Capítulo 2

Memoria Técnica de la Red Institucional

2.1. Objetivo

El objetivo de esta etapa del proyecto es describir de manera detallada la situación actual de la red Institucional del IEMS después de la implementación de la solución, y enunciar las recomendaciones pertinentes para que la Institución las considere como las mínimas necesarias para el mantenimiento de la solución instalada que comprende el proyecto Red Institucional del IEMS.

2.2. Situación actual de la red después de la instalación

Para las oficinas centrales, la segmentación de la red quedó organizada de la siguiente manera:

Se configuraron 5 VLANs de las cuales en la VLAN1 se encuentran los Switches, la VLAN 100 corresponde al segmento ubicado en el edificio 2 del IEMS, donde se encuentra el IDF en el área de telecomunicaciones. La VLAN 200 que comprende el edificio 1 planta baja donde se encuentra el Main Distribution Frame (MDF), la VLAN300 corresponde al edificio 1 planta alta donde el IDF se encuentra en la sala de juntas del Instituto, la VLAN400 donde se encuentra la IP del conmutador de voz sobre IP (en pruebas), y la VLAN600 donde se encuentran los Access Points para los equipos que se conectan de manera inalámbrica.

Cada VLAN corresponde a un bloque subneteado /24 de direcciones de la red 10.0.0.0/16. Se configuraron los equipos de acceso (Switches CISCO) para ser accesados de manera remota por Secure Shell (SSH) a través de la VLAN de administración (VLAN 1).

En la capa de distribución se instalaron 2 Switches interconectados a través de 10 cables lógicamente sumados a través de Etherchannel[18]. Uno de esos Switches fue configurado como servidor de VTP para mejor manejo de las VLANS en la red.

En la capa del núcleo se instalaron dos servidores en Pfsense, que sirven como servidores DHCP. Uno de ellos trabaja como servidor principal para ruteo de tráfico, el segundo sirve como backup o failover. Tienen IPs CARP[19] virtuales que permiten tener un solo Gateway para cada VLAN, y de ésta forma al entrar en funcionamiento el secundario, los equipos de la LAN sigan con el mismo Gateway y sea completamente transparente la transición.

Se instaló un Switch con varias VLANs en la WAN, afuera de la capa de núcleo de la red LAN de las oficinas centrales, esta parte de la red fue creada para tener preparada la interconexión de los planteles a ese Switch. En una VLAN de la WAN también fueron migrados los servidores que dan diversos servicios al IEMS y serán accesibles desde cualquier plantel.

En éste Switch en la VLAN 192 se instaló un infinitum de 4 Mb/s que sirve como salida a internet en caso de que el enlace principal falle, éste módem sólo se utilizará para

[18] Etherchannel es una tecnología ofrecida por los switches cisco que permite agrupar un grupo de puertos físicos en uno lógico con el propósito de proveer resilencia y mayores velocidades de transmisión.

[19] Common Address Redundancy Protocol o CARP es un protocolo que permite compartir a muchos host en un segmento de red una o varias direcciones IP. Su principal propósito es de proveer redundancia de tipo failover, especialmente cuando se usan firewalls o routers. Es un protocolo libre y no patentado, alternativo de HSRP de Cisco, e implementado en sistemas operativos BSD.

contingencias o para cualquier requerimiento especial de una conexión dedicada.

Por lo tanto las VLANs creadas en la WAN de las oficinas centrales fueron: VLAN1, VLAN1000, VLAN2000, VLAN3000 y VLAN192, el tráfico de administración se realizará a través de la VLAN1, El tráfico de datos se dirigirá por la VLAN1000, el de voz por la VLAN2000 y el tráfico de video por la VLAN3000, la salida por el infinitum será por la VLAN192.

En la punta de la WAN y como salida a internet se instaló un Firewall en Pfsense, dicho firewall permite la salida de la VLAN1 y VLAN1000 hacia internet realizando PAT. El tráfico con destino al puerto 80 primero se reenvía hacia el puerto 8080 del servidor de filtrado que se encuentra en la WAN (ver más de filtrado web en sección "Filtrado Web con DansGuardian").

El tráfico de las VLAN2000, y VLAN3000 es aquel generado por equipos de voz y video, y no tiene acceso a los servidores excepto al correspondiente del servicio. Ni tampoco cuenta con salida a internet.

El tráfico de la VLAN2000 y VLAN3000 se encuentran en éste momento en desuso ya que no existe en éste momento teléfonos IP ni equipos de videoconferencia en el Instituto.

Se encuentran bloqueados sitios por contenido, sobre todo sitios que impactan el ancho de banda de la red: páginas de videos, descargas, etc. Así como sitios que comprometen la seguridad de la red: pornografía, warez, cracks, etc. Éste esquema se explica de mejor manera en la sección "Filtrado Web con DansGuardian"

2.3. Diagramas de Interconexión en Oficinas Centrales

2.3.1. Físico de la red LAN de las Oficinas Centrales

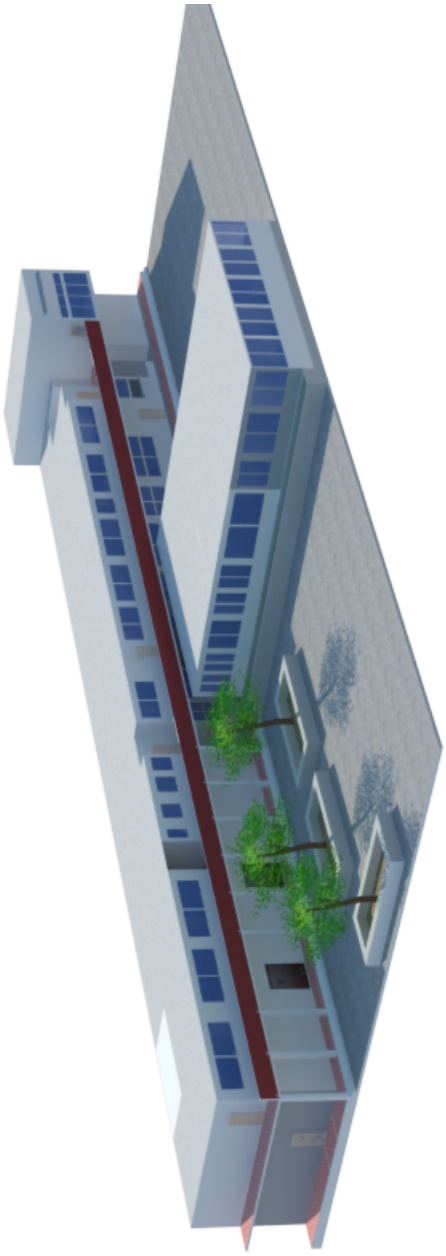

Figura 2.1: Modelo 3D de las oficinas centrales - San Lorenzo

Figura 2.2: Modelo 3D de las Oficinas centrales - San Lorenzo. Mostrando la ubicación de los cuartos de telecomunicaciones.

2.3.2. Lógico de la red LAN de las Oficinas Centrales

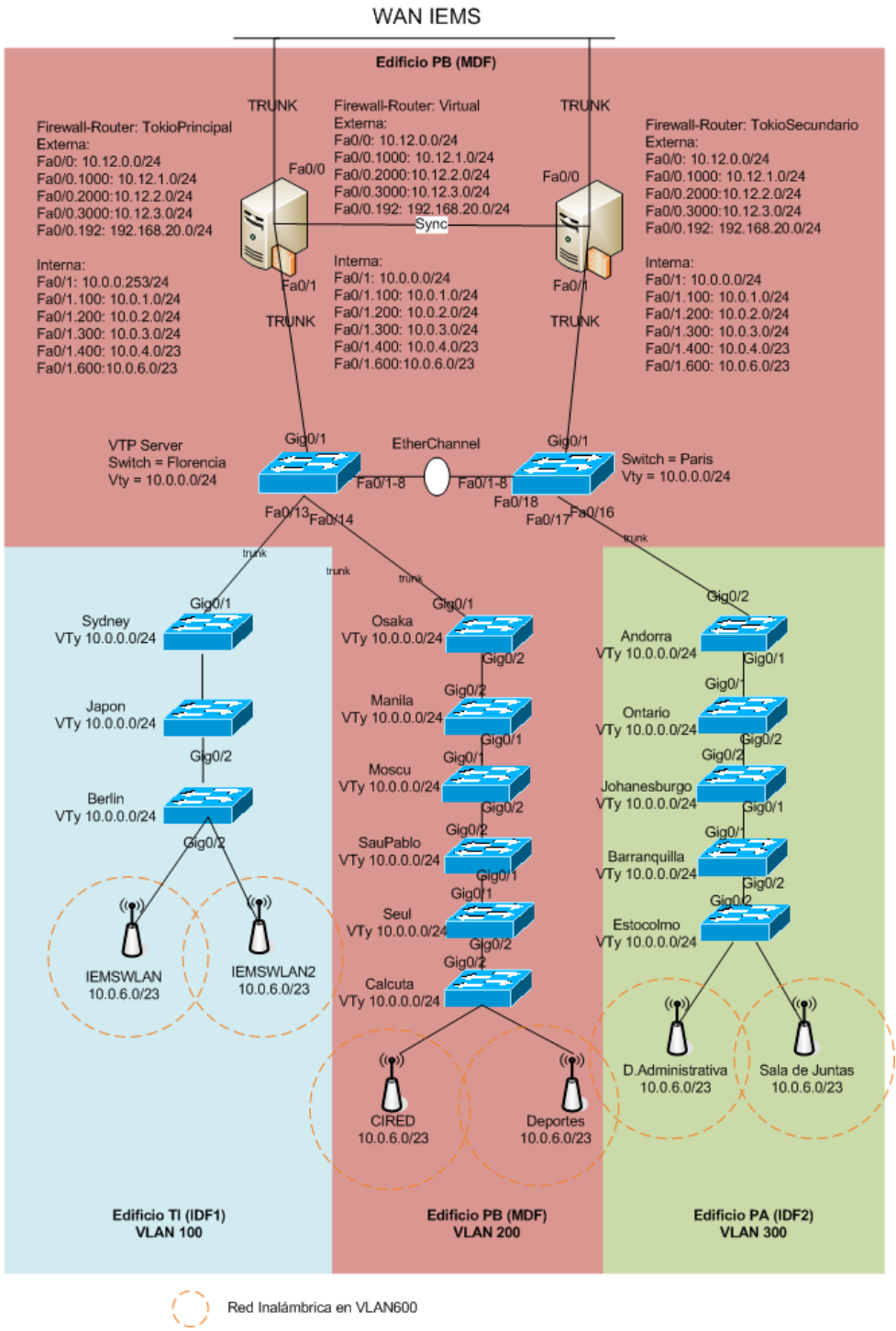

Figura 2.3: Topología lógica actual de la red LAN de las oficinas centrales de San Lorenzo

2.3.3. Lógico de la red WAN actual en las Oficinas Centrales

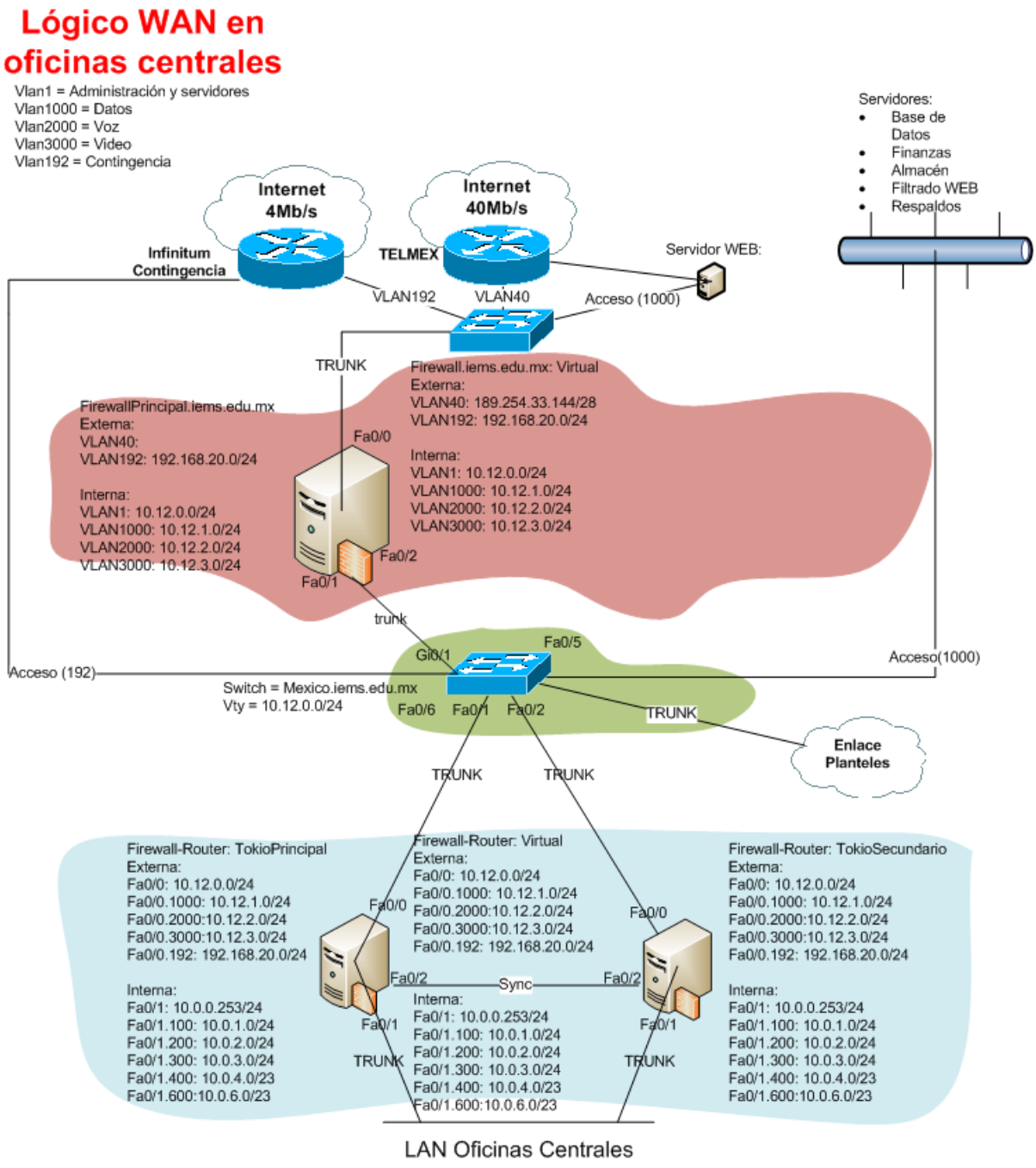

Figura 2.4: Topología lógica de la red WAN actual de las oficinas centrales de San Lorenzo.

2.3.4. Diagrama lógico de la red LAN actual de los planteles

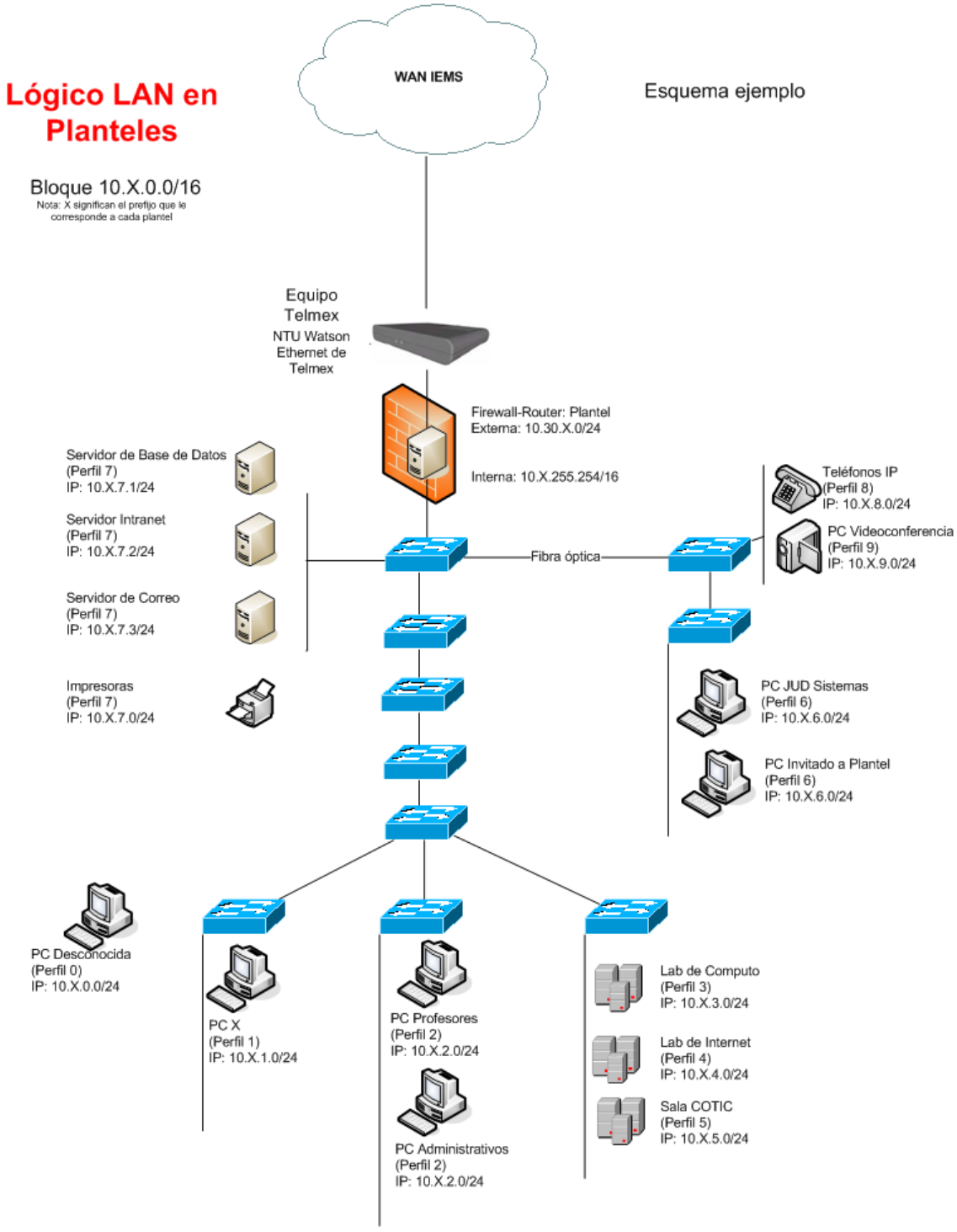

Figura 2.5: Diagrama lógico de la red LAN actual en los planteles

2.3.5. Diagrama lógico de la Red Institucional

En la figura siguiente se presentan todos los enlaces que se tendrán hacia los planteles, sin embargo en la figura a la fecha de creación de éste documento sólo se encuentran en funcionamiento los planteles definidos en la sección "Planteles ya en funcionamiento".

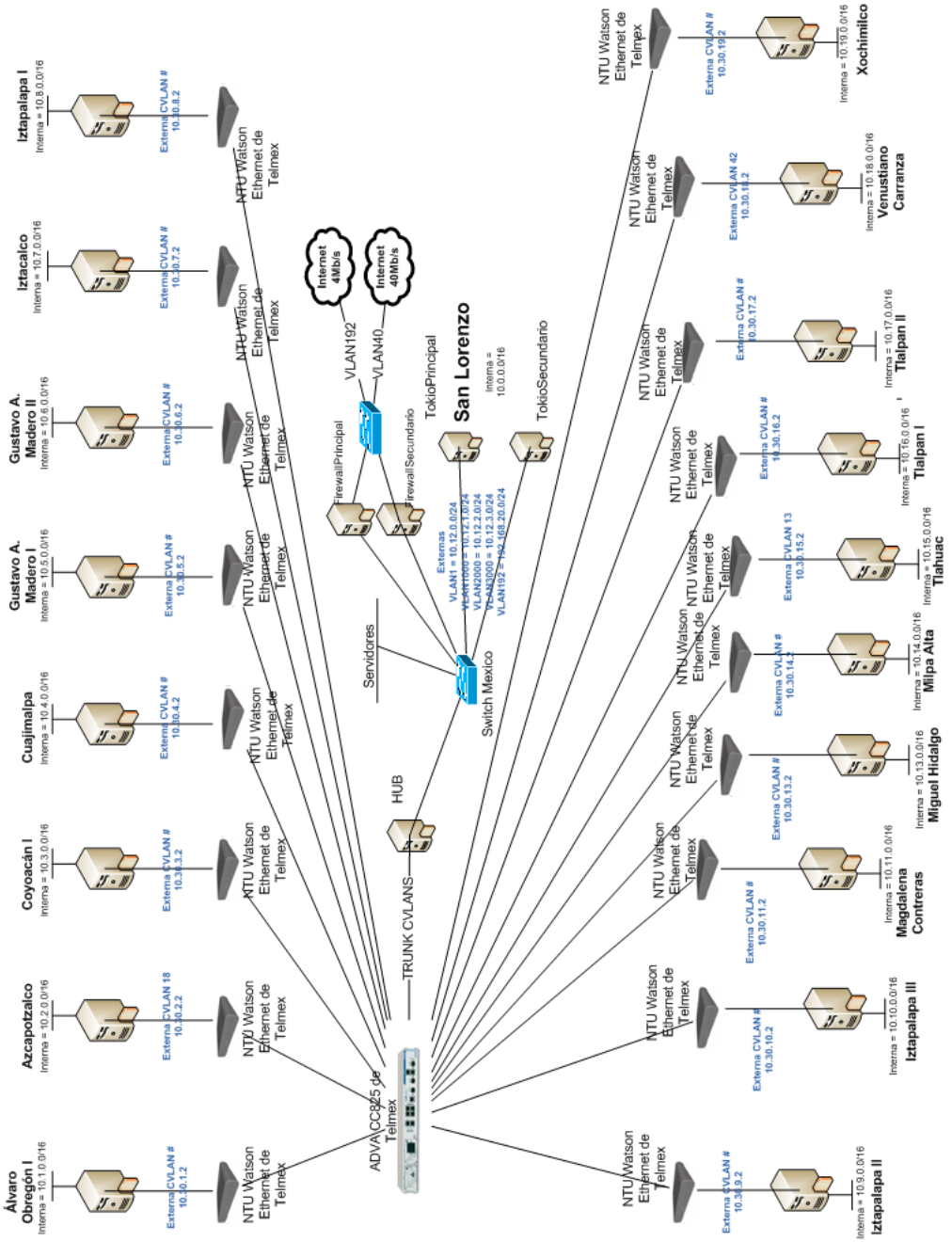

Figura 2.6: Diagrama lógico de la red WAN Institucional, aún en proceso de implementación

2.4. Listado de equipos en oficinas centrales

2.4.1. Propietarios de Telmex

Equipo	Marca	Modelo	Ubicación Física
Módem ADSL	2Wire	2701HG-T Gateway	MDF
Modem ADSL	2WIRE	2701HG-T Gateway	MDF
Router	Cisco	C3825-IPBASEK9-M	MDF
Modem	ADVA	CC825	MDF

Cuadro 2.1: Nuevo listado de equipos en oficinas centrales. Propietarios de Telmex

2.4.2. Propietarios del IEMS

2.4.2.1. Edificio 1 Planta Baja.

Equipo	Marca	Modelo	Hostname	Ubicación Física
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Mexico	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Florencia	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Paris	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	SaoPaulo	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Seul	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Osaka	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Manila	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Moscu	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Calcuta	MDF
Access Point	Linksys	WRT320N	CIRED	Deportes
Access Point	Linksys	WRT320N	DEPORTES	Deportes

Cuadro 2.2: Nuevo listado de equipos propietarios del IEMS. Edificio 1 Planta Baja.

2.4.2.2. Edificio 1 Planta Alta.

Equipo	Marca	Modelo	Hostname	Ubicación Física
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Andorra	IDF2
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Ontario	IDF2
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Johanesburgo	IDF2
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Barranquilla	IDF2
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Estocolmo	IDF2
Access Point	Linksys	WRT54G	D.Administrativa	Dirección Administrativa
Access Point	Linksys	WRT54G	$Saladejuntas_{WLAN}$	Sala de Juntas

Cuadro 2.3: Nuevo listado de equipos propietarios del IEMS. Edificio 1 Planta Alta.

2.4.2.3. Edificio 2.

Equipo	Marca	Modelo	Hostname	Ubicación Física
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Andorra	IDF2
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Ontario	IDF2
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Johanesburgo	IDF2
Access Point	Linksys	WRT54G	IEMSWLAN	Telecomunicaciones
Access Point	Linksys	WRT54G2 V1	IEMSWLAN2	Dirección Innovación

Cuadro 2.4: Nuevo listado de equipos propietarios del IEMS. Edificio 2.

2.4.2.4. Servidores.

Equipo	Marca	Modelo	Servicio	Versión de Software	Ubicación Física
Servidor	DELL	-	Web Principal	Debian GNU/Linux 5.0	MDF
Servidor	LANIX	BRAIN	Web DIT	Debian GNU/Linux 5.0	MDF
Servidor	DELL	-	Filtrado Web	Ubuntu Server 10	MDF
Servidor	DELL	POWEREDGE 2900	Firewall Principal	Pfsense 2.0	MDF
Servidor	DELL	-	TokioPrincipal	Pfsense 2.0	MDF
Servidor	DELL	-	TokioSecundario	Pfsense 2.0	MDF
Servidor	DELL	-	Base de datos general	CentOS Release 5.3 (final)	MDF
Servidor	LANIX	BRAIN	Base de datos almacén	RedHat Enterprise Linux ES Release 3 (Taron)	MDF
Servidor	COMPAQ	EVO	VPN Finanzas	Mandraque Linux Release 9.2 (FiveStar) four I586	MDF
Servidor	DELL	OPTIPLEX GX 620	Web de Servidor 7	CentOS Release 5.3 (final)	MDF
Servidor	DELL	OPTIPLEX GX 280	VPN de Finanzas2	Microsoft Windows XP Profesional Service Pack 2	MDF
Servidor	DELL	-	Hub receptor de planteles	Pfsense 2.0	MDF

Cuadro 2.5: Nuevo listado de equipos propietarios del IEMS. Área de Servidores.

2.5. Avance de Actividades

A continuación se presenta un diagrama que indica las tareas definidas y el porcentaje de avance:

Figura 2.7: Avance de tareas

Actividad	Porcentaje de avance
Separación de Servicios en oficinas centrales - San Lorenzo.	100 %
Segmentación de la Red de las oficinas centrales - San Lorenzo.	100 %
Implementación de Esquema de Seguridad en oficinas centrales - San Lorenzo.	100 %
Creación de segmento WAN en oficinas centrales - San Lorenzo.	100 %
Configuración de salida a internet de 40Mb/s - San Lorenzo.	100 %
Instalación de ADSL en WAN Oficinas Centrales para contingencias. - San Lorenzo	100 %
Generación de políticas de acceso a la red.	80 %
Instalación y configuración de servidor de filtrado web - San Lorenzo.	100 %
Instalación de equipos provistos por TELMEX en cada plantel y oficinas centrales.	40 %
Configuración de Red de cada plantel en base al nuevo direccionamiento.	20 %
Instalación de Firewall-Router en cada plantel.	20 %
Pruebas de conectividad.	20 %
Instalación de servidor de monitoreo.	0 %
Instalación de servidor de Reportes.	20 %
Generación de Entorno de Producción.	64.28 %

Cuadro 2.6: Porcentaje de avance del proyecto 16/Feb/2011

2.6. Planteles ya en funcionamiento

El proveedor de servicios ha entregado el servicio ya de algunos planteles, la empresa divide su entrega en 2 fases:

1. Entrega de medio físico, consta de la visita de viabilidad al plantel, petición de adecuaciones de ser necesarias, la instalación del cobre o fibra óptica de ser necesaria con su respectivo equipo Network Termination Unit (NTU) Watson Ethernet.
2. Configuración del equipo terminal, una vez finalizada la etapa uno se procede a enviar un ingeniero encargado de configurar el equipo NTU del plantel para integrado a la red del proveedor.

El área de Telecomunicaciones del IEMS debe entonces configurar los equipos una vez terminados los trabajos de TELMEX. Los planteles que ya se encuentran en la red se describen en la siguiente sección con sus respectivas pruebas de rendimiento.

2.6.1. Pruebas de rendimiento

En la siguiente tabla se exponen las pruebas de rendimiento efectuadas una vez que el servicio ya se encuentra activo. Como podemos observar ya se encuentran activos 4 planteles, obteniendo porcentajes de mejora en cuanto a medición de ancho de banda como medición de throughput desde el plantel hasta las oficinas centrales.

Plantel	Red Local	IP Pública	Conectividad entre Firewall de plantel y FW principal	Conectividad con servidores	Salida con diferentes perfiles a internet con su respectivo filtrado	Prueba de velocidad (speedtest.net) haciendo uso del enlace viejo	Prueba de velocidad, (speedtest.net) haciendo uso del nuevo enlace	Prueba de ancho de banda de FW principal y FW plantel (IPERF - Haciendo uso de enlace viejo)	Prueba de ancho de banda de FW principal y FW plantel (IPERF - Haciendo uso de enlace nuevo)	Porcentaje de Mejora	Fecha
A. Obregón	10.1.0.0/16	10.30.1.2									
Azcapotzalco	10.2.0.0/16	10.30.2.2									
Coyoacán	10.3.0.0/16	10.30.3.2	si	si	si	1.6Mb/s, 0.129Mb/s	1.98Mb/s, 1.93Mb/s	0.43Mb/s	2.0Mb/s	465.11	19/05/2011
Cuajimalpa	10.4.0.0/16	10.30.4.2	si	si	si	1.13Mb/s, 0.314Mb/s	1.91Mb/s, 1.99Mb/s	0.21Mb/s	1.98Mb/s	982.85	20/05/2011
Gustavo A. Madero I	10.5.0.0/16	10.30.5.2									
Gustavo A. Madero II	10.6.0.0/16	10.30.6.2									
Iztacalco	10.7.0.0/16	10.30.7.2									
Iztapalapa I	10.8.0.0/16	10.30.8.2									
Iztapalapa II	10.9.0.0/16	10.30.9.2									
Iztapalapa III	10.10.0.0/16	10.30.10.2									
M. Contreras	10.11.0.0/16	10.30.11.2									
M. Hidalgo	10.13.0.0/16	10.30.13.2									
Milpa Alta	10.14.0.0/16	10.30.14.2									
Tláhuac	10.15.0.0/16	10.30.15.2	si	si	si	1.3Mb/s, 0.230Mb/s	2.01Mb/s, 1.84Mb/s	0.2Mb/s	2.01Mb/s	1005	15/04/2011
Tlalpan I	10.16.0.0/16	10.30.16.2									
Tlalpan II	10.17.0.0/16	10.30.17.2									
V. Carranza	10.18.0.0/16	10.30.18.2	si	si	si	1.25Mb/s, 0.50Mb/s	1.98Mb/s, 1.88Mb/s	0.40Mb/s	1.70Mb/s	425	23/05/2011
Xochimilco	10.19.0.0/16	10.30.19.2									

Cuadro 2.7: Nuevo listado de equipos propietarios del IEMS. Área de Servidores.

2.7. Login y Password

Se desarrolló un script[20] que realiza la función de actualizar de manera generalizada las contraseñas de acceso a todos los Switches y Routeadores del Instituto. Ésta tarea se realiza automáticamente cada semana y se guardarán las nuevas contraseñas en un servidor.

A la fecha de creación de éste documento la herramienta no se ha vuelto extensiva a las contraseñas de los servidores.

2.8. Filtrado Web con DansGuardian

El filtrado de sitios WEB se encuentra ya operando en un servidor basado en Debian. En dicho servidor se montó el Squid y el DansGuardian en modo transparente lo que permite que los usuarios no necesariamente tengan que poner en su navegador web la IP donde se encuentra el servidor proxy.

Las ventajas de usar un servidor de filtrado aparte del Firewall Principal es que no tienes un solo punto de falla, si llegara a fallar el servidor de filtrado, no se perdería la navegación web sólo que dejaría de existir filtrado.

El DansGuardian usa el squid para montar su servicio, el squid en sí es un servidor de filtrado pero el DansGuardian tiene la capacidad de filtrar por contenido comparando con una lista de palabras, por sitio, url, expresión regular en la url. Además éste se puede integrar con el CLAMAV[21] que sirve para escanear si tiene virus un archivo descargado, aunque ésta función no se vaya a utilizar en éste momento.

El flujo que sigue un paquete para visitar un sitio WEB se ejemplifica en los siguientes 5 pasos:

[20] Un script (cuya traducción literal es 'guion') o archivo de órdenes o archivo de procesamiento por lotes es un programa usualmente simple, que por lo regular se almacena en un archivo de texto plano. Los script son casi siempre interpretados, pero no todo programa interpretado es considerado un script. El uso habitual de los scripts es realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario. Por este uso es frecuente que los shells sean a la vez intérpretes de este tipo de programas.

[21] ClamAV es un software antivirus open source (de licencia GPL) para las plataformas Windows, Linux y otros sistemas operativos semejantes a Unix.

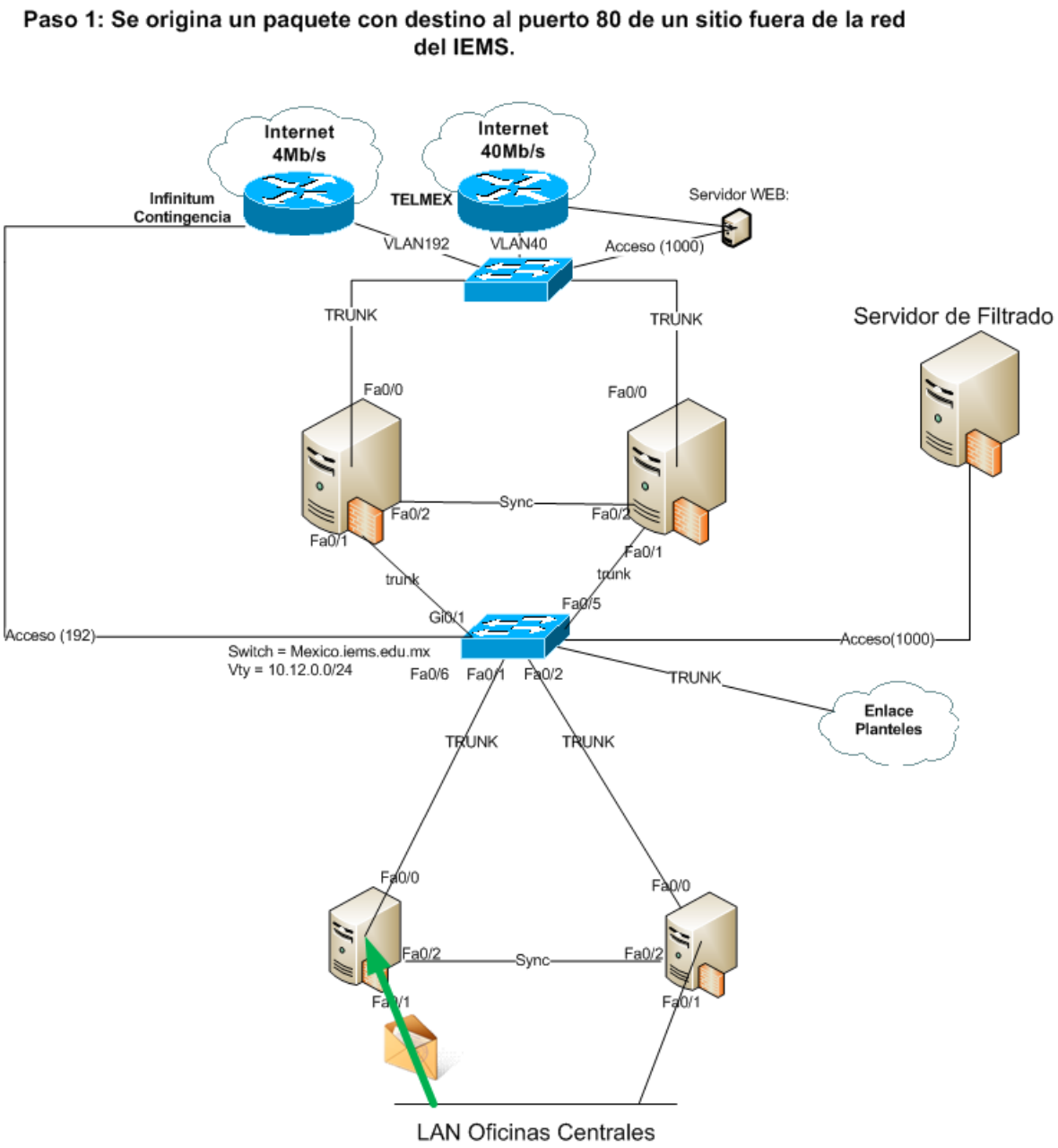

Figura 2.8: Paso 1. Flujo del filtrado Web

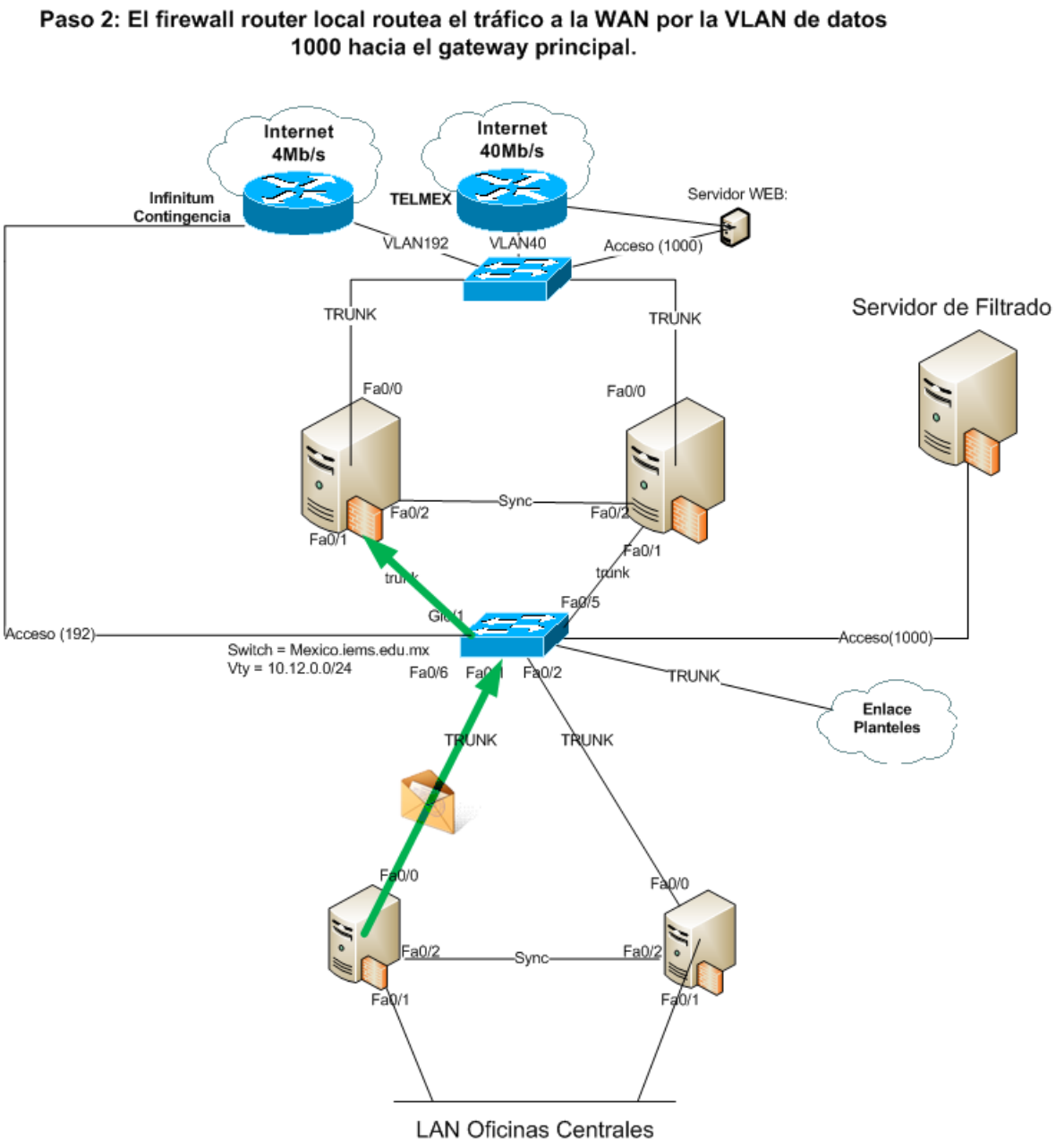

Figura 2.9: Paso 2. Flujo del filtrado Web

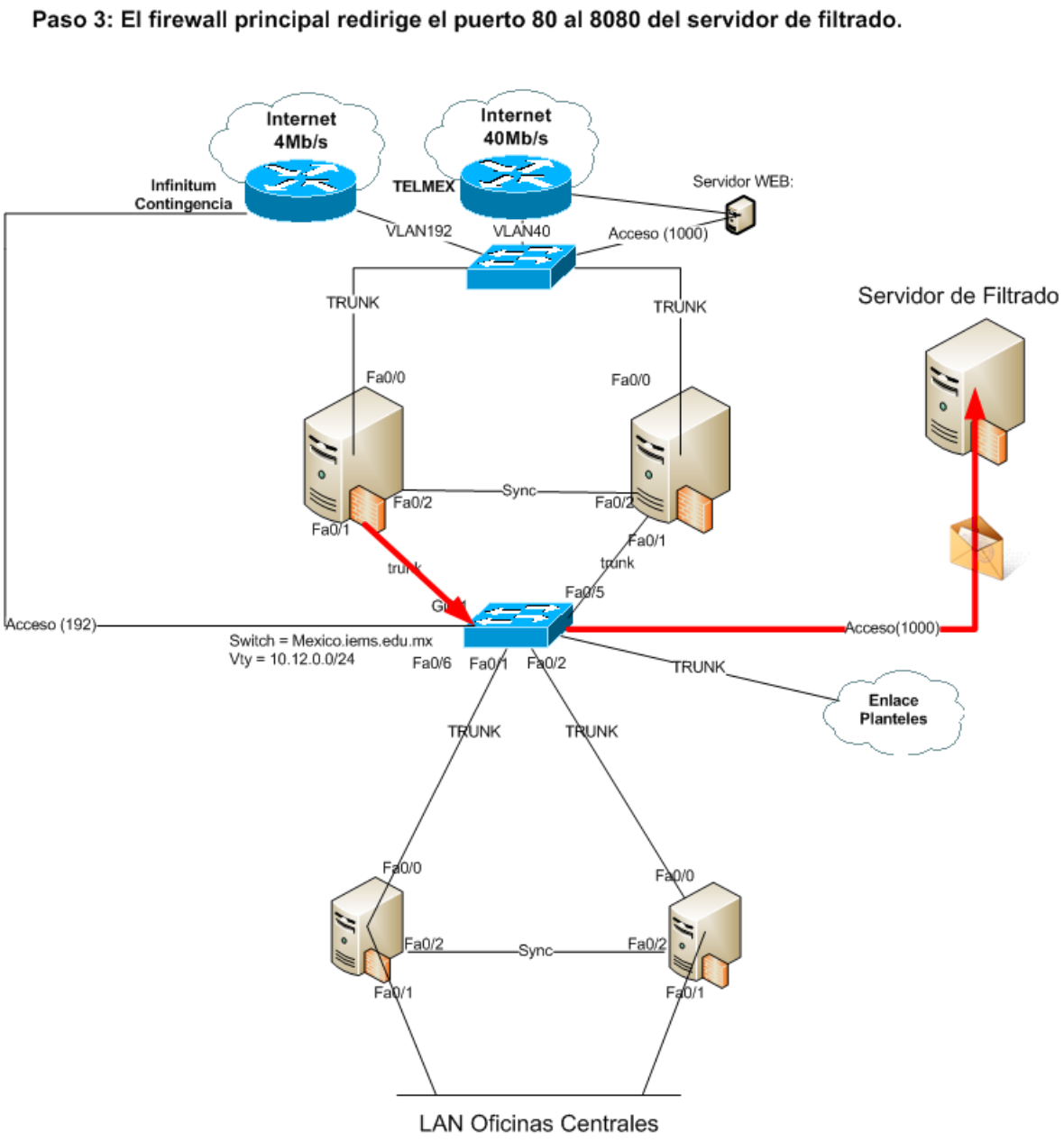

Figura 2.10: Paso 3. Flujo del filtrado Web

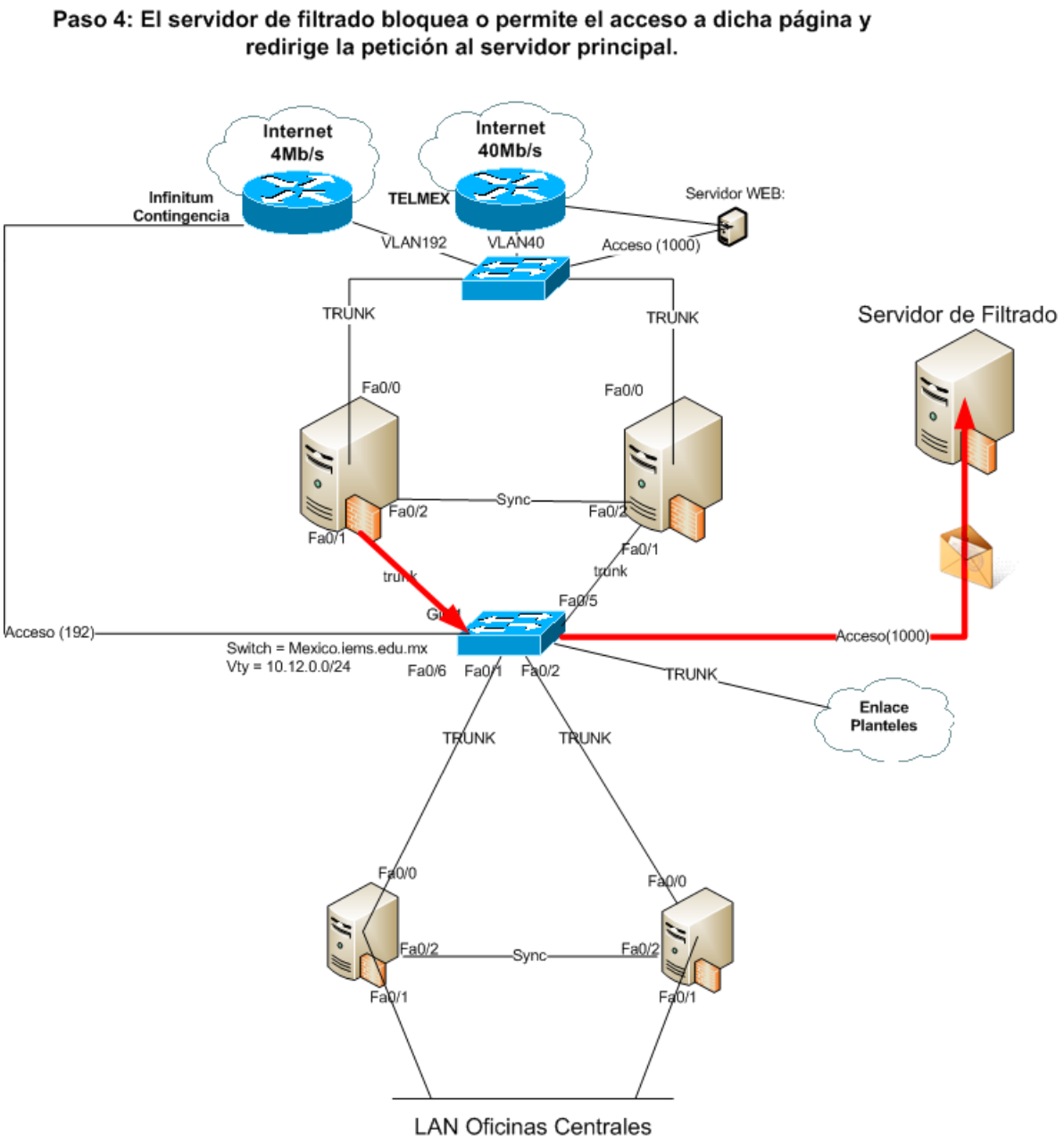

Figura 2.11: Paso 4. Flujo del filtrado Web

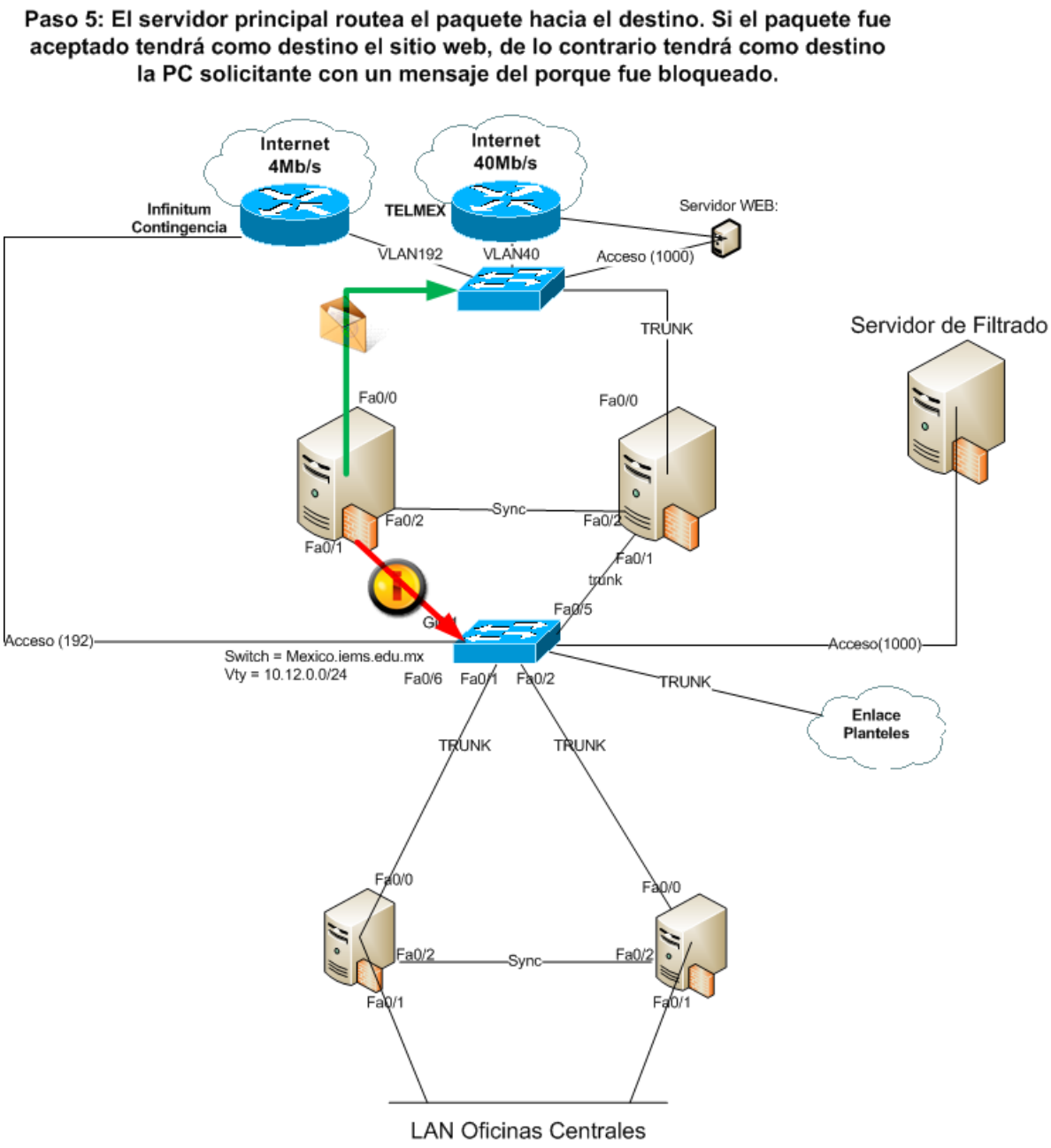

Figura 2.12: Paso 5. Flujo del filtrado Web

La flexibilidad del DansGuardian también nos permite la creación de varios niveles de filtrado o perfiles, en el Instituto se decidió crear 4 perfiles que se exponen a continuación:

Perfil	Característica	Horario en que aplica	Equipos que pertenecen
Perfil 1	Sin filtrado	Todo el día, todos los días	Servidores, PC de administradores de red.
Perfil 2	Filtro normal, se permiten algunas redes sociales.	Lun-Vie 10:30 - 19:30	Administrativos
Perfil 3	Solo correos	Todo el día, todos los días	A consideración.
Perfil 4	Filtro más restrictivo con redes sociales	Todo el día, todos los días	Alumnos.

Cuadro 2.8: Niveles de filtrado, perfiles y equipos que aplica el DansGuardian

Se decidió en base al tráfico expuesto en la figura siguiente que existan horarios donde el filtrado en el perfil 2 no aplique, esto para permitir el uso libre de algunos sitios considerados de esparcimiento por unos y de trabajo por otros.

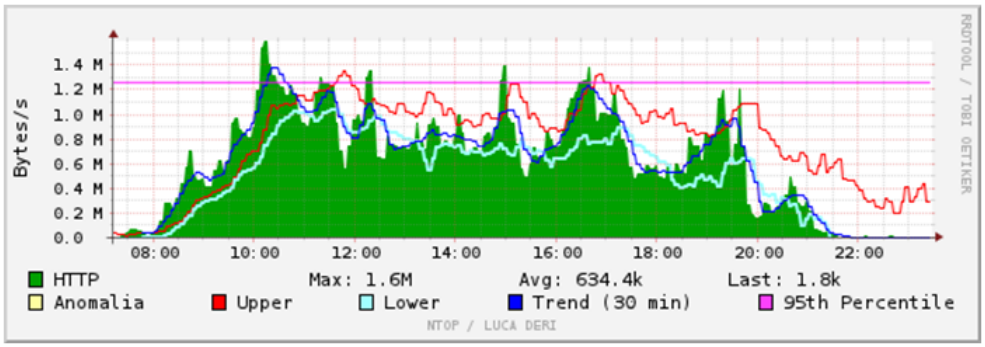

Figura 2.13: Tráfico típico web en el IEMS

El horario de labores es de 9 hasta 8 PM variando de área en área, en la gráfica se observa que el usuario usa el Internet una vez llega de 10 a 11 AM y cuando regresa de la hora de la comida de 5 a 6 PM aproximadamente. Por lo tanto se decidió que exista un periodo de uso libre de internet (a excepción de páginas de contenido sexual o que puedan contener virus, malware o alguna amenaza a la red). A grandes rasgos lo que se intenta bloquear o restringir son las siguientes categorías:

- audio-video
- filehosting
- filesharing
- proxy

- games
- onlinegames
- warez
- spyware
- malware
- hacking
- violence

Además de una lista muy extensa de palabras que se utilizan para comparación con el contenido.

2.9. Configuración de DHCP y DNS

Los usuarios del IEMS también son permitidos llevar su laptop desde su casa, situación que compromete la seguridad de la red debido a que dichas máquinas se encuentran no administradas por el equipo de soporte y telecomunicaciones y por ende pueden contener virus u otras amenazas externas a la red institucional. Por ello se les ha habilitado una alternativa para dichas máquinas que es el uso del wireless que se encuentra libre y aislado en la VLAN 600.

Para las PC del instituto tanto en oficinas centrales como en planteles es necesario tener su dirección MAC en el firewall de lo contrario se presentará un portal cautivo indicando que es necesario que se ponga en contacto con el administrador de la red.

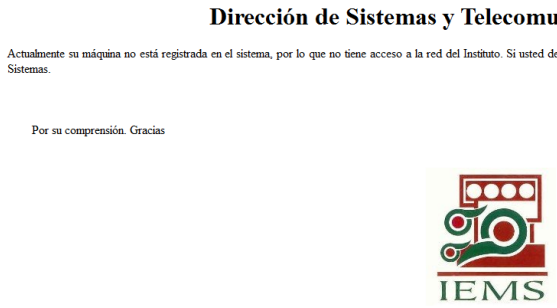

Figura 2.14: Portal cautivo indicando el no registro a la red

Por lo tanto la asignación de dirección IP se hace en los servidores *TokioPricipal* y *TokioSecundario*, ambos en alta disponibilidad. Esto quiere decir que periódicamente se encuentra *TokioPrincipal* replicando a *TokioSecundario* la lista de IP otorgadas.

El proceso de asignación es el siguiente:

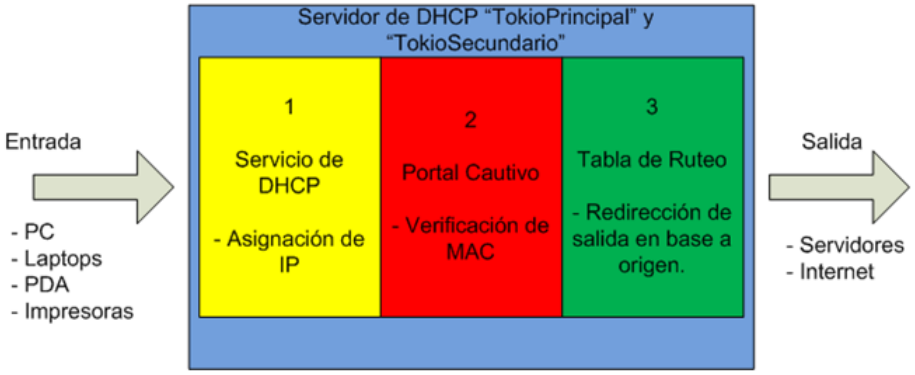

Figura 2.15: Proceso de asignación de IP, verificación de MAC address y enrutamiento en los servidores TokioPrincipal y TokioSecundario.

A continuación se presenta un ejemplo del proceso que sigue una máquina del instituto para la adquisición de IP:

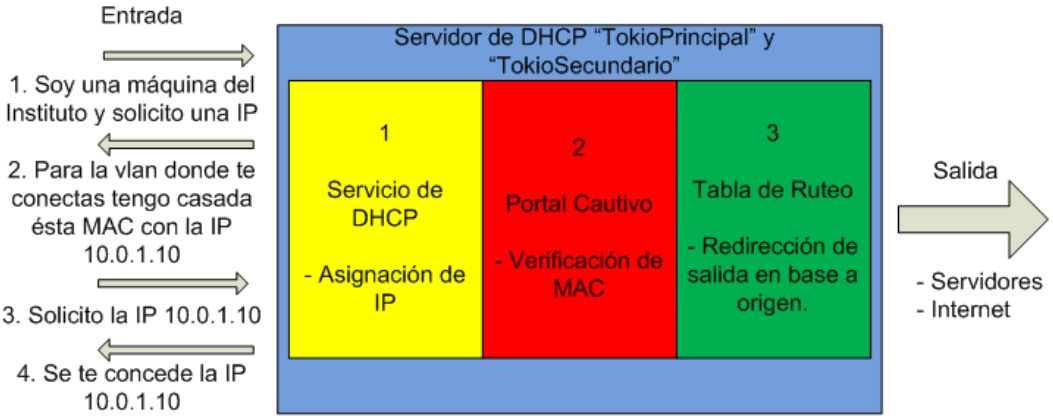

Figura 2.16: Proceso de asignación de IP para una PC conocida en el servidor TokioPrincipal y TokioSecundario.

A continuación se presenta un ejemplo del proceso que sigue una máquina ajena al instituto para la adquisición de IP:

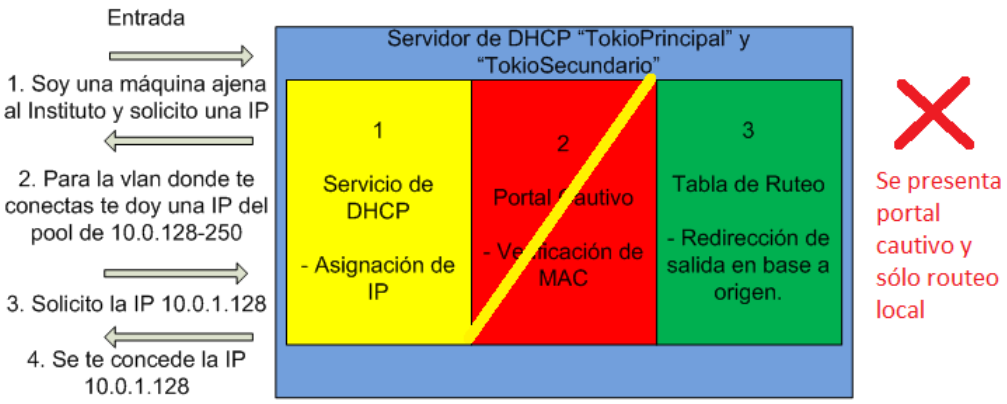

Figura 2.17: Proceso de asignación de IP para una PC ajena en el servidor TokioPrincipal y TokioSecundario.

La función entonces del portal es la de verificar que la IP origen coincide con la MAC, éste proceso es para evitar que un usuario con una máquina ajena al instituto, gane privilegios con el simple hecho de cambiar la IP a una del rango confiable.

Ésta medida de seguridad debe ser en un futuro conjuntada con un servidor VLAN Management Policy Server (VMPS)[22] o mediante Remote Authentication Dial-In User Server (RADIUS)[23] con el estándar 802.1x[24]. Para que la distinción de máquinas del instituto y ajenas no sea solamente a nivel de IP, sino que sea también a nivel de puerto mediante la asignación de una VLAN en un puerto dinámico.

[22]VLAN Management Policy Server o "VMPS.es un servidor que contiene la información de las MAC con su correspondiente VLAN y se encarga de asignar la VLAN de manera dinámica.

[23]RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 User Datagram Protocol (UDP) para establecer sus conexiones. Se integra en un servidor el cual resuelve a los autenticadores típicamente switches o access points el acceso o denegación a la red, la asignación de VLAN, entre otros parámetros, a un suplicante típicamente una PC.

[24]802.1x es un estándar de IEEE que define los mecanismos de autenticación a dispositivos que deseen agregarse a una LAN o WLAN.

2.10. Recomendaciones

Para lograr un completo control de la infraestructura de Tecnologías de la Información (TI), se deben llevar a cabo una serie de actividades que ayuden a mantener el buen funcionamiento así como al rápido restablecimiento en caso de falla de la red. Por lo cual se recomienda lo siguiente:

- Tener respaldos de los scripts de los Routers, Switches y servidores para levantar nuevamente las interfaces en caso de falla eléctrica. Dichos respaldos deben encontrarse en un servidor de Trivial File Transfer Protocol (TFTP), e impresos físicamente.
- No aplicar actualizaciones y no instalar aplicaciones adicionales que no estén previamente probadas.
- No realizar modificaciones sin un previo análisis del impacto que tendrán dichos cambios, por ejemplo, borrar usuarios, resetear puertos, quitar ó agregar comandos, reiniciar equipos, etc.

La frecuencia con que se deben realizar los respaldos depende de que tan frecuentemente se realicen cambios en las configuraciones.

2.11. Conclusiones

En éste documento se describieron los cambios realizados a la red LAN y WAN de las oficinas centrales y las redes de los planteles; los mecanismos utilizados para filtrar el tráfico web y la asignación de IP.

En la LAN de las oficinas centrales tenemos aún una deficiencia en la capa de acceso ya que aún existen muchos dispositivos instalados de manera inalámbrica, éstos dispositivos se planean cablear en un futuro dejando la red inalámbrica aislada de la red LAN, o sea en una VLAN diferente, esto con el objetivo de proveer mejor estabilidad y seguridad a los datos.

Así también encontramos una falta de enlaces redundantes hacia los Switches de distribución de las oficinas centrales (SW Florencia y SW Paris), ésta falta de enlaces deberá ser instalada.

En el núcleo donde se encuentran los equipos Firewalls de la red LAN de las oficinas centrales, encontramos que se encuentran ya trabajando en alta disponibilidad, estos equipos se encuentran teniendo un excelente rendimiento, ya que el Firewall principal se encuentra respaldado por el secundario y viceversa. Estos equipos proveen de routeo entre VLANS y routeo en base a origen, servicio de DNS y DHCP.

En la red WAN de oficinas centrales se instaló con éxito el Switch México en donde se migraron los servidores y en el cual se conectan los enlaces provenientes de cada plantel. Sin embargo todavía es necesario instalar el Firewall que le servirá de espejo al Firewall que otorga la salida a internet.

Se instaló un HUB en la llegada de los enlaces por parte de la empresa de TELMEX, éste HUB deberá también ser respaldado con un servidor en caso de que éste falle.

Se debe aún desarrollar el IPS/IDS, éste podrá ser instalado mediante Snort en modo Inline o en modo IDS. Donde el modo Inline permite descartar los paquetes generados por ciertos programas que cada vez son más difíciles de bloquear ya que usan puertos bien conocidos para enviar tráfico. El modo IDS de Snort permite el bloqueo del dispositivo en un tiempo determinado que genere una alarma. Aunque éste último resulta mucho más agresivo.