Proyecto Final Redes de Computadoras

ACOSTA, FEDERICO ANTONIO
CERVANTES, IGNACIO MANUEL
ZULUAGA BERNAL, DILAN DAVID

UNQ

Licenciatura en informática

Proyecto de Inicial redes y computación

Argentina

2022

Proyecto Inicial de Redes y Computadoras

Presentado por:

ACOSTA, FEDERICO ANTONIO
CERVANTES, IGNACIO MANUEL
ZULUAGA BERNAL, DILAN DAVID

Presentado a:

Zaccagnini, Cesar Luis
Balbiani, Leonardo
Loyola, Sergio

UNQ

Licenciatura de informática

Argentina

2022

Tabla de Contenido

1. Introducción

En este informe se detalla la realización y desarrollo de un proyecto de red para una Bodega “Beodo S.R.L”, la cual cuenta con distintas sedes con distintas especificaciones y requerimientos de servicios. La red fue desarrollada contemplando sus 3 edificios; CABA (principal), San Juan y Mendoza, cumpliendo con cada especificación dada por el cliente y agregando algunas características en pos de brindar mayor fiabilidad y/o funcionalidad a la red.

El planteo y desarrollo de la red fue emulado y puesto a prueba mediante el simulador Cisco Packet Tracer, obteniendo así una vista general y puesta a punto de todos las características con las cuales cuenta la red. Si bien, la red fue planteada en un esquema reducido para evitar redundancia y trabajo innecesario, la misma cuenta con todas las características y funcionalidades requeridas.

2. Marco teórico

DNS

DNS o Domain Name Service es un servicio de consulta de dominios jerárquico, el cual tiene la función de resolver los nombres de dominio (google.com, por ejemplo) respondiendo con sus direcciones IPs respectivas a los hosts que las consulten.

Dicho servicio fue diseñado para poder evitar el tedioso trabajo de acordarse las direcciones IPs de cada dominio, lo cual en Internet como es hoy en dia, es imposible; Las direcciones IPs pueden cambiar sin problema que un usuario cuando consulte por el dominio google.com va a continuar accediendo a la página solicitada sin tener que enterarse de cualquier cambio de dirección.

DNS funciona con una estructura jerárquica, tiene servidores root o raíz, que están ubicados en distintos puntos del mundo a los cuales se dirigen todas las consultas del mundo, posteriormente estos servidores van delegando dependiendo de los dominios consultados a sus respectivos DNS que los gestionen.

HTTP

HTTP o HyperText Transfer Protocol es un protocolo de transferencia de hipertextos el cual permite la transferencia de archivos en la WWW (World Wide Web) mediante formatos HTML, XML, entre otros…

HTTP en un inicio, seguía el esquema de consulta-respuesta entre host y servidor mediante una conexión sin estado, es decir, no guarda ningún tipo de información de conexiones anteriores. La versión más usada a día de hoy es la HTTP/1.1, la cual tiene conexiones persistentes por defecto, entre otras mejoras como la posibilidad de realizar múltiples peticiones en una misma conexión (pipelining).

Dicho protocolo fue desarrollado por el World Wide Web Consortium, que es la entidad que genera los estándares internacionales.

HTTPS

HTTPS o Hypertext Transfer Protocol Secure es un protocolo basado en el protocolo HTTP, es básicamente una versión segura del mismo debido a que HTTP no es seguro y permite interferencias de agentes externos. Una de las pocas diferencias radica en las URLs, HTTPS debe iniciarse con https:// a diferencia del http:// del protocolo HTTP.

SMTP

El protocolo SMTP o Simple Mail Transfer Protocol es un protocolo de transferencia de mensajes, más precisamente el intercambio de correos electrónicos. La única función de este protocolo es el envío de los email.

POP

El protocolo POP o Post Office Protocol, es un protocolo de recepción de correos electrónicos, es prácticamente una oficina postal donde el usuario consulta si recibió algún paquete en un servidor remoto y este último se los devuelve, en caso de que los tuviera. Se utiliza para la recepción de paquetes únicamente, no envía.

UDP

El protocolo UDP o User Datagram Protocol es un protocolo de transferencia de datagramas. UDP no cuenta con control de tráfico ni gestión de errores ni confirmación recepción de paquetes, es un protocolo mínimo a nivel de transporte el cual se utiliza principalmente para enviar rápidamente paquetes sin tener una conexión previa. Sus principales usos son en DHCP y DNS.

No es un protocolo seguro, debido a que no cuenta con confirmación de recepción ni puede asegurar que los paquetes se entregaron en el orden correcto, a diferencia de su contraparte TCP. La principal ventaja es que no provoca mucha carga en la red.

UDP trabaja con datagramas o paquetes enteros, los mismos cuentan con cabeceras con suficiente información para que puedan llegar a sus destinatarios sin intervención del mismo protocolo luego de despacharlo.

TCP

El protocolo TCP o Transmission Control Protocol es un protocolo de transferencia de información, TCP cuenta con control de tráfico, gestión de errores y confirmación de recepción por lo que es un protocolo seguro que garantiza que los paquetes se entregaron en el mismo orden que se enviaron y que no cuentan con ningún error.

TCP es el principal protocolo usado a día de hoy, la mayoría de Internet lo utiliza.

TCP cuenta con un concepto llamado puertos, el cual son distintos puntos de acceso para poder diferenciar una aplicación de otra, al momento de tener múltiples conexiones simultáneas.

Un concepto importante de TCP, es el saludo a tres vías, o three-way shaking, el cual se utiliza para finalizar una conexión mediante tres envíos de paquetes, el primero del cliente al servidor informando que la solicitud de finalización, el segundo del servidor al cliente informando la recepción del primer fin y un segundo paquete indicando a finalización de la conexión al cliente.

IP

La dirección IP (Internet Protocol) es una dirección única e inequívoca que identifica a cada dispositivo que esté conectado a Internet o a una red local, algo así como un número de DNI de cada dispositivo con el cual se comunican entre sí. La dirección IP tiene el siguiente formato: xxx.xxx.xxx.xxx. Por ejemplo, 192.168.145.1.

Existen dos versiones de IP:

IPv4 e IPv6, la última de estas es la más reciente y fue creada con el problema del agotamiento de las direcciones del mundo, actualmente es la menos implementada pero poco a poco está comenzando a tomar más parte de la redes mundiales.

Ruteo

El ruteo es el proceso por el cual se calcula la ruta de un paquete y se busca la mejor forma de llegar a su destino en una red grande, pasando por los múltiples nodos (routers) que tenga dicha red.

Existen distintos protocolos de ruteo (OSPF, RIP, Estático), en este proyecto se utiliza el protocolo de ruteo estático. Dicho protocolo consiste en definir de manera fija cada una de las rutas – en una tabla de ruteo – que los routers deben indicar a cada paquete que pasa por ellos, indicando el next-hop o siguiente salto, a la interfaz del router que corresponda, el siguiente router realiza el mismo trabajo, consulta en su tabla de ruteo la dirección que coincida con el destino del paquete y lo envía a la interfaz del router que corresponda.

En caso de que el destino esté en la red que controla un router, este lo envía directamente por dicha interfaz.

Subneteo

El subneteo o subnetting es una técnica de división de redes en subredes más pequeñas a partir de la original, es muy útil cuando se tienen redes más pequeñas a los segmentos brindados por la empresa o ISP que provea conexión. Con esto, se consiguen redes lógicas más pequeñas y que cada una de estas funcione como una red física aparte de la original, es muy útil cuando se quiere tener varias VLANs o varios segmentos de red separados para varias sedes de una misma empresa.

DHCP

El DHCP (Dynamic Host Configuration Protocol) o Protocolo de Configuración Dinámica de Host, es un protocolo de asignación de IPs de manera dinámica a partir de un servidor previamente configurado.

Dicho servidor debe tener los Pools con las IPs que se tienen disponibles para brindar a los hosts previamente configurados. La solicitud se realiza mediante un envío broadcast de un paquete por parte de un host, la responde únicamente el servidor DHCP informando del Pool disponible, luego el host realiza la solicitud y finalmente el servidor le envía la IP solicitada.

Dicho protocolo es muy útil en una red grande con muchos hosts que no requieren configuraciones específicas o personalizadas, en principal, para no confundir IPs y asignar IPs ocupadas. De igual forma, DHCP ahorra mucha carga de trabajo.

VLAN

VLAN es una técnica para la creación de redes lógicas dentro de una misma red física, dichas redes son totalmente independientes de las demás. Dicha técnica se realiza asignando en un conmutador de paquetes (switch, hub, etc) distintas VLANs a los puertos de entrada Ethernet de este mismo conmutador.

Esta técnica es muy útil cuando se quiere realizar una división de una red de un mismo edificio o varios, en distintos departamentos o agrupaciones de hosts. Por ejemplo, entre el Departamento de Ventas y el Departamento de Marketing.

Cuando se realice la división en VLANs entre distintos conmutadores y se quiera intercomunicar las VLANs se debe utilizar un router que pueda rootear los distintos paquetes a sus respectivas gateways.

NAT

El protocolo NAT (Network Address Translation) o Traducción de Direcciones de Red es un mecanismo de traducción de direcciones IPs Públicas a Privadas y viceversa, el cual es utilizado para ahorrar direcciones públicas debido al gran crecimiento que tuvo Internet

en los últimos años, es imposible contar con que todos los dispositivos tengan dirección IP pública. Dicho mecanismo es realizado por el Router y es configurado ahí mismo.

Dicho mecanismo tiene 3 variantes, NAT Estático, NAT Dinámico y NAT Dinámico con Overload o Sobrecarga.

El NAT Estático consiste en la asociación de una dirección IP Pública con una dirección IP Privada, siempre que se consulte por esa dirección o esa dirección salga, se le asigna la privada o pública según corresponda. Es 1 a 1.

El NAT Dinámico, consiste en la asignación de un Pool de IPs públicas de salida a un Pool de direcciones IPs privadas, esto significa que si un host interno de la red desea salir y comunicarse con el exterior utilizara una dirección IP del Pool público mientras este la conexión activa, una vez finaliza, dicha dirección IP se coloca nuevamente como disponible. Esto último quiere decir que, solamente pueden navegar ciertos números de hosts a la vez en la red pública, según la cantidad de direcciones IPs públicas que se hayan asignado. De igual forma es 1 a 1, únicamente cambia la dirección IP pública asignada a cada dirección privada.

El NAT Dinámico con Overload o Sobrecarga, consiste en la asignación de una dirección IP Pública para todos los hosts internos que quieran navegar en la red, es decir, todos tendrán la misma dirección IP pública, únicamente varían en el puerto sobre el que salen, el cual reconoce y asigna el Router para no perder rastro de cada hosts cuando haya varios a la vez. Este mecanismo es de 1 a muchos, una sola IP pública para muchos hosts privados.

STP: Mejora del UTP (4 pares de hilos de cobre trenzados entre sí, codificados por color y recubiertos de plástico flexible se utiliza mayormente en conexiones de host) con blindaje metálico de cada par trenzado y malla exterior adicional para todo el conjunto.

IEEE 8.22.11 (WI-FI): Protocolo de conexión inalámbrica entre un punto de acceso y un host.

Copper Cross-over: El cable cruzado se cruza o cambia de dirección de extremo a

otro. Utilizado para la conexión entre conmutadores.

Copper Straight-through: Cable de cobre trenzado para uso de redes de área local (LAN).

Serial DTE: Cable serial de transición blindado.

Cable de Fibra Óptica: Cable de transmisión mediante una onda de luz en fibra de vidrio.

Estos dispositivos y tecnologías se encargan del traslado correcto de información de las diferentes sedes, conectando a los equipos a los diferentes DNS y servidores alojados o solicitados en la red.

3. Diseño de capa física

El diseño de la capa física es el siguiente:

IEEE 8.22.11 (WI-FI): Se utilizó para la conexión de dispositivos inalámbricos e impresoras con los AP de cada piso de cada sede.

Copper Cross-over: Se utilizó para la conexión entre distintos host en una misma red lan. Switches con Hosts, PCs con IP Phones, etc.

Copper Straight-through: Se utilizó para la conexión entre conmutadores de paquetes (switches).

Serial DTE: Se utilizó para la conexión entre el Router de borde (CABA) y el Router Internet.

Cable de Fibra Óptica: Se utilizó para conectar las distintas sedes entre sí, los routers más precisamente. Realizando una conexión triangular entre las tres sedes (CABA, SJ, Mendoza), para poder tener mayor fiabilidad en la red en caso de que sucediera algo con el Router de CABA, el resto de la red no resultaría incomunicado.

4. Diseño de capa de enlace

El diseño que respecta a la capa de enlace de este proyecto es el siguiente:

Se divide al segmento de red correspondiente a la sede de CABA, según lo solicitado, en 4 VLANs:

VLAN #1 Sistemas y Centro de Datos:

Agrupa el Departamento de Sistemas y el Centro de Datos.

VLAN #2 Gerencia:

Agrupa la Oficina del Directorio, Oficina de Gerentes, Departamento de Marketing, Sala de Reuniones y el SUM.

VLAN #3 Logística:

Agrupa el Departamento de Prensa, Departamento de Diseño, Departamento de Impresión y el Departamento de Mantenimiento.

VLAN #4 Administración:

Agrupa el Departamento de Facturación y Liquidaciones, Departamento de Contabilidad, Atención al Público, Departamento de RRHH y el Departamento de Compras.

Dicha división, corresponde con lo solicitado dentro de la sede de CABA; que cuenta con 4 pisos y distintos conmutadores de paquetes en el mismo. Se realizó la asignación de los puertos para cada Switch y se realizó la interconexión de dichos switches a partir de uno central para la intercomunicación de las distintas redes VLAN entre sí.

En total, se cuenta con un switch principal que conecta el resto de switches y un switch por cada piso conectado al principal. Esto con el objetivo de obtener una mayor

fiabilidad y no tener una conexión en línea entre cada switch, corriendo el riesgo de que uno falle y el resto se queden totalmente incomunicados.

La interconexión se realizó colocando las interfaces, que conectan los switches entre sí, en modo trunk de igual forma se realizó el protocolo de encapsulamiento necesario en el router que conectaba esa sede. A dicho router se le asignaron distintas interfaces o interfaces virtuales para asignar cada una a una VLAN y contar con conexión entre distintas VLAN de un mismo segmento de red.

5. Diseño de capa de red

El diseño que respecta a la capa de red es el siguiente:

Subneteo:

Se realizó la división de la red de CABA en 4 segmentos distintos, siendo cada uno de estos, parte de una VLAN distinta (sistemas, logística, etc), para poder tener varias subredes independientes dentro de la misma red física (CABA).

Se contaba con el segmento 172.29.1.0 / 24 para la asignación de la red de Beodo CABA, dicha red se dividió en los 4 segmentos correspondientes a:
VLAN Sistemas 172.29.1.0 - 255.255.255.128
VLAN Gerencia 172.29.1.128 - 255.255.255.192
VLAN Logistica 172.29.1.192 - 255.255.255.224
VLAN Administración 172.29.1.224 - 255.255.255.224

Con este subneteo, se contaba con 4 subredes totalmente independientes para cada VLAN.

Se contaba con el segmento 192.168.145.0 / 24 para la asignación de las redes de Beodo Mendoza y Beodo San Juan, se realizó un subneteo para dividir el segmento en 2 subredes más pequeñas:

Beodo San Juan 192.168.145.0 - 255.255.255.192
Beodo Mendoza 192.168.145.64 - 255.255.255.192

Con esto, se contaba con dos segmentos independientes para poder asignar a las distintas sedes. En adición, se ahorraron direcciones IPs correspondientes a la otra mitad del segmento dado inicialmente (192.168.145.128 - 255.255.255.128) debido a que no eran necesarias para estas sedes.

Para las conexiones WAN entre las distintas sedes, se utilizó el segmento anteriormente mencionado (192.168.145.128) para asignar a todas las interfaces de los enrutadores. Quedando de la siguiente manera:

WAN #1 Mendoza - SJ: 192.168.145.128 - 255.255.255.252
WAN #2 CABA - Mendoza: 192.168.145.132 - 255.255.255.252
WAN #3 CABA - SJ: 192.168.145.145.136 - 255.255.255.252

Ruteo:

En lo que respecta al Ruteo de toda la red Beodo, se recurre al protocolo de enrutamiento estático entre las distintas sedes; Se configuraron los distintos routers de cada sede entre sí, para enviar los paquetes al siguiente salto de la sede que corresponda y los paquetes globales a internet, mediante el Router de Borde (CABA). Al contar con una múltiple conexión entre las sedes (triangular), se configuraron todas las rutas en todos los routers para que reconozcan los 3 segmentos de la red (192.168.145.0, 192.168.145.64 y 172.29.1.0).

El router de CABA cuenta con la ruta adicional de 0.0.0.0/0 hacia Internet, para poder enviar los paquetes de Internet al Router Internet.

6. Descripción de servicio DHCP

El servicio DHCP, se implementó de la siguiente manera:

Se utilizaron 3 servidores DHCP que suministran direcciones IPs a todas las sedes, cada servidor corresponde a una sola sede. Los servidores DHCP de San Juan y Mendoza cuentan con un Pool único definido para cada sede y asigna todas las direcciones disponibles sin diferenciar entre los hosts que la soliciten.

El servidor DHCP de CABA cuenta con distintos Pools, definidos para cada VLANs que tiene dicha sede, esto con el objetivo de poner controlar todas las VLANs desde un mismo servidor, contar con un servidor para cada VLAN conlleva una complejidad innecesaria y en un futuro si se requiriera nuevas VLANs, sería más difícil implementarlas.

La red cuenta con un servidor DHCP por sede, para poder tener una mayor fiabilidad en cada sede, si sucede algo con el servidor de CABA, no se quedaría toda la red completa sin el servicio, únicamente CABA. En adición, es más fácil controlar las direcciones con las que cuenta cada sede, al estar en segmentos distintos, es mucho más complejo realizar la diferenciación entre hosts de distintas sedes que soliciten IP.

Los Pools asignados son:

DHCP Mendoza:
IP Inicio: 192.168.145.70
Cantidad de Hosts: 70

DHCP San Juan:
IP Inicio: 192.168.145.10
Cantidad de Hosts: 40

DHCP CABA:
Pool #1 (VLAN-Sistemas):

IP Inicio: 172.29.1.102

Cantidad de Hosts: 25

Pool #2 (VLAN-Gerencia):

IP Inicio: 172.29.1.130

Cantidad de Hosts: 58

Pool #3 (VLAN-Logística):

IP Inicio: 172.29.1.194

Cantidad de Hosts: 28

Pool #4 (VLAN-Administración):

IP Inicio: 172.29.1.226

Cantidad de Hosts: 28

7. Descripción de servicios de capas de aplicación implementados

En las sedes se implementaron los siguientes servicios:

HTTP es implementado en los servidores Web de Beodo (San Juan, Web Principal, Prensa, etc.) utilizados para representar las páginas principales de la empresa Beodo.

HTTPS es implementado en el servidor Intranet Beodo, correspondiente al servidor interno de la empresa Beodo. Se realizó dicho servidor utilizando el protocolo HTTPS para conseguir una conexión segura dentro de la red.

DNS se ve reflejado en los servidores (Beodo Principal, Beodo Secundario, Local Resolver, Beodo Prensa Primario, Beodo Prensa Secundario) dando forma a la red que es necesaria para pedir la información solicitada por el usuario ayudado por los nombres de dominio de los diferentes apartados, los dominios y tareas que gestiona cada uno son los siguientes:

DNS BEODO PRINCIPAL: Gestiona todo el dominio beodo.com.ar, que corresponde a toda la red completa, respondiendo todas las consultas realizadas por los Hosts que no pertenezcan a la red de Beodo. Únicamente contiene las direcciones públicas de los servicios solicitados (web, email, etc).

DNS BEODO SECUNDARIO: Gestiona todo el dominio beodo.com.ar, que corresponde a toda la red completa, respondiendo todas las consultas realizadas por los Hosts que no pertenezcan a la red de Beodo. Únicamente contiene las direcciones públicas de los servicios solicitados (web, email, etc) como servidor secundario.

DNS BEODO PRENSA PRIMARIO: Gestiona todo el dominio prensa.beodo.com.ar, que corresponde al Departamento de Prensa de Beodo.

DNS BEODO PRENSA SECUNDARIO: Gestiona todo el dominio prensa.beodo.com.ar, que corresponde al Departamento de Prensa de Beodo como servidor secundario.

DNS LOCAL RESOLVER: Gestiona todas las consultas provenientes de los Hosts de la red Beodo, consultando a los respectivos servidores superiores por los dominios consultados. De igual forma, contiene las direcciones privadas de los servidores internos de Beodo, para suministrarlos a los hosts pertenecientes a la red que los consulten.

POP3 Y SMTP es usado en el envío, eliminación, emisión y recepción de correos redactados al dominio correo@beodo.com.ar perteneciente a la empresa Beodo. Dicho dominio es gestionado por el servidor principal de email Beodo Email, ubicado en la sede de CABA.

8. Emulación

Para la realización de esta red, se realizó una emulación de todo el esquema recurriendo a un emulador virtual llamado Cisco Packet Tracer; Se planteó el esquema reducido pero aplicando todos los conceptos y servicios solicitados

El simulador (Cisco Packet Tracer) es un programa que permite ver el comportamiento de las redes y su respectiva configuración. Dicho emulador soporta un amplio protocolo de capas de aplicación simulados generando muchas facilidades a la hora de realizar el planteamiento, configuración y testeo de la red.

Se realizó la emulación de la red con todas las sedes de la empresa Beodo, representando completamente todos sus edificios, divididos por pisos y departamentos, comprimiendo el tamaño de la red y colocando a un host para la representación de todos los demás que pertenecen a ese mismo departamento, manteniendo así la funcionalidad de toda la infraestructura pero simplificando en tamaño y manteniendo todos los servicios pedidos (NAT, DNS, Firewall, HTTP, HTTPS, etc) y sus respectivas configuraciones pedidas.

9. Conclusiones

En el transcurso del desarrollo de la red realizada se encontraron diferentes dificultades:

Asignación de VLANs:

Posiblemente, la asignación de VLANs a los distintos departamentos de CABA es la parte más desafiante de todo el proyecto de red, más aún teniendo en cuenta el Subneteo que se debe realizar y la correcta división en subredes tomando en cuenta la cantidad de equipos que tiene cada Departamento. En especial, la configuración del Router para aplicar etiquetado de VLAN a cada subinterfaz.

Representación de equipos externos a la red:

Otra cuestión compleja sin dudas es la representación de los equipos ajenos a la red – google, local resolver, dns primarios, etc. – debido a las diversas formas de realizarlo y el criterio a la hora de colocar los routers o hacer la división entre el ISP, Google y los servidores root DNS.

Relay DHCP:

Si bien, esta característica está ligada fuertemente a la asignación de VLANs, representaba un desafío enorme por sí sola; El planteamiento realizado contaba con un único servidor DHCP por sede, siendo el servidor de CABA el más complejo de configurar debido a la enorme cantidad de equipos con los que contaba dicha red y esto sumado a la división en subredes y VLANs realizada, representó un desafío bastante considerable. Principalmente, de no perder rastro y nota de las direcciones asociadas a los DHCP Pool y a las subinterfaces de las cuales se debía desviar las consultas DHCP mediante IP Helper-Address.

Sin embargo y a pesar de las dificultades encontradas, la red funciona correctamente cumpliendo todos los objetivos planteados en un principio, respetando los requisitos y la arquitectura del edificio (espacios, departamentos , equipos) obteniendo una simulación fiel a los objetivos de la empresa, reducida y más cercana posible a la realidad.