DESARROLLO DE INGENIERÍA BÁSICA PARA INTERCONECTAR UN SISTEMA DE CONTROL CON LA RED CORPORATIVA DE UNA INDUSTRIA

JOSÉ GIRADO CARRILLO
ADALBERTO ARROYO PÉREZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS Y ELECTRÓNICA
CARTAGENA DE INDIAS D. T. y C.
2004

DESARROLLO DE INGENIERÍA BÁSICA PARA INTERCONECTAR UN SISTEMA DE CONTROL CON LA RED CORPORATIVA DE UNA INDUSTRIA

JOSÉ GIRADO CARRILLO
ADALBERTO ARROYO PÉREZ

Monografía presentada como requisito parcial para aprobar el Minor en Comunicaciones y Redes

JAIME ARCILA IRIARTE
Ingeniero Electricista
DIRECTOR

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS Y ELECTRÓNICA
CARTAGENA DE INDIAS D. T. y C.
2004

Cartagena de Indias D. T. y C., Junio de 2004

Señores:
COMITÉ DE EVALUACIÓN DE PROYECTOS
Universidad Tecnológica de Bolívar
LC.

Respetados Señores:

Con toda atención, nos dirigimos a ustedes, con el fin de presentar a su consideración, estudio y aprobación, el trabajo titulado **"DESARROLLO DE INGENIERÍA BÁSICA PARA INTERCONECTAR UN SISTEMA DE CONTROL CON LA RED CORPORATIVA DE UNA INDUSTRIA"**, como requisito parcial para aprobar el Minor en Comunicaciones y Redes.

Atentamente,

JOSÉ GIRADO CARRILLO	**ADALBERTO ARROYO PÉREZ**
CC. 7.918.734 de Cartagena	**CC. 7.918.617 de Cartagena**

AUTORIZACIÓN

Cartagena de Indias D. T. y C., Junio 29 de 2004

Yo, **JOSÉ GIRADO CARRILLO**, Identificado con Número de Cédula **CC # 7.918.734** de **Cartagena de Indias**, Autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR** para hacer uso del Trabajo de Grado Titulado **"DESARROLLO DE INGENIERÍA BÁSICA PARA INTERCONECTAR UN SISTEMA DE CONTROL CON LA RED CORPORATIVA DE UNA INDUSTRIA"** y Publicarlo en el Catálogo Online de la Biblioteca.

_____

JOSÉ GIRADO CARRILLO
CC. 7.918.734 de Cartagena

AUTORIZACIÓN

Cartagena de Indias D. T. y C., Junio 28 de 2004

Yo, **ADALBERTO ARROYO PÉREZ**, Identificado con Número de Cédula **CC # 7.918.617** de **Cartagena de Indias**, Autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR** para hacer uso del Trabajo de Grado Titulado **"DESARROLLO DE INGENIERÍA BÁSICA PARA INTERCONECTAR UN SISTEMA DE CONTROL CON LA RED CORPORATIVA DE UNA INDUSTRIA"** y Publicarlo en el Catálogo Online de la Biblioteca.

_____

ADALBERTO ARROYO PÉREZ
CC. 7.918.617 de Cartagena

Cartagena de Indias D. T. y C., Junio de 2004

Señores:
COMITÉ DE EVALUACIÓN DE PROYECTOS
Universidad Tecnológica de Bolívar
LC.

Respetados Señores:

Tengo el agrado de presentar a su consideración, estudio y aprobación, el trabajo titulado **"DESARROLLO DE INGENIERÍA BÁSICA PARA INTERCONECTAR UN SISTEMA DE CONTROL CON LA RED CORPORATIVA DE UNA INDUSTRIA"**, desarrollado por los estudiantes **José Girado Carrillo** y **Adalberto Arroyo Pérez**.

El presente trabajo es un ejercicio estrictamente académico, el cual fue basado en un escenario industrial que se asemeja a la arquitectura existente de una refinería cuyo nombre no se menciona por razones de seguridad.

Al respecto me permito comunicar que he dirigido el citado trabajo, el cual considero de gran importancia y utilidad.

Atentamente,

JAIME ARCILA IRIARTE
Director del Proyecto

ARTÍCULO 107

La UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no pueden ser explotados sin la correspondiente autorización.

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias D. T. y C., Junio de 2004

Dedico Esta Obra

A dios

Por inspirarme a realizarla y en el que confío me guiará con grandeza y ética en el ejercicio profesional.

A mis padres

Por el maravilloso regalo de la educación y por estar siempre enorgullecidos de mis triunfos.

A mi familia y amigos

Por sus palabras de aliento y hacerme compañía en momentos difíciles.

José Girado Carrillo

"En lo mas Crudo del Invierno Aprendí al Fin, Que Había en mi, un Invencible Verano".

Sófocles.

Dedico Esta Obra

A dios

Por haberme dado sabiduría, tenacidad y fortaleza para culminar esta gran meta. Igualmente le pido me siga mostrando el camino como hasta ahora lo ha hecho, para emprender quizás la parte más difícil, como es mi ejercicio profesional.

A mis padres

Quienes con su ternura, amor y compresión me apoyaron en los momentos más difíciles de ésta ardua etapa de mi vida y a quienes debo gran parte de este éxito que hoy con gran esfuerzo y sacrificio finalizo.

Adalberto Arroyo Pérez

"El Conocimiento Llega a Través de la Acción; tu no Puedes Comprobarlo si no Fantaseas o Evitando Probar".

Sófocles.

Agradecemos

A Leonardo Bonilla Aldana

Por su experiencia, asesoría, y amistad

A Eduardo Gómez Vásquez

Por su justa evaluación

A Isaac Zúñiga Silgado

Por su asesoría y lecciones de vida

A Jaime Arcila Iriarte

Por su orientación

A La Universidad Tecnológica

Por formarnos y corregirnos para enfrentar el mundo

"Bien Parece Que no Estas Cursado en Esto de las Aventuras, Quítate de Ahí y Ponte en Oración Que yo Voy a Entrar con los que se Dicen Gigantes en Fiera y Desigual Batalla".

El Quijote.

CONTENIDO

2. ANÁLISIS DE ALTERNATIVAS TÉCNICO-ECONÓMICAS

2.1 ASPECTOS BÁSICOS DE SEGURIDAD

2.2 REQUERIMIENTOS TÉCNICOS DE DISEÑO

2.3 ANÁLISIS TÉCNICO

2.4 SELECCIÓN DE EQUIPOS

3. DISEÑO DE LA MEJOR ALTERNATIVA

3.1 CONFIGURACIÓN DE SEGURIDAD EN FIREWALLS

3.2 ARQUITECTURA E IMPLEMENTACIÓN MEDIANTE SOLUCIONES CISCO SYSTEMS

3.3 ARQUITECTURA E IMPLEMENTACIÓN MEDIANTE SOLUCIONES 3COM

LISTA DE FIGURAS

Pág

LISTA DE TABLAS

Pág

LISTA DE CUADROS

Pág

LISTA DE ANEXOS

Pág

GLOSARIO

10 BASE T: Estándar de transmisión de Ethernet sobre MIT a 10 Mbps.

100 BASE FX: Especificación para correr Ethernet 100 Mbps sobre fibra óptica.

100 BASE T: Estándar de transmisión sobre MIT de velocidad 100 Mbps.

Address: En redes, la palabra dirección se refiere a un distintivo único para cada nodo de la red.

Administrador: Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman súper usuario.

Algoritmo: Serie de pasos para realizar una tarea específica.

Application Server: Computador destinado a brindar los servicios de una aplicación específica a los usuarios de una red.

ATM: Tecnología de reciente introducción que permite la transmisión de grandes volúmenes de datos a gran velocidad, con tecnología de paquetes retrasados. Se considera la arquitectura del futuro en comunicaciones digitales.

AUI: Conexión utilizada para poder cambiar de tipo de cables.

Backbone Network: Red de Infraestructura. Red que actúa como conductor primario del tráfico de datos de la red. Comúnmente recibe y manda información a otras redes.

Buffer: Espacio físico de memoria destinado a guardar datos temporalmente.

Cable Nivel 5: Cable tipo MIT 4 pares que soporta 100 MHZ.

Caché: Memoria más cercana al CPU, es utilizada como buffer entre el CPU principal y el resto de la computadora. Normalmente es la memoria de más rápida, fina y cara

Communication Server: Computador destinada a dar los servicios de comunicaciones de la red.

Data Address: Localización fisíca dentro del dispositivo de almacenamiento.

Dominio: Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.

Escalabilidad: Característica de los equipos que nos permite ir aumentando velocidad y capacidad en: discos, memoria, procesadores y tarjetas periféricas.

Estación: Computadora que puede realizar procesos.

Ethernet: Estándar de red más popular e implementado. Utiliza *CSMA/CD* con una velocidad de 10 Mbps.

Fast Ethernet: Topología de transmisión digital tipo Ethernet que transmite a 100 Mbps.

FTP: Servicio que permite transferir archivos entre sistemas y entre redes remotas con sistemas diversos. De uso común en Internet.

Gateway: Dispositivo que permite conectar dos redes o sistemas diferentes. Es la puerta de entrada de una red hacia otra.

Host: Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.

Hub: Dispositivo inteligente que sirve de infraestructura para la red. Comúnmente asociado con un concentrador 10 base T con funciones inteligentes de retraso de señal *(retiming)*, y retransmisión de la misma *(repeating)*.

ICMP: Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.

Interface: Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.

Intranet: Red de área amplia con gran infraestructura y acceso privado.

IP: Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.

Patch Panel: Centro de empalme. Lugar donde llegan todos los cableados para conexión a la infraestructura de red.

Path: Nombre asignado a la variable que nos indica las rutas lógicas de los datos.

Ping: Transmisión de datos de prueba para verificar la integridad de la comunicación entre dos sistemas.

Protocolo: Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.

SNMP: Protocolo parte de TCP/IP para el manejo y la administración remota de los recursos de la red.

SPOOL: Controlador de periféricos utilizados simultáneamente por varios procesos.

TCP/IP: Protocolos definidos por catedráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.

TELNET: Utilería de TCP/IP que permite un *logon* remoto sobre un *host*.

Virtual Circuit: Conexión lograda vía programación que se comporta como si existiera conexión física directa.

RESUMEN

TITULO DE LA MONOGRAFÍA

DESARROLLO DE INGENIERÍA BÁSICA PARA INTERCONECTAR UN SISTEMA DE CONTROL CON LA RED CORPORATIVA DE UNA INDUSTRIA.

OBJETIVO GENERAL

Realizar la Ingeniería Básica Para la Interconexión de una Red de Control con la Red Corporativa de una Industria.

OBJETIVOS ESPECÍFICOS

- Analizar el modelo de Red de la Red de Planta, el cual vaya acorde a las necesidades de convergencia de la red de control con la red corporativa de una organización en particular.
- Conocer soluciones de hardware y software de capa dos y capa tres, a la medida de las necesidades de interconexión de la Red de Planta. Realizar un análisis técnico-económico de estas soluciones.
- Describir estrategias de seguridad basados en las políticas de seguridad ya definidas.

BREVE DESCRIPCIÓN DEL PROBLEMA

Las industrias modernas automatizan el control de sus procesos a través de Sistemas de Control Distribuidos, PLC's, sistemas de parada de emergencia, sistemas históricos de información de planta en tiempo real.

La tendencia de todos estos sistemas es la de enlazarse con la red corporativa de las empresas de tal manera que sea factible su gestión, administración, optimización, planeación, programación y control; obviamente con las implicaciones de seguridad.

En general los Sistemas de Control Distribuido trabajan con versiones conocidas y básicas de sistemas operativos (Windows 2000, Unix HPUX, Unix Solaris) y por ende heredan los problemas de seguridad de estas plataformas. En principio el diseño de estos sistemas fue concebido para operar de manera cerrada, de tal manera que no se pensaba en los problemas de seguridad.

Un aspecto que incrementa el problema, es que las aplicaciones que corren sobre las plataformas son propietarias y dejan casi inflexible la posibilidad de mejorar el esquema de seguridad de la plataforma: Tal como servicios que por si solos son inseguros por no tener esquemas de autenticación y es necesario tenerlos disponibles para la correcta funcionalidad de los sistemas de Control.

Muchas veces se obvian aspectos tales como la escalabilidad, la confiabilidad, el desempeño y la extensión.

Para este caso en particular se hace necesario instalar un firewall que haga las veces de gateway en donde se pueda dividir perfectamente los linderos entre los Sistemas de Control y la Red Corporativa.

Se pretende mediante este proyecto, desarrollar ingeniería básica con el objeto de dar soluciones de arquitectura, seguridad y confiabilidad, partiendo del caso particular de una industria en Cartagena, cuyo nombre no se menciona por razones de seguridad.

INTRODUCCIÓN

Hace aproximadamente un año atrás la mencionada industria terminó de implementar casi en su totalidad un nuevo sistema de control distribuido con el objetivo de automatizar las áreas operativas que no se encontraban automatizadas.

En esta implementación no se visiono la futura convergencia entre la red corporativa de la industria y los sistemas de control, mas aun obviando esquemas de seguridad que garanticen la confidencialidad de los datos, sin dejar de lado su eficacia y eficiencia.

Dado el avance en estos sistemas se obliga cada vez mas a la integración de los mismos a fin de optimizar y mejorar todo tipo de gestión que conduzca al mejoramiento de los mismos y que garanticen al personal trabajar en un ambiente mas seguro, garantizando la continuidad de los procesos y sin obviar en ningún momento los aspectos de seguridad.

El análisis y diseño para reestructurar una red industrial es una oportunidad de desarrollar aspectos como: la gestión de usuarios, gestión del hardware, gestión del software, la monitorización de la actividad de red y la seguridad, entre otros, mediante la administración y gestión de redes, aspectos contenidos en la mayoría de los módulos desarrollados en el avance del Minor.

Este obra interesa a cualquier organización, en particular a una importante industria en Cartagena cuyo nombre no se menciona por razones de seguridad y puede ser generalizado para cualquier caso donde se tengan Sistemas de Control Distribuido interconectados a una Red Corporativa.

CAPÍTULO 1

DESCRIPCIÓN GENERAL Y DIAGNÓSTICO DE LA RED DE PLANTA

1.3 DESCRIPCIÓN GENERAL

1.4 ARQUITECTURA DEL SISTEMA ACTUAL

1.3 CONFIGURACIÓN ACTUAL RED DE PLANTA

1.4 DIAGNÓSTICO DE LA RED DE PLANTA

1.1 DESCRIPCIÓN GENERAL

Las actividades de la empresa están organizadas en un Edificio de Control Central (CCB) y cuatro Áreas Estratégicas (Red de Control): area de servicios industriales, área de crudo, área de craking y área de elementos externos; responsables de la actividad productiva de la industria.

1.1.1 Diagrama General de Red - Áreas Operativas de la Empresa

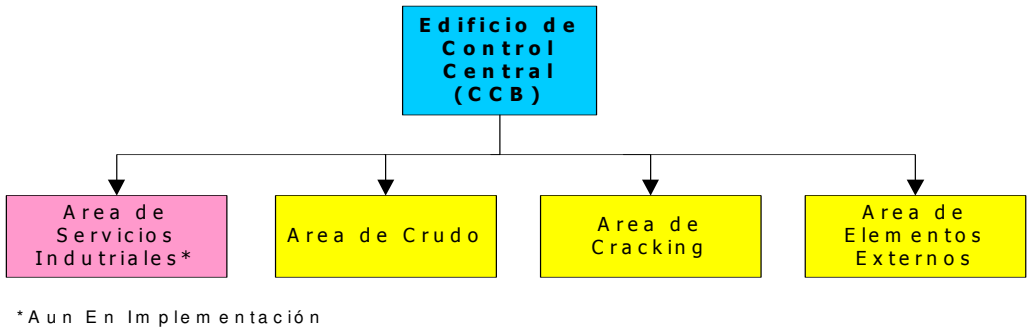


Figura 1. Áreas Operativas de la Empresa

La interconexión a cada una de las consolas utilizadas en el área computacional de la industria se efectúa mediante protocolo TCP/IP. Esto incluye: las Estaciones de Operación ubicadas en los Cuartos Satélites, las Consolas de Información, Ingeniería y de Operador ubicadas en el Cuarto de Control Central y las Consolas de Entrenamiento. En la figura 2 se muestra la extensión de las operaciones de las áreas de la industria con sus Cuartos de Control Satélite, en los cuales se hace efectivo el historial operativo de los procesos y lo que permite realizar operaciones de una determinada área desde diferentes sitios en la planta.

1.1.2 Diagrama de las Áreas de Operación con sus Cuartos de Control Satélite

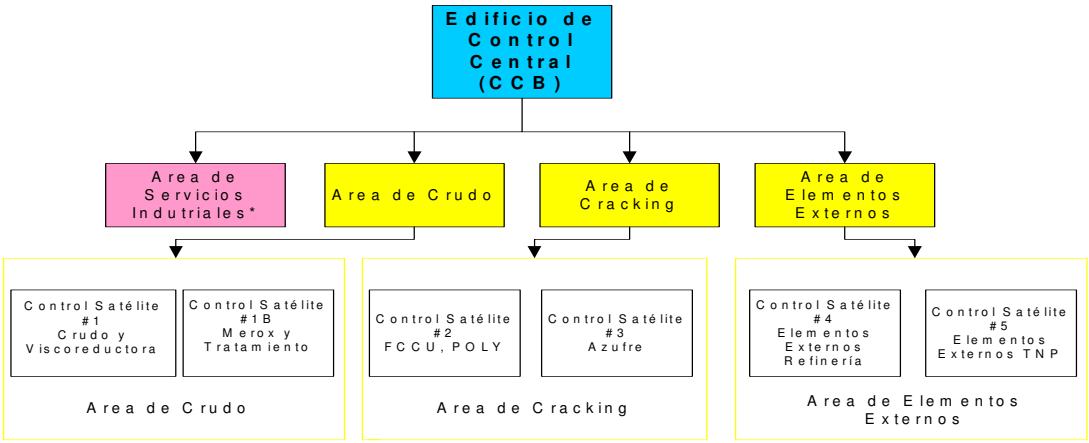


Figura 2. Áreas De Operación Con Sus Cuartos De Control Satélite

1.2 ARQUITECTURA DEL SISTEMA ACTUAL

1.2.1 La Red de Planta

También conocida como la Red Corporativa, es el lugar de control operativo de la mayoría de los procesos de la industria y sobre el cual se halla todo sistematizado y automatizado. La interconexión entre la red de planta y la red de control se realiza a través de un *Switch Atm 3Com Corebuilder 7000* mediante dispositivos de interconexión ubicados en el Cuarto de Comunicaciones.

Para esta interconexión se utilizan:

- 1 Router Switch *3Com SuperStack II 3800* (switch mediador del switch Atm)
- 4 Hubs *3Com SuperStack II HUB 10 Ethernet*, conectados en cascada
- 2 Hubs *3Com SuperStack II Baseline Dual Speed* para Fibra
- 1 Switch *3Com SuperStack II Baseline* a 10/100 Mbps

El switch mediador (*Switch Nivel 3 Superstack II 3800*) interconecta los demás dispositivos de la siguiente manera:

- Interconecta al *Switch Atm 3Com Core Builder 7000*, el cual comunica la red control con la red corporativa.
- Interconecta al grupo de Hubs *3Com SuperStack II*, los cuales se encargan de concentrar la información proveniente del cuarto de computadoras en donde se realizan las tareas de mantenimiento, optimización y reconciliación entre otras.
- Interconecta al switch *3Com SuperStack II Baseline 10/100 Mbps*, el cual enlaza este sistema con los sistemas HoneyWell, Siemens y Foxboro, utilizados en la industria.

1.2.2 Área de Reestructuración (Cuarto de Comunicaciones)

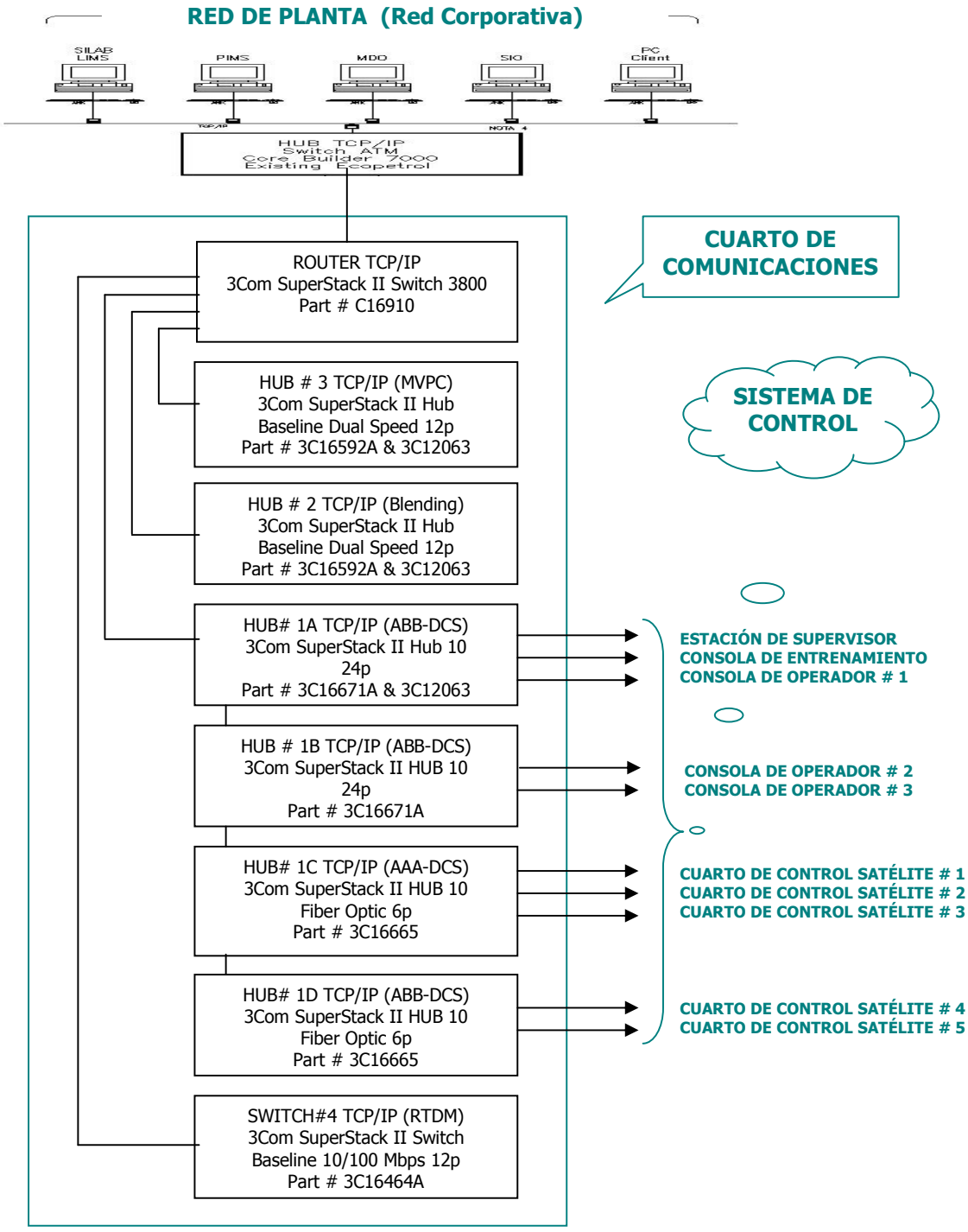
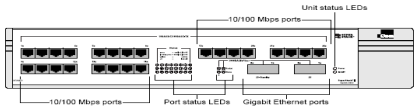
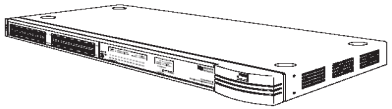
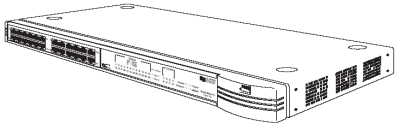
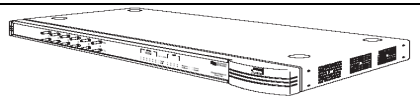
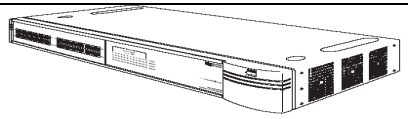


Figura 3. Cuarto de Comunicaciones

1.2.3 Descripción de Dispositivos de Red (Área de Reestructuración)

Fabricante	Referencia	Foto	Numero De Parte	Descripción Básica
3Com	**3Com SuperStack II Router Switch 3800**		**Part # C16910 Router Switch**	24 puertos de salida 10BASE-T/100BASE-TX. Un puerto Gigabit Ethernet, Un puerto redundante Gigabit Ethernet. Extencion maxima de 64 Vlans. Operación completa de nonblocking.
3Com	**3Com SuperStack II Hub Baseline Dual Speed 12p**		**Part # 3C16592A & 3C12063 HUB # 2 y HUB # 3**	12 o 24 puertos RJ-45 10/100. Socket adicional para alimentación redundante. Leds indicadores de trafico y de estado para cada puerto y Led indicador de condicion de estado del hub.
3Com	**3Com SuperStack II Hub 10 24p**		**Part # 3C16671A & 3C12063 HUB # 1A y HUB # 1B**	24 puertos RJ-45 10/100 solo para datos. Leds indicadores de trafico y de estado para cada puerto y Led indicador de condicion de estado del hub.
3Com	**3Com SuperStack II HUB 10 Fiber Optic 6p**		**Part # 3C16665 HUB # 1C y HUB # 1D**	6 puertos de fibra optica multimodo. Leds indicadores de trafico y de estado para cada puerto y Led indicador de condicion de estado del hub.
3Com	**3Com SuperStack II Switch Baseline 10/100 Mbps 12p**		**Part # 3C16464A SWITCH # 4 TCP/IP (RTDM)**	12 puertos de salida Rj45 a 10/100 mbps. Socket adicional para alimentación redundante. Leds indicadores de trafico y de estado para cada puerto y Led indicador de condicion de estado del switche.

Cuadro 1. Dispositivos del Área de Reestructuración

1.2.4 Computadores de la Red de Planta

La Red de Planta esta compuesta por un grupo de computadoras conectadas al switch ATM, utilizando protocolo TCP/IP, mostrado en la figura 3. Los equipos más destacados de esta red son:

- SILabs - Sistema de información de laboratorios.
- RIS. - Base de datos que integra todos los sistemas de la refinería.
- SIO - Sistema de información de operaciones.
- PC Client - Para acceder a la información de la Base de datos en tiempo real.

1.2.5 Sistema de Control de la Industria

La Red de Control[1] implementada en el sistema de control distribuido de la industria es una MasterBus 300. Ésta es una red tipo propietaria utilizada para la interconexión de los equipos (controladores avanzados, estación de operación y aplicación, etc.) de control de la marca ABB.

Específicamente, en la industria se colocó un hub S*tarCoupler* MB300E en cada cuarto satélite, de tal manera que sirviera de concentrador para el controlador avanzado y la estación de operación del satélite. A través de este hub se establece comunicación redundante con el Hub (MB300E) encargado del área de operación respectiva y localizada en el cuarto de comunicaciones. Con este último hub se establece comunicación con las distintas consolas de operación y aplicación del área, ubicadas en el cuarto de control central. En la figura 4 se muestra un diagrama simplificado de la red de control.

Arquitectura de la Red de Control Masterbus 300

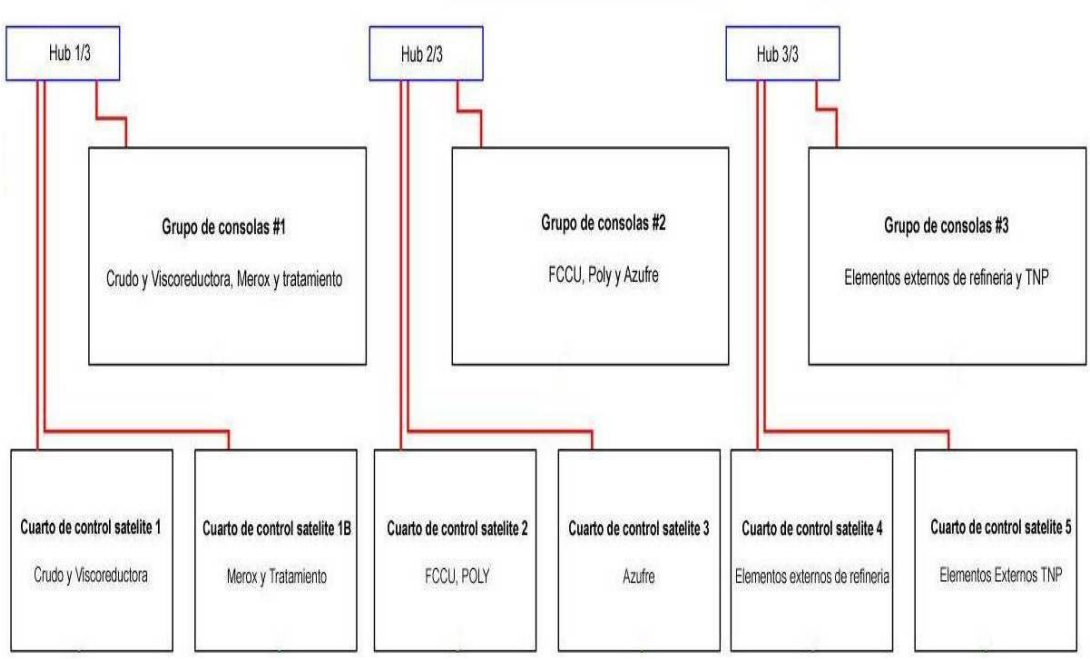


Figura 4. Diagrama de la Red de Control

Para una descripción más detallada del sistema de control y las otras areas de la industria refierase al Anexo D.

Es importante destacar que en las políticas de seguridad a desarrollar no se tendrá en cuenta la red de control MasterBus 300. Esto se debe a que es una red muy segura, ya que es una red de protocolo propietario de ABB.

Además de esto la red de control se encuentra dividida con respecto a las áreas en tres segmentos aislados, ya que no existe comunicación entre los tres hubs, por lo tanto, los servicios de un área no pueden ser accedidos por otra a través de esta red.

1.3 CONFIGURACIÓN ACTUAL RED DE PLANTA

1.3.1 Listado de Equipos

El listado de equipos interconectados a los actuales dispositivos de redes se da a partir de la base de datos del Administrador del Sistema y en base al esquema de configuración de la red de planta teniendo siempre en cuenta que:

- Los equipos del cuarto de computadoras se comunican con el router switch nivel 3 a través de los *hubs 3Com Superstack II* hub # 3 y # 2.
- Los equipos que se conectan al hub # 3 son: *FCCU Optimizer & Modelling, Short Term Scheduling and Target Setting, Data Reconciliation*.
- Los equipos que se conectan al hub # 2 son: *Star Blend y ABC*.
- La red actual se comunica con el router a través del switch *ATM Core Builder 7000*.
- Los PCs de las oficinas del CCB (Edificio de Control Central) se conectan al switch # A y se comunican con el switch ATM a través del switch # B. Tanto el switch # A como el # B tienen como referencia *3Com Superstack II 3300*.
- El área de servicios industriales (consolas Foxboro, Siemens y Honeywell) al igual que el servidor RTDM HP9000 y todas las demás interfases tienen acceso a la red a través del Switch # 4 que es un *3Com Superstack II* switch.
- Las consolas tanto de operador como de aplicación del área de crudo se conectan a la red a través del hub 1A 3Com Superstck hub 10 de igual manera que lo hacen las consolas de entrenamiento.
- Las consolas de las área de cracking y elementos externos van conectadas a través del hub # 1B 3Com Superstck hub 10.

- Las consolas de los cuartos satélites # 1, # 1B, # 2 y # 3 van conectadas a través de fibra óptica al hub # 1C 3Com Superstck hub 10, mientras que las de los cuartos satélites # 4 y # 5 van conectadas al hub # 1D.
- Como se muestra en la figura 3 (pág 5), estos últimos 2 hubs están conectados en cascada por lo que el acceso al router se realiza a través del hub # 1A.
- Los sistemas remotos y el cuarto eléctrico se conectan al router a través del switch # 5.

En la tabla 1 se detalla la lista con las principales características de configuración como: la Localización, Descripción o Función, Nodo Equivalente en La Red de Control (direccion MB300), Tipo de Equipo, Nombre del Host, Dirección a la Red TCP/IP y su conexión a cada dispositivo de red en la Red de Planta.

Esta tabla sirve de guía para realizar el análisis de la red TCP/IP en el desarrollo de la mejor alternativa y para realizar futuras recomendaciones al respecto. Es importante aclarar que las direcciones IP de los dispositivos es ficticia, esto, para no comprometer la seguridad de la industria.

1.3.2 Localización y Configuración de Equipos

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
Hub#2	Estación De Control Avanzado De Blending	PC	Eabc	150.67.13.6	CCB-CONSOLA3
Hub#2	Estación De Control Avanzado	PC	Eabc10	150.67.13.11	CCB-COMUNIC-1
Hub#1A	Estación De Operación #1 Consola De Crudo	OS520	Eas110	150.67.14.11	CCB-CONSOLA1
Hub#1A	Estación De Operación #2 Consola De Crudo	OS520	Eas120	150.67.14.12	CCB-CONSOLA1
Hub#1A	Estación De Operación #3 Consola De Crudo	OS520	Eas130	150.67.14.13	CCB-CONSOLA1
Hub#1A	Estación De Operación #4 Consola De Crudo	OS520	Eas140	150.67.14.14	CCB-CONSOLA1
Hub#1A	Estación De Operación #5 Consola De Crudo	OS520	Eas150	150.67.14.15	CCB-CONSOLA1
Hub#1A	Estación De Operación #6 Consola De Crudo	OS520	Eas160	150.67.14.16	CCB-CONSOLA1
Hub#1A	Estación De Operación #1 Consola De Cracking	OS520	Eas170	150.67.14.17	CCB-CONSOLA2
Hub#1A	Estación De Operación #2 Consola De Cracking	OS520	Eas180	150.67.14.18	CCB-CONSOLA2
Hub#1A	Estación De Operación #3 Consola De Cracking	OS520	Eas190	150.67.14.19	CCB-CONSOLA2
Hub#1A	Estación De Operación #4 Consola De Cracking	OS520	Eas200	150.67.14.20	CCB-CONSOLA2
Hub#1A	Estación De Operación #5 Consola De Cracking	OS520	Eas210	150.67.14.21	CCB-CONSOLA2
Hub#1A	Estación De Operación #6 Consola De Cracking	OS520	Eas220	150.67.14.22	CCB-CONSOLA2
Hub#1B	Estación De Operación #1 Consola De Blending	OS520	Eas230	150.67.14.23	CCB-CONSOLA3
Hub#1B	Estación De Operación #2 Consola De Blending	OS520	Eas240	150.67.14.24	CCB-CONSOLA3
Hub#1B	Estación De Operación #3 Consola De Blending	OS520	Eas250	150.67.14.25	CCB-CONSOLA3
Hub#1B	Estación De Operación #4 Consola De Blending	OS520	Eas260	150.67.14.26	CCB-CONSOLA3
Hub#1B	Estación De Operación #5 Consola De Blending	OS520	Eas270	150.67.14.27	CCB-CONSOLA3
Hub#1B	Estación De Operación #6 Consola De Blending	OS520	Eas280	150.67.14.28	CCB-CONSOLA3
Hub#1A	Estación De Ingeniería Sistema De Crudo	OS520	Eas290	150.67.14.29	CCB-APLICACION1
Hub#1A	Estación De Ingeniería Sistema De Cracking	OS520	Eas300	150.67.14.30	CCB-APLICACION2
Hub#1B	Estación De Ingeniería Sistema De Blending	OS520	Eas310	150.67.14.31	CCB-APLICACION3
Hub#1C	Estación De Operación Local Sistema De Crudo	OS520	Eas380	150.67.14.38	SIH#1-CONSOLA
Hub#1C	Estación De Operación Local Sistema De Tratamiento	OS520	Eas390	150.67.14.39	SIH#1-CONSOLA
Hub#1C	Estación De Operación Local Sistema De Cracking	OS520	Eas400	150.67.14.40	LCB#2-CONSOLA

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
Hub#1C	Estación De Operación Local Sistema De Azufre	OS520	Eas410	150.67.14.041	LCB#3-CONSOLA
Hub#1D	Estación De Operación Local Sistema De Blending Refinería	OS520	Eas420	150.67.14.042	LCB#4-CONSOLA
Hub#1D	Estación De Operación Local Sistema De Blending Tnp	OS520	Eas430	150.67.14.43	LCB#5-CONSOLA
Hub#1B Hub of-Con	Estación De Operación #1 Sistema De Entrenamiento	OS520	Eas610	150.67.14.61	CCB-ENTRENAMIENTO
Hub#1B Hub of-Con	Estación De Operación #2 Sistema De Entrenamiento	OS520	Eas620	150.67.14.62	CCB-ENTRENAMIENTO
Hub#1B Hub of-Con	Estación De Operación #5 Sistema De Entrenamiento	OS520	Eas640	150.67.14.64	CCB-ENTRENAMIENTO
Hub#1B Hub of-Con	Estación De Operación #4 Sistema De Entrenamiento	OS520	Eas650	150.67.14.65	CCB-ENTRENAMIENTO
Hub#1B Hub of-Con	Estación De Operación #3 Sistema De Entrenamiento	OS520	Eas660	150.67.14.66	CCB-ENTRENAMIENTO
Switch#4	Estación De Operación Y Gateway #1 Foxboro	AW51	Eaw030	150.67.14.121	CCB-CONSOLA4
Switch#4	Estación De Operación Y Gateway #1 Foxboro	AW51	Eaw040	150.67.14.122	CCB-CONSOLA4
Switch#4	Estación De Base De Datos En Tiempo Real	UNIX	Ebdtr	150.67.13.1	CCB-COMUNIC-PI
Hub#3	Estación Bently Nevada	PC	Ebn	150.67.13.13	CCB-MANTENIMIENTO
Hub#3	Estación De Analizadores Vistanet	PC	Ecac	150.67.13.10	CCB-MANTENIMIENTO
Hub#1A	Estación De Ingeniería Sistema Abb	PC	Ees00	150.67.14.10	CCB-COMUNIC-1
Switch#5	Estación #1 Sistema De Shutdown De Crudo	PC	Eesd10a	150.67.16.51	CCB-CONSOLA1
Switch#5	Estación #2 Sistema De Shutdown De Crudo	PC	Eesd10b	150.67.16.52	CCB-CONSOLA1
Switch#5	Estación Local Sistema De Shutdown De Crudo	PC	Eesd10c	150.67.16.53	SIH#1-CONSOLA
Switch#5	Estación #1 Sistema De Shutdown De Cracking	PC	Eesd20a	150.67.16.55	CCB-CONSOLA2
Switch#5	Estación #2 Sistema De Shutdown De Cracking	PC	Eesd20b	150.67.16.56	CCB-CONSOLA2
Switch#5	Estación Local Sistema De Shutdown De Cracking	PC	Eesd20c	150.67.16.57	LCB#2-CONSOLA
Switch#5	Estación Local Sistema De Shutdown De Azufre	PC	Eesd20d	150.67.16.58	LCB#3-CONSOLA
Hub#3	Multiplexer Ams Smart Transmitter Interface	MX	Ihmux	150.67.13.8	CCB-MANTENIMIENTO
Hub#3	Estación Ams Smart Transmitter Interface - Hart	PC	Ehpc	150.67.13.7	CCB-MANTENIMIENTO
	Router Super Stack 3800	ETHERNET	Ehub	150.67.16.1	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Red De Planta Abb	ETHERNET	Ehub10	150.67.16.2	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Red De Planta Abb	ETHERNET	Ehub10	150.67.16.2	CCB-COMUNIC-RACK
	Hub 6 Puertos Fibra Óptica	ETHERNET	Ehub10	150.67.16.2	CCB-COMUNIC-

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
	Red De Planta Abb				RACK
	Hub 6 Puertos Fibra Óptica Red De Planta Abb	ETHERNET	Ehub10	150.67.16.2	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Blending	ETHERNET	Ehub20	150.67.16.3	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Control Avanzado	ETHERNET	Ehub30	150.67.16.4	CCB-COMUNIC-RACK
	Swith 12 Puertos Utp Base De Datos En Tiempo Real	ETHERNET	Ehub40	150.67.16.5	CCB-COMUNIC-RACK
	Swith 24 Puertos Utp Esd Y Ups	ETHERNET	Ehub50	150.67.16.6	CCB-COMUNIC-RACK
Hub#3	Pc Portatil Hvac	PORTATIL	Ehvac	150.67.13.12	CCB-MANTENIMIENTO
Hub#1A	Estación De Historia Sistema De Crudo	IMS530	Eims330	150.67.14.33	CCB-APLICACION1
Hub#1A	Estación De Historia Sistema De Cracking	IMS530	Eims340	150.67.14.34	CCB-APLICACION2
Hub#1B	Estación De Historia Sistema De Blending	IMS530	Eims350	150.67.14.35	CCB-APLICACION3
Switch#4	Estación Gateway Pi Sistema De Crudo	IMS530	Eims440	150.67.14.44	CCB-APLICACION1
Switch#4	Estación Gateway Pi Sistema De Cracking	IMS530	Elms450	150.67.14.45	CCB-APLICACION2
Switch#4	Estación Gateway Pi Sistema De Blending	IMS530	Elms460	150.67.14.46	CCB-APLICACION3
Switch#4	Estacion Gateway Pi-Abb	IMS530	Eims470	150.67.14.47	CCB-COMUNIC-1
Hub#1B Hub of-Con	Estación De Historia Sistema De Entrenamiento	IMS530	Eims630	150.67.14.63	CCB-ENTRENAMIENTO
	Impresora Laser A Color Sistema De Entrenamiento	LCP	ILcp10	150.67.15.1	CCB-ENTRENAMIENTO
	Impresora Laser A Color Operadores De Consola	LCP	ILcp20	150.67.15.2	CCB-CONSOLA4
	Impresora Laser A Color Administrador Del Sistema	LCP	Ilcp30	150.67.15.3	CCB-SISTEMA
	Impresora Laser A Color Cuarto De Mantenimiento	LCP	Ilcp40	150.67.15.4	CCB-MANTENIMIENTO
Hub#1A	Impresora Laser A Color Sistema De Ingeniería	LCP	Ilcp50	150.67.15.5	CCB-APLICACION2
Hub#3	Impresora Laser Blanco Y Negro Administrador Pi	LP	ILip60	150.67.15.6	CCB-COMUNIC-1
	Hub Mb300 Para Sistema De Crudo	MB300			CCB-COMUNIC-RACK
	Hub Mb300 Para Sistema De Cracking	MB300			CCB-COMUNIC-RACK
	Hub Mb300 Para Sistema De Blending	MB300			CCB-COMUNIC-RACK
	Star Coupler Mb300 Para Sistema De Crudo	MB300			SIH#1-DCS
	Star Coupler Mb300 Para Sistema De Tratamiento	MB300			SIH#1B-DCS
	Star Coupler Mb300 Para Sistema De Cracking	MB300			SIH#2-DCS
	Star Coupler Mb300 Para Sistema De Azufre	MB300			SIH#3-DCS

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
	Star Coupler Mb300 Para Sistema De Blending Refinería	MB300			SIH#4-DCS
	Star Coupler Mb300 Para Sistema De Blending Tnp	MB300			SIH#5-DCS
	Switche Mb300 Multilan Para Red 11	MB300			CCB-COMUNIC-RACK
	Switche Mb300 Multilan Para Red 12	MB300			CCB-COMUNIC-RACK
	Impresora Matriz De Punto Consola De Crudo 1	MP			CCB-COMUNIC-1
	Impresora Matriz De Punto Consola De Crudo 2	MP			CCB-CONSOLA1
	Impresora Matriz De Punto Consola De Cracking 1	MP			CCB-CONSOLA2
	Impresora Matriz De Punto Consola De Cracking 2	MP			CCB-CONSOLA2
	Impresora Matriz De Punto Consola De Blending 1	MP			CCB-CONSOLA3
	Impresora Matriz De Punto Consola De Blending 1	MP			CCB-CONSOLA3
	Impresora Matriz De Punto A Color Bently Nevada	MP			CCB-MANTENIMIENTO
	Impresora Matriz De Punto Sistema Esd De Crudo	MP			CCB-CONSOLA1
	Impresora Matriz De Punto Sistema Esd De Cracking	MP			CCB-CONSOLA2
Hub#3	Estación Nir	PC	Enir	150.67.13.9	CCB-MANTENIMIENTO
Hub#3	Estación Del Optimizador De Cracking	PC	Eopti	150.67.13.4	CCB-APLICACION2
	Estación De Reconciliacion De Datos	PC	EReda	150.67.13.3	CCB-SISTEMA
N.A.	Estación De Operación #1 Siemens	OT	Esie010	150.67.14.123	CCB-CONSOLA4
N.A.	Estación De Operación #2 Siemens	OT	Esie020	150.67.14.124	CCB-CONSOLA4
N.A.	Estación De Operación #3 Siemens	OT	Esie030	150.67.14.125	CCB-CONSOLA4
N.A.	Estación De Operación #4 Siemens	OT	Esie040	150.67.14.126	CCB-CONSOLA4
Switch#4	Estación Gateway Siemens	XU	Esie050	150.67.14.127	CCB-COMUNIC-PI
	Estación Pc Esclavo Siemens	PC	Esie060	150.67.14.128	CCB-COMUNIC-PI
Hub#2	Estación De Star Blend	PC	Estarb	150.67.13.5	CCB-CONSOLA3
Hub#3	Estacion De Short Term Schedulling	PC	Ests	150.67.13.2	CCB-SISTEMA
Switch#5	Ups No.1 Ccb	UPS		150.67.16.101	CCB-UPS
Switch#5	Ups No.2 Ccb	UPS		150.67.16.102	CCB-UPS
Switch#5	Ups No.3 Ccb	UPS		150.67.16.103	CCB-UPS
Switch#5	Ups No.1 Sih#1	UPS		150.67.16.104	SIH#1
Switch#5	Ups No.2 Sih#1	UPS		150.67.16.105	SIH#1
Switch#5	Ups No.1 Sih#2	UPS		150.67.16.106	SIH#2
Switch#5	Ups No.2 Sih#2	UPS		150.67.16.107	SIH#2
Switch#5	Ups No.1 Sih#3	UPS		150.67.16.108	SIH#3

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
Switch#5	Ups No.2 Sih#3	UPS		150.67.16.109	SIH#3
Hub#1A	Estación De Ingeniería Xterminal Sistema De Crudo	PC	EXterm10	150.67.14.130	CCB-APLICACION1
Hub#1A	Estación De Ingeniería Xterminal Sistema De Cracking	PC	EXterm20	150.67.14.131	CCB-APLICACION2
Hub#1B	Estación De Ingeniería Xterminal Sistema De Blending	PC	EXterm30	150.67.14.132	CCB-APLICACION3

Tabla 1. Esquema Actual de Direccionamiento

En la figura 5 se especifica la configuración por puertos de cada dispositivo con su respectiva conexión a cada consola en el área de los sistemas de control. En el Patch Panel se encuentra escrito y rotulado, la descripción de cada nodo con la dirección IP que utiliza y se describe la consola en la cual operan con la respectiva ubicación dentro de la misma.

Los colores ayudan a una facil interpretación de la conexion de cada nodo, su conexión a cada dispositivo de red y a su vez la interconexión a las consolas en el area del sistema de control.

1.3.3 Configuración por Nodos de Equipos de Red Conectados al Patch Panel

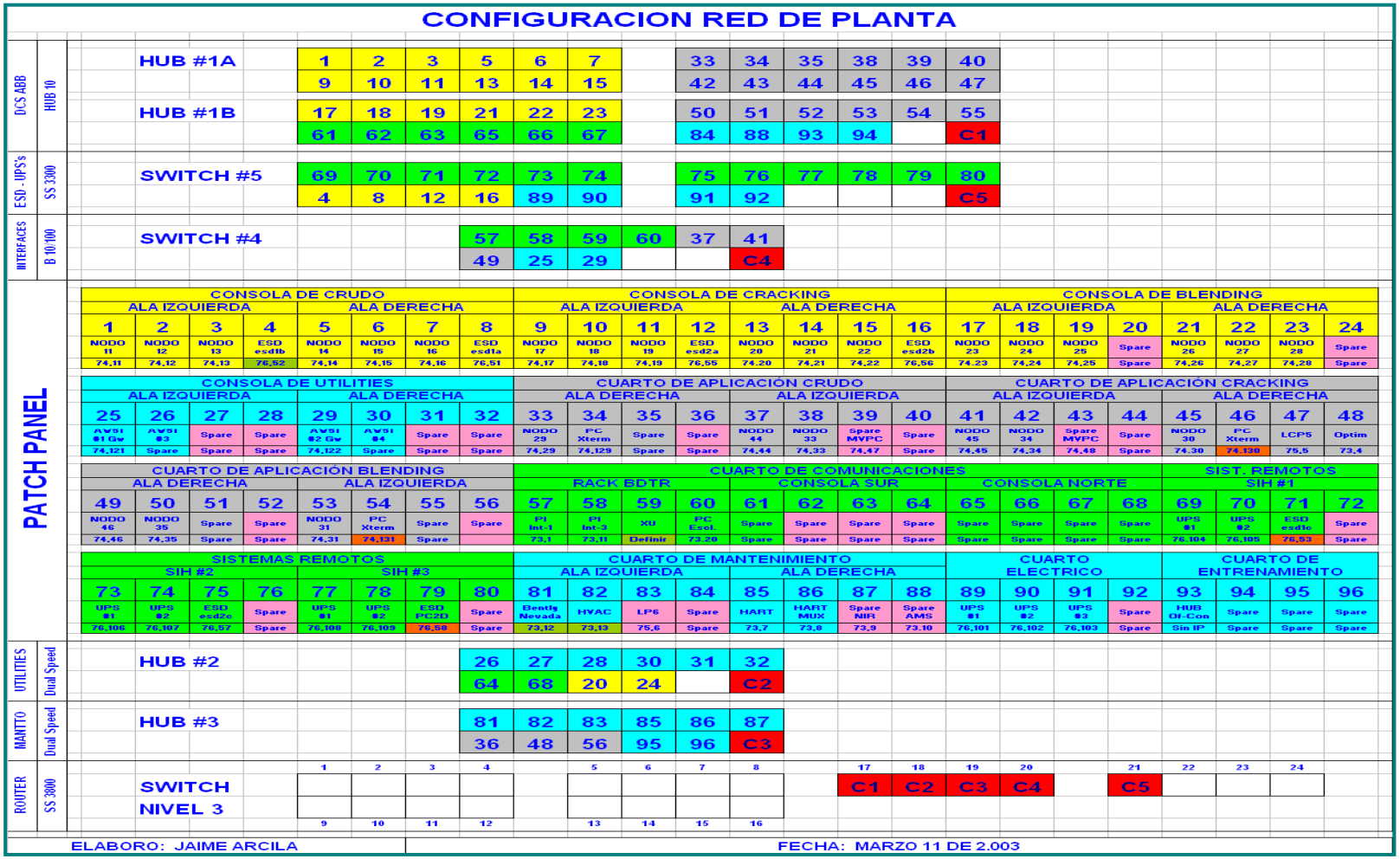


Figura 5. Conexión de Dispositivos de Red al Patch Panel por Nodos

1.4 DIAGNOSTICO DE LA RED DE PLANTA

Esta obra tiene por objeto establecer las bases conceptuales de una metodología que permita la elaboración de un Plan estratégico de Arquitectura, Ingeniería y Equipos, para el proceso de transformación por reestructuración, remodelación o ampliación de las redes de la industria.

La gestión de la Red de Planta nos permite concentrar la administración y monitoreo de los diferentes dispositivos de la red, esto con el fin de poder mantener un pleno control de cada uno de los dispositivos para que de una forma fácil y sencilla se pueda realizar cualquier cambio o modificación requerida. Todo esto basado en un punto central en donde se concentra toda la información de la red.

La gestión de esta Red, además de permitir la administración, nos permite realizar el monitoreo de tráfico dentro de los dispositivos para poder observar parámetros como utilización de los dispositivos y enlaces en términos de ancho de banda y con esto prevenir saturaciones en equipos o enlaces de comunicación, así como poder generar perfiles de tráfico basados en parámetros como calidad de servicio, aplicaciones, o en dispositivos específicos.

1.4.1 Confiabilidad

Las entidades relevantes en una red son nodos y conexiones entre nodos, y en general el principal objetivo buscado es lograr una comunicación segura entre nodos de la red. Los principales problemas a resolver en el análisis y el diseño de la red son, a grandes rasgos, los siguientes:

- Dado un conjunto de nodos que se desean comunicar entre sí, obtener una red óptima en algún sentido (por ejemplo, obtener la máxima cantidad posible de caminos distintos entre

pares de nodos), sujeto a determinadas restricciones (como por ejemplo, costo de conexión entre pares de nodos).

- Dada una red, evaluar de algún modo su confiabilidad (en el sentido de la comunicación entre nodos). Este tipo de problemas están fuertemente relacionados con el ítem anterior, donde en el proceso de búsqueda de la red óptima se deben comparar las confiabilidades de dos o más redes para escoger la mejor, o luego de obtener un resultado a partir de cierto procedimiento se debe evaluar su confiabilidad. Esta obra se centra en la resolución del último problema.

1.4.2 Aspectos de Seguridad

Definición

Una política de seguridad[2] es un conjunto de leyes, reglas y prácticas que regulan la manera en que una organización maneja, protege y distribuye información sensitiva. Es importante tener una política de seguridad de red efectiva y bien pensada que pueda proteger la inversión y recursos de información de una empresa. Sobre todo es importante que la empresa defina claramente y valore qué tan importantes son los recursos e información que se tienen en la red corporativa y dependiendo de esto se justificará el hecho de ser o no necesario que se preste la atención y esfuerzos suficientes para lograr un nivel adecuado de protección. La mayoría de las empresas poseen información sensible y secretos importantes en sus redes, esta información debería ser protegida contra el vandalismo del mismo modo que otros bienes valiosos como propiedades de la corporación y edificios de oficinas.[1]

La definición de una política de seguridad de red no es algo en lo que se pueda establecer un orden lógico o secuencia aceptada de estados debido a que la seguridad es algo muy subjetivo, cada empresa tiene diferentes expectativas, diferentes metas, diferentes formas de valorar lo que va por

[1] Sacado del Texto "Seguridad En Unix Y Redes Versión 2.1", Cap 1 y 2, Num 2-8, Pag 19.

su red, cada negocio tiene distintos requerimientos para almacenar, enviar y comunicar información de manera electrónica; por esto nunca existirá una sola política de seguridad aplicable a 2 organizaciones diferentes. Además, así como los negocios evolucionan para adaptarse a los cambios en las condiciones del mercado, la política de seguridad debe evolucionar para satisfacer las condiciones cambiantes de la tecnología.

Una política de seguridad de red efectiva es algo que todos los usuarios y administradores pueden aceptar y están dispuestos a reforzar, siempre y cuando la política no disminuya la capacidad de la organización, es decir la política de seguridad debe ser de tal forma que no evite que los usuarios cumplan con sus tareas en forma efectiva.

Importancia

Existen muchos factores que justifican el establecimiento de políticas de seguridad para un sitio específico, pero los más determinantes son:

- Ayudan a la organización a darle valor a los recursos que posee.
- Es una infraestructura desde la cual otras estrategias de protección pueden ser desarrolladas.
- Proveen unas claras y consistentes reglas para los usuarios de la red y su interacción con el entorno.
- Contribuyen a la efectividad y direccionan la protección total de la organización.
- Pueden ayudar a responder ante requerimientos legales.
- Ayudan a prevenir incidentes de seguridad.
- Proveen una guía cuando un incidente ocurre.
- Es una planeación estratégica del papel que juega la arquitectura de red al interior de la organización.

- Ayuda en la culturización de los usuarios para el uso de servicios de red e inculca el valor real que ellos representan.

Características

Una política de seguridad es un plan elaborado de acuerdo con los objetivos generales de la organización y en el cual se ve reflejados los intereses de la empresa a cerca de los servicios de red y recursos que se desean proteger de manera efectiva y que representan activos importantes para el normal cumplimiento de la misión institucional. Por esto, la política de seguridad debe cumplir con ciertas características propias de este tipo de planes, como son:

- Debe ser simple y entendible (específica).
- Debe estar siempre disponible.
- Se puede aplicar en cualquier momento a la mayoría de situaciones contempladas.
- Debe ser practicable y desarrollable.
- Se debe poder hacer cumplir.
- Debe ser consistente con otras políticas organizacionales.
- Debe ser estructurada.
- Se establece como una guía, no como una cadena a la cual se tenga que atar para siempre.
- Debe ser cambiante con la variación tecnológica.
- Una política debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas.

Pasos Para Desarrollar una Política de Seguridad

El objetivo perseguido para desarrollar una política de seguridad de red es definir las expectativas de la empresa acerca de su uso y definir procedimientos para prevenir y responder a incidentes de

seguridad provenientes del avanzado mundo de la comunicación global. Definir una política de seguridad de red significa desarrollar procedimientos y planes que salvaguarden los recursos de la red contra pérdidas y daños, por lo tanto es muy importante analizar entre otros los siguientes aspectos:

- Determinar los objetivos y directrices de la organización.
- La política de seguridad debe estar acorde con otras políticas, reglas, regulaciones o leyes ya existentes en la organización; por lo tanto es necesario identificarlas y tenerlas en cuenta al momento de desarrollar la política de seguridad de redes.
- Identificación de los recursos disponibles
- ¿Qué recursos se quieren proteger?
- ¿De quién necesita proteger los recursos?
- Identificación de posibles amenazas
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?
- Verificación frecuente de la política de seguridad de red para ver si los objetivos y circunstancias han cambiado.

En general, el costo de proteger las redes de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad. La política de seguridad debe ser comunicada a cada quien que usa un computador en la red con el fin de que sea ampliamente conocida y se pueda obtener una retroalimentación de los usuarios de la misma para efectos de revisiones periódicas y detección de nuevas amenazas o riesgos.

Huecos de Seguridad en la Red de Planta

En la red de planta de la industria se trabaja con versiones conocidas y básicas de sistemas operativos tales como: Windows 2000, Unix HPUX, Unix Solaris entre otros, por ende se heredan todos los problemas de seguridad de estas plataformas. En principio, el diseño de estos sistemas fueron concebidos para trabajar de manera cerrada, por lo tanto no se pensaba en los problemas de seguridad.

Un aspecto que incrementa esta problemática, es el hecho de que las aplicaciones que corren sobre las plataformas son propietarias y dejan casi inflexible la posibilidad de mejorar el esquema de seguridad de la plataforma, tal como servicios que por si solos son inseguros por no tener esquemas de autenticación vitales en la correcta funcionalidad de todos los servicios sobre el protocolo de comunicaciones TCP/IP.

Amenazas

Base: no existe un sistema 100 % protegido, por tanto la red de planta hereda todos los problemas comunes de ataques a la seguridad de redes. Todo elemento (Hw o Sw) es susceptible de ataque.

Amenazas más Comunes

→ Violaciones con autorización (amenazas internas)

→ Suplantación, spoofing

→ Sobrepasar los controles (bugs de las aplicaciones)

→ Troyanos, BackDoors

1.4.3 Desempeño

El actual desempeño esta sujeto a las caracteristicas tecnicas de los dispositivos en uso. El Gabinete CCB-DCS-C04 se halla compuesto en su totalidad por equipos 3com: 2 hubs con 6 puertos para fibra optica, 2 hubs 10 base-T con 24 puertos, 2 hubs *Baseline Dual Speed* con 12 puertos y un switche Baseline 10/100 de 12 puertos.

El desempeño supone exactamente la medida de las exigencias de comunicación de la red de planta con la red corporativa pero con implicaciones serias de seguridad. Por otra parte se requiere un aumento en el rendimiento de estos dispositivos para una futura convergencia de estas redes.

Loc.	Artículo	Descripción	Comentarios
+4U15	Hub#1C	Hub para Fibra Optica de 6 puertos	Marca: 3COM Super Stack II
+4U16	Hub#1D	Hub para Fibra Optica de 6 puertos	Marca: 3COM Super Stack II
+4U17	Hub#1A	Hub para 10 Base-T de 24 puertos	Marca: 3COM Super Stack II
+4U18	Hub#1B	Hub para 10 Base-T de 24 puertos	Marca: 3COM Super Stack II
+4U29		Cable Tray	Color Negro
+4U20	Hub#2	Baseline Dual Speed de 12 puertos 3C16592A	Marca: 3COM Super Stack II
+4U21	Hub#3	Baseline Dual Speed de 12 puertos 3C16592A	Marca: 3COM Super Stack II
+4U22	Switch#4	Baseline 10/100 de 12 puertos 3C16464A	Marca: 3COM Super Stack II
+4U23		Cable Tray	Color Negro
+4U24	Router	Switch 3800 de 24 puertos 3C16910	Marca: 3COM Super Stack II
+4U37	E272 100A	Breaker de Alimentación Principal	Marca: ABB
+4U37	S272K2A	Switch de Energía y Distribución 2A (5)	Marca: ABB
+4U37	S272K10A	Switch de Energía y Distribución 10A	Marca: ABB
+4U37	ZPE 2.5	Borneras (3) Modelo: 160864	Marca: Weidmüller
+4U42	E272 100A	Breaker de Alimentación Principal	Marca: ABB

Loc.	Artículo	Descripción	Comentarios
+4U42	S272K2A	Switch de Energía y Distribución 2A (4)	Marca: ABB
+4U42	ZPE 2.5	Borneras (3) Modelo: 160864	Marca: Weidmüller
+4U42	S272K3A	Switch de Energía y Distribución 3A (2)	Marca: ABB

Tabla 2. Localización de Dispositivos en el Gabinete

CAPÍTULO 2

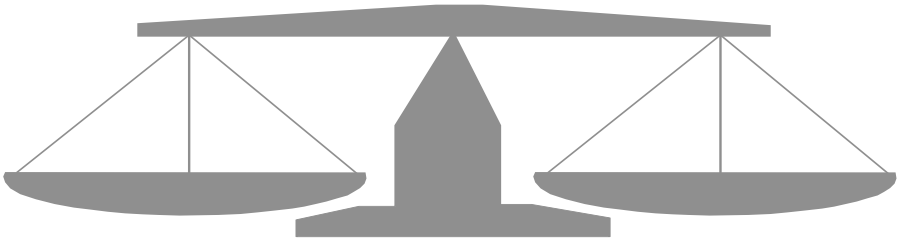
ANÁLISIS DE ALTERNATIVAS TÉCNICO-ECONÓMICAS

2.1 ASPECTOS BÁSICOS DE SEGURIDAD

2.2 REQUERIMIENTOS TÉCNICOS DE DISEÑO

2.3 ANÁLISIS TÉCNICO

2.4 SELECCIÓN DE EQUIPOS



2.1 ASPECTOS BÁSICOS DE SEGURIDAD

2.1.1 Paradigmas Organizacionales en Cuanto a Seguridad[3]

Paradigma: modelo o ejemplo de algo, en filosofía, es un conjunto de ideas filosóficas, teorías científicas y normas metodológicas que influyen en la forma de resolver los problemas en una determinada tradición científica. Sinónimo: prototipo, muestra, canon.[2]

Del paradigma se desprenden las reglas que rigen las investigaciones. Cuando dentro de un paradigma aparecen anomalías excesivas, se produce una revolución científica que consiste precisamente en el cambio de paradigma.

Es muy importante que el auditor conozca los paradigmas que existen en las organizaciones sobre la seguridad, para no encontrarse con un contrincante desconocido. Entre los principales paradigmas que se pueden encontrar veamos los siguientes:

- Generalmente se tiene la idea que los procedimientos de auditoría es responsabilidad del personal del centro de cómputo, pero se debe cambiar este paradigma y conocer que estas son responsabilidades del usuario y del departamento de auditoría interna.
- También muchas compañías cuentan con dispositivos de seguridad física para los computadores y se tiene la idea que los sistemas no pueden ser violados si no se ingresa al centro de cómputo, ya que no se considera el uso de terminales y de sistemas remotos.
- Se piensa también que los casos de seguridad que tratan de seguridad de incendio o robo las aseveraciones: "eso no me puede suceder a mí" o "es poco probable que suceda".

[2] Guia de Seguridad de Redes Para Principiantes, bajado de **www.cisco.com/go/offices**

- También se cree que los computadores y los programas son tan complejos que nadie fuera de su organización los va a entender y no les van a servir, ignorando las personas que puedan captar y usarla para otros fines.
- Los sistemas de seguridad generalmente no consideran la posibilidad de fraude interno que es cometido por el mismo personal en el desarrollo de sus funciones.
- Generalmente se piensa que la seguridad por clave de acceso es inviolable pero no se considera a los delincuentes sofisticados.
- Se suele suponer que los defectos y errores son inevitables.
- También se cree que se hallan fallas porque nada es perfecto.
- Y la creencia de que la seguridad se aumenta solo con la inspección.

El siguiente cuadro es una forma apta para llevar este tipo de información. Aunque no puede ser la mejor, pero permite distinguir las ideas que se pretender explicar.

	Viejo Equilibrio	Nuevo Desequilibrio
RR.HH. Organización Operativo.		

Cuadro 2. Forma Para Desglosar Ideas Auditables

Conclusión

Se deben analizar estos y otros paradigmas de la organización, también es muy importante que el auditor enfrente y evalúe primero sus propios paradigmas y sus paradigmas académicos.

2.1.2 Que Tanta Seguridad se debe Implementar

La seguridad por sí misma hace más difícil el acceso a un sistema al tener que proveer seguros adicionales que los usuarios deben pasar. Por otro lado si ningún tipo de seguridad es

implementada no hay problemas para los usuarios, sino que éstos ocurren cuando la seguridad aumenta.

Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

→ Aumento de la productividad.

→ Aumento de la motivación del personal.

→ Compromiso con la misión de la compañía.

→ Mejora de las relaciones laborales.

→ Ayuda a formar equipos competentes.

→ Mejora de los climas laborales para los RR.HH.

2.2 REQUERIMIENTOS TÉCNICOS DE DISEÑO

Los requerimientos mínimos de diseño por reestructuración de dispositivos de red, es información determinante, suministrada por la Dirección del proyecto de sistematización de la industria, acorde a un estudio previo de necesidades y en base a la visión y misión del ente industrial, sin dejar de lado aspectos como: la confiabilidad, el desempeño y la escalabilidad.

2.2.1 Requerimientos de Reestructuración

Se requiere cambio de switches y hubs con el objeto de satisfacer las siguientes necesidades:

- ✓ Alimentación Redundante.
- ✓ Un Mínimo de 100 Mbps.
- ✓ Switches Totalmente Administrables.
- ✓ Segmento 1: switches administrables que cubran minimo una necesidad de 36 puertos
- ✓ Segmento 2: switches administrables que cubran minimo una necesidad de 24 puertos
- ✓ Segmento 3: switches administrables que cubran minimo una necesidad de 24 puertos
- ✓ Segmento 4: switches administrables que cubran minimo una necesidad de 24 puertos
- ✓ Segmento 5: switches administrables que cubran minimo una necesidad de 24 puertos
- ✓ Segmento 6: switches administrables que cubran minimo una necesidad de 24 puertos

2.2.2 Requerimientos de Router

Se requieren cambios a fin de mejorar: desempeño, confiabilidad y seguridad.

- ✓ Firewall Administrable
- ✓ Un Mínimo de 100 Mbps.

- ✓ Alimentación Redundante.
- ✓ Un puerto de enlace a la red corporativa ATM a más de 100 Mbps o Fast-Ethernet.
- ✓ Mínimo 12 puertos de salida.

2.2.3 Cambio de Patch Panel:

De acuerdo al número de puertos que resulten del diseño final de selección, pero con un 20 % adicional de puertos libres.

Alternativas en Base a los Tópicos: Firewall y Switches

En la actualidad los dispositivos de interconexión ofrecen en sus paquetes aplicaciones firewall, aplicaciones gateway y combinación de estos, el presente estudio se centra en seleccionar la mejor alternativa técnico-económica, según el sofisticado paquete que ofrecen algunos dispositivos, sin dejar de lado el buen desempeño de algunos firewall como dispositivo único.

2.3 ANÁLISIS TÉCNICO

2.3.1 Estado del Arte en Dispositivos de Red

Es importante que la industria se encuentre en sincronía respecto a los fabricantes líderes en el mundo en dispositivos de red. Por una parte, se mantiene a la vanguardia tecnológica, y por otra se permite expandir en un futuro sus oficinas a nivel internacional haciendo menos traumático el acople con tecnologías mundialmente confiables

2.3.2 Alternativas de Cambio de Switches, Routers y Hubs

Algunos fabricantes, como el caso de Cisco Systems, 3COM Y Symantec, predominan con gran fuerza en el mundo de las redes.

Hoy dia los dispositivos han evolucionado a tal punto que los fabricantes ofrecen paquetes que involucran varias capas del modelo OSI, haciendo cada vez mas convergente la funcionalidad de los dispositivos de red.

Cisco Systems	3Com	Symantec
		

Cuadro 3. Fabricantes Mundialmente Confiables

Existen firewalls que hacen las veces de gateway y viceversa, existen routers que hacen las veces de firewalls y viceversa, como tambien existen los llamados router-switchs que mientras ejecutan funciones de capa 2, auxilian y complementan funciones de capa 3, 4, y hasta de capa 5, en fin, la tecnología al punto que evoluciona, tambien busca facilitar la configuración de la amplia gama de dispositivos de red haciéndolos cada vez mas eficientes, robustos y con paquetes que antes solo eran asequibles por las grandes empresas, todo esto ha ido cambiando a medida que se evoluciona en la electrónica de estos dispositivos.

2.3.3 Selección de Dispositivos en Base a Requerimientos Técnicos

Fabricante	Referencia	Interfases Fast Ethernet 10/100	Puertos de Salida	Alimentación Redundante	Procesador	Memoria RAM
CISCO FIREWALL	**Pix 501** 	1	1	No	433-Mhz Intel Celeron Processor	32 MB de Ram O 64 MB de SDRAM
CISCO FIREWALL	**Pix 506** 	2	2	No	300-Mhz Intel Celeron Processor	32 MB de SDRAM
CISCO FIREWALL	**Pix 515** 	2 Expandible a 6	2	No	433 Mhz Intel Celeron Processor	32 MB o 64 MB de SDRAM
CISCO FIREWALL	**Pix 525** 	2 Expandible a 8	2	No	600-Mhz Intel Pentium III Processor	128 MB o 256 MB de SDRAM
CISCO SWITCH SERIE 3550	**3550-24-FX Switch** 	2 Gigabits	24 Puertos en Fibra	Si	433 Mhz Processor	64 MB de SDRAM
CISCO SWITCH SERIE 3750	**3750g-24ts** 	2	24 puertos Ethernet 10/100/1000 y 4 enlaces SFP ascendentes	Si	1000 Mhz	128 Mb
CISCO SWITCH SERIE 3750	**3750g-24t** 	1	24 puertos Ethernet 10/100/1000	Si	1000 Mhz	128 Mb
CISCO SWITCH	**3750-48ts**	3	48 puertos Ethernet 10/100	Si	1000 Mhz	128 Mb

Fabricante	Referencia	Interfases Fast Ethernet 10/100	Puertos de Salida	Alimentación Redundante	Procesador	Memoria RAM
SERIE 3750			y 4 enlaces SFP			
CISCO SWITCH SERIE 3750	**3750-24ts** 	1	24 puertos Ethernet 10/100 y 2 enlaces ascendentes	Si	1000 Mhz	128 Mb
3COM FIREWALL	**3com Office Connect Vpn Firewall** 	1	1	No	100 Mhz	16 Mb Ram
3COM FIREWALL	**3com Superstack 3 Firewall** 	3	3	Si	233 Mhz	16 Mb Ram
3COM SWITCH	**3com Security Switch 6200** 	2	16 puertos	Si	Pentium III 1.26 Ghz,	512 Mb Ram
3COM SWITCH 4400 24 puertos 3C17203	**Familia 3Com Superstack 3 Switch 4400** 	1	24	Si	800 Mhz	256 Mb Ram
3COM SWITCH 4400 48 puertos 3C17204		1	48	Si	800 Mhz	256 Mb Ram
3COM SWITCH 4400 SE 24 puertos 3C17206		1	24	Si	800 Mhz	256 Mb Ram

Fabricante	Referencia	Interfases Fast Ethernet 10/100	Puertos de Salida	Alimentación Redundante	Procesador	Memoria RAM
3COM SWITCH 4400 FX 24 3C17210		1	24 en Fibra	Si	800 Mhz	256 Mb Ram
SYMANTEC FIREWALL	**Symantec Firewall/Vpn 100** 	1	4	No	Procesador ARM7 a 75 Mhz	16 Mb Ram
SYMANTEC FIREWALL	**Symantec Firewall/Vpn 200** 	2	8	No	Procesador ARM7; A 75 Mhz	16 Mb Ram
SYMANTEC FIREWALL	**Symantec (Axent) Firewall/Vpn 200r** 	6	8	No	Procesador ARM7 a 75 Mhz	16 Mb Ram
SYMANTEC GATEWAY	**Gateway Security 5420** 	8	6	No		512 Mb
SYMANTEC GATEWAY	**Gateway Security 5440** 	8	Si 6 (2 Puertos de F.O mm de Cobre Y 4 Sx)	No		1 Gb

Cuadro 4. Dispositivos de Selección en Base a Requerimientos

[3]La presente tabla nos muestra el costo actual de los dispositivos, los cuales fueron seleccionados estrictamente en base a los requerimientos expuestos por el director del proyecto de sistematización de la industria.

Costo de los Dispositivos (A la Fecha)

Fabricante	Referencia De Dispositivo	Precio (Dólares)	Total
CISCO	PIX 501	$375	
	PIX 506	$849	
	PIX 515	$2319	
	PIX 525	$3997	
CISCO SERIE 3550	C3550-24-FX-SMI	$6495	
CISCO SERIE 3750	3750G-24TS	$5990	
	3750G-24T	$6995	
	3750-48TS	$8990	
	3750-24TS	$3995	
3COM	3COM OFFICECONNECT VPN FIREWALL	$285	
	3COM SUPERSTACK 3 FIREWALL	$3233	
	3COM SECURITY SWITCH 6200	$19550	
3COM SERIE 4400	3COM SWITCH 4400 24 3C17203	$1213	
	3COM SWITCH 4400 48 3C17204	$1400	
	3COM SWITCH 4400 SE 24 3C17206	$1300	
	3COM SWITCH 4400 FX 24 3C17210	$1500	
SYMANTEC	SYMANTEC FIREWALL/VPN 100	$280	
	SYMANTEC FIREWALL/VPN 200	$590	
	SYMANTEC FIREWALL/VPN 200R	$650	
	GATEWAY SECURITY 5420	$2915.28	
	GATEWAY SECURITY 5440	$5134	

Tabla 3. Costo de todos los equipos (A la Fecha)[3]

Dos aspectos de suma importancia en la selección de equipos, es el Desempeño, caracterizado por la administración que se hace internamente de los procesos, por lo tanto es esencial tener como referencia una velocidad razonable del procesador y una memoria temporal de gran capacidad que permita disminuir el numero de refrescos de memoria. A continuación se efectua un analisis tecnico de los fabricantes que concursan en la selección de dispositivos en base a los tres aspectos esencialmente requeridos en la reestructuracion de los dispositivos.

[3] Bajado de Paginas Dinamicas, Ver Bibliografía, Pág 78

2.3.4 Evaluación de Las Principales Características Técnicas

Rendimiento de Equipos Cisco Systems

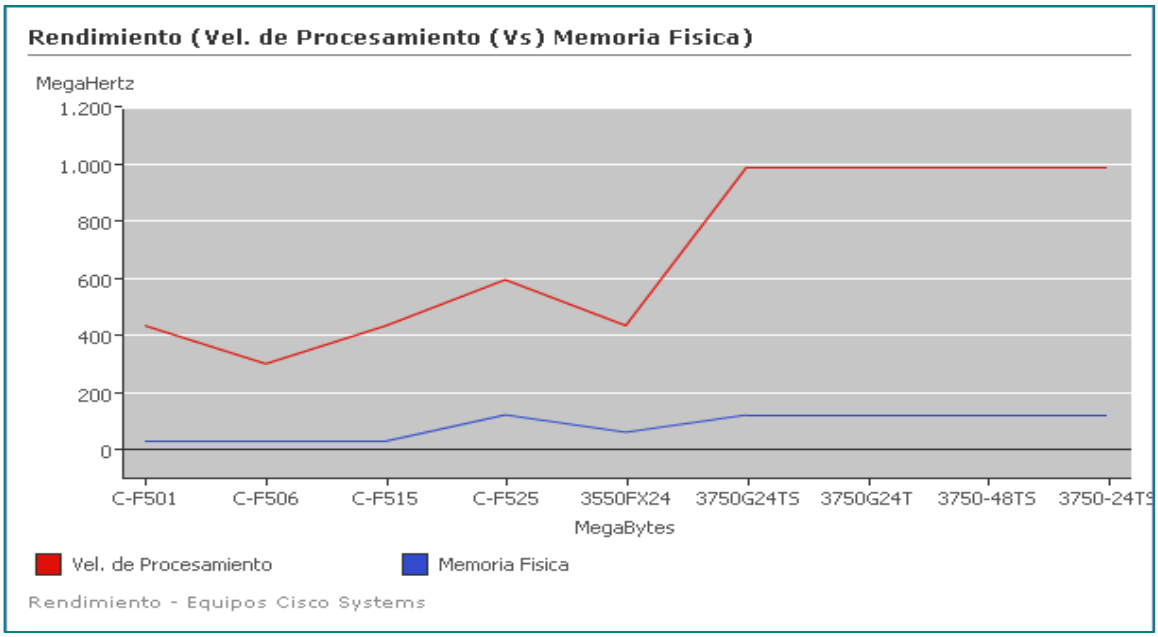


Figura 6. Rendimiento de Equipos Cisco Systems

Escalabilidad en Equipos Cisco Systems

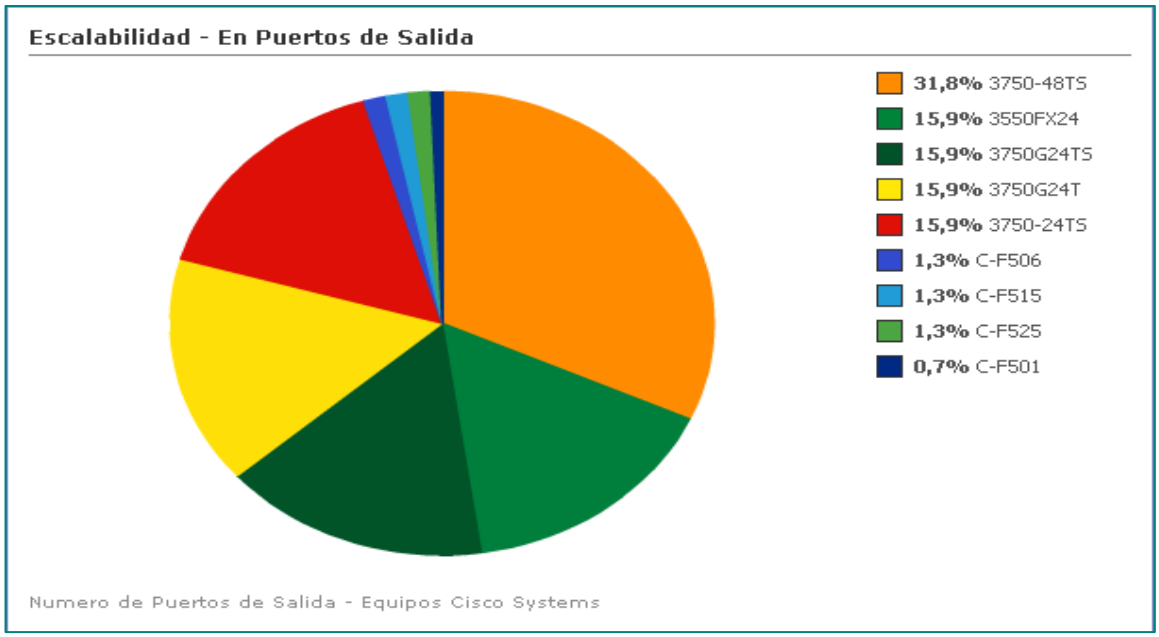


Figura 7. Escalabilidad en Equipos Cisco Systems

Costo de Equipos Cisco Systems

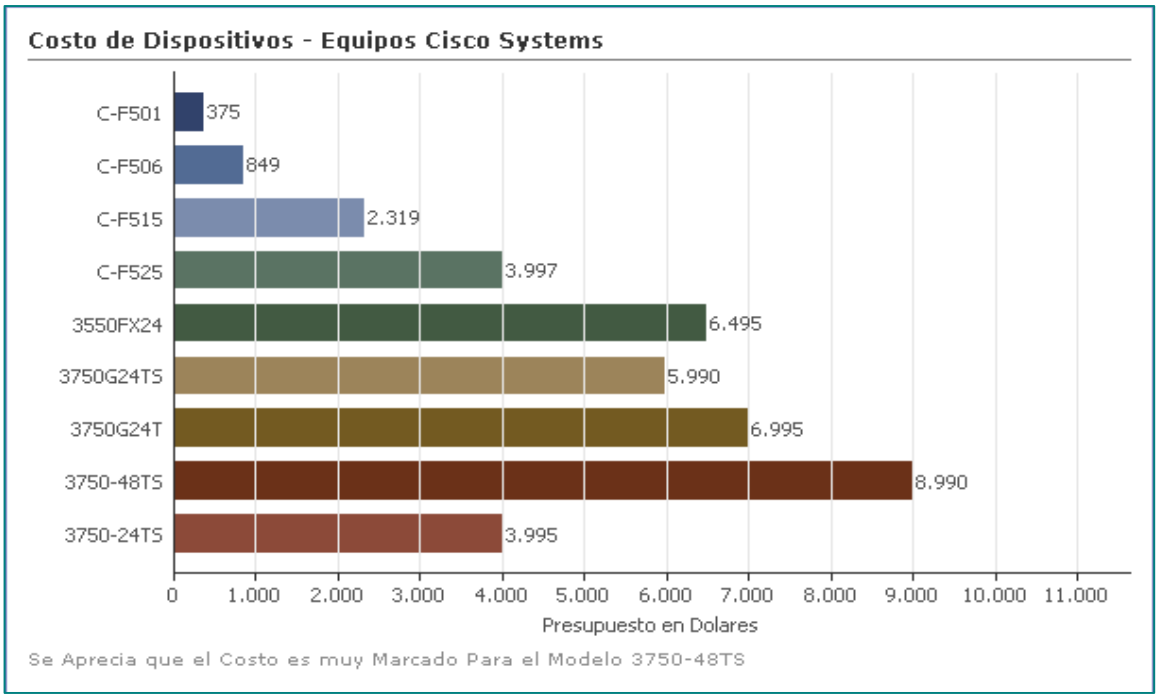


Figura 8. Costo de Equipos Cisco Systems

Rendimiento de Equipos 3com

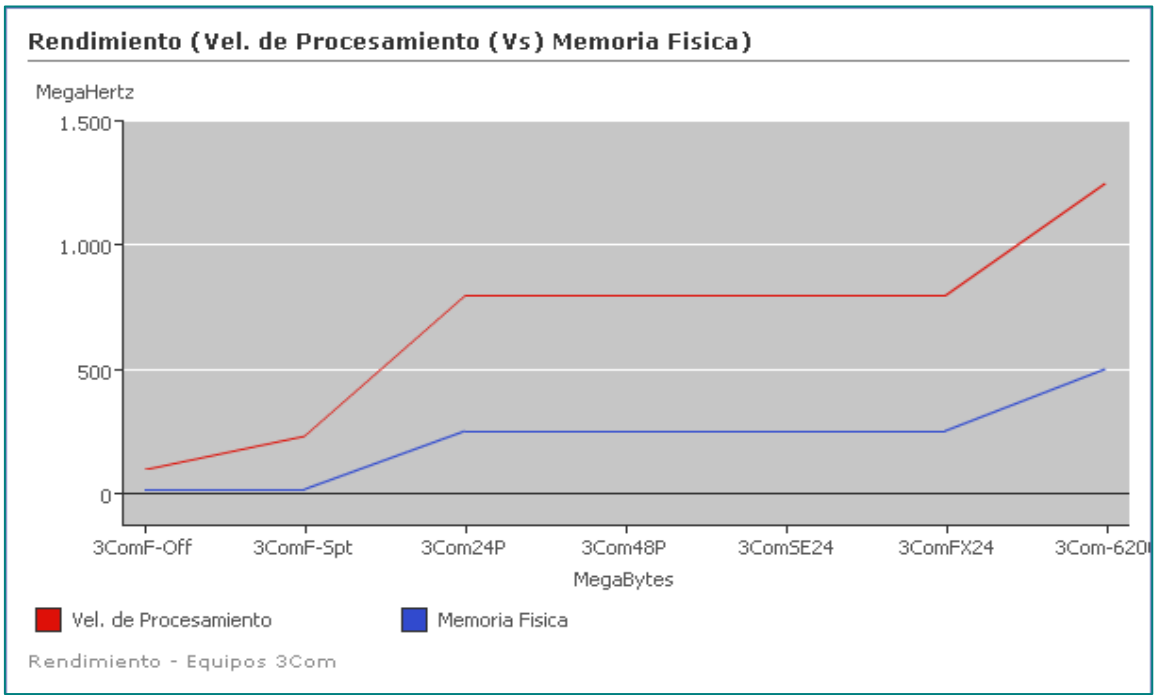


Figura 9. Rendimiento de Equipos 3Com

Escalabilidad en Equipos 3Com

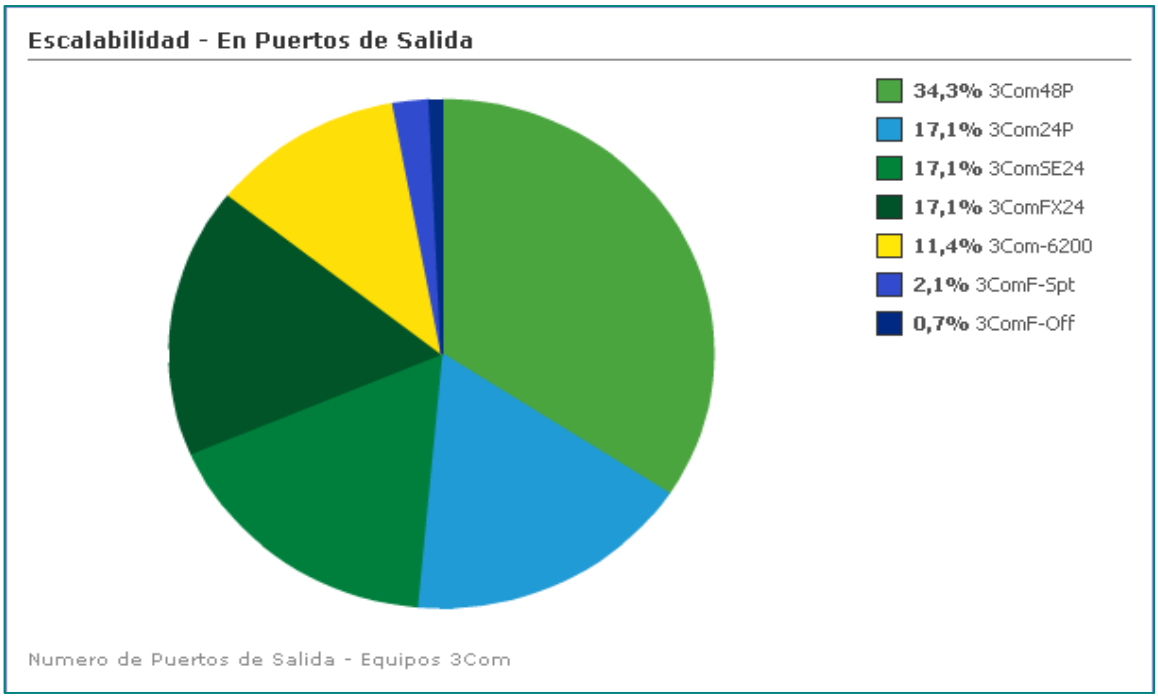


Figura 10. Escalabilidad en Equipos 3Com

Costo de Equipos 3Com

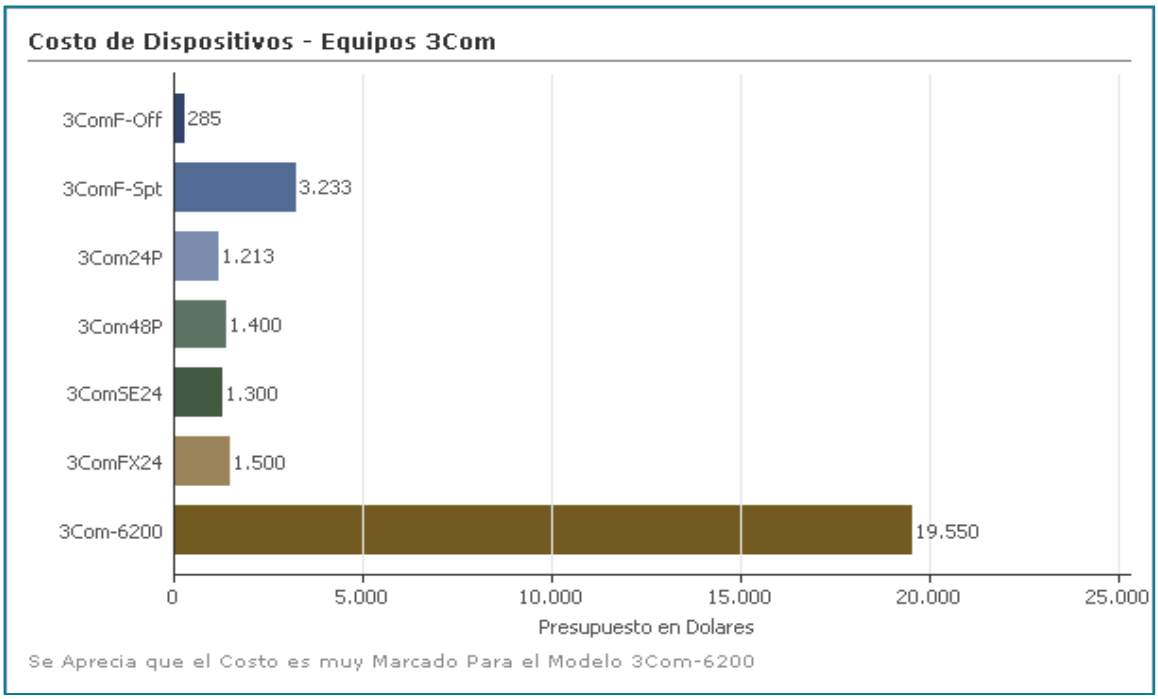


Figura 11. Costo de Equipos 3Com

Rendimiento de Equipos Symantec

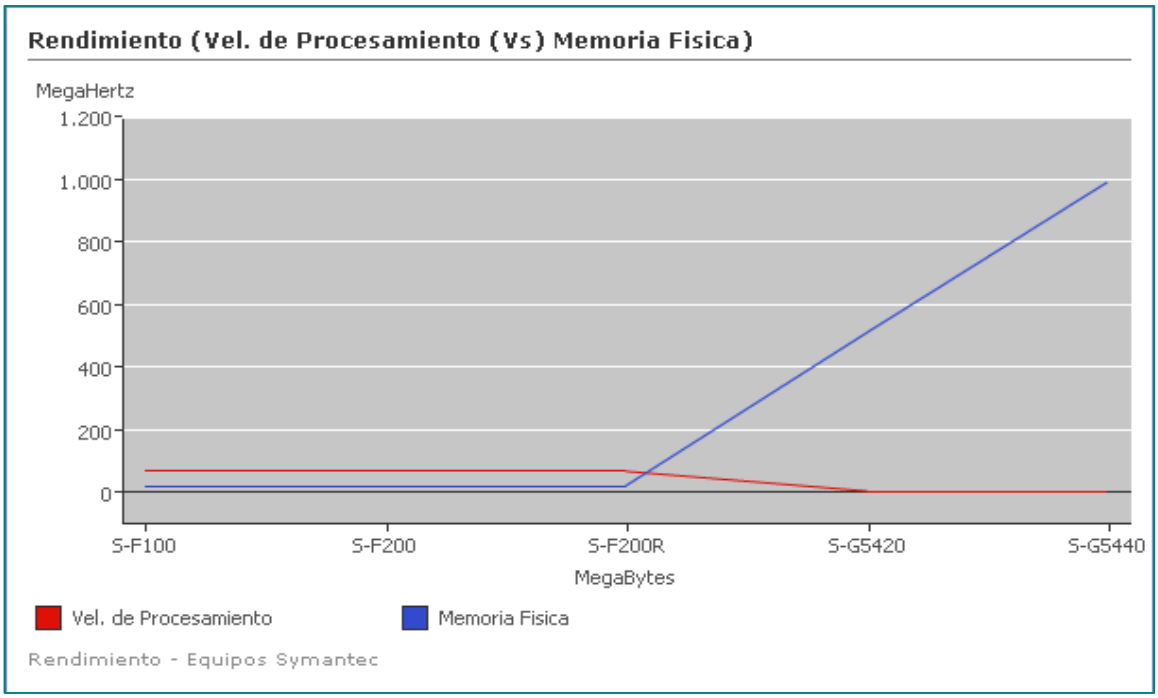


Figura 12. Rendimiento de Equipos Symantec

Escalabilidad en Equipos Symantec

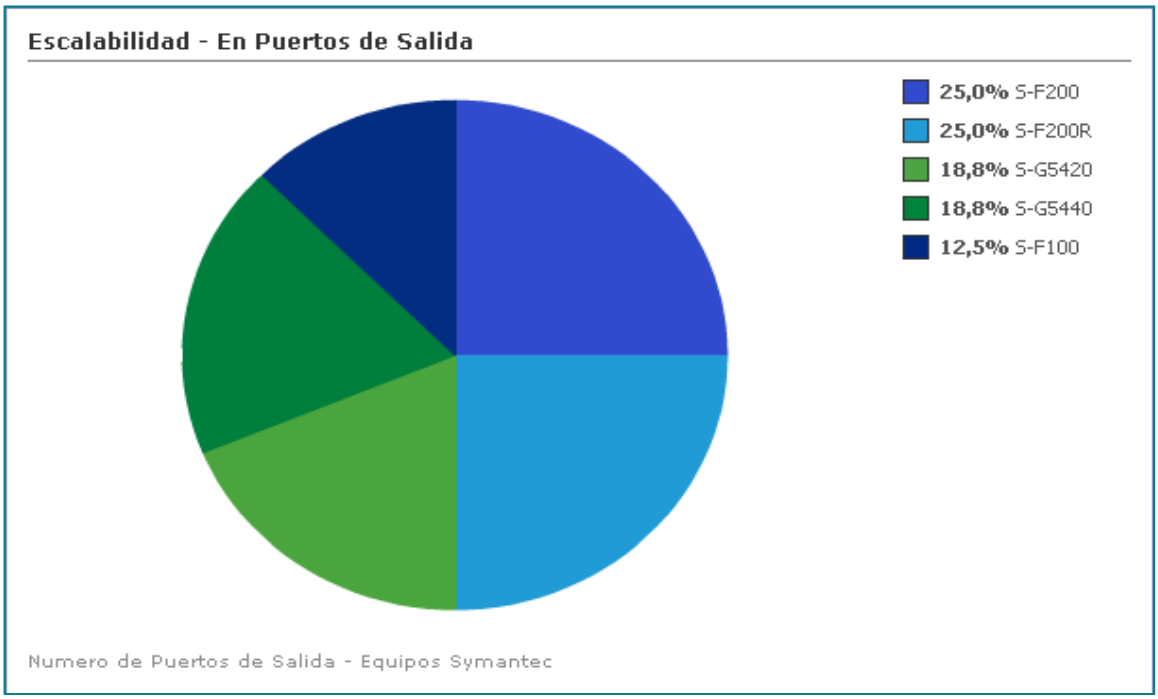


Figura 13. Escalabilidad en Equipos Symantec

Costo de Equipos Symantec

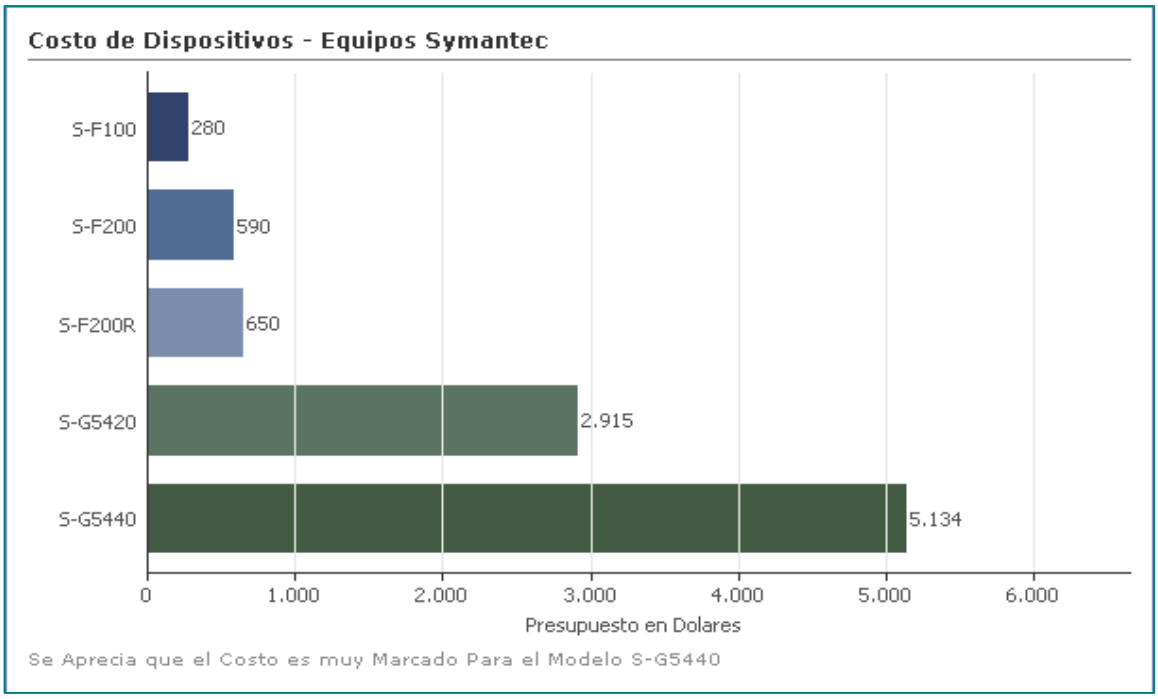


Figura 14. Costo De Equipos Symantec

En teoría informática existe un axioma el cual ratifica la importancia de la velocidad de procesamiento en un dispositivo de red.

Axioma: solamente un proceso y nada más que uno puede ser ejecutado a la vez.

Esto es inherente a la tecnología utilizada para ello y es precisamente este proceso de concurrencia ficticia lo que llamamos Tiempo Compartido.

Otros aspectos de suma importancia al momento de hacer una selección es el número de puertos, sean estos Fast Ethernet o Gigabit Ethernet, la memoria fisica, el buffer de memoria y la memoria cache tambien lo es las alternativas de expansión que me ofrezcan algunos modelos. De esta

manera se evalua el ideal de un 20 % de puertos libres, partiendo de los requerimientos de escalabilidad.

2.4 SELECCIÓN DE EQUIPOS

En la selección se debe tener muy en cuenta la inversión en la cual incurre una organización al momento de llevar a cabo la implementación de una red.

La industria requiere una remodelación de sus dispositivos de red, esto debido a la necesidad obligada de convergencia entre la red corporativa y las áreas operativas, en muchas ocasiones se puede tener muy en cuenta que los costos de invertir en dispositivos de red pueda satisfacer la medida de las necesidades de estar conectado.

Para este caso en particular, no es recomendable ahorrar algún dinero si se trata de proteger la información de la cual se sostiene la correcta operación y ejecución de procesos, como lo es el caso particular de la industria donde debe prevalecer la continuidad de operaciones. Claro esta, que esto no significa realizar gastos que vayan mas alla de lo que realmente amerita una buena reestructuración que a fin de cuentas seria protección a la inversión.

Se debe implementar un sistema de seguridad que garantice la protección de la información, este tipo de inversión, no es recuperable en dinero debido a que hace parte de las estrategias de funcionamiento de cualquier organización, por tanto se gana, desde el momento de vacunar, por decirlo de alguna manera, mis intereses teniendo como punto de partida el tipo de información que fluye por mi red.

Teniendo esto muy en cuenta, las mejores opciones para este caso en particular, se encuentra en los dispositivos Cisco Systems y 3Com por las siguientes razones:

→ Por ser equipos totalmente administrables.

→ Por presentar un mejor desempeño ante los otros equipos evaluados.

→ Por contar con academias de capacitacion en casi que en todo en mundo, permitiendo la formacion del personal que en algun momento este a cargo de los dispositivos de red en cualquiera de las oficinas de la refineria que se encuentran fuera del pais.

→ Por hacer parte de los 3 lideres mundialmente confiables en la actualidad.

→ Por el buen rendimiento y desempeño que presentan de sus equipos.

→ Por permitir apilamiento de la serie escogida, para un desempeño más eficaz y eficiente de sus equipos.

→ Por el respaldo que ofrecen de sus equipos.

→ Y por ultimo, por el soporte tecnico, considerados como los mejores.

2.4.1 Notas de los Fabricantes[4]

Cisco Systems y 3Com se comprometen a minimizar el costo total de propiedad (TCO). Cisco ofrece una cartera de servicios de soporte técnico para ayudar a asegurar que los productos de Cisco funcionan de manera eficaz, permanecen altamente disponibles y aprovechan el software de sistemas más reciente, al igual que 3Com que se caracteriza aun mas por su interfaz amigable. Los servicios y los programas de soporte técnico están disponibles como parte de la solución, servicio y soporte para la conmutación de escritorios y están disponibles directamente desde estos fabricantes o a través de distribuidores autorizados.

Servicio y Soporte Técnico

Características

- Acceso a actualizaciones de software las 24 horas
- Acceso Web a repositorios técnicos
- Soporte técnico telefónico a través del Centro de Asistencia Técnica de Cisco (TAC)
- Sustitución avanzada de piezas de hardware

Ventajas

- Permite una resolución preventiva o acelerada de problemas
- Reducen el TCO al aprovechar la experiencia y los conocimientos de estos fabricantes
- Minimiza el tiempo de inactividad de la red

4

[4] Contenido en las Paginas http://www.cisco.com y http://www.3com.com

2.4.2 Equipos a Utilizar por Selección para Soluciones Cisco Systems

Fabricante	Referencia	Foto	Numero De Parte	Descripción Básica
CISCO FIREWALL	**Cisco PIX 515E Security Appliance**		**Part # PIX-515E-FO-BUN**	2 Interfases Fast Ethernet 10/100, 433 Mhz Intel Celeron Processor, 64 MB de SDRAM y 2 puertos de salida.
CISCO SWITCH SERIE 3750	**Cisco Catalyst 3750G-24T**		**Part # WS-C3750G-24T-E**	1 Interfases Fast Ethernet 10/100/1000,Gigabits 24 puertosde salida, 1000 Mhz de procesador y 128 Mb.
CISCO SWITCH SERIE 3750	**Cisco Catalyst 3750-24TS**		**Part # WS-C3750-24TS-E**	1 Interfases Fast Ethernet 10/100/1000, Alimentación Redundante, 24 puertos de salida Ethernet 10/100/1000 y 2 enlaces ascendentes SI, 1000 Mhz en procesador y 128 Mb de memoria fisica.
CISCO SWITCH SERIE 3550	**Cisco Catalyst 3550-24-FX Switch**		**Part # WS-C3550-24-FX-SMI**	2 Interfases Gigabits Ethernet, Alimentación Redundante, 24 puertos de salida en Fibra, 433 Mhz de Processor y 64 MB de SDRAM

Cuadro 5. Equipos de Selección para Soluciones Cisco Systems

2.4.3 Equipos a Utilizar por Selección para Soluciones 3Com

Fabricante	Referencia	Foto	Numero De Parte	Descripción Básica
3com Switch Security 6200	**3com Security 6200 16-Puertos**		**Part # 3CR13500-73**	2 Interfases Fast Ethernet 10/100, 433 Mhz Processor, 64 MB de SDRAM y 16 puertos de salida.
3com Switch Superstack 3 4400	**3com Superstack 3 4400 24-Pts**		**Part # 3C17203-US**	1 Interfases Fast Ethernet 10/100/1000,Gigabits 24 puertos de salida, 1000 Mhz de procesador y 128 Mb.
3Com Switch Superstack 3 4400 FX	**3Com Superstack 3 4400 FX 24-Pts**		**Part # 3C17210**	2 Interfases Gigabits Ethernet, Alimentación Redundante, 24 puertos de salida en Fibra, 433 Mhz de Processor y 64 MB de SDRAM

Cuadro 6. Equipos de Selección para Soluciones 3Com

2.4.4 Recomendaciones

Siempre que la base tecnologica en la que se fundamentada una empresa sea la escalabilidad, es preferible seguir una linea de productos que sean robustos y ofrescan buen respaldo. Para el caso de la industria, se opta por escoger la serie de productos ***Cisco*** o ***3Com,*** según sea de la preferencia de la industria por sus grandes bondades al momento de optar por la escalabilidad en una red.

Actualmente esta muy de moda en los dispositivos de red el llamado "apilamiento" de dispositivos, que si bien es una buena estrategia comercial para ofrecer un producto y casi obligar al cliente a escalar con una serie especifica del mismo producto, las bondades que se dan mediante el apilamiento son innumerables, entre ellas:

→ Dispositivos con similar arquitectura interna de buses dan seguridad respecto a la estabilidad de las operaciones que el dispositivo lleve a cabo.

→ La tecnología StackWise, se preocupa cada vez mas por hacer cables que permitan a las redes converger aun mas en el tipo de paquetes que fluyen de dispositivo a dispositivo.

→ Otra ventaja importante es que una pila en funcionamiento puede aceptar nuevos miembros o eliminar miembros antiguos sin interrumpir el servicio.

→ Al agregar o quitar switches, el switch principal actualiza automáticamente todas las tablas de enrutamiento para reflejar los cambios. Las actualizaciones se aplican simultáneamente en el nivel global a todos los miembros de la pila.

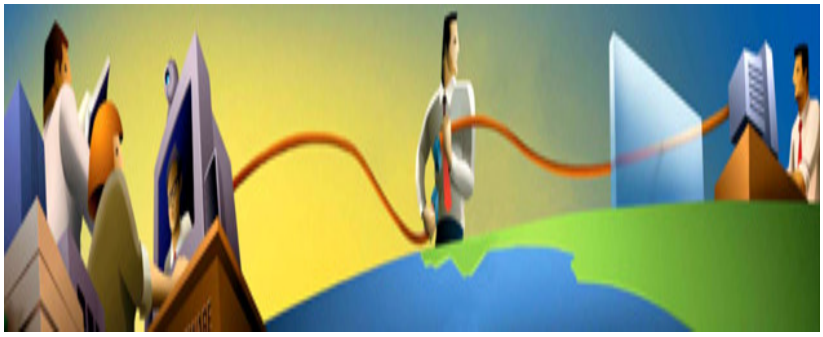
CAPÍTULO 3

DISEÑO DE LA MEJOR ALTERNATIVA

3.1 CONFIGURACIÓN DE SEGURIDAD EN FIREWALLS

3.2 ARQUITECTURA E IMPLEMENTACIÓN MEDIANTE SOLUCIONES CISCO SYSTEMS

3.3 ARQUITECTURA E IMPLEMENTACIÓN MEDIANTE SOLUCIONES 3COM



3.1 CONFIGURACIÓN DE SEGURIDAD EN FIREWALLS[5]

3.1.1 Configuración del Firewall PIX de Cisco

Pasos para acceder al modo de configuración

Paso 1 se inicia el programa de emulación

Paso 2 encender el firewall

Paso 3 después que se cargue la flash, presionar la barra espaciadora

Paso 4 después de cargar, aparece este mensaje en modo no privilegiado:

pixfirewall>

se escribe **enable** y luego **Enter**

Paso 5 aparece lo siguiente:

Password:

Luego de introducir el password presione **Enter**

Paso 6 ahora se encuentra en modo privilegiado, debe aparece:

pixfirewall#

Para definir la ruta predefinida para los routers de la Red:

Paso 1 se hace telnet al router que se quiere conectar o por hyperterminal

Paso 2 se accede al IOS del equipo[5]

[5] Ver Anexo E "Para Tener en Cuenta en la Implementacion de Seguridad"

Paso 3 se coloca la ruta predefinida a la interfaz del firewall con la siguiente orden:

ip route 0.0.0.0 0.0.0.0 *pix_inside_interface_ip_address*

Paso 4 con el comando **show ip route** se verifica la conexión al PIX Firewall quedando la interfaz habilitada

Paso 5 se borra la cache de ARP con **clear arp** luego se introduce **Cntrl-Z** para salir del modo de configuración

Paso 6 desde el router, si se cambia el router por defecto, se usa **write memory** para guardar la configuración en la memoria flash.

Paso 7 se conectan los otros routers y cada perímetro de interfaz del PIX Firewall y se repiten los pasos del 1 al 6.

Paso 8 si hay subredes en los routers conectados al PIX Firewall's, se deben configurar con el router que esta conectado al PIX Firewall y luego se borra la arp de la memoria cache.

Para asignar ip y mascara de subred

El formato de los comandos **ip address** es el siguiente:

ip address inside *ip_address netmask*
ip address outside *ip_address netmask*

Ejemplo:

ip address inside 192.168.1.1 255.255.255.0

Para intercambiar interfaces y niveles de seguridad:

nameif ethernet0 outside security0

nameif ethernet1 inside security100

nameif ethernet2 intf2 security10

El formato del comando **nameif** es el siguiente:

nameif *hardware_id interface security_level*

Configuración del firewall para ruteo estático:

route inside 192.168.5.0 255.255.255.0 192.168.0.2 1

route inside 192.168.6.0 255.255.255.0 192.168.0.2 1

Y ruteo estatico para con interface dmz[6]:

route dmz4 192.168.7.0 255.255.255.0 192.168.4.2 1

route dmz4 192.168.8.0 255.255.255.0 192.168.4.2 1

Usando direcciones globales hacia fuera:

global (outside) 1 209.165.201.5 netmask 255.255.255.224

global (outside) 1 209.165.201.10-209.165.201.20 netmask 255.255.255.224

Zonas con el DMZ

global (dmz1) 1 192.168.1.10-192.168.1.100 netmask 255.255.255.0

global (dmz2) 1 192.168.2.10-192.168.2.100 netmask 255.255.255.0[6]

[6] Sacado del Texto "Seguridad En Unix Y Redes Versión 2.1", Cap 4, Num 15.4.4, Pag 261.

Para remover las listas de acceso ICMP

no access-list acl_in permit icmp any any

no access-list acl_out permit icmp any any

no access-list acl_dmz1 permit icmp any any

Para permitir ICMP se utilice el comando access-list de la siguiente manera:

access-list acl_out permit icmp any any

Para 2 interfaces aplicando NAT Y PAT[7]

Paso 1 se identifican las direcciones ip para cada interfaz

ip address outside 209.165.201.3 255.255.255.224

ip address inside 192.168.3.0 255.255.255.0

Paso 2 se habilitan los comandos nat and pat en el siguiente orden

nat (inside) 1 0 0

Paso 3 se crean direcciones globales que serán traducidas al pasar por el PIX Firewall de la red protegida a la red desprotegida:

global (outside) 1 209.165.201.10-209.165.201.30

global (outside) 1 209.165.201.8

Ejemplo para 2 interfases con NAT:

`nameif ethernet0 outside security0`[7]

[7] Sacado del Texto "Seguridad En Unix Y Redes Versión 2.1", Cap 4, Num 16.4.4, Pag 284.

```
nameif ethernet1 inside security100
interface ethernet0 10baset
interface ethernet1 10baset
ip address outside 209.165.201.3 255.255.255.224
ip address inside  192.168.3.0 255.255.255.0
hostname pixfirewall
arp timeout 14400
no failover
names
pager lines 24
logging buffered debugging
nat (inside) 1 0 0
global (outside) 1 209.165.201.10-209.165.201.30
global (outside) 1 209.165.201.8
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
access-list ping_acl permit icmp any any
access-group ping_acl in interface inside
access-group ping_acl in interface dmz
access-list acl_out permit icmp any any
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00

udp 0:02:00 rpc 0:10:00 h323 0:05:00

sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server community public
mtu outside 1500
mtu inside 1500
```

3.2 ARQUITECTURA E IMPLEMENTACIÓN MEDIANTE SOLUCIONES CISCO SYSTEMS

3.2.1 Configuración Lógica entre la Red de Planta y el Sistema de Control

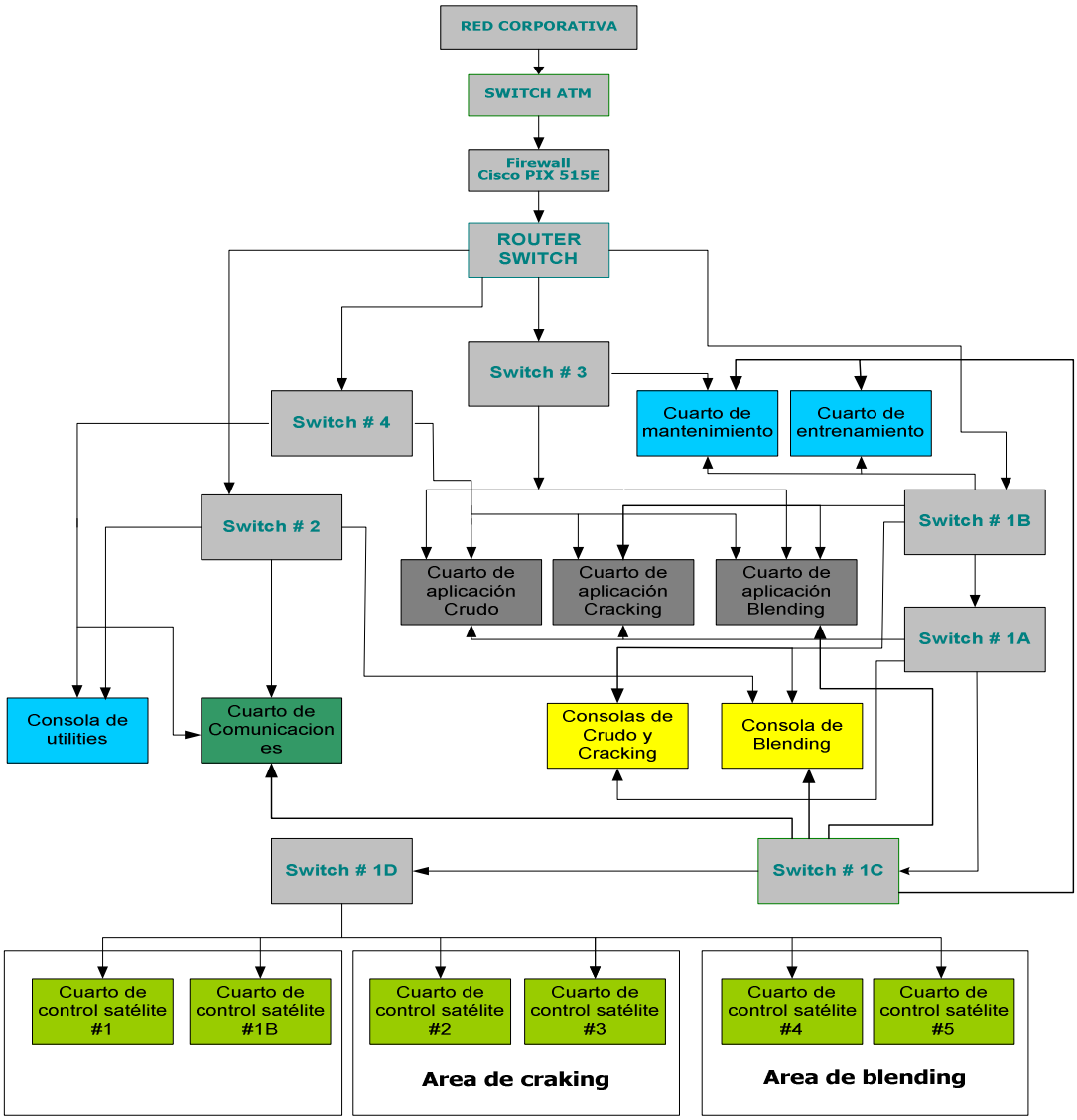


Figura 15. Configuración Lógica entre la Red de Planta y el Sistema de Control

3.2.2 Área Reestructurada (Cuarto de Comunicaciones)

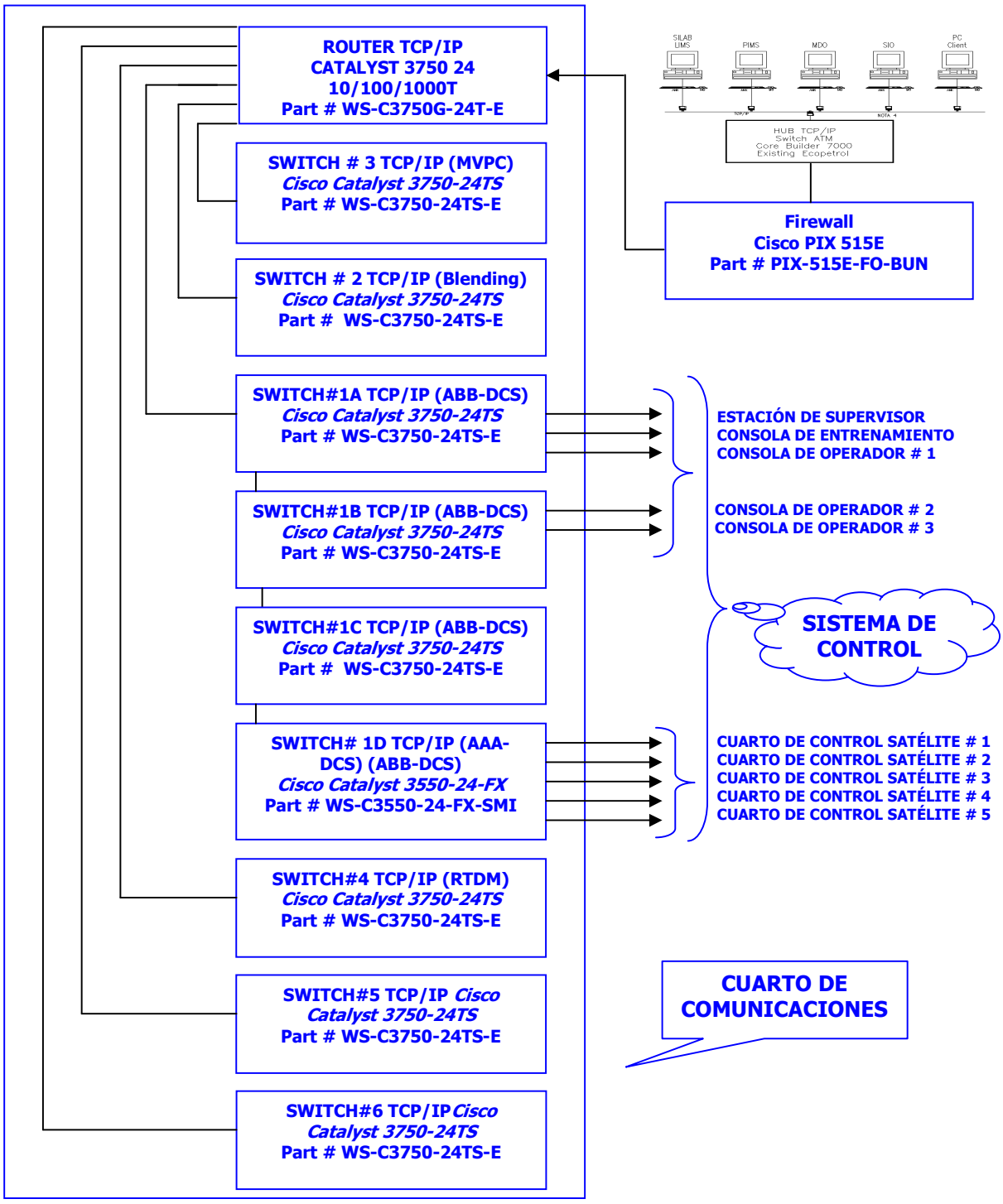


Figura 16. Área Reestructurada (Soluciones Cisco Systems)

3.2.3 Configuración por Nodos de Nuevos Equipos Conectados al Patch Panel

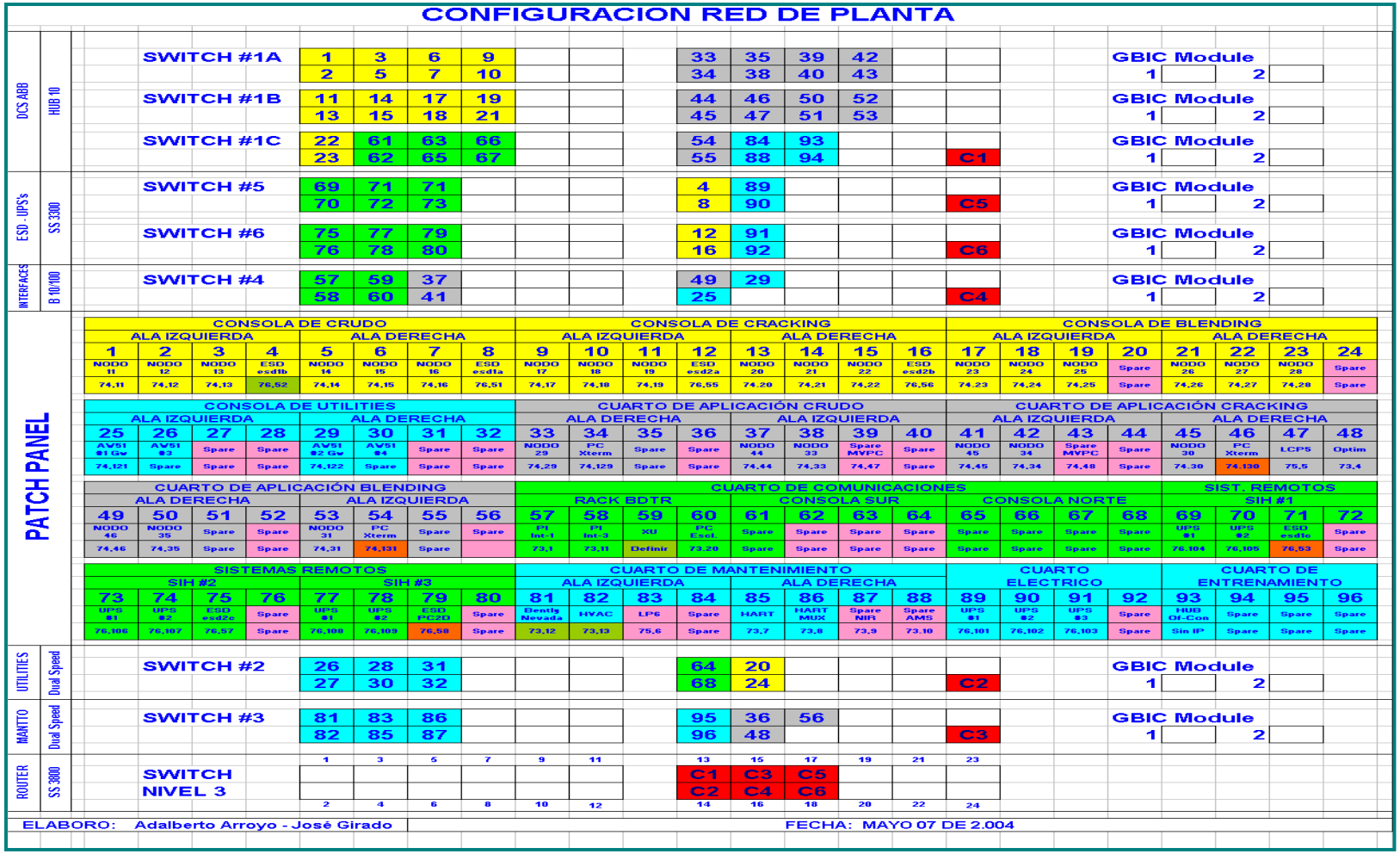


Figura 17. Configuración por Nodos de Equipos Conectados al Patch Panel (Cisco Systems)

3.2.4 Esquema de Direccionamiento (Localización y Configuración de Equipos)

Conexión Red De Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
N/A	Estación De Control Avanzado De Blending	Pc	Eabc	150.67.73.6	Ccb-Consola3
Switch#4	Estación De Control Avanzado	Pc	Eabc10	150.67.73.11	Ccb-Comunic-1
Switch#1a	Estación De Operación #1 Consola De Crudo	Os520	Eas110	150.67.74.11	Ccb-Consola1
Switch#1a	Estación De Operación #2 Consola De Crudo	Os520	Eas120	150.67.74.12	Ccb-Consola1
Switch#1a	Estación De Operación #3 Consola De Crudo	Os520	Eas130	150.67.74.13	Ccb-Consola1
Switch#1a	Estación De Operación #4 Consola De Crudo	Os520	Eas140	150.67.74.14	Ccb-Consola1
Switch#1a	Estación De Operación #5 Consola De Crudo	Os520	Eas150	150.67.74.15	Ccb-Consola1
Switch#1a	Estación De Operación #6 Consola De Crudo	Os520	Eas160	150.67.74.16	Ccb-Consola1
Switch#1a	Estación De Operación #1 Consola De Cracking	Os520	Eas170	150.67.74.17	Ccb-Consola2
Switch#1a	Estación De Operación #2 Consola De Cracking	Os520	Eas180	150.67.74.18	Ccb-Consola2
Switch#1b	Estación De Operación #3 Consola De Cracking	Os520	Eas190	150.67.74.19	Ccb-Consola2
Switch#1b	Estación De Operación #4 Consola De Cracking	Os520	Eas200	150.67.74.20	Ccb-Consola2
Switch#1b	Estación De Operación #5 Consola De Cracking	Os520	Eas210	150.67.74.21	Ccb-Consola2
Switch#1b	Estación De Operación #6 Consola De Cracking	Os520	Eas220	150.67.74.22	Ccb-Consola2
Switch#1b	Estación De Operación #1 Consola De Blending	Os520	Eas230	150.67.74.23	Ccb-Consola3
Switch#1b	Estación De Operación #2 Consola De Blending	Os520	Eas240	150.67.74.24	Ccb-Consola3
Switch#1b	Estación De Operación #3 Consola De Blending	Os520	Eas250	150.67.74.25	Ccb-Consola3
Switch#1b	Estación De Operación #4 Consola De Blending	Os520	Eas260	150.67.74.26	Ccb-Consola3
Switch#1c	Estación De Operación #5 Consola De Blending	Os520	Eas270	150.67.74.27	Ccb-Consola3
Switch#1c	Estación De Operación #6 Consola De Blending	Os520	Eas280	150.67.74.28	Ccb-Consola3
Switch#1a	Estación De Ingeniería Sistema De Crudo	Os520	Eas290	150.67.74.29	Ccb-Aplicacion1
Switch#1b	Estación De Ingeniería Sistema De Cracking	Os520	Eas300	150.67.74.30	Ccb-Aplicacion2
Switch#1b	Estación De Ingeniería Sistema De Blending	Os520	Eas310	150.67.74.31	Ccb-Aplicacion3
Switch#1d	Estación De Operación Local Sistema De Crudo	Os520	Eas380	150.67.74.38	Sih#1-Consola
Switch#1d	Estación De Operación Local Sistema De Tratamiento	Os520	Eas390	150.67.74.39	Sih#1-Consola
Switch#1d	Estación De Operación Local Sistema De Cracking	Os520	Eas400	150.67.74.40	Lcb#2-Consola
Switch#1d	Estación De Operación Local	Os520	Eas410	150.67.74.41	Lcb#3-Consola

Conexión Red De Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
	Sistema De Azufre				
Switch#1d	Estación De Operación Local Sistema De Blending Refinería	Os520	Eas420	150.67.74.42	Lcb#4-Consola
Switch#1d	Estación De Operación Local Sistema De Blending Tnp	Os520	Eas430	150.67.74.43	Lcb#5-Consola
N/A	Estación De Operación #1 Sistema De Entrenamiento	Os520	Eas610	150.67.74.61	Ccb-Entrenamiento
N/A	Estación De Operación #2 Sistema De Entrenamiento	Os520	Eas620	150.67.74.62	Ccb-Entrenamiento
N/A	Estación De Operación #5 Sistema De Entrenamiento	Os520	Eas640	150.67.74.64	Ccb-Entrenamiento
N/A	Estación De Operación #4 Sistema De Entrenamiento	Os520	Eas650	150.67.74.65	Ccb-Entrenamiento
N/A	Estación De Operación #3 Sistema De Entrenamiento	Os520	Eas660	150.67.74.66	Ccb-Entrenamiento
Switch#4	Estación De Operación Y Gateway #1 Foxboro	Aw51	Eaw030	150.67.74.121	Ccb-Consola4
Switch#4	Estación De Operación Y Gateway #1 Foxboro	Aw51	Eaw040	150.67.74.122	Ccb-Consola4
Switch#4	Estación De Base De Datos En Tiempo Real	Unix	Ebdtr	150.67.73.1	Ccb-Comunic-Pi
Switch #3	Estación Bently Nevada	Pc	Ebn	150.67.73.13	Ccb-Mantenimiento
Switch #1c	Estación De Analizadores Vistanet	Pc	Ecac	150.67.73.10	Ccb-Mantenimiento
N/A	Estación De Ingeniería Sistema Abb	Pc	Ees00	150.67.74.10	Ccb-Comunic-1
Switch #5	Estación #1 Sistema De Shutdown De Crudo	Pc	Eesd10a	150.67.76.51	Ccb-Consola1
Switch #5	Estación #2 Sistema De Shutdown De Crudo	Pc	Eesd10b	150.67.76.52	Ccb-Consola1
Switch #5	Estación Local Sistema De Shutdown De Crudo	Pc	Eesd10c	150.67.76.53	Sih#1-Consola
Switch #6	Estación #1 Sistema De Shutdown De Cracking	Pc	Eesd20a	150.67.76.55	Ccb-Consola2
Switch #6	Estación #2 Sistema De Shutdown De Cracking	Pc	Eesd20b	150.67.76.56	Ccb-Consola2
Switch #6	Estación Local Sistema De Shutdown De Cracking	Pc	Eesd20c	150.67.76.57	Lcb#2-Consola
Switch #6	Estación Local Sistema De Shutdown De Azufre	Pc	Eesd20d	150.67.76.58	Lcb#3-Consola
Switch#3	Multiplexer Ams Smart Transmitter Interface	Mx	Ihmux	150.67.73.8	Ccb-Mantenimiento
Switch#3	Estación Ams Smart Transmitter Interface - Hart	Pc	Ehpc	150.67.73.7	Ccb-Mantenimiento
	Router Super Stack 3800	Ethernet	Ehub	150.67.76.1	Ccb-Comunic-Rack
	Hub 24 Puertos Utp Red De Planta Abb	Ethernet	Ehub10	150.67.76.2	Ccb-Comunic-Rack
	Hub 24 Puertos Utp Red De Planta Abb	Ethernet	Ehub10	150.67.76.2	Ccb-Comunic-Rack
	Hub 6 Puertos Fibra Óptica Red De Planta Abb	Ethernet	Ehub10	150.67.76.2	Ccb-Comunic-Rack
	Hub 6 Puertos Fibra Óptica Red De Planta Abb	Ethernet	Ehub10	150.67.76.2	Ccb-Comunic-Rack
	Hub 24 Puertos Utp Blending	Ethernet	Ehub20	150.67.76.3	Ccb-Comunic-Rack

Conexión Red De Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
	Hub 24 Puertos Utp Control Avanzado	Ethernet	Ehub30	150.67.76.4	Ccb-Comunic-Rack
	Swith 12 Puertos Utp Base De Datos En Tiempo Real	Ethernet	Ehub40	150.67.76.5	Ccb-Comunic-Rack
	Swith 24 Puertos Utp Esd Y Ups	Ethernet	Ehub50	150.67.76.6	Ccb-Comunic-Rack
Switch#3	Pc Portatil Hvac	Portatil	Ehvac	150.67.73.12	Ccb-Mantenimiento
Switch #1a	Estación De Historia Sistema De Crudo	Ims530	Eims330	150.67.74.33	Ccb-Aplicacion1
Switch #1a	Estación De Historia Sistema De Cracking	Ims530	Eims340	150.67.74.34	Ccb-Aplicacion2
Switch#1b	Estación De Historia Sistema De Blending	Ims530	Eims350	150.67.74.35	Ccb-Aplicacion3
Switch #4	Estación Gateway Pi Sistema De Crudo	Ims530	Eims440	150.67.74.44	Ccb-Aplicacion1
Switch #4	Estación Gateway Pi Sistema De Cracking	Ims530	Eims450	150.67.74.45	Ccb-Aplicacion2
Switch #4	Estación Gateway Pi Sistema De Blending	Ims530	Eims460	150.67.74.46	Ccb-Aplicacion3
Switch #1a	Estacion Gateway Pi-Abb	Ims530	Eims470	150.67.74.47	Ccb-Comunic-1
N/A	Estación De Historia Sistema De Entrenamiento	Ims530	Eims630	150.67.74.63	Ccb-Entrenamiento
	Impresora Laser A Color Sistema De Entrenamiento	Lcp	Ilcp10	150.67.75.1	Ccb-Entrenamiento
	Impresora Laser A Color Operadores De Consola	Lcp	Ilcp20	150.67.75.2	Ccb-Consola4
	Impresora Laser A Color Administrador Del Sistema	Lcp	Ilcp30	150.67.75.3	Ccb-Sistema
	Impresora Laser A Color Cuarto De Mantenimiento	Lcp	Ilcp40	150.67.75.4	Ccb-Mantenimiento
Switch #1b	Impresora Laser A Color Sistema De Ingeniería	Lcp	Ilcp50	150.67.75.5	Ccb-Aplicacion2
Switch #3	Impresora Laser Blanco Y Negro Administrador Pi	Lp	Ilip60	150.67.75.6	Ccb-Comunic-1
	Hub Mb300 Para Sistema De Crudo	Mb300			Ccb-Comunic-Rack
	Hub Mb300 Para Sistema De Cracking	Mb300			Ccb-Comunic-Rack
	Hub Mb300 Para Sistema De Blending	Mb300			Ccb-Comunic-Rack
	Star Coupler Mb300 Para Sistema De Crudo	Mb300			Sih#1-Dcs
	Star Coupler Mb300 Para Sistema De Tratamiento	Mb300			Sih#1b-Dcs
	Star Coupler Mb300 Para Sistema De Cracking	Mb300			Sih#2-Dcs
	Star Coupler Mb300 Para Sistema De Azufre	Mb300			Sih#3-Dcs
	Star Coupler Mb300 Para Sistema De Blending Refinería	Mb300			Sih#4-Dcs
	Star Coupler Mb300 Para Sistema De Blending Tnp	Mb300			Sih#5-Dcs
	Switche Mb300 Multilan Para Red 11	Mb300			Ccb-Comunic-Rack

Conexión Red De Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
	Switche Mb300 Multilan Para Red 12	Mb300			Ccb-Comunic-Rack
	Impresora Matriz De Punto Consola De Crudo 1	Mp			Ccb-Comunic-1
	Impresora Matriz De Punto Consola De Crudo 2	Mp			Ccb-Consola1
	Impresora Matriz De Punto Consola De Cracking 1	Mp			Ccb-Consola2
	Impresora Matriz De Punto Consola De Cracking 2	Mp			Ccb-Consola2
	Impresora Matriz De Punto Consola De Blending 1	Mp			Ccb-Consola3
	Impresora Matriz De Punto Consola De Blending 1	Mp			Ccb-Consola3
	Impresora Matriz De Punto A Color Bently Nevada	Mp			Ccb-Mantenimiento
	Impresora Matriz De Punto Sistema Esd De Crudo	Mp			Ccb-Consola1
	Impresora Matriz De Punto Sistema Esd De Cracking	Mp			Ccb-Consola2
Switch #3	Estación Nir	Pc	Enir	150.67.73.9	Ccb-Mantenimiento
Switch #3	Estación Del Optimizador De Cracking	Pc	Eopti	150.67.73.4	Ccb-Aplicacion2
	Estación De Reconciliacion De Datos	Pc	Ereda	150.67.73.3	Ccb-Sistema
N.A.	Estación De Operación #1 Siemens	Ot	Esie010	150.67.74.123	Ccb-Consola4
N.A.	Estación De Operación #2 Siemens	Ot	Esie020	150.67.74.124	Ccb-Consola4
N.A.	Estación De Operación #3 Siemens	Ot	Esie030	150.67.74.125	Ccb-Consola4
N.A.	Estación De Operación #4 Siemens	Ot	Esie040	150.67.74.126	Ccb-Consola4
N.A.	Estación Gateway Siemens	Xu	Esie050	150.67.74.127	Ccb-Comunic-Pi
N.A.	Estación Pc Esclavo Siemens	Pc	Esie060	150.67.74.128	Ccb-Comunic-Pi
N.A.	Estación De Star Blend	Pc	Estarb	150.67.73.5	Ccb-Consola3
N.A.	Estacion De Short Term Schedulling	Pc	Ests	150.67.73.2	Ccb-Sistema
Switch #5	Ups No.1 Ccb	Ups		150.67.76.101	Ccb-Ups
Switch #5	Ups No.2 Ccb	Ups		150.67.76.102	Ccb-Ups
Switch #6	Ups No.3 Ccb	Ups		150.67.76.103	Ccb-Ups
Switch #5	Ups No.1 Sih#1	Ups		150.67.76.104	Sih#1
Switch #5	Ups No.2 Sih#1	Ups		150.67.76.105	Sih#1
Switch #5	Ups No.1 Sih#2	Ups		150.67.76.106	Sih#2
Switch #5	Ups No.2 Sih#2	Ups		150.67.76.107	Sih#2
Switch #6	Ups No.1 Sih#3	Ups		150.67.76.108	Sih#3
Switch #6	Ups No.2 Sih#3	Ups		150.67.76.109	Sih#3
Switch#1b	Estación De Ingeniería Xterminal Sistema De Crudo	Pc	Exterm10	150.67.74.130	Ccb-Aplicacion1
Switch#1c	Estación De Ingeniería Xterminal Sistema De Cracking	Pc	Exterm20	150.67.74.131	Ccb-Aplicacion2
N/A	Estación De Ingeniería Xterminal Sistema De Blending	Pc	Exterm30	150.67.74.132	Ccb-Aplicacion3

Tabla 4. Nuevo Esquema de Direccionamiento (Cisco Systems)

3.2.5 Layout del Gabinete CCB-DCS-C04 (Cisco Systems)

Plano U y H del Gabinete CCB-DCS-C04 (Vista Frontal, con la puerta abierta), Plano C (Vista lateral derecha) y Plano A (Vista lateral izquierda). La U es la unidad utilizada para mediciones del gabinete la cual indica 2 pulgadas.

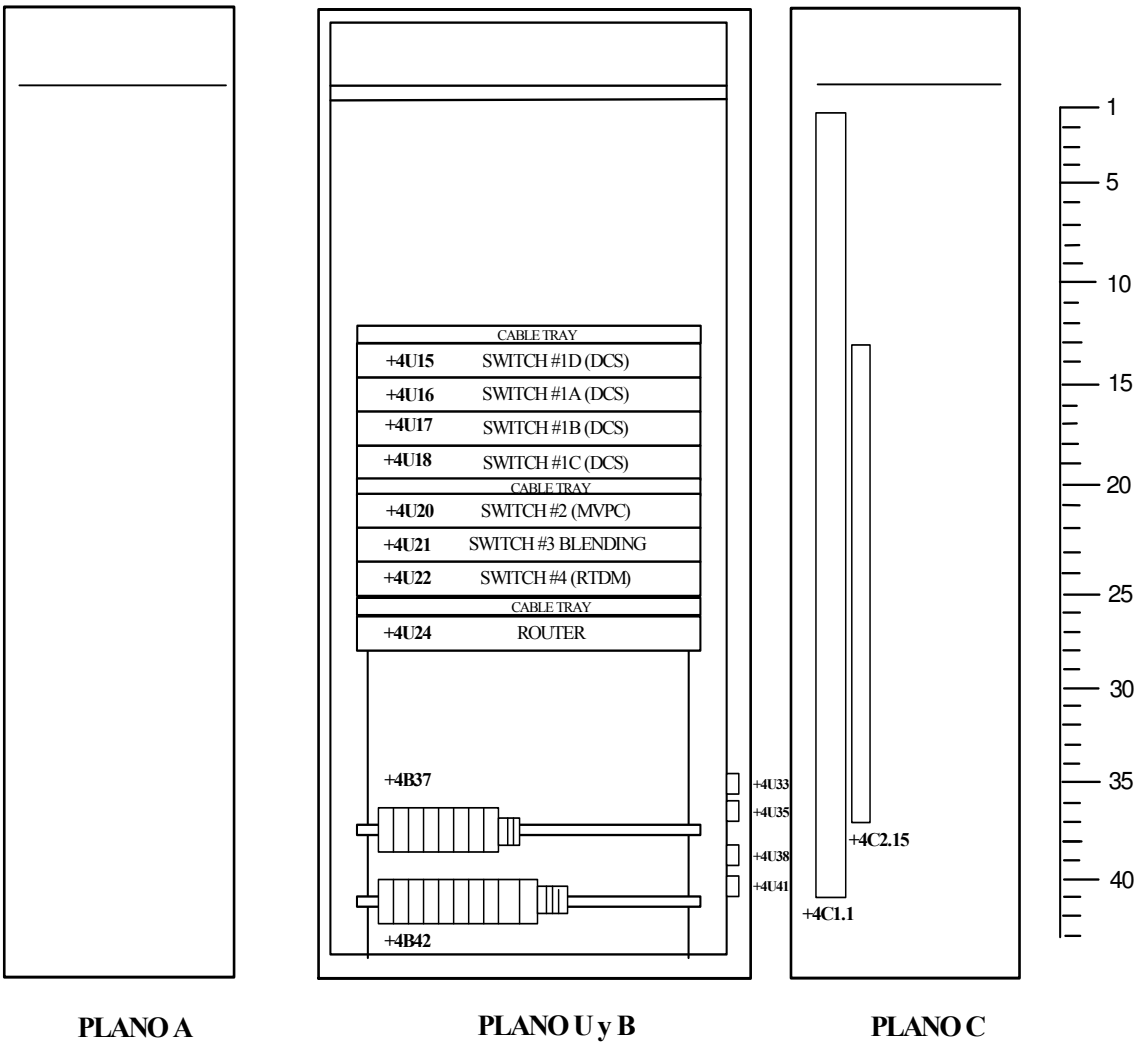


Figura 18. Layout Del Gabinete CCB-DCS-C04 (Cisco Systems)

3.2.6 Layout de los Dispositivos de Red

Componentes del Plano U y B para el Gabinete CCB-DCS-C04.

Artículo	Loc.	Descripción	Comentarios
Switch#1D	+4U15	Switch 24 100BASE-FX Puertos de fibra multimodo	Marca: Cisco Catalyst
Switch#1A	+4U16	Switch 24 puertos 10/100, 2 puertos GBIC	Marca: Cisco Catalyst
Switch#1B	+4U17	Switch 24 puertos 10/100, 2 puertos GBIC	Marca: Cisco Catalyst
Switch#1C	+4U18	Switch 24 puertos 10/100, 2 puertos GBIC	Marca: Cisco Catalyst
	+4U29	Cable Tray	Color Negro
Switch#2	+4U20	Switch 24 puertos 10/100, 2 puertos GBIC	Marca: Cisco Catalyst
Switch#3	+4U21	Switch 24 puertos 10/100, 2 puertos GBIC	Marca: Cisco Catalyst
Switch#4	+4U22	Switch 24 puertos 10/100, 2 puertos GBIC	Marca: Cisco Catalyst
	+4U23	Cable Tray	Color Negro
Router	+4U24	Switch 24 puertos 10/100/1000, 4 SFP uplinks	Marca: Cisco Catalyst
E272 100a	+4U37	Breaker de Alimentación Principal	Marca: ABB
S272k2a	+4U37	Switch de Energía y Distribución 2A (5)	Marca: ABB
S272k10a	+4U37	Switch de Energía y Distribución 10A	Marca: ABB
Zpe 2.5	+4U37	Borneras (3) Modelo: 160864	Marca: Weidmüller
E272 100a	+4U42	Breaker de Alimentación Principal	Marca: ABB
S272k2a	+4U42	Switch de Energía y Distribución 2A (4)	Marca: ABB
Zpe 2.5	+4U42	Borneras (3) Modelo: 160864	Marca: Weidmüller
S272k3a	+4U42	Switch de Energía y Distribución 3A (2)	Marca: ABB

Tabla 5. Layout de Dispositivos de Red (Cisco Systems)

3.2.7 Presupuesto de Equipos

La totalidad del costo de equipos se basa en cotizaciones hechas a traves de paginas dinámicas de actualización de precios, la tabla 6 detalla el costo especifico de cada dispositivo dado en Dólares.

Fabricante	Referencia	Numero De Parte	Cantidad	Costo (En Dólares)	Costo Total
Cisco Firewall	Cisco Pix 515e Security Appliance	Part # PIX-515E-FO-BUN	1	$2319	$2319
Cisco Switch Serie 3750	Cisco Catalyst 3750g-24t	Part # WS-C3750G-24T-E	1	$6995	$6995
Cisco Switch Serie 3750	Cisco Catalyst 3750-24ts	Part # WS-C3750-24TS-E	8	$3995	$31960
Cisco Switch Serie 3550	Cisco Catalyst 3550-24-Fx Switch	Part # WS-C3550-24-FX-SMI	1	$6495	$6495
Siemon	Patch Panel Utp Cat 6 96 Puertos	REF# HD6-96U	3	$810	$2430
Siemon	PATCH CORDS CAT 6 1.5mt	REF# MC6-8-T-(05)-(06)	192	$11,28	$2165,76
Total					$52364,76

Tabla 6. Presupuesto de Equipos (Cisco Systems)

3.4 ARQUITECTURA E IMPLEMENTACIÓN MEDIANTE SOLUCIONES 3COM

3.4.1 Configuración Lógica Entre la Red de Planta y el Sistema de Control

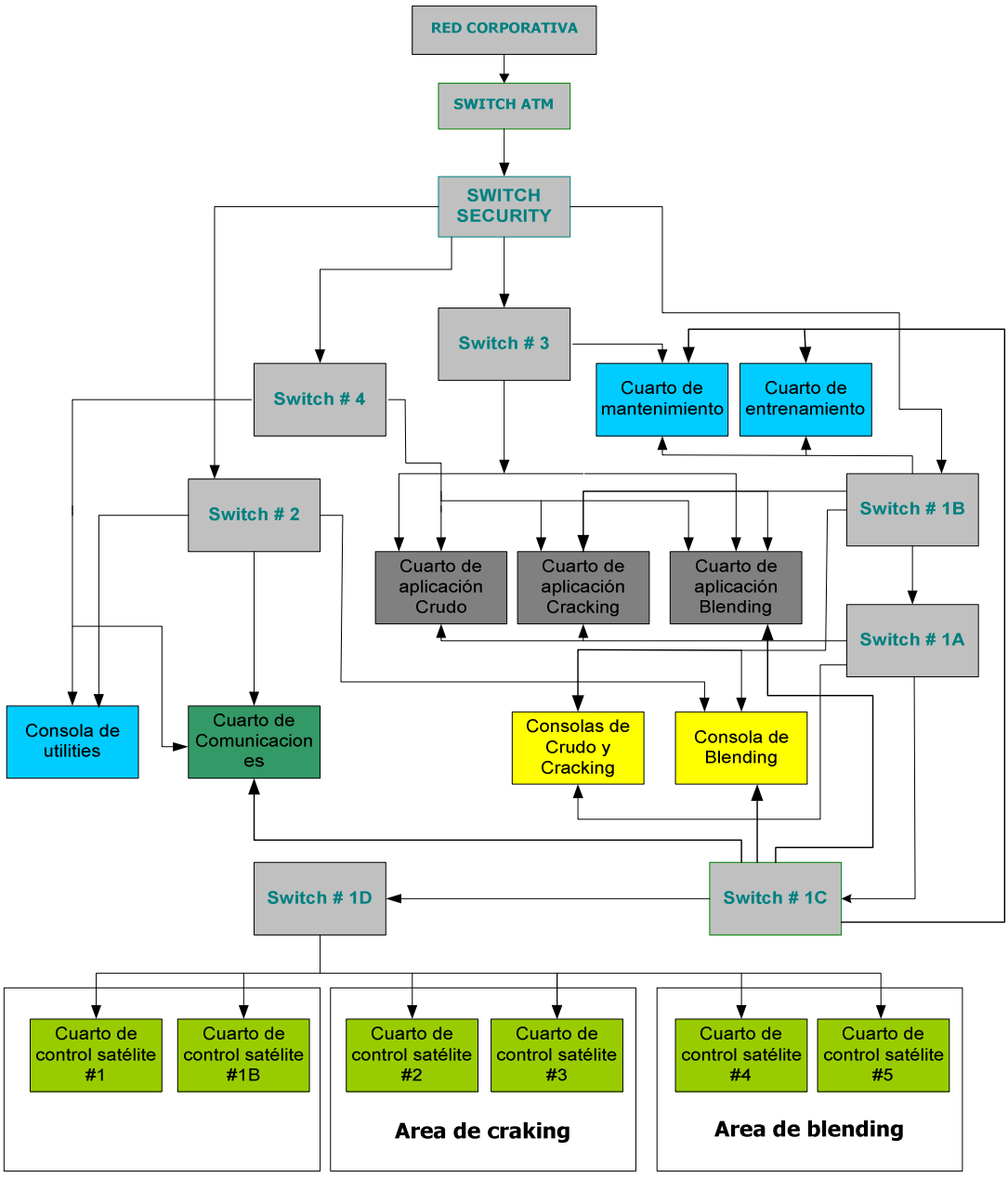


Figura 19. Configuración Lógica entre la Red de Planta y el Sistema de Control (3Com)

3.4.2 Área Reestructurada (Cuarto de Comunicaciones)

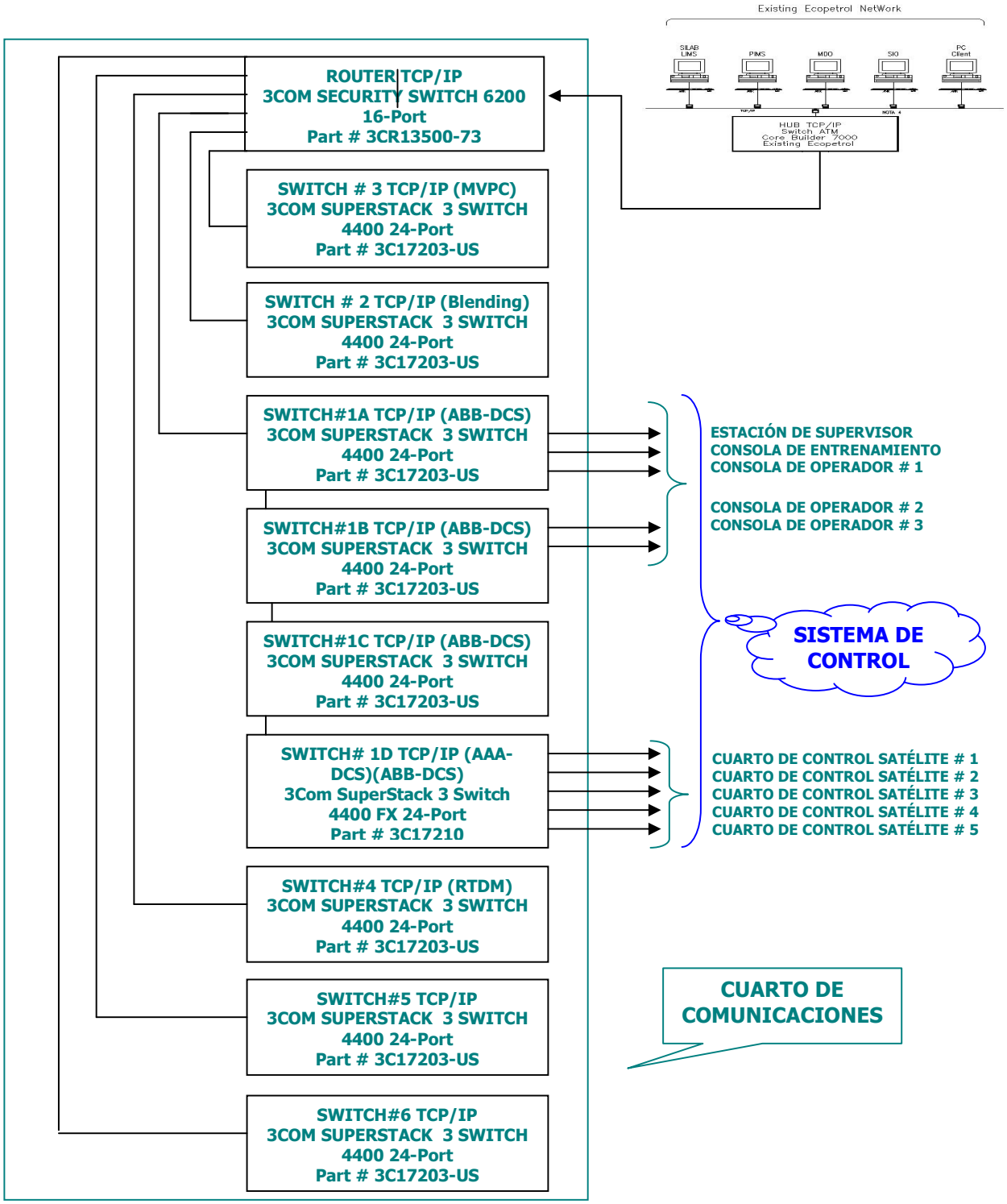


Figura 20. Área Reestructurada (Soluciones 3Com)

3.4.3 Configuración por Nodos de Nuevos Equipos Conectados al Patch Panel

Figura 21. Configuración por Nodos Conectados al Patch Panel (3Com)

3.4.4 Esquema de Direccionamiento (Localización y Configuración de Equipos)

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
N/A	Estación De Control Avanzado De Blending	PC	Eabc	150.67.73.6	CCB-CONSOLA3
SWITCH#4	Estación De Control Avanzado	PC	Eabc10	150.67.73.11	CCB-COMUNIC-1
SWITCH#1A	Estación De Operación #1 Consola De Crudo	OS520	Eas110	150.67.74.11	CCB-CONSOLA1
SWITCH#1A	Estación De Operación #2 Consola De Crudo	OS520	Eas120	150.67.74.12	CCB-CONSOLA1
SWITCH#1A	Estación De Operación #3 Consola De Crudo	OS520	Eas130	150.67.74.13	CCB-CONSOLA1
SWITCH#1A	Estación De Operación #4 Consola De Crudo	OS520	Eas140	150.67.74.14	CCB-CONSOLA1
SWITCH#1A	Estación De Operación #5 Consola De Crudo	OS520	Eas150	150.67.74.15	CCB-CONSOLA1
SWITCH#1A	Estación De Operación #6 Consola De Crudo	OS520	Eas160	150.67.74.16	CCB-CONSOLA1
SWITCH#1A	Estación De Operación #1 Consola De Cracking	OS520	Eas170	150.67.74.17	CCB-CONSOLA2
SWITCH#1A	Estación De Operación #2 Consola De Cracking	OS520	Eas180	150.67.74.18	CCB-CONSOLA2
SWITCH#1B	Estación De Operación #3 Consola De Cracking	OS520	Eas190	150.67.74.19	CCB-CONSOLA2
SWITCH#1B	Estación De Operación #4 Consola De Cracking	OS520	Eas200	150.67.74.20	CCB-CONSOLA2
SWITCH#1B	Estación De Operación #5 Consola De Cracking	OS520	Eas210	150.67.74.21	CCB-CONSOLA2
SWITCH#1B	Estación De Operación #6 Consola De Cracking	OS520	Eas220	150.67.74.22	CCB-CONSOLA2
SWITCH#1B	Estación De Operación #1 Consola De Blending	OS520	Eas230	150.67.74.23	CCB-CONSOLA3
SWITCH#1B	Estación De Operación #2 Consola De Blending	OS520	Eas240	150.67.74.24	CCB-CONSOLA3
SWITCH#1B	Estación De Operación #3 Consola De Blending	OS520	Eas250	150.67.74.25	CCB-CONSOLA3
SWITCH#1B	Estación De Operación #4 Consola De Blending	OS520	Eas260	150.67.74.26	CCB-CONSOLA3
SWITCH#1C	Estación De Operación #5 Consola De Blending	OS520	Eas270	150.67.74.27	CCB-CONSOLA3
SWITCH#1C	Estación De Operación #6 Consola De Blending	OS520	Eas280	150.67.74.28	CCB-CONSOLA3
SWITCH#1A	Estación De Ingeniería Sistema De Crudo	OS520	Eas290	150.67.74.29	CCB-APLICACION1
SWITCH#1B	Estación De Ingeniería Sistema De Cracking	OS520	Eas300	150.67.74.30	CCB-APLICACION2
SWITCH#1B	Estación De Ingeniería Sistema De Blending	OS520	Eas310	150.67.74.31	CCB-APLICACION3
SWITCH#1D	Estación De Operación Local Sistema De Crudo	OS520	Eas380	150.67.74.38	SIH#1-CONSOLA
SWITCH#1D	Estación De Operación Local Sistema De Tratamiento	OS520	Eas390	150.67.74.39	SIH#1-CONSOLA
SWITCH#1D	Estación De Operación Local Sistema De Cracking	OS520	Eas400	150.67.74.40	LCB#2-CONSOLA

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
SWITCH#1D	Estación De Operación Local Sistema De Azufre	OS520	Eas410	150.67.74.41	LCB#3-CONSOLA
SWITCH#1D	Estación De Operación Local Sistema De Blending Refinería	OS520	Eas420	150.67.74.42	LCB#4-CONSOLA
SWITCH#1D	Estación De Operación Local Sistema De Blending Tnp	OS520	Eas430	150.67.74.43	LCB#5-CONSOLA
N/A	Estación De Operación #1 Sistema De Entrenamiento	OS520	Eas610	150.67.74.61	CCB-ENTRENAMIENTO
N/A	Estación De Operación #2 Sistema De Entrenamiento	OS520	Eas620	150.67.74.62	CCB-ENTRENAMIENTO
N/A	Estación De Operación #5 Sistema De Entrenamiento	OS520	Eas640	150.67.74.64	CCB-ENTRENAMIENTO
N/A	Estación De Operación #4 Sistema De Entrenamiento	OS520	Eas650	150.67.74.65	CCB-ENTRENAMIENTO
N/A	Estación De Operación #3 Sistema De Entrenamiento	OS520	Eas660	150.67.74.66	CCB-ENTRENAMIENTO
SWITCH#4	Estación De Operación Y Gateway #1 Foxboro	AW51	Eaw030	150.67.74.121	CCB-CONSOLA4
SWITCH#4	Estación De Operación Y Gateway #1 Foxboro	AW51	Eaw040	150.67.74.122	CCB-CONSOLA4
SWITCH#4	Estación De Base De Datos En Tiempo Real	UNIX	Ebdtr	150.67.73.1	CCB-COMUNIC-PI
SWITCH #3	Estación Bently Nevada	PC	Ebn	150.67.73.13	CCB-MANTENIMIENTO
SWITCH #1C	Estación De Analizadores Vistanet	PC	Ecac	150.67.73.10	CCB-MANTENIMIENTO
N/A	Estación De Ingeniería Sistema Abb	PC	Ees00	150.67.74.10	CCB-COMUNIC-1
SWITCH #5	Estación #1 Sistema De Shutdown De Crudo	PC	Eesd10a	150.67.76.51	CCB-CONSOLA1
SWITCH #5	Estación #2 Sistema De Shutdown De Crudo	PC	Eesd10b	150.67.76.52	CCB-CONSOLA1
SWITCH #5	Estación Local Sistema De Shutdown De Crudo	PC	Eesd10c	150.67.76.53	SIH#1-CONSOLA
SWITCH #6	Estación #1 Sistema De Shutdown De Cracking	PC	Eesd20a	150.67.76.55	CCB-CONSOLA2
SWITCH #6	Estación #2 Sistema De Shutdown De Cracking	PC	Eesd20b	150.67.76.56	CCB-CONSOLA2
SWITCH #6	Estación Local Sistema De Shutdown De Cracking	PC	Eesd20c	150.67.76.57	LCB#2-CONSOLA
SWITCH #6	Estación Local Sistema De Shutdown De Azufre	PC	Eesd20d	150.67.76.58	LCB#3-CONSOLA
SWITCH#3	Multiplexer Ams Smart Transmitter Interface	MX	Ihmux	150.67.73.8	CCB-MANTENIMIENTO
SWITCH#3	Estación Ams Smart Transmitter Interface - Hart	PC	Ehpc	150.67.73.7	CCB-MANTENIMIENTO
	Router Super Stack 3800	ETHERNET	Ehub	150.67.76.1	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Red De Planta Abb	ETHERNET	Ehub10	150.67.76.2	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Red De Planta Abb	ETHERNET	Ehub10	150.67.76.2	CCB-COMUNIC-RACK
	Hub 6 Puertos Fibra Óptica	ETHERNET	Ehub10	150.67.76.2	CCB-COMUNIC-

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
	Red De Planta Abb				RACK
	Hub 6 Puertos Fibra Óptica Red De Planta Abb	ETHERNET	Ehub10	150.67.76.2	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Blending	ETHERNET	Ehub20	150.67.76.3	CCB-COMUNIC-RACK
	Hub 24 Puertos Utp Control Avanzado	ETHERNET	Ehub30	150.67.76.4	CCB-COMUNIC-RACK
	Swith 12 Puertos Utp Base De Datos En Tiempo Real	ETHERNET	Ehub40	150.67.76.5	CCB-COMUNIC-RACK
	Swith 24 Puertos Utp Esd Y Ups	ETHERNET	Ehub50	150.67.76.6	CCB-COMUNIC-RACK
SWITCH#3	Pc Portatil Hvac	PORTATIL	Ehvac	150.67.73.12	CCB-MANTENIMIENTO
SWITCH #1A	Estación De Historia Sistema De Crudo	IMS530	Eims330	150.67.74.33	CCB-APLICACION1
SWITCH #1A	Estación De Historia Sistema De Cracking	IMS530	Eims340	150.67.74.34	CCB-APLICACION2
SWITCH#1B	Estación De Historia Sistema De Blending	IMS530	Eims350	150.67.74.35	CCB-APLICACION3
SWITCH #4	Estación Gateway Pi Sistema De Crudo	IMS530	Eims440	150.67.74.44	CCB-APLICACION1
SWITCH #4	Estación Gateway Pi Sistema De Cracking	IMS530	EIms450	150.67.74.45	CCB-APLICACION2
SWITCH #4	Estación Gateway Pi Sistema De Blending	IMS530	EIms460	150.67.74.46	CCB-APLICACION3
SWITCH #1A	Estacion Gateway Pi-Abb	IMS530	Eims470	150.67.74.47	CCB-COMUNIC-1
N/A	Estación De Historia Sistema De Entrenamiento	IMS530	Eims630	150.67.74.63	CCB-ENTRENAMIENTO
	Impresora Laser A Color Sistema De Entrenamiento	LCP	ILcp10	150.67.75.1	CCB-ENTRENAMIENTO
	Impresora Laser A Color Operadores De Consola	LCP	ILcp20	150.67.75.2	CCB-CONSOLA4
	Impresora Laser A Color Administrador Del Sistema	LCP	Ilcp30	150.67.75.3	CCB-SISTEMA
	Impresora Laser A Color Cuarto De Mantenimiento	LCP	Ilcp40	150.67.75.4	CCB-MANTENIMIENTO
SWITCH #1B	Impresora Laser A Color Sistema De Ingeniería	LCP	Ilcp50	150.67.75.5	CCB-APLICACION2
SWITCH #3	Impresora Laser Blanco Y Negro Administrador Pi	LP	ILip60	150.67.75.6	CCB-COMUNIC-1
	Hub Mb300 Para Sistema De Crudo	MB300			CCB-COMUNIC-RACK
	Hub Mb300 Para Sistema De Cracking	MB300			CCB-COMUNIC-RACK
	Hub Mb300 Para Sistema De Blending	MB300			CCB-COMUNIC-RACK
	Star Coupler Mb300 Para Sistema De Crudo	MB300			SIH#1-DCS
	Star Coupler Mb300 Para Sistema De Tratamiento	MB300			SIH#1B-DCS
	Star Coupler Mb300 Para Sistema De Cracking	MB300			SIH#2-DCS
	Star Coupler Mb300 Para Sistema De Azufre	MB300			SIH#3-DCS

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
	Star Coupler Mb300 Para Sistema De Blending Refinería	MB300			SIH#4-DCS
	Star Coupler Mb300 Para Sistema De Blending Tnp	MB300			SIH#5-DCS
	Switche Mb300 Multilan Para Red 11	MB300			CCB-COMUNIC-RACK
	Switche Mb300 Multilan Para Red 12	MB300			CCB-COMUNIC-RACK
	Impresora Matriz De Punto Consola De Crudo 1	MP			CCB-COMUNIC-1
	Impresora Matriz De Punto Consola De Crudo 2	MP			CCB-CONSOLA1
	Impresora Matriz De Punto Consola De Cracking 1	MP			CCB-CONSOLA2
	Impresora Matriz De Punto Consola De Cracking 2	MP			CCB-CONSOLA2
	Impresora Matriz De Punto Consola De Blending 1	MP			CCB-CONSOLA3
	Impresora Matriz De Punto Consola De Blending 1	MP			CCB-CONSOLA3
	Impresora Matriz De Punto A Color Bently Nevada	MP			CCB-MANTENIMIENTO
	Impresora Matriz De Punto Sistema Esd De Crudo	MP			CCB-CONSOLA1
	Impresora Matriz De Punto Sistema Esd De Cracking	MP			CCB-CONSOLA2
SWITCH #3	Estación Nir	PC	Enir	150.67.73.9	CCB-MANTENIMIENTO
SWITCH #3	Estación Del Optimizador De Cracking	PC	Eopti	150.67.73.4	CCB-APLICACION2
	Estación De Reconciliacion De Datos	PC	EReda	150.67.73.3	CCB-SISTEMA
N.A.	Estación De Operación #1 Siemens	OT	Esie010	150.67.74.123	CCB-CONSOLA4
N.A.	Estación De Operación #2 Siemens	OT	Esie020	150.67.74.124	CCB-CONSOLA4
N.A.	Estación De Operación #3 Siemens	OT	Esie030	150.67.74.125	CCB-CONSOLA4
N.A.	Estación De Operación #4 Siemens	OT	Esie040	150.67.74.126	CCB-CONSOLA4
N.A.	Estación Gateway Siemens	XU	Esie050	150.67.74.127	CCB-COMUNIC-PI
N.A.	Estación Pc Esclavo Siemens	PC	Esie060	150.67.74.128	CCB-COMUNIC-PI
N.A.	Estación De Star Blend	PC	Estarb	150.67.73.5	CCB-CONSOLA3
N.A.	Estacion De Short Term Schedulling	PC	Ests	150.67.73.2	CCB-SISTEMA
SWITCH #5	Ups No.1 Ccb	UPS		150.67.76.101	CCB-UPS
SWITCH #5	Ups No.2 Ccb	UPS		150.67.76.102	CCB-UPS
SWITCH #6	Ups No.3 Ccb	UPS		150.67.76.103	CCB-UPS
SWITCH #5	Ups No.1 Sih#1	UPS		150.67.76.104	SIH#1
SWITCH #5	Ups No.2 Sih#1	UPS		150.67.76.105	SIH#1
SWITCH #5	Ups No.1 Sih#2	UPS		150.67.76.106	SIH#2
SWITCH #5	Ups No.2 Sih#2	UPS		150.67.76.107	SIH#2

Conexión Red de Planta	Descripción Equipo	Código Tipo Equipo	Nombre Host	Dirección TCP-IP	Código Localización
SWITCH #6	Ups No.1 Sih#3	UPS		150.67.76.108	SIH#3
SWITCH #6	Ups No.2 Sih#3	UPS		150.67.76.109	SIH#3
SWITCH#1B	Estación De Ingeniería Xterminal Sistema De Crudo	PC	EXterm10	150.67.74.130	CCB-APLICACION1
SWITCH#1C	Estación De Ingeniería Xterminal Sistema De Cracking	PC	EXterm20	150.67.74.131	CCB-APLICACION2
N/A	Estación De Ingeniería Xterminal Sistema De Blending	PC	EXterm30	150.67.74.132	CCB-APLICACION3

Tabla 7. Nuevo Esquema de Direccionamiento (3Com)

3.3.5 Layout del Gabinete CCB-DCS-C04 (3Com)

Plano U y H del Gabinete CCB-DCS-C04 (Vista Frontal, con la puerta abierta), Plano C (Vista lateral derecha) y Plano A (Vista lateral izquierda).

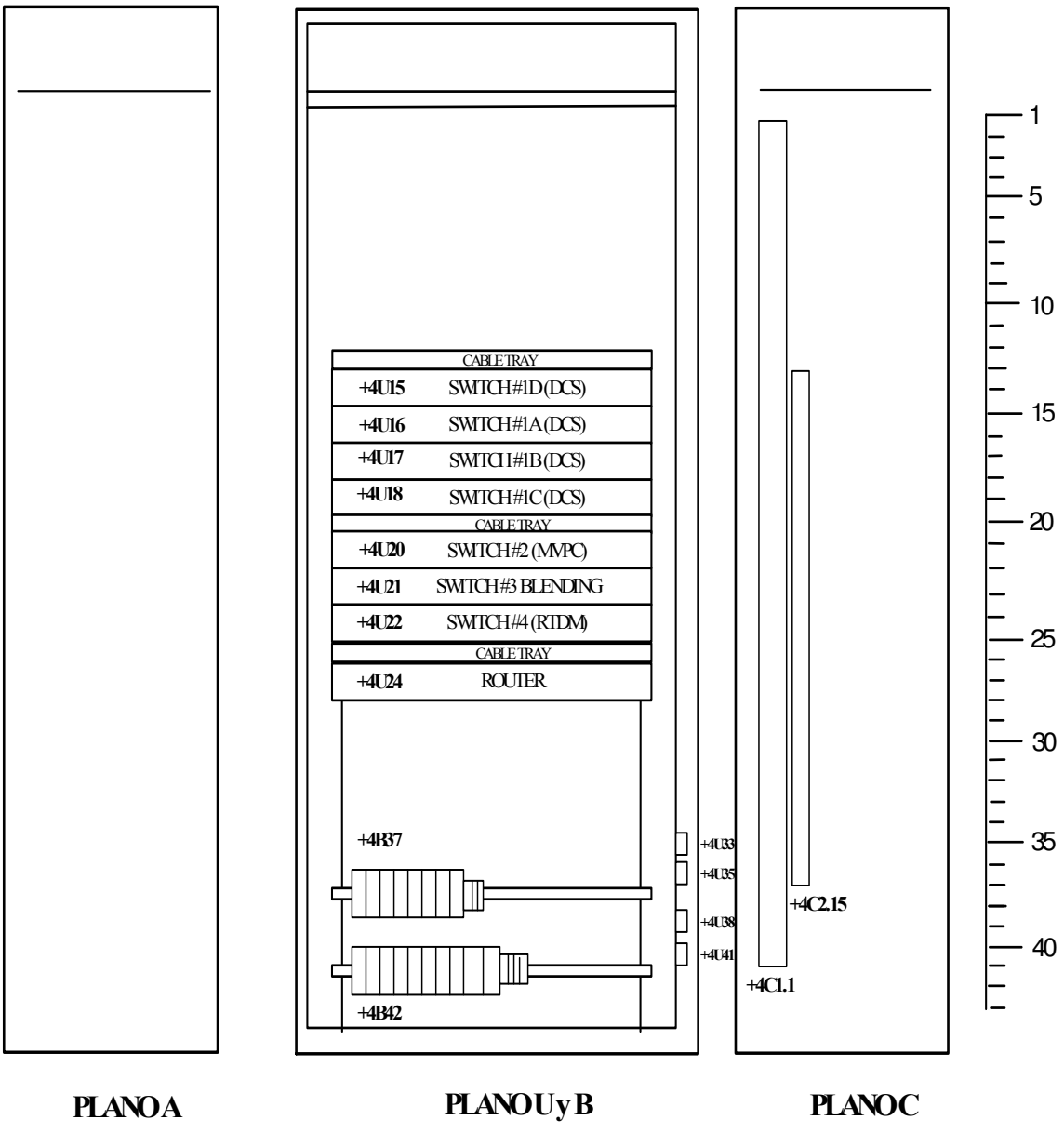


Figura 22. Layout del Gabinete CCB-DCS-C04 (3Com)

3.3.6 Layout de los Dispositivos de Red

Componentes del Plano U y B para el Gabinete CCB-DCS-C04.

Componentes del Plano C Gabinete CCB-DCS-C04

Loc.	Artículo	Descripción	Comentarios
+4C1.1	Canaleta	5 X 8 cm	Color Gris
+4C10.1		Multicontacto de 15	120 VCA

Loc.	Artículo	Descripción	Comentarios
+4U15	Switch#1D	Switch para Fibra Optica de 24 puertos	Marca: 3COM Super Stack 3
+4U16	Switch#1A	Switch para 10Base-T/100Base-TX de 24 puertos	Marca: 3COM Super Stack 3
+4U17	Switch#1D	Switch para 10Base-T/100Base-TX de 24 puertos	Marca: 3COM Super Stack 3
+4U18	Switch#1D	Switch para 10Base-T/100Base-TX de 24 puertos	Marca: 3COM Super Stack 3
+4U29		Cable Tray	Color Negro
+4U20	SWITCH#2	Switch para 10Base-T/100Base-TX de 24 puertos 3C17203-US	Marca: 3COM Super Stack 3
+4U21	SWITCH #3	Switch para 10Base-T/100Base-TX de 24 puertos 3C17203-US	Marca: 3COM Super Stack 3
+4U22	SWITCH #4	Switch para 10Base-T/100Base-TX de 24 puertos 3C17203-US	Marca: 3COM Super Stack 3
+4U23		Cable Tray	Color Negro
+4U24	Router	Security Switch 6200 de 16 puertos 3CR13500-73	Marca: 3COM
+4U37	E272 100A	Breaker de Alimentación Principal	Marca: ABB
+4U37	S272K2A	Switch de Energía y Distribución 2A (5)	Marca: ABB
+4U37	S272K10A	Switch de Energía y Distribución 10A	Marca: ABB
+4U37	ZPE 2.5	Borneras (3) Modelo: 160864	Marca: Weidmüller
+4U42	E272 100A	Breaker de Alimentación Principal	Marca: ABB
+4U42	S272K2A	Switch de Energía y Distribución 2A (4)	Marca: ABB
+4U42	ZPE 2.5	Borneras (3) Modelo: 160864	Marca: Weidmüller
+4U42	S272K3A	Switch de Energía y Distribución 3A (2)	Marca: ABB

Tabla 8. Layout de Dispositivos de Red (3Com)

3.3.7 Presupuesto de Equipos

Para 3Com la totalidad del costo de equipos se basa en cotizaciones hechas a traves de páginas dinámicas de actualización de precios, la tabla 9 detalla el costo especifico de cada dispositivo dado en Dólares

Fabricante	Referencia	Numero De Parte	Cantidad	Costo (En Dólares)	Costo Total
3com Switch Security 6200	3com Security 6200 16-Puertos	Part # 3CR13500-73	1	$19550	$19550
3com Switch Superstack 3 4400	3com Superstack 3 4400 24-Pts	Part # 3C17203-US	8	$1213	$9704
3Com Switch Superstack 3 4400 FX	3Com Superstack 3 4400 FX 24-Pts	Part # 3C17210	1	$2896	$2896
Siemon	Patch Panel Utp Cat 6 96 Puertos	Ref# Hd6-96u	2	$810	$1620
Siemon	PATCH CORDS CAT 6 1.5mt	Ref# Mc6-8-T-(05)-(06)	192	$11,28	$2165,76
Total					$35935,76

Tabla 9. Presupuesto de Equipos (3Com)

CONCLUSIONES

La industria al igual que cualquier organización es vulnerable a cualquier tipo de ataque sea este interno, externo o causado por una mala administración de los servicios de red.

A lo largo de esta obra se demuestra que el administrador del sistema al igual que cualquier usuario, debe poder controlar granularmente los permisos de acceso iniciando por los de su misma información, saber quién mas tiene acceso, qué tipo de acceso tiene y tomar las medidas pertinentes de autenticación.

Al momento de implementar nuestro sistema, no debemos pensar que nadie atacara nuestro sistema únicamente por que este parezca inapreciable, insospechable e invulnerable a los demás, como también no debemos restar importancia a las actualizaciones ni a la solidez general que en un momento dado requiera nuestro sistema.

La evaluación al momento de seleccionar dispositivos de red supone exactamente el mismo tipo de evaluación que hacemos al escoger un computador personal, pues la arquitectura interna y la electrónica de estos dispositivos es muy similar teniendo en cuenta aspectos tales como: el tiempo compartido del procesador y la capacidad de almacenamiento del buffer de memoria entre otros.

Siempre que estemos pensando a futuro, no deberiamos confiar la base de nuestro negocio exclusivamente a equipos que sean de tipo propietario, esto debido ha:

→ Nuevos formatos que sean incompatibles y a la falta de soporte para formatos de versiones anteriores.

→ La dependencia de que única y exclusivamente un sólo fabricante continúe dando soporte al producto.

→ Que nos resta la capacidad de hacer cambios en nuestra tecnología base (hardware, OS, etc.)

Es importante, siempre que sea la escalabilidad la base tecnológica de nuestro negocio, de que es preferible seguir una línea de productos que sean robustos y ofrezcan buen respaldo. Para el caso de la empresa, se deja a opcion de la misma la escojecia, ya sea de equipos ***Cisco System*** *o equipos* ***3Com,*** por sus grandes bondades al momento de optar por la escalabilidad de la red, lo cual es aconsejable para cualquier caso donde se requiera una implementación de este tipo.

Finalmente para este caso en particular, no es recomendable ahorrar algún dinero si se trata de proteger la información de la cual se sostiene la correcta operación y ejecución de los procesos, como lo es el caso particular de esta industria, donde debe prevalecer la continuidad de operaciones ya que esta es la naturaleza de este negocio. Claro esta, que esto no significa realizar gastos que vayan mas allá de lo que realmente amerita una buena reestructuración que a fin de cuentas seria protección a la inversión.

Este tipo de inversión, no es recuperable en dinero debido a que hace parte de las estrategias de funcionamiento de cualquier negocio, por tanto se gana, desde el momento de vacunar, por decirlo de alguna manera, mis intereses teniendo como punto de partida el tipo de información que fluye por una red.

RECOMENDACIONES

Es importante que la industria tome conciencia de la creación y ejecución de políticas de seguridad que permitan garantizar la confidencialidad de los datos, sin dejar de lado su eficiencia y eficacia.

Es necesario que para futuras implementaciones y modificaciones se tengan en cuenta las grandes ventajas y beneficios de utilizar familias o series de dispositivos que sean apilables, esto, con el objeto de ganar rendimiento al momento de hacer extensión en los dispositivos de red.

Es determinante el uso de un software de gestión de redes que permita la verificación continua de las operaciones y el flujo que en determinado instante se quiera comprobar entre dos o más nodos entre los sistemas de control y la red corporativa.

Es importante la capacitación de la persona o de las personas encargadas de la administración y configuración de los dispositivos de red a fin de no acudir a terceros ante cualquier anomalía en la configuración o el funcionamiento de estos equipos.

Considerar fabricantes que ofrezcan un excelente servicio de soporte técnico y actualización, en caso de futuras remodelaciones de los equipos.

Se debe realizar una evaluación de los procesos de red, haciendo seguimientos en cuanto a la seguridad y confiabilidad

Modificar cada cierto periodo de tiempo las estrategias de seguridad a fin de descartar la posibilidad de intrusión tanto interna como externa basándose en las políticas de seguridad ya definidas.

Definir adecuadamente el perímetro de seguridad entre la red corporativa y cada una de las áreas de acceso en los sistemas de control.

Es determinante mantener una auditoria lógica, física, informática y de personal con el objeto de identificar deficiencias en cualquiera de estos cuatro aspectos.

Se recomienda la intervención de auditoria externa para identificar toda deficiencia e ineficacia del personal encargado de la administración de red.

Se recomienda continuar el apilamiento con cualquiera de los fabricantes que se seleccone, de esta manera cualquiera de estos formaria un backplane en Gbps. El apilamiento no requiere puertos de usuario y además se pueden apilar hasta el total de unidades ofrecidas por cualquiera de las familias, al igual que se obtendria un máximo entre 400 y 500 puertos 10/100, 10/100/1000 o una combinación de éstos. Una pila en funcionamiento se autogestiona y autoconfigura. Al agregar o quitar switches, el switch principal actualiza automáticamente todas las tablas de enrutamiento para reflejar los cambios y las actualizaciones se aplicarían simultáneamente en el nivel global a todos los miembros de la pila.

Para futuras implementaciones es importante la compatibilidad con sistemas de alimentación redundante ofrecidas por el fabricante, lo cual daria una mayor redundancia al sistema de alimentación interna para el máximo de dispositivos que ofrezca cada familia, lo que resulta en una mayor tolerancia de fallos y tiempo de actividad de la red.

BIBLIOGRAFIA

SMITH – CORRIPIO. Control Automático De Procesos, Teoría Y Practica, Limusa Noriega Editores. El Sistema De Control De Procesos, Cap1, Pág. 17. Componentes Básicos De Los Sistemas De Control, Cap 5, Pág. 177.

VILLALÓN Huerta, Antonio. Seguridad En Unix Y Redes Versión 2.1. México D.F. Firewalls, Casos De Estudio, Cap 4, Num 16, Pag265. Algunas Herramientas De Seguridad, Tcp Wrappers, Cap 5, Num 21, Pag 375.

"NETWORK SECURITY", Capítulo 7. F. Simonds. McGraw-Hill, 1996.

"Firewalls and Internet Security", Partes I Y II. W.R. Cheswick Y S.M. Bellovin. Addison-Wesley, 1994.

PAGINAS VISITADAS

http://howstuffworks.shopping.com/xPP-Firewalls

http://www.3com.com/products/en_US/detail.jsp?tab=features&pathtype=purchase&sku=WEBBNGARPSSYS

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_security_advisories_list.html

http://www.symantec.com/region/nl/product/vpn200_index.html

http://www.extremenetwork.com

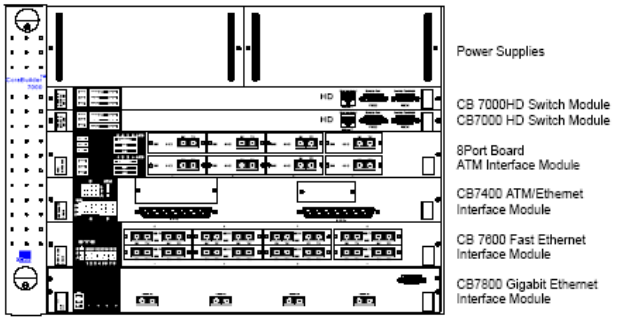
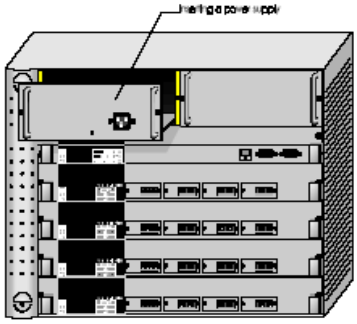
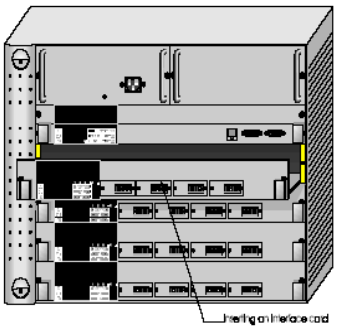
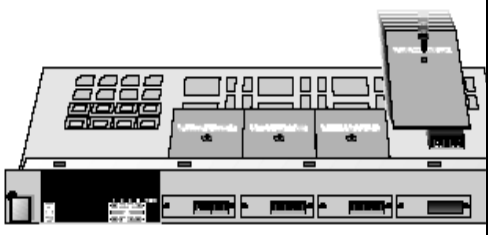
http://www.lafacu.com/apuntes/informatica/redes_teoria/default.htm

ANEXOS

ANEXO A

DESCRIPCIÓN DEL COREBUILDER SWITCH FAMILIA 7000 ATM

DESCRIPCIÓN DEL COREBUILDER SWITCH FAMILIA 7000 ATM

<table>
<tr><th colspan="2">CoreBuilder Switch Familia 7000 ATM</th></tr>
<tr><td> 
</td><td>  </td></tr>
<tr><td>Componentes Generales Del Corebuilder Familia 7000 ATM Switch</td><td>Intercambiador En Caliente De Alimentación Redundante</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>Modulo Intercambiador En Caliente De Interruptor Y Tarjeta Interfaz</td><td>Modulo De Puerto Interfaz ATM</td></tr>
</table>

ANEXO B

PATCH PANELS REQUERIDOS PARA EQUIPOS NUEVOS

PATCH PANELS REQUERIDOS PARA EQUIPOS NUEVOS

SIEMON™

PANELES DE PARCHEO HD® 6	PANELES DE PARCHEO HD® 5
	
Este modelo de Patch Panel con demarcacion de puertos en alto relieve, Incluye: → Acomodador trasero de cables. → Porta etiquetas ó íconos. → Etiquetas de designaciones. → Abrazaderas para cables. → Elementos de montaje.	Este modelo tipo de Patch Panel con demarcacion de puertos en colores Incluye: → Acomodador trasero de cables. → Porta etiquetas de íconos. → Etiquetas de designaciones. → Abrazaderas para cables. → Elementos de montaje.

ANEXO C

DILIGENCIAMIENTO PARA SOLICITUD DE EQUIPOS CISCO SYSTEMS

DILIGENCIAMIENTO PARA SOLICITUD DE EQUIPOS CISCO SYSTEMS

Correo De Respuesta Comercial

Formato De Diligenciamiento

You'll be entered into a quarterly drawing for **free** Cisco Press books by returning this survey! Cisco is dedicated to customer satisfaction and would like to hear your thoughts on these printed manuals. Please visit the Cisco Product Comments on-line survey at **www.cisco.com/go/crc** to submit your comments about accessing Cisco technical manuals. Thank you for your time.

General Information

1 Years of networking experience: _____ Years of experience with Cisco products: _____

2 I have these network types: ___ LAN ___ Backbone ___ WAN
___ Other: _____

3 I have these Cisco products: ___ Switches ___ Routers
___ Other (specify models): _____

4 I perform these types of tasks: ___ H/W installation and/or maintenance ___ S/W configuration
___ Network management ___ Other: _____

5 I use these types of documentation: ___ H/W installation ___ H/W configuration ___ S/W configuration
___ Command reference ___ Quick reference ___ Release notes ___ Online help
___ Other: _____

6 I access this information through: ___ % Cisco.com ___ % CD-ROM ___ % Printed manuals
___ % Other: _____

7 I prefer this access method: ___ Cisco.com ___ CD-ROM ___ Printed manuals
___ Other: _____

8 I use the following three product features the most: _____

Document Information

Document Title: Catalyst 3750 Switch Hardware Installation Guide

Part Number: 78-15136-02 S/W Release (if applicable): <Software Release>

On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:

___ The document is complete.
___ The information is accurate.
___ The information is well organized.
___ The information I wanted was easy to find.
___ The document is written at my technical level of understanding.
___ The information I found was useful to my job.

Please comment on our lowest scores: _____

Mailing Information

Organization Date

Contact Name

Mailing Address

City State/Province Zip/Postal Code

Country Phone ( ) Extension

E-mail Fax ( )

May we contact you further concerning our documentation? ___ Yes ___ No

You can also send us your comments by e-mail to **bug-doc@cisco.com**, or by fax to **408-527-8089**.

When mailing this card from outside of the United States, please enclose in an envelope addressed to the location on the back of this card with the required postage or fax to 1-408-527-8089.

ANEXO D

GENERALIDADES DE UN SISTEMA DE CONTROL

Modelo de un Sistema de Control

Descripción General de un Sistema de Control (GTC)

El GTC consiste en un conjunto de subsistemas que deben trabajar de forma coordinada. Estos subsistemas se encuentran distribuidos físicamente en las instalaciones del GTC. La responsabilidad del sistema de control es el control y monitorización de estos subsistemas y proporcionar una interfaz de usuario homogénea.

La arquitectura física del sistema de control consistirá en una serie de computadores, equipos electrónicos, sensores y actuadores interconectados. Estos elementos serán responsables del control directo de los diferentes subsistemas del GTC. El sistema de control será responsable de otras tareas (e.g. planificación de observaciones, archivo de los datos, análisis de la calidad de los datos) para lo cual existirán un número de estaciones de trabajo conectadas a través de una o más redes de área local, las cuales proveerán acceso a un grupo de servicios centralizados (por ejemplo, catálogos, archivos).

Una arquitectura de software abierta, flexible, distribuida y orientada a objetos debe ser utilizada con el objeto de proveer acceso independiente de la localización a los diferentes servicios distribuidos. Además, estos servicios son requeridos para garantizar un nivel de calidad de servicio. La implementación de esta arquitectura será simplificada mediante el uso de *middleware* distribuido. Este middleware asegurará mediante una política de planificación correcta, que todas las tareas tendrán los recursos necesarios. Se debe suministrar un esqueleto *"plug&play*" donde los diferentes componentes del software de control sean conectados. Esta arquitectura suministrará un entorno homogéneo tal, que el tiempo y coste de desarrollo de los diferentes componentes será reducido.

Arquitectura del Software

La arquitectura del sistema de control debe consistir en un conjunto altamente integrado de sistemas distribuidos por medio de redes en una organización jerárquica. Esta jerarquía debe estar organizada siguiendo el modelo cliente-servidor. El sistema de control debe operar en tiempo real (*quasi-real time*), con una jerarquía de niveles de control y comunicaciones entre procesos. Se hace necesario un gran número de puntos de control y por lo tanto, de procesos para controlarlos. Los planes deben cumplir varios procesos *front-end*, procesos, estaciones de trabajo y servidores.

Al igual que en otros dominios (aviación, telecomunicaciones, multimedia), la garantía de tiempo real es necesaria en el sistema de control de las redes de comunicación, en los sistemas operativos y en los componentes middleware subyacentes, con el objetivo de satisfacer la calidad de servicio requerida.

Los elementos de proceso de un sistema de control pueden utilizar una implementación estándar en tiempo real como por ejemplo; CORBA (*Common Object Request Broker Architecture*) para la comunicación entre objetos a través de redes. Además, la especificación de interfaces debe ser muy importante para el mantenimiento y conservación de la inversión teniendo en cuenta los rápidos cambios tecnológicos. Por ello son muy usados estándares abiertos como RT POSIX o ATM, y también CORBA.

Arquitectura del Hardware

La arquitectura del hardware del sistema de control debería ser totalmente distribuida. Debe consistir en nodos VME llamados unidades de control locales (LCU) con capacidad de proceso en tiempo real conectados directamente a dispositivos físicos del GTC. Estas conexiones tienen que ser capaces de usar un conjunto variado de buses de control (ej., CAN bus, GPIB, Bitbus). Otros nodos de alto nivel llevarán a cabo funciones de coordinación y ofrecerán servicios críticos al resto de los

nodos (ej., envío de eventos, *logging*, monitorización, planificación). Ambas, LCU y las unidades de coordinación, deben ser conectadas por medio de uno o más ATM nodos, para formar la llamada red de control. Este modelo de arquitectura permitiría una configuración dinámica del tráfico del tal forma que cada nodo tendrá un ancho de banda adecuado a sus necesidades. En las circunstancias en las que el ancho de banda es muy grande, se deben usar otros interfaces como SCI o Fiber Channel, Sin embargo, cuando el ancho de banda no sea problema, se podrían usar interfaces más baratos como Ethernet o Fast-Ethernet.

Introducción a los Sistemas SCADA

Definición de Sistema SCADA

SCADA es el acrónimo de *Supervisory Control And Data Acquisition* (Supervisión, Control y Adquisición de Datos). Un SCADA es un sistema basado en computadores que permite supervisar y controlar a distancia una instalación de cualquier tipo. A diferencia de los Sistemas de Control Distribuido, el lazo de control es generalmente cerrado por el operador.

Los Sistemas de Control Distribuido se caracterizan por realizar las acciones de control en forma automática. Hoy en día es fácil hallar un sistema SCADA realizando labores de control automático en cualquiera de sus niveles, aunque su labor principal sea de supervisión y control por parte del operador.

En la tabla 1.2.4.1.1 se muestra un cuadro comparativo de las principales características de los sistemas SCADA y los sistemas de Control Distribuido (DCS) (estas características no son limitantes para uno u otro tipo de sistemas, son típicas).

Diferencias Típicas Entre Sistemas SCADA y DCS

ASPECTO	SCADAs	DCS
TIPO DE ARQUITECTURA	CENTRALIZADA	DISTRIBUIDA
TIPO DE CONTROL PREDOMINANTE	SUPERVISORIO: Lazos de control cerrados por el operador. Adicionalmente: control secuencial y regulatorio.	REGULATORIO: Lazos de control cerrados automáticamente por el sistema. Adicionalmente: control secuencial, batch, algoritmos avanzados, etc.
TIPOS DE VARIABLES	DESACOPLADAS	ACOPLADAS
ÁREA DE ACCIÓN	Áreas geográficamente distribuidas.	Área de la planta.
UNIDADES DE ADQUISICIÓN DE DATOS Y CONTROL	Remotas, PLCs.	Controladores de lazo, PLCs.
MEDIOS DE COMUNICACIÓN	Radio, satélite, líneas telefónicas, conexión directa, LAN, WAN.	Redes de área local, conexión directa.
BASE DE DATOS	CENTRALIZADA	DISTRIBUIDA

Tabla 21. Diferencias Típicas Entre Sistemas SCADA y DCS

El flujo de la información en los sistemas SCADA es como se describe a continuación: El fenómeno físico lo constituye la variable que deseamos medir. Dependiendo del proceso, la naturaleza del fenómeno es muy diversa: presión, temperatura, flujo, potencia, intensidad de corriente, voltaje, ph, densidad, etc. Este fenómeno debe traducirse a una variable que sea inteligible para el sistema SCADA, es decir, en una variable eléctrica. Para ello, se utilizan los sensores o transductores.

Los sensores o transductores convierten las variaciones del fenómeno físico en variaciones proporcionales de una variable eléctrica. Las variables eléctricas más utilizadas son: voltaje, corriente, carga, resistencia o capacitancia. Sin embargo, esta variedad de tipos de señales eléctricas debe ser procesada para ser entendida por el computador digital. Para ello se utilizan acondicionadores de señal, cuya función es la de referenciar estos cambios eléctricos a una misma escala de corriente o voltaje. Además, provee aislamiento eléctrico y filtraje de la señal con el

objeto de proteger el sistema de transientes y ruidos originados en el campo. Una vez acondicionada la señal, la misma se convierte en un valor digital equivalente en el bloque de conversión de datos. Generalmente, esta función es llevada a cabo por un circuito de conversión analógico/digital. El computador almacena esta información, la cual es utilizada para su análisis y para la toma de decisiones. Simultáneamente, se muestra la información al usuario del sistema, en tiempo real.

Basado en la información, el operador puede tomar la decisión de realizar una acción de control sobre el proceso. El operador comanda al computador a realizarla, y de nuevo debe convertirse la información digital a una señal eléctrica. Esta señal eléctrica es procesada por una salida de control, el cual funciona como un acondicionador de señal, la cual la escala para manejar un dispositivo dado: bobina de un relé, setpoint de un controlador, etc.

Necesidad de un Sistema SCADA

Para evaluar si un sistema SCADA es necesario para manejar una instalación dada, el proceso a controlar debe cumplir las siguientes características:

- El número de variables del proceso que se necesita monitorear es alto.
- El proceso está geográficamente distribuido. Esta condición no es limitativa, ya que puede instalarse un SCADA para la supervisión y control de un proceso concentrado en una localidad.
- Las información del proceso se necesita en el momento en que los cambios se producen en el mismo, o en otras palabras, la información se requiere en tiempo real.
- La necesidad de optimizar y facilitar las operaciones de la planta, así como la toma de decisiones, tanto gerenciales como operativas.

- Los beneficios obtenidos en el proceso justifican la inversión en un sistema SCADA. Estos beneficios pueden reflejarse como aumento de la efectividad de la producción, de los niveles de seguridad, etc.
- La complejidad y velocidad del proceso permiten que la mayoría de las acciones de control sean iniciadas por un operador. En caso contrario, se requerirá de un Sistema de Control Automático, el cual lo puede constituir un Sistema de Control Distribuido, PLC's, Controladores a Lazo Cerrado o una combinación de ellos.

Funciones

Dentro de las funciones básicas realizadas por un sistema SCADA están las siguientes:

- Recabar, almacenar y mostrar información, en forma continua y confiable, correspondiente a la señalización de campo: estados de dispositivos, mediciones, alarmas, etc.
- Ejecutar acciones de control iniciadas por el operador, tales como: abrir o cerrar válvulas, arrancar o parar bombas, etc.
- Alertar al operador de cambios detectados en la planta, tanto aquellos que no se consideren normales (alarmas) como cambios que se produzcan en la operación diaria de la planta (eventos). Estos cambios son almacenados en el sistema para su posterior análisis.
- Aplicaciones en general, basadas en la información obtenida por el sistema, tales como: reportes, gráficos de tendencia, historia de variables, cálculos, predicciones, detección de fugas, etc.

ANEXO E

PARA TENER EN CUENTA EN LA IMPLEMENTACIÓN DE SEGURIDAD

IMPLEMENTACIÓN DE SEGURIDAD

Diferentes Tipos de Firewalls (Casos de Estudio)

Así como ha sucedido con algunos tipos de equipos de red, el firewall ha tenido su propia evolución acorde a la creciente necesidad en todos los aspectos de seguridad en redes.

Firewall 1

Quizás el firewall mas utilizado actualmente en Internet es FireWall-1, desarrollado por la empresa israeli Check Point Software Technologies Ltd. (http://www.checkpoint.com/). Este firewall se ejecuta sobre diferentes sistemas Unix (Solaris, AIX, Linux y HP-UX), asi como sobre Windows NT y tambien en `cajas negras' como las desarrolladas por Nokia, que poseen un sistema operativo propio (IPSO) basado en FreeBSD. su caracteristica mas importante es que incorpora una nueva arquitectura dentro del mundo de los firewalls: la inspeccion con estado (stateful inspection). Firewall-1 inserta un modulo denominado *Inspection Module* en el nucleo del sistema operativo sobre el que se instala, en el nivel software mas bajo posible (por debajo incluso del nivel de red), tal como se muestra en la figura 1; asi, desde ese nivel tan bajo, Firewall-1 puede interceptar y analizar todos los paquetes antes de que lleguen al resto del sistema: se garantiza que ningun paquete es procesado por ninguno de los protocolos superiores hasta que Firewall-1 comprueba que no viola la politica de seguridad definida en el mismo.

Firewall-1 es capaz de analizar la informacion de una trama en cada uno de los siete niveles OSI y a la vez analizar informacion de estado registrada de anteriores comunicaciones; el firewall entiende la estructura de los diferentes protocolos tcp/ip (incluso de los ubicados en la capa de aplicación), de forma que el *Inspection Module* extrae la informacion relevante de cada paquete

para construir tablas dinamicas que se actualizan constantemente, tablas que el firewall utiliza para analizar comunicaciones posteriores. En el modulo de inspeccion se implantan las politicas de seguridad definidas en cada empresa mediante un sencillo lenguaje denominado inspect, tambien dise~nado por *Check Point Software Technologies*; desde un interfaz amigable se genera un script en este lenguaje, que se compila y se inserta en el *Inspection Module*.

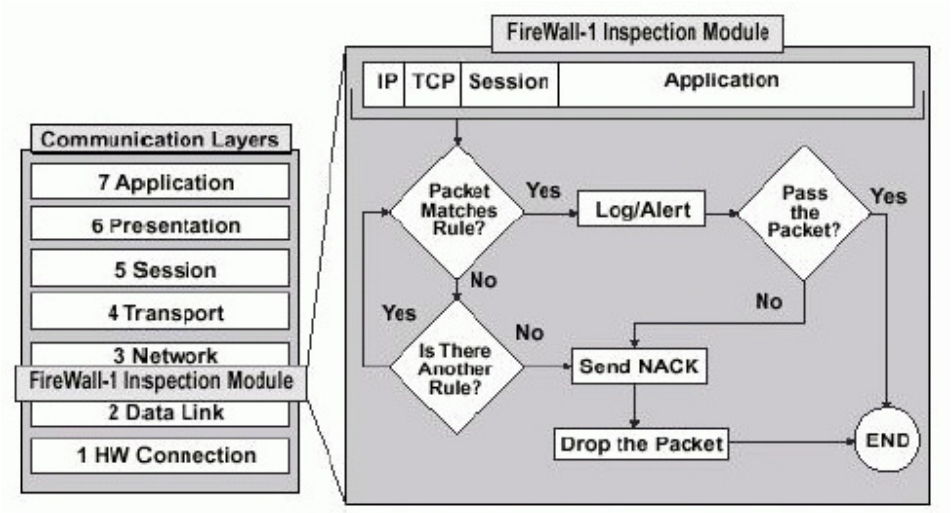


Figura 1. Ubicación del *Inspection Module* Dentro de las Capas del Modelo OSI

Ipfwadm/Ipchains/Iptables

Originalmente en 1994, ipfwadm era la herramienta proporcionada con Linux para la implementacion de politicas de filtrado de paquetes en este clon de Unix; derivaba del codigo de filtrado en BSD (ipfw), y debido a sus limitaciones (por ejemplo, solo puede manejar los protocolos TCP, UDP o ICMP) ipfwadm fue reescrito para convertirse en ipchains a partir del nucleo 2.1.102 (en 1998). Esta nueva herramienta (realmente, todo el subsistema de filtrado de los nucleos 2.2) introdujo bastantes mejoras con respecto a la anterior, pero seguia careciendo de algo fundamental: el estado lleno; era dificil ver a un sistema tan potente como Linux sin una

herramienta de de firewall decente, libre, y `de serie' con el sistema, mientras otros clones de Unix, tambien gratuitos hacia tiempo que la incorporaban, como es el caso de FreeBSD e IPFilter.

IPFilter

IP Filter para muchos clones de Unix (Solaris, IRIX, FreeBSD, NetBSD, HP-UX. . .); su precio (se trata de 16.3. IPFILTER 277 un software gratuito) y sus excelentes caracteristicas tecnicas lo han convertido en una solucion muy interesante para entornos medios donde otros firewalls como Firewall 1 no resultan apropiados por diferentes razones: incluso en Solaris puede ser en muchos casos una alternativa mas interesante que SunScreen Lite, de la propia Sun Microsystems.

Este firewalls permite filtrar el trafico en funcion de diferentes campos de la cabecera IP de una trama, como las clases de seguridad, las direcciones origen y destino y el protocolo o diferentes bits de estado. Ademas es posible utilizarlo como redirector de trafico para configurar proxies transparentes, efectuar NAT e IP Accounting, y ofrece tambien mecanismos de comunicación con el espacio de usuario.

PIX Firewall

PIX (Private Internet eXchange) es una de las soluciones de seguridad ofrecidas por Cisco Systems; se trata de un firewall completamente hardware: a diferencia de otros sistemas firewalls, PIX no se ejecuta en una maquina Unix, sino que incluye un sistema operativo empotrado denominado *Finesse* que desde espacio de usuario se asemeja mas a un router que a un sistema Unix clasico.

El firewall PIX utiliza un algoritmo de proteccion denominado Adaptive Security Algorithm (ASA): a cualquier paquete hacia el interior (generalmente, los provenientes de redes externas que tienen como origen una red protegida) se le aplica este algoritmo antes de dejarles atravesar el firewall, aparte de realizar comprobaciones contra la informacion de estado de la conexion en memoria;

para ello, a cada interfaz del firewall se le asigna un nivel de seguridad comprendido entre 0 (el interfaz menos seguro, externo) y 100 (el mas seguro, interno). La filosofia de funcionamiento del Adaptive Security Algorithm se basa en estas reglas:

→ Ningun paquete puede atravesar el firewall sin tener conexion y estado.

→ Cualquier conexion cuyo origen tiene un nivel de seguridad mayor que el destino,es permitida si no se prohibe explicitamente mediante listas de acceso.

→ Cualquier conexion que tiene como origen una interfaz o red de menor seguridad que su destino es denegada, si no se permite explicitamente mediante listas de acceso.

→ Los paquetes icmp son detenidos a no ser que se habilite su trafico explicitamente.

→ Cualquier intento de violacion de las reglas anteriores es detenido, y un mensaje de alerta es enviado a syslog.

Cuando a un interfaz del firewall llega un paquete proveniente de una red con menor nivel de seguridad que su destino, el firewall le aplica el ASA para verificar que se trata de una trama valida, y en caso de que lo sea comprobar si del host origen se ha establecido una conexion con anterioridad; si no habia una conexion previa, el firewall PIX crea una nueva entrada en su tabla de estados en la que se incluyen los datos necesarios para identificar a la conexion.

Fichero de Importancia en la Seguridad de una Red

se encuentra el fichero inetd, como el mas importante al momento de hacer configuración de politicas que involucren la seguridad de redes, por tanto se da una descripción detallada de su funcionalidad y algunas formas en las que se puede implementar.

Fichero /etc/inetd.conf

Este fichero es el utilizado por el demonio inetd, conocido como el superservidor de red. El demonio inetd es el encargado de ofrecer la mayoria de servicios de un equipo hacia el resto de maquinas, y por tanto se debe cuidar mucho su correctaconfiguracion.

Cada linea (excepto las que comienzan por `#', que son tratadas como comentarios) del archivo /etc/inetd.conf le indica a inetd como se ha de comportar cuando recibe una peticion en cierto puerto; en cada una de ellas existen al menos seis campos (en algunos clones de Unix pueden ser mas, cuyo significado es el siguiente:

Servicio

Este campo indica el nombre del servicio asociado a la linea correspondiente de /etc/inetd.conf; el nombre ha de existir en /etc/services para ser considerado correcto, o en /etc/rpc si se trata de servicios basados en el RPC (Remote Procedure Call) de Sun Microsystems. En este _ultimo caso se ha de acompañar el nombre del servicio con el numero de version RPC, separando ambos con el car_acter `/'.

Socket

Aqui se indica el tipo de socket asociado a la conexion. Aunque dependiendo del clon de Unix utilizado existen una serie de identificadores validos, lo normal es que asociado al protocolo tcp se utilicen sockets de tipo stream, mientras que si el protocolo es udp el tipo del socket sea dgram (datagrama).

Protocolo

El protocolo debe ser un protocolo definido en /etc/protocols, generalmente tcp o udp. Si se trata de servicios RPC, de nuevo hay que indicarlo utilizando rpc antes del nombre del protocolo,

separado de el por el caracter `/' al igual que suceda con el nombre; por ejemplo, en este caso se podria tener protocolos como rpc/tcp o rpc/udp.

Concurrencia

El campo de concurrencia solamente es aplicable a sockets de tipo datagrama (dgram); el resto de tipos han de contener una entrada nowait en este campo. Si el servidor que ha de atender la peticion es multihilo (es decir, puede atender varias peticiones simultaneamente), se debe indicar al sistema de red que libere el socket asociado a una conexion de forma que inetd pueda seguir aceptando peticiones en dicho socket; en este caso se utiliza la opcion nowait. Si por el contrario se trata de un servidor unihilo (acepta peticiones de forma secuencial, hasta que no analiza con una no puede escuchar la siguiente) se especifica wait. Especificar correctamente el modelo de concurrencia a seguir en un determinado servicio es importante para nuestra seguridad, especialmente para prevenir ataques de negacion de servicio (DoS). Si se especifica wait, inetd no se podria atender una peticion hasta que no analice el servicio de la actual, por lo que si este servicio es muy costoso la segunda peticion no seria servida en un tiempo razonable (o incluso nunca, si inetd se queda bloqueado por cualquier motivo). Si por el contrario se especifica nowait, el numero de conexiones simultaneas quizas llegue a ser lo sufcientemente grande como para degradar las prestaciones del sistema, lo que por supuesto no es conveniente para nosotros. Para evitar ataques de este estilo, la mayoria de sistemas Unix actuales permiten especificar (junto a wait o nowait, separado de el por un punto) el numero maximo de peticiones a un servicio durante un intervalo de tiempo (generalmente un minuto), de forma que si este numero se sobrepasa inetd asume que alguien esta intentando una negacion de servicio contra el, por lo que deja de ofrecer ese servicio durante cierto tiempo. Como evidentemente esto tambien es una negacion de servicio,

algo muy comun entre administradores es aprovechar las facilidades de planificacion de Unix para enviar cada poco tiempo la señal sighup al demonio inetd, de forma que este relea su fichero de configuracion y vuelva a funcionar normalmente. Por ejemplo, para conseguir esto se puede añadir al fichero crontab una linea como la siguiente:

```
00,10,20,30,40,50 * * * *        pkill -HUP inetd
```

Con esto se consigue que inetd se reconfigure cada diez minutos.

Usuario

En este campo se ha de indicar el nombre de usuario bajo cuya identidad se ha de ejecutar el programa que atiende cada servicio; esto es asi para poder lanzar servidores sin que posean los privilegios del root, con lo que un posible error en su funcionamiento no tenga consecuencias excesivamente graves. Para el grupo, se asume el grupo primario del usuario especificado, aunque se puede indicar un grupo diferente indicandolo junto al nombre, separado de este por un punto.

Programa

Por ultimo, en cada linea de /etc/inetd.conf se ha de indicar la ruta del programa encargado de servir cada peticion que inetd recibe en un puerto determinado, junto a los argumentos de dicho programa. El servidor inetd es capaz de ofrecer pequeños servicios basado en tcp por si mismo, sin necesidad de invocar a otros programas; ejemplos de este tipo de servicios son time, echo o chargen. En este caso, el valor de este campo ha de ser *internal*. De esta forma, si en /etc/inetd.conf se tiene una linea como telnet stream tcp nowait root /usr/sbin/in.telnetd entonces inetd sabe que cuando reciba una peticion al puerto telnet ha de abrir un socket tipo stream (el habitual para el protocolo tcp) y ejecutar fork() y exec() del programa /usr/sbin/in.telnetd, bajo la identidad de root.

Comandos de Orden para Configuración de Sistemas de Red

La Orden Ifconfig

La orden ifconfig se utiliza para configurar correctamente los interfaces de red de sistemas comunes como por ejemplo, Unix; habitualmente con ifconfig se indican parametros como la direccion ip de la maquina, la maascara de la red local o la direccion de broadcast. Si como parametros se recibe unicamente un nombre de dispositivo, ifconfig nos muestra su configuracion en este momento:

```
anita:/# ifconfig nei0
nei0:  flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>  mtu
1500
inet 192.168.0.3 netmask ffffff00 broadcast 192.168.0.255
ether 0:20:18:72:45:ad
anita:/#
```

se puede utilizar ifconfig para detectar un funcionamiento anomalo de la tarjeta de red; este `funcionamiento anomalo' suele ser la causa (siempre en cuanto a seguridad se trata) de uno de los tres siguientes problemas:

Dirección Ip Incorrecta

Es posible que alguien este realizando un ataque de tipo IP Spoofing utilizando nuestro sistema: si utilizamos la direccion ip de otro equipo, las peticiones que iran a el van a llegar a nosotros2. Estamos suplantando su identidad, hecho que un atacante puede aprovechar para capturar todo tipo de informacion (desde claves hasta correo electronico).

Dirección Mac Incorrecta

Esto puede denotar un ataque similar al anterior, pero mas elaborado: se esta suplantando la identidad de otro equipo no solo a nivel de ip, sino a nivel de direccion mac. Cuando esto sucede, casi con toda seguridad se acompaña de un IP Spoof para conseguir una suplantacion que no sea tan facil de detectar como el IP Spoof a secas.

Tarjeta en Modo Promiscuo

Alguien ha instalado un sniffer en nuestro sistema y ha puesto la tarjeta de red en modo promiscuo, para capturar todas las tramas que esta `ve'. Es un metodo muy utilizado por atacantes que han conseguido privilegio de superusuario en la maquina (es necesario ser root para situar a la tarjeta en este modo de operacion) y se esta dedicando a analizar el trafico de la red en busca de logins y claves de usuarios de otros equipos.

La Orden Route

Este comando se utiliza para configurar las tablas de rutado del nucleo de nuestro sistema. Generalmente en todo equipo de una red local se tiene al menos tres rutas: la de loopback,

utilizando el dispositivo de bucle interno (lo, lo0...), la de red local (localnet), que utiliza la tarjeta de red para comunicarse con equipos dentro del mismo segmento de red, y una default que tambien utiliza la tarjeta para enviar a un router o gateway paquetes que no son para equipos de nuestro segmento. Si no se especica ningun parametro, route muestra la configuracion actual de las tablas de rutado3:

Si route nos muestra una configuracion sospechosa (esto es, las tablas no son las que en el sistema hemos establecido como administradores, aunque todo funcione correctamente) esto puede denotar un ataque de simulacion: alguien ha desviado el trafico por un equipo que se comporta de la misma forma que se comportara el original, pero que seguramente analiza toda la informacion que pasa por el. Hemos de recalcar que esto suele ser transparente al buen funcionamiento del equipo (no notamos ni perdida de paquetes, ni retardos excesivos, ni nada sospechoso), y que ademas el atacante puede modificar los ficheros de arranque del sistema para, en caso de reinicio de la maquina, volver a tener configuradas las rutas a su gusto; estos ficheros suelen ser del tipo /etc/rc.d/rc.inet1 o /etc/rc?.d/S_inet.

Tambien es posible que alguien este utilizando algun elemento utilizado en la conexion entre nuestro sistema y otro (un router, una pasarela. . .) para amenazar la integridad de nuestro equipo; si queremos comprobar el camino que siguen los paquetes desde que salen de la maquina hasta que llegan al destino, podemos utilizar la orden traceroute. Sin embargo, este tipo de ataques es mucho mas dificil de detectar, y casi la unica herramienta asequible para evitarlos es la criptografia.

La Orden Netstat

Esta orden se utiliza para visualizar el estado de diversas estructuras de datos del sistema de red, desde las tablas de rutado hasta el estado de todas las conexiones a y desde nuestra maquina, pasando por las tablas arp, en funcion de los parametros que reciba. En lo referente a la seguridad, netstat se suele utilizar, aparte de para mostrar las tablas de rutado de ciertos sistemas (con la opcion -r), para mostrar los puertos abiertos que escuchan peticiones de red y para visualizar conexiones a nuestro equipo (o desde el) que puedan salirse de lo habitual. El siguiente es un ejemplo de informacion mostrada por netstat:

```
anita:/# netstat -P tcp -f inet -a
TCP
   Local Address         Remote Address     Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
      *.*                  *.*                0      0      0      0 IDLE
      *.sunrpc             *.*                0      0      0      0 LISTEN
      *.*                  *.*                0      0      0      0 IDLE
      *.32771              *.*                0      0      0      0 LISTEN
      *.ftp                *.*                0      0      0      0 LISTEN
      *.telnet             *.*                0      0      0      0 LISTEN
      *.finger             *.*                0      0      0      0 LISTEN
      *.dtspc              *.*                0      0      0      0 LISTEN
      *.lockd              *.*                0      0      0      0 LISTEN
      *.smtp               *.*                0      0      0      0 LISTEN
      *.8888               *.*                0      0      0      0 LISTEN
      *.32772              *.*                0      0      0      0 LISTEN
      *.32773              *.*                0      0      0      0 LISTEN
      *.printer            *.*                0      0      0      0 LISTEN
      *.listen             *.*                0      0      0      0 LISTEN
      *.32774              *.*                0      0      0      0 LISTEN
      *.*                  *.*                0      0      0      0 IDLE
      *.6000               *.*                0      0      0      0 LISTEN
      *.32775              *.*                0      0      0      0 LISTEN
localhost.32777      localhost.32775      32768      0 32768      0 ESTABLISHED
localhost.32775      localhost.32777      32768      0 32768      0 ESTABLISHED
localhost.32780      localhost.32779      32768      0 32768      0 ESTABLISHED
localhost.32779      localhost.32780      32768      0 32768      0 ESTABLISHED
localhost.32783      localhost.32775      32768      0 32768      0 ESTABLISHED
localhost.32775      localhost.32783      32768      0 32768      0 ESTABLISHED
localhost.32786      localhost.32785      32768      0 32768      0 ESTABLISHED
localhost.32785      localhost.32786      32768      0 32768      0 ESTABLISHED
localhost.32789      localhost.32775      32768      0 32768      0 ESTABLISHED
localhost.32775      localhost.32789      32768      0 32768      0 ESTABLISHED
localhost.32792      localhost.32791      32768      0 32768      0 ESTABLISHED
localhost.32791      localhost.32792      32768      0 32768      0 ESTABLISHED
localhost.32810      localhost.6000       32768      0 32768      0 ESTABLISHED
localhost.6000       localhost.32810      32768      0 32768      0 ESTABLISHED
anita.telnet         luisa.2039           16060      0 10136      0 ESTABLISHED
anita.telnet         bgates.microsoft.com.1068 15928 0 10136      0 ESTABLISHED
localhost.32879      localhost.32775      32768      0 32768      0 TIME_WAIT
      *.*                  *.*                0      0      0      0 IDLE
anita:/#
```

Por un lado, en este caso se observa que hay bastantes puertos abiertos, esto es, escuchando peticiones: todos los que presentan un estado listen, como telnet, finger o smtp (si es un servicio con nombre en /etc/services se imprimira este nombre, y si no simplemente el numero de puerto).

Cualquiera puede conectar a este servicio y, si no se puede evitar mediante TCP Wrappers, utilizandolo para enviarle peticiones. Aparte de estos puertos a la espera de conexiones, tambien se observa otro gran numero de conexiones establecidas entre nuestro sistema y otros; casi todas las establecidas (estado established) son de nuestra maquina contra ella misma, lo que a priori no implica consecuencias de seguridad. Otra de ellas es desde un equipo de la red local contra nuestro sistema, lo que tambien es bastante normal y no debe hacernos sospechar nada; sin embargo, hay una conexion que si puede indicar que alguien ha accedido a nuestro sistema de forma no autorizada: si nos fijamos, alguien conecta por telnet desde la maquina *bgates.microsoft.com.*
Es raro que tengamos a un usuario alli, por lo que se debe monitorizar esta conexion y las actividades que esta persona realice; es muy probable que se trate de alguien que ha aprovechado la inseguridad de ciertos sistemas para utilizarlos como plataforma de ataque contra nuestros Unix.

La Orden Ping

El comando ping se utiliza generalmente para testear aspectos de la red, como comprobar que un sistema esta encendido y conectado; esto se consigue enviando a dicha maquina paquetes icmp (de tipo echo request), tramas que causaran que el nucleo del sistema remoto responda con

```
anita:~# ping luisa
luisa is alive
anita:~#
```

paquetes icmp, pero esta vez de tipo *echo response*. Al recibirlos, se asume que la maquina esta encendida:

En otras variantes de Unix (el ejemplo anterior es sobre Solaris) la orden ping produce un resultado con mas informacion:

```
luisa:~# ping -c 1 anita
PING anita (192.168.0.3): 56 data bytes
64 bytes from 192.168.0.3: icmp_seq=0 ttl=255 time=0.2 ms

--- luisa ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
luisa:~#
```

Aunque un simple ping resulta inofensivo en la mayoria de situaciones, existen casos en los que se puede utilizar como un arma (efectiva (para atacar sistemas; por ejemplo, uno de los ataques mas conocidos es el Ping Flood, consistente en saturar una linea lenta con un numero de paquetes icmp suficientemente grande. Esta saturacion causaria una degradacion del servicio importante, incluso la desconexion del sistema si se ataca una linea telefonica (un objetivo muy habitual para los piratas). En este ultimo caso, el de conexiones telefonicas, otro ataque comun (no directamente relacionado con ping, pero en el que se usa esta herramienta como base (consiste en enviar una trama `especial' a un modem, obligandole a analizar la llamada: los modems conmutan a modo comando cuando reciben la orden `+++', y muchos de ellos lo hacen tambien al recibir remotamente esta secuencia de control. Asi, podemos conectar a un puerto donde se ofrezca determinado servicio (como ftp o smtp) en un host con un modem de estas caracteristicas y colgar

el modem remoto sin levantarnos de la silla, simplemente enviando la cadena `+++' seguida de una orden de colgado como `ATH0':

```
luisa:~# telnet XXX.XXX.X.XX 21
Trying XXX.XXX.X.XX...
Connected to XXX.XXX.X.XX.
Escape character is '^]'.
220 gema FTP server (Version wu-2.4.2-academ[BETA-15](1) Fri Oct
22
00:38:20 CDT 1999) ready.
USER +++ATH0
^]
telnet> close
Connection closed.
luisa:~# telnet XXX.XXX.X.XX
Trying XXX.XXX.X.XX...
telnet: Unable to connect to remote host: Network is unreachable
luisa:~#
```

Bien pero, donde entra ping en este ataque? Muy sencillo: al conectar a un servicio para enviar la cadena de caracteres, lo habitual es que el sistema remoto registre la conexion, aunque luego su modem cuelgue. En cambio, muy pocos sistemas registran en los logs un simple ping, por lo que esta orden se convierte en un mecanismo que algunos piratas utilizan para no dejar rastro de sus acciones; esto se consigue de una forma muy sencilla: en la utilidad ping de la mayoria de Unices existe un parametro que permite especificar el contenido del paquete enviado (por ejemplo, `-p' en Linux), por lo que simplemente hemos de insertar (en hexadecimal) la cadena `+++ATH0' en la trama que enviamos al sistema remoto:

```
luisa:~# ping -c 1 XXX.XXX.X.XX
PING XXX.XXX.X.XX (XXX.XXX.X.XX): 56 data bytes
64 bytes from XXX.XXX.X.XX: icmp_seq=0 ttl=255 time=0.2 ms

--- XXX.XXX.X.XX ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 6.5/6.5/6.5 ms
luisa:~# ping -p 2b2b2b415448300d XXX.XXX.X.XX
PING XXX.XXX.X.XX (XXX.XXX.X.XX): 56 data bytes

^C
--- XXX.XXX.X.XX ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
luisa:~# telnet XXX.XXX.X.XX
Trying XXX.XXX.X.XX...
telnet: Unable to connect to remote host: Network is unreachable
luisa:~#
```

Para evitar los problemas relacionados con los paquetes icmp que sistemas remotos puedan enviar a nuestra maquina puede ser conveniente filtrar dicho protocolo mediante un firewall (incluso situado en el propio equipo); si no se tiene esta posibilidad, al menos es interesante registrar las tramas de este tipo que llegan hasta nuestra maquina, con programas como icmpinfo (si hacemos esto, hemos de tener cuidado con las negaciones de servicio ocasionadas por una cantidad de logs excesiva en el disco duro). si es el modem el que presenta el problema anterior, se puede solucionar mediante la cadena de inicializacion `s2=255'.

La Orden Traceroute

Esta orden se utiliza para imprimir la ruta que los paquetes siguen desde nuestro sistema hasta otra maquina; para ello utiliza el campo ttl (Time To Live) del protocolo ip, inicializandolo con valores bajos y aumentandolo conforme va recibiendo tramas icmp de tipo time exceeded. La idea es sencilla: cada vez que un paquete pasa por un router o una pasarela, esta se encarga de decrementar el campo ttl en una unidad; en el caso de que se alcance un valor 0, se devuelve un paquete time exceeded y se descarta la trama. Asi, traceroute inicializa a 1 este campo, lo que ocasiona que el primer router encontrado ya devuelva el mensaje de error; al recibirlo, lo inicializa a 2, y ahora es el segundo router el que descarta el paquete y envia otro mensaje de error, y asi sucesivamente. De esta forma se va construyendo la ruta hasta un determinado host remoto:

```
luisa:~# traceroute www.altavista.com
traceroute to altavista.com (204.152.190.70), 30 hops max, 40 byte
packets
1 annex4.net.upv.es (158.42.240.191) 156.251 ms 144.468 ms 139.855 ms
2 zaurac-r.net.upv.es (158.42.240.250) 159.784 ms 149.734 ms 149.809
ms
3 atlas.cc.upv.es (158.42.1.10) 149.881 ms 149.717 ms 139.853 ms
4 A1-0-3.EB-Valencia1.red.rediris.es (130.206.211.185) 149.863 ms
150.088 ms 149.523 ms
5 A0-1-2.EB-Madrid00.red.rediris.es (130.206.224.5) 189.749 ms
159.698 ms 180.138 ms
13.4. SERVICIOS 225
```

traceroute se utiliza para realizar pruebas, medidas y administracion de una red; introduce mucha sobrecarga, lo que evidentemente puede acarrear problemas de rendimiento, llegando incluso a negaciones de servicio por el elevado tiempo de respuesta que el resto de aplicaciones de red pueden presentar. Ademas, se trata de un programa contenido en un fichero *setuidado*, por lo que es interesante resetear el bit de setuid de forma que solo el root pueda ejecutar la orden: se ha de pensar que un usuario normal rara vez tiene que realizar pruebas sobre la red, por lo que el bit setuid de traceroute no es mas que un posible problema para la seguridad; aunque con ping sucede lo mismo (es un fichero *setuidado*), que un usuario necesite ejecutar traceroute es menos habitual que necesite ejecutar ping (de cualquier forma, tambien se podria resetear el bit setuid de ping).

La Vulnerabilidad en Servicios de Red

Cada puerto abierto en un sistema de red representa una puerta de entrada al mismo, por lo que se debe minimizar el numero ofreciendo solo los servicios estrictamente necesarios. Por ejemplo, si se ofrece el servicio **telnet**, cualquier persona, desde cualquier parte del mundo, podria acceder a nuestra maquina simplemente conociendo (o adivinando) un nombre de usuario y su clave; si ofrecemos el servicio **netstat**, cualquiera podria consultar las conexiones activas de nuestra red simplemente tecleando **telnet maquina.dominio.com netstat**, desde cualquier computador conectado a la red. Pero no solo nos se tiene que limitar a cerrar servicios: hay algunos que, como administradores de un sistema, no vamos a tener mas remedio que ofrecer; en este caso es casi obligatorio restringir su disponibilidad a un numero de maquinas determinado, de aquí la necesidad de los TCP Wrappers, y por supuesto utilizar la _ultima version de los demonios encargados de procesar las peticiones: un demonio no es mas que un programa, y por supuesto es muy dificil que este completamente libre de errores. Un error en el demonio que utilicemos para procesar una peticion puede comprometer la seguridad de todo nuestro sistema, por lo que se recomienda estar atento a listas de seguridad (como bugtraq o cert) en las que se difundan problemas de seguridad y sus soluciones. A todo esto, los puertos mas comunes de monitoreo para un firewall son:

Servicio	Puerto	Protocolo	Ataque
ttymux	1	TCP	Escaneo horizontal
echo	7	TCP/UDP	Escaneo horizontal
systat	7	TCP	Escaneo horizontal
daytime	13	TCP/UDP	Escaneo horizontal
netstat	15	TCP	Escaneo horizontal
finger	79	TCP	Escaneo horizontal/vertical
who	513	UDP	Escaneo horizontal
uucp	540	TCP	Escaneo horizontal/vertical
NetBus	12345	TCP	Troyano
NetBus	12346	TCP	Troyano
NetBus	20034	TCP	Troyano
BackOrifice	31337	UDP	Troyano
Hack´a´Tack	31789	UDP	Troyano
Hack´a´Tack	31790	UDP	Troyano

Figura 2. Puntos Vulnerables de Ataques

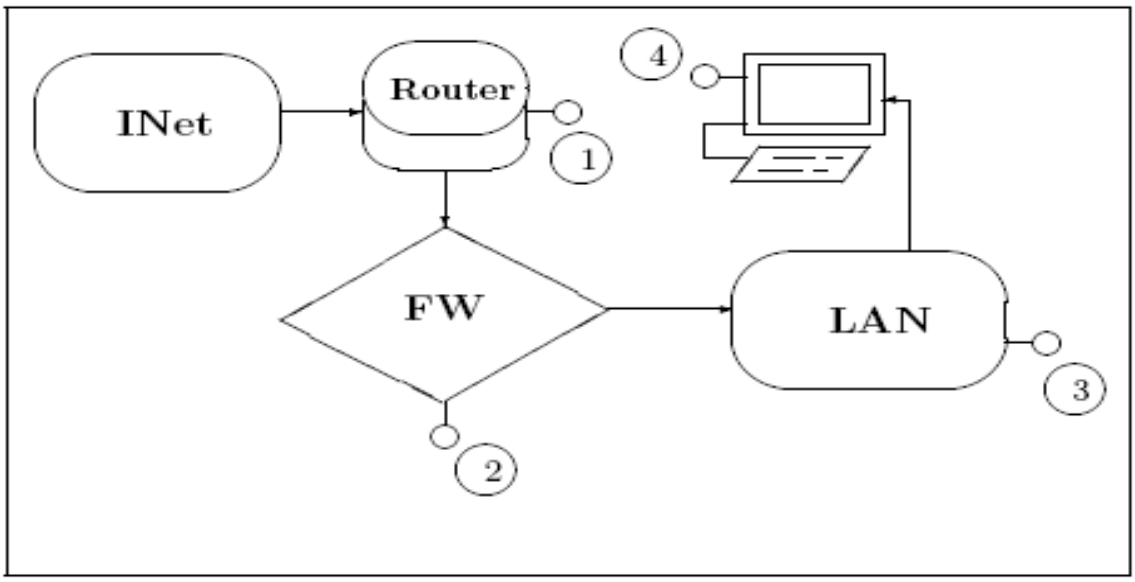


Figura 3. Puntos Clave de Ataques

PUNTOS CLASICOS DE VULNERABILIDAD DE ATAQUES

Utilizando las Herramientas TCP Wrappers Para la Seguridad de Redes

TCP Wrappers

Cualquiera de los puntos de la figura 3 es una potencial puerta de entrada para un atacante, por lo que es muy recomendable cerrar todos los que no necesitemos; realizando un esquema todo o

nada: u ofreciendo un servicio a toda la red o lo denegamos, pero no deberia haber termino medio. Hay una serie de servicios como telnet o ftp que habitualmente no vamos a poder cerrar, ya que los usuarios necesitaran conectar al servidor para trabajar en el o para transferir ficheros; en estos casos es peligroso permitir que cualquier maquina de Internet tenga la posibilidad de acceder a nuestros recursos, por lo que se suele utilizar un programa denominado **TCP Wrappers** para definir una serie de redes o maquinas autorizados a conectar con nuestra red.

Actualmente, cualquier administrador que desee un minimo de seguridad ha de instalar TCP Wrappers en sus equipos; incluso algunos Unices como Linux o BSDI lo ofrecen por defecto al instalar el operativo. Cabe decir que la configuracion del programa puede ser muy elaborada y con muchas opciones; la forma mas basica, suele ser automatica mediante make install 2. en el presente ejemplo se instala TCP Wrappers sobre una maquina Silicon Graphics corriendo IRIX 6.2:

```
llegona_(/) # uname –a
IRIX64 llegona 6.2 06101031 IP28
llegona_(/) #
```

Se da por concluida la compilacion y el resultado esta, por ejemplo, en el directorio /tmp/tcp wrappers 7.6/. Tras compilar el software se habran generado una serie de ficheros ejecutables que se han de copiar a un destino definitivo, por ejemplo a /etc/usr/sbin/:

```
llegona_(/tmp/tcp_wrappers_7.6) # cp `find . –type f –perm –700`
/usr/sbin/
llegona_(/tmp/tcp_wrappers_7.6) #
```

Una vez en su destino definitivo, se ha de modificar el fichero /etc/inetd.conf para indicarle a inetd que ha de utilizar el demonio tcpd (la parte mas importante de TCP Wrappers) a la hora de servir peticiones; para ello, una entrada de la forma:

```
telnet stream tcp nowait root /usr/etc/telnetd
```

se convertir_a en una como

```
telnet stream tcp nowait root /usr/sbin/tcpd /usr/etc/telnetd
```

Como vemos, en lugar de que inetd ejecute directamente el demonio correspondiente a cada servicio, ejecuta el wrapper, y es este el encargado de controlar la ejecucion del demonio real. Tras haber modificado convenientemente /etc/inetd.conf se ha de configurar los servicios que se van a ofrecer a diferentes maquinas o redes; siguiendo una politica restrictiva: todo lo no explicitamente permitido, esta negado. Para ello, en el archivo /etc/hosts.allow indicamos que servicios se ofrecen y a dondese hara, de la siguiente forma:

Donde `demonio' es el nombre del demonio encargado de atender el servicio correspondiente (sendmail, telnetd, fingerd. . . ), y `maquinas' es la especificacion de los hosts a los que les esta permitida la conexion a cada servicio; se trata de una lista separada por espacios donde se pueden incluir desde nombres de sistemas o direcciones IP hasta subdominios, pasando por palabras reservadas como ALL. Asi, si por ejemplo se quiere ofrecer todo a las maquinas .dsic.upv.es, telnet a andercheran.aiind.upv.es y luisvive.euiti.upv.es, y ftp a toda la UPV, se tendra un /etc/hosts.allow de la forma siguiente:

```
llegona_(/) # cat /etc/hosts.allow
ALL: .dsic.upv.es
telnetd: andercheran.aiind.upv.es luisvive.euiti.upv.es
ftpd: .upv.es
llegona_(/) #
```

se acaba de configurar los sistemas con acceso a ciertos demonios; para indicar a TCP Wrappers que los servicios no van a ser ofertados a nadie mas, creado el fichero /etc/hosts.deny y se deniega todo a todos:

```
llegona_(/) # cat /etc/hosts.deny
ALL: ALL
llegona_(/) #
```

Una vez configurado todo, se ha de hacer que inetd relea su fichero de configuración enviandole la señal sighup, por ejemplo con la orden killall -HUP inetd4. A partir de ese momento los cambios han tenido efecto; en funcion de /etc/syslog.conf, pero generalmente en archivos como /var/adm/SYSLOG o /var/adm/messages se puede ver las conexiones aceptadas y las rehusadas:

```
Dec 2 02:16:47 llegona ftpd[18234]: refused connect from
bill.microsoft.com
Dec 2 02:45:23 llegona telnetd[18234]: connect from
corbella.dsic.upv.es
```

Cuando alguien desde una maquina que tiene permiso para acceder a cierto servicio conecte a el no notara nada raro, pero si lo hace desde un equipo no autorizado, la conexion se cerrarra:

```
anita:~# telnet llegona.dsic.upv.es
Trying 158.42.49.37...
Connected to llegona.dsic.upv.es
Escape character is '^]'.
llegona login: Connection closed by foreign host.
anita:~#
```