UNIREMINGTON®
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

# REDES DE DATOS I

## INGENIERÍA DE SISTEMAS

## FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA

Vicerrectoría de Educación a Distancia y virtual

2016

## AUTOR

**Roberto Carlos Guevara Calume**
Ingeniero de sistemas – especialista en redes corporativas e integración de tecnologías. Magister automatización y control industrial
roberto.guevara@uniremington.edu.co

**Nota:** el autor certificó (de manera verbal o escrita) No haber incurrido en fraude científico, plagio o vicios de autoría; en caso contrario eximió de toda responsabilidad a la Corporación Universitaria Remington, y se declaró como el único responsable.

## RESPONSABLES

**Jorge Mauricio Sepúlveda Castaño**
Decano de la Facultad de Ciencias Básicas e Ingeniería
jsepulveda@uniremington.edu.co

**Eduardo Alfredo Castillo Builes**
Vicerrector modalidad distancia y virtual
ecastillo@uniremington.edu.co

**Francisco Javier Álvarez Gómez**
Coordinador CUR-Virtual
falvarez@uniremington.edu.co

## GRUPO DE APOYO

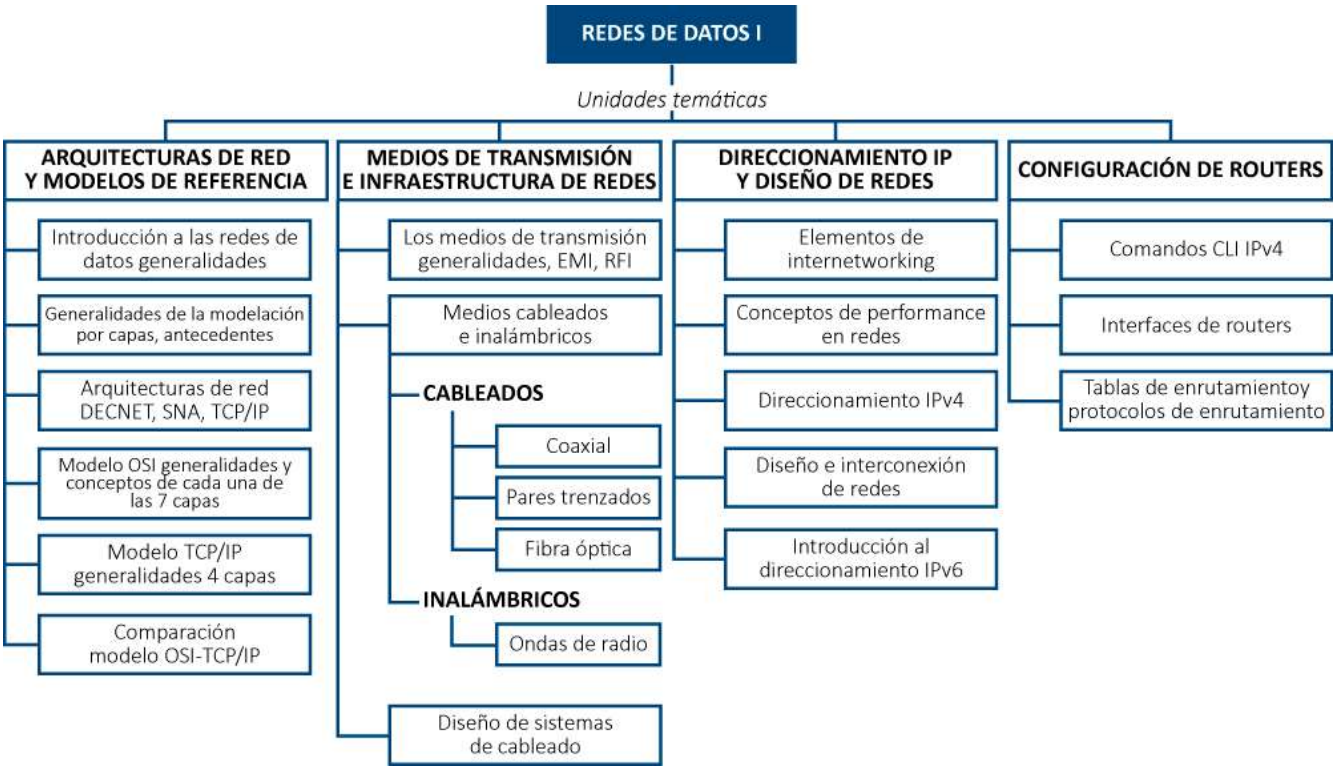
Personal de la Unidad CUR-Virtual
EDICIÓN Y MONTAJE

Primera versión. Febrero de 2011.
Segunda versión. Marzo de 2012
Tercera versión. noviembre de 2015
Cuarta versión 2016

# TABLA DE CONTENIDO

Pág.

# 1 MAPA DE LA ASIGNATURA



# 2 UNIDAD I ARQUITECTURAS DE RED Y MODELOS DE REFERENCIA

Esta unidad temática hace una Introducción a las redes de datos, historia, generalidades de la modelación por capas, se estudian las diferentes Arquitecturas de red.

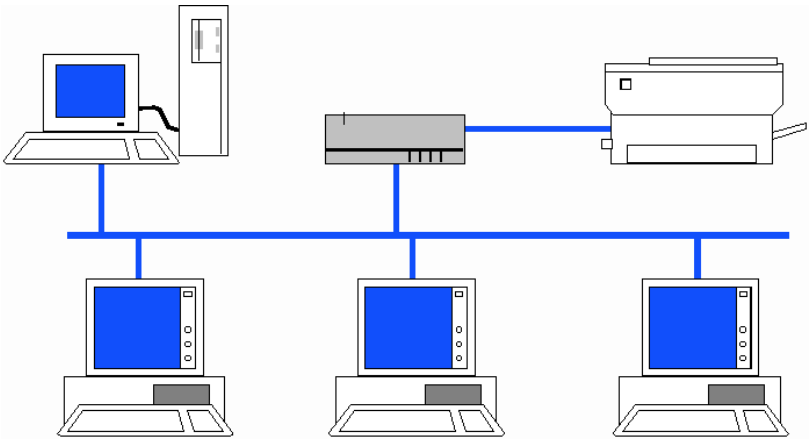
Como punto de partida se usa el modelo OSI Generalidades y conceptos de cada una de las 7 Capas, además se estudia conceptualmente el protocolo TCP/IP haciendo una comparación entre ellos

## 2.1 TEMA 1 INTRODUCCIÓN A LAS REDES DE DATOS GENERALIDADES,

**Las redes de datos** permiten **la interconexión** de muchos elementos, bien sea para **compartir** impresoras, bases de datos, archivos o conexión a internet. A continuación, se hará una introducción a las redes de datos sus generalidades.

### 2.1.1 QUE ES UNA RED DE DATOS

Una red datos, realmente es un conjunto de **elementos de cómputo que se intercomunican entre sí** para ofrecer servicios, el caso más común en pequeñas redes de datos es implementar una red de datos con el fin de **compartir archivos** o por ejemplo una impresora como se muestra en la **¡Error! No se encuentra el origen de la referencia.**



*Ejemplo de una red de datos*

Una definición más formal de una red de datos o red de computadores es **un conjunto equipos** (computadoras y dispositivos), **conectados** por medio de cables, señales, ondas o cualquier otro método de transporte de datos, para compartir información (archivos), recursos (discos, impresoras, programas, etc.) y servicios (acceso a una base de datos, internet, correo electrónico, chat, juegos, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo. (Mansilla, 2015)

Existen otras definiciones sobre que son las redes de datos, puede encontrarlas en (Wikipedia, 2015) y

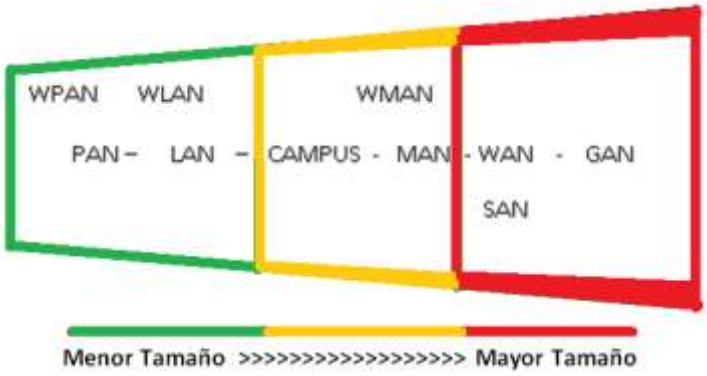
*HTTP://WWW.ECURED.CU/INDEX.PHP/RED_DE_COMPUTADORAS*

## 2.1.2 CLASIFICACIÓN DE LAS REDES DE LOS DATOS

Las redes de datos se pueden clasificar en general, por su cobertura geográfica es decir el área que abarcan, y por la forma en que se interconectan topología física.

### 2.1.2.1 CLASIFICACIÓN SEGÚN SU COBERTURA GEOGRÁFICA

Las redes de datos se clasifican por la cobertura geográfica, es decir según la extensión o espacio que cubren. Las clasificaciones más comunes se muestran en la **¡Error! No se encuentra el origen de la referencia.**




*Clasificación según su cobertura geográfica fuente el autor*

- **PAN**: son redes pequeñas de nominadas Personal Area Network (PAN) estar son redes que permiten la comunicación a pocos metros tal es el caso de las redes
- **WPAN:** Al igual que las redes PAN estas se comunican a pocos metros, pero son íntegramente inalámbricas tal es el caso de las Redes bluetooth que usan los Smartphone, tabletas y portátiles sus siglas corresponden a Wireless Personal Area Network
- **LAN:** por sus siglas en ingles Local Area Netwok, son las redes que típicamente encontramos en los cafés internet e incluso en nuestras casas que puede abarcar alrededor de 100 Metros de radio
- **WLAN**: estas corresponden a las redes inalámbricas tal como las redes WIFI, al igual que las redes LAN abarcan un radio de 100 metros, aunque este es limitado por la interferencia y los obstáculos físicos como paredes, muebles y cualquier elemento físico entre sus nodos
- **SAN:** Corresponde a redes de Storage (Almacenamiento) son redes de alta velocidad que permiten a grandes empresas hacer respaldo "backup" de la información en tiempo real pueden ser abarcar grandes

áreas geográficas. Solo se denominan SAN (Stoarge Area Network) cuando son empleadas con el propósito de hacer respaldo de la información

- **CAMPUS**: También denominadas CAN (Campus Area Network) son redes de mayor cobertura que una red LAN de que pueden intercomunicar computadores en grandes áreas privadas tal es el caso de los campus universitarios o las instalaciones de grandes empresas que pueden tener varios cientos de metros entre sus nodos

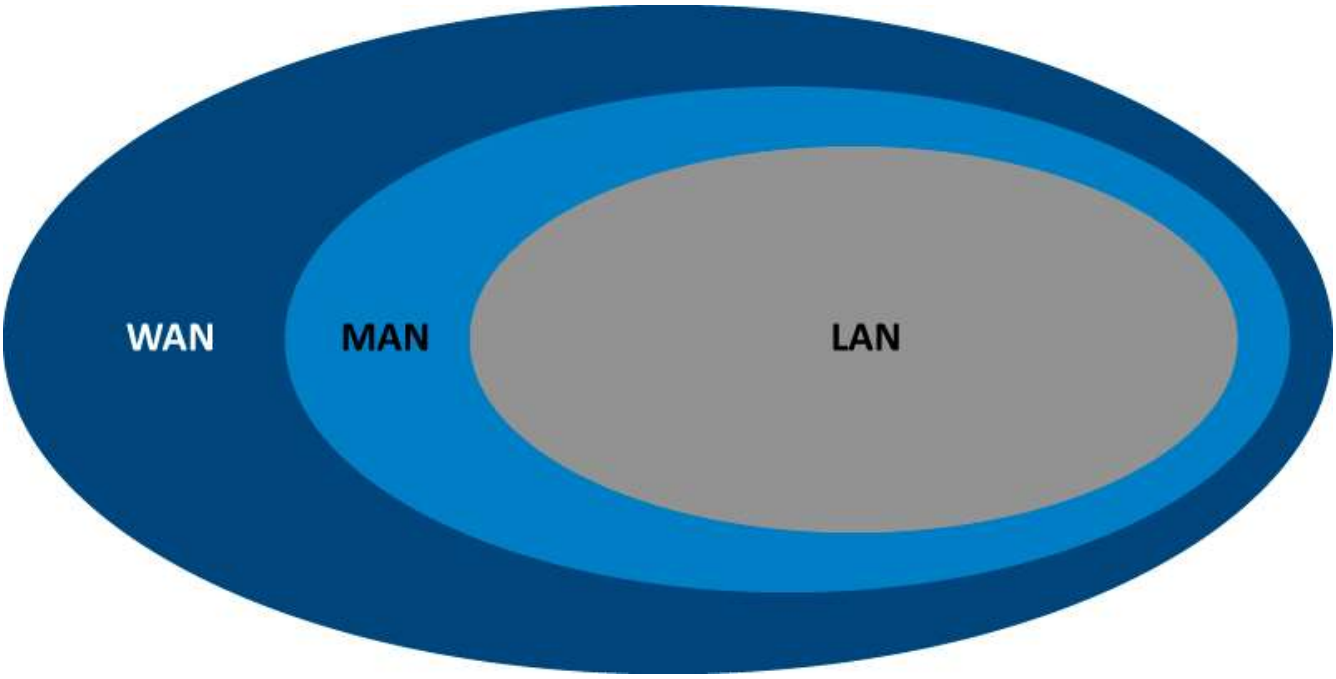
- **MAN:** Corresponde al termino Metropolitan Area Network , Red de área metropolitana, son redes que pueden cubrí ciudades enteras, de ahí su nombre , generalmente requieren la intervención de empresas de interconexión municipales (ISP)

- **WMAN:** Al igual que las MAN estas pueden cubrir una ciudad pero en forma Inalámbrica, esta redes permiten las conexión de varios puntos de red dispersos en una misma ciudad

- **WAN:** Corresponde a redes que pueden interconectar ciudades o incluso países, estas redes requieren la intervención de varios proveedores de interconexión, son redes de gran tamaño cuyas siglas significan Wide Area Network, o Redes de Área Amplia

- **GAN:** Al igual que las WAN estas pueden interconectar países pero estas usan los satélites como medio de comunicación, son de nominadas Global Area Network o Redes de Área Global

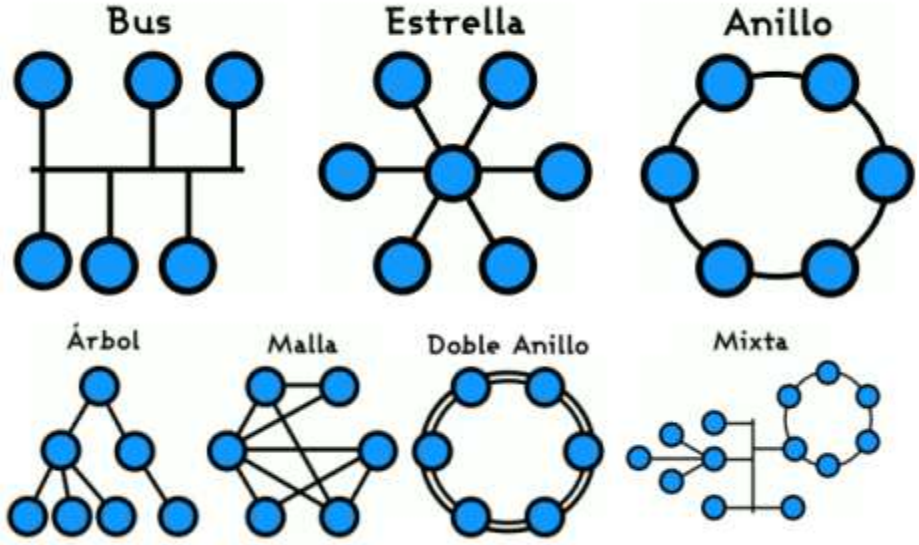
En general los términos más empleados para definir las redes por su cubrimiento geográfico son: **LAN, MAN** y **WAN,** la **¡Error! No se encuentra el origen de la referencia.** muestra las coberturas geográficas de estos tipos de redes.




*Cobertura de redes LAN, MAN y WAN fuente el autor*

## 2.1.2.2 CLASIFICACIÓN SEGÚN LA FORMA EN QUE SE INTERCONECTAN

La forma en que las redes se interconectan es llamada **Topología Física**, La topología física se refiere a **las conexiones físicas** bien sean **alámbricas** o **inalámbricas**, y **dispositivos** que constituyen una red como los PC. La topología física hace referencia a como los dispositivos "ven" como están conectados físicamente unos con otros, las formas más comunes de interconexión se muestran en la siguiente figura:




*Clasificación de las redes según su topología*

- **Topología en BUS:** Se usó principalmente en redes Locales **LAN**, las redes en **BUS** se caracterizan por usar un cable principal a modo de columna vertebral "**BUS**" al cual se conectan cada uno de los nodos. En esta topología física fue usada por las primeras **redes Ethernet.** Son fáciles de instalar cunado existen pocos muy nodos, pero presenta grandes problemas si se intenta conectar un número grande de nodos uno de los problemas es que se alguna parte de cable principal se desconecta toda la red se colapsa. En las redes modernas el **cable principal** se protege dentro de un elemento llamado **Concentrador** lo que **evita el problema** de **desconexión completa**.

- **Topología Física en Estrella:** Esta topología requiere de un nodo principal al cual se interconectan cada uno de los otros nodos formado físicamente una estrella, uno de los problemas con esta topología es que, si el nodo principal falla deshabilitaría toda la red, esta topología se usa actualmente en redes MAN y WAN para interconectar oficinas a la red principal en una compañía.

- **Topología Física en Anillo**: La topología en anillo supone una mejora funcional y de rendimiento sobre la topología en bus ya que permite mayor eficiencia en la red. La topología en anillo en un principio de usó en redes LAN Token Ring, pero su costo era muy elevando, ya no se usa en redes LAN

- **Topología Física en Árbol:** Esta topología es jerárquica y recuerda la forma de un árbol invertido, en esta topología existen nodos terminales, nodos troncales y nodos padre, los nodos terminales se conectan a los nodos troncales que a su vez se conectan con otros nodos de mayor jerarquía llamados nodos padre, es común en redes empresariales de gran tamaño, no aplica para redes LAN. Puede complementar en este enlace

- **Topología Física en Maya:** en esta topología los nodos de interconectan punto a punto a otros nodos, esta topología es típica de redes WAN, no aplica a redes LAN.

- **Topología Física Doble Anillo:** es una variación de la topología en Anillo hoy emplea como un doble anillo de alta velocidad usando fibra óptica en redes FDDI, estas se usan para interconectar redes MAN y WAN, el doble anillo permite la comunicación incluso si partes del anillo quedan intercomunicadas entre sí.

- **Topología Física en Mixta:** como se indica no es una topología pura es más bien una red hibrida que usa varias topologías diferentes para interconexión de sus nodos.

Para ampliar esta información dirígete a

*https://es.wikipedia.org/wiki/Categor%C3%ADa:Topolog%C3%ADa_de_red*

## 2.2 TEMA 2 GENERALIDADES DE LA MODELACIÓN POR CAPAS, ANTECEDENTES.

Desde el inicio de las redes de computadores los ingenieros vieron la necesidad de diseñar modelos estandarizados que permitieran el diseño de protocolos a nivel general, en un principio estos protocolos y estándares se crearon con el fin que los ingenieros de una misma empresa de tecnología pudieran comunicar el hardware y el software fabricados por ellos mismos, o por en cargo a terceros.

Actualmente Estos modelos estandarizados son requeridos para poder normalizar la forma en que los programas y computadores de diferentes fabricantes se puedan comunicar e interactuar entre sí. Dicho de otra manera, sin un patrón o modelo estandarizado sería imposible que computadores o programas de diferentes programadores y fabricantes pudieran comunicarse.

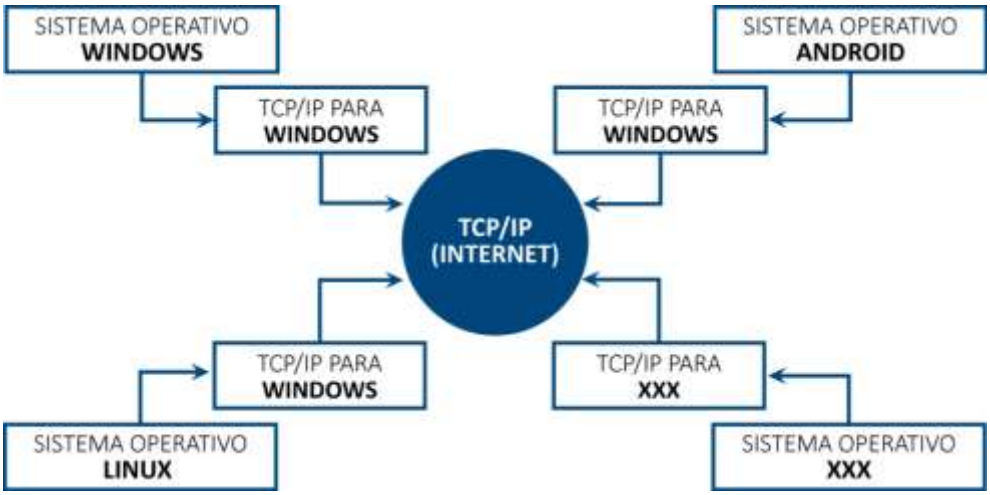
### 2.2.1 QUE ES UN MODELO DE RED

Un modelo de red son una serie de especificaciones técnicas, protocolos y recomendaciones que deben seguir los desarrolladores de software para poder interconectar computadores siguiendo unas normas generales.

Un caso concreto de un modelo de red es el **TCP/IP** este modelo permite que computadores de escritorio, como sistemas PC o MAC de diferentes fabricantes e incluso teléfonos inteligentes y Grandes computadores se puedan comunicar entre si incluso si estos tienen sistemas operativos diferentes como Linux, Windows Android, Solaris o MAC OS.

Un modelo de red dice cómo deben ser realizados los programas para poder intercomunicarse, luego de comprender las especificaciones del modelo de red, los desarrolladores de sistemas operativos, programan estas reglas de tal forma que se adecuen a cada sistema operativo en particular.

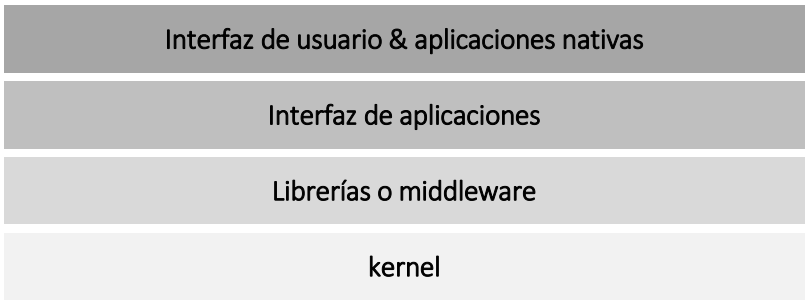
El caso del **TCP/IP** cada sistema operativo bien sea **Linux**, **Windows** o Android crea su propia pila de protocolo **TCP/IP** y la incluye en el sistema operativo para permitir la interconexión, es decir que para que 2 o más computadores se comuniquen es requerido el uso de un protocolo o modelo común que puedan aplicar para hacer la interconexión. En el caso de internet los computadores que quieren conectarse deberán tener una pila de protocolo **TCP/IP** implementada en su sistema operativo.




## 2.2.2 QUE ES LA MODELACIÓN POR CAPAS

Para poder realizar los intercambios de información se crearon varios modelos como el modelo OSI, el cual es un modelo de referencia. Técnicamente hablando los modelos de red o de interconexión de redes como OSI funcionan por capas es decir que para pasar a la capa 1 debe pasar antes por la capa 2, esta técnica se usa en muchos otros escenarios como en el desarrollo de software y el diseño de sistemas operativos.

Un ejemplo en el **modelado por capas** de un sistema operativo se muestra en




En los sistemas operativos para poder acceder al kerner (capa más profunda del sistema operativo) una aplicación que se encuentra en la capa más externa en azul, tiene que pedir servicios a las capas inferiores (interfaz de aplicación en verde) y esta a su vez a las librerías o middleware (en violeta).

En la comunicación de redes ocurre lo mismo, los modelos de redes tienen capas que deben ser recorridas para lograr la comunicación efectiva. En una comunicación por capas cada capa es una unidad funcional que solo se

comunica con las capas superior e inferior, esta capa tiene funciones específicas que no se comparten con otras capas.

Según Andrew Tenenbaum, en general en la creación de un modelo deben atender a los siguientes principios (TANENBAUM, 2003).

- Una capa se debe crear donde se necesite una abstracción diferente
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.
- Los límites de las capas tienen como fin minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser lo suficientemente amplia para no tener que agrupar funciones distintas en la misma capa y suficientemente pequeña para que la arquitectura no se vuelva inmanejable.

# 2.3 TEMA 3 ARQUITECTURAS DE RED DECNET, SNA, TCP/IP

## 2.3.1 QUE ES UNA ARQUITECTURA DE RED.

La arquitectura es el "plan, la conceptualización" con el que se conectan los protocolos y otros programas de software para interconectar equipos de cómputo en una red, en otras palabras, explica detalladamente los pasos y detalles dela comunicación entre en equipos. Esto es benéfico tanto para los usuarios de la red como para los proveedores de hardware y software.

Según muchos autores y diseñadores de redes la arquitectura de red es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto coordinado de productos que se puedan interconectar.

A lo largo de la historia de los computadores ha habido muchas arquitecturas de red, en un principio cada sistema operativo intentaba establecer su propia arquitectura ya que estas las arquitecturas se diseñaban para que trabajaran únicamente para equipos de una misma compañía de tecnología o grupo de compañías y no podían ser usados por otros, entre las arquitecturas más destacadas están:

- Systems Network Architecture (SNA de IBM)

- TCP/IP actualmente usada por internet
- IPX/SPX Internetwork Packet Exchange/Sequenced Packet Exchange), Protocolo Novell
- Appletalk desarrollado por Apple Inc.
- NetBEUI NetBIOS Extended User Interface. Usada por Microsoft en un principio
- DECnet desarrollado por la firma Digital Equipment Corporation.

Sin embargo, las que más han contribuido con la estandarización a nivel mundial son TCP/IP, SNA y DECnet

Para ampliar esta información dirígete a

*https://es.wikipedia.org/wiki/Arquitectura_de_Red*

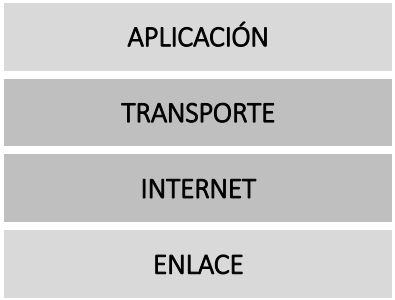
*http://laurapita.blogspot.com.co/2009/03/arquitectura-de-red.html*

## 2.3.2 TCP/IP

La arquitectura TCP/IP fue desarrollada en 1970 por el ministerio de defensa norteamericano ya que necesitaba tener una red que pudiera resistir a todas las condiciones, incluso a una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación como el cobre, las micro ondas, la fibra óptica y transmisión por satélite, el ministerio de defensa deseaba tener una transmisión de paquetes con seguridad de que llegue a su destino en cualquier tipo de condiciones. Esta idea extremadamente ambiciosa condujo a la creación del modelo TCP/IP (ccm.net, 2015).

Contrariamente a otras tecnologías de red propietarias, TCP/IP ha sido desarrollado como una norma abierta. Esto quiere decir que cualquiera puede utilizar TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como norma y su fácil implantación en internet.

Dado que TCP/IP es el protocolo más usado en la actualidad ya que es usado por internet y por todas las redes que se conectan a internet será estudiado con mayor detenimiento en otros capítulos, esta arquitectura se compone de 4 capas como lo muestra la ilustración




El **TCP/IP** es la base de Internet, y sirve para **comunicar** todo tipo de dispositivos, computadoras que utilizan **diferentes sistemas operativos,** minicomputadoras y computadoras centrales sobre redes de área local (**LAN**) y área extensa **(WAN**). **TCP/IP** fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en **ARPANET,** una red de área extensa del departamento de defensa (Alfinal.com , 2015).

### 2.3.3 SNA

Fue desarrollado por IBM en 1974 es una arquitectura que permite la comunicación entre equipos IBM AS/400, es una de las arquitecturas más robustas y seguras de la actualidad y es empleada ampliamente en organizaciones financieras por su confiabilidad.

SNA es una arquitectura de red, que permite que los clientes de IBM construyan sus propias redes privadas, tomando en cuenta a los HOST y a la subred. Un banco, por ejemplo, puede tener una o más CPU's en su Departamento de proceso de datos, y numerosas terminales en cada una de sus sucursales. Con el uso del SNA, todos estos componentes aislados pueden transformarse en un sistema coherente. Antes de la aparición de SNA, IBM tenía varios cientos de productos de comunicación, utilizando tres docenas de métodos de acceso de teleproceso, con más de una docena de protocolos de enlace. La idea al crear la SNA, consistió en eliminar este caos y proporcionar una infraestructura coherente para el proceso distribuido débilmente acoplado. Debido al deseo de varios clientes de IBM de mantener la compatibilidad de todos estos programas y protocolos (mutuamente incompatibles), la arquitectura SNA resulta más complicada de lo que pudo haber sido de no existir estas limitaciones. La SNA efectúa también un gran número de funciones que no se encuentran en otras redes, las cuales aunque resultan muy valiosas para ciertas aplicaciones, tienden a elevar la complejidad total de su arquitectura. (digitum, 2008)

**SNA** tiene **7 capas** o **niveles** funcionales que son mostradas en la **¡Error! No se encuentra el origen de la referencia.**:

**SNA**

| |
|---|
| Transaction services |
| Presentación services |
| Data flow control |
| Transmission control |
| Path control |
| Data link control |
| physical |

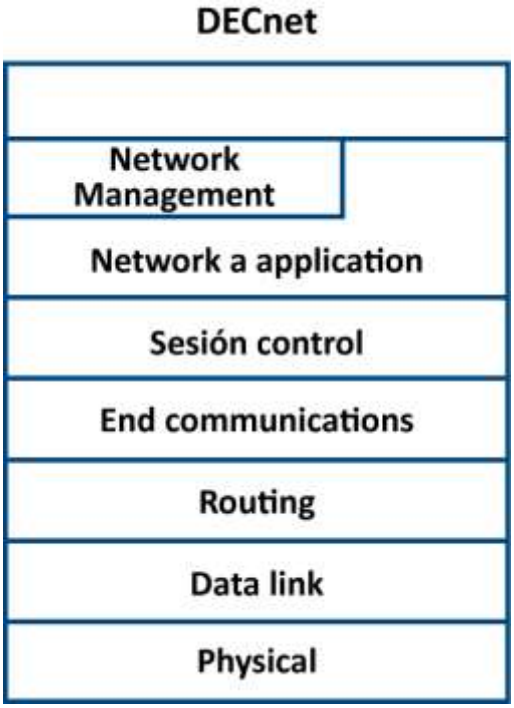
*Capas arquitectura SNA(manque.cl.tripod.com)*

## 2.3.4 DECNET.

**DECnet** es una arquitectura de red diseñada en 1975 por la compañía Equipment Corporation DEC, Como respuesta a la introducción un año antes de la arquitectura SNA de IBM. DECnet permitía la comunicación entre dos mini computadoras PDP-11 directamente lo que dio inicio a las arquitecturas punto a punto.

DECnet es una arquitectura de cinco capas. También conocida como DNA Las capas fisica, de enlace, de transporte y de servicios de la red son casi exactamente a las cuatro capas inferiores del modelo OSI. La quinta capa, la de aplicación, es una mezcla de las capas de presentacion y aplicación del modelo OSI. La DECnet no cuenta con una capa de sesión separada (Kurose & Ross W, 2010).

El objetivo de la DECnet es permitir que diferentes computadoras principales y redes punto a punto, multipunto o conmutadas de manera que los usuarios puedan compartir programas, archivos de datos y dispositivos de terminal remotos. La DECnet ofrece un emulador mediante el cual los sistemas de la Digital Equipment Corporation se pueden interconectar con las macrocomputadoras de IBM (Rojas , 2015)




*Capas DECnet (http://docwiki.cisco.com/)*

## 2.3.5 EJERCICIO DE APRENDIZAJE

Describa según su definición y relacione correctamente (**Lan, man, wan**, entre otros)

| TIPO DE AREA NETWORK | DEFINICIÓN |
|---|---|
| | Corresponde al termino Metropolitan Area Network, Red de área metropolitana, son redes que pueden cubrí ciudades enteras, de ahí su nombre, generalmente requieren la intervención de empresas de interconexión municipales (ISP) |
| | Al igual que las redes PAN estas se comunican a pocos metros pero son íntegramente inalámbricas tal es el caso de las Redes bluetooth que usan los Smartphone, tabletas y portátiles sus siglas corresponden a Wireless Personal Area Network |
| | Al igual que las MAN estas pueden cubrir una ciudad pero en forma Inalámbrica, esta redes permiten las conexión de varios puntos de red dispersos en una misma ciudad |

| | |
|---|---|
| | por sus siglas en ingles Local Area Netwok, son las redes que típicamente encontramos en los café internet e incluso en nuestras casas que puede abarcar alrededor de 100 Metros de radio |
| | estas corresponden a las redes inalámbricas tal como las redes WIFI, al igual que las redes LAN abarcan un radio de 100 metros aunque este es limitado por la interferencia y los obstáculos físicos como paredes, muebles y cualquier elemento físico entre sus nodos |
| | Corresponde a redes de Storage (Almacenamiento) son redes de alta velocidad que permiten a grandes empresas hacer respaldo "backup" de la información en tiempo real pueden ser abarcar grandes áreas geográficas. Solo se denominan SAN (Stoarge Area Network) cuando son empleadas con el propósito de hacer respaldo de la información |
| | Al igual que las WAN estas pueden interconectar países pero estas usan los satélites como medio de comunicación, son de nominadas Global Area Network o Redes de Área Global |
| | son redes pequeñas de nominadas Personal Area Network (PAN) estar son redes que permiten la comunicación a pocos metros tal es el caso de las redes |
| | También denominadas CAN (Campus Area Network) son redes de mayor cobertura que una red LAN de que pueden intercomunicar computadores en grandes áreas privadas tal es el caso de los campus universitarios o las instalaciones de grandes empresas que pueden tener varios cientos de metros entre sus nodos |
| | Corresponde a redes que pueden interconectar ciudades o incluso países, estas redes requieren la intervención de varios proveedores de interconexión, son redes de gran tamaño cuyas siglas significan Wide Área Network, o Redes de Área Amplia |

## 2.3.6 EJERCICIO DE ENTRENAMIENTO

1. Cuál es la diferencia entre un protocolo y una arquitectura de red

2. Según su concepto cual es la arquitectura de red entre (SNA, DECNET y TCP/IP) que más se parece al modelo OSI?

3. Entre TCP/IP y IPX/ SPX cual se usa con más frecuencia en la interconexión de redes justifique su respuesta.

4. ¿Investigue por qué el protocolo NETBEUI no es un protocolo que se pueda usar para comunicar varias redes como INTERNET?

5. Por qué se debe usar un modelo por capas para explicar y diseñar arquitecturas de red

6. Las pilas de protocolos de WINDOWS y LINUX son muy diferentes o son muy parecidas, justifique su respuesta.

7. Que topología de red cree que sea:

    a. Internet

    b. Una red LAN

    c. Una red punto a punto con 2 PC

    d. Una red de cajeros electrónicos

## 2.4 TEMA 4 MODELO OSI GENERALIDADES Y CONCEPTOS DE CADA UNA DE LAS 7 CAPAS

El modelo OSI es un modelo de referencia para la creación de arquitecturas de red se creó, para estandarizar el interconexión de computadores sin importar el fabricante o sistema operativo de las máquinas, el modelo OSI, tiene 7 capas, (TANENBAUM, 2003)

OSI es la abreviatura **de OPEN SYSTEM INTERCONNECTION**, El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1) Interconexión de sistemas abiertos, se creó en 1980, y tomo las características más importantes de los protocolos más usados en ese momento tal es el caso de DECnet, SNA y TCP/IP.

A principios de 1980 el desarrollo de redes originó desorden en muchos sentidos. Se produjo un enorme crecimiento en la cantidad y tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnologías de conexión, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

### 2.4.1 HISTORIA.

Para mediados de 1980, las empresas comenzaron a sufrir las consecuencias de la rápida expansión de computadores y redes. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de conexiones privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño

grupo de empresas controlan todo uso de la tecnología. Las tecnologías de conexión que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la ISO investigó modelos de conexión como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (Systems Network Architecture, SNA) y TCP/IP, a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes. (Wikipedia, 2015). La ISO es una red de los institutos de normas nacionales de 163 países. Este regula la estandarización a nivel mundial de muchas normas

Modelo OSI Generalidades y conceptos de cada una de las 7 Capas.

El modelo OSI está dividido en 7 capas, estas capas se diseñaron siguiendo los principios antes mencionados, las definiciones de las capas se exponen como un consenso a través de documentos y ampliamente difundidos en internet.

| CAPAS | CARACTERÍSTICAS |
|---|---|
| **Capa Física** | Define el **medio físico** de comunicación, bien sea un cable de cobre, fibra óptica o inalámbrica que es utilizado para **la transferencia de información.**<br><br>El medio puede tomar muchos aspectos y formas, y no tiene que ser homogéneo es decir **puede cambiar** entre varios **tipos de cable** e incluso de alámbrico a inalámbrico. |
| **Capa de Enlace de Datos** | Este nivel proporciona facilidades para **la transmisión** de **bloques de datos** entre **dos estaciones** de la red. Esta capa **Organiza los 1's** y **los 0's** del **Nivel Físico**, en **formatos** o **grupos** de **información** llamadas **tramas**, también establece **un esquema de detección** de **errores** para **las retransmisiones** o **reconfiguraciones** de la red. Sin embargo **la principal función** es establecer el **método de acceso**. Se reglamenta que pasos debe realizar el computador para **transmitir** y **recibir mensajes**, también **garantizar** que los computadores envíen datos **sin interferir** el envío de otros computadores, así como **controlar el flujo de datos** de un PC a otro, es decir que un **computador rápido no llene de información** a **un computador lento**.<br><br>En síntesis esta capa realiza **la transferencia** de **datos** a través del **enlace físico**, controla errores, flujo y acceso al medio. |

| | |
|---|---|
| **Capa de Red** | Esta capa proporciona **direccionamiento** y **selección** de **ruta** entre dos PC que pueden estar ubicados **en redes geográficamente distintas** como internet; las funciones principales se pueden resumir en **direccionamiento** y **búsqueda** de **la mejor ruta**.<br><br>**El direccionamiento**, define la forma en que se **"bautizarán"** a cada una de **las redes,** asignándole a cada una de ella una **dirección IP** como por ejemplo 172.16.0.0 también define como se llamará **a cada uno de los computadores** dentro de la red, a cada PC también se le asigna **dirección IP**.<br><br>**La mejor ruta**, es **el mecanismo** que escoge **el mejor camino** a tomar **entre dos redes** geográficamente distantes, se define **el enrutamiento** y **el envío de paquetes** entre redes. Es responsable de **establece**r, **mantener** y **terminar** las conexiones, además esta capa describe **el direccionamiento lógico** y proporciona el **enrutamiento de mensajes**, determinando si un mensaje en particular deberá enviarse al **nivel 4** (**Nivel de Transporte**) o bien al **nivel 2** (**Enlace de datos**). Esta función "**enruta"** y **controla** la **congestión** de **los paquetes de información** en una **sub-red.** |
| **Capa de Transporte** | Este nivel actúa como **un puente** entre **los tres niveles inferiores** totalmente orientados a **las comunicaciones** y **los tres niveles superiores** totalmente orientados al **procesamiento.** Además, **garantiza una entrega confiable** de la **información**. Asegura que la llegada de datos del nivel de red encuentra **las características** de **transmisión** y **calidad de servicio** requerido por la **capa 5** (**Sesión**).Este nivel define como **direccionar la localidad física** de los **dispositivos** de la red. Define una posible **multicanalización** (puede soportar **múltiples conexiones**). Define la manera de **habilitar** y **deshabilitar** las **conexiones entre los nodos**, Determina **el protocolo** que garantiza **el envío del mensaje**, Establece **la transparencia** de datos, así como **la confiabilidad** en **la transferencia de información** entre dos sistemas (Tanenbaum, 2003). |

| | |
|---|---|
| **Capa de Sesión** | Provee **los servicios utilizados** para la **organización** y **sincronización** del diálogo entre **usuarios** y **el manejo** e **intercambio** de datos.<br>Establece:<br>- El **inicio** y **terminación** de la sesión,<br>- **Recuperación** de la sesión,<br>- **Control del diálogo**;<br>- **El orden** en que los mensajes deben fluir entre usuarios finales<br>- **Referencia** los **dispositivos por nombre** y **no por dirección**, y<br>- Permite **escribir programas** que correrán en **cualquier instalación** de la red. (Ross, 2003) |
| **Capa de Presentación** | **Traduce** el formato y **asigna una sintaxis** a los datos para **su transmisión** en la red. Determina **la forma de presentación** de los datos **sin preocuparse** de su **significado** o **semántica**. Tiene tres funciones principales:<br>- **Formateo** de datos,<br>- **Cifrado** de datos, y<br>- **Comprensión** de datos<br>Establece **independencia** a **los procesos de aplicación** considerando **las diferencias** en **la representación** de datos. Proporciona **servicios** para que **el nivel de aplicaciones** pueda **interpretar** el **significado** de los datos **intercambiados.** Opera **el intercambio** y la **visualización**. |
| **Capa de Aplicación** | Proporciona **servicios** al usuario del **Modelo OSI.** Realiza la **comunicación** entre **dos procesos de aplicación**, tales como: programas de aplicación, aplicaciones de red, entre otros. Proporciona **aspectos de comunicaciones** para **aplicaciones específicas** entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), entre otros (TANENBAUM, 2003). |

Gráficamente se puede ver **el modelo OSI** como **una pila de 7 capas**, como el mostrado en **¡Error! No se encuentra el origen de la referencia.**


*Capas del modelo OSI fuente el autor*

## 2.4.2 NOMBRE DE LOS DATOS EN CADA CAPA DEL MODELO OSI

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicaciones de par-a-par en cada uno de estas capa la información cambia de nombre es decir usa un PDU (Protocol Data Unit) diferente ver tabla

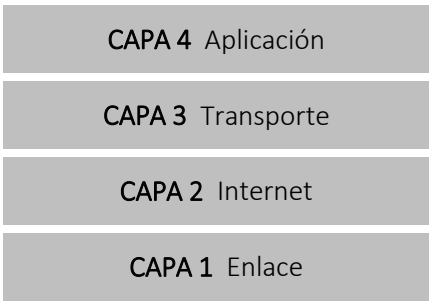
*Tabla 1 Nombre de PDU en cada capa del modelo OSI*

| Capa Numero | Nombre Capa | PDU |
|---|---|---|
| **Capa 1** | Física | Bits |
| **Capa 2** | Enlace | Trama |
| **Capa 3** | Red | Paquete |
| **Capa 4** | transporte | segmento |
| **Capa 5** | sesion | Datos |
| **Capa 6** | Presentación | Datos |
| **Capa 7** | Aplicación | Datos |

# 2.5 TEMA 5 MODELO TCP/IP GENERALIDADES 4 CAPAS

**TCP/IP** significa **Protocolo de control de transmisión/Protocolo de Internet** representa **todas las reglas de comunicación para Internet** y se basa en la noción de **brindar una dirección IP** a cada computador de la red.

Internet se desarrolló para brindar **una red de comunicación** que pudiera continuar funcionando en tiempos de guerra. Aunque la Internet ha evolucionado en formas muy diferentes a las imaginadas por sus arquitectos, todavía se basa en un conjunto de **protocolos TCP/IP.** El diseño de **TCP/IP es ideal para la poderosa y descentralizada red que es Internet.** Como se comentó Todo dispositivo conectado a Internet que desee comunicarse con otros dispositivos en línea debe tener **un identificador exclusivo** llamado **dirección IP** (ccm.net, 2015)




*Capas1, 2 ,3 y 4 del modelo TCP/IP*

- **Capa de aplicación.** Es **el nivel más alto**, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes **TCP/IP**. Una aplicación interactúa con uno de los protocolos de nivel de transporte para **enviar** o **recibir datos**. El programa de aplicación pasa **los datos** en **la forma requerida** hacia **el nivel de transporte** para su entrega.
- **Capa de transporte. La principal tarea** es proporcionar **la comunicación** entre un programa de aplicación y otro y se conoce frecuentemente como **comunicación punto a punto**. La capa de transporte **regula el flujo de información**. Puede también proporcionar **un transporte confiable**, asegurando que los datos lleguen **sin errores** y en **secuencia**. El software de transporte **divide el flujo de datos** que se está enviando **en pequeños fragmentos** (por lo general conocidos como **paquetes**) y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión. Aun cuando en el esquema anterior se utiliza un solo bloque para representar la capa de aplicación, **una computadora de propósito general** puede tener **varios programas de aplicación** accediendo a la internet **al mismo tiempo**. La capa de transporte debe **aceptar** datos desde varios programas de usuario y **enviarlos** a **la capa del siguiente nivel**. Para hacer esto, se añade **información adicional** a cada paquete, incluyendo **códigos** que identifican qué programa de aplicación envía y qué programa debe recibir, así como una suma de verificación para verificar que **el paquete ha llegado intacto** y utiliza **el código de destino** para identificar el programa de aplicación en el que se debe entregar.
- **Capa Internet.** La capa Internet maneja **la comunicación** de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete.
- **Capa de interfaz de red o capa de enlace** El software **TCP/IP** de **nivel inferior** consta de una **capa de interfaz** de red responsable de aceptar **los datagramas IP** y **transmitirlos** hacia una red específica.

También esta capa es la encargada del **acceso al medio**, es decir, indica cuando un computador puede transmitir para **no dañar la información** enviada por otros computadores.

**NOTA:**
Es de anotar que el **TCP/IP no hace especificaciones sobre los medios (cables)** empleados, es decir, **no tiene un nivel físico como el modelo OSI.**

## 2.6 TEMA 6 COMPARACIÓN MODELO OSI - TCP/IP

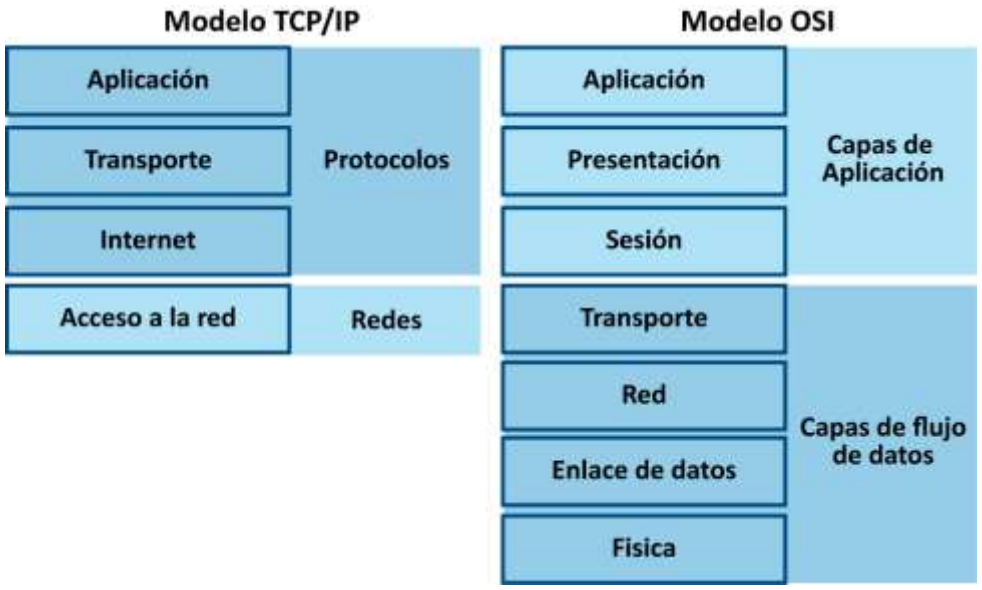
**SIMILITUD ENTRE EL MODELO OSI Y EL MODELO TCPIP**

- Ambos se dividen en capas o niveles.
- Se supone que la tecnología es de conmutación de paquetes (no de conmutación de circuitos).
- Los profesionales de networking deben conocer ambos: OSI como modelo; TCP/IP como arquitectura real.

**DIFERENCIA ENTRE EL MODELO OSI Y EL MODELO TCPIP**

- OSI distingue de forma clara los servicios, las interfaces y los protocolos. TCP/IP no lo hace así, no dejando de forma clara esta separación.
- OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente.
- TCP/IP parece ser más simple porque tiene menos capas.

En cuanto a la disposición y funcionalidad de las capas ambos modelos de pueden contrastar como se ve en la **¡Error! No se encuentra el origen de la referencia.**




*Modelo OSI vs Modelo TCP/IP*

La **¡Error! No se encuentra el origen de la referencia.** muestra que la funcionalidad de las capas física y enlace en el modelo OSI corresponden a las capa de acceso a red en el modelo TCP/IP, de igual forma las capas de red e internet de ambos modelos son equivalentes al igual que las capas de transporte (tienen igual nombre en ambos modelos) por último la capa de aplicación del modelo TCP/IP corresponde a las capas Sesión, Presentación y aplicación el modelo OSI

## 2.6.1 EJERCICIO DE ENTRENAMIENTO

**1. ¿**Realizar un comparativo entre el modelo osi y el modelo tcp/ip?

2. ¿Qué significa que el modelo OSI sea un modelo de referencia?

3. Responda Falso o verdadero y justifique su respuesta

| | |
|---|---|
| a)La PDU de la capa física se llama trama | |
| b)La PDU de la capa redes es el paquete | |
| La capa 4 tiene como PDU transporte | |

Describa las siguientes capas de modelo OSI:

a) Física

b) Red

c) Enlace

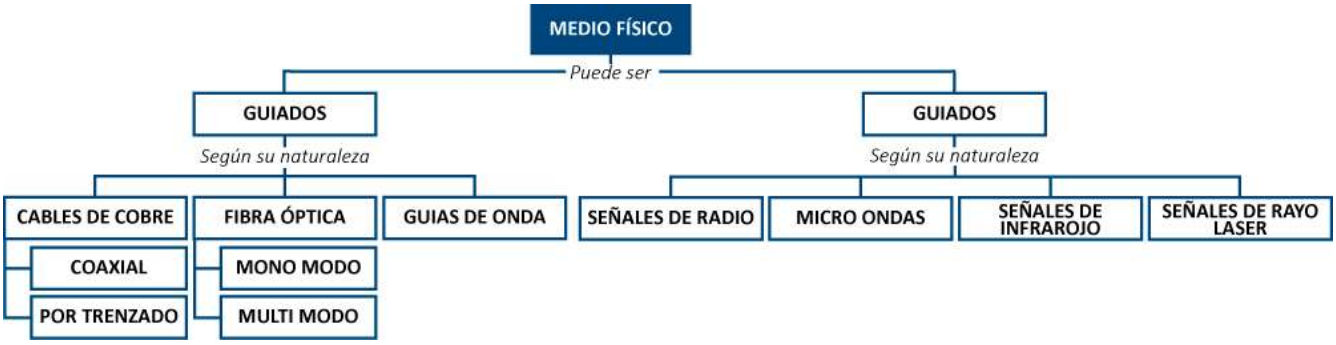
d) Trasporte

# 3 UNIDAD 2 MEDIOS DE TRANSMISION E INFRAESTRUCTURA DE REDES

La palabra medio se usa para identificar la forma de conexión de un dispositivo con la infraestructura de red o con otro equipo, el medio puede ser alámbrico o inalámbrico, los medios son una problemática de la capa física del modelo OSI.

## 3.1 TEMA 1 LOS MEDIOS DE TRANSMISIÓN GENERALIDADES, EMI, RFI

Dependiendo de la forma de conducir la señal a través del medio, los medios de transmisión se pueden clasificar en dos grandes grupos, medios de transmisión guiados y medios de transmisión no guiados. En el contenido del texto se dará vital importancia a los medios guiados, muestra un mapa conceptual de los tipos de medios




*Mapa conceptual de medios fuente el autor*

Los medios guiados fabricados con cobre y los inalámbricos pueden presentar atacados por interferencias externas llamadas EMI (interferencia por electromagnetismo) y RFI (interferencia por Radio frecuencia)

- EMI: La interferencia electromagnética es la perturbación que ocurre en cualquier circuito, componente o sistema electrónico causado por una fuente de radiación electromagnética externa al mismo. Esta perturbación puede interrumpir, degradar o limitar el rendimiento de ese sistema. La fuente de la interferencia puede ser cualquier objeto, ya sea artificial o natural, que posea corrientes eléctricas que varíen rápidamente, como un circuito eléctrico, el Sol o las auroras boreales (Wikipedia, 2015)

- RFI: La interferencia Por radio frecuencia es la perturbación en la transmisión de causado por una fuente de emisión de radio externa al mismo. La fuente de la interferencia puede ser una emisora AM/FM, o cualquier fuente de emisión de radiofrecuencia como una señal de televisión, e incluso el WIFI o un teléfono inalámbrico.

## 3.2 TEMA 2 MEDIOS CABLEADOS E INALÁMBRICOS, FUNCIONES DE LA CAPA FÍSICA,

La capa física el modelo OSI define el cableado usado para implementar la comunicación de las redes de datos estos pueden ser alámbricos en el caso de las redes LAN o inalámbricos en el caso de las redes WLAN (WIFI).

Según el modelo OSI la capa física debe definir las normas aplicables, La función de la capa física de es la de codificar en señales los dígitos binarios que representan las tramas de la capa de enlace de datos, además de transmitir y recibir estas señales a través de los medios físicos. El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama que serán enviados a través de los medios (Pantheanet, 2014)

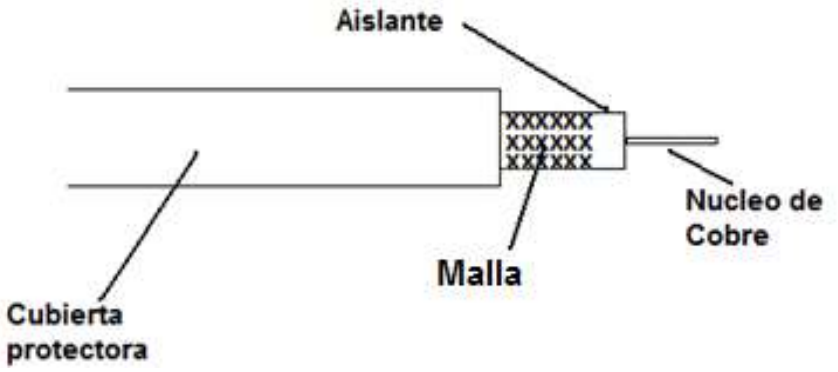
Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), cable coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.
- • Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

Los medios de transmisión más usados para interconectar computadores y redes de datos son el coaxial, los pares trenzados y la fibra óptica.

## 3.3 TEMA 3 CABLE COAXIAL

El coaxial es un medio (cable) de cobre con protección contra la EMI (Interferencias Electro Magnética) es decir apantallado, también está protegido contra el medio ambiente, es decir es blindado. ( **¡Error! No se encuentra el origen de la referencia.**)

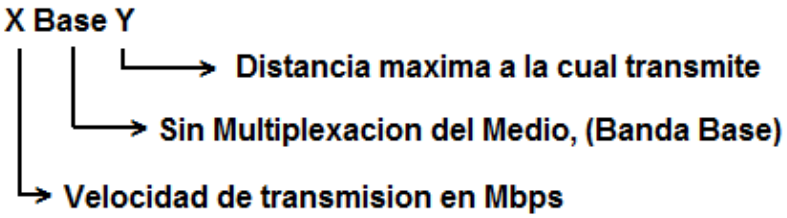



*Esquema Cable Coaxial fuente el autor*

Existen múltiples tipos de cable coaxial, sus diferencias están dadas por su diámetro e impedancia lo cual los hace útiles para ciertas aplicaciones, como en las redes de comunicación de banda ancha, se usan en sistemas de distribución de internet por cable modem y televisión por cable, el coaxial ya no se usa en las redes LAN, pues fue desplazado por el cable UTP.

> El coaxial se no se considera un medio confiable para uso en redes locales LAN, pero está vigente en las redes urbanas de televisión por cable , conexiones a antenas, en las líneas de distribución y en las redes telefónicas interurbanas

La nomenclatura usada para designar los coaxiales usados en redes LAN se puede resumir como en **¡Error! No se encuentra el origen de la referencia.**




*Nomenclatura cableado coaxial fuente el autor*

Algunos ejemplos de la nomenclatura empleada por el coaxial pueden ser:

10BASE5, transmite a 10Mbps y la longitud es de 500m, se considera un cable grueso.

10BASE2, transmite a 10Mbps y la longitud a la que transmite sin problema es 196m (se redondea a 2), este tipo de cable se considera delgado.

En la televisión los cables más usados para el hogar es el RG-6 cable coaxial la

*Tipos de cable RG*

| Tipo | Impedancia [Ω] | Núcleo | dieléctrico | | | Diámetro | | Trenzado | Velocidad |
|---|---|---|---|---|---|---|---|---|---|
| | | | tipo | [in] | [mm] | [in] | [mm] | | |
| RG-6/U | 75 | 1.0 mm | Sólido PE | 0.185 | 4.7 | 0.332 | 8.4 | doble | 0.75 |
| RG-6/UQ | 75 | | Sólido PE | | | 0.298 | 7.62 | | |
| RG-8/U | 50 | 2.17 mm | Sólido PE | 0.285 | 7.2 | 0.405 | 10.3 | | |
| RG-9/U | 51 | | Sólido PE | | | 0.420 | 10.7 | | |
| RG-11/U | 75 | 1.63 mm | Sólido PE | 0.285 | 7.2 | 0.412 | 10.5 | | 0.66 |
| RG-58 | 50 | 0.9 mm | Sólido PE | 0.116 | 2.9 | 0.195 | 5.0 | simple | 0.66 |
| RG-59 | 75 | 0.81 mm | Sólido PE | 0.146 | 3.7 | 0.242 | 6.1 | simple | 0.66 |
| RG-62/U | 92 | | Sólido PE | | | 0.242 | 6.1 | simple | 0.84 |
| RG-62A | 93 | | ASP | | | 0.242 | 6.1 | simple | |
| RG-174/U | 50 | 0.48 mm | Sólido PE | 0.100 | 2.5 | 0.100 | 2.55 | simple | |
| RG-178/U | 50 | 7x0.1 mm Ag pltd Cu clad Steel | PTFE | 0.033 | 0.84 | 0.071 | 1.8 | simple | 0.69 |
| RG-179/U | 75 | 7x0.1 mm Ag pltd Cu | PTFE | 0.063 | 1.6 | 0.098 | 2.5 | simple | 0.67 |
| RG-213/U | 50 | 7x0.0296 en Cu | Sólido PE | 0.285 | 7.2 | 0.405 | 10.3 | simple | 0.66 |
| RG-214/U | 50 | 7x0.0296 en | PTFE | 0.285 | 7.2 | 0.425 | 10.8 | doble | 0.66 |
| RG-218 | 50 | 0.195 en Cu | Sólido PE | 0.660 (0.680?) | 16.76 (17.27?) | 0.870 | 22 | simple | 0.66 |
| RG-223 | 50 | 2.74mm | PE Foam | .285 | 7.24 | .405 | 10.29 | doble | |
| RG-316/U | 50 | 7x0.0067 in | PTFE | 0.060 | 1.5 | 0.102 | 2.6 | simple | |

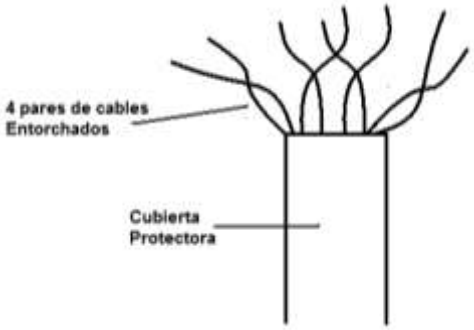
Fuente Wiki http://es.wikipedia.org/wiki/Cable_coaxial

# 3.4 TEMA 4 CABLES DE PARES TRENZADOS

Los pares trenzados son cables usados para la interconexión de redes de datos a nivel de capa física.

Existe una gran cantidad de cables de la familia de los pares trenzados TP (twister pair), entre ellos el UTP, STP, FSTP, S/FTP S/STP S/UTP; a continuación, encontraremos una reseña de cada uno.

**UTP (UNSHIELDED TWISTER PAIR):** Es un cable compuesto por 4 pares de hilos trenzados, para un total de 8 hilos (**¡Error! No se encuentra el origen de la referencia.**), no es resistente a las interferencias externas, EMI o RFI, pues en su construcción no tiene mayas u otro elemento que lo proteja, ya que no es apantallado.




*Esquema de cable UTP fuente el autor*

**Ventajas del cable**

- Cable delgado liviano y flexible, fácil para cruzar entre paredes.
- Tamaño reducido, por lo que no se llenan rápidamente los conductos de cableado.
- Cuesta menos por metro que cualquier otro tipo de cable LAN.
- El UTP puede ser full dúplex y dependiendo otras condiciones full-full dúplex.

**Desventajas**

- **La susceptibilidad del par trenzado a las interferencias electromagnéticas EMI.**
- **La susceptibilidad del par trenzado a las interferencias de radiofrecuencia RFI.**

**Categorías del cable UTP**

**Categoría 1:** Es empleada en las redes telefónicas, transmisión de datos de baja capacidad (hasta 4Mbps).

**Categoría 2:** Empleada en voz de datos, esta categoría consiste de los cables normalizados a 1 MHz.

**Categoría 3:** soporta velocidades de transmisión hasta 10 Mbits/seg. Utilizado para telefonía de voz, 10Base-T Ethernet y Token ring a 4 Mbits/seg.

**Categoría 4:** soporta velocidades hasta 16 Mbits/seg. Es aceptado para Token Ring a 16 Mbits/seg.

**Categoría 5**: Hasta 100 Mbits/seg. Utilizado para Ethernet 100Base-TX.

**Categoría 5e:** Hasta 622 Mbits/seg. Utilizado para Gigabit Ethernet.

**Categoría 6:** Soporta velocidades hasta 1000 Mbits/seg.

**Categoría 6A:** Indica sistemas de cables llamados Categoría 6 Aumentada o más frecuentemente "Categoría 6A", que operan a frecuencias de hasta 550 MHz (tanto para cables no blindados como cables blindados) y proveen transferencias de hasta 10 GBit/s.

**Categoría 7:** Es un estándar de cable para Ethernet y otras tecnologías de interconexión que puede hacerse compatible hacia atrás con los tradicionales de Ethernet actuales Cable de Categoría 5 y Cable de Categoría 6/6A, puede transmitir frecuencias de hasta 600MHz.

**Categoría 7A:** Es parecido al cable categoría 7 es compatible hacia atrás con los tradicionales de Ethernet actuales Cable de Categoría 5, Cable de Categoría 6/6A y 7, puede transmitir frecuencias de hasta 1200MHz.

**Categoría 8:** Es un estándar de cable para Ethernet de alta velocidad usada principalmente en Datacenters, se diseña para soportar altas velocidades de 40Gbps, pero solo a 30 metros, permite trasmitir varios servicios diferentes los datos al gracias a sus múltiples conectores, transmite en frecuencias de hasta 1200MHz, no está pensado para ser usado como cableado en redes LAN por su limitación a 30 Metros.

Dependiendo las categorías del UTP se definen como (ver **¡Error! No se encuentra el origen de la referencia.**):

| | | | |
|---|---|---|---|
| **-** | **10Mbps** | **16Mhz** | Categoría 3 |
| **10BASET** | **10Mbps** | **20Mhz** | Categoría 4 |
| **100BASET** | **100Mbps** | **100Mhz** | Categoría 5 |
| **100BASETX** | **100Mbps** | **150Mhz** | Categoría 5e |
| **1000BASET** | **1000Mbps** | **350Mhz** | Categoría 6 |
| **1000BASETX** | **1000Mbps** | **350Mhz** | Categoría 6A |
| **10GBASET** | **10000Mbps** | **600Mhz** | Categoría 7 |
| **10GBASET** | **10000Mbps** | **1200Mhz** | Categoría 7A |
| **40GBASET** | **40000Mbps** | **1200Mhz** | Categoría 8 |

**Adaptado de http://es.wikipedia.org/wiki/Cable_de_par_trenzado.**

Entre los cables de 10Gigabit existe una amplia variedad

**10GBASE-SR** ("short range") -- Diseñada para funcionar en distancias cortas sobre cableado de fibra optica multi-modo, permite una distancia entre 26 y 82 m dependiendo del tipo de cable. También admite una distancia de 300 m sobre una nueva FIBRA ÓPTICA multi-modo de 2000 MHz·km (usando longitud de onda de 850nm).

**10GBASE-CX4** -- Interfaz de cobre que usa cables INFINIBAND CX4 y conectores InfiniBand 4x para aplicaciones de corto alcance (máximo 15 m ) (tal como conectar un switch a un router). Es la interfaz de menor coste pero también el de menor alcance. 2,5 Gbps por cada cable.

**10GBASE-LX4** -- Usa multiplexión por división de longitud de onda para distancias entre 240 m y 300 m sobre fibra óptica multi-modo. También admite hasta 10 km sobre fibra mono-modo. Usa longitudes de onda alrededor de los 1310 nm.

**10GBASE-LR** ("long range") -- Este estándar permite distancias de hasta 10 km sobre fibra mono-modo (usando 1310nm).

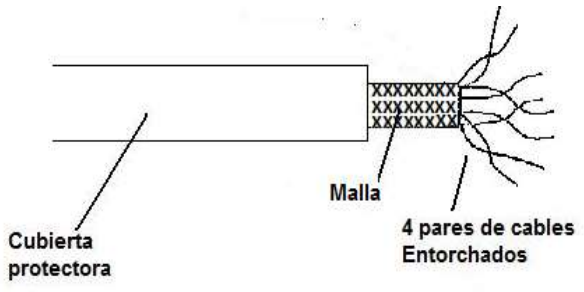
**10GBASE-ER** ("extended range") -- Este estándar permite distancias de hasta 40 km sobre fibra mono-modo (usando 1550nm). Recientemente varios fabricantes han introducido interfaces enchufables de hasta 80-km.

**10GBASE-LRM** - HTTP://WWW.IEEE802.ORG/3/AQ/, 10 Gbit/s sobre cable de FDDI- de 62.5 µm.

**10GBASE-SW**, **10GBASE-LW** y **10GBASE-EW**. Estas variedades usan el WAN PHY, diseñado para interoperar con equipos OC-192/STM-64 SONET/SDH usando una trama ligera SDH/SONET. Se corresponden en el nivel físico con 10GBASE-SR, 10GBASE-LR y 10GBASE-ER respectivamente, y por ello usan los mismos tipos de fibra y permiten las mismas distancias. (No hay un estándar WAN PHY que corresponda al 10GBASE- LX4.).

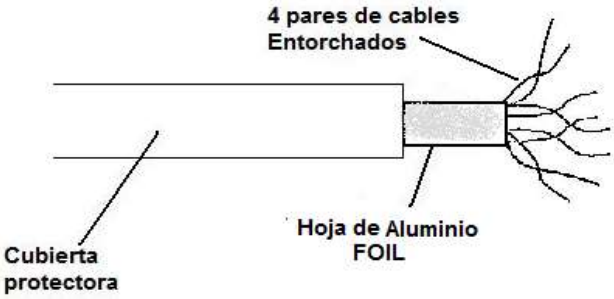
*Tomado de HTTP://ES.WIKIPEDIA.ORG/WIKI/10_GIGABIT_ETHERNET*

**S/UTP, Shield/ Unshield Twister Pair:** Cable UTP apantallado la construcción de estos cables se muestra en **¡Error! No se encuentra el origen de la referencia.**



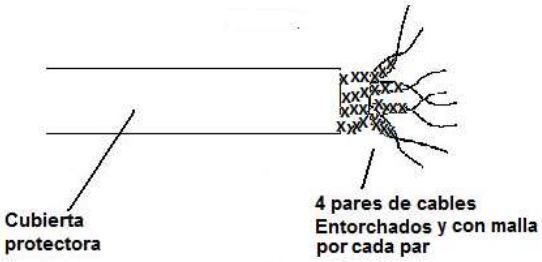

*Esquema S/UTP fuente el autor*

**FTP, Foiled Twister Pair:** Los pares se recubren de una hoja de aluminio (foil), **¡Error! No se encuentra el origen de la referencia.**



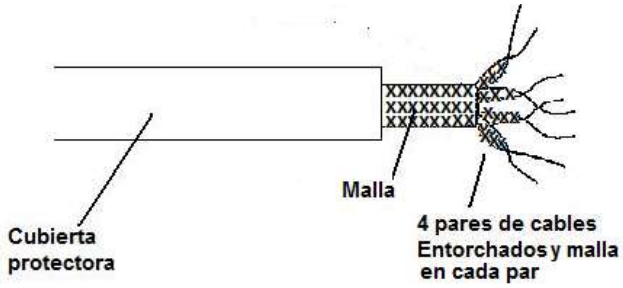

*Esquema cable FTP fuente el autor*

**STP, Shield Twister Pair:** Apantallamiento en cada uno los pares, **¡Error! No se encuentra el origen de la referencia.**



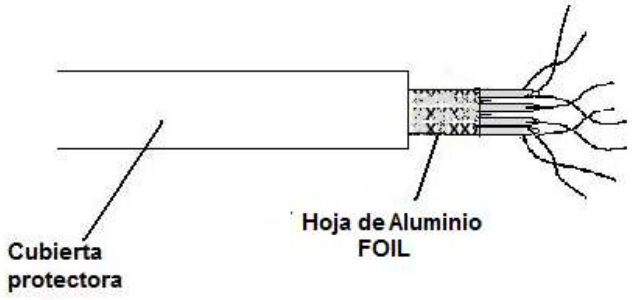

*Esquema STP*

**S/STP, Shield/ Shield Twister Pair:** Es un cable doblemente apantallado, tanto sus pares como el cable en sí. **¡Error! No se encuentra el origen de la referencia.**




*Esquema S/STP fuente el autor*

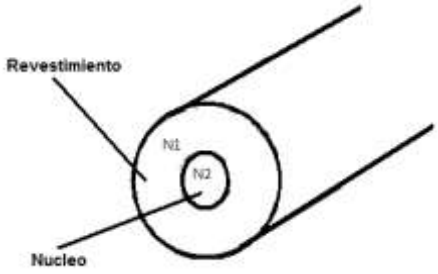
**F/FTP, Foiled/Foiled Twister Pair:** Tanto los pares como el cable están cubiertos de una malla global en forma trenzada. **¡Error! No se encuentra el origen de la referencia.**




*Esquema cable F/FTP fuente el autor*

## 3.5 TEMA 4 CABLES FIBRA OPTICA

La Tecnología consiste un conducto generalmente de fibra de vidrio (polisilicio) que transmite impulsos luminosos normalmente emitidos por un LASER o LED. **¡Error! No se encuentra el origen de la referencia.**




*Fibra Óptica fuente el autor*

Las fibras ópticas que se emplean en aplicaciones a largas distancias son siempre de vidrio; las de plásticos sólo son usadas en redes locales LAN; al interior de la fibra óptica, el haz de luz se refleja. Esto permite transmitir las señales casi sin pérdida por largas distancias. **¡Error! No se encuentra el origen de la referencia.**, **¡Error! No se encuentra el origen de la referencia.**

*Detalle Fibra Óptica multipar fuente el autor*

*Detalle fibra óptica Monopar fuente el autor*

La fibra óptica ha remplazado a los cables de cobre por su costo y beneficio.

**VENTAJAS**

## BAJA ATENUACIÓN

- Las fibras ópticas son el medio físico con menor atenuación. Por lo tanto, se pueden establecer enlaces directos sin repetidores, de 100 a 200 Km con el consiguiente aumento de la fiabilidad y economía en los equipamientos.
- Gran ancho de banda
- La capacidad de transmisión es muy elevada. De hecho 2 fibras ópticas serían capaces de transportar, todas las conversaciones telefónicas de un país, con equipos de transmisión capaces de manejar tal cantidad de información (entre 100 MHz/Km a 10 GHz/Km).

## PESO Y TAMAÑO REDUCIDOS

- El diámetro de una fibra óptica es similar al de un cabello humano. Un cable de 64 fibras ópticas, tiene un diámetro total de 15 a 20 mm. y un peso medio de 250 Kg/km.
- Gran flexibilidad y recursos disponibles
- Los cables de fibra óptica se pueden construir totalmente con materiales dieléctricos, la materia prima utilizada en la fabricación es el dióxido de silicio (Si0 2) que es uno de los recursos más abundantes en la superficie terrestre.

## AISLAMIENTO ELÉCTRICO ENTRE TERMINALES

- Al no existir componentes metálicos (conductores de electricidad) no se producen inducciones de corriente en el cable, por tanto, pueden ser instalados en lugares donde existen peligros de cortes eléctricos.

| AUSENCIA DE RADIACIÓN EMITIDA |
|---|
| • Las fibras ópticas transmiten luz y no emiten radiaciones electromagnéticas que puedan interferir con equipos electrónicos, tampoco se ve afectada por radiaciones emitidas por otros medios, por lo tanto, constituyen el medio más seguro para transmitir información de muy alta calidad sin degradación. Las señales se pueden transmitir a través de zonas eléctricamente ruidosas con muy bajo índice de error y sin interferencias eléctricas. |

**DESVENTAJAS**

- El costo de la fibra sólo se justifica cuando su gran capacidad de ancho de banda y baja atenuación es requerida.
- La fibra óptica no transmite energía eléctrica, esto limita su aplicación donde el terminal de recepción debe ser energizado desde una línea eléctrica.
- La energía debe proveerse por conductores separados.
- Las moléculas de hidrógeno pueden difundirse en las fibras de silicio y producir cambios en la atenuación. El agua corroe la superficie del vidrio y resulta ser el mecanismo más importante para el envejecimiento de la fibra óptica.

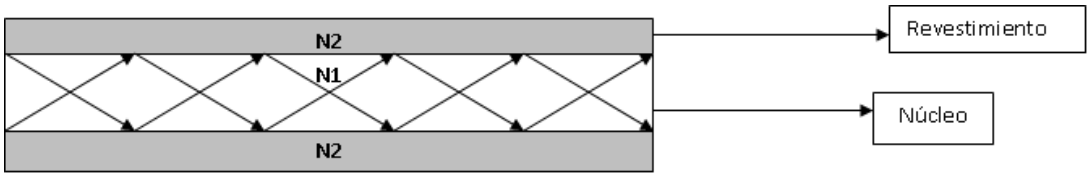
*Para ampliar esta información dirígete a HTTP://WWW.ALEGSA.COM.AR/DIC/FIBRA%20OPTICA.PHP*

**Clasificación De Las Fibras Ópticas**

Para usos en telecomunicaciones se clasifican según el modo de propagación de la luz siendo **Fibras Multimodo** y **Fibras Monomodo**.

- **Fibras ópticas Multimodo**

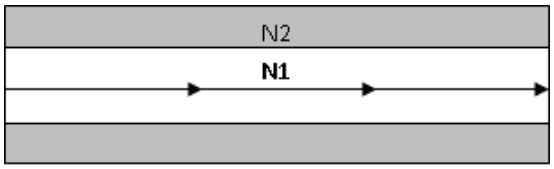
Estas fibras permiten que la luz pueda tener muchas reflexiones al interior de ella a realizar la transmisión (modos de propagación). Se usan en transmisiones a cortas distancias menores a 1 Km.; es simple de diseñar y económico, ***Fibra óptica Multimodo***. La palabra modo significa trayectoria.




**Fibra óptica Multimodo fuente el autor**

- **Fibras ópticas Monomodo**

Se fabrican para que transmitan un solo rayo de luz (un único modo de propagación).**¡Error! No se encuentra el origen de la referencia.**

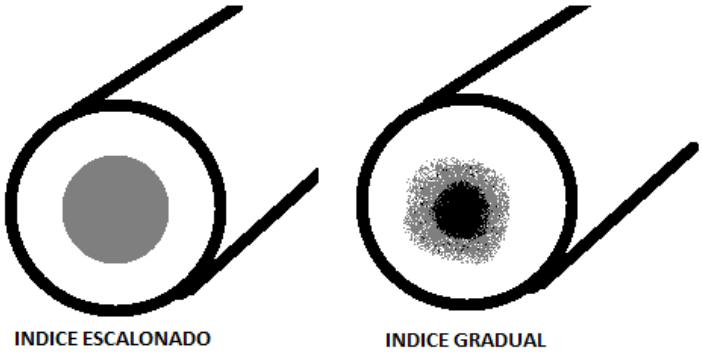



**Fibra óptica Monomodo fuente el autor**

**Tipos de fibra óptica**

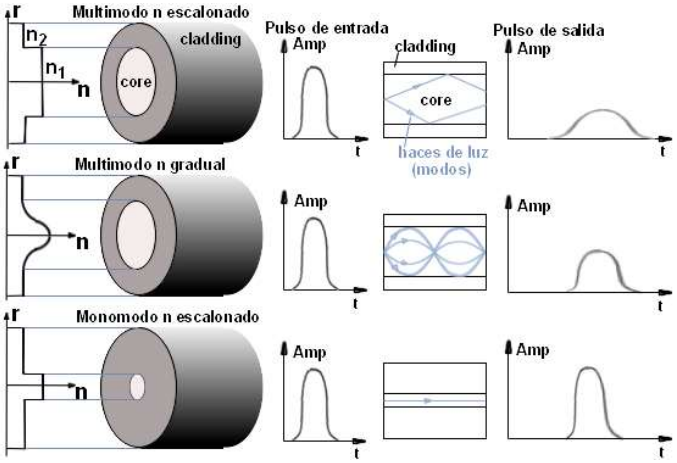
Además de ser monomodo o multimodo las fibras pueden clasificase según las formas en que está disperso el material dopante del núcleo interior de la fibra, esta puede ser de índice Gradual u índice escalonado.

El índice escalonado o salto de índice tiene como resultado un cambio brusco entre los núcleos N1 y N2, el índice gradual o índice gradiente permite un cambio progresivo lo que perite mayores distancias



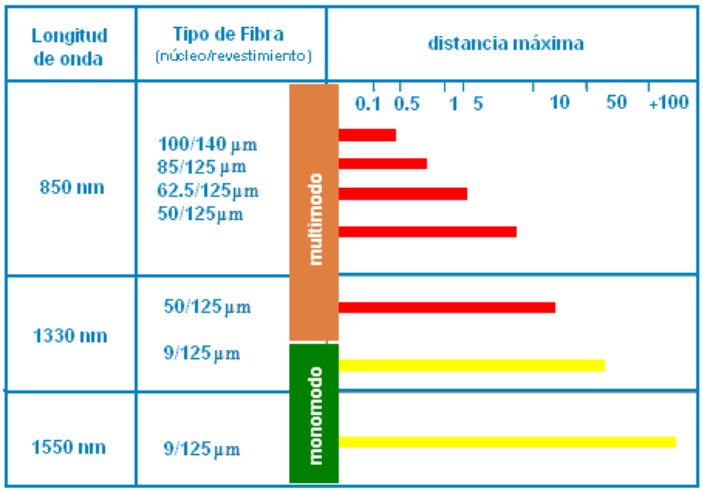

**Índice Gradual e índice Escalonado**

La **¡Error! No se encuentra el origen de la referencia.** muestra como se deteriora la señal enviada en fibras monomodo, y fibras Multimodo de salto de índice y de índice gradiente




**Deterioro de la señal en las fibra ópticas por el índice de refracción fuente (www.yio.com.ar/fo/)**

La **¡Error! No se encuentra el origen de la referencia.** muestra las distancias típicas a las que se puede enviar la información usando fibras ópticas mono monomodo y multimodo.




**Deterioro de la señal por la distancia en fibras Ópticas fuente (nemesis.tel.uva.es/)**

**Ventanas de Fibra óptica**

El termino ventana utiliza especialmente en la transmisión en fibra óptica y se refiere a las distintas frecuencias en las cuales se transmite el haz de luz, es decir, la longitud de onda que tiene el haz de luz.

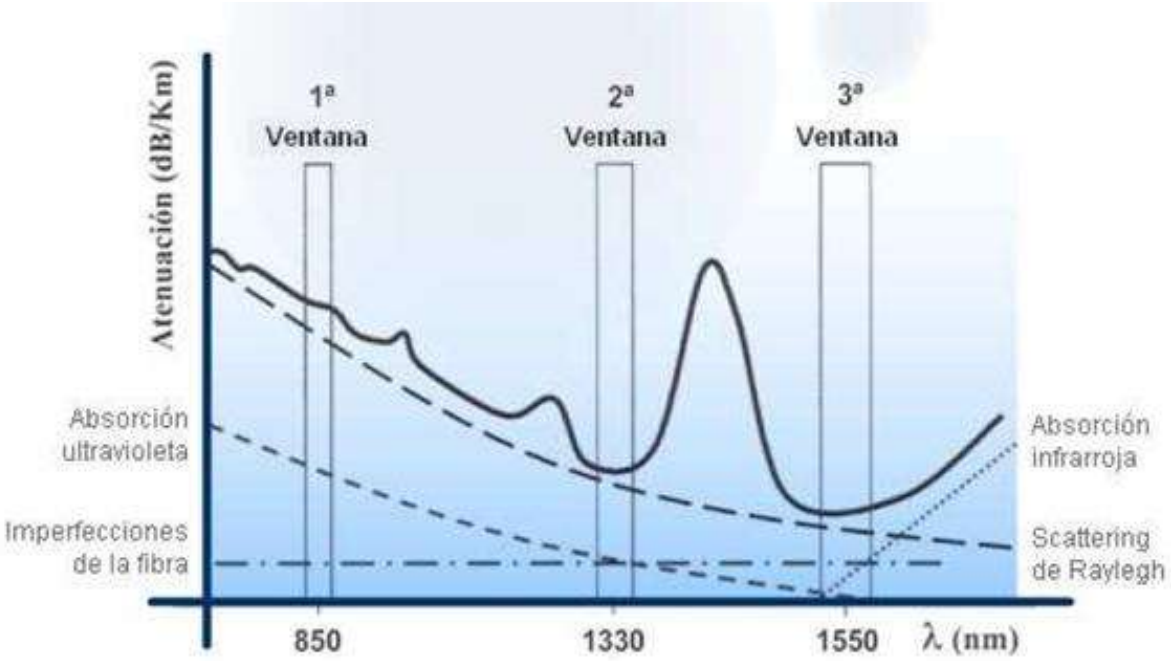
Se usan 3 longitudes de ondas distintas 3 ventanas de trabajo:

· Primera Ventana: 850 nm se logran con LED relativamente económicos, y no se esperan grandes distancias se usan cables multimodo de índice escalonado

· Segunda Ventana: 1310 nm en esta ventana se usan LED potentes o Laser económicos las distancias son relativamente amplias pueden usarse cables monomodo o cables multimodo de índice gradual.

· Tercera Ventana: 1559 nm. En esta ventana se usan laser de alta intensidad y se esperan las mayores distancias posibles, se usa cable MONOMODO

El empleo de las distintas ventanas depende de cómo podemos obtener mejores prestaciones en la transmisión por la fibra óptica, o del equipo óptico en su conjunto. Es decir, obtenemos menos perdidas en esas longitudes de ondas, la **¡Error! No se encuentra el origen de la referencia.** muestra que la atenuación en la tercera ventana 1550nm es la menor de todas las ventanas, por esto se usa para largas distancias, pero requiere equipos costosos, por su lado la primera ventana 850nm tiene una atenuación mucho mayor, pero para lograr 850nm se requieren equipos relativamente económicos, por eto se usa para proyectos que requieran distancias cortas y presupuesto reducido.




**Ventanas fibra óptica fuente (fibraoptica.blog.tartanga.net/)**

## 3.6 TEMA 6 CABLEADO ESTRUCTURADO

El Cableado el medio físico, cables y elementos complementarios a través del cual se interconectan dispositivos de para formar una red, un sistema de cableado es la infraestructura requerida para lograr la trasmisión de datos en forma confiable.

El concepto Cableado estructurado lo definen los siguientes puntos:

• Solución Segura: El cableado se encuentra instalado de tal manera que los usuarios del mismo tienen la facilidad de acceso a lo que deben de tener y el resto del cableado se encuentra perfectamente protegido.

• Solución Longeva: Cuando se instala un cableado estructurado se convierte en parte del edificio, así como lo es la instalación eléctrica, por tanto, este tiene que ser igual de funcional que los demás servicios del edificio. La

gran mayoría de los cableados estructurados pueden dar servicio por unos periodos largos de tiempo que están alrededor de 10 se puede pensar en 15 años, ligados a los avances tecnológicos.

• Modularidad: Capacidad de integrar varias tecnologías sobre el mismo cableado (voz, datos, video) en otras palabras el mismo cableado sin cambios, sirve para telefonía y comunicar los PC,

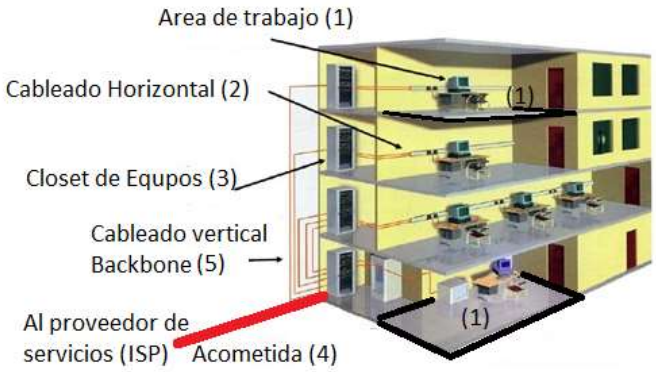
- Fácil Administración: El cableado estructurado se divide en partes manejables que permiten hacerlo confiable y perfectamente administrable, pudiendo así detectar fallas y repararlas fácilmente

## 3.6.1 ¿CUÁLES SON LAS PARTES QUE INTEGRAN UN CABLEADO ESTRUCTURADO?

1. **Área de trabajo** – Su nombre lo dice todo, Es el lugar donde se encuentran el personal trabajando con las computadoras, impresoras, etc. En este lugar se instalan los servicios (nodos de datos, telefonía, energía eléctrica, etc.) Closet de comunicaciones – Es el punto donde se concentran todas las conexiones que se necesitan en el área de trabajo.

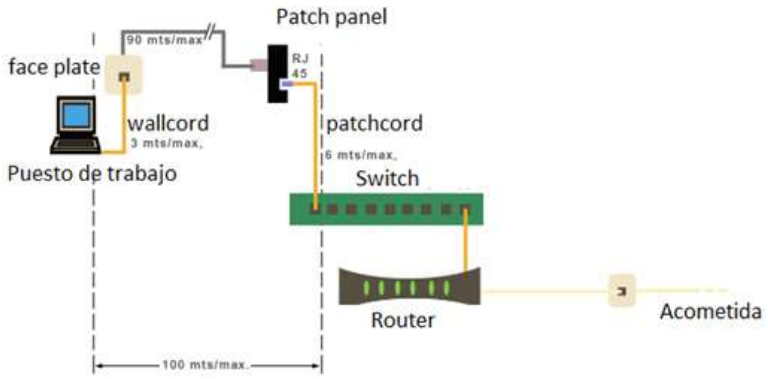
2. **Cableado Horizontal**: es aquel que viaja desde el área de trabajo hasta el closet (armario) de comunicaciones.
3. **Closet de Equipo** – En este cuarto se concentran los servidores de la red, el conmutador telefónico, etc. Este puede ser el mismo espacio físico que el del closet de comunicaciones y de igual forma debe ser de acceso restringido.
4. **Instalaciones de Entrada (Acometida)** – Es el punto donde entran los servicios al edificio y se les realiza una adaptación para unirlos al edificio y hacerlos llegar a los diferentes lugares del edificio en su parte interior. (no necesariamente tienen que ser datos pueden ser las líneas telefónicas, o BackBone que venga de otro edificio, entre otros).
5. **Cableado Vertical (Back Bone)** – Es el medio físico que une 2 redes entre sí.

La **¡Error! No se encuentra el origen de la referencia.** muestra la ubicación de las partes de un cableado estructurado en una edificación



**partes de un sistema de cableado estructurado (fuente adaptado de erik140.blogspot )**

La **¡Error! No se encuentra el origen de la referencia.** muestra las distancias máximas de los tramos de cableado WallCord (6mts), Cableado Horizontal (100mts) y patchcord (3mts)




**Detalle de cableado (fuente westerntel-com.com/)**

- Tenemos **el dispositivo** que queremos conectar a la red, este puede ser **un teléfono**, **una computadora,** o **cualquier otro**, este está en **el puesto de trabajo**.
- **Wallcord** – Debemos de contar con un cable que une este dispositivo a la placa que se encuentra en la pared (en el área de trabajo), este es un cable de alta resistencia y flexible ya que está considerado para ser conectado y desconectado cuantas veces lo requiera el usuario.

*cable de red wallcord (fuente www.electrotelefonicas.com/ )*

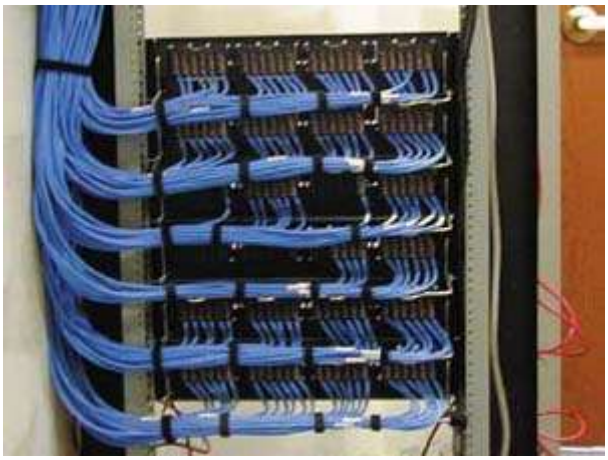
- **Placa con servicios (face plate)** – Esta placa contiene los conectores donde puede ser conectado el dispositivo, pensando en una red de datos, tendremos un conector RJ45 donde puede ser insertado el plug del cable, La misma placa puede combinar servicios (voz, datos, video, entre otros).

**Faceplate (fuente www.electrotelefonicas.com/)**

- **El Patch panel–** Sirve como organizador de las conexiones de la red, para que los elementos relacionados de la red de área local (LAN) y los equipos de conectividad puedan ser fácilmente incorporados al sistema, y además los puertos de conexión de los equipos activos de la red (switch, router, entre otros) no tengan daños por el constante trabajo de retirar e introducir los conectores en sus puertos. Los patch panels son paneles electrónicos que están dentro del rack e interconectan el cableado horizontal con la parte trasera del patch panel.

*Patch panel (fuente www.excel-networking.com/)*

- **Patch Cord** –Es el segmento de cable que une el patchpanel con el Switch, es ekl cableado que está dentro del armario de comunicaciones o rack



**Patchcord (fuente www.westerntel-com.com/)**

## 3.6.2 ¿CUÁNDO SE JUSTIFICA INSTALAR UN CABLEADO ESTRUCTURADO?

Cuando se desee tener una red confiable. El cableado, este es el medio físico que interconecta la red y si no se tiene bien instalado ponemos en riesgo el buen funcionamiento de la misma.

Cuando se desee integrar una solución de largo plazo para la integración de redes. Esto significa hacer las cosas bien desde el principio, el cableado estructurado garantiza que pese a las nuevas innovaciones de los fabricantes de tecnología, estos buscan que el cableado estructurado no se altere, ya que este una vez que se instala se convierte en parte del edificio. La media de uso que se considera para un cableado estructurado es de 10 años o un poco mas

Cuando el número de dispositivos de red que se va a conectar justifique la instalación de un cableado estructurado para su fácil administración y confiabilidad en el largo plazo. (de 10 dispositivos de red en adelante). Si hablamos de una pequeña oficina (menos de 10 dispositivos de red), puede ser que la inversión que representa hacer un cableado estructurado no se justifique y por tanto se puede optar por un cableado mas informal instalado de la mejor manera posible

# 3.7 TEMA 7 DISEÑO DE UN CABLEADO ESTRUCTURADO

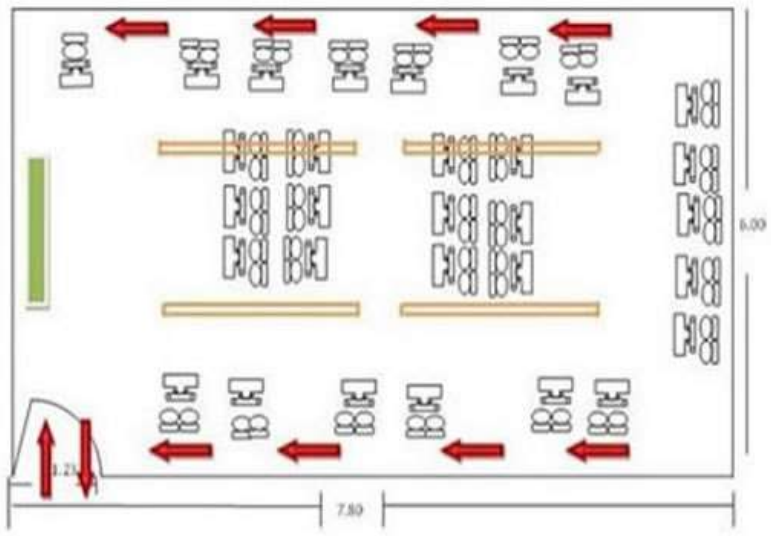
Se entiende por mapa o plano a la representación gráfica en dos dimensiones (2D) y tamaño reducido (a escala) de un terreno o territorio real (3D). Es decir, es un dibujo que trata de representar un espacio real o un paisaje, pero visto desde arriba, como si lo observásemos desde un avión. (ieslasllamas.com).

El plano de red permite recorrer espacios desconocidos, calcular distancias y decidir recorridos posibles de las canaletas y cableado. El mapa es una herramienta imprescindible para el diseño fisco de una red por varias razones:

- En él están representadas las balizas que marcan los espacios para que las personas puedan caminar.
- Ayuda a posicionarnos en el área de red y a decidir que recorrido es el más ventajoso para economizar cable o ductos como canaletas.
- Ayuda a estimar los costos del cableado a tirar.
- Muestra obstáculos o dificultades existentes.

## 3.7.1 PLANOS ARQUITECTÓNICOS

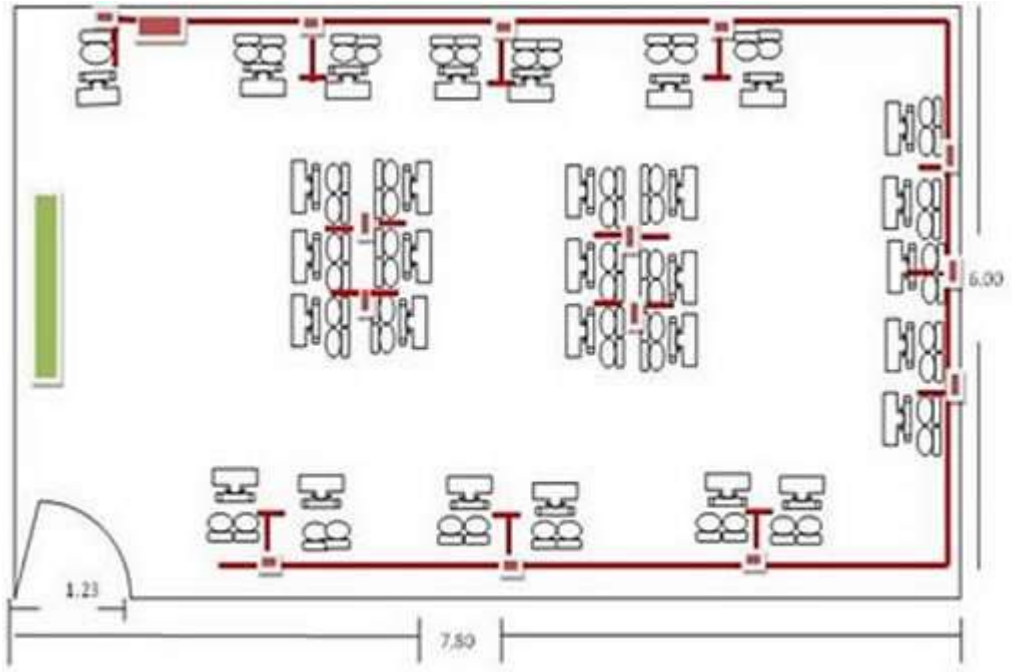
Definen la infraestructura muros paredes distancias, accesos y distribución de las áreas de trabajo




*Plano arquitectónico (fuente el autor )*

## 3.7.2 PLANO ELÉCTRICO

Define la distribución de tomas y demás elementos eléctricos, cableados caja de distribución, caja de breakers. Un ejemplo es se muestra en ***Plano eléctrico***

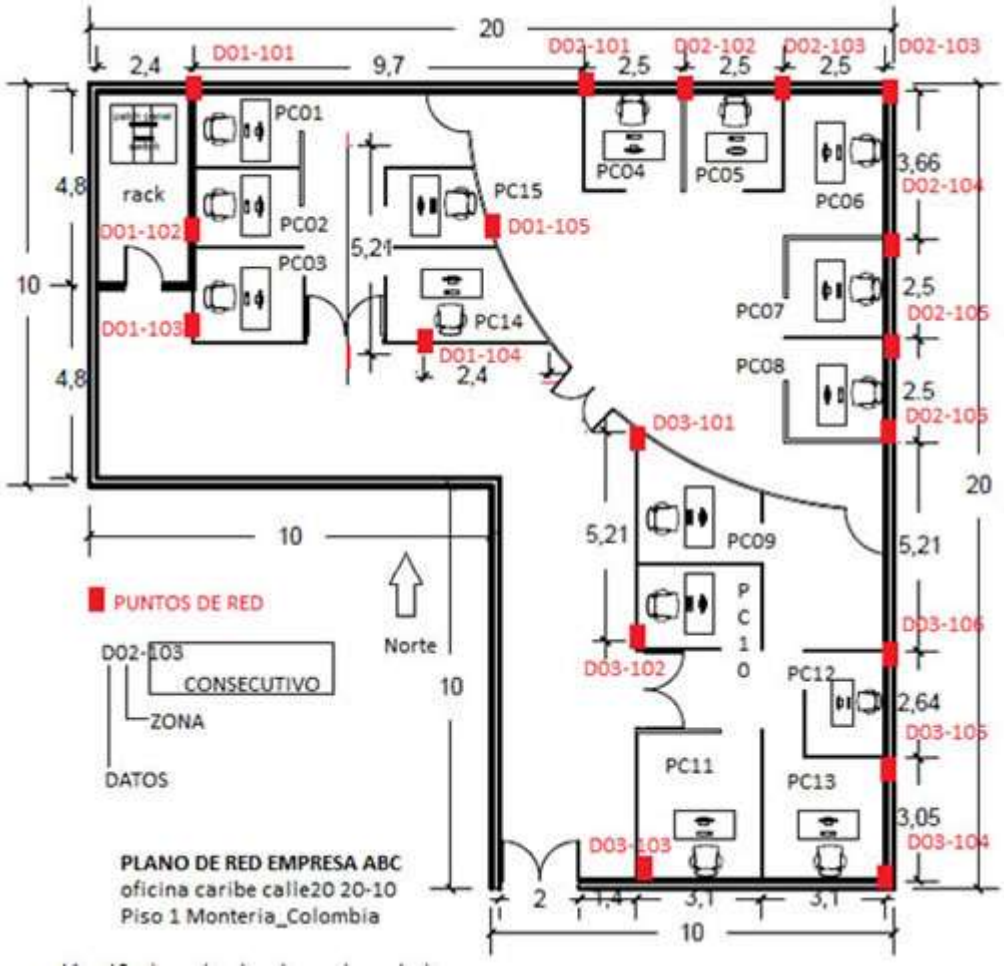



**Plano eléctrico (fuente el autor)**

## 3.7.3 PLANO DE REDES

Junto con el plano eléctrico es el más importante para los asuntos diseño de cableado. Los planos de redes como el de la **¡Error! No se encuentra el origen de la referencia.** deben tener al menos:

- Ubicación de cada uno de los puntos de red
- Medidas de a cada punto de red al armario de comunicaciones (no solo de los muros)
- Descripción de nomenclatura y Nomenclatura de puntos de red (EIA/TIA 606)
- Datos de empresa
- Ubicación de los elementos de red




*Plano red (fuente el autor)*

**Recomendación de Ubicación de los elementos de internetworking**

Use un compás para trazar círculos que representen un radio de 50 m (a escala). a partir de cada ubicación del rack potencial. Cada uno de los dispositivos de red que dibuje en su plano deberá quedar dentro de uno de estos círculos)

Luego conteste a las siguientes **preguntas**:

1) ¿Alguno de los círculos se superpone?
2) ¿Se puede eliminar alguna de las posibles ubicaciones de armarios para el cableado?
3) ¿Alguno de los círculos abarca todos los dispositivos que se conectarán a la red?

4) ¿Cuál de las posibles ubicaciones del armario para el cableado parece ser la mejor?

5) ¿Hay algún círculo en el que sólo algunos dispositivos queden fuera del área de captación?

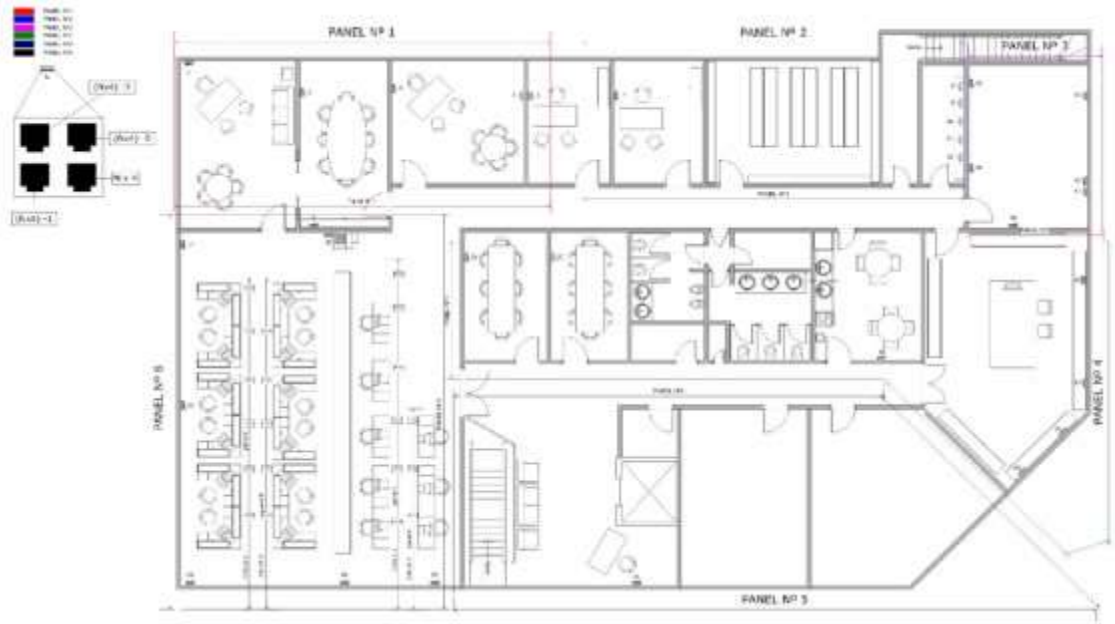
6) ¿Qué armario para el cableado potencial está más cercano a la acometida externa?

7) Basándose en sus respuestas, haga una lista de las tres mejores ubicaciones posibles para los armarios para el cableado.

8) Teniendo en cuenta sus respuestas, ¿cuántos armarios para el cableado piensa que serán necesarios para esta red?

9) ¿Cuáles son las ventajas y desventajas de cada una de las posibles ubicaciones de armario para el cableado que aparecen en el plano de red?

Además de los planos eléctrico y de red es requerido un plano de piso, **¡Error! No se encuentra el origen de la referencia.**, en este se plasma la ubicación del mobiliario, mesas, sillas, elementos decorativos, y otra información relevante en cuanto al uso de los espacios.



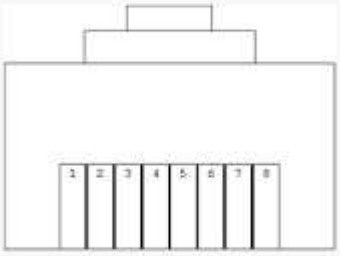

**Plano de piso**

## 3.7.4 NORMAS EIA/TIA

A mediados de la década de 1980, la TIA (Telecommunications Industry Association) y la EIA (Electronic Industries Association) comenzó a desarrollar métodos de cableado de edificios, con la intención de desarrollar un sistema de cableado uniforme que apoyar los productos de múltiples fabricantes y entornos.

El estándar de cableado estructurado TIA / EIA definen la forma de diseñar, construir y administrar un sistema de cableado que es estructurado, lo que significa que el sistema está diseñado en bloques que tienen características de rendimiento muy específicos. Los bloques se integran de una manera jerárquica para crear un sistema de comunicación unificado. Por ejemplo, el grupo de trabajo LAN representan un bloque con los requerimientos de menor rendimiento que el bloque de red troncal, que requiere un cable de alto rendimiento de fibra óptica en la mayoría de los casos. (Lilwatne, 2012)

La norma define el uso de cable de fibra óptica (monomodo y multimodo), cable STP (par trenzado con blindaje), y UTP (par trenzado sin blindaje) de cable.

| Pin | Color T568A | Color T568B | Pines en conector macho (hembra invertidos) |
|---|---|---|---|
| 1 | Blanco/Verde (W-G) | Blanco/Naranja (W-O) |  |
| 2 | Verde (G) | Naranja (O) | |
| 3 | Blanco/Naranja (W-O) | Blanco/Verde (W-G) | |
| 4 | Azul (BL) | Azul (BL) | |
| 5 | Blanco/Azul (W-BL) | Blanco/Azul (W-BL) | |
| 6 | Naranja (O) | Verde (G) | |
| 7 | Blanco/Marrón (W-BR) | Blanco/Marrón (W-BR) | |
| 8 | Marrón (BR) | Marrón (BR) | |

**Código de colores norma T568 A/B (fuente lilwatne.blogspot.com.co/ )**

Las Normas y Publicaciones de Ingeniería de TIA/EIA se diseñan con el objetivo de servir al interés público eliminando los malentendidos entre fabricantes y compradores, facilitando la intercambiabilidad y mejoramiento de los productos y ayudando al comprador a seleccionar y obtener con la menor demora posible el producto mejor adaptado a sus necesidades particulares.

### 3.7.4.1 ESTANDAR TIA/EIA 568-A

En octubre de 1995, el modelo 568 fue corregido por el TIA/EIA 568-A que absorbió entre otras modificaciones los boletines TSB-36 y TSB-40.

Esta norma, regula todo lo concerniente a:

- Sistemas de cableado estructurado para edificios comerciales
- Parámetros de medios de comunicación que determinan el rendimiento.
- Disposiciones de conexión y sujeción para asegurar la interconexión.

### 3.7.4.2 PROPÓSITO DEL ESTÁNDAR TIA/EIA 568-A:

- Establecer un cableado estándar genérico de telecomunicaciones para respaldar un ambiente multiproveedor
- Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
- Establecer un criterio de ejecución y técnico para varias configuraciones de sistemas de cableados.
- Proteger las inversiones realizadas por el cliente (como mínimo 10 a 15 años)
- Las normas TIA/EIA fueron creadas como norma de industria en un país, pero se han empleado como normas internacionales por ser las primeras en crearse.

### 3.7.4.3 ESTANDAR TIA/EIA 568 B

Para abril del año 2001 se completó la revisión “B” de la norma de cableado de Telecomunicaciones para edificios comerciales (Comercial Building telecommunications Cabling Standard).

La norma se subdivide en **tres documentos** que constituyen normas separadas (EIA/TIA):

- ANSI/TIA/EIA-568-B.1-2001
- ANSI/TIA/EIA-568-B.2-2001
- ANSI/TIA/EIA-568-B.3-2000

### 3.7.4.4 ESTANDAR TIA/EIA 568 C

Pocos documentos tienen tanto efecto en la industria del cableado estructurado como la serie de estándares ANSI/TIA/EIA-568-B. Así, Cuando el Comité de Ingeniería para Requisitos del Cableado de Telecomunicaciones para Usuarios de Instalaciones Comerciales anunció la aprobación de la serie de estándares ANSI/TIA/EIA-568-C, se despertó gran interés en el mercado. En algunos casos, ese interés se expresó como desesperación y estuvo acompañado de crujir de dientes, generalmente por parte de aquellos quienes no habían terminado de comprender la serie de estándares 568-B. (EIA/TIA)

**TIA**-568. B se actualizó para incluir los siguientes nuevos estándares:

**TIA-568 Rev. C.0** "Cableado de telecomunicaciones genérico para instalaciones de clientes"

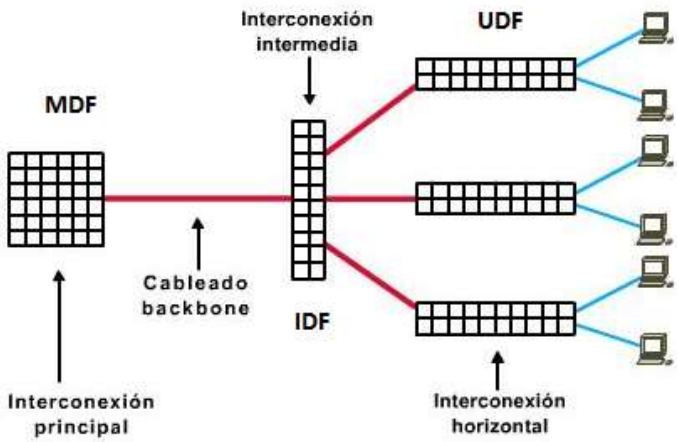
**TIA-568 Rev. C.1** "Estándar de cableado de telecomunicaciones para edificios comerciales"

**TIA-568 Rev. C.2** "Estándar de componentes y cableado de telecomunicaciones de par trenzado balanceado"

**TIA-568 Rev. C.3** "Estándar de componentes de cableado de fibra óptica"

El tipo de cableado que el estándar **TIA/EIA-568** específica para realizar la conexión de los armarios para el cableado entre sí en una LAN Ethernet con topología en estrella extendida se denomina cableado backbone. A veces, para diferenciarlo del cableado horizontal, podrá ver que el cableado backbone también se denomina cableado vertical, este comprende:

- Tendidos de cableado backbone
- Conexiones cruzadas (cross-connects) intermedias y principales
- Terminaciones mecánicas
- Cables de conmutación utilizados para establecer conexiones cruzadas entre cableados backbone




**Ubicación de MDF, IDF y UDF adaptación el autor**

**UDF: User Distribution Frame** Armario que conecta los computadores de los usuarios finales al centro de cableado, se conecta por un cable al IDF más cercano.

**IDF**: **Intermediate Distribution Fame**, Interconexión horizontal. Armario para el cableado donde los UDF se conectan a un panel de conmutación, que a su vez se conecta mediante un cableado backbone al MDF

**MDF**: **Main Distribution Frame** Interconexión principal. Armario para el cableado que sirve como punto central en una topología en estrella y en el que el cableado backbone de la LAN se conecta a la Internet

### 3.7.4.5 ANSI / TIA / EIA - 569 – **A NORMA DE CONSTRUCCIÓN** COMERCIAL PARA ESPACIOS Y RECORRIDOS DE TELECOMUNICACIONES

Esta norma se creó en 1990 como el resultado de un esfuerzo conjunto de la Asociación Canadiense de Normas (CSA) y Asociación de las Industrias Electrónicas (EIA). Se publican de manera separada en EE.UU. y Canadá, aunque las secciones centrales de las dos sean muy semejantes. La edición actual es de febrero de 1998. Esta norma indica los siguientes elementos para espacios y recorridos de telecomunicaciones en construcciones:

- Recorridos Horizontales.
- Armarios de Telecomunicaciones.
- Recorridos para *Backbones.*
- Sala de Equipos.
- Estación de Trabajo.

- Sala de Entrada de Servicios.

Para ampliar esta información dirígete a http://www.galeon.com/30008ceti/tarea3.html

### 3.7.4.6 EIA/TIA 606ESTÁNDAR DE ADMINISTRACIÓN PARA LA INFRAESTRUCTURA DE TELECOMUNICACIONES DE EDIFICIOS COMERCIALES

La **norma 606** es vital para **el buen funcionamiento del cableado estructurado** ya que habla sobre la identificación de cada uno de **los subsistemas** basado en etiquetas, códigos y colores, con la finalidad de que se puedan identificar cada uno de los servicios que en algún momento se tengan que habilitar o deshabilitar. Esto es muy importante, ya que en la documentación que se debe entregar al usuario final, la norma dice que se tendrá que especificar la forma en que está distribuida la red, por dónde viaja, qué puntos conecta y los medios que utiliza (tipos de cables y derivaciones).

La norma **TIA/EIA 606** proporciona **una guía** que puede ser utilizada para **la ejecución** de la **administración** de los **sistemas de cableado**.

Resulta fundamental para lograr una cotización adecuada suministrar a los oferentes la mayor cantidad de información posible. En particular, es muy importante proveerlos de planos de todos los pisos, en los que se detallen:

1.- Ubicación de los gabinetes de telecomunicaciones

2.- Ubicación de ductos a utilizar para cableado vertical

3.- Disposición detallada de los puestos de trabajo

4.- Ubicación de los tableros eléctricos en caso de ser requeridos

## 3.7.5 EJERCICIO DE ENTRENAMINETO

1. Responda falso o verdadero, justificando debidamente su respuesta:

| | |
|---|---|
| ¿Emi es la sigla de un elemento de las capa 4 del modelo osi? | |

| | |
|---|---|
| El cable coaxial es un cable formado por ocho pares de hilos ? | |
| 10Baset se refiere a un cable coaxial | |
| La velocidad de transferencia puede ser expresada como MBps | |

1. Describa los siguientes tipos de cable UTP, FTP, STP
2. Llene la siguiente tabla

| Tipo de cable | Velocidad máxima de trasmisión en 100MTS | Frecuencias máxima de trabajo |
|---|---|---|
| UTP cat 5E | | |
| UTP cat 6 | | |
| UTP cat 6A | | |
| UTP cat 7 | | |
| UTP cat 7A | | |

# 4 UNIDAD 3 DIRECCIONAMIENTO IP Y DISEÑO DE REDES

Esta unidad revisa los elementos de red como Hubs, switchs y routers, la capa 3 del modelo OSI, el direccionamiento IPV4 y el diseño de redes

## 4.1 TEMA 1 ELEMENTOS DE RED INTERNETWORKING

### 4.1.1 NIC: (CAPA 2)

A partir de la tarjeta de interfaz de red, la discusión se traslada a la capa dos, la capa de enlace de datos, del modelo OSI. En términos de aspecto, una tarjeta de interfaz de red (tarjeta NIC o NIC) es un pequeño circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard o dispositivo periférico de un computador. También se denomina adaptador de red. En los computadores portátiles (laptop/notebook), las NIC generalmente tienen el tamaño de una tarjeta PCMCIA. Su función es adaptar el dispositivo host al medio de red.

Las NIC se consideran dispositivos de la Capa 2 debido a que cada NIC individual en cualquier lugar del mundo lleva un nombre codificado único, denominado dirección de Control de acceso al medio (MAC). Esta dirección se utiliza para controlar la comunicación de datos para el host de la red.

En algunos casos, el tipo de conector de la NIC no concuerda con el tipo de medios con los que usted debe conectarse. Un buen ejemplo de ello es el router Cisco 2500. En el router hay conectores AUI (Interfaz de unidad de conexión) y usted debe conectar el router a un cable Ethernet UTP Cat5. Para hacer esto, se usa un transceptor (transmisor/receptor). El transceptor convierte un tipo de señal o conector en otro (por ej., para conectar una interfaz AUI de 15 pins a un jack RJ-45, o para convertir señales eléctricas en señales ópticas). Se considera un dispositivo de Capa 1, dado que sólo analiza los bits y ninguna otra información acerca de la dirección o de protocolos de niveles más altos.

Las NIC no tienen ningún símbolo estandarizado. Se da a entender que siempre que haya dispositivos de red conectados a un medio de red, existe alguna clase de NIC o un dispositivo similar, aunque por lo general no aparezcan. Siempre que haya un punto en una topología, significa que hay una NIC o una interfaz (puerto), que actúa al menos como parte de una NIC.

## 4.1.2 HUBS (CONCENTRADORES) :(CAPA 1)

Símbolo:

El propósito de un **hub** es **regenerar y retemporizar las señales de red**. Esto se realiza a nivel de los bits para un gran número de hosts (por ej., 4, 8 o incluso 24) utilizando un proceso denominado concentración.

También se denomina **repetidor multipuerto**.

La diferencia es **la cantidad de cables** que se conectan al dispositivo.

Las razones por las que se usan los hubs son crear **un punto de conexión central** para los medios de cableado y **aumentar la confiabilidad** de la red.

La confiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red. Esta es la diferencia con la topología de bus, en la que, si un cable falla, esto causa una interrupción en toda la red. Los hubs se consideran dispositivos de la Capa 1 dado que sólo regeneran la señal y la envían por medio de un broadcast de ella a todos los puertos (conexiones de red).

En redes, hay distintas clasificaciones de los hubs. La primera clasificación corresponde a **los hubs activos o pasivos.** La mayoría de los hubs modernos **son activos**; toman energía desde un suministro de alimentación para **regenerar las señales** de red. Algunos hubs se denominan **dispositivos pasivos** dado que simplemente **dividen la señal entre múltiples usuarios**, lo que es similar a utilizar un cable "Y" en un reproductor de CD para usar más de un conjunto de auriculares. Los **hubs pasivos no regeneran los bits**, de modo que **no extienden** la longitud del cable, sino que simplemente permiten que **uno o más hosts se conecten** al **mismo segmento** de **cable**.

Otra clasificación de los hubs corresponde a **hubs inteligentes** y **hubs no inteligentes**.

- **Los hubs inteligentes** tienen puertos de consola, lo que significa que se pueden programar para administrar el tráfico de red.

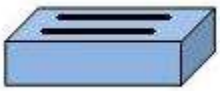
- **Los hubs no inteligentes** simplemente toman una señal de red entrante y la repiten hacia cada uno de los puertos sin la capacidad de realizar ninguna administración.

La función del hub en una red token ring se ejecuta a través de la Unidad de conexión al medio (MAU). Físicamente, es similar a un hub, pero la tecnología token ring es muy distinta. En las FDDI, la MAU se denomina concentrador. Las MAU también son dispositivos de la Capa 1.

**Los repetidores multipuerto** combinan **las propiedades** de **amplificación** y de **retemporización** de los repetidores con la conectividad. Es normal que existan 4, 8, 12 y hasta 24 puertos en los repetidores multipuerto. Esto permite que **varios dispositivos** se **interconecten** de forma **económica** y **sencilla.** Los **repetidores multipuerto** a menudo se llaman **hubs**, en lugar de repetidores, cuando se hace referencia a los dispositivos que sirven como centro de **una red de topología en estrella**. Los hubs son dispositivos de interred muy comunes. Dado que el hub típico "no administrado" simplemente requiere alimentación y jacks RJ-45 conectados, son excelentes para configurar una red con rapidez. Al igual que los repetidores en los que se basan, sólo manejan bits y son dispositivos de la Capa 1.

## 4.1.3 SWITCHES:(CAPA 2)

Simbolo:



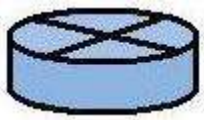
Un switch, al igual que un puente, es **un dispositivo de la capa 2.** De hecho, el switch se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto. La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, hacen que la LAN sea mucho más eficiente. Los switches hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos.

A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión, dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red). La diferencia entre un hub y un switch está dada por lo que sucede dentro del dispositivo.

El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, pensemos en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total (la velocidad de transmisión de datos en el backbone de la red).

## 4.1.4 ROUTERS (ENRUTADORES) :(CAPA 3)

Símbolo:



Un router es un dispositivo que encamina o enruta el tráfico desde una red conectada a uno de sus puertos físicos, hacia otra red conectada en otro de sus puertos. El router es un dispositivo que trabaja a nivel de red.

Para ello necesita:

- **Saber la dirección de destino**: ¿a dónde va la información que necesita ser enrutada?
- **Identificar las fuentes de la información a ser encaminada**: ¿Cuál es origen de la información?
- **Descubrir las rutas**: ¿Cuáles son las posibles rutas iniciales, o caminos, a los destinos de interés?
- **Seleccionar rutas**: ¿Cuál es el mejor camino para el destino que se requiere?
- **Mantener y verificar la información de routing**: ¿Está la información sobre el camino hacia el destino, actualizada?

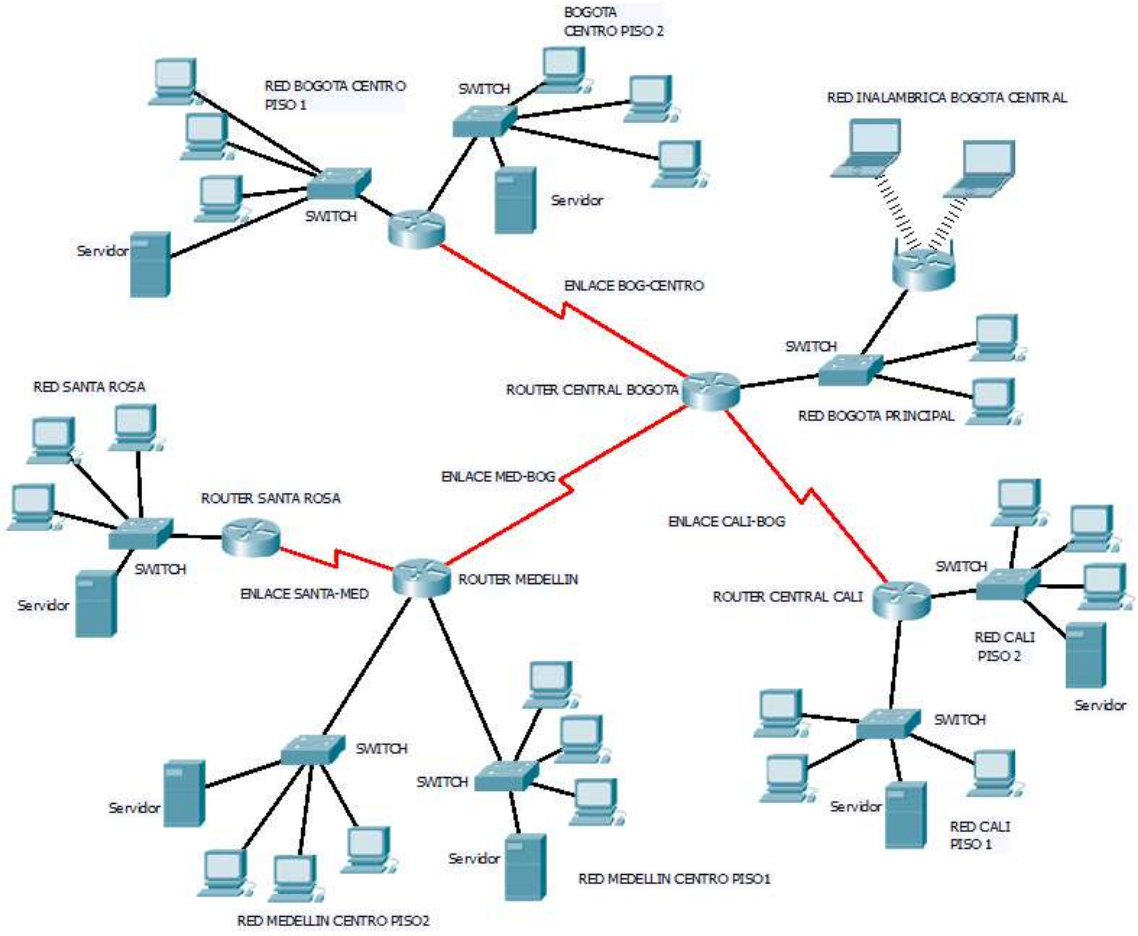
**Diferentes tipos de enrutadores fuente http://cdn.slidesharecdn.com/**

La información de routing que el router obtiene del administrador de red o de otros routers, la sitúa en su tabla de rutas. El router se remitirá a esta tabla para decidir por qué interfaz se manda la información en base a su dirección destino. Si la red destino está directamente conectada, el router ya conoce qué interfaz debe utilizar. Si la red destino no está directamente conectada, entonces el router debe aprender la mejor ruta posible que debe utilizar para enviar los paquetes. Esta información puede aprenderla de las siguientes maneras:

- Introducida manualmente por el administrador de red (routing estático)

- Recogida a través de procesos de routing dinámico activados en los routers.

Esta última utiliza protocolos de enrutamiento como RIP, IGRP, BGP, EIGRP, OSPF




**Esquema de una red ubicación de dispositivos fuente el autor**

## 4.1.5 COLISIONES Y DOMINIO DE COLISIONES

Uno de los problemas que se puede producir, cuando dos bits se propagan al mismo tiempo en la misma red, es una colisión. En una red pequeña y de baja velocidad es posible implementar un sistema que permita que sólo dos computadores envíen mensajes, cada uno por turnos. Esto significa que ambas pueden mandar mensajes, pero sólo podría haber un bit en el sistema. El problema es que en las grandes redes hay muchos computadores conectados, cada uno de los cuales desea comunicar miles de millones de bits por segundo. También es importante recordar que los "bits" en realidad son paquetes que contienen muchos bits.

Se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes como, por ejemplo, los repetidores, puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo. Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos.

http://es.slideshare.net/Betty77ma/colisiones-dominios-de-colisin-y-segmentacin

El área dentro de la red donde los paquetes se originan y colisionan, se denomina dominio de colisión, e incluye todos los entornos de medios compartidos. Por ejemplo, un alambre puede estar conectado con otro a través de cables de conexión, transceptores, paneles de conexión, repetidores e incluso hubs. Todas estas interconexiones de la Capa 1 forman parte del dominio de colisión.

Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención). Por ejemplo, un sistema digital sólo puede reconocer dos estados de voltaje, luz u ondas electromagnéticas. Por lo tanto, en una colisión, las señales interfieren, o colisionan, entre sí. Al igual que lo que ocurre con dos automóviles, que no pueden ocupar el mismo espacio, o la misma carretera, al mismo tiempo, tampoco es posible que dos señales ocupen el mismo medio simultáneamente.

### 4.1.6 REPETIDORES Y DOMINIO DE COLISIÓN

Los repetidores regeneran y retemporizar los bits, pero no pueden filtrar el flujo de tráfico que pasa por ellos. Los datos (bits) que llegan a uno de los puertos del repetidor se envían a todos los demás puertos. El uso de repetidor extiende el dominio de colisión, por lo tanto, la red a ambos lados del repetidor es un dominio de colisión de mayor tamaño.

### 4.1.7 HUBS Y DOMINIO DE COLISIÓN

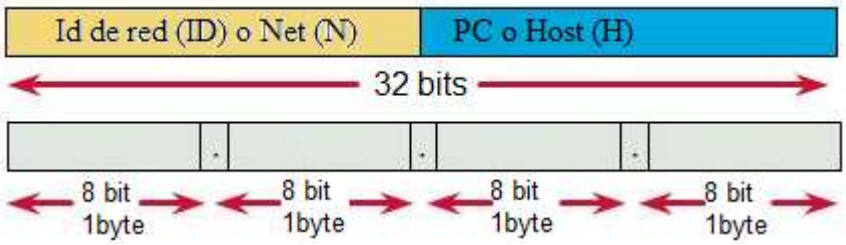
Ya hemos aprendido que el otro nombre del hub es repetidor multipuerto. Cualquier señal que entre a un puerto del hub se regenera, retemporiza y se envía desde todos los demás puertos. Por lo tanto, los hubs, que son útiles para conectar grandes cantidades de computadores, extienden los dominios de colisión. El resultado final es el deterioro del desempeño de la red si todos los computadores en esa red exigen anchos de banda elevados, simultáneamente.

Tanto los repetidores como los hubs son dispositivos de la Capa 1 y, por lo tanto, no ejecutan ninguna filtración del tráfico de red, si se amplía un tendido de cables mediante un repetidor y se termina ese tendido mediante un hub, esto simplemente da como resultado un dominio de colisión de mayor tamaño.

## 4.2 TEMA 2 DIRECCIONAMIENTO IPV4

Una dirección IP (internet protocol) es un número único para cada computador dentro de una red que puede indicar dónde está un PC o al menos en que red se encuentra. Un ejemplo serio 219.113.4.2. Es tarea de los protocolos de mayor nivel (protocolos en otras capas como el DNS) hacer corresponder direcciones de internet con nombres como WWW.GOOGLE.COM o WWW.RCGALUME.UHOSTFULL.COM a su dirección IP.

Las direcciones ip están compuestas por 32 bit, los 32 bits se dividen en una parte para red (N Net) y otra para PC (H o Host)




**Componentes de una dirección IP fuente (Cisco)**

Es decir que una dirección ip es una sucesión de 32 ceros o unos como:

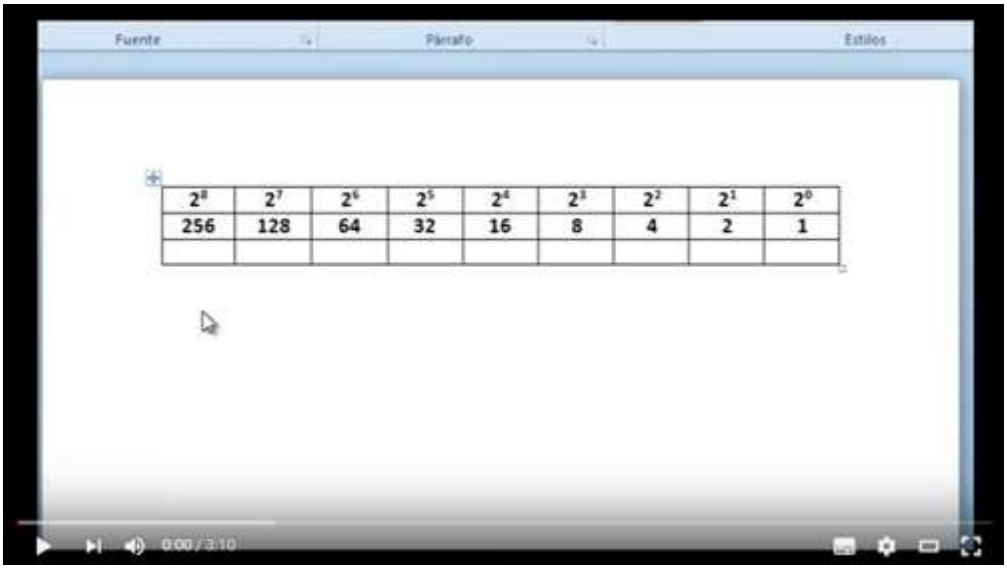
10101100000100000111101011001100

La dirección ip se divide en 4 partes de 8 bits, 32/4 = 8, cada una de esas partes se llaman octeto, cada octeto se separa por un punto.

10101100.00010000.01111010.11001100

Si cada octeto binario se convierte a decimal queda 172.16.122.204 que es un ejemplo de dirección IP.

Para ampliar comprender como convertir una dirección ip en binarios a decimal mira este video.




**Convertir de Decimal a Binario sin dividir** *Enlace*

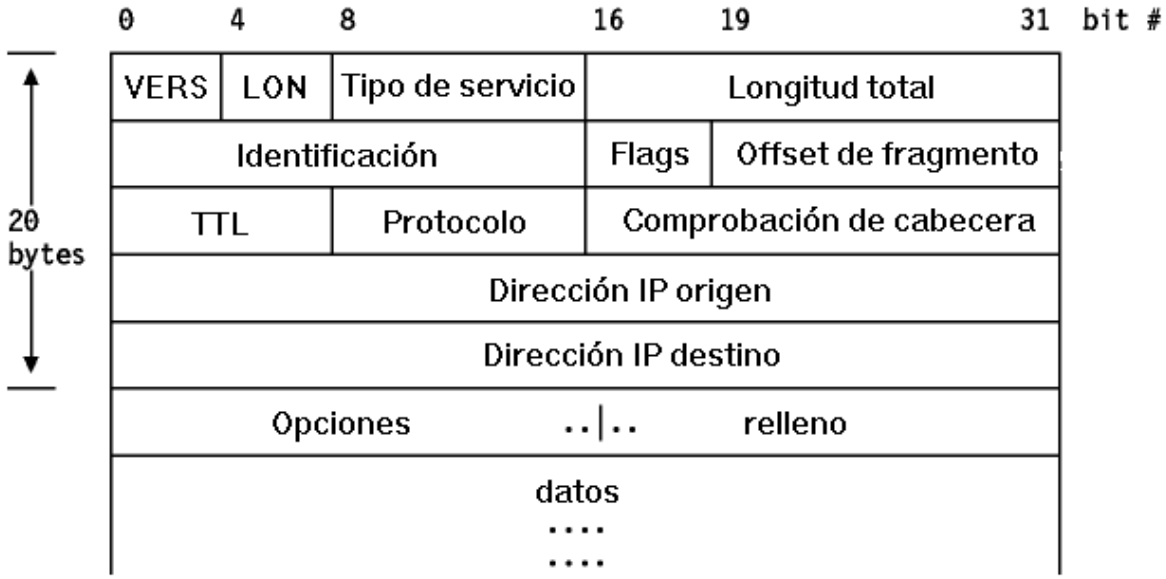
La dirección IP contiene la información necesaria para **enrutar** (enviar un paquete a través de la red o a través de internet ) a otro pc, par esto requiere información como IP origen IP destino la información a transportar y un mecanismo de detección de errores **( HTTP://WWW.MONOGRAFIAS.COM )**

| IP ORIGEN | IP DESTINO | INFORMACION | DETECION DE ERRORES |
|---|---|---|---|

*Ejemplo de campos mínimos de una dirección IP fuente el autor*

Cada dirección origen y destino contiene realmente una dirección de 32 bits. El campo de dirección origen contiene la dirección IP del dispositivo que envía el paquete. El campo destino contiene la dirección IP del dispositivo que recibe el paquete. La información son los datos que vienen de la capa 2.

El protocolo IP realmente es más complejo ver y tiene más campos, la distribución de campos del protocolo IP es la siguiente (fuente **www.cicei.com ).**




*Ejemplo de Cabecera de un Datagrama Internet tomado **www.cicei.com***

Hay 3 clases de direcciones IP: si se convierte en binario En la Clase A, el bit más significativo es 0,los 7 bits siguientes son la red, y los 24 bits restantes son la dirección local; en la Clase B, los dos bits más significativos son uno-cero ("10"), los 14 bits siguientes son la red y los últimos 16 bits son la dirección local; en la Clase C, los tres bits más significativos son uno-uno-cero ("110"), los 21 bits siguientes son la red y los 8 restantes son la dirección local. La clases de red D y E se usan para propósitos especiales, por ejemplo las redes clase D se usa para aplicaciones Multicast, y las redes clase E para Investigación (Adaptado de ).

***http://www.cicei.com/ocon/gsi/tut_tcpip/3376c22.html***

Direccionamiento IP usadas para computadores en redes internas o internet

| CLASES | FORMATO | NÚMERO DE PC | RANGO DE DIRECCIONES IP |
|---|---|---|---|
| A | N.H.H.H | 16,777,215 | 1.0.0.0 a la 127.0.0.0 |
| B | N.N.H.H | 65,535 | 128.0.0.0 a la 191.255.0.0 |
| C | N.N.N.H | 255 | 192.0.0.0 a la 223.255.255.0 |

*Fuente el autor*

Las redes además de ser clase A b o C pueden ser públicas o privadas una dirección privada se usa al interior de una casa o una empresa y una dirección pública se encuentra en internet como es el caso de google.

Para cada red A, B o C hay un rango de direcciones y dentro de este rango hay un sub rango que es privado

*Tabla 5 rangos públicos y privados*

| CLASE | RANGO | REDES PRIVADAS | REDES PÚBLICAS |
|---|---|---|---|
| A | 0.0.0.0 – 127.0.0.0 | 10.0.0.0 | 0.0.0.0 – 127.0.0.0 excluyendo la 10.0.0.0 que es privada |
| B | 128.0.0.0 - 191.255.0.0 | 172.16.0.0-172.31.0.0 | 128.0.0.0-191.255.0.0 excluyendo el rango 172.16.0.0-172.31.0.0 que son privadas |
| C | 192.0.0.0 - 223.255.255.0 | 192.168.0.0-192.168.255.0 | 192.0.0.0 - 223.255.255.0 excluyendo el rango 192.168.0.0-192.168.255.0 que son privadas |


**Dirección IP públicas y privadas (ISP)** *Enlace*

La N en el formato especifica cuantos octetos son reservados para net (es decir la red), y el H especifica cuantos Octetos son reservados para Hosts (es decir los PC), en la clase B se asignan igual cantidad de redes que de computadores dentro de las redes. En una clase C se cuenta con muy pocos bits para PC. Una IP es clase A, B o C según el rango donde se encuentre.

la red 127 de la Clase A pruebas de diagnóstico conocidas como loopback (ida y regreso), el cual permite a las computadoras enviarse a ellas mismas un paquete sin afectar el ancho de banda de la red. También existen una clase D y una clase E. La clase D es usada para multicast de grupos de datos de una determinada aplicación o servicio de un servidor. La clase E está reservada para usos experimentales.


*TCP IP CISCO CCNA1* *Enlace*

### 4.2.1 ID DE RED

Es el nombre que se da a la red y no se pude dar a un computador la id de red se reconoce por tener 0 en la parte de host, el número de 0s varía según la clase.

### 4.2.2 EJERCICIO DE APRENDIZAJE

| CLASE | Forma del ID de red | ejemplo | Numero de ceros en binario en la parte de HOST |
|---|---|---|---|
| A | X.0.0.0 | 10.0.0.0<br>3.0.0.0<br>22.0.0.0 | 8+8+8=24<br>tres últimos en cero |
| B | X.X.0.0 | 130.1.0.0<br>172.16.0.0<br>190.0.0.0<br>(el 190.0 es la red) | 8+8=16<br>Dos últimos en cero |
| C | X.X.X.0 | 193.1.1.0<br>201.16.20.0<br>192.168.0.0<br>(el 192.168.0 es la red) | 8=8<br>Solo ultimo en 0 |

### 4.2.3 BROADCAST

Es la dirección IP que se da para que un computador pueda mandar un mensaje a todos los computadores de la red y no se pude dar a un computador la id de red se reconoce por tener 1s en la parte de host, el número de 1s varía según la clase.

### 4.2.4 EJERCICIO DE APRENDIZAJE

| CLASE | Forma del ID de red | Ejemplo<br>ID DE RED / BROADCAST | Numero de ceros en binario en la parte de HOST |
|---|---|---|---|
| A | X.255.255.255 | 10.0.0.0 / 10.255.255.255<br>3.0.0.0 / 3.255.255.255<br>22.0.0.0 / 22.255.255.255 | 8+8+8=24<br>tres últimos en uno |
| B | X.X. 255. 255 | 130.1.0.0 / 130.1.255.255<br>172.16.0.0 / 172.16.255.255<br>190.0.0.0 / 190.0.255.255<br>(el 190.0 es la red) | 8+8=16<br>Dos últimos en uno |
| C | X.X.X. 255 | 193.1.1.0 / 193.1.1.255<br>201.16.20.0 / 201.16.20.255<br>192.168.0.0 / 192.168.0.255<br>(el 192.168.0 es la red) | 8=8<br>Solo último en uno |

## 4.3 TEMA 3 MÁSCARA RED

Es el indicador que divide formalmente la parte de red de la parte de host colocando 1s a la parte de red y 0s a la parte de host varía según la clase.

### 4.3.1 EJERCICIO DE APRENDIZAJE

| CLASE | Forma del ID de red | Ejemplo<br>ID DE RED / Mascara | Numero de ceros en binario en la parte de HOST |
|---|---|---|---|
| A | X.0.0.0 | 10.0.0.0 / 255.255.255.0<br>3.0.0.0 / 255.255.255.0<br>22.0.0.0 / 255.255.255.0 | 8+8+8=24<br>tres últimos en uno |
| B | X.X.0.0 | 130.1.0.0 / 255.255.0.0<br>172.16.0.0 / 255.255.0.0<br>190.0.0.0 / 255.255.0.0<br>(el 190.0 es la red) | 8+8=16<br>Dos últimos en uno |

| | | | |
|---|---|---|---|
| **C** | **X.X.X.0** | **193.1.1.0 / 255.255.255.0**<br>**201.16.20.0 / 255.255.255.0**<br>**192.168.0.0 / 255.255.255.0**<br>**(el 192.168.0.0 es la red)** | **8=8**<br>**Solo último en uno** |

## 4.3.2 DIRECCIÓN IP DE UN PC

Es la dirección IP que se da para que un computador que no es ni el Id de red (parte de host en 0s) ni el broadcast (parte de host en 1s)

## 4.3.3 EJERCICIO DE APRENDIZAJE

| CLASE | ID de red | Rango IP Según red<br>Desde / hasta |
|---|---|---|
| **A** | **10.0.0.0**<br>**3.0.0.0**<br>**22.0.0.0** | **10.0.0.1 / 10.255.255.254**<br>**3.0.0.1 / 3.255.255.254**<br>**22.0.0.1 / 22. 255.255.254** |
| **B** | **130.1.0.0 172.16.0.0 190.0.0.0** | **130.1.0.1 / 130.1.255.255**<br>**172.16.0.1 / 172.16.255.254**<br>**190.0.0.1 / 190.0.255.254**<br>**(el 190.0 es la red)** |
| **C** | **193.1.1.**<br>**201.16.20 192.168.0.0** | **193.1.1.1 / 193.1.1.254**<br>**201.16.20.1 / 255.255.255.0**<br>**192.168.0.0 / 255.255.255.0**<br>**(el 192.168.0 es la red)** |

Puedes complementar sobre direccionamiento IPV4

https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

# 4.4 TEMA 4 DISEÑO DE REDES

## 4.4.1 METODOLOGÍA PLANTEADA

Área de aplicación: Esta metodología puede ser aplicada en asignaturas o cursos donde se tenga como objeto de estudio las redes de datos y como competencia especifica el diseño redes de datos, abordado desde capa 3 del modelo OSI, la metodología se limita a indicar la estudiante como plasmar un diseño, partiendo de un esquema conceptual de la red o de un enunciado, sin hacer especificaciones de los aspectos de funcionamiento de los dispositivos de internetworking, como nubes enlaces y enrutadores, ni cuestiones teóricas

Aplicación del método: En las asignaturas redes de datos además de comprender el funcionamiento de los elementos de internetworking una de las competencias que se esperan de un estudiante, es el diseño esquemático del diseño del diseño de red donde pueda aplicar los conocimientos de capa 3, como la asignación del direccionamiento IP según la cantidad de PC conectados, la configuración de router y las tablas de enrutamiento.

El método permite que el estudiante realice una abstracción del diseño, el cual será fácilmente evaluable sin requerir emuladores o el uso de comandos, lo que implica que el estudiante se enfoque en el diseño y no en su implementación, evitando consideraciones de marcas y equipos empleados.

**Pasos del método**

Se propone dividir el proceso de diseño en 4 pasos independientes y secuenciales del diseño de una red WAN, como se verá en la figura puesta a continuación:

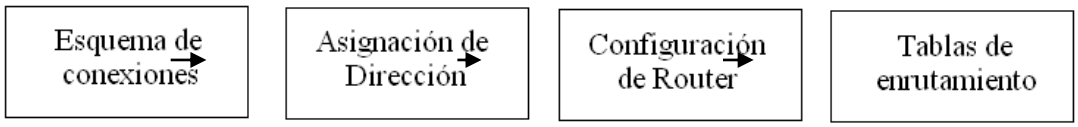



*Diagrama de los pasos propuestos por el método*

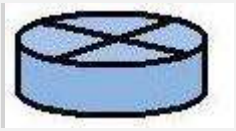
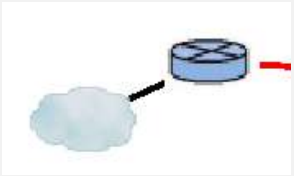
## 4.4.2 DESCRIPCIÓN DE LA METODOLOGÍA.

Se describen cada uno de los pasos que propone la metodología, definiendo los elementos requeridos.

**Pasos propuestos**

**Paso 1. Esquema de conexiones**, así como los mapas mentales son diagramas que permiten representar palabras, ideas, tareas, u otros conceptos de una idea, para representar las redes de datos se requiere un esquema de conexiones, en este esquema se debe mostrar claramente las interconexiones que existen entre las redes y los enrutadores, se debe diseñar la red acorde a un enunciado eligiendo cada elemento, básicamente interfaces, routers, redes finales y redes de enlace.

*Elementos empleados en el diseño*

| | | |
|---|---|---|
| **Enrutadores** | Se refiere a los dispositivos de capa 3 que permiten el encaminamiento de los paquetes , debe emplearse solo 1 por localidad (ciudad) |  |
| **Interfaces** | Son las tarjetas asociadas al router que permiten la conexión física de los elementos de internet working, FastEthernet ,Seriales , debe usar una por cada red diferente en la misma localidad | F0/0, F0/1 etc.<br>S0/0/0 , S0/0, S0/1 etc |
| **Redes de enlace** | Son las redes que permiten las conexiones entre ciudades distantes, tienen forma de rayo e indican ciudades diferentes, o enlaces proveídos por terceros. |  |
| **Redes Finales** | Son la redes de usuarios finales donde están los PC, se conectan generalmente a los routers |  |

*Fuente el autor*

**Paso 2**: **<u>Asignación de direccionamiento IP</u>**: permite asignar la clase de red según la cantidad de PC que tengan las redes A, B, o C, haciendo uso se la siguiente regla: debe usar la red sugerida, de lo contrario debe usar la red que contenga en forma más estricta la cantidad de pc requeridos iniciando desde la clase C, debe emplear **¡Error! No se encuentra el origen de la referencia.**

*Clase rango y numero de redes*

| Clase | Rango | Redes privadas | N° de Redes | N° de Host Por Red | Máscara de Red estándar |
|---|---|---|---|---|---|
| A | 0.0.0.0 – 127.0.0.0 | 10.0.0.0 | 128 | 16.777.214 | 255.0.0.0 |
| B | 128.0.0.0 - 191.255.0.0 | 172.16.0.0-172.31.0.0 | 16.384 | 65.534 | 255.255.0.0 |
| C | 192.0.0.0 - 223.255.255.0 | 192.168.0.0-<br>192.168.255.0 | 2.097.152 | 254 | 255.255.255.0 |

Para la escogencia de la clase de una red, por ejemplo, si la red tiene 300 pc se analiza que esta cantidad de pc no es soportada por una clase C (254 pc según tabla 1), se podría pensar en clase B o A pero se debe escoger B ya que es la clase que contiene de forma más estrecha los 300 PC.

Luego de escoger la red más adecuada debe decidir si es pública o privada, esto depende del enunciado, para cada red debe darse la máscara y default Gateway según

*Paramentos de la asignación IP*

| | |
|---|---|
| Nombre de la Red | |
| ID-Red | |
| Máscara | |
| Default Gateway | |

Se recomienda usar como Default Gateway el usar el último pc disponible de la red, esto cobra mayor valor pedagógico cuando se usan subredes pues verifica la pericia del estudiante para realizar el cálculo de cuál sería la última disponible de la red IP de la red.

Si se tuviera una red en Medellín pública con 10 pc, es decir clase C se llenaría asi

| | |
|---|---|
| Nombre de la Red | MEDELLÍN |
| ID-Red | 200.0.0.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 200.0.0.254 |

Para las redes de enlace que comunican las ciudades entre sí, no debe especificar el Default Gateway, ya que este encaminamiento es labor del enrutador

**Paso 3: Configuración de router:** En este paso el alumno especifica la dirección IP de cada una de las interfaces del Router, al margen de la marca sistema operativo o referencia del router a configurar, se deben especificar las IP tanto seriales como Ethernet, este paso está en concordancia directa con las direcciones ip asignadas a las redes en el paso anterior, se propone que se use una tabla similar a tabla 3.

| Nombre del Router | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 192.168.1.254 | /24 |
| S0/0/0 | 172.16.0.0 | /16 |

| | | |
|---|---|---|
| S/0/0/1 | 200.0.0.1 | /24 |

Se recomienda en las redes de enlace usar la primera y la última dirección ip de la red elegida en el paso anterior, esto también verifica la pericia del estudiante para realizar el cálculo de cuál sería la última y la primera IP disponible de la red.

**Paso 4**. Tablas de enrutamiento: Dado que se pueden usar múltiples protocolos de enrutamiento como Rip u OSPF, este paso busca evaluar la pericia del estudiante para indicar el estado de las tablas de enrutamiento si se usara un protocolo como RIP, o si estas rutas se dieran en forma estática al router, se propone el uso de la siguiente tabla.

*Tabla configuración de routers*

| Nombre del Router | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| | | | | |
| | | | | |
| | | | | |

*Fuente el autor*

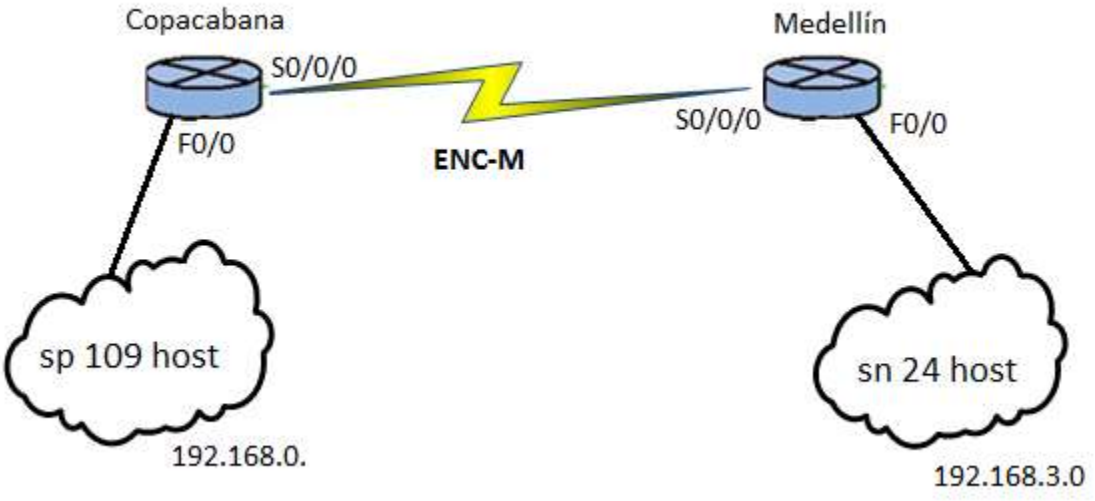
## 4.4.3 EJERCICIOS DE APRENDIZAJE

La empresa de ABC está ubicada en el municipio de Copacabana, por sus buenos ingresos ha decidido crear otra sede en la ciudad de Medellín. La sede de Copacabana cuenta con 109 host (PC), mientras que la sede de Medellín solo cuenta con 24 host. Diseñe una red para dar comunicación a estas dos sedes.

¿Qué pasos deben seguirse y cómo se configura?

El primer paso es diseñar la red del enunciado eligiendo cada elemento que contendrá. En cada uno de ellos debemos configurar varias cosas: nombres, routers, tipo de interfaces (Serial, Ethernet), configuración IP, entre otros; así que, en este ejemplo la red completa constara de 3 redes, en la cual interactuarán 2 routers, llamados Copacabana y Medellín, ambos conectados entre sí por sus interfaces Seriales (S0/0/0) respectivamente, esta conexión serial se llamara ENC-M (1ª red). En el router Copacabana se encuentra la sede principal de ABC (2ª red: sp), mientras que en el router Medellín se encuentra su nueva sede (3ª red: sn), ambas utilizando una interfaz Fast Ethernet (F0/0) con la cual se podrán conectar a los routers. Las tres redes son clase C ya que ésta soporta hasta 254 host.

**PASO 1:**




Una vez, diseñado, procedemos a realizar el direccionamiento IP el cual consiste en darle a cada red una dirección IP, máscara de subred y un default gateway.

Una dirección IP (ID) Consta de una parte que identifica de forma única la red y otra que identifica de forma única el computador dentro de la red facilitando la interconexión de diversas redes sin que se produzca conflictos entre ellas. La dirección IP en este caso es clase C privada.

La máscara de subred (MK) Es una combinación de bits que sirve para indicar a los dispositivos qué parte de la dirección IP es el número de la red, y qué parte es la correspondiente al host.

Default Gateway (DG) es una puerta de enlace por defecto al cual se envía todo paquete que no tiene un destino en la tabla de enrutamiento, enviando el paquete por una ruta por defecto. Siempre se le asigna la antepenúltima dirección IP, ya que la última es destinada para el broadcast.

**PASO 2**

DIRECCIONAMIENTO IP

| | |
|---|---|
| Nombre de la Red | SP |
| ID-Red | 192.168.1.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.168.1.254 |

| | |
|---|---|
| Nombre de la Red | ENC-M |
| ID-Red | 192.168.2.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | No por ser una red de enlace |

| | |
|---|---|
| Nombre de la Red | SN |
| ID-Red | 192.168.3.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.168.3.254 |

El Router es utilizado enviar paquetes entre redes y adaptar los paquetes de información, cuando los puntos de origen y destino pertenecen a distintas redes, por eso el siguiente paso es la configuración de routers desde sus interfaces de salida (S0/0/0 y F0/0) respectivamente, utilizando el Default Gateway y el número de octetos de la máscara de red.

| ROUTER COPACABANA | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 192.168.1.254 | /24 |
| S0/0/0 | 192.168.2.1(primer PC) | /24 |

| ROUTER MEDELLÍN | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 192.168.3.254 | /24 |
| S0/0/0 | 192.168.2.254 (último Pc) | /24 |

A la hora de configurar los routers se observa que las interfaces seriales no tienen Gateway, en este caso, se utiliza la dirección IP de la red a la que hacen enlace por su interfaz de salida, pero para ser diferenciada se le asigna un host.

Lo último que se hace es la tabla de enrutamiento constituida por una serie rutas que contienen información acerca de dónde están situados los identificadores de red, acompañado del número de octetos de la máscara de red, y a cuantos saltos o si está conectada directamente al router.

| ROUTER COPACABANA | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 192.168.1.0 | /24 | Conectado | 0 (conectada) |
| S0/0/0 | 192.168.3.0 | /24 | 192.168.2.2 | 1 salto |
| S0/0/0 | 192.168.2.0 | /24 | Conectado | 0 (conectada) |

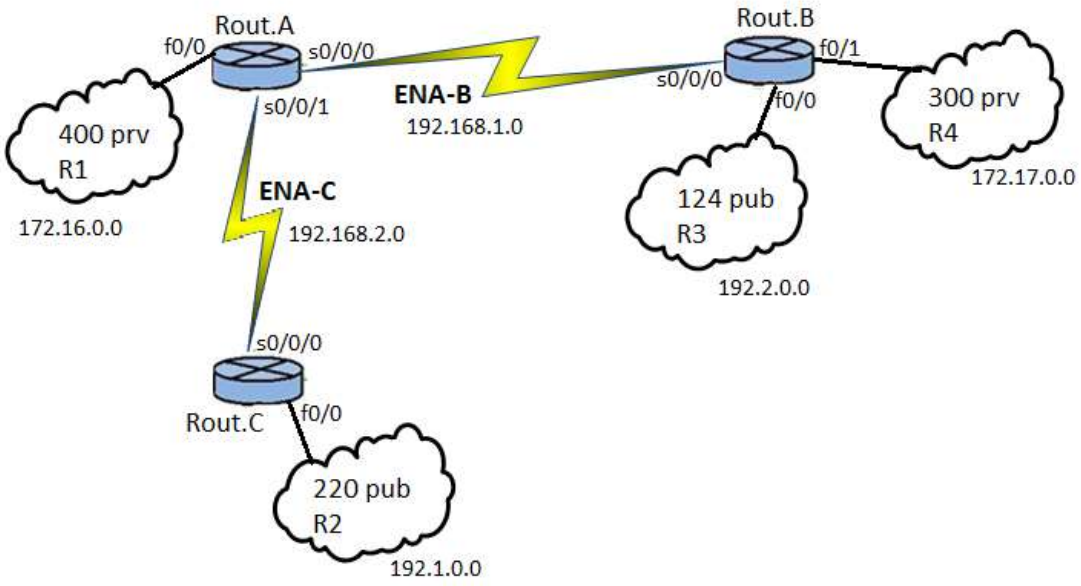
| ROUTER MEDELLÍN | | | | |
|---|---|---|---|---|
| Interface | Red Destino | Máscara | Próximo salto | Número de saltos |
| F0/0 | 192.168.3.0 | /24 | Conectado | 0 (conectada) |
| S0/0/0 | 192.168.1.0 | /24 | 192.168.2.1 | 1 salto |
| S0/0/0 | 192.168.2.0 | /24 | Conectado | 0 0 (conectada) |

Nota: C= Conectada directamente al router al que se hace referencia.

1= Número de saltos para conectarse a esa red.

Una empresa X tiene varias redes distribuidas en diferentes regiones como se muestra en la figura, determinar para cada una de ellas el direccionamiento IP, configuración de routers y tabla de enrutamiento.

**PASO 1**




Nótese que en la gráfica anterior tenemos:

- Cuatro redes privadas R1 y R4 ambas clase B, ENA-B y ENA-C clase C
- Dos redes públicas R2 y R3 clase C
- Tres enrutadores llamados Rout.A, Rout.B, y Rout.C.

Se definieron **los tipos de interfaces** (Serial, Ethernet)

Una vez analizada la información que se nos da, procedemos a realizar el direccionamiento IP de cada una de las redes.

**PASO 2**

**DIRECCIONAMIENTO IP**

| | |
|---|---|
| Nombre de la Red | R1 (clase B privada 400Pc) |
| ID-Red | 172.16.0.0 |
| Máscara | 255.255.0.0 |
| Default Gateway | 172.16.255.254 |

| | |
|---|---|
| Nombre de la Red | R2 (Clase c publica 220PC) |
| ID-Red | 192.1.0.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.1.0.254 |

| | |
|---|---|
| Nombre de la Red | R3 (C publica 124 PC) |
| ID-Red | 192.2.0.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.2.0.254 |

| | |
|---|---|
| Nombre de la Red | R4 (B privada 300 PC) |
| ID-Red | 172.17.0.0 |
| Máscara | 255.255.0.0 |
| Default Gateway | 172.17.255.254 |

| | |
|---|---|
| Nombre de la Red | ENA-B (enlace RA y RB) |
| ID-Red | 192.168.1.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | No tiene  es un enlace |

| | |
|---|---|
| Nombre de la Red | ENA-C |
| ID-Red | 192.168.2.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | |

**PASO 3**

**CONFIGURACIÓN DE ROUTERS**

| ROUT.A | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 172.16.255.254 (último pc) | /16 |
| S0/0/0 | 192.168.1.1 (primer PC) | /24 |
| S0/0/1 | 192.168.2.1 (primer PC) | /24 |

| ROUT.B | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 192.2.0.254 (ultimo PC) | /24 |
| F0/1 | 172.17.255.254 (ultimo PC) | /16 |
| S0/0/0 | 192.168.1.254 (ultimo PC) | /24 |

| ROUT.C | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 192.1.0.254 (último PC) | /24 |
| S0/0/0 | 192.168.2.254 (último PC) | /24 |

**PASO 4**

**TABLA DE ENRUTAMIENTO**

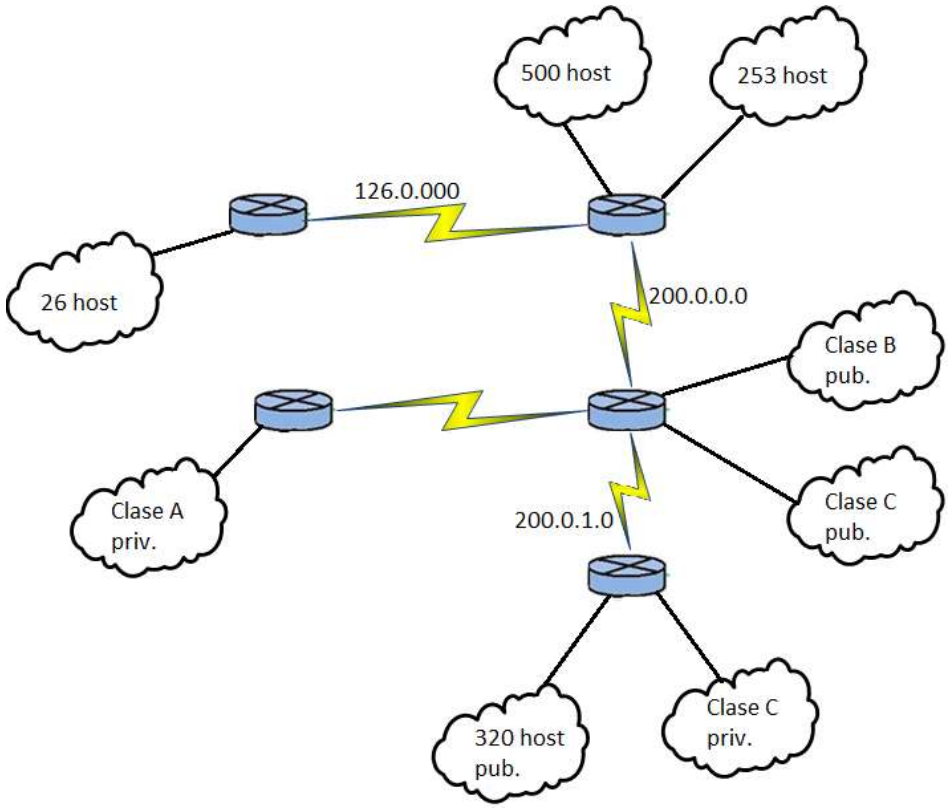
| ROUT.A | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 172.16.0.0 | 255.255.0.0 | Conectado | 0 |
| S0/0/0 | 192.168.1.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 192.2.0.0 | 255.255.255.0 | 192.168.1.255 | 1 |
| S0/0/0 | 172.17.0.0 | 255.255.0.0 | 192.168.1.255 | 1 |
| S0/0/1 | 192.168.2.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/1 | 192.1.0.0 | 255.255.255.0 | 192.168.2.255 | 1 |

| ROUT.B | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 192.2.0.0 | 255.255.255.0 | Conectado | 0 |
| F0/1 | 172.17.0.0 | 255.255.0.0 | Conectado | 0 |
| S0/0/0 | 192.168.1.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 172.16.0.0 | 255.255.0.0 | 192.168.1.1 | 1 |
| S0/0/0 | 192.168.2.0 | 255.255.255.0 | 192.168.1.1 | 1 |
| S0/0/0 | 192.1.0.0 | 255.255.255.0 | 192.168.1.1 | 2 |

| ROUT.C | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 192.1.0.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 192.168.2.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 172.16.0.0 | 255.255.0.0 | 192.168.2.1 | 1 |
| S0/0/0 | 192.168.1.0 | 255.255.255.0 | 192.168.2.1 | 1 |
| S0/0/0 | 192.2.0.0 | 255.255.255.0 | 192.168.2.1 | 2 |
| S0/0/0 | 172.17.0.0 | 255.255.0.0 | 192.168.2.1 | 2 |

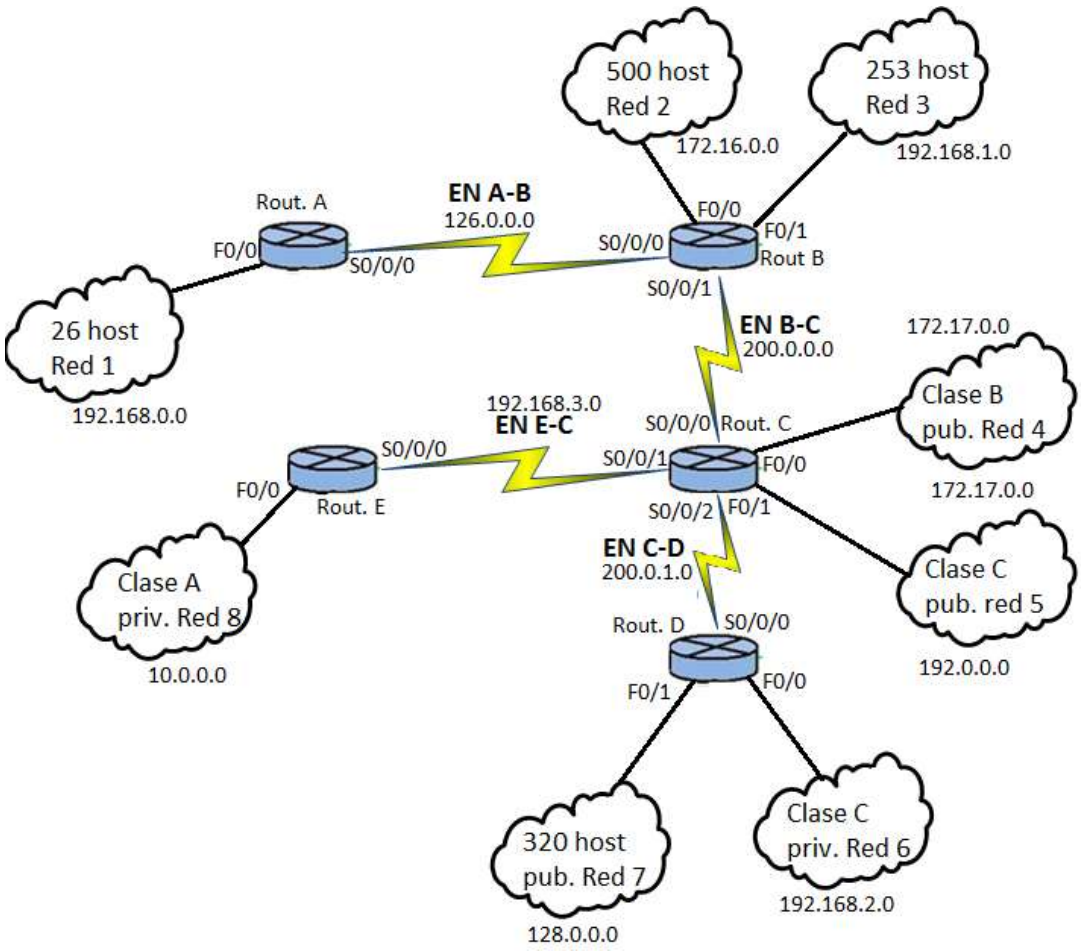
## 4.4.4 EJERCICIO DE APRENDIZAJE

En base al siguiente gráfico, realizar el diseño respectivo a toda la red global, el direccionamiento IP, configuración de routers y tabla de enrutamiento.



En primer lugar, se da nombre a cada una de las redes, a las interfaces y a los routers, cuando no se dice si una red es pública o privada se toma la red como una clase privada.

**PASO 1**




En total se tienen 12 redes conectadas entre sí mediante 5 routers interconectados por una conexión serial.

**PASO 2**

**DIRECCIONAMIENTO IP**

| | |
|---|---|
| Nombre de la Red | RED 1 |
| ID-Red | 192.168.0.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.168.0.254 |

| | |
|---|---|
| Nombre de la Red | RED 2 |
| ID-Red | 172.16.0.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 172.16.255.254 |

| | |
|---|---|
| Nombre de la Red | RED 3 |
| ID-Red | 192.168.1.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.168.1.254 |

| | |
|---|---|
| Nombre de la Red | RED 4 |
| ID-Red | 172.17.0.0 |
| Máscara | 255.255.0.0 |
| Default Gateway | 172.17.255.254 |

| | |
|---|---|
| Nombre de la Red | RED 5 |
| ID-Red | 192.0.0.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.0.0.254 |

| | |
|---|---|
| Nombre de la Red | RED 6 |
| ID-Red | 192.168.2.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | 192.168.2.254 |

| | |
|---|---|
| Nombre de la Red | RED 7 |
| ID-Red | 128.0.0.0 |
| Máscara | 255.255.0.0 |
| Default Gateway | 128.0.255.254 |

| | |
|---|---|
| Nombre de la Red | RED 8 |
| ID-Red | 10.0.0.0 |
| Máscara | 255.0.0.0 |
| Default Gateway | 10.255.255.254 |

| | |
|---|---|
| Nombre de la Red | ENC-D |
| ID-Red | 200.0.1.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | |

| | |
|---|---|
| Nombre de la Red | ENA-B |
| ID-Red | 126.0.0.0 |
| Máscara | 255.255.0.0 |
| Default Gateway | |

| | |
|---|---|
| Nombre de la Red | ENC-E |
| ID-Red | 192.168.3.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | |

| | |
|---|---|
| Nombre de la Red | ANB-C |
| ID-Red | 200.0.0.0 |
| Máscara | 255.255.255.0 |
| Default Gateway | |

**PASO 3**

**CONFIGURACIÓN DE ROUTER**

| ROUTER A | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 192.168.0.254 | /24 |
| S0/0/0 | 126.0.0.1 | /24 |

| ROUTER B | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 172.16.255.254 | /16 |
| F0/1 | 192.168.1.254 | /24 |
| S0/0/0 | 126.255.255.254 | /8 |
| S0/0/1 | 200.0.0.1 | /24 |

| ROUTER C | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 172.17.255.254 | /16 |
| F0/1 | 192.0.0.254 | /24 |
| S0/0/0 | 200.0.0.1 | /24 |
| S0/0/1 | 192.168.3.1 | /24 |
| S0/0/2 | 200.0.1.1 | /24 |

| ROUTER D | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 192.168.2.254 | /24 |
| F0/1 | 128.0.255.254 | /16 |
| S0/0/0 | 200.0.1.254 | /24 |

| ROUTER E | | |
|---|---|---|
| **Interface** | **Dirección IP** | **Máscara en formato /x** |
| F0/0 | 10.255.255.254 | /8 |
| S0/0/0 | 192.168.3.254 | /24 |

**PASO 4**

**TABLA DE ENRUTAMIENTO**

| ROUTER A | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 192.168.0.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 126.0.0.0 | 255.0.0.0 | Conectado | 0 |
| S0/0/0 | 172.16.0.0 | 255.255.0.0 | 126.0.0.254 | 1 |
| S0/0/0 | 192.168.1.0 | 255.255.255.0 | 126.255.255.224 | 1 |
| S0/0/0 | 200.0.0.0 | 255.255.255.0 | 126.255.255.224 | 1 |
| S0/0/0 | 172.17.0.0 | 255.255.0.0 | 126.255.255.224 | 2 |
| S0/0/0 | 192.0.0.0 | 255.255.255.0 | 126.255.255.224 | 2 |
| S0/0/0 | 200.0.1.0 | 255.255.255.0 | 126.255.255.224 | 2 |
| S0/0/0 | 192.168.2.0 | 255.255.255.0 | 126.255.255.224 | 3 |
| S0/0/0 | 128.0.0.0 | 255.255.0.0 | 126.255.255.224 | 3 |
| S0/0/0 | 192.168.3.0 | 255.255.255.0 | 126.255.255.224 | 2 |
| S0/0/0 | 10.0.0.0 | 126.255.255.224 | 126.255.255.224 | 3 |

| ROUTER B | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 172.16.0.0 | 255.255.0.0 | Conectado | 0 |
| F0/1 | 192.168.1.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 126.0.0.0 | 255.255.0.0 | Conectado | 0 |
| S0/0/0 | 192.168.0.0 | 255.255.255.0 | 126.0.0.1 | 1 |
| S0/0/1 | 200.0.0.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/1 | 172.17.0.0 | 255.255.255.0 | 200.0.0.254 | 1 |
| S0/0/1 | 192.0.0.0 | 255.255.255.0 | 200.0.0.254 | 1 |
| S0/0/1 | 200.0.1.0 | 255.255.255.0 | 200.0.0.254 | 1 |
| S0/0/1 | 192.168.2.0 | 255.255.255.0 | 200.0.0.254 | 2 |
| S0/0/1 | 128.0.0.0 | 255.255.0.0 | 200.0.0.254 | 2 |
| S0/0/1 | 192.168.3.0 | 255.255.255.0 | 200.0.0.254 | 1 |
| S0/0/1 | 10.0.0.0 | 255.0.0.0 | 200.0.0.254 | 2 |

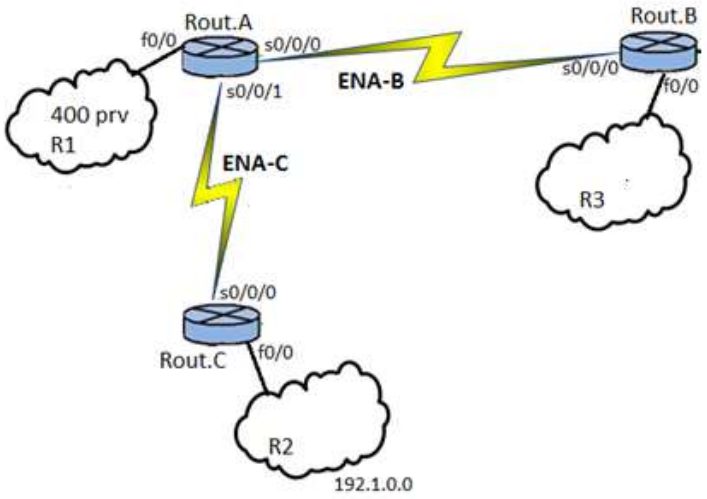
| ROUTER C | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 172.16.0.0 | 255.255.0.0 | Conectado | 0 |
| F0/1 | 192.0.0.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 200.0.0.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 172.16.0.0 | 255.255.0.0 | 200.0.0.1 | 1 |
| S0/0/0 | 192.168.1.0 | 255.255.255.0 | 200.0.0.1 | 1 |
| S0/0/0 | 126.0.0.0 | 255.255.0.0 | 200.0.0.1 | 1 |
| S0/0/0 | 192.168.0.0 | 255.255.255.0 | 200.0.0.1 | 2 |
| S0/0/1 | 192.168.3.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/1 | 10.0.0.0 | 255.0.0.0 | 192.168.3.2 | 1 |
| S0/0/2 | 200.0.1.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/2 | 192.168.2.0 | 255.255.255.0 | 200.0.1.2 | 1 |
| S0/0/2 | 128.0.0.0 | 255.255.0.0 | 200.0.1.2 | 1 |

| ROUTER D | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 192.168.2.0 | 255.255.255.0 | Conectado | 0 |
| F0/1 | 128.0.0.0 | 255.255.0.0 | Conectado | 0 |
| S0/0/0 | 200.0.1.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 172.17.0.0 | 255.255.0.0 | 200.0.1.1 | 1 |
| S0/0/0 | 192.0.0.0 | 255.255.255.0 | 200.0.1.1 | 1 |
| S0/0/0 | 200.0.0.0 | 255.255.255.0 | 200.0.1.1 | 1 |
| S0/0/0 | 172.16.0.0 | 255.255.0.0 | 200.0.1.1 | 2 |
| S0/0/0 | 192.168.1.0 | 255.255.255.0 | 200.0.1.1 | 2 |
| S0/0/0 | 126.0.0.0 | 255.255.0.0 | 200.0.1.1 | 2 |
| S0/0/0 | 192.168.0.0 | 255.255.255.0 | 200.0.1.1 | 3 |
| S0/0/0 | 192.168.3.0 | 255.255.255.0 | 200.0.1.1 | 1 |
| S0/0/0 | 10.0.0.0 | 255.0.0.0 | 200.0.1.1 | 2 |

| ROUTER E | | | | |
|---|---|---|---|---|
| **Interface** | **Red Destino** | **Máscara** | **Próximo salto** | **Número de saltos** |
| F0/0 | 10.0.0.0 | 255.0.0.0 | Conectado | 0 |
| S0/0/0 | 192.168.3.0 | 255.255.255.0 | Conectado | 0 |
| S0/0/0 | 200.0.1.0 | 255.255.255.0 | 192.168.3. 254 | 1 |
| S0/0/0 | 192.168.2.0 | 255.255.255.0 | 192.168.3. 254 | 2 |
| S0/0/0 | 128.0.0.0 | 255.255.0.0 | 192.168.3. 254 | 2 |
| S0/0/0 | 172.17.0.0 | 255.255.0.0 | 192.168.3.254 | 1 |
| S0/0/0 | 192.0.0.0 | 255.255.255.0 | 192.168.3. 254 | 1 |
| S0/0/0 | 200.0.0.0 | 255.255.255.0 | 192.168.3. 254 | 1 |
| S0/0/0 | 172.16.0.0 | 255.255.0.0 | 192.168.3. 254 | 2 |
| S0/0/0 | 192.168.1.0 | 255.255.255.0 | 192.168.3. 254 | 2 |
| S0/0/0 | 126.0.0.0 | 255.255.0.0 | 192.168.3. 254 | 2 |
| S0/0/0 | 198.168.0.0 | 255.255.255.0 | 192.168.3. 254 | 3 |

### 4.4.5 EJERCICIOS DE ENTRENAMIENTO

Una empresa X tiene varias redes distribuidas en diferentes regiones como se muestra en la figura, determinar para cada una de ellas el direccionamiento IP, configuración de routers y tabla de enrutamiento.




## 4.5 TEMA 5 INTRODUCCIÓN A IPV6

El protocolo IP es el lenguaje con el que se comunican entre sí los equipos como se explicó anteriormente. Cada dispositivo tener una dirección IP para que funcione a través de Internet.

En Colombia la mayoría de equipos están operando con tecnología IPv4, que son direcciones asignadas en cuatro números, cada uno de tres dígitos. Sin embargo, el 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet) entregó el último bloque de direcciones disponibles con tecnología IPv4, lo cual obliga a todos los países del mundo a hacer una transición al protocolo IPv6. (Mintic.gov.co)

Las direcciones IPV4 usan 32 bit lo que supone un direccionamiento de $2^{32}$ direcciones posibles es decir de 4.294.967.296 direcciones usables estas cuatro mil doscientas noventa y cuatro millones de direcciones ip hoy dia son insuficientes lo que implica que ya no hay nuevos bloques de direcciones IPV4 para entregar.

Aunque existen muchos mecanismos implementados desde los 80 para preservar las direcciones ip como el bloque de direcciones privadas en cada una de las redes y el uso de NAT esto finalmente resulto ser insuficiente.

## 4.6 TEMA 6 NOTACIÓN PARA LAS DIRECCIONES IPV6

Las direcciones IPv6, son de de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales.

Si una ipv4 son 32 bits

10101010101010101010101010101010

Una ipv6 son 128

10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
01010101010101010101010101010101010101010

Por ejemplo

2001:0db8:85a3:08d3:1319:8a2e: 0370:7334

La anterior es una dirección IPv6 válida.

Por asuntos de comodidad se puede comprimir un grupo de cuatro "0000" por::

Por ejemplo,

2001:0db8:85a3:**0000**:1319:8a2e: 0370:7344

Se puede comprimir en:

---

2001:0db8:85a3**::**1319:8a2e: 0370:7344

## 4.6.1 EJERCICIO DE APRENDIZAJE

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

2001:0DB8:0000:0000: 0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0: 0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:0DB8::1428:57ab

Los ceros iniciales en un grupo también se pueden omitir:

2001:0DB8:02de::0e13
2001:DB8:2de::e13

Si la dirección es una dirección IPv4, los últimos 32 bits pueden escribirse en base decimal, así:

::ffff:192.168.89.9 (IPv4 en IPv6 base decimal)
::ffff:c0a8:5909 (IPV4 en IPV6 escrita en formato hexadecimal)

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a :

0000:0000:0000: 0000:0000:0000: 874B:2B34 o::874B:2B34. Entonces, se puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser::135.75.43.52.

Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

Cuando lo que se desea es identificar un rango de direcciones diferenciable por medio de los primeros bits, se añade este número de bits tras el carácter de barra "/". Por ejemplo:

2001:0DB8::1428:57AB/96 sería equivalente a 2001:0DB8::
2001:0DB8::874B:2B34/96 sería equivalente a 2001:0DB8:: y por supuesto también a
2001:0DB8::1428:57AB/96

## 4.6.2 IDENTIFICACIÓN DE LOS TIPOS DE DIRECCIONES

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los rangos definidos por los primeros bits de cada dirección.

::/128

La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1/127

La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.

::1.2.3.4/96

La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.

::ffff:0:0/96

La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.

fe80::/10

El prefijo de enlace local (en inglés link local) específica que la dirección sólo es válida en el enlace físico local.

fec0::

El prefijo de emplazamiento local (en inglés site-local prefix) específica que la dirección sólo es válida dentro de una organización local. La RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial. Se deben sustituir por direcciones Local IPv6 Únicast.

ff00::/8

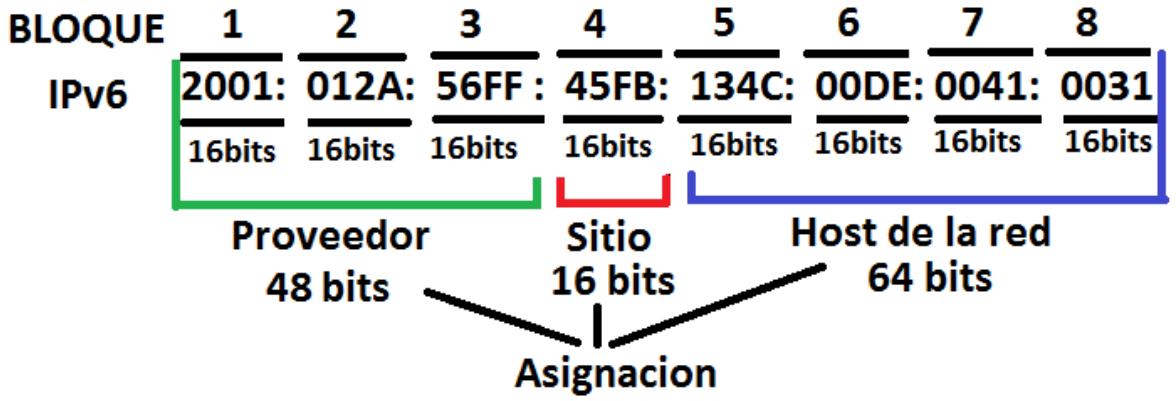
El prefijo de multicast. Se usa para las direcciones multicast.

Hay que resaltar que no existen las direcciones de difusión (en inglés broadcast) en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast FF01::1/128, denominada todos los nodos (en inglés all nodes)

Una de las diferencias más marcadas es que IPv6 tiene un tamaño de 128 bits es decir $2^{128}$ es decir 3,402823669209384634633746074317 7e+38 direcciones disponibles estas 340 sixtillones de direcciones (340 millones de millones de millones de millones de millones de millones de millones ) son una gran cantidad de direcciones su repesentacion se realiza en números en 8 bloques de 16 bits escritos en hexadecimales asi

2001:0000:02AA:34FF: 2567:11BC: 23AC:00C2

Una dirección ipv6 tiene además de los 8 bloques de 16 bits, una estructura donde se asignan 32 bits a los proveedores de red a nivel mundial y espacio de 16 bits para distribución a clientes (sitio) y 64 bits a cada pc. La parte de proveedor(48) + sitio(16) sería la parte de red (64) y los 64 restantes se asignan a la parte de host Asi:




*Distribución de dirección ipv6 fuente el autor*

La máscara de red es se representa en formato /x donde x es al igual que en ipv4 es el numero bit de la parte de host

Algunas diferencias entre ipv4 e ipv6

*Comparación ipv4 ipv6 resumen*

| | Protocolo de Internet versión 4 (IPv4) | Protocolo de Internet versión 6 (IPv6) |
|---|---|---|
| Lanzado en | 1981 | 1999 |
| Tamaño de las direcciones | Número de 32 bits | Número de 128 bits |
| Formato de las direcciones | Notación decimal con puntos: 192.149.252.76 | Notación hexadecimal: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD |
| Notación de prefijos | 192.149.0.0/24 | 3FFE:F200:0234::/48 |
| Cantidad de direcciones | $2^{32}$ = ~4,000,000,000 | $2^{128}$ = ~340,000,000,000,000,000,000,000,000,000,000,000 |

## 4.6.3 EJERCICIO DE ENTRENAMIENTO

1) Por cuantos bits eta conformada una dirección IPv4
2) Por cuantos bits eta conformada una dirección IPv4
3) Una máscara 255.255.0.0 pertenece a una red IPv6 ¿por qué?
4) Una red con mascara /60 puede ser una red clase B, justificar respuesta
5) Una red con mascara /60 puede ser una red clase A, justificar respuesta
6) Una red con mascara /60 puede ser una red clase C, justificar respuesta
7) Una red con mascara /60 puede ser una red IPv4, justificar respuesta
8) Simplifique la IP 2001:0000:002A:0000:2567:0000: 0000:00C2
9) Simplifique la IP 2001:0000:0000:0001:2567:0000: 0000:00C2

# 5 UNIDAD 4 CONFIGURACIÓN DE ROUTERS Y DIVISION DE REDES

Configurar routers cisco empleando packet tracer y determinar las rutas para enviar paquetes empleando rutas estáticas.

Los routers se configuran desde una línea de comandos llamado CLI

```
         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#
```

*Ejemplo de comandos usados en un router el autor*

## 5.1 TEMA 1 ENRUTAMIENTO ESTÁTICO:

Las rutas estáticas son definidas manualmente por el administrador para que el router aprenda sobre una red remota. Las rutas estáticas necesitan pocos recursos del sistema, es recomendable utilizarlas cuando nuestra red esté compuesta por unos cuantos routers o que la red se conecte a internet solamente a través de un único ISP.

El comando para configurar una ruta estática es "ip route" y su sintaxis más simple esla siguiente:

router(config)# **ip route** *direccion-red mascara-subred { direccion-ip | interfaz-salida }*
Donde:

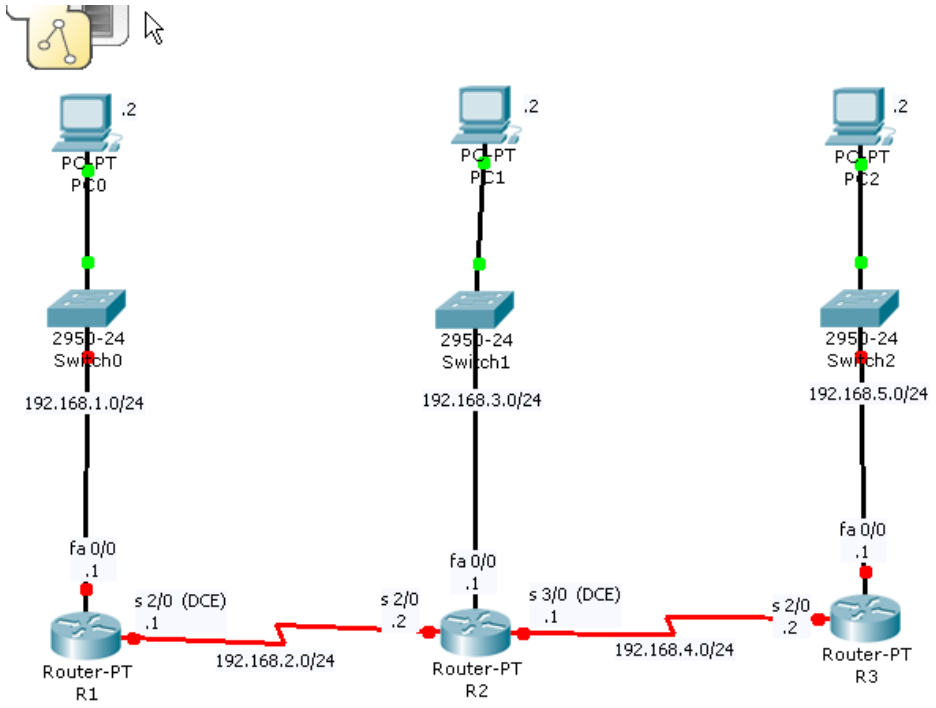
***dirección-red:*** Es la dirección de la red remota que deseamos alcanzar.
***máscara-subred*:** máscara de subred de la red remota.
***dirección-ip*:** Dirección ip de la interfaz del router vecino (ip del siguiente salto).
***interfaz-salida:*** Interfaz que utilizará el router para enviar paquetes a la red remota de destino.

Por lo tanto, una ruta estática puede configurarse de 2 maneras:

router(config)# **ip route** *direccion-red mascara-subred direccion-ip*
router(config)# **ip route** *direccion-red mascara-subred interfaz-salida*

## 5.1.1 EJERCICIO DE APRENDIZAJE

Dado el siguiente esquema:




Configure lo básico en cada router de la siguiente topología:

**R1:**

| | |
|---|---|
| Router> enable<br>Router # configure terminal<br>Router(config) # hostname R1<br>R1(config)#interface fastethernet 0/0<br>R1(config-if)#ip address 192.168.1.1 255.255.255.0<br>R1(config-if)#no shutdown<br>R1(config-if)#exit<br><br>R1(config)#interface serial 2/0 | Enable: pasa de modo usuario (>) a modo privilegiado (#)<br><br>Hostname: cambia el nombre del router<br><br>Interface: entra a una interface especifica<br><br>Ip address: Coloca una ip a una interface<br><br>No shutdown : habilita una interface |

| | |
|---|---|
| R1(config-if)#ip address 192.168.2.1 255.255.255.0<br>R1(config-if)#clock rate 56000<br>R1(config-if)#no shutdown<br>R1(config-if)#exit<br>R1(config)#exit<br>R2# | Exit : Sale de un submenú |

**R2:**

| | |
|---|---|
| Router> enable<br>Router # configure terminal<br>Router(config) # hostname R2<br>R2(config)#interface fastethernet 0/0<br>R2(config-if)#ip address 192.168.3.1 255.255.255.0<br>R2(config-if)#no shutdown<br>R2(config-if)#exit<br>R2(config)#interface serial 2/0<br>R2(config-if)#ip address 192.168.2.2 255.255.255.0<br>R2(config-if)#no shutdown<br>R2(config-if)#exit<br>R2(config)#interface serial 3/0<br>R2(config-if)#ip address 192.168.4.1 255.255.255.0<br>R2(config-if)#clock rate 56000<br>R2(config-if)#no shutdown<br>R2(config-if)#exit<br>R2(config)#exit<br>R2# | Enable: pasa de modo usuario (>) a modo privilegiado (#)<br><br>Hostname: cambia el nombre del router<br><br>Interface: entra a una interface especifica<br><br>Ip address: Coloca una ip a una interface<br><br>No shutdown : habilita una interface<br><br>Exit : Sale de un submenú |

**R3:**

| | |
|---|---|
| Router> enable<br>Router # configure terminal<br>Router(config) # hostname R3<br>R3(config)#interface fastethernet 0/0<br>R3(config-if)#ip address 192.168.5.1 255.255.255.0<br>R3(config-if)#no shutdown<br>R3(config-if)#exit<br>R3(config)#interface serial 2/0<br>R3(config-if)#ip address 192.168.4.2 255.255.255.0<br>R3(config-if)#no shutdown<br>R3(config-if)#exit | Enable: pasa de modo usuario (>) a modo privilegiado (#)<br><br>Hostname: cambia el nombre del router<br><br>Interface: entra a una interface especifica<br><br>Ip address: Coloca una ip a una interface<br><br>No shutdown : habilita una interface<br><br>Exit : Sale de un submenú |

| | |
|---|---|
| R3(config)#exit<br>R3# | |

El siguiente paso es configurar las PC's con su dirección de red, máscara de subred y puerta de enlace predeterminada que de hecho no tiene nada de complicado, de esta manera tendremos conexión entre las redes conectadas directamente a cada router, pero como le hacemos, por ejemplo, para que R1 pueda mandar datos a las subredes de R3. Aquí es donde entra el enrutamiento estático definido por el administrador tomando en cuenta la sintaxis antes mencionada:

**Rutas estáticas con la interfaz de salida**

| | |
|---|---|
| **R1:**<br><br>R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2<br>R1(config)#ip route 192.168.4.0 255.255.255.0 192.168.2.2<br>R1(config)#ip route 192.168.5.0 255.255.255.0 192.168.2.2 | **Se le enseña a llegar a las redes no adyacentes** 192.168.3.0, 192.168.4.0, 192.168.5,0 |
| **R2:**<br><br>R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.1<br>R2(config)#ip route 192.168.5.0 255.255.255.0 192.168.4.2 | **Se le enseña a llegar a las redes no adyacentes** 192.168.1.0, 192.168.5.0 |
| **R3:**<br><br>R3(config)#ip route 192.168.1.0 255.255.255.0 192.168.4.1<br>R3(config)#ip route 192.168.2.0 255.255.255.0 192.168.4.1<br>R3(config)#ip route 192.168.3.0 255.255.255.0 192.168.4.1 | **Se le enseña a llegar a las redes no adyacentes** 192.168.1.0, 192.168.2.0, 192.168.3.0 |

**Rutas estáticas con la ip del siguiente salto**

Con esto tendremos acceso a todas nuestras redes desde cualquier LAN y así es como funciona el enrutamiento estático

**Ruta Estática por Defecto**

Una ruta estática por defecto, es aquella que siempre va a coincidir con los paquetes cuya red de destino, no se encuentre disponible en la tabla de enrutamiento ya que su dirección de red y máscara de subred es 0.0.0.0; Su sintaxis es:

router(config)#**ip route** *0.0.0.0 0.0.0.0 { ip-siguiente-salto | interfaz-salida }*

Este video es un complemento valioso sobre la configuración de routers ipv4 direccionamiento estático se muestra a continuación

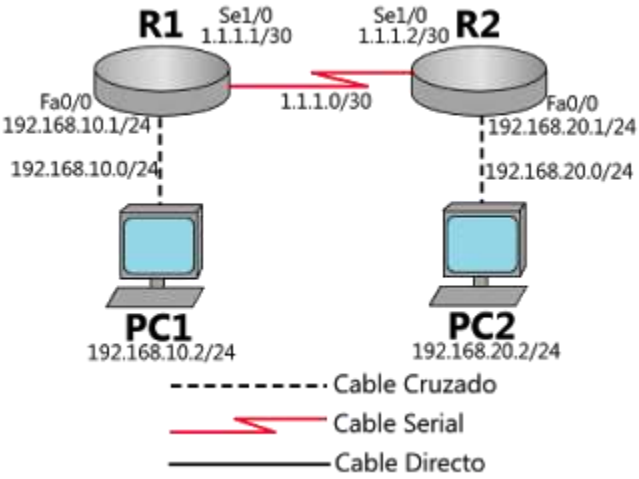

*Conexion Routers RCGCalume Enlace*


*Basico router statico RCGCalume Enlace*

## 5.2 TEMA 2 ENRUTAMIENTO DINÁMICO CON RIP EN ROUTERS CISCO

La configuración del enrutamiento dinámico de routers Cisco mediante el protocolo RIP.

## 5.2.1 EJERCICIO DE APRENDIZAJE




Como podemos ver en el diagrama, tenemos dos routers R1 y R2 que se comunican mediante la red 1.1.1.0/30 a través de sus interfaces seriales 1.1.1.1/30 y 1.1.1.2/30 respectivamente. Adicionalmente, tenemos dos computadoras PC1 y PC2 que se comunican con los routers R1 y R2 mediante las redes 192.168.10.0/24 y 192.168.20.0/24 respectivamente.

En este ejemplo, vamos a configurar los equipos R1 y R2 para lograr conectividad entre los equipos PC1 y PC2 usando enrutamiento dinámico con el protocolo RIP. El protocolo RIP (Routing Information Protocol) es un protocolo de enrutamiento por vector-distancia y utiliza el número de saltos como métrica para la selección de rutas.

El comando para configurar el enrutamiento estático mediante el protocolo RIP es router rip. Para agregar las redes se usa el comando network [dirección_red] donde [dirección_red] es la dirección de la red con clase directamente conectada al router. Por ejemplo, para la red 1.1.1.0(clase A) su dirección con clase es 1.0.0.0, para la red 172.16.26.0(clase B) su dirección con clase es 172.16.0.0 y para la red 192.168.35.0(clase C) su dirección con clase es 192.168.35.0. Como se observa en el diagrama, en el router R1 las redes directamente conectadas son 192.168.10.0/24 y 1.1.1.0/30 y para el router R2 las redes directamente conectadas son 192.168.20.0/24 y 1.1.1.0/30.

**Configuración de los routers R1 y R2**

Procedemos a configurar el nombre, la interfaz fastEthernet y la interfaz serial de los routers R1 y R2 según el diagrama de red. Se usa la misma configuración para las interfaces que se usó en el Enrutamiento Estático y sigue los pasos indicados en los puntos Configuración del Router R1 y Configuración del Router R2 para configurar los equipos.

Hasta este punto, hemos configurado R1 y R2 para que tengan su configuración de interfaces, todavía no hemos configurado el enrutamiento dinámico en los equipos. Antes de continuar, podemos hacer uso del comando ping para probar la conectividad entre los equipos.

**Configuración del enrutamiento dinámico entre R1 y R2**

En R1, luego de configurar las interfaces igual que en el enrutamiento estático, entramos al modo de configuración global y configuramos el enrutamiento dinámico ingresando las redes directamente conectadas a R1:

| | |
|---|---|
| **R1**<br><br>R1>enable<br>R1#configure terminal<br>R1(config)#router rip<br>R1(config-router)#network 1.0.0.0<br>R1(config-router)#network 192.168.10.0<br>R1(config-router)#exit<br>R1(config)#exit<br>R1# | Router rip: habilita el direccionamiento dinámico RIP<br><br>Network: especifica las redes que se publicaran para anúncialas a los otros routers<br><br>Se configuran únicamente las redes que están configuradas directamente 1.0.0.0 y 192.168.10.0 |
| De manera análoga, realizamos el procedimiento para R2:<br><br>**R2**<br><br>R2>enable<br>R2#configure terminal<br>R2(config)#router rip<br>R2(config-router)#network 1.0.0.0<br>R2(config-router)#network 192.168.20.0<br>R2(config-router)#exit<br>R2(config)#exit<br>R2# | Router rip: habilita el direccionamiento dinámico RIP<br><br>Network: especifica las redes que se publicaran para anúncialas a los otros routers<br><br>Se configuran únicamente las redes que están configuradas directamente 1.0.0.0 y 192.168.20.0 |

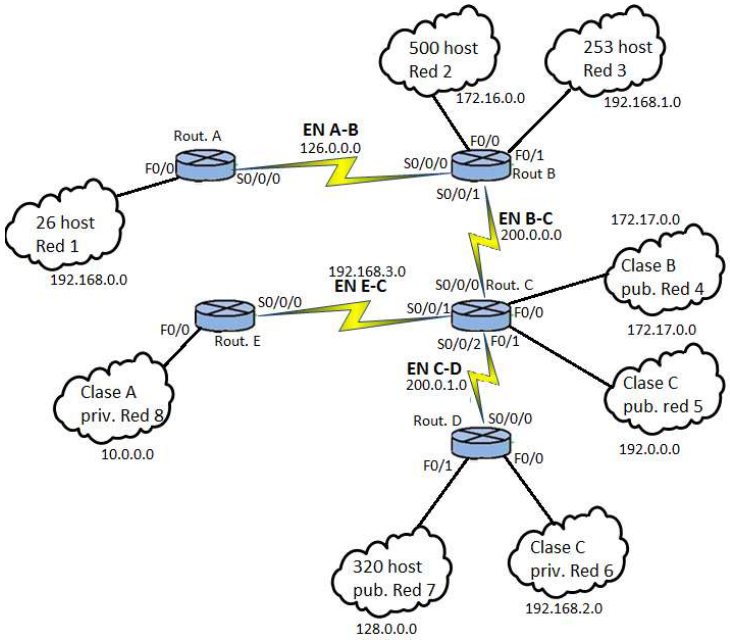
Y listo, tenemos los equipos configurados con enrutamiento dinámico usando el protocolo RIP.

Este video es un complemento valioso sobre, Un ejemplo de la configuración de routers ipv4 direccionamiento estático se muestra a continuación


*Configuracion RIP Enlace*

## 5.2.2 EJERCICIO DE ENTRENAMIENTO

Configure cada router de la siguiente red usando **enrutamiento estático** y luego desarrolle usando **enrutamiento dinámico.**



## 5.3 TEMA 3 OTROS COMANDOS

Para ver la configuración del enrutamiento dinámico se usa el comando **show ip protocols**.

*R1# show ip protocols*

Para ver la configuración completa de un router se usa el comando **show running-config** .

*R1# show running-config*

Podemos verificar que el enrutamiento funciona haciendo ping a las interfaces fastEthernet de R1 y R2. Por ejemplo, para verificar el enrutamiento en R1:

*R1>ping 192.168.20.1*

Para probar el enrutamiento en R2:

*R2>ping 192.168.10.1*

También se puede usar este comando desde los PC.

Para probar la conectividad entre los hosts (PC1 y PC2), solo es necesario configurar la dirección IP, la máscara de red y la dirección IP de la puerta de enlace para cada uno. Para PC1 la puerta de enlace sería la interfaz Ethernet 0/0 de R1 cuya dirección IP es 192.168.10.1 y para PC2 la puerta de enlace sería la interfaz Ethernet 0/0 de R2 cuya dirección IP es 192.168.20.1. Luego queda probar la conectividad con el comando **ping**. Por ejemplo, para PC1 el comando es **ping 192.168.20.2** y para PC2 el comando es **ping 192.168.10.2**

## 5.4 TEMA 4 DIVISION DE REDES EN SUB-REDES

Es posible dividir una red en redes más pequeñas sub redes, Cuando las redes se subdividen en subredes la máscara cambia, para ambientar esto suponga que se tiene una red clase B 172.2.0.0 y se quiere dividir en 6 subredes más pequeñas

### 5.4.1 PROCEDIMIENTO

Encontrar por cada subred ID de Red, Dirección de broadcast, Rango de direcciones de host y máscara de subred

Cuantos bits deben separarse para crear 6 subredes de la red clase b 172.2.0.0, para hacer el 6 (número de redes) en binario necesitamos, 3 bits puesto que el 6 en binario es 110

**6 en binario es 110 (3 bits)**

1. Debemos separar 3bit del campo HOST 172.3 es el campo de red y 0.0 es el campo de host

| RED | | HOST | |
|---|---|---|---|
| 172 | 2 | 0 | 0 |
| 10101100 | 00000010 | 000 | 00000000000 |

2. Con esta información sabemos que podemos crear redes desde 000 a 111 o sea 8 redes como solo requerimos 6 las otras 2 **no se usan**!!

| | RED 0 | RED 1 | RED 2 | RED 3 | RED 4 | RED 5 | RED 6 | RED 7 |
|---|---|---|---|---|---|---|---|---|
| BINARIO | 000 | 001 (1) | 010 (2) | 011 (3) | 100 (4) | 101 (5) | 110 (6) | 111 (7) |
| Utilizable | No | Si | Si | Si | Si | Si | Si | No |

Calculemos la máscara, Para una red clase B como la anterior, sabemos que la máscara por defecto de una red clase B es

| Notación Binaria | Notación Decimal |
|---|---|
| 11111111.11111111.00000000.00000000 | 255.255.0.0 |

Como se tomaron 3 bit del campo HOST la nueva máscara queda

| Notación Binaria | Notación Decimal |
|---|---|
| 11111111.11111111.11100000.00000000 | 255.255.224.0 |

La subred 00101100.00000000.00000010.00000000.00000000 (172.2.0.0) no se utiliza.

Se comienza por la subred 00101100.00000010.00100000.00000000 (172.2.32.0) esta puede usar nodos desde 0000000000000001 (1) a 1111111111110 (8190), recuerde la primera dirección es el ID de Red y la última es la dirección de broadcast.

00101100.00000010.00100000.00000000 es el ID de RED en la subred 001

00101100.00000010.00100000.00000001 es el primer HOST en la subred 001

00101100.00000010.00111111.11111110 es el último HOST en la subred 001

**Convirtiendo a decimal**

172.2.32.0 es el ID de RED en la subred 001

172.2.32.1 es el primer HOST en la subred 001

172.2.63.254 es el último HOST en la subred 001

172.2.63.255 es la dirección de broadcast

La siguiente red es 010 (2) debe continuar con el número siguiente a la dirección de broadcast de la subred anterior y cambiar cada 8190 Host así

172.2.64.0 es el ID de RED en la subred 010

172.2.64.1 es el primer HOST en la subred 010

172.2.95.254 es el último HOST en la subred 010

172.2.95.255 es la dirección de broadcast

En forma tabular se tiene que la división de 172.2.0.0 mascara 255.255.0.0 en 6 redes que da asi:

| | ID RED | Rango | Broadcast | Máscara |
|---|---|---|---|---|
| RED 0 | 172.2.0.0 | No Se Utiliza | | |
| RED 1 | 172.2.32.0 | 172.2.32.1- 172.2.63.254 | 172.2.64.255 | 255.255.224.0 |
| RED 2 | 172.2.64.0 | 172.2.64.1- 172.95.254 | 172.2.98.255 | 255.255.224.0 |
| RED 3 | 172.2.96.0 | 172.2.96.1-172.2.127.254 | 172.2.127.255 | 255.255.224.0 |
| RED 4 | 172.2.128.0 | 172.2.128.1- 172.2.159.254 | 172.2.159.255 | 255.255.224.0 |
| RED 5 | 172.2.160.0 | 172.2.160.1-172.2.192.254 | 172.2.159.255 | 255.255.224.0 |
| RED 6 | 172.2.192.0 | 172.2.192.1- 172.2.224.254 | 172.2.159.255 | 255.255.224.0 |
| RED 7 | 172.2.224.0 | No Se Utiliza | | |

La siguiente gigante tabla pude ser útil para convertir cada octeto de binario a decimal y decimal a binario

*Tabla 1 Valor decimal de las posiciones de bits*

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Valor |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 128 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 192 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 224 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 240 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 248 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 252 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 254 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 255 |

*Fuente El autor*

## 5.4.2 EJERCICIO DE APRENDIZAJE 1

Divide la red 192.168.10.0 máscara 255.255.255.0 en 2 subredes

1. Comprobar si se pueden tener esas subredes con la configuración dada.

Si, si es posible tener las 2 subredes, porque hay suficientes bits a 0 en la máscara. Hay 8 bits a cero (y 28 es mayor que 2), como se puede observar en la mascará:

11111111.11111111.11111111.00000000

Los bits a 0 son los bits en verde. Esta máscara la ampliaremos para crear subredes, la ampliaremos cambiando ceros por unos de forma que volvamos a obtener una máscara que sea correcta.

2. Calcular el número de bits mínimo para las subredes.

Para tener las subredes que has especificado es necesario utilizar al menos 2 bits, porque 22=4 y este resultado es mayor o igual a 2 (que son el número de subredes que necesitas). Esos bits son los que deberás modificar para cambiar el número de subred.

Ahora, fíjate bien, a continuación, se expone la máscara origen indicando en verde los bits que serán utilizados para especificar (en la dirección ip) el número de subred:

11111111.11111111.11111111.00000000

3. Calcular la máscara ampliada.

Ahora, partiendo del calculo que se ha hecho en el paso de antes, calcular los bits reservados para indicar el número de subred, calculamos la máscara ampliada cambiando esos ceros reservados para subredes en unos, o lo que es lo mismo, los bits que se han marcado como verdes debemos convertirlos en unos. Tal y como se indica a continuación:

Máscara origen: 11111111.11111111.11111111.00000000 (255.255.255.0)

Máscara ampliada: 11111111.11111111.11111111.11000000 (255.255.255.192)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada (todas las mismas). Los unos en color verde de la máscara ampliada son los que tendremos que cambiar en la dirección IP para indicar el número de subred.

4. ¿Cuántos equipos habrá por subred?

Los ceros de la máscara ampliada son los que utilizaremos para indicar el número de host dentro de cada subred. Como puedes observar en la máscara ampliada, tenemos 6 bits reservados para indicar el número de host dentro de cada subred y esto nos permite tener 26-2 hosts por subred, o lo que es lo mismo, 62 hosts.

5. ¿Qué tenemos que modificar en la dirección de red?

Ahora, la máscara ampliada nos indica que bits podemos cambiar en la dirección de red. La dirección de red para la dirección ip que has indicado es: 192.168.10.0, con lo que, según la máscara ampliada, los bits que modificaríamos sería:

```
Máscara ampliada: 11111111.11111111.11111111.11000000 - 255.255.255.192
Dirección de red: 11000000.10101000.00001010.00000000 - 192.168.10.0
```

Como puedes observar, los bits en rojo, son los que estaban de la máscara anterior, y esos no se podrán modificar, son intocables. Los bits en verde son los que modificaremos para indicar la subred, pero ojo, los cambiamos en la dirección de red, no en la máscara ampliada, y los bits en azul los cambiamos para indicar la dirección del equipo.

6. Listado de las subredes que habría.

A continuación, se muestran todas las subredes que se podrían crear con la configuración dada. Ten en cuenta que la dirección de subred indica el primer equipo de la subred y que la dirección de broadcast el último equipo de dicha subred. Además, ten en cuenta que todas las subredes tienen la misma máscara ampliada (255.255.255.192):

| Nº de Subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 192.168.10.0 (11000000.10101000.00001010.00000000) | 192.168.10.63 (11000000.10101000.00001010.00111111) |
| 1 | 192.168.10.64 (11000000.10101000.00001010.01000000) | 192.168.10.127 (11000000.10101000.00001010.01111111) |
| 2 | 192.168.10.128 (11000000.10101000.00001010.10000000) | 192.168.10.191 (11000000.10101000.00001010.10111111) |
| 3 | 192.168.10.192 (11000000.10101000.00001010.11000000) | 192.168.10.255 (11000000.10101000.00001010.11111111) |

**Nota**: Observa que la única diferencia entre la dirección de red y la dirección de broadcast es que en la sección del número de host (los bits en azul), en la dirección de red son todos cero y en la dirección de broadcast son todo unos. Entre el rango comprendido entre la dirección de red y la de broadcast estarán todos los equipos de la subred.

## 5.4.3 EJERCICIO DE APRENDIZAJE 2

Divide la red 192.168.10.0 con máscara 255.255.255.0 en 5 sub redes

1. Comprobar si se pueden tener esas subredes con la configuración dada.

Si, si es posible tener las 5 subredes, porque hay suficientes bits a 0 en la máscara. Hay 8 bits a cero (y 28 es mayor que 5), como se puede observar en la mascará:

11111111.11111111.11111111.00000000

Los bits a 0 son los bits en verde. Esta máscara la ampliaremos para crear subredes, la ampliaremos cambiando ceros por unos de forma que volvamos a obtener una máscara que sea correcta.

2. Calcular el número de bits mínimo para las subredes.

Para tener las subredes que has especificado es necesario utilizar al menos 3 bits, porque 23=8 y este resultado es mayor o igual a 5 (que son el número de subredes que necesitas). Esos bits son los que deberás modificar para cambiar el número de subred.

Ahora, fíjate bien, a continuación, se expone la máscara origen indicando en verde los bits que serán utilizados para especificar (en la dirección ip) el número de subred:

11111111.11111111.11111111.00000000

3. Calcular la máscara ampliada.

Ahora, partiendo del calculo que se ha hecho en el paso de antes, calcular los bits reservados para indicar el número de subred, calculamos la máscara ampliada cambiando esos ceros reservados para subredes en unos, o lo que es lo mismo, los bits que se han marcado como verdes debemos convertirlos en unos. Tal y como se indica a continuación:

Máscara origen: 11111111.11111111.11111111.00000000 (255.255.255.0)

Máscara ampliada: 11111111.11111111.11111111.11100000 (255.255.255.224)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada (todas las mismas). Los unos en color verde de la máscara ampliada son los que tendremos que cambiar en la dirección IP para indicar el número de subred.

4. ¿Cuántos equipos habrá por subred?

Los ceros de la máscara ampliada son los que utilizaremos para indicar el número de host dentro de cada subred. Como puedes observar en la máscara ampliada, tenemos 5 bits reservados para indicar el número de host dentro de cada subred y esto nos permite tener 25-2 hosts por subred, o lo que es lo mismo, 30 hosts.

5. ¿Qué tenemos que modificar en la dirección de red?

Ahora, la máscara ampliada nos indica que bits podemos cambiar en la dirección de red. La dirección de red para la dirección ip que has indicado es: 192.168.10.0, con lo que según la máscara ampliada, los bits que modificaríamos sería:

```
Máscara ampliada: 11111111.11111111.11111111.11100000 - 255.255.255.224
Dirección de red: 11000000.10101000.00001010.00000000 - 192.168.10.0
```

Como puedes observar, los bits en rojo, son los que estaban de la máscara anterior, y esos no se podrán modificar, son intocables. Los bits en verde son los que modificaremos para indicar la subred, pero ojo, los cambiamos en la dirección de red, no en la máscara ampliada, y los bits en azul los cambiamos para indicar la dirección del equipo.

6. Listado de las subredes que habría

A continuación, se muestran todas las subredes que se podrían crear con la configuración dada. Ten en cuenta que la dirección de subred indica el primer equipo de la subred y que la dirección de broadcast el último equipo de dicha subred. Además, ten en cuenta que todas las subredes tienen la misma máscara ampliada (255.255.255.224):

| Nº de Subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 192.168.10.0<br>(11000000.10101000.00001010.00000000) | 192.168.10.31<br>(11000000.10101000.00001010.00011111) |
| 1 | 192.168.10.32<br>(11000000.10101000.00001010.00100000) | 192.168.10.63<br>(11000000.10101000.00001010.00111111) |
| 2 | 192.168.10.64<br>(11000000.10101000.00001010.01000000) | 192.168.10.95<br>(11000000.10101000.00001010.01011111) |
| 3 | 192.168.10.96<br>(11000000.10101000.00001010.01100000) | 192.168.10.127<br>(11000000.10101000.00001010.01111111) |

| | | |
|---|---|---|
| 4 | 192.168.10.128 (11000000.10101000.00001010.10000000) | 192.168.10.159 (11000000.10101000.00001010.10011111) |
| 5 | 192.168.10.160 (11000000.10101000.00001010.10100000) | 192.168.10.191 (11000000.10101000.00001010.10111111) |
| 6 | 192.168.10.192 (11000000.10101000.00001010.11000000) | 192.168.10.223 (11000000.10101000.00001010.11011111) |
| 7 | 192.168.10.224 (11000000.10101000.00001010.11100000) | 192.168.10.255 (11000000.10101000.00001010.11111111) |

**Nota:** Observa que la única diferencia entre la dirección de red y la dirección de broadcast es que en la sección del número de host (los bits en azul), en la dirección de red son todos cero y en la dirección de broadcast son todo unos. Entre el rango comprendido entre la dirección de red y la de broadcast estarán todos los equipos de la subred.

## 5.4.4 EJERCICIO DE APRENDIZAJE 3

Divide la red 172.0.0.0 con máscara 255.255.0.0 en 2 sub redes

1. Comprobar si se pueden tener esas subredes con la configuración dada.

Si, si es posible tener las 2 subredes, porque hay suficientes bits a 0 en la máscara. Hay 16 bits a cero (y 216 es mayor que 2), como se puede observar en la máscara:

11111111.11111111.00000000.00000000

Los bits a 0 son los bits en verde. Esta máscara la ampliaremos para crear subredes, la ampliaremos cambiando ceros por unos de forma que volvamos a obtener una máscara que sea correcta.

2. Calcular el número de bits mínimo para las subredes.

Para tener las subredes que has especificado es necesario utilizar al menos 2 bits, porque 22=4 y este resultado es mayor o igual a 2 (que son el número de subredes que necesitas). Esos bits son los que deberás modificar para cambiar el número de subred.

Ahora, fíjate bien, a continuación, se expone la máscara origen indicando en verde los bits que serán utilizados para especificar (en la dirección ip) el número de subred:

11111111.11111111.00000000.00000000

3. Calcular la máscara ampliada.

Ahora, partiendo del calculo que se ha hecho en el paso de antes, calcular los bits reservados para indicar el número de subred, calculamos la máscara ampliada cambiando esos ceros reservados para subredes en unos, o lo que es lo mismo, los bits que se han marcado como verdes debemos convertirlos en unos. Tal y como se indica a continuación:

Máscara origen: 11111111.11111111.00000000.00000000 (255.255.0.0)

Máscara ampliada: 11111111.11111111.11000000.00000000 (255.255.192.0)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada (todas las mismas). Los unos en color verde de la máscara ampliada son los que tendremos que cambiar en la dirección IP para indicar el número de subred..

4. ¿Cuántos equipos habrá por subred?

Los ceros de la máscara ampliada son los que utilizaremos para indicar el número de host dentro de cada subred. Como puedes observar en la máscara ampliada, tenemos 14 bits reservados para indicar el número de host dentro de cada subred y esto nos permite tener 214-2 hosts por subred, o lo que es lo mismo, 16382 hosts.

5. ¿Qué tenemos que modificar en la dirección de red?

Ahora, la máscara ampliada nos indica que bits podemos cambiar en la dirección de red. La dirección de red para la dirección ip que has indicado es: 172.0.0.0, con lo que, según la máscara ampliada, los bits que modificaríamos sería:

```
Máscara ampliada: 11111111.11111111.11000000.00000000 - 255.255.192.0
Dirección de red: 10101100.00000000.00000000.00000000 - 172.0.0.0
```

Como puedes observar, los bits en rojo, son los que estaban de la máscara anterior, y esos no se podrán modificar, son intocables. Los bits en verde son los que modificaremos para indicar la subred, pero ojo, los cambiamos en la dirección de red, no en la máscara ampliada, y los bits en azul los cambiamos para indicar la dirección del equipo.

6. Listado de las subredes que habría

A continuación, se muestran todas las subredes que se podrían crear con la configuración dada. Ten en cuenta que la dirección de subred indica el primer equipo de la subred y que la dirección de broadcast el último equipo de dicha subred. Además, ten en cuenta que todas las subredes tienen la misma máscara ampliada (255.255.192.0):

| Nº de Subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 172.0.0.0 (10101100.00000000.00000000.00000000) | 172.0.63.255 (10101100.00000000.00111111.11111111) |
| 1 | 172.0.64.0 (10101100.00000000.01000000.00000000) | 172.0.127.255 (10101100.00000000.01111111.11111111) |
| 2 | 172.0.128.0 (10101100.00000000.10000000.00000000) | 172.0.191.255 (10101100.00000000.10111111.11111111) |
| 3 | 172.0.192.0 (10101100.00000000.11000000.00000000) | 172.0.255.255 (10101100.00000000.11111111.11111111) |

Recuerda la subred 0 (primera) y 3 (última no deben ser usadas)

**Nota:** Observa que la única diferencia entre la dirección de red y la dirección de broadcast es que en la sección del número de host (los bits en azul), en la dirección de red son todos cero y en la dirección de broadcast son todo unos. Entre el rango comprendido entre la dirección de red y la de broadcast estarán todos los equipos de la subred.

## 5.4.5 EJERCICIO DE APRENDIZAJE 4

Divide la red 10.0.0.0 máscara 255.255.255.0 en 2 subredes

1. Comprobar si se pueden tener esas subredes con la configuración dada.

Si, si es posible tener las 2 subredes, porque hay suficientes bits a 0 en la máscara. Hay 8 bits a cero (y 28 es mayor que 2), como se puede observar en la mascará:

11111111.11111111.11111111.00000000

Los bits a 0 son los bits en verde. Esta máscara la ampliaremos para crear subredes, la ampliaremos cambiando ceros por unos de forma que volvamos a obtener una máscara que sea correcta.

2. Calcular el número de bits mínimo para las subredes.

Para tener las subredes que has especificado es necesario utilizar al menos 2 bits, porque 22=4 y este resultado es mayor o igual a 2 (que son el número de subredes que necesitas). Esos bits son los que deberás modificar para cambiar el número de subred.

Ahora, fíjate bien, a continuación, se expone la máscara origen indicando en verde los bits que serán utilizados para especificar (en la dirección ip) el número de subred:

11111111.11111111.11111111.00000000

3. Calcular la máscara ampliada.

Ahora, partiendo del calculo que se ha hecho en el paso de antes, calcular los bits reservados para indicar el número de subred, calculamos la máscara ampliada cambiando esos ceros reservados para subredes en unos, o lo que es lo mismo, los bits que se han marcado como verdes debemos convertirlos en unos. Tal y como se indica a continuación:

Máscara origen: 11111111.11111111.11111111.00000000 (255.255.255.0)

Máscara ampliada: 11111111.11111111.11111111.11000000 (255.255.255.192)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada (todas las mismas). Los unos en color verde de la máscara ampliada son los que tendremos que cambiar en la dirección IP para indicar el número de subred.

4. ¿Cuántos equipos habrá por subred?

Los ceros de la máscara ampliada son los que utilizaremos para indicar el número de host dentro de cada subred. Como puedes observar en la máscara ampliada, tenemos 6 bits reservados para indicar el número de host dentro de cada subred y esto nos permite tener 26-2 hosts por subred, o lo que es lo mismo, 62 hosts.

5. ¿Qué tenemos que modificar en la dirección de red?

Ahora, la máscara ampliada nos indica que bits podemos cambiar en la dirección de red. La dirección de red para la dirección ip que has indicado es: 10.0.0.0, con lo que según la máscara ampliada, los bits que modificaríamos sería:

```
Máscara ampliada: 11111111.11111111.11111111.11000000 - 255.255.255.192
Dirección de red: 00001010.00000000.00000000.00000000 - 10.0.0.0
```

Como puedes observar, los bits en rojo, son los que estaban de la máscara anterior, y esos no se podrán modificar, son intocables. Los bits en verde son los que modificaremos para indicar la subred, pero ojo, los cambiamos en la dirección de red, no en la máscara ampliada, y los bits en azul los cambiamos para indicar la dirección del equipo.

6. Listado de las subredes que habría

A continuación, se muestran todas las subredes que se podrían crear con la configuración dada. Ten en cuenta que la dirección de subred indica el primer equipo de la subred y que la dirección de broadcast el último equipo de dicha subred. Además, ten en cuenta que todas las subredes tienen la misma máscara ampliada (255.255.255.192):

| Nº de Subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 10.0.0.0<br>(00001010.00000000.00000000.00000000) | 10.0.0.63<br>(00001010.00000000.00000000.00111111) |
| 1 | 10.0.0.64<br>(00001010.00000000.00000000.01000000) | 10.0.0.127<br>(00001010.00000000.00000000.01111111) |
| 2 | 10.0.0.128<br>(00001010.00000000.00000000.10000000) | 10.0.0.191<br>(00001010.00000000.00000000.10111111) |
| 3 | 10.0.0.192<br>(00001010.00000000.00000000.11000000) | 10.0.0.255<br>(00001010.00000000.00000000.11111111) |

**Nota:** Observa que la única diferencia entre la dirección de red y la dirección de broadcast es que en la sección del número de host (los bits en azul), en la dirección de red son todos cero y en la dirección de broadcast son todo unos. Entre el rango comprendido entre la dirección de red y la de broadcast estarán todos los equipos de la subred.

## 5.4.6 EJERCICIO DE APRENDIZAJE 5

Divide la red 175.2.7.0 máscara 255.255.255.0 en 10 subredes

1. Comprobar si se pueden tener esas subredes con la configuración dada.

Si, si es posible tener las 10 subredes, porque hay suficientes bits a 0 en la máscara. Hay 8 bits a cero (y 28 es mayor que 10), como se puede observar en la mascará:

11111111.11111111.11111111.00000000

Los bits a 0 son los bits en verde. Esta máscara la ampliaremos para crear subredes, la ampliaremos cambiando ceros por unos de forma que volvamos a obtener una máscara que sea correcta.

2. Calcular el número de bits mínimo para las subredes.

Para tener las subredes que has especificado es necesario utilizar al menos 4 bits, porque 24=16 y este resultado es mayor o igual a 10 (que son el número de subredes que necesitas). Esos bits son los que deberás modificar para cambiar el número de subred.

Ahora, fíjate bien, a continuación, se expone la máscara origen indicando en verde los bits que serán utilizados para especificar (en la dirección ip) el número de subred:

11111111.11111111.11111111.00000000

3. Calcular la máscara ampliada.

Ahora, partiendo del calculo que se ha hecho en el paso de antes, calcular los bits reservados para indicar el número de subred, calculamos la máscara ampliada cambiando esos ceros reservados para subredes en unos, o lo que es lo mismo, los bits que se han marcado como verdes debemos convertirlos en unos. Tal y como se indica a continuación:

Máscara origen: 11111111.11111111.11111111.00000000 (255.255.255.0)

Máscara ampliada: 11111111.11111111.11111111.11110000 (255.255.255.240)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada (todas las mismas). Los unos en color verde de la máscara ampliada son los que tendremos que cambiar en la dirección IP para indicar el número de subred.

4. ¿Cuántos equipos habrá por subred?

Los ceros de la máscara ampliada son los que utilizaremos para indicar el número de host dentro de cada subred. Como puedes observar en la máscara ampliada, tenemos 4 bits reservados para indicar el número de host dentro de cada subred y esto nos permite tener 24-2 hosts por subred, o lo que es lo mismo, 14 hosts.

5. ¿Qué tenemos que modificar en la dirección de red?

Ahora, la máscara ampliada nos indica que bits podemos cambiar en la dirección de red. La dirección de red para la dirección ip que has indicado es: 175.2.7.0, con lo que según la máscara ampliada, los bits que modificaríamos sería:

```
Máscara ampliada: 11111111.11111111.11111111.11110000 - 255.255.255.240
Dirección de red: 10101111.00000010.00000111.00000000 - 175.2.7.0
```

Como puedes observar, los bits en rojo, son los que estaban de la máscara anterior, y esos no se podrán modificar, son intocables. Los bits en verde son los que modificaremos para indicar la subred, pero ojo, los

cambiamos en la dirección de red, no en la máscara ampliada, y los bits en azul los cambiamos para indicar la dirección del equipo.

6. Listado de las subredes que habría

A continuación, se muestran todas las subredes que se podrían crear con la configuración dada. Ten en cuenta que la dirección de subred indica el primer equipo de la subred y que la dirección de broadcast el último equipo de dicha subred. Además, ten en cuenta que todas las subredes tienen la misma máscara ampliada (255.255.255.240):

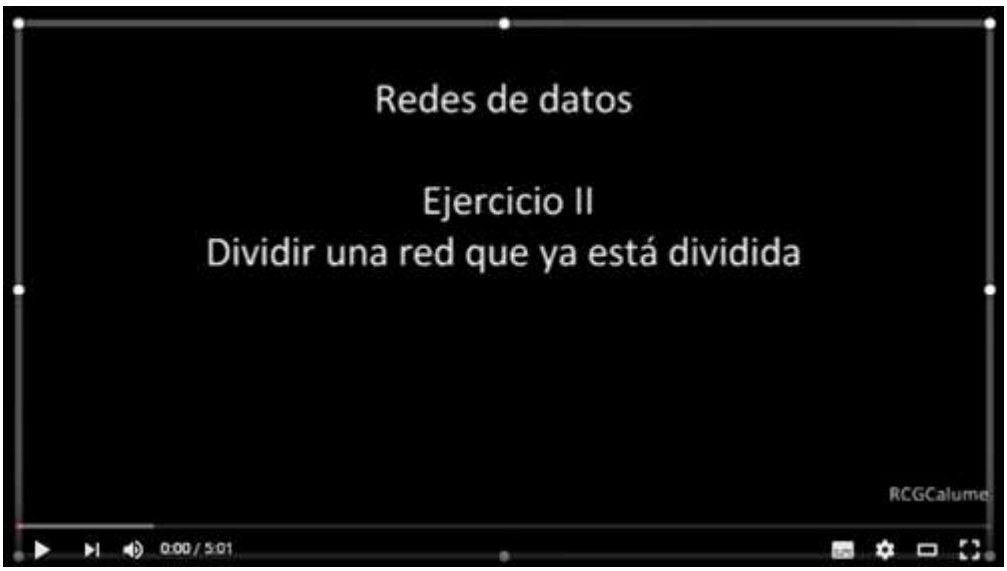
| Nº de Subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 175.2.7.0<br>(10101111.00000010.00000111.00000000) | 175.2.7.15<br>(10101111.00000010.00000111.00001111) |
| 1 | 175.2.7.16<br>(10101111.00000010.00000111.00010000) | 175.2.7.31<br>(10101111.00000010.00000111.00011111) |
| 2 | 175.2.7.32<br>(10101111.00000010.00000111.00100000) | 175.2.7.47<br>(10101111.00000010.00000111.00101111) |
| 3 | 175.2.7.48<br>(10101111.00000010.00000111.00110000) | 175.2.7.63<br>(10101111.00000010.00000111.00111111) |
| 4 | 175.2.7.64<br>(10101111.00000010.00000111.01000000) | 175.2.7.79<br>(10101111.00000010.00000111.01001111) |
| 5 | 175.2.7.80<br>(10101111.00000010.00000111.01010000) | 175.2.7.95<br>(10101111.00000010.00000111.01011111) |
| 6 | 175.2.7.96<br>(10101111.00000010.00000111.01100000) | 175.2.7.111<br>(10101111.00000010.00000111.01101111) |

| | | |
|---|---|---|
| 7 | 175.2.7.112<br>(10101111.00000010.00000111.01110000) | 175.2.7.127<br>(10101111.00000010.00000111.01111111) |
| 8 | 175.2.7.128<br>(10101111.00000010.00000111.10000000) | 175.2.7.143<br>(10101111.00000010.00000111.10001111) |
| 9 | 175.2.7.144<br>(10101111.00000010.00000111.10010000) | 175.2.7.159<br>(10101111.00000010.00000111.10011111) |
| 10 | 175.2.7.160<br>(10101111.00000010.00000111.10100000) | 175.2.7.175<br>(10101111.00000010.00000111.10101111) |
| 11 | 175.2.7.176<br>(10101111.00000010.00000111.10110000) | 175.2.7.191<br>(10101111.00000010.00000111.10111111) |
| 12 | 175.2.7.192<br>(10101111.00000010.00000111.11000000) | 175.2.7.207<br>(10101111.00000010.00000111.11001111) |
| 13 | 175.2.7.208<br>(10101111.00000010.00000111.11010000) | 175.2.7.223<br>(10101111.00000010.00000111.11011111) |
| 14 | 175.2.7.224<br>(10101111.00000010.00000111.11100000) | 175.2.7.239<br>(10101111.00000010.00000111.11101111) |
| 15 | 175.2.7.240<br>(10101111.00000010.00000111.11110000) | 175.2.7.255<br>(10101111.00000010.00000111.11111111) |

**Nota:** Observa que la única diferencia entre la dirección de red y la dirección de broadcast es que en la sección del número de host (los bits en azul), en la dirección de red son todos cero y en la dirección de broadcast son todo unos. Entre el rango comprendido entre la dirección de red y la de broadcast estarán todos los equipos de la subred.

Este video es un complemento valioso sobre Un  ejemplo de la división de redes


*REDESDIVIDIR01 Enlace*



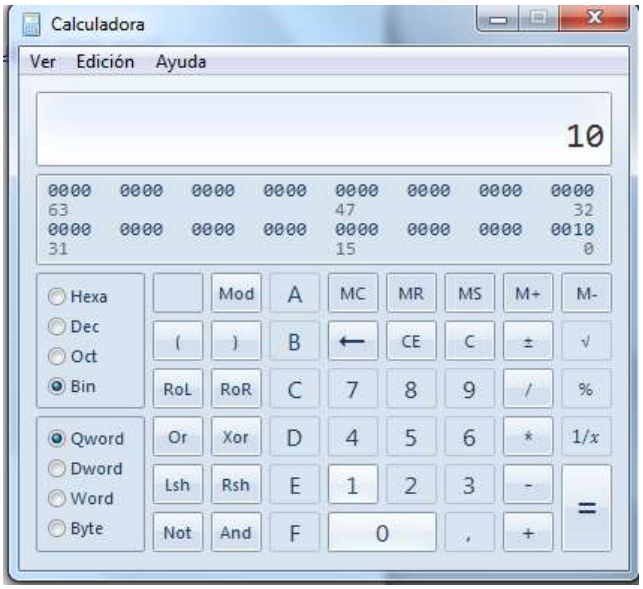

*REDESDIVIDIR02 Enlace*

## 5.4.7 HERRAMIENTAS CALCULO SUB REDES IP:

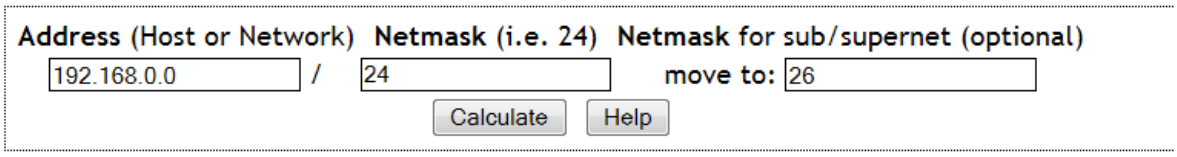
## 5.4.8 EJERCICIO DE APRENDIZAJE

Se requiere dividir la red 192.168.0.0 en 2 redes

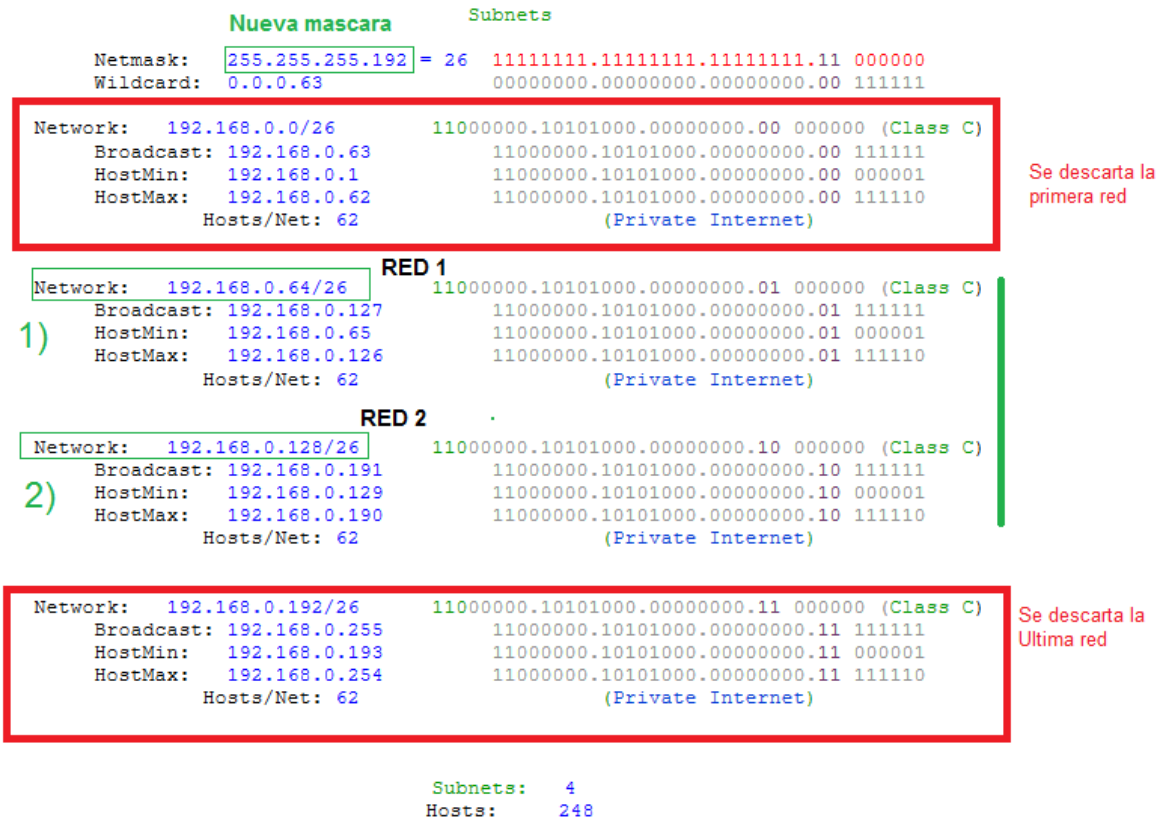
Usamos una calculadora para convertir el 2 (dos redes) en binario




Para esto se requieren 2 bits (10) se digita la red 192.168.0.0 como la máscara es 255.255.255.0 por ser una clase C esto indica /24 debe moverse a 26 pues la nueva máscara es la, máscara inicial + los bit nuevos en este caso 2 quedaría 24+2=26.




El software calcula las dos redes, la nueva máscara y el primer pc de la red (HostMin) el último PC(HostMax) y el broadcast.




## 5.4.9 EJERCICIO DE ENTRENAMINETO

1. Usando una calculadora IP divida una red 10.0.0.0 mascara 255.0.0.0 en 10 redes

2. Usando una calculadora IP divida una red 172.0.0.0 mascara 255.255.0.0 en 15 redes

Este video enseña la teoría y la práctica paso a paso como hacer una división de red empleado un lenguaje sencillo y de forma práctica, usando un ejemplo se explica todos y cada uno de los pasos realizados para dividir redes (subneting).


*Configuración RIP Enlace*

# 6 PISTAS DE APRENDIZAJE

**Recuerde que** Las arquitecturas de rede se dividen en capas

**Tenga presente que** el modelo OSI es un modelo de referencia y fue posterior a los modelos TCP/IP , DECNET y SNA. OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente

**Es necesario recordar que** las 7 capas del modelo OSI son: Fisica, Enlace, Red, Transporte, Sesión, Presentación y Aplicación

**Recuerde que** funcionalidad de las capas física y enlace en el modelo OSI corresponden a las capa de acceso a red en el modelo TCP/IP, de igual forma las capas de red e internet de ambos modelos son equivalentes al igual que las capas de transporte (tienen igual nombre en ambos modelos) por último la capa de aplicación del modelo TCP/IP corresponde a las capas Sesión, Presentación y aplicación el modelo OSI

El cable UTP (UNSHIELDED TWISTER PAIR):Es un cable compuesto por 4 pares de hilos trenzados, para un total de 8 hilos (**¡Error! No se encuentra el origen de la referencia.**), no es resistente a las interferencias externas, EMI o RFI, pues en su construcción no tiene mayas u otro elemento que lo proteja, ya que no es apantallado.

Existe una gran cantidad de cables de la familia de los pares trenzados TP (twister pair), entre ellos el UTP, STP, FSTP, S/FTP S/STP S/UTP; a continuación, encontraremos una reseña de cada uno.

Las fibras ópticas transmiten luz y no emiten radiaciones electromagnéticas que puedan interferir con equipos electrónicos, tampoco se ve afectada por radiaciones emitidas por otros medios, por lo tanto, constituyen el medio más seguro para transmitir información de muy alta calidad sin degradación. Las señales se pueden transmitir a través de zonas eléctricamente ruidosas con muy bajo índice de error y sin interferencias eléctricas.

El Cableado es el medio físico, cables y elementos complementarios a través del cual se interconectan dispositivos de para formar una red, un sistema de cableado es la infraestructura requerida para lograr la trasmisión de datos en forma confiable.

TIA (Telecommunications Industry Association) y la EIA (Electronic Industries Association) comenzó a desarrollar métodos de cableado de edificios, con la intención de desarrollar un sistema de cableado uniforme que apoyar los productos de múltiples fabricantes y entornos.

El tipo de cableado que el estándar TIA/EIA-568 específica para realizar la conexión de los armarios para el cableado entre sí en una LAN Ethernet con topología en estrella extendida se denomina cableado backbone

Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

**Ten presente que** Una dirección IPV4 (internet protocol versión 4) es un número único para cada computador dentro de una red que puede indicar dónde está un PC o al menos en que red se encuentra. Un ejemplo serio 219.113.4.2. mientras que una dirección IPV6 tiene una apariencia como 2001:0000:02AA:34FF:2567:11BC:23AC:00C2

Las direcciones ipv4 pueden direccionar 4.294.967.296 computadores mientras que ipv6 puede direccionar estas 340 sixtillones de direcciones (340 millones de millones de millones de millones de millones de millones).

# 7 GLOSARIO

100BaseFx: Especificación Fast Ethernet (IEEE 802.3) para fibra óptica en topología estrella.

100BaseTx: Especificación Fast Ethernet (IEEE 802.3) para cable multipar trenzado en topología estrella.

10Base-2: Especificación Ethernet (IEEE 802.3) que utiliza tipo de cable coaxial RG-58 muy económico y probado. Topología en bus.

10Base-5: Especificación Ethernet (IEEE 802.3) que utiliza cable coaxilRG-8 o RG-11, utilizado originalmente en la primera etapa de desarrollo. Topología en bus.

10Base-FL: Especificación Ethernet (IEEE 802.3) que utiliza fibra óptica en topología en estrella.

10Base-T: Especificación Ethernet (IEEE 802.3) que utiliza cable multípar trenzado en topología estrella.

## A

**ATM** ( Asynchronus Transfer Mode ): ATM es una tecnología de conmutación y multiplexado de alta velocidad, usada para trasmitir diferentes tipos de tráfico simultáneamente, incluyendo voz, video y datos.

## B

**Backbone:** Enlace troncal usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías.

**Bridge**: Dispositivo usado para conectar dos redes y hacer que las mismas funcionen como si fueran una. Típicamente se utilizan para dividir una red en redes más pequeñas, para incrementar el rendimiento.

**Bus Topology:** Topología de Bus: En una topología de Bus cada nodo se conecta a un cable común. No se requiere un hub en una red con topología de bus.

## C

**Cable Coaxil**: Se trata de un cable de cobre rodeado de aislación, un conductor secundario que actúa como ¨ tierra ¨ y una cubierta de plástico externa.

**Cable:** Conducto que conecta dispositivos de la red entre sí. El tipo de cable a utilizar depende del tamaño de la red y la topología de la misma.

## E

**Ethernet:** Ethernet fue desarrollado en PARC con la participación de

**Robert Metcalfe** fundador de 3Com, es un set de estándares para infraestructura de red.

## F

**Fast Ethernet:** Un nuevo estándar de Ethernet que provee velocidad de 100Megabits por segundo ( a diferencia de los 10 megabits por segundo delas redes Ethernet ).

**FDDI** ( FiberDistributed Data Interface): Interfaz de datos distribuidos por fibra óptica . Se trata de una red de 100 Megabits por segundo en topología en estrella o anillo muy utilizada en backbones, hoy desplazada por nuevas tecnologías como ATM.

**Firewall:** Una computadora que corre un software especial utilizado para prevenir el acceso de usuarios no autorizados a la red. Todo el tráficode la red debe pasar primero a través de la computadora del firewall.

## G

**Gateway:** Dispositivo utilizado para conectar diferentes tipos de ambientes operativos. Típicamente se usan para conectar redes LAN a minicomputadores o mainframes.

## H

**Hub:** Concentrador. Dispositivo que se utiliza típicamente en topología en estrella como punto central de una red, donde por ende confluyen todos los enlaces de los diferentes dispositivos de la red.

## I

**Internet:** Internet se define generalmente como la red de redes mundial. Las redes que son parte de esta red se pueden comunicar entre sí a través de un protocolo denominado, TCP/IP (Transmission ControlProtocol/ Internet Protocol).

**Intranet:** Las Intranets son redes corporativas que utilizan los protocolos y herramientas de Internet. Si esta red se encuentra a su vez conectada a Internet, generalmente se la protege mediante firewalls.

## L

**LAN:** Local Area Network o red de área local: Se trata de una red de comunicación de datos geográficamente limitada (no supera por lo general un radio de un kilómetro).

## N

**Network:** (red) Una red de computadoras es un sistema de comunicación dedatos que conecta entre si sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversostipos de redes.

**Network Interface Card:** Tarjetas adaptadoras ubicadas dentro de las computadoras que especifican el tipo de red a utilizar (Ethernet, FDDI, ATM) y que a través de ellas son el vínculo de conexión entre la computadora y la red.

**Network OperatingSystem:** Un sistema operativo que incluye programas para comunicarse con otras computadoras a través de una red y compartir recursos.

**Nodo:** Un dispositivo de la red, generalmente una computadora o una impresora.

## P

**Par trenzado:** Cable similar a los pares telefónicos estándar, que consiste en dos cables aislados "trenzados" entre sí y encapsulados en plástico. Los pares aislados vienen en dos formas: cubiertos y descubiertos.

**Protocolo:** Un conjunto de reglas formales que describen como se trasmiten los datos, especialmente a través de la red.

## R

**Repetidor:** Un dispositivo que intensifica las señales de la red. Los repetidores se usan cuando el largo total de los cables de la red es más largo que el máximo permitido por el tipo de cable. No en todos los casos se pueden utilizar.

**Router? Ruteador**: Dispositivo que dirige el tráfico entre redes y que es capaz de determinar los caminos mas eficientes, asegurando un alto rendimiento.

## S

**Server (servidor):** Sistema que proporciona recursos (por ejemplo, servidores de archivos, servidores de nombres). In Internet este términose utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la red.

**Star Ring Topology?** Topología Estrella: En las topologías Star Ring o estrella, los nodos radian desde un hub. El hub o concentrador es diferente dependiendo de la tecnología utilizada Ethernet, FDDI, etc. La mayor ventaja de esta topología es que si un nodo falla, la red continúa funcionando.

**Switch:** Un dispositivo de red capaz de realizar una serie de tareas de administración, incluyendo el redireccionamiento de los datos.

## T

**Token ring (red en anillo):** Una red en anillo es un tipo de LAN connodos cableados en anillo. Cada nodo pasa constantemente un mensaje de control ("token") al siguiente, de tal forma que cualquier nodo que tiene un "token" puede enviar un mensaje.

**Topología:** La "forma" de la red. Predominan tres tipos de tecnologías: Bus, Estrella y Anillo.

**TrascendNetworking:** Tecnologías de 3Com para la construcción de grandes redes corporativas. Consiste en tres elementos principales, rendimiento escalable, alcance extensible y administración del crecimiento.

## W

**WAN- Wide Area Network:** Red de área amplia: Una red generalmente construida con líneas en serie que se extiende a distancias mayores a un kilómetro.

# 8 BIBLIOGRAFÍA

*ccm.net*. (2015). Recuperado el 02 de 11 de 2015, de CCM: http://es.ccm.net/faq/2528-el-modelo-tcp-ip

Alfinal.com . (2015). *alfinal.com/*. Recuperado el 10 de 10 de 2015, de http://www.alfinal.com/Temas/tcpip.php

digitum. (2008). *digitum.um.es*. Recuperado el 2 de 11 de 2015, de digitum.um.es: https://digitum.um.es/xmlui/bitstream/10201/2855/1/AriasOrdoez.pdf

Kurose , J. F., & Ross W, K. (2010). *Redes de computadores.* España: Pearson.

Mansilla, C. M. (2015). *http://www.fca.unl.edu.ar/.* Recuperado el 10 de 11 de 2015, de http://www.fca.unl.edu.ar/: http://www.fca.unl.edu.ar/informaticabasica/Redes.pdf

Rojas , F. (2015). *felix-rojas.blogspot*. Recuperado el 2 de 10 de 2015, de http://felix-rojas.blogspot.com.co/2012/07/arquitectura-dra-o-decnet.html

TANENBAUM, A. (2003). *Redes de Computadores.* Mexico: PEARSON EDUCACIÓN.

Wikipedia. (2015). *wikipedia.org.* Recuperado el 1 de 10 de 2015, de wikipedia.org