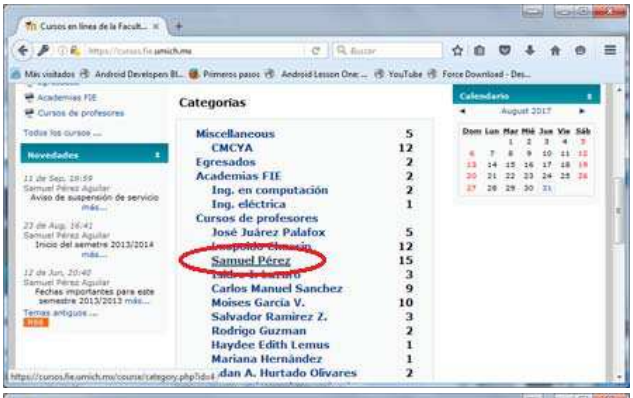
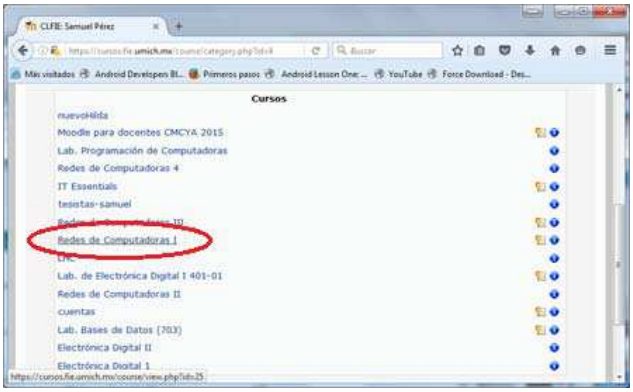
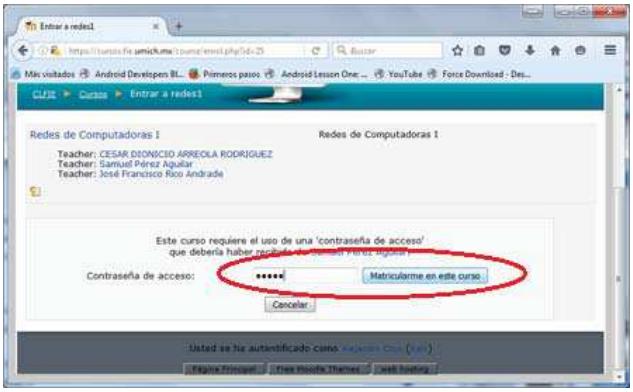
Práctica 1.1

- Presentación
- Politicas Generales del Curso
  - Matricularse en curso en línea.

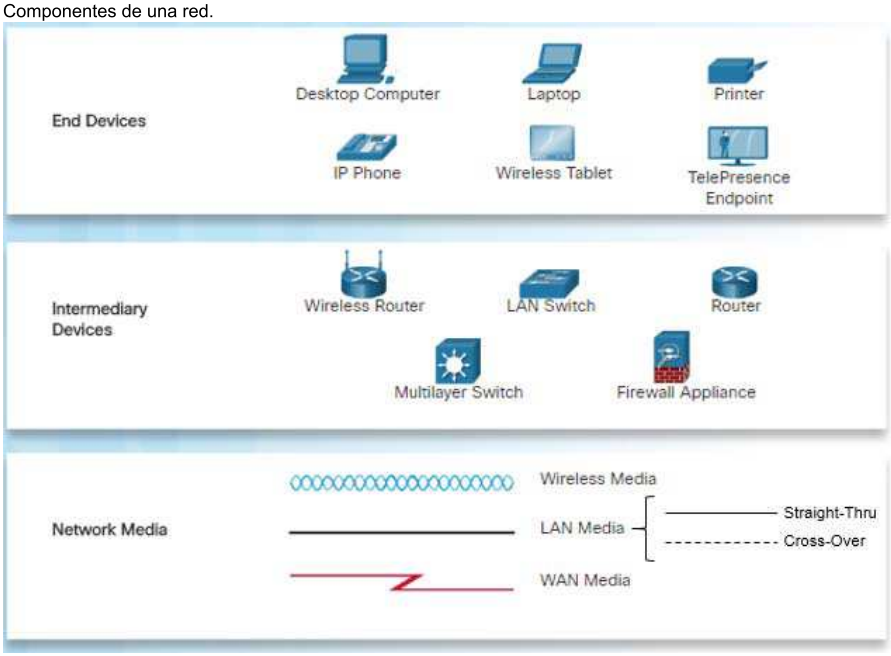






- Políticas del Curso 2017/2018

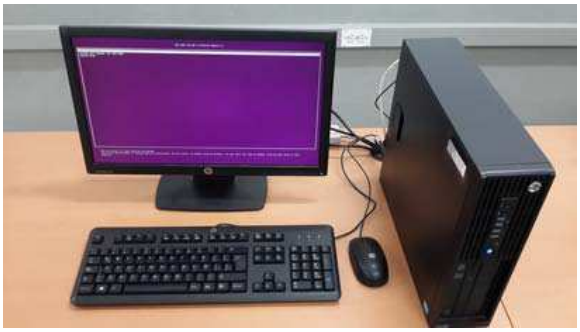
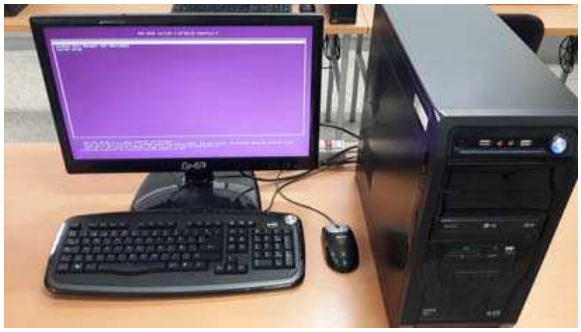
- Explicación de la estructura y políticas del Laboratorio de Redes
  - Componentes de una red.



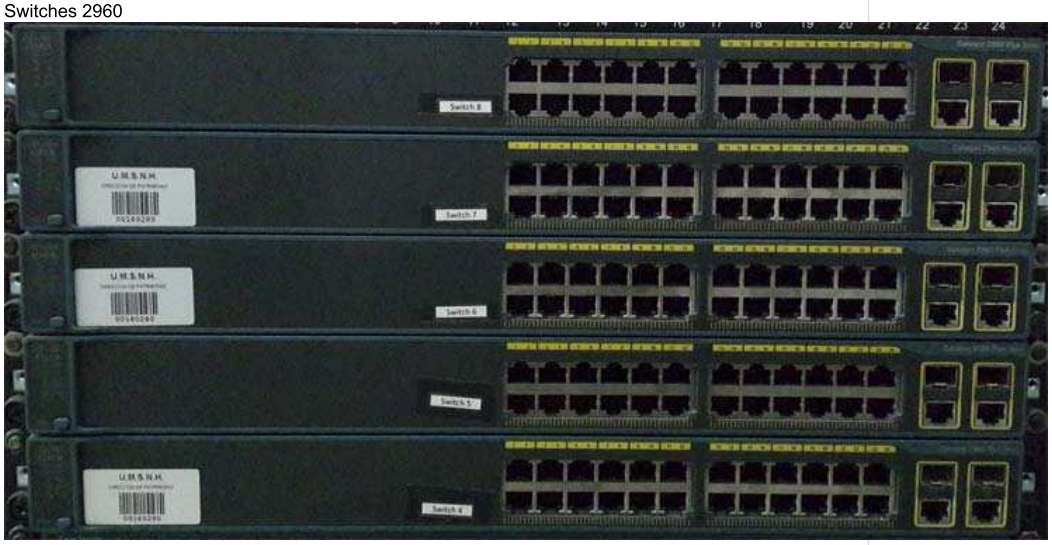
  - Rack: término inglés que se emplea para nombrar a la estructura que permite sostener o albergar un dispositivo tecnológico.

- Reguladores: alimentan equipo en el rack.
  - 

- Equipos Finales
  - El Laboratorio de Redes y Comunicaciones cuenta con 3 tipos de PCs principales:

- PCs HP 
- PCs Ghia 
- PCs Acer 
  - Todas las máquinas HP y GHIA estan conectadas al rack frontal
  - Las pcs Acer se conectan al rack posterior.
  - Para iniciar sesión en cualquier computadora, utilizar tanto para usuario como contraseña: "ccna"
- Equipos Intermedios
  - Switches 2950

- Switches 2960



- Router 1841

- Router 2911

  - Mesas
    - Las mesas al igual que las pcs tienen un numero asignado p.e. ccna05
    - Dicho número se considera de Este a Oeste y de Sur a Norte.
    - El numero de cada mesa puede localizarse en las tomas de servicio de la intranet.
    - Las PCs tienen ese mismo número en un etiqueta debajo del mouse y teclado.

- Servicios de Red por Mesa 

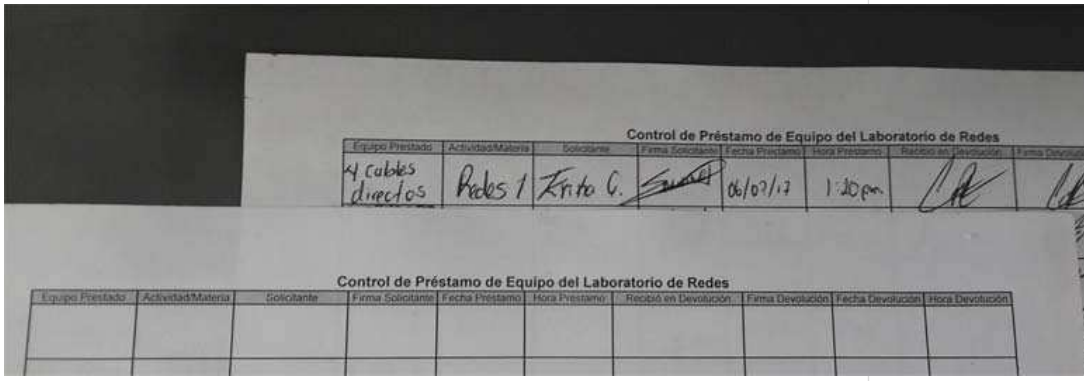
- Cada mesa cuenta con dos jacks rj45 blancos, uno azul y uno negro.
  - Excepciones:
    - En la mesa 13 hay 2 azules pero uno mas oscuro que el otro, el mas oscuro debe ser considerado como negro.
    - En la mesa 14 hay 2 azules pero uno esta marcado con número, el que tiene número debe ser considerado como blanco.
- Número de Mesa = Número de Equipo 

- Paneles de Parcheo:
  - Un panel de parcheo, es el elemento encargado de recibir todos los cables del cableado estructurado.
  - Sirve para que los elementos finales de la red de área local (LAN) y los equipos intermedios puedan interconectarse fácilmente.
  - Extremo en el rack del cableado hacia las mesas.
  - 

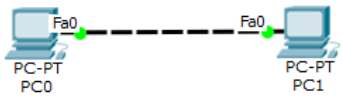
  - Los jack azules y blancos de cada mesa se identifican en el panel de parcheo con etiquetas del mismo color(Los azules en azul, los blancos en blanco)
    Los jacks en negro se identifican en el patch panel por etiquetas en color amarillo descolorido.

        - Los jack blancos de cada mesa tienen un numero 1 o 2 y en conjunto con el numero de mesa Vgr; 5, forman 5.1 y 5.2 y eso identifica ese puerto en el rack (Vgr; jack color blanco con etiqueta 5.1).
        - Hay cables que van del rack frontal al rack posterior, y se identifican con los numeros del panel de parcheo:
            - el 21 con el 21
            - el 22 con el 22
            - el 23 con el 23
            - el 24 con el 24
            - En ambos paneles de parcheo.
    - Cables
        - Directo vs Cruzado

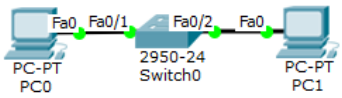
    - Prestamos
        -



- Interconexión de dispositivos:
    - Directamente mediante cable cruzado



        -
    - Conmutados mediante un switch y cables directos.



        -

- Compartir Carpetas en Windows

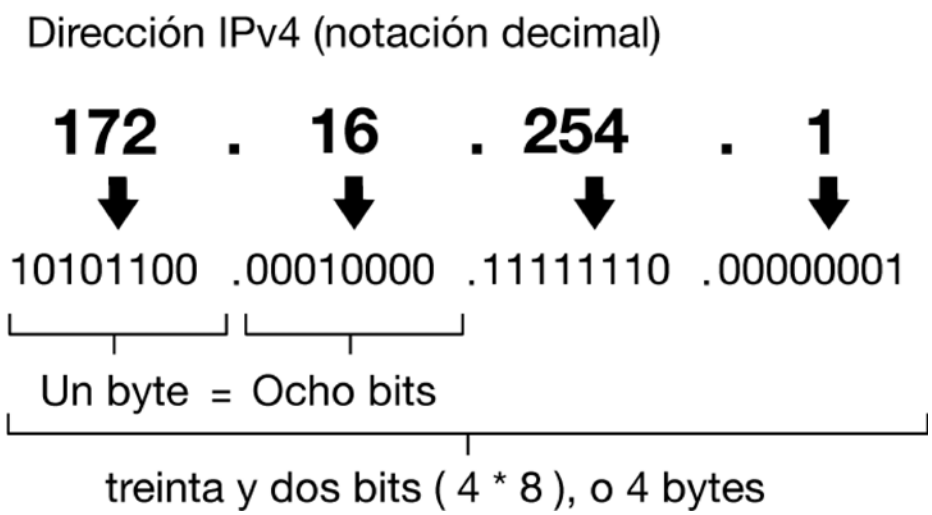
- **Tarea 1.1:** Investigar e implementar comparticion de carpetas entre Windows y Linux.
- **Tarea 1.2**: Investigar sobre redes AD-Hoc por 802.11 e implementar con 2 laptops (Una Windows y otra Linux).

- **Notas**:
    - Establecer Direcciones IP entre: 192.168.1.1 y 192.168.1.253
    - Establecer Mascara de Subred: 255.255.255.0

- Establecer Puerta de Enlace como: 192.168.1.254
    - Como establecer una dirección ip estática en Windos 8.1.
    - Como establecer una dirección ip estática en Windos 7.
    - Como establecer una dirección ip estática en Ubuntu 14.04

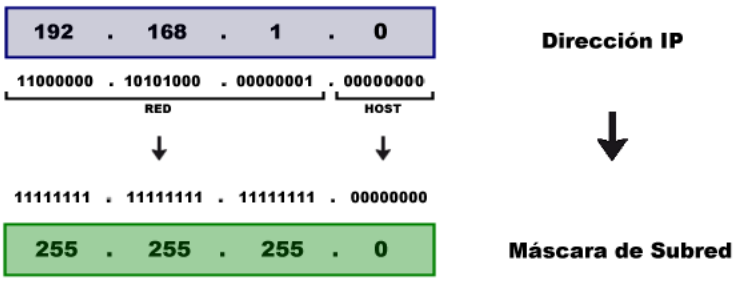
- **Preparación para siguiente práctica:** Recordar conversiones binario/decimal y decimal/binario.

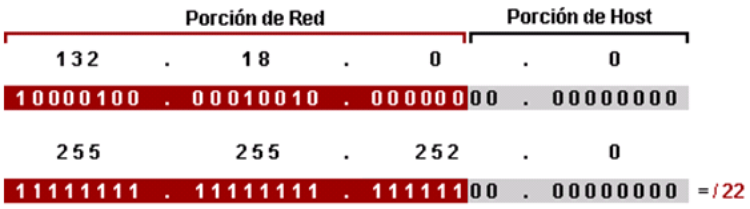
- Descripción Básica del Direccionamiento IPv4
  - Dirección IPv4: Identificador de Red (valor de 32 bits)
    - Representación Decimal con Puntos:

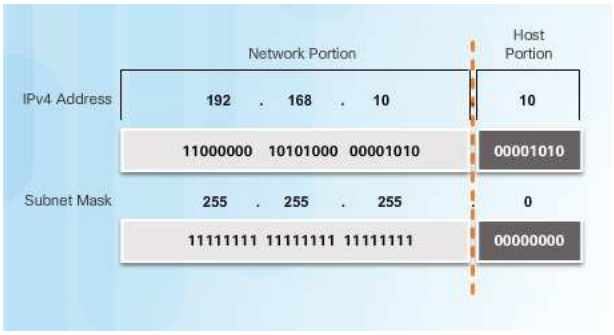


  - Mascara de Subred: Identifica porción de red y de host de una IP.
    - 1s consecutivos de izquierda a derecha: Porción de Red.
      Cantidad de 1s --> notación de Prefijo (/#1s)
    - 0s consecutivos de derecha a izquierda: Porción de Host

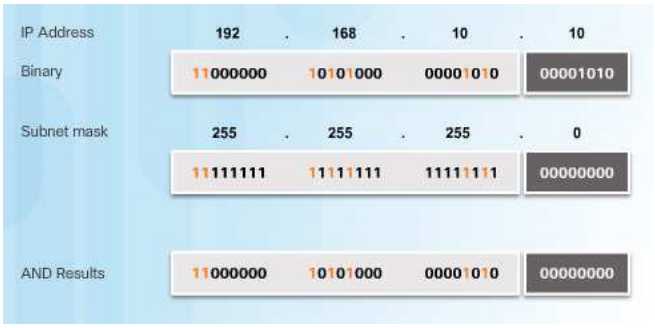
Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30







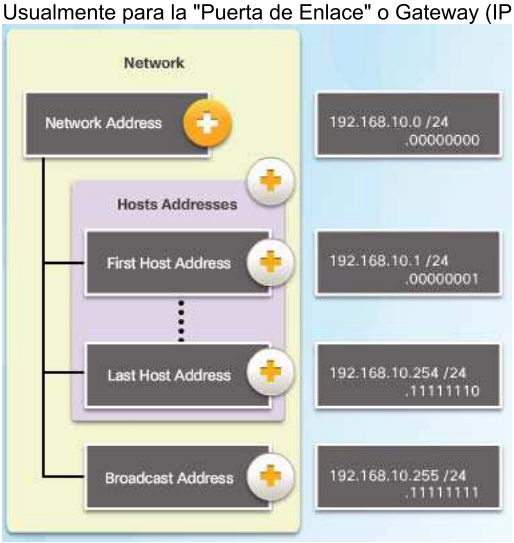
- Dirección de Red: Manera de referirse a una red
  - Contiene 0s en todos los bits de host
  - Dirección de Red = Dirección IP & Mascara de Subred



- Direcciones de Broadcast: Para comunicación con todos los hosts de una red.
  - Contiene 1s en todos los bits de host
  - Broadcast = Red | (! Mascara)

- Dirección de Host: Identifica a un dispositivo
  - Contiene 0s y 1s en los bits de host (No todos 0s y no todos 1s).
  - Primer host
    - Bit menos significativo de host en 1 el resto en 0
    - Primer host = Dirección de Red + 1

  - Último Host
    - Bit menos significativo de host en 0 el resto en 1
    - Último Host = Broadcast - 1
    - Usualmente para la "Puerta de Enlace" o Gateway (IP del dispositivo que permite llegar a otras redes)



- Cantidad de Hosts en una red: 2^(bits de host)-2

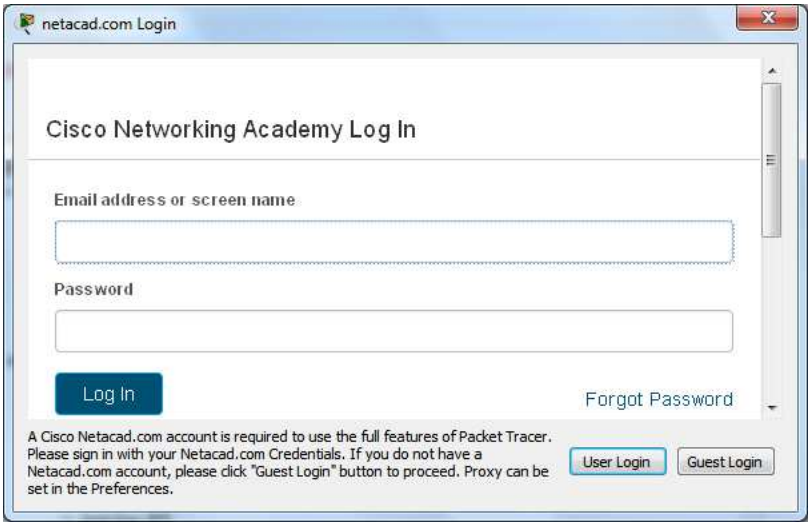
- Ejemplos:

	Dotted Decimal	Significant bits shown in binary
Network Address	**10.1.1.0/24**	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.254	10.1.1.11111110
Broadcast Address	10.1.1.255	10.1.1.11111111
Number of hosts: 2^8 – 2 = 254 hosts		

Network Address	**10.1.1.0/25**	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.126	10.1.1.01111110
Broadcast Address	10.1.1.127	10.1.1.01111111
Number of hosts: 2^7 – 2 = 126 hosts		

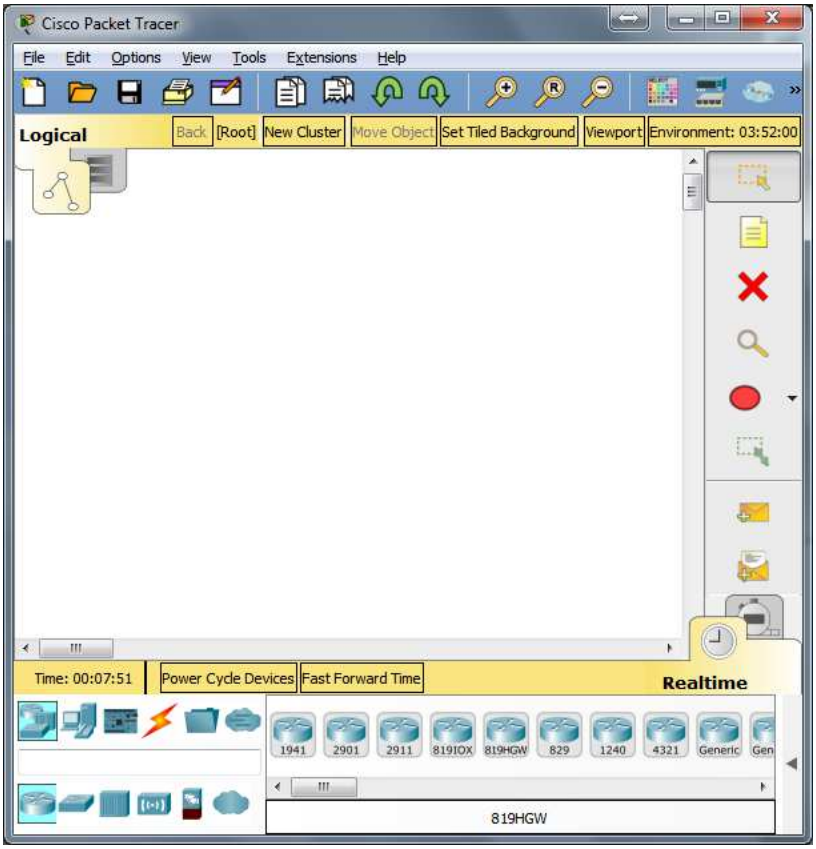
Network Address	**10.1.1.0/26**	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.62	10.1.1.00111110
Broadcast Address	10.1.1.63	10.1.1.00111111
Number of hosts: 2^6 – 2 = 62 hosts		

- Introducción a Packet Tracer.
  - Herramienta para la simulación y visualización de redes
  - 

  - Descargar Packet Tracer.
    - Iniciar sesión en https://www.netacad.com
    - --> Recursos --> Descargar PacketTracer
  - Iniciar PT
    - 

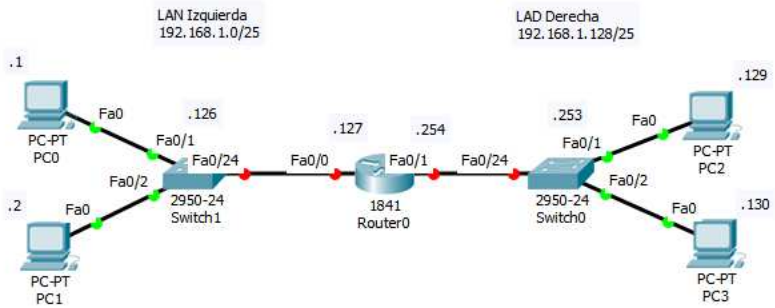
    - Iniciar Sesión con credenciales de Netacad

- Interactuar con la Interface Gráfica de Usuario.

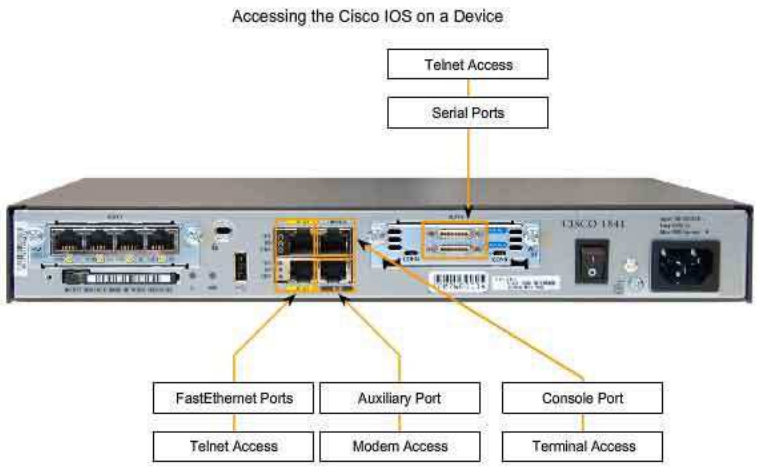


  - Cursos de PacketTracer
  - Video Tutoriales PT.

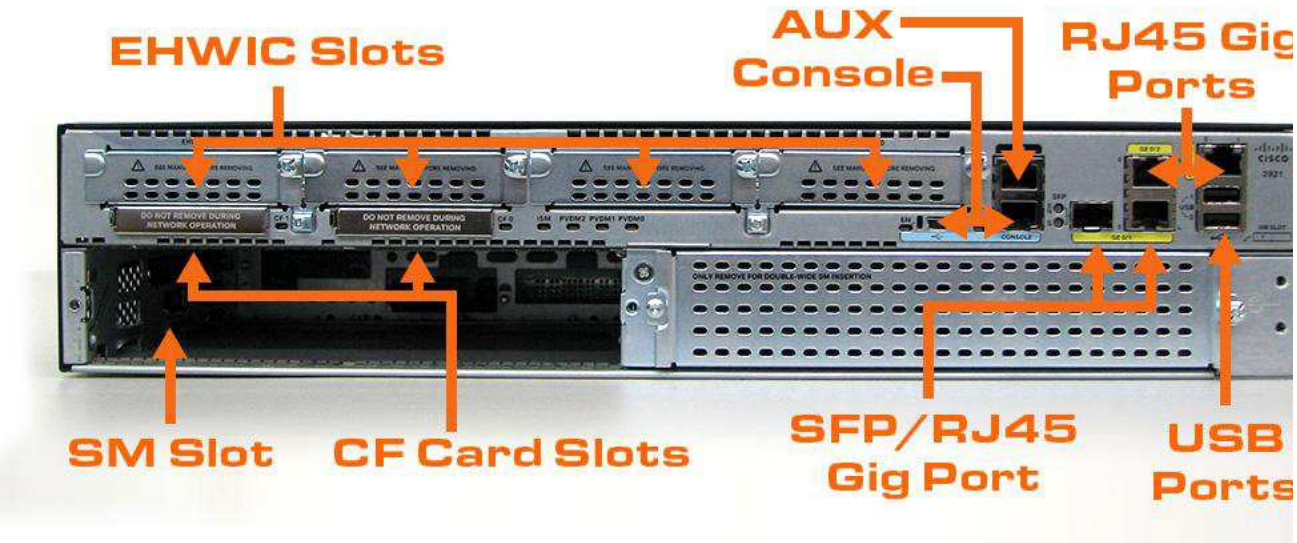
- Armado de una topología sencilla (Un Router + 2 Switches + 2PCs) en P.T.
  - Cantidad de Redes: 2



  - Conexión por consola a un dispositivo Cisco (Windows/Linux)
    - Router 1841



- Router 2911



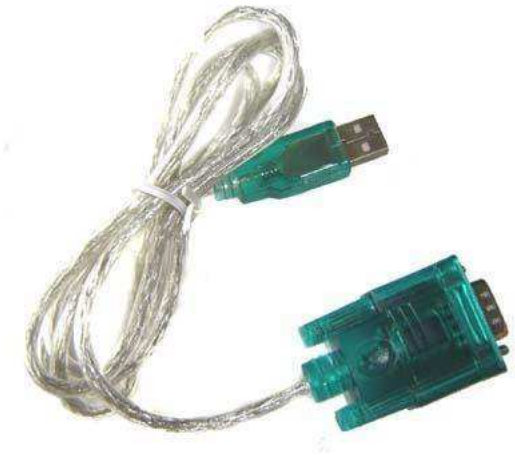
- Acceso a Puertos de Consola en Switches:
  - 
- Cables de Consola
  - Roll-Over + Adaptador JackRJ45 --> DB9 Female

Rollover wired Cables

  - Cable de Consola Serial (Puerto DB9)

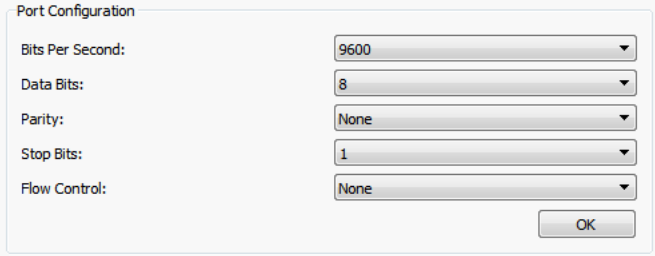
  - Algunas computadoras mas actuales no cuentan con puerto serial de conector DB9.

- Se requiere adaptador Serial a USB



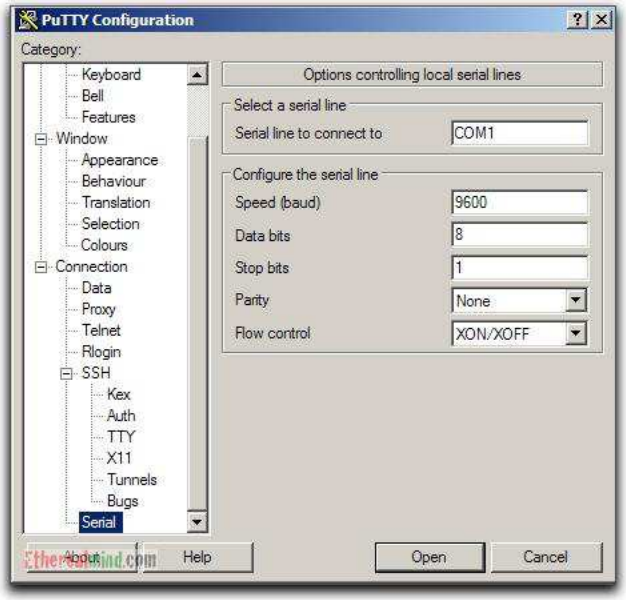
- Cable de Consola USB

- Software de Emulación de Terminal.
  - Parámetros Generales a Configurar:



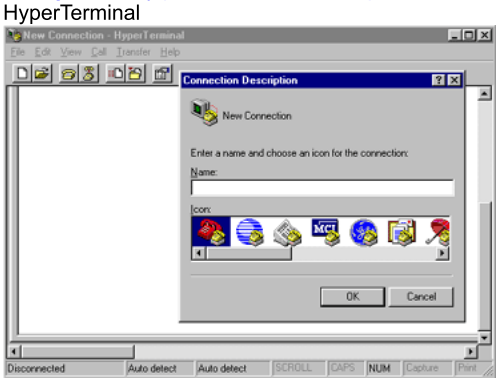
  - Software Windows

- Putty



Configurar Putty para acceder a un dispositivo Cisco.

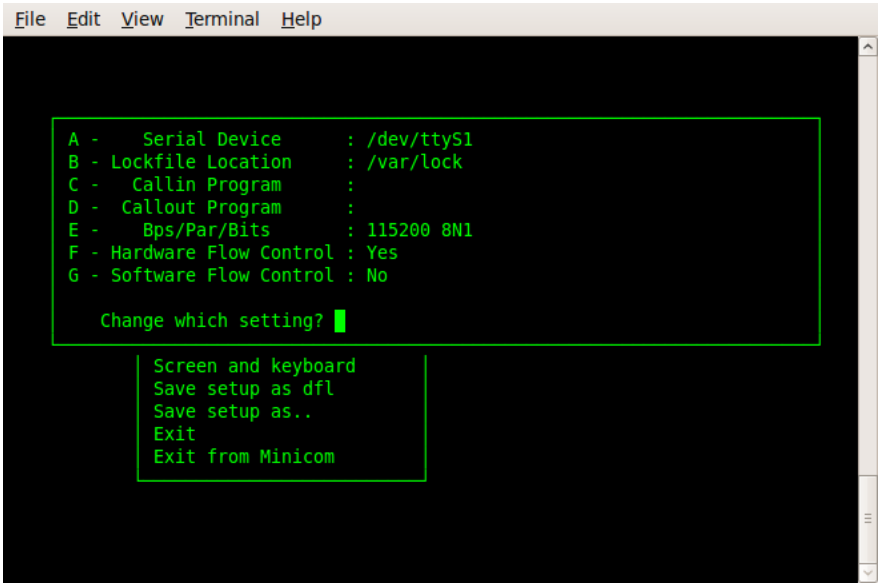
- HyperTerminal



Configurar Hyperterminal para acceder a un dispositivo Cisco.

- Entre Otros

- Software Linux
  - minicom



  - Configurar minicom para acceder a un dispositivo Cisco.
  - Alternativa.

- Establecer la configuración Básica mediante línea de comandos del IOS (CLI).
  - Nombre de Dispositivo
    - `Router(config)# hostname R`
  - Banner
    - `R(config)# banner motd @ Mensaje @`
  - Deshabilitar busqueda DNS
    - `R(config)# no ip dommain-lookup`

        - Contraseñas y su encriptación
            - `R(config)# enable password cisco123`
            - `R(config)# service password-encryption`

              vs
            - `R(config)# enable secret cisco123`
        - Configuración de Líneas
            - `R(config)#line {console 0 | vty 0-15}`
            - Contraseñas de Login
                - `R(config-line)# password cisco123`
                - `R(config-line)# login`
            - Tiempo de Inactividad
                - `R(config-line)# exec-timeout 5 30`
            - Sincronía de mensajes de logs
                - `R(config-line)# logging synchronous`
        - Configuración de Interfaces
            - `R(config)# interface FastEthernet {0/0| 0/1}`
            - `R(config)# interface Serial {0/0/1 | 0/0/1}`
            - `S(config)# interface vlan 1`
        - Descripción de Interfaces
            - `R(config-int)# description LAN Fulana`
        - Asignación de IPs a interfaces.
            - `R(config-int)# ip address 192.168.1.1 255.255.255.0`
        - Gateway en Switches
            - `S(config)# ip default-gateway 192.168.1.1`

    - Guardar configuración en NVRAM
        - `R# copy copy running-config startup-config`

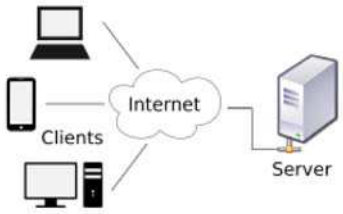
- Configuración Estática de Interfaces de Red en PCs físicas.
    - Como establecer una dirección ip estática en Windos 8.1.
    - Como establecer una dirección ip estática en Windos 7.
    - Como establecer una dirección ip estática en Ubuntu 14.04

- Respaldo de la configuración de dispositivos Cisco.
    - Via Portapapeles / TFTP
        - `R# copy running-config tftp`

- Recuperación de Configuración ante, contraseñas perdidas y Limpieza o Eliminación de Configuraciones.
    - Switch:
        - Presionar Botón "Mode"
        - `flash_init`
        - `load_helper`
        - `delete flash:config.text`
        - `delete flash:vlan.dat`
        - `boot`
    - Router:
        - Send Break (`Ctrl+Pause` / `Ctrl+A, F`)
        - `confreg 0x2142` ! Ignora NVRAM
        - `reset`
        - `config-register 0x2102` ! Inicio Normal
        - `reload`
        - `show version` ! Verificar valor del registro para Inicio Normal

- Tarea 2.1.1: Configuración de Topología en Equipos Físicos (2PCs windows + 2PCs Linux).
    - Dar un nombre a cada equipo y nombrar el Router con el nombre del equipo.
- Tarea 2.1.2: Intercambiar archivos de configuración entre Equipos y restaurar configuraciones sin conocer las contraseñas.

- **Preparación para siguiente práctica:**
    - Lectura sobre servidores web, sniffers y sockets TCP/IP.

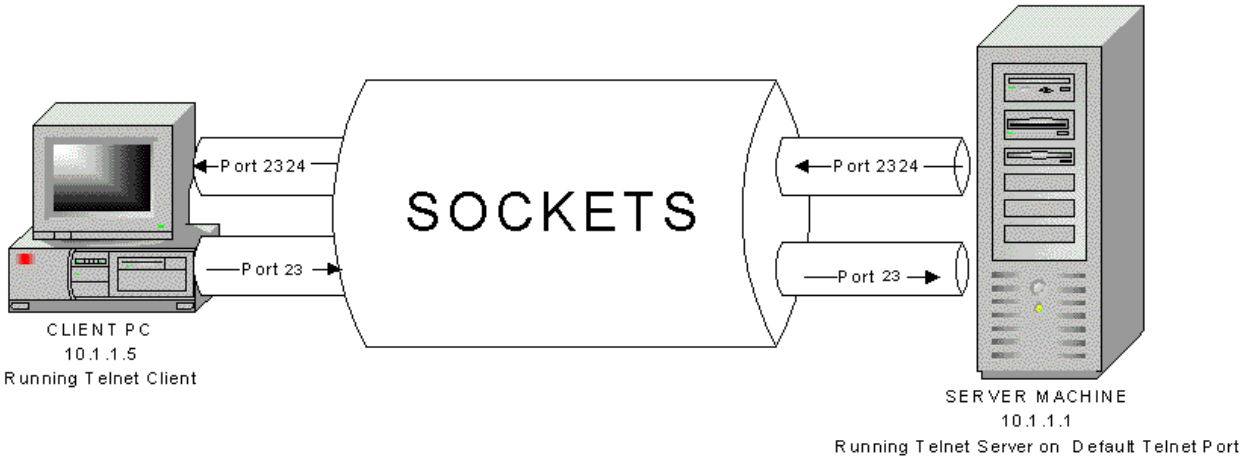
- Arquitectura Cliente Servidor:
  - 

  - Modelo de diseño de software en el que tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes.
    - Vgr; Servidor Web (Apache) vs Cliente Web (Firefox)
- Instalación de un servidor web
  - Instalación Configuración básica de un servidor web Apache
    - `$ sudo apt-get update`
    - `$ sudo apt-get install apache2`
    - Verificar en navegador web 127.0.0.1
    - Modificar configuración
      - `$ cd /etc/apache2`
      - `$ ls -F`

        ```
        apache2.conf envvars magic mods-enabled/ sites-available/
        conf.d/ httpd.conf mods-available/ ports.conf sites-enabled/
        ```
    - **apache2.conf**: Archivo principal de configuración. Casi cualquier configuración puede realizarse aquí, aunque se recomeinda subdividir en varios archivos para mantener un orden.
    - **ports.conf**: Archivo utilizado para especificar puertos de los hosts virtuales.
    - **conf.d/**: Este directorio es utilizado para controlar aspectos específicos de la configuración de Apache. Por ejemplo para definir configuraciones SSL.
    - **sites-available/**: Este directorio contiene todos los archivos de los hosts virtuales que definen diferentes sitios web. Esto ayuda a identificar que contenidos serán servidos ante diferentes solicitudes.
    - **sites-enabled/**: Este subdirectorio establece que definiciones de hosts virtuales están siendo utilizadas. Usualmente son ligas simbólicas a archivos definidos en "sites-available".
    - **mods-[enabled,available]/**: Estos directorios son similares en en funcionamiento al directorio sites, pero definen modulos que pueden ser cargados de manera opcional.

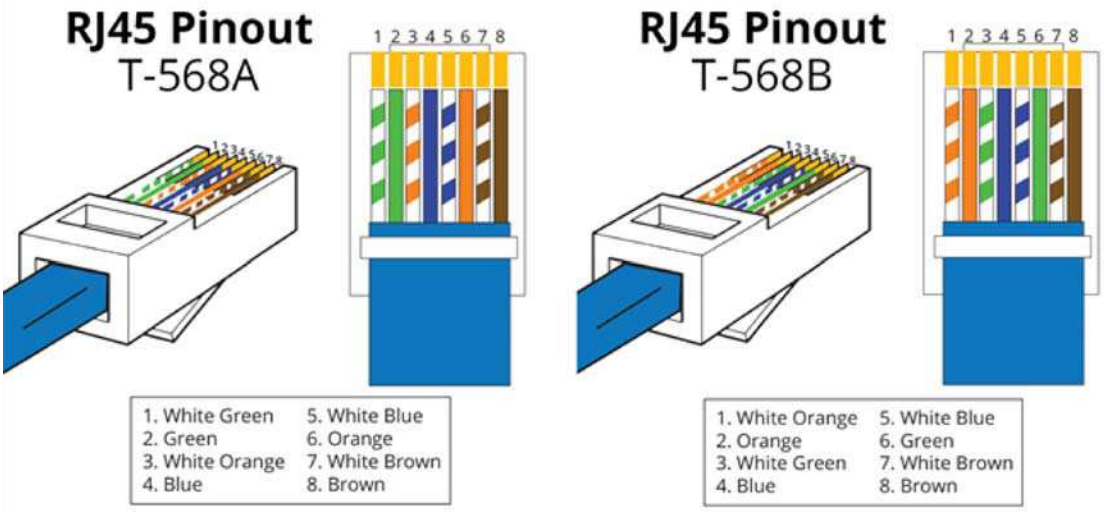
    - Acciones sobre el demonio.
      - `$ sudo /etc/init.d/apache2 start #start apache`
      - `$ sudo /etc/init.d/apache2 stop #stop apache`
      - `$ sudo /etc/init.d/apache2 restart #restart apache`
  - Modificación del archívo indice y puerto de escucha
  - **Tarea 3.1:** Instalar y configurar un servidor TFTP
- Análisis de Tráfico con Wireshark
  - Descripción básica de WireShark
  - Análisis de tráfico por capas de una comunicaicón HTTP
  - Nota: Puede encontrar información sobre como filtrar tráfico aquí.
  - **Tarea 3.2:** Análisis de tráfico por capas de una comunicaicón TFTP al respaldar una configuración de un Router/Switch
    - `Router#copy running-config tftp`
    - `Address or name of remote host []? <ip_serv_tftp>`
    - `Destination file name [Router-config]? <Nombre_del_archivo_a_guardar | Enter>`
    - `Writing running-config.....!!`
    - `[OK - ???? bytes]`
    - `???? bytes copied in ?.?? secs`
    - `Router#`
- Programación de Aplicaciones de Red:
  - Modelos de Redes:
    - OSIvsTCP/IP
    - Ejemplo:
      - Capa 1: Interfaces de Red y Cables (RJ45/UTP)
      - Capa 2: Codificación de Señales (MLT3/PAM5)
      - Capa 3: Identificación Lógica de Dispositivos y Tránsito de Paquetes (IP / Enrutamiento)
      - Capa 4: Identificación de Aplicaciones en el Dispositivo y Control de Transmisión de Segmentos (Puertos / TCP/UDP)
      - Capa 5: Identificar Sesión en un Aplicación (Pestaña del Navegador)

        - Capa 6: Define mecanismos de cifrado y compresión de datos de usuario, y renderizado (HTML --> Página Web)
        - Capa 7: Define mensajes a utilizar por la aplicación (HTTP: GET/POST/Parámetros)
    - Sockets:
        - Mecanismo para intercambiar datos entre dos aplicaciones (Cliente/Servidor).
        -



    - Programación de Sockets en C.
    - Programación de Sockets en Java.
- Envío de datos en estructuras por sockets en C y Java
    - Descripción básica para envio de datos mediante estructuras de datos.
        - Transferencia de Archivos de Texto en C
            - Servidor.
            - Cliente.
    - **Tarea 3.3:** Envío de un archivo binario en fragmentos de un equipo a otro mediante el uso deestructuras de datos con sockets (C | Java).
        - Deberá entregar 2 versiones, una que use sockets UDP, como los vistos en clase y otra que utilice sockets TCP (Investigar).

- Realizar Cables de Red UTP/RJ45 a la Medida.
  - **EIA/TIA-568-B** son tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones.
  - EIA/TIA-568-B (2001), sustituye a TIA/EIA-568-A (obsoletos).
    - Determina asignación de pares/pines en los cables de 8 hilos y 100 ohmios (cable de par trenzado):
      - T568A y T568B (Por defecto para Straight-Through).



    - Es un error nombarlos como estándares T568A y T568B.
    - Es incluso todavía peor llamarlos estándares TIA/EIA-568A y TIA/EIA-568B.

- **Material:**
  - Cable Unshielded Twisted Pair (UTP)
    UTP Cat5e vs UTP Cat6
    CablesUTP

  - Plug RJ45 Cat5e:

  - Plug RJ45 Cat6:
    PlugRJ45Cat6_00PlugRJ45Cat6
  - Jack RJ45 Cat5e vs Jack RJ45 Cat6:
    Jacks 5vs6

- Pinzas para Crimpar:

- Stripper:

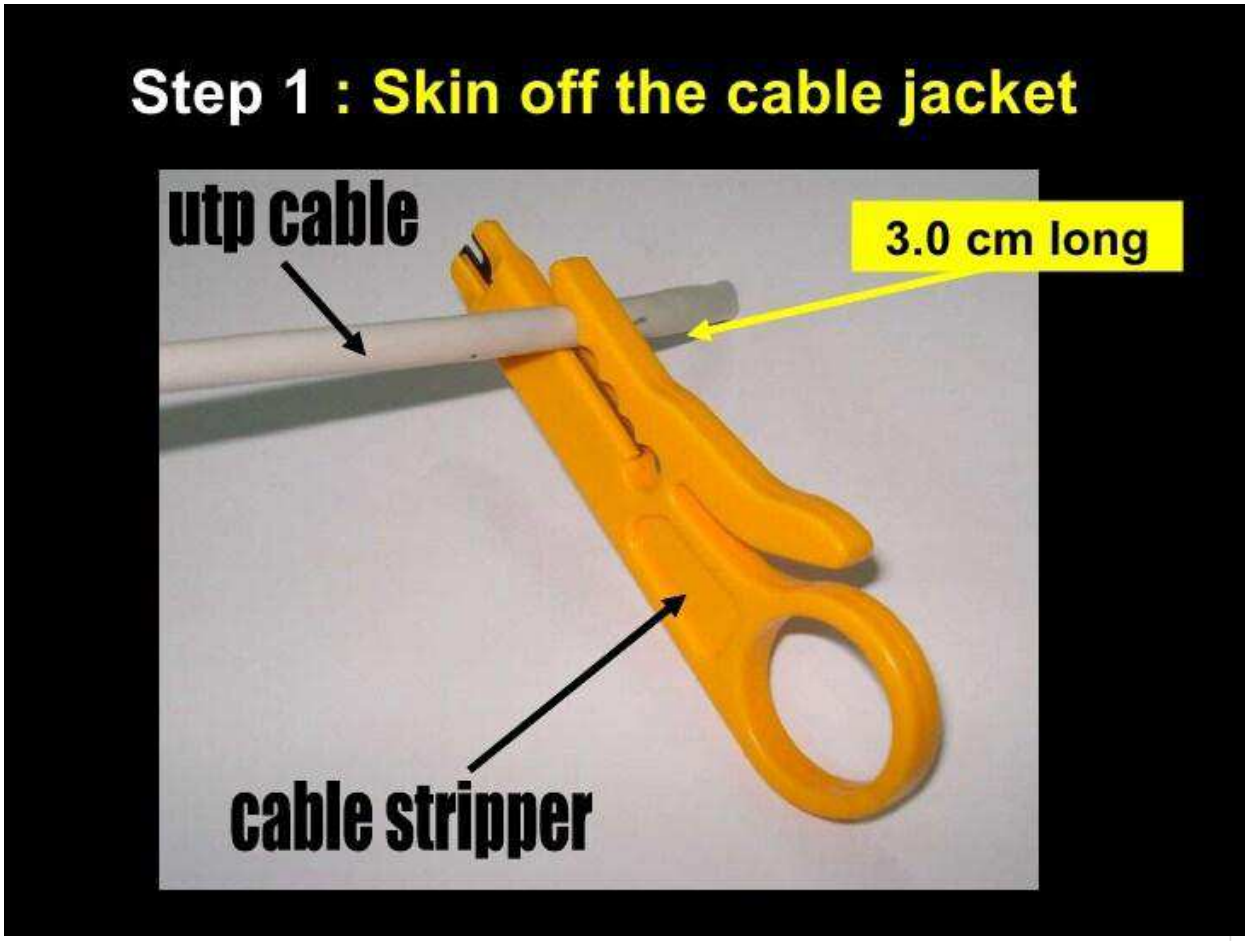
- Herramienta de Impacto:

- Navaja Reversible:

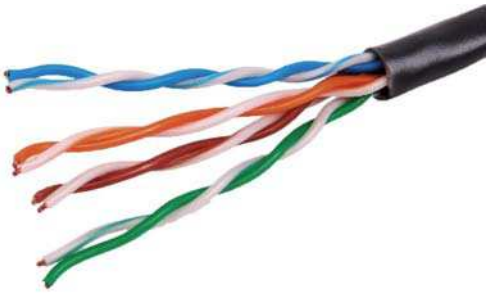
- Verificador de Cableado UTP:

- **Creación de un Cable Straight Through (Ambos extremos T568B)**
  - Cortar un tramo de Cable UTP (80cm Aprox)
    - Las pinzas de crimpar en la parte posterior, tienen una navaja para facilitar el cortado de cable.

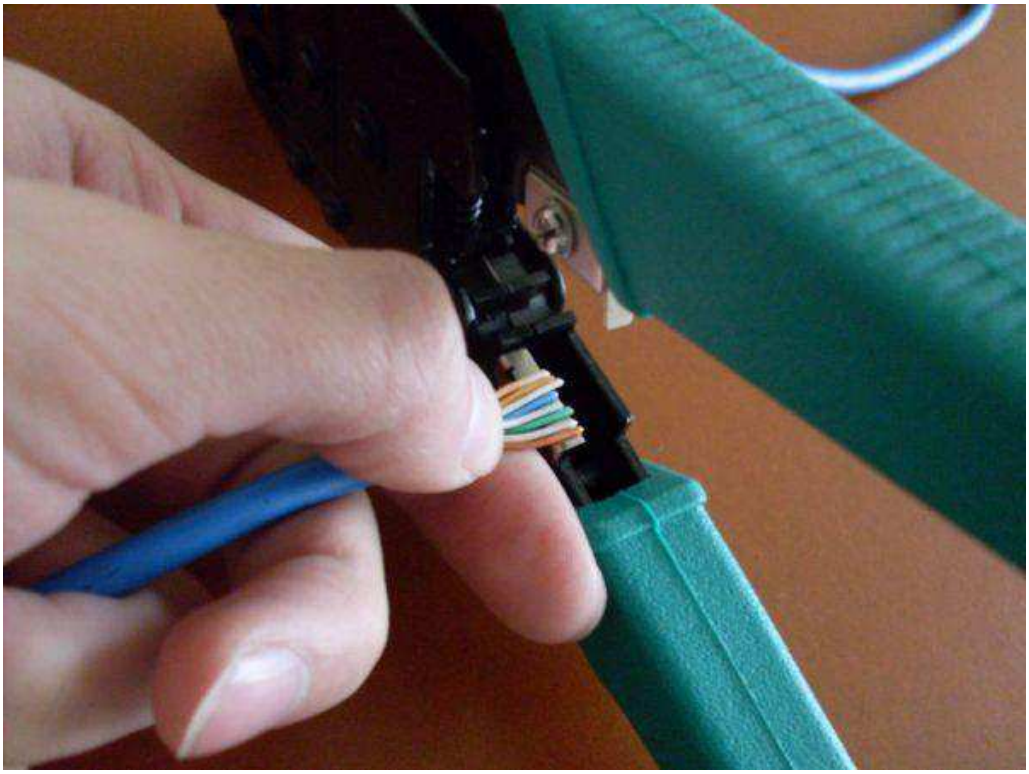
  - Desvestir 3cm (aprox) de cada extremo, con la ayuda de un stripper o una navaja, girando gentilmente alrededor del cable UTP, teniendo cuidado de no trozar los hilos internos.



- Una vez desvestido el cable debería lucir como las siguientes imágenes dependiendo de la categoría de su cable.

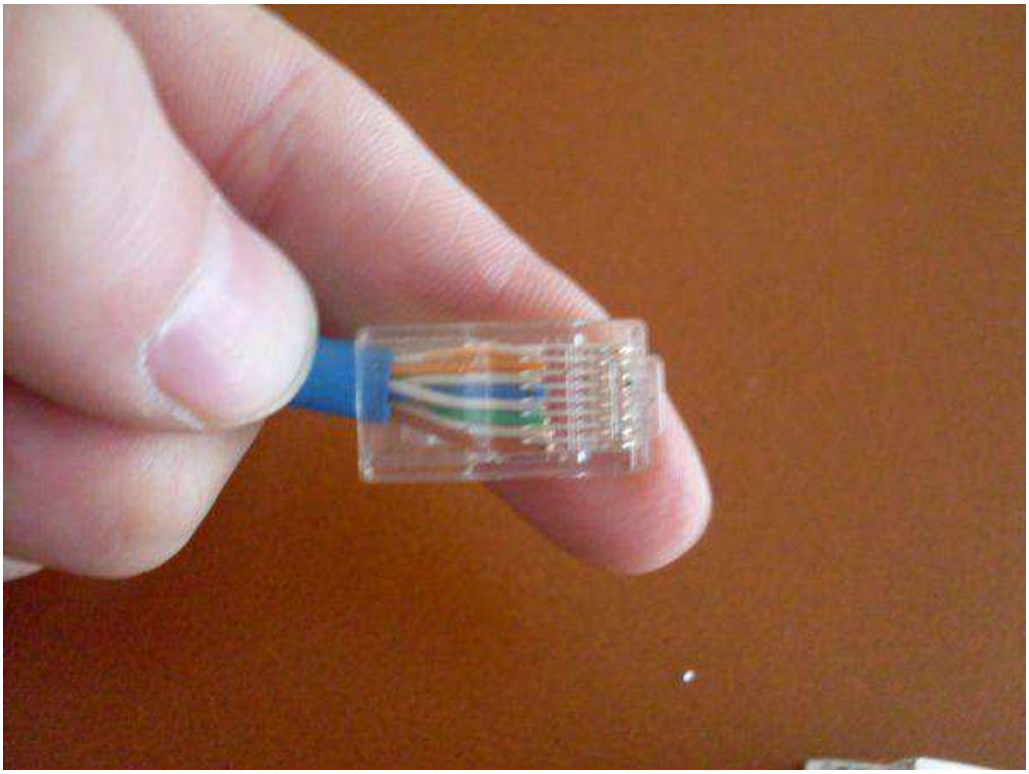


  - Categoría 5
  - Categoría 6: Utp6Desvestido
- Alinear y recortar los hilos acorde a la categoría del plug (Cat6 debe mantener trenzado dentro del plug, uso de guía opcional):

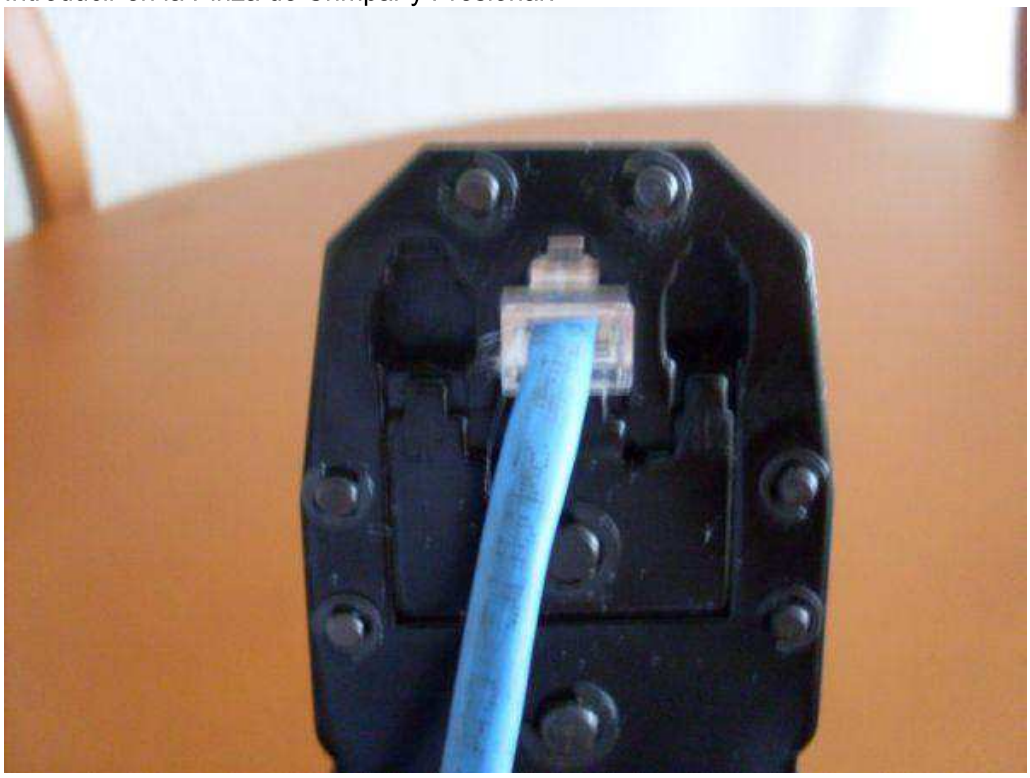


AlinearCat6

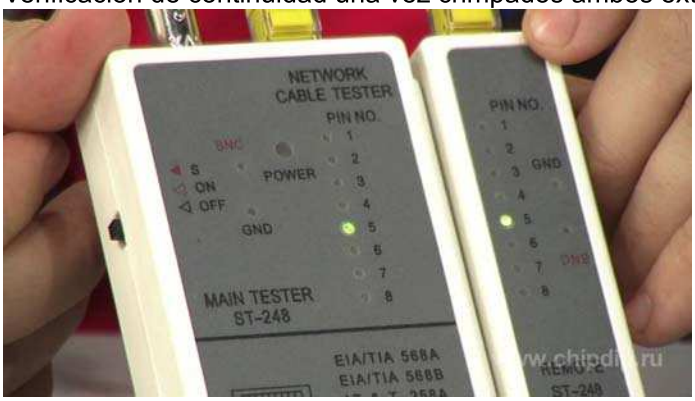
- Introducir hilos al Plug (Todos los hilos deben llegar hasta el tope del plug, y el revestimiento debe sobrepasar la muesca):



- Introducir en la Pinza de Crimpar y Presionar:

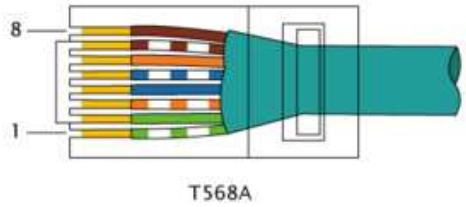


- Verificación Visual:
  CrimpadoCorrecto
- Verificación de continuidad una vez crimpados ambos extremos:



- **Creación de una mini-extensión Cross-Over.**

- Crimpar en un extremo un Plug con el pinout T568-A

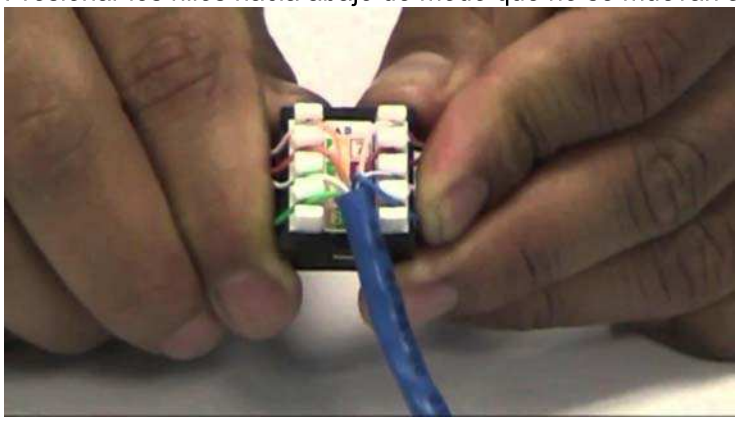


T568A

- Crimpar en el otro extremo un Jack RJ45 T568-B
  - Ubicar la posición de los hilos acorde al pinout y color.

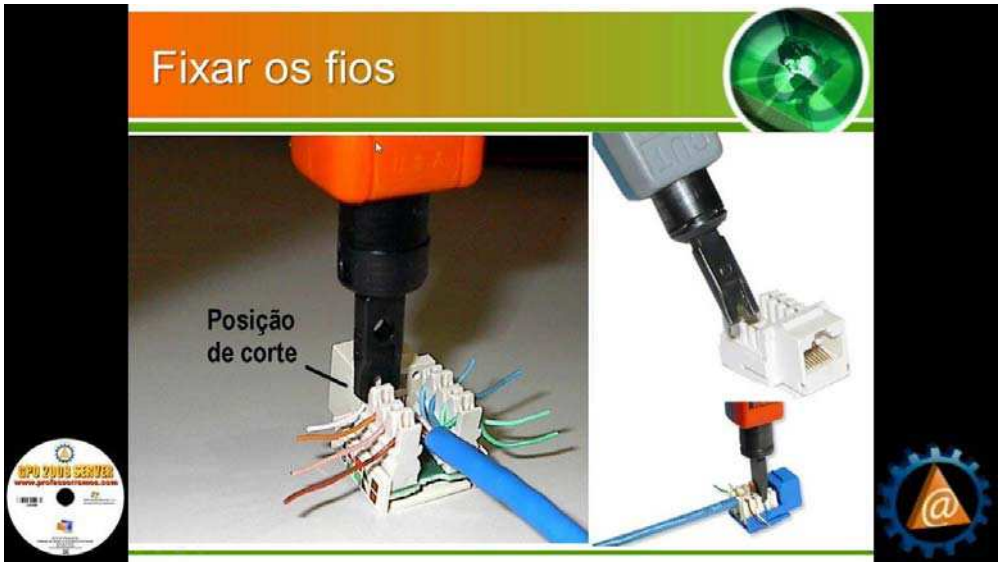
  - Desvestir 5cm de UTP y colocar en la posición adecuada:

- Presionar los hilos hacia abajo de modo que no se muevan al soltarlos:



- Colocar Navaja Reversible a la Herramienta de Impacto.

- Cuidadosamente coloque la herrmaienta de impacto en posición de corte y presionar cada hilo del jack hasta escuche un chasquido.



  - Verificar conectividad pines 1,2 con 3,6.

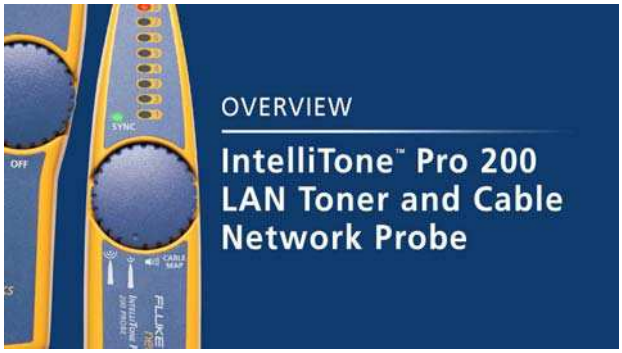
- Uso del generador de tonos, para identificar un cable dentro de un manojo.
  - El Generador de Tonos.

  - Mejor conocido como Pollo:

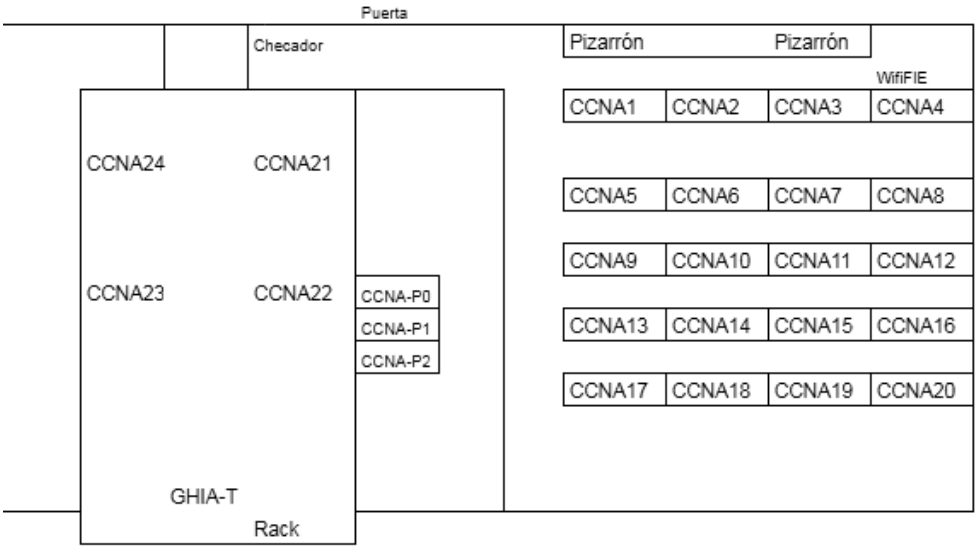
- Conectar un extremo del cable a buscar, al generador de tonos:

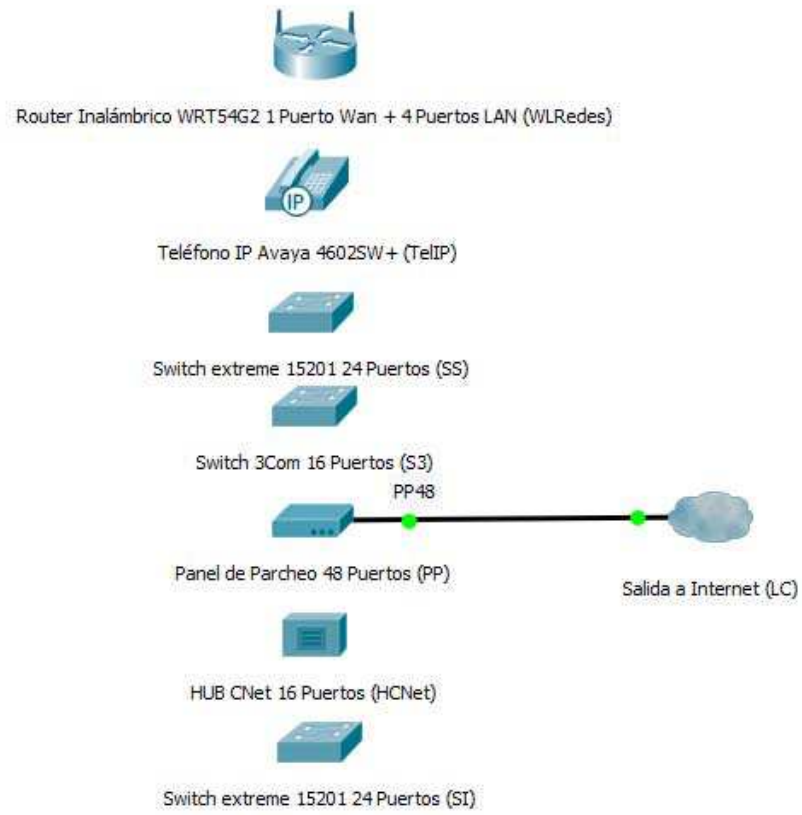
- Verificar la correcta operación del generador de tonos y el sensor (emisor de tonos).

- Probar identificar cables en muro de tablarroca/manojo de cables:



Actividad Práctica 4.1: Para 3 PCs del laboratorio y un equipio adicional: identificar los cable de red en la topología física del laboratorio, hasta su salida a internet, en el panel de parcheo del cubiculo puerto 48.



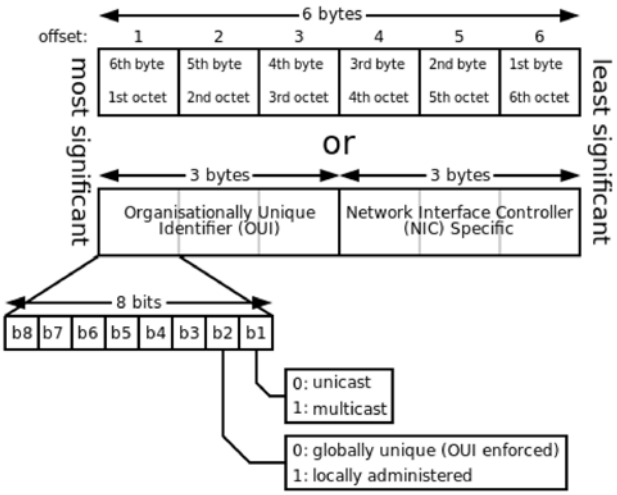


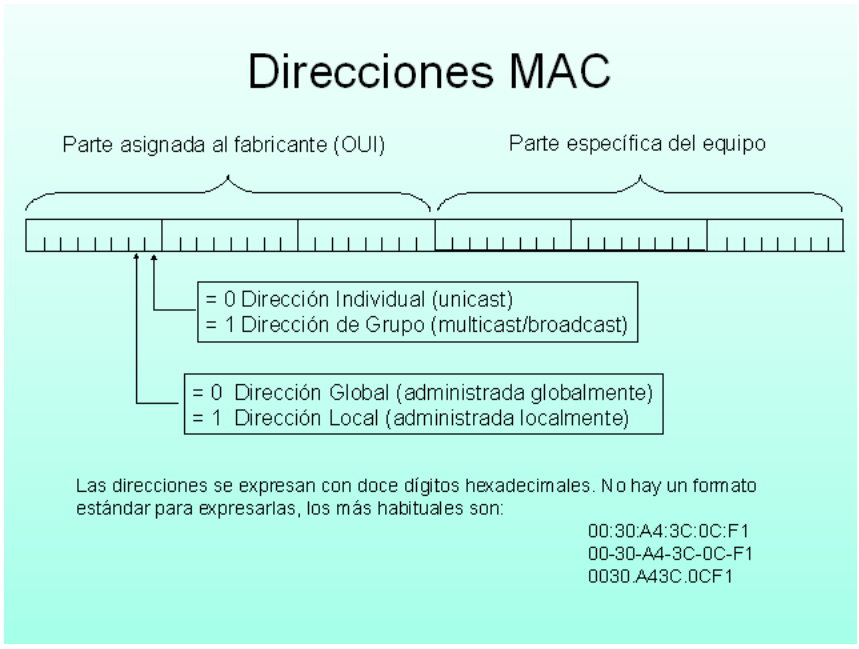
Notas:

- Deberá identificar en un diagrama de topología, las conexiones desde el equipo final, hasta el puerto 48 del Panel de Parcheo y adicionalmente escribir los puertos de cada equipo a los que se interconectan los cables (Vgr; CCNA01 --> PP30 --> HCNet8 --> HCNet1 --> SI23 --> SI12 --> PP48).
- Deberá des-energizar los equipos o desconectar sus cables para realizar la identificación del cableado.

- **Práctica 4.2 (5)**

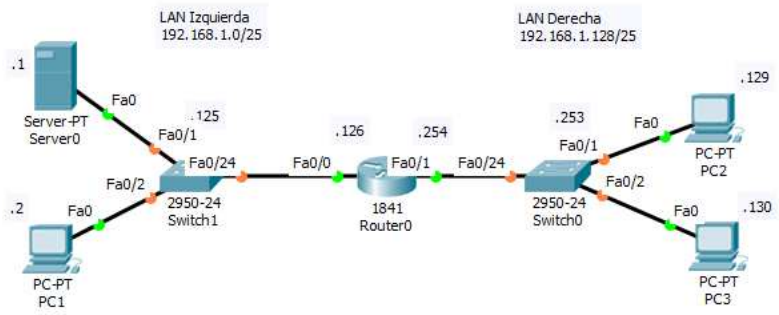
- **1. Conversión entre unidades (bps, Kbps, Mbps, bytes por segundo, etc)**
  - Definiciones de velocidades de transmisión.
    - Bandwidth: capacidad teórica del medio físico para transmitir señales.
    - Throughput: capacidad real de una red para transmitir datos de control y de usuario.
    - Goodput: capacidad real para transmitir datos de usuario.
  - Cálculo manual y comprobar.
  - Calculo de tiempos de descarga, en base a tamaños de archivo y ancho de banda.
  - **Actividad 1:** Calcular en base al tamaño de un archivo, el tiempo que debería tardar en transferirse a una velocidad determinada, Realizar la descarga limitada con wget del archivo en cuestión y justificar las diferencias entre el valor teórico calculado y la duración real de la descarga.
- **2. Análisis de OUIs, tipos de MACs y protocolo ARP**
  - **Direcciones MAC**
    - Dirección de control de acceso al medio (Media Access Control Address).
    - Identificador único asignado a las interfaces de red.
    - Utilizadas como direcciones de red para la mayoría de las tecnologías de red IEEE 802 como Ethernet o WiFi.
    - Se encuentran en la Capa 2 del modelo OSI.



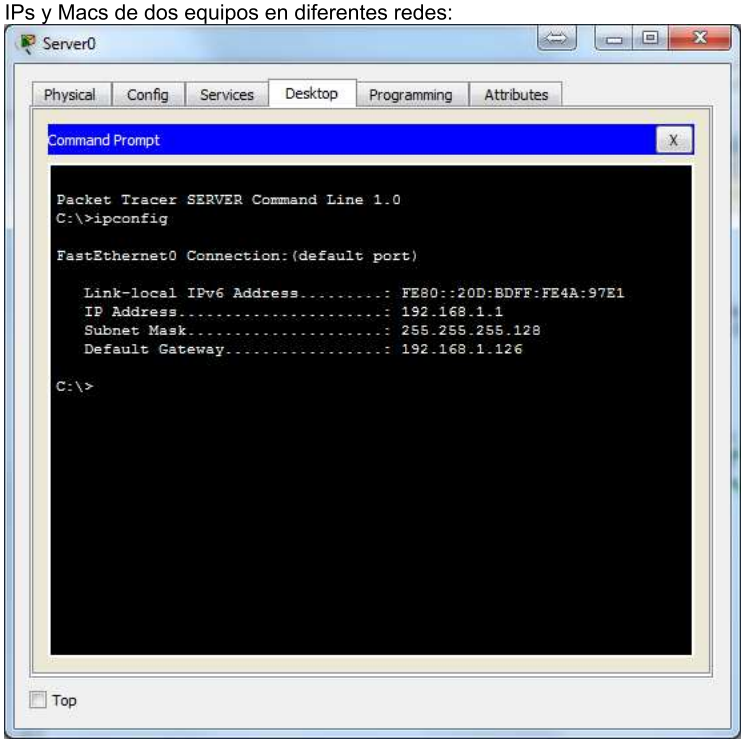


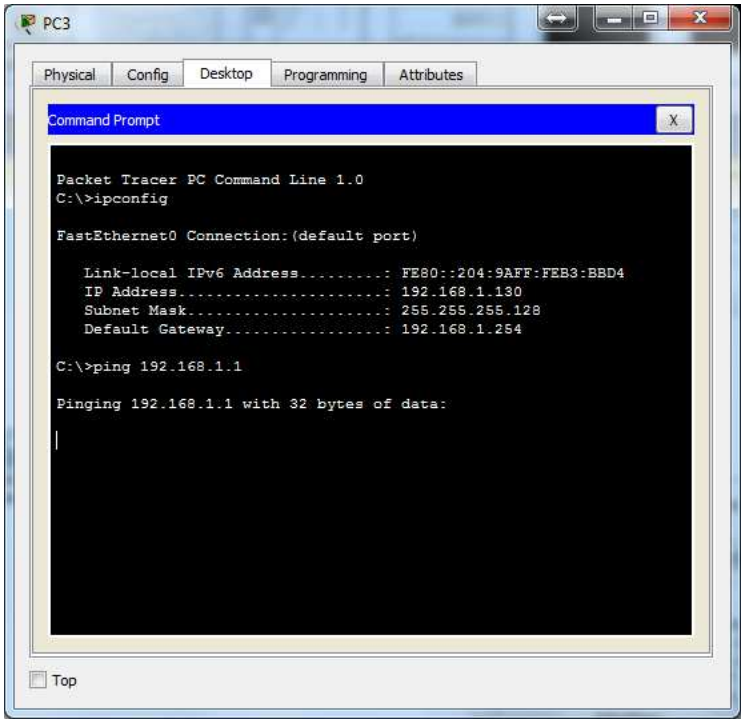
  - Modos de Transmisión Ethernet.
    - Unicast: 0 en el menos significativo del byte mas significativo.
    - Multicast: 1 en el menos significativo del byte mas significativo.
    - Broadcast: 1 en todos los bits.
  - ...er administradas universalmente o localmente.
    - Universalmente: es única por dispositivo por fabricante.

        - Primeros 3 octetos (más significativos) identifican la organización y se conocen como OUI (Organizationally Unique Identifier, Identificador Único Organizacional).
        - Los siguientes tres octetos (asignados por la organización)identifican de manera única al dipositivo.
    - Localmente: Invalida la dirección universal.
        - Direcciones asignadas a un dispositivo por el administrador de red.
        - Las direcciones administradas localmente no contienen OUIs.
- **ARP (Address Resolution Protocol).**
    - Protocolo para crear pares IP-MAC, es decir, relacionar una dirección IP con una dirección MAC.
        - Un nodo de red no conoce la dirección MAC a la cuál debe de enviar un marco.
        - Hace una petición ARP mediante transmisión broadcast preguntando ¿Quién tiene ésta IP?
        - El dispositivo con dicha IP, deberá responder indicando su dirección MAC al nodo origen.
        - Cuando el nodo origen recibe la respuesta, puede terminar de formar el marco Ethernet.
- **Análisis de tramas de capa de enlace.**
    - Trafico ICMP / IP entre equipos de diferentes redes.
        - Topología:

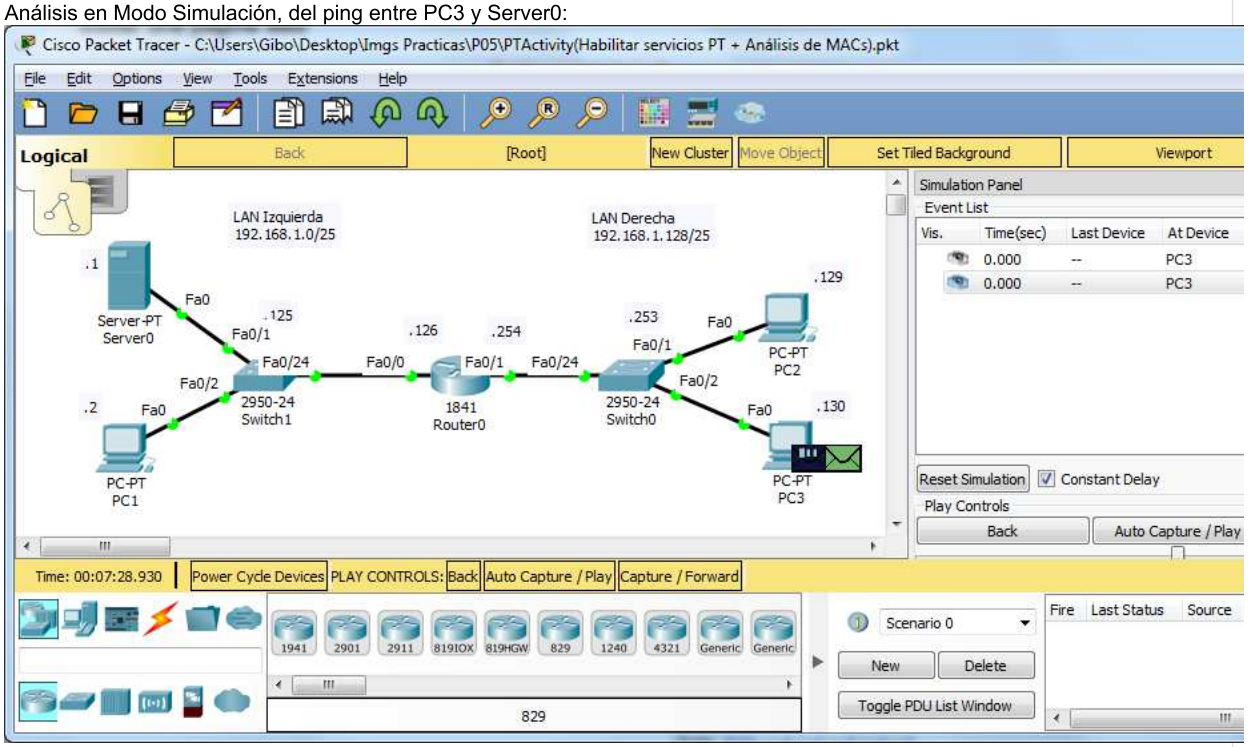


        - IPs y Macs de dos equipos en diferentes redes:

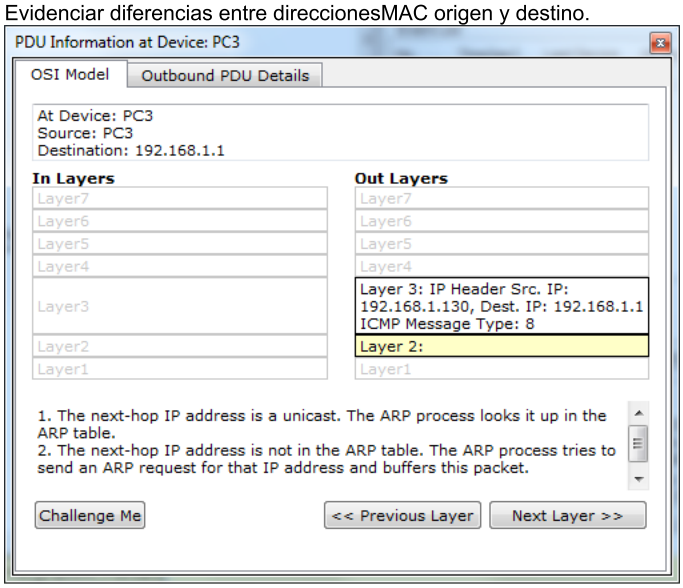


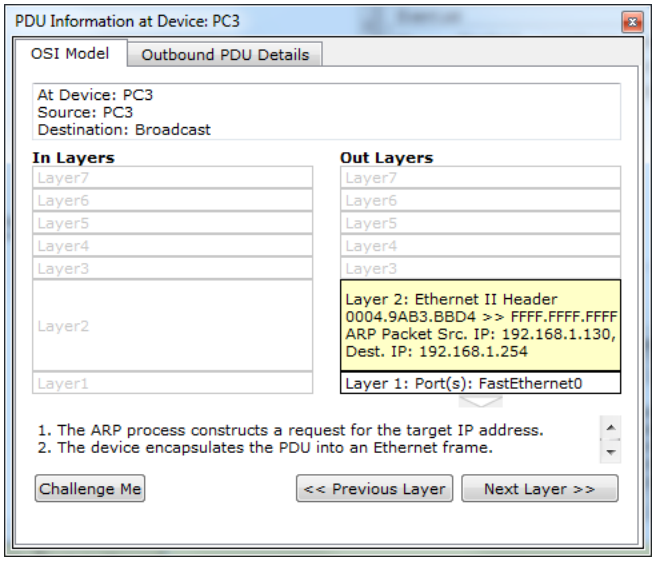


- Análisis en Modo Simulación, del ping entre PC3 y Server0:

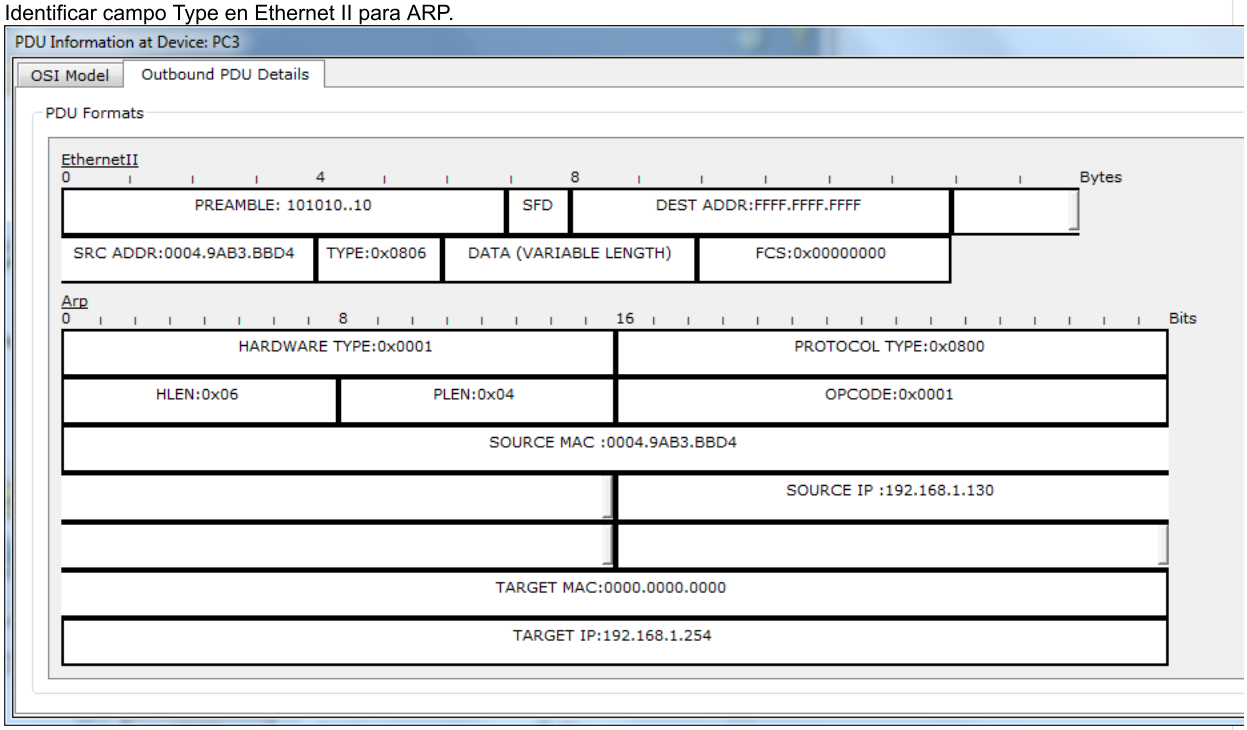


- Evidenciar diferencias entre direccionesMAC origen y destino.

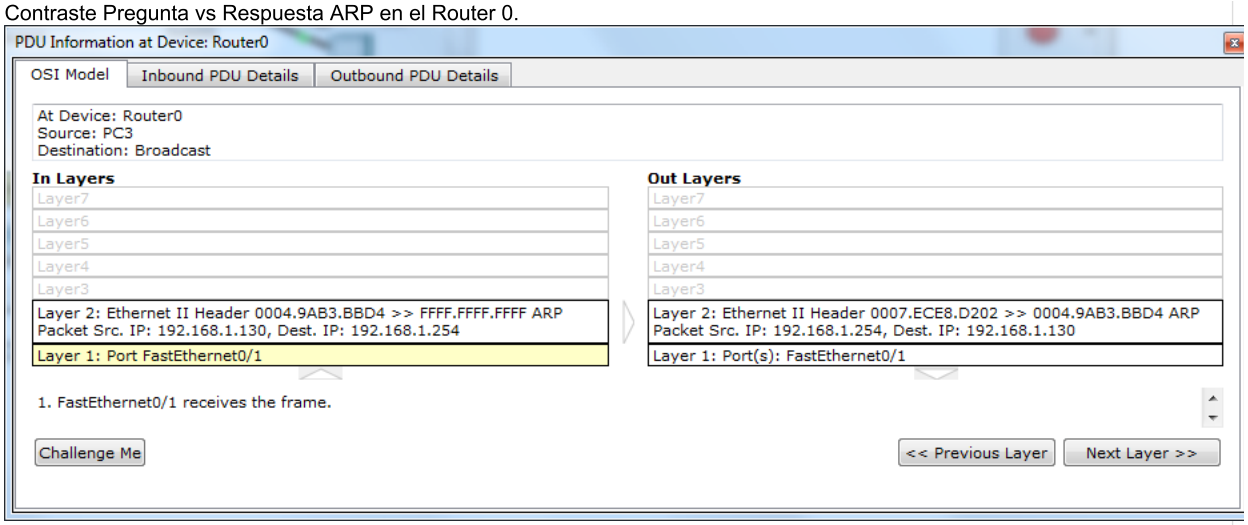




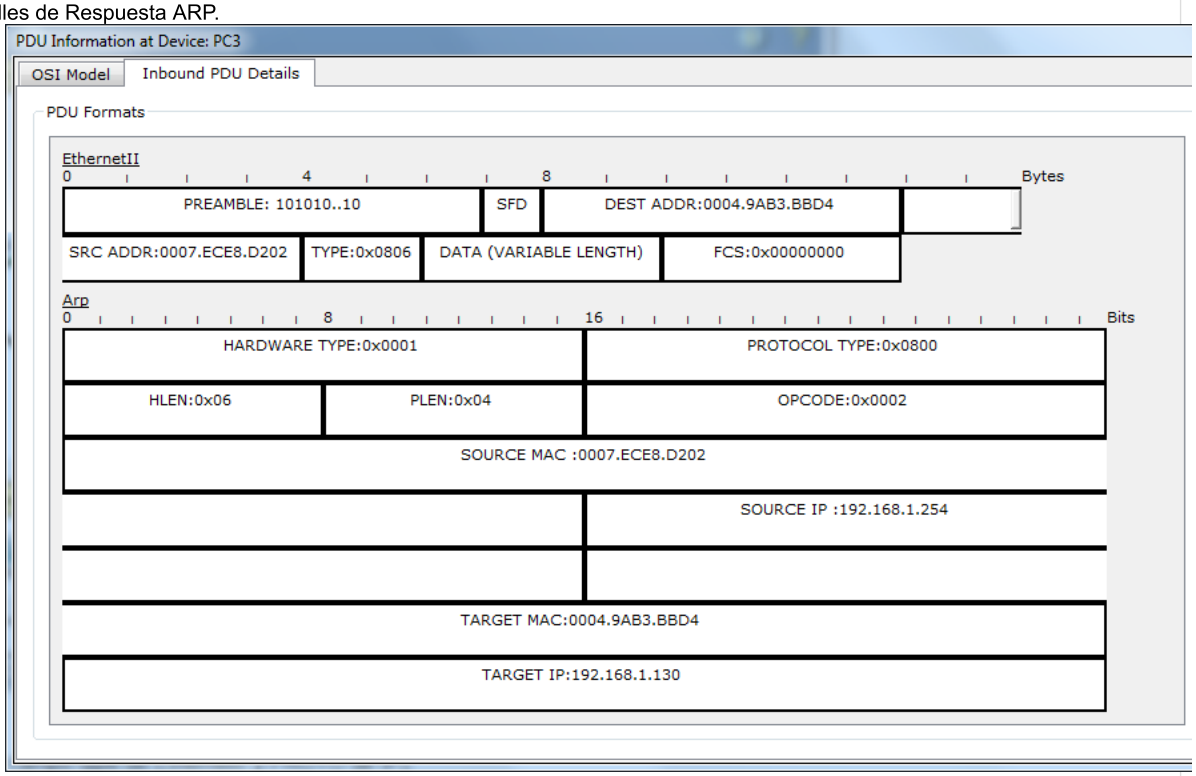
- Identificar campo Type en Ethernet II para ARP.



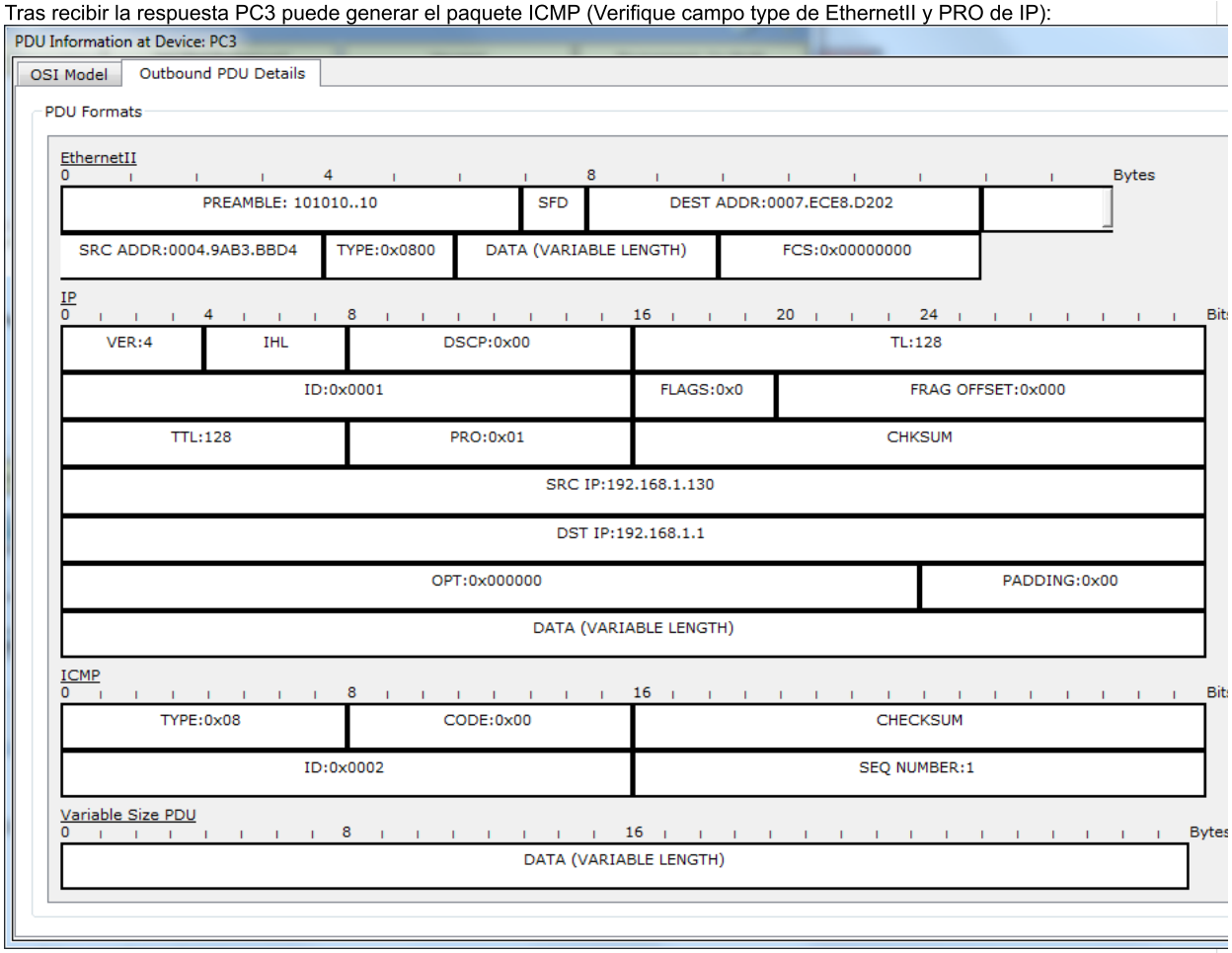
- Contraste Pregunta vs Respuesta ARP en el Router 0.



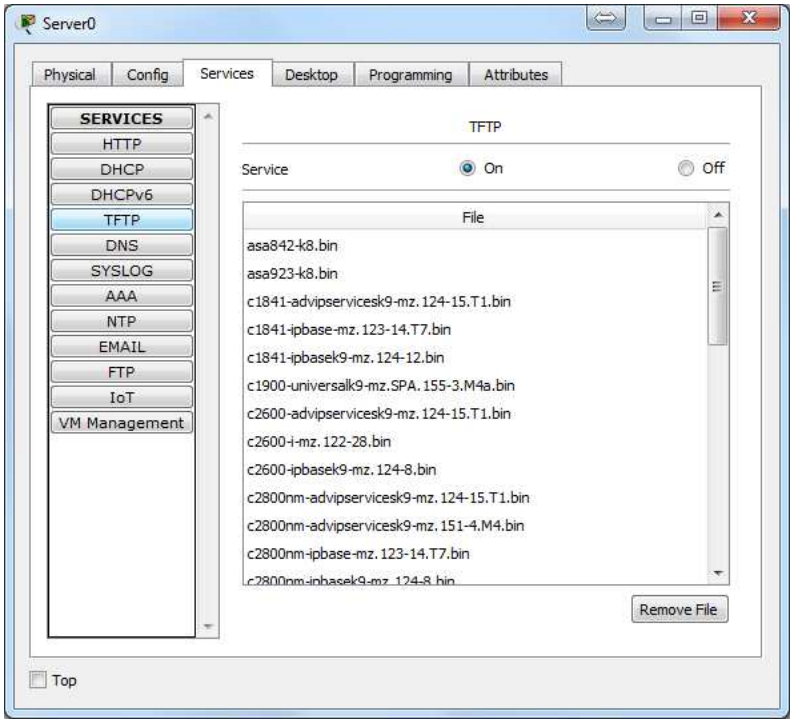
- Detalles de Respuesta ARP.

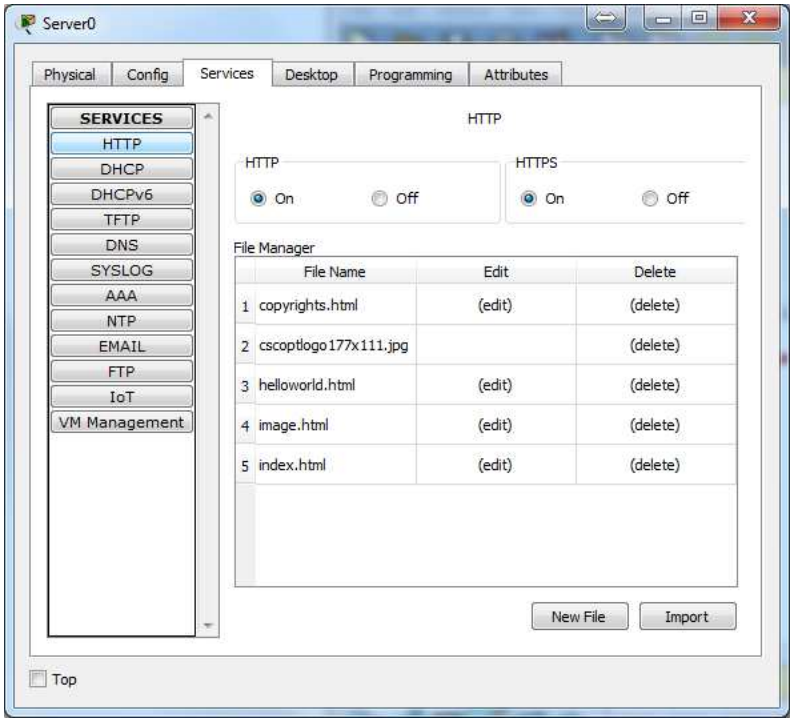


- Tras recibir la respuesta PC3 puede generar el paquete ICMP (Verifique campo type de EthernetII y PRO de IP):



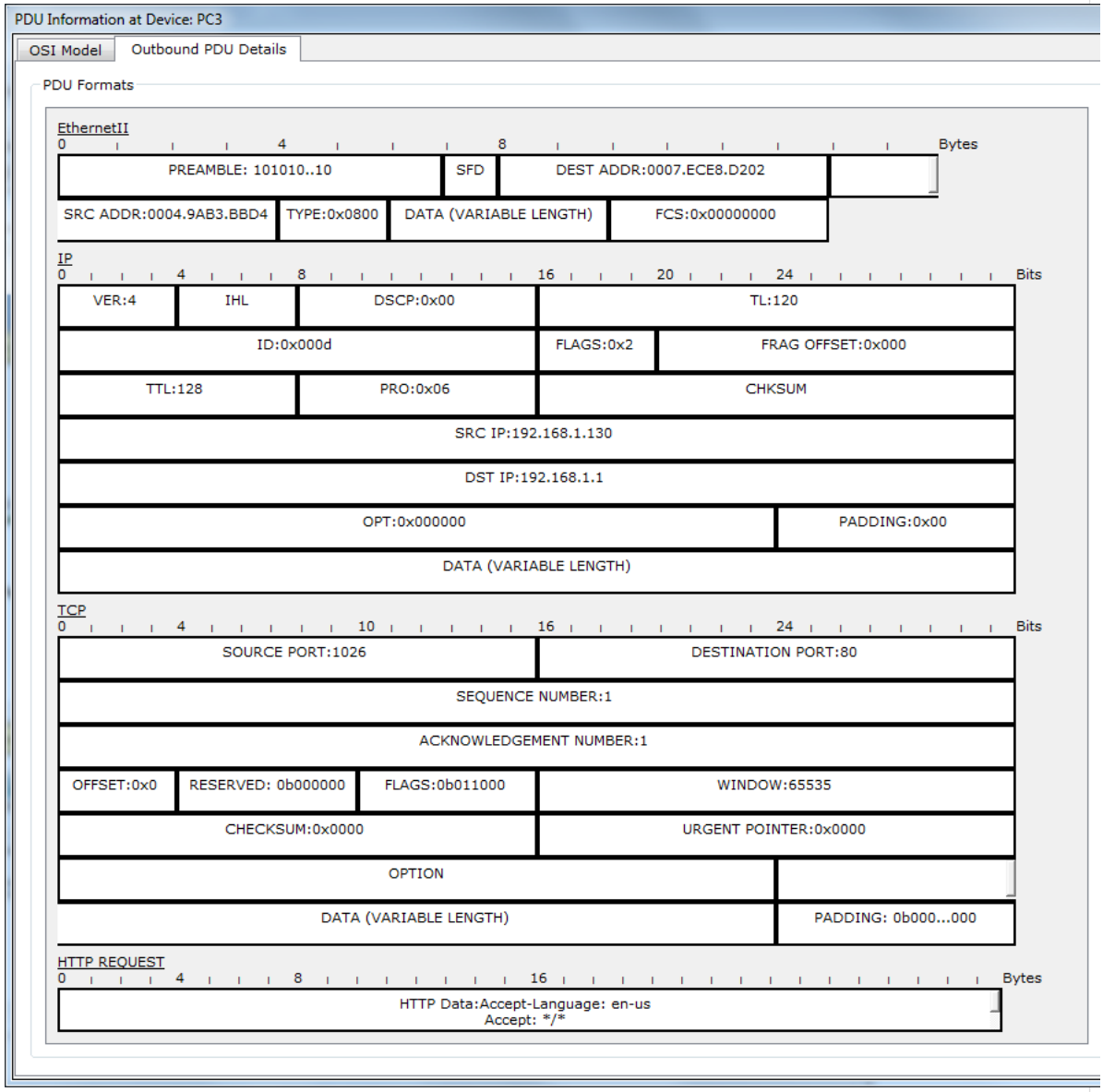
- Activación de Servicios (HTTP/TFTP) en P.T.



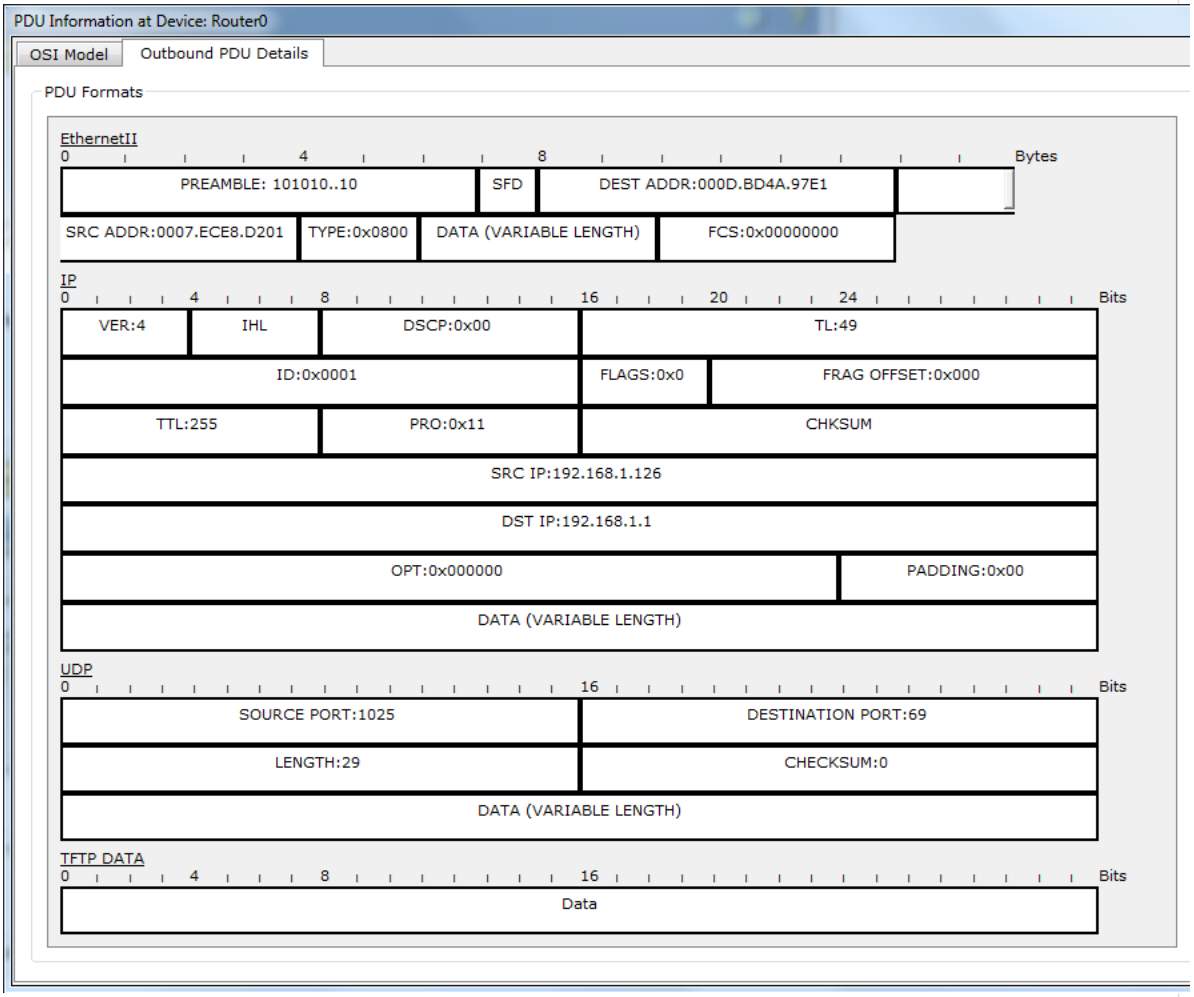


- Identificar valores del campo protocolo (cabecera de trama) para transferecias de datos por HTTP y TFTP.

- Transmisión HTTP:

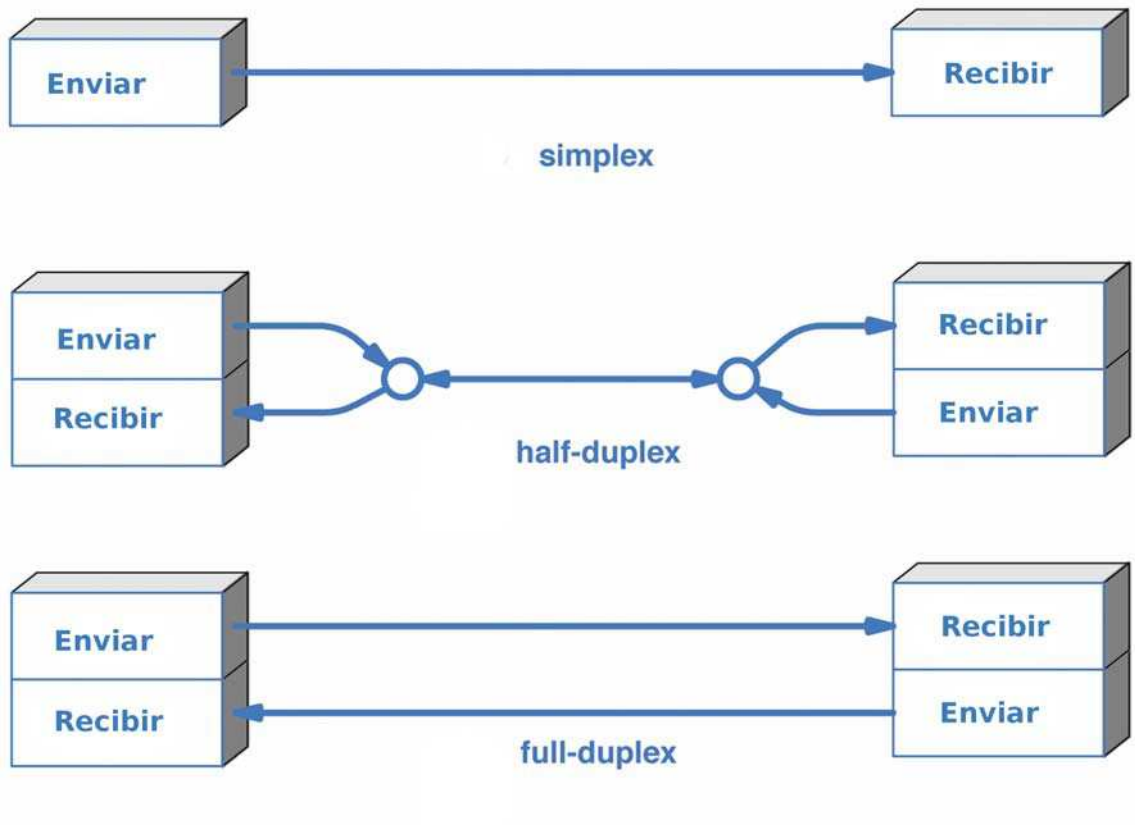


- Transmisión TFTP:



  - **Actividad 2:** Replicar Actividad de PacketTracer en Equipos Físicos capturando tráfico con Wireshark

- **3. Configuración de tipo de transmisión duplex en switches (half/full/auto).**
  - Modos de transmisión:
    - **Simplex: Transmisión en un solo sentido.**
    - **Duplex: Transmisión en ambos sentidos.**
      - **Half-Duplex: Transmisión en solo un sentido a la vez.**
      - **Full-Duplex: Transmisión en ambos sentidos a la vez.**



- Variar modo duplex en switches.
  - S> enable
  - S# configure terminal
  - S(config)# interface FastEthernet 0/n
  - S(config-if)# duplex [half | full | auto]

- Variar modo duplex en PCs (ethtool).
  - Por defecto las tarjetas de red se encuentran en modo duplex-auto.
  - Cambiar el modo requiere el paquete ethtool.
    - Establecer modo HalfDuplex:

      ```
      # ethtool -s eth1 speed 100 duplex half autoneg off
      ```

    - Establecer modo FullDuplex:

      ```
      # ethtool -s eth1 speed 100 duplex full autoneg off
      ```

- **Actividad 3:** Transferencia de un archivo con scp entre dos maquinas ubuntu conectadas mediante un switch y evidenciar las diferencias para las posibles combinaciones:

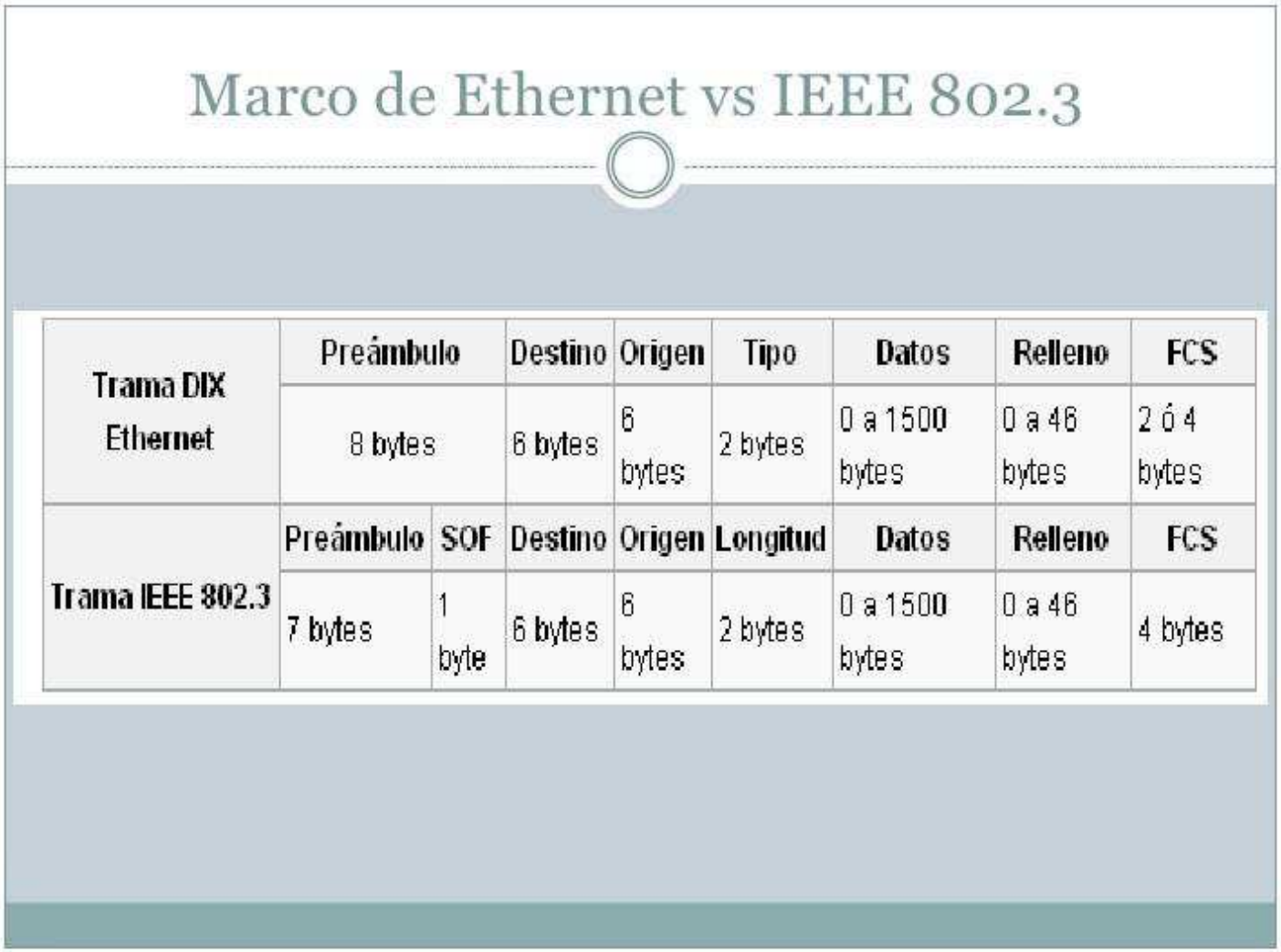
PC	**Switch**
auto	auto
	half
	full
half	auto
	half
	full
full	auto
	half
	full

Protocolo 1: de Ventana Deslizante: Parada y Espera

Descripción
Tarea 4.2: Implementar Parada y Espera en la transferencia de archivos binario entre una comunicación cliente y servidor.

Redes de Computadoras I

Formatos de Trama Ethernet



Trama DIX Ethernet	Preámbulo		Destino	Origen	Tipo	Datos	Relleno	FCS
	8 bytes		6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	2 ó 4 bytes
Trama IEEE 802.3	Preámbulo	SOF	Destino	Origen	Longitud	Datos	Relleno	FCS
	7 bytes	1 byte	6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	4 bytes

Principales Diferencias:

- **3er campo:**
  - **Eth2: EtherType** (Valores >= 0x600)
    - Ejemplos: (ARP 0x0806, IP 0x800)
  - **802.3: Longitud** (Valores < 0x600=1536)
    - Ejemplo: (Maximum Transfer Unit - MTU for Ethernet: 0x5DC=1500)
    - Tamaño mínimo válido: **64 bytes**.
    - Tamaño máximo válido: **1518 bytes**.
    - Tamaño fuera del rango se considera error ó colisión.

- **Marcos Ethernet** llevan preambulo de 64bits para dar tiempo al receptor de que se aliste.
  - 10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010

- **Marcos IEEE** llevan preambulo de 63bits y un indicador de inicio de trama, para dar tiempo al receptor de que se aliste y si no escucho completo el alistamiento sepa cuando termina y comienzan los datos.
    - 10101010 10101010 10101010 10101010 10101010 10101010 10101010 *10101011*

El Campo Secuencia de verificación de trama (FCS).

- Campo de 4 bytes = 32bits
- Utiliza una comprobación de redundancia cíclica (CRC).
    - Código de detección de errores basado en el residuo de una división de polinomios.
    - Ver Ejemplo.
- Se utiliza para detectar errores en una trama.
    - El emisor incluye CRC en el campo FCS de la trama.
    - El receptor recibe la trama y genera una CRC a partir de los datos.
    - Si los cálculos coinciden,
        - No contiene errores (dátos integros).
    - Si no coinciden
        - Los datos se corrompieron, --> se descarta la trama.

- **Actividad de Programación**:
    - Realizar un programa en C ó Java que reciba 2 parámetros desde línea de comandos:
        - El nombre de un archivo.
        - Un polinomio para CRC.
    - Calcule el CRC del archivo indicado, acorde al polinomio indicado.

Tipos de Switches Ethernet

- **Store & Forward:**
    - Espera a recibir trama completa.
    - Calcula CRC
    - Si es válido
        - Lee la dirección destino
        - Determina el puerto de salida
        - Reenvía la trama
    - Si no es válido
        - Desecha la trama
- **Cut-Through:**
    - Espera a recibir al menos algunos bits de la cabecera.
    - Lee la dirección MAC destino
    - Determina el puerto de salida
    - Reenvía los bits sin verificar la trama
    - Dos Tipos:

        - **Fast-Forward:**
            - Buffer pequeño (6 bytes); solo lee MAC destino y reenvía.
        - **Fragment Free:**
            - Buffer 64bytes; verifica errores en la cabecera; y reenvía.

Diferencia entre Switch y Hub

- **Hub:** replica tráfico a todos puertos excepto x el que se recibió (Inundar).
- **Switch:** solo envía tramas al destinatario una vez que sabe donde está.
    - Switch se basa en tabla MAC aka. CAM (Content Adressable Memory Table / Bridging Table - MAC Address Table)
    - Si CAM no contiene entrada para el destino
        - Inunda.
    - Solo inunda en dos casos:
        - Broadcast
        - Unicast desconocido
    - *Verificar en P.T.*
    - Consecuencias inundación: Hosts que no deberían ver marcos, los ven

Problema de seguridad en un switch: Cuando un switch actua como hub

- Debilidades: MAC address table finita.
    - Los switches gama alta pueden almacenar cientos de miles de entradas:
        - Cisco Catalyst Express 500 - 8000 entradas
        - Cisco Catalyst 2048g - 16000 entradas
        - ...
        - Cisco Catalyst 6500/7600 - 131072
    - Posible forzar la inundación:
        - Llenar la tabla MAC (MAC Flooding).
            - Dos posibilidades:
                - Bufer circular
                - Envejecimiento
            - Independientemente, mantener siempre CAM llena provoca que tarde o temprano el switch actue como hub
            - Nota: un switch almacena en su tabla MAC únicamente direcciones unicast.

Ataque: MAC Spoofing

- Un atacante, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
- Posterior a la inundación.
- Una vez que el atacante ha conseguido una dirección MAC legítima puede inyectar tráfico malicioso. Lo cual ocasiona que el switch envíe el tráfico al puerto incorrecto.
- ¿Es lo mismo que el MAC Flooding? No, pero se sirve de él.
    - Atacante genera tráfico con diferentes direcciones MAC unicast origen, para inundar tabla MAC del switch y forzarlo a inundar.
- Puede generar DoS, la misma MAC no puede aparecer dos veces en la tabla CAM del switch (contrario a las tablas ARP de los hosts como se verá más adelante).

Posibles Soluciones:

- Seguridad de Puerto
    - Se configura un número límite sobre la cantidad de marcos que se aprenden de forma dinámica a través de un puerto.

    - S(conf-if)# switchport portsecurity
    - S(conf-if)# switchport portsecurity mac-address {sticky | H.H.H}
    - S(conf-if)# switchport portsecurity maximum {1-132}

    - S# show port-security

- Notificación de actividad de direcciones MAC

    - Muchos switches pueden ser configurados para advertir al administrador sobre movimientos frecuentes.

    - mac-address-table notification mac-move

- Protección de inundación unicast.

    - Establecer un límite definido por el usuario sobre la cantidad de inundación aceptada.

    - mac-address-table unicast-flood limit

ARP - Address Resolution Protocol

- Corre encima de Ethernet (Packet Type: 0x0806)
- Encuentra MAC de siguiente salto (Host/Gateway)

    - Request: Broadcast: Quién tiene la IP xx.xx.xx.xx??
    - Reply: Unicast: IP xx.xx.xx.xx = MAC yy:yy:yy:yy:yy:yy
    - Almacena equivalencia en Tabla ARP del cliente ARP.
    - Gratuite ARP:
        - Respuestas ARP no solicitadas.
        - Respuestas automáticas cada determinado tiempo.

- Riezgos:
    - No Autenticación: las respuestas ARP no van "firmadas" de ninguna manera.
    - Fugas de Información: todos los host de la red aprenden el par IP-MAC de un ARP gratuito.
    - Problemas de Disponibilidad: como todos los dispositivos deben de recibir las peticiones ARP y procesarlas, un atacante puede generar miles de peticiones por segundo gastando ancho de banda y tiempo de procesamiento.

Ataque: ARP Spoofing

- Objetivo: Capturar todos los paquetes IP incluso en una red switcheada.
- También conocido como envenenamiento ARP (ARP poisoning).
- Se logra enviando respuestas ARP falsas y no solicitadas.
    - Provoca tablas ARP con información falsa.
        - Reenviar paquetes capturados a destinatarios válidos.
        - Destinatario válido responde a solicitante original sin darse cuenta.
    - Solo efectivo en la misma red.

- ¿Qué pasa si el host suplantado es la puerta de enlace?

Posibles Soluciones:

- Utilizar un switch capa 3: los switches capa 3 analizan el tráfico y conocen el mapeo IP-MAC correcto. Con dicho conocimiento, pueden analizar el tráfico ARP y determinar si la información dentro de una respuesta ARP es válida. A esta técnica se le conoce como Inspección Dinámica ARP (DAI).

- Protección de Hosts: los hosts pueden ser protegidos ignorando el ARP gratuito o mediante el uso de entradas ARP estáticas.

- Sistemas de detección de intrusos (IDS): herramientas como ARPwatch.

Actividad Práctica:

1. Realizar una Ataque **"MAC Flood"** para desbordar la tabla MAC de un switch Catalyst y forzarlo a Inundar.
2. Realizar un **"ARP Spoof"**
3. Identificar las **diferencias** y reportar al profesor.

- **Nota:** Puede guiarse con el siguiente tutorial, o utilizar cualquier fuente de Internet.

Tarea: Instalar FTP en servidor propio. Crear manual de instalación/configuración.

- **Enrutamiento**:
  - Proceso en el que los hosts (finales o intermedios) aprenden sobre redes *lógicas* remotas, encuentran las rutas posibles para llegar a ellas y escogen las mejores rutas para intercambiar datos entre las mismas.
  - Se basa en una tabla de enrutamiento:
    - Tres columnas mínimo:
      - Dirección de **Red Destino**
      - **Mascara de Subred** de la red destino
      - Interface de **salida o** ip de **siguiente destino**
  - El dispositivo a enrutar:
    - Lee la IP destino del paquete que llega a cualquiera de sus interfaces.
    - Por cada entrada de su tabla de enrutamiento calcula:
      - Posible Red Destino = IP destino del paquete entrante & Mascara de red destino en la tabla de enrutamiento.
      - Si Posible Red Destino == Red Destino en la entrada de la tabla.
        - Re-envía a interface de salida o ip de siguiente salto.
        - Deja de buscar en la tabla.

- **Enrutamiento en un host final**
  - `route print`
  - `netstat -r`

  - Presenta tres secciones relacionadas con las redes IP conocidas:
    - **Lista de interfaces:** enumera las direcciones de control de acceso al medio (MAC) y el número de interfaz asignado de cada interfaz con capacidad de red en el host, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.
    - **Tabla de rutas IPv4:** enumera todas las rutas IPv4 conocidas, incluidas las conexiones directas, las rutas de red locales y las rutas predeterminadas locales.
    - **Tabla de rutas IPv6:** enumera todas las rutas IPv6 conocidas, incluidas las conexiones directas, las rutas de red locales y las rutas predeterminadas locales.

```
C:\Users\PC1> netstat -r

<Resultado omitido>

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
     192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
    192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
===========================================================================
<Resultado omitido>
```

- La ilustración muestra solo tabla de rutas IPv4 :
  - Cinco columnas:
    - *Destino de red*:redes que se pueden alcanzar.
    - *Máscara de red*: indica al host cómo determinar la porción de red.
    - *Puerta de acceso*: Dirección para llegar a una red remota.
    - *Interfaz*: MAC de la interfaz física utilizada para enviar el paquete.
    - *Métrica:* costo de cada ruta.
  - Cinco secciones de redes Destino:
    - 0.0.0.0
      - La ruta predeterminada local.
      - Todos los paquetes con destinos que no coincidan con otras rutas de la tabla de enrutamiento se reenvían al gateway.
      - Todos los destinos que no coincidan se envían al gateway.
    - 127.0.0.0 – 127.255.255.255
      - Direcciones loopback ó conexión directa al host local.
    - 192.168.10.0 - 192.168.10.255
      - Direcciones de la red local.
      - Todos los paquetes con destino a la red local salen por la interfaz 192.168.10.10 (IP local).
    - 224.0.0.0
      - Direcciones multicast de clase D.
      - Se envía por todas las interfaces disponibles.
    - 255.255.255.255
      - Broadcast limitado.
      - Se envía por todas las interfaces disponibles.

- **Enrutamiento entre Redes (en un Host Intermedio ó Router)**
  - Permite a un router transferir información de una red a otra buscando que el paquete encuentre su destino.
  - El router representa la unión de múltiples redes IP.
  - Un router re-envia paquetes basado en la dirección IP de destino y las rutas que se encuentren en su tabla de enrutamiento.

  - Descripción de tipos de rutas en un router:

1. *Rutas directamente conectadas.* Aprendidas a partir de la configuración ip de interfaces.
2. *Rutas configuradas estáticamente.* configuradas manualmente por el administrador para indicar un camino hacia un destino conocido.
    - Deben actualizarse manualmente.
    - Necesitan pocos recursos.
    - Recomendable para redes pequeñas.
3. *Rutas por defecto.* Configuradas manualmente por el administrador para indicar un camino hacia cualquier destino desconocido.

- Configuración una ruta estática.
    - `R(conf)# ip route dirección-red mascara-subred { siguiente-salto | interfaz-salida }`

    - Dónde:
        - *dirección-red*: es la dirección de la red a la que se desea llegar.
        - *mascara-subred*: es la mascara de la red a la que se desea llegar.
        - *siguiente-salto:* Es la dirección IP dentro del rango de alguna de las redes directamente conectadas (No la IP del router que se está configurando), del siguiente salto (router), en el camino hacia la red destino.
        - *interfaz-salida*: Es un interfaz del router local, a la cual está conectado el siguiente salto (router), en el camino hacia la red destino.
    - Nota: En base al tercer parámetro se denominan 3 tipos comunes (no siempre es así), de rutas:
    - De siguiente salto: La red destino se encuentra a mas de un router de distancia (usa ip de siguiente salto).
    - Conectada: La red destino se encuentra a menos de un router de distancia (usa interface de salida).
    - Completamente especificada: La red destino se encuentra a mas de un router de distancia y debe atravesar por una red de Acceso Multiples (usa ip de siguiente salto e interface de salida).

- Configuración de una ruta por defecto.
    - `R(conf)# ip route 0.0.0.0 0.0.0.0 { siguiente-salto | interfaz-salida }`

    - Dónde:
        - *0.0.0.0*: referencia a cualquier dirección de red desconocida.
        - *0.0.0.0*: mascara de la red de cualquier red desconocida.
        - *siguiente-salto*: Dirección IP del siguiente salto ó router conectado a una red local (No la IP del router que se está configurando), en el camino hacia la red destino.
        - *interfaz-salida*: Es un interfaz del router local, a la cual está conectado el siguiente salto (router), en el camino hacia la red destino.

- Cada ruta agregada al router se almacena en la “Tabla de enrutamiento”, la cual puede visualizarse con el comando:
    - `R# show ip route`
        - La tabla de enrutamiento muestra primeramente un caracter que indica el origen de la ruta:

            - `C connected`
            - `S static`

- `* candidate default`

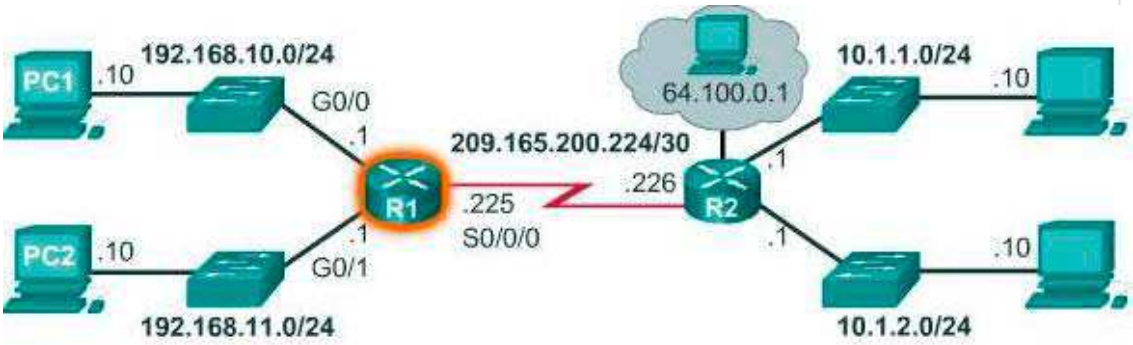
- Por ejemplo:
  - `S 209.165.200.224 is directly connected, Serial0/0/1`
  - `C 209.165.200.228 is directly connected, FastEthernet0/0`
  - `S* 0.0.0.0/0 is directly connected, Serial0/0/0`

- Enseguida aparecen la red y mascara del destino, así como la interfaz de salida o dirección de siguiente salto.

- Cuando se usan protocolos de enrutamiento dinámico aparece un parámetro adicional entre corchetes, denominado [Distancia Administrativa / Costo], por ejemplo:
  - `R 10.1.8.0 [120/1] via 10.1.244.2, 00:00:03, Serial0/0/0`
  - `R 10.1.12.0 [120/1] via 10.1.244.2, 00:00:03, Serial0/0/0`
  - `R 10.1.16.0 [120/1] via 10.1.248.2, 00:00:02, Serial0/0/1`

  - La Distancia Administrativa es un número entre 0 y 255, que indica la confiabilidad y prioridad del origen de una ruta.
    - Cada protocolo de enrutamiento dinámico tiene un nivel de confiabilidad diferente
  - El costo indica la dificultad de alcanzar una red destino (y es diferente en cada protocolo de enrutamiento dinámico).

- Rutas usando IP de siguiente salto vs Interfaz de Salida
  - Siguiente Salto
    - Dirección del dispositivo que procesará el paquete a continuación.
    - Para un host en una red, la dirección del gateway predeterminado (interfaz del router) es el siguiente salto para todos los paquetes que se deben enviar a otra red.
    - En la tabla de enrutamiento de un router, cada ruta a una red remota incluye un siguiente salto.
    - Cuando un paquete destinado a una red remota llega al router, este busca una correspondencia entre la red de destino y una ruta en la tabla de enrutamiento. Si se encuentra una coincidencia, el router reenvía el paquete a la dirección IP del router de siguiente salto mediante la interfaz que se identificó con la entrada de la ruta.
    - Un router de siguiente salto es el gateway a las redes remotas.
    - Por ejemplo, en la ilustración, un paquete que llega al R1 destinado a la red 10.1.1.0 o la red 10.1.2.0 se reenvía a la dirección de siguiente salto 209.165.200.226 mediante la interfaz serial 0/0/0.



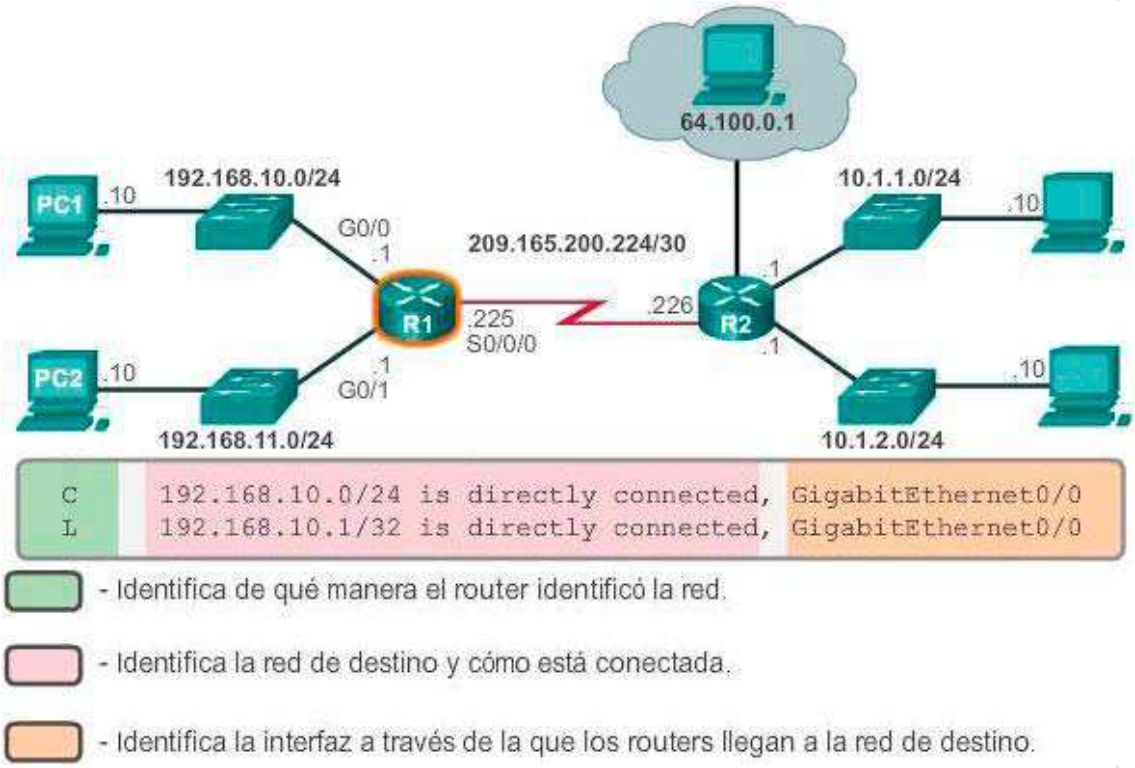

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
```

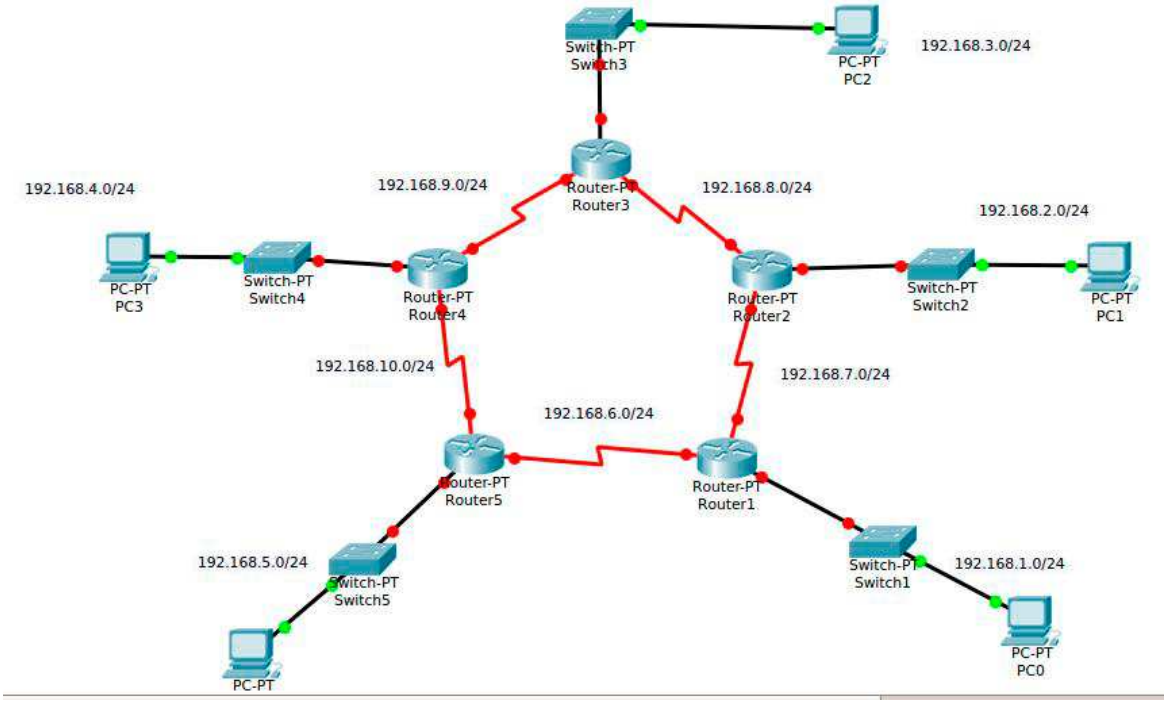
- Las redes conectadas directamente a un router no tienen dirección de siguiente salto, porque los routers pueden reenviar los paquetes en forma directa a los hosts en esas redes mediante la interfaz designada.

- Interfaz de salida
  - La interfaz de salida se rotula como “C” en la ilustración.
  - Identifica la interfaz de salida que se debe utilizar al reenviar paquetes a la red de destino.

  - En general, los routers tienen varias interfaces configuradas.
  - La tabla de enrutamiento almacena información sobre las rutas conectadas directamente y las remotas.
  - Tal como ocurre con las redes conectadas directamente, el origen de la ruta identifica cómo se descubrió la ruta.
  - Por ejemplo, los códigos comunes para las redes remotas incluyen lo siguiente:
    - S: indica que un administrador creó la ruta manualmente para llegar a una red específica. Esto se conoce como “ruta estática”.
    - D: indica que la ruta se obtuvo de forma dinámica de otro router mediante el protocolo de enrutamiento de gateway interior mejorado (EIGRP).
    - O: indica que la ruta se obtuvo de forma dinámica de otro router mediante el protocolo de enrutamiento Open Shortest Path First (OSPF).



- **Actividad Práctica:**



  - Para la topología mostrada:
    - Configurar cada router, para que todos los routers tengan una Tabla de Enrutamiento, que encamine los paquetes de cada una de sus subredes hacia las subredes de los otros routers.
      - Realizar enrutamiento de la topología con 5 routers en forma de pentágono, y una LAN por cada Router.
      - Agregar el direccionamiento estático para que toda la topología tenga conectividad.
      - Enumerar las redes, enrutar redes pares por la derecha y nones por la izquierda (considere que al encontrarse en cada router se encuentra viendo

hacia el centro del pentágono).
    - Registre los comandos para configurar a cada uno de los routers.

- Entregar por equipo, en equipo físico, replicar el enrutamiento de la topología de 5 routers en forma de pentagono, y una LAN por cada Router (Para interconectar los routers frontales con los posteriores utilice cables cruzados). Agregando el enrutamiento estático para que toda la topología tenga conectividad. Numerar las redes, enrutar redes pares por la derecha, y nones por laizquierda.

Historia del Direccionamiento IP

- IPv4 (RFC 760 - 1980)
  - Estandar de direccionamiento del Departamento de Defensa USA (ARPA Net).
  - Etiqueta numérica asignada a cada dispositivo que participa en una red conectada por el protocolo de Internet.
- IPv4 ClassFull (RFC 791 - 1981)
  - Ausencia de Mascaras de Subred.
  - Clases determinadas por los bits más significativos (a la izquierda) de la dirección IP:
    - **0** para las redes de Clase A (Equivalente a /8)
      - 0.0.0.0 a 127.255.255.255
    - **10** para las redes de Clase B (Equivalente a /16)
      - 128.0.0.0 a 191.255.255.255
    - **110** para las redes de Clase C (Equivalente a /24)
      - 192.0.0.0 a 223.255.255.255
    - **1110** para las redes de Clase D (usadas para transmisiones multicast)
      - 224.0.0.0 a 239.255.255.255
    - **11110** para las redes de Clase E (usadas para investigación y experimentación)
      - 240.0.0.0 a 255.255.255.255
  - Identifica 2 porciones de una IP.
    - Red (ClassFull) / Host
- IPv4 Mascaras de Subred y planeación de subredes (RFC917 - 1984)
  - Capacidad de los hosts para utilizar una mascara de subred, para diferenciar porciones de red en una dirección ip.
  - Introducción de las mascaras de subred.
- IPv4 Subnetting ClassFull (RFC950 - 1985)
  - Los routers de todo el mundo no estaban preparados para soportar Mascaras de Subred, los hosts si.
  - Permite seguir usando los mismos routers realizando divisiones de una red ClassFull en subredes mas pequeñas.
  - Identifica 3 porciones de una IP.
    - Red (ClassFull) / Subred / Host
  - Todas las redes usan la misma máscara.
  - No es posible utilizar las subredes que incluyen la dirección de red ó la dirección de broadcast de la red ClassFull (ocasionan conflictos de enrutamiento).
- IPv4 CIDR / VLSM (RFC 1518 y RFC 1519 - 1993)
  - División de rangos de direcciones IP independiente de la clase a la que hubiese pertenecido en el pasado.
  - Identifica 2 porciones de una IP.
    - Subred / Host
  - Cada subred puede tener un tamaño diferente acorde a la cantidad de ips necesarias.
- IPv4 Subnetting ClassLess (RFC 1878 - 1995)
  - Los routers del mundo ya soportan CIDR, los hosts también; los ingenieros no pueden seguir el paso de la tecnología (la gente se reusa al cambio).
  - Se sigue realizando subnetting se ve al VLSM como algo complicado.
  - Con la sola diferencia que:
    - Desaparece el conflicto de enrutamiento que involucraba a las las subredes que incluyen la dirección de red ó la dirección de broadcast de la red ClassFull
- IPv4 NAT / PAT
  - Persistencia de las personas en seguir utilizando Direccionamiento Classfull y Subnettig provocaron un agotamiento apresurado del espacio de direccionamiento IPv4.
  - VLSM optimiza el uso de IPs, pero ya es demasiado tarde.
    - Empresas grandes todavía tienen asignadas redes ClassFull:
      - General Electrick - /8 = 16777216 IPs
      - Apple - /8 = 16777216 IPs
      - UMSNH - /16 = 65536
  - Admite interconectividad de redes de cualquier tamaño en los rangos de las IPs Privadas (RFC 1918)
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255
  - Requiere al menos una dirección IP pública.
  - Tres tipos:
  - NAT Estático.
    - Traduce una a una IP pública x Privada.
  - NAT Dinámica
    - Traduce alguna IP Privada x una IP Pública.
  - PAT
    - Traduce IPs Privadas y Puerto de Cliente x una o mas IPs Públicas.
- IPv6 + Subnetting
  - Espacio de direccionamiento de 128bits
  - Suficiente para direccionar 7 IPs a cada átomo del cuerpo humano de todos los habitantes de la tierra.
  - Un ISP suele asignar una /32 a /64 por cliente (El doble del espacio IPv4).
  - El cliente puede subdividir mediante Subnetting:
    - Al límite del Nibble
    - Dentro del Nibble

Subnetting ClassFull

- Permite subdividir una red ClassFull en N subredes.
- Define 3 partes de una IP:
    - `<network-number><subnet-number><host-number>`
- Ejemplificar Generalidades:
    - Puede usarse cualquier tamaño para la porción de subred según se requiera, sin invadir nunca la porción de red.
    - Una vez elegido el tamaño de la porción de subred, todas las subredes usan ese tamaño.
    - El tamaño de la porción de subred, determina como codificar los valores de subred.
    - Los valores de subred siempre se codificarán con la longitud elegida.
    - Los bits de la porción de subred se agregan a la mascara de red en 1 para indicar la mascara de subred.
- Dos enfoques:
    - Por necesidad de subredes.
    - Por necesidad de hosts de la subred mas grande.

    - Ejemplificar Subnetting Classfull por necesidad de subredes:
        - Se requiere direccionar N (Vgr; 31) subredes, a partir de una dirección IP ClassFull (Vgr; 150.216.1.70/16).
            1. Obtener la dirección de red classfull.
            2. Calcular la cantidad de bits necesarios para representar N+2 subredes.

               Donde:
               N: es la cantidad de subredes requeridas
               2: son las dos subredes que no pueden utilizarse por contener las direcciones de red y de broadcast de la red classfull.
            3. Definir la nueva porción para subred en el espacio IP: Tomar la cantidad de bits calculados para el espacio de subred; a partir de la porción de host de la dirección de red classfull, de izquierda a derecha, a partir del límite de la porción de red, disminuyendo así, la cantidad de bits en la porción de host.
            4. Definir la máscara de subred, donde los 1s consecutivos se prolonguen a lo largo de las porciones de red y subred.
            5. Asignar hosts y subredes según las necesidades particulares.

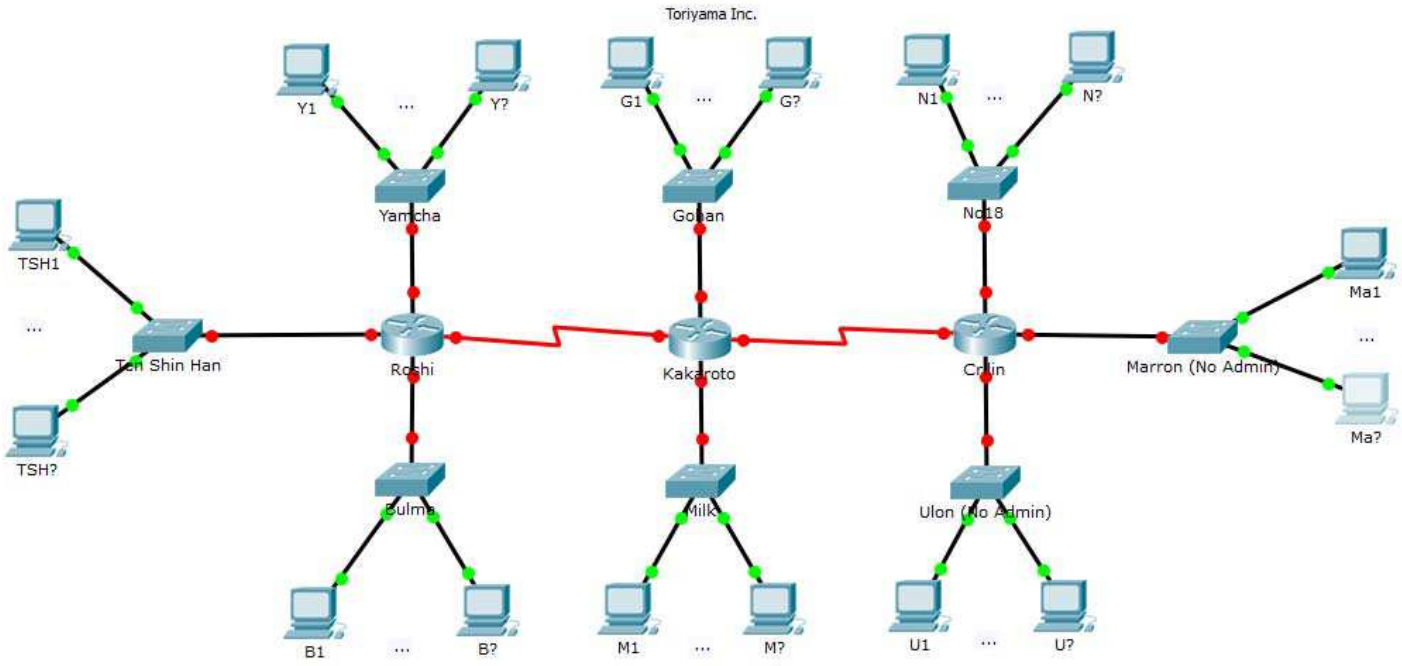
    - Ejemplificar Subnetting Classfull por necesidad de hosts:
        - Se requiere direccionar M (Vgr; 450) hosts por subred, a partir de una dirección IP ClassFull (Vgr; 150.216.1.70/16).
            1. Obtener la dirección de red classfull.
            2. Calcular la cantidad de bits necesarios para representar M+2 IPs.

               Donde:
               M: es la cantidad de hosts requeridos por subred.
               2: son las dos IPs que no pueden utilizarse para host (direcciones de subred y de broadcast).
            3. Definir la nueva porción para host y subred en el espacio IP: Tomar la cantidad de bits calculados para el espacio de host; a partir de la porción de host de la dirección de red classfull, de derecha a izquierda, sin invadir la porción de red y dejando espacio suficiente para la porción de subred.
            4. Definir la máscara de subred, donde los 1s consecutivos se prolonguen a lo largo de las porciones de red y subred.
            5. Asignar hosts y subredes según las necesidades particulares.

Subnetting ClassLess

- Mismo procedimiento de Subnetting ClassFull pero:
    - Admite el uso de subredes 0 y última.
    - Ejemplificar.
        - Vgr; 31 subredes, a partir de la dirección IP ClassFull 150.216.1.70/16.
        - Vgr; 450 hosts, a partir de la dirección IP ClassFull 150.216.1.70/16.

Ejercicios de Subnetting para una topología dada:



Actividad Práctica: Resolver el Subnetting para el PacketTracer y las necesidades indicadas, realizar configuraciones básicas de IOS y enrutar.

Descripción del algoritmo de ARQ Stop-and-Wait + Timer + CRC.

Tarea: Implementar ARQ Stop-and-Wait + Timer con verificación de CRC por paquete, para entrega 13 de Noviembre.

Aviso: 2a Evaluación Parcial, hasta Subnetting: Miercoles 30 de Octubre 12:00Hrs.

CIDR/VLSM IPv4

- IPv4 **CIDR / VLSM** (RFC 1518 y RFC 1519 - 1993)
  - Agrupación / División de rangos de direcciones IP independiente de la clase a la que hubiese pertenecido en el pasado.
    - **CIDR.**
      - Permite mayor flexibilidad al considerar rangos de direcciones IP como redes separadas.
      - Reemplaza la nomenclatura IP previa de nombrar direcciones IP respecto a Clases.
        - En vez de asignar bloques de direcciones en los límites de los octetos, (/8, /16 y /24 bits), CIDR asignaprefijos de longitud arbitraria denominados Bloques CIDR.
      - Los **Bloques CIDR** IPv4 se identifican mediante la sintaxis de las direcciones IPv4: Cuatro números decimales separados por puntos, seguidos de una barra de división y un número de 0 a 32;
        - Vgr; A.B.C.D/N.
        - Donde:
          - A.B.C.D se interpretan como una dirección IPv4 (Dirección de subred)
          - /N representa el número de bits comunes a todas las direcciones incluidas en el bloque CIDR (Equivale a la cantidad de 1s en la mascara de subred, con los que indica que bits pertenecen a la porción de subred, y cuales a la porción de host).
        - La siguiente tabla muestra algunos detalles de algunos bloques CIDR IPv4

CIDR	No. de redes por clase	Hosts	Máscara
/32	1/256 C	1	255.255.255.255
/31	1/128 C	2	255.255.255.254
/30	1/64 C	4	255.255.255.252
/29	1/32 C	8	255.255.255.248
/28	1/16 C	16	255.255.255.240
/27	1/8 C	32	255.255.255.224
/26	1/4 C	64	255.255.255.192
/25	1/2 C	128	255.255.255.128
/24	1 C	256	255.255.255.0
/23	2 C	512	255.255.254.0
/22	4 C	1,024	255.255.252.0
/21	8 C	2,048	255.255.248.0
/20	16 C	4,096	255.255.240.0
/19	32 C	8,192	255.255.224.0
/18	64 C	16,384	255.255.192.0
/17	128 C	32,768	255.255.128.0
/16	256 C, 1 B	65,536	255.255.0.0
/15	512 C, 2 B	131,072	255.254.0.0
/14	1,024 C, 4 B	262,144	255.252.0.0
/13	2,048 C, 8 B	524,288	255.248.0.0
/12	4,096 C, 16 B	1,048,576	255.240.0.0
/11	8,192 C, 32 B	2,097,152	255.224.0.0
/10	16,384 C, 64 B	4,194,304	255.192.0.0
/9	32,768 C, 128B	8,388,608	255.128.0.0
/8	65,536 C, 256B, 1 A	16,777,216	255.0.0.0
/7	131,072 C, 512B, 2 A	33,554,432	254.0.0.0
/6	262,144 C, 1,024 B, 4 A	67,108,864	252.0.0.0
/5	524,288 C, 2,048 B, 8 A	134,217,728	248.0.0.0
/4	1,048,576 C, 4,096 B, 16 A	268,435,456	240.0.0.0
/3	2,097,152 C, 8,192 B, 32 A	536,870,912	224.0.0.0
/2	4,194,304 C, 16,384 B, 64 A	1,073,741,824	192.0.0.0
/1	8,388,608 C, 32,768 B, 128 A	2,147,483,648	128.0.0.0
/0	16,777,216 C, 65,536 B, 256 A	4,294,967,296	0.0.0.0

      - **VLSM** permite dividir un espacio de red en subredes de diferentes tamaños (con diferentes mascaras de subred).

- La máscara de subred varía según la cantidad de bits que se toman prestados para una subred específica, de lo cual deriva la palabra “variable” de VLSM.
- Surge al observar el desperdicio de direcciones IP al dividir una red mediante Subneting (todas las redes son del mismo tamaño); el cual, llega al extremo en redes punto a punto (Vgr; Enlaces WAN), que sólo necesitan de dos a cuatro direcciones IP.

- Se Identifican 2 porciones de una IP.
  - Subred / Host

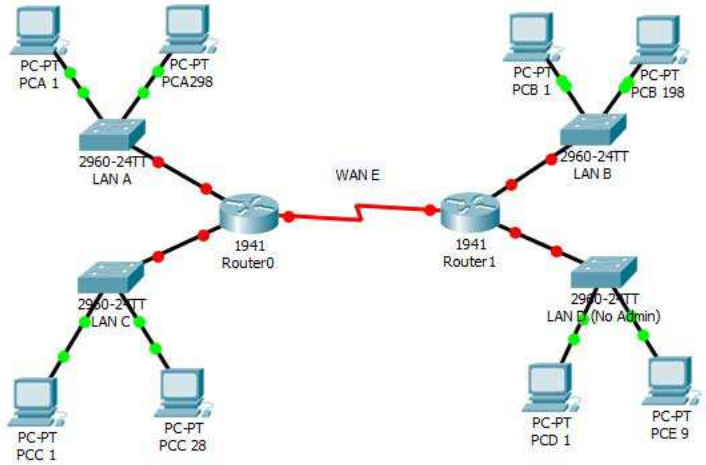
- Ejemplo: Considere la existencia de varias redes (A, B, C, D y E), con las necesidades de hosts mostradas en la siguiente tabla:

RED	Host
B	28
E	28
A	14
D	7
C	2

- Su direccionamiento no está sujeto a un tamaño fijo, sino que se adapta a la potencia de 2 más cercana a cada necesidad.

Subred	Red	Ip de Subred	Rango de Ip asignables		Broadcast	Mascara
			Desde	Hasta		
Cero	B	200.20.30.0	200.20.30.1	200.20.30.30	200.20.30.31	/27
Uno	D	200.20.30.32	200.20.30.33	200.20.30.62	200.20.30.63	/27
Dos	A	200.20.30.64	200.20.30.65	200.20.30.78	200.20.30.79	/28
Tres	E	200.20.30.80	200.20.30.81	200.20.30.94	200.20.30.95	/28
cuatro	C	200.20.30.96	200.20.30.97	200.20.30.98	200.20.30.99	/30

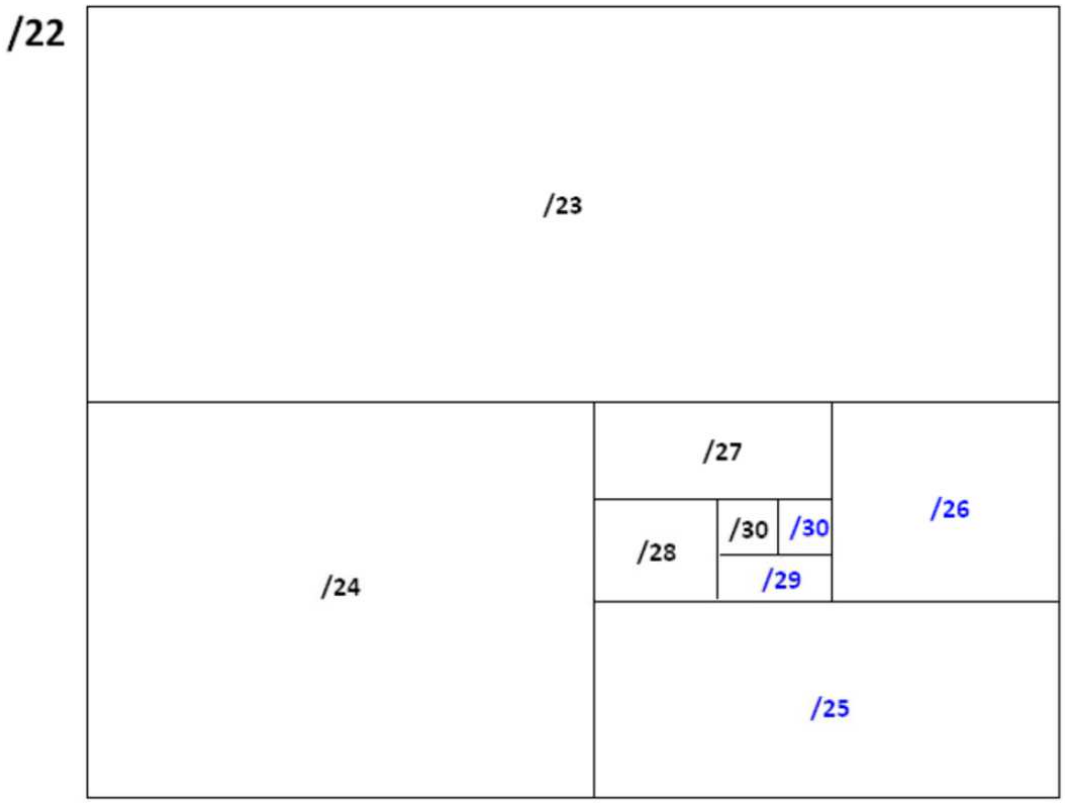
- **Ejemplo de calculo de Bloques CIDR y VLSM** para una topología dada:



  - Obtener el bloque CIDR para direccionar la topología, en base a sus necesidades y considerando que la IP 1.2.3.100 se encuentra dentro del bloque.
    - Resumen de Necesidades y Subbloques CIDR correspondientes:
      - A. 300 hosts --> /23
      - B. 200 hosts --> /24
      - C. 30 hosts --> / 27
      - D. 10 hosts --> /28
      - E. 2 hosts --> / 30

    - Análisis para determinar el prefijo del Bloque CIDR inicial.

- Puede verse un bloque CIDR como un cuadrado que puede dividirse en bloques mas pequeños (Prefijos mas grandes)



  - Para determinar el bloque inicial se deben agrupar las necesidades por pares (en ocasiones se requerirá considerar algunos bloques CIDR adicionales, que quedarán libres para crecimiento futuro, como los marcados en azul), hasta que no queden mas necesidades por agregar.
- Con el Prefijo obtenido (/22) y la IP contenida en el bloque, realizar un and binario para obtener la dirección de red, del bloque CIDR
  - Para la dirección IP: 1.2.3.100/22
    - Dirección de host binaria: 00000001. 00000010. 00000011. 01100100
    - Mascara de subred binaria: 11111111. 11111111. 11111100. 00000000
    - Dirección de Red binaria: 00000001. 00000010. 00000000. 00000000
    - Dirección de Red: 1.2.0.0/22
    - Dirección de Difusión: 1.2.3.255/22

- División por VLSM, para el bloque CIDR Calculado (1.2.0.0/22):
  - Subdividir bloque CIDR y asignar por necesidad, de mayor a menor:
    - 1.2.0.0/23 -> A
    - 1.2.2.0/23 -> Se Divide
      |___1.2.2.0/24 -> B
      |___1.2.3.0/24 -> Se Divide
      .....|___1.2.3.0/25 -> Se Divide
      .....|.....|___1.2.3.0/26 -> Se Divide
      .....|.....|.....|___1.2.3.0/27 -> C
      .....|.....|.....|___1.2.3.32/27 -> Se Divide
      .....|.....|.....|___1.2.3.32/28 -> D
      .....|.....|.....|___1.2.3.48/28 -> Se Divide
      .....|.....|.....|___1.2.3.48/29 -> Se Divide
      .....|.....|.....|.....|___1.2.3.48/30 -> E
      .....|.....|.....|.....|___1.2.3.52/30 -> Libre
      .....|.....|.....|___1.2.3.56/29 -> Libre
      .....|.....|___1.2.3.64/26 -> Libre
      .....|___1.2.3.128/25 -> Libre

  - Registrar el Direccionamiento Final con VLSM, para 1.2.0.0/22:

Subred	Requerimientos de Hosts	Dirección de Red	Direcciones IP útiles
A	300	1.2.0.0/23	2^9 – 2 = 510
B	200	1.2.2.0/24	2^8 – 2 = 254
C	30	1.2.3.0/27	2^5 – 2 = 30
D	10	1.2.3.32/28	2^4 – 2 = 14
E	2	1.2.3.48/30	2^2 – 2 = 4
Libre	-	1.2.3.52/30	2^2 – 2 = 4
Libre	-	1.2.3.56/29	2^3 – 2 = 6
Libre	-	1.2.3.64/26	2^6 – 2 = 62
Libre	-	1.2.3.128/25	2^7 – 2 = 126

- Comparar desperdicio IP Subnetting vs VLSM.
  - Para la dirección IP 1.2.3.100, con VLSM se utilizó un prefijo /22 quedando aun direcciones de Red libres que se podrán utilizar en un futuro.
  - Con Subneting el prefijo /22 no hubiese sido suficiente. Para el requerimiento de 5 subredes se ocuparían 3 bits y para el requerimiento de 300 hosts en la red más grande se ocuparían 9 bits, por tanto se hubiesen requerido 12 bits, es decir, un prefijo /20, por lo que el desperdicio con Subneting es muy notable, comparado con VLSM.

- Mas ejercicios en el pizarrón.
- **Actividad Práctica**: Resolver VLSM para el PacketTracer y las necesidades indicadas, realizar configuraciones básicas de IOS y enrutar.
  - Cada equipo deberá elegir una dirección IP apartir de la cual calcular el bloque CIDR inicial.
  - Comparar desperdicio IP Subnetting vs VLSM.

Redes de Computadoras I

- **Actividad Práctica 1:** Analizar con Wireshark al menos dos protocolo de capa de aplicación popular (no web y al menos uno cuyo tráfico no esté encriptado): Netflix, Cinepolis Click, Spotify, Crunchyroll, Dropbox, Mega, Skype, Cliente Torrent, Kodi, eMule, Ares, Google Earth, LOL, WoW, Fortnite, Apex Legends, Rocket League u otros videojuegos online, etc...
  - Reportar:
    - IP(s) a la(s) que se envía el tráfico.
    - Determinar si es P2P ó Cliente-Servidor.
    - Protocolo de capa de transporte utilizado.
    - Puerto del lado servidor y cliente.
    - Si el tráfico de capa de aplicación es encriptado o no
    - Si no está encriptado:
      - Interpretar y describir al menos dos mensajes del protocolo de capa de aplicación.

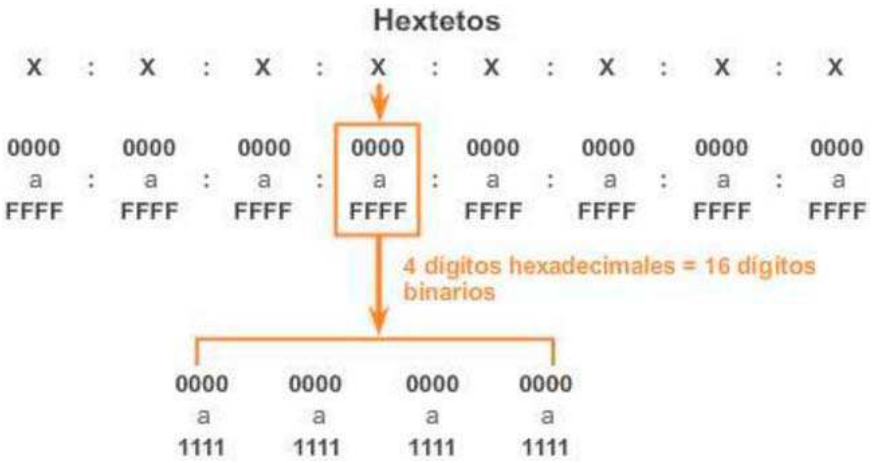
- **Actividad Práctica 2:** Describir en no mas de un párrafo, los generales (propósito y datos reportados en la actividad anterior), de los siguientes protocolos de capa de aplicación:
  - SSH
  - DNS
  - FTP
  - DHCP
  - SMTP
  - POP3
  - IMAP
  - SYSLOG
  - NTP
  - SNMP
  - NFS
  - FTPs
  - Cualquier otro no visto o mencionado hasta ahora en el laboratorio.

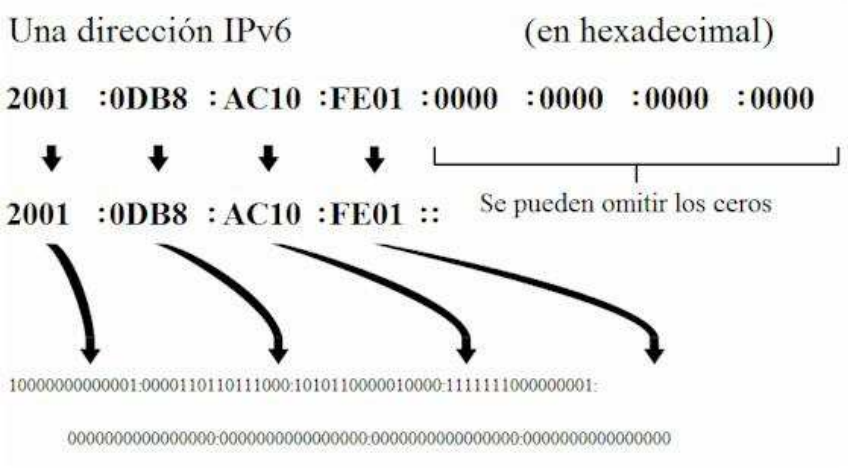
- **Actividad Práctica para entrega Final:** Instalación y Puesta en Marcha de 4 servicios de capa de aplicación por equipo, en una computadora propia con Linux (ponerse de acuerdo, no se admiten repetidos):
  - Elegir 2
    - SSH
    - DNS
    - FTP
    - DHCP
    - Sendmail (SMTP, POP3, IMAP)
  - Elegir 2
    - SYSLOG
    - NTP
    - SNMP
    - NFS
    - FTPs

- Deberán entregarse los servicios funcionando en el equipo propio, así como un manual técnico de instalación y puesta en marcha, siendo la redacción lo mas específico posible.
  - Redacción en 3a persona (impersonal)
  - Uso de Referencias Bibliográficas en formato IEEE.
  - Códigos y comandos se presentan en letra courier, el resto de la redacción en cualquier otro tipo de letra.
  - Las imágenes deben llevar un título inferior, y deben estar referidas a lo largo del manual, por su número de figura.
  - Las tablas deben llevar un titulo superior y ser referidas en el manual por su número de tabla.

IPv6

- **IPV6**
  - Versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar IPv4 RFC 791.
- **Necesidad**
  - IETF sabía que CIDR era solo una solución temporal para el agotamiento de IPs
  - Necesario desarrollar un nuevo protocolo.
  - En 1994, IETF comenzó a trabajar en el sucesor de IPv4, que finalmente fue IPv6.
  - IPv6 tiene un mayor espacio de direcciones: 128 bits (340 sextillones de direcciones).
- **Representación y formato**
  - Las direcciones IPv6 se representan mediante valores hexadecimales.
  - Bytes de 00000000 hasta 11111111 se representan en valores hexadecimales como el intervalo de 00 a FF.
  - Cuatro bits se representan mediante un único dígito hexadecimal, con un total de 32 valores hexadecimales.
  - No distinguen mayúsculas de minúsculas y pueden escribirse en minúscula o en mayúscula.
  - El formato preferido para escribir una dirección IPv6 es x:x:x:x:x:x:x:x, donde cada “x” consta de cuatro valores hexadecimales (denominado informalmente: hexteto).

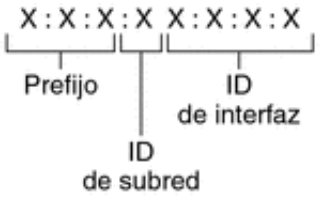




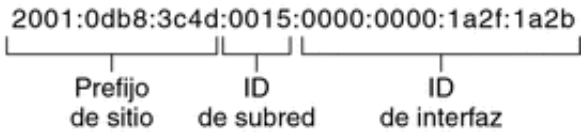
- Reglas de reducción [0 - ..]

- **Regla 1**: Omisión de ceros iniciales.
  - Permite reducir la notación de direcciones IPv6 omitiendo cualquier 0 (cero) inicial en cualquier sección de 16 bits o hexteto. Por ejemplo:
    - 01AB puede representarse como 1AB.
    - 09F0 puede representarse como 9F0.
    - 0A00 puede representarse como A00.
    - 00AB puede representarse como AB.
- **Regla 2:** Omisión de los segmentos compuestos únicamente por ceros.
  - Dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más hextetos compuestos solo por ceros.
  - Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible.
  - Cuando se utiliza junto con la técnica de omisión de ceros iniciales, la notación de direcciones IPv6 generalmente se puede reducir de manera considerable. Esto se suele conocer como "*formato comprimido*".
  - Ejemplos:
    - Dirección incorrecta:
      - 2001:0DB8::ABCD::1234
    - Ejemplos de expansiones posibles:
      - 2001:0DB8::ABCD:0000:0000:1234
      - 2001:0DB8::ABCD:0000:0000:0000:1234
      - 2001:0DB8:0000:ABCD::1234
      - 2001:0DB8:0000:0000:ABCD::1234

- **Estructura General de las Sirecciones IPv6**
  -
    - Un bloque de direcciones IPv6 se compone de 3 secciones principales:
      - **Prefijo Global de Enrutamiento**: hasta /48
      - **ID de subred**: de /48 a /64
      - **ID de Interface:** de /64 a /128



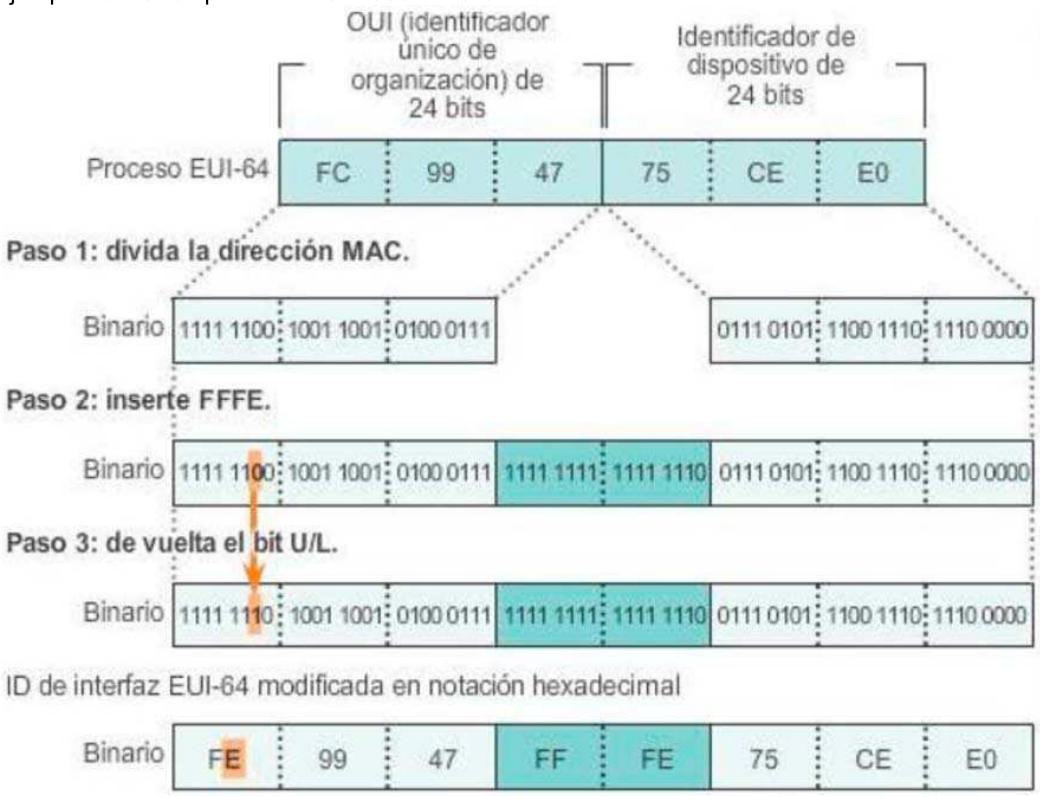
Ejemplo:



      - **Notas sobre el ID de Interfáz y el EUI-64 (Proceso Modificado de Identificador Único Extendido) de IEEE**
        - EUI-64 utiliza la dirección
          MAC de Ethernet de 48 bits e introduce otros 16 bits en medio de la MAC para crear una ID de interfaz de 64 bits.
        - Las MAC de Ethernet, se representan en hexadecimal y constan de dos partes:
          - Identificador único de organización (OUI) de 24 bits (seis dígitos hexadecimales)
          - Identificador de dispositivo: valor de 24 bits (seis dígitos hexadecimales)

        - Las ID de interfaz EUI-64 constan de tres partes:
          - OUI de 24 bits de la MAC, con el séptimo bit (bit universal/local, U/L) negado.
          - Valor de 16 bits FFFE
          - Identificador de dispositivo de 24 bits de la MAC.

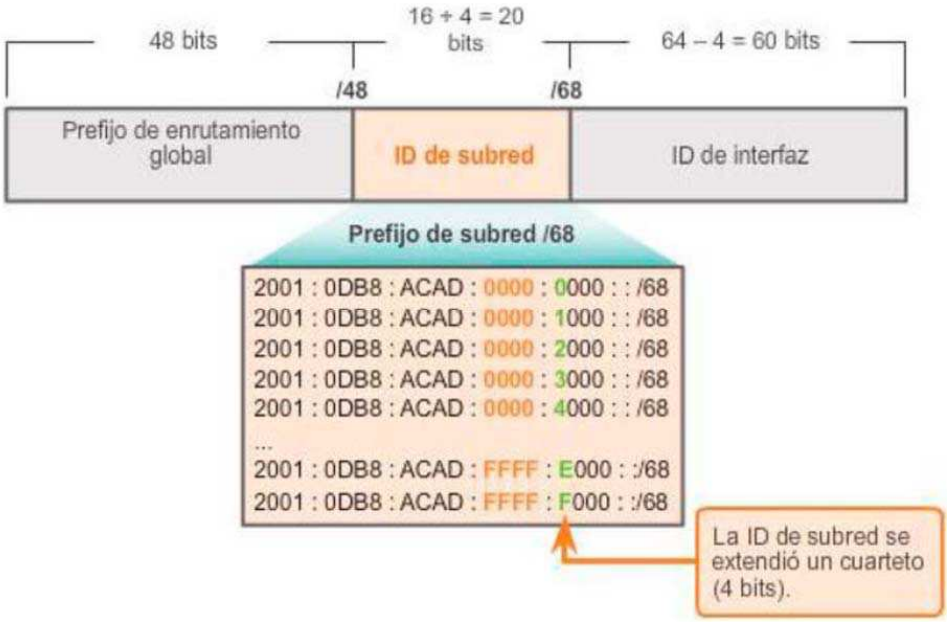
- Ejemplo de EUI-64 para la MAC: FC99:4775:CEE0.



  - EUI-64 perdió popularidad por considerarse una exposición de la privacidad del cliente, al utilizarse como ID de Interfáz para navegar en Internet mediante IPv6 (las direcciones MAC solo tienen relevancia en la red local, las direcciones IP son visibles por donde quiera que transite el tráfico).

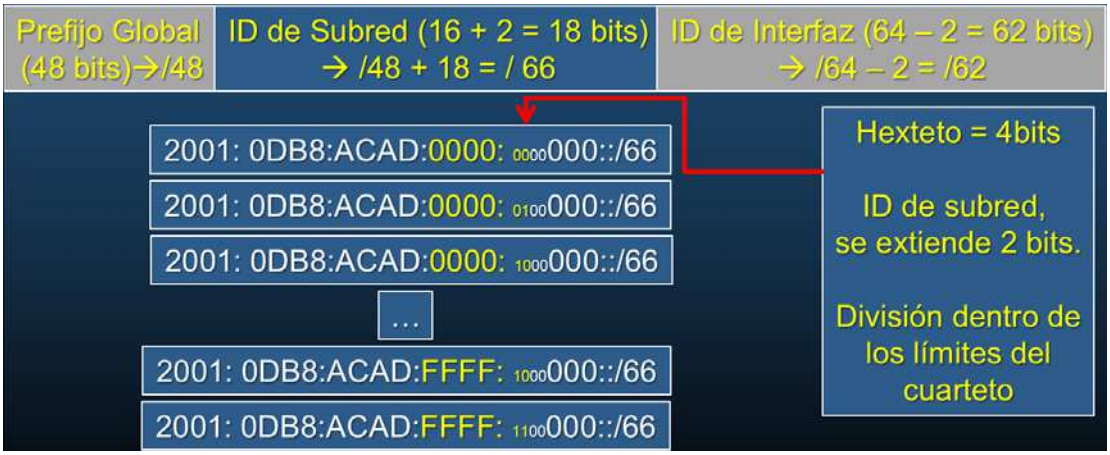
- **Tipos de direcciones IPv6:**
  - Existen seis tipos de direcciones IPv6 unicast, pero las más representativas son las siguientes:
    - **Unicast global:** son direcciones enrutables de Internet globalmente exclusivas, su rango es **[2000::/3 a 3FFF::/3]**
    - **Link Local:** se utilizan para comunicarse con otros dispositivos en el mismo enlace local “subred”, su rango es **[FE80::/10 a FEBF::/10]**
      - Repetibles, no enrutables
    - **Loopback:** Utilizada por los hosts para enviarse paquetes a sí mismos. No se puede asignar a una interfaz física. La dirección IPv6 de loopback está formada por todos ceros, excepto el último bit, representado como **[::1/128]**
    - **Dirección sin especificar:** es una dirección compuesta solo por ceros representada como **::/128** o, simplemente, **::** en formato comprimido.
      - No puede asignarse a una interfaz y solo se utiliza como dirección de origen en un paquete IPv6 cuando el dispositivo aún no tiene una dirección IPv6 permanente o cuando el origen del paquete es irrelevante para el destino.
  - **Multicast:** Las direcciones IPv6 multicast se utilizan para enviar un único paquete IPv6 a varios destinos, su rango es **[FF00::/8]**
  - **All Nodes Multicast:** A diferencia de IPv4, IPv6 no tiene una dirección de broadcast por subred. Sin embargo, existe una dirección IPv6 multicast de todos los nodos que brinda el mismo resultado, **[FF01::1]**

- **Subnetting IPv6**
  - Los espacios de direcciones IPv6 no se dividen en subredes para ahorrar direcciones, sino para realizar un diseño lógico jerárquico de la red.
  - La división en subredes se realiza principalemnte mediante la ID de subred de 16 bits.
    - Admite un total de 65 536 subredes /64 y no requiere tomar prestados bits de la ID de interfaz (porción de host de la dirección).
    - El prefijo de enrutamiento global es igual para todas las subredes. Solo cambian el ID de Subred y el ID de Interfaz.
    - **Subredes al Límite del Nibble:**
      - Cuando sea necesario es posible extender la ID de subred al tomar prestados bits de la ID de interfaz; siendo recomendable realizar la división en subredes en el límite de un Nibble.
      - Por Ejemplo:



        - Como se muestra en la ilustración, el prefijo de subred /64 se extiende 4 bits o 1 cuarteto a /68. Esto reduce el tamaño de la ID de interfaz en 4 bits, es decir, de 64 a 60 bits.

    - La división en subredes en los límites de los cuartetos significa que solo se utilizan máscaras de subred alineadas en cuartetos. Comenzando en /64, las máscaras de subred alineadas en cuartetos son /68, /72, /76, /80, etcétera.

- **Subredes Dentro del límite del Nibble**
    - Cuando se requiera extender la ID de subred, y se desee optimizar el espacio del ID de Interface, es posible tomar prestados N bits de la ID de interfaz; no necesariamente al límite de un Nibble.
    - Ejemplo:
    - 

    - Resulta en las subredes:
        - 2001:0DB8:ACAD:0000:0000::/66
        - 2001:0DB8:ACAD:0000:4000::/66
        - 2001:0DB8:ACAD:0000:8000::/66
        - ...
        - 2001:0DB8:ACAD:FFFF:8000::/66
        - 2001:0DB8:ACAD:FFFF:C000::/66

- **Configuración IPv6 en IOS**
    - Activación IPv6 en router.
        - `(config)# ipv6 unicast-routing`
    - Configuración de IPv6 en Interfaces
        - Dirección *Unicast Global*
            - `(config-if)#ipv6 address x:x:x:x:x:x:x:x/x`
        - `(config-if)# ipv6 x:x:x:x:x:x:x:x link-local`

- Dirección por *Configuración Automática Sin Estado (SLAAC)*: Usa EUI-64 para ID de Interface, tomando el prefijo y subred del gateway de la red; ya sea Unicast ó Local Link.
  - `(config-if)#ipv6 address autoconfig`
  - **Nota:** PacketTracer requiere que los equipos preconfigurados usen una longitud de prefijo /64.

- Revisión de configuraciones IPv6 por interfaces:
  - `# show ipv6 interfaces brief`

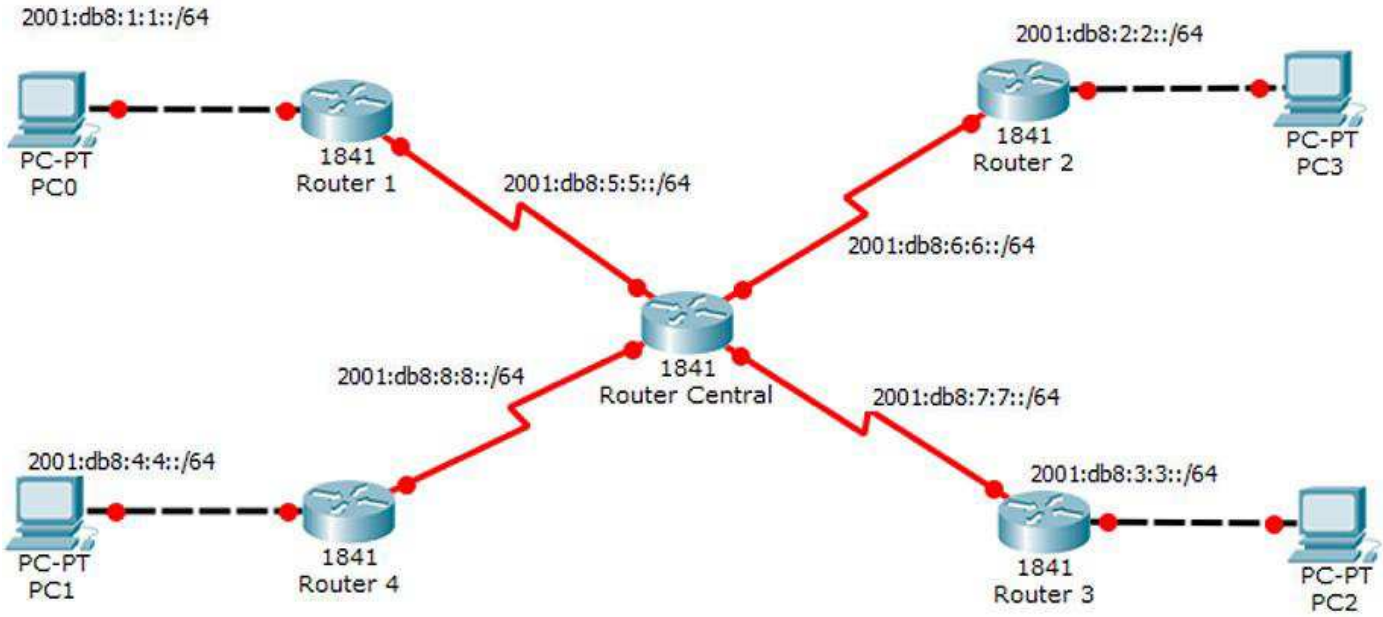
- Análisis de la tabla de enrutamiento IPv6
  - `# show ipv6 route`
- Configuración de rutas estáticas y por default.
  - `(config)# ipv6 route x:x:x:x::/x [interface_salida] [ipv6_siguiente_salto]`
  - `(config)# ipv6 route ::/0 [interface_salida] [ipv6_siguiente_salto]`

  - **Nota:** Actualmente PacketTracer no se soportan rutas por redes Link-Local si no están complentamente especificadas.
  - **Nota 2:** Eventualmente PacketTracer pierde las rutas ipv6 que utilicen ips Link-Local de siguiente salto, sobre todo al reiniciar los equipos, o cerrar y volver a abrir una topología. Esto puede sobrellevarse, quitando todas las rutas y volviendolas a poner, una vez que todos los dispositivos están encendidos y tienen conectividad capa 2 (Los equipos físicos no tienen este problema).

- Ejemplo de Configuración IPv6: Ejercicio

- Solución.

- **Actividad Práctica:** Configuración IPv6 en la siguiente topología en equipos físicos. Pida ayuda para cambiar las interfaces de red seriales de los routers, o utilice UTP cruzados de ser necesario.



- Para cada host/interfaz, configurar una dirección IPv6 unicast global (Subnetear y docuemntar a gusto de cada equipo; aunque para ejemplificar se utilize 2001:db8::/32) y link-local(fe80::/10)
- En cada router agregar las rutas necesarias para que exista conectividad desde cualquier host a cualquier otro host.
- **Nota:** El direccionamiento deberá ser lo suficientemente ingenioso por cada equipo, para que no existan duplicados.
  - Vgr; C0CA:C0C0:DEAD:FEA:FE0::C15:C0
- **Nota:** Utilize Link-Local y Autoconfiguración, al menos en una red/equipo.

redes1

Redes de Computadoras I

- Manejo de sesiones TCP
  - Descripvión breve (Diapositivas Capitulo 7 18-26)
  - Diferencias entre ventana deslizante TCP (Capa 4) y protocolos de ventana deslizante para control de enlace de datos (Capa 2).
    - Funciones de capa de enlace:
      - Control de acceso al medio (MAC - Hardware a Software)
      - Control de enlace de lógico (LLC - Software)
        - Creación de Tramas
        - Control de flujo y errores
          - Protocolos de transmisión
            - Simplest: Solo envío de tramas, sin control de flujo (Falla ante perdida de tramas).
            - Parada y Espera: Envia trama de datos y espera trama de acuse (Falla ante perdida de tramas).
            - Petición de respuesta automática (ARQ) con Parada y Espera: Parada y Espera con Retransmisión por timer (Transmisión confiable pero muy lenta).
            - ARQ con vuelta atrás en N: defineun tamaño de ventana y envía todas las tramas dentro de la ventana, acuses por trama, al acusar fin de ventana se recorre e inicia ventana nueva, temporizador vencido reenvía toda la ventana (Transmisión confiable mas rápida que ARQ con parada y espera si no hay fallos, ante fallos desperdicia tiempo y uso del medio).
            - ARQ con repetición selectiva: Envio de tramas por ventana, uso de acuses positivos y negativos para evitar desperdicio en eluso del canal.
      - GSM utiliza ARQ.
      - ITU-T define ARQ-Selective-Repeat como estándar para transmisiones de datos por líneas de energía y cables coaxiales.
      - Ethernet no usa ventana deslizante.
        - TCP resuelve el problema de comunicación confiable.
  - **Actividad:** *Realizar por equipo un diagrama de Flujo para emisor y receptor, de cualquiera de los protocolos ARQ*

- Saludo 3 way hand-shake de TCP
  - Análisis en una captura de tráfico para una conexión HTTP
  - Evidenciar mediante ejemplo de sockets TCP.
- Intercambio de flujogramas y manejo de ventanas TCP
  - Análisis en una captura de tráfico para una conexión HTTP.
  - Filtrado de tráfico por IP/Puerto/Protocolo *Vgr;*
    - *tcp.port==80*
    - *ip.addr==192.168.1.149 and tcp.port ==80*
  - Evidenciar en WireShark la diferencia en números de secuencia entre emisor-receptor.
    - No son 0 ambos, WireShark los muestra así pero son valores aleatorios, para evidenciar, deshabilitar números de secuencia relativos en:

      Edición> Preferencias> Protocolos> TCP

Desactive la opción: " *Números de secuencia relativa* "

- Cierre de conexión TCP
  - Análisis en una captura de tráfico para una conexión HTTP
  - Evidenciar mediante ejemplo de sockets TCP, utilizando shutdown, y diferenciar de close.
- Netstat
  - Establecer conexiones TCP mediante Telnet a servicios bién conocidos y evidenciar con Netstat
  - Diferenciar estado LISTEN vs ESTABLISHED

Recordatorio: entrega de transmisión confiable.
Tarea: Evidenciar estados de conexión mediante ejemplo de sockets TCP, debugueando paso a paso (ddd).

Uso de sockets no bloqueantes, para gestión de retransmisiones.

- Semestre 14-15
- # Ventana Deslizante
  - # Descripción de transporte fiable por ventana deslizante go-back-N
  - # Tarea: Implementación del algoritmo go-back-N.

Inclusión de Dipositivos Inalámbricos a Topologías de Red

- **Descripción del funcionamiento de los tipos de NAT.**
  - Static NAT: Mapea una dirección IP privada con una dirección IP pública de forma estática.
    - Cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet.
    - Útil cuando un dispositivo tiene que ser accesible desde fuera de la red.
    - Desventaja: Por cada equipo que se desee tenga acceso a Internet se debe contratar una IP pública
    - Vgr; En NAT Estático, el host con la dirección IP 192.168.32.10 siempre se traducirá por la dirección 213.18.123.110.

    
    Static Nat

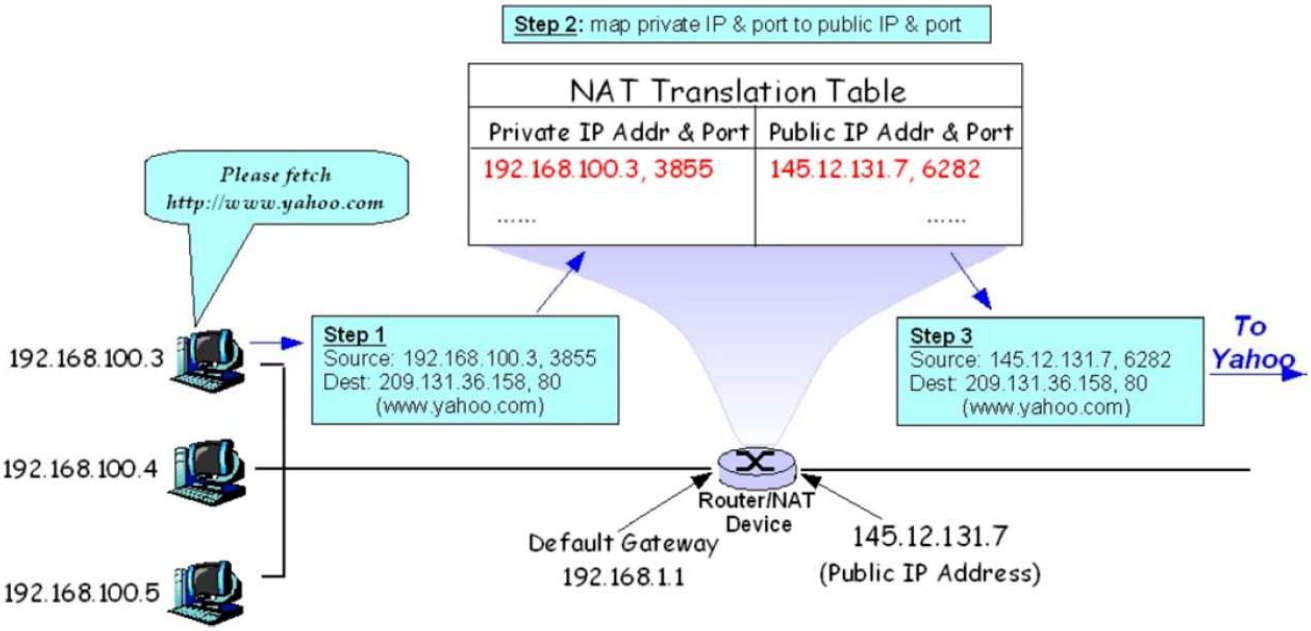
  - Dynamic NAT:
    - Utiliza un pool de N IPs públicas para un pool de M IPs privadas que serán mapeadas de forma dinámica y a demanda.
    - Las primeras N máquinas de las M con IP privada en conectarse, tendrán acceso a Internet.
    - Vgr; En NAT dinámico, el host con la dirección IP 192.168.32.10 será traducida por la primer dirección disponible en el rango desde 213.18.123.100 hasta 213.18.123.150.

    
    Nat Dinámico

  - Overloading (PAT): NAT con sobrecarga o PAT (Port Address Translation).
    - Consiste en utilizar una única dirección IP pública para mapear múltiples direcciones IPs privadas.
    - Ventajas en dos enfoques:
      - El cliente necesita contratar una sola dirección IP pública para que las máquinas de su red tengan acceso a Internet, (ahorro económico).
      - Ahorro de un número importante de IPs públicas, lo que demora el agotamiento de las mismas.
    - PAT hace uso de múltiples puertos para manejar las conexiones de cada host interno, por lo que una única dirección IP pública mapea múltiples IPs privadas.
      - El router arma una tabla que le permite saber a qué máquina de la red interna debe dirigir la respuesta.
    - Vgr; En PAT, la dirección IP de cada host en la red privada será traducida por la misma dirección IP pública (213.18.123.100), pero con un número de puerto origen diferente.

    
    PAT

- **Uso de PAT**
  - En la imagen, la PC con la dirección 192.168.100.3 quiere acceder a www.yahoo.com (209.131.36.158).



  - El socket está formado por la siguiente información:

IP Origen:	192.168.100.3
Puerto Origen:	3855
IP Destino:	209.131.36.158
Puerto Destino:	80

  - Al llegar al router, este hace PAT y modifica dicha información por la siguiente:

IP Origen:	145.12.131.7 (IP pública en la

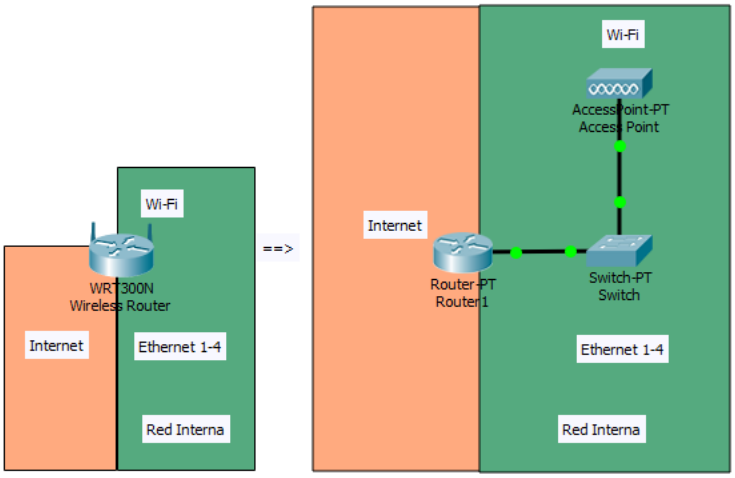
	interfaz del Router)
Puerto Origen:	6285
IP Destino:	209.131.36.158
Puerto Destino:	80

- El tráfico de retorno realiza la traducción inversa en base a la información almacenada en la tabla PAT del Router.

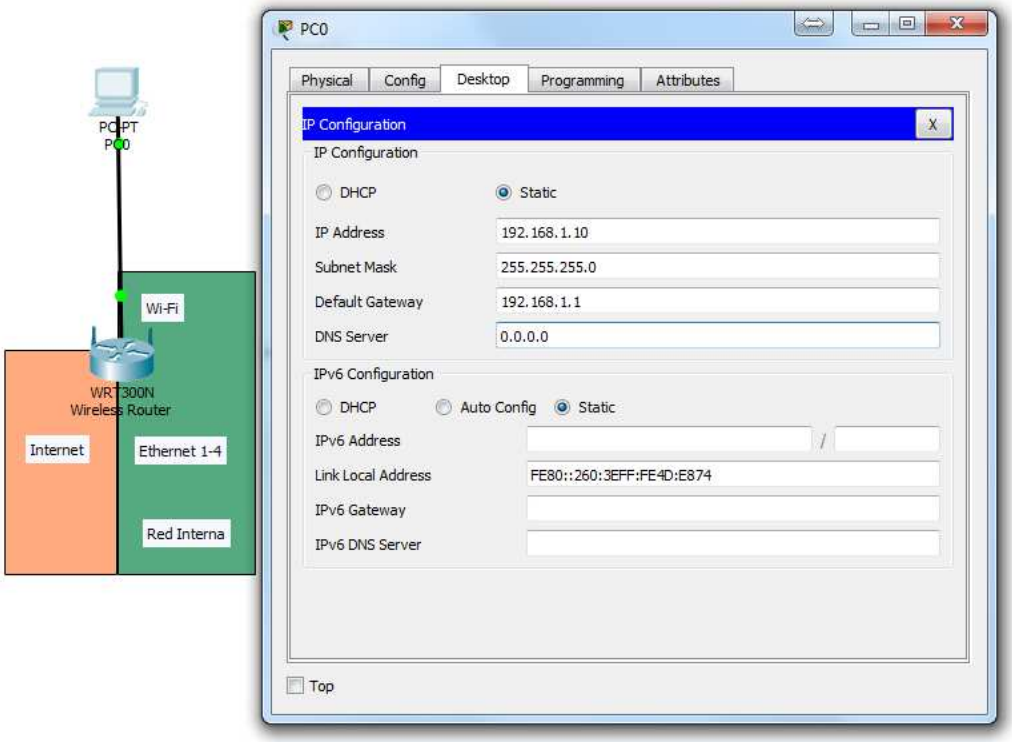
- **Configuración de Routers Inalámbricos Linksys WRT54G2 / WRT300N**

WRT54G2

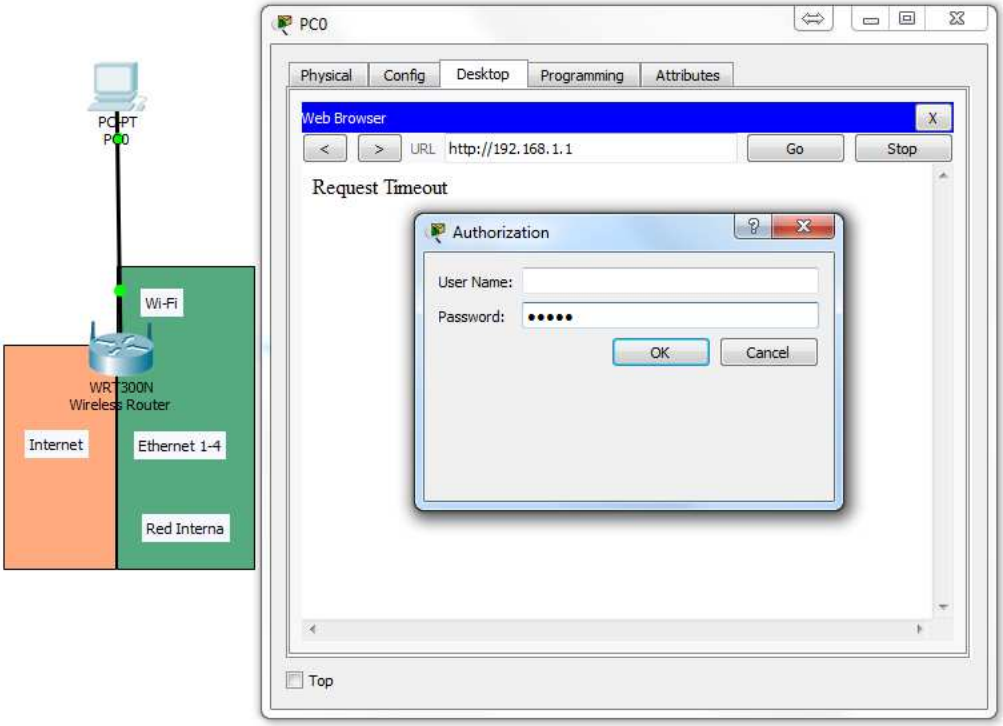
- Un router inalámbrico incluye, tres dispositivos en uno:
  1. Punto de acceso inalámbrico, que permite a dispositivos finales, conectarse a la red sin necesidad de cables.
  2. Un switch Ethernet 10/100 de 4 puertos de dúplex completo para conectar dispositivos finales Ethernet por medio de cables.
  3. Un router que une todos los elementos y permite compartir una conexión a Internet vía Ethernet con toda la red interna.
     - Puede hacer la función de servidor DHCP de la red interna y admite paso a través de VPN.



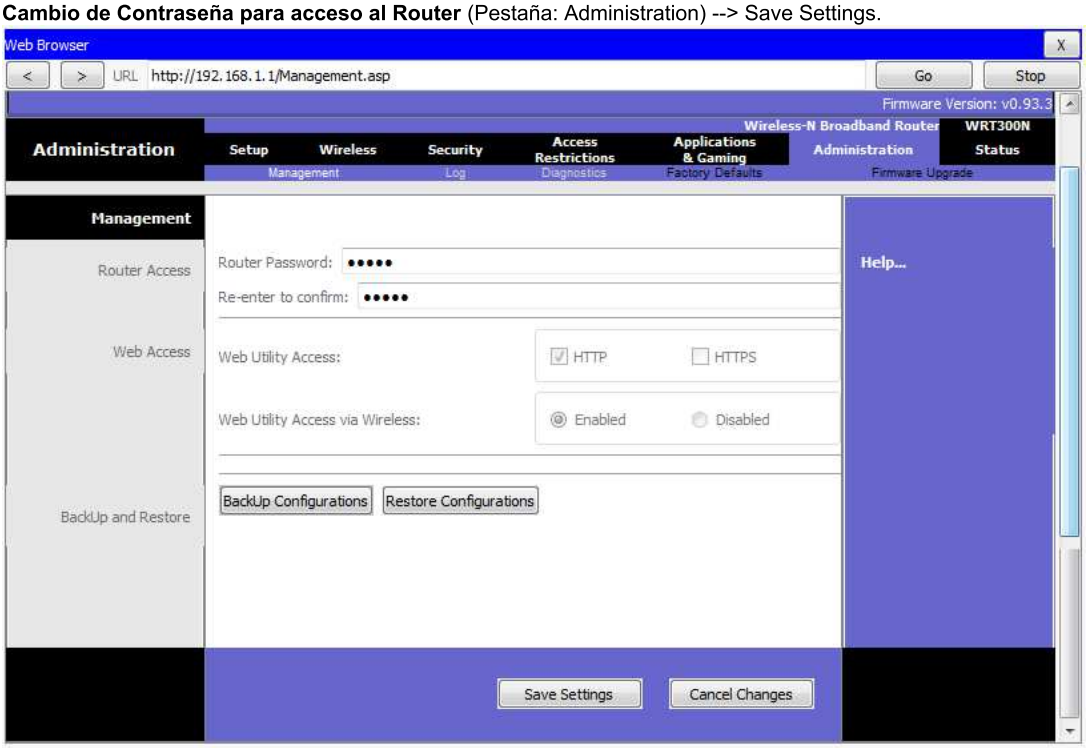
- **Acceso a GUI de Configuración.**
  - Conectar una PC a la red interna del WRT54G2 (cable cruzado), y configurar con una ip de la misma (192.168.1.0/24 para WRT54G ó 192.168.0.0/24 para WRT300N).



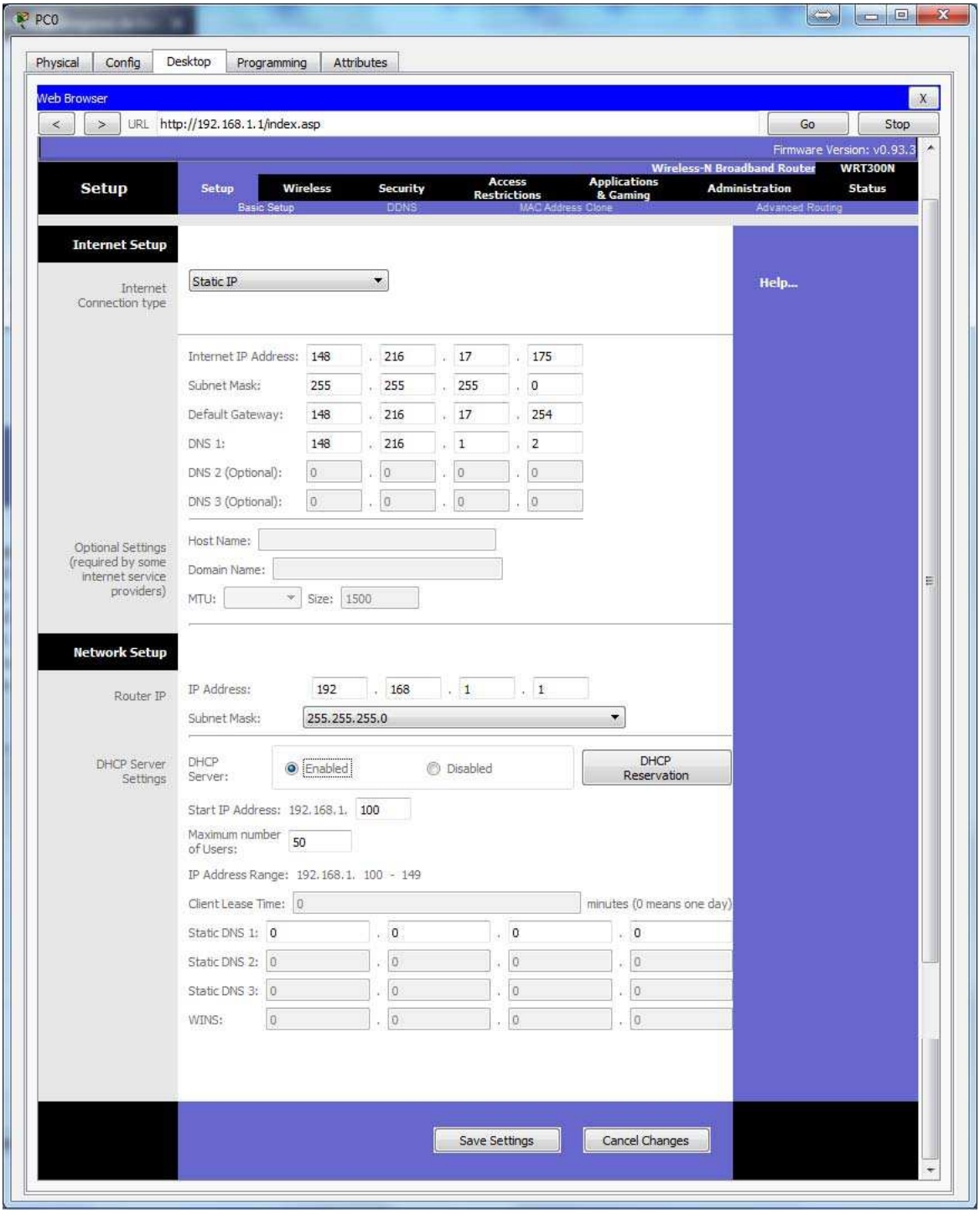
- En un navegador web abrir 192.168.1.1 (192.168.0.1 Para Routers WRT300N)
  - Usuario: vacío (WRT54G) / admin (WRT300N)
  - Contraseña: admin



- **Cambio de Contraseña para acceso al Router** (Pestaña: Administration) --> Save Settings.



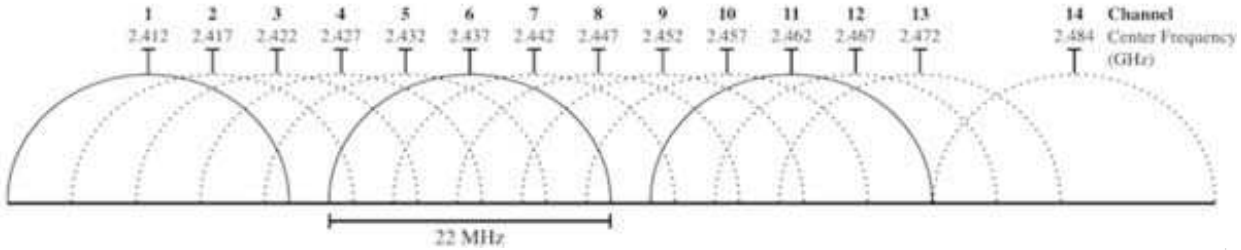
- **Configuración IPv4** (Setup)
  - **Internet:** Permite configurar la interface del Router correspondiente a la red externa (Puerto: Internet).
  - **Network** (PAT): Permite configurar la interface del Router correspondiente a la red interna (Interface de red a donde se conecta el switch con el AP).
  - **DHCP**: Permite especificar el pool de direcciones de la red interna que se utilizarán para configurar automáticamente los clientes móviles.



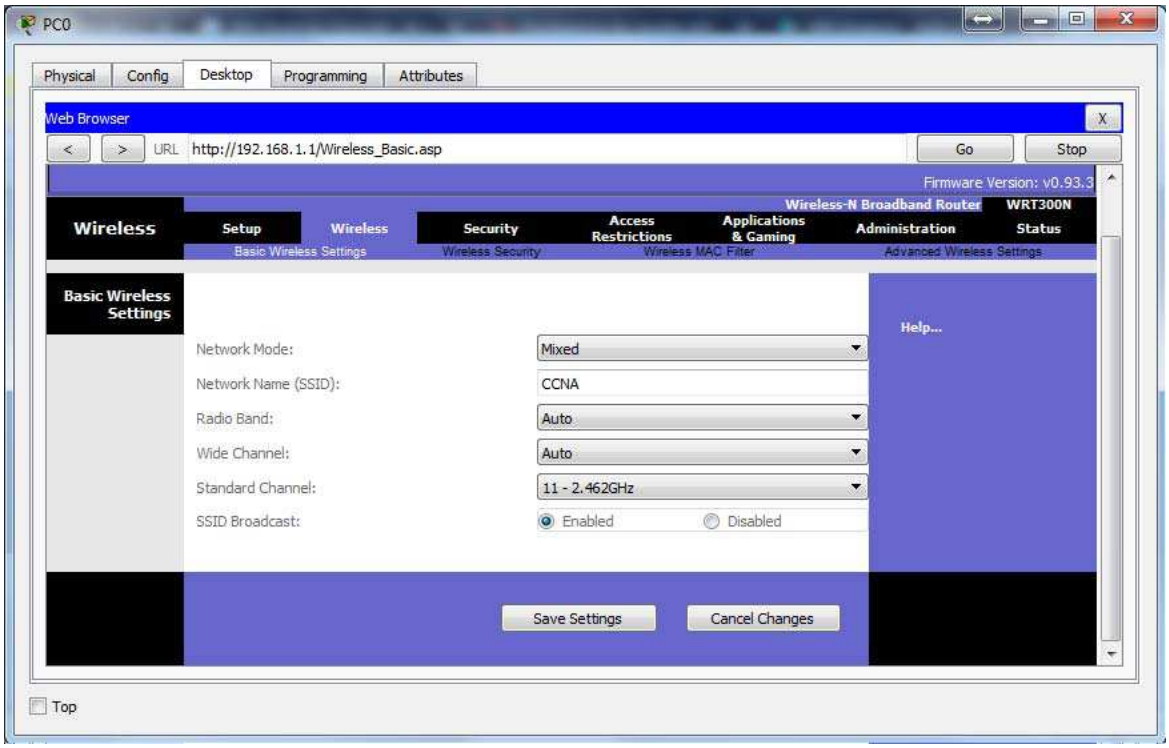
- **Save Settings**: Permite guardar los cambiosrealizados.

- **Configuración Inalámbrica** (Wireless): Permite establecer los parámetros para la operación de la red inalámbrica:
  - **Modo de Operación**: Permite elegir la versión del protocolo 802.11 a utilizar.
    - 802.11b / 802.11g / 802.11n.
    - Mixto
  - **Network Name / SSID**: Establece el Identificador de la red Inalámbrica.
  - **Canales**: Wi-Fi cuenta con 11 canales (en América; 13 en Auropa) de 22MHz de ancho y separados por 5MHz (traslapados a poco mas de 3/4 de canal, para transmisión de señales).
    - 1 – 2.412 GHz
    - 2 – 2.417 GHz
    - 3 – 2.422 GHz
    - 4 – 2.427 GHz
    - 5 – 2.432 GHz
    - 6 – 2.437 GHz
    - 7 – 2.442 GHz
    - 8 – 2.447 GHz
    - 9 – 2.452 GHz
    - 10 – 2.457 GHz

- 11 – 2.462 GHz



- Lo recomendable es realizar un escaneo de señales (Vgr; con Wifi Analyser para Android) y elegir un canal que no posea traslape con ninguno de los que ya se estén utilizando (O el menor traslape posible).

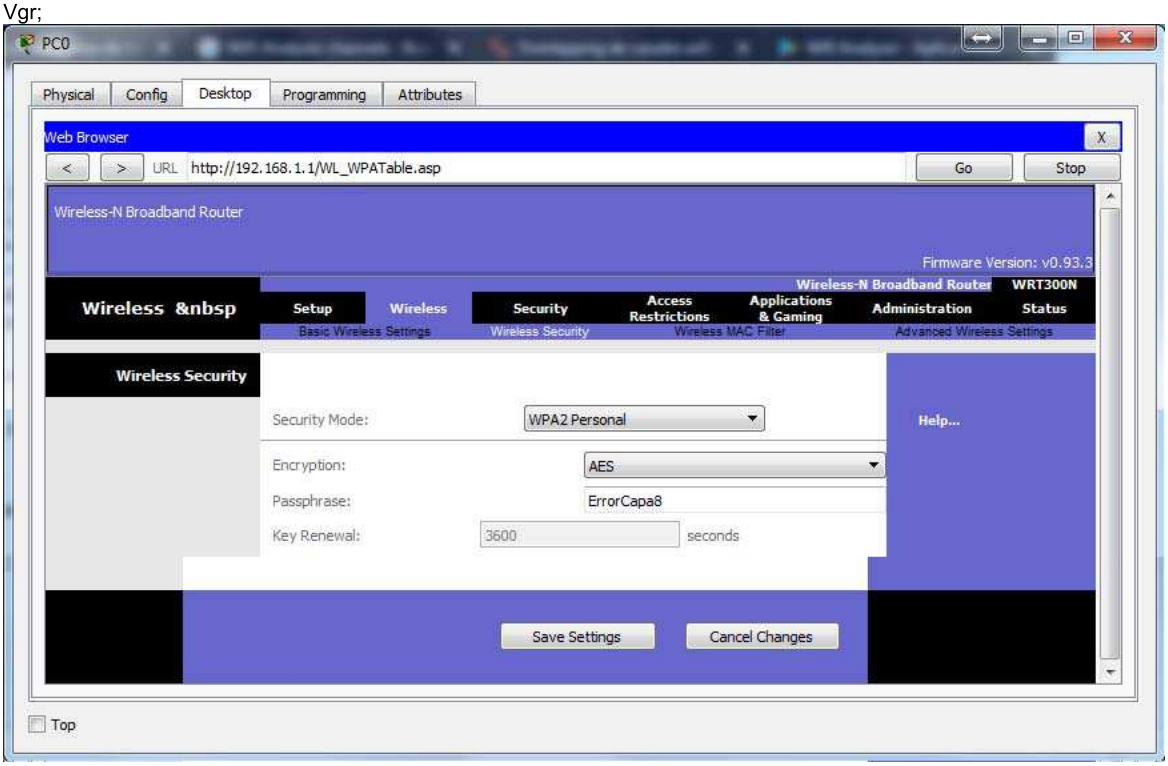


- **Save Settings**: Permite guardar los cambiosrealizados.

- **Seguridad Inalámbrica**: Permite Definir parámetros para controlar quienes tendrán acceso a la red inalámbrica (Wireless / Wireless Security).
  - **WEP**: Seguridad equivalente a cable.
    - Busca emular el hecho de que solo quién posee un cable se puede conectar al switch (Solo quién posee la contraseña se puede conectar al AP).
    - Cifrado, fácil de romper (Cualquiera puede conseguir un cable UTP).
  - **WPA**: Mejora de WEP, mejores prácticas de cifrado. (No tan fácil de romper).
  - **WPA2**: Mejora de WPA, mejores prácticas de cifrado. (Menos fácil de romper).

  - **Personal**: Contraseña que se comparte con los usuarios o clientes de la red.
  - **Enterprise**: Usuarios y contraseñas son administradas por un servidor de autenticación.

- Vgr;



  - **Save Settings**: Permite guardar los cambiosrealizados.

- Actividades Prácticas:
  - Armado de Topología, Direccionar, documentar, enrutar y configurar direccionamiento IPv4 (Incluidas las WLANs) e IPv6 (Excepto WLANs) para la topología de la tierra media.
  - Replicar en P.T. la actividad de Armado y configuración de la topología de la tierra media.

Felices Fiestas