Universidad Nacional Autónoma de México

Facultad de Ingeniería

Administración de Redes
Profesora: Ing. Magdalena Reyes Granados

Proyecto Final

Concurso de licitación para empresas de telefonía de VoIP

Equipo Mitnick

Integrantes:
Cabrera Beltrán Héctor Eduardo
Jiménez Juárez Jesús
Melgoza Illescas Ángela Sofía
Prado Padilla José Gerardo

Grupo: 01

Semestre 2021-1

Índice

Introducción

Los sistemas telefónicos analógicos, se refieren a los sistemas telefónicos tradicionales que convierten las señales de voz en ondas eléctricas de diferentes amplitudes y frecuencias. Estas ondas son recibidas por el intercambio telefónico y dirigidas al receptor en el otro extremo de la línea.

Estos sistemas cuentan con muchas limitaciones; un número de teléfono está asociado con una línea y, por lo tanto, solo puede admitir una conversación a la vez. Además, los sistemas analógicos solo poseen características básicas como retención, silencio, rellamada, marcación rápida y transferencia de llamadas.

Por otro lado, los sistemas telefónicos VoIP funcionan convirtiendo señales de teléfono analógicas en señales digitales que se pueden entregar a través de Internet. Los sistemas telefónicos VoIP utilizan la tecnología PSN (Packet Switching Network) donde las señales de voz recibidas en los paquetes de datos pequeños se transmiten de manera secuencial para que la señal de voz se pueda generar en el extremo receptor.

Características avanzadas

Los sistemas VoIP son redes telefónicas privadas, lo que hace que la comunicación sea más segura. Estos sistemas también ofrecen más características que los sistemas analógicos tradicionales, como el identificador de llamadas, el correo de voz, el desvío de llamadas e, incluso, proporcionan acceso a la organización de videoconferencias. Además, se pueden integrar con aplicaciones de terceros, haciéndolos más flexibles.

Costo-Efectividad

La ventaja más importante que hace que los sistemas VoIP sean más ideales que los sistemas telefónicos analógicos es la rentabilidad. Estos sistemas ofrecen mejor calidad-precio con su gama de características y menores costos de instalación y uso. Además, la comunicación de larga distancia es casi gratuita en los sistemas VoIP. Esto permite a las organizaciones promover su alcance eficazmente a través de varias ubicaciones geográficas.

Escalabilidad

Los sistemas telefónicos tradicionales se limitan al número de líneas conectadas. Agregar más líneas sólo es posible con una actualización en hardware. VoIP tiene un número ilimitado de líneas, ya que sólo se basa en Internet.

Objetivo

El presente proyecto tiene como objetivo dar solución a los requerimientos de comunicaciones de voz expuestos por un cliente que busca la migración hacia esta tecnología debido a los beneficios que ofrece, tales como reducir los costos de enlace de llamadas, beneficios al implementar una infraestructura de red única o mejora de la flexibilidad empresarial.

Por otro lado, para nosotros como estudiantes es importante poner en práctica el aprendizaje obtenido para construir una red que cuente con servicios de VLAN y más específicamente, de VoIP además de plantearnos el escenario en el que nos podríamos encontrar si en un momento dado quisiéramos desarrollar una propuesta para un concurso de licitación.

Justificación

El proyecto de renovación de la red trae diversos beneficios, que se presentan a continuación.

Servicio de VoIP

Una de las razones más importantes por las que las pymes se están pasando a la telefonía IP es que consiguen rebajar los costos en gran medida debido a que el precio por minuto de una llamada por VoIP es muchísimo más económico que mediante una línea de telefonía tradicional.

Teniendo en cuenta que la voz humana va de los 50 Hz hasta los 8 kHz, es importante destacar que la telefonía tradicional tan solo alcanza el rango de frecuencias de los 300 Hz hasta los 3.4 kHz y que la VoIP proporciona audio desde los 50Hz hasta los 7 kHz, lo cual se adecua mucho más a la realidad.

A diferencia de la telefonía tradicional, la tecnología VoIP está gestionada por un software, que una vez instalado admite todas las líneas que se deseen añadir, sin costo adicional, aparte del costo del teléfono en sí mismo.

Algunas de las funciones que ofrece un servicio de VoIP son:

- Identificación avanzada de llamadas.
- Llamadas en espera.
- IVR (respuesta de voz interactiva).
- Visualización del detalle de llamadas realizadas o recibidas.
- Grabación de llamadas.

Cambio de los routers

El principal beneficio de cambiar al Router Cisco 2811 es que ofrece múltiples servicios para mejorar la productividad y disminuir costos. La serie 2800 de routers Cisco de servicios integrados, logra de forma inteligente incrustar datos, seguridad, voz y servicios inalámbricos en un único sistema. Además, cuenta con la capacidad de ofrecer múltiples servicios de alta calidad simultáneos a velocidad de cable a múltiples conexiones T1/E1/xDSL. Los routers ofrecen opciones de procesamiento de llamadas integrado y soporte de correo de voz, interfaces de alta densidad para una amplia gama de requisitos de conectividad, además del rendimiento y densidad suficientes de ranura para las futuras necesidades de expansión de la red.

Teléfonos IP

Los teléfonos IP son en apariencia igual que un teléfono tradicional, pero estos utilizan una tecnología que les permite conectarse directamente al módem, o a través de WiFi. Los conmutadores PBX IP (Private Branch eXchange) están basados en software que permite conseguir varias funcionalidades y servicios que son normalmente muy difíciles y costosos de implementar con un PBX propietario tradicional (red telefónica privada utilizada dentro de una empresa).

Una posibilidad podría ser utilizar dispositivos ATA (adaptador de teléfono análogo) que consiste en un dispositivo conectado por un lado al teléfono tradicional, y por el otro lado al enlace a internet. Es la manera más simple de conectarse a través de tecnología VoIP. Sin embargo, la calidad de la conexión no suele ser óptima y puede ocasionar ciertas deficiencias en la comunicación.

Seguridad lógica

- ACL: Las ACL que se aplican a una interfaz del router permiten controlar el flujo del tráfico permitiendo o denegando el acceso a la red de acuerdo a alguna condición y evitar así que personas no autorizadas o indeseables tengan la libertad de acceder a la empresa. Asimismo, con un Sistema de Control de Acceso, se proporciona un nivel básico de seguridad de acceso a la red que el administrador puede modificar o bloquear según sea necesario al hacer el filtrado de paquetes.

- SSH: En las conexiones realizadas por medio de SSH, toda la información viaja de forma encriptada, lo cual lo convierte en uno de los medios más seguros al momento de trabajar en un servidor gracias a que proporciona servicios para transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. Adicionalmente el cliente SSH y el servidor usan firmas digitales para verificar su identidad.

- Servidor Syslog: gracias al envío de mensajes de registro de una red informática se puede obtener información sobre la seguridad del sistema, por ejemplo:

- Un intento de acceso con contraseña equivocada.
- Un acceso correcto al sistema.
- Anomalías: variaciones en el funcionamiento normal del sistema.
- Alertas cuando ocurre alguna condición especial.

- Información sobre las actividades del sistema operativo.
- Errores del hardware o el software.

Seguridad física

La seguridad física consiste en la protección de las personas, la propiedad y los activos físicos, de acciones y eventos que podrían causar daños o pérdidas. En esencia, esta seguridad incluye disuasión física, detección de intrusos y respuesta ante amenazas; las principales amenazas incluyen posibles actos de error humano, actos involuntarios, actos deliberados de espionaje y desastres naturales.

La seguridad física se reduce en gran medida a un par de componentes principales: control de acceso y vigilancia.

- Control de acceso: El control de acceso abarca barreras hacia los espacios donde se encuentran los componentes que requieren seguridad adicional, por lo que se debe contar con restricciones biométricas.

- Vigilancia: Una forma de vigilancia puede ser un elemento disuasorio contra la actividad criminal, para esto se opta por algún tipo de CCTV, o circuito cerrado de televisión. Además de que las cámaras proporcionan evidencia de actividad criminal, también pueden detener intrusos potenciales, contando con señalización clara que indique a las personas que existen tales cámaras.

Software

- Asterisk

Asterisk es un framework de código abierto para la creación de aplicaciones de comunicaciones. Asterisk convierte un equipo ordinario en un servidor de comunicaciones. Asterisk funciona en sistemas IP PBX, VoIP gateways, servidores de conferencias y otras soluciones personalizadas. Asterisk es libre y de código abierto, patrocinado por Sangoma.

Asterisk se distribuye bajo una licencia dual: una licencia de código abierto y una licencia comercial. La licencia de código abierto bajo la que se distribuye Asterisk es la GNU Public License versión 2 (GPLv2). Esta licencia se adapta completamente al uso de Asterisk, para la mayoría de las personas y organizaciones, ya que estos usuarios no distribuyen modificaciones de propiedad, adiciones o derivados de Asterisk y no requieren la protección legal de una licencia comercial.

<u>Características</u>

- Receptor de alarma
- Anexo de mensaje
- Autenticación
- Operador automatizado
- Listas negras
- Registros acerca de detalles de llamadas
- Monitoreo de llamadas

- Cola de llamadas
- Grabación de llamadas
- Transferencia de llamadas
- Llamadas en espera
- Marcar por nombre
- Macros
- TDMoE (Multiplexación por división de tiempo a través de Ethernet)
- Permite la conexión directa de Asterisk PBX
- Cero latencia
- Permite la integración de instalaciones físicamente separadas
- Permite un plan de marcado unificado en varias oficinas
- Entre muchas más

- PuTTY

PuTTY es un programa de terminal versátil para Windows, además del cliente SSH gratuito más popular del mundo. Es compatible con SSH, telnet y conexiones raw socket con una buena emulación de terminal. Admite la autenticación de clave pública y el inicio de sesión único de Kerberos. También incluye implementaciones SFTP y SCP de línea de comandos.

Características

- Cliente de Windows
- Soporte de Windows de 32 y 64 bits
- Admite cliente SSH, cliente telnet, cliente SFTP (solo línea de comandos) y cliente rlogin. Se admiten los protocolos SSH2 y SSH1. Sin embargo, se debe tener en cuenta que el uso de SSH1 no se recomienda por razones de seguridad
- Admite la autenticación de clave pública y la autenticación Active Directory/Kerberos
- Transferencias de archivos solo mediante programas de línea de comandos independientes. No hay soporte de transferencia de archivos integrado

Propuesta

Se plantea implementar una estructura híbrida, ya que estas combinan dos o más estructuras de distintas topologías y su principal ventaja es el grado de flexibilidad que proporcionan, ya que existen pocas limitaciones en las estructuras de red que una configuración híbrida no pueda acomodar.

Para ello, se tiene pensado instalar una topología de anillo, puesto que cada dispositivo está conectado solamente con los de cada lado, y, cuando se transmiten los datos, los paquetes viajan a lo largo del círculo, moviéndose a través de cada uno de los nodos intermedios hasta que llegan a su destino. Esto permite que los repetidores se puedan utilizar para asegurarse de que los paquetes lleguen correctamente y sin pérdida de datos. También, dado que solo un dispositivo en la red envía datos a la vez, se reduce en gran medida el riesgo de colisiones de paquetes, haciendo que estas topologías sean eficientes en la transmisión de datos sin errores.

Junto con la topología anteriormente mencionada, se usará una topología de estrella. Estas permiten administrar cómodamente toda la red desde una única ubicación, dado que cada uno de los nodos está conectado de forma independiente a un dispositivo central. Asimismo, si uno deja de funcionar, el resto de la red seguirá trabajando, lo que ocasiona que la topología de estrella posea un diseño de red estable y seguro, al igual que, los dispositivos se pueden agregar, quitar y modificar sin desconectar toda la red. Y, en cuanto a la parte física, la topología de estrella utiliza relativamente poco cableado para conectar completamente la red; la simplicidad del diseño de red facilita el trabajo de los administradores, ya que es fácil identificar dónde se producen errores o problemas de rendimiento.

Respecto al cableado, utilizaremos uno de los dos estándares, ya sea ANSI/EIA/TIA-568A o ANSI/EIA/TIA-568B, dado que necesitamos conectar dispositivos diferentes entre sí, como un switch con un ordenador o un router con un switch. Esto sería para la realización de cableado directo. Y, si se tuviese que escoger uno de los dos estándares, sería el segundo, dado que es mucho más común dentro de los diseños de redes.

Posterior a la instalación de la red, contemplando el reemplazo de los routers y de los teléfonos analógicos, se realizarán las configuraciones necesarias en cada dispositivos para cumplir con las características de la seguridad lógica explicadas anteriormente.

Además, si el cliente así lo requiere, se procederá a instalar los dispositivos pertinentes a la seguridad física, que sería un conjunto de cámaras de seguridad (CCTV) y un lector biométrico de huella digital para restringir el acceso al cuarto de telecomunicaciones. Sin embargo, en caso de no optar por estas medidas de seguridad, el cliente debe estar consciente de que cuenta con medidas pertinentes para asegurar la integridad de sus equipos, ya que, de no ser así, se expone a distintas amenazas, como un competidor que entra al lugar donde se encuentran los dispositivos o un empleado descontento que roba físicamente datos confidenciales, lo que podría conllevar a ataques de software, actos de robo, vandalismo, sabotaje, alteración de la información y compromiso de propiedad intelectual.

Desarrollo

Realizamos una topología con VLSM, en donde consideramos los siguientes números de hosts en cada una de las subredes que se tenían disponibles.

Subred	Hosts
B	70
D	60
A	40
C	30
WAN1	2

WAN2	2
WAN3	2

Subred	Segmento	Rango IPs útiles	Gateway	Máscara	Broadcast
B	182.3.0.0/25	182.3.0.1 182.3.0.126	182.3.0.126	255.255.255.128	182.3.0.127
D	182.3.0.128/26	182.3.0.129 182.3.0.190	182.3.0.190	255.255.255.192	182.3.0.191
A	182.3.0.192/26	182.3.0.193 182.3.0.254	182.3.0.254	255.255.255.192	182.3.0.255
C	182.3.1.0/27	182.3.1.1 182.3.1.30	182.3.1.30	255.255.255.224	182.3.1.31
WAN1	182.3.1.32/30	182.3.1.33 182.3.1.34	182.3.1.34	255.255.255.252	182.3.1.35
WAN2	182.3.1.36/30	182.3.1.37 182.3.1.38	182.3.1.38	255.255.255.252	182.3.1.39
WAN3	182.3.1.40/30	182.3.1.41 182.3.1.42	182.3.1.42	255.255.255.252	182.3.1.43

Operaciones para la obtención de cada una de las subredes

Subred B

2^7 - 2 = 126 >= 70 (7 porciones de hosts son los que se van a usar)
32 - 7 = 25 (Prefijo) → Máscara 255.255.255.128
255-128 = 128

Subred D

2^6 - 2 = 62 >= 60 (6 porciones de hosts son los que se van a usar)
32 - 6 = 26 (Prefijo) → Máscara 255.255.255.192
255-192 = 64

Subred A

2^6 - 2 = 62 >= 40 (6 porciones de hosts son los que se van a usar)
32 - 6 = 26 (Prefijo) → Máscara 255.255.255.192
255-192 = 64

Subred C

2^5 - 2 = 30 >= 30 (5 porciones de hosts son los que se van a usar)
32 - 5 = 27 (Prefijo) → Máscara 255.255.255.224
255-192 = 64

WANs

2^2 - 2 = 2 >= 2 (2 porciones de hosts son los que se van a usar)
32 - 2 = 30 (Prefijo) → Máscara 255.255.255.252
255-192 = 64

Mientras que las subredes de VoIP quedarían de la siguiente manera.

182.3.210.0/24 → VoIP 1
182.3.220.0/24 → VoIP 2
182.3.230.0/24 → VoIP 3
182.3.240.0/24 → VoIP 4

Configuración de los routers

Todos los comandos que se verán a continuación se deben aplicar para cada router.

Para dar direcciones IP por medio de DHCP, primero se excluyen las direcciones del gateway, así como direcciones estáticas que se vayan a utilizar, y posteriormente se procede a crear el pool.

ip dhcp excluded-address **IP_a_excluir**
ip dhcp pool **nombre_servidor_dhcp**
default-router **gateway**
network **segmento_de_red máscara**

Para configurar el DHCP de voz, se siguen los mismos comandos mostrados anteriormente, solo se debe agregar la siguiente línea:
option 150 ip **gateway**

A continuación, se establece una dirección IP para cada subinterfaz; se tendrá una por cada VLAN conectada al router.

interface fa **interfaz-id.vlan-id**
encapsulation dot1q **vlan-id**
ip address **gateway máscara**
description **nombre_servidor_dhcp**

Una vez que se tiene lista la interfaz fastethernet con sus respectivas IPs por cada VLAN, se procede a levantar la interfaz.

interface fa **interfaz-id**
no shutdown

En cuanto a las interfaces seriales, se ingresa a la configuración de cada una, se le establece su IP y se levanta.

interface serial **interfaz-id**
ip address **dirección_ip máscara**
no shutdown

Posteriormente, se realiza el enrutamiento utilizando el protocolo OSPF.

router ospf **ID**
network **segmento_conectado_directamente wildcard** area **área**

Donde:
ID: ID del proceso, sirve para saber qué routers, de determinado proceso, hacen una función especial.
área: Se coloca el área a la que pertenece ese segmento de red. Siempre se empieza con el área 0.

Se debe considerar que se coloca la línea *network* tantas veces como segmentos que tenga conectado el router directamente.

Después, se configura el servicio VoIP.

telephony-service
max-dn **N°_máximo_extensiones**
max-ephones **N°_máximo_ephones**
auto assign 1 to 10
ip source-address **gateway** port 2000

Se establece el número de extensión de cada teléfono.

ephone-dn **extensión-id**
number **N°_extensión**

Y se concluye con el enrutamiento de comunicación de VoIP.

dial-peer voice **enrutador_id** voip
destination-pattern **extensión_destino**
session target ipv4:**dirección_ip**

Donde:
enrutador_id: Corresponde a cualquier valor unitario (1, 2, 3, ...).
extensión_destino: Número de extensión con la que se desea comunicar.
dirección_ip: Señala el camino que se tomará para que exista comunicación VoIP con la extensión de destino.

El Access Control List (ACL) lo aplicamos para que solo la PC del administrador pueda ingresar por medio de SSH, de igual manera vamos a aplicar la configuración del último mencionado para que se pueda ingresar por control remoto. Los comandos a ejecutar son los siguientes:

username **USERNAME** secret **CONTRASEÑA**
enable secret **CONTRASEÑA_ENABLE**
hostname **NOMBRE_ROUTER**
ip domain-name **DOMINIO_ROUTER**
crypto key generate rsa
ip ssh authentication-retries 2
ip ssh time-out 60
aaa new-model
line vty 0 4
login local
transport input ssh
access-class 21 in
exit
access-list 21 permit host **IP_PC**
access-list 21 deny any

En el que **USERNAME** es el usuario que se va a registrar, **CONTRASEÑA** es la clave que le daremos al usuario para su acceso. **CONTRASEÑA_ENABLE** es la clave para poder acceder al modo privilegiado dentro del router. **DOMINIO_ROUTER** es el dominio que le vamos a dar al router e **IP_PC** es la IP del PC del administrador de las áreas locales de red.

Configuración de los switches

Para el caso de la seguridad en los puertos de los switches, al menos en la interfaz del administrador, lo que se implementó fue port-security. Para los switches 0, 1 y 3, que son los que tienen la computadora configurada para que esta solo ingrese por medio de SSH, la configuración se realiza de la siguiente manera:

interface **Interface_PC**
switchport mode access
switchport port-security
switchport port-security mac **MAC_ADDRESS_PC**
switchport port-security maximum 1
ex

En el que **Interface_PC** es puerto del switch que está conectada a la PC del administrador de red y **MAC_ADDRESS_PC** es la dirección MAC de la PC con la que únicamente se va a tener comunicación.

Ahora, si se quiere agregar una IP al switch, tiene que ser de la siguiente manera, esto para que pueda aplicarse el protocolo de NTP y el de SYSLOG.

interface vlan **N°_VLAN_DATOS**
ip address **IP_ÚTIL_DISPONIBLE MASK_DATOS**
no shutdown
exit
ip default-gateway **GATEWAY_DATOS**

En el que **N°_VLAN_DATOS** es el número de VLAN de datos con el que configuramos el switch para que así fuese, **IP_ÚTIL_DISPONIBLE** es la IP que vamos a utilizar para poder identificar el dispositivo, mientras que **MASK_DATOS** es la máscara que pertenece a la subred y por último **GATEWAY_DATOS** es el gateway que se configuró en la subred al momento de realizar DHCP.

Configuración tanto en los routers como en los switches

Se implementa en estos el protocolo SYSLOG para que haya un servidor que esté recibiendo los eventos que pasaron tanto en los dispositivos de capa 2 y 3. Se configuró de la siguiente manera:

logging host **IP del Server SYSLOG**
service timestamps log datetime msec

En donde **IP del Server SYSLOG** es la IP de los tres servidores que tenemos en la topología. (182.3.0.125, 182.3.0.189, 182.3.1.29)

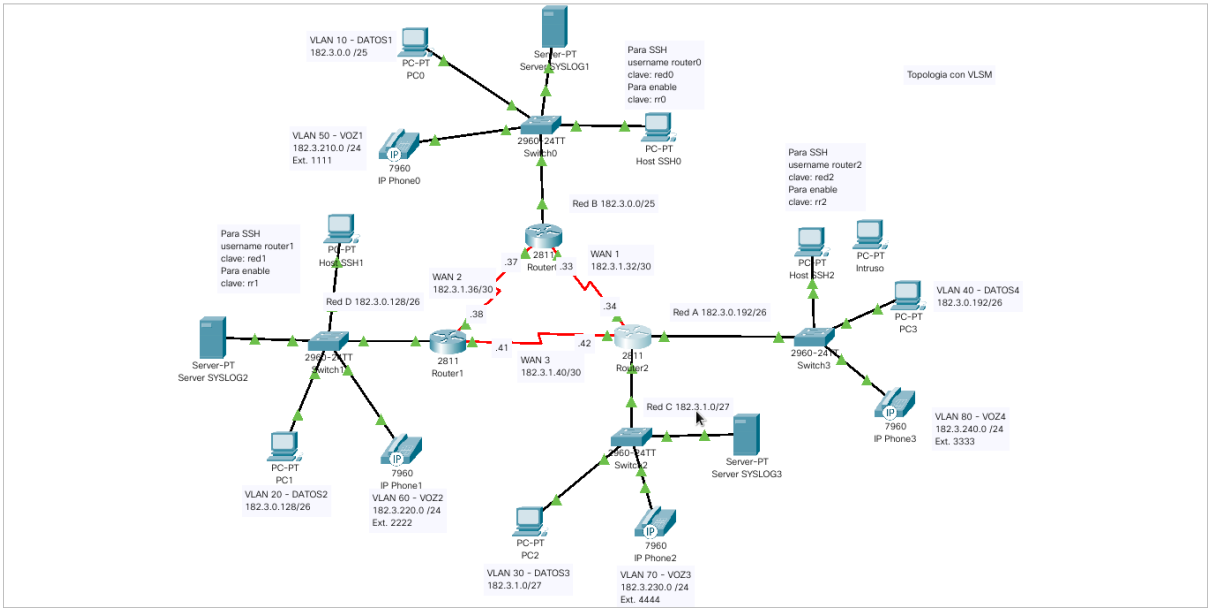
También se configuró el protocolo NTP para que uno de los servidores proporcione la fecha y el tiempo a los demás dispositivos. Tanto en los routers como en los switches se tiene que escribir el siguiente comando:

ntp server **IP del server NTP**

IP del server NTP es la IP del servidor que proporciona la fecha y el tiempo, el cual es **182.3.0.125**

Implementación

La topología será la siguiente:



Tiempo de instalación

El proyecto se prevé que esté completo y entregado con una planeación de dos semanas:

Días 1 - 3: Medición y detección de riesgos.

Se realizará un estudio del estado de la infraestructura implementada, se hará un monitoreo de la integridad lógica de la red y se revisará si cuenta con las normatividades de implementación, un estado físico íntegro, se identificarán los posibles riesgos existentes, así como se realizarán las mediciones necesarias para la implementación del hardware recomendado. Se realizará un análisis de la forma de implementación para afectar en su minoría la operación de su empresa.

Después de esta etapa se tendrá un presupuesto final.

Días 4 - 10: Implementación paulatina de la red, respetando una parcial continuidad de la operación.

Basándonos en el análisis realizado, se implementará la instalación tanto de hardware como de software, se mitigará los riesgos en caso de existir y al finalizar la instalación, se realizarán pruebas de funcionamiento y seguridad.

Días 11 - 15: Monitoreo y control del funcionamiento global de la red.

Se hará un monitoreo mientras continúa la operación de su empresa, revisando que se cumplan al 100% las medidas implementadas. El día 13 se entregará un informe comparativo con lo establecido en la infraestructura anterior. Cualquier control necesario se notificará e implementará en los días 14 y 15.

Cotización

Equipo e infraestructura

- Router 2811

  $3 500.00 USD

  Cantidad: 3

  Total: $10 500 USD

- Módulo WIC-2T

  $900.00 USD

  Cantidad: 3

  Total: $2 700 USD

- Teléfono VoIP 7960

  $200.00 USD

  Cantidad: 30

  Total: $6 000 USD

- Cable UTP categoría 6

  $0.50 USD por metro

- Cable Serial

  $10.00 - $180.00 USD

  Cantidad: 3

Subtotal equipo e infraestructura: $19 200.00 USD

Seguridad Física

- Sistema de cámaras CCTV

  8 cámaras

  1 TB de almacenamiento

  Total: $410.00 USD

- Cerradura con lector biométrico

  Total: $90.00 USD

- Sistema de alarma de seguridad

  Total: $155.00 USD

- No - Break

  155.00 USD

  Cantidad: 3

  Total: $465.00 USD

- Site

  $750.00 USD

  Cantidad: 3

  Total: $2250.00 USD

Total seguridad física: $3 370.00 USD

Instalación y configuración

- Gestión por 4 ingenieros a cargo, para cada uno: $7.70 USD por hora

  2 semanas de implementación contemplan 120 horas de trabajo.

  Subtotal: $924.00 USD

  Total: $3 696.00 USD

Conclusiones

Cabrera Beltrán Héctor Eduardo

Con este trabajo pude poner en práctica los conocimientos adquiridos a lo largo del semestre, principalmente la configuración de VoIP, desarrollo de VLSM, creación e implementación de VLANs, configuración de listas de acceso y un cliente SSH.

Además, me permitió ver las distintas características que se deben contemplar para un proyecto de licitación, como las herramientas necesarias para llevar a cabo los requisitos, es decir, el hardware y software que se usará, las medidas de seguridad tanto físicas como lógicas, junto con la cotización de todos los elementos necesarios, y el tiempo que se debe considerar, para completar un proyecto.

Por último, fue de ayuda para ver los precios de distintos dispositivos, al igual que software, en el mundo real. Dado que, durante el curso se trabaja únicamente con simulaciones, es difícil pensar en el valor de los equipos que se utilizan, ya que, por lo regular, se cuenta con un enfoque meramente teórico. Sin embargo, al momento de realizar una planeación para un proyecto, hay que considerar el costo-beneficio que poseen distintos equipos a la hora de tomar una decisión.

Jiménez Juárez Jesús

La realización del proyecto nos permitió repasar todo lo aprendido en las clases, a pesar de la situación por la que pasamos, aplicamos también los conocimientos de asignaturas que anteriormente habíamos acreditado. Sin tomar en cuenta que esto es un concurso por ver qué equipo es el que mejor da solución a una empresa en particular, nos ayuda a crecer tanto académico como profesional, dado que nos da experiencia en realizar la documentación, investigación, en la preparación de cada uno de los puntos de los procesos administrativos que se vieron en clase, así como las habilidades necesarias para poder resolver los problemas que se van presentando durante la ejecución de un proyecto de este tipo.

Respecto a las diferentes actividades que se llevaron a cabo, vimos que hay diferentes maneras de poder darle más seguridad a nuestros sistemas y aplicar la triada de seguridad, además de no repudio, control de acceso y autenticidad. Con esto, se reafirma que los conocimientos que se han dado a lo largo de estos años están siendo beneficiados aplicándose en este tipo de proyectos.

Melgoza Illescas Ángela Sofía

Gracias a la realización de este proyecto tuvimos un acercamiento a lo que podría ser una situación real en un futuro al competir en un concurso de licitación, porque aunque sea un proyecto meramente académico tuvimos la experiencia de armar el proyecto, investigar sobre el software y hardware más conveniente, además de comparar los precios que implica cada uno de los componentes de una re, cosa que en otras clases generalmente no hacemos pero que siempre es importante tomar en cuenta para cuando nos encontremos en el campo laboral.

En lo personal creo que trabajar en este proyecto nos dió la oportunidad de poner en práctica la mayor parte de los conocimientos que hemos adquirido tanto en esta materia como en su antecesora, lo que es un buen complemento y un ejercicio bastante útil para darnos una idea de la forma en la que se debe llevar un proyecto similar en un entorno real.

Prado Padilla José Gerardo

Este proyecto fue un acercamiento muy grande a la realidad, por lo que lo considero muy enriquecedor ya que es muy completa la experiencia al implementarlo pues realizamos un proceso administrativo de una red que comienza desde el análisis y la planeación, pasando por cotizaciones y la forma de implementar hasta una exposición para ganar la licitación. Me parece muy bueno que en la facultad los profesores implementen este tipo de retos a los

estudiantes ya que es una preparación más completa que el hecho de sólo dejar armar una red como proyecto.

Académicamente el proyecto también fue muy enriquecedor ya que nos plantea el reto de diseñar y construir una red agregando y manejando todos los conceptos teóricos y prácticos vistos en laboratorio y teoría, por lo que me ayudó tener bien claros los conceptos para aplicarlos en el desarrollo, así como también me hizo darme cuenta de la cantidad de procesos aplicados y aprendidos a lo largo del semestre.

Referencias

- Horizon Telecom. (2017). *VoIP vs Analog Phone Systems.* Recuperado el 15 de enero de 2021, de https://www.horizontelecom.co.uk/blog/voip-vs-analog-phone-systems/
- Avende. (2019). *Analog Phone Systems vs. VoIP Phone Systems.* Recuperado el 15 de enero de 2021, de https://avende.com/analog-phone-systems-vs-voip-phone-systems/
- Sarenet. (2020). *Ventajas de la VoIP frente a la telefonía tradicional.* Recuperado el 15 de enero de 2021, de https://blog.sarenet.es/ventajas-voip-telefonia-analogica/
- 3cX. (s.f.). *¿Qué es un Conmutador IP o PBX IP?* Recuperado el 15 de enero de 2021, de https://www.3cx.es/voip-sip/conmutador-ip-pbx-ip/
- Red Hat Enterprise (s.f.). *Protocolo SSH*. Recuperado el 15 de enero de 2021, de https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html
- Tech Club. (2016). *¿Qué es SYSLOG?* Recuperado el 15 de enero de 2021, de https://techclub.tajamar.es/syslog/
- DNS Stuff. (2019). *What Is Network Topology? Best Guide to Types and Diagrams.* Recuperado el 15 de enero de 2021, de https://www.dnsstuff.com/what-is-network-topology
- Swinhoe, D. (2018). *What is physical security? How to keep your facilities and devices safe from on-site attackers.* Recuperado el 15 de enero de 2021, de https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html
- Precios recuperados el 18 de enero de 2021 de https://itprice.com/
- Asterisk. (s.f.). *Getting Started with Asterisk.* Recuperado el 18 de enero de 2021, de https://www.asterisk.org/get-started/
- Asterisk. (s.f.). *Asterisk Software.* Recuperado el 18 de enero de 2021, de https://www.asterisk.org/products/software/
- Asterisk. (s.f.). *Features Available in Asterisk.* Recuperado el 18 de enero de 2021, de https://www.asterisk.org/get-started/features/
- SSH Academy. (s.f.). *PuTTY - World's Most Popular Free SSH Client.* Recuperado el 18 de enero de 2021, de https://www.ssh.com/ssh/putty/