones de enrutamiento). La complejidad de la lógica de enrutamiento está oculta por la relativa simplicidad de la forma física del router. El tipo más común de routers actualmente un tipo de computadora altamente especializada; contiene los mismos componentes básicos que otras computadoras. Entre estos componentes se incluyen los siguientes:

- Una unidad central de procesamiento (CPU).
- Memoria de acceso aleatorio (RAM)
- Un sistema básico de entrada / salida (810S).
- Un sistema operativo (OS).
- Una placa madre.
- Puertos físicos de entrada / salida (E/S),
- Una fuente de energía, un chasis y una "cubierta metálica".

La gran mayoría de los componentes de un router permanecen siempre ocultos a los ojos de los administradores de redes por la cubierta metálica del chasis. Estos componentes son extremadamente fiables y, en condiciones normales de funcionamiento, no deberían ver la luz del día. Las excepciones obvias a esta visión general se están expandiendo.



Fig. 1.21 Parte posterior de un Router

En el momento en que necesite añadir más recursos al router, tendrá que quitar esta cubierta. Normalmente, dichos recursos incluyen memoria o puertos de E/S.

Los componentes con los que más frecuentemente se encontrará un administrador de redes son:

El sistema operativo y los puertos de E/S. El sistema operativo de un router es el software que controla los distintos componentes hardware y los hace utilizables. La mayoría de los administradores de redes utilizan una interfaz de línea de comandos para desarrollar una configuración lógica. La configuración es un perfil del sistema: los números, las posiciones, los tipos de cada puerto E/S, y detalles tales como la información de direccionamiento y de ancho de banda. La configuración de un router también puede incluir información de seguridad como a qué usuarios les está permitido acceder a puertos de E/S específicos y modos de configuración.

Los puertos de E/S son el único componente físico del router que los administradores de redes ven en su rutina. Los puertos confirman la capacidad única del router para interconectar aparentemente combinaciones infinitas de tecnologías de transmisión LAN y WAN. Cada una de éstas, LAN o WAN, debe tener su propio puerto de E/S en el router. Estos puertos funcionan como una tarjeta de interfaz de red (NIC) en una computadora conectada a una LAN; están relacionados con el medio y los mecanismos de entramado esperados y proporcionan las interfaces físicas apropiadas. Muchas de estas interfaces físicas se parecen bastante entre sí. Este parecido físico contradice las diferencias entre las funciones de capa superior de estas tecnologías. Por tanto, es más útil examinar las tecnologías de transmisión que examinar las interfaces físicas específicas.

### 1.5.2. Funciones de un router

Igual de importantes que proporcionar interconectividad física para múltiples redes son las funciones lógicas que realiza un router. Estas funciones hacen que las interconexiones físicas se puedan utilizar. Por ejemplo, las comunicaciones entre redes necesitan que al menos una ruta física interconecte las computadoras de origen y destino. Sin embargo, tener y utilizar una ruta física son dos cosas muy diferentes. Específicamente, las computadoras de origen y destino deben hablar un lenguaje común (un protocolo enrutado). También ayuda el hecho de si los routers que están entre ellas también hablan un lenguaje común (un protocolo de enrutamiento) y coinciden en cuál es la mejor ruta física. Además, algunas de las funciones más sobresalientes que puede proporcionar un router son éstas:

- Interconectividad física.
- Interconectividad lógica.
- Cálculo y mantenimiento de una ruta.
- Seguridad.

#### 1.5.2.1. Interconectividad física

Un router tiene un mínimo de dos (y frecuentemente muchos más) puertos de E/S físicos. Los puertos de E/S, o interfaces, como son más conocidos, se utilizan para conectar físicamente servicios de transmisión de red a un router. Cada puerto se conecta a una placa de circuitos que está conectada a la placa madre del router. Por tanto, la placa madre en realidad proporciona interconectividad entre múltiples redes.

El administrador de la red debe configurar cada interfaz mediante la consola del router. La configuración incluye la definición del número de puertos de la interfaz del router, la tecnología de transmisión específica y el ancho de banda disponible en la red conectada a esa interfaz, y los tipos de protocolos que se utilizarán a través de esa interfaz. Los parámetros que se deben definir

varían según el tipo de interfaz de red.

### 1.5.2.2. Interconectividad lógica

Una interfaz de routers se puede activar tan pronto como sea configurada. La configuración de la interfaz identifica el tipo de servicio de transmisión al que está conectada, la dirección IP de la interfaz y la dirección de la red a la que está conectada. A partir de la activación de un puerto, el router comienza a controlar inmediatamente todos los paquetes que se están transmitiendo por la red conectada al nuevo puerto activado. Esto le permite "conocer" las direcciones IP de las redes y los hosts que residen en las redes que se pueden alcanzar mediante ese puerto. Estas direcciones están almacenadas en tablas de enrutamiento. Las tablas de enrutamiento correlacionan el número de puerto de cada interfaz del router con las direcciones de capa de red que se pueden alcanzar (directa o indirectamente) mediante ese puerto.

También se puede configurar un router con una ruta predeterminada. Una ruta predeterminada asocia una interfaz de router específica con una dirección de destino desconocida. Esto permite que un router envíe un datagrama a destinos que todavía no conoce. Las rutas predeterminadas también se pueden utilizar de otras formas. Por ejemplo, se pueden utilizar para minimizar el crecimiento de las tablas de enrutamiento, o para reducir la cantidad de tráfico generado entre routers mientras éstos intercambian información de enrutamiento.

### 1.5.2.3. Cálculo y mantenimiento de una ruta

Los routers se comunican entre sí utilizando un protocolo predeterminado, un protocolo de enrutamiento. Los protocolos de enrutamiento permiten que los routers hagan lo siguiente:

- Identificar rutas potenciales a redes de destino específicas.
- Realizar un cálculo matemático, basado en el algoritmo del protocolo de enrutamiento, para determinar la ruta óptima a cada destino.
- Controlar continuamente la red para detectar cualquier cambio en la topología que pueda representar rutas conocidas no válidas.

Existen muchos tipos distintos de protocolos de enrutamiento. Algunos, como el Protocolo de información de enrutamiento (RIP), son bastante sencillos.

Otros, como el Protocolo Primero la ruta libre más corta (OSPF), son extremadamente potentes y ricos en elementos, pero complicados. En general, los protocolos de enrutamiento pueden optar por dos planteamientos para tomar decisiones de enrutamiento: vectores de distancia y estados de enlace. Un protocolo de enrutamiento por vector de distancia toma decisiones basándose en algunas medidas de la distancia entre las computadoras de origen y destino.

Un protocolo de estado de enlace basa sus decisiones en varios estados de los enlaces, o servicios de transmisión, que interconectan las computadoras de origen y destino. Ninguna es correcta o errónea: sólo son formas distintas de tomar decisiones. Sin embargo, ofrecen diferentes niveles de rendimiento, incluyendo los tiempos de convergencia.

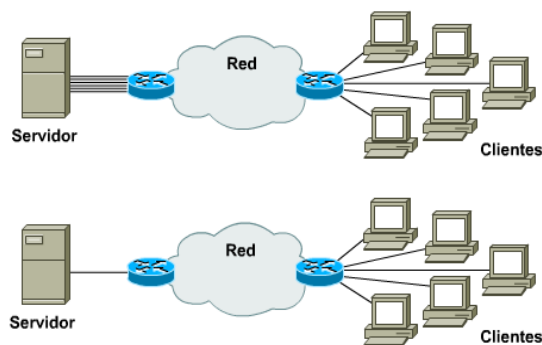


Fig. 1.22 Rutas en Internet.

Puede evaluar los protocolos de enrutamiento empleando varios criterios más específicos que sólo los planteamientos que utilizan. Algunos de los criterios con más sentido son los siguientes:

- *Punto óptimo.* Describe la capacidad de un protocolo de enrutamiento para seleccionar la mejor ruta disponible. Por desgracia, la palabra "mejor" es ambigua. Existen distintas formas de evaluar rutas diferentes para un destino dado. Cada forma podría dar como resultado la selección de una ruta "mejor" diferente dependiendo de los criterios empleados. Los criterios que utilizan los protocolos de enrutamiento para calcular y evaluar las rutas se llaman métricas de enrutamiento. Se utiliza una amplia variedad de métricas, y varían ampliamente según el protocolo de enrutamiento. Una métrica sencilla es el número de saltos, es decir el número de saltos, o routers, que hay entre las computadoras de origen y destino.
- *Eficiencia.* Otro criterio a considerar cuando se evalúan protocolos de enrutamiento es su eficiencia operacional. La eficiencia operacional se puede medir examinando los recursos físicos, incluyendo la RAM del router y el tiempo de CPU; y, el ancho de banda de la red necesario para un cierto protocolo de enrutamiento. Puede que necesite consultar al fabricante o vendedor del router para determinar las eficiencias relativas de los protocolos que va a considerar.
- *Resistencia.* Un protocolo de enrutamiento debería actuar de forma fiable en todo momento, no sólo cuando la red sea estable. Las condiciones de error, incluidos los fallos del hardware o de los servicios de transmisión, errores de configuración del router y cargas fuertes de tráfico, afectan adversamente a la red. Por tanto, es primordial que un protocolo de enrutamiento funcione correctamente durante los periodos de fallos o inestabilidad de la red.
- *Convergencia.* Debido a que son dispositivos inteligentes, los routers pueden detectar automáticamente cambios en la internetwork. Cuando se detecta un cambio, todos los routers implicados deben converger en un nuevo acuerdo sobre la topología de la red y volver a calcular las rutas a los destinos conocidos de acuerdo a este cambio. Este proceso de alcanzar un acuerdo mutuo se llama convergencia. Cada protocolo de enrutamiento emplea mecanismos distintos para detectar y comunicar cambios en la red. Por tanto, cada uno converge a una velocidad diferente. En general cuanto más lentamente converge un protocolo de enrutamiento, mayor es la posibilidad de que se interrumpa el servicio a través de la internetwork.
- *Escalabilidad.* La escalabilidad de una red es su capacidad para crecer. Aunque el crecimiento no sea un requisito en las organizaciones, el protocolo de enrutamiento que seleccione debería poder escalarse para cumplir el crecimiento proyectado para la red.

## 1.6 Componentes de redes inalámbricas

### 1.6.1 Punto de acceso

Un punto de acceso es un "concentrador" inalámbrico. El transmisor/receptor conecta entre sí los nodos de la red inalámbrica y normalmente también sirve de puente entre ellos y la red cableada. Un conjunto de puntos de acceso (coordinados) se pueden conectar unos con otros para crear una gran red inalámbrica.



Fig. 1.23 Punto de Acceso.

Desde el punto de vista de los clientes inalámbricos (como las computadoras portátiles o las estaciones móviles), un punto de acceso provee un cable virtual entre los clientes asociados. Este “cable inalámbrico” conecta tanto a los clientes entre sí, como los clientes con la red cableada.

Un punto de acceso debe distinguirse de un enrutador inalámbrico, que es muy común en el mercado actual. Un enrutador inalámbrico es una combinación entre un punto de acceso y un enrutador, y puede ejecutar tareas más complejas que las de un punto de acceso. Considere un enrutador inalámbrico como un puente inalámbrico (entre la red inalámbrica y la red Ethernet) y un enrutador (con características de enrutamiento IP).

Los clientes se conectan a un punto de acceso mediante su nombre. Este mecanismo de identificación se conoce como SSID-Service Set Identifier- (Identificador del Conjunto de Servicio) y debe ser el mismo para todos los miembros de una red inalámbrica específica. Todos los punto de acceso y clientes que pertenecen a un mismo ESS -Extended Service Set- (Conjunto de Servicio extendido) se deben configurar con el mismo ID (ESSID). Cuando hablamos de SSID pensamos en la etiqueta de un punto (socket) de Ethernet.

Conectarse a una red inalámbrica con SSID “x” es equivalente a conectar su computador a un punto de red sobre una pared identificado con la etiqueta “x”.

### 1.6.2 Antenas para WiFi

Hay que recordar que para la transmisión inalámbrica se deben tener en cuenta las características de la antena que se conectara al Acces Point (Punto de Acceso). Que da acceso a internet o a la intranet, para ampliar la distancia de cobertura.

Cuando hablamos de **WiFi** nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día. WiFi, también llamada WLAN (*wireless LAN*, red inalámbrica) o estándar IEEE 802.11. WiFi no es una abreviatura de *Wireless Fidelity*, simplemente es un nombre comercial. En la actualidad podemos encontrar con dos tipos de comunicación WiFi:

- 802.11b, que emite a 11 Mb/seg, y
- 802.11g, más rápida, a 54 MB/seg.

De hecho, son su velocidad y alcance (unos 100-150 metros en hardware asequible) lo convierten en una fórmula perfecta para el acceso a internet sin cables<sup>2</sup>.



Fig. 1.24 Señales WiFi.

Existen 3 tipos de antenas según como se quiera amplificar esa distancia:

**1.6.2.1 Antenas direccionales:** Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance, actúa de forma parecida a un foco de luz que emite un haz concreto y estrecho pero de forma intensa (más alcance).



Fig. 1.25 Antenas direccional.

El alcance de una antena direccional viene determinado por una combinación de los dBi<sup>3</sup> de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

**1.6.2.2 Antena omnidireccional:** Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena omnidireccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones con menor alcance.

<sup>2</sup> <http://www.aulaclie.es/articulos/wifi.html>

<sup>3</sup> es una unidad para medir la ganancia de una antena en referencia a una antena isótropa teórica. El valor de dBi corresponde a la ganancia de una antena ideal (teórica) que irradia la potencia recibida de un dispositivo al que está conectado, y al cual también transmite las señales recibidas desde el espacio, sin considerar ni pérdidas ni ganancias externas o adicionales de potencias.



Fig. 1.26 Antena omnidireccional.

Las antenas omnidireccionales “envían” la información teóricamente a 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

**1.6.2.3 Antena sectorial:** Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. Para tener una cobertura de 360° (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar: tres antenas sectoriales de 120° o 4 antenas sectoriales de 80°. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.



Fig. 1.27 Antena sectorial.

### 1.6.3 Clientes inalámbricos

Un cliente inalámbrico es cualquier estación inalámbrica que se conecta a una red de área local (LAN–Local Area Network) inalámbrica para compartir sus recursos. Una estación inalámbrica se define como cualquier computador con una tarjeta adaptadora de red inalámbrica instalada que transmite y recibe señales de radio frecuencia (RF). Algunos de los clientes inalámbricos más comunes son las computadoras portátiles, PDAs<sup>4</sup>, equipos de vigilancia y teléfonos inalámbricos de VoIP<sup>5</sup>.

<sup>4</sup> **PDA**, del inglés *personal digital assistant* (*asistente digital personal*), es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura. <http://es.wikipedia.org/wiki/PDA>

<sup>5</sup> **Voz sobre Protocolo de Internet**, también llamado **Voz IP**, **VoIP**, **VoIP** (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de

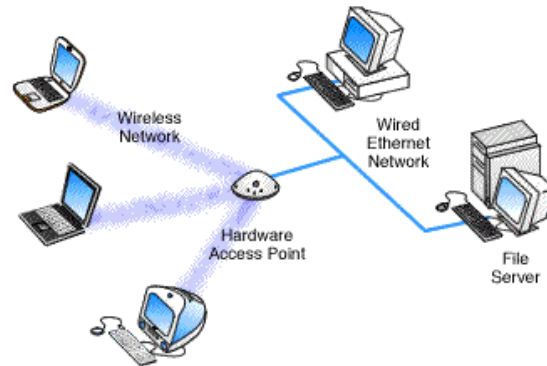


Fig. 1.28 Clientes inalámbricos.

## 1.7 Modos de operación de redes inalámbricas

El conjunto de estándares 802.11 definen dos modos fundamentales para redes inalámbricas:

1. Ad hoc.
2. Infraestructura.

Es importante comprender que no siempre, los modos se ven reflejados directamente en la topología. Por ejemplo, un enlace punto a punto puede ser implementado en modo *ad hoc* o Infraestructura y nos podríamos imaginar una red en estrella construida por conexiones *ad hoc*. El modo puede ser visto como la configuración individual de la tarjeta inalámbrica de un nodo, más que como una característica de toda una infraestructura.

### 1.7.1 Modo ad hoc (IBSS)

El modo *ad hoc*, también conocido como punto a punto, es un método para que los clientes inalámbricos puedan establecer una comunicación directa entre sí. Al permitir que los clientes inalámbricos operen en modo *ad hoc*, no es necesario involucrar un punto de acceso central. Todos los nodos de una red *ad hoc* se pueden comunicar directamente con otros clientes. Cada cliente inalámbrico en una red *ad hoc* debería configurar su adaptador inalámbrico en modo *ad hoc* y usar los mismos SSID (es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.) y “número de canal” de la red.

Una red *ad hoc* normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca unos de otros. En una red *ad hoc* el rendimiento es menor a medida que el

---

Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes, en lugar de enviarla en forma analógica, a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (sigla de *Public Switched Telephone Network*, Red Telefónica Pública Conmutada).

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. Estos pueden verse como aplicaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), inventada por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las redes de área local (LAN).

Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP.

- VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva *la tecnología* que permite comunicar voz sobre el protocolo IP.
- Telefonía sobre IP es el servicio telefónico disponible al público, por tanto con numeración E.164, realizado con tecnología de VoIP.

[http://es.wikipedia.org/wiki/Voz\\_sobre\\_IP](http://es.wikipedia.org/wiki/Voz_sobre_IP)



número de nodos crece. Para conectar una red *ad hoc* a una red de área local (LAN) cableada o a Internet, se requiere instalar una Puerta de enlace o *Gateway* especial.

### 1.7.2 Infraestructura (BSS)

Contrario al modo *ad hoc* donde no hay un elemento central, en el modo de infraestructura hay un elemento de “coordinación”: un punto de acceso o estación base. Si el punto de acceso se conecta a una red Ethernet cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID. Para asegurar que se maximice la capacidad total de la red, no configure el mismo canal en todos los puntos de acceso que se encuentran en la misma área física. Los clientes descubrirán (a través del escaneo de la red) cuál canal está usando el punto de acceso de manera que no se requiere que ellos conozcan de antemano el número de canal. En redes IEEE 802.11 el modo de infraestructura es conocido como Conjunto de Servicios Básicos (BSS – Basic Service Set). También se conoce como Maestro y Cliente.

### 1.8 Ejemplos reales de infraestructura inalámbrica

En la vida real las redes inalámbricas son a menudo combinaciones de diferentes topologías. Veamos tres ejemplos para su discusión.

#### Ejemplo1: Una red típica de oficina con una parte inalámbrica

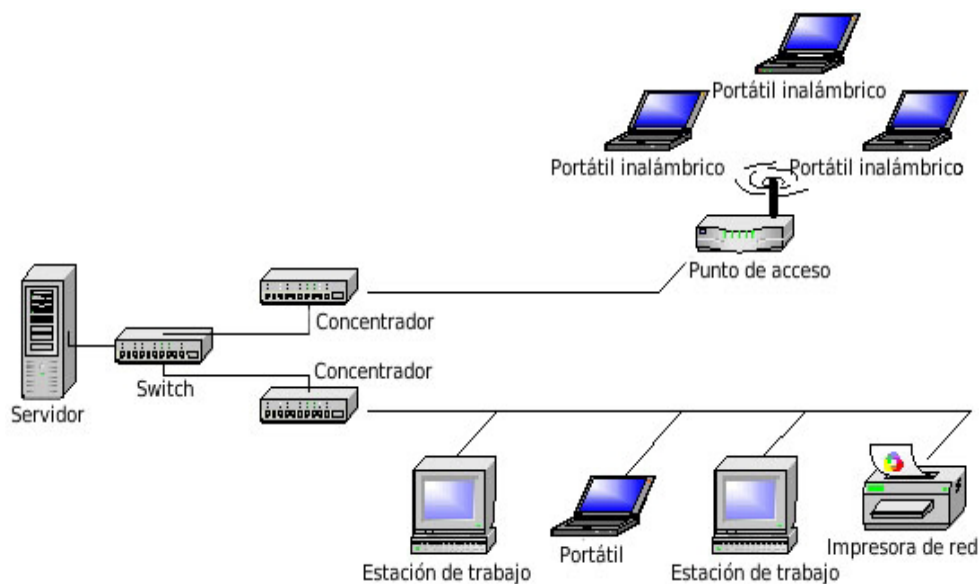
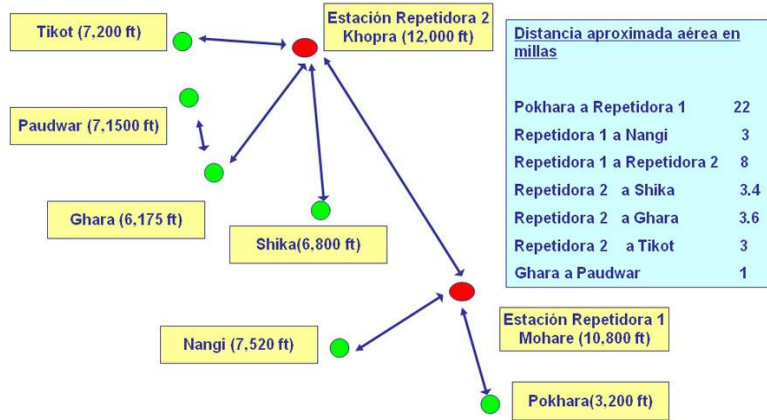


Fig. 1.29 Red típica de oficina.

**Ejemplo 2: Dorsal (Backbone) de una red empresarial.**



**Fig. 1.30 Red Empresarial**

**Ejemplo 3: Red inalámbrica de red corporativa**

Observar en la figura 1.31:

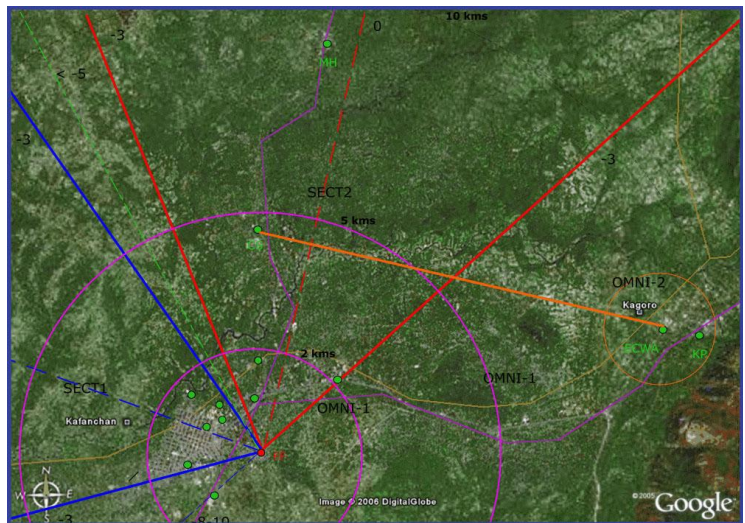
**Nodo rojo (FF):** Centro de operaciones de la red (NOC - Network Operation Center) con conexión a Internet (VSAT).

**Nodo verde:** Clientes inalámbricos.

**Enlace naranja:** Enlace punto a punto.

**Sector azul:** Topología de estrella (SECT1) cubriendo 5 nodos

**Sector rojo:** Topología de estrella (SECT2) cubriendo 5 nodos



**Figura 1.31 Red inalámbrica Corporativa**

**1.9 Consideraciones**

La topología de una red define la distribución física y lógica de la conexión entre sus nodos. Dependiendo del propósito y naturaleza de una red, una topología puede ser más apropiada que otra.

- ¿La red debe ser escalable o se debe diseñar sólo para algunos nodos?
- ¿La eficiencia de los costos es más importante que la confiabilidad y la redundancia?
- ¿Qué rango de cobertura se requiere?
- ¿Para cuantos nodos?
- ¿Cómo es el terreno del sitio en donde se implementará?

Todas estas preguntas y muchas más, deben ser consideradas en el proceso de diseño de la topología de una red cableada o inalámbrica.

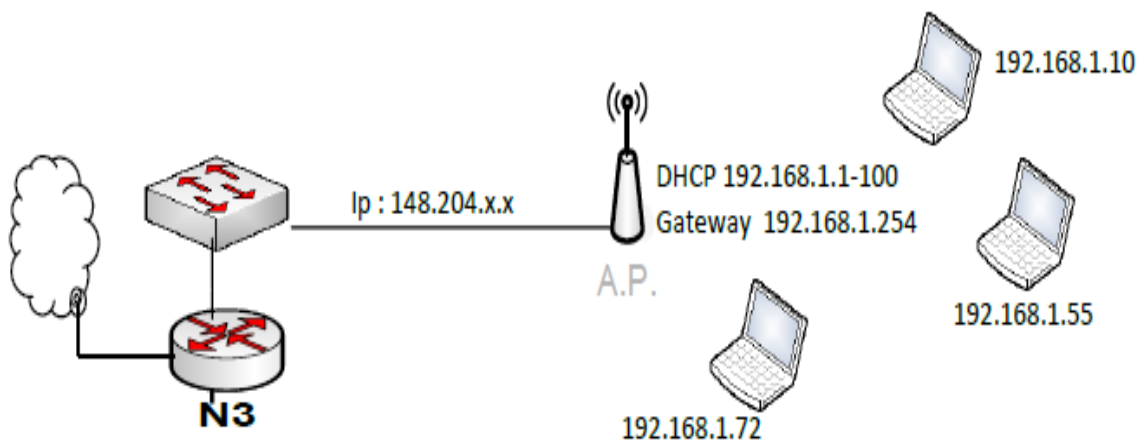
## Capítulo 2

### Estado inicial de la red académica

#### 2.1 Situación Inicial

Como todo sistema de redes, la tendencia es en primera instancia hacer una red híbrida, con accesos cableados y cobertura inalámbrica, y refiriéndonos a esta última la demanda de este tipo de acceso es cada vez mayor (entre alumnos, personal académico y de apoyo). Por lo que en la unidad académica (La Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas: UPIITA) se decidió implementar algunos servicios de red inalámbrica. En un principio con algunos problemas y deficiencias, debido al equipo que se utilizaba para tal fin (Access points linksys y 3com) los cuales resolvían una pequeña parte del problema en el servicio de cobertura inalámbrica.

Se instalaron algunos de los equipos que se mencionan en el capítulo tres en diversos puntos de la unidad, los cuales fueron configurados con una IP homologada como proveedor de WAN y una subred clase C como servicio de DHCP en su esquema de salida:



2.1 Esquema inicial

De esta forma se distribuyeron en diversos puntos para cubrir la demanda de los equipos inalámbricos quedando de la siguiente forma:

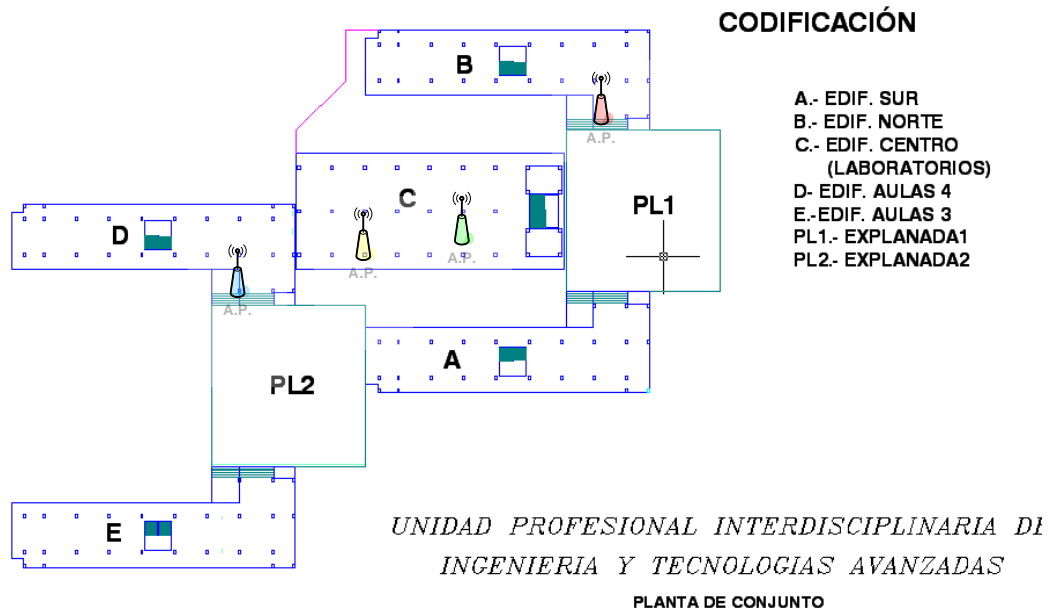


Figura 2.2 Ubicación de Sites

## 2.2 Equipos usados para la WLAN.

Para el primer diseño de la red inalámbrica de la UPIITA fueron usados equipos convencionales y comerciales de conectividad inalámbrica, los cuales fueron configurados cada uno bajo el esquema (Fig. 2.1) de situación inicial y cuya función era la de transmitir la señal de la red inalámbrica para los usuarios

### 2.2.1 Medición de Huella de alcance

A continuación se presentan las mediciones hechas para establecer la huella de alcance de la red inalámbrica en función de la ubicación de los equipos en puntos establecidos para la distribución de la misma.

### 2.2.2 Huella en edificio Norte

Debido a la ubicación del AP (Edificio Norte, primer piso, salón 212 [Área de Impresión I-UDI] ), esta huella cubre los requerimientos de red inalámbrica para el mismo edificio (B), la Explanada 1 (PL1), parte del edificio Sur (A primero , segundo y tercer nivel), e incluso la primer planta lado Norte del edificio Centro (C).

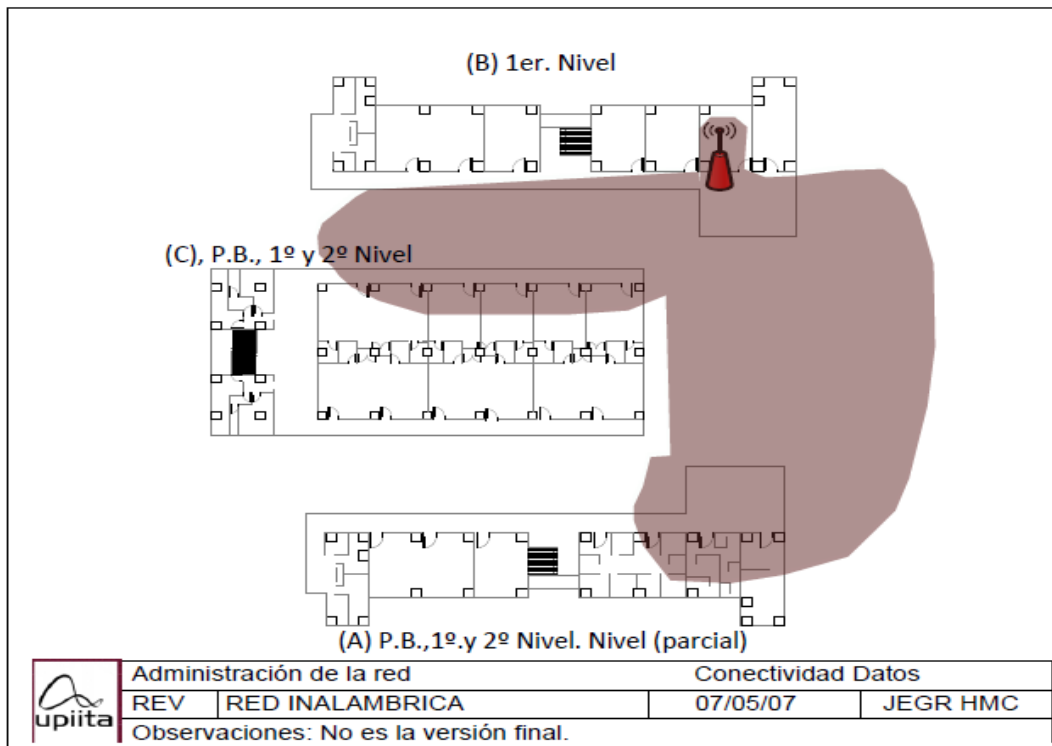


Figura 2.3 Huella inalámbrica Edif, Nte.

### 2.2.2.1 Huella en edificio Centro

En este edificio se dispusieron dos AP's , uno en la planta baja del edificio en el área de biblioteca (Aula **L1**) para dar cobertura a los usuarios de la misma (**C** planta baja), parte de la planta baja del edificio norte (**B**) y parte del edificio sur (**A**); y otro más en el primer nivel en el laboratorio de Telemática, con el fin de dar alcance a los usuarios de esta zona (**C**) primer nivel y parte de la explanada 2 (**PL2**)

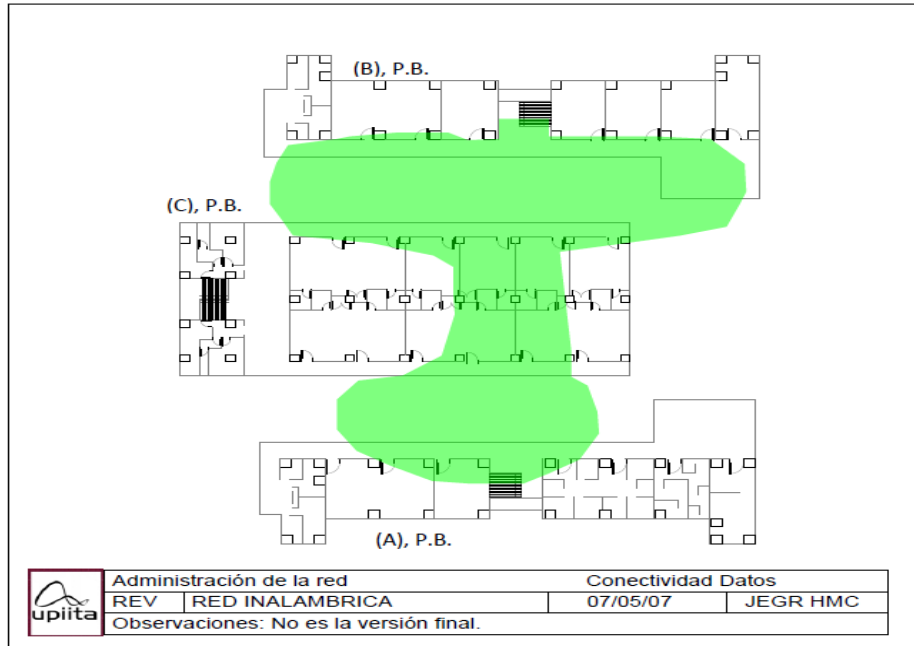


Figura 2.4 Huella Inalámbrica Edif. Centro (biblioteca)

Huella en edificio Centro (continuación)

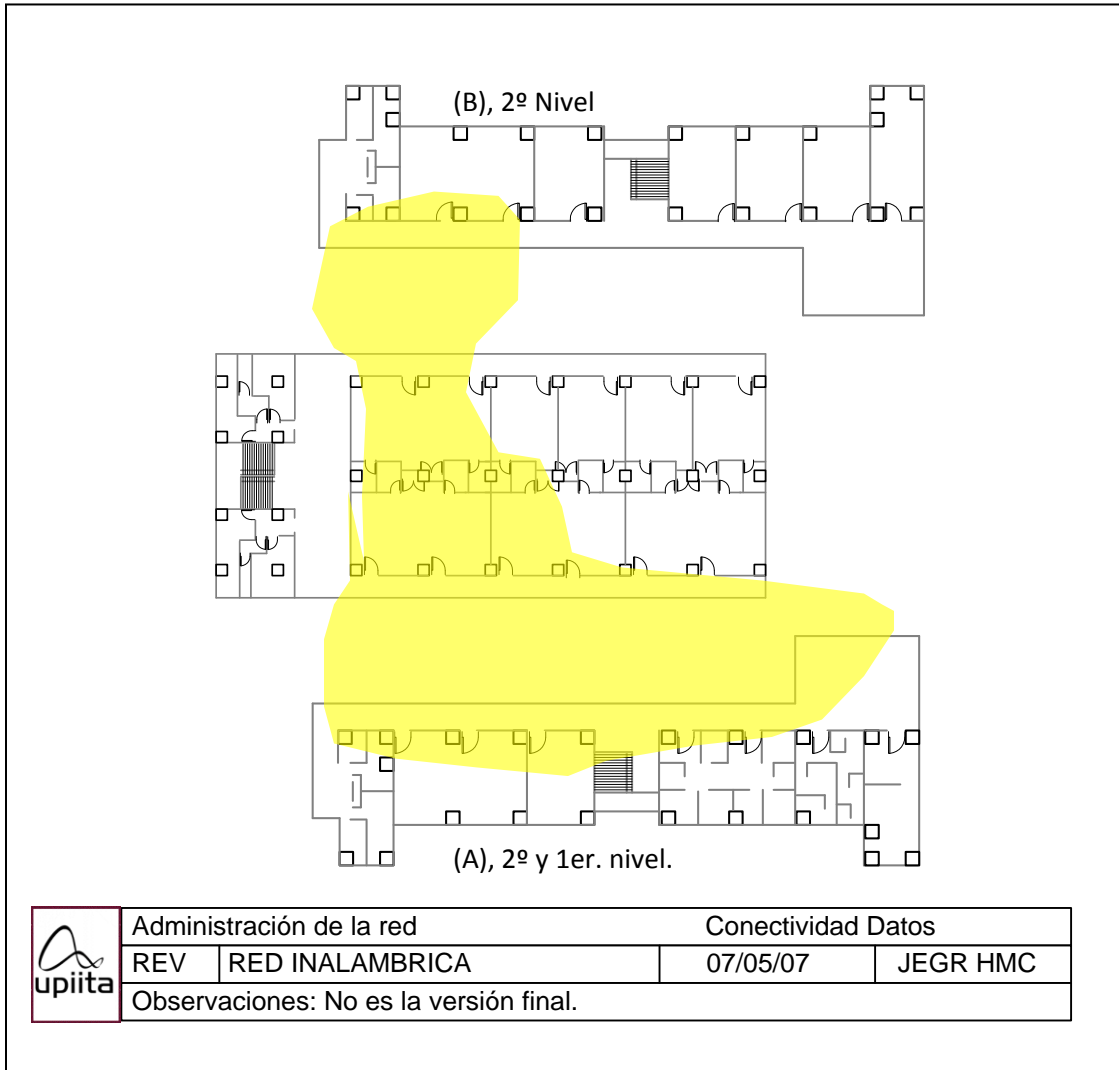


Figura 2.5 Huella inal. edif. Cent. (Cont)

### 2.2.2.2 Huella en edificio Aulas 4

Con la ubicación de este AP (**2º Nivel edificio D**) en el área de la academia de Ciencias Sociales, se cubre esa mismo zona, así como parte del edificio contiguo (**C**), la explanada 2 (**PL2**) y parte del edificio aulas 4 (**E**).

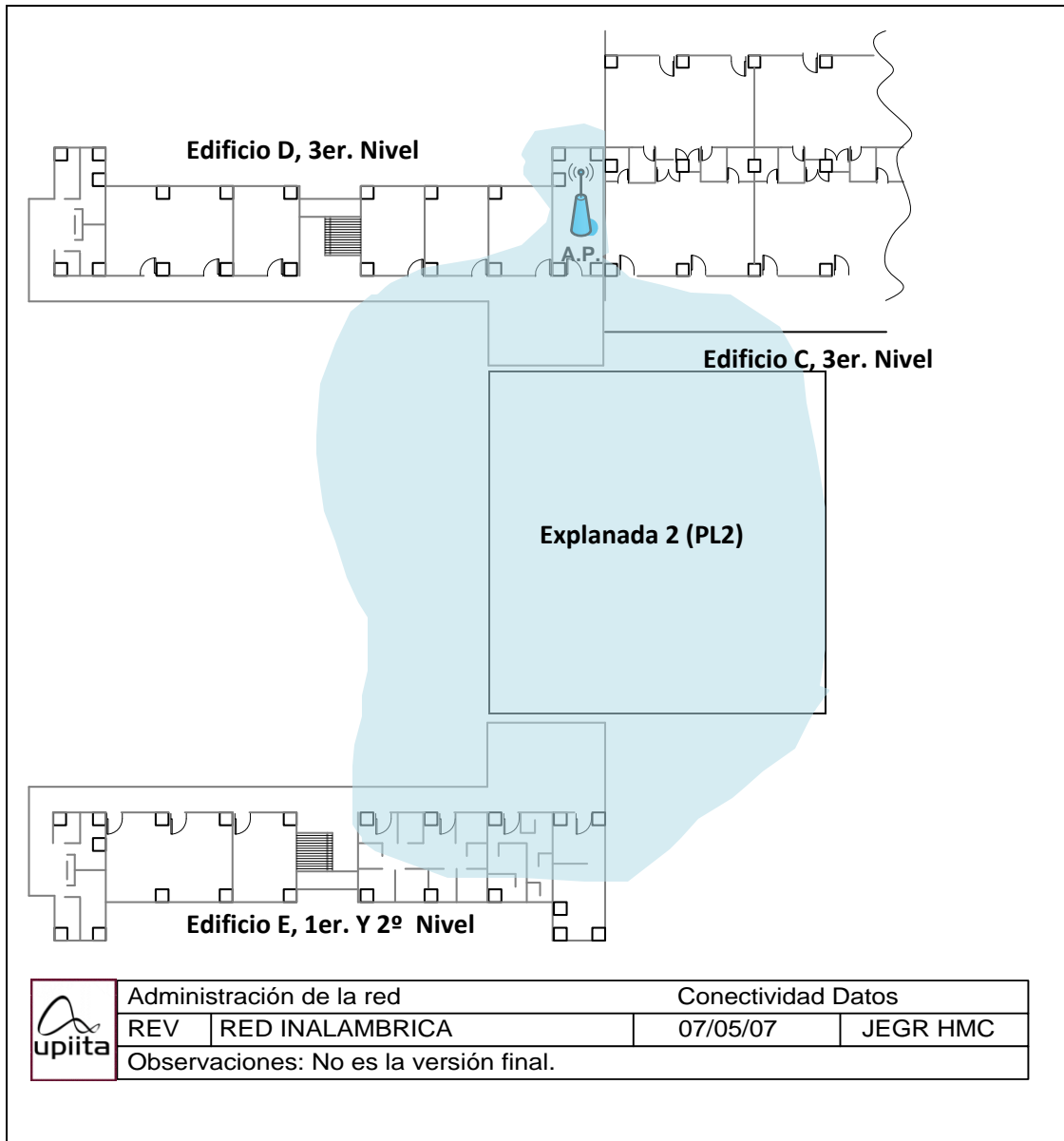


Fig. 2.6 Huella en edificio Aulas 4



### 2.2.2.3 Plano de conjunto

Podemos observar que de esta forma quedo cubierta en un 80 % la zona de pasillos, escaleras y estancias en los diferentes niveles de los edificios de la unidad utilizados por los usuarios de red inalámbrica; cabe aclarar que existe una atenuación debida a los materiales de construcción de los edificios, por lo que las huellas de las diferentes señales inalámbricas se pierden o disminuyen notablemente al interior de los salones y laboratorios de clases, en la mayoría de los casos.

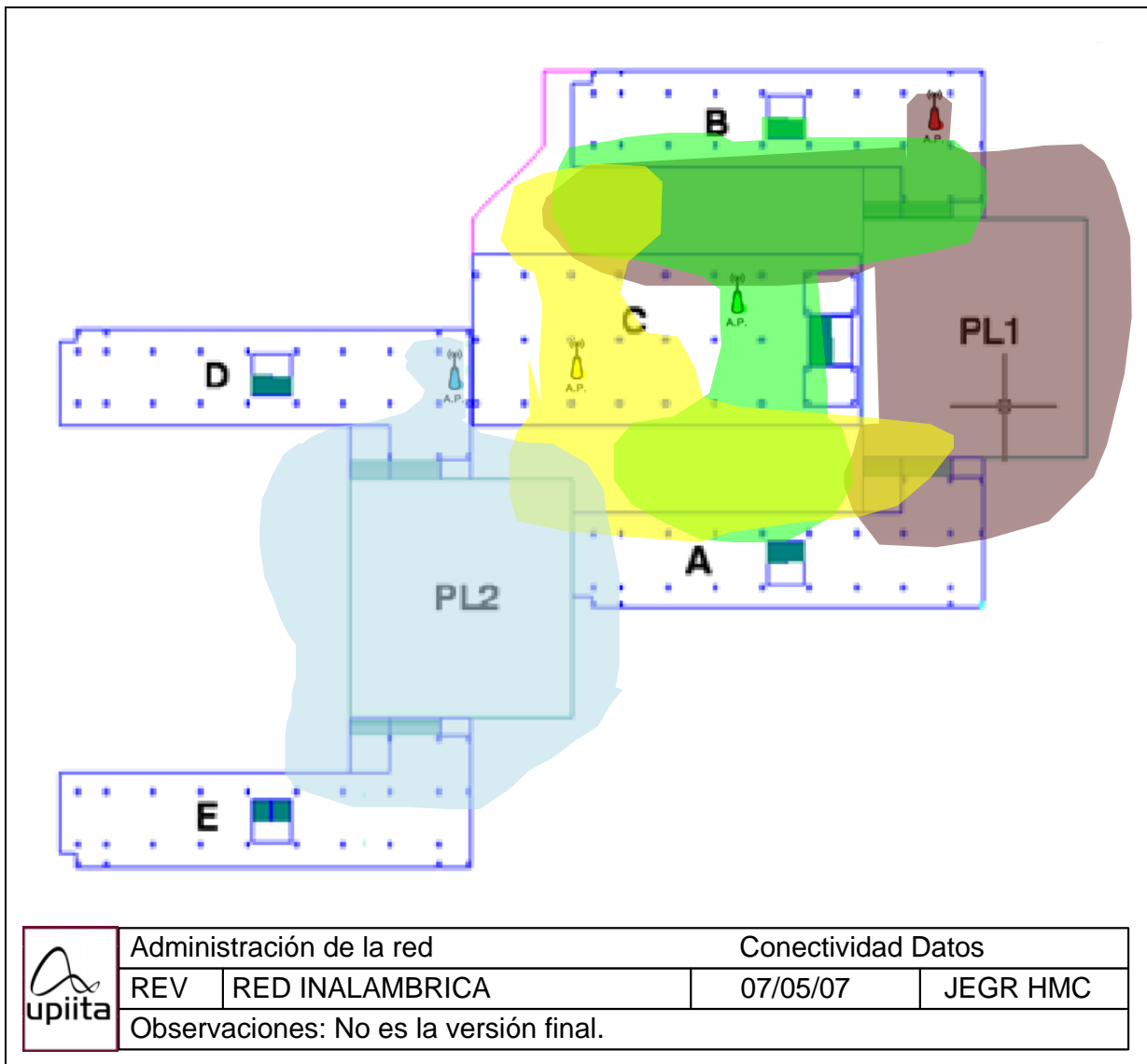


Figura 2.7 Plano de conjunto

Equipo / Marca	Ubicación	Color	Cobertura
A.P.1 (3Com)	Edificio B 1er Nivel	ROJO	<ul style="list-style-type: none"> <li>• Aula 212 (imp-UDI) Edif. B</li> <li>• 1er Nivel Edificio B (pasillos)</li> <li>• P.B. Edificio C (pasillos)</li> <li>• 1er. Nivel Edificio C (Pasillo norte.)</li> </ul>
A.P.1 (D-Link)	Edificio C (biblioteca) P.B.	VERDE	<ul style="list-style-type: none"> <li>• Aula Biblioteca y pasillo norte de edificio C</li> <li>• P.B. Edificio B</li> <li>• P.B. Edificio C lado sur (parcial)</li> <li>• P.B. Edificio A lado sur (parcial)</li> </ul>
A.P.3 (3Com)	Edificio C 2º Nivel (Lab. Telemática)	AMARILLO	<ul style="list-style-type: none"> <li>• Aula Telemática y pasillo de edificio C lado sur y parte del norte</li> <li>• Pasillos 1er y 2º nivel de edificio A</li> </ul>
A.P.1 (Linksys)	Edificio D salón 421 (Acad. C. Sociales)	AZUL	<ul style="list-style-type: none"> <li>• Aula 412 de edificio D (Academia de C. Sociales.)</li> <li>• Pasillo de 2º nivel de edificio D</li> <li>• Pasillo de 2º nivel de edificio C</li> <li>• Explanada PL2</li> <li>• P.B. de edificio E</li> <li>• 1er nivel de edificio E</li> </ul>

Tabla 2.1 Áreas cobertura de red inalámbrica – Uso Académico.

### 2.2.3 Metodología de control

Para ofrecer el servicio inalámbrico se configuraron los equipos bajo los siguientes parámetros

NOMBRE	DESCRIPCIÓN	Dato real
SSID	Nombre de la red	UDI-UPIITA-(aa)/(pl)
Contraseña	Contraseña para acceder a la interfaz de gestión	Personal UDI
Método de autenticación	Mecanismo establecido para controlar el acceso	WEP
“Shared secret”	Secreto compartido entre el punto de acceso y el equipo.	Clave cifrada de 64 bits cambiada cada semestre
Esquema de asignación de direcciones IP de cliente	Rangos de direcciones que se utilizarán para asignar direcciones a los clientes	192.168.2.1 - 192.168.2.150
Dirección IP mediante la activación del DHCP en cada equipo	Dirección del servidor que usan los clientes para resolver direcciones	192.168.2.254

Tabla 2.2 Metodología de control

También se pensó en un modo que hiciera a los usuarios traer su equipo, para darlo de alta dentro de la red mediante el uso de una clave WEP homogenizada en todos los Access Point, mediante la publicación del servicio de red inalámbrica en la unidad; en la cual, se solicita al usuario traer su equipo a la UDI (Unidad Disciplinaria) para que el personal de esta, registre los equipos y verifique los siguientes puntos:

- Ser alumno inscrito y con credencial vigente
- Tener instalado un antivirus vigente y actualizado
- Presentar la última verificación del antivirus

- Tener un spyware (anti espías) activo
- Proporcionar el nombre de equipo, tipo de sistema operativo y Mac de las redes Ethernet y Wireless.

### **2.3 Inconvenientes**

Trabajando de este modo, se descubrieron algunos puntos débiles en este esquema de red, los cuales traen como consecuencia diversos problemas, algunos de mayor relevancia y que se citan a continuación:

#### **2.3.1 Bajo o nulo control sobre los usuarios.**

Al registrar los equipos en la red inalámbrica y su posterior navegación en esta, no se tiene claramente definida la actividad del usuario en esta, por lo que no se sabe a ciencia cierta qué tipo de páginas visita o qué ataques realiza.

#### **2.3.2 Descubrimiento de la clave WEP de los equipos por parte de usuarios ilícitos.**

Al tener funcionando el servicio de la red inalámbrica, algunos usuarios registrados de forma oficial, instalaron en sus equipos en el mejor de los casos, software para poder conocer la clave WEP introducida; o en su defecto quienes se abstienen de registrar sus equipos, utilizan software de inyección de paquetes para descubrir mediante algunos procesos las claves WEP directamente de los equipos aprovechando vulnerabilidades de la red misma.

#### **2.3.3 Infiltración de usuarios a la red homologada.**

Debido a ciertas debilidades en los AP's, se permite al usuario ver las redes disponibles en la unidad, no solo las inalámbricas sino también las pertenecientes a diversas áreas de la UPIITA, como la de las computadoras en las academias, laboratorios y otras áreas que, si en su momento tenían recursos compartidos, se podía tener acceso a ellos de forma fácil o mediante métodos de descifrado más complejos, poniendo en riesgo la seguridad en la red de la unidad.

#### 2.4.4 Alta propagación de virus

Esta propagación entre los usuarios de la red inalámbrica es debida a los accesos ilegales de equipos a esta, los cuales no son verificados por la UDI y cuyos equipos están infectados con virus: gusanos, troyanos, etc, y que al pasar información por la red inalámbrica, infectan de manera automática a los equipos en la misma e incluso llegando a generar grandes tormentas de broadcast debido a la propagación de todo el software malintencionado.



Figura 2.8 Alta propagación de virus

#### 2.4.5 Robo o clonación de IPs del segmento institucional

Algunos usuarios descubrieron que, una vez teniendo la clave WEP, los AP's simplemente funcionaban como una pasarela y aprovechando esta vulnerabilidad configuraron en sus equipos (PC) portátiles de forma manual una dirección ip del rango perteneciente a la unidad (192.168.222.x) provocando conflictos de IP's duplicadas con otros usuarios de la red cableada, e incluso interfiriendo con las IP's de los equipos de conectividad (switches y AP's)

#### 2.4 Inseguridad

Al ser detectadas todas las fallas de seguridad mencionadas, se pensó en algún método para comenzar a corregir estas vulnerabilidades en la red inalámbrica, por lo que se pensó en que las MAC obtenidas originalmente para control de los usuarios fueran introducidas dentro de la configuración de los equipos mediante sus capacidades de admisión

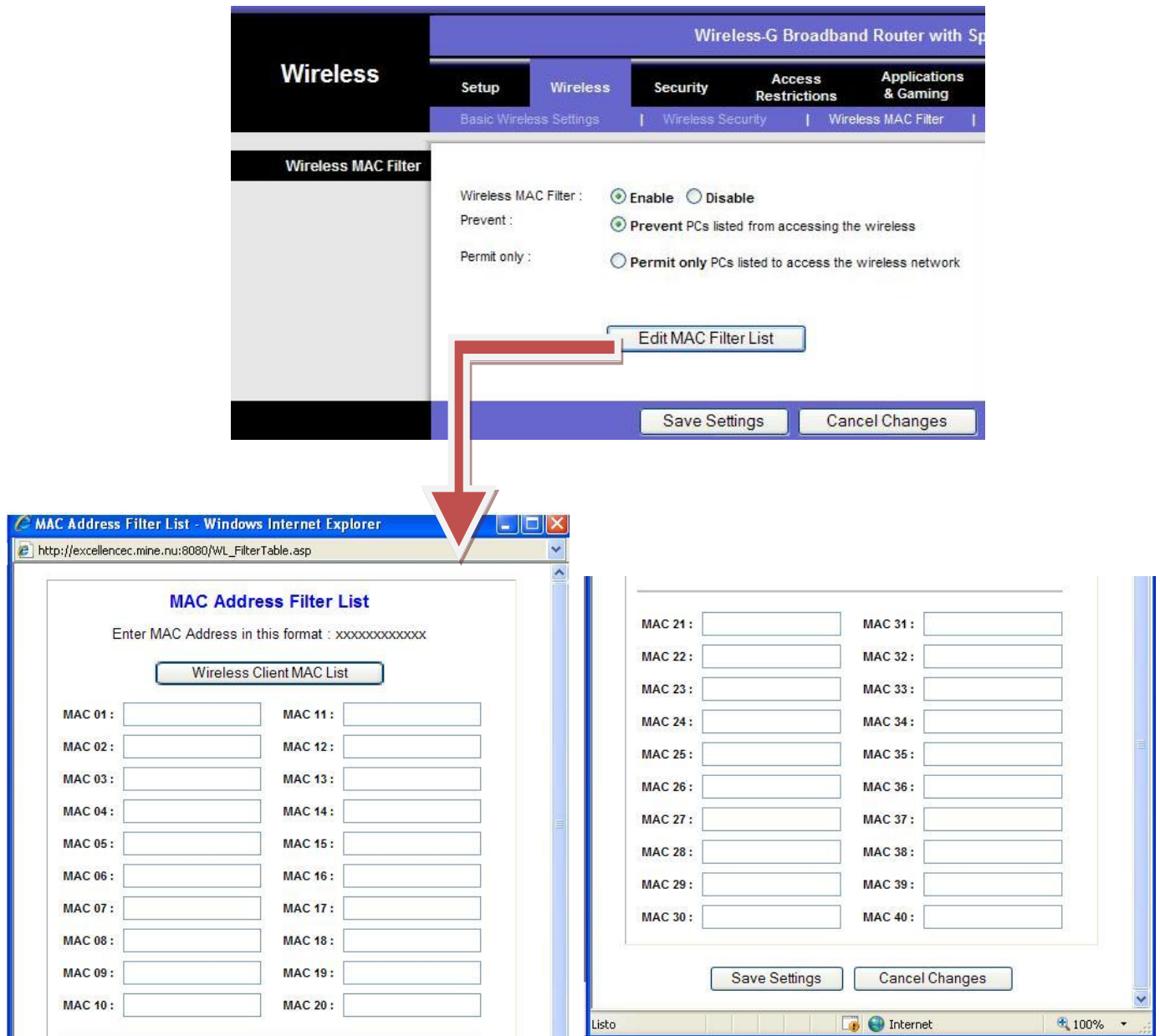


Fig. 2.9 captura de direcciones MAC.

Como se puede observaren la figura 2.9, aparentemente los equipos permitían capturar entre 30 y 40 MAC de usuario, que si bien no eran suficientes, al menos se podría pensar en establecer una forma de seguridad para la admisión de equipos a la red inalámbrica.

Surge entonces otro problema, y es que debido a que los equipos son del tipo comercial, no soportan una carga máxima de direcciones MAC y comienzan a volverse

inestables, se traban o aun estando visibles y al alcance, deniegan servicio inalámbrico a todos los usuarios.

Por tal motivo y como medida provisional se decide cambiar la clave de WEP con cierta periodicidad, para tratar de minimizar los accesos no autorizados.

En base a la experiencia hemos observado que los equipos comerciales son útiles solo en casos de radiación de huella no muy amplia, es decir, algunos departamentos y áreas más exclusivas y bien delimitadas, y zonas en donde no se rebase cierta cantidad de usuarios conectados simultáneamente, es por eso que se procede a reestructurar esta red y rediseñarla para dar un mejor servicio a los usuarios inalámbricos, ofreciendo mayor seguridad a los usuarios de la red cableada.

## Capítulo 3 Diseño y configuración de la VLAN inalámbrica

### 3.1. Visión general para el diseño del sistema.

Al plantear el diseño de la red inalámbrica se debe tener en cuenta no solo el equipo inalámbrico, antenas o switches a utilizar, sino todo el conjunto que actualmente conforma la red cableada completa de la UPIITA (Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas ), dado que se harán uso de estos para poder llegar al diseño perseguido para los fines de este documento, por tanto se piensa ir integrando a la red que ya existe de modo gradual con la finalidad de no interferir en ningún modo con la estructura actual y evitar posibles conflictos de conectividad en las diferentes áreas en donde se sitúen los equipos, basándonos en estándares y normas ya establecidas (Cableado estructurado 568, A-B; 802.11 a, b y g) con el fin de lograr un alto desempeño en los equipos y ofrecer la mayor calidad posible.

Actualmente la unidad cuenta con 5 sites de comunicaciones (1 en cada edificio en la planta baja) interconectados con fibra óptica, basados en el estándar 803.3z y en la que una de las características principales es la Velocidad de proceso de datos de 1000 Mbps entre equipos los cuales ubicados en la planta baja de los 5 edificios, como se muestra en la figura 3.1, y cuya canalización también se muestra en el diagrama.

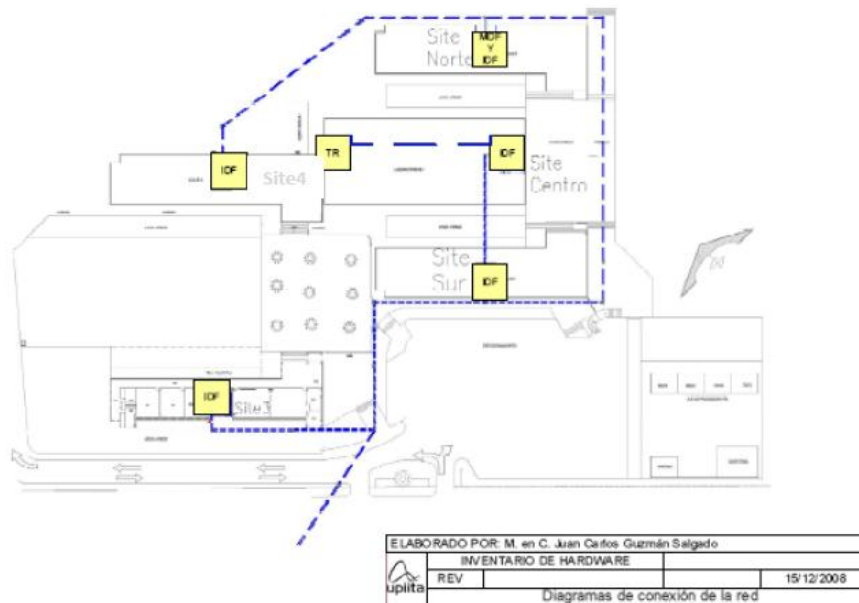


Figura 3.1 Conectividad por fibra óptica.



### 3.1.1. Interconexión Actual

Esquemáticamente la interconexión de los equipos se muestra en la siguiente figura.

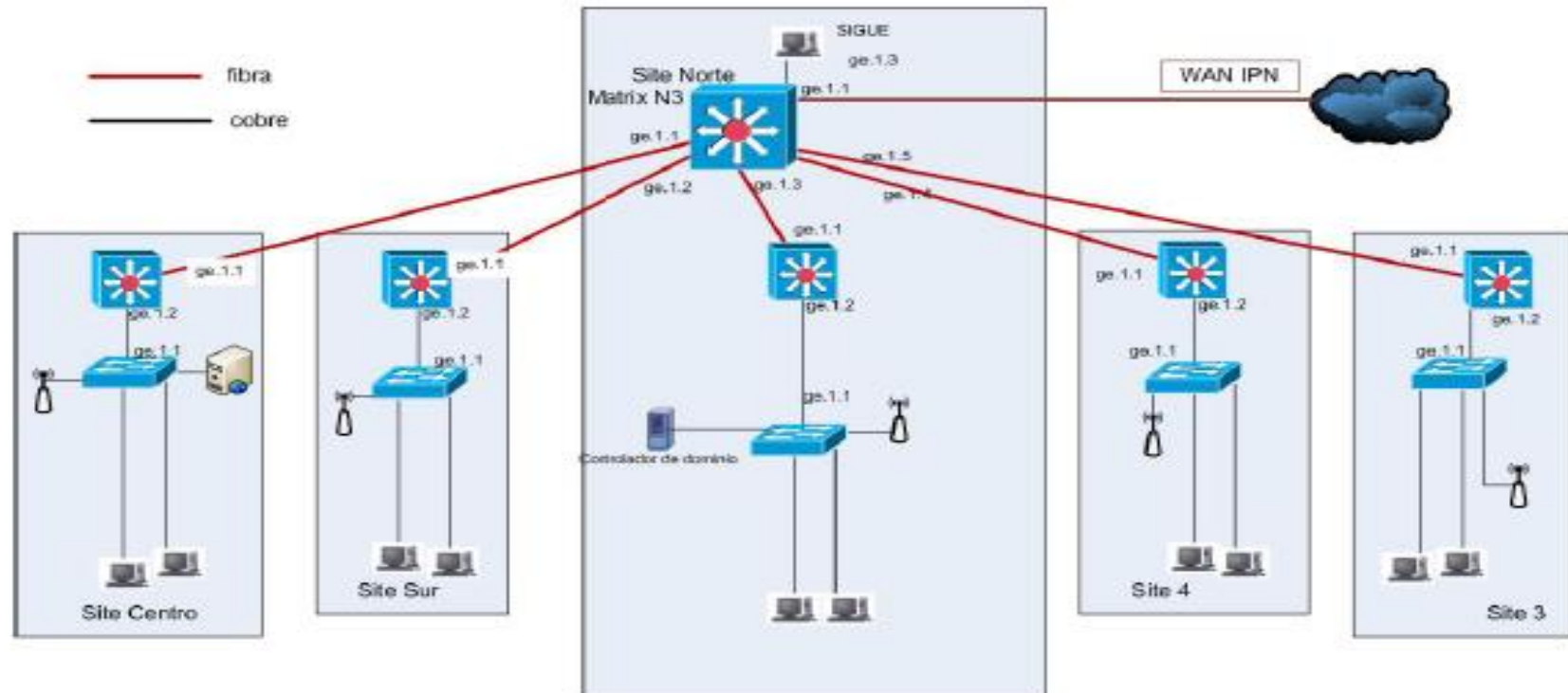


Figura 3.2 Interconexión por fibra óptica.

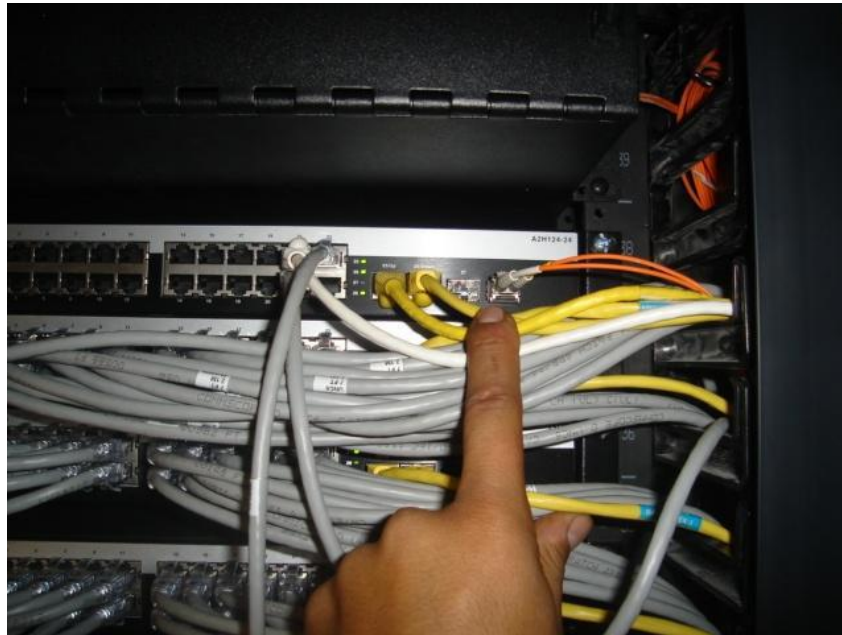


Figura 3.3 Interconexión por fibra



Figura 3.4 Distribuidor de Fibra óptica

### 3.1.2 Ubicación de equipos de Capa 2

Estos sites cuentan con tecnología de la marca enterasys de alto desempeño cuyas características se enlistan a continuación, seguido por la imagen de los mismos (ver tabla 3.1):

SITE DE COMPUTO SUR							
PIEZA	MARCA	MODELO	NO. SERIE O SERVICE TAG	CARACTERÍSTICAS TÉCNICAS	SOFTWARE	SERVICIOS	OBSERVACIONES
Distribuidor de Fibra Optica	Lucent	N/A	N/A	12 HILOS	N/A	CONECTIVIDAD DE F.O. A EDIF NORTE	10 PTOS LIBRES
Distribuidor de fibra optica	***	***	***	ENLACE MULTIMODO 12 HILOS	N/A	CONECTIVIDAD DE EDIF SUR A AULAS 3	10 PTOS LIBRES
Distribuidor de fibra optica	***	***	***	12 HILOS (6 PARES)	N/A	CONECTIVIDAD DE AULAS 2 A AULAS 1/AULAS 2 A AULAS 3/AULAS2 A LAB1/	4 PARES OCUPADOS (1 PAR TELEFONIA AULAS )
Distribuidor de fibra optica	***	***	***	24 HILOS	N/A	CONECTIVIDAD CINVESTAV 3-4 TELEFONIA	4 HILOS OCUPADOS
switch	Enterasys	A2H124-24	06360769905F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 PTOS FO LIBRES 18 ETH LIBRES 1 PTO SERIAL
switch	Enterasys	A2H124-24	08424359225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK

Tabla 3.1 Equipos de Site SUR

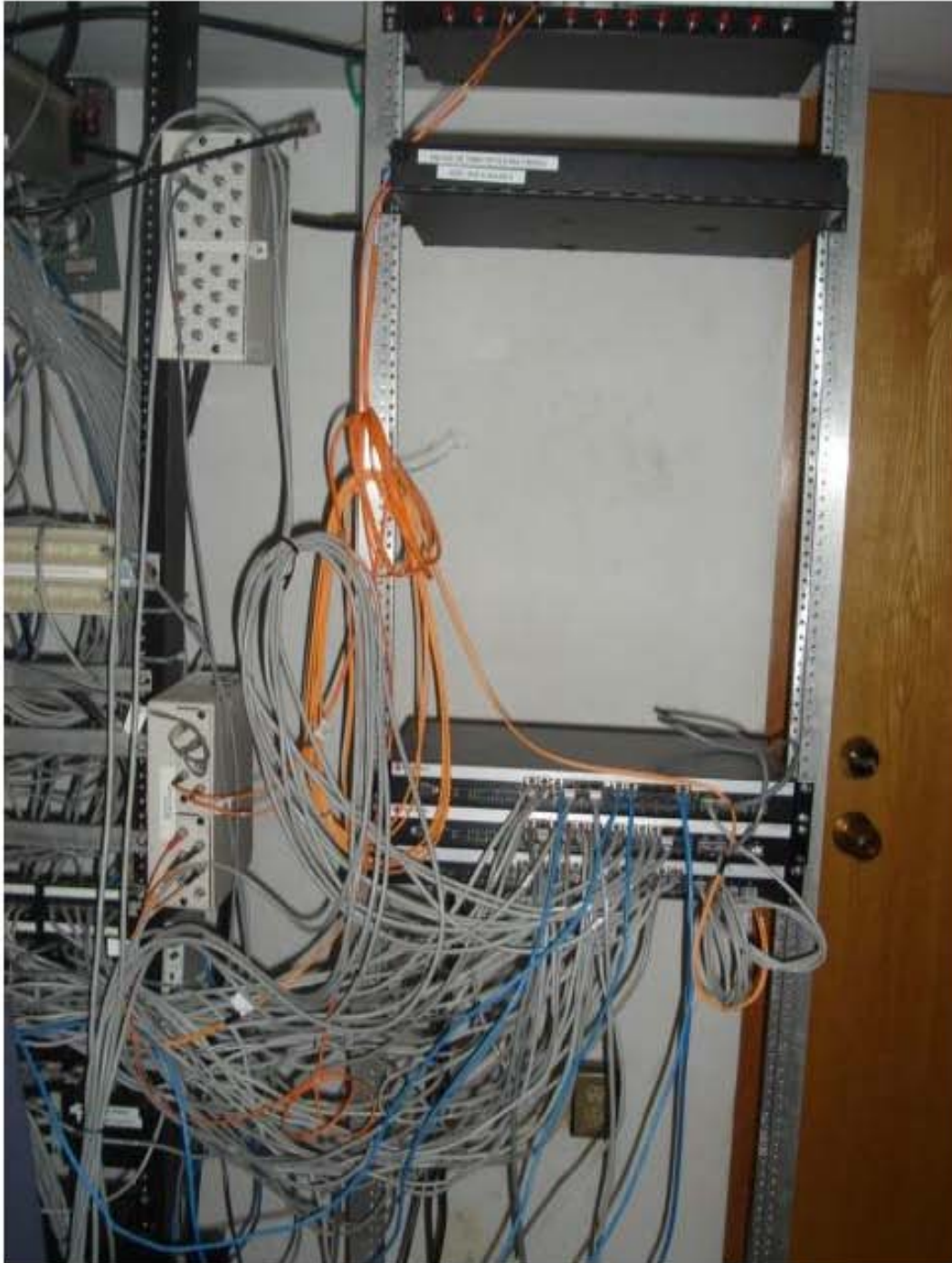


Figura 3.5 Rack Site sur

Site de cómputo centro.

SITE DE COMPUTO CENTRO							
PIEZA	MARCA	MODELO	NO. SERIE O SERVICE TAG	CARACTERÍSTICAS TÉCNICAS	SOFTWARE	SERVICIOS	OBSERVACIONES
Panel de conexiones pasivo 48 puertos	PowerSum Panel	1100PSE	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	22 PTOS LIBRES
Panel de conexiones pasivo 48 puertos	Modular Rack Panel	1100 cat5 PS	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	12 PTOS LIBRES
Panel de conexiones pasivo 24 puertos	Modular Rack Panel	1101 cat5 PS	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	22 PTOS LIBRES
Panel de conexiones pasivo 48 puertos	Modular Rack Panel	1100 cat5 PS	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE VOZ	22 PTOS LIBRES
switch	Enterasys	A2H124-24	06331009905F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 PTOS FO LIBRES 4 PTOS ETH LIBRES
switch	Enterasys	A2H124-24	06360770905F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 PTOS FO LIBRES 13 PTOS ETH LIBRES
switch	Enterasys	A2H124-24	06331010905F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 PTOS FO LIBRES 11 PTOS ETH LIBRES
switch	Enterasys	A2H124-24	08422472225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 1 PTO FO LIBRE 6 PTOS ETH LIBRES
Distribuidor de Fibra Optica	Lucent	N/A	N/A	12 PTOS (HILOS)	N/A	CONECTIVIDAD DE F.O. DE EDIF AU LAS 1 A EDIF LABS1	10 PTOS LIBRES
No Break	POWERCOM MGE	ULT3000 RM	20211074	INPUT:100/110/115/120 VOLTS 50/60Hz 30.5A	***	ALIMENTACION DE CORRIENTE	TIENE PTO SERIAL

Tabla 3.2 Equipo en Site 3



Figura 3.6a Rack Site Centro (Cerrado)



Figura 3.6b Rack Site Centro (Abierto)

SITE DE COMPUTO 3							
PIEZA	MARCA	MODELO	NO. SERIE O SERVICE TAG	CARACTERÍSTICAS TÉCNICAS	SOFTWARE	SERVICIOS	OBSERVACIONES
<b>RACK 1</b>							
Distribuidor de fibra optica	***	***	***	ENLACE MULTIMODO 12 HILOS	N/A	CONECTIVIDAD DE AULAS3 A EDIF SUR	10 HILOS LIBRES
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	47 PTOS DISPONIBLES
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	45 PTOS DISPONIBLES
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	11 PTOS DISPONIBLES
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	0 PTOS DISPONIBLES
switch	Enterasys	A2H124-24	08422489225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 1 FO DISPONIBLES 1 SERIAL 0 ETH LIBRES
switch	Enterasys	A2H124-24	08422470225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 FO DISPONIBLES 1 SERIAL 0 ETH LIBRES
switch	Enterasys	A2H124-24	06360934905F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 FO DISPONIBLES 1 SERIAL
switch	Enterasys	A2H124-24	0842252222F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 FO DISPONIBLES 1 SERIAL

Tabla 3.3 Equipo en Site 4

SITE DE COMPUTO 3							
PIEZA	MARCA	MODELO	NO. SERIE O SERVICE TAG	CARACTERÍSTICAS TÉCNICAS	SOFTWARE	SERVICIOS	OBSERVACIONES
<b>RACK 2</b>							
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	0 PTOS DISPONIBLES
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	0 PTOS DISPONIBLES
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	19 PTOS DISPONIBLES
Panel de conexiones pasivo 48 puertos	Uniprise cat 6	Uniprise cat 6	N/A	48 PTOS CAT 6	N/A	CONECTIVIDAD DE DATOS	15 PTOS DISPONIBLES
switch	Enterasys	A2H124-48	08172009225F	switch 48 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 PTOS FO DISPONIBLES 1 SERIAL 0 PTOS ETH LIBRES
switch	Enterasys	A2H124-48	08172017225F	switch 48 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 PTOS FO DISPONIBLES 1 SERIAL 0 PTOS ETH LIBRES
switch	Enterasys	A2H124-48	08172022225F	switch 48 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 2 PTOS FO DISPONIBLES 1 SERIAL 1 PTO ETH LIBRE
Panel de conexiones multipares	***	***	***	MULTIPAR (50 PARES)	N/A	CONECTIVIDAD DE AULAS 3 A EDIFICIO SUR	

Tabla 3.4 Equipo en Site 4





Fig. 3.7 Racks y equipos de Site 3

SITE DE COMPUTO 4							
PIEZA	MARCA	MODELO	NO. SERIE O SERVICE TAG	CARACTERÍSTICAS TÉCNICAS	SOFTWARE	SERVICIOS	OBSERVACIONES
Distribuidor de fibra optica	***	***	N/A	ENLACE MULTIMODO 12 HILOS	N/A	CONECTIVIDAD DE F.O DE EDIF 2 A EDIF4	
Panel de conexiones pasivo 48 puertos	SYSTIMAX	1100	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	33 PTOS LIBRES
Panel de conexiones pasivo 48 puertos	SYSTIMAX	1100	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	38 PTOS LIBRES
Panel de conexiones pasivo 48 puertos	SYSTIMAX	1100	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	16 PTOS LIBRES
Panel de conexiones pasivo 48 puertos	SYSTIMAX	1100	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	30 PTOS LIBRES
switch	Enterasys	B2H124-24	06370223905F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	
switch	Enterasys	B2H124-24	08422468225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	
switch	Enterasys	B2H124-24	08422492225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	
switch	Enterasys	B2H124-24	08424356225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	
switch	Enterasys	B2H124-24	08424357225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	

Tabla 3.5 Equipos en Site 4



Fig. 3.8 Rack de Site 4

SITE DE COMPUTO NORTE							
PIEZA	MARCA	MODELO	NO. SERIE O SERVICE TAG	CARACTERÍSTICAS TÉCNICAS	SOFTWARE	SERVICIOS	OBSERVACIONES
Panel de conexiones pasivo 48 puertos	PowerSum Panel	1100PSE	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	0 PTOS LIBRES
Panel de conexiones pasivo 24 puertos	Modular Rack Panel	1100 cat5 PS	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	17 PTOS LIBRES
Panel de conexiones pasivo 48 puertos	Modular Rack Panel	1101 cat5 PS	N/A	TIA-EIA-T568 B WIRING	N/A	CONEXIONES DE DATOS	0 PTOS LIBRES
switch	Enterasys	A2H124-24	08422483225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS (AULA Proxy)	SIN STACK 1 PTO ETH LIBRE 2 PTOS FO LIBRES
switch	Enterasys	A2H124-24	08424358225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 0 PTO ETH LIBRE 2 PTOS FO LIBRES
switch	Enterasys	A2H124-24	06360937905F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 1 PTO ETH LIBRE 2 PTOS FO LIBRES
switch	Enterasys	A2H124-24	08424360225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	EN STACK 21 PTO ETH LIBRES
switch	Enterasys	A2H124-24	08422484225F	switch 24 ptos	CLI/FIRMWARE	CONECTIVIDAD DE DATOS	SIN STACK 4 PTOS ETH LIBRES 2 PTOS FO LIBRES
Distribuidor de fibra optica	RAD	FOM-E1/T1	450990	115 VAC 1PTO TX Y PT RX 2 1 PTO SERIE PTOS COAXIAL IN AND OUT	CLI	CONECTIVIDAD DE DATOS	
Distribuidor de fibra optica	***	***	N/A	ENLACE MONOMODO 12 HILOS	N/A	CONECTIVIDAD MONOMODO DE F.O	
Distribuidor de fibra optica	***	***	N/A	ENLACE MONOMODO 12 HILOS	N/A	CONECTIVIDAD MONOMODO DE F.O DE DIRECCION GENERAL A UPIITA	
Distribuidor de fibra optica	***	***	N/A	ENLACE MULTIMODO 12 HILOS	N/A	CONECTIVIDAD MULTIMODO DE F.O EDIFICIO CENTRO A EDIFICIO NUEVO	
Router	Enterasys	N3	AR79NF	6 PTOS F.O 24 PTOS ETHERNET	CLI/FIRMWARE	CONECTIVIDAD DESDE DCYC A UPIITA	5 ptos F.O ocupados 8 ptos eth ocupados
POWER	Enterasys	7C203-1	AR79NF	100-125 VOLTS 12A 200-240 VOLTS 6A 50/60 Hz	N/A	ALIMENTACION DE CORRIENTE	
POWER SUPPLY	Enterasys	7C203-1	AR79NF	100-125 VOLTS 12A 200-240 VOLTS 6A 50/60 Hz	N/A	ALIMENTACION DE CORRIENTE	

Tabla 3.6 Equipo en Site Norte

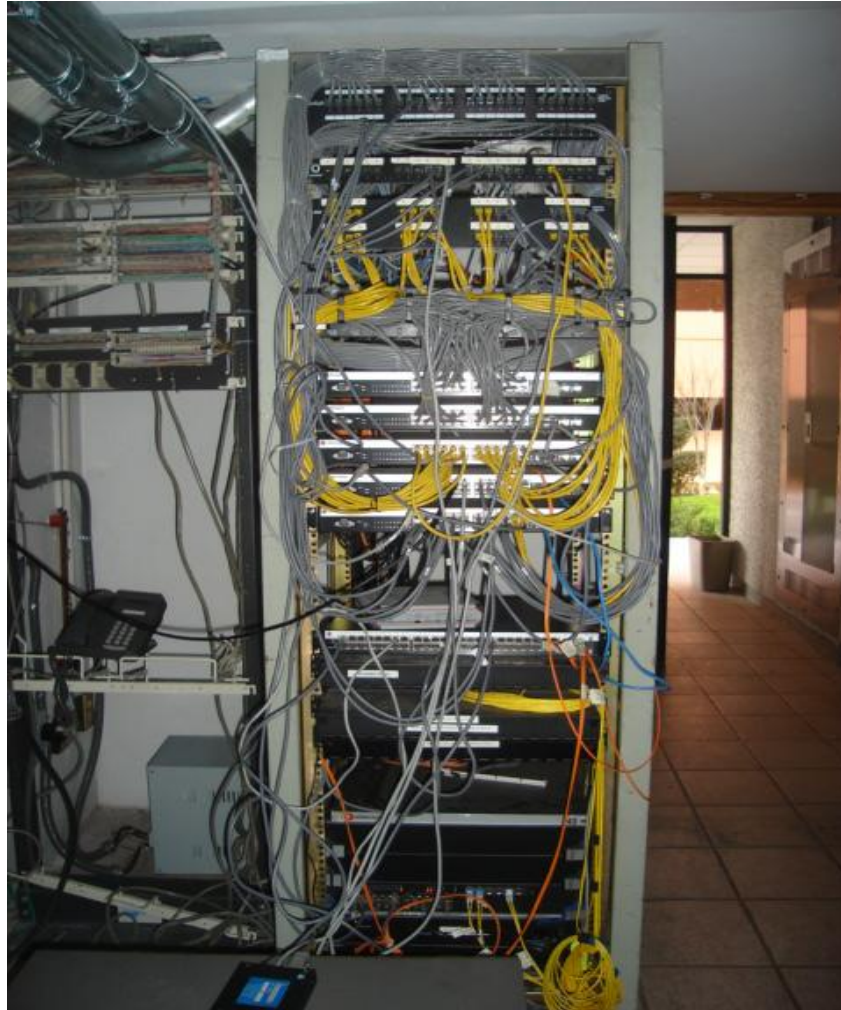


Figura 3.9 Rack y equipo en Site Norte

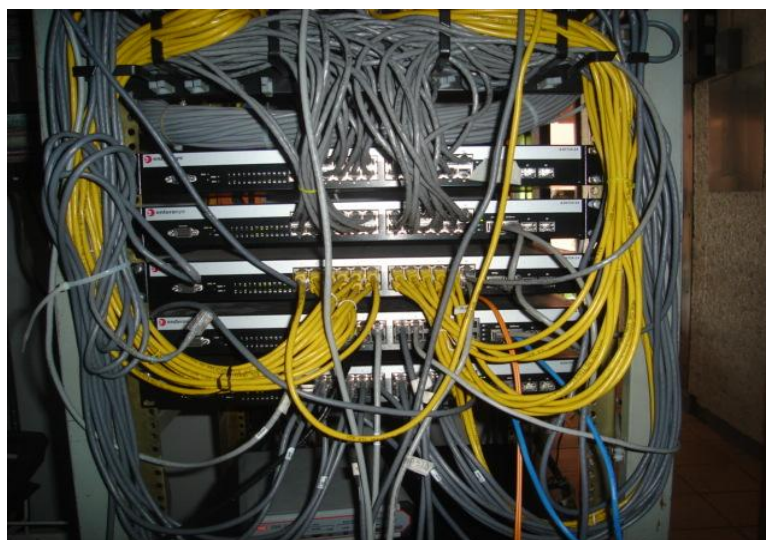


Figura 3.10 Conectividad en Switches de Site norte

### 3.1.3 Compatibilidad entre equipos

Para realizar la tarea de creación de la VLAN (acrónimo de **Virtual LAN**, 'Red de Área Local Virtual) para la red inalámbrica, es necesario señalar que los equipos actuales cumplen con las normas y estándares para dicho fin:

- IEEE 803.1Q. Mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).
- IEEE 803.1P. Es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico.
- IEEE 803.10. Permite al tráfico de la LAN llevar un identificador de VLAN, permitiendo así la conmutación selectiva de paquetes.

### 3.2 Conexión de equipos inalámbricos más robustos

Para distribuir la red inalámbrica se hace la instalación de los equipos Enterasys RoamAbout<sup>1</sup>, los cuales tienen la gran ventaja de poseer un conector adicional a las antenas del propio equipo, para conectar el mismo a una antena externa.

Para evitar pérdidas de señal entre los RoamAbout y las antenas, se colocaron estos lo más cercano posible a las antenas.

---

<sup>1</sup> RoamAbout soluciones Wireless incluyen una amplia variedad de puntos de acceso, controladores, capacidades de gestión, seguridad y software de planificación, así como una plataforma única abierta a la integración de aplicaciones. Reconocido por ofrecer una solución 802.11n completa sin pérdida de la cobertura o la funcionalidad utilizando los 802,3 af PoE (Power over Ethernet) las infraestructuras, RoamAbout Wireless es la más efectiva solución WLAN de energía eficiente y rentable en el mercado hoy.

La solución RoamAbout Wireless:

- Optimiza la distribución de la carga de procesamiento entre el punto de acceso y control para ofrecer un rendimiento excepcional, sin dejar de ser fácil de manejar
- Maneja las funciones complejas, sensibles al tiempo, tales como Calidad de Servicio (QoS), cifrado y gestión de radiofrecuencia por el punto de acceso (AP), mientras que las funciones globales como la configuración, movilidad y control de políticas están centralizadas en el controlador
- Utiliza una innovadora arquitectura híbrida para optimizar la transmisión de tráfico en una base por solicitud de un mejor desempeño y confiabilidad en la alineación con el negocio de las necesidades específicas
- Ofrece una infraestructura de WLAN que se puede ampliar fácilmente con el tiempo para apoyar a las nuevas tecnologías de alto rendimiento y soluciones



**Fig. 3.11 Montaje del punto de acceso RoamAbout.**



**Fig. 3.12 Conexión de antena Sectorial al punto de acceso RoamAbout.**

### 3.2.1 Determinación de puertos de switch para su posterior uso en la VLAN

Se realizó la conexión de los equipos inalámbricos a los puertos establecidos en el switch (ubicado en el site correspondiente), para la implementación de la VLAN de red inalámbrica (puertos 22,23 y 24).

## 3.3 Ubicación de antenas

### 3.3.1 Antena Omnidireccional

Actualmente se cuenta con dos antenas, una de tipo omnidireccional ubicada en el edificio Norte (primer nivel)



**Fig. 3.13 Antena Omnidireccional.**

### 3.3.2 Antena Sectorial

La segunda antena con la que se cuenta, de tipo sectorial ubicada en el edificio, Aulas 4 (primer nivel) mostrada en la figura 3.14 y 3.15.



Fig. 3.15 Antena Sectorial (posterior)

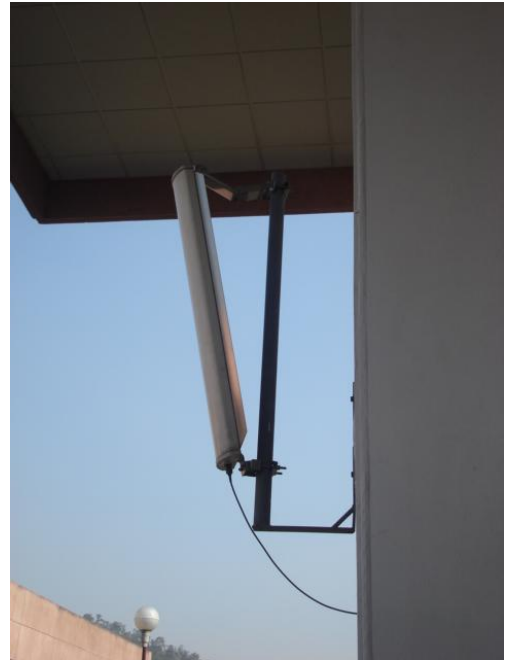


Fig. 3.14 Antena Sectorial

### 3.4 DHCP<sup>2</sup> por servidor

Para mejorar la seguridad en la red tanto inalámbrica como cableada, se implementó un servidor basado en sistema operativo Linux, el cual realiza la función de asignar direcciones IP del tipo 193.168.10.x (Clase C) a la red inalámbrica, además de contar con una interfaz para la captura de las direcciones MAC de los usuarios, esto con dos objetivos:

1. Obligar a que el usuario regrese cada semestre a renovar su acceso a la red inalámbrica

---

<sup>2</sup> **DHCP** (sigla en inglés de **D**ynamic **H**ost **C**onfiguration **P**rotocol - **Protocolo de configuración dinámica de host**) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.



2. Facilidad de detección de equipos sospechosos de generar tráfico excesivo, envío de virus, troyanos y/o gusanos en la red inalámbrica para su consiguiente aislamiento de forma sencilla e inmediata.

Dentro de este nuevo esquema se pensó en dicho servidor, precisamente para no interferir de manera continua en los equipos de switcheo en la captura de las direcciones MAC, sino que mediante la interfaz gráfica del servidor, fuese posible habilitar o deshabilitar las MAC ya capturadas .

#### Conectividad del servidor DHCP

Es necesario señalar que este servidor cuenta con dos tarjetas de red integradas , una de las cuales, tiene una dirección perteneciente al rango institucional, y la otra perteneciente al rango de direcciones privadas para el servicio de la red inalámbrica y a su vez esta última conectada a la VLAN de red inalámbrica y cuya configuración se muestra a continuación:

```

ddns-update-style interim;
option subnet-mask      255.255.255.0;^M
option broadcast-address 123.123.123.255;^M
option routers 123.123.123.1;^M
option domain-name-servers 148.204.103.2, 148.204.103.3,
10.204.221.7, 10.204.103.30, 10.204.103.31, 200.33.146.193;^M
class "lista" {
    match pick-first-value (option dhcp-client-identifier,
hardware);
    }^M
class "tonta" {
    match pick-first-value (option dhcp-client-identifier,
hardware);
    }^M

subclass "lista"      1:00:23:8B:05:A4:7C;^M
subclass "lista"      1:00:21:6B:B7:29:34;    #guru
.
.
.
subclass "tonta"      1:10:23:8B:05:A4:7C;^M

subnet 123.123.123.0 netmask 255.255.255.0{^M
    default-lease-time 60;^M
    max-lease-time 60;^M
    pool {^M
        #deny members of "tonta" ;^M
        allow members of "lista" ;^M
        range 123.123.123.10
123.123.123.110;^M
    }^M

```

Figura 3.16 Configuración de DHCP en Linux

### 3.4.1 Ubicación física

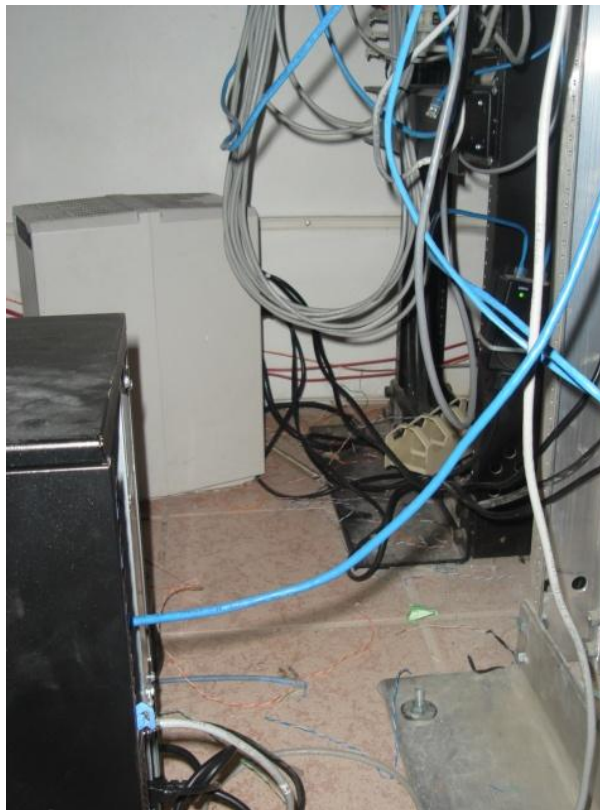
Este servidor se encuentra ubicado en el site sur (edificio Aulas 1) y se encuentra conectado mediante una de sus interfaces, directamente a los switches para poder tener salida a internet, y a la VLAN de red inalámbrica, al puerto 23 del en Switch A2H124-24 en el rack de ese site



Fig. 3.17 Servidor DHCP en Linux



**Fig. 3.18** Conexión de dos tarjetas del Servidor DHCP - Cable Gris conectado a la VLAN de inalámbrica – Cable Azul Conectado al segmento Institucional



**Fig. 3.19** Vista lateral de conexiones del Servidor DHCP

### 3.5 Proceso de registro para usuarios

El proceso de registro de usuarios contempla los siguientes pasos para su registro y alta en la red inalámbrica

## Configuración de acceso a red inalámbrica

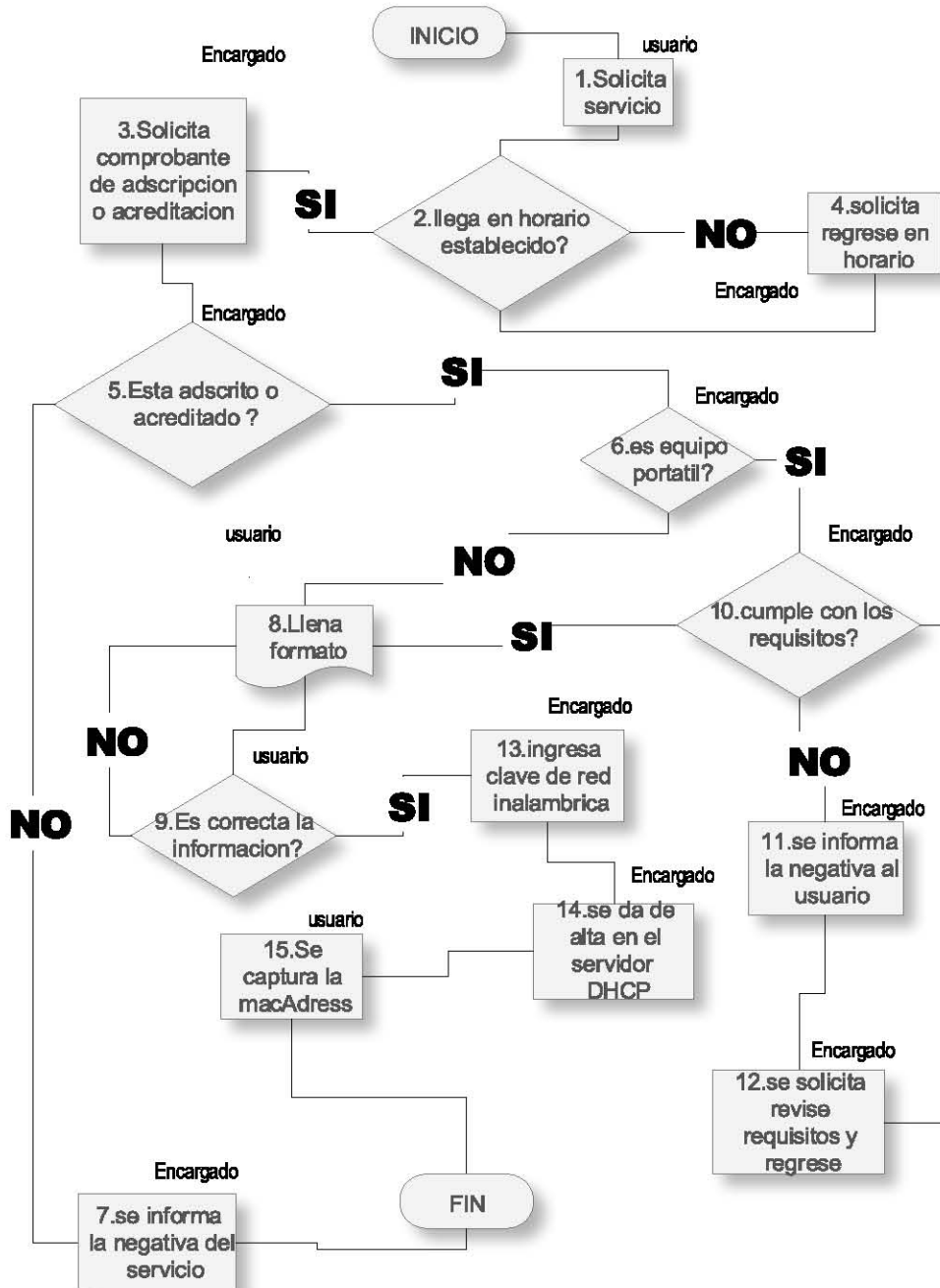


Fig. 3.20 Diagrama de proceso para configuración de Inalámbrica a clientes

Los pasos que se deben cubrir se enlistan de forma más simplificada:

RESPONSABLE	DESCRIPCION DE ACTIVIDADES	FORMATO Y/O DOCUMENTO
Usuario	1.usuario llega a las instalaciones de la Unidad de Informática a solicitar el servicio	
Usuario	3. Se encuentra en el horario establecido? No, sigue paso 4 Si, sigue paso 3	
Técnico docente	3.Solicita comprobante de adscripción o acreditación UPIITA-IPN vigente sigue paso 5	
Técnico docente	4.solicita regrese en el horario establecido y verifique los requisitos solicitados por la unidad de Informática sigue paso 1	
Técnico docente	5. está adscrito el usuario que solicita el servicio? Si, sigue paso 6 No, sigue paso 7	
Técnico Docente	6.el equipo que desea configurar el usuario es portátil? Si, sigue paso 10 No, sigue paso 8	
Técnico Docente	7.se informa al usuario que solamente los alumnos, personal docente y administrativos vigentes en el semestre activo podrán hacer uso de este servicio	
Técnico Docente	8.el usuario llena el formato de servicio inalámbrico a servicios externos correctamente Si, sigue paso 10 No sigue paso 9	Formato de Servicio Inalámbrico a Servicios Externos
Técnico docente	9. Esta correcta la información que el usuario proporcione? Si, sigue paso 13 No, sigue 8	Formato de Servicio Inalámbrico a Servicios Externos
Técnico docente	10. cumple con los requisitos establecidos por la Unidad de Informática? Si, sigue paso 8 No, sigue paso 11	
Técnico docente	11.se informa al usuario que no se le dará el servicio ya que no cumple los requisitos establecidos por la Unidad de Informática	
Técnico docente	13.Se le solicita al usuario que verifique los requisitos y regrese cuando cumpla con todos	
Técnico Docente	13.Ingresa clave de red inalámbrica del equipo del usuario	

Tabla 3.6 Pasos para registro

Al cumplir el usuario con los requisitos de registro, se le solicita llene el formato en el cual se obtienen sus direcciones MAC, tanto Ethernet, como Inalámbrica, llenándolo de acuerdo a las especificaciones mostradas, Tabla 3.7:

<b>Formato de Servicio Inalámbrico a Servicios Externos</b>			
<b>Datos de Usuario</b>		Fecha:	
Nombre: ( 1 )	Apellido Paterno:	Apellido Materno	Telefono: ( 2 )
# Boleta o de Empleado: ( 3 )	Semestre: ( 4 )	Grupo: ( 5 )	e-mail:( 6 )
<b>Datos del Equipo</b>			
Marca: ( 7 )	Modelo: ( 8 )	Ethernet: ( 9 ) 00:00:00:00:00:00	Wireless: ( 10 ) 00:00:00:00:00:00
<b>Sistema Operativo</b>			
Tipo de Sistema: ( 11 )		Versión: ( 12 )	
<b>UDI</b>			
Nombre del Host: ( 13 )		Grupo de Trabajo: ( 14 )	

Tabla 3.7 Formato de registro

- 1.- Anotar nombre completo del usuario que solicita el servicio
- 3.- Anotar número telefónico del usuario que solicita el servicio
- 3.- Anotar numero de boleta o numero de empleado según sea el caso
- 4.- Si es alumno anotar el número de semestre que cursa
- 5.-Si es alumno anotar el grupo a que pertenece
- 6.- Anotar correo electrónico del usuario que solicita el servicio
- 7.- Anotar la marca del equipo que se conectara a la red inalámbrica
- 8.-Anotar el modelo del equipo que se conectara a la red inalámbrica
- 9.- Anotar el número de serie que aparece en ethernet
- 10.-Anotar el número de serie que aparece en tarjeta inalámbrica
- 11.- Anotar el tipo de sistema operativo del equipo a conectar
- 13.- Anotar la versión del sistema operativo del equipo a conectar
- 13.- Anotar el nombre que le pone el usuario
- 14.- Anotar si tiene grupo de llo contrario, no se pone nada

### 3.6 Implementación de VLAN para la red inalámbrica

Recordemos que una VLAN (acrónimo de **Virtual LAN**, ‘red de área local virtual’) es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLAN's pueden coexistir en un único switch físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local que no deberían intercambiar datos usando la red local.

Bajo este concepto, estamos aislando a los usuarios de la red inalámbrica y de esta forma cubriendo varios puntos como el robo o clonación de direcciones IP del segmento institucional, la infiltración de usuarios hacia la red de la unidad, la propagación de virus desde los usuarios de inalámbrica a los usuarios de la red cableada, todos estos mencionados como principales problemas de Inseguridad.

#### 3.6.1 Equipos, puertos Involucrados y configuración

Los equipos inalámbricos Enterasys RoamAbout se configuran en un principio desde modo consola para establecer la adquisición de una dirección IP via DHCP, y posteriormente se configuró la activación de HTTP, por cuestión de facilidad, única y exclusivamente para configuración en modo gráfico, al término de esta, se deshabilitará el modo de configuración por HTTP.

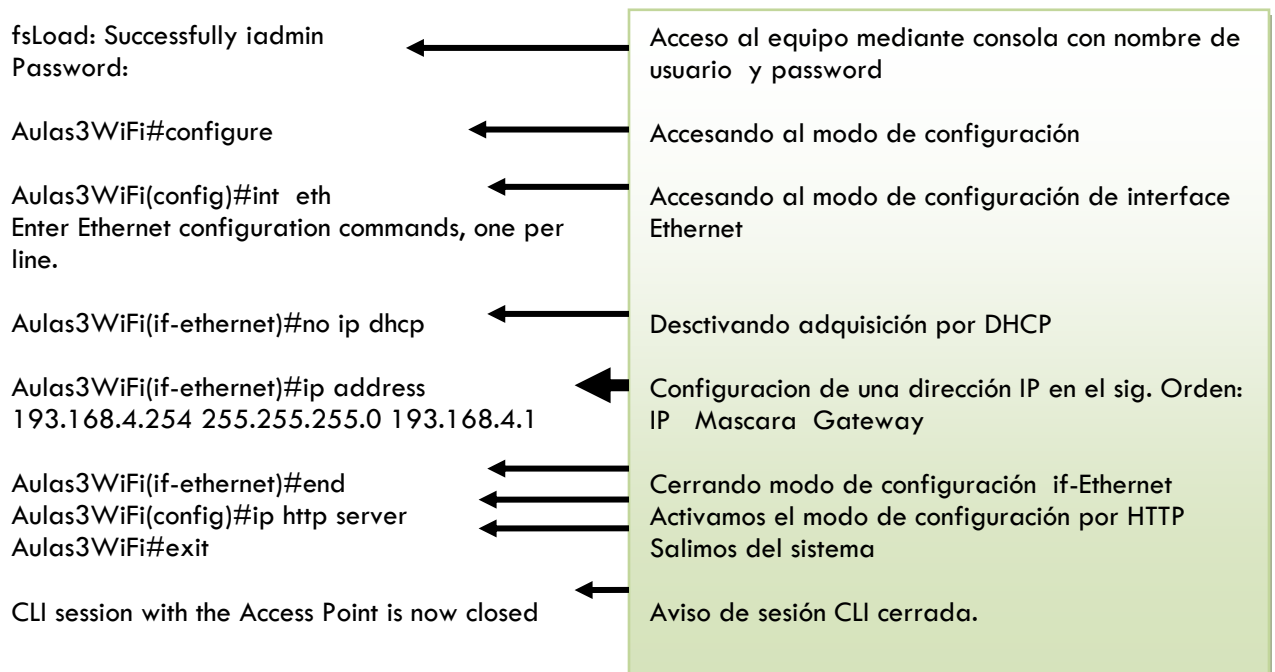
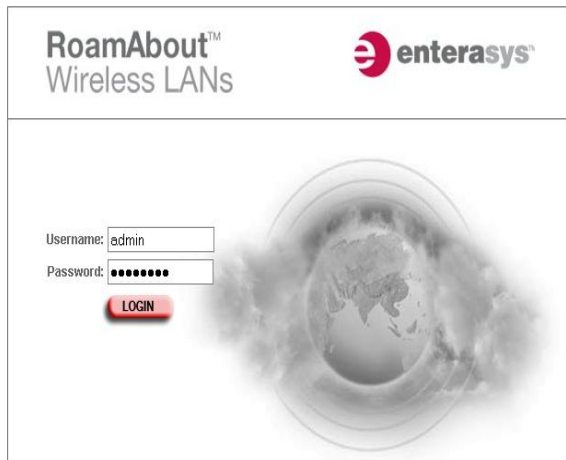


Fig. 3.21 Configuración inicial del punto de acceso.

De esta forma fue posible establecer algunas configuraciones mediante HTTP.



Como podemos observar se hace el acceso mediante el usuario y Password del equipo, de forma inmediata nos solicita algunos datos para identificación del mismo y contacto con el responsable.

Fig. 3.22 Identificación y contacto para el A.P.

Al pasar a la configuración de TCP/IP, además de observar la ip ya establecida, también se le asigno como servidores de DNS, la dirección del servidor que fungirá como DHCP (en Linux.)

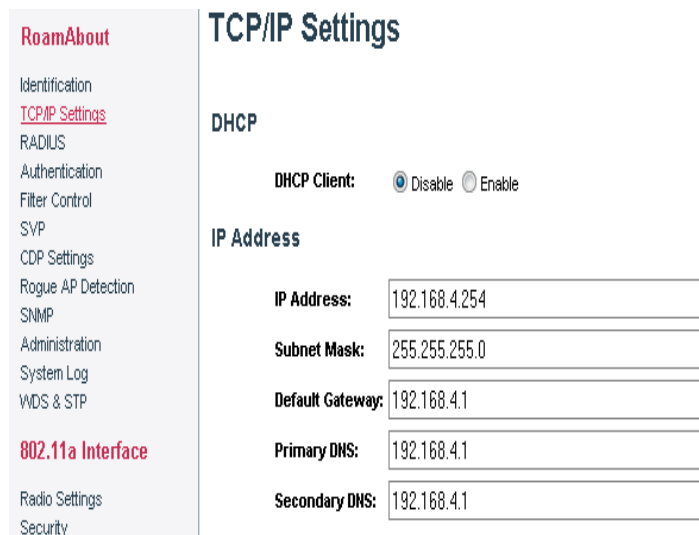
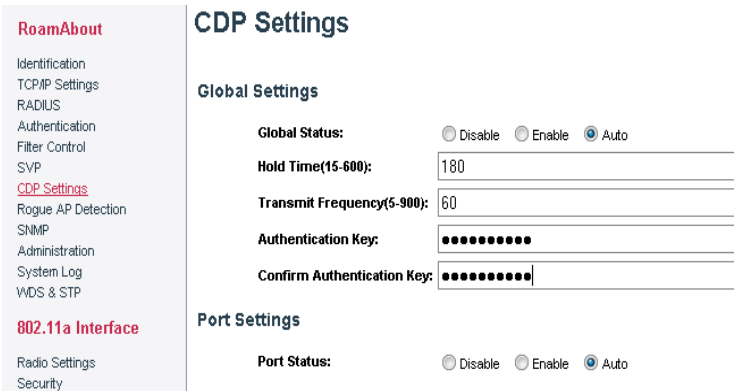


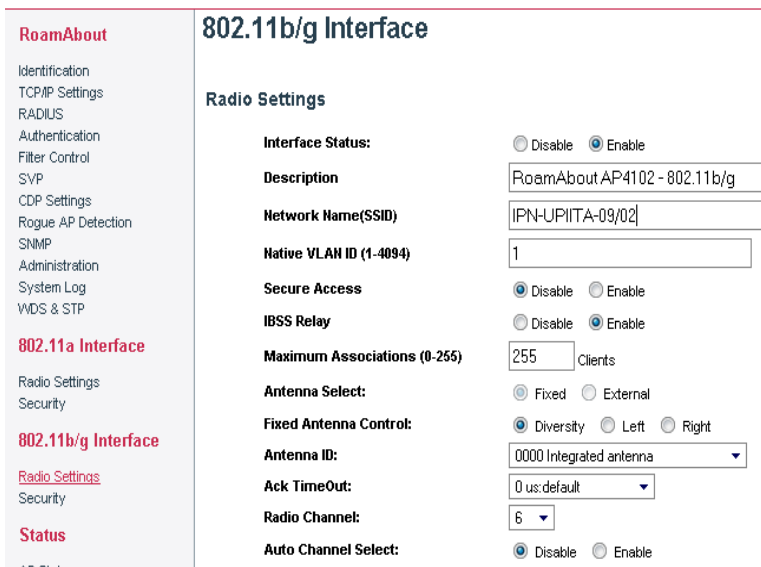
Fig. 3.23 Asignación de DNS para el A.P.





Del mismo modo, ajustamos ahora la clave de autenticación, para el acceso de los usuarios a la red inalámbrica.

Fig. 3.24 Creación de Clave Autenticación



Ahora, se le asigna el nombre para la SSID, y sea más práctico hallar la red inalámbrica de la UPIITA, además de que en cada equipo se vario el valor del canal, para evitar conflictos por interferencias entre los mismos equipos.

Fig. 3.25 Configuración de SSID

Se solicita entonces al sistema que muestre el status, en donde, entre otras cosas se muestra información del AP, su MAC, IP y servicios habilitados.

AP System Configuration

Serial Number	08160156236A
System Up Time	0 days, 0 hours, 26 minutes, 13 seconds
MAC Address	00-11-88-BF-B0-4B
System Name	IPN-UPITA-09/02
System Contact	Oscar Hernandez 56812
IP Address	192.168.4.254
IP default-gateway	192.168.4.1
HTTP Server	ENABLED
HTTP Server Port	80
HTTPS Server	ENABLED
HTTPS Server Port	443
Version	V1.1.51

Fig. 3.26 Vista de parámetros

The screenshot shows the configuration page for the AP. On the left is a navigation menu with categories like Identification, TCP/IP Settings, and Status. The main content area is divided into several sections:

- DHCP**: DHCP Client is set to  Disable.
- IP Address**: IP Address is 192.168.4.254, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.4.1, Primary DNS is 192.168.4.1, and Secondary DNS is 192.168.4.1.
- Web Servers**: HTTP Server is  Disable, HTTP Port is 80, HTTPS Server is  Disable, and HTTPS Port is 443.
- Telnet & SSH Settings**: Telnet Server is  Disable, SSH Server is  Enable, and SSH Port is 22.

Finalmente por seguridad se deshabilita el acceso a la configuración vía HTTP, Telnet, y únicamente se permitirá el acceso vía SSH, ya que una vez instalados los equipos, cualquier configuración se realizará vía remota.

Fig. 3.27 Desactivación de HTTP

### 3.6.2 Configuración de VLAN

Para la generación de la VLAN inalámbrica se usaron equipos Enterasys A2H124-24 y se usara una VLAN por puerto , asignando los puertos 22, 23 y 24 en los switches ubicados en el edificio Aulas 4 y el edificio Sur (aulas 1) , a continuación se muestra su configuración:

```

Edificio Aulas 3 (su)->set VLAN create 1001
Edificio Aulas 3 (su)->set VLAN name wireless

Edificio Aulas 3 (su)->show VLAN 1001

VLAN: 1001          NAME: wireless
VLAN Type: Permanent
Egress Ports
None.
Forbidden Egress Ports
None.
Untagged ports
None.

Edificio Aulas 3 (su)->set port VLAN fe.1.22 1001 modify-egress
Edificio Aulas 3(su)->show VLAN

VLAN: 1            NAME: DEFAULT VLAN
VLAN Type: Default
Egress Ports
fe.1.21, ge.1.28, fe.3.7-8, fe.3.10-15, fe.3.17-21, fe.4.2-3, fe.4.6, fe.4.8, fe.4.11-
12, fe.4.14, fe.4.19-20, fe.5.2, fe.5.5, fe.5.7-9, fe.5.11-12, fe.5.14, fe.5.16, fe.5.18,
fe.5.20
Forbidden Egress Ports
None.
Untagged ports
fe.1.21, ge.1.28, fe.3.7-8, fe.3.10-15, fe.3.17-21, fe.4.2-3, fe.4.6, fe.4.8, fe.4.11-
12, fe.4.14, fe.4.19-20, fe.5.2, fe.5.5, fe.5.7-9, fe.5.11-12, fe.5.14, fe.5.16, fe.5.18,
fe.5.20

VLAN: 1001         NAME: wireless
VLAN Type: Permanent
Egress Ports
fe.1.22, ge.1.28
Forbidden Egress Ports
None.
Untagged ports
fe.1.22

VLAN: 1002         NAME: Zinred
VLAN Type: Permanent
Egress Ports
ge.1.28
Forbidden Egress Ports
None.
Untagged ports
None.

Edificio Aulas 3(su)->

```

Fig. 3.28 Creación de VLAN y asignación de puertos

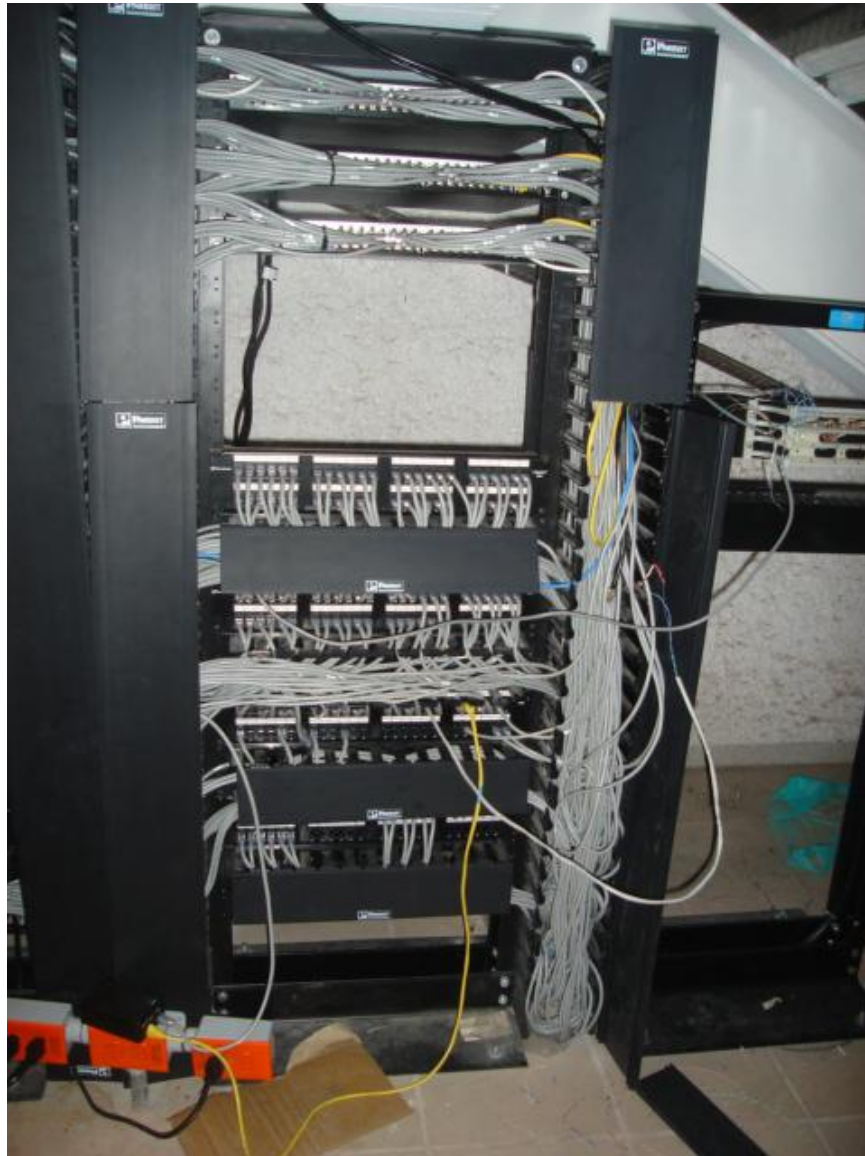


Fig. 3.29 Switches empleados para configuración de VLAN

### 3.7 Pruebas en Campo

Desde diferentes puntos en la unidad y mediante el uso del comando PING se trató de llevar a cabo la comunicación con otros equipos y servicios fuera de la VLAN de la red inalámbrica.

También, directamente en los equipos se hizo la prueba utilizando el mismo comando, pero conectado a otro puerto fuera de los especificados para esta red (22,23

y24) y ahora en sentido opuesto, es decir, tratando de comunicarse con algún equipo de la red inalámbrica, desde la red cableada.

### 3.8 Situación actual

El trabajo realizado es la fase inicial de la reestructuración y diseño de la parte correspondiente a la red inalámbrica, por lo que la cobertura actual se muestra en el esquema y actualmente quedan un par de AP's comerciales para brindar servicio a ciertas áreas, los cuales se pretende reemplazar a corto plazo para homogeneizar la red tanto alámbrica e inalámbrica y cubrir los puntos de seguridad detectados para este esquema.

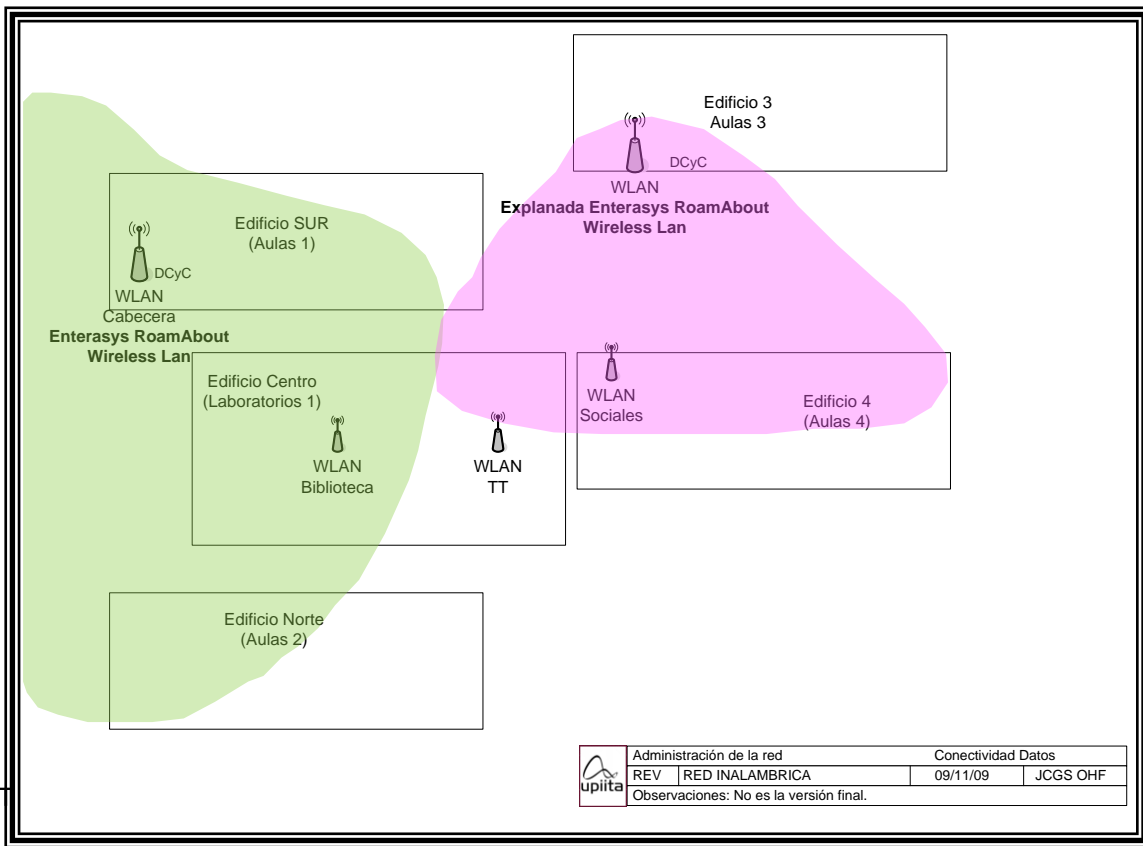


Fig. 3.30 Análisis de huellas de alcance inalámbrico

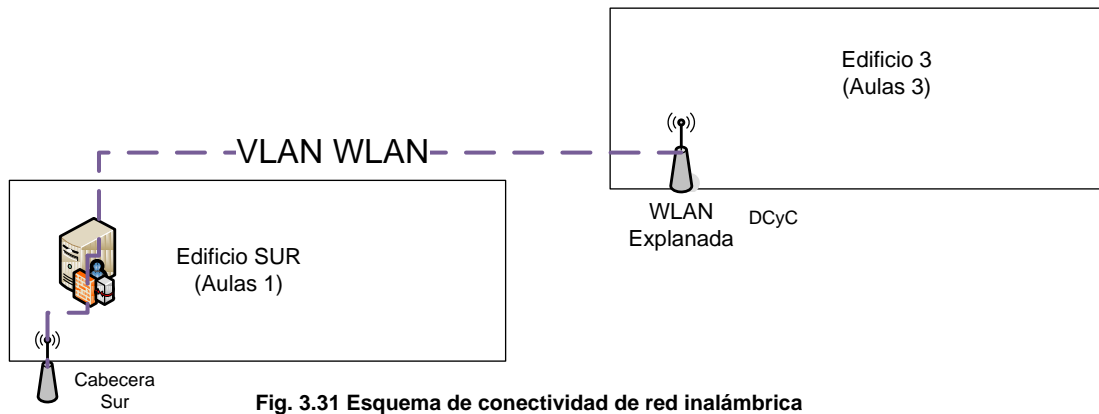


Fig. 3.31 Esquema de conectividad de red inalámbrica

Con el uso del servidor DHCP para fácil manejo de las direcciones MAC (ENA/DISABLE) la tarea de capturar direcciones MAC en los switches y cada vez que haya un cambio en la configuración de la clave WEP, dado que en su mayoría, los usuarios de la inalámbrica son los mismos, más los que se incrementan cada semestre por lo que simplemente se activa o desactiva el acceso al servicio de las direcciones MAC indicadas por el administrador, por lo que incluso sería factible publicar la clave WEP de la red inalámbrica sin temor a ser evadidos por los usuarios o tener accesos no deseados ya que todo quedara en función de la MAC registrada y activada para este servicio.

## Conclusiones

Como toda red, no se ha concluido el proceso de expansión, por la razón que está en continuo crecimiento, y aunque la implementación de la VLAN para la red inalámbrica es satisfactoria, aun faltan áreas por cubrir, por lo que este proceso se seguirá llevando a cabo en cuanto se cuenten con los recursos para instalar más antenas en otros puntos clave de la unidad.

Además, la implementación de VLANs se pretende llevar a cabo no solo para los servicios de inalámbrico, sino para todas las áreas, jefaturas y subdirecciones, con el fin de separar el tráfico de cada zona y disminuir y aislar conflictos de conectividad.

La configuración primariamente la realizamos por el puerto de consola, directamente del equipo, porque al tratar de usar las interfaces Web del Vertical Horizont, encontramos dificultades del tiempo de vida de la sesión, además de la autenticación por Web es muy lenta y no muestra bien los resultados. Por esto recomendamos que las sesiones de trabajo inicial o de configuración de muchos parámetros se realicen directamente en el equipo y las actualizaciones o modificaciones menores se realicen por la interfase Web.

Un detalle importante que encontramos al estar configurando el equipo, fue un menú de configuración de seguridad el cual nos permitió adicionar seguridad por medio de autenticación a cada uno de los puestos del equipo. Esto se conjuntó con las VLANs creadas para cumplir cabalmente con los requerimientos del departamento de cómputo y comunicaciones de la escuela de la siguiente forma:

- Las direcciones IP pertenecen a una VLAN para evitar servicios de red en colisión
- Las direcciones IP especifican a cada uno de los equipos al que pertenecen y se lleva un registro de los mismos
- La autenticación de puertos controla la cantidad de equipos a los que se les puede dar servicio

- La autenticación de equipos evita la entrada de computadoras a la red sin un registro previo.

Las VLANs dan libertad a los usuarios de consolidar servicios de prueba, sin que entren en conflicto con otras áreas de la unidad





## Glosario de términos

### A

**AI Artificial Intelligence.** Inteligencia Artificial. Parte de la informática que estudia la simulación de la inteligencia.

**Access Provider** Proveedor de Acceso Centro servidor que da acceso lógico a Internet, es decir sirve de pasarela (Gateway) entre el usuario final e Internet.

**ACK Acknowledgment.** Reconocimiento. Señal de respuesta.

**ADSL Asymmetric Digital Subscriber Line.** Línea Digital Asimétrica de Abonado. Sistema asimétrico de transmisión de datos sobre líneas telefónicas convencionales. Existen sistemas en funcionamiento que alcanzan velocidades de 1,5 y 6 Megabits por segundo en un sentido y entre 16 y 576 Kilobits en el otro.

**ANSI American National Standard Institute.** Instituto Nacional Americano de Estándar.

**API Application Program Interface.** Interfaz de Aplicación del Programa. Es el conjunto de rutinas del sistema que se pueden usar en un programa para la gestión de entrada/salida, gestión de ficheros etc.

**APPLET** Aplicación escrita en JAVA y compilada.

**Archie** Software utilizado para localizar archivos en servidores FTP. A partir de 1994 ha caído en desuso debido a la aparición del WWW, o Web.

**ARPA Advanced Research Projects Agency.** Agencia de Proyectos de Investigación Avanzada.

**ARPANET Advanced Research Projects Agency Network.** Red de la Agencia de Proyectos de Investigación Avanzada. Red militar Norteamericana a través de líneas telefónicas de la que posteriormente derivó Internet.

**ASAP As Soon As Possible.** Tan Pronto Como Sea Posible. Mandato u opción en una red o programa que determina la prioridad de una tarea.

**ASCII. American Standard Code for Information Interchange.** Estándar Americano para Intercambio de Información. La tabla básica de caracteres ASCII esta compuesta por 128 caracteres incluyendo símbolos y caracteres de control. Existe una versión extendida de 256

**ASN Autonomus System Number.** Número de sistema autónomo. Grupo de Routers y redes controlados por una única autoridad administrativa.

**ATM Asynchronous Transmission Mode.** Modo de Transmisión Asíncrona. Sistema de

transmisión de datos usado en banda ancha para aprovechar al máximo la capacidad de una línea. Se trata de un sistema de conmutación de paquetes que soporta velocidades de hasta 1,2 Gbps. Implementación normalizada (por ITU) de Cell Relay, técnica de conmutación de paquetes que utiliza celdas de longitud fija.

**AUI** Asociación de usuarios de Internet.

**Avatar** Identidad representada gráficamente que adopta un usuario que se conecta a un CHAT con capacidades gráficas.

### B

**Backbone** Estructura de transmisión de datos de una red o conjunto de ellas en Internet. Literalmente: "columna vertebral"

**Bandwith Ancho de Banda.** Capacidad de un medio de transmisión.

**BBS Bulletin Board System.** Tablero de Anuncios Electrónico. Servidor de comunicaciones que proporciona a los usuarios servicios variados como e-mail o transferencia de ficheros. Originalmente funcionaban a través de líneas telefónicas normales, en la actualidad se pueden encontrar también en Internet.

**Ban Prohibir.** Usado normalmente en IRC. Acto de prohibir la entrada de un usuario "NICK" a un canal.

**Baud Baudio.** Unidad de medida. Número de cambios de estado de una señal por segundo.

**BIOS Basic Input Output System.** Sistema Básico de Entrada/Salida. Programa residente normalmente en Eprom que controla la iteraciones básicas entre el hardware y el Software.

**BIT Binary Digit.** Dígito Binario. Unidad mínima de información, puede tener dos estados "0" o "1".

**BITNET Because It's Time NETWORK.** Porque es tiempo de red. Red internacional de computadoras de instituciones educativas. Esta red está conectada a Internet y algunas de las herramientas más comunes hoy en día, como los servidores de correo Listservs, se originaron en ella. Actualmente está en proceso de desaparición conforme sus miembros se integran a Internet.

**Bookmark Marca.** Anotación normalmente de una dirección WWW o URL que queda archivada para su posterior uso.

**BOOTP Bootstrap Protocol.** Protocolo de Arranque-Asignación. Proporciona a una máquina una dirección IP, Gateway y Netmask. Usado en comunicaciones a través de línea telefónica.

**BOT Automatismo**, programa o script que realiza funciones que de otra manera habría que hacer de forma manual.

**Bounce Rebote**. Devolución de un mensaje de correo electrónico debido a problemas para entregarlo a su destinatario.

**BPDU**: Bridge Protocol Data Unit (ISO/IEC 15802-3)

**BPS Bits per second**. Bits por segundo. Medida de la velocidad de transmisión de datos en la transmisión en serie.

**Bridge**. Puente. Dispositivo que interconecta redes de área local (LAN) en la capa de enlace de datos OSI. Filtra y retransmite tramas según las direcciones a Nivel MAC.

**Browser. Navegador**. Término aplicado normalmente a los programas que permiten acceder al servicio WWW.

**BUS. Vía o canal de Transmisión**. Típicamente un BUS es una conexión eléctrica de uno o más conductores, en el cual todos los dispositivos ligados reciben simultáneamente todo lo que se transmite

## C

**Callback** Sistema muy empleado en EE.UU. para llamadas internacionales consistente en (previo abono) llamar a un Tlf. indicar el número con el que queremos contactar y colgar. Posteriormente se recibe una llamada que nos comunica con el número deseado.

**Carrier** Operador de Telefonía que proporciona conexión a Internet a alto nivel.

Caudal Cantidad de ocupación en un ancho de banda. Ejp. En una línea de 1Mbps. puede haber un caudal de 256Kbps. con lo que los 768Kbps. restantes de el ancho de banda permanecen desocupados.

**CCITT**. International Consultative Committee on Telegraphy and Telephony. Comité Consultivo de Telegrafía y Telefonía. Organización que establece estándares internacionales sobre telecomunicaciones.

**CD. Compact Disc**. Disco Compacto. Disco Optico de 12 cm de diámetro para almacenamiento binario. Su capacidad "formateado" es de 660 Mb. Usado en principio para almacenar audio. Cuando se usa para almacenamiento de datos genéricos es llamado CD-ROM.

**CDA**. Communications Decency Act. Acta de decencia en las Telecomunicaciones. Proyecto de ley americano que pretendía ejercer una especie de censura sobre Internet. Por el momento ha sido declarado anticonstitucional.

**CERN. Conseil Europeen pour la Recherche Nucleaire**. Consejo Europeo para la Investigación Nuclear. Institución europea que desarrolló, para sus necesidades internas, el primer navegador y el primer servidor WWW. Y por tanto el HTTP. Ha contribuido decisivamente a la difusión de esta tecnología y es uno de los rectores del W3 Consortium

**CERT. Computer Emergency Response Team**. Equipo de Respuesta a Emergencias Informáticas.

**CFI**: Canonical Format Indicator

**CG. Computer Graphics**. Gráficos de Computador.

**CGI Common Gateway Interface**. Interfaz de Acceso Común. Programas usados para hacer llamadas a rutinas o controlar otros programas o bases de datos desde una página Web. También pueden generar directamente HTML.

**CHAT** Charla. Ver IRC.

**CIR Committed Information Rate**. Es el Caudal mínimo de información que garantiza el operador telefónico al cliente (normalmente el proveedor de acceso) el resto del ancho de banda esta pues sujeto al estado de la red y las necesidades del operador telefónico.

**CIX Comercial Internet Exchange**. Intercambio Comercial Internet.

**Codificación del Control Lógico de Control (LLC)** usado del direccionamiento LLC de la trama como un protocolo asociado con el Servicio de la trama de transporte de datos de la MAC.

**Connection Provider** Proveedor de Conexión Entidad que proporciona y gestiona enlace físico a Internet

**COOKIE** Pequeño trozo de datos que entrega el programa servidor de HTTP al navegador WWW para que este lo guarde. Normalmente se trata de información sobre la conexión o los datos requeridos, de esta manera puede saber que hizo el usuario en la ultima visita.

**Cracker** Individuo con amplios conocimientos informáticos que desprotege/piratea programas o produce daños en sistemas o redes.

**CSLIP Compressed Serial Line Protocol**. Protocolo de Línea Serie Comprimido. Es una versión mejorada del SLIP desarrollada por Van Jacobson. Principalmente se trata de en lugar de enviar las cabeceras completas de los paquetes enviar solo las diferencias.

**CSMA Carrier Sense Multiple Access**. Acceso Múltiple por Detección de Portadora. Protocolo de Red para compartir un canal. Antes de transmitir la estación emisora comprueba si el canal esta libre.

**CSMA/CD Carrier Sense Multiple Access / Collision Detection.** Detección de portadora de acceso múltiple / colisión. En este protocolo las estaciones escucha al bus y sólo transmiten cuando el bus está desocupado. Si se produce una colisión el paquete es transmitido tras un intervalo (time-out) aleatorio.

## D

**DATAGRAM Datagrama.** Usualmente se refiere a la estructura interna de un paquete de datos.

**DCD Data Carrier Detected.** Detectada Portadora de Datos.

**DCE Data Communication Equipment.** Equipo de Comunicación de Datos

**DDE Dynamic Data Exchange.** Intercambio Dinámico de Datos. Conjunto de especificaciones de Microsoft para el intercambio de datos y control de flujo entre aplicaciones.

**DES Data Encryption Standard.Algoritmo de Encriptacion de Estándar.** Algoritmo desarrollado por IBM, utiliza bloques de datos de 64 bits y una clave de 56 bits. Es utilizado por el gobierno americano.

**Dialup Marcar.** Establecer una conexión de datos a traves de una línea telefónica.

**DNS Domain Name System.** Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1

**Domain Dominio.** Sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. eej: mercadeo.com

**Download Literalmente "Bajar Carga".** Se refiere al acto de transferir un fichero/s desde un servidor a nuestro computador. En español: " bajarse un programa "

**Downsizing.** El concepto de "downsizing" en computación, cuya traducción mas lógica podría ser la de "integración hacia micros", es la interconexión de redes de microcomputadoras con mini computadoras y computadoras de orden principal.

**DownStream** Flujo de datos de un computador remoto al nuestro.

**DS-3. Digital Signal 3.** Señal Digital Jerarquía 3 (45 Mbps para un T3).

**DSP Digital Signal Procesor.** Procesador Digital de Señal.

**DSR Data Set Ready (MODEM).**

**DTE Data Terminal Equipment.** Equipo Terminal de Datos. Se refiere por ejemplo al

computador conectado a un modem que recibe datos de este.

**DTMF Dual Tone Multifrequency.** Multi frecuencia de doble tono. Son los tonos que se utilizan en telefonía para marcar un número telefónico.

**DTR Data Transfer Ready.** Preparado para Transmitir Datos (MODEM).

**DUPLEX** Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir/transmitir. Existen dos modalidades HALF-DUPLEX: Cuando puede recibir y transmitir alternativamente y FULL-DUPLEX cuando puede hacer ambas cosas simultáneamente.

**DVB Digital Video Broadcast.** video Digital para Emisión. Formato de video digital que cumple los requisitos para ser considerado Broadcast, es decir, con calidad para ser emitido en cualquiera de los sistemas de televisión existentes.

**DVD Digital Video Disk.** Nuevo estándar en dispositivos de almacenamiento masivo con formato de CD pero que llega a 14 GB de capacidad.

## E

**EBCDIC Extended Bynary Coded Decimal Interchange Code.** Código Extendido de Binario Codificado Decimal. Sistema mejorado de empaquetamiento de números decimales en sistema binario.

**ECC Error Checking and Correction.** Chequeo y Corrección de errores.

**EFF Electronic Frontier Foundation.** Fundación Frontera Electrónica. Organización para la defensa de los derechos en el Cyberspacio.

**EIA Electronics Industry Association.** Organismo responsable de publicar normas RS (Recommended Standars), relacionadas con la comunicación entre computadoras y terminales. (Ej: RS-232)

**E-ISS:** Enhanced Internal Sublayer Service

**E-mail Electronic Mail.** Correo Electrónico. Sistema de mensajería informática similar en muchos aspectos al correo ordinario pero muchísimo más rápido.

**EPROM.** Erasable Programmable Read Only Memory. Memoria borrable programable sólo de lectura.

**Ethernet.** Diseño de red de área local normalizado como IEEE 802.3. Utiliza transmisión a 10 Mbps por un bus Coaxial. Método de acceso es CSMA/CD.

**ETSI European Telecommunication Standards Intitute.** Instituto Europeo de Estándares en Telecomunicaciones.

**E-ZINE Electronic Magazine.** Revista Electrónica. Cualquier revista producida para su difusión por medios informáticos, principalmente por Internet.

## F

**FAQ Frequent Asked Question.** Preguntas Formuladas Frecuentemente. Las "faqs" de un sistema son archivos con las preguntas y respuestas más habituales sobre el mismo.

**FAT File Allocation Table.** Tabla de Localización de Ficheros. Sistema de organización de ficheros en discos duros. Muy usado en PC.

**FCS:** Frame Check Sequence

**FDDI Fiber Digital Device Interface.** Dispositivo Interface de Fibra (óptica) Digital.

**Finger. Literalmente "dedo".** Facilidad que permite averiguar información básica sobre usuarios de Internet o Unix.

**FID:** Filter Identifier

**FIX. Federal Interagency eXchange.** Interagencia Federal de Intercambio.

**Firewall.** Cortina de Fuego. Router diseñado para proveer seguridad en la periferia de la red. Se trata de cualquier programa que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.

**Frame. Estructura.** También trama de datos. Grupo de bits transmitido de manera serial sobre un canal de comunicación. En Browsers de WWW como Netscape se refiere a una estructura de sub-ventanas dentro de un documento HTML.

**Frame Relay.** Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

**Frame Relay** la función de Forwarding Process que envía las tramas siguiendo los puertos de un Switch.

**FTP. File Transfer Protocol.** Protocolo de Transferencia de Archivos. Uno de los protocolos de transferencia de ficheros mas usado en Internet.

**Full Duplex.** Circuito o dispositivo que permite la transmisión en ambos sentidos simultáneamente.

**FXO. Foreign Exchange Office.** Central Externa. Voz que emula una extensión de PABX tal como aparece ante la central telefónica para la conexión de una PABX a un multiplexor.

## G

**GARP:** Generic Attribute Registration Protocol (ISO/IEC 15802-3)

**Gateway. Pasarela.** Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

**GID:** GARP Information Declaration (ISO/IEC 15802-3)

**GIF Graphics Interchange Format.** Formato Grafico de Intercambio.

**GIP:** GARP Information Propagation (ISO/IEC 15802-3)

**GIX Global Internet Exchange.** Intercambio Global Internet.

**GMRP:** GARP Multicast Registration Protocol

**GMT Greenwich Mean Time.** Hora de Referencia de Greenwich. Equivalente a UT.

**Gopher.** Nombre dado en Internet al servicio de rastreo de información organizado en menús jerarquizados

**GSM Global System Mobile communications.**

Sistema Global de Comunicaciones Móviles. Sistema digital de telecomunicaciones principalmente usado para telefonía móvil. Existe compatibilidad entre redes por tanto un teléfono **GSM** puede funcionar teóricamente en todo el mundo. En EE.UU. esta situado en la banda de los 1900MHZ y es llamado DCS-1900.

**GT Global Time. Tiempo Global.** Sistema horario de referencia en Internet.

**GUI Graphic User Interface.** Interfase Gráfico de Usuario.

**GVRP:** GARP VLAN Registration Protocol

## H

**Hacker** Experto en informática capaz de de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

**Hardware.** A los componentes que es posible ver y tocar se les llama en jerga computacional "hardware", palabra inglesa cuyo significado es máquina o "cosa dura".

**Half Duplex.** Un circuito que permite de manera alternante la transmisión y la recepción de señales, pero no de manera simultánea.

**Hayes.** Norma desarrollada por el fabricante Hayes para el control de modems mediante comandos.

**HDLC High-Level Data Link Control.** Control de Enlace de Datos de Alto Nivel. Es un protocolo orientado al bit.

**HDSL High bit rate Digital Subscriber Line.** Línea Digital de Abonado de alta velocidad. Sistema de transmisión de datos de alta velocidad que utiliza dos pares trenzados. Se consiguen velocidades superiores al Megabit en ambos sentidos.

**Header Cabecera.** Primera parte de un paquete de datos que contiene información sobre las características de este.

**Hit.** Se usa para referirse a cada vez que un link es pulsado en una página WEB. Literalmente "golpe".

**Homepage.** Página principal o inicial de un sitio WEB.

**Host. Anfitrión.** Computador conectado a Internet. Computador en general.

**HPFS High Performance File System.** Sistema de Archivos de Alto Rendimiento. Sistema que utiliza el OS/2 opcionalmente para organizar el disco duro en lugar del habitual de FAT.

**HTML HyperText Markup Language.** Lenguaje de Marcas de Hipertexto. Lenguaje para elaborar paginas Web actualmente se encuentra en su versión 3. Fue desarrollado en el CERN.

**HTTP HyperText Transfer Protocol.** Protocolo de Transferencia de **Hypertexto**. Protocolo usado en WWW.

## I

**IANA Internet Assigned Number Authority.** Autoridad de Asignación de Números en Internet. Se trata de la entidad que gestiona la asignación de direcciones IP en Internet.

**ICMP Internet Control Message Protocol.** Protocolo Internet de Control de Mensajes.

**IEEE Institute of Electrical and Electronics Engineers.** Instituto de Ingenieros Eléctricos y Electrónicos. Asociación Norteamericana. IEEE 802.3 Protocolo para la red LAN de la IEEE que especifica una implementación del nivel físico y de la subcapa MAC, en la capa de enlace de datos. El IEEE 802.3 utiliza CSMA/CD a una variedad de velocidades de acceso sobre una variedad de medios físicos. Extensiones del estándar IEEE 802.3 especifica implementaciones para Fast Ethernet.

**IETF Internet Engineering Task Force.** Grupo de Tareas de Ingeniería de Internet. Asociación de técnicos que organizan las tareas de ingeniería principalmente de telecomunicaciones en Internet. Por ejemplo: mejorar protocolos o declarar obsoletos otros.

**INDEPENDENT VLAN LEARNING (IVL):** configuración y operación del proceso de aprendizaje y filtraje de la Base de Datos semejante para una configuración de VLANs, si

se da una dirección MAC individual es aprendida en una VLAN, esta información no es usada para encaminar o tomar decisiones de filtrado debido a que las direcciones están relativamente en otra VLAN configurada.

**Independent VLAN Learning (IVL) Bridge** un tipo de puenteo que solo soporta aprendizaje de VLAN Independiente.

**INTERNET.** Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.

**INTERNIC** Entidad administrativa de Internet que se encarga de gestionar los nombres de dominio en EE.UU.

**INTRANET** Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW. IP Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de internet. También se refiere a las direcciones de red Internet.

**IPI Intelligent Peripheral Interface.** Interface Inteligente de Periféricos. En ATM: Initial Protocol Identifier. identificador Inicial de Protocolo.

**IPX Internet Packet Exchange.** Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

**IRC Internet Relay Chat. Canal de Chat de Internet.** Sistema para transmisión de texto multiusuario a través de un servidor IRC. Usado normalmente para conversar on-line también sirve para transmitir ficheros.

**ISDN Integrated Services Digital Network.** Red Digital de Servicios Integrados. Servicio provisto por una empresa de comunicaciones que permite transmitir simultáneamente diversos tipos de datos digitales conmutados y voz.

**ISO International Standard Organization.** Organización Internacional de Estándares.

**ISP Internet Service Provider.** Proveedor de Servicios Internet.

**ISS Internet Security Scanner.** Rastreador de Seguridad de Internet. Programa que busca puntos vulnerables de la red con relación a la seguridad.

**ISS:** Internal Sublayer Service (Clause 7, ISO/IEC 15802-3)

**ITU International Telecommunications Union.** Unión Internacional de Telecomunicaciones. Forma parte de la CCITT. Organización que desarrolla estándares a nivel mundial para la tecnología de las telecomunicaciones.

**IVL:** Independent VLAN Learning

## J

**JAVA** Lenguaje de programación orientado a objeto parecido al C++. Usado en WWW para la tele carga y tele ejecución de programas en el computador cliente. Desarrollado por Sun microsystems.

**JAVASCRIPT** Programa escrito en el lenguaje script de Java que es interpretado por la aplicación cliente, normalmente un navegador (Browser).

**JPEG Join Photograph Expert Group.** Unión de Grupo de Expertos Fotográficos. Formato gráfico con perdidas que consigue elevados ratios de compresión.

## K

**Kick "Patada".** Usado normalmente en IRC. Acto de echar a un usuario de un canal.

**Knowbot** Robot de conocimiento o robot virtual. Se trata de un tipo de PDA.

## L

**LAN Local Area Network. Red de Área Local.** Una red de área local es un sistema de comunicación de alta velocidad de transmisión. Estos sistemas están diseñados para permitir la comunicación y transmisión de datos entre estaciones de trabajo inteligentes, comúnmente conocidas como Computadoras Personales. Todas las PCs, conectadas a una red local, pueden enviar y recibir información. Como su mismo nombre lo indica, una red local es un sistema que cubre distancias cortas. Una red local se limita a una planta o un edificio.

**LAPM Link Access Procedure for Modems.** Procedimiento de Acceso a Enlace para Modems.

**Layer Capa.** En protocolos o en OSI se refiere a los distintos niveles de estructura de paquete o de enlace respectivamente.

**LCP Link Control Protocol.** Protocolo de Control de Enlace

Link Enlace. Unión. Se llama así a las partes de una página WEB que nos llevan a otra parte de la misma o nos enlaza con otro servidor.

Linux Versión Shareware del conocido sistema operativo Unix. Es un sistema multitarea multiusuario de 32 bits para PC.

**Legacy region (región legal)** la configuración de segmentos de LAN semejantes interconectados físicamente entre par de segmentos usando ISO/IEC 158002-3-adaptada, VLAN-inadvertida por los switches MAC.

**LLC:** Logical Link Control (ISO/IEC 8802-2)

**LU Logic Unit.** Unidad Lógica.

**Lock Cerrado.** Bloqueado.

**LS:** Least-significant

## M

**MAC Media Access Control.** Control de Acceso a Medio. Protocolo que define las condiciones en las cuales las estaciones de trabajo acceden al medio. su uso está difundido en las LAN. en las LAN tipo IEEE la capa MAC es la subcapa más baja del protocolo de la capa de enlace de datos.

**MAC:** Medium Access Control (IEEE 802)

**MAN Metropolitan Area Network.** Red de Área Metropolitana.

**MBONE Multicast Backbone.** Red virtual que utiliza los mismos dispositivos físicos que la propia Internet con objeto de transmitir datos con protocolos Multicast.

**MIB:** Management Information Base (ISO/IEC 7498-4)

**MIME Multipurpose Internet Mail Extensions.** Extensiones Multi propósito de Correo Internet. Extensiones del protocolo de correo de Internet que permiten incluir información adicional al simple texto.

**MMX Multi Media eXtensions. Extensiones Multimedia.** Juego de instrucciones extra que incorporan los nuevos microprocesadores Pentium orientado a conseguir una mayor velocidad de ejecución de aplicaciones que procesan o mueven grandes bloques de datos.

**MNP Microcom Networking Protocol.** Protocolo de Redes de Microcom. Protocolo de corrección de errores desarrollado por Microcom muy usado en comunicaciones con MODEM. Existen varios niveles MNP2(asíncrono), MNP3(síncrono) y MNP4(síncrono).

**MODEM Modulator/Demodulator. Modulador/Demodulador.** Dispositivo que adapta las señales digitales para su transmisión a través de una línea analógica. Normalmente telefónica.

**MPEG Motion Pictures Expert Group.** Grupo de Expertos en Imagen en Movimiento. Formato gráfico de almacenamiento de video. Utiliza como el JPEG compresión con perdidas alcanzando ratios muy altos.

**MROUTER Multicast Router.** Ruteador que soporta Protocolos Multicasting.

**MRU Maximum Receive Unit.** Unidad Máxima de Recepción. En algunos protocolos de Internet se refiere al máximo tamaño del paquete de datos.

**MS:** Most-significant

**MS-DOS Microsoft Disk Operating System.** Sistema Operativo en Disco de Microsoft. Sistema operativo muy extendido en PC del tipo de línea de comandos.

**MSDU:** MAC Service Data Unit (ISO/IEC 15802-1)

**MTU Maximum Transmission Unit.** Unidad Máxima de Transmisión. Tamaño máximo de paquete en protocolos IP como el SLIP.

**MUD Multi User Dimension.** Dimensión Multi Usuario. Sistemas de juegos multiusuario de Internet.

**MULTICASTING** Técnica de transmisión de datos a través de Internet en la que se envían paquetes desde un punto a varios simultáneamente.

## N

**NACR Network Announcement Request.** Petición de participación en la Red. Es la petición de alta en Internet para una sub red o dominio.

**NAP Network Access Point.** Punto de Acceso a la Red. Normalmente se refiere a los tres puntos principales por los que se accede a la red Internet en U.S.

**NC Network Computer.** Computador de Red. Computador concebido para funcionar conectado a Internet. Según muchos el futuro. Se trata de equipos de hardware muy reducido ( algunos no tienen ni disco duro).

**NCFI:** Non-Canonical Format Indicator

**NCP Network Control Protocol.** Protocolo de Control de Red. Es un protocolo del Network Layer

**NET** Red

**NETBIOS Network BIOS.** Network Basic Input/Output System. Bios de una red, es decir, Sistema Básico de Entrada/Salida de red.

**Netiquette Etiqueta de la RED.** Formas y usos comunes para el uso de los servicios de Internet. Se podría llamar la "educación" de los usuarios de Internet.

**Netizen** Ciudadano de la Red.

**NEWS Noticias.** Servicio de Internet con una estructura de "tablón de anuncios" dividido en temas y países en los que los usuarios de determinados grupos de interés dejan o responden a mensajes relacionados con el mencionado grupo.

**Nick** Nombre o pseudónimo que utiliza un usuario de IRC.

**Nodo** Por definición punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red. Punto de interconexión a una RED.

**NSA National Security Agency.** Agencia Nacional de Seguridad. Organismo americano para la seguridad entre otras asuntos relacionados con la informática.

**NSF National Science Foundation.** Fundación Nacional de Ciencia. Fundación americana que gestiona gran parte de los recursos de Internet.

## O

**OEM Original Equipment Manufactured.** Manufactura de Equipo Original. Empresa que compra un producto a un fabricante y lo integra en un producto propio. Todos los fabricantes por ejemplo, que incluyen un Pentium en su equipo actúan como OEM.

**OS2 Operating System 2.** Sistema operativo de 32 bits multitarea creado por IBM. Creado para PC con entorno gráfico de usuario. La versión actual es la 4 la cual soporta ordenes habladas y dictado.

**OSI Open Systems Interconnection.** Interconexión de Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO. Divide las tareas de la red en siete niveles.

## P

**Packet Driver** Pequeño programa situado entre la tarjeta de red y el programa de TCP de manera que proporciona un interfaz estándar que los programas pueden usar como si de un driver se tratase.

**Packet** Paquete Cantidad mínima de datos que se transmite en una red o entre dispositivos. Tiene una estructura y longitud distinta según el protocolo al que pertenezca. También llamado TRAMA.

**PAN Personal Área Network.** Red de Área Personal. Sistema de red conectado directamente a la piel. La transmisión de datos se realiza por contacto físico.

**PAP Password Authentication Protocol.** Protocolo de Autenticación por Password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante password.

**PBX Private Branch Exchange.** Central Privada  
**PDA Personal Digital Assistant.** Asistente Personal Digital. Programa que se encarga de atender a un usuario concreto en tareas como búsquedas de información o selecciones atendiendo a criterios personales del mismo. Suele tener tecnología de IA (Inteligencia Artificial).

**PDU:** Protocol Data Unit

**PEER** En una conexión punto a punto se refiere a cada uno de los extremos.

**PEM Private Enhanced Mail.** Correo Privado Mejorado. Sistema de correo con encriptamiento.

**PERL** Lenguaje para manipular textos, ficheros y procesos. Con estructura de script. Desarrollado por Larry Wall, es multiplataforma ya que funciona en Unix.

**PGP Pretty Good Privacy.** Excelente clave pública de seguridad desarrollada por Phil Zimmerman y mejorada por muchos otros incluyendo a Hal Finney, Branko Lankester, and Peter Gutmann.

**Phracker** Pirata informático que se vale de las redes telefónicas para acceder a otros sistemas o simplemente para no pagar teléfono.

**PICS:** Protocol Implementation Conformance Statement

**PIN Personal Identification Number.** Número Personal de Identificación. Número secreto asociado a una persona o usuario de un servicio mediante el cual se accede al mismo. Se podría decir que es una "Password" numérica.

**PING Packet Internet Groper.** Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host está disponible. Envía paquetes de control para comprobar si el anfitrión está activo y los devuelve.

**PNG Portable Network Graphics.** Gráficos Portables de Red. Formato gráfico muy completo especialmente pensado para redes.

**POP Post Office Protocol.** Protocolo de Oficina de Correos. Protocolo usado por computadores personales para manejar el correo sobre todo en recepción.

**POST Power On Self Test.** AutoTest de Encendido. Serie de comprobaciones que hace un computador de sus dispositivos al ser encendido.

**POTS Plain Old Telephone Services.** Servicios Telefónicos Planos Antiguos.

**PPP Point to Point Protocol.** Protocolo Punto a Punto. Un sucesor del **SLIP**. El PPP provee las conexiones sobre los circuitos síncronos o asíncronos, entre router y router, o entre host y la red. Protocolo Internet para establecer enlace entre dos puntos.

**PPV. Pay Per View.** Pagar Para Ver. Se refiere a las televisiones llamadas "interactivas" o "televisión a la carta" en las que hay que pagar por cada programa que se selecciona para ver.

**Priority-tagged frame:** esta trama esta en el encabezado transportando información de prioridad, pero no transporta información sin identificarse como parte de una VLAN.

**PROXY.** Servidor Caché. El Proxy es un servidor de que conectado normalmente al servidor de

acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.

**PU Physical Unit.** Unidad Física.

**PVID:** Port VID

**PVC Permanent Virtual Circuit.** Circuito Virtual Permanente. Línea punto a punto virtual establecida normalmente mediante conmutaciones de carácter permanente. Es decir a través de un circuito establecido.

## Q

**QAM** Quadrature Amplitude Modulation. Modulación de Amplitud en Cuadratura. Sistema de modulación para transmisión de datos y telecomunicaciones.

## R

**RARP Reverse Address Resolution Protocol.** Protocolo de Resolución de Dirección de Retorno. Protocolo de bajo nivel para la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

**RAM Random Access Memory.** Memoria de Acceso Aleatorio. Varios son los tipos de memoria que se usa en las computadoras. La más conocida son las RAM. Se les llama así porque es posible dirigirse directamente a la célula donde se encuentra almacenada la información. Su principal característica es que la información se almacena en ellas provisoriamente, pudiendo ser grabadas una y otra vez, al igual que un cassette de sonido. La memoria RAM se puede comparar a un escritorio, donde se coloca los papeles con que se va a trabajar. Mientras más grande el escritorio más papeles soporta simultáneamente para ser procesados.

**RAS Remote Access Server.** Servidor de Acceso Remoto.

**Retrain** Se llama así a la acción que ejecuta un modem para re establecer el sincronismo con el otro modem después de una pérdida de comunicación.

**RDSI Red Digital de Servicios Integrados.** Red de telefónica con anchos de banda desde 64Kbps. Similar a la red telefónica de voz en cuanto a necesidades de instalación de cara al abonado, pero digital. En inglés ISDN.

**RFC Request For Comment.** Petición de comentarios. Serie de documentos iniciada en 1967 que describe el conjunto de protocolos de



Internet. Los RFC son elaborados por la comunidad Internet.

**RIF:** Routing Information Field (ISO/IEC 8802-5)

**RIP Routing Information Protocol.** Protocolo de Información de Routing.

**ROM Read Only Memory.** Memoria sólo de lectura. Las memorias ROM se usan para mantener instrucciones permanentes, que no deben borrarse nunca. Estas memorias vienen grabadas de fábrica. Son como los discos fonográficos, que sólo permiten reproducir el sonido. Tienen la ventaja de ser de alta velocidad y bajo costo.

**ROOT Raíz.** En sistemas de ficheros se refiere al directorio raíz. En Unix se refiere al usuario principal.

**Router** Dispositivo conectado a dos o mas redes que se encarga únicamente de tareas de comunicaciones

**RS-232** Conjunto de estándares especificando varias características eléctricas y mecánicas para interfaces entre computadoras terminales y modems. Normalmente presenta 25 pines. Virtualmente idéntica a V.24

**RS-422** Interfaz física más rápida que la RS-232 y para distancias de cableados mayores.

**RSA Rivest, Shamir, Adelman** [public key encryption algorithm]. Algoritmo de encriptación de clave pública desarrollado por Rivest, Shamir y Adelman.

**RTC** Red Telefónica Conmutada. Red Telefónica para la transmisión de voz.

**RTP Real Time Protocol.** Protocolo de Tiempo Real. Protocolo utilizado para la transmisión de información en tiempo real como por ejemplo audio y video en una video-conferencia.

**RWIN Receive Window.** Ventana de recepción. Parámetro de TCP que determina la cantidad máxima de datos que puede recibir el computador que actúa como receptor.

**RX** Abreviatura de Recepción o Recibiendo.

## S

**SATAN Security Analysis Tool for Auditing Networks.** Herramienta de Análisis de Seguridad para la Auditoria de Redes. Conjunto de programas escritos por Dan Farmer junto con Wietse Venema para la detección de problemas relacionados con la seguridad.

**SDH Synchronous Digital Hierarchy.** Estándar Europeo que define un grupo de formato que son transmitidos usando señalización óptica sobre fibra. El SDH es similar al SONET, con un rango básico de 155.52 Mbps, diseñado para viajar a STM-1.

**SDLC Synchronous Data Link Controller.** Controlador de Enlace de Datos Síncrono. También se trata de un protocolo para enlace síncrono a través de línea telefónica. Protocolo propietario de IBM orientado al bit.

**SDSL Symmetric Digital Subscriber Line.** Línea Digital Simétrica de Abonado. Sistema de transferencia de datos de alta velocidad en líneas telefónicas normales.

**SEPP Secure Electronic Payment Protocol.** Protocolo de Pago Electrónico Seguro. Sistema de pago a través de Internet desarrollado por Netscape y Mastercard.

**SGML Standard Generalized Markup Language.** Lenguaje de Anotaciones Generales. Lenguaje del que deriva el HTML.

**S-HTTP Secure HTTP.** HTTP seguro. Protocolo HTTP mejorado con funciones de seguridad con clave simétrica.

**Shared Virtual Local Area Network (VLAN) Learning (SVL) Bridge:** un tipo de puenteo que solo soporta Shared VLAN Learning.

**Shared Virtual Local Area Network (VLAN) Learning (SVL):** la configuración y operación de el proceso de aprendizaje y filtrado de Base de Datos semejante, dados por la configuración de VLAN, si una dirección MAC individual es aprendida en una VLAN, es usada la información para encaminar información tomando decisiones de las direcciones relativamente de todas las otras VLANs configuradas.

**Shared Virtual Local Area Network (VLAN) Learning (SVL)/ Independent Virtual Local Area Network (VLAN) Learning (IVL) Bridge:** este es un tipo de puenteo que simultáneamente soporta Shared VLAN Learning y Independent VLAN Learning.

**SIM Single Identification Module.** Módulo Simple de Identificación. Normalmente se refiere a una tarjeta: Tarjeta SIM. Que identifica y a través de ella da servicio a un usuario, su uso más común es el los teléfonos GSM.

**SLIP Serial Line Internet Protocol.** Protocolo Internet en Línea Serial. Protocolo, antecesor del PPP, que permite establecer conexiones TCP/IP a través de enlaces seriales.

**SmartCard Tarjeta Inteligente.** Tarjeta del formato estándar de crédito que incorpora un microchip ( EEPROM o Microprocesador ) que almacena información y/o la procesa. Por ejemplo las tarjetas telefónicas (EEPROM) o las tarjetas SIM de teléfonos móviles (Microprocesador).

**SMTP Simple Mail Transfer Protocol.** Protocolo de Transferencia Simple de Correo. Es el protocolo usado para transportar el correo a través de Internet.

**SMS Short Message Service.** Servicio de Mensajes Cortos. Servicio de mensajería electrónica de texto entre teléfonos GSM. Gracias a esta capacidad se puede enviar también e-mail desde un teléfono GSM y recibir mensajes desde Internet, aunque esta posibilidad parece ser que aún no funciona en España.

**SNA System Network Architecture.** Arquitectura de Sistemas de Redes. Arquitectura de red exclusiva de IBM. Principalmente orientada a Mainframes.

**Sniffer Literalmente "Husmeador".** Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. Normalmente su uso es ilegal.

**Software.** Esta palabra inglesa que significa "cosa suave", tiene dos significados: (a) uno amplio, de "procedimientos lógicos, para la cooperación armónica de un grupo de personas y máquinas, persiguiendo un objetivo común"; (b) el otro restringido, de "programas de computadora", o conjunto de instrucciones, que se pone en la memoria de una computadora para dirigir sus operaciones.

**Spam / Spammer** Se llama así al "bombardeo" con correo electrónico, es decir, mandar grandes cantidades de correo o mensajes muy largos.

**Spider** Robot-Web. Programa que automáticamente recorre la WWW recogiendo páginas Web y visitando los Links que estas contienen.

**STPID:** SNAP-encoded Tag Protocol Identifier

**SQL Structured Query Language.** Lenguaje de Petición Estructurada. Lenguaje para base de datos.

**SSL Secure Sockets Layer.** Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

**STT Secure Transaction Technology.** Tecnología de Transacción Segura. Sistema desarrollado por Microsoft y Visa para el comercio electrónico en Internet.

**SVL:** Shared VLAN Learning

## T

**Tagged frame:** es una trama que contiene una etiqueta en el encabezado inmediatamente seguida de la dirección MAC fuente en el campo de la trama o, si la trama contiene un campo de información de ruteo, inmediatamente seguida de la información del campo de ruteo. Estas son dos tipos de etiquetas de trama: VLAN-tagged frames y priority-tagged frames.

**T1** Velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 1.54 Mbps a través de una red telefónica.

**T3** Velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 44.7 Mbps a través de una red telefónica.

**TCM** Trellis-Coded Modulation

**TCI:** Tag Control Information

**TCP/IP Transmission Control Protocol / Internet Protocol.** Protocolo de Control de Transmisión / Protocolo Internet. Nombre común para una serie de protocolos desarrollados por DARPA en los Estados Unidos en los años 70, para dar soporte a la construcción de redes interconectadas a nivel mundial. TCP corresponde a la capa (layer) de transporte del model OSI y ofrece transmisión de datos. El IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal característica es comunicar sistemas diferentes. Fueron diseñados inicialmente para ambiente Unix por Victor G. Cerf y Robert E. Kahn. El TCP / IP son básicamente dos de los mejores protocolos conocidos.

**TELNET** Protocolo y aplicaciones que permiten conexión como terminal remota a una computadora anfitriona, en una localización remota.

**Time-out** Parámetro que indica a un programa el tiempo máximo de espera antes de abortar una tarea o función. También mensaje de error.

**Tipo de Codificación Ethernet:** el uso del tipo de interpretación de la IEEE 802.3 tipo/longitud en el campo de la trama como un protocolo que se asocia con el Servicio de la trama de transporte de datos de la MAC.

**Throughput.** Transferencia Real. Cantidad de datos que son transmitidos a algún punto de la red.

**Trama (Frame)** una unidad de transmisión de datos en una IEEE 802 LAN MAC que llevan un protocolo de unidad de datos (PDU) seguido de la dirección MAC. Están estos tres tipos de tramas: desetiquetar (untagged), etiquetado-VLAN (VLAN-tagged) y prioridad de etiquetado (priority-tagged).

**TTD Telefonica Transmisión de Datos.** División de Telefónica para la transmisión de datos.

**TTL Time To Live.Tiempo de Vida.** Contador interno que incorporan los paquetes Multicast y determinan su propagación.

**TPID:** Tag Protocol Identifier

**Tunneling** Transporte de paquetes Multicast a través de dispositivos y Routers unicast. Los paquetes multicast se encuentran encapsulados como paquetes normales de esta manera pueden

viajar por Internet a través de dispositivos que solo soportan protocolos unicast.

TX Abreviatura de Transmisión o Transmitiendo.

## U

**UDP User Datagram Protocol.** Protocolo de Datagrama de Usuario. Protocolo abierto en el que el usuario (programador) define su propio tipo de paquete.

**UNICAST** Se refiere a Protocolos o Dispositivos que transmiten los paquetes de datos de una dirección IP a otra dirección IP.

**UNIX** Sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas mas conocidos como MS-DOS están basadas en este sistema muy extendido para grandes servidores. Internet no se puede comprender en su totalidad sin conocer el Unix, ya que las comunicaciones son una parte fundamental en Unix.

**Untagged frame:** es una trama que no contiene una etiqueta en el encabezado de la trama inmediatamente sigue la dirección fuente MAC al campo de la trama o, si la trama contiene un campo de información de ruteo, inmediatamente sigue la información del campo de ruteo.

**URL** Uniform Resource Locator. Localizador Uniforme de Recursos. Denominación que no solo representa una dirección de Internet sino que apunta aun recurso concreto dentro de esa dirección.

**USB** Universal Serial Bus. Bus Serie Universal.

**UT** Universal Time. Hora Universal. Ver GMT.

**UUCP** Unix to Unix Communication Protocol. Protocolo de Comunicaciones de Unix a Unix. Uno de los protocolos que utilizan los sistemas Unix para comunicarse entre si.

**UUENCODE** Unix to Unix Encoding. Codificador Unix a Unix. Método de transmitir archivos binarios en mensajes electrónicos ASCII.

## V

**VID:** VLAN Identifier

**VINES** Virtual Integrated Network Service. Sistema Operativo para Red desarrollado y manufacturado por Sun Systems.

**VR** Virtual Reality. Realidad Virtual.

**VRML** Virtual Reality Modeling Language. Lenguaje para Modelado de Realidad Virtual. Lenguaje para crear mundos virtuales en la Web.

**Virtual Bridged Local Area Network (LAN)** es cuando existen una o más VLAN puenteadas dejando definir, crear y mantener VLANs.

**Virtual Local Area Network (VLAN)** una sub-configuración de la topología activa de un puente LAN, asociado con cada VLAN es un identificador (VID).

**VLAN-aware:** es una propiedad de puentes o de estaciones finales que reconocen y soportan VLAN con tramas etiquetadas.

**VLAN-tagged frame:** es una trama etiquetada cuyo encabezado transporta ambos: identificadores VLAN y prioridad de información.

**VLAN-unaware:** una propiedad de los puentes o estaciones finales que no reconocen VLAN-tagged frames.

## W

**WAIS Wide Area Information Server** Servidores de Información de Área Amplia. Sistema de obtención de información patrocinado por **Apple**, Thinking Machines y Dow Jones.

**WAN** Wide Area Network. Red de Área Ancha.

**Wanderer.** Robot-Web. Ver Spider.

**Warez** Software pirata que ha sido desprotegido.

**Web Site.** Sitio en el World Wide Web. Conjunto de páginas Web que forman una unidad de presentación, como una revista o libro. Un sitio está formado por una colección de páginas Web. RELI - Revista en Línea puede considerarse un sitio web. Una de las páginas del sitio es este glosario.

**Webcam** Cámara conectada a una página WEB a través de la cual los visitantes pueden ver imágenes normalmente en directo.

**WINDOWS** Pseudo sistema operativo, que funciona basado en el DOS. Más bien se trata de un entorno gráfico con algunas capacidades multitarea. La versión actual WINDOWS 95 funciona parcialmente a 32 bits.

**WWW, WEB o W3 World Wide Web.** Telaraña mundial. Sistema de arquitectura cliente-servidor para distribución y obtención de información en Internet, basado en hipertexto e hipermedia. Fue creado en el Laboratorio de Física de Energía Nuclear del CERN, en Suiza, en 1991 y ha sido el elemento clave en el desarrollo y masificación del uso de Internet.

## X

**X Window System.** Sistema de Ventanas X. El sistema de Ventanas X permite que cada ventana se conecte con una computadora remota.

**X.25 Protocolo de transmisión de datos.** Establece circuitos virtuales, enlaces y canales. Es una tecnología antigua de red usado en Europa.

# Z

**ZIP Zone Information Protocol.** Protocolo de Información de Zona.

## Bibliografía

1. **Andrew S. Tanenbaum.**: “Redes de computadoras”, Tercera Edición, Pearson Education, pp. 814, México 1997
2. **Douglas E. Comer.**: “Redes globales de información con Internet y TCP/IP”, Tercera Edición, Pretince Hall, Vol. I, pp. 621, México 1995
3. **Merilee Ford, H. Kim Lew, Steve Spainer, Tim Stevenson.**: “Tecnologías de Interconectividad de redes”, Pearson, pp. 736, Mexico 1998
4. **Carlos Muñoz Razo.**: “Cómo elaborar y asesorar una investigación de Tesis”, Primera edición, Pearson Education, pp. 300, México 1998
5. **Cisco System, Inc.**: “Guía del segundo año”, Segunda Edición, Cisco System, pp. 736, España 2001

## Manuales de Enterasys Networkers

802.1 Q VLANS Course

Enterasys Specialist SmartSwitch Router Configuration Course

Vertical Horizon VH-2402s Fast Ethernet Switch Management Guide

Vertical Horizon VH-2402s Fast Ethernet Switch User Guide

802.1 Q VLAN User Guide Local Management Introduction

802.1 Q VLAN User's Guide

SmatTrunk User's Guide

802.1 Q VLAN User Guide Local Management Suplement

## Mesografía

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw\\_6\\_3/config\\_gd/vlans.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/config_gd/vlans.htm),

Tutorial de Configuración de vlans por cisco

<http://www.nwfusion.com/index.html>, Manual de configuración por nwfusion

<http://www.iol.unh.edu/training/vlan/sld002.htm>, Manual de entrenamiento por Hadriel Kaplan

[http://www.intel.com/network/connectivity/resources/doc\\_library/tech\\_brief/virtual\\_lans.htm](http://www.intel.com/network/connectivity/resources/doc_library/tech_brief/virtual_lans.htm),

Manual de intel para la configuración de vlans

<http://www.monografias.com/trabajos12/intrants/intrants.shtml>, articulo sobre implementación de seguridad sobre vlans

[http://www.intel.com/network/connectivity/resources/doc\\_library/tech\\_brief/virtual\\_lans.pdf](http://www.intel.com/network/connectivity/resources/doc_library/tech_brief/virtual_lans.pdf), como configurar vlans con equipos intel

<http://www.angelfire.com/al2/Comunicaciones/enlaces.html>, documentación técnica por la Universidad del Táchira

<http://www.consulintel.es/Html/Tutoriales/Articulos/smds.html>, articulo llamado Redes Virtuales: El primer paso hacia la ubicuidad geográfica.

## Normas

- 802.1V-2001 IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridge Local Area Networks - Amendment 2: VLAN Classification by Protocol and Port (Amendment to IEEE 802.1Q, 1998 Edition) 2001