PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Facultad de Ciencias e Ingeniería

Diseño y Administración centralizada de Redes WLAN CENTRUM Católica

Tesis para la optar el título de ingeniero Electrónico

Presentado por:

Michael Guillermo Mendoza Huerta

19990669

Lima - PERÚ

2010

ÍNDICE

INDICE DE PLANOS

INDICE DE ESQUEMAS

ANEXOS CONTENIDOS EN EL CD

RESUMEN

Esta tesis tiene como objetivo el diseño de una red de acceso inalámbrico para los alumnos del Centro de Negocios de la Pontificia Universidad católica del Perú (CENTRUM), así como, la integración de un sistema centralizado de administración; este diseño proporcionará un esquema de red con mayor área de cobertura y seguridad de acceso, así como la administración, control y monitoreo de manera centralizada para el personal de Sistemas.

El diseño estará basado en la asignación de Vlan´s en base a perfiles del usuario, usando una plataforma de Software y Hardware del fabricante Cisco, así como servidores de Base de Datos para la adecuada autenticación y asignación de los perfiles de acceso establecidos.

Las instrucciones para establecer el método y los objetivos perseguidos proporcionaran una herramienta eficaz, para lo cual se debe rediseñar la red para obtener los resultados deseados, desarrollando los siguientes puntos:

- La situación actual del acceso a la red por parte del alumnado, que comprende el análisis de diversos factores, así como el servicio que actualmente se brinda, el cual origina la declaración del marco problemático del rediseño de la red de acceso inalámbrico para el alumnado.
- El estudio de la inserción y desarrollo de nuevas tecnologías de acceso, seguridad, control y administración, lo que permitirá establecer un modelo teórico basado en definiciones operativas, así mismo, indicadores cualitativos y cuantitativos.
- Las especificaciones de la propuesta de rediseño de la red en base al objetivo planteado, la situación actual de la red y las soluciones tecnológicas existentes.
- Presentación del diseño de acceso inalámbrico a la red y la gestión centralizada del mismo en los locales de CENTRUM Católica en el Perú.

INTRODUCCIÓN

Actualmente, el uso de Internet es el servicio más utilizado a nivel mundial para búsquedas y consultas académicas; para su uso, actualmente se cuenta con dos métodos de acceso, el acceso cableado y el acceso inalámbrico. En el caso del acceso inalámbrico se han desarrollado múltiples avances tecnológicos, sobre todo en los campos que necesitaban mejoras, tales como la seguridad de acceso, la fiabilidad de conexión y sobre todo un nuevo concepto, la administración centralizada en esquemas de grandes infraestructuras.

CENTRUM cuenta actualmente con cerca de 2000 alumnos en su campus de Lima y alrededor de 1000 alumnos entre sus locales de provincia: Arequipa, Cusco, Chiclayo, Trujillo, Cajamarca y Piura (Dato obtenido de la Oficina Académica de CENTRUM - Junio 2009). La necesidad de obtener información y comunicación demanda una gran cantidad de conexiones de usuario por parte del alumnado, la falta de cobertura, control y administración en la red Inalámbrica del campus de Lima sumados a los problemas que actualmente presenta el servicio de acceso inalámbrico en los locales de provincias, como por ejemplo, desconexión involuntaria de usuarios, demora en acceso a la red y falta de control de acceso entre otros, ha originado una necesidad de mejora en el servicio de acceso inalámbrico brindado.

Siendo estas necesidades tomadas en cuenta por el área de Sistemas de la PUCP, se desarrollo en conjunto con los distintos proveedores tecnológicos propuestas de solución, a fin de obtener mejoras en la administración de las redes inalámbricas en CENTRUM y permitir atender las necesidades descritas.

CAPITULO 1
ANALISIS DEL ACCESO DEL ALUMNADO A LA RED

El presente capítulo tiene como objetivo mostrar el estado actual de la red de datos de CENTRUM Católica.

Se iniciará con una breve introducción de la situación actual de la red de CENTRUM Católica para luego pasar a la descripción de las sedes que intervendrán en el diseño, mostrar el esquema de interconexión en cada sede, presentar los tipos de usuarios existentes y finalmente enumerar los niveles de administración actual del servicio brindado al alumnado. Toda esta recopilación de información nos permitirá conocer el estado actual de la red Inalámbrica en CENTRUM y además identificar las necesidades que determinan el desarrollo de un nuevo diseño de acceso inalámbrico.

1.1 Descripción

CENTRUM Católica es un proyecto iniciado por la PUCP (Pontificia Universidad Católica del Perú) en el año 2001, actualmente cuenta con programas de doctorados, maestrías, diplomaturas, intercambios y cursos libre en su sede de Lima. En cuanto a programas fuera de Lima cuenta con seis sedes para el dictado de programas de postgrado en el interior del país y un programa Internacional en Quito Ecuador (Dato obtenido de la Oficina Académica de CENTRUM - Junio 2009).

CENTRUM fue reconocida por la revista América Economía como “La Escuela de Negocios número uno del Perú 2007, 2008 y 2009 (América Economía 2007, 2008 y 2009).
CENTRUM Católica se encuentra a la vanguardia de nuevas y mejoras tecnológicas que le ayuden a alcanzar el nivel más alto de educación en cada uno de sus programas.

1.2 Sedes

CENTRUM inicio actividades en el año 2001 con su campus en la ciudad de Lima, este campus alberga toda su infraestructura de red. Debido al rápido aumento en demanda por los programas especialmente de maestrías, se abrieron programas en seis provincias del Perú y recientemente uno en el extranjero.

Las sedes de provincia, así como el programa Internacional en Quito, adoptaron un esquema distinto al de Lima, pues aunque la demanda era alta en ese momento, no era lo suficiente para cubrir los costos de una infraestructura propia, similar a la de Lima. A continuación se revisa la infraestructura del campus principal de Lima así como la solución que se ideó en su momento para las sedes de provincias.

1.2.1 Situación Actual

1.2.1.1 Sede Lima

El campus de CENTRUM se encuentra ubicado en Lima, específicamente en el distrito de Santiago de Surco. Cuenta con aulas de clase, salas de estudio orientado a la discusión grupal de los estudiantes, auditorio, biblioteca y espacios “comunes” como cafetería, comedor y corredores donde se puede encontrar alumnos trabajando en sus laptops casi todos los días. A continuación se presenta un cuadro resumen con las cantidades aproximadas de alumnos por ambientes dentro de la sede Lima de CENTRUM.

Tabla 1: Capacidad de Alumnado por ubicaciones en CENTRUM Católica – Sede Lima

CENTRUM CATÓLICA - CAPACIDAD DE ALUMNADO - SEDE LIMA		
Ambiente	**Alumnos por Ambiente**	**Total de Alumnos**
Aulas de Clase (17)	40	680
Biblioteca	45	45
Salas de Estudio (23)	5	115
Cafetería	75	75
Corredores	40	40
Auditorio	561	561
TOTAL		1516

Elaboración: Propia

Como se puede ver en la tabla 1, la mayor presencia de alumnado a la vez que se podría tener en el campus de Lima es de 1516 participantes (se considerará 1600 alumnos para

efectos del diseño del sistema de Administración). En los Planos 1-A y 1-B se muestra el campus de CENTRUM para una mayor comprensión de la distribución de las aulas, auditorio, salas de estudio y demás. Esta información permitirá dimensionar adecuadamente el diseño del nuevo esquema de acceso inalámbrico para el alumnado.

Adicionalmente CENTRUM a mediados del 2008 inició contratos con Hoteles en Lima por el alquiler de espacios para dictado de clases de Educación Ejecutiva, debido a que las aulas disponibles en el campus principal no se daban abasto para la demanda requerida; esto es, la cantidad de alumnado superaba la cifra considerada en aulas de la tabla 1.

A continuación se presenta la tabla 2, con información referente a los hoteles con los que CENTRUM católica mantiene contrato y la cantidad de alumnado por cada uno de ellos.

Tabla 2: Alumnos en Hoteles – Sede Lima

CENTRUM CATÓLICA - ALUMNOS EN HOTELES - SEDE LIMA	
Hotel	**Alumnos**
Sol de Oro	150
Casa Andina	100
MyN	150
TOTAL	400

Elaboración: Área de Marketing – CENTRUM Católica

De la tabla 2 se puede ver que existe una demanda de aproximadamente 400 alumnos en locales externos a CENTRUM, la solución del acceso a Internet para estos alumnos se considera dentro del contrato de alquiler, por lo que estos requerimientos se excluyen del presente estudio, sin embargo esta cantidad de alumnos se considerará en el nuevo diseño de la red Inalámbrica.

1.2.1.2 Sedes Provincias

Para el caso de los programas dictados en el interior del país, CENTRUM cuenta con sedes en seis ciudades del Perú. Para el dictado de clases mantiene contrato con hoteles por Infraestructura debido a que no cuenta con locales propios; sin embargo, es responsable del acceso a internet de los alumnos para lo cual realiza el despliegue de infraestructura de red temporal. En la Tabla 3 se muestra la cantidad de alumnos en cada una de las sedes de provincia.

Tabla 3: Cantidad de Alumnos – Sedes Provincias

CENTRUM CATÓLICA - CANTIDAD DE ALUMNOS - SEDES PROVINCIAS		
Ciudad - Hotel	**Programas**	**Alumnos**
Arequipa- Cabildo Empresarial	4	116
Cusco - José Antonio	3	97
Chiclayo - Las Garzas	4	126
Trujillo - El Golf	4	113
Cajamarca - Continental	3	72
Piura - Rio Verde	5	115
TOTAL		639

Elaboración: Área de Marketing – CENTRUM Católica

De la Tabla 3 se puede observar que la cantidad de programas por ciudad es considerable y la proyección es aumentar a mediano plazo. Para el diseño de la presente tesis se considerará 700 alumnos con necesidad de acceso a Internet en las ciudades del interior del país.

1.2.2 Proyección al 2010

1.2.2.1 Sede Lima

A mediados del año 2008 la cantidad de alumnado de CENTRUM superó la capacidad de las instalaciones de su campus principal, originando el uso de salas alquiladas en hoteles. Para atender este crecimiento CENTRUM diseño un proyecto de un nuevo edificio dentro del campus a iniciarse a fines de Julio del 2009, cuya capacidad se muestra en la Tabla 4.

Tabla 4: Capacidad de Alumnado en nuevo edificio – Sede Lima

CENTRUM CATÓLICA - ALUMNADO PROYECTO NUEVO EDIFICIO - SEDE LIMA		
Ambiente	**Alumnos**	**Total de Alumnos**
Aulas de Clase (6)	60	360
Corredores	40	40
TOTAL		400

Elaboración: Propia

En el Plano 1-A se considera la incorporación del nuevo edificio al campus de CENTRUM. La consideración de este nuevo edificio nos permitirá dimensionar adecuadamente el diseño del nuevo esquema de acceso inalámbrico para el alumnado.

1.2.2.2 Sedes Provincias

En cuanto a la situación de las sedes para los programas en provincia, CENTRUM presentará los siguientes cambios para los próximos dos años:

a) Nuevas sedes: CENTRUM tiene proyectado extender el número de ciudades donde actualmente dicta programas de maestría, siendo las tres próximas Huancayo, Iquitos y Puerto Maldonado.

Tabla 5: Proyección de alumnado nuevas sedes – Sedes Provincias

CENTRUM CATÓLICA - PROYECCIÓN DE ALUMNADO NUEVAS SEDES PROVINCIAS		
Ciudad - Hotel	**Programas**	**Alumnos**
Huancayo - Presidente	2	60
Puerto Maldonado - Pendiente	2	60
Iquitos - Pendiente	2	60
TOTAL		180

Elaboración: Área de Marketing – CENTRUM Católica

La tabla 5 nos muestra la proyección de alumnado en provincias; con miras al diseño del acceso Inalámbrico, se considerara 200 alumnos.

b) Nuevos programas: CENTRUM proyecta la incorporación de nuevos programas de Postgrado para las sedes de provincia que actualmente ya cuentan con programas de maestría, programas como Diplomaturas, lo que incrementara la cantidad de alumnos, se muestra la proyección de alumnado para estos nuevos programas.

Tabla 6: Proyección de alumnado en nuevos programas – Sedes Provincias

CENTRUM CATÓLICA - PROYECCIÓN DE ALUMNOS NUEVOS PROGRAMAS	
Ciudad	**Alumnos**
Chiclayo	40
Trujillo	40
Arequipa	40
Huancayo	40
Piura	40
TOTAL	200

Elaboración: Área de Marketing – CENTRUM Católica

En la tabla 6 se muestra la proyección del alumnado para los nuevos programas postgrado en provincias, con miras al diseño se asumirá 200 alumnos.

c) Locales a medida en provincias: Mediante contrato con un proveedor externo, se viene desarrollando un proyecto de infraestructura que permitirá contar con sedes temporales que incorporen una infraestructura adecuada para CENTRUM. Se proyecta que la primera sede en contar con este tipo de locales será la ciudad de Chiclayo proyectado para inicios del 2010. Esto permitirá un diseño más simple de la red, sin embargo es necesario el desplazamiento de la infraestructura actual instalada en los hoteles.

1.2.3 Resumen

De la información obtenida del campus de Lima y provincia, se tiene la cantidad de alumnos actuales y proyectados presentados en la Tabla 7:

Tabla 7: Alumnado CENTRUM – Situación actual y proyectada 2010

CENTRUM CATÓLICA - ALUMNADO A NIVEL NACIONAL		
Sede	**Situación Actual**	**Proyección 2010**
Lima	1600	2000
Hoteles Lima	400	0
Provincias	700	1100
TOTAL	2700	3100

Elaboración: Propia

La cantidad de alumnos a considerar para fines del diseño de la red Inalámbrica que propone la presente tesis, considerando todos los escenarios de dictado de programas en Lima y provincias será de 4500 alumnos.

1.3 Infraestructura de Red Actual

En el presente apartado se mostrará la infraestructura de red actual que posee CENTRUM en su campus de Lima, así como en cada una de las ciudades del interior del país.
Con este análisis se obtendrá el inventario y esquema actual que soporta el servicio de acceso inalámbrico en cada sede, permitiendo establecer las consideraciones técnicas para el diseño a proponer.

1.3.1 Sede Lima

Se presenta la Infraestructura de red de la sede de Lima analizando el acceso a internet actual (Enlace de fibra oscura con PUCP Sede Pando), la infraestructura local y el alcance actual del despliegue Inalámbrico.

1.3.1.1 Enlace dedicado CENTRUM – PUCP

CENTRUM no cuenta con un enlace de salida directa a internet, en su lugar cuenta con dos enlaces dedicados de fibra con la Sede Pando de PUCP, siendo los siguientes:

Tabla 8: Enlaces de conexión entre CENTRUM – PUCP Sede Pando

CENTRUM CATÓLICA - ENLACES DE CONEXIÓN CENTRUM - PUCP			
Enlace	**Estado**	**Proveedor**	**Capacidad**
1	Activo	Telefónica del Perú	1 GB
2	Backup	Telmex	2 MB

Elaboración: Área de TI – CENTRUM Católica

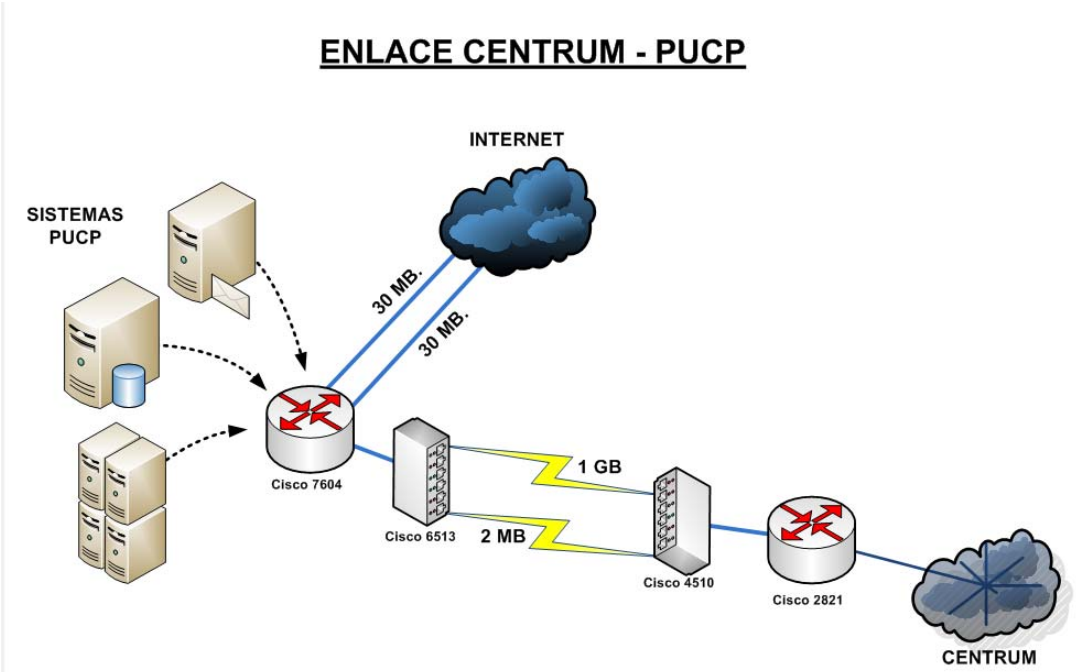
El motivo del Ancho de Banda del enlace principal entre la sede Pando de PUCP y CENTRUM es que la totalidad de los servicios usados por personal y alumnado de CENTRUM se encuentran alojados directamente en la sede de Pando, entre estos servicios se encuentran el Campus Virtual de la universidad, correo electrónico, sistema de bibliotecas, acceso a Internet, etc. Por su parte la sede Pando de PUCP cuenta con dos enlaces para la salida a internet con dos distintos proveedores, los cuales se muestran en la Tabla 9:

Tabla 9: Enlaces de salida a Internet PUCP

CENTRUM CATÓLICA - ENLACES DE SALIDA A INTERNET PUCP			
Enlace	**Estado**	**Proveedor**	**Capacidad**
1	Activo	Telmex	30 MB
2	Activo	Global Crossing	30 MB

Elaboración: Área de Redes - PUCP

A continuación, se muestra el esquema de conectividad a internet enfocado desde el punto de vista del acceso para CENTRUM.



Esquema 1: Enlaces CENTRUM – PUCP

1.3.1.2 Infraestructura Local

Para el estudio de la infraestructura de la red local de CENTRUM, dividiremos el análisis en dos capas, la infraestructura Core y la infraestructura de borde.

A. Infraestructura Core

El Core de la red de comunicaciones en CENTRUM está basado en el Switch de capa 3 modelo Cisco 4510R. Todas las solicitudes hechas por los usuarios a sistemas de PUCP o por acceso a Internet pasan a través de los Switches de borde (Switches de brindan acceso en aulas, cafeterías, salas de estudio, etc.) hasta llegar al Switch principal usando las líneas de fibra dedicadas, en donde a través de un MUX del proveedor de Servicios viajan por el enlace dedicado con PUCP para llegar a los servicios ubicados en la sede Pando. El Switch principal permite además la separación de Vlan's, el uso de telefonía IP, entre otros servicios.

B. Infraestructura de Borde

Diseñada en Topología estrella, todos los Switches de borde llegan al Switch principal a través de líneas de fibra oscura. A continuación se detalla las ubicaciones y acceso brindado por los Switches de borde.

- Aulas de Clase

  Cada una de las 17 aulas de clase posee un Switch de borde para el acceso del alumnado en clases.

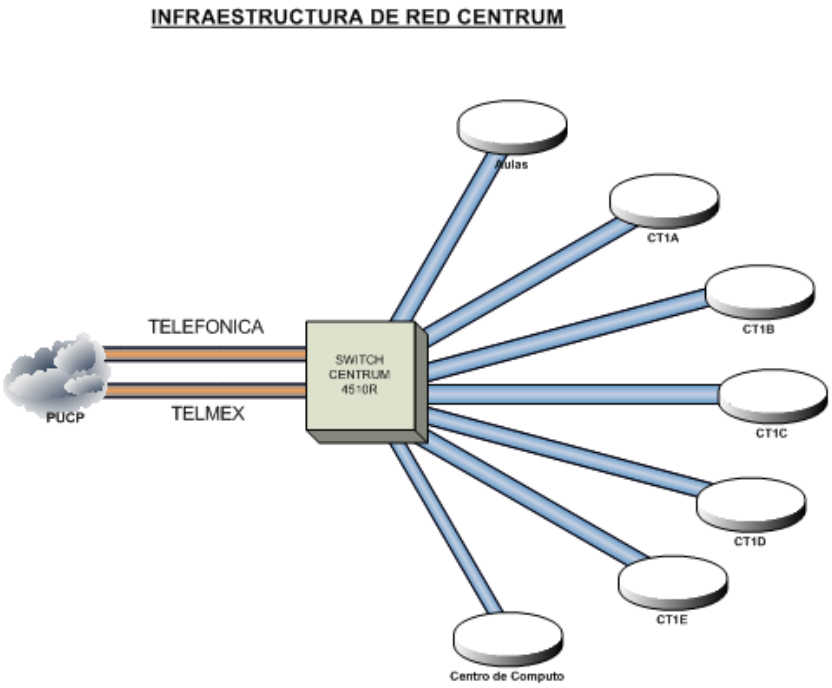
- Salas de estudio y biblioteca

  Para las salas de estudio del 2do piso se cuenta con un Switch de borde ubicado en el Cuarto de Tableros 1C (CT-1C). Para las salas de estudio del 3er piso y biblioteca se cuenta con dos Switches de borde ubicados en el Centro de cómputo.

- Personal Administrativo

  Para el acceso Administrativo se cuenta con cuatro Racks de comunicaciones ubicados en el área de Mantenimiento de Servicios (CT-1A), en el área de caja (CT-1B), en el auditorio (CT-1D) y en el nuevo edificio de Alianzas (CT-1E); estos Switches permiten el acceso a las áreas de Marketing, Administración, Consultoría, Soporte Académico, Maestrías, Alianzas y a las diversas áreas de Mantenimiento. El personal de Tecnologías de la Información está ubicado junto al Centro de Cómputo y tienen conexión a la red a través de uno de los Switches de borde ubicados en el mismo Centro de Cómputo.

A continuación se muestra un modelo simplificado de la Infraestructura de red de CENTRUM.



Esquema 2: Infraestructura de Red CENTRUM Católica

En el Plano 2, se adjunta la Infraestructura de la red local de Centrum – Sede Lima.

Una característica importante en los Switches actuales es la característica de soportar PoE (Power Over Ethernet) que permite energizar equipos sin necesidad de contar con tomas de energía adicionales, usando para este fin el cableado UTP de la red. De los Switches de borde distribuidos en el campus de CENTRUM Católica no todos poseen la característica de PoE. A continuación se adjunta la lista de Switches con los que actualmente cuenta CENTRUM en la sede de Lima.

Tabla 10: Inventario de Switches - Sede Lima

CENTRUM CATÓLICA - INVENTARIO DE SWITCHES SEDE LIMA				
Ubicación	**Equipo**	**Modelo**	**PoE**	**Puertos**
CT-1A	Cisco 3560	WS-C3560-48PS-S	Si	48
	Cisco 3560	WS-C3560-48PS-S	Si	48
CT-1B	Cisco 3560	WS-C3560-48PS-S	Si	48
	Cisco 3560	WS-C3560-48PS-S	Si	48
	Cisco 3560	WS-C3560-48PS-S	Si	48
	Cisco 3550	WS-C3550-24PWR-SMI	Si	24
CT-1C	Cisco 3560	WS-C3560-48PS-S	Si	48
	Cisco 3550	WS-C3550-24PWR-SMI	Si	24
CT-1D	Cisco 3550	WS-C3550-24PWR-SMI	Si	24
CT-1E	Cisco 3560	WS-C3560-48PS-S	Si	48
DATACENTER	Cisco 3560	WS-C3560-48PS-S	Si	48
	Cisco 3524	WS-C3524-XL-EN	No	24
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 2950	WS-C2950G-48-EI	No	48
AULAS	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 2960G	WS-C2960G-48TC-L	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3524	WS-C3548-XL-EN	No	48
	Cisco 2960G	WS-C2960G-48TC-L	No	48
	Cisco 3524	WS-C3548-XL-EN	No	48
	Cisco 3560	WS-C3560-48PS-S	Si	48
	Cisco 2960G	WS-C2960G-48TC-L	No	48
	Cisco 2950	WS-C2950G-48-EI	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 2950	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 2960G	WS-C2960G-48TC-L	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48
	Cisco 3548	WS-C3548-XL-EN	No	48

Elaboración: Propia

1.3.1.3 Infraestructura Inalámbrica

Todos los alumnos de CENTRUM tienen como requisito indispensable de clases, el contar con una laptop dedicada netamente al estudio. En la actualidad todas las laptops incorporan dispositivos WLAN (Wireless Local Area Network) que posibilitan el acceso inalámbrico, por lo que es importante revisar la distribución de puntos de acceso inalámbrico con los que cuenta CENTRUM en cada uno de sus sedes.

En los Planos 3-A y 3-B se presentan los planos de CENTRUM en donde se han identificado las áreas con mayor uso Inalámbrico por parte del alumnado. Así mismo, se han identificado los AP´s con los que se cuenta actualmente en el campus y el área de cobertura que brindan, siendo esta ultima variable y dependiente de factores como material de construcción del edificio, cambios en la intensidad de la señal Inalámbrica, cambios en la intensidad del ruido presente, factores ambientes, etc.

De los Planos 3-A y 3-B, se puede confirmar que CENTRUM cuenta con dos AP´s para brindar el servicio de acceso Inalámbrico en todo el campus. Ambas antenas se encuentran ubicadas en la biblioteca y en la cafetería respectivamente para otorgar la mayor cobertura posible al alumnado fuera de aulas. En cuanto a la conectividad con la red interna, el AP ubicado en Biblioteca tiene conectividad a través de un Switch de borde ubicado en el Centro de Cómputo y el segundo Access Point lo tiene a través de un Switch de borde ubicado en la sala de tableros CT-1B.

Finalmente, revisando la Tabla 1 se sabe que la mayor cantidad de alumnos que podría conectarse a la red inalámbrica fuera de las aulas de clase supera los 330, esto es, sin considerar los alumnos que estando en Aulas o en Auditorio pudieran llegar a detectar la red Inalámbrica y conectarse.

A. Equipamiento

   Daremos una breve descripción de los equipos inalámbricos que actualmente posee CENTRUM Católica, esta información nos permitirá concluir la revisión del esquema de red actual y prever las compatibilidades del diseño a proponer con el Hardware que se posee actualmente.

   Los dos AP´s que tiene actualmente CENTRUM son modelo Cisco Aironet AG1242 los cuales trabajan bajo los estándares IEEE 802.11 a/b/g. La gestión de estos Access Point es realizada por personal de Soporte TI quienes se conectan vía HTTP a cada uno y revisa periódicamente el estatus.

Tabla 11: Infraestructura Inalámbrica – Sede Lima

CENTRUM CATÓLICA – INFRAESTRUCTURA INALAMBRICA	
Marca	Cisco
Modelo	Aironet 1242AG
Tipo	Outdoor
Protocolo de Interconexión de datos	802.11 a/b/g
Protocolo de Gestión remota	SNMP, Telnet, HTTP y HTTPS

Elaboración: Propia

1.3.2 Sedes Provincias

El acceso a Internet para los alumnos en los locales de provincia, es distinto al de Lima, a continuación se detalla el esquema de red actual en cada sede de CENTRUM.

1.3.2.1 Infraestructura de Acceso

Los alumnos de CENTRUM tienen la necesidad de acceder a internet a fin de realizar búsquedas y consultas; la solución temporal brindada por CENTRUM en las sedes de provincia es a través de líneas Speedy Negocios Avanzando de 5 MB, contratadas al ISP (Internet Service Provider) que en este caso es Telefónica.

Esta solución de acceso a Internet presenta muchos inconvenientes y estos son confirmados por el área de Soporte TI al recibir constantes quejas por parte del alumnado de provincias y por los mismos profesores que viajan a dictar las clases, a pesar de que los profesores cuentan con conexión cableada y la conexión de todo el alumnado es netamente inalámbrica. A continuación se presenta el inventario de líneas Speedy con las que se cuenta en cada una de las ciudades.

Tabla 12: Líneas Speedy provincias

CENTRUM CATÓLICA - LÍNEAS SPEEDY - SEDES PROVINCIAS				
Sede	**Programas**	**Aulas**	**Hotel de dictado**	**Líneas Speedy**
Arequipa	4	4	Cabildo Empresarial	Speedy Neg. Avanz. 3MB al 25%
			Cabildo Empresarial	Speedy Neg. Avanz. 3MB al 25%
			Cabildo Empresarial	Speedy Neg. Avanz. 3MB al 25%
Cusco	3	2	Hotel José Antonio	Speedy Neg. Avanz. 5 MB al 25%
			Hotel José Antonio	Speedy Neg. Avanz. 5 MB al 25%
Chiclayo	4	4	Hotel Las Garzas	Speedy Neg. Avanz. 5MB al 25%
			Hotel Las Garzas	Speedy Neg. Avanz. 5MB al 25%
			Hotel Las Garzas	Speedy Neg. Avanz. 5MB al 25%
Cajamarca	3	3	Gran Hotel Continental	Speedy Neg. Avanz. 5MB al 25%
			Gran Hotel Continental	Speedy Neg. Avanz. 5MB al 25%
			Gran Hotel Continental	Speedy Neg. Avanz. 5MB al 25%
Trujillo	4	3	Gran Hotel El Golf	Speedy Neg. Avanz. 5 MB al 25%
			Gran Hotel El Golf	Speedy Neg. Avanz. 5 MB al 25%
			Gran Hotel El Golf	Speedy Neg. Avanz. 5 MB al 25%
Piura	5	3	Hotel Rio Verde	Speedy Neg. Avanz. 5 MB al 25%
			Hotel Rio Verde	Speedy Neg. Avanz. 5 MB al 25%
			Hotel Rio Verde	Speedy Neg. Avanz. 5 MB al 25%

Elaboración: Área de TI – CENTRUM Católica

1.3.2.2 Análisis del Ancho de Banda

En cada una de las sedes en provincia de CENTRUM, se cuenta con un promedio de 40 alumnos por programa y el promedio del número de aulas por provincia es de tres, por lo tanto se cuenta en promedio con 120 alumnos concurrentes por sede.

A continuación se presentan unos cálculos sobre el ancho de banda que tendría cada alumno basándonos en algunas consideraciones técnicas y en el Ancho de Banda garantizado por proveedor; es importante revisar las velocidades de transmisión que otorga y que garantiza Telefónica (dos términos no muy frecuentemente difundidos y muchas veces confundidos) bajo la modalidad contratada de Speedy Negocios Avanzados 5MB. En la tabla 13 se presentan los detalles de las velocidades de transmisión otorgadas por el proveedor.

Tabla 13: Tráfico en Líneas Speedy CENTRUM – Sedes provincias

CENTRUM CATÓLICA - VELOCIDAD LINEAS SPEEDY - SEDES PROVINCIAS				
Proveedor	Tráfico Máximo		Tráfico Garantizado	
	Download	Upload	Download	Upload
Telefónica	Hasta 5000Kbps	Hasta 512 Kbps	Mínimo 1250 Kbps	Mínimo 128 Kbps
Telefónica	Hasta 3000Kbps	Hasta 512 Kbps	Mínimo 768 Kbps	Mínimo 128 Kbps

Elaboración: Telefónica del Perú

Como segundo punto importante, mencionar que aunque se cuente con más de una línea Speedy de acceso por sede cada alumno solo podrá asociarse a una línea, la misma que compartirá con los demás alumnos asociados a esta misma línea para el acceso a Internet, esto significa que una mayor cantidad de líneas no necesariamente significa un mayor Ancho de Banda.

La tercera consideración para estos cálculos es que todos los alumnos transmiten el mismo periodo de tiempo por igual, simplificando esto consideraciones, como el que un alumno use el medio un mayor tiempo que los demás.

Finalmente se está considerando la cercanía de las aulas y por ende la cobertura de los módems usados actualmente por los alumnos (en las sedes de provincia no se cuenta con AP´s para el acceso Inalámbrico, todo es centralizado en los módems instalados por el proveedor), además se están considerando dos escenarios el primero es en el que se tiene el mejor Ancho de Banda esto es con la menor cantidad de alumnos y el segundo es cuando se tiene el menor Ancho de Banda esto es con la mayor concurrencia de alumnos en los ambientes. A continuación se presentan estos datos en las tablas 14 y 15:

Tabla 14: Estudio del Ancho de Banda – Mejor Escenario – Sedes Provincia

CENTRUM CATÓLICA - ESTUDIO DEL ACCESO A INTERNET - CASO MEJOR ANCHO DE BANDA - SEDES PROVINCIA								
Sede	Cantidad de Líneas Speedy	Cantidad de Programas	Cantidad de Aulas	Alumnos por programa	Velocidad Promedio Download (Kbps)	Velocidad Promedio Upload (Kbps)	Velocidad Garantizada Download (Kbps)	Velocidad Garantizada Upload (Kbps)
Arequipa	3	4	4	35/16/24/41	833.33	85.33	208.33	21.33
Cusco	3	3	2	30/30/37	500	51	125	12.8
Chiclayo	3	4	4	20/40/42/24	714.28	73.14	178.57	18.28
Trujillo	3	4	3	19/29/31/34	714.28	73.14	178.57	18.28
Cajamarca	3	3	3	14/27/31	1000	102.4	250	25.6
Piura	3	5	3	12/20/35/19/29	1250	128	312.5	32

Elaboración: Propia

Tabla 15: Estudio del Ancho de Banda – Peor Escenario – Sedes Provincia

CENTRUM CATÓLICA - ESTUDIO DEL ACCESO A INTERNET LOCALES PROVINCIAS - CASO PEOR ANCHO DE BANDA - SEDES PROVINCIA								
ciudad	Cantidad de Líneas Speedy	Cantidad de Programas	Cantidad de Aulas	Alumnos por programa	Velocidad Promedio Download (Kbps)	Velocidad Promedio Upload (Kbps)	Velocidad Garantizada Download (Kbps)	Velocidad Garantizada Upload (Kbps)
Arequipa	3	4	4	35/16/24/41	128.2	13.12	32.05	3.28
Cusco	3	3	2	30/30/37	217.39	22.26	54.34	5.56
Chiclayo	3	4	4	20/40/42/24	119.04	12.19	29.76	3.04
Trujillo	3	4	3	19/29/31/34	156.25	16	39.06	4
Cajamarca	3	3	3	14/27/31	208.33	21.33	52.08	5.33
Piura	3	5	3	12/20/35/19/29	185.18	18.96	46.29	4.71

Elaboración: Propia

Para los cálculos mostrados se ha considerado que existe una distribución uniforme del alumnado en cada una de las líneas de acceso. Analizando los datos obtenidos podemos verificar como decae pronunciadamente el Ancho de Banda en el 2do escenario (Caso con mayor concurrencia), tanto para subida como para bajada; sin embargo se debe notar que el Ancho de Banda garantizado por el proveedor es mucho más bajo, llegando incluso a valores de 3.04 Kbps en el peor de los casos.

Para finalizar este breve análisis se detalla a continuación un cálculo para la subida de archivos (actividad normalmente realizada por los profesores y alumnos en las clases) que es donde se observa el menor Ancho de Banda, estos cálculos están basados en los valores obtenidos en la tabla 14 y 15 y considerando unos archivos de 600KB y de 2000 KB.

Tabla 16: Análisis en tiempo de subida por archivos – Sedes Provincias

Archivo de 600 Kbps - Tiempo de Subida	
Mejor Ancho de Banda Promedio	2 segundos
Peor Ancho de Banda Promedio	6 segundos
Mejor Ancho de Banda Garantizado	6 segundos
Peor Ancho de Banda Garantizado	21 segundos
Archivo de 2000 Kbps - Tiempo de Subida	
Mejor Ancho de Banda Promedio	30 segundos
Peor Ancho de Banda Promedio	166 segundos (3 min.)
Mejor Ancho de Banda Garantizado	120 segundos (2 min.)
Peor Ancho de Banda Garantizado	658 segundos (11 min.)

Elaboración: Propia

Observando los datos obtenidos, podemos confirmar debidamente que la mayoría de problemas presentes en las sedes de provincia se debe a la falta de facilidades técnicas en la subida de archivos, en donde subir un archivo de 2Mb puede tomar hasta 11 minutos, esto último sin contar la disponibilidad del servicio por parte de PUCP, a donde constantemente se suben archivos de diferentes partes del mundo, lo cual podría aumentar

el tiempo de espera. Adicionalmente a una correcta selección de acceso a internet para las necesidades identificadas, es igual de importante un correcto diseño local de la WLAN.

A continuación se revisará en detalle la situación actual de cada sede y se brindarán recomendaciones para una correcta instalación de una WLAN.

1.3.2.3 Equipamiento y diseño WLAN

Cuando se instala el servicio de Speedy (conexión ADSL para acceso a Internet – Proveedor Telefónica) se usa el número de abonado de la vivienda y a través de un modem se brinda el acceso a internet. El servicio Speedy brinda soluciones del tipo “Home”, las cuales no están diseñadas para soportar el acceso de múltiples usuarios simultáneamente. El modem que permite la salida a internet usando la línea telefónica muchas veces cumple la labor de ser un Router inalámbrico para las conexiones provocando que el equipo trabaje al límite en más de una función, lo que no es recomendable para atender solicitudes de más de 15 o 20 clientes.

Cumplir con estas recomendaciones evitará demoras en el acceso de los usuarios y problemas de colapso en el equipo mismo (este límite podría variar dependiendo de las especificaciones del equipo). Retomando las simplificaciones en el ultimo cálculo mostrado se cuenta con 120 alumnos clientes en promedio y solo 3 Módems inalámbricos, esto es, conexión de alrededor de 40 alumnos por cada Router inalámbrico lo cual producirá definitivamente lentitud de acceso y desconexión de usuarios de manera aleatoria al estar duplicando o incluso triplicando la cantidad de usuarios recomendada.

Como se puede ver en este pequeño análisis, los problemas presentes en las sedes de provincia están directamente relacionados al tipo de acceso a internet y al diseño de las redes inalámbricas locales. En los Planos 4-A, 4-B, 4-C, 4-D, 4-E, 4-F, se muestran las redes Inalámbricas actuales de cada sede en provincia de CENTRUM Católica.

1.4 Acceso a Red de Usuarios

El acceso a red en CENTRUM está orientado a suplir las necesidades de conexión a Internet y servicios corporativos para el personal Administrativo, así como el acceso a Internet para el alumnado.

1.4.1 Clasificación de Usuarios

Como se acaba de mencionar, los tipos de usuario a los que se les debe brindar acceso a internet son el personal Administrativo y el Alumnado; no se analizará en detalle el modo de acceso para la parte Administrativa pues este se mantendrá invariable al nuevo diseño de la red inalámbrica.

1.4.1.1 Personal Administrativo

CENTRUM cuenta actualmente con alrededor de 200 usuarios como personal Administrativo distribuidos entre las áreas de Marketing, Administración, Consultoría, Informática, Soporte Académico, Maestrías, Alianzas, Investigación y las diversas Áreas de Mantenimiento. Todos los usuarios que son personal de CENTRUM están incluidos en la una Vlan con acceso a las aplicaciones y servidores del parque informático PUCP. Como dato general, PUCP ha medido el consumo del Ancho de Banda de la fibra oscura de conexión entre CENTRUM y PUCP obteniendo que actualmente solo se consume el 10% de su capacidad en horas pico.

1.4.1.2 Alumnado

Actualmente CENTRUM cuenta con alrededor de 2000 alumnos en Lima y 1000 alumnos en sedes de provincia. Las necesidades de acceso a Internet para un alumno de CENTRUM son el uso de los servicios PUCP y de páginas web de consulta e investigación académica. Los alumnos son asignados en una de dos Vlan´s (las Vlan´s son asignadas de acuerdo al perfil del alumno, este punto se revisará en el punto 1.4.3), estas dos Vlan tienen acceso a los servicios PUCP disponible para todo el alumnado, bloqueando además cualquiera

acceso hacia la red del personal Administrativo. El modo de acceso se revisará a continuación en detalle.

1.4.2 Modos de Acceso

El acceso a red brindado por CENTRUM al alumnado está segmentado en dos modos, el modo de acceso Alámbrico y el modo de acceso Inalámbrico. Cabe mencionar que ambos tipos de acceso no son distintos en cuanto a variedad del servicio, más si en la cobertura y el alcance del mismo. Así mismo, el control de acceso actual y la seguridad está presente en el modo de acceso Alámbrico, este y otros detalles se mencionaran a continuación.

1.4.2.1 Modo Alámbrico

Diseñado para ofrecer conectividad segura en zonas críticas, hace uso de cables UTP categoría 5 y está Implementado actualmente en todas las instalaciones de CENTRUM; soporta el principal medio de acceso a red para el personal Administrativo. Para el alumnado se encuentra presente en todas las aulas de clase, biblioteca y módulos de estudio. El control de acceso de usuarios que se tiene actualmente aplica directamente sobre este tipo de acceso como se comentará en el apartado de Perfiles de acceso.

1.4.2.2 Modo Inalámbrico

Destinado originalmente para el acceso del alumnado en áreas libres y fuera de clases como Corredores y cafeterías, además de servir como conexión de respaldo en la biblioteca en el caso de que los puertos Ethernet de esta queden superados por el número de alumnos. El modo de acceso inalámbrico no fue diseñado para ser usado en aulas de clase, sin embargo, se conoce de casos en los cuales la señal inalámbrica llega al salón.

El acceso inalámbrico no cuenta con restricción de acceso de ningún tipo, esto es, el acceso a cualquier página o aplicación es permitido, salvo la restricción del acceso a la red Administrativa. En cuanto a la seguridad de acceso de las antenas inalámbricas, esta es mínima, actualmente no se cuenta con una autenticación de usuario ni con una clave de acceso, dejando abierta posibles infiltraciones de atacantes a la red misma.

Finalmente, las conexiones inalámbricas llegan a través de los Access Point a los Switches de borde para luego llegar al Centro de Cómputo de manera similar a las conexiones por cable.

1.4.3 Perfiles de Acceso

En los ambientes externos al salón de clase el acceso a internet para el alumnado no tiene restricciones en cuanto a páginas web, Messenger, etc., sin embargo, CENTRUM cuenta con directivas de acceso divididos en tres perfiles para alumnos, los cuales son:

- Perfil 1: Alumno en clase
- Perfil 2: Alumno fuera de clase
- Perfil 3: Alumno en evaluación

A continuación se detalla cada uno de los perfiles.

1.4.3.1 Alumnos en Clase

Cuando un alumno se encuentra en clase, según directiva establecida por CENTRUM, el alumno solo debe tener acceso a los sistemas PUCP necesarios para el normal desarrollo de la clase, esta configuración es llevada a cabo por personal de TI quienes configuran los Switches de borde de cada aula previamente a cada inicio de clase para permitir solamente el acceso deseado, lo cual se logra pasando todos los puertos del Switch de borde del aula a la Vlan de “alumno en clase”.

1.4.3.2 Alumnos fuera de Clase

El segundo escenario es cuando el alumno no se encuentra en clase, por lo tanto debe tener acceso libre desde cualquier ubicación de CENTRUM, incluyendo esto a las mismas aulas de clase, personal de TI debe configurar todos los puertos de los Switches de dichas aulas a la Vlan de “Acceso libre”.

1.4.3.3 Alumno en Evaluación

Este último caso es realmente una particularidad del primer caso. Cuando una clase tiene programado un examen, los alumnos de dicha clase no deben tener conexión a internet ni intranet. Para este perfil, personal de TI debe revisar los horarios de clase e identificar los días y horas de examen para configurar el apagado de los puertos Ethernet del Switch de Aula y así evitar cualquier conexión no deseada.

Hay dos puntos importantes a tomar en cuenta y que escapan al control del esquema revisado.

- No se puede controlar la conexión de un alumno a un Access Point desde un aula de clase. Esto debido a que el alcance de la antena es variable debido a distintos factores como se comentó previamente y además depende del alcance del mismo dispositivo WLAN de la laptop del alumno.
- Desde el año 2009 empresas telefónicas proveen el servicio de internet móvil lo cual tampoco puede ser filtrado en las aulas.

1.5 Administración de la Red

La responsabilidad de administración, calidad y soporte del servicio de red a nivel de Infraestructura en CENTRUM Católica; es compartida por dos áreas las cuales son: Soporte TI y Tecnologías de la Información.

1.5.1 Administración de Primer Nivel

A cargo de personal de Soporte TI, son los encargados de la atención a los usuarios finales y su labor se centra en la configuración del lado del cliente; además se encargan de realizar las pruebas básicas y descartes necesarios.

1.5.2 Administración de Segundo Nivel

Labor a cargo de los Ingenieros de Infraestructura, los que al recibir una solicitud de incidencia o atención de parte de personal de Soporte TI, revisan la configuración y modifican la misma en los Switches o Router respectivos. Este es el ultimo nivel de soporte dentro de CENTRUM, el siguiente nivel es directamente la revisión de enlaces entre PUCP y CENTRUM, responsabilidad que recae directamente en los ingenieros de PUCP.

1.5.3 Administración en Provincias

Actualmente no se cuenta con una administración en los equipos de comunicación en los locales de provincias; tal como se comentó, el acceso a internet en los locales de provincias está siendo proporcionado a través de líneas Speedy.

CENTRUM lleva un control con personal que labora en estas ciudades, son ellos quienes reportan las incidencias de los alumnos y que posteriormente son elevadas al proveedor a través de personal Soporte TI. Esta es una de las brechas que superará el diseño de control e integración que plantea la presente tesis.

1.6 Necesidades de Mejoras Identificadas en la Red Inalámbrica

En base a los datos revisados, se ha identificado la necesidad de contar con una mejora en el diseño de acceso inalámbrico, tanto para la sede de Lima como para las sedes de provincia en CENTRUM, lo cual involucra una mejora en los siguientes puntos:

- Mejora de Infraestructura inalámbrica en Lima: Es necesario brindar el servicio de acceso inalámbrico en todo el campus, esto mejorara la cobertura de acceso; por lo tanto, es necesario incluir una mayor cantidad de puntos de acceso.
- Automatización en la asignación de perfiles inalámbricos: La administración en la asignación de perfiles a los alumnos demanda una alta carga laboral; por lo que es necesario contar con un nivel de automatización en la asignación de los mismos.
- Implementación de niveles de seguridad inalámbrica: No se cuenta con una seguridad de acceso a la red inalámbrica. Es prioridad incorporar un nivel mínimo de seguridad como por ejemplo el uso de claves de acceso.

- Mejora de Infraestructura inalámbrica en provincias: Es necesario estandarizar y mejorar el diseño del acceso inalámbrico en los locales de provincia, lo cual conllevara una inversión para la mejora de infraestructura inalámbrica actual.
- Mejora en la administración de los Access Point: Se debe mejorar la gestión de los Access Point administrados en Lima e incorporar a los de Provincias, por lo cual es necesario considerar una herramienta que integre y centralice la administración.

CAPITULO 2
REDES DE ACCESO: DEFINICIÓN Y SISTEMAS DE ADMINISTRACIÓN

En este capítulo se mostrarán los avances tecnológicos logrados hasta el momento para el acceso a red de usuarios. Se mencionará las características de estas nuevas tecnologías que definirán la posterior propuesta y diseño del sistema.

2.1 Modos de Acceso

Los modos de acceso a una red de datos son: El acceso Alámbrico y el Inalámbrico de los cuales como se irá viendo se desprenderán algunas variantes con mayor o menor auge hoy en día.

2.1.1 Modo de Acceso Alámbrico

Este modo de acceso hace referencia a todas las topologías que usan cableado para la conexión de sus terminales. El tipo de cableado define las velocidades y rendimiento del medio de transmisión. A continuación se muestra una tabla resumen con las características de los principales tipos de cables más usados actualmente.

Tabla 17: Características de los principales medios cableados

PRINCIPALES MEDIOS CABLEADOS - CARACTERISTICAS		
Características	UTP Categoría 5	Fibra Oscura
Distancias	100 m.	100 Km
Velocidades	10/100/1000 Mbps	Hasta 1 Tbps
Costo	Bajo	Elevado
Uso	Cableado Local	Equipos críticos para el acceso a red
Medio de transmisión	Cobre	Fibra de Vidrio

Elaboración: Propia

Finalmente, la seguridad de una red de acceso cableada es por infraestructura de diseño la más segura que existe, dado que todos los datos viajan por un medio que está controlado y

seguro dentro de la misma empresa. Para poder infringir la seguridad de una red cableada habría que infiltrarse en un ambiente donde se tenga el acceso a un puerto de red o encontrar un hueco en la seguridad de la empresa por el cual ingresar a la red.

2.1.2 Modo de Acceso Inalámbrico

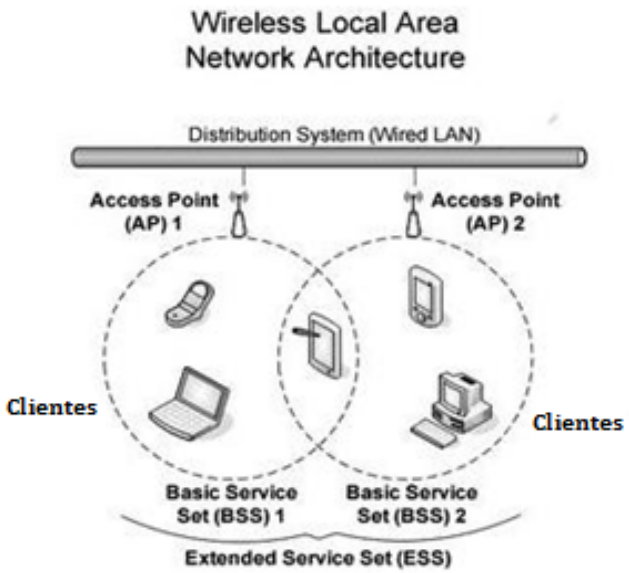
La nueva tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas en el desarrollo de sistemas de comunicación. La flexibilidad y la movilidad que proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas redes se haya incrementado desde el año 2002.

A continuación se presentan las principales tecnologías Inalámbricas desarrolladas y de mayor uso actualmente.

2.1.2.1 WLAN (Wireless Local Area Network)

Las redes WLAN denominadas también redes WiFi, son redes basadas en el uso de Ondas Electromagnéticas (OEM) que permiten enviar información sin contar con conectividad física. El esquema de funcionamiento de este tipo de infraestructuras comprende los siguientes elementos:

- Access Point: Punto de acceso inalámbrico que brinda el acceso a red para los clientes.
- Clientes: Usuarios que solicitan conexión inalámbrica.
- Distribution System: Permite el medio de conexión entre el Access Point y la red cableada.



Esquema 3: Arquitectura de Redes WLAN

Es importante mencionar que si bien las WLAN son conocidas como redes WiFi, el termino WiFi realmente hace referencia al cumplimiento de un certificado otorgado por el WiFi Alliance (antes conocido como WECA) el cual es el encargado de adoptar, probar y certificar los equipos que cumplen con los estándares 802.11 (WLAN). El desarrollo en la tecnología de las WLAN en los últimos años principalmente se ha orientado en dos frentes, mejorar la velocidad de transmisión y la seguridad.

A. Mejoras en la velocidad

En cuanto a velocidades de transmisión, las mejoras han sido palpables desde inicios de 1997 cuando la IEEE desarrollo la primera red Wireless a la que nombró 802.11, estándar que solo soportaba 2 Mbps de ancho de banda.

Posteriormente en Julio de 1999 la IEEE mejora el estándar 802.11 creando la especificación 802.11b la cual usaba la misma frecuencia de transmisión (2.4 GHz) que la 802.11 pero permitía anchos de banda de hasta 11 Mbps. La frecuencia 2.4 GHz es de uso libre por lo que su uso puede estar expuesto a interferencias de otros dispositivos que usen la misma frecuencia como el microondas, teléfonos Inalámbricos, entre otros.

Mientras 802.11b salió al mercado también lo hizo una segunda especificación de la IEEE, el 802.11a la cual no tuvo tanta popularidad como el 802.11b debido al elevado costo de sus productos, razón por la cual se le podía encontrar en ambientes

empresariales. 802.11a soporta velocidades de hasta 54 Mbps y trabaja en una frecuencia de 5 GHz; la alta frecuencia de transmisión comparada con el 802.11b reduce el área de cobertura manteniéndolo por debajo al manejado por 802.11b. La frecuencia de 5 GHz es más propensa a interferencia al atravesar paredes u otros obstáculos, por otro lado sufre menor interferencia de otros dispositivos al ser una banda menos usada que la de 2.4 GHz.

Entre los años 2002 y 2003 la IEEE desarrolla un nuevo estándar denominado 802.11g que combinaba las mejores características de los dos estándares previos. 802.11g soporta transferencias de hasta 54 Mbps y usa la frecuencia de 2.4 GHz permitiendo obtener la mayor cobertura posible. Un factor muy importante es que este nuevo estándar permite la compatibilidad con el estándar 802.11b, esto es, AP´s desarrollados con el estándar 802.11g son compatibles con dispositivos de usuarios desarrollados para el uso del estándar 802.11b.

Finalmente el nuevo estándar de la IEEE es el 802.11n, estándar que ha sido diseñado para mejorar el ancho de banda ofrecido por los estándares anteriores; esto último lo logra utilizando varias señales inalámbricas y antenas (tecnología llamada MIMO) en lugar de solo una. Cuando el estándar esté listo podrá soportar transferencias de hasta 300 Mbps y tendrá una cobertura mayor que los estándares anteriores debido a la mejora de sus señales. Los equipos desarrollados con tecnología 802.11n soportaran la compatibilidad con el estándar 802.11g. Se muestra la tabla 18 con la comparación de los estándares mencionados:

Tabla 18: Comparación entre los estándares 802.11 a, b, g y n

COMPARACIÓN ENTRE LOS ESTANDARES 802.11 A, B, G Y N				
Característica	**IEEE 802.11a**	**IEEE802.11b**	**IEEE 802.11g**	**IEEE 802.11n**
Frecuencia/Ancho de Banda	5 GHz	2.4 GHz (83.5 GHz)	2.4 GHz (83.5 GHz)	2.4 GHz y 5 GHz
Modulación	OFDM	DSSS	OFDM	MIMO
Ancho de Banda por Canal	20 MHz (6 canales utilizables)	22 MHz (3canales)	22 MHz (3 canales)	20 GHz 40 GHz
Tasa de transmisión	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Cobertura Interior/Exterior	30/50 Metros	50/150 Metros	30/50 Metros	
Usuarios Simultáneos	64 usuarios	32 usuarios	50 usuarios	

Elaboración: Propia

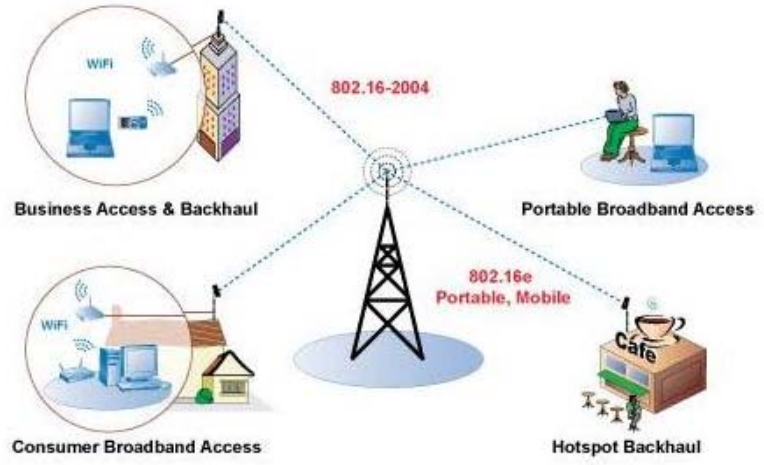
B. Mejoras en la seguridad

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha abierto nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma. Varios son los riesgos derivables de este factor. Por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un AP ilegal más potente que capte las estaciones clientes en lugar del AP legítimo.

A pesar de los riesgos mencionados, existen soluciones y mecanismos de seguridad para impedir que cualquiera pueda introducirse en una red. Unos mecanismos son seguros, otros, como el protocolo WEP fácilmente superables por programas incluso distribuidos gratuitamente por internet. Todas estas mejoras y más se detallaran en el apartado 2.3.

2.1.2.2 WIMAX (Worldwide Interoperability for Microwave Access)

Estándar de transmisión inalámbrica de datos en áreas de hasta 48 km de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base. El protocolo que caracteriza esta tecnología es el IEEE 802.16. Se presenta la arquitectura de interconexión para redes WIMAX.



Esquema 4: Arquitectura de redes WIMAX

2.1.2.3 Redes de Telefonía Móvil

Los servicios brindados por la telefonía móvil han ido aumentando y mejorando en el transcurrir del tiempo y esto gracias a la incorporación de nuevos estándares. Se ha pasado de la generación 2G que se caracterizó por ofrecer servicios digitales y en la cual surgieron numerosos sistemas como GSM (Global System for Mobile Communications) que permitió velocidades de transmisión de datos de hasta 9.6 Kbps hacia la generación 2.5G, con tecnologías de comunicación móviles como GPRS (General Packet Radio Service) que ofrecen velocidades de hasta 40 Kbps en el enlace descendente y 9.6 Kbps en el enlace de subida. Otra de las ventajas de GPRS fue contar con una tarifación por tráfico, convirtiéndolo en el portador ideal para servicios como WAP, SMS, Internet y servicios de comunicación como correo electrónico y World Wide Web.

Actualmente se brindan servicios de la generación 3G, los cuales se caracteriza por ofrecer la convergencia de voz y datos, siendo apta para aplicaciones multimedia y alta transferencia de datos, pudiéndose alcanzar velocidades de hasta 2 Mbps En esta generación se encuentra el estándar UMTS (Universal Mobile Telecommunication System) que dentro de sus características presenta conexión a la red todo el tiempo, diferentes formas de tarifación, ancho de banda asimétrico en el enlace ascendente y descendente, configuración de calidad de servicio, integración de la tecnología y estándares de redes fijas y móviles, entorno de servicios personalizado, entre otros. A continuación se presenta un cuadro resumen de las tecnologías de acceso revisadas.

Tabla 19: Tecnologías de acceso Inalámbrico en el Perú

TECNOLOGÍAS DE ACCESO INALAMBRICO EN EL PERÚ			
Tecnología	Velocidades	Cobertura	Dispositivos de Acceso
WiFi	hasta 54 Mbps	Hasta 35 metros	Laptops, PDA, Celulares
WIMAX	Hasta 124 Mbps	Hasta 50 Kilómetros	Antenas receptoras
2G (GSM)	Hasta 9.6 Kbps	Cobertura de Telefonía Móvil	Laptops y Celulares
2.5G (GPRS)	Hasta 40 Kbps	Cobertura de Telefonía Móvil	Laptops y Celulares
3G (UMTS)	Hasta 2 Mbps	Cobertura de Telefonía Móvil	Laptops y Celulares

Elaboración: Propia

2.2 Acceso de Usuarios en WLAN

En este apartado se revisará la tecnología y el desarrollo de los dispositivos usados por los clientes en el acceso a red y la infraestructura de las WLAN.

2.2.1 Dispositivos usados por el usuario

La necesidad de estar conectado a la "red" el mayor tiempo posible, ha generado el desarrollo de equipos cada vez más portables. Esta evolución ha permitido una mejora considerable en la comunicación de datos al instante, aumentando la productividad en las diversas áreas de desarrollo humano.

Hace unos años el único medio de estar conectados a la "red" era mediante el uso de una PC conectada a Internet; hoy en día el desarrollo tecnológico ha generado la evolución de dispositivos cada vez más livianos y portables, por ejemplo, laptops, PDA´s, teléfonos celulares, etc. A continuación se presenta de forma resumida los equipos más usados actualmente por los usuarios para la conexión a la red.

- Laptops

  Probablemente el dispositivo de mayor desarrollo en los últimos 10 años, mejorando considerablemente su rendimiento y diseño permite la movilidad de los clientes. Actualmente todas las laptops integran puertos de red Ethernet y una tarjeta de red inalámbrica para conexiones WiFi.

- PDA (Personal Digital Assistant)

  Creado originalmente como agenda electrónica hoy permite ver películas, crear documentos, conectar dispositivos GPS, conectarse a una red inalámbrica, etc. Similar a una laptop pero con mayor portabilidad, en los últimos años ha perdido el auge de sus inicios ya que comienzan a ser sustituidos por los Smartphone.

- Teléfonos

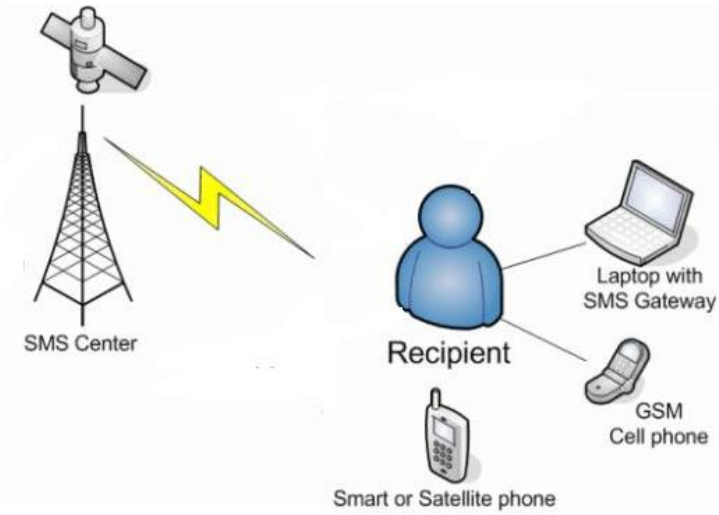
  Sin duda el dispositivo más usado actualmente. El acceso a red a través de este dispositivo se puede lograr haciendo uso de una de las dos tecnologías mencionadas a continuación.

Teléfonos con WiFi: Son teléfonos celulares que incorporan una pequeña tarjeta Wireless para la conexión a redes WLAN, permitiendo así la descarga de correos, navegar por internet entre otros.

Teléfonos con tecnología 3G: Equipos celulares que permiten la conectividad a red a través de las centrales telefónicas.

Actualmente la mayoría de los teléfonos modernos denominados “Smartphone” incorporan ambas funcionalidades. A continuación se presentan los modelos de conectividad para los dispositivos WiFi y tecnología 3G mencionados:

Esquema 5: Modelo de acceso a red - Tecnología WiFi



Esquema 6: Modelo de acceso a red - Tecnología móvil 3G

2.2.2 Infraestructura de Acceso

En un inicio el despliegue de redes Inalámbricas no era común, básicamente se podía encontrar redes Inalámbricas solo en algunos ambientes empresariales, esto debido al elevado costo de los equipos y a las carencias de seguridad encontradas.

La rápida evolución de la tecnología inalámbrica (IEEE802.11) ha permitido el desarrollo de nueva infraestructura de acceso a un costo mucho menor, haciendo posible contar hoy en día con acceso Inalámbrico en diversos lugares, incluso en zonas públicas, como por ejemplo Aeropuertos, Centros Comerciales, Universidades, Cafeterías e incluso plazas y parques, estos puntos de acceso son denominados HotSpot.

Como se ha mencionado anteriormente, la arquitectura de acceso inalámbrico se encuentra conformada por tres elementos.

1. Access Point
2. Dispositivos Clientes
3. Sistema de Distribución

De los tres elementos mostrados, los que han tenido un mayor impacto en la adopción de redes Inalámbricas desde el punto de vista económico, han sido el Access Point y los dispositivos clientes.

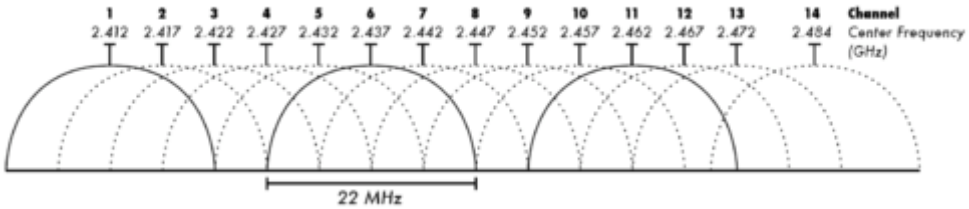
2.2.2.1 Access Point

Este dispositivo es el encargado de permitir el acceso de los clientes Inalámbricos, actuando como un Hub de conexión. Inicialmente el costo de estos equipos era elevado, la inserción de nuevos fabricantes y la demanda de equipos ha generado una disminución en el costo de los mismos. Actualmente se encuentran disponibles en marcas como Cisco, 3com, Trendnet, DLink, etc. Los Access Point en cuanto a arquitectura de trabajo son desarrollados en dos modos de trabajo.

A. Tipo Outdoor: Access Point desarrollados para ofrecer conectividad en ambientes externos o abiertos como Campus Universitarios o minas. Presentan un diseño conservador que los protege de los cambios climatológicos.

B. Tipo Indoor: Access Point desarrollados para ofrecer conectividad en ambientes cerrados o internos como oficinas o aulas de clase. Presentan un diseño estéticamente más refinado.

Un punto adicional y muy importante a considerar en el estudio de los AP es el uso de canales de transmisión. Basándonos en las normas del FCC (Organismo Americano), el cual regula el uso del espectro en transmisiones WiFi (Para el caso de Europa es el ETSI), el espectro de transmisión es dividido en canales (11 para FCC y 14 para ETSI) los cuales cuentan con una separación entre ellos de 5 MHz como se presenta en la siguiente figura:



Esquema 7: División del Espectro en Canales de transmisión para 802.11

Un adecuado uso de los canales a fin de evitar interferencia entre ellos es el uso de canales lo suficientemente alejados para que el Ancho de Banda de uno no interfiera con otro, en tal medida, es recomendable el uso de los canales 1, 6 y 11 para las transmisiones WiFi.

En cuanto a la funcionalidad, además de permitir la conectividad de usuarios, algunos fabricantes han orientado la función de los Access Point en dos esquemas de uso.

A. Modo Standalone: En este modo de trabajo, el equipo actúa como un solo ente, sin conocer que pasa a su alrededor, almacena toda la configuración el mismo y ofrece todos los servicios que soporta con sus propios recursos. Estos equipos debido a los servicios soportados deben poseer un mínimo de Hardware lo cual incrementa el costo de compra, además que la administración es por equipo, ocasionando un costo en recursos para la administración en grandes despliegues. Este modo de trabajo no es recomendable en ambientes con muchos Access Point debido a la gran carga laboral de la administración, sin embargo, para empresas o negocios pequeños son la mejor forma de iniciar los despliegues inalámbricos.

B. Modo Integrado: Con la rápida adopción de los sistemas inalámbricos surgió un nuevo reto, la administración. En empresas con grandes despliegues inalámbricos era un gran inconveniente la configuración y administración de los Access Point por separado. Empresas como Cisco y 3com identificaron esta necesidad y desarrollaron todo un sistema centralizado de administración de redes Inalámbricas. En estos nuevos esquemas centralizados los Access Point ya no trabajan de manera aislada sino como parte de todo un sistema. Debido a que los servicios ya no se centralizan en los Access Point estos ya no necesitan contar con altos recursos de Hardware disminuyendo el costo de los equipos.

Empresas como 3com desarrollaron modelos de AP´s distintos en Hardware para el modo Standalone y para el modelo integrado. Soluciones como las de Cisco presentan el mismo equipo a nivel de Hardware para ambos modos, sin embargo, versiones distintas de IOS (Sistema Operativo del equipo) instalado permite trabajar en uno u otro esquema deseado.

De esta manera podemos verificar que los Access Point cumplen una labor importante dentro de la arquitectura de la red inalámbrica y que sus precios y funcionalidades pueden variar de acuerdo al esquema de solución adoptado por la empresa.

2.2.2.2 Dispositivos Clientes

El acceso de los clientes a la red Inalámbrica se da gracias al uso de una tarjeta inalámbrica que permite la comunicación con los AP´s. Las tarjetas Inalámbricas no eran muy comunes para computadoras de escritorio, debido a que las dimensiones de estas dificultaban su movilidad. Por otro lado, las laptops incorporaban tarjetas Inalámbricas y poseían dimensiones que permitían la movilidad del cliente, sin embargo, el costo inicial de las laptops era muy elevado. Ante la inserción de nuevos fabricantes de portátiles en el mercado local, el precio disminuyo permitiendo una mayor demanda.

Por otro lado, hoy en día se pueden encontrar diversos fabricantes de tarjetas inalámbricas y su uso se ha extendido incluso a computadores de escritorio, entre las principales marcas podemos encontrar Intel, Cisco, DLink, etc. Un detalle importante a tomar en cuenta es que muchos fabricantes desarrollan la mayoría de los servicios del Software de administración de la tarjeta Inalámbrica a esquemas de su misma marca. Así, por ejemplo, los AP de Cisco trabajan con la totalidad de aplicaciones para un cliente que cuente con una tarjeta Inalámbrica Cisco, este comportamiento se repite en los demás fabricantes.

2.3 Seguridad de acceso

Desde la concepción del uso del aire como medio de transmisión en las redes inalámbricas, la mayor tarea de investigación y desarrollo ha sido ofrecer un nivel de seguridad adecuado para esta nueva tecnología. Ningún tipo de red es 100% segura, incluso las redes con cables sufren de distintos tipos de vulnerabilidades. Las redes inalámbricas son aun más vulnerables que las redes con cables, debido a la propagación de la señal en todas las direcciones y al fácil acceso de la misma.

En este apartado se revisarán las principales debilidades de seguridad en las redes Inalámbricas que indujeron ataques ya conocidos actualmente y que posteriormente fueron superados con nuevos protocolos de seguridad, así mismo se detallara la evolución de estos protocolos.

2.3.1 Principales ataques en redes inalámbricas

Desde los primeros despliegues de redes Inalámbricas, diversos problemas de seguridad han sido explotados y posteriormente superados con el uso de protocolos de seguridad. A continuación se presenta una lista de los principales ataques de seguridad identificados a lo largo de los últimos años.

A. Rogue Access Point

En este tipo de ataque el intruso introduce un AP de gran alcance a los usuarios permitiendo la conexión de los mismos para finalmente acceder al tráfico enviado.

B. Man in the Middle

Ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. Para esto el atacante hace creer al cliente que él es el AP y al AP que él es cliente.

C. ARP Spoofing

Conocido también como ARP Poisining, trabaja de manera similar al ataque “Man in the Middle”. El principio del ARP Spoofing es enviar mensajes ARP falsos a la red, asociando la MAC del atacante con la IP de otro nodo (el nodo atacado), como por ejemplo la puerta de enlace predeterminada. Todos los mensajes enviados a la dirección IP de ese nodo serán enviados al atacante en lugar de su destino original.

D. Denial of Service (DoS)

Ataque que consiste en negar algún tipo de recurso o servicio, puede ser usado para inundar la red con pedidos de disociación imposibilitando así el acceso de los usuarios.

E. Dictionary Attack

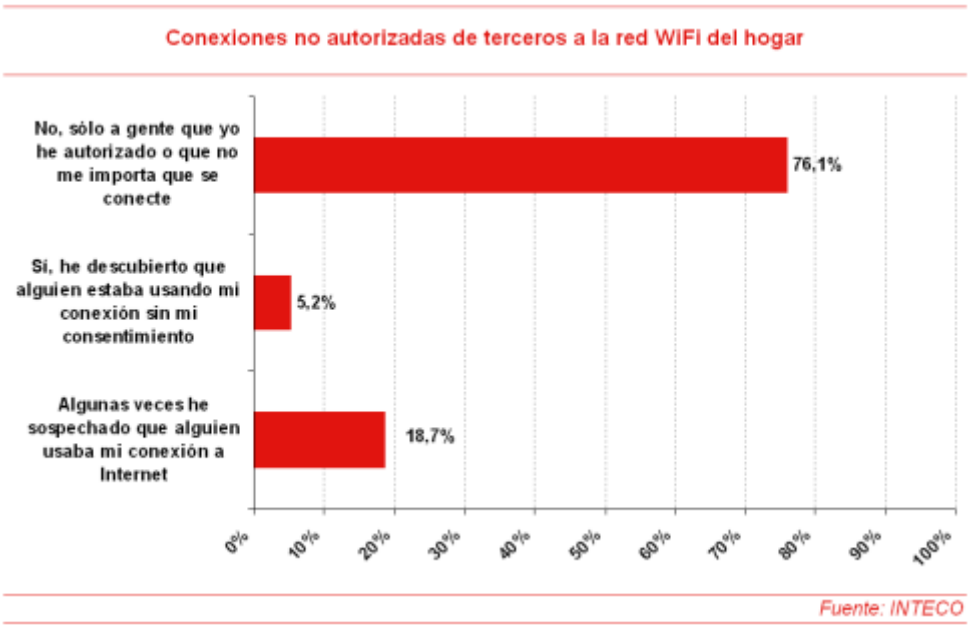
El ataque de diccionario es un método que consiste en averiguar una contraseña probando con todas las palabras del diccionario.

F. Ataques de recuperación de claves

El ataque de recuperación de claves es un método que consiste en capturar tramas de un cliente y a través de la ejecución de un programa obtener la clave de acceso, este ataque fue concretamente probado y declarado en el uso con WEP.

Para finalizar el recuento de los principales ataques a redes Inalámbricas identificados hasta hoy en día es importante mencionar que los ataques por parte de los intrusos son posteriores a la identificación de redes Inalámbricas con baja seguridad de acceso. Cada tipo de ataque explota una vulnerabilidad descubierta; al proceso de ubicación, identificación y clasificación por niveles de seguridad de redes Inalámbricas se le conoce como Wardriving y Warchalcking.

A continuación se muestra como referencia un esquema de indicadores tomados entre Abril y Junio del 2008 que muestra el porcentaje de intrusos detectados en redes privadas en hogares, esta encuesta fue tomada en España.



Esquema 8: Encuesta de seguridad e infiltración en redes inalámbricas - España 2008

2.3.2 Protocolos de seguridad

Las redes Inalámbricas se basan en un medio compartido y el riesgo de su uso aumenta considerablemente si no se aplica en la transmisión alguna protección de seguridad.

Los protocolos criptográficos son la protección frente a la intercepción del tráfico. La seguridad de las redes debe cumplir con tres objetivos primordiales:

- Confidencialidad

  Es el término utilizado para describir los datos que se encuentran protegidos ante la intercepción de cualquier parte no autorizada.

- Integridad

  Significa que los datos no han sido modificados desde el emisor hasta el receptor.

- Autenticación

  Es la base en cuestiones de seguridad, pues parte de la fiabilidad de los datos es conocer con certeza el origen.

A continuación se presenta el resumen de la evolución de los protocolos de seguridad en los últimos años.

Tabla 20: Resumen cronológico de estándares de seguridad Inalámbrica

Fecha	Estándar	Comentario
1997	802.11 / WEP	802.11 salió al mercado para ofrecer soluciones Inalámbricas con velocidades de 1Mbps y 2 Mbps y usando WEP como seguridad.
1999	802.11a	802.11a es lanzado al mercado con velocidades de hasta 54 Mbps pero con una frecuenta distinta, se sigue usando WEP.
1999	802.11b	A finales de 1999 lanzan 802.11b con velocidades de 5.5 Mbps y 11 Mbps pero guardando compatibilidad con el estándar original.
2001	802.1X	En abril del 2001 es desarrollado el protocolo 802.1X para paliar las necesidades de seguridad.
2003	802.11g	802.11g es lanzado al mercado con velocidades de hasta 54 Mbps manteniendo compatibilidad con la frecuencia original.
2003	Protocolos ULAP	Los protocolos ULA (Upper Layer Protocol) fueron soluciones propietarias temporales mientras se terminaba el 802.11i
2003	WPA	A mediados del 2003 sale la primera versión de WPA (WPA1) que se basa en el tercer borrador de 802.11i con la implementación de TKIP
2004	802.11i	Finalización del nuevo estándar de seguridad, incluyen nuevos protocolos rediseñando WEP.
2004	WPA 2	Lanzado a mediados del 2004 y cumple con el estándar 802.11i

Elaboración: Propia

Hace unos años WEP se consideraba un sistema de seguridad poco seguro, ante esto la IEEE formo un grupo de trabajo llamando 802.11i para mejorar la seguridad en la capa MAC. Entre el intervalo de tiempo desde la investigación y estudio de los fallos WEP y el

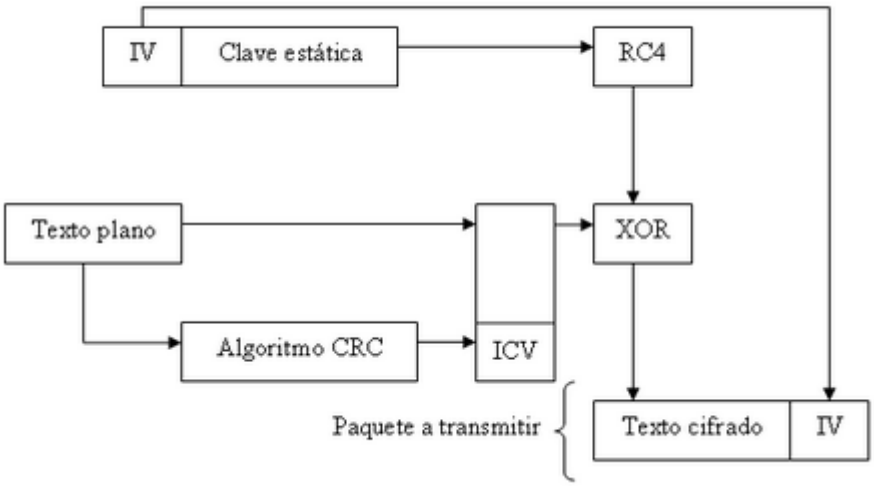
desarrollo de nuevas tecnologías, los administradores de red optaron por protocolos de seguridad de capas superiores en la pila como IPSEC (Capa 3), SSL (Capa 4) y SSH (Capa 7) que ofrecían un nivel de seguridad mayor a WEP. Con el desarrollo de nuevas tecnologías en la capa de enlace, los protocolos de seguridad de capas mayores pasaron a dejar de usarse pues su uso era bastante complejo y limitado. Una solución de redes Inalámbricas seguras es a través del uso de estas nuevas tecnologías de la capa de enlace y posteriormente determinar si se requiere el uso de protocolos adicionales de capas superiores. A continuación se revisa en detalle los principales protocolos de seguridad desarrollados hasta la fecha.

2.3.2.1 WEP (Wired Equivalent Privacy)

Protocolo de seguridad implantado en el estándar 802.11 y desarrollado en la capa MAC. WEP comprime y cifra los datos que se envían a través de las ondas de radio para que solo el destinatario asociado pueda acceder a ellos, los niveles de seguridad brindados por WEP son cifrados de 64 y 128 bits. WEP utiliza el algoritmo de encriptación RC4 proporcionado por RSA Security para proteger los datos.

WEP trabaja con claves de acceso que son configuradas en el AP y en los clientes, permitiendo configurar hasta 4 claves de acceso, ante un cambio de la clave de acceso en el AP, el mismo cambio debe ser realizado en todos los clientes manualmente.

El modo de trabajo de WEP no se detallará por no ser el objetivo de la presente tesis; sin embargo se muestra el esquema de trabajo de WEP en donde a partir de la carga útil a proteger, la clave secreta y el Vector de Inicialización (IV) se obtiene una trama cifrada para la transmisión.



Esquema 9: Esquema de trabajo de WEP

Tras el lanzamiento de WEP se pensó que cubriría todos los niveles de seguridad requeridos para los enlaces Inalámbricos. Sin embargo, veremos que WEP no otorga los niveles deseados pues durante los primeros cuatro años de vida de 802.11, los investigadores descubrieron la gran inseguridad en el uso de este protocolo. Los criptógrafos han identificado fallos en WEP que se han venido corrigiendo eventualmente con la incorporación de nuevos protocolos, sin embargo, los fallos más problemáticos y difíciles de corregir son los fallos de errores de implantación. Estos fallos de diseño fueron publicados cuando el grupo Internet Security Applications Authentication and Cryptography (ISAAC) de la universidad de California, Berkeley hizo un análisis del estándar WEP. Se presenta en resumen los puntos identificados por el grupo ISAAC

1. La administración manual de claves, el nuevo sistema de claves debe ser dinámico.
2. La longitud del secreto compartido es de solo 40 bits, luego de la publicación de los fallos en WEP, la longitud de la clave extendida es de 104 bits.
3. Códigos de flujo vulnerables al análisis cuando se reutiliza el flujo de claves.
4. WEP utiliza CRC para la comprobación de integridad el cual no es criptográficamente seguro.
5. Ataque al punto de acceso en la retransmisión de tramas cifrados por WEP, haciendo posible que el punto de acceso retransmita la información a la estación del atacante.

2.3.2.2 Autenticación de usuarios con 802.1X

WEP intentaba ofrecer muchas soluciones para múltiples problemas, por un lado la autenticación mediante el uso de claves para los usuarios y por otro la confidencialidad usando el cifrado de datos a medida que recorrían los enlaces Inalámbricos. En conclusiones finales WEP no funciona particularmente bien.

En abril del 2001 es lanzado el protocolo 802.1X que aborda el problema de autenticación proporcionada en la capa de enlace. Hasta la fecha 802.1X ha madurado bastante y a diferencia de WEP que autentica a las maquinas, 802.1X autentica al usuario, ofreciendo mayor flexibilidad y seguridad, además permite la autenticación mutua entre los clientes y la red, asegurando que los clientes se conecten a redes legitimas y autorizadas. 802.1X posee un esquema que se basa en tres componentes principales:

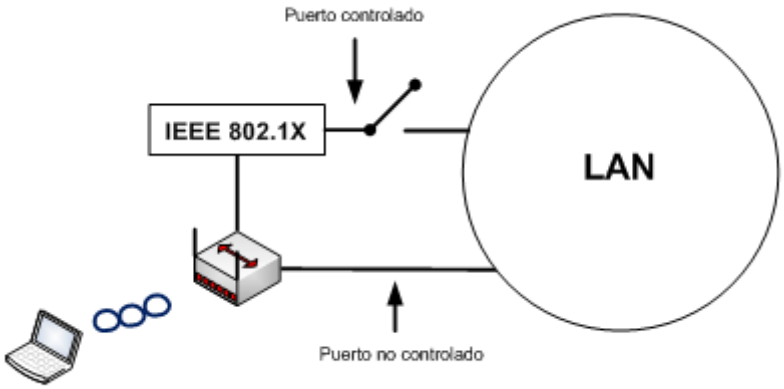
- El solicitante: Generalmente el software del equipo del cliente.
- El autenticador: El punto de acceso.
- El Servidor de Autenticación (AS): Encargado de realizar la autenticación real de las credenciales proporcionadas por el cliente.

El servidor de Autenticación yace en la red cableada pero también es posible su implementación en un punto de acceso. El tipo de servidor podría ser RADIUS (Remote Authentication Dial-In User Server) u otro compatible con 802.1X.

El estándar 802.1X introduce un nuevo concepto de autenticación, el concepto de puerto habilitado/inhabilitado. Cuando un cliente intenta conectarse con un AP, este lo detecta y activa un puerto lógico para autenticarlo, en esta fase este puerto de comunicación permanece deshabilitado permitiendo solamente tráfico relacionado a 802.1X. El cliente usando EAP (Extensible Authentication Protocol) brinda su identidad al punto de acceso quien remitirá la solicitud al servidor de autenticación, en donde en base a las credenciales que posea el cliente, se permitirá o negara el acceso a la red. Si el acceso es concedido el puerto de comunicación pasa a estado habilitado, permitiendo así la transmisión de data.

Debido a que múltiples clientes inalámbricos deben compartir el mismo canal para efectuar transmisiones se necesita una extensión del protocolo 802.1X para permitir que un Punto de

Acceso reconozca el tráfico de cada cliente. Esto se consigue mediante el intercambio de una clave de sesión única asignada a cada cliente. Solo clientes autenticados cuentan con una clave de inicio de sesión asignada por el AP que le permite a este discernir entre tráfico de clientes autenticados y clientes sin autenticar. Con este simple esquema centralizado de funcionamiento, 802.1X tiene el potencial de simplificar la gestión de grandes despliegues inalámbricos. A continuación se muestra el esquema de puerto habilitado/Inhabilitado manejado por 802.1X.



Esquema 10: Puerto habilitado / Inhabilitado de 802.1X

2.3.2.3 Protocolos ULAP (EAP en 802.1X)

802.1X trabaja conjuntamente con el protocolo EAP (Extensible Authentication Protocol) para la autenticación. EAP es un protocolo de estructura que en lugar de definir como se deben autenticar los usuarios permite a los diseñadores de protocolos crear sus propios métodos EAP que finalmente ejecutan los niveles de autenticación. EAP ha sido el protocolo usado por soluciones propietarias para crear sus modelos de seguridad en el periodo de tiempo en el que el grupo 802.11i se encontraba aun trabajando en el nuevo estándar.

Actualmente existe en el mercado una diversidad de soluciones propietarias aplicadas a las capas más altas del modelo OSI, los cuales son conocidos como protocolos ULA (Upper Layer Protocol) teniendo entre las principales a las siguientes:

- LEAP (EAP-Cisco Wireless)

  Desarrollado por Cisco, basa su popularidad por ser el primero y durante mucho tiempo el único mecanismo de autenticación basado en password y proporcionar acceso a clientes con distintos Sistemas Operativos. LEAP presenta un esquema de autenticación compatible con la Base de Datos del AD de Microsoft.

- EAP-TLS

  Propuesto por Microsoft, ofrece una fuerte autenticación mutua basada en credenciales de seguridad y llaves dinámicas, el único punto débil es que requiere un despliegue de certificados digitales en todos los usuarios de la red así como en los servidores RADIUS.

- EAP-TTLS

  Propuesto por Funk Software y Certicom, permite una fuerte autenticación mutua basada en credenciales de seguridad y llaves dinámicas pero solamente requiere que los certificados digitales sean distribuidos a los servidores RADIUS. Compatible con base de datos de usuarios como Windows Active Directory, SQL, LDAP, etc.

- EAP-PEAP

  Propuesto por Microsoft, Cisco y RSA Security. Utiliza el TLS (Transport Layer Security) para establecer un túnel e intercambiar certificados. En este caso los certificados disminuyen de cientos o miles a unos pocos que puede generarse a través de un emisor de certificados pequeño.

- EAP-FAST

  Propuesto por Cisco para reemplazar a LEAP y PEAP por las debilidades encontradas en el primero y la complejidad de uso del segundo. El uso de certificados digitales es opcional. EAP-FAST usa una credencial de protección de acceso (PAC) para establecer un túnel TLS para que el cliente envíe las credenciales de acceso al servidor de autentificación. Compatible con MS-CAHPv2 para la autenticación interna.

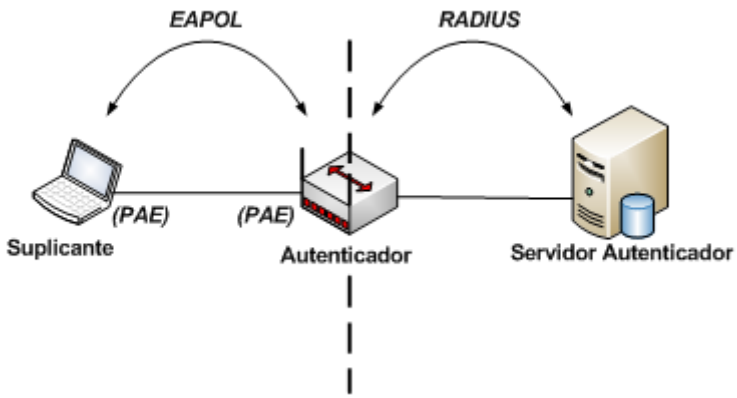
A continuación se muestra la Tabla 21 con la comparación de los protocolos EAP revisados:

Tabla 21: Protocolos de seguridad ULAP

TEMA	LEAP (Cisco)	EAP-TLS	EAP-TTLS	EAP-PEAP	EAP-FAST
Solución de Seguridad	Patente	Estándar	Estándar	Estándar	Patente
Certificados-Clientes	No requiere	Si	Opcional	Opcional	Opcional
Certificado-Servidor	No requiere	Si	Si	Si	Opcional
Credenciales de Seguridad	Deficiente	Buena	Buena	Buena	Buena
Soporta Autenticación BD	AD	AD	AD, SQL, LDAP	No	AD, SQL, LDAP
Intercambio de llaves dinámicas	Si	Si	Si	Si	Si
Autenticación Mutua	Si	Si	Si	Si	Si

Elaboración: Propia

Finalmente se muestra la arquitectura de autenticación de 802.1X usando tramas EAP entre el cliente y el AP y tramas RADIUS entre el AP y el servidor de Autenticación.



Esquema 11: Arquitectura de Autenticación 802.1X

2.3.2.4 Estándar 802.11i

802.1X proporciono la estructura para la autenticación y administración de claves, dos de los puntos débiles de WEP, el otro fallo pendiente era la falta de confidencialidad.

802.11i ofrece una solución para superar las vulnerabilidades en el cifrado de la capa de enlace, para lo cual utiliza el protocolo de claves temporales (TKIP, Temporal Key Integrity Protocol) y el protocolo de modo de contador con CB-MAC (CCMP, Counter Mode with CBC-MAC Protocol).

A. TKIP (Temporal Key Integrity CBC-MAC Protocol)

La principal motivación de desarrollo para TKIP fue actualizar la seguridad de Hardware basado en WEP. Esto es, permite el cambio de claves dinámicamente manteniendo la compatibilidad con el Hardware utilizado actualmente.

Para hacer frente a los ataques WEP, TKIP incorpora dos mejoras, las cuales son aumentar el tamaño del vector de Inicialización y la mezcla de claves.

TKIP dobla la longitud del vector de Inicialización de 24 a 48 bits, este aumento incrementa el tamaño del espacio de 16 millones a 281 trillones. TKIP también realiza la mezcla de claves RC4 usada para cada trama. La mezcla de claves de cifrado amplía más el espacio del vector de Inicialización. Al cambiar la clave para cada trama TKIP evita la recopilación de información que comparten los mismos bits secretos de datos para el atacante. Las mejoras incluidas por TKIP han permitido brindar mejoras de seguridad contra ataques como por ejemplo, ataques de recuperación de claves.

B. CCMP (Counter Mode with CBC-MAC Protocol)

Este protocolo fue desarrollado desde cero por la IEEE y está basado en el código de bloque Estándar de Cifrado Avanzado (AES, Advanced Encryption Standard). 802.11i acuerda el uso de AES con claves de 128 bits.

Este protocolo de seguridad de la capa de enlace permite el uso de una misma clave en el cifrado para la confidencialidad, así como para crear un valor de comprobación de integridad criptográficamente seguro. El uso de CCMP es obligatorio si se está usando 802.11i.

2.3.2.5 WPA

El acceso protegido a Wi-Fi (WPA, Wi-Fi Protected Access) es un estándar comercial proporcionado por Wi-Fi Alliance. Resolver los problemas de diseño descubiertos en WEP llevo a la IEEE a la generación de nuevos protocolos, TKIP y CCMP, sin embargo, CCMP fue desarrollado desde cero, siendo lógico esperar que TKIP estuviera listo mucho antes que CCMP.

Para mejorar los problemas de seguridad y ofrecer cierta tranquilidad a los usuarios 802.11; Wi-Fi Alliance agilizo el despliegue de TKIP introduciendo un estándar comercial WPA. La

versión 1 de WPA se basa en el tercer borrador de 802.11i finalizado a mediados del 2003 y la versión 2 de WPA que cumple con todos los estándares de 802.11i (TKIP y CCMP) fue lanzada a mediados del 2004.

2.4 Gestión y Administración de Redes Inalámbricas

Las redes inalámbricas configuradas con características básicas de acceso generalmente poseen un diseño inadecuado para grandes despliegues, encontrándose instaladas como un conjunto de AP´s distribuidos con el propósito de cubrir un área deseada. Este tipo de esquemas Inalámbricos presentan por lo general los siguientes inconvenientes:

- No contar con una cobertura homogénea en todas las zonas deseadas dejando "huecos de cobertura", los que forman parte de la problemática de despliegue de este tipo de redes cuyas condiciones se vuelven más críticas al considerar esquemas que impliquen una cantidad elevada de AP (cientos de dispositivos WLAN).
- Al no tener una adecuada gestión de los equipos, se presentan problemas de control de acceso, seguridad, monitoreo del servicio, congestión, monitoreo de fallos, entre otros.

Por lo tanto, la gestión de los equipos es un punto clave que permite un nivel de escalabilidad alta y controlada para los Administradores de red. Entre las principales ventajas de contar con una plataforma de Administración para redes Inalámbricas de mediando a gran tamaño, podemos mencionar las siguientes:

- Simplificación en las configuraciones, despliegues y Administración de los AP´s.
- Administración total de toda la red Inalámbrica, permitiendo conocer que está pasando en cualquier lugar en cualquier momento.
- Control y monitoreo de todos los AP´s, usuarios, protocolos de seguridad usados por los clientes, entre otros.
- Generación de reportes de toda la red Inalámbrica, permitiendo así conocer el performance de la misma en todo momento.

Los puntos mencionados son posibles de lograr en un esquema integrado, sin embargo, bajo el esquema de equipos Standalone lograr estas funciones demandaría una alta

cantidad de recursos humanos y tiempo. Debido a esto, varios fabricantes desarrollaron soluciones bajo el esquema de productos integrados. A continuación se muestra una revisión de las principales soluciones desarrolladas por los proveedores de tecnología en infraestructuras inalámbricas y disponibles hoy en el mercado.

2.4.1 Solución DLink

Fundada en 1986, DLink basa sus productos principalmente en conectividad Ethernet, desarrollando soluciones en la comunicación de voz y data.
En el campo de las redes inalámbricas, DLink ofrece soluciones en los sectores de casa, pequeñas y medianas empresas. Sin embargo, todas las soluciones de DLink son dispositivos con mejoras técnicas con Access Point trabajando en modo "Standalone", sin involucrar una mejora en la administración.

Durante el Q3 de 2009, DLink anuncio nuevos productos que permiten una mejora en la gestión y administración de sus puntos de acceso inalámbrico, destinados a redes pequeñas. La nueva herramienta ha sido llamada "AP Array" y viene integrada en todos los productos de la generación de DLink, asimismo muchos de los equipos antiguos también podrán contar con esta utilidad haciendo una actualización del firmware.

AP Array, permite manejar hasta ocho puntos de acceso y configurar uno de los puntos de acceso como principal para posteriormente replicar su configuración en los demás. Ofreciendo un nivel de administración básico y sencillo. DLink ofrece una solución integral orientada a empresas muy pequeñas por la poca cantidad de puntos de acceso que permite administrar.

2.4.2 Solución 3com

Fundada en 1979, dedicada a mejorar los problemas de seguridad, facilidad de uso y rendimiento en las redes actuales. Dentro de las soluciones desarrolladas por 3com orientadas a redes inalámbricas se puede observar una mayor preocupación en el desarrollo de una plataforma de gestión y centralización de la administración.

La plataforma inalámbrica desarrollada por 3com permite cubrir varios de los requisitos que un administrador de red pudiera encontrar previo a la implementación de la misma. La solución inalámbrica propuesta por 3com denominada “3com Wireless LAN Mobility” se basa en el uso de los siguientes dispositivos:

2.4.2.1 3com Wireless LAN Managed Access Point

En la gamma de puntos de acceso, 3com presenta soluciones en AP con modalidades de trabajo Standalone denominadas “FAT AP” y puntos de acceso con modalidad de trabajo centralizada denominados “FIT AP”. Los FAT AP como por ejemplo el 3com Wireless 8760, son equipos que incorporan la administración, seguridad, configuración y todo lo necesario en el equipo mismo, exigiendo esto mayores recursos y por ende un mayor costo del dispositivo. Por otro lado los FIT AP como por ejemplo el 3com Wireless 3950, son equipos que se encargan de tareas puntuales como la encriptación de la información, las demás tareas son centralizadas y ejecutadas por el 3com Wireless Switch Manager y el 3com Wireless LAN Controller.

2.4.2.2 3com Wireless LAN Controller

Este equipo diseñado por 3com permite la administración de los Access Point 3com, integrando decenas y hasta centenas de Access Point. El 3com Wireless LAN Controller al usarse en conjunto con el 3com Wireless Switch Manager Software permite ofrecer servicios adicionales a la Administración de la red Inalámbrica.

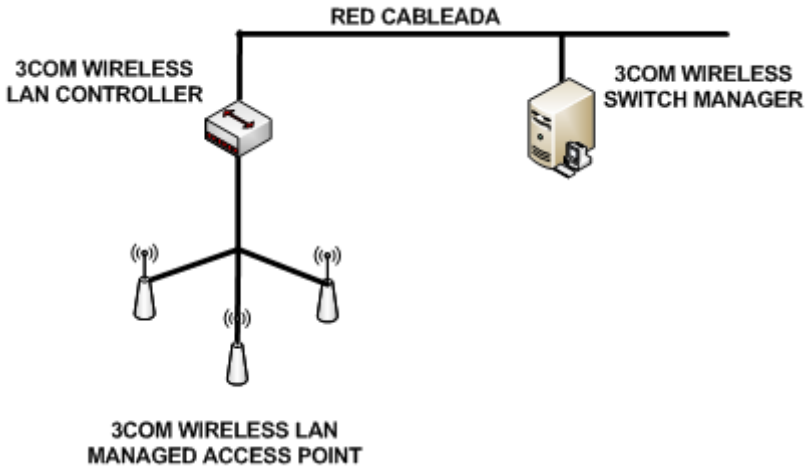
2.4.2.3 3com Wireless Switch Manager Software

Software de administración en reglas y políticas para la red inalámbrica, se integra con el Wireless LAN Controller en su aplicación. Actúa como el cerebro del sistema permitiendo una administración más sencilla y flexible de la red, su instalación es compatible con servidores Microsoft.

Estos dos equipos (El 3com Wireless Switch Software y el 3com Wireless LAN Controller) trabajan conjuntamente para ofrecer además de la Administración servicios agregados como Roaming, balanceo de carga, protección contra ataques, autenticación, encriptación entre

otros; permitiendo brindar una solución atractiva a un costo adecuado y con una seguridad extendida a todos sus clientes móviles.

A continuación se muestra el esquema de trabajo propuesta por 3com para la implantación y administración de sus redes inalámbricas.



Esquema 12: Solución 3COM para la Administración de redes Inalámbricas

2.4.2.4 Ventajas del Sistema

Como se mencionó, la plataforma centralizada desarrollada por 3com trae consigo mejoras, algunas de las cuales son detalladas a continuación.

A. Autenticación: Permite el despliegue de usuarios con contraseñas o certificados digitales para el acceso centralizando usando servidores AAA (como servidores RADIUS)

B. Encriptación: Ofrece compatibilidad trabajando con WEP dinámico, WPA/TKIP y WPA/AES. Adicionalmente incorpora herramientas automatizadas para la gestión y control de la seguridad como la detección de puntos de accesos de intrusos.

C. Herramientas para el despliegue de nuevos equipos: Incorpora una herramienta la cual usando un plano de la zona a cubrir y los puntos de acceso ya instalados como input, permite calcular y mostrar las mejores ubicaciones de nuevos puntos de

acceso, dejando así de lado el método antiguo de prueba error, el cual consta de instalar los equipos y probar la cobertura.

D. Seguridad ante ataques: 3com Wireless LAN Mobility System incorpora herramientas adicionales para mejorar el despliegue y contrarrestar ataques externos, como por ejemplo, los siguientes:

- Rogue Access: Hace frente a este tipo de intrusiones usando los puntos de acceso distribuidos, los cuales pueden detectar SSID no autorizados para comunicar al Controller el cual comparara la MAC del nuevo dispositivo con la lista que él tiene y al no encontrarlo emitirá una alerta de intrusión al Administrador.

- Denial of Services (DoS): Ante este tipo de ataques, el sistema propuesto por 3com establece que cuando un cliente excede el tiempo especificado de asociación, el cliente automáticamente es colocado en una lista negra, en la que permanecerá hasta que el Administrador lo considere.

2.4.3 Solución Cisco

Fundada en 1984 es una empresa dedicada a brindar soluciones de Networking, actualmente presenta soluciones en redes inalámbricas tanto para empresas que usan equipos de manera distribuida, como para empresas que adquieren todo un sistema integrado y unificado.

El esquema de administración de redes Inalámbricas de Cisco tiene varios niveles y diversos productos que trabajan a nivel de capas y servicios. Entre los principales productos para redes Inalámbricas en el mercado desarrollados por Cisco tenemos los Access Point, el Wireless LAN Controller, el Cisco Wireless System, el Cisco Secure Access Control, entre otros.

La creación de un sistema unificado involucro la tarea de centralizar la mayoría de los servicios en un dispositivo central y permitir la comunicación de este con todos los demás dispositivos involucrados. Para este requerimiento Cisco desarrollo un nuevo lenguaje de

comunicación, un nuevo protocolo el cual fue llamado Lightweight Access Point Protocol (LWAPP).

2.4.3.1 Lightweight Access Point (LAP)

En la solución unificada, integrada y centralizada presentada por Cisco los equipos de control y gestión deberían ser capaces de comunicarse y obtener los datos necesarios de los Access Point, sin poner en riesgo la seguridad en ninguna capa del sistema. Los objetivos presentados tras la creación de LWAPP fueron:

- Utilizar AP´s con el Hardware básico y de bajo costo, para lo cual se le debe quitar todo el trabajo necesario de estos equipos.
- Centralizar el trabajo de filtrado, QoS y autenticación en un dispositivo centralizado.
- Proponer un mecanismo de encapsulación y transporte.

A continuación se presentan los productos más utilizados para la administración de las redes Inalámbricas disponibles hoy en el mercado por Cisco.

2.4.3.2 Wireless LAN Controller (WLC)

El WLC de Cisco ofrece al Administrador una plataforma centralizada para la administración de todos los AP´s integrados al sistema, permitiendo configurar de una manera sencilla nuevos despliegues, protocolos de seguridad de acceso por usuarios y prioridades en la transmisión de data ofreciendo además diseños de redundancia del servicio proporcionando todo esto una alta calidad de confiabilidad. El WLC establece una comunicación constantes con los AP´s configurados en su interface a través de paquetes encapsulados transmitidos cada 5 minutos, permitiendo esto controlar y mantener un estado saludable de la red. La interfaz de administración del WLC es a través de un browser de internet. Cisco ofrece modelos de WLC´s que permiten manejar desde pocos AP´s hasta otros que manejan cientos de ellos, con una variedad de modelos que permiten integrar toda una gran gama de posibilidades, además para una fácil integración con una infraestructura de red ya instalada, existen modelos de controladores que se pueden integrar a un Router, a un Switch o simplemente adicionar a la red como un nuevo equipo en un Rack de comunicaciones. A continuación se presentan los modelos de WLC´s de Cisco actualmente en el mercado:

A. Standalone Controllers: Estos controladores son equipos diseñados para ser instalados en cualquier Rack de comunicaciones y se encuentran en los siguientes modelos:

- Cisco 5500 Series WLC: Permite la administración de 100 y 250 AP´s.
- Cisco 4400 Series WLC: Permite la administración de 12,25, 50 y 100 AP´s.
- Cisco 2100 Series WLC: Permite la administración de 6, 12 y 25 AP´s.

B. Integrated Controllers and Controller Modules: Estos controladores son módulos diseñados para ser integrados en Switches o Routers y se pueden encontrar en los siguientes modelos:

- Cisco Catalyst 6500 Series / 7600 Series Wireless Services Module (WiSM): Permite la administración de hasta 250 AP´s.
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controller: Permite la administración de hasta 25 y 50 AP´s.
- Cisco Wireless LAN Controller Module: Permite la administración de 6, 8, 12 o 25 AP´s y pueden ser integrados en los Integrated Services Routers 2800, 3800 y en el 3700 Services Routers.

2.4.3.3 Cisco Wireless System (WCS)

Cisco Wireless System (WCS), es la plataforma de Cisco que permite planificar, desplegar, monitorear, solucionar y generar reportes en las redes Inalámbricas. Esta plataforma permite conocer las necesidades de pequeñas, medianas y grandes empresas, integrando una diversidad de herramientas para el diagnostico y control del estado de las redes.

La plataforma se encuentra disponible para ser instalada en un servidor Windows o Linux y permite la administración de cientos de WLC o miles de AP´s. La licencia básica para la instalación del WCS permite la administración de hasta un máximo de 50 AP´s, sin embargo, para ambientes más grandes se pueden adquirir licencias adicionales que son agregadas a las que ya se tienen, las opciones disponibles ofrecen administración para 50 AP´s, 100 AP´s y 500 AP´s.
Dentro del alcance de esta plataforma podemos resumir los siguientes puntos:

- Planeamiento: Las herramientas incluidas otorgan un panorama completo de las señales RF de los AP´s, permitiendo así un adecuado diseño en futuras instalaciones.
- Despliegue: Cuenta con plantillas predeterminadas para la automatización en la administración de la red.
- Monitoreo: A través de su interfaz gráfica es posible identificar las fuentes de incidencias, así como el rendimiento en línea de la red, todo esto a través de lecturas de señales RF.
- Manejo de Incidencias: Integra herramientas que permiten conocer el detalle de las incidencias, la causa y solución de las mismas.
- Reportes: Otorga la flexibilidad de mostrar toda la información concerniente a nuestra red.

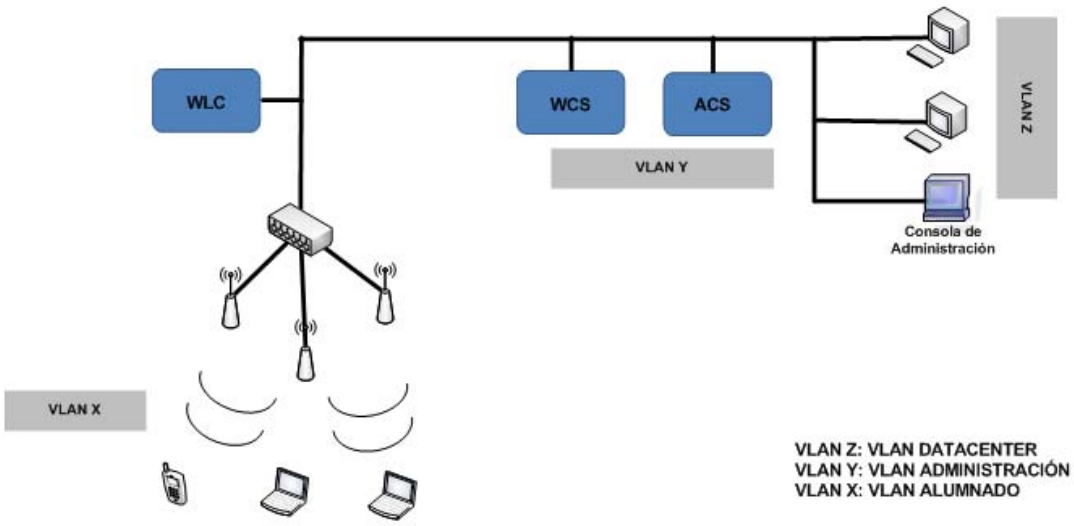
2.4.3.4 Cisco Secure Access Control (ACS)

El Cisco Secure Access (ACS), brinda la plataforma de centralización para la administración de políticas de acceso y se encuentra disponible tanto en Appliance como para ser instalado en un servidor Windows.

El ACS permite centralizar la autenticación, los accesos de usuarios y la administración de políticas de acceso. Dentro de las compatibilidades de este sistema podemos mencionar los siguientes:

- Databases Options: Permite la creación de una base de datos para la autenticación de usuarios, así como la integración de bases de datos existentes como Active Directory, LDAP, ODBC, entre otros.
- Authentication Protocols: Soporta varios protocolos de autenticación como PAP, CHAP, MS-CHAP, EAP, PEAP, entre otros.
- Network Access Policies: Permite la configuración de complejas políticas de acceso, como por ejemplo, restricción de dispositivos, horarios de acceso, escenarios de validación, entre otros.

A continuación se muestra la arquitectura de trabajo propuesta por Cisco, haciendo uso de los equipos mencionados para la implantación y administración de sus redes inalámbricas.



Esquema 13: Solución Cisco para la Administración de redes Inalámbricas

2.4.3.5 Ventajas del Sistema

A continuación se revisarán algunas mejoras introducidas por este nuevo modelo de administración desarrollado por Cisco:

A. Mejoras en despliegue

Usando una solución basada en AP´s trabajando individualmente, se debe configurar cada AP contando con tiempos elevados de configuración y pudiendo involucrar esta labor algún error involuntario. Adicionalmente en requerimientos de más de una Vlan de acceso para los clientes (por ejemplo, Vlan de invitados), es necesario la extensión de las mismas Vlan's a través de múltiples Switches hasta la capa de acceso de la red lo cual aumenta las configuraciones por cada Switch, introduce broadcast de dominio largo y aumenta los riesgos de seguridad.

En una solución integrada, el WLC usando imágenes embebidas permite la configuración y actualización necesaria de manera simultánea en todos los AP; así mismo, el subneteo y trunking de VLAN´S no es necesario llevarlo hasta la capa de acceso de la red pues el WLC centraliza el trunking simplificando así el despliegue y administración de las WLAN.

B. Administración dinámica de Radio Frecuencia (RF)

Las redes inalámbricas usando AP´s en modo Standalone generalmente son desplegadas con un plan donde cada AP tiene un canal y una potencia fija, esto es diseñado acorde a una predicción de RF usando simuladores de ambientes de RF; sin embargo, estas simulaciones se hacen sin contar con todos los datos necesarios, por ejemplo la interferencia en el mismo canal por señales cercanas o interferencias de edificios o equipos que usen la misma banda de frecuencia; por lo tanto no deja de ser solo un estimado del comportamiento de la RF. En un sistema integrado el WLC y el WCS permiten conocer y visualizar la intensidad de las señales entre los AP´s en la misma red. Esta información es usada por el sistema para crear topologías dinámicas de RF. Cuando un nuevo AP es instalado en la red, este busca al WLC y le envía información como la dirección MAC y la intensidad de las señales inalámbricas de sus vecinos en paquetes encriptados, con esta información el WLC sintoniza cada AP cercano al nuevo AP para una óptima intensidad en capacidad y cobertura, toda esta información se puede visualizar gracias al WCS.

C. Mejoras de Seguridad

El sistema dinámico de RF permite detectar intrusos en la red, usando los AP´s y el WLC los cuales actuaran como “recolectores de datos” y “sensores IDS”. De la misma manera en que los AP´s pueden detectar la señal de los otros AP´s, también pueden obtener información de la señal de los clientes para el seguimiento o identificación, esta información es reenviada por el WLC al WCS (Wireless Control System) y al Wireless Location Appliance.

D. Balanceo de Usuarios

802.11 otorga a cada cliente el mismo tiempo para transmitir y cada cliente decide a que AP asociarse, generalmente este es al AP con mayor intensidad de señal. Debido a que las señales de RF no son fijas, la mayoría de los clientes pueden asociarse al mismo AP disminuyendo esto el performance de este AP que tendría más clientes conservando el mismo tiempo de acceso al medio; esta desventaja es llamada “Meeting Room Effect”.

En el sistema Unificado de Cisco, los WLC tienen información actualizada sobre las señales de los AP en la red, además cuando un cliente “sondea” un AP el WLC escucha este “sondeo” decidiendo posteriormente que AP debe responder, en base a

su relación de Intensidad de Señal con la Intensidad del ruido en el cliente y las conexiones actuales.

E. Roaming

Tener una solución basada en AP´s en modo Standalone y permitir Roaming, involucra extender las Vlan's entre múltiples Switches hasta la capa de acceso de la red, introduciendo broadcast de dominio largo.

Con un sistema centralizado todos los AP reciben una dirección IP de la red local de Administración; los clientes tendrán una dirección IP de la sub red en donde está conectado el WLC (no la red Administrativa de la empresa) y enviaran data que será encapsulada en paquetes LWAPP y enviados por un túnel a través de la red de la empresa hacia el WLC. El WLC es el encargado de centralizar toda la administración del Roaming y del túnel entre una red y otra. Así mismo, el Roaming usando un sistema centralizado permite la mejora de servicios, como por ejemplo la voz sobre IP, ya que a diferencia del despliegue por AP´s individuales mejora la predicción del CAC (Call Admission Control) permitiendo identificar las llamadas a fin de contar con suficiente capacidad de tránsito entre AP´s.

Para finalizar este capítulo, se muestran dos herramientas desarrolladas netamente para la administración de ciertos servicios dentro de una red inalámbrica; este tipo de soluciones generalmente son implantadas sobre la infraestructura de una red ya instalada, por lo que muchas veces se deben realizar algunas modificaciones en la infraestructura a fin de implantar este modelo de solución. Por otro lado si se está analizando la instalación de una red inalámbrica desde el inicio y los objetivos son similares a los abarcados por este tipo de solución, podría considerarse su uso. A continuación se mencionan las dos opciones más resaltables actualmente en el mercado.

2.4.4 Solución Esemtia

Empresa española fundada en el año 2001, orientada a brindar soluciones avanzadas en el campo de las Tecnologías de la Información y servicios móviles. NetDiligens es un producto de Esemtia, desarrollado en Linux, permite optimizar la gestión y administración de las redes

informáticas ofreciendo servicios integrados como la función de un Router, Firewall, lista de acceso, filtro de contenidos (proxy), gestión de Ancho de Banda, monitorización, entre otros.

Esemtia integra muchas funciones en un solo equipo, muchas veces esta práctica no es recomendable y por el contrario existe una tendencia entre los administradores de TI para la distribución de los servicios en más de un equipo. Además, revisando las especificaciones técnicas del producto, se verifica que el Appliance no cuenta con muchos recursos de Hardware, por lo que centralizar todos estos servicios en este equipo podría traer consecuencias como la lentitud en horas puntas o con el aumento de clientes.

2.4.5 Solución Amigopod

Empresa creada en el año 2006 en Sídney, ofrece soluciones de administración sencilla para el acceso a red. Amigopod brinda soluciones de acceso a invitados para redes inalámbricas. El equipo que brinda esta solución es una Appliance diseñado para suplir las necesidades de acceso inmediato para los visitantes (desde 50 a 1000 visitantes).
Básicamente esta solución está orientada a ofrecer un servicio muy sencillo, brindar acceso a los visitantes a una red inalámbrica y administrar este servicio sin necesidad de contar con conocimientos informáticos. Este tipo de necesidades es bastante común en casos como hoteles, instalaciones deportivas, transporte, etc.

CAPITULO 3
PROPUESTA DEL SISTEMA

En el presente capítulo se mencionarán los requisitos necesarios que debe cumplir la solución al marco problemático descrito en el Capitulo 1 haciendo uso de las tecnologías referentes revisadas en el Capitulo 2. Finalmente se mostrará un listado de las principales características que incluirá el diseño de solución propuesto.

3.1 Hipótesis

Dada la necesidad de contar con una red inalámbrica que soporte muchos puntos de acceso, gran cantidad usuarios con diferentes perfiles, seguridad, capacidad de ampliaciones futuras y gestión centralizada y existiendo las tecnologías de acceso y de gestión de redes Inalámbricas en el mercado orientadas a brindar solución a ese tipo de necesidades; se propone el diseño de una red de acceso inalámbrico que permita ofrecer niveles adecuados de confiabilidad, seguridad y rendimiento para los clientes así como la gestión centralizada para los administradores del sistema.

3.2 Objetivos

3.2.1 Objetivo Principal

Diseñar una red que garantice los niveles de cobertura, acceso, rendimiento, seguridad y administración de acuerdo a la necesidad de CENTRUM.

3.2.2 Objetivos Secundarios

- Conocer la problemática actual de acceso inalámbrico de CENTRUM y sus sedes de provincia.
- Identificar las necesidades de demanda, seguridad y gestión necesarias para un mejor servicio de acceso a información brindado por CENTRUM.
- Identificar las deficiencias de los sistemas de red Inalámbricas actuales.
- Familiarizarse continuamente con los nuevos productos de los proveedores en la línea de redes Inalámbricas.
- Conocer las diversas soluciones para gestionar las redes inalámbricas.
- Conocimientos avanzados en el diseño y comportamiento de las redes Inalámbricas.
- Calcular y revisar las mejoras del nuevo diseño de red Inalámbrica.
- Determinar los costos de la solución a implementar.

3.3 Características

El sistema propuesto contará con las siguientes características.

- Escalabilidad

Permite la administración desde pocos AP (desde 6) hasta cientos de ellos, permitiendo el crecimiento hacia grandes redes sin mayores modificaciones del diseño original, ofreciendo la flexibilidad de agregar nuevos equipos o nuevas licencias.

- Rendimiento

Cuenta con un control de acceso a la WLAN por AP balanceando los clientes y garantizando los mejores escenarios de conectividad. Asimismo, el comportamiento dinámico de las señales RF permite contar con niveles homogéneos de cobertura.

- Seguridad

Contará con niveles de seguridad basados en la autenticación de los usuarios usando 802.1x y el uso del protocolo EAP-FAST para la protección de las credenciales de acceso.

- Monitoreo en línea

Permite el monitoreo en línea del estado de los equipos, las señales inalámbricas e interferencias externas.

- Manejo y asignación de perfiles en clientes

El sistema ofrece un nivel de automatización y prevención en la asignación de perfiles de los clientes al conectarse a la WLAN, permitiendo la disminución de carga laboral. Adicionalmente permite contar con el perfil invitado, sin poner en riesgo la seguridad de la red.

- Políticas de red

El sistema permite la programación de configuraciones en grupo, además de poder agendar dichas configuraciones, lo cual lo hace un sistema bastante flexible.

- Administración centralizada

La administración de todo el sistema se logrará desde una consola de administración centralizada contando con los niveles adecuados de seguridad.

- Roaming

La cobertura de señal RF y los controladores del sistema, garantizan el Roaming para el uso de aplicativos como el de la Voz sobre IP.

- Gestión de incidencias

Permite establecer avisos de alerta ante cualquier incidencia presentada en los equipos del sistema usando para su difusión correos electrónicos o mensajes de texto.

- Intranet e Internet en provincias

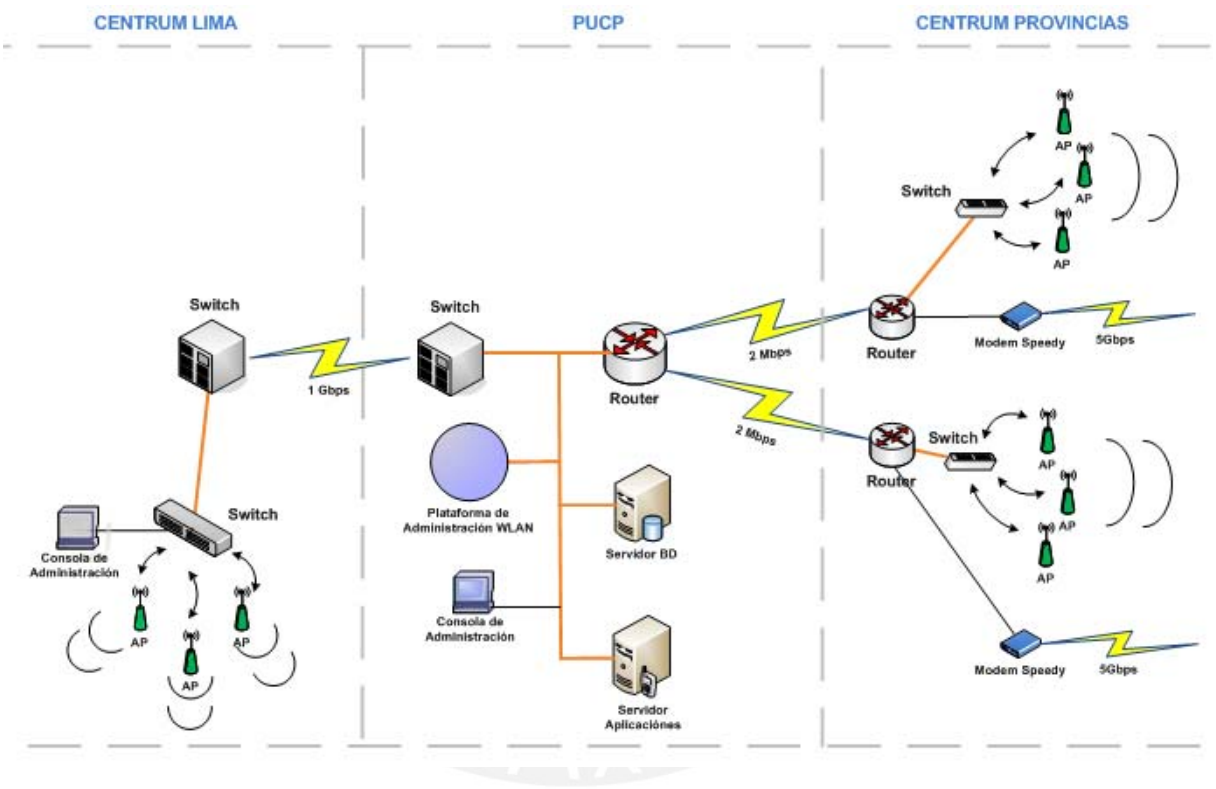
El sistema permite reconocer las solicitudes de Intranet de las de Internet en provincias, garantizando el uso total del Ancho de Banda dedicado a la Intranet para un adecuado uso.

- Respaldo del servicio

Los equipos que permiten la administración de la red, contaran con un sistema de contingencia del servicio, que permitirá garantizar el servicio en Lima y provincias.

3.4 Propuesta

La solución propuesta involucra el despliegue de 86 Access Point distribuidos entre las sedes de CENTRUM Católica a nivel nacional y la instalación de aplicaciones CISCO (Hardware y Software) para el manejo de perfiles de clientes contando con un nivel adecuado de seguridad; así como la centralización y administración de toda la red Inalámbrica desde una consola en la red Interna. A continuación se muestra el esquema reducido del diseño propuesto:



Esquema 14: Propuesta de Diseño de la red Inalámbrica

CAPITULO 4
DISEÑO DE LA SOLUCIÓN INALAMBRICA Y DEL SISTEMA DE ADMINISTRACIÓN

De la revisión de las distintas soluciones presentes actualmente en el mercado para esquemas de redes Inalámbricas y contrastándolas con las necesidades actúales de CENTRUM Católica; se determina que la propuesta desarrollada por Cisco ofrece la opción más adecuada debido al alcance de la solución, la seguridad del sistema, la robustez de la plataforma, el manejo de usuarios así como la escalabilidad y la compatibilidad que presenta con el esquema actual Inalámbrico de CENTRUM.

4.1 Diseño de la Red Inalámbrica

En este apartado se replanteará el diseño Inalámbrico local de cada una de las sedes de CENTRUM con miras a la integración y la gestión centralizada de la administración del sistema a nivel nacional.

4.1.1 Distribución de los AP en las Sedes de CENTRUM

Se presenta la nueva distribución de los Access Point en cada una de las sedes de CENTRUM, tomando como factores de diseño la cantidad de alumnos, el área de cobertura, la interferencia entre AP´s, el material de construcción y la distribución de los alumnos en las aulas. Es importante mencionar que las coberturas mostradas a continuación son coberturas proyectadas y basadas en la experiencia en el trabajo de redes Inalámbricas y que además probablemente el campo de cobertura sea mayor al momento del despliegue, sin embargo, para efectos del análisis de la presente tesis este factor pasa a ser secundario al tener en cuenta el uso de protocolos de autenticación y perfiles de acceso.

A continuación se presenta en detalle el diseño Inalámbrico de cada una de las sedes de CENTRUM. Para efectos de cada diseño de las sedes de provincia, se consideró los datos mostrados en la tabla 14 y 15 de la presente tesis (Estudio del Ancho de Banda – Sedes Provincia).

A. Sede de Lima

- Aulas

  CENTRUM cuenta con 17 aulas destinadas al dictado de clases con una capacidad total de 680 alumnos (40 alumnos por aula aproximadamente), considerando que un máximo de 20 alumnos se conecta por AP, se determina el uso de un total de 34 AP´s.

- Cafeterías

  Se cuenta con dos cafeterías, la cafetería 1 (1er piso) con una capacidad de 50 alumnos, considerando que un máximo de 25 alumnos se conecta por AP, se determina el uso de 2 AP´s. La cafetería 2 (2do piso) con una capacidad de 25 alumnos, considerando que un máximo de 25 alumnos se conecta por AP, se determina el uso de 1 AP.

- Auditorio

  El Auditorio cuenta con una capacidad de 561 usuarios, donde solo es necesario garantizar el 20% de la conectividad total (definido por CENTRUM); por lo tanto, se desea brindar el acceso a 113 alumnos, considerando que un máximo de 23 alumnos se conecta por AP, se determina el uso de 5 AP´s.

- Salas de estudio

  Se cuentan con 23 salas de estudio distribuidas entre el segundo y el tercer piso con una capacidad total de 115 alumnos, considerando que un máximo de 23 alumnos se conecta por AP, se determina el uso de 5 AP´s.

- Biblioteca

  Con una capacidad total de 45 alumnos, considerando que un máximo de 23 alumnos se conecta por AP, se determina el uso de 2 AP´s.

- Corredores

  Se cuenta con Áreas libres o corredores ubicados en el segundo y el tercer piso, desde donde los alumnos usan el servicio Inalámbrico, se identificó una necesidad de conexión de aproximada de 40 alumnos, considerando que un máximo de 20 alumnos se conecta a un AP, se determina el uso de 2 AP´s.

A continuación se muestra un ejemplo de la distribución de los AP´s en las aulas de CENTRUM.

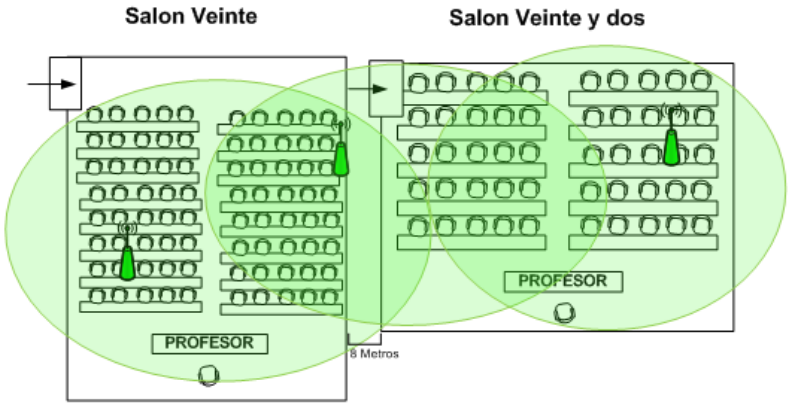
Esquema 15: Muestra de instalación de AP – Sede Lima

B. Arequipa

Actualmente cuenta con cuatro aulas destinadas al dictado de clases y 116 alumnos divididos en cuatro programas. Dos aulas se encuentran ubicadas en el primer piso separadas 20 metros una de otra y otras dos aulas en el segundo piso separadas 2 metros una de la otra.

Para el primer piso, debido a la distancia entre aulas y considerando que un máximo de 21 alumnos se conecta a cada AP, es necesario el uso de 2 AP´s por aulas. En el segundo piso, debido a la cercanía y considerando que un máximo de 22 alumnos se conecta a cada AP, es necesario el uso de 3 AP´s en total.

Resumiendo, para cubrir las necesidades de conexión y brindar una adecuada cobertura en todas las aulas de clase en la sede de Arequipa, se determina el uso de 7 AP´s. A continuación se muestra como ejemplo una de las aulas del segundo piso de Arequipa con la distribución de los AP´s.



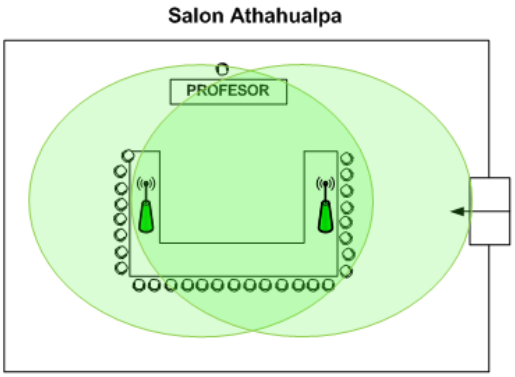
Esquema 16: Propuesta de red Inalámbrica – Sede Arequipa

En el Plano 5-A se muestra la ubicación y cobertura de todos los AP´s mencionados para la sede de Arequipa.

C. Cajamarca

Actualmente cuenta con tres aulas destinadas al dictado de clases y 72 alumnos divididos en tres programas. Un aula está ubicada en el primer piso y las otras dos en el quinto piso divididas por una distancia de 10 metros. Debido a la separación de las aulas y considerando que un máximo de 29 alumnos se conecte a cada AP en cualquiera de las aulas, se determina el uso de dos AP´s por aula.

Resumiendo, para cubrir las necesidades de conexión y brindar una adecuada cobertura en todas las aulas de clase en la sede de Cajamarca, se determina el uso de 6 AP´s. A continuación se muestra como ejemplo el aula del primer piso de Cajamarca con la distribución de los AP´s.



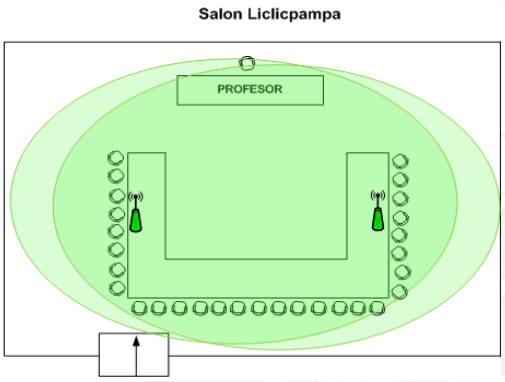
Esquema 17: Propuesta de red Inalámbrica – Sede Cajamarca

En el Plano 5-B se muestra la ubicación y cobertura de todos los AP´s mencionados para la sede de Cajamarca.

D. Cusco

Actualmente cuenta con dos aulas destinadas al dictado de clases y 97 alumnos divididos en tres programas. Las dos aulas se encuentran ubicadas en el primer piso y separadas por una pared gruesa de concreto que debilita las señales Inalámbricas; considerando que un máximo de 19 alumnos se conecta a cada AP en cualquiera de las aulas, se determina el uso de dos AP´s por aula.

Resumiendo, para cubrir las necesidades de conexión y brindar una adecuada cobertura en todas las aulas de clase en la sede de Cusco, se determina el uso de 4 AP´s. A continuación se muestra como ejemplo una de las aulas de Cusco con la distribución de los AP´s.



Esquema 18: Propuesta de red Inalámbrica – Sede Cusco

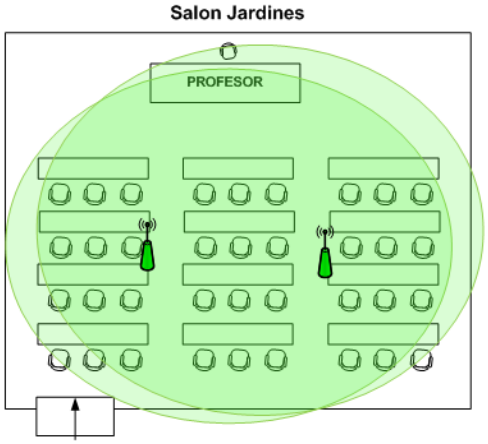
En el Plano 5-C se muestra la ubicación y cobertura de todos los AP´s mencionados para la sede de Cusco.

E. Piura

Actualmente cuenta con tres aulas destinadas al dictado de clases y 115 alumnos divididos en 5 programas. Las tres aulas se encuentran en el mismo piso, estando una de ellas separada de las otras dos por 20 metros. Para el caso del aula más alejada y considerando que un máximo de 18 alumnos se conecta a cada AP, se determina el uso de dos AP´s. En el caso de las otras dos aulas, debido a la

cercanía de las aulas y considerando que un máximo de 22 alumnos se conecta a cada AP, se determina el uso de 3 AP´s.

Resumiendo, para cubrir las necesidades de conexión y brindar una adecuada cobertura en todas las aulas de clase en la sede de Piura, se determina el uso de 5 AP. A continuación se muestra como ejemplo una de las aulas de Piura con la distribución de los AP´s.



Esquema 19: Propuesta de red Inalámbrica – Sede Piura

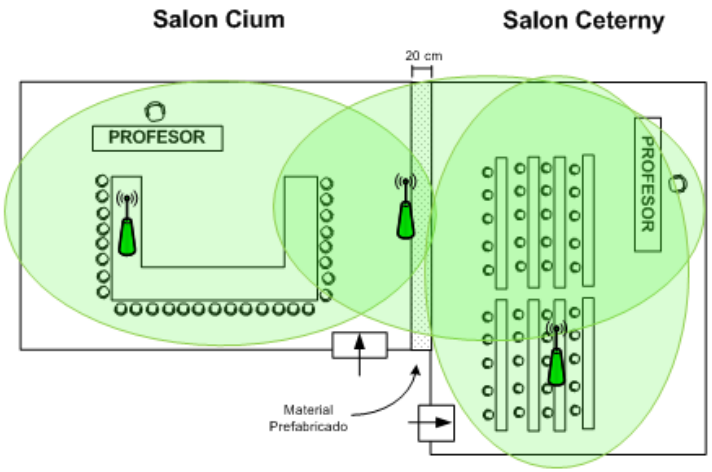
En el Plano 5-D se muestra la ubicación y cobertura de todos los AP´s mencionados para la sede de Piura.

F. Chiclayo

Actualmente cuenta con 4 aulas destinadas al dictado de clases y 126 alumnos divididos en 4 programas. Las aulas se encuentran en el segundo y en el séptimo piso. Las dos aulas del segundo piso se encuentran juntas y las dos aulas del séptimo piso alejadas 5 metros una de la otra. Para el caso del segundo piso, debido a la cercanía de las aulas y considerando que un máximo de 28 alumnos se conecta a cada AP, se determina el uso de 3 AP´s. Para el caso del séptimo piso, debido a que las aulas se encuentran lo suficientemente separadas y considerando que un máximo de 21 alumnos se conecta a cada AP, se determina el uso de 4 AP´s.

Resumiendo, para cubrir las necesidades de conexión y brindar una adecuada cobertura en todas las aulas de clase en la sede de Chiclayo, se determina el uso de

7 AP´s. A continuación se muestra como ejemplo una de las aulas de Chiclayo con la distribución de los AP´s.



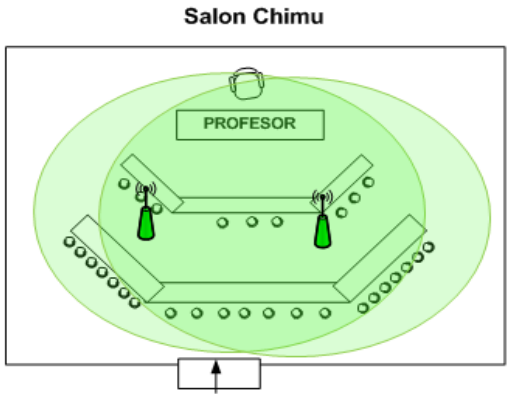
Esquema 20: Propuesta de red Inalámbrica – Sede Chiclayo

En el Plano 5-E se muestra la ubicación y cobertura de todos los AP´s mencionados para la sede de Chiclayo.

G. Trujillo

Actualmente cuenta con 3 aulas destinadas al dictado de clases y 113 alumnos divididos en 4 programas. Una de las aulas se encuentra ubicada en el primer piso y las otras dos en el segundo piso separadas por una distancia de 15 metros. Debido a la distancia de separación de las aulas del segundo piso y considerando que un máximo de 19 alumnos se conecta a cada AP, se determina el uso de dos AP´s por aula.

Resumiendo, para cubrir las necesidades de conexión y brindar una adecuada cobertura en todas las aulas de clase en la sede de Trujillo, se determina el uso de 6 AP´s. A continuación se muestra como ejemplo una de las aulas del segundo piso de Trujillo con la distribución de los AP´s.



Esquema 21: Propuesta de red Inalámbrica – Sede Trujillo

En el Plano 5-F se muestra la ubicación y cobertura de todos los AP´s mencionados para la sede de Trujillo.

A continuación, se presenta un cuadro resumen de la cantidad de AP´s necesarios para el re-diseño de las redes Inalámbricas a implementar en las sedes de CENTRUM a nivel nacional:

Tabla 22: Cantidad de AP´s requeridos a nivel nacional

CENTRUM CATÓLICA - CANTIDAD DE AP´S REQUERIDOS A NIVEL NACIONAL			
Ubicación - Sede	Detallado	Cantidad de AP	Máximo alumnado por AP
Lima	Aulas de Clase	34	20
	Cafeteria 1 (1er piso)	2	25
	Cafeteria 2 (2do piso)	1	25
	Auditorio	5	23
	Salas de estudio 2do piso	3	24
	Salas de estudio 3er piso	2	23
	Biblioteca	2	23
	Halls / Zonas libres	2	20
Provincias	Arequipa	7	22
	Cajamarca	6	29
	Cusco	4	19
	Piura	5	22
	Chiclayo	7	28
	Trujillo	6	19
TOTAL		86	

Elaboración: Propia

4.1.2 Equipos de Acceso

Los AP´s integran parte de la arquitectura que permite el ingreso de los clientes a la red. En el punto anterior se detalló la necesidad de contar con 86 AP´s para cubrir la necesidad de cobertura y disponibilidad del servicio para el alumnado a nivel nacional. En este apartado se definirán los modelos de los AP´s basándonos en el ambiente de trabajo y requerimientos de cada una de las sedes de CENTRUM.

A continuación se presentan los AP´s considerados para el diseño de las redes Inalámbricas en cada una de las sedes de CENTRUM Católica. Dado que los escenarios son similares, se presenta la Tabla 23 con el resumen de los equipos considerados.

Tabla 23: Modelos de AP´s a ser usados en el despliegue Inalámbrico

CENTRUM CATÓLICA - MODELOS DE AP´S A SER INSTALADOS				
Sede	**Cantidad de AP**	**Arquitectura de trabajo**	**Modelo**	**Accesorios**
Lima	5	Outdoor	Cisco AP1242AG	2 Antenas externas de 2.2 dBi
	46	Indoor	Cisco AP1130AG	Antenas incluidas internamente
Arequipa	7	Indoor	Cisco AP1130AG	Antenas incluidas internamente
Cajamarca	6	Indoor	Cisco AP1130AG	Antenas incluidas internamente
Cusco	4	Indoor	Cisco AP1130AG	Antenas incluidas internamente
Piura	5	Indoor	Cisco AP1130AG	Antenas incluidas internamente
Chiclayo	7	Indoor	Cisco AP1130AG	Antenas incluidas internamente
Trujillo	6	Indoor	Cisco AP1130AG	Antenas incluidas internamente

Elaboración: Propia

Resumiendo, es necesario contar con 5 AP´s Outdoor modelo Cisco AP 1242AG y 81 AP´s Indoor modelo Cisco AP 1130AG para brindar un adecuado acceso Inalámbrico en todas las sedes de CENTRUM Católica.

A continuación se muestra una imagen de los AP´s seleccionados (no se están incluyendo las antenas para el caso del AP1242AG).

CISCOAP1242AG

CISCOAP1130AG

Esquema 22: Modelos de AP's considerados en la propuesta de red Inalámbrica

Se adjunta como Anexo 1 el Datasheet del AP Cisco 1242AG.
Se adjunta como Anexo 2 el Datasheet del AP Cisco 1130AG.

4.1.3 Infraestructura de Acceso

Para el funcionamiento de los AP´s es necesario contar con un punto de red y una toma de energía. Las facilidades técnicas de infraestructura en Lima y provincia son distintas, por lo cual se revisará en detalle cada una de las sedes. Se recomienda estandarizar los puertos de los Switches en donde serán conectados los AP´s, esto simplificara la administración y gestión de los mismos.

A. Lima

Dado que la sede de Lima cuenta con toda una infraestructura de red ya establecida, se procede a detallar las conexiones necesarias.

- Para el caso de las aulas de clase, los AP´s serán conectados en puertos del Switch de la misma aula, por lo tanto se debe reservar dos puertos por aula; como se ha presentado en la Tabla 10 (Inventario de Switches Sede Lima), no todos los Switches de aula cuentan con el soporte para PoE, siendo necesario la renovación de 17 Switches (En cuatro aulas solo es necesario cambiar uno de los Switches) a un modelo que soporten PoE, se propone la estandarización con el modelo Cisco Catalyst 3560-48PS.

- Para la conexión de los AP´s a ser ubicados en la Biblioteca y en la cafetería del segundo piso se deben reservar cuatro puertos en los Switches del Centro de Cómputo.
- Para los AP´s a ser ubicados en la Cafetería del 1er. Piso se deben reservar dos puertos en los Switches del cuarto de tablero CT-1C.
- Para los AP´s a ser ubicados en el auditorio se deben reservar cinco puertos en el Switch del cuarto de tablero CT-1D.
- Para los AP´s ubicados en los Corredores (Pérgola y parte externa de la Biblioteca) se deberá reservar un puerto en el Switch del aula 206 y un puerto en el Switch del aula 309 respectivamente.

Se adjunta en los Planos 6-A y 6-B las conexiones de los AP´s a los respectivos Switches de borde en el campus de Lima. Así mismo, se adjuntan los Planos 7-A y 7-B con la cobertura mínima proyectada de Acceso Inalámbrico bajo el nuevo diseño propuesto en la presente tesis.

A continuación se presenta el Switch Cisco Catalyst 3560-48PS, modelo de Switch considerado estándar para la sede de Lima.

Esquema 23: Switch Cisco Catalyst 3560-48PS

Se adjunta como Anexo 3 el Datasheet del Switch Cisco Catalyst 3560-48PS.

Para el caso de provincias, debido a que no se cuenta con una infraestructura ya establecida y que las aulas de clase no son fijas ni propias de CENTRUM, la solución de Infraestructura debe ofrecer la mayor flexibilidad posible.

En base a las necesidades determinadas en la presente tesis, se considera el uso de Routers ISR (Integrated Services Routers), que además de permitir el enlace WAN

de cada una de las sedes de provincia con el campus principal en Lima, permite incorporar una serie de módulos adicionales con recursos propios, ofreciendo la ventaja de integrar nuevos servicios a medida de las necesidades del cliente, con por ejemplo, el modulo del Switch de puertos Ethernet, que soporta PoE eliminando la tarea de instalar puntos de energía para cada AP.

B. Provincias

Se presenta el análisis para el caso de Arequipa, el mismo trato se replica para las demás sedes.

- Arequipa

Se determinó el uso de 7 AP´s; para la conectividad a red de estos equipos es necesaria la habilitación de 7 puertos de red. Dado el escenario de contar con un Router, un Switch de acceso y debido a que no se cuenta con una infraestructura de red ya establecida en la sede de Arequipa, se determina el uso de los siguientes equipos.

Tabla 24: Equipos de Infraestructura de red – Arequipa

CENTRUM CATÓLICA - Equipos de Infraestructura de red - Arequipa		
Equipo	Modelo	Descripción
Router	Cisco 2811	Brinda enlace WAN con la sede de Lima
Modulo HWIC-D	Cisco Ethernet Switch 9 Puertos	Brinda puertos Ethernet de acceso LAN

Elaboración: Propia

La incorporación de estos equipos permitirá establecer el enlace dedicado con la sede de Lima, brindando 9 puertos para la conexión de los AP´s y 2 puertos Giga adicionales.

En base a lo revisado en las sedes de provincia, se determinó que la arquitectura es similar, por lo que se resume el requerimiento de equipos de comunicación en la Tabla 30.

Tabla 30: Resumen de equipos de infraestructura a nivel nacional

CENTRUM CATÓLICA - EQUIPOS DE INFRAESTRUCTURA A NIVEL NACIONAL			
Sede	**Equipo**	**Modelo**	**Cantidad**
Lima	Switch	Cisco 3560-48PS	17
Arequipa	Router	Cisco 2811 ISR	1
	Modulo HWIC-D	Cisco Ethernet Switch 9 puertos	1
Cajamarca	Router	Cisco 2811 ISR	1
	Modulo HWIC-D	Cisco Ethernet Switch 9 puertos	1
Cusco	Router	Cisco 2811 ISR	1
	Modulo HWIC-D	Cisco Ethernet Switch 9 puertos	1
Piura	Router	Cisco 2811 ISR	1
	Modulo HWIC-D	Cisco Ethernet Switch 9 puertos	1
Chiclayo	Router	Cisco 2811 ISR	1
	Modulo HWIC-D	Cisco Ethernet Switch 9 puertos	1
Trujillo	Router	Cisco 2811 ISR	1
	Modulo HWIC-D	Cisco Ethernet Switch 9 puertos	1
TOTAL			29

Elaboración: Propia

A continuación se presenta el Router modelo Cisco 2811 ISR considerado para la integración de red de las sedes de provincia.

Esquema 24: Router Cisco 2811 ISR

Se adjunta como Anexo 4 el Datasheet del Router Cisco 2811 ISR.
Se adjunta como Anexo 5 el Datasheet del modulo de 9 puertos HWIC-D.

4.2 Diseño del Sistema de Administración

En los puntos anteriores se ha presentado el diseño de la solución Inalámbrica local en cada una de las sedes de CENTRUM Católica a nivel nacional, así como la necesidad de los equipos involucrados en la solución de acceso para la red local y para la conexión WAN.

Debido a que se cuenta con una cantidad alta de AP´s (86 a nivel nacional); se incorpora al diseño planteado un sistema de Administración para la red Inalámbrica, el mismo que permitirá la centralización de la gestión y la integración del control en toda la red.

El sistema propuesto además de permitir la administración de la red Inalámbrica, incorpora herramientas que permiten el establecimiento de políticas de seguridad y configuración de alertas, así como el despliegue de infraestructura adicional y la administración de perfiles. A continuación se detallarán los equipos en Software y Hardware que soportarán la base de la administración del sistema. Se presentan los equipos involucrados en la solución del Sistema de Administración y centralización de las redes Inalámbricas de CENTRUM a nivel nacional.

4.2.1 Wireless LAN Controller (WLC)

El Wireless LAN Controller es el principal elemento a considerar en el despliegue de un Sistema de Administración de redes Inalámbricas debido a que permite integrar y administrar los AP´s en una sola plataforma.

Se desplegarán WLC´s en cada una de las sedes de CENTRUM a fin de administrar los AP´s instalados localmente en cada sede, este diseño permitirá utilizar prácticamente todo el Ancho de banda de los enlaces WAN para la transmisión de la data. La cantidad de WLC y licencias a considerar para cada sede dependerán de la cantidad de AP´s que se deban administrar. A continuación se revisa en detalle cada una de las sedes de CENTRUM y se presentan los controladores necesarios para cada caso.

A. Lima

   Se determinó el uso de 51 AP´s en el campus de Lima, considerando un crecimiento del 25% es necesario el uso de un controlador que permita la administración de hasta 75AP´s, se determina el uso de dos Cisco 4404 Series WLAN Controller con licencias de administración para 100 AP's.

B. Provincias

La cantidad de AP´s a instalar, determinan el uso del Cisco Wireless LAN Controller Module Network con licencia de administración para 12 AP´s el cual se integrará al Router Cisco 2811 ISR.

A continuación se muestra la Tabla 31 con el cuadro resumen por la cantidad de controladores a considerar en el despliegue de la administración de la red Inalámbrica a nivel nacional.

Tabla 31: Resumen de controladores Wireless a nivel nacional

CENTRUM CATÓLICA - RESUMEN DE CONTROLADORES WIRELESS (WLC)			
SEDE	**CANTIDAD DE AP´s**	**MARGEN DE 25% - AP´s**	**MODELO**
Lima	51	75	4404 Series WLAN Controller for up 100 AP (2)
Arequipa	7	9	Cisco Wireless LAN Controller Module for up 12 AP
Cajamarca	6	8	Cisco Wireless LAN Controller Module for up 12 AP
Cusco	4	5	Cisco Wireless LAN Controller Module for up 12 AP
Piura	5	6	Cisco Wireless LAN Controller Module for up 12 AP
Chiclayo	7	9	Cisco Wireless LAN Controller Module for up 12 AP
Trujillo	6	8	Cisco Wireless LAN Controller Module for up 12 AP
TOTAL	86	120	

Elaboración: Propia

Así mismo se presenta una imagen del controlador Cisco 4404 que se incluye para la sede principal de Lima y del controlador en modulo para las sedes de provincia.

Esquema 25: Controlador Wireless Cisco 4404

Esquema 26: Módulo de controlador Wireless 12 AP's

Se adjunta como Anexo 6 magnética el Datasheet del WLC 4404.
Se adjunta como Anexo 7 el Datasheet del modulo de controlador para 12 AP´s.

4.2.2 Cisco Secure Access (ACS)

Como parte del diseño planteado se incorpora un Cisco Secure Access (ACS) para la autenticación y control de acceso de usuarios a la red Inalámbrica, así como para la administración de políticas de control y seguridad.

El Cisco Secure ACS 4.2 for Windows será instalado en un servidor dedicado que deberá ser ubicado en el Datacenter de la sede principal de Lima. La red en la cual será instalado el Servidor será la de los servidores sin presentar esto último algún inconveniente con las sub redes a administrar en Lima o provincias.

La cantidad de usuarios que puede administrar el ACS no será un problema con la expansión o incremento de usuarios, pues el ACS hará las consultas a una base de datos, la cual almacena los usuarios, contraseñas y detalles necesarios para la identificación. Debido a que la cantidad de usuarios no será un limitante, se considera un solo ACS para la administración de todos los usuarios a nivel nacional de CENTRUM Católica. A continuación se presentan los requerimientos mínimos necesarios en Hardware y Software para el servidor que hospede al ACS. Se adjunta como Anexo 8 el Datasheet del ACS Versión 4.2

Tabla 32: Requerimientos de servidor para instalación del ACS

CENTRUM CATÓLICA - REQUERIMIENTOS DE SERVIDOR PARA HOSPEDAR AL ACS	
Componente	**Especificaciones**
CPU	Procesador Pentium IV de 1.8 GHz o superior
Memoria del Sistema	2 GB
Memoria Virtual	1 GB
Disco Duro	20 GB
Sistema Operativo	Windows Server 2003 Edición Estándar o superior

Elaboración: Cisco System

4.2.3 Cisco Wireless Control System (WCS)

Como parte diseño planteado se considera el uso de un Wireless Control System (WCS) para el monitoreo y mejora de rendimiento en la red Inalámbrica de CENTRUM a nivel

nacional, adicionalmente el WCS permitirá la generación de reportes personalizados necesarios.

La función principal que desempeñara el WCS en el presente diseño es la de garantizar el buen estado de la red Inalámbrica, esto a través del monitoreo constante del mapa de la distribución de los AP´s así como de los mensajes de alerta de los equipos instalados.

El WCS es un aplicativo que será instalado en el mismo servidor en el que se instalará el ACS, la red a la cual pertenecerá será la misma de los servidores, sin presentar esto último algún inconveniente con las sub redes a monitorear en Lima y provincias. A continuación se presenta los requisitos mínimos de Hardware y Software necesarios para la instalación y uso del WCS. Así mismo, se adjunta como Anexo 9 el Datasheet del WCS.

Tabla 33: Requerimientos de servidor para instalación del WCS

CENTRUM CATÓLICA - REQUERIMIENTOS DE SERVIDOR PARA HOSPEDAR AL WCS	
Componente	**Especificaciones**
CPU	Intel CPU 2 GHz o superior
Memoria del Sistema	2 GB
Memoria Virtual	1 GB
Disco Duro	80 GB
Sistema Operativo	Windows Server 2003 Edición Estándar o superior

Elaboración: Cisco System

La licencia de compra por la administración del WCS permite la administración inicial de 50 AP´s. En el diseño de acceso a la red Inalámbrica de CENTRUM se ha considerado el despliegue de 86 AP´s, por lo que se considera la compra de una licencia adicional para la administración de 50 AP´s más; teniendo una capacidad total de administración de 100 AP´s, ofreciendo la posibilidad de crecimiento en infraestructura Inalámbrica de hasta en 14 nuevos AP´s. Sin embargo, de ser necesaria la administración de un número mayor de equipos, se adjunta como Anexo 10 la Guía de Licenciamiento y órdenes de compra del WCS.

4.2.4 Integración de Servicios de Administración

Debido a que tanto el ACS 4.2 for Windows como el WCS for Windows se alojarán en el mismo servidor, es importante definir los requerimientos mínimos de Hardware y software que debe tener el equipo para poder administrar y trabajar con ambos aplicativos.

Basándonos en los requerimientos mínimos de cada aplicativo, se presentan los requerimientos finales del equipo que alojará ambas aplicaciones.

Tabla 34: Requerimientos de servidor para instalación del WCS y ACS

CENTRUM CATÓLICA - REQUERIMIENTOS DE SERVIDOR PARA HOSPEDAR EL SISTEMA DE ADMINISTRACIÓN WIRELESS (WCS Y ACS)	
Componente	Especificaciones
CPU	Procesador Core dos Duo de 2.8 GHz o superior
Memoria del Sistema	4 GB
Memoria Virtual	2 GB
Disco Duro	200 GB
Sistema Operativo	Windows Server 2003 Edición Estándar o superior

Elaboración: Cisco System

4.3 Seguridad y Acceso de Usuarios

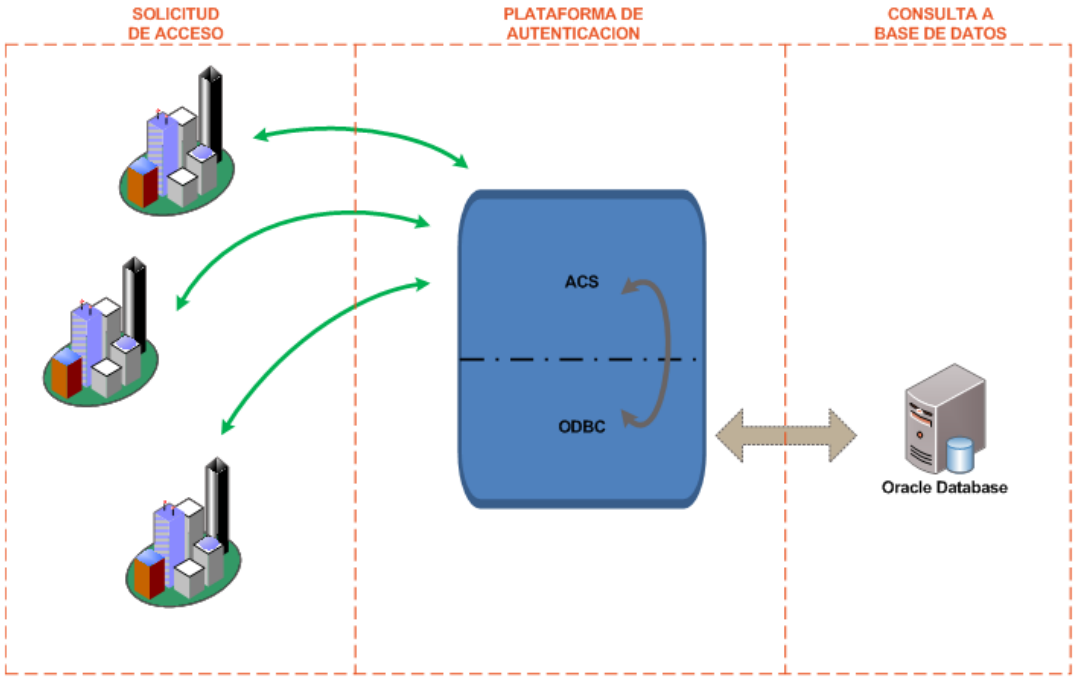
Los usuarios del servicio de acceso a Internet Inalámbrico motivo de la presente tesis son los alumnos de los programas de CENTRUM a nivel nacional, sin embargo, es importante recordar que CENTRUM es parte de la PUCP, por lo tanto, se ha visto conveniente extender el acceso de la red Inalámbrica de CENTRUM a nivel nacional para todos los alumnos de la PUCP. En este apartado revisaremos las consideraciones técnicas a considerar a fin de lograr los objetivos establecidos.

4.3.1 Autenticación de Usuarios

Para conseguir el acceso de todos los alumnos de la PUCP a la red Inalámbrica desplegada por CENTRUM, se considera el uso de las credenciales de autenticación que son distribuidas a cada alumno por parte de la universidad. Estos certificados son para el acceso al correo electrónico y a la intranet de cada alumno. Los certificados entregados constan de un usuario y un Password y son almacenados en una base de datos Oracle que reside en la sede Pando de PUCP.

El ACS que es el encargado de autenticar los usuarios para el acceso a la red Inalámbrica hará las consultas a esta base de datos para determinar la autenticidad del alumno. El ACS no permite realizar consultas directas a bases de datos externas como Oracle, sin embargo, permite usar el estándar ODBC (Open Database Connectivity) el cual traducirá las consultas del ACS hacia la base de datos. El ODBC se ejecutará en el mismo servidor que hospeda el

ACS y el WCS y creara la interfaz entre el ACS y la base de datos; a continuación se presenta el esquema de autenticación de usuarios que plantea la presente tesis:



Esquema 27: Arquitectura de Autenticación de Usuarios PUCP (ACS y ODBC)

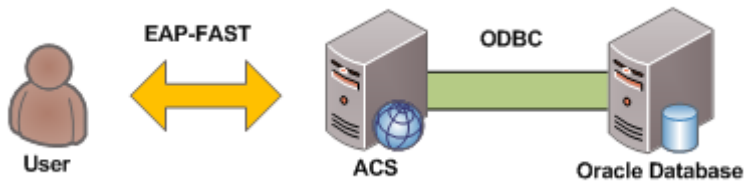
El esquema mostrado permite no solo la seguridad de acceso por parte de los usuarios autorizados, sino que además extiende el uso del servicio Inalámbrico a todos los alumnos de pregrado y postgrado de la PUCP a nivel nacional; las credenciales de seguridad garantizan la autenticación por usuario, superando inconvenientes como el uso de credenciales de otro usuario y la de no depender de claves que pueden cambiar o que simplemente se pueden olvidar, esto debido a que los datos de acceso a la red Inalámbrica son datos que el alumno usa para el acceso a su información personal almacenada por la universidad; si el alumno cambia la clave en el sistema, también cambia la clave de acceso a la red Inalámbrica pues la base de datos es la misma, permitiendo esto unificar el sistema Inalámbrico a los sistemas ya administrados por la PUCP bajo los mismos estándares de acceso.

Con respecto al Servidor en donde se alojará el ODBC y a la necesidad de recursos adicionales de Hardware para el correcto funcionamiento del mismo, se consideró en los requerimientos de Administración unas características superiores con el fin de soportar aplicaciones básicas como esta.

4.3.2 Seguridad de Acceso de usuarios

Debido a que las credenciales de acceso a la red Inalámbrica que posee cada alumno son las mismas usadas para el acceso a su información académica y personal, la seguridad involucrada en el envío de estas credenciales para la autenticación debe ser la mejor posible. Se debe tener en cuenta que cada alumno posee su propio equipo personal para conectarse a la red Inalámbrica y la cantidad de alumnos en toda la comunidad PUCP supera los 10,000 alumnos. En tal sentido es necesario utilizar un mecanismo de autenticación que ofrezca un nivel alto de seguridad y confidencialidad, así como de fácil uso y brindar una gran flexibilidad en el despliegue a los usuarios finales.

En base a lo mostrado y a los protocolos de seguridad revisados, se determina el uso del protocolo de encriptación EAP-FAST por ofrecer la seguridad necesaria en la transmisión de las credenciales de autenticación, sin la necesidad de contar con certificados digitales en el servidor o en cliente obligatoriamente. EAP-FAST permite brindar una alta seguridad en el envío de las credenciales de acceso usando un canal encriptado para el envío y recepción de las credenciales del usuario; así como la transmisión de comunicación encriptado entre los usuarios y el ACS (entre los usuarios y el AP la comunicación es inalámbrica). Posteriormente el ACS a través del ODBC hará la consulta a la BD Oracle para confirmar el acceso o el rechazo de la solicitud (esta segunda parte es llevada netamente en la parte cableada de la red). A continuación se muestra el esquema de trabajo para la transmisión y recepción de los paquetes de autenticación del usuario:



Esquema 28: Transmisión y Recepción de Paquetes para la Autenticación de Usuarios

4.3.3 Asignación de Perfiles

Debido a que el estado que adopta cada alumno en el día es muy dinámico y que el despliegue de la red Inalámbrica es uno solo, asignar el perfil deseado a cada alumno está condicionado a que el alumno este o no en clase. En tal medida, se determino que si el alumno se encuentra en clase, el alumno debe conectarse a la Vlan de “alumno en clase” sin importar donde se encuentre físicamente; por otro lado si el alumno no se encuentra en clase, el alumno debe conectarse a la Vlan de “Acceso libre”. En el punto anterior se detallo la seguridad para el envío de las credenciales de acceso del alumno a la red, estas credenciales confirman la autenticidad de que el alumno sea quien dice ser. Ahora explicaremos como identificar al alumno en la red y a través del uso de atributos asignar el perfil deseado.

En la Base de Datos que aloja las credenciales de los usuarios, se debe identificar a los alumnos de CENTRUM y de acuerdo al programa en el que estos se encuentran inscritos (Por ejemplo: MBAG25) se les asignará este detalle a fin de poder identificarlos al momento de intentar acceder a la red y asignarles las configuraciones respectivas.

Cuando el ACS confirma la identidad del usuario, solicita los atributos necesarios relacionados con el alumno a la BD y asigna el atributo de grupo al usuario. Por otro lado, el ACS posee un mapeo interno que permite relacionar usuarios de Bases de Datos externas con un mapeo de grupos internos basándose en los atributos recibidos, este mapeo permitirá la asignación de perfiles dinámicos y por consecuencia de asignación de Vlan´s. Cuando el ACS en base al atributo de grupo sepa que el alumno pertenece a un grupo específico, hará una búsqueda para determinar el mapeo de este grupo con el de su base interna, el perfil asignado y configurado en el grupo de la base interna del ACS será aplicado a todos los usuarios con el atributo del grupo determinado. De esta manera todos los alumnos de CENTRUM tendrán como atributo su programa de postgrado como parte del usuario en la Base de Datos. Al acceder un alumno de CENTRUM a la red Inalámbrica, el ACS revisara el atributo y asignara la Vlan correspondiente. Un punto necesario dentro de la administración en la asignación de Vlan´s es asegurar que los alumnos en clases tengan configurado la Vlan adecuada, esta tarea involucra configurar diariamente y cada hora en el ACS los programas que tengan programada una clase.

Los cambios de Vlan para alumnos en clase y solicitados excepcionalmente por los profesores serán realizados de manera manual tal como se hizo para aplicar la Vlan de Alumno en clase y se aplicarán directamente en la configuración de grupos del ACS. Ante un cambio de Vlan, se debe forzar al ACS a aplicar las políticas a los usuarios de dicho grupo, permitiendo esto el cambio de Vlan en el mismo instante. Para los alumnos que no pertenezcan a CENTRUM pero si a PUCP se les mapeará a un grupo por defecto con su atributo respectivo que estará asociado a una "VLAN de usuarios PUCP", la cual brindará un acceso adecuado a internet con las precauciones de seguridad convenientes.

4.3.4 Usuarios Invitados

Para todos los usuarios que no pertenezcan a la comunidad PUCP como proveedores, alumnos externos, profesores, etc. se desplegará un SSID adicional denominado "WiFi Invitados", el cual brindará un acceso limitado a personal externo sin poner en riesgo la seguridad de la red interna. La red de Invitados estará desplegada a nivel nacional en todos los puntos en donde se encuentre la red del alumnado.

A continuación se adjunta en el Anexo 11 el Diagrama de flujo para la asignación de VLAN en los casos de solicitudes de acceso a la red Inalámbrica por parte de los alumnos de CENTRUM, alumnos de PUCP y externos. Así mismo, se adjunta en el Anexo 12 el Diagrama de flujo para el caso de un cambio manual de Vlan a un grupo determinado de alumnos.

4.4 Enlaces WAN

La red Inalámbrica de CENTRUM Católica será desplegada a nivel nacional y el Sistema de Administración planteado basa su funcionamiento en la implementación de los enlaces dedicados entre la sede principal de PUCP en Lima y las sedes de provincia. A continuación se brindará las consideraciones de Ancho de Banda necesarias para la administración de la red Inalámbrica a nivel nacional, así como el Ancho de Banda estimado para la transmisión de data requerida por cada una de las sedes de provincia. Finalmente se considera un enlace adicional de acceso a Internet externo por cada sede.

4.4.1 Enlaces dedicados

Actualmente CENTRUM cuenta con seis sedes en provincia, en cada sede se implementará una red Inalámbrica local, la cuales formaran parte de una sola red Inalámbrica unificada y administrada desde Lima.

La administración y comunicación de red Inalámbrica se da gracias al uso de enlaces dedicados que permitirán interconectar las sedes de provincias con la sede de Lima y así formar una única red. La administración del sistema podrá realizarse desde cualquier punto de la red contando con los permisos de seguridad necesarios.

Debido a que toda la infraestructura de Administración de la red Inalámbrica se encuentra en la sede de Lima, todo el monitoreo, transmisión y recepción de información así como la autenticación de los usuarios deberá ser enviada a Lima a través de los enlaces dedicados. Sin embargo, se ha considerado en el diseño el uso de un WLC por cada una de las sedes de provincia, permitiendo esto que los WLC locales monitoreen las redes Inalámbricas locales, para el caso de la autenticación de los usuarios si bien la solicitud será enviada a la BD, esto será necesario solo la primera vez pues los WLC almacenan en cache las solicitudes anteriores sin necesidad de volver a enviar una nueva solicitud ante cada pedido del usuario, a menos que este cambie la contraseña de acceso. La comunicación entre los WLC locales de las sedes de provincia y el WLC de la sede de Lima se dará con una periodicidad de cinco minutos y será netamente entre ellos para actualizar el estado de la red Inalámbrica.

Todo lo expuesto nos permite asegurar que casi la totalidad del ancho de Banda disponible con las sedes de provincias será netamente usado para el envío y recepción de información concerniente a consultas de los alumnos de CENTRUM.

4.4.1.1 Ancho de Banda para Usuarios

La necesidad del acceso a internet por parte del alumnado de CENTRUM es aproximadamente un 90% a los sistemas de la Universidad y un 10% para el acceso a consultas externas. Los sistemas y el correo electrónico de la universidad están alojados en la sede de Lima y son accedidos a través de una plataforma Web.

Como se mostró en la tabla 15, el gran problema en el esquema de red actual en las sedes de provincia es el poco Ancho de Banda disponible para la subida de archivos a los Sistemas de la Institución. Este valor de "Upload" nos definirá el Ancho de banda necesario para los enlaces dedicados a instalar en cada sede. Para poder determinar un Ancho de Banda adecuado para los enlaces dedicados a instalar en las sedes de provincia, se presenta el siguiente cálculo para enlaces de 1Mb y 2 Mb con "Upload" de archivos de 1MB y 2MB.

Tabla 35: Upload de Archivos de 1Mb y 2 Mb con enlace dedicado de 1 Mb

UPLOAD DE ARCHIVOS CON ENLACE DEDICADO A 1 Mb				
Ciudad	Alumnos	Ancho de Banda por alumno	Upload de Archivo de 1 Mb	Upload de Archivo de 2 Mb
Trujillo	94	10.63 Kb	1.5 min	3 min
Chiclayo	126	7.9 Kb	2 min	4 min
Piura	84	11.9 Kb	1.5 min	3 min
Arequipa	116	8.62 Kb	2 min	4 min
Cajamarca	72	13.8 Kb	1.5 min	3 min
Cusco	67	15 Kb	1 min	2 min

Elaboración: Propia

Tabla 36: Upload de Archivos de 1 Mb y 2 Mb con enlace dedicado de 2 Mb

UPLOAD DE ARCHIVOS CON ENLACE DEDICADO A 2 Mb				
Ciudad	Alumnos	Ancho de Banda por alumno	Upload de Archivo de 1 Mb	Upload de Archivo de 2 Mb
Trujillo	94	21.26 Kb	0.75 min	1.5 min
Chiclayo	126	15.8 Kb	1 min	2 min
Piura	84	23.8 Kb	0.5 min	1.5 min
Arequipa	116	17.24 Kb	1 min	2 min
Cajamarca	72	27.6 Kb	0.75 min	1.5 min
Cusco	67	30 Kb	0.5 min	1 min

Elaboración: Propia

En base a los cálculos mostrados, se determina el Ancho de Banda mínimo de los enlaces dedicados a considerar en las sedes de provincia.

Tabla 37: Ancho de banda y Upload de Archivos para las sedes de provincia

ANCHO DE BANDA Y UPLOAD DE ARCHIVOS PARA LAS SEDES DE PROVINCIA				
Ciudad	Ancho de Banda	Alumnos	Upload de Archivo de 1 Mb	Upload de Archivo de 2 Mb
Trujillo	1 Mb	94	0.75 min	1.5 min
Chiclayo	2 Mb	126	1 min	2 min
Piura	1 Mb	84	0.5 min	1.5 min
Arequipa	2 Mb	116	1 min	2 min
Cajamarca	1 Mb	72	0.75 min	1.5 min
Cusco	1 Mb	67	0.5 min	1 min

Elaboración: Propia

Si bien los tiempos para la subida de archivos de 2 Mb son considerables, se debe tener en cuenta que estamos en el supuesto extremo de que todos los alumnos suben un archivo de ese tamaño al mismo tiempo lo cual es bastante difícil de encontrar, puesto que es el profesor el que generalmente sube los archivos pesados.

Finalmente, el sistema propuesto asigna todo el Ancho de Banda del enlace dedicado para las necesidades educativas de CENTRUM; en el punto 4.4.2 se mostrará el re-direccionamiento de las solicitudes externas a PUCP, como por ejemplo acceso a páginas externas.

4.4.1.2 Ancho de Banda para Administración

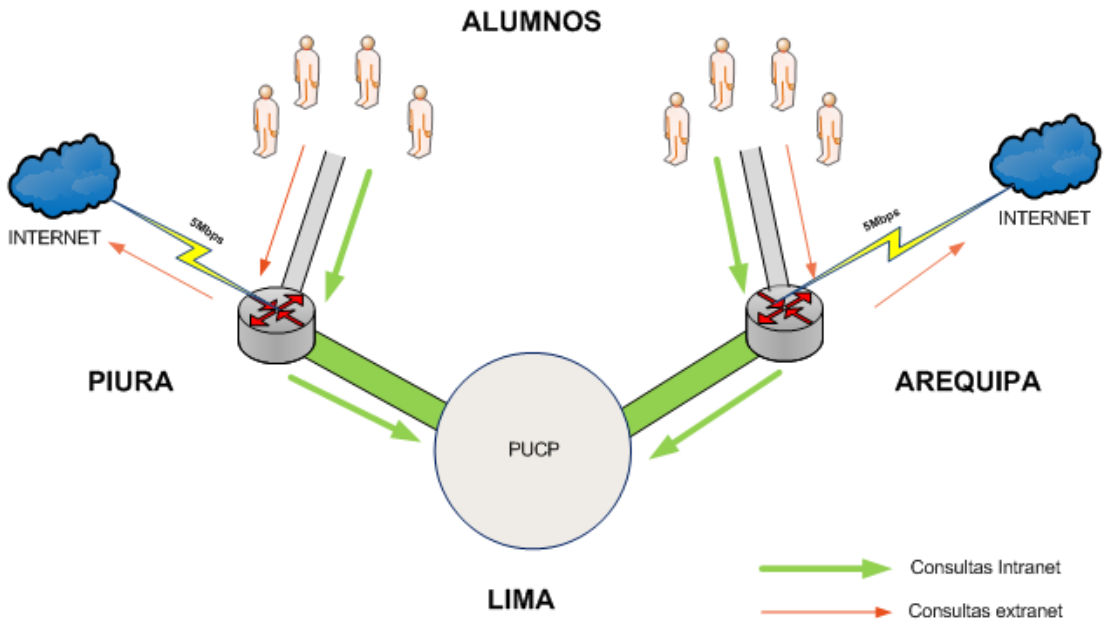
La administración de la red Inalámbrica centraliza su funcionamiento en la sede de Lima. Todos los controladores dispuestos en Lima y provincia se comunicaran con el ACS cada cierto tiempo para informar sobre el estado de las redes Inalámbricas de cada sede.

La transmisión de paquetes de información sobre el estado de cada red local en las sedes de provincia es mínima gracias a la consideración de un controlador por cada sede, este diseño eliminará la necesidad del envío de mensajes entre los AP´s de las sedes de provincia y el controlador de Lima que se daría en promedio cada 5 minutos en el supuesto de no contar con el despliegue a nivel nacional; instalando un controlador por cada sede se reduce la transmisión a solo paquetes de actualización entre los controladores.

Por lo tanto, se determina que el Ancho de banda adicional a considerar para la administración de la red es mínimo y con los requerimientos de Ancho de banda definidos en el punto anterior estaría totalmente cubierto.

4.4.2 Enlaces para el Acceso Externo – Línea ADSL

Uno de los principales inconvenientes al momento de ofrecer un modelo de servicio de Internet a usuarios, como es el caso de de la presente tesis, es que muchas veces los usuarios usan el servicio para un fin distinto al establecido. Por ejemplo, CENTRUM ha comprobado que los alumnos de Lima y provincia muchas veces usan el servicio de Internet para el acceso a otro tipo de páginas o simplemente para la comunicación en línea (chat). Este tipo consultas por parte de los alumnos consumen el reducido Ancho de banda sobretodo en las sedes de provincia, afectando el servicio para otros usuarios que si usan el servicio adecuadamente, transformándose esto en una mala percepción del servicio. Para solucionar este inconveniente se ha determinado el uso de una línea ADSL Speedy (Proveedor Telefónica) de 5MB al 25% por cada sede, esta línea será instalada en el Router de cada sede de provincia y configurada para atender las solicitudes de acceso a páginas o servicios distintos a los determinados por CENTRUM. Si bien este enlace Speedy puede congestionarse no afectará de ninguna manera el Ancho de banda destinado para consultas a los servicios de PUCP. De ser necesario asegurar el buen uso de la línea de acceso externo se podría incorporar un proxy o servidor de filtros. Se presenta el esquema de balanceo de carga en las sedes de provincia considerando el enlace ADSL para el caso de consultas externas.



Esquema 29: Balanceo de carga de red para las consultas en las sedes de provincia

4.5 Sistemas de Contingencia

El principal objetivo de un sistema de contingencia es mantener activo el servicio brindado. En tal medida, se presentan los puntos clave a asegurar en el diseño planteado para el buen funcionamiento de la red Inalámbrica.

- AP´s: Mantener un Stock mínimo de AP´s para reemplazar en cualquiera de las sedes de CENTRM. El sistema permite almacenar imágenes de S.O para los AP´s, permitiendo tener configurado y listo un equipo en menos de 2 horas.
- WLC: Configurar controladores de contingencia. En el caso de falla de un controlador en una sede de provincia, la autenticación de los usuarios locales se harán contra el controlador en Lima, hasta que el controlador fallido sea repuesto. En el caso de que el controlador de Lima falle, entrara en operación el controlador de Backup, el cual también responderá a las consultas de los usuarios y controladores de provincias.
- WCS y ACS: Para el caso del WCS y el ACS se deben respaldar con frecuencia los sistemas de archivos y bases de datos para restaurarlos en otro servidor con características similares. En caso de falla del WCS no habrá un impacto directo en el performance del servicio más si en los reportes. En el caso de falla del ACS se

perderá el sistema de seguridad de autenticación de la red y todos los usuarios accederán a la Vlan de acceso libre.

4.6 Costos de Implementación

El diseño planteado involucra el uso de equipos con los que actualmente CENTRUM no cuenta. Se adjunta en el Anexo 13 el detalle completo de los equipos involucrados en la solución con sus respectivos precios de lista actualmente en el mercado.

En la tabla 38 se muestra un cuadro resumen de los costos estimados para la implementación del diseño propuesto por la presente tesis.

Tabla 38: Resumen de Costos estimados para la Implementación

CENTRUM CATÓLICA: RESUMEN DE COSTOS ESTIMADOS PARA LA IMPLEMENTACIÓN				
Descripción	**Detalle**	**Costo Unitario**	**Cantidad**	**Costo Total**
Equipos	Puntos de Acceso 1242AG	$899	5	$4,495
Equipos	Puntos de Acceso 1131AG	$699	81	$56,619
Equipos	Switches Cisco PoE	$9,495	17	$161,415
Equipos	WLC4404	$34,995	2	$69,990
Equipos	Router ISR 2811	$2,825	6	$16,950
Equipos	Módulos HWIC 9 Puertos	$1,080	6	$6,480
Equipos	ACS 4.2	$8,995	1	$8,995
Equipos	WCS 3.0	$3,995	1	$3,995
Equipos	WCS licencias adicionales	$5,995	1	$5,995
Materiales de Instalación	Cables	$1,500	1	$1,500
Personal Técnico	Instalación de Equipos	$5,500	1	$5,500
Ingeniero responsable	Supervisión del proyecto	$5,000	1	$5,000
Total Estimado				$346,934

Elaboración: Propia

CONCLUSIONES

- En base a la revisión y análisis en cada una de las sedes, se rediseño y estandarizo la red Inalámbrica actual de CENTRUM Católica a nivel nacional.

- Debido al incremento de la necesidad de acceso Inalámbrico, se vio la necesidad de implementar un sistema integral de gestión centralizado.

- De los diversos proveedores de soluciones de gestión, los productos de la empresa Cisco son los que mejor se adaptan a la necesidad del proyecto.

- Para brindar diferentes niveles de acceso y poder garantizar la seguridad del sistema, se determinó la creación de perfiles de usuarios.

- Para el funcionamiento del sistema a nivel nacional, se determinó la necesidad de líneas dedicadas, así como el cálculo de sus respectivos Anchos de Banda.

- Finalmente, un adecuado diseño en redes Inalámbricas y la centralización de la administración de toda la red a través de una única plataforma, ofrecen una solución adecuada para una red de gran tamaño como la planteada por CENTRUM, cumpliendo así el objetivo principal de esta tesis.

RECOMENDACIONES

Para asegurar una adecuada administración de toda la red Inalámbrica de CENTRUM se requiere estandarizar ciertas tareas:

- Monitorear de manera continua el estado de toda la red Inalámbrica.
- Mantener actualizado el mapeo interno de configuración del sistema de autenticación ACS.
- Revisar constantemente los avisos y alertas de la plataforma.

El sistema ofrece la ventaja de incorporar servicios adicionales en la red, como la implementación de VoIP, con un tiempo mucho menor al de un despliegue en redes convencionales y un mejor performance debido al manejo de paquetes del aplicativo.

También se recomienda como una segunda etapa de la tesis, el diseño de una interfaz entre la Base de datos que maneja el horario de clases en CENTRUM y el mapeo interno del ACS, permitiendo esto el mapeo automático de las Vlan´s a los grupos.

BIBLIOGRAFIA

MATTHEW S. GAST
2005 Redes Wireless 802.11 Configuración y Administración de redes Inalámbricas Madrid O´Reilly

EARLE E. AARON
2006 Wireless Security Handbook NorthWest (U.S.A.) Auerbach Publications

GEIER, JIM
2008 Implementing 802.1x Security Solutions for Wired and Wireless Networks Indianápolis (U.S.A.) Wiley Publishing

STALLINGS, WILLIAM
2005 Wireless Communications & Networks Segunda Edición Upper Soddle River, New Jersey (U.S.A.) Pearson Prentice Hall

VERGARA, KERVIN
2007 Topología de red: Malla, Estrella, Árbol, bus y Anillo [en línea] <http://www.bloginformatico.com/topologia-de-red.php>

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
2010 Official IEEE 802.11 Working Group Project Timelines Published – Standards, Amendments, and Recommended Practices [en línea] Junio [Consultado 2010/05/14] <http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm>

SELTZE, LARRY
2008 WPA Cracked – What It Means *Security Watch* [en línea] Noviembre [13/11/2008] <http://blogs.pcmag.com/securitywatch/2008/11/wpa_cracked_what_it_means.php>

BRADLEY, MITCHELL
2007 Wireless Standards – 802.11b 802.11a 802.11g and 802.11n The 802.11 Family Explained [en línea] <http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm>

DUFFY MARSAN, CAROLYN
2009 New DOS Attacks threaten Wireless Data Networks [en línea]
Junio [05/06/2009]
<http://www.networkworld.com/news/2009/060509-wireless-dos-threats.html>

HERNANDO, MANUEL
2009 Sistema de gestión D-Link AP Array Technology Channel News [en línea]
Junio [01/06/2009]
<http://www.revistatcn.com/id4277/sistema-de-gestion-d-link-ap-array>

PISANO, E. DANIEL
2007 El Sistema Cifrado WEP (*Blog de Formato Web*) [Blog]
<http://www.formatoweb.com.ar/blog/2007/11/24/el-sistema-de-cifrado-wep/>

WV
2007 Diferencia entre WEP y WPA [en línea]
<http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa/>

TELEFÓNICA DEL PERÚ
2010 Tarifas de Speedy Telefónica [en línea] Lima [Consultado 2009/11/14]
<http://www.telefonica.com.pe/speedy/>

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN
2008 Conexión no Autorizada de terceros a la red Wi-Fi del hogar [en línea] Madrid Abril Junio [Consultado 2009/11/12]
<http://www.inteco.es/indicators/Seguridad/Observatorio/Indicadores/Indicador_INT60>

AMÉRICA ECONOMÍA
2007 Ranking de las Mejores escuelas de Negocios en Latinoamérica [en línea] Abril
<http://rankings.americaeconomia.com/2010/mba/ranking-america-latina.php>