Instituto Tecnológico y de Estudios Superiores de Monterrey TC2036

Implementación de Redes Seguras

Interconectando una PYME a un proveedor de servicio utilizando un grupo reducido de direcciones IP públicas.

|  |
| --- |
| **Objetivo**: Configurar equipos de interconexión de red y habilitar los servicios de DHCP y NAT para conectar una red local con un proveedor de servicio. |
| **Subcompetencia de área:** SICT0401 Aplica los estándares y normas en el ejercicio de su profesión, manifestándolos como referencia a seguir en la solución de problemas computacionales y tecnologías de información. |
| **Subcompetencia de carrera:** STE0302 Selecciona el protocolo de comunicación. Selecciona el protocolo de comunicación de acuerdo a su aplicación. |

Los espacios de coworking o espacios de trabajo colaborativo, son instalaciones de trabajo en las que varias personas comparten el lugar físico con el fin de mejorar su productividad, hacer networking e inclusive reducir los costos de servicios y de renta de un espacio.

El coworking representa una gran oportunidad de negocio en México, así como en otros países, ya que representa una opción favorable para pequeñas empresas, startups y freelancers [1]. Un ejemplo de estos negocios es **COHAUS**, un espacio de coworking que ofrece desde espacios libres de trabajo y escritorios fijos, hasta salas de juntas y oficinas bien equipadas.[2]

Vamos a considerar el equipo de red de un negocio de coworking como **COHAUS**. Cada pieza de infraestructura pertenece al segmento de **administradores,** al segmento de **servicios** o al segmento de **usuarios**.

El segmento de **Administradores** está dedicado al personal del establecimiento y está constituido de no más de seis equipos terminales. Entre estos equipos están: dos cámaras web, dos puntos de venta, una impresora y una PC para el administrador. La asignación de direcciones IP, máscaras, puertas de enlace predeterminadas y DNS se asignan manualmente.

El segmento de **Servicios** está constituido por un servidor local, un teléfono IP y una impresora. Las direcciones IP de los equipos terminales se asignan manualmente.

Finalmente, en el segmento de **Usuarios** simplemente se encuentran los equipos personales conectados físicamente a la red. En este segmento de red existe la posibilidad de conectar hasta 80 equipos. Este segmento contiene una mezcla interesante de red alámbrica y red inalámbrica. La asignación de direcciones IP a los equipos del segmento de usuarios se realiza por **DHCP**.

Ahora tu labor es diseñar y configurar los equipos de interconexión de la red de **COHAUS** usando el simulador de Packet Tracer y comprobar que las configuraciones realizadas son exitosas.

Utiliza la aplicación del PacketTracer de CISCO y la Figura 1 (incluida en este documento) para: (a) completar el diseño lógico de la red, (b) la configuración del router y switches (c) la instalación del servicio de DHCP para asignar direcciones a los equipos terminales del segmento usuarios, (d) la instalación del servicio de NAT estático y dinámico y

1. las pruebas de conectividad necesarias y que permitan verificar la configuración correcta de los equipos de interconexión y de los equipos terminales.

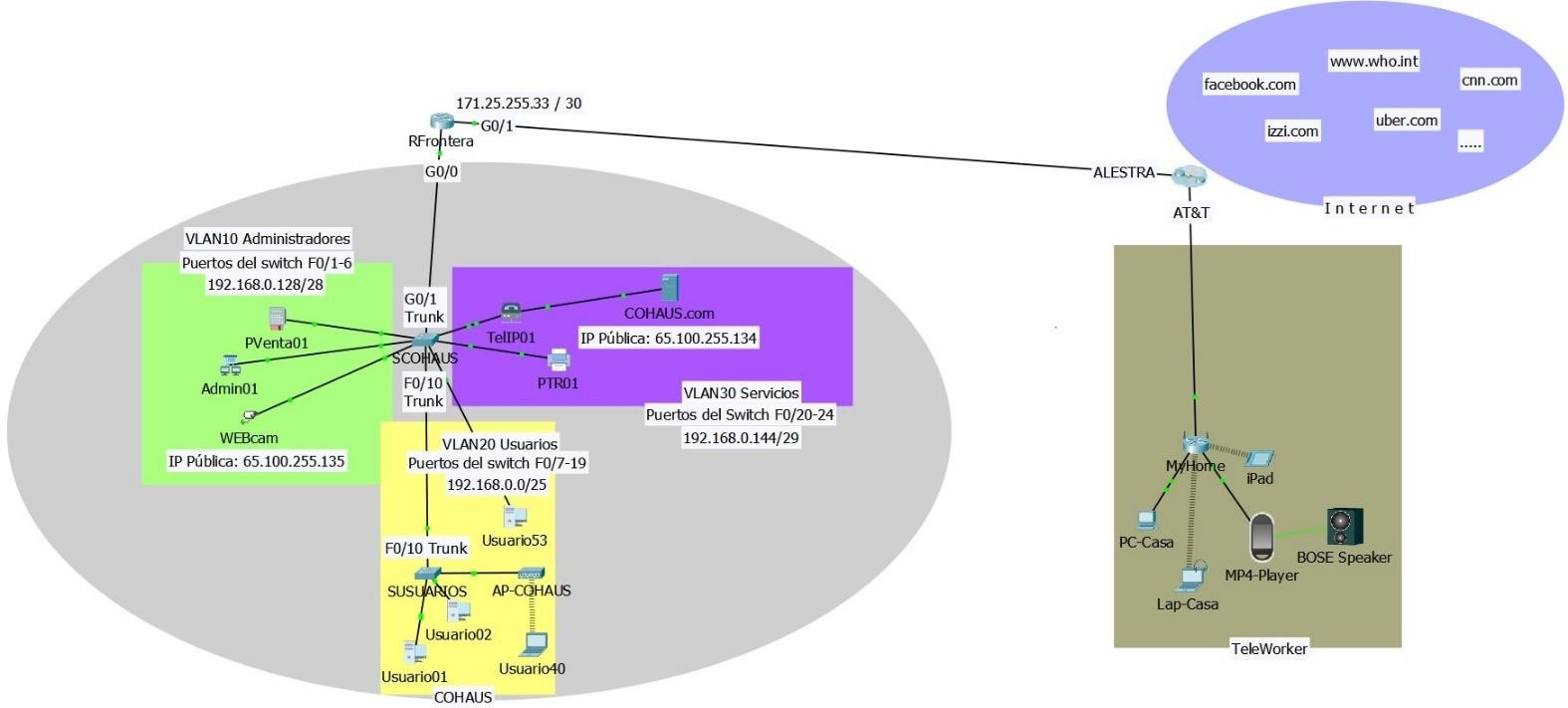


Figura 1. Diseño físico de la red.

La dirección IP a utilizar para realizar la configuración de los equipos de interconexión y la configuración de cada equipo terminal, es **192.168.0.0** con prefijo original de red **/24**.

El **VLSM** calculado con base en la descripción de equipos terminales que se requieren conectar en cada segmento de red está indicado en la Tabla 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Requisitos de Conectividad** | **Prefijo Red** | **IP Bloque** | **Máscara** | **Primera IP válida** | **Última IP válida** |
| **Usuarios** | **/25** | **192.168.0.0** | **255.255.255.128** | **192.168.0.1** | **192.168.0.126** |
| **Administradores** | **/28** | **192.168.0.128** | **255.255.255.240** | **192.168.0.129** | **192.168.0.142** |
| **Servicios** | **/29** | **192.168.0.144** | **255.255.255.248** | **192.168.0.145** | **192.168.0.150** |

Tabla 1

* 1. Asigna, de acuerdo a lo que se pide en la Tabla 2, las direcciones IP de las interfaces de los equipos de interconexión y su máscara en notación punto decimal. Anota en la Tabla 2 esta información.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **RFrontera** | **G0/0.10** | Última IP válida de la subred Administradores | 255.255.255.240 | N/A |
|  | **G0/0.20** | Última IP válida de la subred Usuarios | 255.255.255.128 | N/A |
|  | **G0/0.30** | Última IP válida de la subred Servicios | 255.255.255.248 | N/A |
|  | **G0/1** | 172.25.255.33 | 255.255.255.252 | N/A |
| **Usuario01** | **NIC** | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| **Usuario02** | **NIC** | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| **Usuario03** | **NIC** | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| **PVenta01** | **NIC** | Primera IP válida del bloque correspondiente | 255.255.255.240 | Dirección IP de la subinterfaz G0/0.10 |
| **CámaraWEB** | **NIC** | Segunda IP válida del bloque correspondiente | 255.255.255.240 | Dirección IP de la subinterfaz G0/0.10 |
| **Manager** | **NIC** | Tercera IP válida del bloque correspondiente | 255.255.255.240 | Dirección IP de la subinterfaz G0/0.10 |
| **ServidorLocal** | **NIC** | Primera IP válida del bloque correspondiente | 255.255.255.248 | Dirección IP de la subinterfaz G0/0.30 |
| **Impresora** | **NIC** | Segunda IP válida del bloque correspondiente | 255.255.255.248 | Dirección IP de la subinterfaz G0/0.30 |

Tabla 2

* 1. Realiza, con base en la información de la Tabla 2, la configuración manual de las interfaces de red de los equipos de las subredes de **Administradores** y **Servicios**. Utiliza, para todos los equipos terminales, la dirección 8.8.8.8 como la dirección IP del servidor DNS.
  2. Realiza la configuración de las interfaces y subinterfaces del **Router Frontera**. Deshabilita el **DNS**. Asigna

**RFrontera** como nombre del equipo.

* 1. Realiza la configuración de las **VLANs** del switch **SUsers**. Asocia a cada **VLAN** los puertos que le correspondan. Establece como **trunk** el puerto definido para tales fines.
  2. Realiza la configuración de las **VLANs** del switch **SCompany**. Hostame **SCompany**. Asocia a cada **VLAN** los puertos que le correspondan. Establece como **trunk** los puertos definidos para tales fines.

Realiza pruebas de conectividad de la PC Admin01 a la dirección IP del server y de la impresora del segmento

# Servicios.

* 1. Instala en el **RFrontera** el servicio de **DHCP** utilizando el bloque de direcciones IP y máscara del segmento de

**Usuarios**, la dirección IP de la subinterfaz g0/0.20 como la dirección IP para el dafault-router y la dirección

8.8.8.8 como la dirección IP del dns-server.

* 1. Utiliza, del bloque de direcciones IP públicas **65.100.255.128 /29**, las direcciones IP **65.100.255.134** y **65.100.255.135** para realizar la traducción estática de la dirección IP privada del servidor **COHAUS.com** y respectivamentede la cámara web. El resto de las direcciones del pool será utilizado para realizar el NAT dinámico para todos los equipos de la red y así lograr la conectividad con el exterior.

**NOTA**: Utiliza toda la información disponible en el diseño físico de la red (Figura 1) para realizar una configuración exitosa.

# Para comprobar la configuración realizada:

1. Accede desde los equipos terminales **Usuario01**, **Usuario02**, **Usuario53** y **Admin01**, a la dirección IP privada del servidor **COHAUS.com**. Si las pruebas son exitosas, tu configuración de VLANs y DHCP son correctas. En caso contrario, deberás encontrar y corregir la falla.

Realiza impresiones de pantalla completa de las pruebas de conectividad realizadas y preséntalas como evidencia en el siguiente recuadro.

1. Accede desde los equipos terminales **Usuario01**, **Usuario02**, **Usuario53** y **Admin01**, a los servidores externos: Uber.com, Facebook.com, LOL.com. Si las pruebas son exitosas, tu configuración de NAT dinámico son correctas. En caso contrario, deberás encontrar y corregir la falla.

Realiza impresiones de pantalla completa de las pruebas de conectividad realizadas y preséntalas como evidencia en el siguiente recuadro.

1. Finalmente, para comprobar que la cámara web y el servidor COHAUS.com está correcta debes acceder desde cualquiera de los dispositivos del TeleWorker y acceder, vía web, a COHAUS.com y a la dirección IP pública de la cámara web, Si las pruebas son exitosas, tu configuración de NAT estático es correcta. En caso contrario, deberás encontrar y corregir la falla.

Realiza impresiones de pantalla completa de las pruebas de conectividad realizadas y preséntalas como evidencia en el siguiente recuadro.

**Referencias**

1. Solís, A. (2018). *Guía Forbes de Coworking: todo lo que necesitas saber*. Recuperado de [https://www.forbes.com.mx/guia-forbes-de-coworking-todo-lo-que-](https://www.forbes.com.mx/guia-forbes-de-coworking-todo-lo-que-necesitas-saber/) [necesitas-saber/](https://www.forbes.com.mx/guia-forbes-de-coworking-todo-lo-que-necesitas-saber/)
2. COHAUS. (s.f.). *Paquetes*. Recuperado de <https://cohaus.work/paquetes/>