



Universidad Nacional Autónoma de México
Facultad de Ingeniería

**“Proyectos de automatización de procesos en la red
UNINET”**

**INFORME DE ACTIVIDADES PROFESIONALES
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN**

**PRESENTA
JUAN ANTONIO CARDONA SÁNCHEZ**

**ASESORA
M.C. Ma. Jaquelina López Barrientos**



México, D.F.

2013

Índice

Introducción	5
Capítulo 1 Organigrama De La Empresa.....	7
Capítulo 2 Proyectos	14
2.1. Proyecto1. Carrier Ethernet	15
2.1.1. Direccionamiento IP	17
2.1.2. Red de acceso	18
2.1.3 Redes de Transporte.....	19
2.1.4. Red de transporte SDH	20
2.1.5. Red de transporte Carrier Ethernet.....	20
2.1.6. Red de acceso al servicio	21
2.2. Proyecto2. Infraestructura.	25
2.2.1. Áreas en OSPF:	26
2.2.2. Tipos de Áreas en OSPF:.....	26
2.2.3. Tipo de autenticación utilizado en la red.....	27
2.2.4. Modelos y topologías para equipos PE.....	29
2.2.5. Equipos para servicio INFINITUM iadsl, ipdsl y dsl (BRAS).....	29
2.2.6. OSPF en equipos BRAS.....	31
2.2.7. BGP en equipos BRAS.....	31
2.2.8. Equipos con funcionalidad INET.....	32
2.2.9. Equipos con funcionalidad SECTORIAL	32
2.2.10. OSPF en equipos sectoriales	35
2.2.11. Equipos con funcionalidad REGIONAL.....	35
2.2.12. OSPF en equipos regionales	36
2.2.13. BGP en equipos regionales.....	37
2.2.14. Equipos con funcionalidad BACK BONE.	38
2.2.15. BUP: Equipos de respaldo de los BB.	38
2.2.16. OSPF y BGP en equipos Back Bone.....	38
2.2.17. Protocolo EGP (External Gateway Protocol).....	39
2.2.18. Equipos con funcionalidad RRIDE.....	40
Capítulo 3 Proyectos de automatización de procesos en la red UNINET.....	44
3.1. Proyectos de automatización de procesos.....	45
3.1.1. Topología de solución	46
3.1.2 SISTEMA 1. Generador de descripciones para interfaces en la red uniNet.....	47
3.1.3. Planteamiento del problema 1	47
3.1.4. Interfaz con enlaces.	51
3.1.5. Interfaz con conexiones.....	53
3.1.6. Interfaz con Interconexiones	54
3.1.7. Solución para el problema 1.....	55
3.1.8. Planteamiento del problema 2.....	59

3.1.9. Documentación de Plan de Implementación.....	60
3.1.10. Políticas.....	61
3.1.11. Solución al problema 2	63
3.1.12. Planteamiento del problema 3.....	69
3.1.13. Solución al problema 3	70
Conclusiones	78
Glosario.....	82
Mesografía.....	84

Agradecimientos

A mis padres Antonia Sánchez y Juan Carlos Cardona, por su apoyo incondicional y todo lo que he logrado gracias a sus consejos y esfuerzos para llegar hasta donde hoy me encuentro.

A la M.C. Ma. Jaquelina López Barrientos, quien nunca desiste para transmitir ese conocimiento en las aulas que hasta hoy llevo conmigo y por depositar su esperanza en mí al aceptar ser mi asesora del paso final de la carrera.

A mis hermanos Ricardo, Rosalba y Carlos, quienes soportaron mis travesuras y siempre que los necesito ahí están para apoyarme.

A Tania Martínez, por compartir mis locuras, ayudarme a ver las cosas desde otros puntos de vista, estar a mi lado cuando más la necesito y ayudarme a levantar en las situaciones más difíciles.

A mis primos Oscar, Belem, Manuel, Susana y Ana, por ser como unos hermanos con los que he compartido situaciones geniales y están conmigo en las buenas y en las malas.

A mis tíos Marta, Manuel, Leticia y Víctor, por ser como padres en el momento que estaba a su cargo y cuidarme como si fuera uno de ellos.

A los ingenieros Eréndira Santacruz, Gerardo Jiménez, Guadalupe Vázquez y Santiago Ramírez, por aceptarme como miembro de su equipo de trabajo y contribuir en la segunda parte de mi formación como ingeniero

A mis amigos Lino González, Carlos Martínez, Jorge Hernández, por ser un verdadero ejemplo a seguir y compartir momentos inimaginables y por ser eso... Amigos.

A la familia Martínez Cisneros, Por permitirme entrar en su hogar y enseñarme el valor sin igual que tiene una familia.

An abstract graphic on the left side of the page, featuring a dense, chaotic network of black and blue lines. The lines vary in thickness and curvature, creating a sense of movement and complexity. Some lines are straight, while others are curved or looped. The background is white, and the overall effect is that of a tangled web or a complex network structure.

Introducción

Terminé las materias correspondientes a la carrera de Ingeniería en Computación en el módulo de Redes y Seguridad en Junio de 2012 y en el mismo mes ingresé al campo laboral en el consorcio Red Uno TELMEX en el departamento de Gestión de Cambios y Configuraciones en donde actualmente me encuentro desempeñando mis labores profesionales realizando actividades en la red de datos uniNet con el rol de administrador de liberaciones e implementaciones.

Red Uno TELMEX se ha distinguido como una entidad socialmente responsable, congruente con sus Valores y Principios y además, por fortalecer internamente la conducta ética de nosotros los integrantes.

Igualmente, la empresa brinda la oportunidad para responder de manera completa y actualizada a las condiciones emergentes del entorno en que hoy día vivimos en el ámbito de las redes de datos, estas respuestas indudablemente son innovaciones y diferentes opciones tecnológicas, al mercado actual de las telecomunicaciones más competido, más globalizado y más exigente.

La empresa tiene las siguientes misión y visión:

Misión

“Ser un grupo líder en telecomunicaciones, proporcionando a nuestros Clientes soluciones integrales de gran valor, innovadoras y de clase mundial, a través del desarrollo humano, y de la aplicación y administración de tecnología de punta.”

Visión

“Consolidar el liderazgo de Consorcio Red Uno en el mercado nacional, expandiendo su penetración de servicios de telecomunicaciones en todos los mercados posibles, para ubicarnos como una de las empresas de más rápido y mejor crecimiento a nivel mundial. “



Capítulo 1

Organigrama De La Empresa

La empresa está constituida por diversos departamentos dedicados a la recepción de infraestructura, el control de los cambios en la red, fallas, medición de desempeño, desarrollo de herramientas que faciliten la operación y documentación, soporte técnico proactivo y reactivo, dichos departamentos están descritos en la tabla t1.1 con las siglas que los identifican:

Tabla t1.1 Departamentos que conforman a Red Uno.

Nombre del departamento	Siglas
Cambio Tecnológico	CAMTEC
Control de Cambios	CC
Desempeño de red	DESRED
Gestión de Cambios y Configuraciones	GCC
Gestión de Fallas Acceso Residencial	GFR
Gestión de Fallas Corporativo	GFC
Gestión de Fallas Dorsal	GFD
Ingeniería	ING
Soporte Técnico Proactivo	STP
Soporte Técnico Reactivo	STR

Yo me incorporé al departamento de Gestión de Cambios y Configuraciones el cual tiene el organigrama descrito en la imagen I1.1 y en el cual participamos 10 personas para cubrir las tareas esenciales del departamento que son:

- a) Atención a solicitudes de cambios de IP's fijas
- b) Atención a interconexiones
- c) Atención a solicitudes de gestión de interfaces
- d) Atención a migraciones de equipos ip DSLAM
- e) Corrección de campos erróneos en la base de datos para tener correctamente documentados los cambios en la red

COMERCIAL

OPERACIONES

SOPORTE

AREAS COMISIONADAS

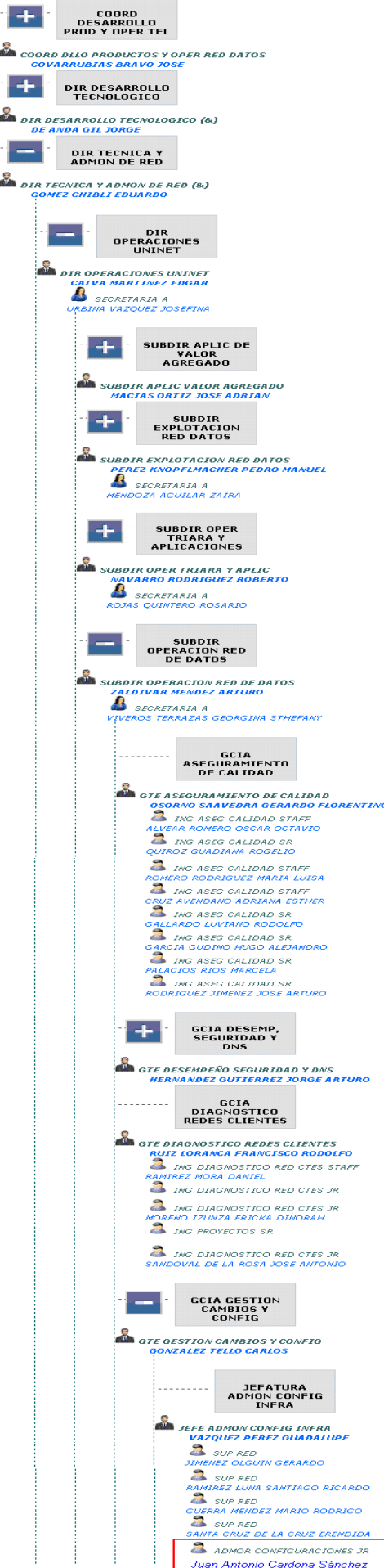


Imagen I1.1 Organigrama de Red Uno

Para cumplir las tareas antes descritas, el departamento Gestión de Cambios y Configuraciones (GCC) está integrado por:

- Director operaciones de la red de datos – Ing. Edgar Calva Martínez
- Subdirector operaciones de la red de datos - Ing. Arturo Zaldívar Méndez
- Gerente - Ing. Carlos González Tello
- Subgerente - Ing. Guadalupe Vásquez Pérez
- Supervisores de red - Ing. Eréndida Santa Cruz e Ing. Gerardo Jiménez Olguín
- Administrador de configuraciones STAFF - Juan Antonio Cardona Sánchez

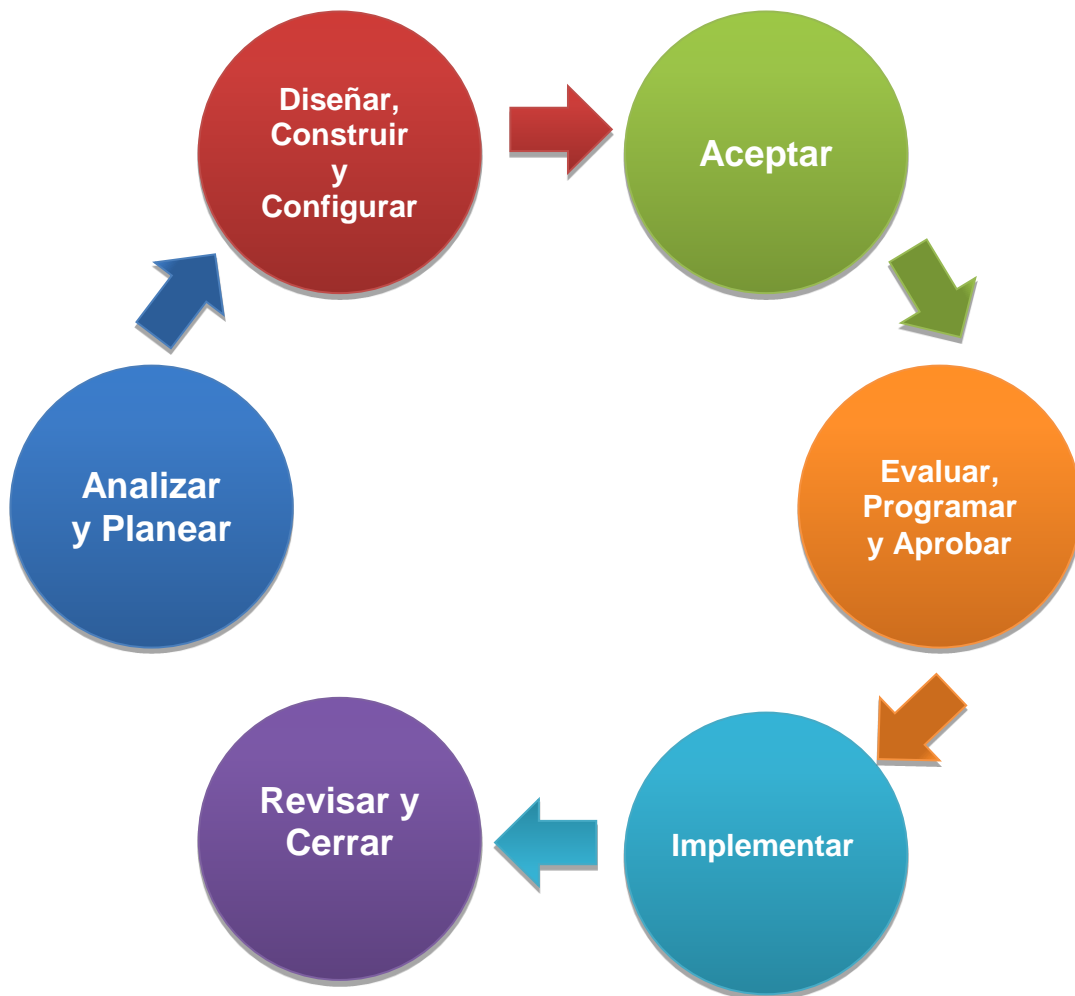
En Red Uno en el departamento de GCC se manejan tres proyectos los cuales son:

- Carrier Ethernet
- Infraestructura
- Intervenciones

Los proyectos se distinguen entre sí por las operaciones en la red uniNet que conciernen a cada uno de ellos, todas estas actividades basadas en una correcta documentación apegada al proceso de ISO 20000 por medio de los RFC (Request For Change / Solicitud de Cambio) que contendrá “n” numero de implementaciones pero sólo una deberá de ser exitosa si es que se llevó a cabo de una manera adecuada y no se puso en riesgo el servicio así como la correcta funcionalidad de dicha implementación, entonces tendrán su correspondiente Elemento de Configuración (CI Configuration Item) que es el componente de infraestructura o elemento que está, o estará, bajo el control de la gestión de configuración. Todo esto estará registrándose para su consulta en una CMDDB (Configuration Management Data Base / Base de Datos de Gestión de Configuraciones) el objetivo de ello es tener un mayor control de cada actividad realizada en la red.

Para la realización de una implementación en la red, en cada actividad son necesarios documentos que respalden la configuración o movimientos en los equipos, a estos documentos los llamamos CU o Plan de intervención el cual contiene las actividades previas, durante y después de la implementación.

Estos tres proyectos se rigen por el proceso de Gestión de Liberaciones e Implementaciones el cual tiene el flujo descrito en la imagen I1.2



I1.2 Flujo del proceso de Gestión de Liberaciones e Implementaciones

A continuación se describen cada una de las seis actividades correspondientes a este flujo:

01- Analizar y Planear: Registrar el requerimiento para la liberación de un servicio nuevo o modificado y asegurar que contenga la información necesaria para que se cumpla la totalidad del proceso.

02- Diseñar, Construir y Configurar: Generar el diseño de liberación que considere los elementos necesarios para su implementación. Construir y configurar el ambiente de prueba piloto, para probar el diseño de liberación y garantizar que dicho ambiente cuente con los requerimientos necesarios para habilitar el diseño de liberación.

03- Aceptar: Ejecutar las pruebas en el ambiente de prueba piloto y validar que se cubran los criterios de aceptación.

04- Evaluar, Programar y Aprobar: Validar que las solicitudes de implementación contengan la información necesaria para poder ejecutar la petición. Generar el plan de implementación asegurando la disponibilidad de los recursos y aprobar la solicitud de implementación.

05- Implementar: Asegurar que las implementaciones se ejecuten con las condiciones requeridas. Ejecutar lo establecido en el Plan de intervención.

06- Revisar y Cerrar: Asegurar y validar el correcto funcionamiento del servicio y documentar los resultados. Analizar y diagnosticar el comportamiento no esperado del servicio y aplicar acciones en caso necesario para restablecer el servicio a las condiciones iniciales.

A continuación se describen los roles del personal:

Dueño del proceso de Liberaciones e Implementaciones: Autorizar el diseño y definir elementos de estrategia para asegurar el proceso y la mejora continua.

Administrador del proceso de Liberaciones e Implementaciones: Planear y coordinar las actividades requeridas para la ejecución y monitoreo del proceso.

Supervisor de implementaciones: Garantizar que las actividades referentes a la implementación, revisión y cierre se realicen conforme a lo establecido en el proceso de Gestión de liberaciones e implementaciones.

Administrador de liberaciones Implementaciones: Participar activamente en las pruebas, evaluación, liberación e implementación para entregar valor al solicitante.

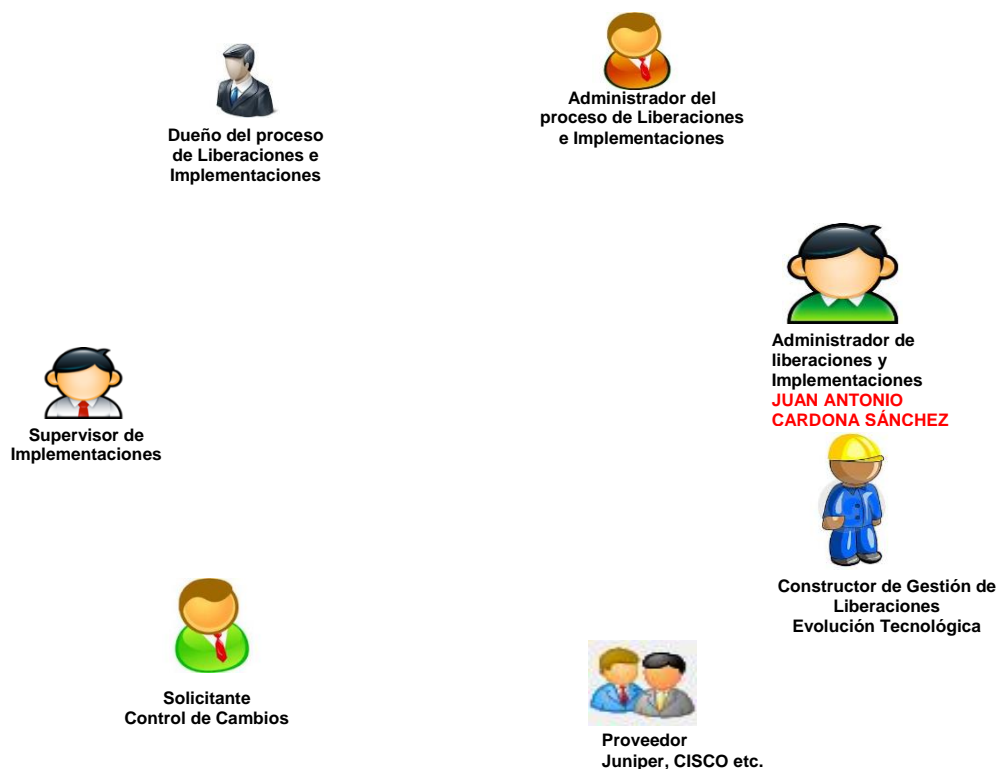
Constructor de Gestión de Liberaciones: Construir el ambiente de prueba piloto para evaluar las solicitudes de liberación de servicios nuevos o

modificados.

Solicitante: Asegurarse que los requerimientos de un servicio nuevo o modificado implementados cumplan con lo solicitado.

Proveedor: Colaborar con la construcción y configuración del ambiente de prueba piloto.

En el departamento GCC el personal tiene diversos roles y yo me ubico en el de administrador de implementaciones, en la imagen I1.3 se muestra el personal y el rol que tienen dentro del proceso.



11.3 Roles del personal



Capítulo 2

Proyectos

2.1. Proyecto1. Carrier Ethernet

Este es el primer proyecto en el que participé, a mi ingreso a la empresa, fui asignado al departamento de Gestión de Cambios y Configuraciones (GCC) como Administrador de configuraciones en el horario de 8:00 a 16:00, y cabe mencionar que el proyecto está operando desde antes de mi ingreso a la organización.

- Objetivo del proyecto: Definir la arquitectura del servicio de acceso a Internet con las diferentes tecnologías de acceso alámbricas e inalámbricas, alcance y consideraciones de diseño que se utilizan para conectar los usuarios a la red.
- Participantes: Administradores de configuraciones, solicitantes de cambios a la red intermediarios entre el cliente y el departamento de gestión de cambios y configuraciones (OPERTELES), este departamento está operando con alrededor de 20 personas rolando en tres turnos (matutino, vespertino, y horario de oficina).

El servicio de INFINITUM que ofrece TELMEX es una conexión directa de acceso a Internet de alta velocidad que utilizan como medio de acceso la línea telefónica (Loop local) con tecnología DSL (Digital Subscriber Line) que por medio de un Spliter (filtros pasivos) separa la comunicación de voz y datos permitiendo una llamada y la navegación en internet en forma simultánea, el servicio también se ofrece por medio de tecnologías inalámbricas como WIMAX.

La tecnología DSL es una familia de tecnologías alámbricas que cumplen con la creciente demanda del mercado por acceso a internet, cada vez a mayores velocidades independientemente de la tecnología de acceso el subcriptor o usuario cuenta con un equipo que es el que se conecta al spliter y éste a su vez a la línea telefónica o loop local llamado MODEM o Residential Gateway, de esta familia las tecnologías que se han utilizado son:

-ADSL (Asymmetric Digital Subscriber Line): Alcanza velocidades de hasta 8Mbps de Downstream y 768 Kbps de Upstream, con una dependencia directa de las

características que se pueden tener en distancia, calidad de loop local, ruido y convivencia con otros servicios.

-Adsl 2 + (Asymmetric Digital Subscriber Line 2 Plus): Se alcanzan velocidades de hasta 24 Mbps de Downstream y 1.5 Mbps de Upstream, con una dependencia directa de las características de distancia, calidad de loop local ruido y convivencia con otros servicios.

-GPON (Gigabit Passive Optical Network) o fibra a la casa, esta alcanza velocidades de hasta 100 Mbps de Down/Up stream siendo otra alternativa de tecnologías alámbricas. Esta consiste en una red de fibra óptica pasiva, no requiere repetidores dentro de la red ni fuentes de poder intermedias, solo splitters.

En las tecnologías inalámbricas se cuenta con WIMAX (Worldwide Interoperability for Macrowave Access o interoperabilidad mundial de acceso por microondas), diseñado como una alternativa de acceso de banda ancha tipo dsl, siendo también una forma de conectar nodos Wifi en una red de área Metropolitana (MAN), también se podría definir como un sistema de comunicación digital y puede operar tanto en una banda licenciada como en una banda libre.

WIMAX puede proveer acceso de banda ancha inalámbrica hasta una distancia de 50 Km, si lo comparamos con el protocolo inalámbrico 802.11 (Wifi) el cual está diseñado como una solución para redes inalámbricas de área local bajo el uso de una banda no licenciada y cuyo cobertura es mucho menor (Dependiendo de la implementación pueden cubrirse alrededor de 100 metros), por lo que las características requeridas para ofrecer el servicio residencial se cubren con el uso de WIMAX bajo una banda licenciada.

En la oficina central de TELMEX o en algunos casos en el poste o en el registro de distribución de la calle se cuenta con equipos de acceso alámbricos llamados DSLAM, mini dslam o tba, para las tecnologías xDSL y OLT para la tecnología GPON, a los que se conocen los módem u ONTs de los usuarios para el caso

de WIMAX se cuenta con Radio Base que ofrecen el acceso inalámbrico. Todas las tecnologías de acceso que he mencionado con excepción de WIMAX, se conectan con el mismo edificio a las redes ATM, SDH, y Carrier Ethernet con interfaces ATM o Gigabit Ethernet según sea el caso, siendo estas redes los medios de transporte de TELMEX para conectar los equipos de acceso a los equipos BRAS de los nodos de agregación o locales de UniNet.

La arquitectura del servicio INFINITUM aquí descrita tiene una cobertura a nivel nacional, utilizando las diferentes tecnologías de acceso inalámbricas como:

- ADSL
- ADSL2+
- VDSL
- GPON

Y tecnologías inalámbricas tales como:

WIMAX

2.1.1. Direccionamiento IP

Los pools que se configuran en los BRAS, se asignan del direccionamiento reservado para INFINITUM considerado en la tabla t2.1

Tabla t2.1 Asignación de prefijos a pools.

Capacidad de equipo en sesiones PPPoE	Espacio de direcciones mínimo	Diagonal del prefijo mínimo	Espacio de direcciones IP máximo	Diagonal del prefijo máximo
2500	2000	/21	2000	/21
4000	2000	/21	4096	/20
18000	2000	/21	16000	/18
32000	2000	/21	32000	/17
48000	2000	/21	32000	/17
64000	2000	/21	32000	/17
96000	2000	/21	64000	/16

La arquitectura del servicio INFINITUM cumple con las siguientes características:

- Escalable
- Flexible
- Segura
- Con Calidad de servicio
- Basada en estandares

La arquitectura se compone de diferentes redes de infraestructura que interconectan los equipos que soportan el servicio como:

- Red de acceso
- Redes de transporte
- Red IP de Acceso al servicio

2.1.2. Red de acceso

La red de acceso es el segmento de red que se extiende entre la central telefónica de TELMEX y la vivienda del usuario, ese último tramo de conexión que llega hasta los hogares es lo que se conoce como bucle de abonado, loop local o último kilómetro, esta red esta compuesta por los equipos que llamamos de acceso o agregación de último kilómetro estos equipos pueden ser de tecnologías DSL en ATM o IP y equipos con tecnología óptica como:

Los equipos con tecnología ATM son:

- * DSLAMs
- * MiniDSLAMS
- * NAMs

Los equipos con tecnología IP son:

- * DSLAMs
- * TBAS (Terminal de Banda Ancha) 1 y 2

Los equipos con tecnología optica optica son:

- * OLTs en GPON

En estos equipos de acceso se conectan los equipos MODEM de los usuarios por medio local en cobre (par de cobre), u ópticos (Par de fibras).

La conexión entre el módem del cliente con el puerto módem de equipo de acceso es por medio de DSL y un PVC en ATM.

La conexión entre el equipo de acceso ATM con la red de transporte ATM es por medio de interfaces STM-1s en ATM.

La conexión entre los equipos de acceso IP con la red de transporte SDH o Carrier Ethernet es por medio de interfaces Gigabit Ethernet

La conexión entre los equipos ONT y los OLT es mediante fibra óptica en una arquitectura Punto – Multipunto en IP.

La conexión entre los equipos OLT y ala red de transporte Carrier Ethernet es por medio de interfaces Gigabit Ethernet IP.

2.1.3 Redes de Transporte

Red de transporte ATM

LA red de transporte ATM (legacy), es una tecnología de switching basada en unidades de datos llamadas celdas. ATM opera en modo orientado a la conexión por medio de un protocolo de señalización, una vez establecida la conexión las celdas de ATM incluyen información que permita identificar a la conexión a la cual pertenecen.

En una red ATM las comunicaciones se establecen a través de un conjunto de dispositivos intermediarios llamados switches, estos equipos forman el segmento de red que conecta los equipos de acceso o agregación con los equipos de acceso al servicio o BRAS.

Los switches que forman esta red de transporte son:

GX, estos equipos son los que forman el Backbone de la red ATM

PSAX, estos equipos son los equipos de agregación de la red ATM la cantidad

de circuitos virtuales (VPis/VCIIs) que se multiplexan en estos tubos, estos circuitos son terminados en los BRAS.

2.1.4. Red de transporte SDH

La red de transporte SDH de nueva generación es la tecnología dominante en la capa Física OSI de transporte de las actuales redes de fibra óptica, su misión es transportar y gestionar gran cantidad de tipos de tráfico diferentes sobre la infraestructura física.

SDH es un protocolo de transporte basado en la existencia de una referencia temporal común (Reloj primario), que se multiplexa diferentes señales dentro de una jerarquía comun flexible y gestiona su transmisión de forma eficiente a través de fibra óptica, con mecanismos internos de protección.

Los switches ópticos de SDH forman el segmento de red que interconectan los equipos de acceso IP o Ethernet con los equipos BRAS, en donde estos últimos se terminan la VLANs que inician en los diferentes tipos de IP DSLAMs que he mencionado.

2.1.5. Red de transporte Carrier Ethernet

La red Carrier Ethernet es una red de transporte metropolitano con funcionalidades de MPLS para rápida convergencia mediante conexiones punto a punto, esta red esta compuesta por closters con equipos switches Ethernet con funciones de L2 y L3 con una jerarquía de tres niveles que son mencionados de mayor a menor y son:

- Equipos de distribución
- Equipos de agregación de alta densidad
- Equipos de agregación de baja densidad

Los equipos de acceso se conectan a los Switches de agregación de alta y baja densidad y los BRAS se conectan a los equipos de distribución

2.1.6. Red de acceso al servicio

La red de acceso al servicio es el segmento de red que se encuentra entre las redes de transporte que he mencionado y el backbone IP de UniNet, esta red está compuesta por enrutadores con funciones de BRAS, distribuidos a nivel nacional en nodos de agregación de alta densidad o locales en los nodos que no son de agregación pero que tienen alta densidad local de usuarios, con las siguientes funcionalidades:

→ Terminación de circuitos virtuales o PVCs (VPI/VCI) que inician en los equipos de acceso (DSLAMs) los cuales se transportan la sesiones de PPPoE de cada uno de los usuarios.

→ Terminación de circuitos virtuales de gestión de cada uno de los DSLAMs

→ Terminación de VLans que inician en las interfaces de Up Link de los equipos de acceso (DSLAMs) y que transportan las sesiones de PPPoE de cada uno de los usuarios.

→ Terminación de VLans de gestión de cada uno de los DSLAMs

→ Terminación de las sesiones PPPoE que inicia cada uno de los módems de los usuarios.

→ Genera una interfaz virtual para cada una de las sesiones de PPPoE en las que se aplican políticas de QoS.

→ Inicia la sesión de accounting con el RADIUS de cada una de las sesiones de PPPoE en la que se envía la información de Realy Agent que recibe de los equipos de acceso (DSLAMs) y por medio de la cual tenemos huella de los usuarios.

→ Asigna las direcciones ip /32 de pools locales a los usuarios, una vez que estos son validados y autorizados por los RADIUS.

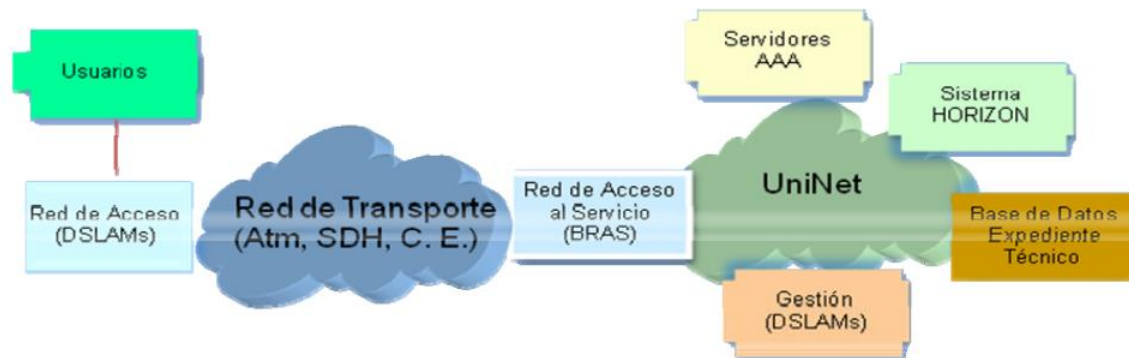
→ Control de ancho de banda, acorde al perfil que tiene autorizado por RADIUS el usuario o con perfiles genéricos.

→ Enrutamiento del tráfico que generan los usuarios hacia y desde el Internet Global.

→ Aplicación de políticas como el redirect para el servicio de valor agregado como el de envió de mensajes a los usuarios cuando estos generan trafico de

http.

La imagen I2.1 describe los módulos funcionales que componen la red de acceso al servicio.



I2.1 Módulos Funcionales

Usuarios: Forman una red de módems de diferentes proveedores que le dan conectividad a las redes locales de los hogares por medio de las diferentes tecnologías que he mencionado como xDSL y GPON.

Red de Acceso: La red de acceso está formada por los equipos de agregación de diferentes tecnologías que conectan a la red, los módems de los usuarios, esta red está formada por equipos como:

ATM: Equipos que soportan poco mas de 700 puertos

→ DSLAMs (Digital Subscriber Line Access Multiplexer), estos equipos son de gabinete de central y se consideran de alta densidad de puertos, siendo ésta desde 700 puertos en adelante.

→ Mini DSLAMs, estos equipos son de gabinete de intemperie, son de baja densidad de puertos, siendo desde 48 a 96 puertos.

→ Nodos de Acceso para Narrowband y Broadband mejor conocidos localmente como NAMs (Nodo de Acceso Multiservicio), estos equipos son de gabinete de central de mediana densidad, de hasta 300 puertos por repisa con un máximo de dos repisas por gabinete, estos equipos soportan tanto servicios de POTS como de ADSL y HDSL.

IP: Equipos que soportan tecnologías con mayor número de puertos

→ DSLAMS, son equipos de gabinete de central de alta densidad que soportan desde 800 a más de 1000 puertos.

→ Mini IP DSLAMs o conocidos localmente como TBAs (Terminal de Banda Ancha), estos equipos son de gabinete de intermedia de baja densidad de 48 a 96 puertos.

Ópticos: Equipos que tienen mayor número de puertos para usuarios que los IP

→ OLTs, son equipos de gabinete de central de alta densidad que soportan hasta 3584 usuarios en 56 puertos PON.

Red de Transporte: El transporte de TELMEX está compuesto por diferentes redes que ya he mencionado y su función en lo que se refiere al servicio de Infinitum, es la de conectar la red de acceso con la red de acceso al servicio.

Red de Acceso al Servicio: Son los equipos routers dedicados con funciones de BRAS que están instalados en forma distribuida en las centrales en los nodos de agregación de UniNet a nivel nacional, para hacer la agregación de las sesiones de PPPoE, además de hacer la función de LAC para servicios como la reventa de Infinitum.

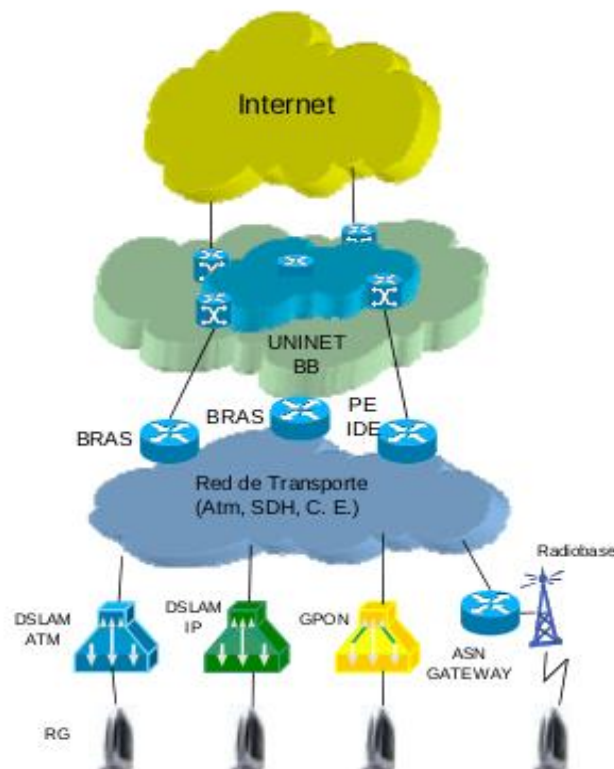
Servidores AAA: Se trata de un conjunto de servidores de RADIUS distribuidos en 4 regiones operativas: Norte, Occidente, Centro y Sureste. Su arquitectura es de dos niveles, con diferentes funciones en cada nivel, el primero lo conforman los servidores AAA globales y el segundo los AAA locales, donde la función del nivel global es identificar el servicio e independizar la infraestructura de acceso y la función del nivel local. La función del nivel local es la de realizar el proceso de validación del usuario final, así como la asignación del perfil del servicio correspondiente.

Sistema Horizon: Es el sistema de aprovisionamiento de cuentas de usuario, este es alimentado por diferentes sistemas, siendo el principal PISA, que es donde se generan las órdenes para altas, cambios y bajas del servicio.

Gestión DSLAMs: Los gestores de los diferentes proveedores se ubican en Triara Monterrey en una DMZ ya que gestionan equipos en banda a través de la red UniNet y algunos otros fuera de banda a través de la RCDT, estos servidores se encargan del aprovisionamiento del servicio así como del monitoreo de los equipos.

Base de Datos Expediente Técnico: Son varias las bases de datos con la información de los usuarios como: Número de teléfono del servicio, Modelo y numero de serie del módem, DSLAM y puerto al que se conecta, username, BRAS al que se conecta, ancho de banda contratado.

La imagen I2.2 muestra la topología de conectividad del servicio



I2.2 Topología de conectividad del servicio

Lo antes descrito engloba al proyecto Carrier Ethernet en el que mi participación es hasta la fecha el llevar a cabo el monitoreo y la integridad de clientes de INFINITUM navegando en los routers de borde de UniNet, recibir y configurar interconexiones hacia los equipos de TELMEX donde se estarán conectando

todos los equipos ip DSLAM que son los encargados de brindar el transporte del servicio de INFINITUM, gestionar las interfaces de una interconexión ya recibida que servirá de GATEWAY para los equipos colgando de dicha interfaz, mantener una correcta documentación de cada elemento de red esto lo realicé a mi ingreso a la empresa durante aproximadamente un mes posteriormente estuve trabajando en la red dorsal (proyecto infraestructura) regresando de nuevo al Proyecto de Carrier Ethernet por los cambios de roles y ubicación de personal que se acostumbran en la organización cada 6 meses aproximadamente.

2.2 Proyecto2. Infraestructura.

Este es el segundo proyecto en el que participé, aproximadamente al mes y medio de mi ingreso a la empresa siguiendo con el puesto de Administrador de configuraciones en el horario de 9:00 a 18:30, y cabe mencionar que el proyecto está operando desde antes de mi ingreso a la organización.

- Objetivo del proyecto: Definir la arquitectura de tránsito y forwarding del tráfico de todos los servicios PE (Provider Edge) de datos proveniente de los equipos de acceso Border router que brinda acceso a internet con las diferentes tecnologías de acceso, mantener la infraestructura de los equipos de uniNet con base en la recepción de equipos, enlaces, interconexiones, redundancias conexiones a los proveedores internacionales y nacionales.
- Participantes: Administradores de configuraciones, solicitantes de cambios a la red intermediarios entre el cliente y el departamento de gestión de cambios y configuraciones (OPERTELES), este departamento está operando con alrededor de 20 personas rolando en tres turnos (matutino, vespertino, y horario de oficina), departamento de Control de Cambios este departamento cuenta con alrededor de 30 personas operando las 24 horas del día.

Para este proyecto lo iré explicando por secciones empezando por el protocolo de enrutamiento utilizado en uniNet OSPF (Open Shortest Path First) y los diferentes equipos con las funcionalidades correspondientes.

OSPF es un protocolo que tiene las siguientes características:

- Protocolo link-state
- De tipo classless
- Regido por costos
- Rápida convergencia
- Soporta VLSM
- No propietario de Cisco
- Protocolo escalable

La operación de OSPF está basada en los siguientes puntos:

- Utiliza el protocolo Hello para mantener adyacencias
- Asignación de un DR de ser necesario en una red en particular
- Necesario que cada router tenga un dirección de red asignada que funcione como ID
- OSPF usa el protocolo link-state request/update para propagar a la red algún cambio en su topología

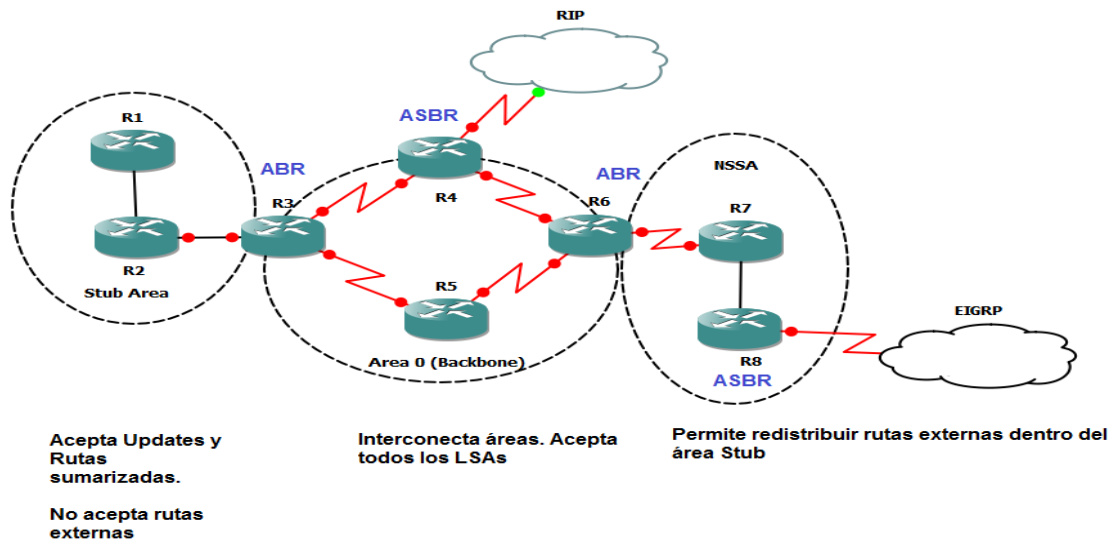
2.2.1. Áreas en OSPF:

- 50 a 100 routers por área
- Mantener direccionamiento disponible
- Áreas separadas por un área backbone

2.2.2. Tipos de Áreas en OSPF:

- Standard
- Backbone (Área 0)
- Stub Área
- Not-so-stuby Área (NSSA)

En la figura I2.3 se ejemplifican las áreas de OSPF



12.3 se ejemplificación de las áreas de OSPF

2.2.3. Tipo de autenticación utilizado en la red

Un router confía en que la información de enrutamiento proviene de un router que debería estar enviando información. Un router también confía en que la información no haya sido alterada a lo largo de la ruta. Para garantizar esta confianza, los routers de un área específica pueden configurarse para autenticarse entre sí.

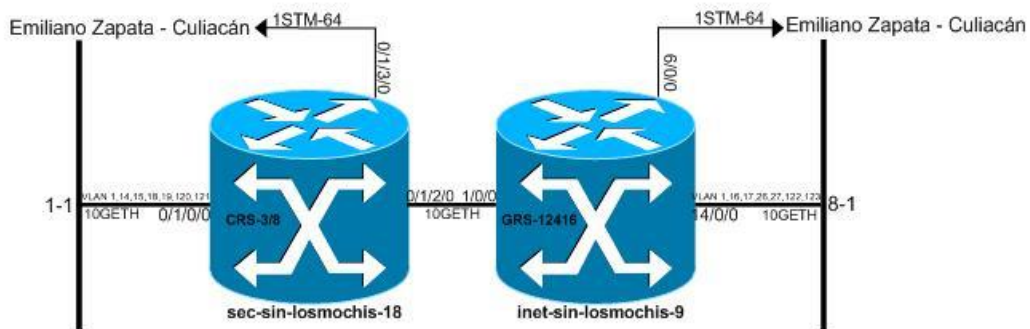
Cada interfaz OSPF puede presentar una clave de autenticación para que la usen los routers que envían información de OSPF hacia otros routers del segmento. La clave de autenticación, conocida como contraseña, es un secreto compartido entre los routers. Esta clave se utiliza para generar los datos de autenticación en el encabezado del paquete de OSPF. La contraseña puede contener hasta ocho caracteres, y se necesita utilizar la siguiente sintaxis de comando para configurar la autenticación de OSPF:

```
Router(config-if)#ip ospf message-digest-key key-id encryption-type md5 key
```

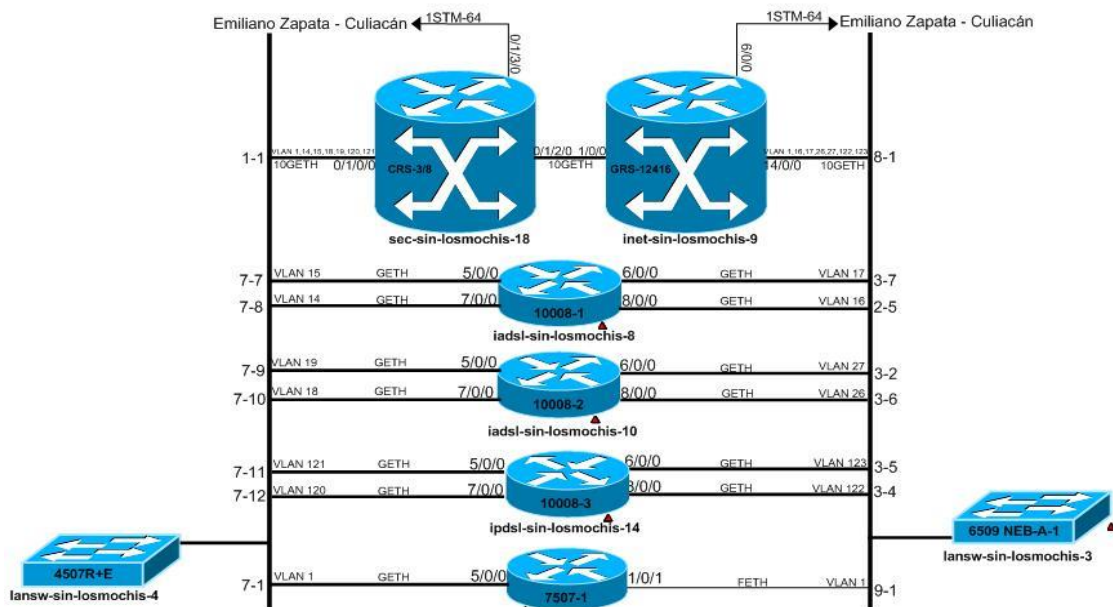
Una vez configurada la contraseña, se debe habilitar la autenticación:

```
Router(config-router)#area area-id authentication message-digest
```

Los tipos de redes utilizados en uniNet son los que se presentan en las figuras I2.4 y I2.5 donde la primera corresponde a Point to Point y la segunda a Point to Multipoint:



I2.4 Point-to-Point.



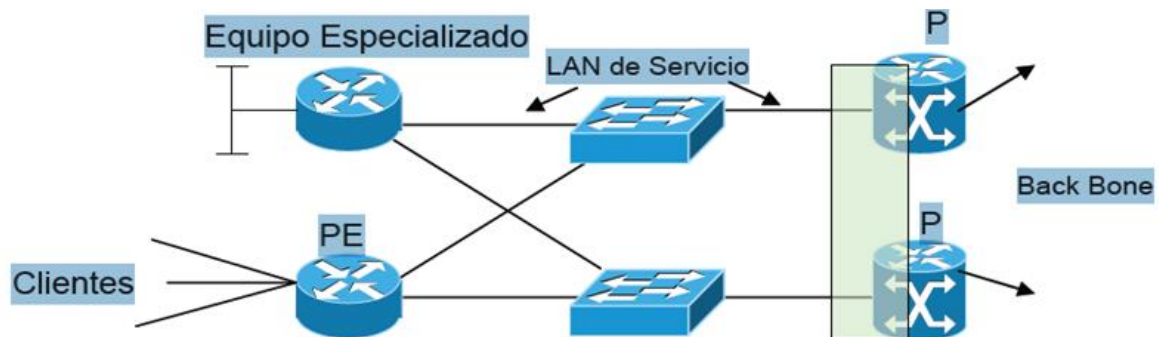
I2.5 Point-to-Multipoint.

2.2.4. Modelos y topologías para equipos PE

En la red Uninet las conexiones hacia los lanswitches, como conexiones de trabajo y conexiones de respaldo.

LAN_TRABAJO: LAN por la que transita todo el tráfico del nodo.

LAN_RESPALDO: LAN que solo se utilizaba en caso de contingencia. Por lo que se consideraba infraestructura “no utilizada”, en la imagen I2.6 se ilustra la topología entre los equipos PE con la LAN de servicio.



I2.6 Topología LAN trabajoy respaldo.

El valor del ancho de banda de las interfaces que conectan hacia ambas LANs deben de ser el valor del ancho de banda físico de la interfaz.

En todas las interfaces que conectan hacia la LAN deberán tener configurado el mismo costo de OSPF indicado para el tipo de interfaz.

2.2.5. Equipos para servicio INFINITUM iadsl, ipdsl y dsl (BRAS)

Los equipos BRAS (Broadband Remote Access Server), son utilizados en la red UNINET para el servicio INFINUTUM, servicio que ofrece TELMEX mediante una conexión directa de acceso a Internet de alta velocidad, utilizando como medio de acceso la línea telefónica.

Los modelos de equipos utilizados para esta funcionalidad son:

- Juniper E320
- Cisco 10008 (con procesadoras PRE-2 y PRE-4)
- Cisco 7206
- Cisco ASR1006 (solo existe un equipo presente)

La diferencia entre ellos, radica en la cantidad de usuarios que soporta cada plataforma.

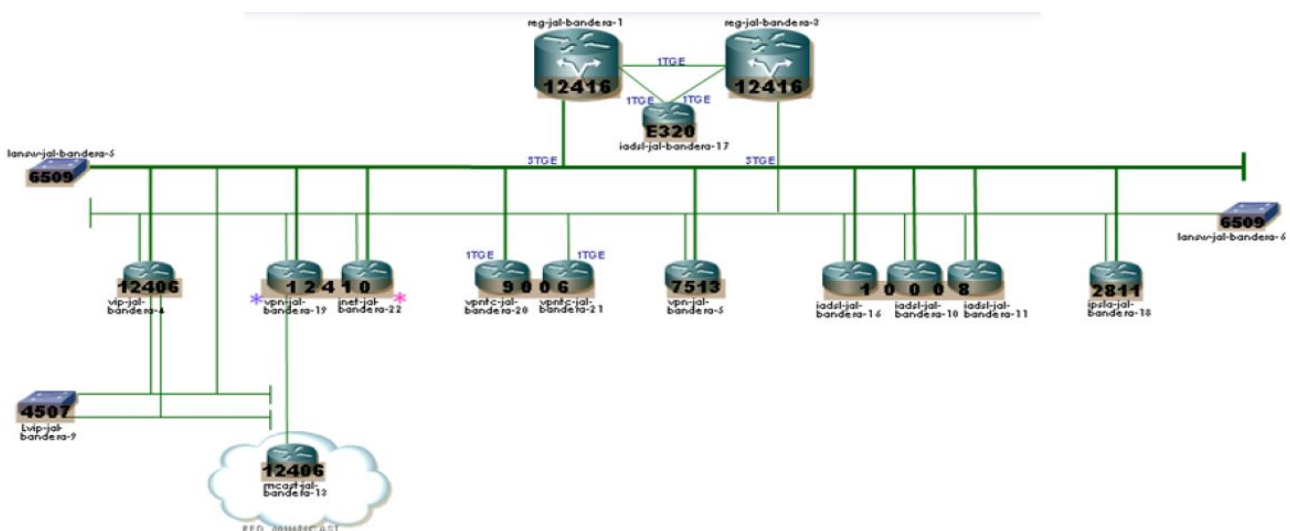
Las diferencias entre la decisión de un hostname radican en la tecnología que maneja el equipo:

dsl: Solo tiene interfaces ATM y los equipos de agregación de TELMEX que se conectan son únicamente DSLAM's.

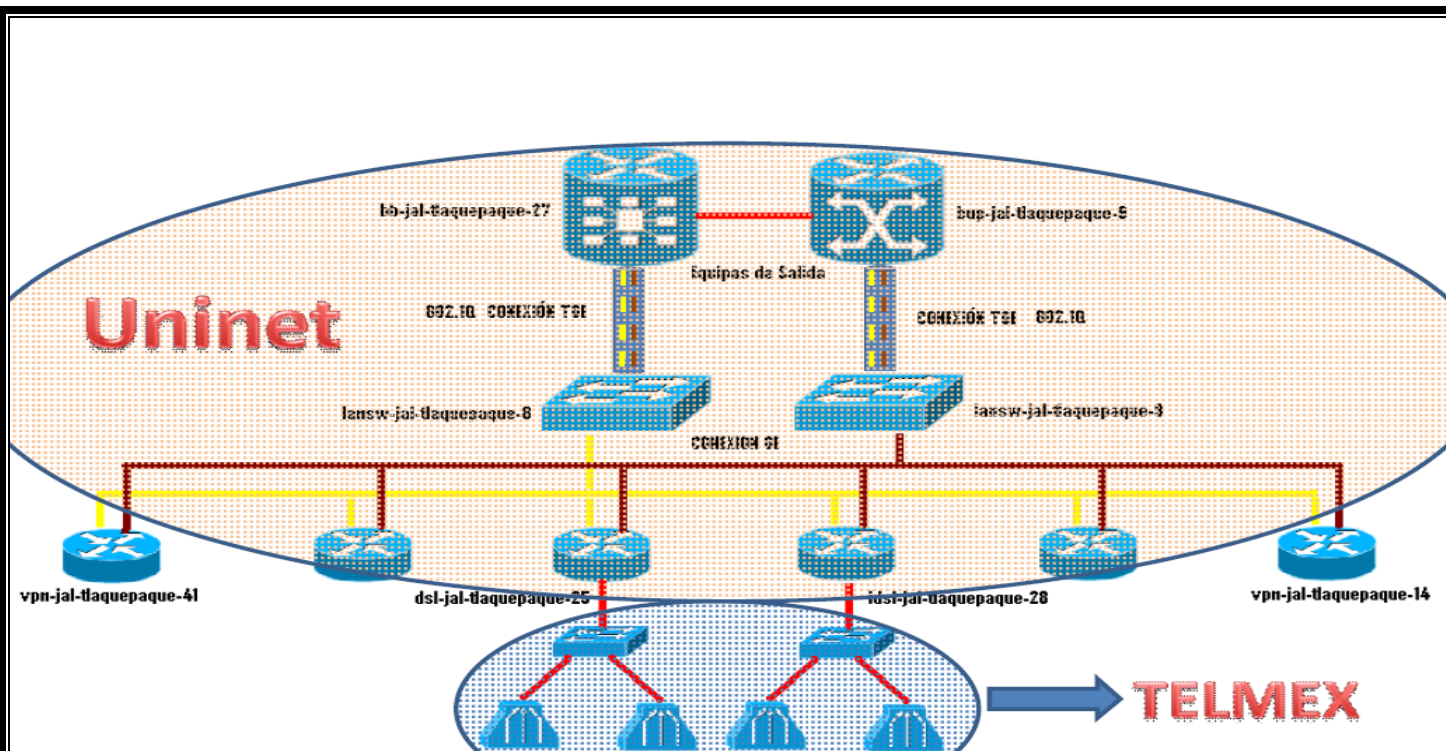
lpdsl: Solo tienen interfaces GigabitEthernet y los equipos de agregación de TELMEX que se conectan son TIBAS, ISAM, TBA y GPON.

iadsl (híbridos): Tienen interfaces ATM y GigabitEthernet y se conectan a el cualquier equipos de agregación de TELMEX.

En la imagen I2.7 se muestran las conexiones hacia las LANs de servicio, mientras que en la imagen I2.8 se ilustra la conexión de los equipos IPDSLAMs hacia los equipos BRAS de UNINET por medio de uplinks.



I2.7 Conexión de equipos BRAS hacia las LANs de servicio



12.8 Conexión por medio de uplinks de equipos IPDSLAMs (TELMEX) hacia Los equipos BRAS (UNINET).

2.2.6. OSPF en equipos BRAS

En los equipos BRAS que se reciben mediante una conexión BTB o mediante una conexión a LAN, es necesario meter el NET ID de la conexión y la ip de la interfaz L0 en el proceso de OSPF 64512, esto se hace con los siguientes comandos.

- network <NET-ID> <Wild Card> area A.B.C.D
- network <loopback0> <0.0.0.0> area A.B.C.D

Para todas las conexiones Ethernet punto a punto es necesario aplicar el Comando: ip ospf network point-to-point, en IOS-XR a nivel de OSPF y en IOS e IOS-XE a nivel de interfaz.

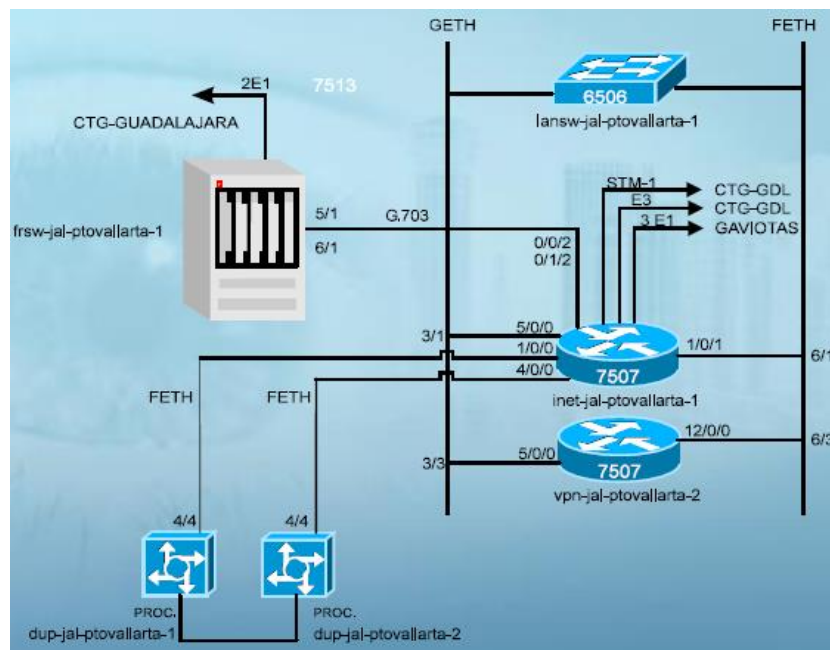
2.2.7. BGP en equipos BRAS

Sólo manejan sesiones de iBGP, esta se establece con el equipo que le da salida, siendo el dsl cliente del equipo de salida. En la configuración de la sesión en el equipo de salida.

2.2.8. Equipos con funcionalidad INET

Los equipos con funcionalidad INET son routers de tránsito que comparte funciones con la concentración de servicios de internet como: Internet Directo Empresarial (IDE), conexiones hacia Frame Relay (local y remoto) y dial up (lan local, nas o enrutador remoto) o cualquiera de sus combinaciones.

En la imagen I2.9 se ilustra la topología, Inet concentrando FR y dup.



I2.9 Inet concentrando FR y dup

En caso de que los equipos dup se encuentren en una LAN se agrega a la red ospf y la interfaz se pone en pasiva, en caso de que se encuentre conectado directo al equipo inet se agrega a bgp, en los equipos inet se agregan pooles con rutas estáticas para los usuarios de dial-up y El equipo inet utilizan ibgp hacia su equipo de salida que son los equipos sectoriales.

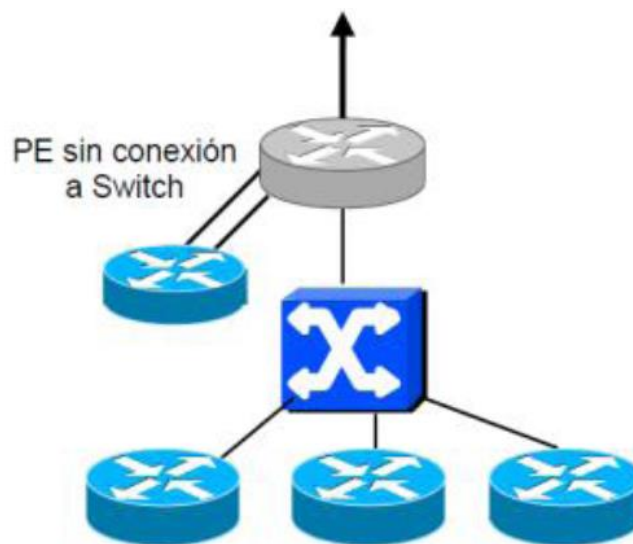
2.2.9. Equipos con funcionalidad SECTORIAL

Enrutador de tránsito que tiene enlaces hacia equipos regionales (Se explican más adelante), puede concentrar equipos de acceso, no realiza funciones de acceso al servicio al cliente. Este tipo de equipos solo concentran un nivel de Dial (cualquier tecnología) o DSL, no concentra a otros o localidades, tampoco

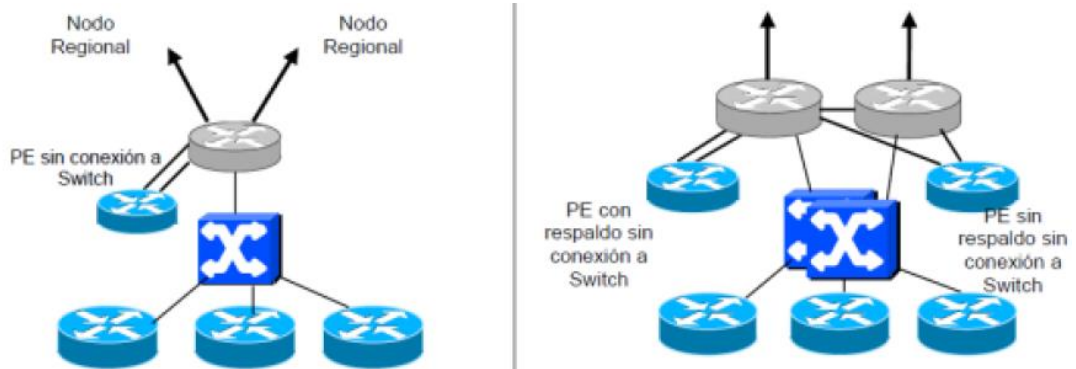
realizan funciones de tránsito a POPs (Point Of Presence) otros POPs de la red. Los nodos Sectoriales se conectan directamente a los equipos de tránsito Regionales.

Sí existe un nodo Sectorial con servicios de IDE, VPN o bien sean nodos DSL, estos se deberán de concentrar en 2 equipos Regionales, pudiendo ser estos enrutadores del mismo POP o de distinto POP. Zonas con múltiples POPs sectoriales pueden ofrecer IDE y VPN solo en el POP sectorial que cuente con 2 enlaces a nodos regionales o enrutadores regionales de nodo backbone de cualquier POP. Se permite que un nodo sectorial con equipo de tránsito se conecte a equipos regionales de ciudades distintas.

En la imagen I2.10 se ilustra una topología del tipo Nodo sectorial con equipo de tránsito con un sólo enlace a equipo regional, por otro lado en la imagen I2.11 se ilustra la topología tipo Nodo sectorial con equipo de tránsito con dos enlaces a dos equipos regionales.

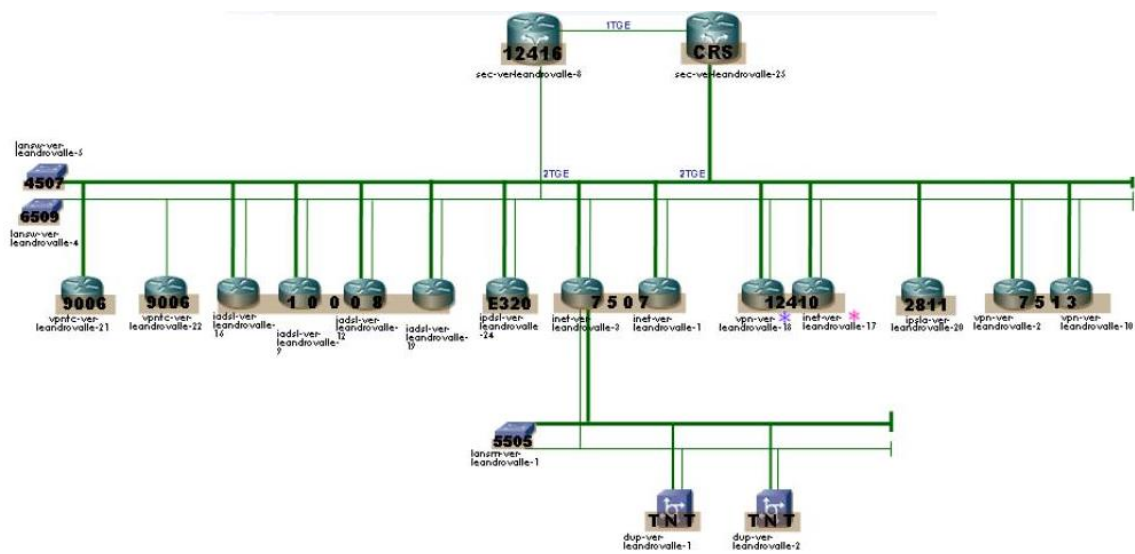


I2.10 Nodo sectorial con equipo de tránsito con un sólo enlace a equipo regional.



I2.11 Nodo sectorial con equipo de tránsito con dos enlaces a dos equipos regionales.

La imagen I2.12 ilustra un nodo real.



I2.12 Nodo real

2.2.10. OSPF en equipos sectoriales

Los enrutadores que hacen las funciones de tránsito en cualquier tipo de POP serán los equipos Router Designado (DR) y Router Designado de Respaldo (BDR), en el caso de existir solamente un enrutador de tránsito, este será el DR en donde:

DR: Lleva a cabo tareas de envío y sincronización.

BDR: Solo actuara si el falla (DR).

Para asegurar que estos equipos cumplan esta función todos los enrutadores de la LAN que no sean estos tendrán el comando "ip ospf priority 0"

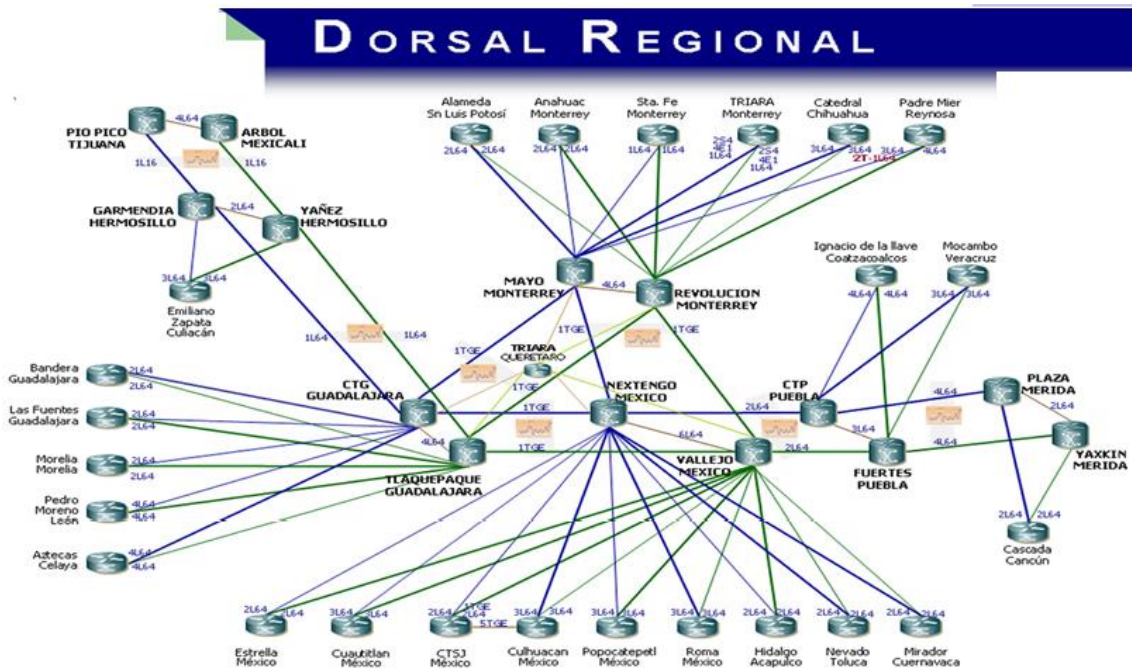
2.2.11. Equipos con funcionalidad REGIONAL.

El equipo Regional realiza funciones de concentración de otros Pop's y de tránsito hacia el Backbone. La conexión hacia el nivel de Backbone es con al menos 2 enlaces diversos independientemente del ancho de banda. Los equipos Regionales se clasifican de la siguiente forma:

Nacionales.- Funciones de concentración y tránsito para una región o regiones del país.

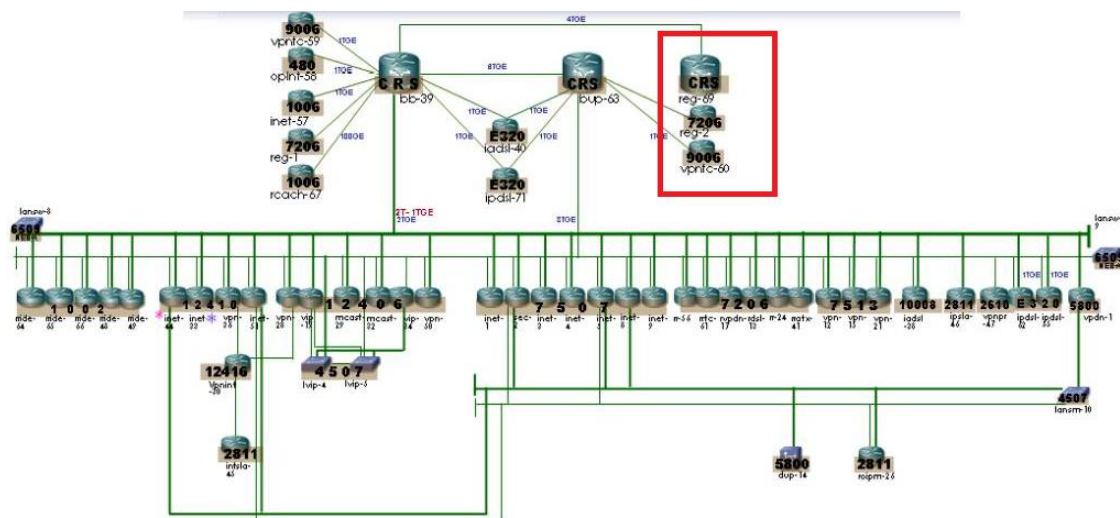
Metropolitanos.- Funciones de concentración y transito dentro de una misma zona metropolitana.

En uniNet se cuentan con una variedad de nodos regionales como se muestra en la imagen I2.13



12.13 Nodos Regionales

A manera de ejemplo se muestra un nodo funcional imagen 12.14.



12.14Ejemplo de nodo real en uniNet.

2.2.12. OSPF en equipos regionales

Los enrutadores que hacen las funciones de tránsito en cualquier tipo de POP serán los equipos Router Designado (DR) y Router Designado de Respaldo

(BDR), en el caso de existir solamente un enrutador de tránsito, este será el DR en donde:

DR: Lleva a cabo tareas de envío y sincronización.

BDR: Solo actuara si el falla (DR).

Para asegurar que estos equipos cumplan esta función todos los enrutadores de la LAN que no sean estos tendrán el comando "ip ospf priority 0".

En los enlaces GigabitEthernet ó TenGigabitEthernet punto a punto que conecten dos equipos de infraestructura ya sea entre niveles de Backbone a Regional, de regional a sectorial, Back-to-back entre equipos de tránsito de un nodo regional o sectorial, back-to-back el tipo de interface de OSPF deberá forzarse a punto a punto utilizando el comando: ip ospf network point-to-point.

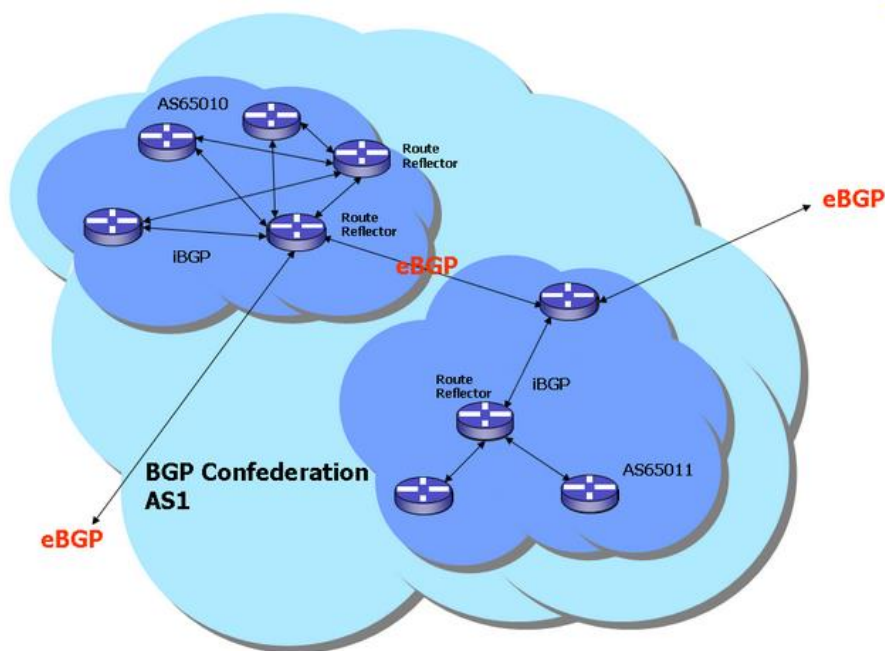
2.2.13. BGP en equipos regionales

Los equipos Regionales se encargan de enviar actualizaciones de rutas a todos los routers directamente conectados (Clientes) a través de BGP, esto sirve para ahorrar recursos de la red y evitar que esté completamente interconectada.

Configuración de Route Reflector (Este equipo se explica más adelante):

- El router reflector contará con sesiones de iBGP con los BB y BUP, con sus clientes (Pe) de servicios (DSL – IDE) o equipos Sectoriales de otras regiones.
- Las sesiones de eBGP con las que contará será con clientes como Telgua Correo Triara que cuentan con diferente AS.

A continuación se muestra la topología para BGP (Imagen I2.15)



12.15 BGP en equipos regionales

2.2.14. Equipos con funcionalidad BACK BONE.

Los BB (Back Bone) y BUP (Back Up) tienen como objetivo hacer el tránsito y forwarding del tráfico de todos los servicios PE'S de acceso a clientes y otros servicios (RADIUS, DNS, PE IDE, PE VPN Y BRAS)

2.2.15. BUP: Equipos de respaldo de los BB.

Los BB se encuentran a Nivel Dorsal de la red, y realizan funciones de tránsito e intercambio de información de enrutamiento.

2.2.16. OSPF y BGP en equipos Back Bone.

El proceso OSPF es: 64512

Área: 0.0.0.0 en BB Nacionales, cambia para los BB internacionales de acuerdo al Sistema Autónomo al que correspondan.

Las interfaces de las interconexiones o los enlaces Tenga o Giga, deberán ser configuradas como:

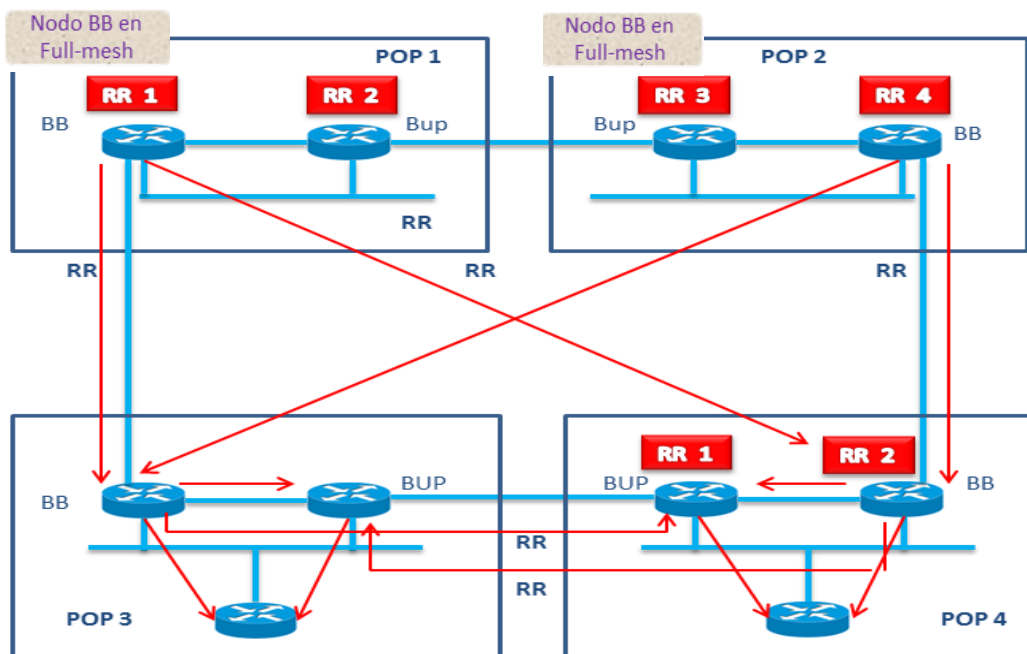
Ip network point-to-point

Con el fin de cumplir la política de respaldo de BGP, será necesario aplicar un Filter-list en el protocolo OSPF en el área que conecta a USA que no permita el anuncio de la interface Loopback 0 del enrutador BB del mismo POP, para que cuando se caiga el enlace primario del POP también se caiga la sesión en BGP.

2.2.17. Protocolo EGP (External Gateway Protocol)

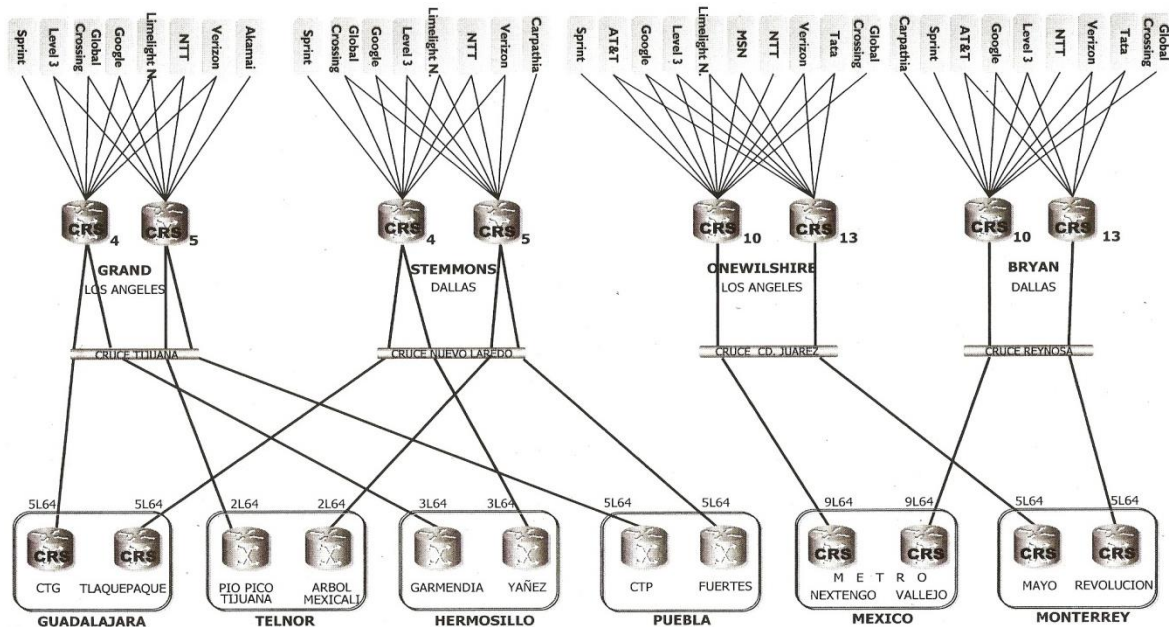
- Permite establecer sesiones de vecinos:
- Mismo sistema Autónomo (iBGP): Sistema Autónomo de Uninet 8151
- En diferente sistema autónomo (eBGP).

Para iBGP Tiene relación con vecinos internos del tipo Fully Meshed → Configuración Route reflector: Puebla Mérida Hermosillo y Tijuana. La imagen I2.16 muestra las secciones Fully Meshed entre los equipos Back Bone y los equipos Route reflector.



I2.16 iBGP en uniNet

En la imagen I2.17 tenemos la topología a nivel back bone y se pueden apreciar las conexiones con los carriers o proveedores a los cuales se tienen peticiones desde un cliente en casa.



I2.17 Topología a nivel Back Bone

2.2.18. Equipos con funcionalidad RRIDE

Los RRIDE no están orientados a ser enrutadores propiamente, los RRIDE están orientados a la distribución de las rutas dentro de un SA (Sistema Autónomo), reflejando las rutas aprendidas a sus clientes RRc.

La finalidad de estos equipos es incrementar la disponibilidad y escalabilidad de la red a través de:

- Otorgar mayor redundancia y disponibilidad en la red.
- Evitar la saturación en equipos en cuanto a rendimiento y procesamiento.
- Establecer sesiones BGP

Los Route Reflector contarán con la topología de redundancia adecuada para garantizar el correcto funcionamiento de los servicios de Internet.

El crecimiento de los Route Reflector será en pares, cada uno adecuado a cada malla, en cada nodo que lo requiera de acuerdo al número de cliente.

Para cuidar la integridad de la tabla de enrutamiento, se establecen relaciones de vecinos BGP en full-mesh esto en mallas .

Dependerá del tipo de sesión que se establezca interna iBGP o externa eBGP.

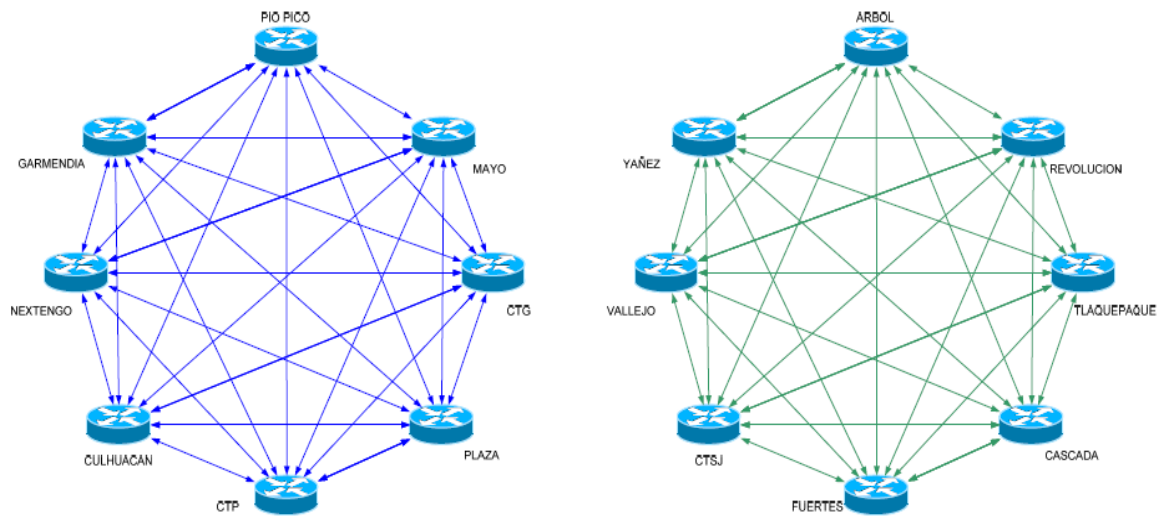
- Las rutas aprendidas eBGP son enviada a todos los vecinos.
- Las rutas aprendidas iBGP son enviadas a vecinos eBGP.
- Las rutas originadas localmente son enviadas a todos los vecinos.

Al conjunto de RRs y sus respectivos RRc se conocen como CLUSTERS.

Un Cluster es una división lógica de un grupo de enrutadores que se adecúan a la conexión física de la red. Para el caso de la arquitectura de UNINET:

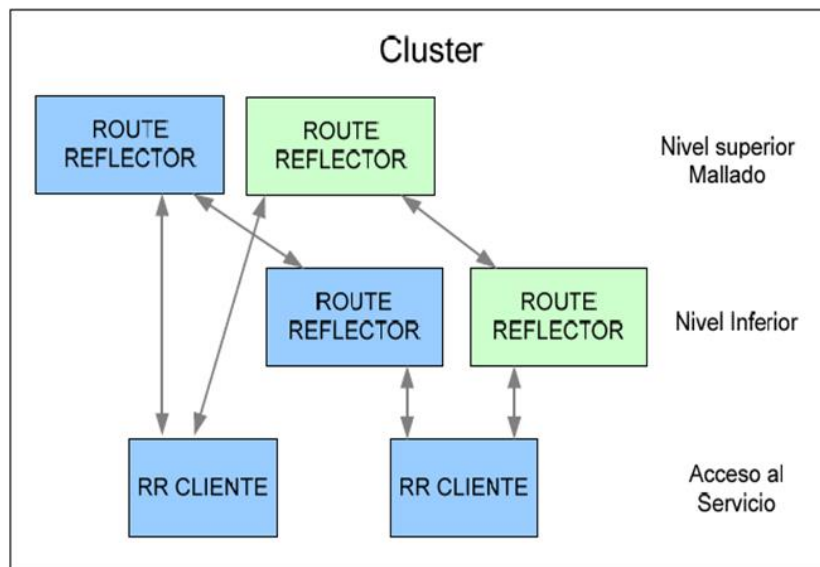
- Guadalajara
- Monterrey
- Hermosillo
- México1
- Telnor
- México2
- Puebla
- Mérida

En la figura I2.18 se muestran las mallas con los route reflectors en uniNet



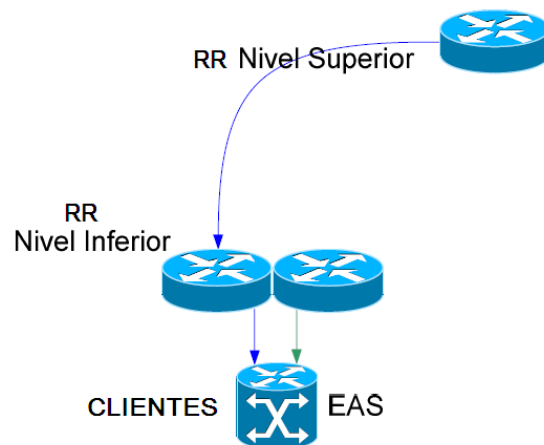
I2.18 Mallas conformadas con Route Reflectors con sesiones Fully Meshed.

En la figura I2.20 Se muestran los módulos funcionales.



I2.20 Módulos funcionales.

En la figura I2.21 se muestra un ejemplo de la topología entre route reflectors de nivel superior y de nivel inferior.



I2.21 Topología Entre RR de nivel Superior y de nivel inferior.

Lo antes descrito engloba al proyecto Infraestructura en el que mi participación fue llevar a cabo la recepción de enlaces punto a punto que va desde configuración básica en ambas interfaces (Cuando ambas puntas corresponden a uniNet) hasta que ambos equipos tengan comunicación de capa 3 por medio de un ping, validación de adyacencia por medio de los protocolos CDP, ARP en caso de ser enlaces hacia un carrier solo una punta es la que se configura, para los enlaces entre equipos de uniNet realicé documentos para el enrutamiento que se realizaban a partir de las 8 de la noche por políticas de la empresa.

Me dediqué a la recepción de equipos de las distintas funcionalidades desde la conexión fuera de banda por medio de equipos de acceso remoto hasta realizar un documento para el enrutamiento del equipo en uniNEt, así como la configuración básica o completa de cada uno de ellos, estos rubros se decidían dependiendo la actividad si se realizaría una migración o se pondría un equipo nuevo en operación. Mantener una correcta documentación de cada elemento de red esto lo realicé a mi ingreso a la empresa durante aproximadamente 6 meses.



Capítulo 3

Proyectos de

Automatización

De procesos en

La red UNINET

3.1. Proyectos de automatización de procesos en la red UNINET

En uniNet se lleva a cabo una completa y correcta documentación acerca de cada implementación efectuada en la red por medio de una herramienta llamada Service Manager, en dichas implementaciones se detectan tres problemas tanto técnicos como de documentación principales.

- Las descripciones en cada interfaz que se conectan ya sea a un enlace o una interconexión se configuran de manera manual existiendo inconsistencias en la nomenclatura impuesta en las normas de uniNet.
 - No se tiene control de los clientes de hotSpot, tampoco de la infraestructura dada de alta en seguridad uniNet por lo tanto tampoco de su direccionamiento
 - En los procesos que se realizan en automático no se tienen contempladas las interconexiones tipo Carrier Ethernet.
-
- Objetivo del proyecto: Dar solución a las problemáticas detectadas por medio de un sistema híbrido (Cliente-Servidor).
 - Participantes: Administradores de configuraciones, Supervisores de Implementaciones.

Propuesta:

Se plantean tres sistemas WEB con características de seguridad para dar solución a cada una de las problemáticas detectadas.

1. GENERADOR DE DESCRIPCIONES PARA INTERFACES EN LA RED UNINET
2. PROCESO ITX CE
3. HOT SPOT

3.1.1. Topología de solución

Para la solución a los problemas detectados en uniNet se propone un sistema híbrido (Cliente y servidor) ya que realizará procesos en automático y es necesaria este tipo de arquitectura.

Se requieren de los siguientes elementos de red para poder conformar el sistema.

-Cliente: Computadora que utiliza un ingeniero que introducirá los datos necesarios mediante interfaces WEB al sistema para que este realice los procesos necesarios.

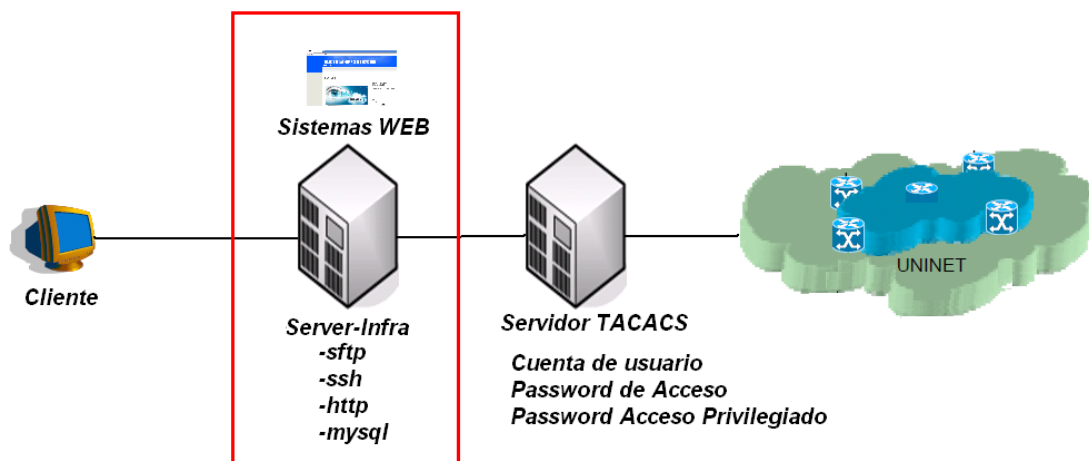
-Server-Infra (Cliente y Servidor): Será el servidor del Cliente quien recibe los datos de entrada y realiza los procesos necesarios (En algunas ocasiones realiza una segunda petición al servidor de TACACS) para así entregar salidas de Valor al ingeniero que opera en uniNet, cuenta con los servicios:

- **SFTP (Secure File Transfer Protocol):** Servicio que utiliza el protocolo que sirve para cargar y descargar archivos de manera segura para y desde Server-Infra.
- **SSH (Secure Shell):** Servicio que utiliza protocolo que nos ayuda a tener acceso remoto al servidor desde el cliente de manera segura ya que todos los datos viajan de manera cifrada.
- **HTTP(Hypertext Transfer Protocol):** Servicio que utiliza el protocolo usado en cada transacción de WWW (World Wide Web) y las peticiones se realizan desde el cliente por medio de un navegador WEB o "User Agent".
- **MySQL:** Es un servicio de gestión de base de datos que ayudará a guardar la información necesaria para que pueda operar el Server-Infra mediante autenticaciones y algunos otros campos.

-Servidor TACACS (Terminal Access Controller Acces Control System): Permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red o no, este servidor no es

gestionable por el departamento de Gestión de Cambios y Configuraciones si no por el departamento de Seguridad, en el Servidor TACACS se tienen datos de alta los usuarios que tienen los privilegios para acceder a los equipos de uniNet .

En la imagen I3.0 se muestra la arquitectura funcional del Server-Infra



I3.0 Arquitectura funcional del Server-Infra

3.1.2 SISTEMA 1. Generador de descripciones para interfaces en la red uniNet.

3.1.3. .Planteamiento del problema 1

Para poder generar una descripción de manera correcta se tienen ciertas normas, se define la nomenclatura a utilizar en los equipos de la red IP de nueva generación por su nivel funcional y de topología.

La nomenclatura estará basada en el nivel que ocupa cada equipo dentro de la topología de la red.

- Los nombres de las centrales serán los mismos que utiliza TELMEX para cada una de ellas.
- La nomenclatura estará basada en la capacidad de caracteres que posea cada equipo.

La red de IP de Nueva Generación tiene tres niveles: backbone de servicios, acceso al servicio y CPE, la nomenclatura para los equipos estará basada en el nivel que ocupan en la topología de la red; en la cual están definidos los siguientes niveles jerárquicos:

- Backbone
- Regional
- Sectorial

Antes de proceder a la correspondiente explicación de cada descripción cabe mencionar las diferencias entre ENLACE, CONEXIÓN, e INTERCONEXIÓN así como las tablas que ayudarán a comprender la nomenclatura.

- Un ENLACE se establece entre los nodos que conforman la red UniNet.
- Una CONEXIÓN se establece entre equipos ubicados en el mismo nodo, independientemente del número de salas que lo conformen.
- Una INTERCONEXIÓN se establece entre equipos ubicados en el mismo nodo, con la infraestructura de otro proveedor de servicios.

En la tabla T3.1 se explican las siglas para cada tipo de enlace

T3.1 Siglas para tipo de enlace nacional, internacional o intercambio.

TIPO DE ENLACE	DEFINICION
BBI	Enlace entre Nodo de Backbone Nacional y Nodo de Backbone Internacional
BBN	Enlaces entre Nodos de Backbone Nacionales
CAC	Enlace de nodos UniNet con servicio de Caching.
CAR	Enlaces entre un Nodo UniNet para transporte de trafico con un carrier.
INT	Enlace Internacional de Salida a Internet
NST	Enlace de nodos UniNet con nodo satelital.
PEE	Enlace entre un Nodo UniNet con intercambio de tráfico de internet hacia otras redes.
REG	Enlace entre Nodo Regional-Regional y Regional-Backbone
SEC	Enlace entre Nodo Sectorial-Sectorial, Sectorial-Regional o Sectorial-Backbone
SEAD	Enlace entre un nodo Sectorial que agrega servicios de DSL y/o Dial-Up vía la Red de Transporte Telmex con tecnología DWDM hacia otro nodo Sectorial, Regional o de Backbone
SEAS	Enlace entre un nodo Sectorial que agrega servicios de DSL y/o Dial-Up vía la Red de Transporte Telmex con tecnología SDH hacia otro nodo Sectorial, Regional o de Backbone

En la tabla T3.2 se muestran los carriers hacia donde uniNet tienen enlaces

T3.2 Tabla de Carriers

CARRIER
ATT
BRITISH TELECOM
GBLX
LEVEL3
NTT
ORANGE
SBC
SPRINT
VERIZON

En la tabla T3.3 se muestran los peer's hacia donde uniNet tienen enlaces

T3.3 Tabla de Peer

PEER	TIPO
AKAMAI	INTERNACIONAL Y NACIONAL
ALESTRA	NACIONAL
ATT	NACIONAL
AVANTEL	NACIONAL
BESTEL	NACIONAL
GLOBALCROSSING	INTERNACIONAL
GOOGLE	INTERNACIONAL
IUSACELL	NACIONAL
LIMELIGHT NETWORKS	INTERNACIONAL
MARCATEL	NACIONAL
MCM	NACIONAL
METRORED	NACIONAL
MSN	INTERNACIONAL
PROTEL	NACIONAL

En la tabla T3.4 se describen las velocidades en los medios de transmisión.

T3.4 Velocidades en los medios de transmisión

TIPO DE ENLACE	DESCRIPCION
E1	Enlace de 2048 Kbps
E3	Enlace de 34 Kbps
FT	Enlace de 100 Mbps
STM1	Enlace de 155 Mbps
STM4	Enlace de 622 Mbps
STM16	Enlace de 2.5 Gbps
STM64	Enlace de 10 Gbps
GE	Enlace de 1 Gbps
TGE	Enlace de 10 Gbps
100GE	Enlace de 10 Gbps

En la tabla T3.5, T3.6, T3.7 y T3.8 se describen el tipo de conexiones General, Dorsal, Acceso e IPTV correspondientemente.

T3.5 Tipo de conexión General

TIPO DE CONEXIÓN	DESCRIPCION
BTB	Back to Back (router-router / lansw-lansw)
ROUTER	LAN Switch-router / NAS-router
NAS	Router-NAS

T3.6 Tipo de conexión Dorsal

TIPO DE CONEXIÓN	DESCRIPCION
LANSW_TRABAJO	LAN primaria o default de la red
LANSW_RESPALDO	LAN secundaria o de respaldo de la red.

T3.7 Tipo de conexión Acceso

TIPO DE CONEXIÓN	DESCRIPCION
LANSM_TRABAJO	LAN primaria o default de servicios y gestión.
LANSM_RESPALDO	LAN secundaria o respaldo de servicios y gestión.
LAN_PRIVADA_TRABAJO	LAN primaria o default para el servicio WiFi Infinitum Móvil.
LAN_PRIVADA_RESPALDO	LAN secundaria o respaldo del servicio WiFi Infinitum Móvil.
LAN_PUBLICA_TRABAJO	LAN primaria pública o default para el servicio WiFi Infinitum Móvil.
LAN_PUBLICA_RESPALDO	LAN secundaria pública o respaldo del servicio WiFi Infinitum Móvil.

T3.8 Tipo de conexión Para IPTV

TIPO DE CONEXIÓN	DESCRIPCION
LAN_IPTV_TBJ	LAN primaria o default para servicio de IPTV.
LAN_IPTV_RSP	LAN secundaria o de respaldo para el servicio de IPTV.
LAN_MONITOREO	LAN para Monitoreo del servicio IPTV.
LAN_VOIP_TBJ	LAN IPTV primaria con VoIP
LAN_VOIP_RSP	LAN IPTV secundaria con VoIP

En la tabla T3.9 se describen los tipos de interconexiones

T3.9 Tipos de interconexiones

TIPO DE INTERCONEXION	DESCRIPCION
A_TELMEX	Anillo de Telmex
ABEX_ATT	Exchange de ATT
CE_PE_AMX	CE-AMX a PE-AMX
CE_TELMEX	Cluster Carrier Ethernet
DSLAM_ATM	Equipo DSLAM por ATM
DSLAM_IP	Equipo DSLAM por IP
EQ_CLIENTE	Equipos del cliente.
GX_IP	Equipo GX por IP
NNI_ATT	PE del NNI
NNI_BT	PE del NNI
NODO_SATELITAL	PE a Satelital
PSAX_ATM	Equipo PSAX por ATM
PSAX_IP	Equipo PSAX por IP
TBA	Equipo TBA
TELNOR	Equipos Telnor

3.1.4. Interfaz con enlaces.

La nomenclatura para la identificación de los enlaces, en una interfaz física, se ajustará de la siguiente manera:

ENLACE A [tipo de enlace] [capacidad del enlace] A [nomenclatura interfaz equipo destino/ carrier / peering] [referencia] [clave de aceptación][iniciales de quien configura] [fecha (dd/mm/aa)]

En donde:

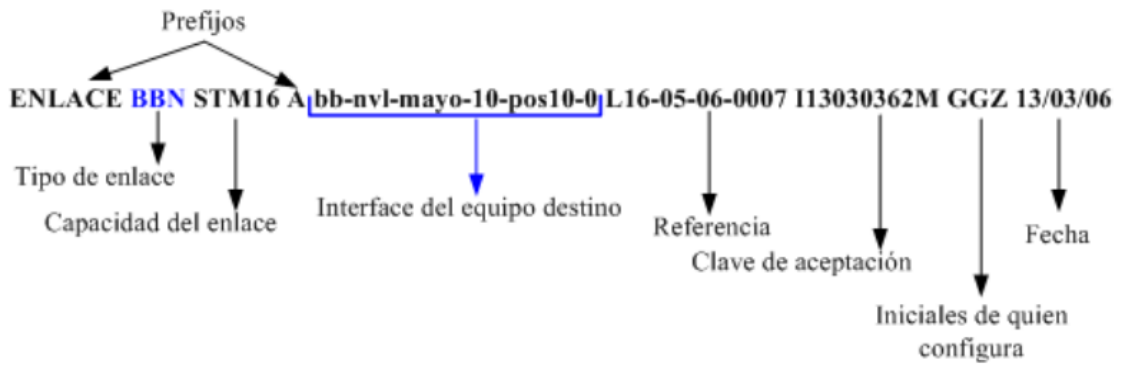
ENLACE, A [tipo de enlace] : Prefijos. Nivel jerárquico del enlace de transmisión, de acuerdo a la Siglas para Tipo de Enlace Nacional, Internacional o Intercambio, con letras mayúsculas.

Capacidad del enlace: Tipo de enlace a emplearse, de acuerdo a las Siglas para Capacidad de Enlaces, con letras mayúsculas.

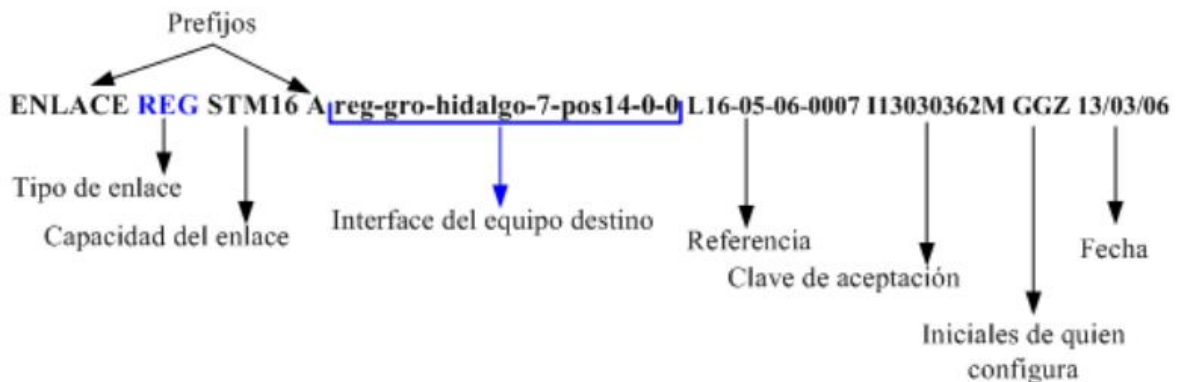
Nomenclatura interfaz equipo destino carrier / peering : Conforme a lo establecido en la nomenclatura para Interfaz equipo destino, con letras minúsculas. Nombre del Carrier, de acuerdo a la Tabla de Carriers , con letras mayúsculas. Nombre del Peer nacional o internacional, de acuerdo a la Tabla de Peer , con letras mayúsculas.

Referencia, clave de aceptación, iniciales de quien configura y fecha: Número con el cual se identifica al enlace, con letras mayúsculas. Número con el cual se recibe al enlace, con letras mayúsculas. Iniciales de ingeniero que configura el enlace, con letras mayúsculas. Fecha en la cual se configura la interface, con el formato dd/mm/aa.

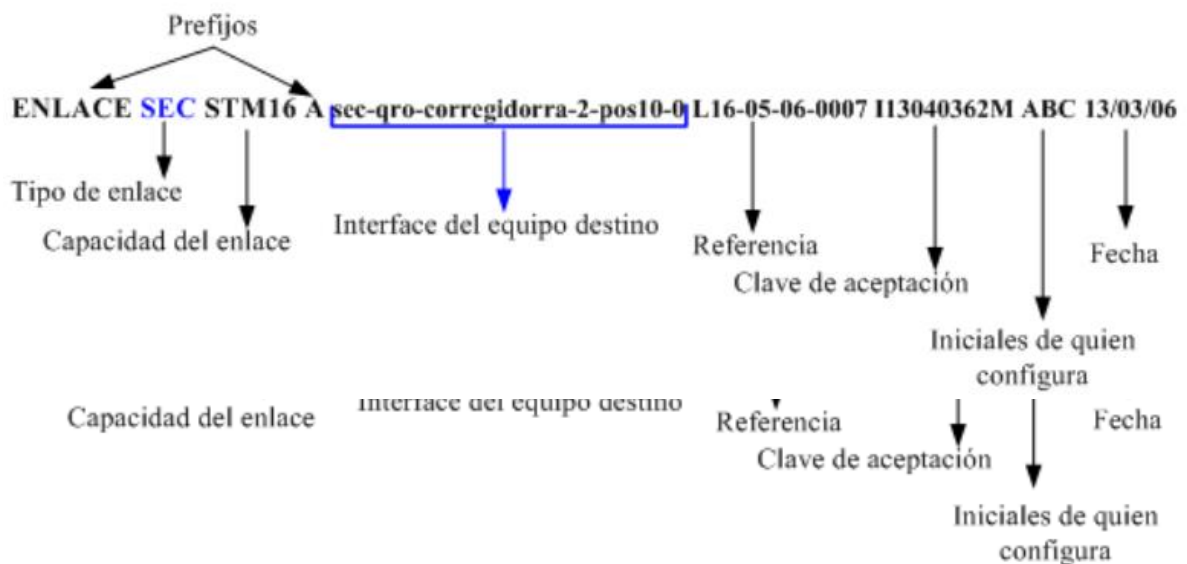
En las imágenes I3.1, I3.2, I3.3, I3.4, I3.5 y I3.6 se muestran ejemplos de descripciones correctas para la parte de los ENLACES:



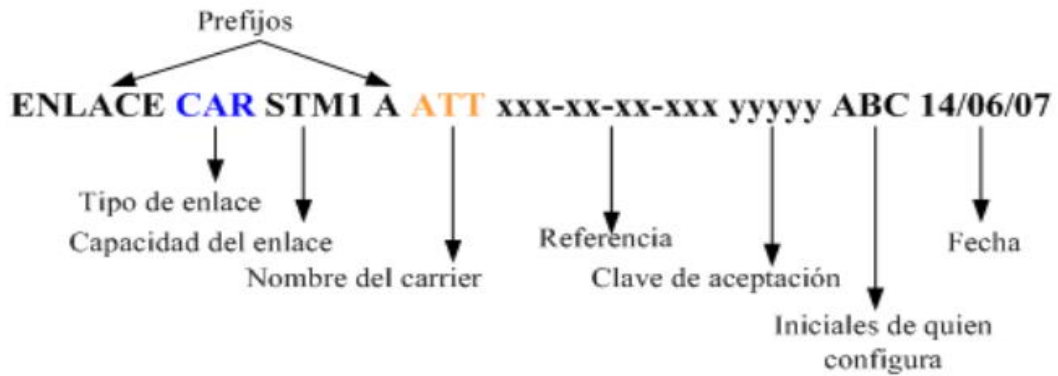
13.1 Ejemplo de la Nomenclatura para Identificar un Enlace de Backbone Nacional



13.2 Ejemplo de la Nomenclatura para Identificar un Enlace Regional.



13.4 Ejemplo para Enlace Sectorial que solo Agrega Servicios de DSL y/o Dial-Up.



13.5 Ejemplo de la Nomenclatura para Identificar un Carrier



13.6 Ejemplo de la Nomenclatura para Identificar un Peer

3.1.5. Interfaz con conexiones.

La nomenclatura para la identificación de las conexiones, se ajustará de la siguiente manera:

CONEXION [capacidad del enlace] A [nomenclatura interfaz equipo destino] [tipo de conexión] [iniciales de quien configura] [fecha (dd/mm/aa)]

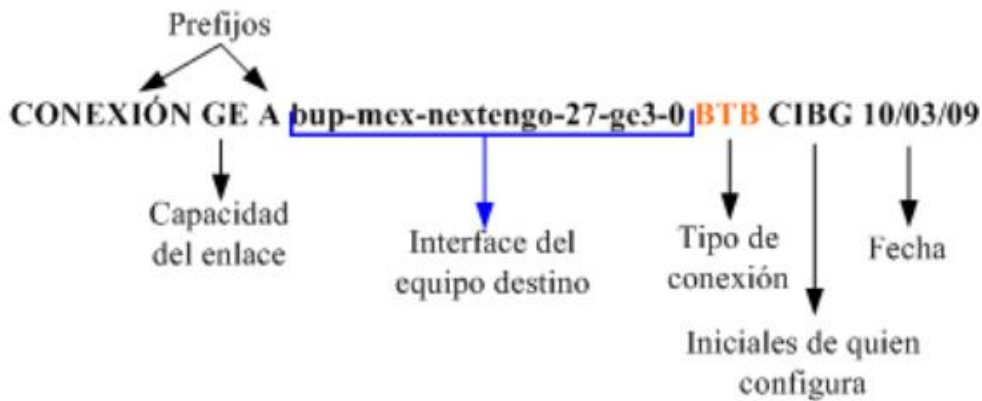
En donde:

CONEXIÓN A, capacidad del enlace: Prefijos. Tipo de enlace a emplearse, de acuerdo a las Siglas para Capacidad de Enlaces, con letras mayúsculas.

Nomenclatura interfaz, equipo destino, tipo de conexión: Conforme a lo establecido en la nomenclatura para Interfaz equipo destino, con letras minúsculas, Tipo de conexión a emplearse, de acuerdo a la Tabla de Tipos de

Conexión, con letras mayúsculas.

Iniciales de quien configura y fecha: Iniciales de ingeniero que configura el enlace, con letras mayúsculas, Fecha en la cual se configura la interface, con el formato dd/mm/aa.



13.7 Ejemplo del Identificador para Conexiones en una Interfaz

3.1.6. Interfaz con Interconexiones

La nomenclatura para la identificación de las interconexiones, se ajustará de la siguiente manera:

INTERCONEXION [capacidad del enlace] A [equipo destino] [tipo de conexión] [referencia] [clave de aceptación][iniciales de quien configura] [fecha (dd/mm/aa)]

En donde:

INTERCONEXION, A capacidad del enlace: Prefijos. Tipo de enlace a emplearse, de acuerdo a las Siglas para Capacidad de Enlaces, con letras mayúsculas.

Equipo destino tipo de conexión: Identificador del equipo destino (proveedor de servicios), con letras minúsculas. Tipo de interconexión a emplearse, de acuerdo a la Tabla de Tipos de Conexión con letras mayúsculas

Referencia: Número con el cual se identifica a la interconexión, con letras

mayúsculas.

Clave de aceptación: Número con el cual se recibe al enlace, con letras mayúsculas.

Iniciales de quien configura y fecha: Iniciales de ingeniero que configura el enlace, con letras mayúsculas y fecha en la cual se configura la interface, con el formato dd/mm/aa.

3.1.7. Solución para el problema 1

Propuse un sistema WEB que con base en las entradas necesarias para que realicen correctamente las descripciones con base en las normas que se rigen en uniNet para este rubro.

Autenticación (imagen I3.8)

El usuario debe de estar previamente dado de alta en la base de datos en servidor para poder acceder al sistema.



I3.8 Interfaz de usuario para ingresar la autenticación

Menú principal (imagen I3.9).

Se muestra el nombre del ingeniero que se autentique, así mismo se muestra el menú principal en donde se deberá de elegir la pestaña GENERADOR DE DESCRIPCIONES PARA INTERFACES EN LA RED UNINET



I3.9 Interfaz del menú principal

Menú de descripciones (Imagen I3.10)

Se desplegará un menú con las pestañas correspondientes para la generación de descripciones que el ingeniero deberá elegir, y dos links para descargar las normas de nomenclaturas para descripciones.



13.10 Interfaz del menú de descripciones

Al elegir algunas de las opciones para generar las descripciones de manera Automática se muestra un formulario para indicar las entradas al sistema (Imagen 3.11).



13.11 Interfaz del formulario de entradas al sistema para generar descripciones

Cabe mencionar que no se permiten caracteres que no deban de ir en la descripción en cuestión por lo que se reduce aun más el margen de error en caso de espacios se eliminan en automático para que solo vallan los espacios que realmente deben de ir conforme a la norma. Al presionar en el botón de GO se crea la descripción con base en las normas establecidas por uniNet, el cual el ingeniero a cargo deberá de pegar a nivel de configuración de la interfaz correspondiente (Imagen I3.12).



13.12 Generación en Automático de la descripción en la interfaz

Este proceso se lleva a cabo de manera automática en base a la corrección de posibles errores humanos como por ejemplo el poner espacios de mas o poner letras mayúsculas, al limpiar cada una de las cadenas de entrada el sistema las concatena con los espacios que se deben de tener en cuenta, todo esto con código en PHP como se muestra en la imagen I3.13.

```
$inicialesnew=strtoupper($inicialesnew);  
$claveacceptnew=strtoupper($claveacceptnew);  
$referencianew=strtoupper($referencianew);  
$description="description " . $interconexion . " " . $capacidad . " A " . $equipodestinonew . "-" . $puerto . $slotnew . " " . $tipoconexion . " " . $referencianew . " " . $claveacceptnew . " " . $inicialesnew . " " . $fecha;
```

I3.13 Fragmento de código en PHP que concatena las cadenas para la generación de la descripción en interfaces

3.1.8. Planteamiento del problema 2

Como se ha comentado con anterioridad en uniNet se tienen ciertas políticas de documentación en el departamento de Gestión de Cambios Y Configuraciones, donde generamos un paquete llamado Plan de Implementación el cual se describe a continuación.

Descripción de la problemática

3.1.9. Documentación de Plan de Implementación.

El Plan de implementación consta de los siguientes puntos véase la tabla T3.10:

Puntos del Plan de Implementación	Tipo de evidencia	Evidencia
a. Entregables de implementación acordados (adjuntos)	Archivos adjuntos	<ul style="list-style-type: none">• Checklist de condiciones iniciales• Respaldo Inicial• Respaldo Final• Log
b. Fecha de implementación	Campo de la Implementación	<ul style="list-style-type: none">• Implementación → <i>Fecha Planeada de Inicio</i>
c. Errores conocidos y problemas en caso de aplicar	Registros	<ul style="list-style-type: none">• Cola de Errores Conocidos / Cola de Problemas
d. Definición de Ventana de afectación	Campo del cambio	<ul style="list-style-type: none">• Cambio → Campos Variables → <i>Tiempo de Afectación (minutos)</i>
e. Definición de Ventana de intervención	Campo de la Implementación	<ul style="list-style-type: none">• Implementación → <i>Fecha Planeada de Inicio / Fecha Planeada de Fin</i>
f. RFC	Cambio	<ul style="list-style-type: none">• Implementación → <i>Registros relacionados</i>
g. Plan de Intervención ó CU (incluye el Plan de retorno)	Archivo Adjunto	<ul style="list-style-type: none">• Carpeta PI

T3.10 Documentación de Plan de Implementación

3.1.10. Políticas

1. Se deberá adjuntar un archivo **.rar** con la siguiente nomenclatura :
P_IMP_DDMMAA_ <SIGLAS ING>_ <NODO (en caso de que sean más de un nodo se nombra VARIOS)>

Ejemplos: P_IMP_071112_JCS_MAYO → para un solo nodo.
 P_IMP_071112_JCS_VARIOS → para más de un nodo.

2. El archivo **.rar** deberá contener las siguientes carpetas:
 - Seguimiento
 - PI (Plan de Intervención)
 - Validación Final

La carpeta generada en .rar contiene los archivos descritos en la tabla T3.11 dependiendo de la actividad que se realice: para el caso de las interconexiones Carrier Ethernet se muestran en color rojo los rubros que deben de llevar.

Nombre de la Carpeta		
Seguimiento	PI	Validación Final
Todos los archivos siguientes: <ul style="list-style-type: none"> • MAM_OFICIAL • Respaldo Inicial (equipo_INICIO) • Respaldo Final (equipo_FIN) • Log (equipo_LOG) • Checklist de condiciones Iniciales (equipo_INICIALES) 	El que aplique: <ul style="list-style-type: none"> • PI Genérico / PI Específico (Asegurar que SIEMPRE traiga la pestaña Backout) 	El / los que apliquen: <ul style="list-style-type: none"> • Validación IP Libre • Checklist Enlaces • Checklist Equipos • Winmerge • Pinger • Validación de servicio

T3.11 Documentación de Plan de Implementación

3. Si un Cambio tiene relacionado un Proyecto se deberán adjuntar el archivo **.rar** en el **PROYECTO**.
4. Si un Cambio **NO** tiene relacionado un Proyecto se deberán adjuntar el archivo **.rar** en el mismo **CAMBIO**.

Se detecta que al realizar una interconexión entre un equipo con funcionalidad dsl de uniNet y los equipos de TELMEX se otorga una ventana de tiempo de 1 hora, en este tiempo tenemos que realizar el plan de implementación con las políticas descritas con anterioridad además de configurar el puerto en el que se está recibiendo la interconexión en cuestión conforme a.....

Para equipos JUNIPER E320

interface gigabitEthernet X/X/X

mtu 1522 → Tamaño máximo en bytes que puede enviarse Y/O recibirse

duplex full → Ponemos en modo full duplex la interface para mantener una comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea

speed 1000 → Velocidad en megabits por Segundo

encapsulation vlan → configure las Vlan como un método de encapsulación para la interfaz

auto-configure vlan → Configura la interface Vlan estática para apoyar la detección automática de una subinterfaz VLAN dinámica.

Para equipos CISCO 10000

interface GigabitEthernet X/X/X

description ITX GE A NOMBRE_INTERCONEXION CE_TELMEX
REFERENCIA CLAVE_ACEPTACIÓN SIGLAS_CONFIGURADOR FECHA

no ip address → indicamos que la interface no tendrá una ip

no ip unreachable → Medida de seguridad recomendada para evitar ataques DoS

no ip proxy-arp → Para que no se mapeen las direcciones ip con una única dirección MAC que es la del router.

no negotiation auto → desactivar la auto negociación y es necesario ya que los equipos de TELMEX lo manejan de la misma manera, y de no concordar, no se establecería el LINK entre los equipos.

hold-queue 4096 in → Cola de entrada cae si el número del buffer alcanza su nivel máximo los valores van de 0 y 4096

hold-queue 4096 out → Cola de salida cae si el número del buffer alcanza su nivel máximo los valores van de 0 y 4096

Cabe mencionar que en ocasiones los compañeros en sitio o personal de CNS tardan un poco más del tiempo acordado para la ventana de tiempo lo que ocasiona que no se siga el proceso que lleva a cabo uniNet y para solventarlo es necesario pedir una ventana más de tiempo a los supervisores.

3.1.11. Solución al problema 2

Propuse un sistema WEB que con base en las entradas necesarias realicé la configuración y los respaldos necesarios en un menor tiempo, Anteriormente por parte de uniNet tardábamos un aproximado de 30 a 40 minutos en generar toda la documentación requerida con el apartado generado en el Server-Infra tardamos menos de hecho en 15 minutos aproximadamente y opera como se describe a continuación.

Autenticación (Imagen 3.14)

El usuario debe de estar previamente dado de alta en la base de datos del servidor para poder acceder al sistema.



13.14 Interfaz de usuario para ingresar la autenticación

Menú principal (Imagen I3.15)

Se muestra el nombre del ingeniero que se autentique, así mismo se muestra el menú principal en donde se deberá de elegir la pestaña PROCESO ITX CE



13.15 Interfaz del menú principal

Llenar el formulario correctamente con base en los rubros definidos en la imagen I3.16:

- Equipo CON DIVISIONAL.
- Puerto por lo general son en puertos Giga
- Slot: Solo poner el puerto con la nomenclatura x/x/x
- La fecha está por default
- Ingresar la referencia de la interconexión



I3.16 Interfaz del formulario de entradas al sistema para el proceso de interconexiones y generación de documentación en automático.

Confirmar la configuración que se realizará en el equipo (El sistema detectara si es Cisco 10000 o Juniper E320) (Imagen I3.17)



CONFIGURACION QUE SE REALIZARA EN EL EQUIPO iadsl-jal-lasfuentes-22.gdl EN LA INTERFAZ: GigabitEthernet11/0/2 conforme a:

En Cisco 10000

```
interface GigabitEthernet11/0/2
no ip address
no ip unreachable
no ip proxy-arp
no negotiation auto
hold-queue 4096 in
hold-queue 4096 out
```

En Juniper E320

```
interface GigabitEthernet11/0/2
mtu 1522
duplex full
speed 1000
encapsulation vlan
auto-configure vlan
```

ACEPTAR

13.17 interfaz de confirmación de la configuración que se realizará en el equipo e interfaz indicados

Esperar de 10 a 15 minutos en lo que se realizan todos los scripts alrededor de 6 los cuales fueron escritos en Bash debido a la facilidad de la comunicación entre equipos UNIX y las llamadas al sistema que realizan, estos scripts se hicieron de una manera jerárquica ya que un solo scrip manda a llamar a los demás como se muestra en la imagen I3.18

```

#!/bin/bash
cd /var/www/html/menu/description/scripts/carrier
./070613YRG-1305-1085version.sh > 070613YRG-1305-1085informe.txt
cd /var/www/html/menu/description/scripts/carrier
cat 070613YRG-1305-1085informe.txt | grep "isco*" > 070613YRG-1305-1085lineascisco.txt
lineas=$(wc -l < 070613YRG-1305-1085lineascisco.txt)
echo $lineas
if [ "$lineas" == "0" ]; then
echo "equipo juniper"
rm -rf ./070613YRG-1305-1085respaldocisco.sh
./070613YRG-1305-1085respaldojuniper.sh > 070613YRG-1305-1085loginicial.txt
./070613YRG-1305-1085configjuniperscript.sh > 070613YRG-1305-1085logconf.txt
./070613YRG-1305-1085respaldojuniper.sh > 070613YRG-1305-1085logfinal.txt
diff 070613YRG-1305-1085loginitial.txt 070613YRG-1305-1085logfinal.txt > 070613YRG-1305-1085diff.txt
else
echo "equipo cisco"
rm -rf ./070613YRG-1305-1085respaldojuniper.sh
./070613YRG-1305-1085respaldocisco.sh > 070613YRG-1305-1085loginicial.txt
./070613YRG-1305-1085configciscoscript.sh > 070613YRG-1305-1085logconf.txt
./070613YRG-1305-1085respaldocisco.sh > 070613YRG-1305-1085logfinal.txt
diff 070613YRG-1305-1085loginitial.txt 070613YRG-1305-1085logfinal.txt > 070613YRG-1305-1085diff.txt
fi
rm -rf 070613YRG-1305-1085lineascisco.txt
rm -rf 070613YRG-1305-1085informe.txt
cd /var/www/html/menu/description/scripts/carrier/respaldos/
mkdir P_IMP_070613_JCS_SANTAFE
cd /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE
mkdir SEGUIMIENTO VALIDACION_FINAL PI
cd /var/www/html/menu/description/scripts/carrier/PI/
cp CU_Alta_de_Interconexiones.xls /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE/PI/
cd /var/www/html/menu/description/scripts/carrier
mv 070613YRG-1305-1085loginitial.txt /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE/SEGUIMIENTO/
mv 070613YRG-1305-1085logconf.txt /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE/SEGUIMIENTO/
mv 070613YRG-1305-1085logfinal.txt /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE/SEGUIMIENTO/
mv 070613YRG-1305-1085diff.txt /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE/VALIDACION_FINAL/
cd /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE/SEGUIMIENTO/
mv 070613YRG-1305-1085loginitial.txt iadsl-nvl-santafe-18.mtu_INICIO.txt
mv 070613YRG-1305-1085logconf.txt iadsl-nvl-santafe-18.mtu_LOG.txt
mv 070613YRG-1305-1085logfinal.txt iadsl-nvl-santafe-18.mtu_FIN.txt
unix2dos iadsl-nvl-santafe-18.mtu_INICIO.txt iadsl-nvl-santafe-18.mtu_LOG.txt iadsl-nvl-santafe-18.mtu_FIN.txt
cd /var/www/html/menu/description/scripts/carrier/respaldos/P_IMP_070613_JCS_SANTAFE/VALIDACION_FINAL/
mv 070613YRG-1305-1085diff.txt iadsl-nvl-santafe-18.mtu_COMPARACION.txt
unix2dos iadsl-nvl-santafe-18.mtu_COMPARACION.txt

```

13.18 Script padre que realiza los movimientos entre las carpetas y manda a llamar a los scripts de conexiones remotas al servidor TACACS

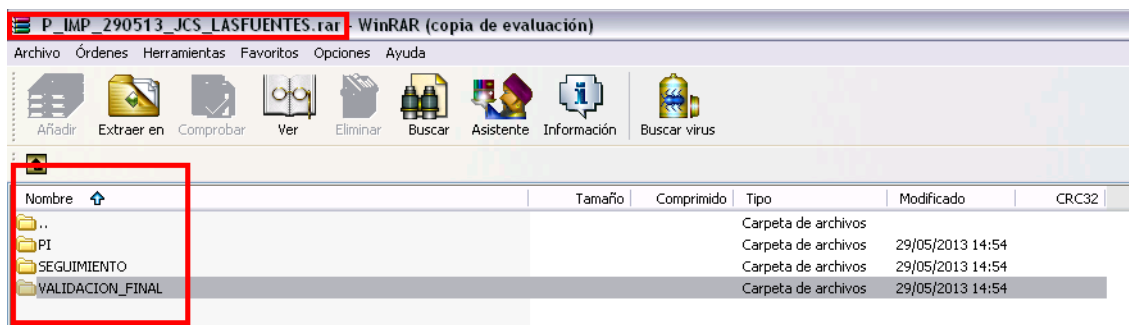
Durante ese mismo lapso de tiempo también se realizan los procesos correspondientes y debe aparecer entonces la siguiente vista con la palabra **DOWNLOAD** dar click y se descargará nuestro plan de implementación particular con las carpetas correspondientes a PI, Seguimiento y Validación Final listas para ser anexados a nuestros cambios (Imágenes I3.19 a I3.24).



13.19 Lanzamiento para descargar plan de implementacion



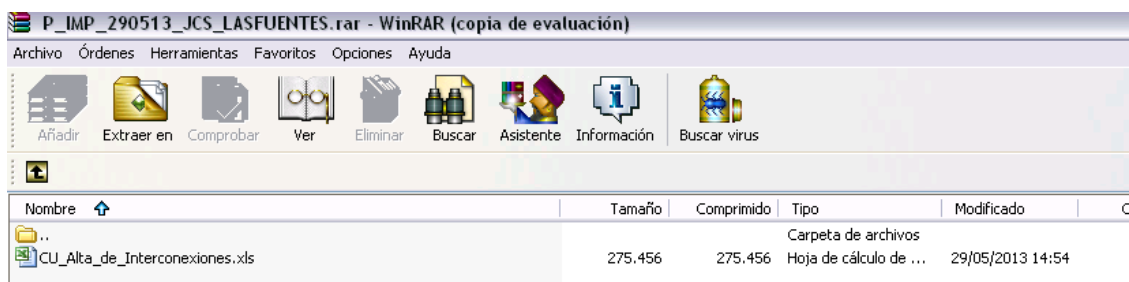
13.20 Descarga desde Server-Infra al cliente del Plan de implementacion



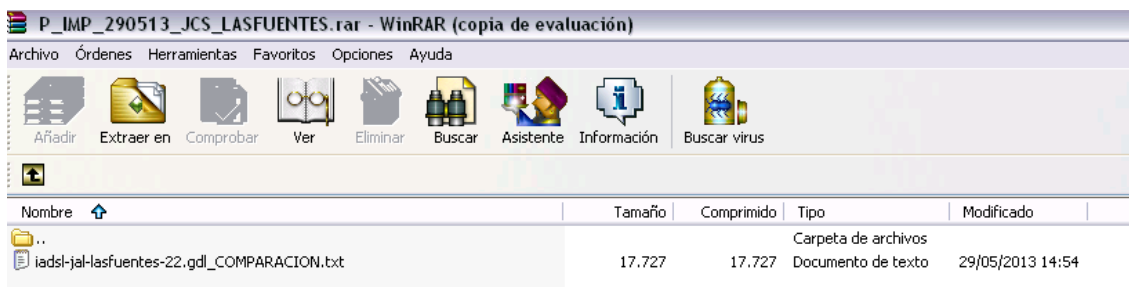
13.21 Carpetas acordadas para el plan de implementacion



13.22 Archivos acordados que deben estar en Seguimiento



13.23 Plan de Intervencion contenido en la carpeta PI



13.24 Comparacion de la configuracion del equipo entre antes de la implementacion y despues.

3.1.12. Planteamiento del problema 3

Telmex provee acceso a Internet para usuarios residenciales mediante diferentes tecnologías de acceso como puede ser dial-up, DSL, WiFi Móvil, etc. Wifi Móvil en INFINITUM es la modalidad de acceso a Internet que utiliza WiFi para ofrecer acceso a Internet en sitios Públicos.

Detecté que se tenía un total descontrol en cuanto a la infraestructura que se tenía dada de alta en uniNet ya que no toda es gestionable debido a que se

migraron a la plataforma de MERAKI sin notificar ya que fueron decisiones que tomaron por parte de TELMEX. Por consiguiente el direccionamiento otorgado a estos sitios públicos que en su momento se recibieron por uniNet se tiene de alguna manera ocupado.

Cabe mencionar que la infraestructura para Prodigy Móvil se encuentra en sitios públicos expuesta a que los departamentos de sistemas o por políticas se desactive.

3.1.13. Solución al problema 3

Con ayuda de mis compañeros se realiza una auditoría de todos los MODEM ROUTER dados de alta en el servidor de seguridad que aún podemos gestionar y se aplicó una auditoría con los siguientes rubros:

- ¿Ping exitoso?
- ¿Telnet exitoso?
- Vecinos en CDP
- APs conectados
- ¿APs Alcanzables por TELNET?
- NETID
- Nombre del sitio o pool
- Tunnel Gre Nextengo
- Tunnel Gre CTG
- Comentarios
- Person

Todo esto con la finalidad de tener una base de datos donde se tenga un mayor control de la infraestructura activa e inactiva así como del direccionamiento dedicado para Prodigy Movil.

Propuse un sistema WEB que muestra la base de datos precisa de toda la infraestructura gestionable y no gestionable por parte de uniNet además con

base en las entradas necesarias realicé auditorias de respaldos de infraestructura “ACTIVA” de manera automática.

Autenticación (Imagen I3.25)

El usuario debe de estar previamente dado de alta en la base de datos del servidor para poder acceder al sistema.



I3.25 Interfaz de usuario para ingresar la autenticación

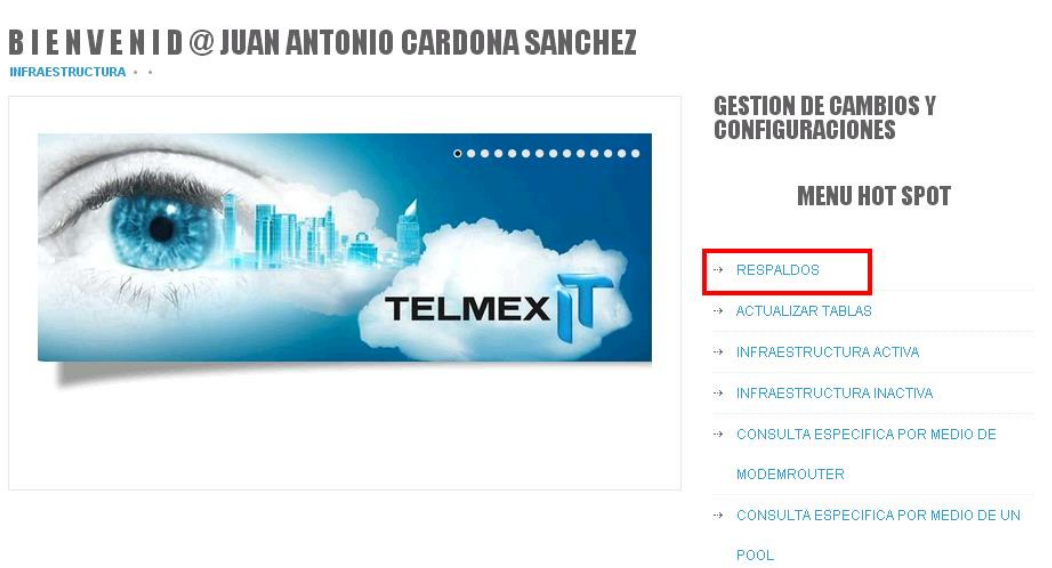
Menú principal (Imagen I3.26)

Se muestra el nombre del ingeniero que se autentique, así mismo se muestra el menú principal en donde se deberá de elegir la pestaña Hot Spot.



I3.26 Interfaz del menú principal

Ingresar a la pestaña RESPALDOS (Imagen I3.27)

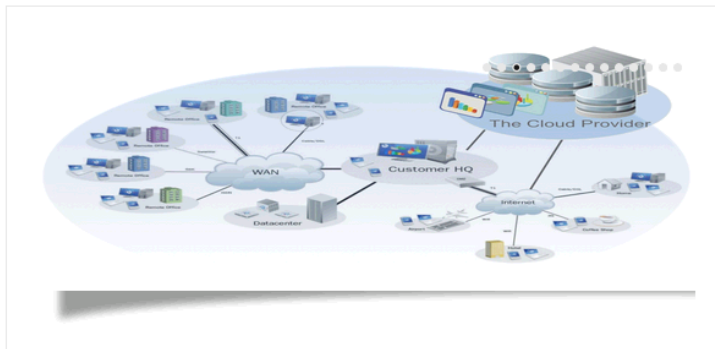


I3.27 Interfaz del menú de Hot Spot

Aparecen 2 opciones en donde se puede generar una auditoría o consultar una auditoría realizada con anterioridad (Imagen I3.28).

BIENVENID @ JUAN ANTONIO CARDONA SANCHEZ

INFRAESTRUCTURA



GESTION DE CAMBIOS Y CONFIGURACIONES

MENU HOT SPOT

- GENERAR AUDITORIA
- CONSULTAR AUDITORIAS

13.28 interfaz Menú para Auditorias.

Al dar click en la pestaña auditoría se nos muestra la siguiente vista donde ingresaremos la fecha en formato **DDMMAA** Presionar en el botón GO y esperar hasta que se presente la siguiente ventana (Imagen 13.29).



GENERAR AUDITORIA, INGRESAR FECHA:

FECHA DDMMAA: 290513

GO

CONSULTAS HOT SPOT

- RESPALDOS
- ACTUALIZAR TABLAS
- INFRAESTRUCTURA ACTIVA
- INFRAESTRUCTURA INACTIVA
- CONSULTA ESPECIFICA POR MEDIO DE MODEMROUTER
- CONSULTA ESPECIFICA POR MEDIO DE UN POOL

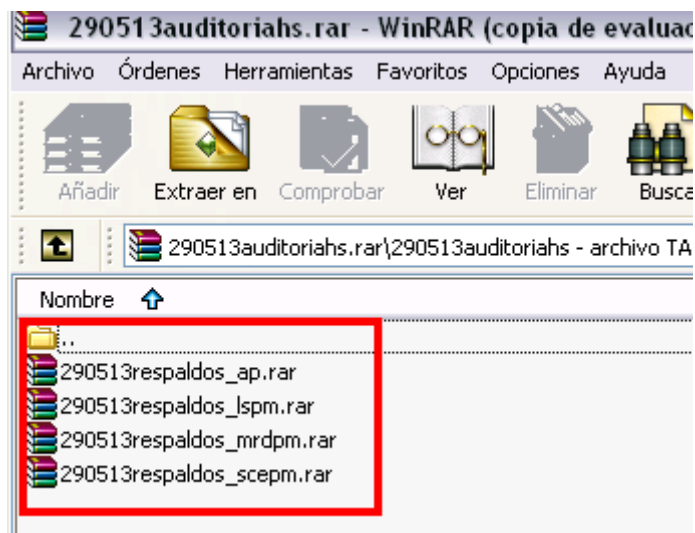
13.29 Entrada de la fecha para disparar la auditoria de la infraestructura activa de manera automática.

Damos click en **DOWNLOAD** Se nos descargará nuestra auditoría con equipos mrdpm (Modem Router para Prodigy Movil), lspm (Lanswitch para Prodigy Móvil). Ap (Puntos de acceso o antenas) y scep (Solución centralizada de Prodigy Móvil) (Imagen 13.30).

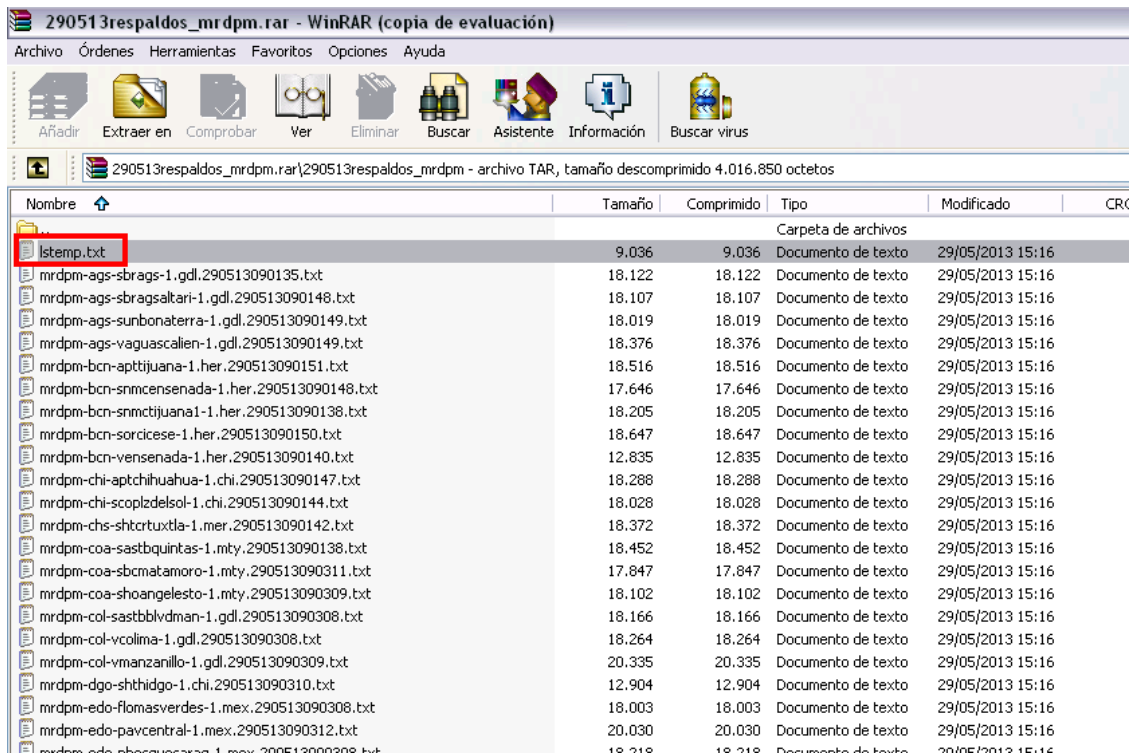


I3.30 Lanzamiento para descargar Auditoría con respaldos de la infraestructura activa

Entrar a la carpeta correspondiente a mrdpm y abrir el archivo ltemp.txt que contiene la lista de todos los mrdpm que se alcanzaron en la fecha ingresada (Imagen I3.32 a I3.34).



I3.32 Auditoría de infraestructura Activa

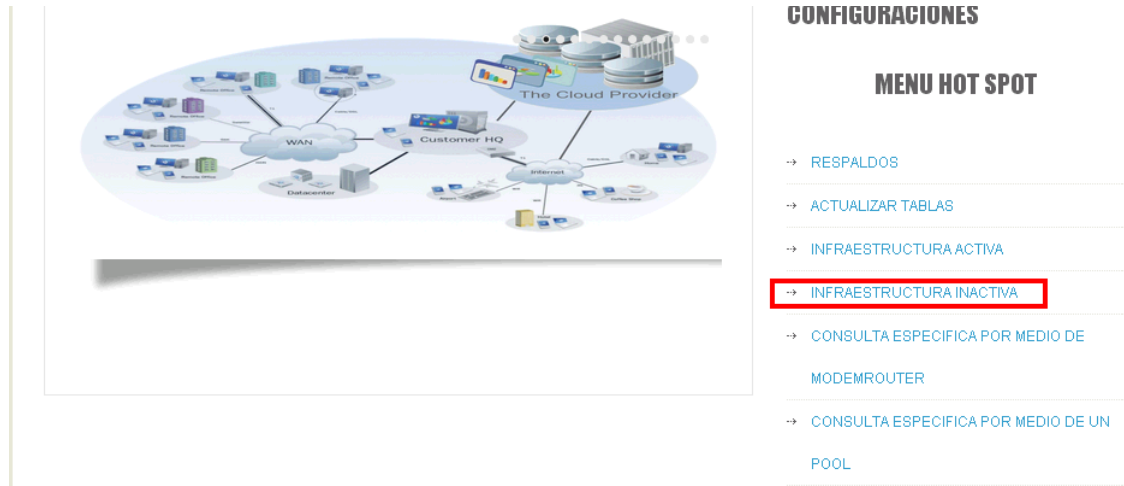


13.33 Archivos de respaldo de cada equipo activo

- 1 mrdpm-ags-sbrags-1.gdl.290513090135
- 2 mrdpm-ags-sbragsaltari-1.gdl.290513090148
- 3 mrdpm-ags-sunbonaterra-1.gdl.290513090149
- 4 mrdpm-ags-vaguascalien-1.gdl.290513090149
- 5 mrdpm-bcn-apttijuana-1.her.290513090151
- 6 mrdpm-bcn-snmcensenada-1.her.290513090148
- 7 mrdpm-bcn-snmctijuana1-1.her.290513090138
- 8 mrdpm-bcn-sorcicese-1.her.290513090150
- 9 mrdpm-bcn-vensenada-1.her.290513090140
- 10 mrdpm-chi-aptchiuahua-1.chi.290513090147
- 11 mrdpm-chi-scoplzdelzol-1.chi.290513090144
- 12 mrdpm-chs-shtcrtuxtla-1.mer.290513090142
- 13 mrdpm-coa-sastbquintas-1.mty.290513090138
- 14 mrdpm-coa-sbcmatamor-1.mty.290513090311
- 15 mrdpm-coa-shoangelesto-1.mty.290513090309
- 16 mrdpm-col-sastbbldman-1.gdl.290513090308
- 17 mrdpm-col-vcolima-1.gdl.290513090308
- 18 mrdpm-col-vmanzanillo-1.gdl.290513090309
- 19 mrdpm-dgo-shthidgo-1.chi.290513090310
- 20 mrdpm-edo-flomasverdes-1.mex.290513090308
- 21 mrdpm-edo-pavcentral-1.mex.290513090312
- 22 mrdpm-edo-pbosquesarag-1.mex.290513090308
- 23 mrdpm-edo-pcdjdnezahu-1.mex.290513090309
- 24 mrdpm-edo-pheroestecam-1.mex.290513090308
- 25 mrdpm-edo-plopezportil-1.mex.290513090308
- 26 mrdpm-edo-pplarboledas-1.mex.290513090307
- 27 mrdpm-edo-pstmaberrioz-1.mex.290513090307
- 28 mrdpm-edo-samcalamedas-1.mex.290513090302
- 29 mrdpm-edo-samcsnmateo-1.mex.290513090307
- 30 mrdpm-edo-sastbherradu-1.mex.290513090305
- 31 mrdpm-edo-sastbunvanah-1.mex.290513090305

13.34 Lista de mrdpm que fueron auditados en la fecha indicada.

Damos click en el botón menú y después en infraestructura inactiva (Imagen I3.35)



I3.35 Interfaz del menú de Hot Spot

De la lista generada identificar que equipos si contestaron Para auditarlo (Imagen I3.36).

SE TIENEN 1051 REGISTROS PARA ESTA CONSULTA

HOSTNAME	PING EXITOSO?	TELNET EXITOSO?	VECINOS EN CDP	APs CONECTADOS	ALCA POR
mrdpm-edo-pchurubusco-1.mex 201.154.4.17	NO	NO	N/A	N/A	
mrdpm-edo-pcoacalco-1.mex 201.154.1.143	NO	NO	N/A	N/A	

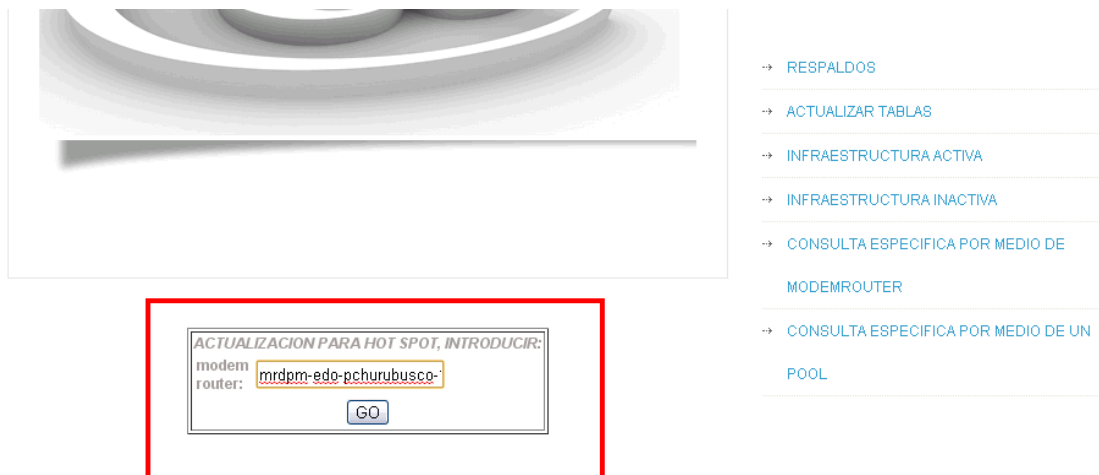
I3.36 Base de datos de equipos que hasta el momento no se tienen auditados.

Al ser identificado un equipo que ha contestado vamos a la pestaña ACTUALIZAR TABLAS (I3.37).



I3.37 Interfaz del menú de Hot Spot

Ingresamos el nombre del mrdpm **sin divisional** y presionamos en GO (Imagen I3.38)



I3.38 Ejemplo del ingreso de datos al sistema para poder aplicar el Update

Se muestra una tabla con los datos actuales, Actualizamos datos y presionamos GO, vamos a la pestaña de INFRAESTRUCTURA ACTIVA y debe estar ahí nuestro mrdpm con los datos actualizados (Imágenes I3.39 a I3.40):

SE TIENEN 1 REGISTROS PARA ESTA CONSULTA

ID	HOSTNAME	PING EXITOSO?	TELNET EXITOSO?	VECINOS EN CDP	APs CONECTADOS	APs ALCANSABLES POR TELNET	NETID RED	GATEWAY	SITIO O POOL	TUNEL GRE NEXTENGO	TUNNEL GRE CTG	COMENTARIOS
1	mrdpm-edo-pchurubusco-1.mex 201.154.4.17	NO	NO	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

VALORES PARA ACTUALIZAR

ID:

HOSTNAME:

PING EXITOSO?:

TELNET EXITOSO?:

VECINOS EN CDP:

APs CONECTADOS:

APs ALCANSABLES POR TELNET?:

NET ID RED:

GATEWAY:

SITIO O POOL:

TUNEL GRE NEXTENGO:

TUNNEL GRE CTG:

COMENTARIOS:

PERSONE:

I3.39 Llenado de los datos para realizar el Update

SE TIENEN 239 REGISTROS PARA ESTA CONSULTA

HOSTNAME	PING EXITOSO?	TELNET EXITOSO?	VECINOS EN CDP	APs CONE
mrdpm-edo-pheroestecam-1.mex	SI	SI	ap-edo-pheroestecam-1 (201.136.54.157)	ap-edo-phero

I3.40 Base de datos de infraestructura auditada



Conclusiones

Problema 1

Con base en la problemática que se tenía en UNINET con respecto a las descripciones en las interfaces con base en las normas que se rigen en UNINET.

Para poder generar una descripción de manera correcta se tienen ciertas normas, de las cuales concluyo que se ha solucionado el problema con la automatización de la generación de las descripciones con base en las entradas que ingresan los ingenieros que utilizan la herramienta impactando directamente en la mejora de las descripciones, además de eliminar el margen de error en dichas descripciones.

Problema 2

Con la automatización de la generación del plan de implementación para las interconexiones tipo Carrier Ethernet se reduce el margen de error para la generación del mismo, impactando de manera favorable ya que se utilizan única y exclusivamente las nomenclaturas y los documentos que debe de llevar apeguándose a las políticas de documentación de UNINET.

Problema 3

Con la automatización de las auditorías de los sitios de Hot Spot se tiene un beneficio importante, ya que contamos con una base de datos de la infraestructura activa e inactiva así como los respectivos respaldos de los equipos que se involucran en este tipo de sitio, esta base de datos se alimenta cada que se considere necesario por medio del sistema WEB.

Adicionalmente tenemos que el sistema híbrido también se encuentra funcionando como alojador de archivos con planes de intervención, y documentos que se solicitan subir por parte de la jefatura para la consulta de los mismos y de esta manera evitar que se utilicen planes de implementación que

están en desuso o simplemente la consulta de archivos para las operaciones del departamento.

Así, con la manera en la que opera el sistema híbrido se encontró la forma de entrar a los equipos que conforman la infraestructura en la red de UNINET y se tendrá el beneficio de realizar reportes, auditorías, respaldos y documentaciones de manera automática según el departamento lo requiera.

Finalmente, cabe mencionar que la formación que obtuve en la Facultad de Ingeniería me ha permitido incorporarme exitosamente al campo laboral y desempeñar los conocimientos adquiridos y sobre todo aplicarlos para la solución de problemas que detecto.

Glosario.

Siglas	Definición
Adsl 2 +	Asymmetric Digital Subscriber Line 2 Plus
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BB	Backbone
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BRAS	Broadband Remote Access Server
BTB	Back-to-Back
BUP	Back Up de Backbone
CE	Carrier Ethernet
CI	Configuration Item
CMDB	Configuration Management Data Base
DNS	Domain Name System
DoS	Denial of Service
DR	Designated Router
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
E	Ethernet
EBGP	External BGP
GPON	Gigabit Passive Optical Network
HDSL	High-bit-rate digital subscriber line
HTTP	Hypertext Transfer Protocol
IBGP	Internal BGP
IDE	Infraestructuras de Datos Espaciales
IMP	Implementación
IOS	Internetworking Operating System
IP	Internet Protocol
ITX	Interconexión
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
MODEM	Modulator Demodulator
MRDPM	Modem-Routers de Prodigy móvil
MTU	Maximum Transfer Unit
NAMs	Nodo de Acceso Multiservicio
OLT	Optical Line Termination
ONT	Optical Network Termination
OPERTELES	Atención a operadores

Siglas	Definición
OSPF	Open Shortest Path First
P	Plan
PE	Provider Edge
PI	Plan de Intervención
POPs	Point Of Presence
PPPoE	Point-to-Point Protocol over Ethernet
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
REG	Regional
RFC	Request For Change
RRIDE	Route Reflector IDE
SCEMP	Solución centralizada de Prodigy Móvil
SDH	Synchronous Digital Hierarchy
SEC	Sectorial
SFTP	Secure File Transfer Protocol
Splitter	filtros pasivos
SQL	Structured Query Language
SSH	Secure Shell
TACACS	Terminal Access Controller Acces Control System
TBAS	Terminal de Banda Ancha
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WIMAX	Worldwide Interoperability for Macrowave Access

Mesografía.

- *Telmex Uninet 20k guía de uso Liberaciones e Implementaciones.pdf* Disponible en la intranet de las oficinas de red uno
- *Proceso de Gestión de Liberaciones e Implementaciones.ppt* Disponible en la intranet de las oficinas de red uno
- *DD_WiFi_Movil_Arquitectura_Centralizada.pdf* Disponible en la intranet de las oficinas de red uno
- *EQUIPOS CON FUNCIONALIDAD RR.pdf* Disponible en la intranet de las oficinas de red uno
- *PRESENTACIÓN BRAS.pdf* Disponible en la intranet de las oficinas de red uno
- *Topologías y Jerarquías Estándar en UniNet.pdf* Disponible en la intranet de las oficinas de red uno
- *OSPF en UNINET.ppt pdf* Disponible en la intranet de las oficinas de red uno
- *DD_Serv_INFINITUM.pdf* Disponible en la intranet de las oficinas de red uno
- *Políticas de documentación iso20k uninet.doc pdf* Disponible en la intranet de las oficinas de red uno