REDES I

Ricardo López Bulla

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Redes I
Ricardo López Bulla
Bogotá D.C.

Fundación Universitaria del Área Andina. 2018

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

Redes I

ISBN (impreso): **978-958-5462-97-7**

Fundación Universitaria del Área Andina
Calle 70 No. 12-55, Bogotá, Colombia
Tel: +57 (1) 7424218 Ext. 1231
Correo electrónico: publicaciones@areandina.edu.co

Director editorial: Eduardo Mora Bejarano
Coordinador editorial: Camilo Andrés Cuéllar Mejía
Corrección de estilo y diagramación: Dirección Nacional de Operaciones Virtuales
Conversión de módulos virtuales: Katherine Medina

BANDERA INSTITUCIONAL

Pablo Oliveros Marmolejo †
Gustavo Eastman Vélez
Miembros Fundadores

Diego Molano Vega
Presidente del Consejo Superior y Asamblea General

José Leonardo Valencia Molano
Rector Nacional
Representante Legal

Martha Patricia Castellanos Saavedra
Vicerrectora Nacional Académica

Jorge Andrés Rubio Peña
Vicerrector Nacional de Crecimiento y Desarrollo

Tatiana Guzmán Granados
Vicerrectora Nacional de Experiencia Areandina

Edgar Orlando Cote Rojas
Rector – Seccional Pereira

Gelca Patricia Gutiérrez Barranco
Rectora – Sede Valledupar

María Angélica Pacheco Chica
Secretaria General

Eduardo Mora Bejarano
Director Nacional de Investigación

Camilo Andrés Cuéllar Mejía
Subdirector Nacional de Publicaciones

REDES I

Ricardo López Bulla

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

ÍNDICE

EJE 1

Introducción 7
Desarrollo Temático 8
Bibliografía 27

EJE 2

Introducción 29
Desarrollo Temático 30
Bibliografía 54

EJE 3

Introducción 57
Desarrollo Temático 58
Bibliografía 72

EJE 4

Introducción 75
Desarrollo Temático 76
Bibliografía 92

REDES I

Ricardo López Bulla

EJE 1

Conceptualicemos

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

INTRODUCCIÓN

El módulo Redes I es una visión inicial al tema de la infraestructura, fundamental como eje de formación ya que, es una de las áreas en las que se requiere mayor número de profesionales en ingeniería de sistemas.

¿Concebir vivir sin redes? ¡Es algo inimaginable! Las redes hacen parte fundamental de nuestro diario vivir y han transformado el mundo entero.

Pensemos... ¿Qué pasaría si un día no tuviéramos, teléfonos, Internet, televisión, energía eléctrica, acueducto, gas, entre otros?, pero ¿qué tienen en común estos servicios?

Durante el desarrollo de este primer eje, trabajaremos los conceptos básicos de redes, su clasificación, tipos de dispositivos, medios de transmisión. Estos conceptos estarán acompañados de lecturas complementarias, videocápsulas, mapas conceptuales, entre otros; además de una actividad de aprendizaje que permite reforzar los conocimientos.

Introducción a redes de datos

Debemos comenzar por entender el significado de red; cuando nos referimos a red de energía, red telefónica, red social, red informática, hacemos referencia a un conjunto de elementos interconectados con un objetivo común.

En el caso particular de una red de datos o red de telecomunicaciones, hablamos de un conjunto de dispositivos electrónicos interconectados con el objetivo de intercambiar información. Este tipo de red requiere tres componentes fundamentales estos son: dispositivos, medios y aplicaciones.

Dispositivos

Estos son los elementos físicos que intervienen en la comunicación hacen parte de lo que se denomina hardware, se clasifica en dispositivos finales o terminales y dispositivos intermediarios. Dichos dispositivos pueden ser:

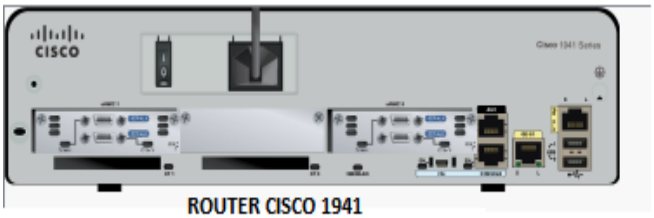
Hardware
hace referencia a la parte física o tangible

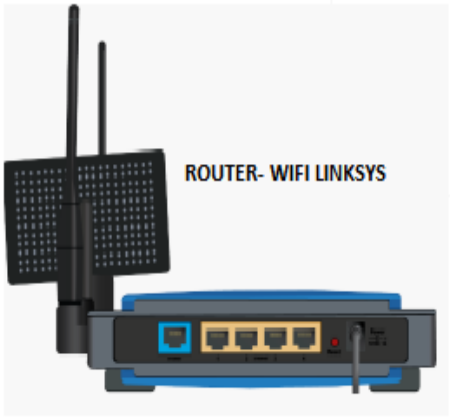
1. **Equipos terminales:**

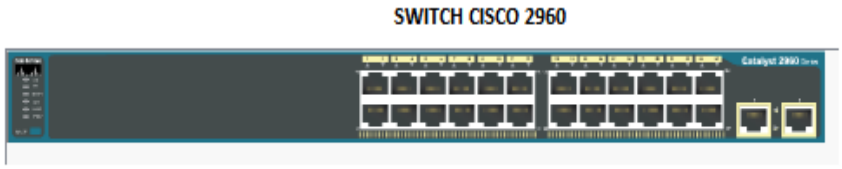
Figura 1. Dispositivos finales
Fuente: propia

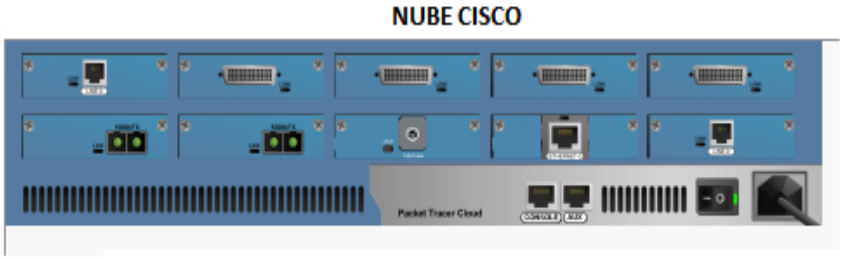
Dispositivos que son el origen o destino del mensaje y requieren un identificador para poder enviar o recibir la información. dentro de estos dispositivos tenemos portátiles, PC, PDA, teléfonos, *smartphone*, entre otros.

2. Equipos intermediarios: son aquellos dispositivos que permiten interconectar los equipos terminales a la red y proporcionan interconectividad y flujo de datos, ejemplo de estos son: *switch*, *router*, AP (*Access Point*).









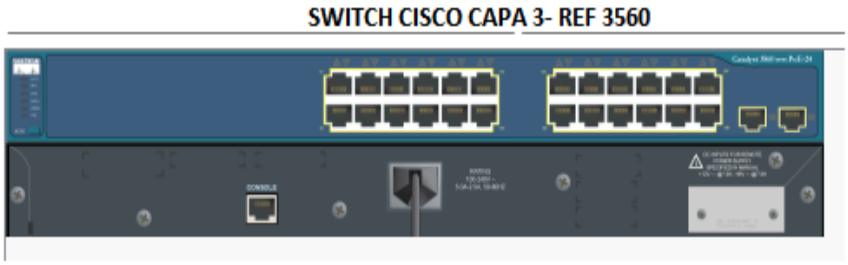


Figura 2. Dispositivos Intermediarios
Fuente: propia

Medios

Son los elementos encargados de conectar los equipos terminales con los equipos intermediarios, por ellos viaja la información; los principales medios son hilos de cobre (par de cobre, par trenzado, coaxial), fibra óptica (hilo de vidrio o plástico), y señales inalámbricas, es decir aquella que no necesitan de un medio físico para interconectar los dispositivos (radio frecuencia RF, infrarrojo, *Bluetooth*).

Aplicaciones son los programas, parte lógica que permite la interacción con el usuario se le denomina software, ejemplo de esto (*Office, Paint, Windows,* entre otros).

Software
Parte lógica, conjunto de rutinas que cumplen una tarea, también llamado, programas o aplicaciones.

Figura 3. Medios de conexión
Fuente: propia

Clasificación de las redes

Instrucción

Veamos el mapa conceptual con un panorama general de la clasificación de las redes. Este mapa se encuentra en los recursos de aprendizaje del eje.

Ahora bien, las redes se pueden clasificar de diversas formas no existe una unificación en este tema, para entendimiento del mismo las clasificamos por:

Por su alcance o cobertura: hace referencia a la distancia física de su alcance dentro de estas tenemos:

- **PAN (*Personal Area Network*):** es una red de área personal que se caracteriza por tener conexión punto a punto y un alcance no superior a 10 metros, ejemplo de esta seria a un teléfono celular conectado por cable a computador, también una conexión Bluetooth entre dos dispositivos terminales.

- **LAN (*Local Area Network*):** es una red de área local que se caracteriza por interconectar varios dispositivos terminales con la ayuda de un dispositivo intermediario comúnmente un switch o un router wifi su alcance no supera los 100 metros. Es la red más utilizada a nivel hogar y empresa.

- **CAN (*Campus Area Network*):** red de área de campus encargada de interconectar varias redes LAN pertenecientes a una universidad, empresa, en una extensión geográfica limitada.

- **MAN (*Metropolitan Area Network*):** red de área metropolitana que se encarga de conectar redes diversas CAN a alta velocidad en un área geográficamente extensa como una ciudad.

- **WAN (*Wide Area Network*):** redes de área extensa multiplataforma, capaz de conectar al mundo, la red pública más común en esta categoría es Internet, pero pueden crearse redes WAN privadas.

Por su relación funcional: según su relación funcional tenemos:

- **Peer to Peer (de igual a igual):** en la cual no existe un ente que domine, organice, regule el tráfico, la información, la seguridad. Todas las máquinas son independientes, el ejemplo más claro de este es un grupo de trabajo donde cada máquina actúa de forma autónoma.

- **Cliente–servidor:** red en la cual existe una jerarquía, es decir se tiene un ente central que controla, regula, asegura, el acceso a la información y solamente se actúa con permiso de este. Ejemplo un directorio activo desde el cual se generan políticas administrativas a la red.

Por la direccionalidad de los datos: esta clasificación hace referencia al modo en que viajan los datos por la red, y lo podemos clasificar en:

- **Modo simplex:** los datos viajan en una única dirección y un único sentido, existe un emisor y muchos receptores, los receptores no pueden interactuar con el emisor por el mismo medio. Ejemplo de esta red es la televisión y la radio.

- **Modo dúplex:** el emisor y receptor pueden interactuar por el mismo medio y dependiendo de la interacción este modo dúplex se subdivide en:

    - ***Half-Duplex*:** se puede interactuar, pero no simultáneamente es decir o se emite o se recibe información, pero no al mismo tiempo. Ejemplo de este tipo de red es la radiotelefonía utilizada por las empresas de taxis, la policía y entidades de emergencia. La gran ventaja de este tipo de red es que es de multidifusión, también las redes wifi utilizan este modo de comunicación.

    - ***Full-Duplex*:** en este tipo de red la interacción es simultánea se puede enviar y recibir información al mismo tiempo. Ejemplo de este tipo de comunicación es la telefonía, los PC conectados por medio físico, el Internet, entre otros.

Por el tipo de conexión: se clasifican según la manera en que se conectan los dispositivos terminales a los dispositivos intermediarios y entre ellos, puede ser:

- **Medios guiados:** cuando las señales se transportan por un medio físico (coaxial, UTP, fibra, par de cobre).

- **Medios no guiados:** cuando la señal se transporta por el aire, por medio de ondas o señales (radio frecuencia, micro ondas, infrarrojo, *Bluetooth*).

Para fortalecer los conceptos se recomienda que consulte el siguiente libro, específicamente el capítulo 2 Introducción a las redes:

Visitar página

Redes: diseño, actualización y reparación.

goo.gl/5yK2WG

Gastón Carlos Hillar.

Por topología: describe la forma como se conectan los dispositivos terminales a la red, la distribución de cables y las conexiones a dispositivos intermediarios pueden ser anillo, bus, estrella, malla, árbol, entre otras.

La figura topología física, describe la ubicación de dispositivos terminales e intermediarios en la red:

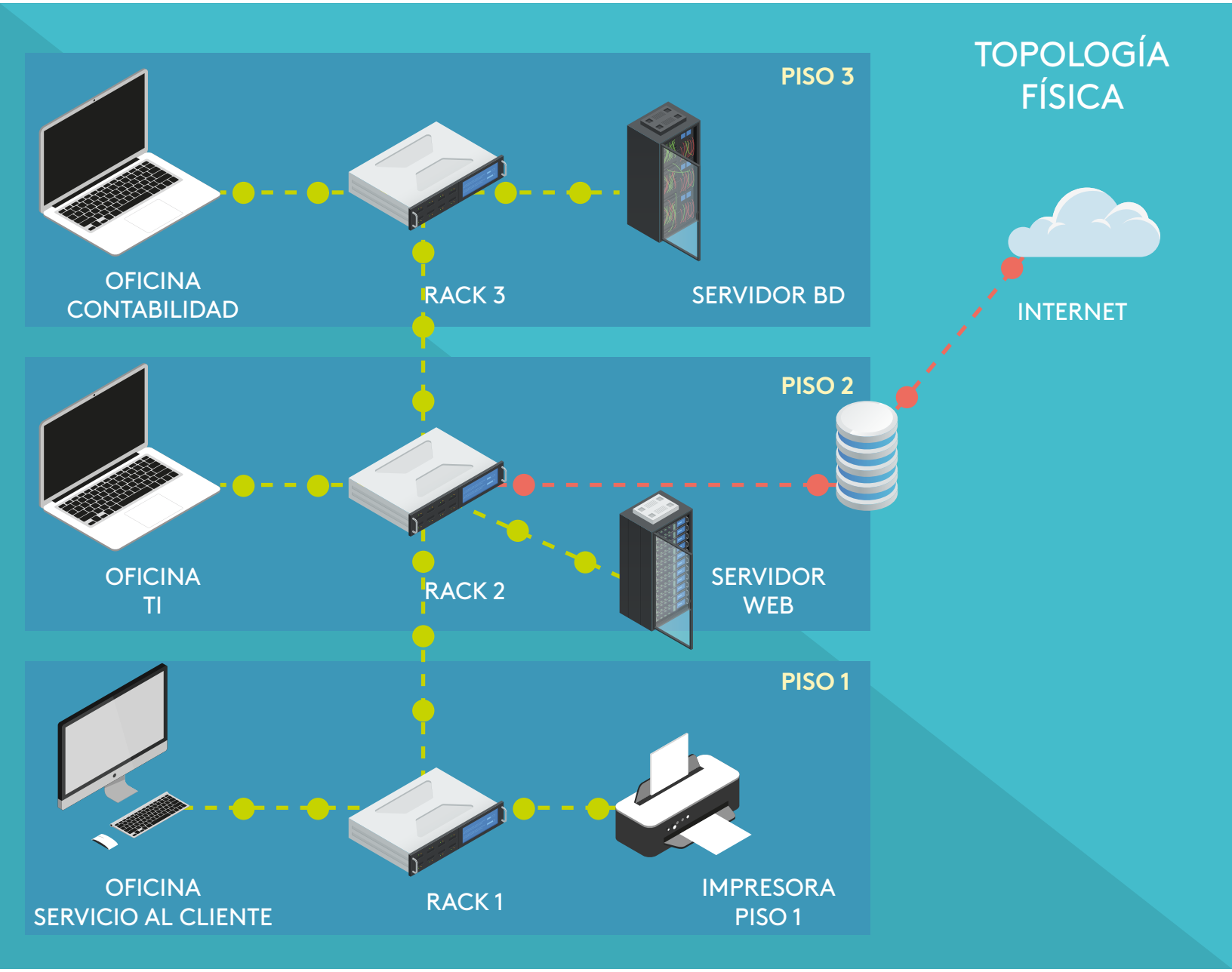


Figura 4. Topología física
Fuente: propia

La figura topología lógica describe el esquema de direccionamiento y los puertos a los que está conectado cada dispositivo.

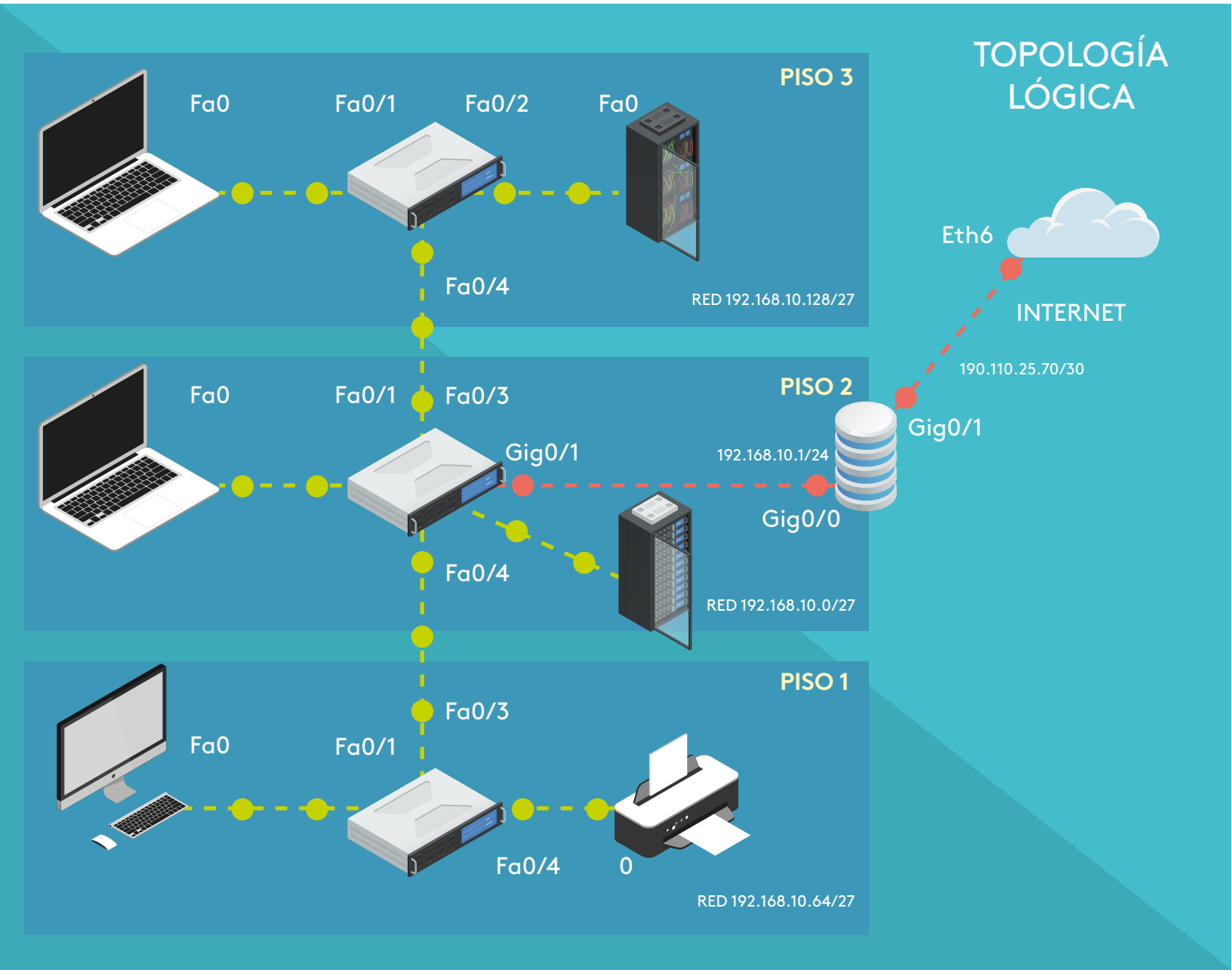


Figura 5. Topología lógica
Fuente: propia

Modelos de comunicación

Para empezar, veamos la videocápsula:

Video

Modelo de referencia OSI.

youtu.be/RiQnT36Kawo

El modelo de referencia usado para la comunicación de las redes es el modelo OSI (*Open Systems Interconnection*) es un modelo que describe la comunicación por medio de una pila de protocolos, formado por 7 capas, cada una de ellas dependiente de la capa anterior y ligada a la capa posterior, como bien se indica es un modelo de referencia no configurable, ni aplicable a ningún sistema.

¡Tengamos en cuenta!

En la actualidad se habla de capa 8, la cual hace referencia al error humano, pero esto no es estandarizado ni aprobado por la ISO.

El modelo que aplicaremos será entonces el modelo TCP/IP el cual se conoce con el nombre de modelo de Internet, trabaja con una pila de protocolos de cuatro capas relacionadas directamente con el modelo OSI, el modelo TCP/IP es el más popular en la configuración de sistemas de comunicación.

Figura 6. Comparación modelo OSI vs Modelo TCP/IP
Fuente: propia

Capa de acceso a la red (TCP/IP)

Esta capa de acceso a la red del modelo TCP/IP comprende la capa física del modelo OSI en la cual se define las especificaciones eléctricas, la transmisión de bit, las señales y los medios que se utilizan para dicha transmisión, como también las características de *hardware* necesarias para la red.

Los protocolos utilizados en esta capa son *Ethernet* IEEE802.3, *token ring* IEEE802.5, FDDI, entre otros.

La capa de acceso también abarca la capa de enlace de datos del modelo OSI, la cual se encarga del direccionamiento lógico es decir la dirección MAC, y de la sub capa LLC.

Los protocolos de esta capa PPP e IEEE802.2

Para ampliar esta información, les invitamos a visitar el siguiente sitio web:

MAC
Media Access Control, es el identificador único asignado por el fabricante a un dispositivo.

LLC
Logical Link Control, control de enlace lógico, define la forma que los datos son transferidos por el medio físico.

Visitar página

Protocolo Ethernet. goo.gl/W79Cko

Cisco Networking Academy.

Sistemas de conversión binaria, decimal y hexadecimal

La información en sistema informático se transmite mediante bit (*Binary digit*) el cual se define como la unidad mínima de información, el bit solo puede tener dos valores (0, 1) por tal motivo, toda información debe convertirse a sistema binario para ser transportada. La conversión de decimal a binario se puede dar con divisiones sucesivas:

Veamos una videocápsula sobre la conversión de sistemas de numeración:

Video

Conversión de sistemas de numeración.

youtu.be/l6uSJdm-uus

Ejemplo:

24 (decimal) convertirlo en binario

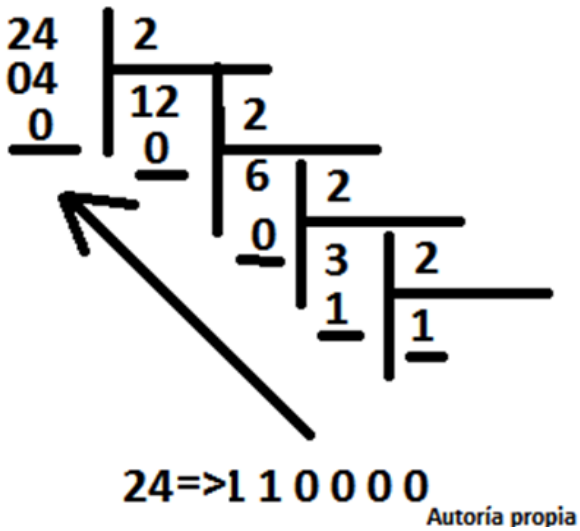


Figura 7. Conversión a binario
Fuente: propia

Pero existe una manera más práctica y fácil de realizar dicha conversión sin necesidad de desarrollar divisiones sucesivas, veamos a continuación.

Conversión binaria a decimal

Ejemplo 1: convertir el número binario 11111111 a decimal.

Decimal	128	64	32	16	8	4	2	1
Potencia	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binario	1	1	1	1	1	1	1	1

Tabla 1. Tabla de conversión binario a decimal y decimal a binario
Fuente: Propia

Pasos:

1. Realizamos la tabla de conversión.

2. Colocamos el número binario que queramos convertir.

3. Realizamos la suma de las casillas decimales que se encuentren encendidas (en 1) en la correspondiente casilla binario.

Para el ejemplo, como todas las casillas binarias están encendidas (en 1), sumaremos todos los valores decimales:

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255.

Esto quiere decir que el valor binario 11111111 corresponde al decimal 255.

Ejemplo 2: convertir el número binario 10001101 a decimal.

Decimal	128	64	32	16	8	4	2	1
Potencia	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binario	1	0	0	0	1	1	0	1

Tabla 2. Tabla de conversión a decimal número específico
Fuente: propia

Aplicamos los pasos mencionados, para este ejemplo sumaremos las casillas decimales que se encuentren encendidas (en 1) en la correspondiente casilla binaria.

128 + 8 + 4 + 1 = 141 quiere decir que 141 equivale a 10001101.

Conversión decimal a binario

De forma inversa si tenemos un valor decimal y lo queremos convertir en binario.

Ejemplo 160 convertirlo a binario.

Decimal	128	64	32	16	8	4	2	1
Potencia	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binario	1	0	1	0	0	0	0	0

Tabla 3. Tabla de conversión decimal a binario número específico
Fuente: propia

Pasos

1. Comenzamos encendiendo el valor binario más cercano por debajo al número decimal, para nuestro caso 128 es decir encendemos el primer bit.

2. Luego sumamos el bit adyacente 64 => 128 + 64 = 192, como el valor sobrepasa al número buscado apagamos el segundo bit y encendemos el tercero y repetimos la acción. 128 + 32 = 160 con este valor obtenemos el número buscado entonces encendemos dicho bit y todos los demás quedarán apagados.

160 decimales equivalen a 10100000.

Conversión hexadecimal a binario

El sistema hexadecimal está formado por 16 dígitos los cuales van del 0 - 9 y de la letra A, a la F, en donde A = 10; B = 11; C = 12; D = 13; E = 14; F = 15.

Como se requieren 16 dígitos, se necesitan 4 bit para abarcar todos los posibles valores entonces tendríamos:

Convertir la letra F a binario => como la letra F equivale a 15, comenzamos encendiendo el valor binario más cercano por debajo al número decimal, para nuestro caso 8, luego sumamos el bit adyacente => 8 + 4 = 12 como nos sirve encendemos ese segundo bit, luego prendemos el adyacente => 8 + 4 + 2 = 14 como nos sirve encendemos este bit y sumamos el siguiente adyacente => 8 + 4 + 2 + 1 = 15 con este valor obtenemos el valor buscado, entonces también se enciende y queda como resultado F = 15 (decimal) equivale a 1111 en binario.

Decimal	8	4	2	1
Potencia	2^3	2^2	2^1	2^0
Binario	1	1	1	1

Tabla 4. Tabla de conversión binario a hexadecimal y hexadecimal a binario
Fuente: propia

Instrucción

A este punto les invitamos a desarrollar la actividad de repaso 1.

Organizaciones de estandarización

Para empezar, veamos una videocápsula sobre la normatividad en redes:

Video

Redes - Normatividad de redes.

youtu.be/qYTic5l9o7o

Los estándares abiertos fomentan la interoperabilidad de los diversos dispositivos, la creación de múltiples marcas, la innovación tecnológica, garantizando la sana competencia y el no monopolio. La importancia de conocer los estándares y las entidades certificadoras es que al momento de adquirir un equipo, cables u otros dispositivos verifiquemos que estos son compatibles.

Existen organizaciones de estandarización en el área de redes y telecomunicaciones:

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), entidad encargada de elaborar estándares para equipos que utilizan sistemas eléctricos y/o electrónicos. En el área de las redes y comunicaciones el principal estándar es IEEE 802 del cual se destacan:

- IEEE802.2 LLC.
- IEEE802.3 *Ethernet*.
- IEEE802.11 *Wireless* LAN Wifi.
- IEEE802.15 *Wireless PAN Bluetooth*.
- IEEE802.16 *BroadBand Wireless Wi-Max*.
- IEEE802.18 Normativa de radio.
- IEEE802.24 Grupo de asesoría técnica sobre redes inteligentes.

IEEE802
Número de estándar asignado a normalizar estándares de redes de datos y comunicaciones.

EIA (Asociación Industrial Electrónica). Encargada de estandarizar el cableado eléctrico y de datos.

TIA (Asociación Industrias de las Telecomunicaciones). Responsable de desarrollar estándares de comunicación.

UIT-T (Unión Internacional de Telecomunicaciones). Define estándares para la comunicación de banda ancha.

ISOC (Sociedad de Internet). Promueve el uso de Internet Abierto.

IAB (Consejo de Arquitectura de Internet). Responsable del desarrollo de estándares de Internet.

IETF (Grupo de Trabajo de Ingeniería de Internet). Desarrolla y mantiene actualiza las tecnologías de Internet.

IRTF (Grupo de Trabajo de Investigación de Internet). Encargado de investigar los protocolos de Internet a largo plazo.

ICCAN (Corporación de Internet para la Asignación de Nombre y Números), coordina la asignación de direcciones IP, nombres de dominios, e información de TCP/IP.

IANA (Autoridad de Números Asignados de Internet). Encargada de administrar y supervisar la asignación de direcciones IP y nombres de dominio.

Tenga en cuenta que: los estándares de capa física se implementan en el *hardware* (IEEE, TIA/EIA, ANSI, ISO), mientras los estándares TCP/IP se implementan en el *software* y los rige la IETF.

Medios de red

Las redes pueden utilizar diversos medios de comunicación cuando estos son guiados se suele utilizar, fibra óptica, par de cobre, UTP y coaxial. Veamos cada uno de ellos:

Fibra óptica

Es un hilo de vidrio que permite transmitir impulsos de luz a altas velocidades y con la ventaja de ser totalmente inmune a EMI (interferencia electromagnética) y a RFI (interferencia de radiofrecuencia), se utiliza para conexiones troncales interconectando dispositivos de red, en la actualidad se ofrecen redes GPON llegando la fibra hasta al abonado final.

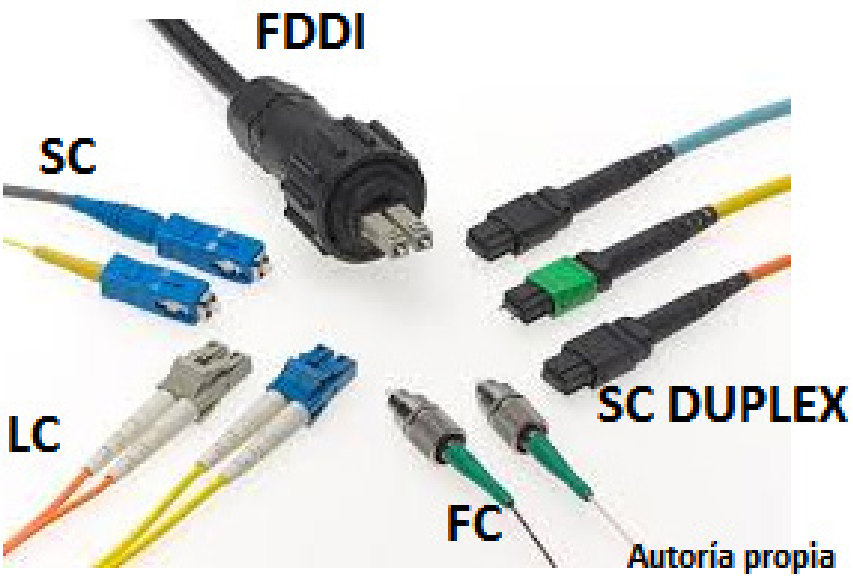


Figura 8. Conectores fibra óptica
Autoría Propia

Par de cobre

Este es un cable ampliamente utilizado en las redes de telecomunicaciones, gracias a sus características especiales para transportar señales eléctricas a alta frecuencia, en la actualidad ha venido siendo reemplazado paulatinamente por la fibra óptica gracias a las mejoras de calidad de esta última.

Cable coaxial

El cable coaxial está formado por un hilo central de cobre (conductor eléctrico), utilizado para la transmisión de señales eléctricas, recubierto de una capa plástica aislante, encima de esta una malla de cobre tejida que actuará como blindaje del conductor eléctrico, por último, en su envoltura exterior se recubre con polímero que evitará daños menores.

Figura 9. Cable coaxial
Fuente: propia

En la actualidad el cable coaxial se utiliza para conectar las redes de televisión, las instalaciones de Internet por cable, al igual que las antenas de redes inalámbricas.

Cable UTP

Le invitamos a ver una videocápsula sobre cómo hacer cable *Ethernet* Rj45:

Video

Cómo hacer cable Ethernet Rj45.

youtu.be/gPWI9CagoFw

El cable par trenzado comúnmente utilizado en redes LAN, está formado por 8 hilos los cuales se encuentran trenzados en pares con diferente grado de torsión de acuerdo a la función que cumple cada par, alcanza una distancia máxima de 100 metros y está regido por la norma TIA/EIA 568B (estándar de cableado estructurado en edificios comerciales) dentro de sus características tiene la asignación de pines en cables de 8 hilos UTP denominada T568A y T568B. El trenzado de los cables reduce o cancela la EMI interferencia electromagnética.

Color	Función
Blanco/Naranja y Naranja	Encargado de enviar o recibir información
Blanco/Verde y verde	Encargado de enviar o recibir información
Blanco/Azul y Azul	Neutro -bidireccional
Blanco/Café y Café	Tierra- bidireccional

Tabla 5. Tabla de función por color de cable UTP
Fuente: propia

Número de Pin	Función
1	Tx - transmite
2	Tx - transmite
3	Rx - Recibe
4	BDD+
5	BDD-
6	Rx - Recibe
7	BDD+
8	BDD-

Tabla 6. Tabla de función de cada color de cable UTP
Fuente: propia

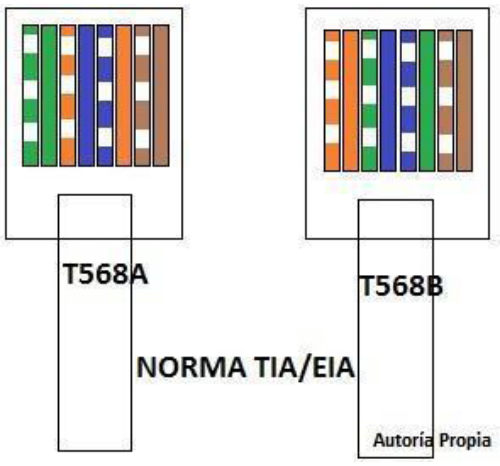


Figura 10. Norma de colores TIA/EIA 568
Fuente: propia

BIBLIOGRAFÍA

Bellido, Q. (2014). *Equipos de interconexión y servicios de red (UF1879)*. Madrid, España: IC Editorial.

Bermúdez, L. (2012). *Montaje de infraestructuras de redes locales de datos: UF1121*. Madrid, España: IC Editorial.

Boronat, S., y Montagud, C. (2013). *Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF*. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Calvo, G. (2014). *Gestión de redes telemáticas (UF1880)*. Madrid, España: IC Editorial.

Feria, G. (2009). *Modelo OSI*. Córdoba, Argentina: El Cid Editor | apuntes.

García, M. (2012). *Mantenimiento de infraestructuras de redes locales de datos (MF0600_2)*. Málaga, España: IC Editorial.

Hillar, G. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana HASA.

Íñigo, G., Barceló, O., y Cerdà, A. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.

Martínez, Y., y Riaño, V. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.

Molina, R. (2014). *Implantación de los elementos de la red local*. Madrid, España: RA-MA Editorial.

Mora, J. (2014). *Desarrollo del proyecto de la red telemática (UF1870)*. Madrid, España: IC Editorial.

Purser, M. (1990). *Redes de telecomunicación y ordenadores*. Madrid, España: Ediciones Díaz de Santos.

Roa, B. (2013). *Seguridad informática*. Madrid, España: McGraw-Hill España.

Robledo, S. (2002). Redes de computadoras. Ciudad de México, México: Instituto Politécnico Nacional.

Romero, J. (2009). *Estudio de subnetting, VLSM, Cidr y comandos de administración y configuración de routers*. Córdoba, Argentina: El Cid Editor | Apuntes.

S.L. Innovación y Cualificación. (2012). *Guía para el docente y solucionarios: montaje y mantenimiento de sistemas de telefonía e infraestructuras de redes locales de datos*. Málaga, España: IC Editorial.

Vásquez, D. (2009). *Base de la teleinformática*. Córdoba, Argentina: El Cid Editor | apuntes.

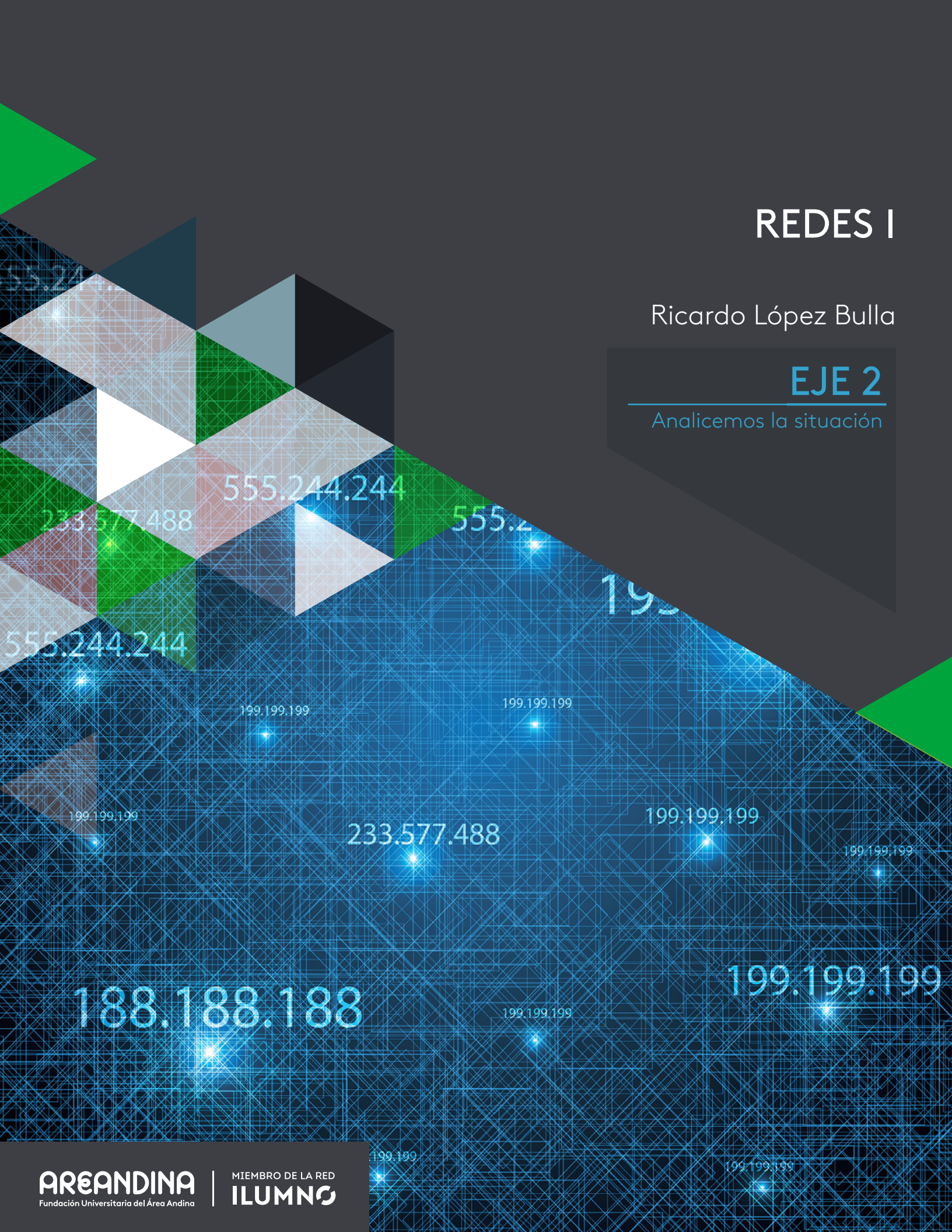
Velte, T., y Velte, A. (2008). *Manual de Cisco*. Ciudad de México, México: McGraw-Hill Interamericana.

REDES I

Ricardo López Bulla

EJE 2

Analicemos la situación



AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

INTRODUCCIÓN

El direccionamiento IP es el elemento fundamental de la comunicación entre dispositivos, cada dispositivo que se conecta a la red debe tener una dirección que le permitirá acceder a esta.

Pero entonces.... ¿cuál es mi dirección?, ¿quién me asigna la dirección?, ¿qué dirección debe utilizarse?, ¿cuántas direcciones requiero si me conecto desde diversas redes?

En el desarrollo de este eje trataremos los aspectos más relevantes respecto al direccionamiento IPv4 e IPv6, acompañado de lecturas complementarias, videocápsulas y una actividad de refuerzo.

Aspectos importantes sobre las redes de datos

Capa de Internet (TCP/IP)

La capa de Internet del modelo TCP/IP es equivalente a la capa de red (capa 3) del modelo OSI ya que, cumplen las mismas funciones.

Esta capa se encarga de cuatro funciones básicas:

- Direccionamiento lógico,
- empaquetamiento de la PDU,
- enrutamiento de los paquetes y
- desencapsulamiento de los mismos.

Direccionamiento lógico: es el proceso de asignar una dirección IP (*Internet Protocol*) única, a cada terminal que se conecta a la red.

Empaquetamiento: es el proceso de encapsular la unidad de datos del protocolo (PDU) que llega de la capa de transporte, agregando encabezado de protocolo IP, la dirección de origen y la dirección de destino.

Para ampliar el tema le invitamos a visitar el siguiente sitio:

Visitar página

Movimiento de datos en la red. https://goo.gl/swTSKE
Cisco Networking Academy.

Figura 1. PDU capa de red
Fuente: propia

Enrutamiento de paquetes: esta capa gestiona el envío de paquetes de una red a otra diferente, para dicho proceso se requiere un dispositivo (capa 3) denominado *router*, el cual tiene la capacidad de reconocer todas las rutas posibles y seleccionar la mejor ruta.

Desencapsulamiento: en esta capa se genera el proceso inverso al encapsulamiento. Cuando el paquete llega al destino la capa de red se encarga de retirar la cabecera IP.

Ahora bien, ahondemos en el direccionamiento lógico.

La dirección lógica se denomina IP (Protocolo de Internet) y es la que permite que los dispositivos terminales puedan conectarse a determinada red.

Toda dirección IP está formada por dos partes, una parte que identifica la red y otra que identifica los *hosts* (dispositivos terminales).

Figura 2. Formato IPv4, Formato IPv6
Fuente: propia

Se han desarrollado dos protocolos de direccionamiento IP la versión IPv4 y la versión IPv6.

Direccionamiento IPv4

Para empezar, veamos la videocápsula sobre direccionamiento IPv4:

Video

Direccionamiento IP. https://youtu.be/2e_8eTzgWow

La dirección IPv4 o protocolo de Internet versión 4 es un valor numérico de 32 bit lo que significa que el número máximo de direcciones IPv4 = 2^{32} = 4.294.967.296, es decir un poco más de 4 mil millones de direcciones.

Tenga en cuenta: aunque exista una cantidad muy grande de direcciones IPv4. El crecimiento exponencial de Internet y de dispositivos móviles conectados a la web generó el agotamiento de las mismas. En año 2011 la IANA, entidad encargada de la administración de direcciones IP en el mundo, anunció el agotamiento de las direcciones IPv4.

IANA
Internet Assigned Numbers Authority.

Las direcciones IPv4 se representan con cuatro grupos de 8 bit lo que se denomina "cuatro octetos" y a su representación decimal se le denomina "decimal punteada" ya que se representa por cuatro grupos de números decimales separados por un punto.

Ejemplo

Representación binaria de la dirección IPv4 (cuatro grupos de ocho bits).

11111111 10101000 00010100 11111100

Representación decimal puntada dirección IPv4.

192. 168. 20. 252

Para reafirmar el conocimiento los invito a generar análisis de un libro que pueden encontrar en la siguiente dirección:

Visitar página

Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. https://goo.gl/Ut3U6q

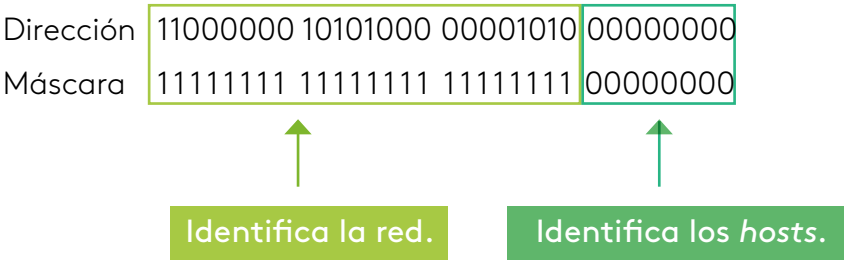
Fernando Boronat Seguí y Mario Montagud Climent.

Leer especialmente el capítulo 2 La Familia de Protocolos TCP/IP.

Máscara de red

Es una combinación de bits agrupados que van a determinar que parte de la dirección de IPv4 es quien identifica la red y que parte identifica los *hosts*, la máscara de red se representa por cuatro octetos, los cuales tomarán el valor de uno de aquellos que representen la red y el valor de cero los bits que representan los *hosts*. Es importante aclarar que los bits que representan la red, deben ser consecutivos adyacentes en su encendido, el cual se dará de izquierda a derecha.

Ejemplo en binario:



Mismo ejemplo en notación decimal punteado:

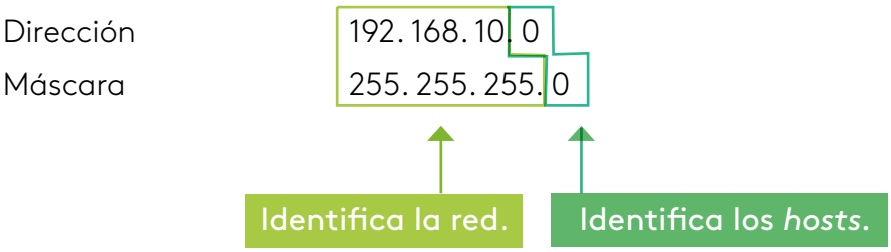


Figura 3.
Fuente: propia

Si analizamos la dirección y la máscara del ejemplo anterior, observamos que los bits de los tres primeros octetos de la máscara están encendidos (1) como la máscara es quien define la red, quiere decir que la red está representada por los tres primeros octetos, de aquí podemos enunciar una primera ley "Para que dos máquinas se vean deben estar en la misma red o el mismo segmento de red".

Analicemos: ¿las siguientes direcciones hacen parte de la misma red? y ¿por qué?

Host 1	Representación IPv4 binario	IPv4 decimal
Dirección	10101100 00010000 11100011 10100010	172. 16 .227.162
Mascara	11111111 11111111 00000000 00000000	255. 255. 0. 0

Host 2	Representación IPv4 binario	IPv4 decimal
Dirección	10101100 00011000 11100011 10101100	172. 24 .227.162
Mascara	11111111 11111111 00000000 00000000	255. 255. 0. 0

Tabla 1. Direcciones de red IPv4
Fuente: propia

A simple vista es difícil dar una respuesta a esta pregunta, pero si realizamos la operación AND entre la dirección IPv4 y la máscara de esa dirección se obtendrá la red a la que pertenece dicha dirección.

Atención:

La operación AND compara los dos números binarios por columna, si los dos valores son 1(uno), el resultado es 1(uno), pero si alguno de los valores o los dos valores son 0(cero) el resultado es 0(cero), el valor resultante de toda la operación es el identificador de red.

Instrucción

A este punto le invitamos a desarrollar la actividad de repaso 1, Descubriendo máquinas en la red. Operadores AND.

Host 1	Representación IPv4 binario	IPv4 decimal
Dirección	10101100 00010000 11100011 10100010	172. 16 .227.162
Mascara	11111111 11111111 00000000 00000000	255. 255. 0. 0
AND	10101100 00010000 00000000 00000000	172.16. 0. 0

Host 2	Representación IPv4 binario	IPv4 decimal
Dirección	10101100 00011000 11100011 10101100	172. 24 .227.162
Mascara	11111111 11111111 00000000 00000000	255. 255. 0. 0
AND	10101100 00011000 00000000 00000000	172. 24. 0. 0

Tabla 2. Direcciones de red IPv4 operación AND
Fuente: propia

De la operación anterior podemos concluir que las direcciones de host dadas se encuentran en diferente red, la primera pertenece a la red 172.16.0.0 y la segunda a la 172.24.0.0

Clases

Debido a la gran cantidad de direcciones IPv4 que existente (4.294.967.296) se hizo necesaria la agrupación de direcciones con características similares a lo que se le denominó clase. Dichas clases permiten generar redes de diversos tamaños asignado un determinado número de bit a la red y otro grupo de bit para identificar el *host*.

En el siguiente cuadro podemos observar la clase, la característica común de la clase, el rango de direcciones, la máscara o prefijo, el número de red en cada clase y el número de host en la misma.

Clase	Bit de mayor peso	Inicio rango	Fin - rango	Mascara y prefijo o número de bit asignados a la red	Número de redes	Número de dispositivos terminales
A	0	1.1.1.1	127.255.255.255	255.0.0.0 /8	126	16`777.214
B	10	128.0.0.0	192.255.255.255	255.255.0.0/16	16.384	65.534
C	110	192.168.0.1	223.255.255.255	255.255.255.0/24	2´097.152	254
D	1110	224.0.0.0	239.255.255.255	---	---	----
E	11110	240.0.0.0	255.255.2555.255	---	---	----

Tabla 3. Clases direcciones IPv4
Fuente: propia

Redes clase A

Si analizamos en binario cualquier dirección del rango de la clase A. ¿Qué tienen en común estas direcciones?

Valor decimal clase A	Valor binario clase A
1	0 0 0 0 0 0 0 1
60	0 0 1 1 1 1 0 0
100	0 1 1 0 0 1 0 0
120	0 1 1 1 1 0 0 0
127	0 1 1 1 1 1 1 1

Tabla 4. Rango clase A - direcciones IPv4
Fuente: propia

En la clase **A** todas las direcciones van tener el primer bit apagado es decir en valor 0 (cero) y esa es su característica común, además su máscara va estar definida por el primer octeto, esto quiere decir que la red va a definirse en el primer octeto (/8) los demás octetos serán asignados a *host*.

Determinando la red en una dirección clase A por medio de operador AND:

Clase A	Representación binario	decimal
Dirección host	00001010 10101101 00010010 00100000	10.173.18.32
Mascara	11111111 00000000 00000000 00000000	255. 0. 0. 0
AND = ID RED	00001010 00000000 00000000 00000000	10. 0. 0. 0

Tabla 5. Rango clase A - direcciones IPv4 -AND
Fuente: propia

La red que se obtiene como resultado de la operación AND es 10.0.0.0 con mascara 255.0.0.0 (también se puede representar como 10.0.0.0/8).

Otro elemento que podemos concluir es que en la clase **A** tenemos 126 redes disponibles y cada red dispone de 2^{24} - 2 direcciones IPv4, es decir 16´777.216 direcciones.

Tenga en cuenta: se habla de 126 redes (aunque en la realidad son 127) lo que pasa es que existe el rango de dirección 127.X.X.X que está reservado para pruebas con la misma máquina y se le denomina dirección de loopback o interfaz de red virtual, dicho rango no se puede asignar a ninguna red pública ni privada, pero si se pueden generar interfaz loopback con direcciones locales y/o públicas.

El mayor inconveniente de las redes clase **A** es la gran cantidad de direcciones IPv4 que asignan, lo cual genera complejidad en su gestión, administración y causa un dominio de *broadcast* tan grande que vuelve inoperante la red.

Dominio de *broadcast*
O dominio de difusión de una red, es el área de la red en el que un dispositivo terminal puede transmitir sin depender de un *router*.

Le invitamos a ver la videocápsula sobre dominios de *broadcast*:

Video

Dominios de broadcast. https://youtu.be/oM5ntlgb2B4

Otro problema es el número de direcciones desperdiciadas, pues no existe ninguna red empresarial que necesite los más de 16 millones de direcciones que ofrece, por tal motivo en la actualidad es improbable encontrar una red clase **A**.

Redes clase B

Tomemos al azar algunas direcciones clase B y analicemos los elementos en común:

Valor decimal clase B	Valor binario clase B
128	1 0 0 0 0 0 0 0
150	1 0 0 1 0 1 1 0
173	1 0 1 0 1 1 0 1
185	1 0 1 1 1 0 0 1
191	1 0 1 1 1 1 1 1

Tabla 6. Rango clase B - direcciones IPv4
Fuente: propia

Determinamos entonces que los bits comunes en las redes clase **B** son los dos primeros, ya que el primer bit esta encendido (1) y el segundo bit está apagado (0) en todas las direcciones del segmento clase B, al igual la máscara que define la red clase **B** que va a estar formada por los primeros 16 bits (/16) es decir los dos primeros octetos.

Determinando la red en una dirección clase B por medio de operador AND:

Clase B	Representación binario	decimal
Dirección *host*	10010110 00100000 00010010 10111111	150. 33.18.191
Mascara	11111111 11111111 00000000 00000000	255.255. 0. 0
AND= ID RED	10010110 00100000 00000000 00000000	150. 33. 0. 0

Tabla 7. Rango clase B - direcciones IPv4 - AND
Fuente: propia

La red resultante es la 150.33.0.0 con mascara 255.255.0.0 (150.33.0.0/16).

De la tabla anterior también concluimos que tenemos disponible 16.384 redes y que cada red puede albergar una cantidad de 2^{16} - 2 *host* es decir 65.535 dispositivos.

En clase B existe un rango denominado *Link* Local (de enlace local) el cual por medio del procedimiento Apipa de Windows asigna una dirección de forma automática cuando no existe un servidor DHCP, esta dirección **no** es enrutable y su rango es 169.254.X.X

Apipa
Automatic Private IP Addressing, es la dirección que se asigna automáticamente cuando no hay un servidor DHCP disponible. El rango es 169.254.1.0 a 169.254.254.255. Esta dirección no es enrutable.

DHCP
Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host, asigna de forma dinámica direcciones IP.

Instrucción

A este punto, le invitamos a desarrollar la actividad de repaso 2.

Redes clase C

Las redes clase C son el tipo de red más común en la actualidad a nivel de hogares y oficinas pequeñas ¿Por qué?

Analicemos lo común de las redes clase C.

Valor decimal clase C	Valor binario clase C
192	1 1 0 0 0 0 0 0
200	1 1 0 0 1 0 0 0
207	1 1 0 0 1 1 1 1
219	1 1 0 1 1 0 1 1
223	1 1 0 1 1 1 1 1

Tabla 8. Rango clase C - direcciones IPv4
Fuente: propia

Lo común en la clase C son los 3 primeros bits, los dos primeros están encendidos (1) y el tercero está apagado (0).

La máscara de red de la clase C está dada por los tres primeros octetos de la misma, es decir la red se va definir a 24 bits (/24).

Determinando la red en una dirección clase C por medio de operador AND:

Clase C	Representación binario	decimal
Dirección ***host***	11000000 10101000 00000001 00001111	192.168. 1. 15
Mascara	11111111 11111111 11111111 00000000	255.255. 255. 0
AND= ID RED	11000000 10101000 00000001 00000000	192.168. 1. 0

Tabla 9. Rango clase A - direcciones IPv4 - AND
Fuente: propia

La red resultante es 192.168.1.0 255.255.255.0 (192.168.1.0/24).

Analizando la tabla podemos concluir que en clase C tenemos disponibles 2´097.052 redes y 8 bits para host es decir $2^8 - 2 = 254$ direcciones para dispositivos.

¿Por qué le restamos dos al cálculo de host disponibles?

Tenga en cuenta:

1. Los bits de la máscara que están apagados son el número de bit que se le asignan al *host*.
2. El valor que va después de la "/" representa el número de bits asignados a la red.
3. La primera dirección disponible de la red será el identificador de red (ID Red) y **no** se le puede asignar a una máquina.
4. La última dirección de la red se le asigna al identificador de *broadcast* de la red (ID *broadcast*) y **no** es una dirección válida para asignar a un dispositivo.
5. Para calcular el número de host disponible en una red aplicamos **#host= 2^n-2** (donde n = al número de bit apagados en la máscara y el 2 son las direcciones de ID RED y el ID de *broadcast* que no se podrán utilizar en ese rango.

Redes clase D

Las direcciones clase D se reservaron para el envío de *multicast* en una red IPv4, esta dirección dirige los paquetes de un dispositivo a un grupo de IP, enviando mensajes a grupos específicos.

Estas direcciones **no** son asignables ni configurables en dispositivos.

Ejemplo

Ejemplo de dirección clase D: 224.0.0.1 255.255.255.0

Redes clase E

La IETF (Fuerza de Tareas de Ingeniería de Internet) reservo estas direcciones para investigación no se asignan ni se utilizan y su rango va de la 240 a la 255.

Para profundizar el conocimiento los invito a realizar la lectura complementaria:

Visitar página

Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. https://goo.gl/Ut3U6q

Fernando Boronat Seguí y Mario Montagud Climent.

Leer especialmente el capítulo 3 Asignación de direcciones IPv4.

Distribución y asignación de direcciones IP a nivel mundial

¿Puedo colocar cualquier dirección a mi red?

No, si coloco cualquier dirección lo más probable es que se presente un conflicto de red.

Para evitar estos inconvenientes se crearon entidades internacionales que se encargaron de organizar el direccionamiento IP, los nombres de dominios, la administración de diversos protocolos de red, entre otros, a esta entidad se le llamó Icann (Corporación de Internet para la Asignación de Nombres y Números) por sus siglas en inglés.

Con el crecimiento de dominios, direcciones, protocolos, estándares de Internet la Icann asigna la supervisión de direcciones IP y nombres de dominio a la IANA (Autoridad de Números Asignados a Internet), quien a su vez organiza el direccionamiento IP por regiones y crea los denominados RIR (Registro Regional de Internet) los cuales se encargan de la organización, administración, distribución, de direcciones IP en la región designada.

RIR	Región que administra
Lacnic	Latinoamérica y el Caribe.
ARIN	Estado Unidos y Canadá.
RIPE NCC	Europa
Afrinic	África.
Apnic	Asia y Pacífico.

Tabla 10. Operadores RIR en el mundo
Fuente: propia

El RIR que le corresponde a Colombia es Lacnic (Registro de Direcciones de Internet para Latinoamérica y el Caribe), se encuentra ubicado en Montevideo, Uruguay y realiza constantemente capacitaciones gratuitas sobre direccionamiento IP con certificación internacional. Cualquier problema de direccionamiento, nombres de dominio se debe acudir al ISP.

ISP
ISP proveedor de servicios del-internet (ETB, Claro, Movistar, otros).

Visitar página

Para mayor información visitar la página de LACNIC http://www.lacnic.net/

Veamos una videocápsula que explica el proceso de transición de IPv4 a IPv6:

Video

Lacnic Webinar: IPv6 e IoT. https://youtu.be/fjrlmKM1mbY

Direcciones IPv4 privadas y públicas

Para empezar, veamos la videocápsula sobre direcciones públicas y privadas:

Video

RedesUNAH. https://youtu.be/u5RcmwBqwAs

La división en clases es uno de los grandes problemas que presenta IPv4 ya que en redes a las que inicialmente se les asignó una dirección con clase A o con clase B presentaban un alto índice de desperdicio de direcciones, y esto llevó al agotamiento prematuro de direcciones IPv4.

Hacia el año de 1994 la RFC publicó la propuesta de generar rangos de direcciones privadas para ser usadas únicamente dentro de redes locales.

RFC
Request for Comments, serie de publicaciones de IETF.

NAT
(Network Address Traslation) técnica de enmascaramiento de red para que varias direcciones privadas (no enrutables) salgan a internet por medio de una dirección pública.

Rangos de redes privadas:

Inicio de rango	Fin de rango	Cantidad de IP
10.0.0.0	10.255.255.255	16´777.214
172.16.0.0	172.31.255.255	1´048.574
192.168.0.0	192.168.255.255	65.534

Tabla 11. Rango privado - direcciones IPv4
Fuente: propia

Estos rangos privados son los que en la actualidad se deben configurar en redes LAN, estas direcciones no son enrutables, lo que significa que necesitan de un proceso extra para poder salir al exterior, normalmente este proceso es NAT.

Esto quiere decir que un gran número de máquinas locales, con direcciones locales requerirán **una única** dirección pública para poder salir a Internet, optimizando el uso de las direcciones IPv4 públicas.

Pongamos un ejemplo la Fundación Universitaria del Área Andina cuenta con más de 4 mil equipos terminales que requieren salida a Internet, todos estos equipos están configurados con una dirección privada 172.18.X.X, como estas direcciones no son enrutables se debe configurar un servidor NAT con dirección pública ejemplo 104.25.216.30, para que cualquier petición de la red privada sea atendida y salga a Internet, con la dirección pública, es decir enmascarando la dirección privada.

También existen una serie de direcciones IPv4 de uso especial es decir que no se asignan a redes públicas ni privadas pues están reservadas para usos exclusivos, debemos tener mucho cuidado con el uso de estas direcciones.

Veamos los rangos de direcciones especiales IPv4:

Dirección	Función
0.0.0.0	Reservada por la IANA.
100.64.0.0/10	NAT Masivo - NAT a gran escala.
127.X.X.X/8	Dirección de Loopback o bucle invertido (pruebas con la misma máquina).
169.254.X.X/16	Dirección de enlace local de Windows "Apipa" (Dirección privada IP automática).
192.0.2.X/24	Direcciones TEST-NET.
224.0.0.0/8	**Dirección de *Multicast*.**
255.255.255.255	**Dirección de *Broadcast*.**

Tabla 12. Rango direcciones especiales IPv4
Fuente: propia

Direccionamiento IPv6

Para comenzar, veamos la videocápsula sobre direccionamiento IPv6 y las técnicas para resumir dichas direcciones:

Video

IPv6 CAP. https://youtu.be/UTCn2n5-tKI

En el año 1994 la IETF propone el protocolo IPng (*IP Next Generation*), el cual es publicado 1996 por RFC2460. Este protocolo es presentado como la gran solución al inconveniente de agotamiento de direcciones IPv4.

Toda dirección IP está formada por un identificador de red y un identificador de *host*, en IPv6 al identificador de red se le denomina **prefijo** y al identificador de *host* **interfaz**.

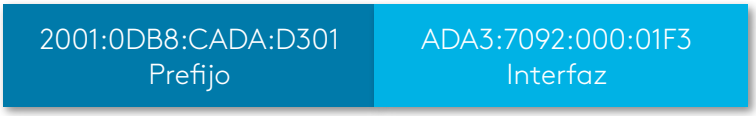


Figura 4.
Fuente: propia

Antes de continuar, visite el siguiente sitio web del Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic):

Visitar página

¿Qué es IPv6? https://goo.gl/RQGrdw

Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

La dirección IPv6 como lo vemos en el ejemplo se forma de 8 grupos de cuatro dígitos hexadecimales separados por el identificador ":".

Cada dígito hexadecimal está formado por 4 bits por consiguiente cada grupo de cuatro dígitos hexadecimales está compuesto por 16 bits y se le denomina hexteto, como la dirección IPv6 se compone de 8 hextetos tenemos entonces que la dirección IPv6 está formada por 128 bits.

Hexteto
Grupo de 16 bits o cuatro dígitos hexadecimales consecutivos dentro del mismo segmento.

Al tener 128 bits tendremos 2128 número de direcciones posibles para asignar a dispositivos, esto da un valor aproximado de 340 sextillones de direcciones, además de la extensión del número de direcciones la IETF aprovechó el nuevo desarrollo para mejorar las limitaciones que tenía IPv4, entre sus mejoras tenemos:

1. Mayor rango de direcciones 128 bits lo cual permite 340 sextillones de direcciones IP.
2. Mayor seguridad (IPsec por defecto).
3. Mayor capacidad de transmisión.
4. Mejor calidad del servicio.
5. Menos campos en el encabezado lo cual lo hace más eficiente.
6. Desaparece el *broadcast* (los mensajes serán *unicast* o *multicast*).
7. Se minimiza el uso de NAT (existe para pruebas, pero no se utiliza).
8. Se eliminan las clases (principal error de IPv4).
9. Se mejora el protocolo ICMPv6.
10. Se genera un proceso de direccionamiento automático sin necesidad de DHCPv6.

Para afianzar el conocimiento los invito a realizar la lectura complementaria:

Visitar página

Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. https://goo.gl/Ut3U6q

Fernando Boronat Seguí y Mario Montagud Climent.

Leer especialmente el capítulo 6 *IP Versión 6*.

Reglas para reducir la notación de direcciones IPv6

Instrucción

Vamos a desarrollar la actividad de repaso 3, teniendo en cuenta lo enunciado a continuación:

Debido a la extensión de las direcciones IPv6 se han creado una serie de normas o reglas que permiten reducir la longitud de su notación sin modificar la dirección original.

Regla 1: si los cuatro dígitos de un hexteto son ceros se reemplaza por un único cero.

Ejemplo:

Dirección Ipv6 original 2001:0DB8:000A:0DF0:**0000**:**0000**:0020:0001/64

Dirección remplazando hextetos de ceros 2001:0DB8:000A:0DF0:**0**:**0**:0020:1/64

Regla 2: reducir o eliminar los ceros que se encuentren a la izquierda de un segmento o hexteto (grupo de 16 bits).

Dirección Ipv6 original 2001:**0**DB8:**000**A:**0**DF0:**0**: **0**:**00**20:0001/64

Dirección omitiendo ceros iniciales 2001:DB8:A:DF0:**0**:**0**:20:1/64

Regla 3: reemplazar una única vez en la dirección IPv6 los segmentos (hextetos) consecutivos de ceros por dos puntos:

Ejemplo 1:

Dirección IPv6 original	2001:0DB8:**0000**:**0000**:**0000**:00AC:0000:000F/64
Aplicando regla 1	2001:0DB8:**0**:**0**:**0**:**00**AC:0:000F/64
Aplicando regla 2	2001:DB8: **0**:**0**:**0**: AC:**0**: F/64
Aplicando regla 3	2001:DB8::AC:**0**:F/64 dirección resumida.

Ejemplo 2:

Dirección original	2001:0000:0000:00DA:**0000**:**0000**:**000F**:**0**FEA/64

Para este caso especial aparecen dos grupos de ceros consecutivos, pero la regla dice que se debe aplicar el reemplazo una sola vez en la dirección IPv6, entonces podemos escoger cualquiera de los dos grupos a reemplazar y el otro grupo dejarlo igual:

Dirección original	2001:**0000**:**0000**:**00**DA:0000:0000:000F:0FEA/64
Aplicando regla 1	2001:**0**:**0**:**00**DA:0:0:000F:0FEA/64
Aplicando regla 2	2001:**0**:**0**:DA:**0**:**0**:F:FEA/64
Aplicando regla 3	2001::DA:**0**:**0**:F:FEA/64 dirección resumida.
Opción 2	2001:**0**:**0**:DA::F:FEA/64 dirección resumida.

Es de anotar que las dos direcciones resumidas son válidas y equivalen a la misma dirección IPv6 original.

En IPv6 existen un grupo de direcciones especiales reservadas que no se deben configurar en equipos terminales y cumplen una función específica dentro de estas tenemos:

Direcciones IPv6 de unidifusión reservadas

IPv6	Función
::/128	Dirección no especifica.
::/0	Ruta por defecto.
:: 1/128	Bucle invertido – ***Loopback***.
FE80**::**/10	Dirección Link-Local.
FC00**::**/7- FDFF**::**/7	Local única ULA(antiguas privadas).
2000**::**/3- 3FFF**::**/3	Global ***unicast*** (antiguas públicas).

Tabla 13. Rango direcciones especiales IPv6
Fuente: propia

El rango 2000::/3 a 3FFF FC00::/7- FDFF::/7/3 (Global *unicast*) es el rango de direcciones de unidifusión que se le asignará a todo equipo terminal, representa lo que en IPv4 serían las direcciones públicas, en IPv6 debido a la cantidad de direcciones existentes **todos** los dispositivos terminales tendrán direcciones públicas, evitando el NAT.

Dentro de este rango tenemos la dirección 2001:DB8::/32 la cual se reserva para documentación o estudio.

El rango FC00::/7- FDFF::/7 Local única ULA es lo que en IPv4 se conocía como direcciones privadas, estas direcciones **no** son enrutables.

Direccionamiento estático y dinámico

Las direcciones IP se pueden asignar de manera estática y dinámica.

El direccionamiento estático es la configuración manual de las direcciones a cada uno de los dispositivos de la red, se recomienda en las pequeñas empresas, café Internet y en general centros de cómputo con pocos dispositivos.

Pasos para acceder al modo de configuración de la dirección IPv4:

1. Inicio.
2. Panel de control.
3. Centro de redes y recursos compartidos.
4. Cambiar configuración del adaptador de red.
5. Clic secundario sobre el dispositivo a configurar.
6. Propiedades.
7. Protocolo de Internet versión 4.
8. Propiedades.

Tenga en cuenta: la combinación de teclas Windows+R escribir ncpa.cpl es la forma rápida de llegar a las propiedades del dispositivo de red.

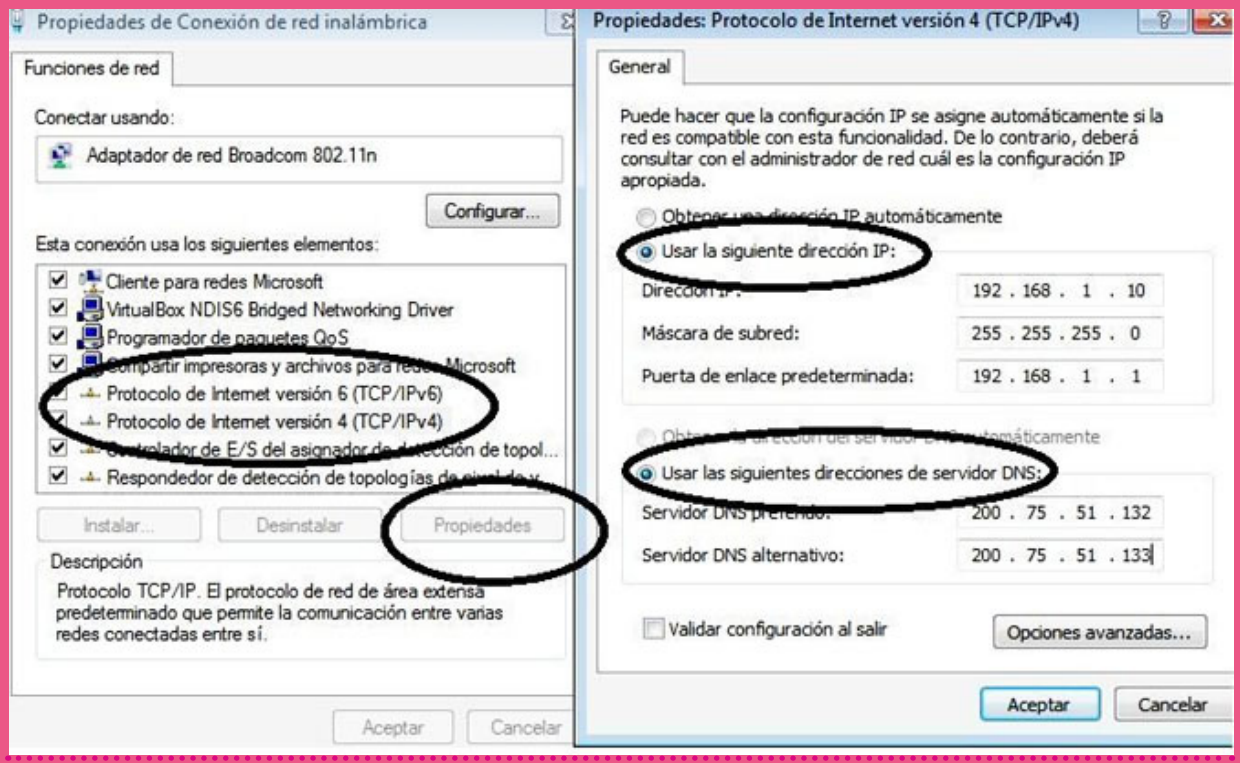


Figura 5. Configuración dirección IPv4 en equipo Windows
Fuente: propia

La ventaja del direccionamiento estático es que no requiere de un protocolo adicional ni un servidor para la asignación de direcciones, también ofrece niveles de seguridad porque se requiere saber el rango de direcciones configuradas para poder ser parte de la misma, así mismo se optimizan los recursos ya que no se sobrecarga de trabajo el *router* ni el servidor.

La desventaja es que en redes grandes es complicado llevar el control de direcciones, además es fácil de cometer errores y colocar la red en conflicto, por otra parte, se hace más compleja la administración de la red.

Configuración de la dirección estática en IPv6

Los pasos son similares a IPv4, una vez en el menú de propiedades, conexión del dispositivo, seleccionamos protocolo de Internet versión 6, luego propiedades y seleccionamos la opción usar la siguiente dirección IPv6 y usar la siguiente dirección de servidor DNS y se procede a escribir la dirección tanto IPv6 como la dirección de DNS.

Acceso rápido a opciones de red, tecla Windows+R escribir ncpa.cpl

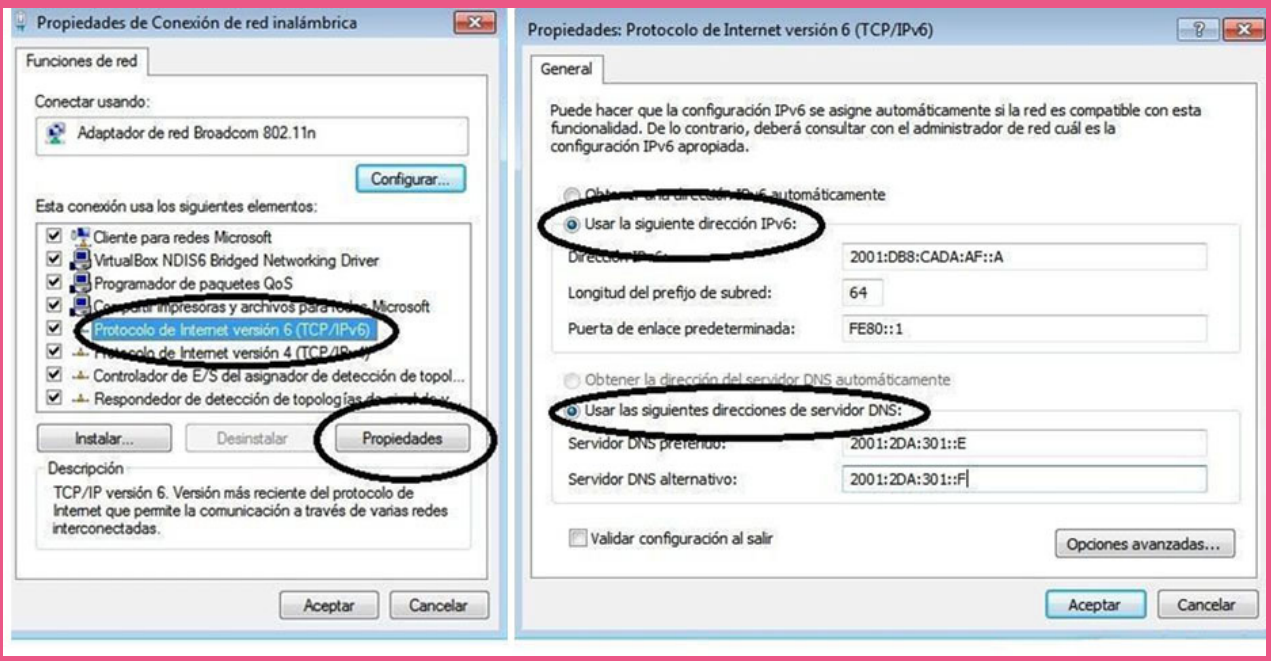


Figura 6. Configuración dirección IPv6 en equipo Windows
Fuente: propia

Direccionamiento dinámico

Para configurar el direccionamiento dinámico en IPv4 se requiere el protocolo DHCP (*Dynamic Host Configuration Protocol*) Protocolo de configuración dinámica de *host*, el cual asigna direcciones IPv4 de forma dinámica, previa configuración en un servidor DHCP o de un router con DHCP configurado.

La configuración dinámica de IP optimiza los procesos administrativos, brinda seguridad por medio del control de accesos a la red, evita conflictos de direcciones, pero consume recursos de servidor o *router*, Se recomienda en redes medianas y grandes (aunque en la actualidad los *router* wifi caseros que nos ofrecen los ISP ya traen habilitado por defecto el DHCP).

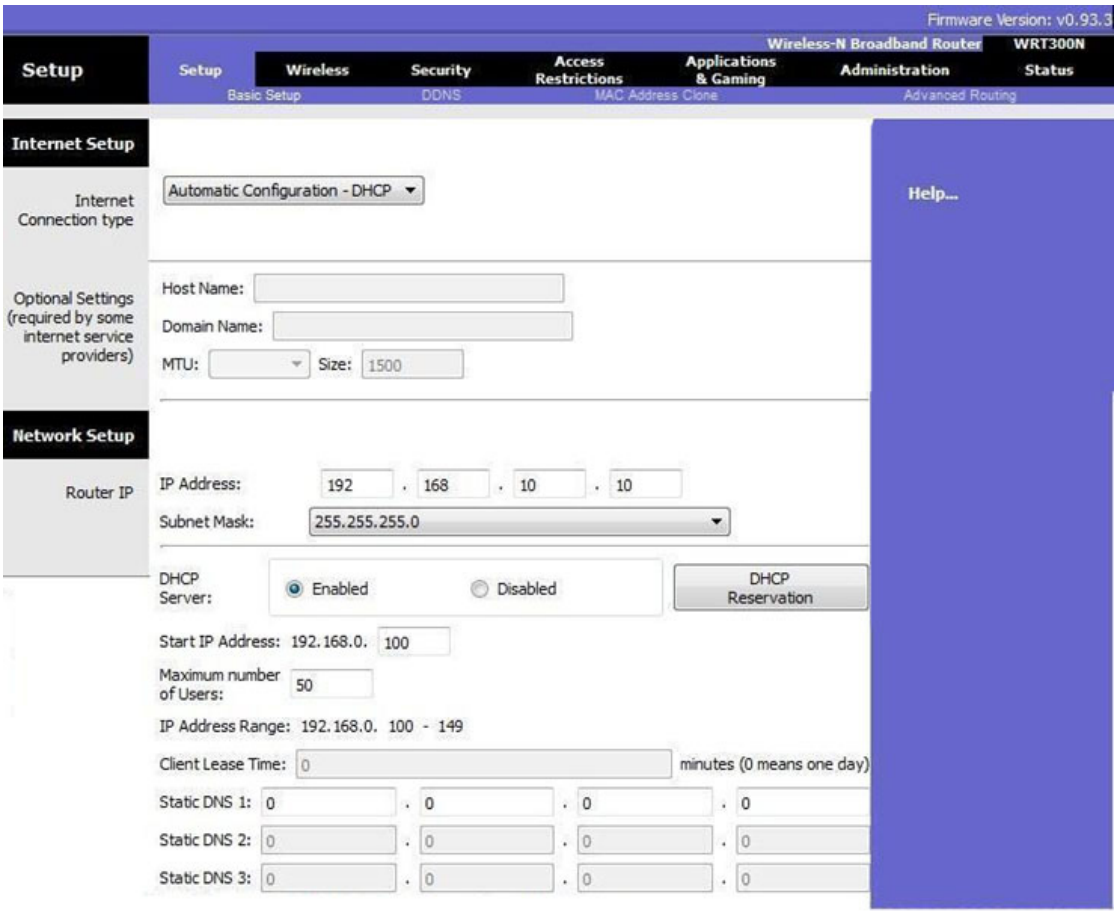


Figura 7. Configuración DHCP en router wifi *LinkSys*
Fuente: propia

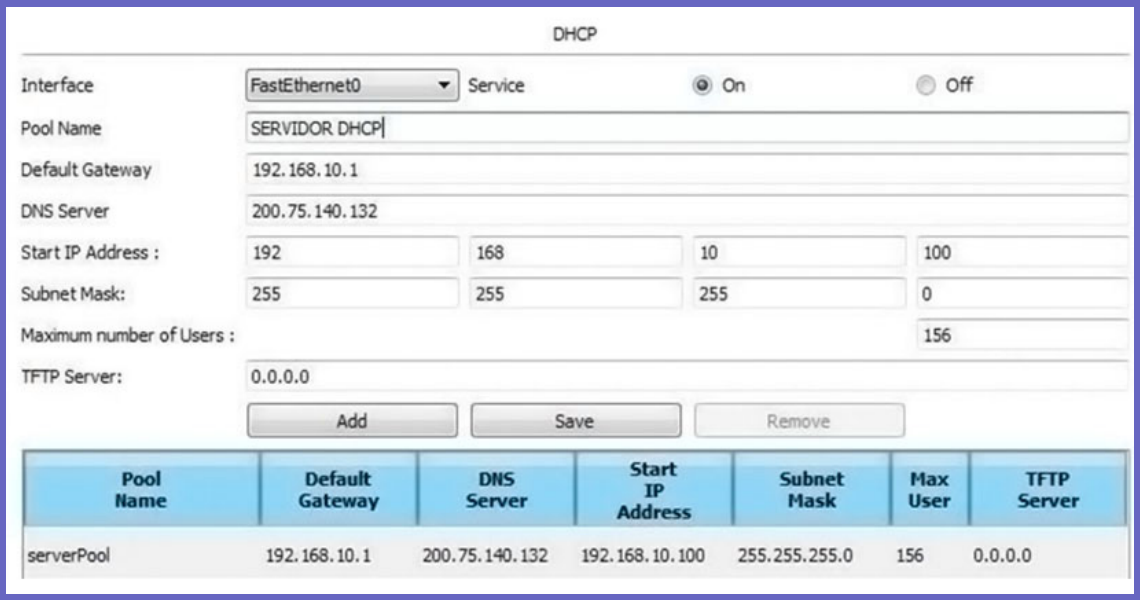


Figura 8. Configuración DHCP IPv4 en *router* wifi *LinkSys*
Fuente: propia

En IPv6 El direccionamiento dinámico se puede dar de tres formas diferentes:

1. Solo SLAAC autoconfiguración de dirección sin estado, asigna una dirección IPv6 sin necesidad de disponer de un servidor DCHPV6, utiliza el proceso EUI-64 para auto configurar la dirección.

1. SLACC + DHCP autoconfigura la dirección IP, pero requiere DHCPv6 para obtener información adicional como los DNS.

1. Solo DHCPv6 información con estado, obliga a la obtención de direcciones IPv6 por medio de DHCPv6 no permite autoconfiguración, guarda la información de las direcciones asignadas.

Le recomendamos ampliar la información, visitando el siguiente sitio:

Visitar página

Proceso EUI-64 en Direcciones IPv6 unicast. https://goo.gl/tzXt1d *Cisco Networking Academy*.

La configuración DCHPV6 se genera mediante servidor DHCPv6 o mediante *router* DHCPv6, los equipos caseros *router* wifi que asignan los ISP no admiten en protocolo IPv6.

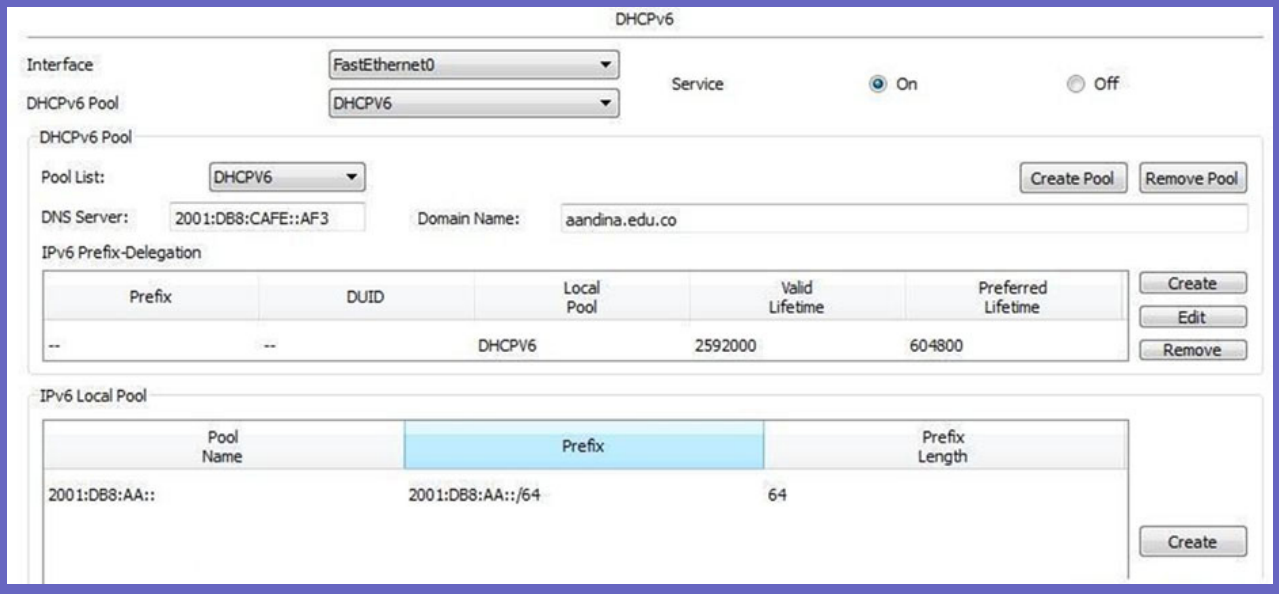


Figura 9. Configuración DHCP IPv6 en *router* wifi *LinkSys*
Fuente: propia

Figura 10. Configuración DHCP IPv6 en *router Cisco*
Fuente: propia

BIBLIOGRAFÍA

Bellido, Q. (2014). *Equipos de interconexión y servicios de red* (UF1879). Madrid, España: IC Editorial.

Bermúdez, L. (2012). *Montaje de infraestructuras de redes locales de datos: UF1121*. Madrid, España: IC Editorial.

Boronat, S., y Montagud, C. (2013). *Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF*. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Calvo, G. (2014). *Gestión de redes telemáticas (UF1880)*. Madrid, España: IC Editorial.

Feria, G. (2009). *Modelo OSI*. Córdoba, Argentina: El Cid Editor | apuntes.

García, M. (2012). *Mantenimiento de infraestructuras de redes locales de datos (MF0600_2)*. Málaga, España: IC Editorial.

Íñigo, G., Barceló, O., y Cerdà, A. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.

Martínez, Y., y Riaño, V. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.

Molina, R. (2014). *Implantación de los elementos de la red local*. Madrid, España: RA-MA Editorial.

Mora, J. (2014). *Desarrollo del proyecto de la red telemática (UF1870)*. Madrid, España: IC Editorial.

Purser, M. (1990). *Redes de telecomunicación y ordenadores*. Madrid, España: Ediciones Díaz de Santos.

Roa, B. (2013). *Seguridad informática*. Madrid, España: McGraw-Hill España.

Robledo, S. (2002). Redes de computadoras. Ciudad de México, México: Instituto Politécnico Nacional.

Romero, J. (2009). *Estudio de subnetting, VLSM, Cidr y comandos de administración y configuración de routers*. Córdoba, Argentina: El Cid Editor | Apuntes.

BIBLIOGRAFÍA

S.L. Innovación y Cualificación. (2012). *Guía para el docente y solucionarios: montaje y mantenimiento de sistemas de telefonía e infraestructuras de redes locales de datos*. Málaga, España: IC Editorial.

Vásquez, D. (2009). *Base de la teleinformática*. Córdoba, Argentina: El Cid Editor | apuntes.

Velte, T., y Velte, A. (2008). *Manual de Cisco*. Ciudad de México, México: McGraw-Hill Interamericana.

REDES I

Ricardo López Bulla

EJE 3

Pongamos en práctica

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

INTRODUCCIÓN

Es hora de poner en práctica nuestros conocimientos, en este eje desarrollaremos habilidades en el diseño e implementación de una red de área local, nos apoyaremos en un simulador denominado *Packet tracer* el cual se explicará en el transcurso del módulo.

Una buena práctica antes de ir a campo a desarrollar el montaje, es el uso de simuladores que permitan detectar posibles fallos en el diseño, por ello en el desarrollo temático veremos qué es un simulador, cuáles están disponibles y cómo diseñar la red en los mismos.

Análisis y diseño para la simulación de una red

El diseño de redes está determinado por diversos componentes y dispositivos que al interactuar permiten optimizar los recursos de la misma, la decisión de cuáles dispositivos utilizar, donde ubicarlos, qué servicios instalar, como configurarlos es decisión del administrador de red y solo podrá ver su efectividad al momento de la implementación y puesta en marcha, pero ¿si no da el rendimiento esperado o presenta fallas?

Para prever estos problemas y tener una visión previa de lo que será la red se han desarrollado una serie de simuladores que permiten generar entornos de prueba en ambientes similares a los reales, ayudan a determinar el rendimiento de la red, descartar errores, desarrollar análisis del diseño propuesto, verificar funcionalidad y posibles fallos, optimizando la implementación y ofreciendo un mejor servicio.

Los principales y más utilizados simuladores son:

- GNS3.
- *Packet tracer*.
- CNet Network Simulator.

GNS3

Simulador gráfico de redes de libre distribución (software libre) que permite emular desde la topología más básica hasta la más compleja, ejecuta diversos IOS de dispositivos Cisco, se considera la más potente de las herramientas de simulación de redes en ambientes profesionales, permite simular el tráfico de red y desarrollar análisis del mismo ya que cuenta con emulador de *Wireshark*.

La debilidad de GNS3 es que requiere de una máquina potente para poder correr y que se deben adquirir los IOS de cada dispositivo que se quiera agregar.

Packet tracer

Packet tracer es el simulador de redes más popular en ambientes educativos, gracias a la interfaz amigable e intuitiva que presenta, al bajo consumo de recursos de máquina que requiere, la posibilidad de diseñar ambientes reales (no complejos) en muy poco tiempo y con alta precisión.

Packet tracer es un programa propietario de Cisco (utilizado en las academias de formación CCNA), admite la selección, conectividad, configuración de diversos dispositivos *router*, *switch*, PC, nubes, dispositivos inalámbricos, entre otros.

Cisco
Es la empresa líder del mercado en el desarrollo de dispositivos de interconexión.

CCNA
Cisco Certified Network Associate, certificación que se entrega a los profesionales de infraestructura de red e Internet.

Las versiones superiores a 7.0 están adaptadas para generar ambientes IoT (Internet de todo).

En *Packet tracer* se pueden simular redes con direccionamiento IPv4 e IPv6, configurar redes con CIDR (*subnetting*), implementar VLAN, asegurar puertos e interfaces, además soporta la configuración de diversos protocolos de enrutamiento RIP v2, RIPng, OSPFv2, OSPFv3, EIGP y BGP. Lo utilizaremos como herramienta pedagógica para comprensión de los conceptos.

Entre las principales ventajas de *Packet tracer* se destacan, el bajo consumo de recursos de máquina lo cual permite ser instalado en cualquier tipo de dispositivo incluso en teléfonos celulares, su interfaz es amigable e intuitiva, tiene pre instalado los IOS de *Cisco*, presenta dos modos de simulación (*Realtime* y *simulation mode*), el modo de simulación permite ver y analizar cómo se desplaza paso a paso la información y el análisis de la PDU desde el modelo OSI.

CIDR
ClassLess Inter-Domain Routing, enrutamiento entre dominios, define las subredes.

IOS
Sistema operativo de dispositivos Cisco.

Dentro de las debilidades de este simulador tenemos las limitaciones en el desarrollo de redes complejas, la poca variedad de dispositivos que presenta y la no compatibilidad con otras marcas de dispositivos.

Conociendo la interfaz

La siguiente figura nos muestra la interfaz de trabajo de *Packet tracer*.

El menú principal presenta opciones de archivo, edición, ver, herramientas, extensiones y ayuda, con funciones similares a la mayoría de programas (guardar, copiar, cortar, imprimir y otras).

El menú lateral barra de herramientas permite seleccionar, documentar, borrar, ampliar, reducir, generar forma y fondo, y un elemento muy importante (sobre cerrado, sobre abierto) para el manejo de la PDU envió de paquetes, también nos muestra los dos modos de trabajo, presentación tiempo real y modo simulación.

El área de trabajo es el área donde se desarrollarán las implementaciones requeridas.

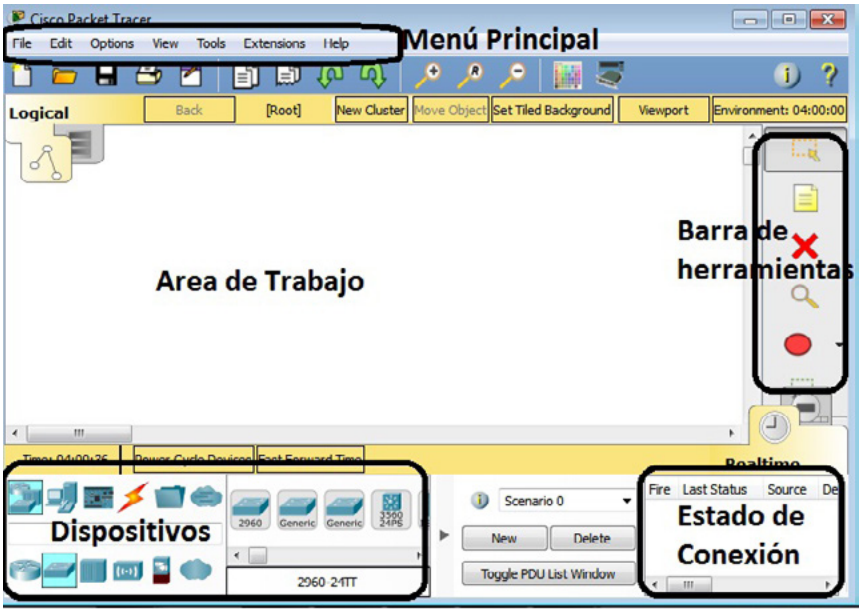


Figura 1. Interfaz de trabajo *Packet tracer*
Fuente: propia

PDU
Unidad de protocolo de datos.

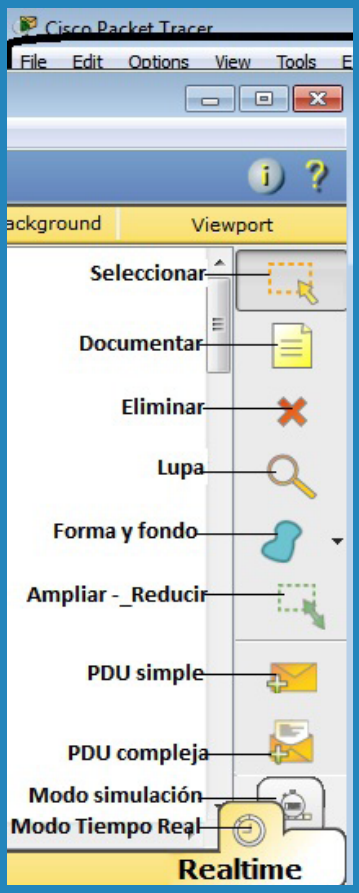
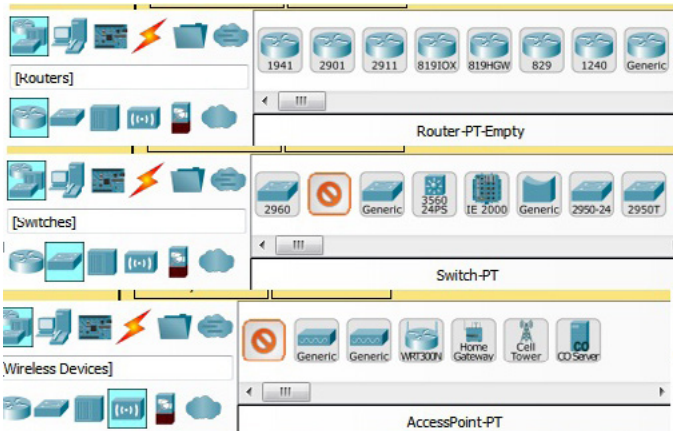


Figura 2. Menú barra de herramientas
Fuente: propia

El menú dispositivo (parte inferior izquierda) nos presenta los diversos dispositivos que se pueden utilizar en el simulador, intermediarios, terminales y medios de conexión.

El primer icono representa los dispositivos intermediarios entre los que tendremos *router*, *switch*, *Hub*, *Access-Point*, dispositivos de seguridad y nubes, al dar clic en el dispositivo que requerimos, se nos despliega un submenú gráfico que muestra los dispositivos específicos disponibles y de allí los podemos seleccionar y pasar al área de trabajo.

La siguiente gráfica muestra algunos dispositivos intermediarios que usa *Packet tracer*:



Router

Switch

Access- Point

Figura 3. Menú de dispositivos intermediarios en *Packet tracer*
Fuente: propia

El segundo icono del menú de dispositivos nos presenta el conjunto de dispositivos finales es decir los que interactúan directamente con el usuario entre ellos tenemos PC, portátiles, servidores, impresoras de red, teléfonos análogos, teléfonos Voip, televisores, *smartphone*, tablet, entre otros.

La siguiente figura muestra algunos dispositivos finales que presenta *Packet tracer*.

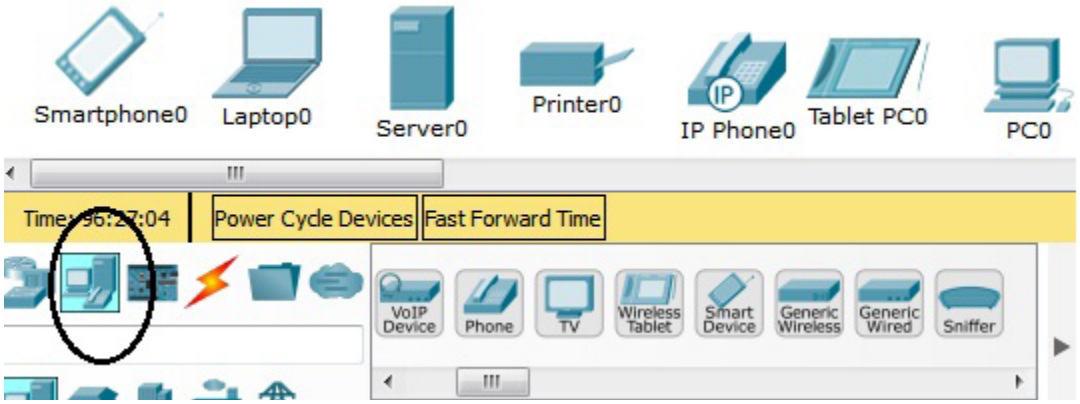


Figura 4. Menú de dispositivos finales en *Packet tracer*
Fuente: propia

Dentro del mismo menú de dispositivos finales y en versiones superiores a *Packet tracer* 7.0 encontramos elementos que permiten desarrollar simulaciones aplicando IoT (Internet de Todo o Internet de las cosas), para hogar y oficina. Dentro de estos elementos encontramos detectores de humo, termostatos, controladores para luces, puertas, ventanas, aires acondicionados, paneles solares, entre otros muchos elementos que pueden ser controlados y programados por medio de dispositivos terminales.

Video

Internet de las cosas.

https://youtu.be/RhC50M5qlF0

En la siguiente figura observados algunos de los elementos usados para IoT que se pueden programar y se incluyen en *Packet tracer*.

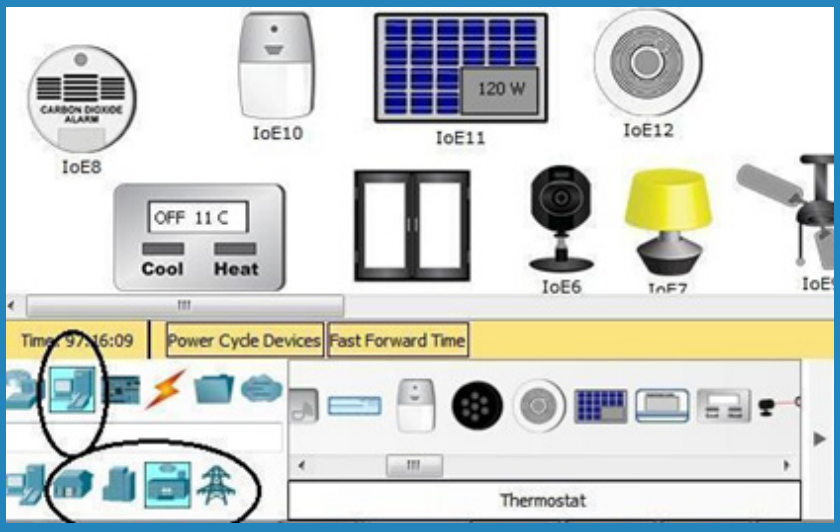


Figura 5. Dispositivos IoT en *Packet tracer*
Fuente: propia

Visitar página

Implantación de los elementos de la red local.

https://goo.gl/jVdofb

Francisco Molina.

Capítulo 2
Elementos de una red de área local - Dispositivos de red.

Otro elemento importante y requerido para la instalación de la red, son los medios de conexión los cuales interconectarán los dispositivos. Dentro de *Packet tracer* encontramos, cable de consola, cable UTP directo, cable UTP cruzado, fibra óptica, cable telefónico, cables serial DTE y DCE, cable USB y cable de conexión para dispositivos IoT.

Video

Selección de cable UTP y fibra óptica.

http://bit.ly/2wR3qdO

La siguiente figura ilustra los medios ofrecidos por el simulador.

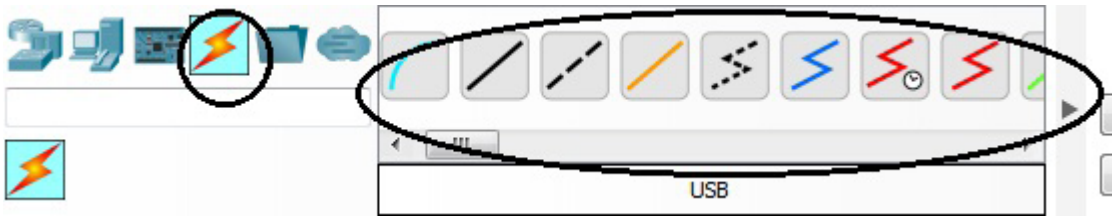


Figura 6. Menú de medios de conexión en *Packet tracer*
Fuente: propia

Diseñando nuestra red

Instrucción

Para dar introducción al tema los invito a ver el videorelato "Configuración de red PAN y Red LAN en Packet tracer", en el cual explico cómo se configura una red Pan; LAN y una red WLAN.

Con la ayuda del *Packet tracer* generaremos una serie de redes e identificaremos componentes, características y funcionalidades.

Tenga en cuenta: estos retos no son calificables, son de aprendizaje, sea lo más honesto posible con usted mismo, solo así podrá desarrollar habilidades en la configuración e instalación de las redes. ¿Está dispuesto a aprender?, Manos a la obra.

RETO 1

Le solicitan asesoría sobre la mejor opción para conectar dos dispositivos que requieren compartir información:

01 ¿Qué preguntas son necesarias antes de comenzar? (genere una lista de preguntas que considere necesarias).

02 ¿Qué recursos necesito para que se puedan comunicar? (elaborar una lista de elementos que considere necesarios).

03 Diseñé en *Packet tracer* la red, ¿Utilicé todos los recursos qué pensó?, ¿me faltaron recursos?, ¿qué funcionalidad tiene cada recurso en la red que diseñé? (dar explicación a cada punto).

04 ¿Existe otra forma de conectar los dos dispositivos? (consultar y explicar las alternativas).

Comparemos resultados:

Si analizamos el reto que se nos propone, es uno de los temas más comunes en el desarrollo de las redes, y muchas veces sin saberlo hemos diseñado e implementado una red.

- ¿Ha implementado, instalado o configurado alguna vez una red?
- ¿Ha compartido alguna vez información entre dispositivos?, por ejemplo, ha enviado fotos, imágenes, videos, audios y/o textos a otro *smartphone*.
- ¿Ha descargado a su computador información desde un *smartphone*?
- ¿Ha conectado una impresora un teclado, un mouse a un computador?

Si alguna de estas respuestas es positiva ¡Felicitaciones! Lleva un gran camino recorrido en el mundo de las redes, pues ha dado solución al objetivo de la red, la comunicación.

Dando respuesta al reto, respecto a: ¿Qué preguntas son necesarias antes de comenzar?

La pregunta básica para determinar cómo diseñar la red, se responde por medio del conocimiento sobre los dispositivos que necesita conectar, (computadores, *smartphone*, *tablet*, PDA) ¿Qué dispositivos va a conectar? **Dependiendo de los dispositivos a conectar se generan diversas alternativas, por ejemplo:**

Se requiere conectar dos computadoras portátiles; veamos las alternativas:

- Vía inalámbrica *Bluetooth* o infrarrojo.
- Por medio de un cable de red conectándolos directamente.
- Por medio de un dispositivo wifi.
- Por medio de un *switch*.

Video

Los riesgos de conectarse a una red wifi pública.

https://youtu.be/EUs8o3SNJrw

De acuerdo a la alternativa seleccionada se requieren ciertos recursos. Si se opta por la conexión vía inalámbrica, *Bluetooth*, o infrarrojo se debe verificar que los dos dispositivos posean tarjeta *Bluetooth*, o infrarrojo y proceder a sincronizarlos, (no se requiere dispositivos intermediarios).

En la siguiente figura observamos conexión vía *Bluetooth*:

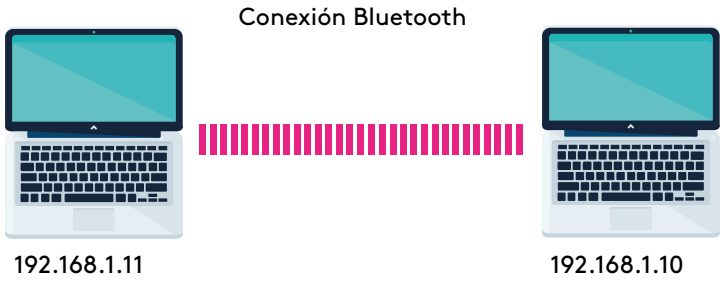


Figura 7. Conexión Bluetooth en Packet tracer
Fuente: propia

Si la opción es conectar directamente los dos computadores por medio de cable de red, se requiere tarjeta de red, cable cruzado (en sistemas operativos superiores a Windows 7, permite conectar cable directo, porque brinda una tecnología MDIX que realiza la función de cruzado de forma lógica), configurar una dirección IP en cada equipo, y compartir el recurso que se requiera, no se necesita ningún dispositivo intermediario.

En la siguiente figura observamos la conexión directa por cable:

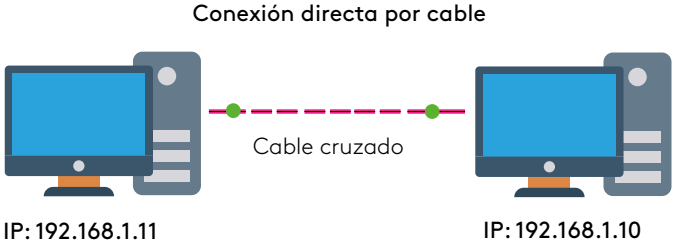


Figura 8. Conexión directa por cable en Packet tracer
Fuente: propia

La tercera opción es conectarnos con la ayuda de un dispositivo intermediario, para el caso un *switch*, se requerirá entonces que los equipos cuenten con una tarjeta de red *Ethernet* y un cable *Patch cord* para conectar el equipo con el *switch*, y una dirección IP configurada en cada PC.

Patch cord

Cable corto de red que permite la conexión entre el dispositivo final y la red.

En la siguiente figura observamos la conexión por medio de un *switch*:

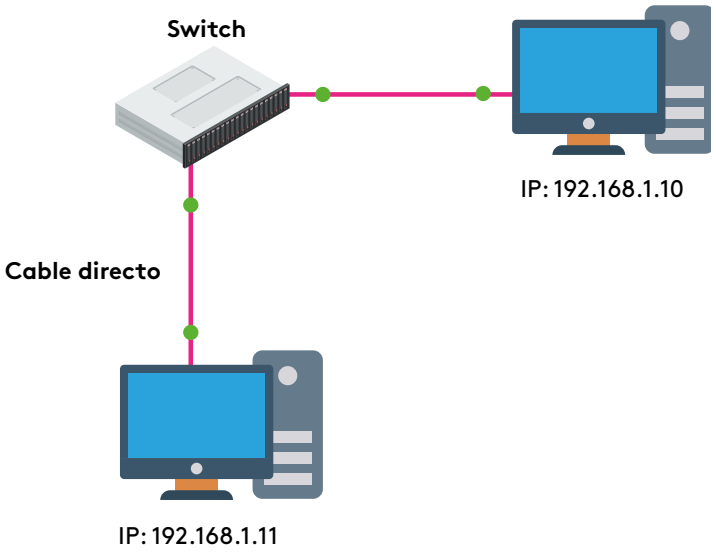


Figura 9. Conexión por medio de switch - Packet tracer
Fuente: propia

La última opción planteada es la conexión Inalámbrica vía wifi, es decir con la intervención de un *router* wifi que servirá de intermediario entre los dispositivos, cada equipo terminal requerirá de una tarjeta de red wifi, y una dirección IP.

En la siguiente figura observamos la conexión por medio de un *router* wifi:

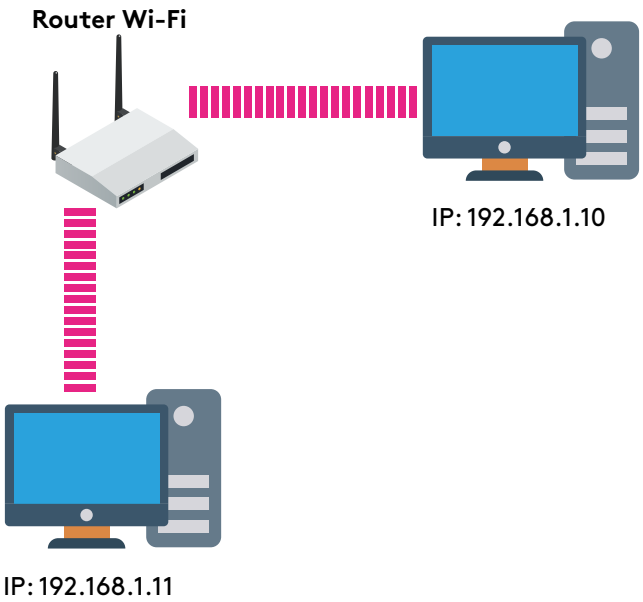


Figura 10. Conexión wifi - Packet tracer
Fuente: propia

Visitar página

Implantación de los elementos de la red local.
Francisco Molina.

https://goo.gl/jVdofb

Capítulo 5 Verificación y prueba de elementos de conectividad de redes de área local.

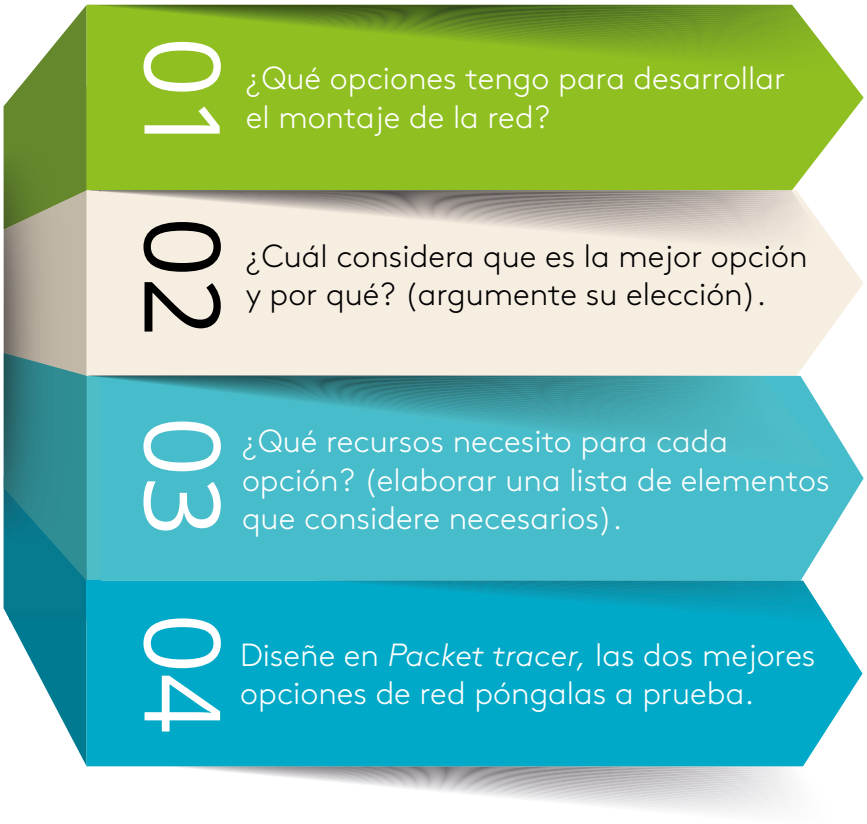
RETO 2

Se solicita que desarrolle el diseño y montaje de una oficina de cómputo que cuenta con cuatro computadoras, una impresora de red y conectividad a Internet.

Video

Elementos de una red.

http://bit.ly/2i6VKS4



Para resolver este reto debemos iniciar por el análisis de la cantidad de dispositivos que requieren conectividad, los recursos que se compartirán y los servicios a utilizar.

Necesitamos conectar 6 dispositivos, 4 PC, una impresora de red y el módem ADSL que nos permitirá salir a Internet (el modem lo asigna el ISP, al contratar el servicio de Internet).

La **primera opción** será conectarlos por medios guiados (cables), es decir elaborar un diseño de cableado estructurado para lo cual necesitamos que todos los dispositivos a conectar cuenten con una tarjeta de red NIC, por ser más de dos dispositivos no es factible conectar directamente los PC entre sí, por consiguiente se requiere de un dispositivo intermediario que actúe como conmutador, este dispositivo será un *switch*, para alojar el *switch* y el modem que nos asigna el ISP de una forma organizada se requiere de un rack, (base, cabina o armario para colocar dispositivos de red).

ISP
Proveedor de servicios de Internet.

Medios guiados
Es la conectividad con cable entre dispositivos.

Cableado estructurado
Es el tendido de cables de manera organizada que interconecta los diversos dispositivos de red y permite la integración de diversos servicios.

Rack
Es la estructura metálica que soporta los dispositivos de red.

Visitar página

Implantación de los elementos de la red local.
Francisco Molina.

https://goo.gl/jVdofbb

Capítulo 4 El armario de comunicaciones.

La siguiente figura muestra la topología de red del caso planteado:

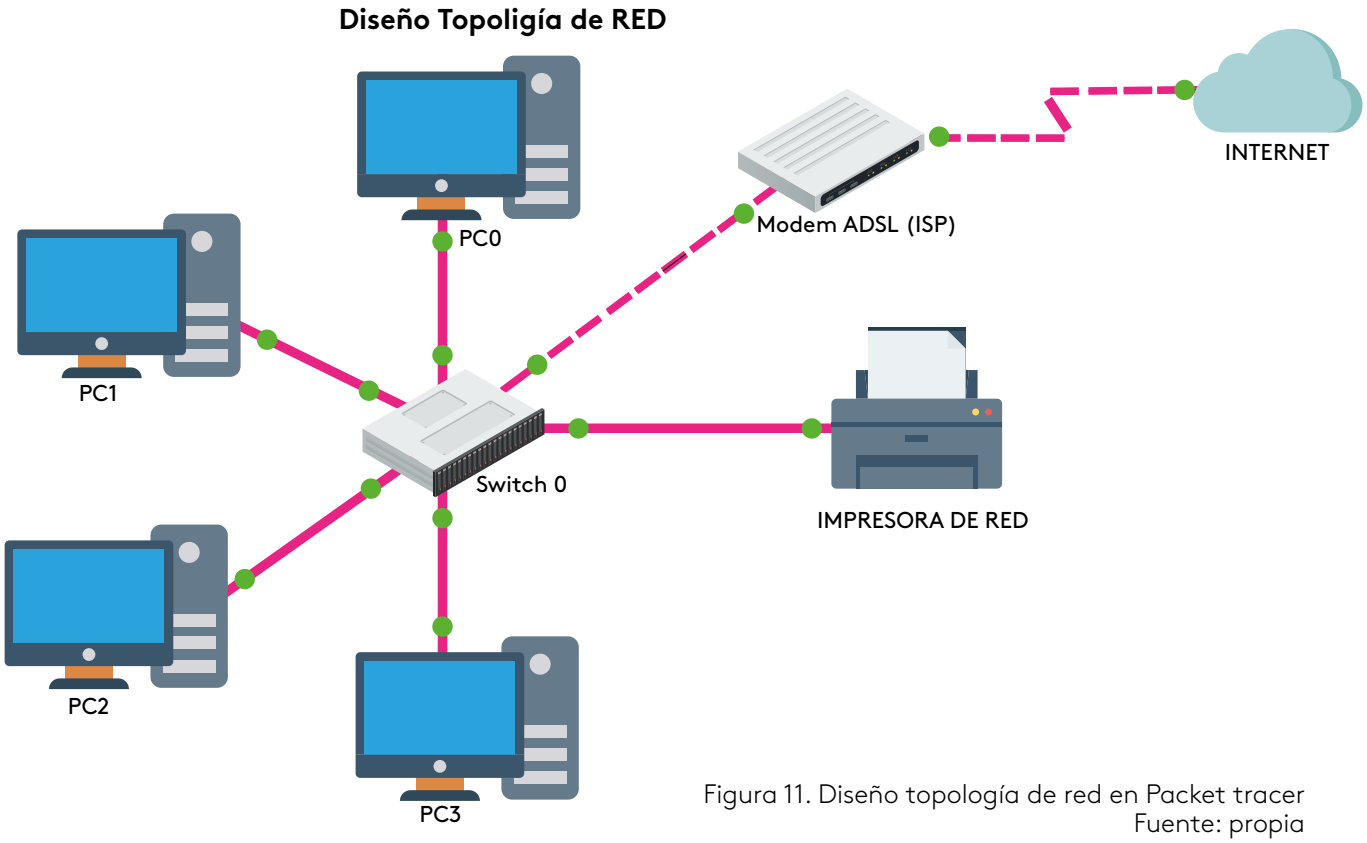


Figura 11. Diseño topología de red en Packet tracer
Fuente: propia

Una vez interconectados los dispositivos procedemos a generar la tabla de direccionamiento IP.

Tabla de direccionamiento IP:

Dispositivo	Interfaz	Dirección IP	Mascara	*Gateway*
Switch O	Vlan 1	192.168.1.2	255.255.255.0	192.168.1.1
PC0	Nic	192.168.1.10	255.255.255.0	192.168.1.1
PC1	Nic	192.168.1.11	255.255.255.0	192.168.1.1
PC2	Nic	192.168.1.12	255.255.255.0	192.168.1.1
PC3	Nic	192.168.1.13	255.255.255.0	192.168.1.1
Impresora de red	Nic	192.168.1.5	255.255.255.0	No aplica
Modem ADSL	G0/0	192.168.1.1	255.255.255.0	No aplica

Tabla 1. Tabla de direccionamiento IP
Fuente: propia

Una vez interconectados los equipos y con direccionamiento asignado podrán compartir recursos y servicios.

La **segunda alternativa** es diseñar una red con medios no guiados, es decir una red inalámbrica (para nuestro caso wifi).

En este diseño necesitamos que los equipos tengan instalada una tarjeta de red inalámbrica, un *router* wifi y que el módem esté conectado al *router* wifi por medio de cable.

Es importante aclarar que la mayoría de *router* wifi son multipropósito, es decir sirven de *router*, de *switch* y de enlace inalámbrico, evitando la compra de dispositivos adicionales.

La siguiente figura nos muestra el diseño de la topología:

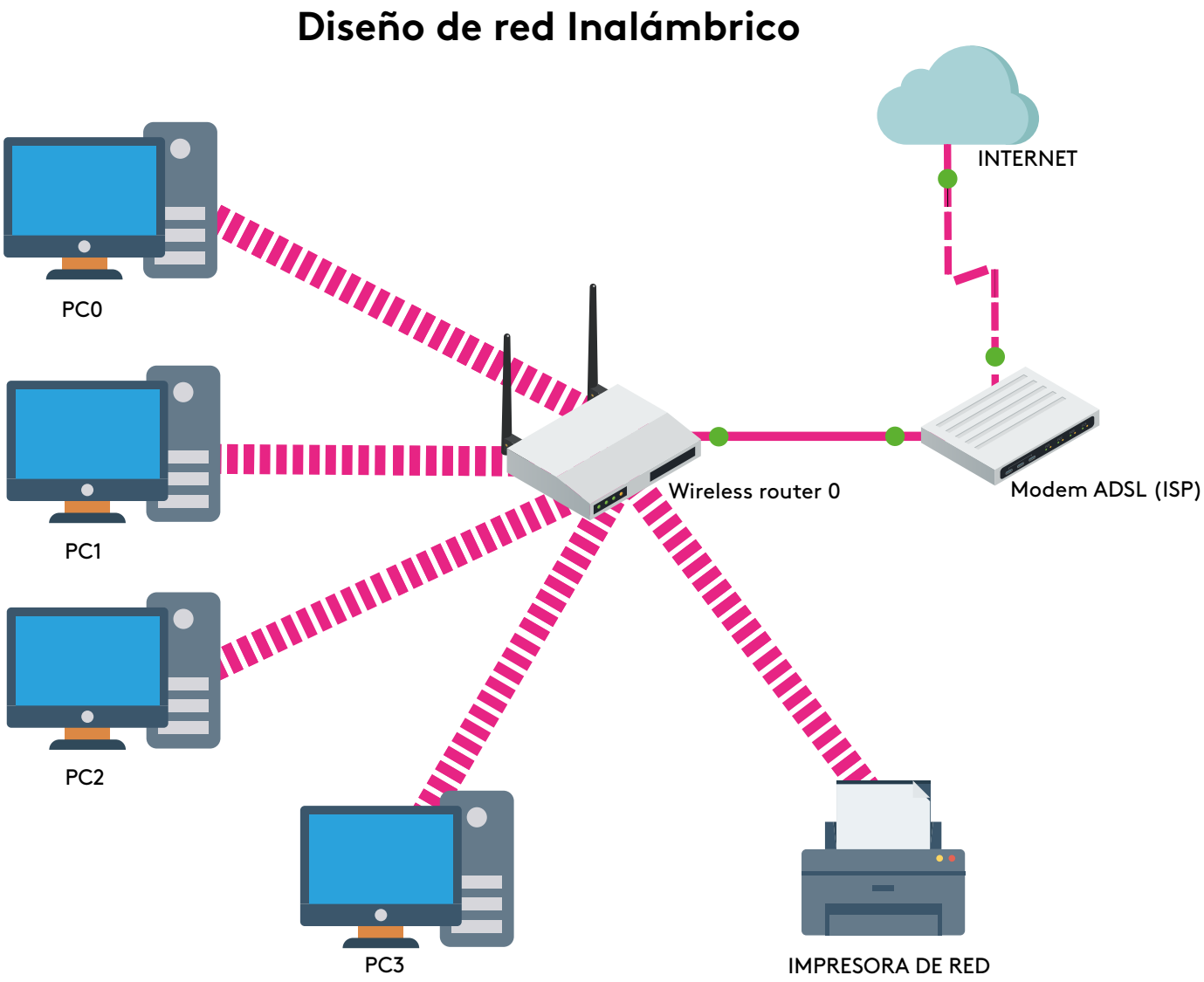


Figura 12. Diseño de red inalámbrico - *Packet tracer*
Fuente: propia

Visitar página

Computo móvil, leer Redes móviles.
Arturo Mejía Reyes.

https://goo.gl/cgmerL

Tenga en cuenta: el *router* wifi por defecto trae configurado DHCP facilitando la asignación de direcciones IP.

DHCP

(Dynamic Host Configuration Protocol) protocolo de asignación dinámica de direcciones IP.

Cuadro comparativo medios guiado - medios no guiados.

Medios	Ventajas	Desventajas
Medios guiados	• Estabilidad. • Alcance. • Velocidad de Tx. • Escalabilidad. • Comunicación Full dúplex.	• Costos. • Requerimientos. • Obra de cableado estructurado. • No movilidad.
Medios no guiados	• Movilidad. • Facilidad de instalación. • No requiere obra de cableado. • Económica.	• Alcance. • Velocidad de Tx. • Escalabilidad. • Cobertura. • Comunicación Half dúplex.

Tabla 2. Cuadro comparativo medios guiados – medios no guiados
Fuente: propia

En conclusión, las dos redes tienen sus ventajas y desventajas, debemos evaluar la viabilidad, los requerimientos y un análisis de costo beneficio para tomar una la mejor decisión.

Instrucción

Ahora bien, a este punto le invitamos a desarrollar el caso simulado "Implementando una red".

BIBLIOGRAFÍA

Bellido, Q. (2014). *Equipos de interconexión y servicios de red (UF1879)*. Madrid, España: IC Editorial.

Bermúdez, L. (2012). *Montaje de infraestructuras de redes locales de datos: UF1121*. Madrid, España: IC Editorial.

Calvo, G. (2014). *Gestión de redes telemáticas (UF1880)*. Madrid, España: IC Editorial.

Feria, G. (2009). *Modelo OSI*. Córdoba, Argentina: El Cid Editor | apuntes.

García, M. (2012). *Mantenimiento de infraestructuras de redes locales de datos (MF0600_2)*. Málaga, España: IC Editorial.

Íñigo, G., Barceló, O., y Cerdà, A. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.

Martínez, Y., y Riaño, V. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.

Molina, R. (2014). *Implantación de los elementos de la red local*. Madrid, España: RA-MA Editorial.

Mora, J. (2014). *Desarrollo del proyecto de la red telemática (UF1870)*. Madrid, España: IC Editorial.

Purser, M. (1990). *Redes de telecomunicación y ordenadores*. Madrid, España: Ediciones Díaz de Santos.

Roa, B. (2013). *Seguridad informática*. Madrid, España: McGraw-Hill España.

BIBLIOGRAFÍA

Robledo, S. (2002). *Redes de computadoras*. Ciudad de México, México: Instituto Politécnico Nacional.

Romero, J. (2009). *Estudio de subnetting, VLSM, Cidr y comandos de administración y configuración de routers*. Córdoba, Argentina: El Cid Editor | Apuntes.

S.L. Innovación y Cualificación. (2012). *Guía para el docente y solucionarios: montaje y mantenimiento de sistemas de telefonía e infraestructuras de redes locales de datos*. Málaga, España: IC Editorial.

Vásquez, D. (2009). *Base de la teleinformática*. Córdoba, Argentina: El Cid Editor | apuntes.

Velte, T., y Velte, A. (2008). *Manual de Cisco*. Ciudad de México, México: McGraw-Hill Interamericana.

REDES I

Ricardo López Bulla

EJE 4

Propongamos

Protocol

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

INTRODUCCIÓN

El objetivo de una red debe apuntar a servir al usuario final, el cual sin mayor conocimiento puede hacer uso de esta y sacar el mayor provecho de los servicios que ofrece, voz, datos, video, mensajes, entre otros.

El departamento de TI debe velar porque estos servicios estén disponibles, sean confiables y brinden un alto nivel de integridad.

En el desarrollo de este eje se trabajará la capa de transporte y la capa de aplicación del modelo TCP/IP y su relación con el modelo OSI, para lo cual contaremos con un mapa conceptual, videocápsulas, actividades de refuerzo, entre otros, se recomienda desarrollar todas las actividades propuestas.

Instrucción

Es importante que, desde ahora, consulte las instrucciones de la actividad de evaluación que deberán desarrollar de manera colaborativa.

Capas

Capa de transporte

Para empezar, veamos un mapa conceptual que ilustra la capa de transporte:

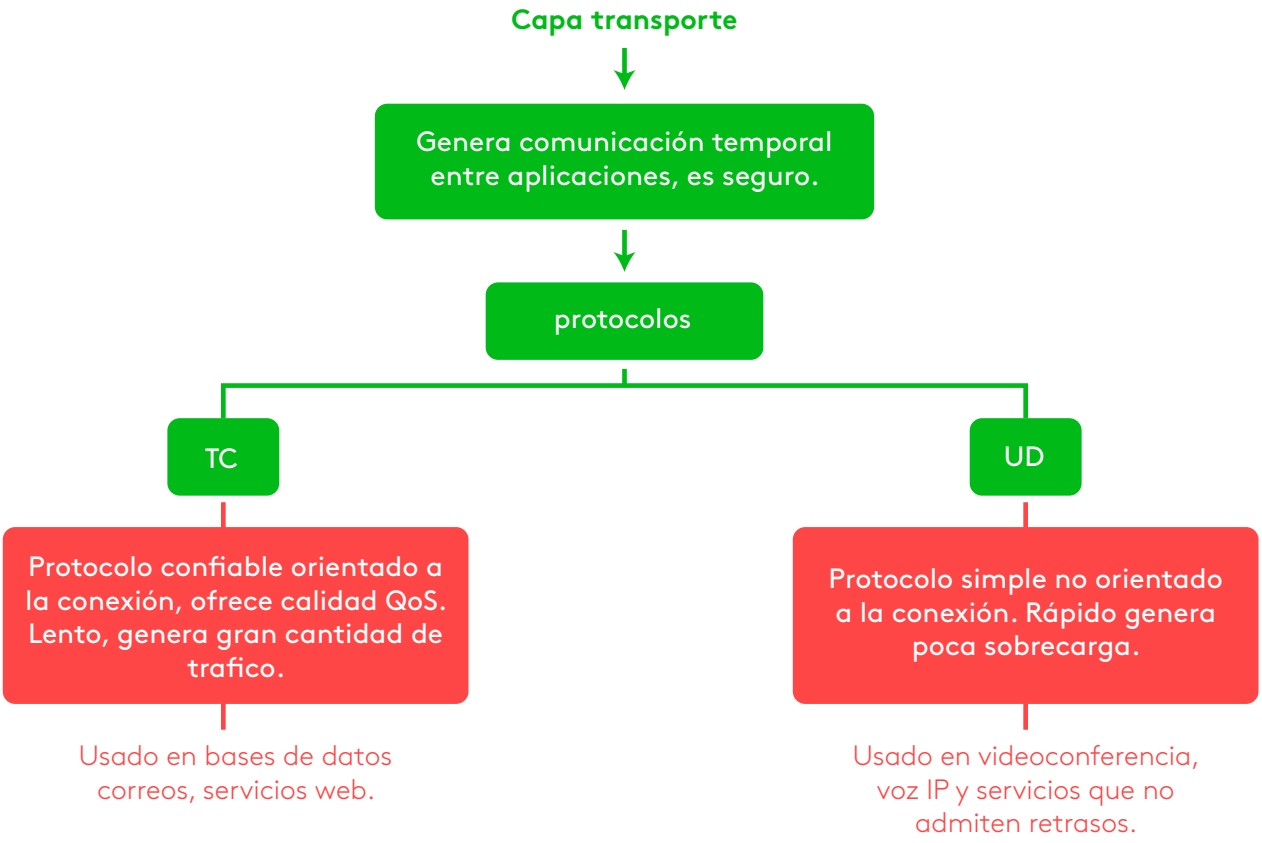


Figura 1. Mapa conceptual capa de transporte
Fuente: propia

La capa de transporte denominada capa 4 del modelo OSI se encarga de generar una comunicación temporal entre aplicaciones que desean intercambiar datos, realizando un seguimiento a dicha conversación desde el origen hasta el destino, es la intermediaria entre la capa de aplicación y la capa de red.

Veamos una videocápsula que nos explica la funcionalidad de la capa de transporte y los protocolos UDP y TCP:

Video

Capa de transporte ½.
https://youtu.be/sFLjtTff8UA

¡Continuemos!

En la capa de transporte a la PDU se le denomina segmento, ya que esta capa es la encargada de recibir los datos de la capa de aplicación y dividirlos en segmentos más pequeños para que estos sean más fáciles de transportar y administrar. A cada segmento se le agrega un encabezado para su rearmado y para realizar seguimiento al mismo.

En la capa de transporte trabajan los protocolos TCP y UDP los cuales describirán cómo se usa la información del encabezado para rearmar los datos de flujo y enviarlos a la capa de aplicación de tal forma que sean entendidos por esta.

TCP
Protocolo de control de transmisión.

UDP
Protocolo de datagrama de usuario.

Conversaciones
Hace referencia a los datos que fluyen entre una aplicación origen y un destino.

Además, también debe garantizar que, aunque se ejecuten varias aplicaciones en los dispositivos cada aplicación reciba los datos correctos, para que esto suceda utiliza la asignación de un número de puerto a cada aplicación, el cual será su identificación en el dispositivo. Cualquier programa o *software* que requiera acceder a la red necesitará este identificador.

Por otra parte, la segmentación de los datos permite que la red pueda ser utilizada por varias aplicaciones al tiempo a esto se le denomina multiplexión.

Analicemos... Si no se segmentan los datos ¿Qué pasaría al ver un video o una película en línea?

Como bien lo sabemos los videos consumen muchos recursos de red, si no se segmenta el video se consumiría todo el ancho de banda de la red, impidiendo que otras aplicaciones pudiesen transportar datos por la red de forma simultáneamente, generando lentitud, retrasos de comunicación, exceso de, control de errores, entre otros.

Otra tarea importante de la capa de transporte, es la administración de la confiabilidad de las conversaciones.

Para profundizar en el tema los invito a realizar la lectura del libro:

Visitar página

La red Internet. El modelo TCP/IP. https://goo.gl/yixt8j

Andrés Aznar López.

Especialmente el capítulo 4 Modelo TCP/IP el tema Nivel de transporte.

Protocolo TCP

Para comenzar veamos una videocápsula que nos explica las características de los protocolos de la capa de transporte UDP y TCP:

Video

Protocolos UDP-TCP.

https://youtu.be/JnXO7L4gcJo

El protocolo TCP se considera un protocolo confiable porque garantiza que los datos lleguen al destino, por medio de un mensaje de confirmación de recibido ACK, asegurando la entrega del paquete.

TCP es un protocolo orientado a la conexión esto quiere decir que se debe generar un anuncio entre emisor-receptor y ser aceptado por ambas partes antes de comenzar a transmitir.

Por lo anterior TCP es un protocolo más pesado y lento, pues debe agregar campos en el encabezado TCP y genera mayor tráfico en la red por el ACK.

Las aplicaciones apropiadas para este protocolo son aquellas que requieren confiabilidad sin importar el retraso, ejemplo de estas son las bases de datos, el correo electrónico, los navegadores web, entre otros, cualquier pérdida de datos afectará la integridad de la información y puede llegar a dejarla inservible.

Entre las tareas TCP tiene que:

- Establecer la conexión.
- Enumerar y dar seguimiento a los segmentos.
- Monitorear el flujo de datos.
- Ordenar los segmentos para rearmar los datos.
- Controlar el flujo de datos.
- Confirmar recibido de datos, de no confirmar hacer reenvió de los datos.

Protocolo UDP

El protocolo UDP es un protocolo simple y no confiable ya que no garantiza que los datos lleguen al destino, tiene menos campos en el encabezado lo cual lo hace más rápido que el TCP.

UDP proporciona funciones básicas en entrega de datos con muy poca sobrecarga y hace una muy buena relación de costo beneficio, de acá la importancia de este protocolo ya que no siempre se requiere de una confirmación en las aplicaciones.

UDP se conoce como un protocolo de máximo esfuerzo (poco confiable), no orientado a la conexión es decir no hay un establecimiento de sesión previa entre emisor y receptor, los datos se reconstruyen en el orden que se reciben si se pierde algún segmento de datos no se reenvía, se omite y se trata de reconstruir con la información que llegó, su gran ventaja la rapidez de transmisión.

Las aplicaciones que toleran pérdida de datos pero que requieren una entrega sin retraso son las adecuadas para este protocolo, por ejemplo: Voip, video en directo, audio, entre otros.

Cada aplicación requiere un número de puerto que lo asocia al tipo de conversación, de esta manera se pueden tener múltiples aplicaciones en un mismo instante y los datos serán entregados de forma apropiada a la aplicación requerida.

Para profundizar en el tema los invito a realizar la lectura del libro:

Visitar página

La red Internet. El modelo TCP/IP. https://goo.gl/yixt8j

Rafael Castaño.

Especialmente el capítulo 9 *Capa de transporte*.

IANA
Autoridad de números asignados de Internet.

Firewall
Firewall o cortafuegos brinda seguridad a los equipos bloqueando puertos.

Números de puertos

La IANA entidad encargada de controlar la asignación de direcciones IP, nombres de dominios; también se encarga de la asignación de los puertos para aplicaciones o procesos, cuenta con 65.535 puertos divididos en tres grupos, puertos bien conocidos, puertos registrados y puertos dinámicos.

La siguiente tabla muestra los rangos de puertos y su descripción:

Nombre	Rango de puertos	Descripción
Puertos bien conocidos	0 - 1023	Se utilizan para los principales servicios correo, servicios web, transferencia de archivos, entre otros.
Puertos registrado	1024- 49151	Se asignan a procesos o aplicaciones específicas como programas o *software*, la compañía desarrolladora del *software* lo debe solicitar a la IANA.
Puertos dinámicos y/o privados	49152- 65353	Puerto dinámico que se utiliza para identificar una aplicación-cliente durante la comunicación.

Tabla 1. Rangos de puertos y su descripción
Fuente: propia

Es importante conocer los puertos más utilizados, ya que de estos depende la comunicación, el Firewall por defecto y como medida de protección bloquea la mayoría de los puertos y esto podrá causar traumatismos en la red al no poder acceder a procesos, servicios y/o programas.

La siguiente tabla muestra algunos de los principales puertos y su descripción:

# Puerto	Tipo	Nombre	Descripción
21	TCP	FTP	Protocolo de transferencia de archivos.
22	TCP	SSH	Conexión remota segura.
23	TCP	TELNET	Conexión remota no segura.
25	TCP	SMTP	Protocolo simple de transferencia de correo.
69	UDP	TFTP	Protocolo de transferencia simple de archivo.
80	TCP	HTTP	Protocolo de transferencia de hipertexto www (Internet).
88	TCP	KERBEROS	Agente de autenticación.
110	TCP	POP3	Protocolo de correo.
123	UDP	NTP	Protocolo de sincronización de tiempo.
143	TCP	IMAP	Protocolo de acceso a mensajes de Internet.
443	TCP	HTTPS	Transferencia segura de páginas de Internet.

Tabla 2. Rangos de puertos más usados y su descripción.
Fuente: propia

```
C:\Users\RicardoL>netstat -n -a

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:843          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:17600        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27015        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27015        127.0.0.1:49159        ESTABLISHED
  TCP    127.0.0.1:27015        127.0.0.1:50586        ESTABLISHED
  TCP    127.0.0.1:45777        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49159        127.0.0.1:27015        ESTABLISHED
  TCP    127.0.0.1:49583        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:50586        127.0.0.1:27015        ESTABLISHED
  TCP    127.0.0.1:51300        127.0.0.1:51301        ESTABLISHED
  TCP    127.0.0.1:51301        127.0.0.1:51300        ESTABLISHED
  TCP    127.0.0.1:51308        127.0.0.1:51309        ESTABLISHED
  TCP    127.0.0.1:51309        127.0.0.1:51308        ESTABLISHED
  TCP    127.0.0.1:58067        127.0.0.1:58068        ESTABLISHED
  TCP    127.0.0.1:58068        127.0.0.1:58067        ESTABLISHED
  TCP    169.254.221.231:139    0.0.0.0:0              LISTENING
  TCP    192.168.0.8:80         0.0.0.0:0              LISTENING
  TCP    192.168.0.8:139        0.0.0.0:0              LISTENING
  TCP    192.168.0.8:443        0.0.0.0:0              LISTENING
  TCP    192.168.0.8:22139      0.0.0.0:0              LISTENING
  TCP    192.168.0.8:49237      177.191.88.195:443     SYN_SENT
  TCP    192.168.0.8:63280      65.55.252.167:443      ESTABLISHED
  TCP    192.168.0.8:63282      64.4.23.146:33033      ESTABLISHED
  TCP    192.168.0.8:63289      50.16.228.90:80        ESTABLISHED
  TCP    192.168.0.8:63320      52.225.133.157:443     ESTABLISHED
  TCP    192.168.0.8:63327      157.56.17.248:443      ESTABLISHED
  TCP    192.168.0.8:63709      108.177.11.188:5228    ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  UDP    127.0.0.1:56401        *:*
  UDP    127.0.0.1:60810        *:*
  UDP    127.0.0.1:60811        *:*
  UDP    127.0.0.1:63299        *:*
  UDP    127.0.0.1:63300        *:*
  UDP    169.254.221.231:137    *:*
  UDP    169.254.221.231:138    *:*
  UDP    169.254.221.231:1900   *:*
  UDP    169.254.221.231:5353   *:*
  UDP    192.168.0.8:137        *:*
  UDP    192.168.0.8:138        *:*
  UDP    192.168.0.8:443        *:*
  UDP    192.168.0.8:1900       *:*
  UDP    192.168.0.8:22139      *:*
  UDP    192.168.0.8:56400      *:*
  UDP    [fe80::3cf3:addc:af1a:dde7%17]:1900  *:*
  UDP    [fe80::3cf3:addc:af1a:dde7%17]:5353  *:*
  UDP    [fe80::bc60:124b:3590:6ba2%12]:1900  *:*
  UDP    [fe80::bc60:124b:3590:6ba2%12]:56396  *:*
```

Comandos importantes para trabajo en redes

***Netstat*:** es una herramienta que permite descubrir los puertos activos locales y remotos al igual que el tipo de protocolo utilizado TCP o UDP y el estado en que se encuentra la conexión.

En la siguiente figura observamos los resultados de *netstat*.

Figura 2. Resultados de emitir el comando *netstat*
Fuente: propia

***IPconfig*:** es una aplicación de Windows que nos permite reconocer los parámetros de configuración de la red TCP/IP, nos muestra la dirección física (NIC) de cada dispositivo disponible en el equipo, la dirección IP configurada, la máscara de red, el *gateway* al igual que los DNS.

En la siguiente figura observamos los resultados del comando *IPconfig*.

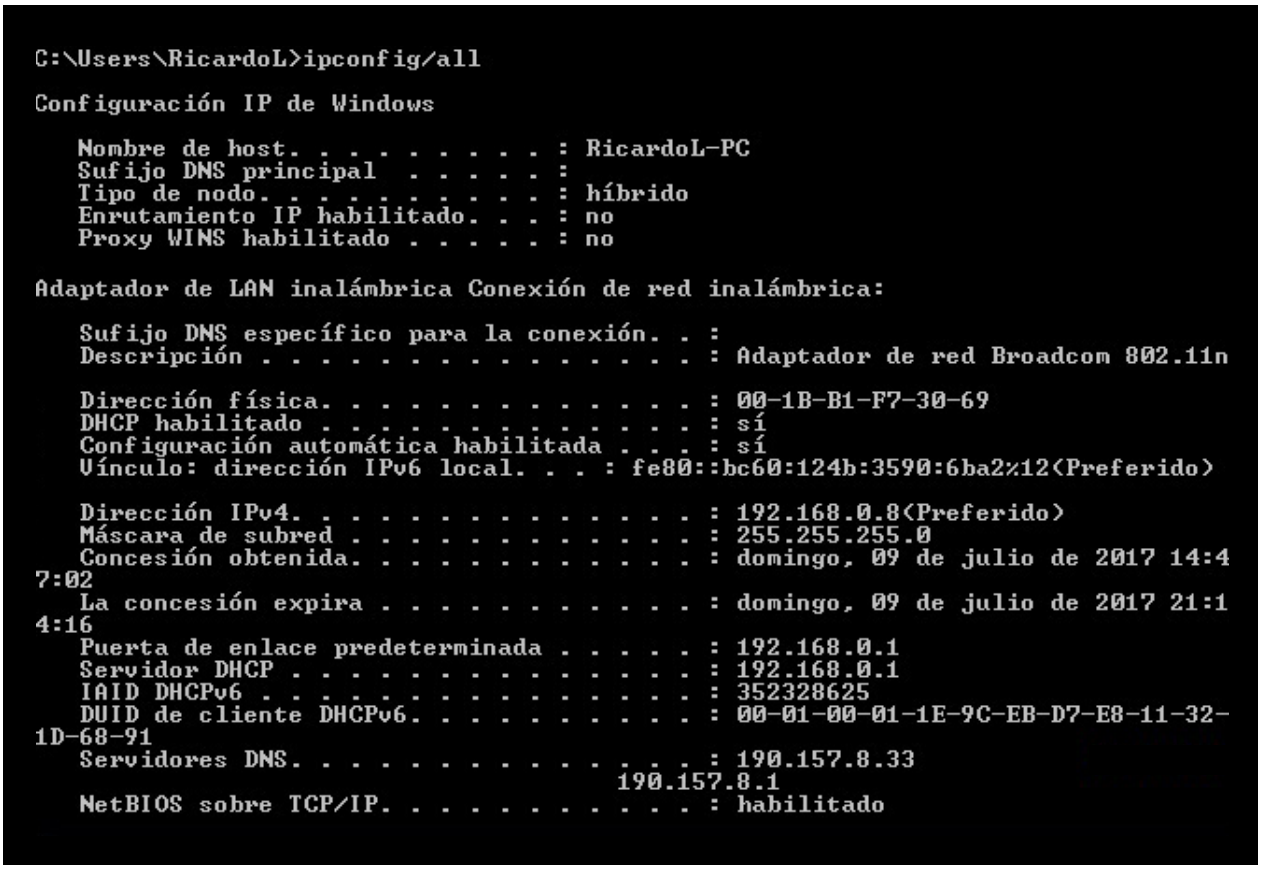


Figura 3. Resultado de emitir el comando IPconfig
Fuente: propia

De la imagen anterior podemos extraer datos importantes que nos ayudarán a configurar la red y a detectar posibles errores.

Entre los datos más relevantes tenemos:

1. Dirección Mac 00-1B-B1-F7-30-39 (dirección física de la tarjeta de red NIC inalámbrica).
2. Dirección IPv4 192.168.0.8
3. Mascara 255.255.255.0
4. *Gateway* (puerta de enlace) 192.168.0.1
5. Servidor DHCP 192.168.0.1
6. Servidor DNS 190.157.8.33 y 190.157.8.1

Aparte de la información extraída también nos indica que estamos recibiendo una dirección dinámica que pertenece a un rango privado clase C 192.168.0.0/24 por medio de un servidor DHCP y que esta dirección tiene un tiempo límite o de expiración.

Por otra parte, es importante observar que la puerta de enlace o *gateway* está en la misma red que la dirección del equipo. Mientras que los DNS pertenecen a una red externa pública.

***Ping*:** es una utilidad de ECO que permite comprobar la conectividad con otras máquinas utiliza el protocolo ICMP en IPv4 y el protocolo ICMPv6 para IPv6. Envía 4 paquetes y muestra el estado, velocidad y calidad de la red.

ICMP
Internet Control Message Protocol o protocolo de mensajes de control de Internet, utilizado con fines de diagnóstico.

En Windows se ejecuta en la consola de comandos de DOS, en los *router* se ejecuta en modo privilegiado.

Se puede dar *ping* a una dirección IP o a un nombre de dominio.

En la siguiente figura observamos los resultados del *ping* por dirección y por nombre de dominio.

```
:\Users\RicardoL>ping 216.58.222.206

aciendo ping a 216.58.222.206 con 32 bytes de datos:
espuesta desde 216.58.222.206: bytes=32 tiempo=22ms TTL=57
espuesta desde 216.58.222.206: bytes=32 tiempo=19ms TTL=57
espuesta desde 216.58.222.206: bytes=32 tiempo=14ms TTL=57
espuesta desde 216.58.222.206: bytes=32 tiempo=19ms TTL=57

stadísticas de ping para 216.58.222.206:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
iempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 14ms, Máximo = 22ms, Media = 18ms

:\Users\RicardoL>PING CISCO.COM

aciendo ping a CISCO.COM [72.163.4.161] con 32 bytes de datos:
espuesta desde 72.163.4.161: bytes=32 tiempo=117ms TTL=240
espuesta desde 72.163.4.161: bytes=32 tiempo=154ms TTL=240
espuesta desde 72.163.4.161: bytes=32 tiempo=170ms TTL=240
espuesta desde 72.163.4.161: bytes=32 tiempo=129ms TTL=240

stadísticas de ping para 72.163.4.161:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
iempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 117ms, Máximo = 170ms, Media = 142ms
```

Figura 4. Resultado de emitir el comando *ping*
Fuente: propia

De la imagen anterior podemos concluir que existe comunicación con la dirección IP pública 216.58.222.206 con un tiempo promedio de respuesta de 18 ms.

También es interesante observar que, si tengo el nombre de dominio, el comando *ping* me ayudará a descubrir la dirección IP, si observamos la parte media de la imagen vemos que se realiza *ping* al dominio **cisco.com** y él nos responde con la dirección IPv4 del servidor el cual tiene la dirección pública 72.163.4.161 y un tiempo promedio de 142 ms.

Consultemos: ¿Cuál será la razón para que el tiempo de respuesta de la primera dirección sea tan diferente al tiempo de respuesta del servidor *Cisco*?

***Tracert*:** esta aplicación de diagnóstico ECO permite hacer seguimiento de un paquete desde el origen hasta el destino, mostrándonos el camino que toma el paquete, el tiempo que dura y los saltos que da (# de *router* por los que pasa).

Tracert al igual que el PING utiliza el protocolo ICMP.

En la siguiente figura observamos los resultados del comando *tracert*.

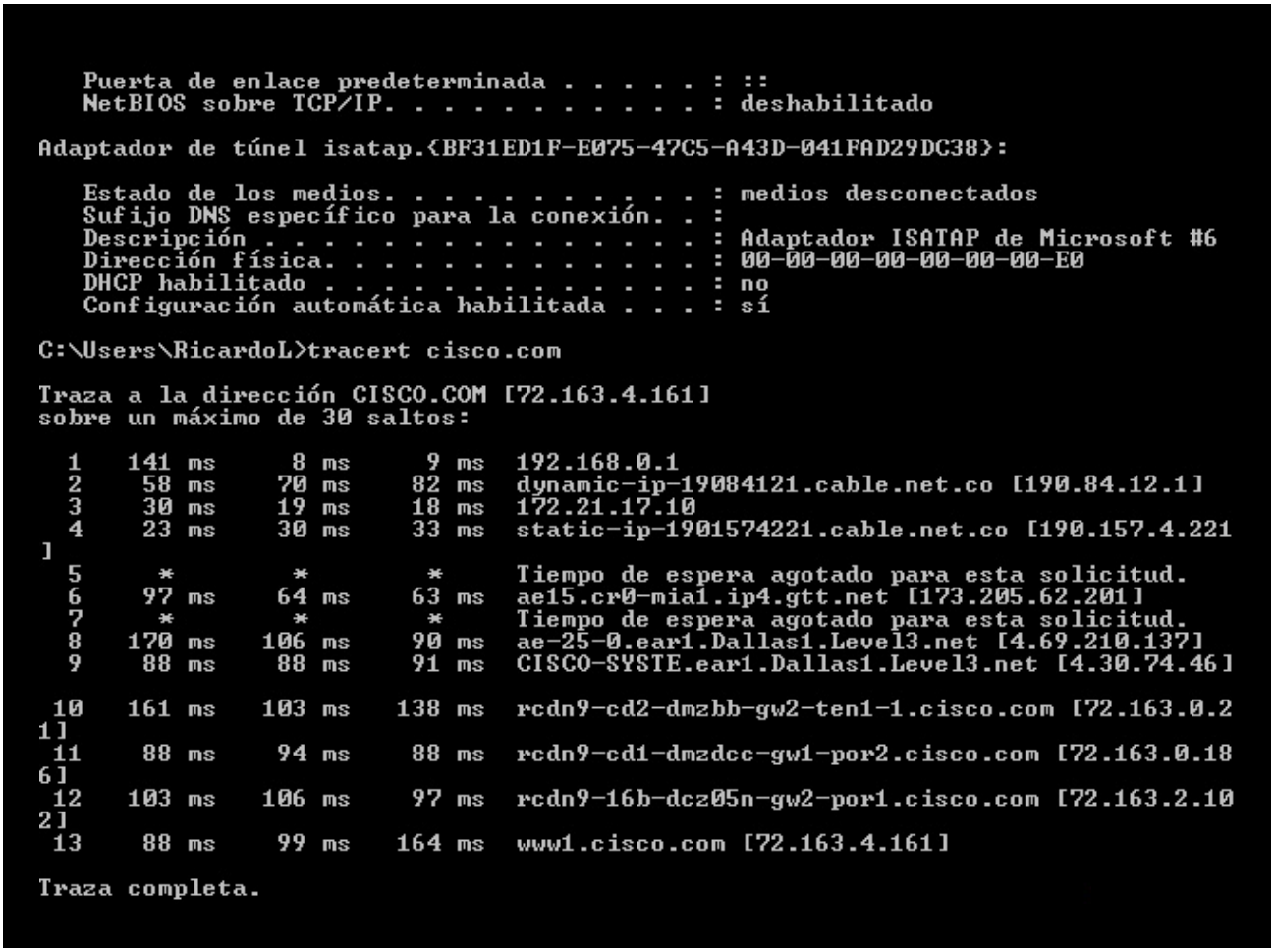


Figura 5. Resultado de emitir el comando *tracert*
Fuente: propia

En la imagen anterior observamos que al generar la traza para el dominio **cisco.com** este se completa en 13 saltos, pero se generaron dos saltos fallidos es decir el número de *router* por los que pasa el paquete es 11.

Podríamos determinar la ubicación geográfica de cada *router* con la dirección pública que nos muestra, y con la ayuda de páginas como:

Visitar página

Geolocalizar IP. https://goo.gl/3sXyfM

Ver Dirección de Geo IP. http://es.geoipview.com

En estas páginas basta poner la dirección IP pública y nos mostrara en un mapa donde está localizado el servidor.

Instrucción

Los invito a desarrollar la actividad de repaso 1, con la cual desarrollarán destrezas en el uso de comandos que permiten generar seguimiento a la red.

Capa de aplicación modelo TCP/IP

Para dar inicio al tema los invito a observar la videocápsula "Capa de aplicación" en la cual se explica el funcionamiento de dicha capa y los principales protocolos que actúan en esta:

Video

Capa de aplicación del modelo TCP/IP. https://youtu.be/hIXWhQkCpaw

El proceso de transmisión de información está dado por las cuatro capas inferiores del modelo OSI (capa física, capa de enlace de datos, capa de red y capa de transporte), la capa de aplicación no interviene en este proceso.

Les recomiendo leer el capítulo 10 del siguiente libro:

Lectura recomendada

Redes locales. https://goo.gl/R24CL6

Rafael Castaño.

Analicemos el mapa conceptual a continuación:

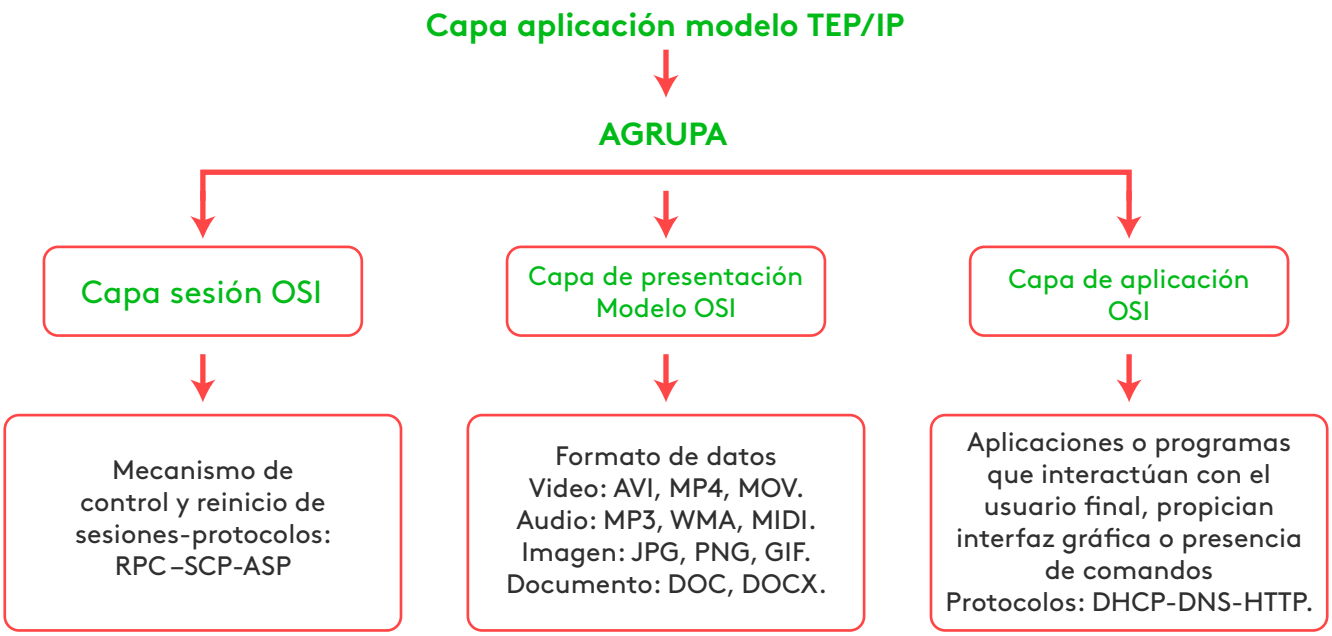


Figura 6. Mapa conceptual capa de aplicación
Fuente: propia

La capa de aplicación del modelo TCP/IP abarca las tres capas superiores del modelo OSI (sesión, presentación y aplicación), es la capa que se encarga de interactuar con el usuario final, en esta capa a la PDU se le denomina DATO.

La capa de aplicación está determinada por los protocolos y las aplicaciones a usuario final. Los protocolos de esta capa permiten intercambiar datos entre programas determinando permisos y aplicaciones asociadas para poderse ejecutar.

Existen múltiples protocolos en capa de aplicación entre los más utilizados tenemos HTTP, HTTPS, FTP, IMAP, DNS, SMTP, POP3.

Capa de sesión: es la quinta capa del modelo OSI, en esta capa se generan mecanismos de control entre aplicaciones, creando y manteniendo control de diálogo (*Half-dúplex, full-dúplex*), y reiniciando sesiones que se interrumpen o han estado inactivas.

Dentro de los protocolos de esta capa tenemos:

- RPC protocolo que permite ejecutar código de forma remota.
- SCP protocolo que permite ejecutar código de forma remota y de forma segura, ya que hace uso del protocolo SSH.
- ASP protocolo de sesión desarrollado por *Apple*, proporciona servicios de solicitud de respuestas, se encarga del establecimiento de la sesión, su mantenimiento y cierre.

Los servicios ofrecidos por la capa de sesión **no** son indispensables, en muchas aplicaciones no se requieren dichos servicios.

Capa de presentación: esta capa tiene como funciones dar formato a los datos para que sean reconocidos por otros dispositivos, comprimir los datos en el origen para luego descomprimirlo en el destino, al igual que cifrar los datos en el origen y descifrarlos en el destino.

Es importante reconocer el formato de los datos para determinar qué aplicación los puede abrir, los formatos vienen dados por las extensiones que acompañan el nombre del archivo después del punto.

Ejemplos: dibujo1.JPG, tarea.DOCX, estadística.XLS

Del ejemplo anterior concluimos que:

- El archivo "dibujo1" es una imagen, pues trae el formato de imagen JPG;
- El archivo "tarea" es un archivo de texto pues presenta extensión DOCX;
- El archivo "estadística" es una hoja de cálculo ya que su extensión es XLS.

Entre los principales formatos de audio video e imagen tenemos:

Tipo de formato	Tipo de documento
GIF, JPG, BMP, PNG	Imágenes
AVI, MP4, WMV,MOV	Vídeos
MP3, MP4, WMA, WAV, MIDI	Audio

Tabla 3. Rangos de puertos más usados y su descripción
Fuente: propia

Capa de aplicación: es la capa final del modelo OSI (capa 7) y del modelo TCP/IP (capa 4), encargada de aplicaciones o programas que interactúan con el usuario final, proporcionando interfaz entre las aplicaciones y comunicación con el usuario, define los protocolos que requieren las aplicaciones para el intercambio de datos.

Lectura recomendada

Capa de Aplicación

Aníbal Coto Cortés.

Esta capa es de gran crecimiento ya que continuamente se crean programas, protocolos y servicios.

Los invito a ver la videocápsula "Capa de aplicación y funcionalidad de los protocolos, CCNA 1", con la cual aclaran dudas respecto a la funcionalidad de la capa de aplicación:

Video

Capa de aplicación y funcionalidad de los protocolos.

https://youtu.be/ZWiYVRBnSI0

Manos a la obra

En esta sección nos dedicaremos a entender algunos de los protocolos más importantes de la capa de aplicación y desarrollar la configuración con la ayuda de simuladores.

Requerimientos: simulador *Packet tracer*, dos *switch* 2960, dos servidores y seis computadores.

Realizar la topología que aparece en la siguiente imagen.

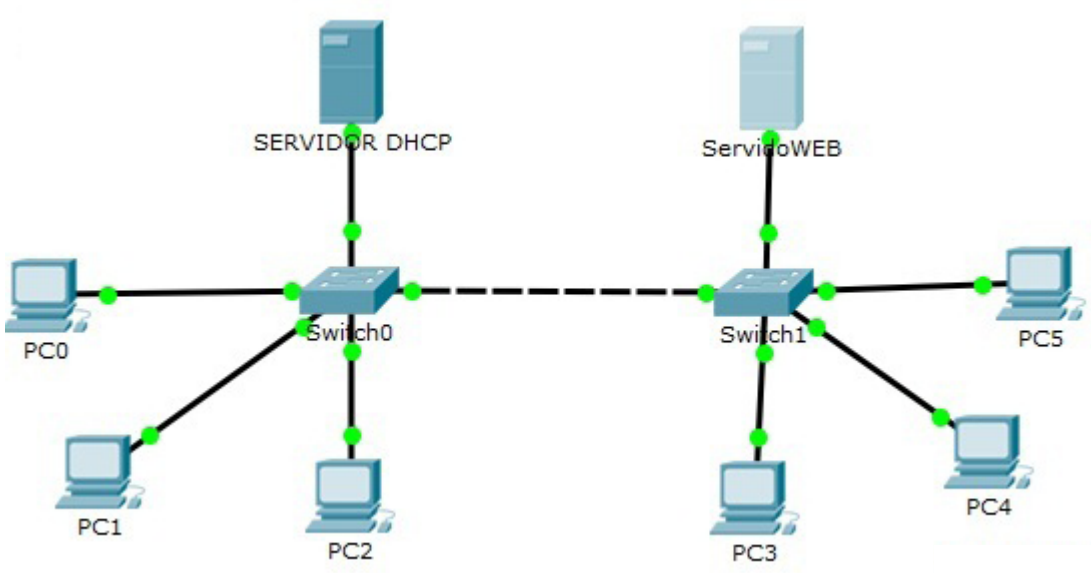


Figura 7. Topología a realizar
Fuente: propia

Protocolo DCHP (*Dynamic Host Configuration Protocol*): protocolo de configuración dinámica de *host*, este protocolo permite realizar la asignación dinámica de direcciones IP al *host*. Se puede configurar desde un servidor o desde un dispositivo capa 3, *switch* multicapa (capa 3) o *router* (la configuración por medio de *switch* multicapa y *router* se trabajará en materias posteriores).

Configuración del servidor DHCP

1. Asignar dirección IP estática al servidor DHCP, dirección de *gateway* y dirección de DNS. Con los siguientes datos, IP 192.168.1.10, mascara 255.255.255.0, puerta de enlace 192.168.1.1, y DNS 100.10.75.32

2. Dentro del servidor nos dirigimos a pestaña ***Service***, luego clic en el servicio DHCP, y procedemos a configurar la dirección de *gateway*, y la dirección de DNS que se entregará a los equipos, también podemos elegir desde qué dirección comenzará a asignar IP (para el ejemplo 192.168.1.100) y cuantas direcciones asignarás, una vez asignado todos los valores damos clic en ***Save*** si todo está bien nos debe mostrar en la parte inferior la información que hemos configurado.

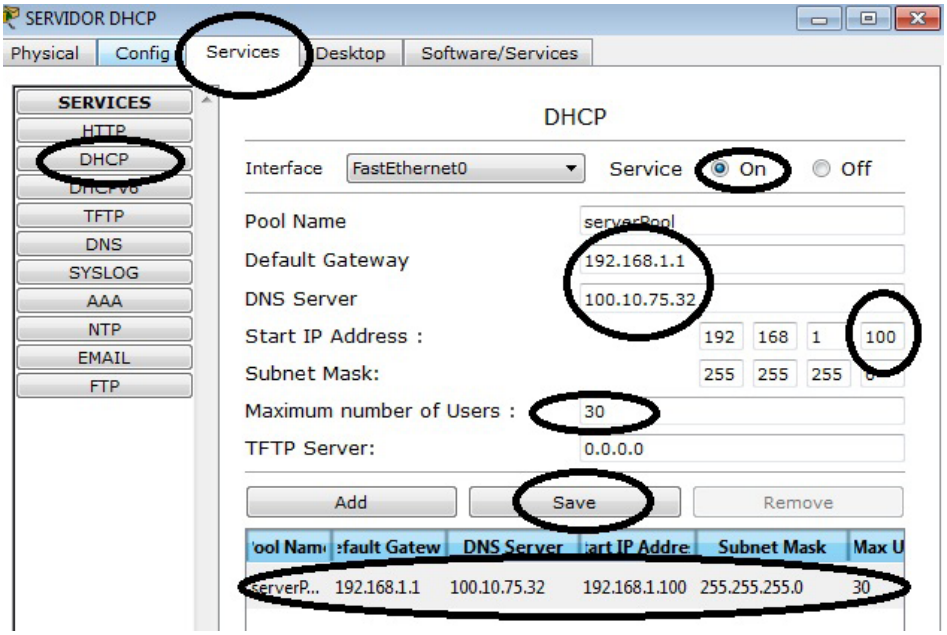


Figura 8. Pestaña *service*
Fuente: propia

3. Una vez configurados todos los parámetros del servidor DCHP, el servicio se debe iniciar (**on**).

4. Para que los PC reciban dirección IP es necesario colocar cada equipo en modo DHCP de configuración IP.

En la siguiente imagen observamos que tan pronto colocamos el PC en modo DHCP, este recibe la primera dirección del rango de direcciones IP disponibles del DHCP, al igual que la máscara, puerta de enlace y DNS:

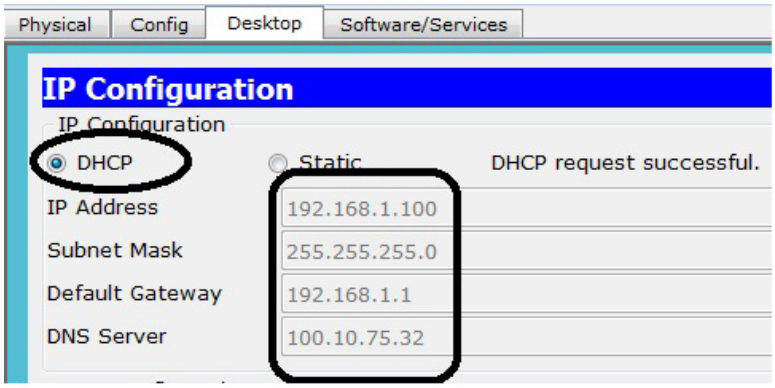


Figura 9. PC en modo DHCP
Fuente: propia

5. Una vez asignada la dirección IP a todos los equipos, realizar pruebas de conectividad mediante envió de paquetes.

Atención: una buena práctica administrativa es asignar direccionamiento estático a todos los servidores, equipos activos de red, e impresoras de red.

Protocolo HTTP: protocolo de transferencia de hipertexto, este genera un servicio web mediante el servidor HTTP o servidor web, el cual permite el acceso y el hospedaje o alojamiento a una página web.

Entre los principales tipos de servidores web del mercado tenemos:

- **Apache**: servidor gratuito de código abierto y multiplataforma; comúnmente lo encontramos en las *suites* de desarrollo web como *Wamp server*.
- **IIS**: propietario de Microsoft, viene preinstalado con los sistemas operativos Windows *server* y solo funciona con máquinas Windows.
- **Sun *Java***: el servidor *Sun Java* web *server* propietario de Sun, en la actualidad es de código abierto y multiplataforma.

Configurando servidor web en *Packet tracer*

Dentro del menú servicios de los servidores en *Packet tracer* se cuenta con la opción HTTP.

1. Abrir el servidor web del ejemplo anterior, configurar la dirección IP 192.168.10.11 y los de más parámetros iguales al servidor DHCP.
2. Nos ubicamos en la pestaña **Servicios** y seleccionamos el menú HTTP.
3. Seleccionar la opción Index.html (index.html es el identificador de la página principal del dominio), y clic en editar (lo editamos para personalizar el ejercicio y comprobar el funcionamiento).
4. Se abre el editor HTML que contiene el código de una página web de ejemplo, la cual se puede editar (para nuestro caso cambiaremos el texto "*Cisco Packet tracer*" por "Fundación Universitaria Del Área Andina".
5. Salvar y activar el servicio de http y https (por defecto en *Packet tracer* viene activo **on**).
6. Ingresar a cualquier PC pestaña *desktop* y seleccionamos el navegador (*web browser*).
7. En la URL, escribir la dirección del servidor web, al dar clic se visualizará la página web que se había editado.

Para reafirmar conocimientos sobre los protocolos web recomiendo la lectura complementaria:

Visitar página

La red Internet. El modelo TCP/IP. https://goo.gl/yixt8j

Andrés Aznar López.

Especialmente el capítulo *5 Desarrollo de aplicaciones web*.

En la siguiente imagen observamos la activación del servidor HTTP y la edición del archivo Index.html:

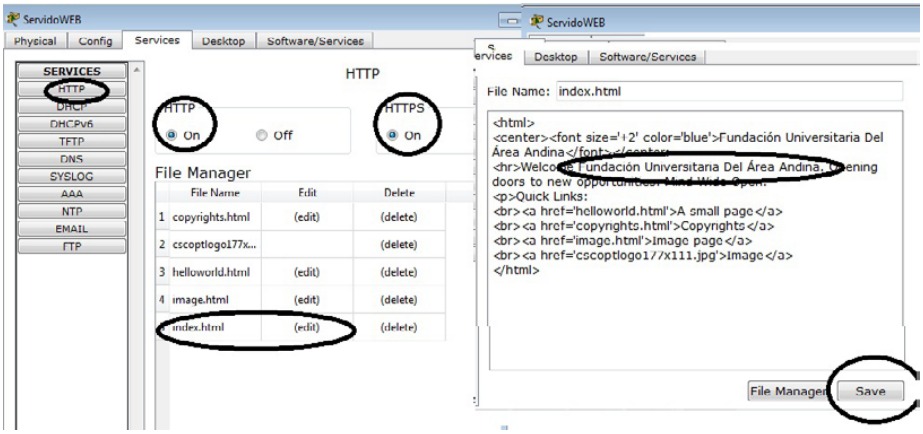


Figura 10. activación del servidor HTTP y la edición del archivo Index.html
Fuente: propia

En la siguiente imagen se observa el acceso vía navegador web desde el PC al servidor HTTP y a la página web editada.

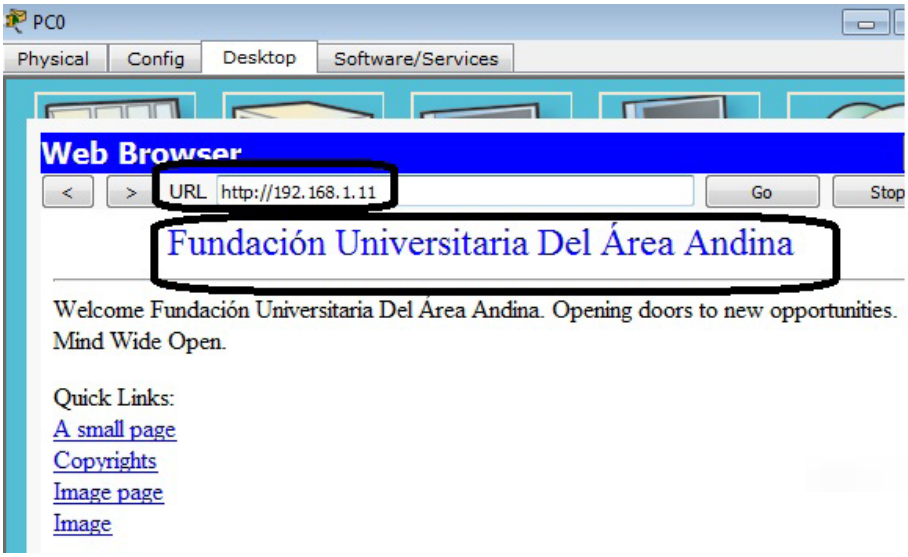


Figura 11. Acceso vía navegador web desde el PC al servidor HTTP y a la página web editada
Fuente: propia

Propongamos: ¿Qué otros servicios son fundamentales en la configuración de una red de área local LAN?

Instrucción

A este punto le invitamos a desarrollar la actividad de repaso 2.

BIBLIOGRAFÍA

Aznar, L. (2005). *La red Internet. El modelo TCP/IP.* Madrid, España: Grupo Abantos Formación y Consultoría.

Bellido, Q. (2014). *Equipos de interconexión y servicios de red (UF1879)*. Madrid, España: IC Editorial.

Bermúdez, L. (2012). *Montaje de infraestructuras de redes locales de datos: UF1121*. Madrid, España: IC Editorial.

Calvo, G. (2014). *Gestión de redes telemáticas (UF1880)*. Madrid, España: IC Editorial.

Castaño, R., y López, F. (2013). *Redes locales.* Madrid, España: Macmillan Iberia, S.A

Feria, G. (2009). *Modelo OSI.* Córdoba, Argentina: El Cid Editor | apuntes.

García, M. (2012). *Mantenimiento de infraestructuras de redes locales de datos (MF0600_2)*. Málaga, España: IC Editorial.

Íñigo, G., Barceló, O., y Cerdà, A. (2008). *Estructura de redes de computadores.* Barcelona, España: Editorial UOC.

Martínez, Y., y Riaño, V. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6.* Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.

Molina, R. (2014). *Implantación de los elementos de la red local.* Madrid, España: RA-MA Editorial.

Mora, J. (2014). *Desarrollo del proyecto de la red telemática (UF1870)*. Madrid, España: IC Editorial.

Purser, M. (1990). *Redes de telecomunicación y ordenadores.* Madrid, España: Ediciones Díaz de Santos.

Roa, B. (2013). *Seguridad informática.* Madrid, España: McGraw-Hill España.

Robledo, S. (2002). Redes de computadoras. Ciudad de México, México: Instituto Politécnico Nacional.

BIBLIOGRAFÍA

Romero, J. (2009). *Estudio de subnetting, VLSM, Cidr y comandos de administración y configuración de routers*. Córdoba, Argentina: El Cid Editor | Apuntes.

S.L. Innovación y Cualificación. (2012). *Guía para el docente y solucionarios: montaje y mantenimiento de sistemas de telefonía e infraestructuras de redes locales de datos*. Málaga, España: IC Editorial.

Vásquez, D. (2009). *Base de la teleinformática*. Córdoba, Argentina: El Cid Editor | apuntes.

Velte, T., y Velte, A. (2008). *Manual de Cisco*. Ciudad de México, México: McGraw-Hill Interamericana.

Esta obra se terminó de editar en el mes de Septiembre 2018
Tipografá BrownStd Light, 12 puntos
Bogotá D.C,-Colombia.

AREANDINA

Fundación Universitaria del Área Andina

MIEMBRO DE LA RED

ILUMNO