08-10-2015

Informe TP Inicial

**Índice**

1. Objetivo
2. Introducción
3. Marco teórico
4. Diseño
   1. Capa 1
   2. Capa 2
   3. Capa 3
5. Conclusiones
6. **Objetivo**

La realización de un proyecto en el cual se integren todos los temas que incumben a la materia.

1. **Introducción**

Se desea desarrollar el proyecto de una red de datos para una Facultad que cuenta con la siguiente condición geográfica y edilicia:

La Facultad posee 3 sedes, la principal situada en la Ciudad Autónoma de Buenos Aires, otra en Avellaneda y la última en Quilmes.

* + El edificio de CABA posee las siguientes características: es un edificio de 10 pisos, de los cuales la Facultad posee y hace uso de los pisos 1º , 2º, 7º y 10º.
    - En el piso 10 se aloja el Centro de Datos que posee 10 racks y capacidad para 100 servidores, teniendo conectividad 802.3 Ethernet para el doble de puestos que posibles servidores. También se encuentra:
      * Las oficinas del Departamento de Sistemas (30)
      * La oficina del Decanato de la Facultad (10)
      * La Secretaría Académica (15)
      * Secretaría de Extensión, Cultura y Bienestar (15)
      * Secretaría Investigación Científica y Tecnológica (15)
      * Secretaría Hacienda (20)
    - En el 7º piso se encuentra:
      * La Secretaría General (20)
      * Secretaría de Hábitat (30)
      * Facturación y Liquidaciones (20)
      * Departamento de Personal (30)
    - En el 2º piso se encuentra:
      * El Departamento de Alumnos (40)
      * El Departamento de Graduados (80)
    - En el 1º piso se encuentra:
      * Aula 11 (20)
      * Aula 12 (60)
      * Aula 13 (20)
      * El Acceso Público a Internet (60)
      * La Bedelía (4)

En esta sede, las redes se encuentran segmentadas en redes virtuales de acuerdo a los siguientes grupos de pertenencia (en color para facilitar la identificación):

* De la Secretaría Académica dependen:
  + las aulas, Bedelía y los Departamentos de Alumnos y de Graduados.
* De la Secretaría Hacienda:
  + el Departamento de Personal y el Departamento de Facturación y Liquidaciones.
* De la Secretaría General:
  + el Decanato y el Acceso Público a Internet.
  + El edificio de Quilmes es de propiedad íntegra de la Facultad y tiene 2 pisos:
    - En el 2º piso se encuentra:
      * La Bedelía (4)
      * El Cuarto de Servidores y Conectividad (6 servidores).
    - En el 1º piso se encuentra:
      * Aula 11 (20)
      * Aula 12 (20)
      * Aula 13 (40)
      * Aula 14 (20)
  + El edificio de Avellaneda tiene 4 pisos, de los cuales la Facultad posee y hace uso sólo del 2º piso. En ese piso encontramos:
    - * Aula 21 (20)
      * Aula 22 (20)
      * Aula 23 (40)
      * La Bedelía (5)
      * Cuarto de Servidores y Conectividad (4 servidores).

El nombre de dominio de la Facultad será *unq.edu.ar* y será administrado por el Departamento de Sistemas en el DNS primario de la Facultad. Además se delegará la administración del subdominio sh.unq.edu.ar a la Secretaría de Hacienda que administrará su propio servidor DNS primario.

La Facultad contará con los siguientes servicios.

* En CABA:
  + Servidor Web principal que contendrá toda información general sobre la Facultad.
  + Servidor Web seguro contendrá la Intranet de la Secretaría de Hacienda
  + Servicio de correo electrónico. Todas las direcciones de correo electrónico serán de la forma *usuario@unq.edu.ar*.
* En Quilmes:
  + Servidor web que brindará información sobre las actividades específicas de esa sede.
  + Un firewall encargado de bloquear todo el tráfico proveniente de internet excepto el acceso al servidor web con el objetivo de proteger las computadoras y servicios de la sede.
* En todas las sedes:
  + Cada piso tendrá un punto de acceso wireless que ofrecerán acceso a la red bajo la identificación “Wunq”.
  + Cada piso tendrá al menos una impresora de red accesible y utilizable por todos los usuarios de ese piso.
  + Un sniffer encargado de revisar y analizar el tráfico de red.

1. **Marco** **teórico**

Como el segmento de red que brinda el proveedor es el 200.32.5.128/25, implica que disponemos para la interacción con internet de 126 IPs ya que la máscara de red con valor 25 significa que solo los últimos 7 bits de las IPs va a variar de IP a IP, osea que disponemos en neto de 2^7 = 128 IPs, pero tanto la primera IP (200.32.5.128) como la última (200.32.5.255) no están disponibles ya que la primera identifica la red y la otra es la dirección de broadcast de la red.

Ya que la cantidad de servidores, puestos de trabajo y routers sumados superan por mucho esta cantidad de IPs, decidimos usar internamente tramos de red privada y el sistema NAT para exponer los servicios web.

En la sede CABA hay 489 puestos, la de Avellaneda 89 y en la de Quilmes 104. Para cada una de las sedes se utiliza un servidor DHCP para asignarles las IPs dinámicamente a cada uno de los puestos.

Un servidor HDCP es un servidor que implementa el protocolo DHCP que permite que los usuarios conectados al servidor puedan obtener dinámicamente sus parámetros de configuración de red. Este protocolo trabaja en la capa de aplicación según el modelo OSI. En el servidor DHCP se especifican los rangos de IPs disponibles para las asignaciones, el servidor DNS y el gateway de todos los puestos conectados al servidor.

Un servidor DNS es un servidor donde se traducen nombres de nodos de red en direcciones IP. Allí están declarados registros donde están las reglas de conversión y otras configuraciones. Este protocolo trabaja en la capa de aplicación según el modelo OSI. Existen diferentes tipos de registros, cada uno con su propósito:

* SOA: en estos registro se configura el servidor DNS en sí mismo.
* A: en estos registros se configuran propiamente dicho la relación entre los nombres de dominio y las IPs.
* NS: en estos registros se configuran la relación entre los nombres de dominio y otro servidor DNS donde se resuelven.
* CNAME: en estos registros se configuran los alias de los nombres de dominio.
* MX: en estos registros se Indica el host que se encarga del procesamiento del correo electrónico de ese dominio.

En la red implementamos los diferentes servicios pedidos: servidores web, servidor de correo, impresoras, puntos de acceso wireless y sniffers. Los tres primeros servicios se alocan en servidores con IP estáticos ya que necesitan ser inequívocamente identificados en la red; los sniffers no necesitan IP ya que trabajan en la capa inmediatamente inferior (capa de enlace) puesto que consisten en una placa de red en modo promiscuo o monitor, que archiva todo el tráfico de red que pasa ella.

Los servidores web están divididos en dos grupos: los que trabajan con protocolo HTTP y los que lo hacen con protocolo HTTPS, ambos protocolos de capa de aplicación. A través de estos protocolos, los clientes que lo requieran pueden obtener los conjuntos de archivos que hacen a una página web: HTML, CSS, JS, etc. La principal diferencia entre HTTPS y HTTP es que en el primero la información que va del cliente al servidor viaja cifrada, lo que permite que frente a una eventual captura de estos datos no sea posible obtener directamente la información que contienen, en cambio en el segundo los datos viajan en texto plano.

Cada una de las sedes posee su propio tramo de red. Para poder conectar las redes entre sí se ubicó un router en cada red y se los interconectó. Para esto fue necesario especificar en cada uno cómo llegar de una red a otra. Además, hay un router más que media entre la intranet y la internet.

1. **Diseño** 
   1. **Capa 1**

Para la interconexión de las sedes se usó fibra óptica por su velocidad. Para conectar los diferentes pisos de cada una de las sedes se implementó un cableado vertical con fibra óptica para ahorrarnos el problema de la diferencia de impedancia. La comunicación en cada piso se da por cableado trenzado.

* 1. **Capa 2**

En la sede CABA se implementaron 3 VLANs adicionales a la default: una para todas las dependencias de la Secretaria Académica, otra para las que dependen de la Secretaría de Hacienda y una tercera para las de la Secretaría General. Para lograrlo se configuraron piso a piso los routers involucrados en la comunicación entre las terminales de cada una de las dependencias y los servidores y el gateway. La comunicación entre las VLANs se da en el router que hace de gateway por medio de la declaración de interfaces lógicas virtuales sobre la interfaz con la que se conecta a la red interna de la sede CABA (fastEthernet 4/0 – 4/01 – 4/02 – 4/03).

* 1. **Capa 3**

En cada sede se usó para sus redes internas un tramo diferente de IPs privadas:

* CABA: 10.255.0.0/16
* Avellaneda: 172.16.0.0/16
* Quilmes: 192.168.0.0/16

A su vez, para las VLANs de la sede CABA se subneteó en los siguientes tramos:

* VLAN 2 (Sec. Académica): 10.255.1.0/22
* VLAN 3 (Sec. Hacienda): 10.255.5.0/22
* VLAN 4 (Sec. General): 10.255.9.0/22

A continuación, algunas IPs relevantes:

**Servidores web**

* unq.edu.ar 10.255.255.100
* campus.unq.edu 10.255.255.101
* info.campus.unq.edu.ar 10.255.255.102
* sh.unq.edu.ar 10.255.255.103

**Servidor de correo**

* Mail 10.255.255.230

**Servidores DHCP**

* + CABA
    - Default 10.255.255.254
    - VLAN 2 10.255.1.254
    - VLAN 3 10.255.5.254
    - VLAN 4 10.255.9.254

* + Avellaneda
    - Default 172.16.255.254

* + Quilmes
    - Default 192.168.255.254

**Servidores DNS**

* DNS-primario 10.255.255.250
* DNS-secundario 10.255.255.251
* DNS-Hacienda-Primario 10.255.255.240
* DNS-Hacienda-Secundario 10.255.255.241

1. **Conclusiones**

La necesidad de ahorrar en dispositivos físicos (routers, switches, servidores DHCP, cables, etc) y la limitación de posibles IPs que impone el protocolo IPv4 conllevo al desarrollo de tecnologías que buscan minimizar lo más posible estos inconvenientes: separación de tramos de red para uso privado, NAT y PAT y VLANs. Al ser tecnologías de capa 2 para arriba, implica que su implementación se da por medio de la configuración de los dispositivos de la red lo que conlleva a que la topología deje de ser el centro en el diseño de la red y pase a ser una herramienta para simplificar la implementación de estas tecnologías. A su vez, al no verse representadas estas configuraciones en la topología, es más complicado seguir el rastro sobre cómo interactúan los equipos en la red, lo cual puede llevar a confusiones. Para superar este obstáculo es fundamental diseñar antes de implementar y llevar una buena documentación siempre actualizada.