UNIVERSIDAD NACIONAL DE EDUCACIÓN

Enrique Guzmán y Valle

*Alma Máter del Magisterio Nacional*

FACULTAD DE TECNOLOGÍA

Escuela Profesional de Electrónica y Telecomunicaciones

**MONOGRAFÍA**

# Protocolo de comunicación TCP/IP y ethernet

Examen de Suficiencia Profesional Res. Nº 0493-2018-D-FATEC

Presentada por:

**Sánchez Luis, Carlos Marx**

Para optar al Título Profesional de Licenciado en Educación

Especialidad: Telecomunicaciones e Informática

Lima, Perú

2018

**MONOGRAFÍA**

# Protocolo de comunicación TCP/IP y ethernet

Designación de Jurado Resolución N° 0493-2018-D-FATEC

**Dr. La Rosa Longobardi, Carlos Jacinto**

Presidente

**Dr. Niño Cueva, Danés Carlos Enrique**

Secretario

**Mg. Chirinos Armas, Daniel Ramón**

Vocal

Línea de investigación: Tecnología y soportes educativos

**Dedicatoria**

*A Dios, por acompañarme día a día.*

*A mis padres, por ser inspiradores de superación a mi vida.*

*A mis profesores, por su incondicional apoyo.*

## Índice de contenidos

# Lista de tablas

## Lista de figuras

# Introducción

TCP / IP fue creado e introducido por el Departamento de Defensa de los Estados Unidos. En 1972 y se conectó a ARPANET (Red de agencias de proyectos de investigación avanzada), que era la organización regional del Departamento de Defensa como un método de correspondencia para las diversas oficinas de los Estados Unidos. El cambio a TCP / IP en ARPANET se terminó en 1983.

El grupo de convenciones de Internet se conoce como la disposición de las convenciones del sistema que ejecuta la pila de convenciones en la que se basa Internet y que permiten la transmisión de información entre sistemas de PC.

Las dos convenciones más importantes que además fueron las primeras en caracterizarse y, además, las más utilizadas son TCP (Protocolo de control de transmisión o Protocolo de control de transmisión) e IP (Protocolo de Internet o Protocolo de Internet), por lo que también se alude como Protocolo TCP / IP Conjunto. Los tipos de convenciones existentes superan los cien, a los que podemos hacer referencia como los más conocidos HTTP, FTP, SMTP, POP, ARP, etc.

TCP / IP es la etapa que admite Internet y permite la correspondencia entre varios marcos de trabajo en varias PC, independientemente de si se trata de sistemas de vecindad (LAN) o de zona amplia (WAN).

Aún siguen diversos textos proponiendo controversias sobre si el protocolo TCP/IP de cinco niveles o capas, se encuentra dentro del modelo OSI (Interconexión de Sistemas Abiertos u OpenSystems Interconnection) el cual cuenta con siete niveles o capas.

En la presente monografía se abarca el modelo TCP/IP con sus cinco niveles o capas y cada una con sus protocolos más relevantes.

# Capítulo I

# Generalidades

## 1.1 Redes de computadoras

### 1.1.1 Definición.

Una organización de PC, conocida a la vez red de ordenadores o red informática, es una gran cantidad para hardware (PC y / o gadgets) asociados por enlaces, signos, ondas o alguna otra técnica para el transporte de información, que ofrece datos (registros), activos (CD -ROM, impresoras, etc.), administraciones (acceso web, correo electrónico, conversación, juegos) (Palet, 2007, p.56).

### 1.1.2 Clasificación de redes.

#### *1.1.2.1 Por alcance.*

Según su alcance existe el PAN (personal area network) conecta las PC y los periféricos en una pequeña zona, dentro de una casa o en el hogar" asi mismo el LAN (local área network) conecta computadoras y periféricos en un área que no supera los 200$m^2$, dentro de un edificio. Luego está el CAN (Campus Area Network) conecta computadoras y periféricos en un área geográfica limitada, como un campo militar o universitario, seguido por el MAN (Metropolitan Area Network) conecta computadoras y periféricos en un área geográfica amplia, ciudad o provincia,

finalmente tenemos al WAN (Wide Area Network) conecta computadoras y periféricos en un área geográfica muy amplia, países y continentes (Stalling, 2000, p.22).

Existen métodos de conexión para cada red y estos pueden ser medios guiados y medios no guiados.

Medios guiados como cable mellizos, coaxial, cable de par trenzado, cable UTP, fibra óptica y otros tipos de cables.

Medios no guiados como, radio, infrarrojos, microondas, láser, radio frecuencia, wifi y otros.

#### *1.1.2.2 Por el acceso de sus usuarios.*

Red pública: “Un sistema abierto se caracteriza por ser un sistema que cualquiera puede utilizar. Es un sistema de PC interconectadas, apto para compartir datos y que permite a los clientes impartir poca atención a su área de tierra.” (Andrew, 2003, p.56).

Red privada: “un sistema privado se caracterizaría como un sistema que debe ser utilizado por ciertas personas y que está diseñado con una palabra secreta individual” (Andrew, 2003, p.56).

### 1.1.3 Topología de una red.

La Topología de un sistema, es la situación de la interconexión entre los problemas principales y el servidor, existe tanto la topología astuta (la forma en que se controla el movimiento de la información), como la topología física en la tarea física de el cableado de la estructura (Palet, 2007, p.56).

Las topologías del marco físico más percibidas son tipo estrella, tipo bus lineal y tipo anillo.

### *1.1.3.1 Topología de estrella.*

Según Pérez (2001) Se organizan intercambios en los que todos los terminales están asociados con un centro focal, Hub o Switch, en el caso de que una de las PC no funcione, esto no influye en las demás, siempre que el "servidor" no esté inactivo.

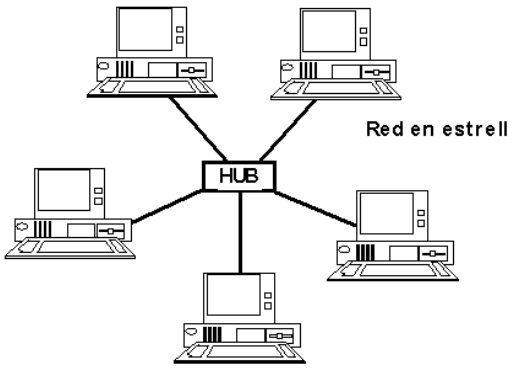



*Figura 1.* Topología de Estrella. Fuente: Pérez, 2001.

### *1.1.3.2 Topología bus lineal.*

Todas las PC están asociadas con un enlace focal, llamado "transporte" o "columna vertebral y los sistemas de transporte directo son los menos exigentes de introducir y, por lo general, son modestos, ya que nunca se volverán a utilizar a la luz del hecho de que se introdujeron en un enlace coaxial (Stalling, 2000, p.76).

### *1.1.3.3 Topología de anillo.*

Pérez (2001) señala que **“**Todas las PC o concentradores están asociados entre sí, formando una cadena o círculo cerrado” (p.99).

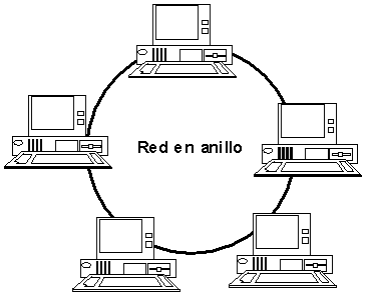



*Figura 2.* Topología de Anillo. Fuente: Pérez, 2001.

### *1.1.3.4 Árbol.*

"La topología en árbol También se llama topología de estrella diseminada. Al igual que en la topología en estrella, los dispositivos en la interfaz del sistema con un punto que es un cuadro de intersección, llamado HUB" (Palet, 2007, p.87).

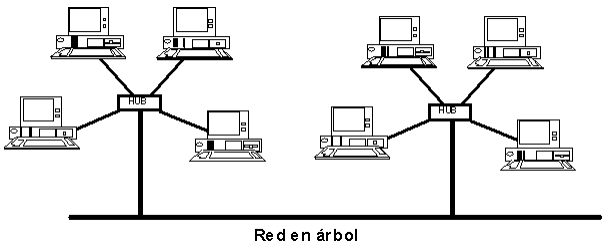



*Figura 3.* Topología en Árbol. Fuente: Pérez, 2001.

## 1.1.4 Componentes de una red.

Palet (2007) señala:

Servidor o server es la máquina principal del sistema, que se encarga de supervisar los activos del sistema y la progresión de los datos. Estación de trabajo (Workstation): Es una PC que está físicamente asociada con el servidor a través de algún tipo de enlace o medio, incluida la onda espiral o infrarroja. Sistema Operativo de Red: Es la interfaz (Software) que se encarga de gestionar y controlar en forma general el lan. Recursos a compartir: Cuando discutimos los activos para compartir, estamos discutiendo cada uno de esos dispositivos de equipo que tienen un gasto alucinante y que son innovadores o registros que la asociación desea transmitir a todos los trabajadores o ciertos representantes en una región (p.57).

# Capítulo II

# Introducción al TCP/IP

## 2.1 Acerca del TCP/IP

TCP / IP Es una colección para espectáculos estándar de la industria planificados para intercomunicar enormes marcos. (WAN = Wide Area Networks).

La abreviatura TCP / IP se origina en el Protocolo de control de transmisión / Protocolo de Internet.

Vamos a intentar dar en esta parte, algunas ideas sobre TPC / IP, su redacción y aclarar cómo la Internet Society hace el estándar de Internet.

### 2.1.1 El Proceso de estandarización de Internet.

Se desarrolla una reunión universal de voluntarios llamada Internet Society para hacer frente a la acumulación de convenciones TCP / IP. Los principios para TCP / IP se distribuyen en una progresión de registros llamada Solicitud de comentarios, o esencialmente RFC. Debemos recordar que Internet fue concebida como gratuita y procede como gratuita. Posteriormente, esta no es una asociación "propietaria" de Internet o sus avances. Ellos están a cargo de su ubicación.

#### *2.1.1.1 ISOC.*

"Internet SOCiety (ISOC) se creó en 1992 como una asociación mundial a cargo de las innovaciones de trabajo en Internet y las aplicaciones de Internet. Su diseño fundamental es apoyar la mejora y la accesibilidad de Internet" (Andrew, 2003, p.39).

#### *2.1.1.2 IAB.*

El IAB (Internet Architecture Board) es la reunión especializada de ISOC a cargo de las alternativas estándar de Internet, distribuyendo RFC y observando los formularios estándar de Internet.

La IAF organiza el IETF (Grupo de trabajo de ingeniería de Internet), IANA (Autoridad de números asignados de Internet) y el IRTF (Grupo de trabajo de investigación de Internet). El IETF elabora estándares y programas de Internet, y mira y responde a problemas específicos en Internet, IANA analiza y organiza el recado de un identificador único en Internet: las direcciones IP. La reunión IRTF se encarga de organizar todos los ejercicios relacionados con TCP / IP (Stalling, 2000, p.45).

### 2.1.2 Visión general de la Arquitectura TCP/IP.

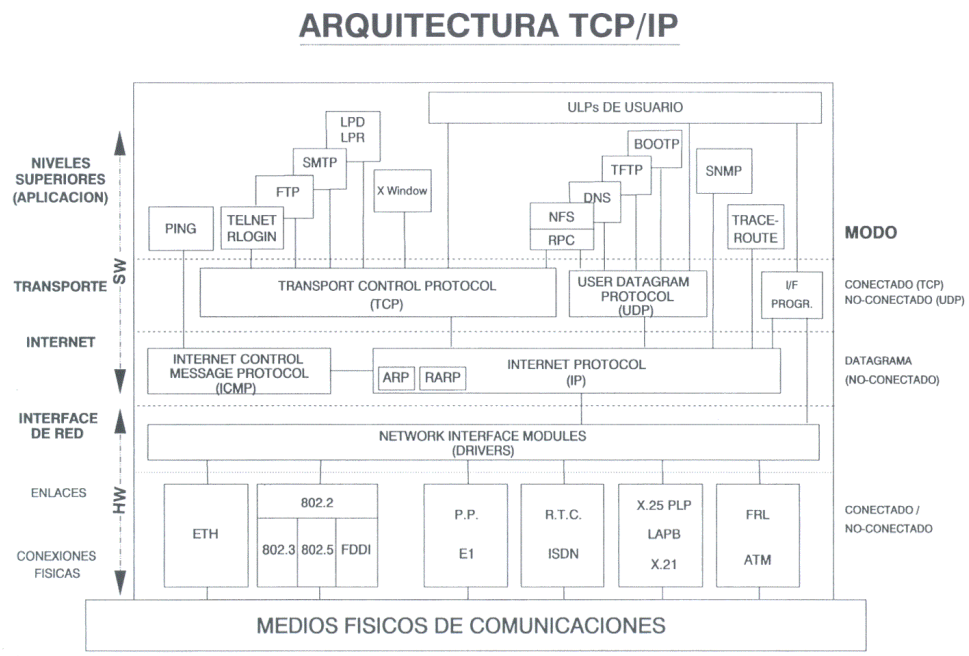



*Figura 4.* Arquitectura TCP/Ip. Fuente: Stalling, 2000.

### 2.1.3 El modelo de 4 capas.

"A pesar de que este modelo es general en todas las ejecuciones de TCP / IP, a lo largo de este archivo, nos adheriremos a su uso en Microsoft Windows" (James, 2001, p. 112).

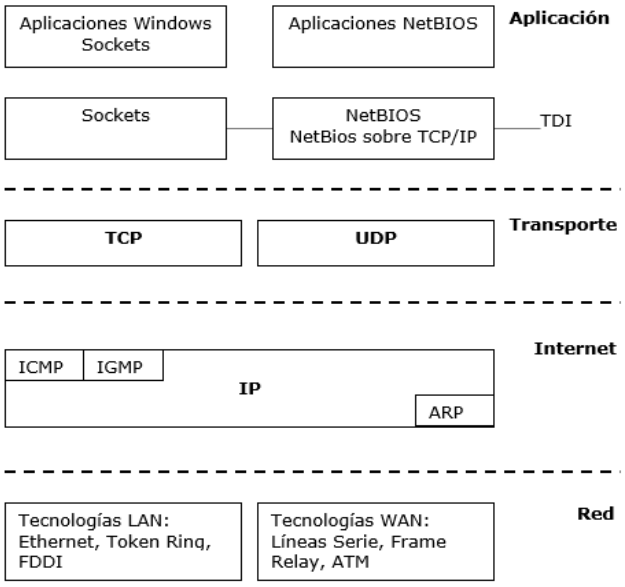



*Figura 5.* Modelo de 4 Capas. Fuente: James, 2001.

#### *2.1.3.1 Capa de red (Acceso a la Red)*.

La razón de este tipo de capa es la capa de interfaz de marco. Esta capa se encarga de enviar y tolerar sobres (estructuras o alrededores). En cualquier caso, comenzando ahora y en el futuro previsible, me gusta dejar la expresión en inglés, ya que generalmente se reconoce en la fraseología de PC), que son las parcelas de datos que movimiento en un cono organizar una 'unidad directa'. La capa del sistema envía tripas al sistema y recupera los contornos del sistema. (Andrew, 2003, p. 59).

#### *2.1.3.2 Capa de internet.*

La palabra datagrama no es una palabra castellana, sin embargo, se percibe adicionalmente en la redacción de la PC como 'paquete de datos' y esta capa también ejecuta todas las figuras de dirección de paquete (Andrew, 2003).

Los cuatro programas de Internet son: Protocolo web (IP), Protocolo de resolución de direcciones (ARP), Protocolo de mensajes de control de Internet (ICMP) y Protocolo de gestión de grupos de internet (IGMP) (James, 2001).

#### *2.1.3.3 Capa de transporte.*

“La capa del vehículo: nos da el grado de "sesión" en la correspondencia. Las dos convenciones de vehículos concebibles son TCP (Protocolo de control de transmisión) y UDP” (Andrew, 2003, p.76).

“TCP nos da una especie de disponibilidad "situada en asociación". Se utiliza regularmente para intercambiar mucha información a la vez. También se maneja en aplicaciones que necesiten "reconocimiento" o aprobación (ACK: afirmación) de la información obtenida” (James, 2001, p.98).

“El UDP Proporciona asociación de correspondencia y no garantiza el transporte de paquetes. Las aplicaciones que utilizan UDP envían regularmente cantidades modestas de información sobre el doble” (Palet, 2007, p.56).

#### *2.1.3.4* **Capa de aplicación.**

“En este modelo es la capa de aplicación. Esta es la capa que usan las aplicaciones para llegar al borde. Existen algunas utilidades y asociaciones en la capa de aplicación, por ejemplo: FTP, Telnet, SNMP y DNS” (Stalling, 2000, p.43).

# Capítulo III

# Acceso a la red

## 3.1 Tecnologías de interface de red

"La IP utiliza la garantía de gadget de marco (NDIS: interfaz de gadget de sistema específico) para enviar alojamientos a la capa de marco. IP fortalece los avances de LAN y WAN" (Stalling, 2000, p.78).

> Los desarrollos de LAN impulsados por TCP / IP consolidan los avances de Ethernet Token Ring (Ethenet II y 802.3), ArcNet y MAN (Red de área metropolitana), por ejemplo, interfaz de datos de fibra óptica (FDDI: interfaz de información transmitida de fibra) (Andrew, 2003, p.12).

"La utilización de TCP / IP en un área WAN puede requerir beneficios RAS aprobados, o incluso equipo adicional. Las dos clases principales de avances WAN fortificados son: líneas sucesivas y paquetes negociados" (Palet, 2007, p.45).

### 3.1.1 Protocolos sobre líneas serie.

El TCP / IP se envía en las líneas consecutivas incorporadas con los programas SLIP (Protocolo de Internet de línea serie) o bajo PPP (Protocolo de punto a punto). Este último caso es el que usamos con mayor frecuencia cuando utilizamos cualquier módem para cooperar con Internet (Palet, 2007).

Según Stalling (2000) SLIP es un estándar de la industria hecho a mediados de la década de 1980 para ayudar a TCP / IP en contornos de baja velocidad, utilizando máquinas RAS de Windows NT (o Windows 2000) que ejecutan Windows, pueden utilizar TCP / IP y SLIP para dar a máquinas remotas.

### 3.1.2 ARP.

El ARP (Protocolo de resolución de direcciones), es una parte de las capas TCP / IP, adquiere direcciones de equipos de las máquinas situadas en el sistema físico equivalentes (James, 2001).

ARP Se encarga de obtener las ubicaciones de los equipos de las máquinas TCP / IP en los sistemas que dependen de la 'comunicación'. ARP utiliza una comunicación cercana de la dirección IP del objetivo para encontrar la dirección del equipo de la máquina o puerta del objetivo. (Por puerta deberíamos comprender un interruptor - interruptor - o cualquier máquina que nos proporcione desde nuestra disposición de vecindario o nuestra sección de sistema cercana, a otras partes del sistema de vecindario a diferentes sistemas, por ejemplo, Internet) (Stalling, 2000).

Cuando el ARP obtiene la dirección del equipo, tanto la dirección IP como la dirección del equipo se guardan en un pasaje en la tienda ARP. ARP comprueba constantemente la tienda de ARP para una dirección IP antes de comenzar una solicitud por medio de comunicarse con el sistema (Stalling, 2000).

### 3.1.3 Resolviendo una dirección IP local.

Antes de que pueda producirse la correspondencia entre dos máquinas, la dirección IP de cada máquina debe construirse como una zona física (equipo). La técnica de

objetivo regional une una garantía ARP y una reacción ARP. Intentaremos aclararlo en el documento adjunto (Palet, 2007, p.78).

Ejemplo:

1) Una petición ARP Comienza cada vez que una máquina intenta hablar con otra. En el momento en que la IP confirma que la dirección IP está en el arreglo del vecindario.

2) En el caso de que no pueda descubrir el área en su propia reserva, ARP envía una solicitud con una consulta, por ejemplo, "Quién tiene esta dirección IP, envíeme la ubicación de su PC". Cada máquina en close by framework recibe el mensaje enviado y comprueba si se hace referencia a su propia dirección IP.

3) Al final, La máquina de objetivos comprueba que la solicitud coordina su propia dirección IP y envía una reacción ARP directamente a la máquina que menciona, ya que la dirección del equipo del abogado figura en el mensaje.

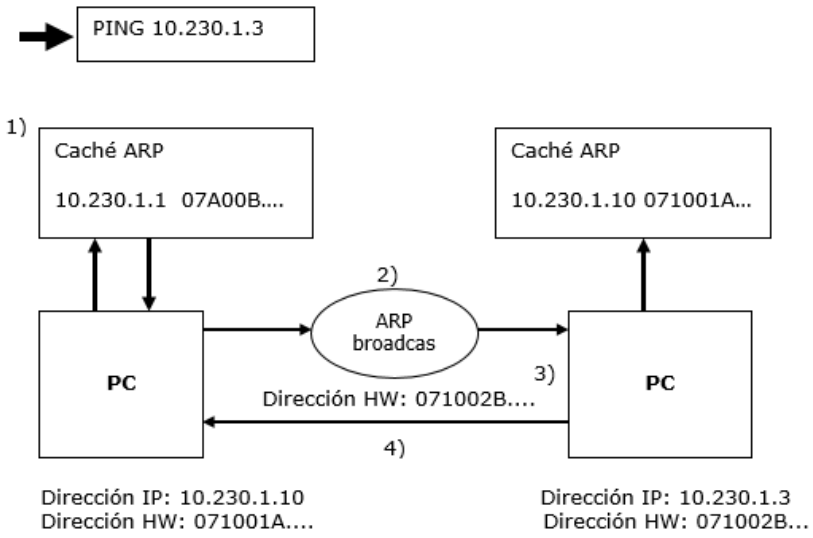



*Figura 6.* Resolviendo una Dirección IP Local. Fuente: Palet, 2007.

### 3.1.4 Resolviendo una dirección IP remota.

ARP Además, nos permite tener dos máquinas de varios contornos enseñados. En esta circunstancia, la demanda de ARP a través de la correspondencia es para el segmento

predeterminado y no para la dirección IP de la máquina objetivo. Es decir, la solicitud ofrecida es elegir el cambio que los datagramas pueden enviar a la máquina de meta en la carcasa. (Stalling, 2000, p.51).

Deberíamos ver el respaldo ejemplo:

1) Cuando Comenzamos la solicitud, la dirección del objetivo de IP se distingue por tener un lugar con un arreglo 'remoto'. La máquina de arranque comprueba su tabla de "cursos" para descubrir un camino hacia la máquina o hacia el objetivo de organizar.

2) Si no descubre una contraparte para la entrada, en ese momento se envía una solicitud ARP a través de la comunicación para la dirección de la puerta en lugar de para la ubicación de la máquina de gol. El conmutador reaccionará a la máquina fuente con 'su' dirección de equipo propia.

3) En el conmutador, la dirección IP del objetivo también se examina para verificar si es vecina o remota. En el caso de que sea una vecindad, el conmutador utiliza el método ARP (primero en la tienda y luego mediante comunicación) para adquirir la dirección de su equipo.

4) Después de la máquina de gol, la solicitud, esto reacciona con un mensaje de reacción ICMP.

5) Si la dirección del equipo de la entrada no está en la tienda ARP, una solicitud de comunicación lo obtendrá.

### 3.1.5 La caché ARP.

“Para tratar de limitar la cantidad de comunicaciones al sistema, el ARP mantiene constantemente el equipo realizado que se resolvió por primera vez. Broadcasting*”* (Andrew, 2003, p.78).

"En algunas ejecuciones TCP / IP cuando se utiliza un pasaje en la reserva ARP, se incluyen 10 minutos adicionales de vida. En Microsoft Windows, este componente no está actualizado" (Andrew, 2003, pág. 39).

### 3.1.6 ICMP e IGMP.

Si bien IP es el programa para enviar, ICMP (Protocolo de mensajes de control de Internet) nos informa sobre errores y mensajes de control para admitir IP. IP utiliza IGMP (Protocolo de administración de grupos de Internet) para iluminar los conmutadores que tienen (máquinas) de una reunión específica disponible en un marco (Perez, 2001, p.44).

#### *3.1.6.1 ICMP.*

"ICMP No espera transformar la IP en una convención segura y sólida. Simplemente imparte errores e informa condiciones explícitas. Los mensajes ICMP se envían como datagramas IP y, en este sentido, no son confiables en sí mismos" (Palet, 2007, p.77).

#### *3.1.6.2 IGMP.*

Es lo que podría contrastarse y los mensajes ICMP, sin embargo, entre conmutadores en lugar de entre máquinas en las que un host interviene en una de sus terminaciones.

Los mensajes IGMP se envían como datagramas IP y de esta manera no son sólidos en sí mismos.

IGMP se caracteriza en RFC 1112.

# Capítulo IV

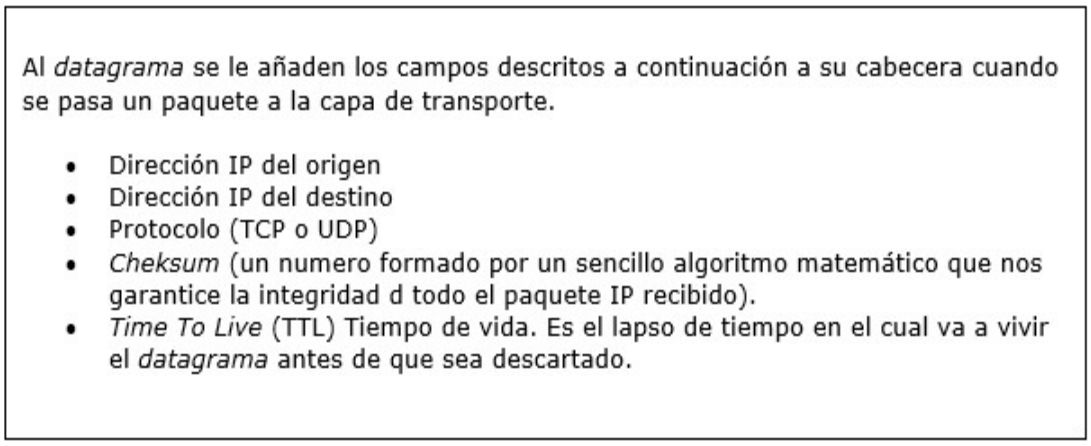
# Enrutamiento en la Internet

## 4.1 Encaminamiento IP

### 4.1.1 Protocolo IP.

IP Es el programa de afiliación fundamental responsable de enviar y coordinar paquetes entre máquinas (has), IP no reproduce una sesión antes de intercambiar información. El avance autorizado no es sólido, ya que funciona sin transmisión asegura. En el camino, un paquete se puede perder, cambiar en reuniones, duplicar, conceder o incluso cortar (James, 2001).

IP no requiere una correspondencia ACK (insistencia) cuando se adquieren los datos.


Al *datagrama* se le añaden los campos descritos a continuación a su cabecera cuando se pasa un paquete a la capa de transporte.

- Dirección IP del origen
- Dirección IP del destino
- Protocolo (TCP o UDP)
- *Cheksum* (un numero formado por un sencillo algoritmo matemático que nos garantice la integridad d todo el paquete IP recibido).
- *Time To Live* (TTL) Tiempo de vida. Es el lapso de tiempo en el cual va a vivir el *datagrama* antes de que sea descartado.

*Figura 7.* Esquema datagrama. Fuente: James, 2001.

#### *4.1.1.1 IP en el router.*

En el momento en que un conmutador obtiene un paquete, el paquete se pasa a la capa IP que hace el acompañamiento:

1) Disminución del campo TTL (Tiempo de vida) independientemente 1. En general, disminuirá en un agregado mayor si el interruptor está atornillado. En caso de que el TLL llegue al indicador de cero, el paquete será expulsado.

2) La IP puede aislar el paquete en pequeñas parcelas si la parcela es irrazonablemente larga para las líneas de ejecución del conmutador.

3) Si el paquete se está dividiendo, la IP crea otro encabezado para cada nuevo paquete al que se une.

4) El IP calcula los nuevos *cheksum.*

En el siguiente host, el paquete subirá en el stak (pila o capa normal) a TCP o UDP. Esta metodología se comparte nuevamente en cada cambio hasta que el paquete encuentre su objetivo definitivo, en este momento, el paquete llega a su último objetivo, el IP reunirá las reuniones como podría haber sido el paquete principal (Andrew, 2003, p.55).

#### *4.1.1.2 Estructuras de paquetes direccionales IP.*

Podemos observar campos del paquete IP en la versión cuatro del protocolo TCP/IP (versión actual) en las siguientes tablas:

Tabla 1
*Estructura del paquete IP*

| Campos | Funciones |
|---|---|
| Versión | Se utilizan 4 bits para indicar la versión del IP. Actualmente se usa mas la v4 que la v6. |
| Longitud de la cabecera | Se utilizan 4 octetos que indican el número de IP de 32 bits en la cabecera. |
| Tipo de Servicios | Se usa 8 bits indicando la calidad del servicio esperado por este datagrama para la comunicación a través de routers en la red. |
| Longitud total | 16 bits se usan para la longitud total conteniendo la cabecera del datagrama. |
| Identificación | 16 bits se usan para identificar este paquete. Si el paquete fuese fragmentado, todos los segmentos que estuviesen esta misma identificación serán usados para reensamblarlos en el host destino. |
| Protocolo | 8 bits serán usados para identificar el tipo de protocolo. |

*Nota:* Componentes y partes de una IP. Fuente: Andrew, 2003.

### *4.1.1.3 Cabecera IP.*

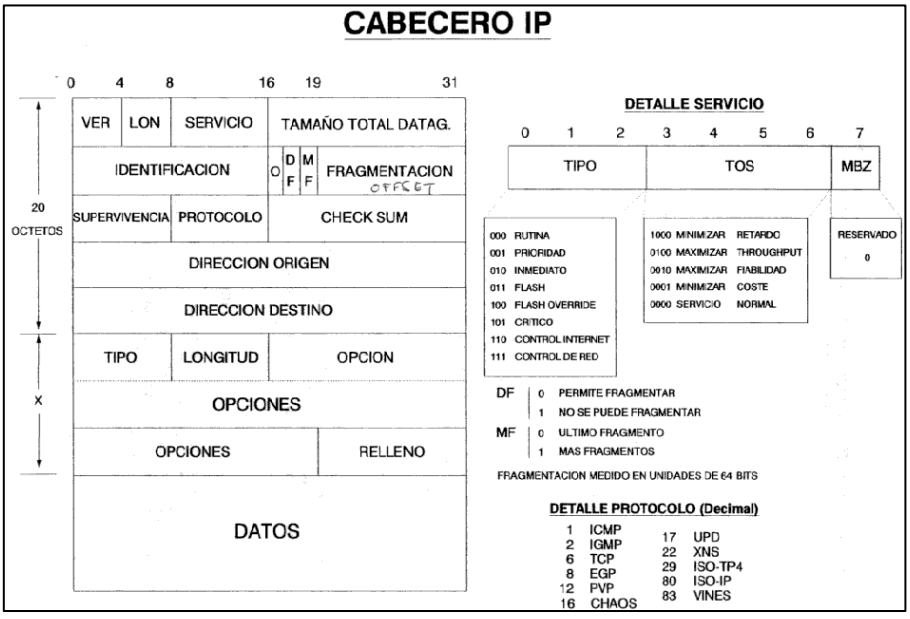



*Figura 8*. Cabecera IP. Fuente: Andrew, 2003.

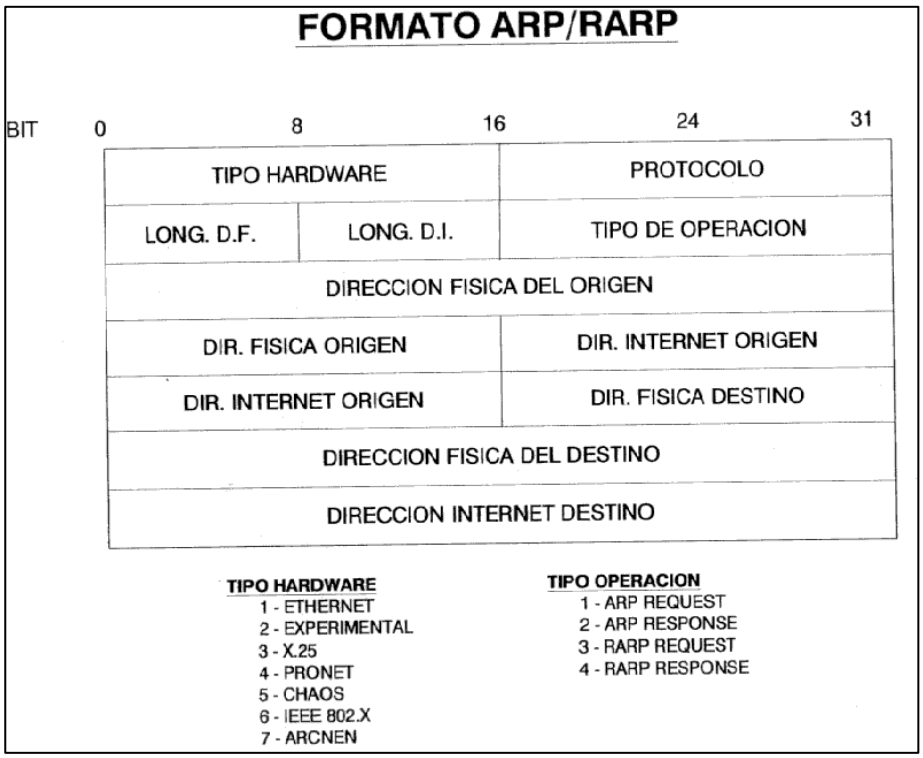



*Figura 9.* Formato ARP/RARP. Fuente: Andrew, 2003.

### 4.1.2 Direccionamiento y enrutamiento de IP.

#### *4.1.2.1 La dirección IP.*

La dirección IP distingue el área de un marco en el sistema. Es comparable a una dirección de carretera y número de entrada. Es decir, es único en su clase. Dos bulevares con un nombre y números de entrada similares no pueden existir en una ciudad similar, cada dirección IP tiene dos secciones. Uno de ellos reconoce la RED y los diferentes distinguen la máquina dentro de la que se organizan. Todas las máquinas que tienen un lugar con un sistema similar requieren un número similar de RED, que también debería ser especial en Internet.

##### *4.1.2.1.1 Identificación de red e identificación de host.*

Hay dos asociaciones con aludir a una dirección IP, método paralelo y disposición decimal con contactos. Cada dirección IP tiene 32 bits de longitud y se compone de 4 campos

de 8 piezas, llamados bytes u octetos. Los octetos son guardados por contactos y cada uno de ellos habla con un número decimal en algún lugar dentro del alcance de cero y 255. Los 4 octetos, es decir, de los 32 bits de una IP una parte identifica la red y otra parte identifica los hosts para ser ubicado en la red (Stalling, 2000).

"El método menos mencionado para intentar leer con cautela una dirección IP para personas es mediante la utilización de documentación decimal con motas" (Perez, 2001, p.34).

Veremos debajo de un caso de una dirección IP en binario y decimal con puntos:

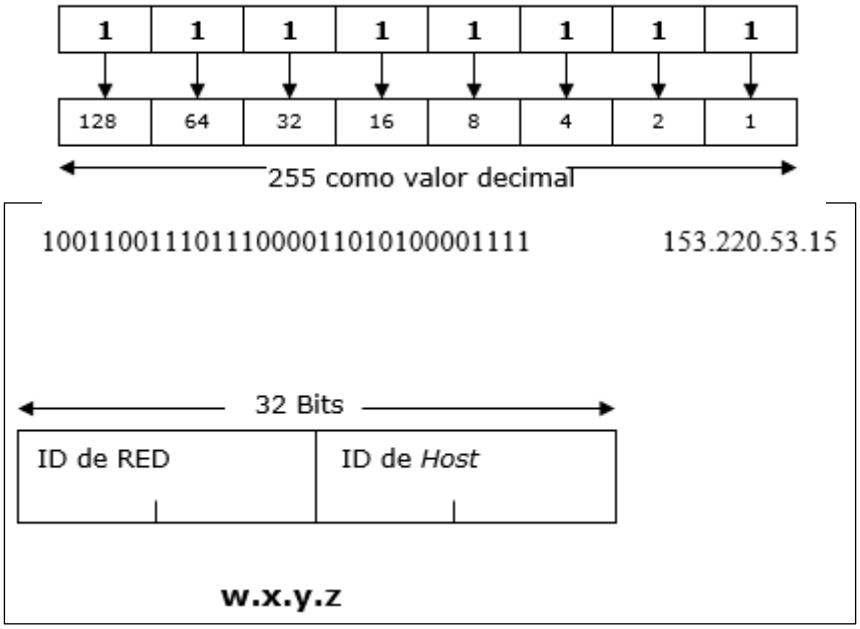



*Figura 10.* Identificación de Red y Host. Fuente: Stalling, 2000.

*4.1.2.1.2Convirtiendo direcciones IP de binario a decimal.*

La IP contiene 32 Bits divididos en 4 octetos de 8 bits cada uno, para cambiar los rumbos de doble a decimal, recuerde que cada bit de un octeto tiene un valor decimal, cuando convertimos cada pieza en un curso de acción decimal, la evaluación más llamativa de un octeto es 255 (Tanenbaum, 2015).

Un método rápido para cambiar de doble a decimal y viceversa es calcular Windows.

### *4.1.2.2 Clases de Direcciones.*

"Hay dos tipos distintos de direcciones IP. Cada clase retrata la parte de la dirección IP que separa la RED y la parte que percibe la cantidad de hosts dentro de esa disposición" (James, 2001, p.91).

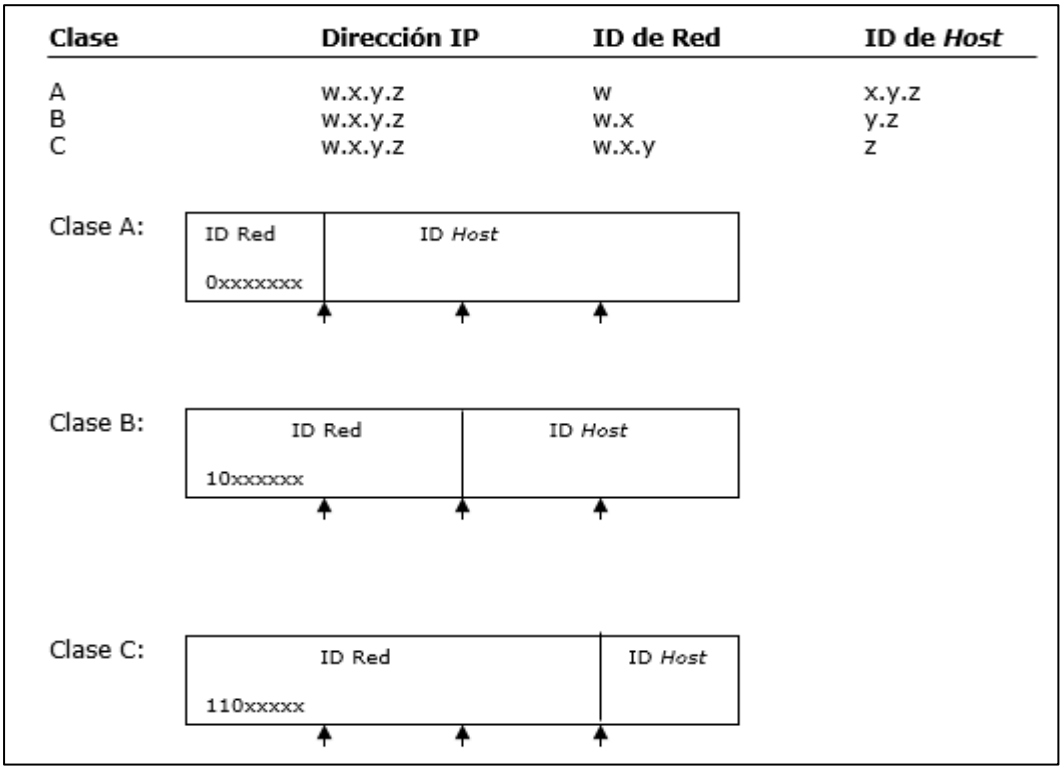



*Figura 11*. Clases de Direcciones. Fuente: James, 2001.

Clase An, son direcciones del tipo w.x.y.z donde 'w' habla a la RED y x.y.z el número de host dentro del sistema. En la tabla adjunta podemos ver las clases A, B y C.

#### *4.1.2.2.1 Clase A.*

Las ubicaciones de clase A se asignan para bordes con un número colosal de hosts. El bit de solicitud más sorprendente en una región de clase A es constantemente cero. Los siguientes 7 bits implican que el octeto central es la prueba ROJA. El resto de los

24 bits (los últimos 3 octetos) hablan con el número de host. Esto permite un total de 126 cajas y alrededor de 17 millones de hosts para cada caja (Palet, 2007, p.78).

*4.1.2.2.2 Clase B.*

Los métodos de clase B para vehículos se distribuyen para bordes de tamaño medio /enorme, los dos bits ocultos del octeto fundamental de los dominios de clase B son confiablemente 1 0. Los siguientes 14 bits que totalizan los dos octetos básicos son la prueba conspicua de la RED, el resto de los 16 bits de los últimos dos octetos hablan con el ID del host Esto propone 16,384 afueras y alrededor de 65,000 ha en cada borde (Stalling, 2000, p.45).

*4.1.2.2.3 Clase C.*

Clase C Se utiliza para pequeñas LAN (vecindario). Los tres bits principales del octeto guía adolescente son fuertes 1 0. Los siguientes 21 bits que incorporan los 3 octetos esenciales abordan la prueba prominente de una asociación de clase C. Los últimos 8 bits (último octeto) abordan la afirmación indiscutible del have (Palet, 2007).

*4.1.2.2.4Clase D.*

Las zonas de clase D se utilizan para el uso de acumulación de multidifusión. Una reunión de multidifusión puede incluir un anfitrión o ninguno de ellos. Los 4 bits de solicitud más impactantes en el octeto básico en una clase D son confiables 1 0. El resto de los bits administra la reunión particular donde el cliente queda cautivado (Andrew, 2003, p.76).

*4.1.2.2.5 Clase E.*

Las clases E son de tipo exploratorio y no son accesibles para uso general y se guardan para algún tiempo posterior. Los 4 bits del byte de solicitud más sorprendente en una clase E se establecen constantemente a 1 1 1 1 (Perez, 2001, p.42).

### *4.1.2.3 Principios de Direccionamiento.*

No hay principios para repartir las direcciones IP. De esta manera, se deben seguir ciertos estándares para garantizar que se relegue un número de ID de host y RED legítimo.

¿Qué tal si percibimos cómo asignar direcciones IP en una situación ROJA?

Hay algunas reglas que deben seguirse para asignar una identificación de red e identificaciones de host.

*4.1.2.3.1Asignando Identificaciones de RED.*

Se requiere un número NET extraordinario para cada sistema y asociaciones de territorio amplio. En el caso de que nos estemos asociando libremente a Internet, deberíamos obtener una prueba reconocible del sistema del 'Centro de información de red web' (InterNIC). En el caso de que no planeemos una interfaz abierta a Internet, podemos elegir cualquier número o ID de sistema sustancial según lo indicado por las premisas anteriores.

En caso de que nuestro sistema esté asociado por conmutadores, se requiere un nuevo número de RED para cada asociación de región amplia.

Por ejemplo, en el siguiente dibujo:

- Redes 1 y 3, representas dos redes conectadas – encaminadas: *routed.*
- Red 2 representa la conexión WAN entre los *routers.*

- La Red 2, requiere una identificación de RED que haga de interface entre los dos routers.

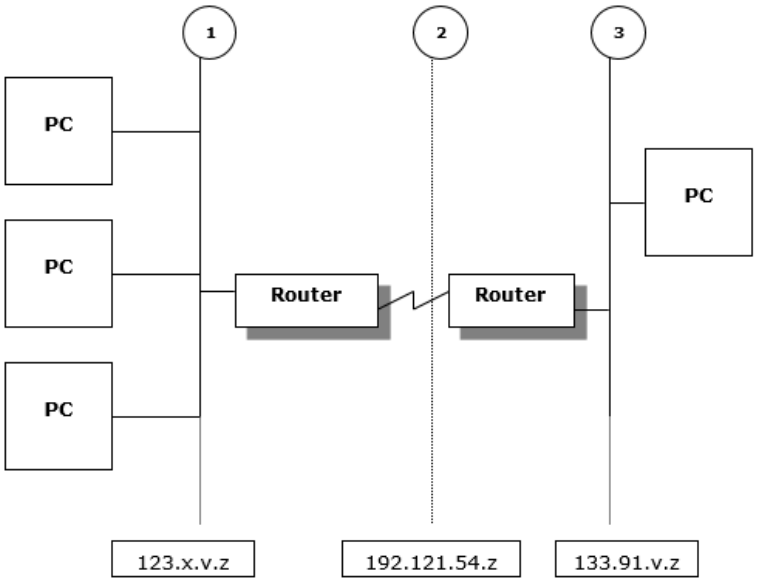



*Figura 12.* Asignando Identificaciones de Red. Fuente: Perez, 2001.

*4.1.2.3.2Asignando ID a los hosts.*

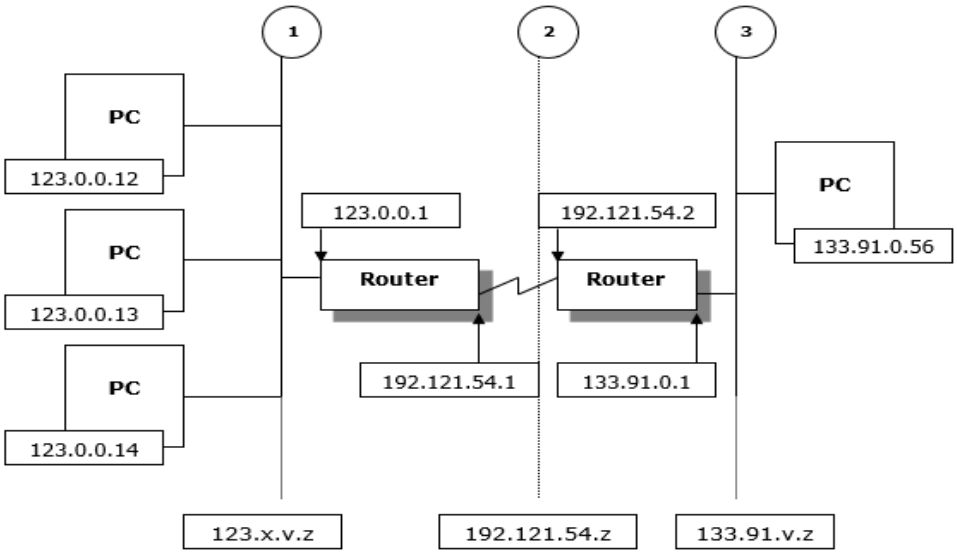



*Figura 13.* Asignando ID a los Hosts. Fuente: Perez, 2001.

Un número de host (tiene una ID) ve un TCP / IP en una RED y debe ser notable para esa ID de RED. Cada uno de los TCP que tienen, incluidas las interfaces para

los conmutadores, requieren una prueba particular cautivadora. La ID del interruptor es la dirección IP planificada como la estación de trabajo de entrada predeterminada. (Stalling, 2000, p.198).

En el modelo anterior, para el host 123.0.0.13, su portal predeterminado sería 123.0.0.1.

Los rangos a usar para asignar ID de *hosts* en una red privada se puede observar mejor en la tabla:

Tabla 2
*Identificaciones de hots válidas.*

| Clase | Inicio | Fin |
|---|---|---|
| A | W.0.0.1 | W.255.255.254 |
| B | W.X.0.1 | W.X.255.254 |
| C | W.X.Y.1 | W.X.Y.254 |

*Nota:* Distribución de los octetos según la clase de IP. Fuente: Andrew, 2003.

*4.1.2.3.3Sugerencias para asignar números de hosts.*

"La metodología más competente para asignar una impresionante dirección IP. Puede, por ejemplo, numerar todos los hosts continuamente o puede designar un número que pueda percibirse adecuadamente" (James, 2001, p.66).

### 4.1.3 Máscaras de red y dirección IPh.

"Cada host en un marco TCP / IP requiere una capa de marco (propagación de subred). Veremos la inspiración que impulsa una máscara de red y cómo es una parte del método que utiliza la IP para enviar paquetes" (Andrew, 2003, p.54).

Una extensión de marco es una dirección de 32 partes que se utiliza para "guardar" una parte de la dirección IP para percibir la prueba que distingue el marco de la ID del host. Esto

es fundamental con el objetivo que TCP / IP puede elegir cuando una dirección IP tiene un lugar en el marco cercano o en un marco remoto (Perez, 2001).

#### *4.1.3.1 Máscaras de red por defecto.*

Se utiliza un velo de sistema predeterminado en los sistemas TCP / IP cuando no están subredes. Todos los hosts TCP / IP requieren esta cobertura, independientemente de si están en un fragmento de sistema solitario. La cobertura predeterminada que podemos utilizar se basa en la clase 'dirección (Palet, 2007, p.76).

Tabla 3
*Máscaras de red por defecto.*

| Clase | 1 bit usado para la máscara de red y 0 bit asignado a host | Valor en decimal |
|---|---|---|
| A | 11111111 00000000 00000000 00000000 | 255.0.0.0 |
| B | 11111111 11111111 00000000 00000000 | 255.255.0.0 |
| C | 11111111 11111111 11111111 00000000 | 255.255.255.0 |

*Nota:* Distribución de la masca de red según la clase de IP. Fuente: Palet, 2007.

#### *4.1.3.2 Determinando el destino de un paquete.*

Un todo paralelo (AND) es el procedimiento interno que utiliza la IP para decidir cuándo un paquete está vinculado a un host cercano (en el vecindario se organiza) o remoto (en un sistema remoto). Dado que la IP utiliza el AND en el interior, no necesitaremos realizar este recado regularmente (James, 2001, p.45).

En el caso de que este resultado no coordine, el paquete se enviará a la ubicación de un interruptor o pasaje predeterminado.

En el caso de que los dos bits se establezcan en 1, el resultado es 1. En algún otro caso, el resultado es cero. Podemos verlo en la tabla adjunta:

Tabla 4
*Destino de Paquete.*

| Combinación de Bit | Resultados |
|---|---|
| 1 AND 1 | 1 |
| 1 AND 0 | 0 |
| 0 AND 1 | 0 |
| 0 AND 0 | 0 |

*Nota:* Tabla de valores para el operador AND. Fuente: James, 2001.

Como ejemplo:

| | | | | |
|---|---|---|---|---|
| Dirección de Red: | 10010110 | 11010000 | 00001011 | 11100010 |
| Máscara: | 11111111 | 11111111 | 00000000 | 00000000 |
| Resultado: | 10010110 | 11010000 | 00000000 | 00000000 |

### 4.1.4 Direcciones IP con la versión 6.0.

"Bajo la tendencia actual de 32 bits que se ejecuta en la adaptación 4.0 (IPv4), es raro organizar piezas de prueba distintivas (organizar ID). Deberíamos ver un poco cuál es el destino de las direcciones IP" (James, 2001, p.32).

El espacio de ubicación extendido es una de las principales características de Ipv6. IPv6 tiene 128 bits como áreas de origen y direcciones de destino (algunas veces más notables que IPv4). 128 bits pueden expresar cantidades de demanda de 3 * 10 elevadas a 38 ubicaciones (James, 2001, p.92).

En IPv6, un área puede ser del tipo:

4b3e: 23ed: f234: 452a: aec4: 32e2: 78ea: ff34

### 4.1.5 Subredes.

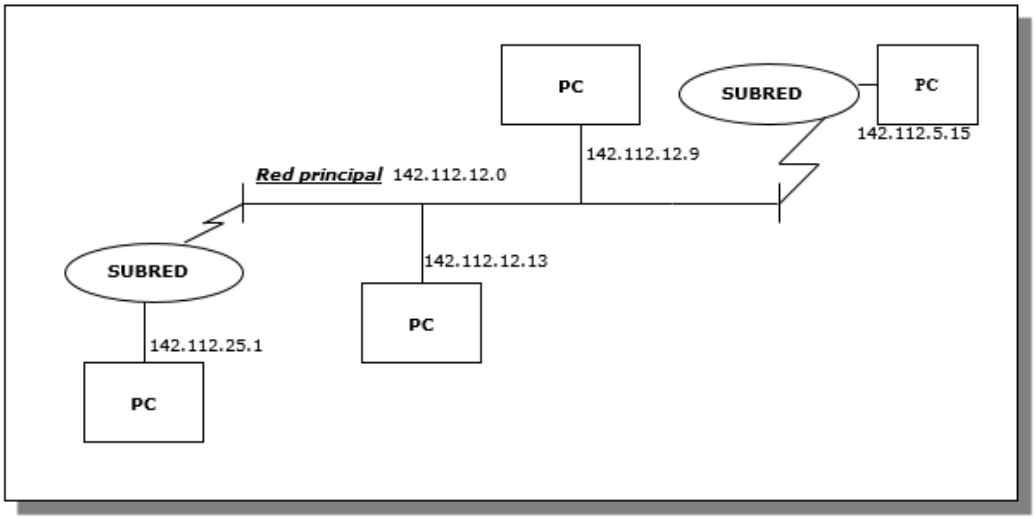



*Figura 14.* Sub Redes. Fuente: Palet, 2007.

#### *4.1.5.1 Introducción a las Subredes.*

Una subred es un fragmento físico de la condición TCP / IP que utiliza una dirección IP obtenida de una ID de sistema única. Tenga en cuenta que una organización o asociación tiene una identificación del sistema que la junta de InterNIC distribuye (Palet, 2007, p.56).

Se puede lograr múltiples beneficios al crear subredes:

Combine diferentes topologías de framework, por ejemplo, Ethernet y Token Ring.

Conquiste las restricciones de los avances contemporáneos, por ejemplo, superando el número más extraordinario de hosts por porción.

Educar la obstrucción organizada al desviar el tráfico y reducir broadcasting.

#### *4.1.5.2 Implementando las subredes.*

Antes de ejecutar subredes, se podra resolver las necesidades actuales y planificar los requisitos futuros. Esta lista de pequeños procedimientos nos puede controlar:

1) Determinar la medida de las partes físicas en nuestro marco.

2) Determine la cantidad de direcciones de host en cada parte física del marco. Cada host TCP / IP requiere independientemente de una dirección IP.

3) Según las multiples necesidades, caracterice:

• Una máscara de red que identifique todo el sistema

• Una ID de subred única para la parte física.

• Una identificación de host por cada subred.

#### *4.1.5.3 Máscaras de bits en las subredes.*

Antes de caracterizar una cubierta de subred, se sugiere decidir la cantidad de fragmentos y host por porción que necesitaremos más adelante, cuantos más bits usemos en las cubiertas de subred, incrementaran las subredes que serán accesibles, por ejemplo, aquellos modelos que se acompañan en la clase B demuestran la conexión entre la cantidad de bits y la cantidad de subredes y hosts (Palet, 2007, p.56).

3 bits = 6 subredes = 8000 hosts para cada subred (aproximadamente)

8 bits = 254 subredes = 254 hosts para cada subred.

La utilización de una cantidad mayor de bits de lo que normalmente sería apropiado nos permitirá construir la cantidad de subredes, sin embargo, limitará la cantidad de hosts en cada subred. En el caso de que los bits importantes se utilicen para las subredes actuales, nos permitirá expandir la cantidad de hosts, sin embargo, estaremos limitados a la cantidad de las primeras subredes caracterizadas (Andrew, 2003).

#### *4.1.5.4 Máscara de bits contiguos.*

Dado que las subredes se caracterizan por la cubierta de subred, el ejecutivo no está obligado a elegir los bits de solicitud más elevados para el velo de subred. En el

momento en que el problema de la subred se caracterizó por primera vez en RFC 950, se prescribió que se utilizaran bits de solicitud más altos como prueba reconocible de subred. Hoy, sea como sea, algunos vendedores de conmutadores refuerzan la utilización de solicitudes más bajas o incluso bits no ordenados en piezas de prueba (ID) distintivas de subred (Stalling, 2000, p.56).

#### *4.1.5.5 Tablas de Conversión.*

La subred de registros de la tabla adjunta cubre oficialmente cambiada a decimal utilizando un octeto para sistemas de clase A.

Tabla 5
*Conversión de clase A.*

| Número de Sub redes | Número de bits | Máscara de sub red | Nº de host para sub red |
|---|---|---|---|
| 0 | 1 | Inválido | Inválido |
| 2 | 2 | 255.192.0.0 | 4.194.302 |
| 6 | 3 | 255.224.0.0 | 2.097.150 |
| 14 | 4 | 255.240.0.0 | 1.048.574 |
| 30 | 5 | 255.248.0.0 | 524.286 |
| 62 | 6 | 255.252.0.0 | 262.142 |
| 126 | 7 | 255.254.0.0 | 131.070 |
| 254 | 8 | 255.255.0.0 | 65.534 |

*Nota:* Se usa esta tabla para generar la cantidad de sub redes que se desea. Fuente: Stalling, 2000.

La siguiente tabla muestra los tipos de máscaras de subred ya convertidas a decimal usando un octeto para las redes de clase B.

Tabla 6
*Conversión de clase B.*

| Número de Sub redes | Número de bits | Máscara de sub red | Nº de host para sub red |
|---|---|---|---|
| 0 | 1 | Inválido | Inválido |
| 2 | 2 | 255.255.192.016.382 | |
| 6 | 3 | 255.255.224.08.190 | |
| 14 | 4 | 255.255.240.04.094 | |
| 30 | 5 | 255.255.248.02.046 | |
| 62 | 6 | 255.255.252.01.022 | |
| 126 | 7 | 255.255.254.0.510 | |
| 254 | 8 | 255.255.255.0.254 | |

*Nota:* Se usa esta tabla para generar la cantidad de sub redes que se desea. Fuente: Stalling, 2000.

La siguiente tabla muestra los tipos de máscaras de subred ya convertidas a decimal utilizando un octeto para las redes de clase C.

Tabla 7
*Tabla de conversión de clase C.*

| Número de Sub redes | Número de bits | Máscara de sub red | Nº de host para sub red |
|---|---|---|---|
| 0 | 1 | Inválido | Inválido |
| 2 | 2 | 255.255.255.192 | 62 |
| 6 | 3 | 255.255.255.224 | 30 |
| 14 | 4 | 255.255.255.240 | 14 |
| 30 | 5 | 255.255.255.248 | 6 |
| 62 | 6 | 255.255.255.252 | 2 |
| 126 | 7 | Inválido | Inválido |
| 254 | 8 | Inválido | Inválido |

*Nota:* Se usa esta tabla para generar la cantidad de sub redes que se desea. Fuente: Stalling, 2000.

#### *4.1.5.6 Subredes utilizando más de un octeto.*

Hasta este punto, se ha utilizado un octeto dividido en sus 8 bits para representar la propagación de subred. Tarde o temprano, podría ser focal (y valioso), confinado en subredes, utilizar más de un octeto. Esto puede permitirnos una adaptabilidad progresivamente maravillosa en el territorio (Stalling, 2000, p.91).

Hay una forma más directa. Dado que las PC que estamos utilizando están en una Intranet, podemos utilizar una estructura privada. En este sentido, si elegimos esta condición para difundir una clase A del tipo de sistema privado 10.0.0.0, también podríamos estructurar la mejora de los requisitos previos de la afiliación (Stalling, 2000, p.77).

Tabla 8.
*Subredes utilizando más de un octeto.*

| ID de red | Máscara de sub red | En binario |
|---|---|---|
| 10.0.0.0 | 255.255.248.0 | 11111111.11111111.11111000.00000000 |

*Nota:* En el ejemplo se muestra una máscara de red de dos octetos y 5 bits. Fuente: Stalling, 2000.

Si usamos 13 bits para establecer una máscara de subred en clase A, podemos tener 8190 subredes y cada subred con una posibilidad de 2046 hosts.

### 4.1.6 Definiendo IDs de subred.

“Los identificadores de subred (ID) se caracterizan por utilizar un número similar de bits que se utilizan para caracterizar la mordida de subred. Hay dos técnicas únicas para caracterizar un alcance de ID de subred para un sistema en Internet” (James, 2001, p.78).

> Podemos caracterizar la ID de subred utilizando una cantidad similar de bits que utilizamos para el velo de subred. Estas posibles mezclas de bits los evaluarán y los convertirán a disposición decimal. Los avances que acompañan indican la mejor manera de caracterizar un alcance de ID de subred para un sistema en Internet (Palet, 2007, p.67).

1) Utilizando un número similar de bits que se utilizan para calcular la cobertura de subred, enumeramos cada combinación imaginable.

2) Disponemos de la considerable cantidad de cualidades que su sustancia es cada uno de los ceros o unos. Cada uno de los ceros o unos son direcciones IP no válidas, ya que cada cero específica "este sistema solo" y cada uno de ellos coordina la cobertura de subred.

3) Convierta las cualidades de cada subred a decimal. Cada valor decimal habla a una subred solitaria. Este valor se utilizará para caracterizar la extensión del host para esa subred.

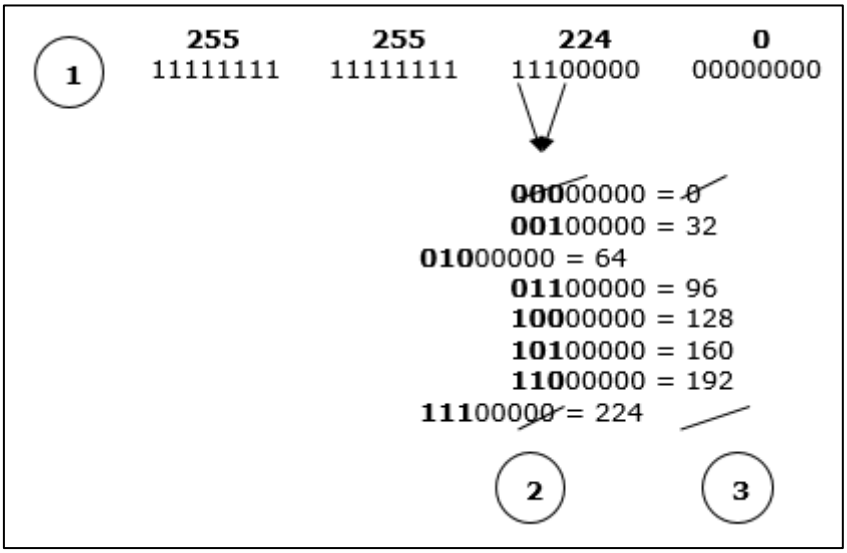



*Figura 15*. ID's de Subred. Fuente: Palet, 2007.

#### *4.1.6.1 Un caso especial de direcciones de subred.*

"Los ID de subred con cada uno de los ceros o todos en uno se conocen como ocurrencias excepcionales únicas de direcciones de subred. Al construir subredes, no se recomienda utilizar estas direcciones" (James, 2001, p.37).

### 4.1.7 Definiendo IDs de hosts en una subred.

"Podemos seguir una pequeña filosofía para elegir la cantidad de hosts por subred. A decir verdad, para la situación en que hemos retratado las ID de subred, para entonces hemos descrito con éxito las ID de host de cada subred" (Stalling, 2000, p.89).

La consecuencia de cada valor fijo que ya hemos visto demuestra el inicio de un alcance de ID de host. Sigamos con la figura de ejemplo:

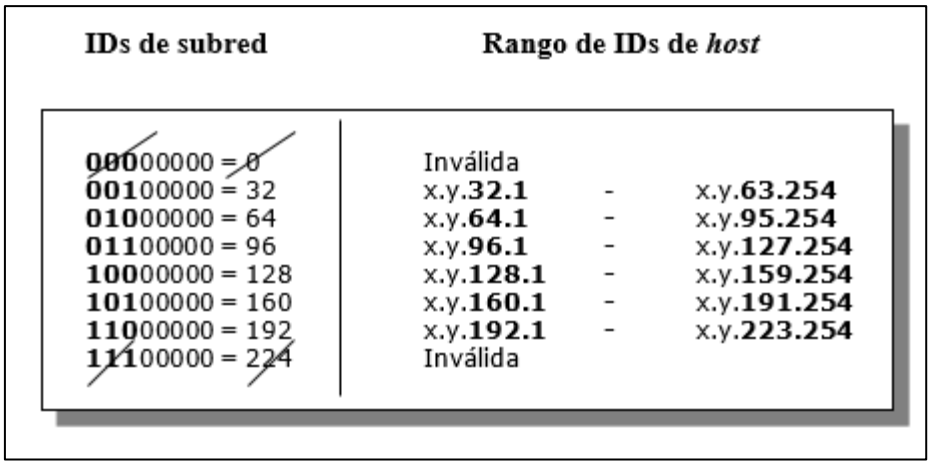



*Figura 16.* ID's de Hosts en una Subred. Fuente: Stalling, 2000.

#### *4.1.7.1 Como determinar el número de hosts por subred.*

1) Calcule la cantidad de bits abiertos para la ID del host. Por ejemplo, en el caso de que estemos en una dirección de clase B, que utiliza 16 bits para la ID del caso y 2 bits para la ID de subred, nos deja 14 bits para la ID del host.

2) Convierta la estimación doble de los bits de ID del host a decimal. Por ejemplo, 11111111111111 en doble (14 bits) es 16383 en organización decimal.

3) Restar 1.

### 4.1.8 Implementando routing de IP.

Routing (encaminar) Es la forma de elegir la forma en que se enviarán los paquetes. La dirección ocurre cuando enviamos paquetes a través de un interruptor a la luz del hecho de que el host objetivo no está en nuestro sistema, un interruptor es una máquina o dispositivo que avanza las parcelas comenzando con un sistema físico y luego al siguiente (Perez, 2001, p.35).

Sea como fuere, antes de enviar el paquete, debe hacerse la elección con respecto a dónde debe enviarse. Esta elección debe ser realizada por todos los hosts, ya sea nuestro propio host o cualquier switch a través del cual el paquete experimente, para

decidirse por la elección de dirección, la capa IP aconseja una tabla de curso que se guarda en la memoria (Perez, 2001, p.98).

Ofrézcanos la oportunidad de imaginar que nuestra máquina puede tener más de un conector de carcasa. Esta es la situación de los interruptores e incluso el caso de una PC doméstica, con una tarjeta de cubierta y con un módem (Perez, 2001, p.67).

1) Cuando un anfitrión espera hablar con otro anfitrión, la IP inicialmente decide si el objetivo es organizar el vecindario o en otro sistema.

2) Si el objetivo es un host remoto (está en otro sistema), la IP busca en la tabla del curso un curso concebible para encontrar el objetivo en el sistema remoto.

3) Si no hay un curso inequívoco, IP utiliza la entrada predeterminada para enviar el paquete al conmutador.

4) En el conmutador, una vez más, se aconseja su tabla de cursos, para seguir buscando un host remoto o un sistema.

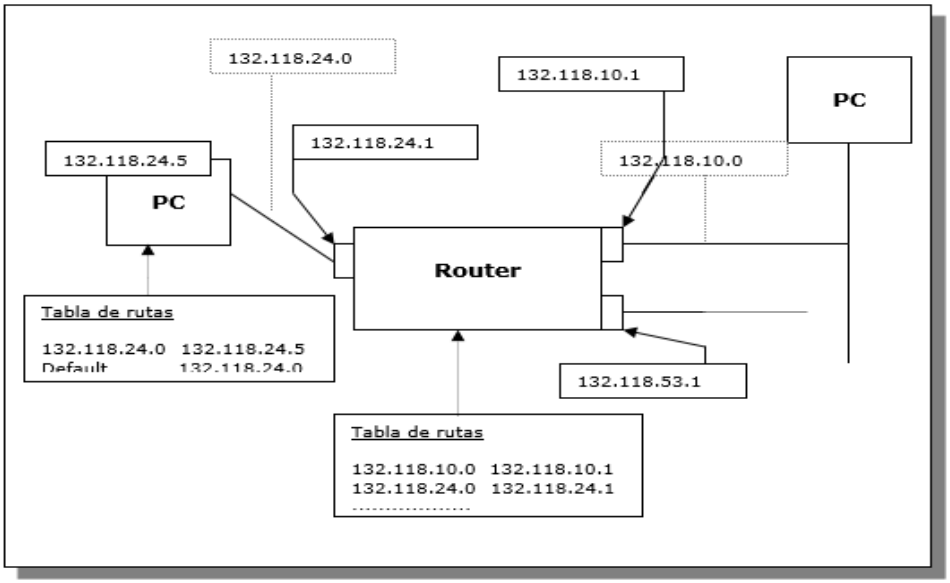



*Figura 17.* Implementando Routing de IP. Fuente: James, 2001.

Según James (2001) “a medida que descubrimos cada conmutador, el paquete se envía al siguiente conmutador. Esto se conoce como un salto” (p.56). Finalmente, el

paquete se transmite a la meta que tiene. En el caso de que no se descubra ningún curso, se envía un mensaje de error a la fuente.

#### *4.1.8.1 Detección de un Gateway muerto (dead gateway).*

TCP / IP TCP / IP envía un paquete a la puerta predeterminada hasta que recibe un ACK. En caso de que se supere el tiempo normal del parámetro de disposición TCP / IP TCP max data retransmissions y haya algunas entradas diseñadas en esa PC, el TCP / IP exige que la IP cambie a la siguiente puerta predeterminada.

#### *4.1.8.2 Encaminamiento (routing) de IP estático versus dinámico.*

La forma en que los conmutadores obtienen datos depende de si los conmutadores permiten la dirección IP estática o dinámica.

Los interruptores estáticos necesitan tablas de cursos para ensamblarse y actualizarse físicamente. En el caso de que cambie un curso, los interruptores estáticos no iluminan a nadie con respecto a este cambio, es decir, los interruptores estáticos intercambian datos con interruptores dinámicos.

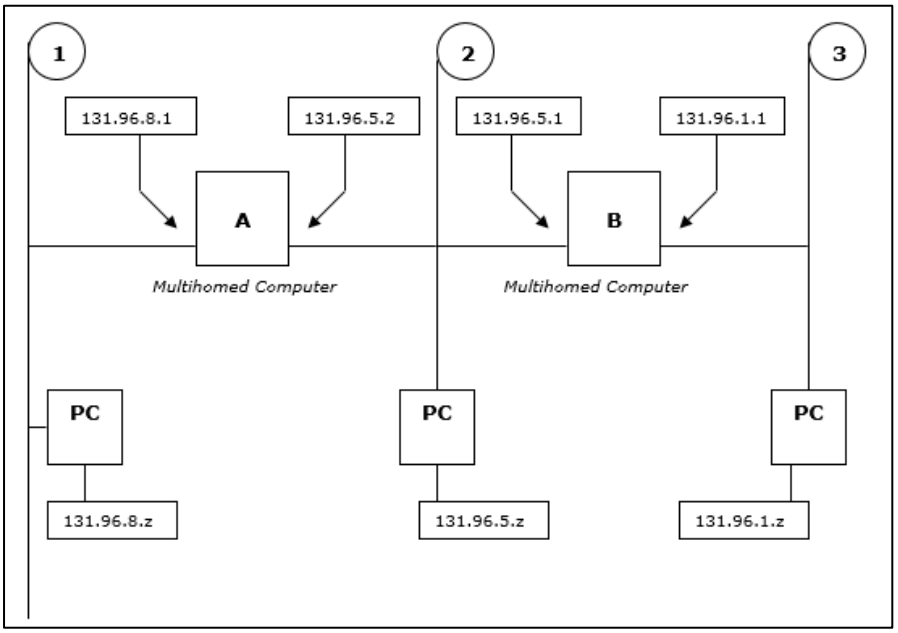



*Figura 18.* Enrutamiento Estático de IP. Fuente: Palet, 2007.

### 4.1.9 Enrutamiento estático de IP.

Para enviar paquetes IP a diferentes sistemas, debemos diseñar cada uno de los conmutadores estáticos de sistema. Deberíamos ingresar el diseño de conmutador y cambiar la tabla de cursos para cada sistema o subred de todos nuestros arreglos de trabajo (Stalling, 2000, p.78).

#### *4.1.9.1 Configurando los routers estáticos.*

"En una conexión de trabajo con, en cualquier caso, un interruptor estático, tenemos que diseñar el pasaje de la mesa de dirección de cada interruptor para que "aparezca" cada sistema conocido" (Palet, 2007, p.67).

Deberíamos adherirnos al modelo anterior y percibir cómo debemos diseñar cada uno de los interruptores A y B.

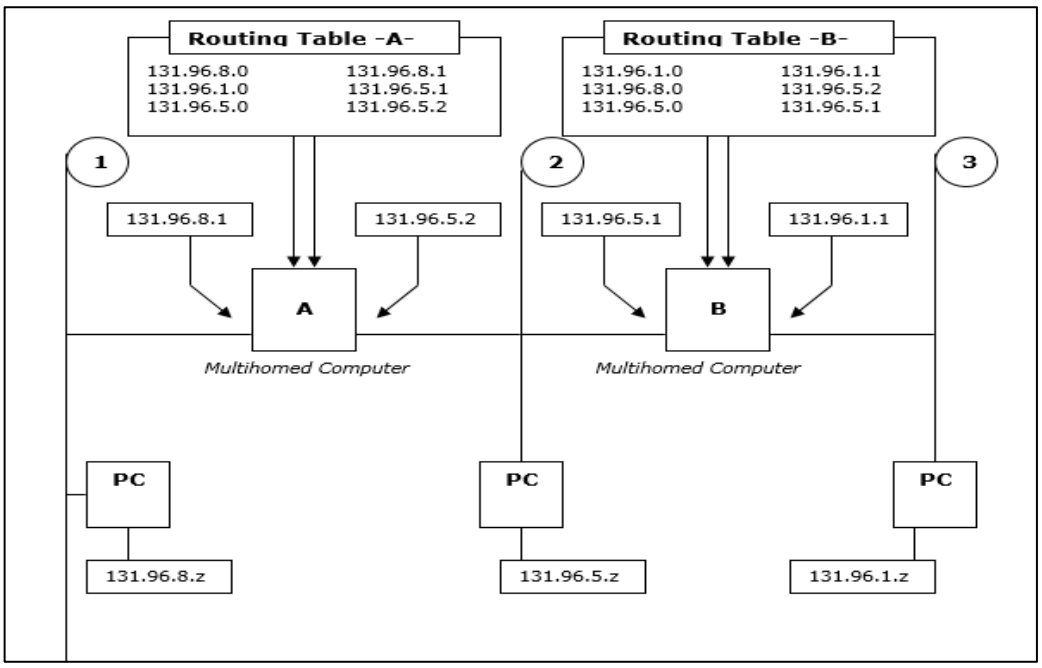



*Figura 19*. Configurando los Reuters Estático. Fuente: Palet, 2007.

### *4.1.9.2 Usando la dirección del Gateway por defecto.*

"Una de las estrategias para diseñar un conmutador estático sin agregar físicamente cursos a la tabla de cursos es organizar como la dirección de puerta predeterminada como la interfaz de vecindario de otra 'PC en el sistema básico" (Stalling, 2000, p.173).

### *4.1.9.3 Construyendo una tabla de rutas.*

Podemos agregar datos a la tabla del curso, utilizando el orden del curso. La dirección de impresión del curso se puede utilizar para ver los pasajes predeterminados en las tablas del curso, se debe agregar una información estática a los conmutadores estáticos de todos los sistemas en los que no está organizada otra interfaz (Andrew, 2003, p.56).

Una sección estática incorpora los siguientes:

- Dirección de red. El ID del sistema o el nombre del sistema del objetivo se organizan.

En el caso de que se utilice un nombre de sistema para caracterizar el objetivo, debe

encontrarse en el registro de 'Sistemas'. (Veremos estos problemas de objetivos de nombre en secciones posteriores).

- Máscara de red. El velo de subred para esa dirección del sistema.
- Dirección de la entrada. La dirección IP o el nombre de host de la interfaz de objetivo del sistema.

#### *4.1.9.4 Entradas por defecto en la tabla de rutas.*

"La tabla de rutas que mantiene Windows con las entradas por defecto lo podemos ver en la siguiente tabla" (James, 2001, p.56).

Tabla 9
*Entradas por defecto en la tabla de rutas.*

| Dirección | Descripción |
|---|---|
| 0.0.0.0 | Se usa predeterminada para aquellas direcciones que no se encuentran en la tabla de direcciones o rutas. |
| SUBNET BROADCAST | Aquella dirección usada para broadcasting en la subred local. |
| NETWORK BROADCAST | Aquella dirección usada para broadcasting a la red. |
| LOCAL LOOPBACK | Aquella dirección usada para pruebas de configuración de IP y conexiones. |
| LOCAL NETWORK | Aquella dirección usada para enviar paquetes de datos a los host en la red de área local. |

*Nota:* Direcciones asignadas de manera automática en la tabla de ruta. Fuente: James, 2001.

#### *4.1.9.5 Añadiendo entradas estáticas.*

Se puede usar la orden o comando **route** para agregar direcciones a la tabla de rutas.

Tabla 10
*Añadiendo entradas estáticas*

| Comandos | Función |
|---|---|
| Route add | Añadir una ruta. |
| Route -p add | Añadir una ruta persistente. |
| Route delete | Borrar una ruta. |
| Route change | Modificar un ruta. |
| Route print | Devuelve la tabla de rutas. |
| Route -f | Elimina todas las rutas. |

*Nota*: Procedimiento en comandos para poder configurar y asignar una IP a un host. Fuente: James, 2001.

### 4.1.10 RIP.

"La convención RIP (Protocolo de información de enrutamiento) para IP alienta el intercambio de datos de dirección en un arreglo de IP. Todos los mensajes RIP se envían bajo el puerto UPD 520" (Andrew, 2003, p.78).

RIP permite que los conmutadores intercambien datos sobre las ubicaciones de IP de los sistemas y la 'separación' de estos sistemas, el contador de saltos es la cantidad de interruptores que se deben cruzar para llegar a la meta. Los sistemas que necesitan al menos 16 rebotes se consideran "inaccesibles. (Stalling, 2000, p.67).

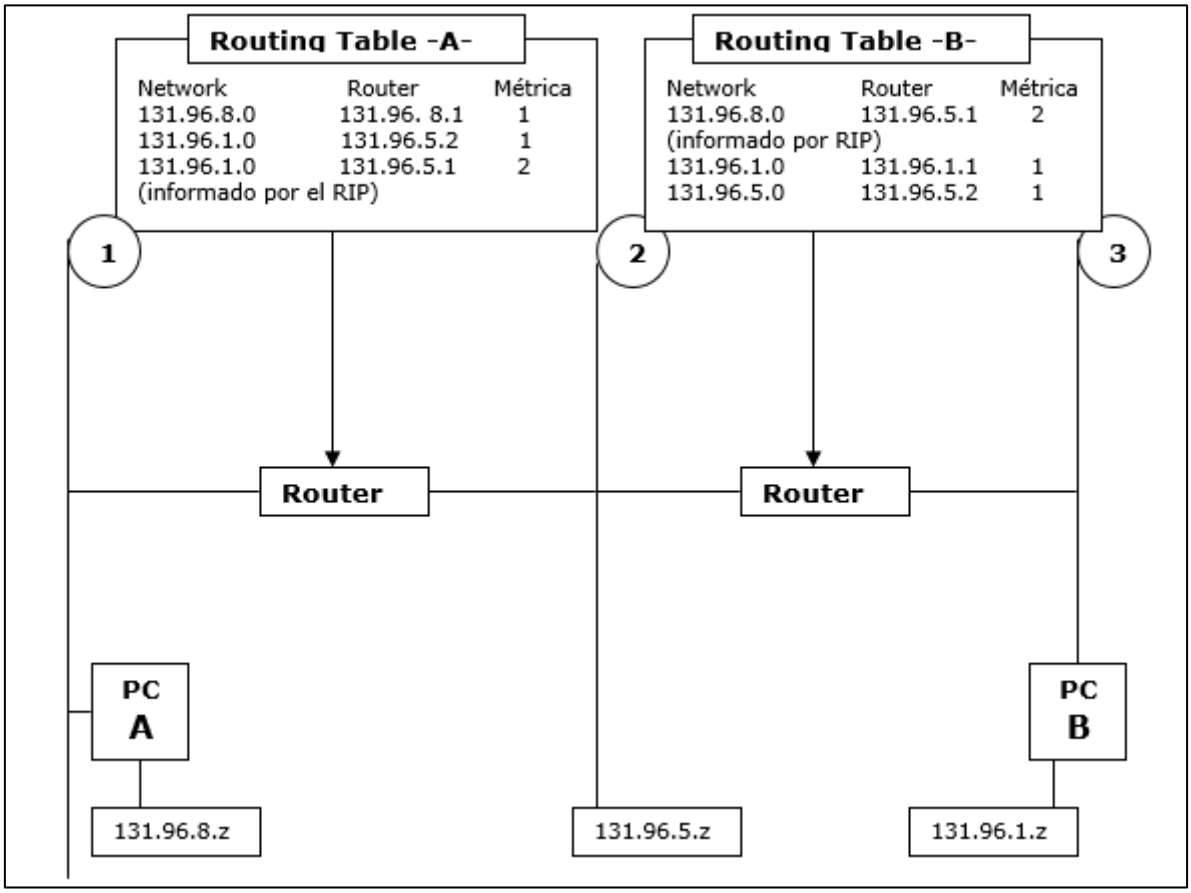



*Figura 20.* Protocolo RIP. Fuente: Palet, 2007.

El sistema adjunto muestra tres subredes asociadas con dos interruptores con la convención de dirección RIP habilitada. El conmutador A envía la comunicación para organizar 2, y todos los conmutadores RIP dinámicos en el sistema 2 informan esto para organizar 1. Los conmutadores también actualizan la tabla de rebote en caso de que encuentren un curso más corto (Palet, 2007, p.78).

# Capítulo V

# Transporte TCP y UDP

## 5.1 Servicios de transporte

### 5.1.1 Servicios proporcionados a las capas superiores.

Un objetivo definitivo de la capa del vehículo es proporcionar ayuda capaz, confiable y razonable a sus clientes, que normalmente son estrategias de capa de aplicación. Para lograr este objetivo, la capa del vehículo utiliza las organizaciones dadas por la capa del marco. El engranaje o la programación de la capa del vehículo que es responsable del vehículo se conoce como un componente del vehículo, que podría estar en el punto focal del esquema de trabajo, en una metodología alternativa, en un paquete de biblioteca o en la tarjeta del marco de referencia (Stalling, 2000, p.94).

### 5.1.2 Primitivas del servicio de transporte.

Para permitir que los clientes accedan a la administración del vehículo, la capa del vehículo debe dar algunas actividades a los programas de aplicación, es decir, una interfaz de administración del vehículo. La administración de cada vehículo tiene su propia interfaz. Para ver lo esencial, en este segmento analizaremos inicialmente una administración básica del vehículo y su interfaz (Palet, 2007, p.89).

La administración del vehículo es como la administración del sistema, sin embargo, hay algunos contrastes significativos. Los sistemas genuinos pueden perder paquetes, por lo que la administración suele ser problemática.

### 5.1.3 Sockets de berkeley.

"Esta es otra reunión de nativos de vehículos, los nativos utilizados en UNIX para TCP. En general, son básicamente los mismos que los anteriores, sin embargo, ofrecen más aspectos destacados y adaptabilidad" (Andrew, 2003, p.67).

### 5.1.4 Elementos de los protocolos de transporte.

La administración del vehículo se actualiza a través de una convención del vehículo entre dos sustancias del vehículo. En puntos de vista específicos, las convenciones de transporte toman las convenciones del sistema. Ambos están a cargo del control de errores, secuenciación y control de flujo (Stalling, 2000, p.78).

### 5.1.5 Direccionamiento.

En el momento en que un procedimiento desea establecer una asociación con una PC de aplicación remota, debe determinar con cuál interactuará, la estrategia que se utiliza regularmente es caracterizar las direcciones de transporte en las que los procedimientos pueden sintonizarse para las demandas de asociación. (Perez, 2001, p.56).

### 5.1.6 Establecimiento de una conexión.

Establecer una asociación parece ser simple, pero realmente es sorprendentemente problemático, desde el principio, sin duda, es suficiente enviar un TPDU con la

solicitud de asociación y esperar que el otro reconozca la asociación, una es utilizar direcciones de vehículos prescindibles, en esta metodología, cada vez que necesitamos una ubicación, la hacemos (James, 2001, p.45).

### 5.1.7 Control de flujo y almacenamiento en buffer.

Con respecto a la forma en que se manejan las asociaciones mientras se usan, uno de los puntos de vista clave es el control de flujo, se espera que un plan evite que un transmisor rápido se inunde a un beneficiario moderado, la distinción principal es que un conmutador generalmente tiene pocas líneas y un host puede tener varias asociaciones (James, 2001, p.67).

### 5.1.8 Recuperación de caídas.

En el caso de que los hosts y los conmutadores puedan sufrir bloqueos, la recuperación es fundamental, en el caso de que el elemento del vehículo esté completamente dentro de los hosts, la recuperación de accidentes e interruptores del sistema es básica, en el caso de que la capa del sistema administre datagramas, las sustancias de transporte anticipan la pérdida de algunas TPDU constantemente y se dan cuenta de cómo lidiar con ellas (Stalling, 2000, p.89).

### 5.1.9 Protocolos de transporte de internet.

#### *5.1.9.1 TCP.*

TCP es una administración de transporte organizada por asociación. Es absolutamente sólido.

Los datos TCP se transmiten en bits y se realiza una sesión antes de que las máquinas puedan intercambiar datos.

La reunión ACK declara el paso correcto de un bit a la siguiente máquina. Para cada sección enviada, el destinatario debe restablecer un ACK dentro de un período predeterminado.

Para cada sección enviada, el destinatario debe restaurar un ACK dentro de un marco de tiempo predefinido

*5.1.9.1.1 Puertos.*

Las aplicaciones de '*sockets'* se ven notablemente en una máquina que usa un número de puerto de introducción de puerto '. Por ejemplo, un servidor FTP utiliza un puerto TCP específico para que algunas aplicaciones puedan visitarlo.

Los puertos pueden utilizar cualquier número en algún lugar dentro del alcance de 0 y 65536.

*5.1.9.1.2 Sockets.*

Palet (2007) señala :

> que el archivo adjunto es una idea como un controlador de registro y esto funciona como un propósito final de la correspondencia del sistema. Una aplicación puede hacer un archivo adjunto para enviar información organizada a una aplicación remota. La información será sólida enviada bajo esta asociación (p.176).

*5.1.9.1.3 Puertos TCP.*

"Un puerto TCP nos da una zona para la transmisión de mensajes. Los números de puerto inferiores a 256 se representan como los puertos más utilizados" (Stalling, 2000, p.78).

*5.1.9.1.4 Sesiones TCP.*

Una sesión TCP comienza de tres maneras diferentes. La motivación detrás de estas tres formas diferentes es sincronizar el envío y la aceptación de porciones, iluminando a la otra máquina con respecto a la medida de la información que está equipada para obtener de una huelga y estableciendo una asociación virtual (Stalling, 2000, p.78).

La máquina que acepta envía un ACK a la solicitud que restaura una sección con:

El banner de sincronización puesto.

Un número de disposición que muestra el byte inicial de la sección que se envió recientemente.

Un ACK con el número de disposición del byte primario de la siguiente sección que espera obtener.

El host emisor de datos retorna a enviar un segmento donde está el número de secuencia ACK. Este momento es donde la conexión se establece hasta generar una nueva.

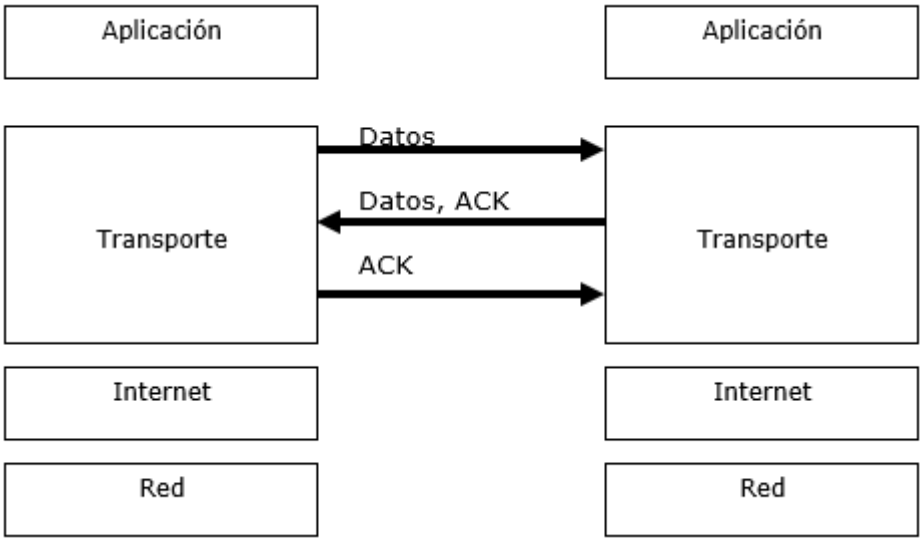



*Figura 21*. Sesiones TCP. Fuente: Stalling, 2000.

El TCP utiliza un proceso similar para terminar una conexión. Esto garantiza que las maquinas en conexión terminen de transmitir y recibir todos los datos.

*5.1.9.1.5 Ventanas de apertura en el TCP.*

Los amortiguadores TCP para la transmisión entre dos máquinas se terminan utilizando ventanas. Cada máquina TCP mantiene dos ventanas: una para adquirir información y otra para enviar información. El tamaño de las ventanas muestra el grado de información que una totalidad justa puede obtener en la parte posterior de una de las máquinas (Andrew, 2003, p.33).

*5.1.9.1.6 Estructura de los paquetes TCP.*

Tabla 11
*Campos de la cabecera del TCP.*

| Campos | Funciones |
|---|---|
| PUERTO ORIGEN | Puerto TCP emisor de dato. |
| PUERTO DESTINO | Puerto TCP receptor o destino de máquina. |
| NUMERO ACK | El número de la secuencia del siguiente byte que se espera recibir. |
| LONGITUD DE DATOS | Longitud en byte del segmento TCP. |
| RESERVADOS | Reservado para otros usos a futuro. |
| FLAGS | Especifica este campo, cuál será el contenido del siguiente. segmento. |
| VENTANA | Espacio que queda disponible en la ventana del TCP. |
| CHECKSUM | Numero para verificar el control de la cabecera. |
| APUNTADOR | Cuando se envía datos relevantes, detallados así en el campo. |
| URGENTE | Este campo se apunta al final de los datos la jerarquía necesaria. |

*Nota:* Estructura y parte de la cabecera TCP. Fuente: Andrew, 2003.

Todas las porciones TCP tienen dos secciones: información y encabezado. La tabla adjunta registra los campos en el encabezado TCP:

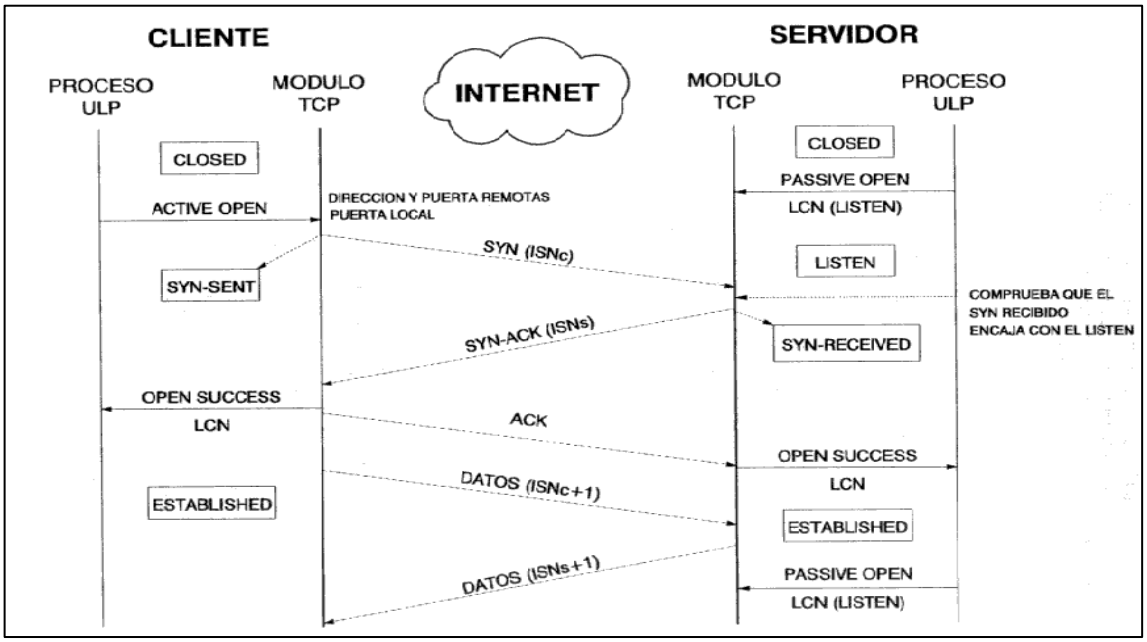



*Figura 22*. Cabecera TCP. Fuente: Palet, 2007.

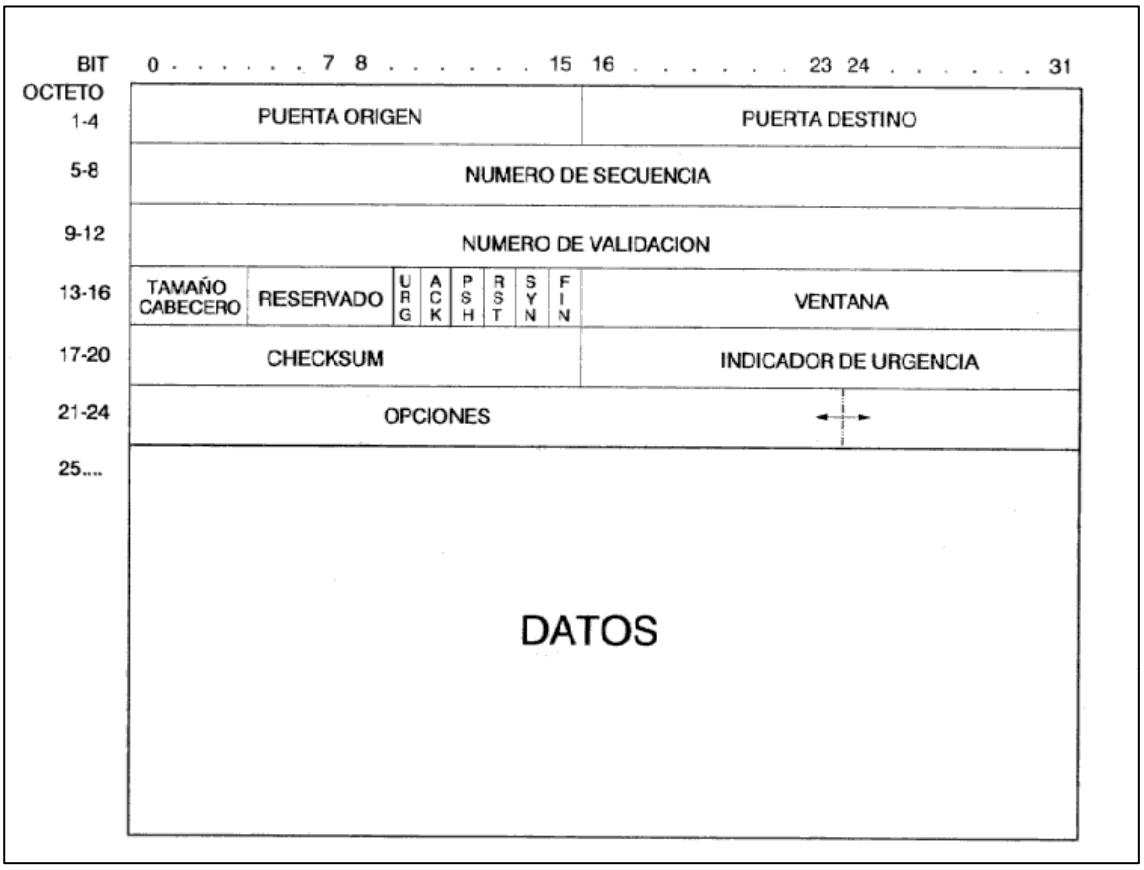



*Figura 23*. Conexión TCP. Fuente: Palet, 2007.

### *5.1.9.2 UDP.*

Client Datagram Protocol 'UDP es una administración de envío de datagramas sin certificación de transporte. Esta técnica se llama no asociada, diferente al TCP que, al configurar una sesión, se llama "asociada" de esta manera, no se garantiza el aterrizaje en el objetivo de un datagrama o la disposición de transporte correcta (Palet, 2007, p.99).

#### *5.1.9.2.1 Puertos UD.*

"Para utilizar UDP, una aplicación debe dar una dirección IP y un número de puerto de la aplicación objetivo, una capacidad de puerto como una línea de mensajes multiplexada que generalmente puede recibir algunos mensajes" (Perez, 2001, p.78).

Tabla 12
*Puerto UDP*

| 15 | NETSTAT | Estado de la red |
|---|---|---|
| 53 | DOMAIN | DNS (domain name server) |
| 69 | TFTP | Trivial file transfer protocol |
| 137 | NETBIOS-NS | Servicios de seudónimos NETBIOS |
| 138 | NETBIOS-DGM | Servicios de datagramas NETBIOS |
| 161 | SNMP | Monitor de red SNMP |

*Nota:* Significados de los puertos según el estado de la red. Fuente: Pérez, 2001.

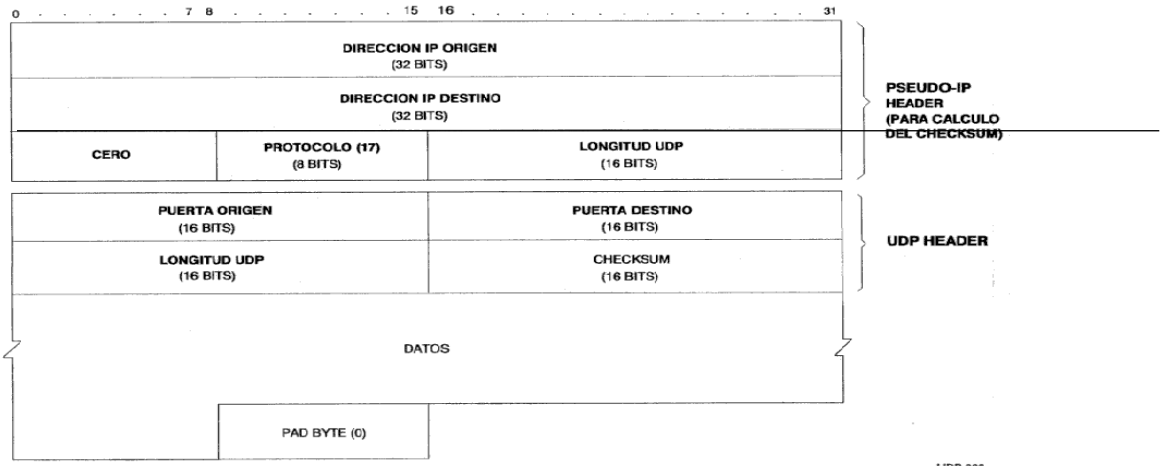



*Figura 24.* Formato UDP. Fuente: Palet, 2007.

# Capítulo VI

# Nivel de aplicación en TCP/IP

## 6.1 Protocolos de aplicación

### 6.1.1 File transfer protocol FTP.

En una situación del sistema, es normal que necesite duplicar registros entre varias PC. ¿Por qué motivo es tan confuso de vez en cuando? Los productores de PC han concebido muchos marcos de grabación. Estos marcos contrastan en muchas sutilezas menores y, además, en un par de sutilezas significativas. No es solo un problema que haya varios productores.

Regularmente, los marcos de PC solicitan que el cliente ingrese un identificador de asociación y una palabra secreta para ver o controlar los registros. No obstante, de vez en cuando es valioso crear una región abierta de archivos. FTP ofrece dos tipos de administraciones para ajustar tanto el acceso a datos abiertos compartidos como el acceso a documentos privados:

Acceso remoto a archivos públicos por medio de conexiones “anónimas”.

Acceso remoto a archivos privados, restringido a usuarios que cuenten con un identificador de conexión al sistema y un passwors.

Veamos un sencillo acceso a los datos públicos de un ordenador:

Tabla 13
*Protocolo de aplicación FTP*

| Orden | Descripción |
|---|---|
| HELP | Muestra en forma de lista todos los comandos FTP que puede usar. |
| STATUS | Se utiliza para visualizar algunas de las configuraciones y el estado de la máquina cliente. |
| BINARY | Esta orden cambia del modo ASCII (envío de documentos de texto) al modo binario, incluye programas e imágenes para su envío. |
| ASCII | Inverso al anterior devuelve a su estado natural es decir a el modo ASCII. |
| TYPE | Te muestra el estado de la transferencia en uso, ya sea binario o ASCII. |
| USER | Se usa para reiniciar una sesión en la conexión FTP en curso, con nombre de usuario distinto. Después, le solicitaran un nuevo password. |
| LS | Genera la lista de archivo que se encuentran en la carpeta o directorio, también muestra detalles de los archivos. |
| PWD | Devuelve el nombre completo del directorio o carpeta actual. |
| CD | El nombre de la orden es change directory (cambiar el directorio) y te permite desplazarte de directorio en directorio por todos sus niveles, incluso volviendo al directorio principal. |
| MKDIR | Te permite crear directorios nuevos en UNIX o Windows, siempre y cuando el usuario tenga los permisos de acceso permitidos. |
| RMDIR | Te permite eliminar directorios en UNIX o Windows, siempre y cuando el usuario tenga los permisos de acceso permitidos. |
| GET | Te permite rescatar archivos del servidor, es decir puedes llevar a tu servidor loca los archivos de otro servidor remoto, siempre y cuando el usuario tenga los permisos de acceso permitidos. |
| PUT | Esta orden se usa para enviar un archivo local al servidor, es decir puedes mandar archivos al servidor remoto desde tu servidor local, siempre y cuando el usuario tenga los permisos de acceso permitidos. |
| OPEN | Te permite finalizar la sesión y abrir una nueva sesión en otro servidor FTP. |
| CLOSE | Finaliza la sesión, dejando al programa FTP encendido. |

*Nota:* Comandos más utilizados en el protocolo FTP. Fuente: Palet, 2007.

Como debería ser obvio del discurso anterior, un cliente coopera con un procedimiento del cliente FTP del vecindario. La programación cercana del cliente participa en una discusión formal con el proceso del servidor remoto FTP a través de una asociación de control. En el momento en que el cliente final ingresa a un intercambio o registra la orden de la junta, la dirección se convierte en una de las abreviaturas poco comunes de la asociación de control.

En el caso de que el cliente exija un movimiento de documentos, se abre una asociación de información diferente y el registro se replica a través de esa asociación. Las asociaciones de información también se utilizan para transmitir publicaciones de catálogo. La figura que acompaña muestra este modelo. El servidor normalmente usa el puerto 20 para su parte de la asociación de negociación.

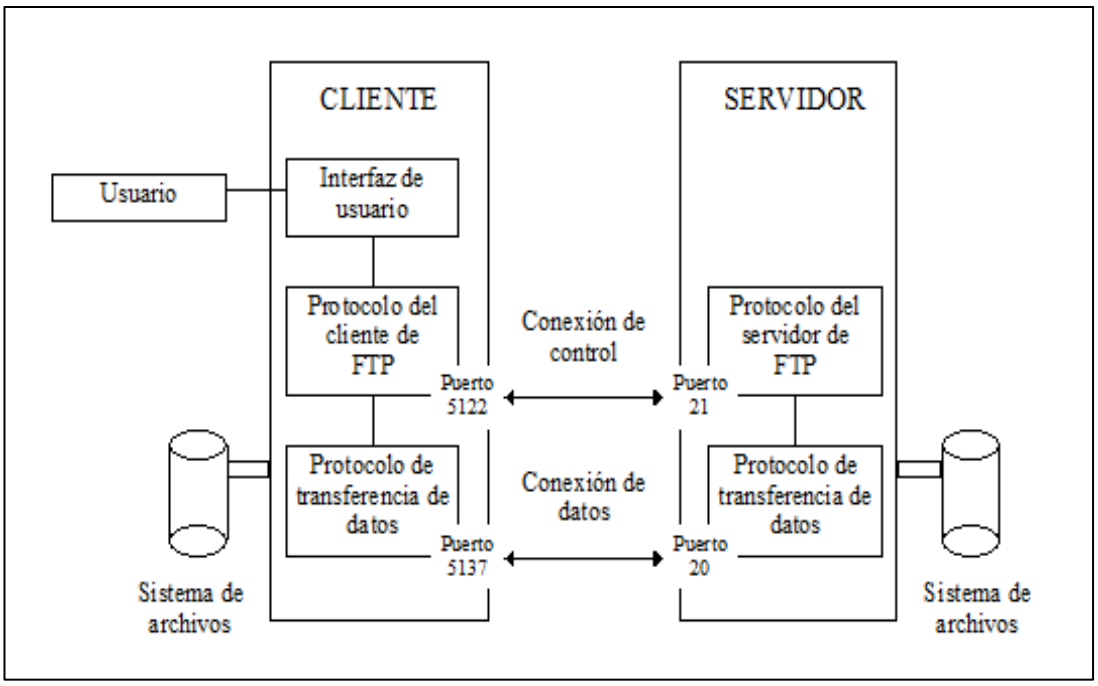



*Figura 25*. File Transfer Protocol. Fuente: Palet, 2007.

Durante el discurso pasado, el cliente final mencionó una diferencia en el catálogo para duplicar un registro. Esta solicitud se convirtió en una orden FTP formal y se envió al servidor FTP remoto a través de la asociación de control. El movimiento del documento fue realizado por la asociación de información gratuita que se realizó por este motivo.

### *6.1.1.1 Comandos de FTP.*

¿Qué tipo de instrucciones se pueden enviar a través de la asociación de control? Hay diferentes tipos de direcciones. Las más amplias son las instrucciones de validación, que permiten a un cliente proclamar el identificador, la frase secreta y el registro que se utilizarán para muchos ejercicios FTP; Instrucciones de movimiento de archivos, que permiten al cliente duplicar al menos un documento que comienza con una PC y luego a la siguiente, agrega un documento vecino a un registro remoto, y así sucesivamente.

```
ftp> help
Commands may be abbreviated.  Commands are:
!               debug           mget            pwd             status
$               dir             mkdir           quit            struct
account         disconnect      mls             quote           system
append          form            mode            recv            sunique
ascii           get             modtime         reget           tenex
bell            glob            mput            rstatus         trace
binary          hash            newer           rhelp           type
bye             help            nmap            rename          user
case            idle            nlist           reset           umask
cd              image           ntrans          restart         verbose
cdup            lcd             open            rmdir           ?
chmod           ls              prompt          runique
close           macdef          proxy           send
cr              mdelete         senador      site
delete          mdir            put             size
ftp>
```

*Figura 26.* Comandos de File Transfer Protocol. Fuente: Palet, 2007

En algunos casos, la interfaz de vecindario no tiene directamente el orden que el cliente necesita enviar (sin embargo, es accesible desde la PC remota). Una ejecución FTP decente tendrá la dirección de la declaración (verdaderamente entre comillas), que le permite componer la orden formal según lo necesite enviar. Esa articulación se transmitirá a través de la asociación de control precisamente como fue compuesta. En consecuencia, podría ser valioso conocer las instrucciones formales y sus parámetros. Desde aquí demostraremos esas instrucciones como tablas.

Tabla 14
*Comandos de autorización de acceso a archivos*

| **Comando** | **Definición** | **Parámetros** |
|---|---|---|
| USER | Reconoce al usuario | Identificador |
| PASS | Proporciona la nueva contraseña | Contraseña |
| ACCT | Proporciona una nueva cuenta | ID de la cuenta |
| REIN | Reinicia el modo de comienzo | Ninguno |
| QUIT | Finaliza la sesión | Ninguno |
| ABOR | Retira el anterior comando u orden y su transferencia de datos o conexión asociada | Ninguno |

*Nota:* Comandos TCP para acceder a archivos desde consola. Fuente: Palet, 2007.

Tabla 15
*Comando de gestión de archivos y directorios.*

| Comando | Definición | Parámetro(s) |
|---|---|---|
| CWD | Escoge otro directorio del servidor | Nombre de carpeta. |
| CDUP | Escoge al directorio padre | Ninguno. |
| DELE | Eliminar uno o más archivo | Nombre de archivo |
| LIST | Lista información de archivos | Nombre de carpeta, listado de archivos. Ninguno si se trata la carpeta de trabajo |
| MKD | Genera un nuevo directorio o carpeta | Nombre de carpeta |
| NLST | Muestra en lista los archivos de uno o más directorio o carpeta | Nombre de la carpeta o ninguno para la carpeta de trabajo |
| PWD | Imprime el nombre del directorio o carpeta de trabajo | Ninguno |
| RMD | Borra un directorio o carpeta | Nombre de carpeta |
| RNFR | Identifica un archivo y lo renombra | Nombre de carpeta |
| RNTO | Renombra un archivo | Nombre de carpeta |
| SMNT | Arma un diferente sistema de archivos | Identificador |

*Nota*: Comandos para administración de archivos y carpetas. Fuente: Palet, 2007.

Tabla 16

*Comando que define el tipo, la estructura y el modo*

| Comandos | Definiciones | Parámetros |
|---|---|---|
| TYPE | Reconoce el tipo de dato y también el formato de impreso, si existe para la transferencia. | A- ASCII, E- EBCDIC, I Imagen binario, N No impreso, T telnet, C (ASA). |
| STRU | Gestiona los archivos | F -FILE O R – REGISTRO |
| MODE | Formato de la conexión | S -FLUJO O STREAM, B – BLOQUE, C- COMPRIMIDO. |

*Nota:* Comandos para definir el tipo la forma y el diseño en TCP. Fuente: Palet, 2007.

Tabla 17

*Comando que realiza la transferencia de archivos*

| Comando | Definición |
|---|---|
| RETR | Recupera o regenera un file. |
| STOR | Sirve para guardar, salvar un archivo, save file. |
| STOU | Genera un archivo único con nombre sin lugar a duplicado. |
| APPE | Agrega los archivos locales un remoto. |
| ALLO | Permite que haya lugar para los datos o archivos siguientes. |
| REST | Resetear o reiniciar. |
| RNTO | Renombrar un archivo |

*Nota:* Comandos más usados desde la consola para configuraciones básicas. Fuente: Palet, 2007.

Tabla 18

*Otros comandos de información al usuario*

| Comandos | Definiciones | Parámetros |
|---|---|---|
| HELP | Ayuda con información para los servidores. | Ninguno |
| NOOP | Pide respuesta del servicio. | Ninguno |
| SITE | Se usa para sub comandos del servidor pero no son el estándar, así mismo pueden necesitarse para el servidor. | Ninguno |
| SYST | Gestiona el sistema operativo del servidor. | Ninguno |
| STAT | Muestra el estado de la conexión y sus parámetros. | Ninguno |

*Nota:* Algunos otros comandos más. Fuente: Palet, 2007.

### *6.1.1.2 Protocolo trivial de transferencia de archivos (TFTP).*

Hay aplicaciones para duplicar documentos que requieren un grado básico de utilidad. Por ejemplo, el volcado subyacente de los registros de programación y diseño al arrancar un interruptor, un punto central o una estación de trabajo sin círculo se realiza mejor utilizando una convención que es excepcionalmente básica.

Todos los cuadrados deben contener 512 octetos de información, con la excepción del último, que sirve para marcar la parte del trato. En el caso de que el tamaño del documento sea diferente de 512, el último cuadrado comprende solo el encabezado, sin información. Los cuadrados de información están numerados, comenzando con 1. Cada ACK contiene el número cuadrado de la información que está afirmando. Hay cinco tipos de unidades de datos de protocolo:

Los mensajes equivocados demuestran condiciones, por ejemplo, "documento no encontrado" o "ausencia de espacio para componer el registro en la placa”.

Cada cabecera de TFTP empieza con un código de operación que señala el tipo de unidad de datos de protocolo (PDU - Protocol Data Unit). El formato de las PDU se puede aprecia en la figura a continuación:

Petición de lectura:

| 2 octetos | Cadena | 1 octeto | Cadena | 1 octeto |
|---|---|---|---|---|
| Código de op.=1 | Nombre de archivo | 0 | Modo | 0 |

Petición de escritura:

| 2 octetos | Cadena | 1 octeto | Cadena | 1 octeto |
|---|---|---|---|---|
| Código de op.=2 | Nombre de archivo | 0 | Modo | 0 |

Datos:

| 2 octetos | 2 octetos | |
|---|---|---|
| Código de op.=3 | Nº de bloque | Datos |

Confirmación:

| 2 octetos | 2 octetos |
|---|---|
| Código de op.=4 | Nº de bloque |

Error:

| 2 octetos | 2 octetos | Cadena | 1 octeto |
|---|---|---|---|
| Código de op.=5 | Código de error | Mensaje de error | 0 |

*Figura 27.* Formato de las PDUs en TFTP. Fuente: Palet, 2007

Tenga en cuenta que el tamaño de las demandas de lectura y las solicitudes de redacción fluctúa dependiendo del tamaño del nombre del documento y el identificador de modo, cada uno con una cadena de contenido.

#### *6.1.1.3 Modelo de emulación de terminal de telnet.*

Como se muestra en la figura siguiente, un usuario de un terminal real interacciona con el programa cliente de *telnet* local. El programa cliente de *telnet* tiene que aceptar las pulsaciones del teclado del usuario, interpretarlas y mostrar la salida en la pantalla del usuario de forma consistente con la emulación en uso.

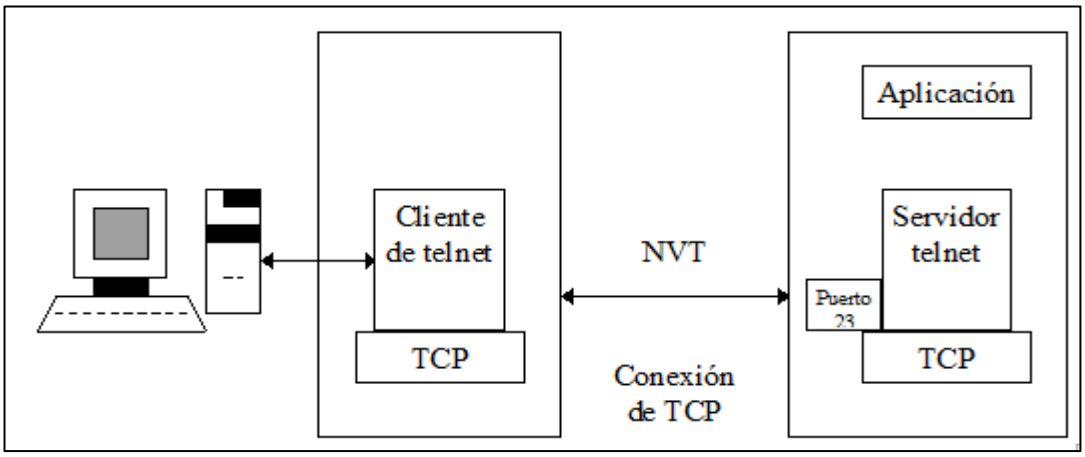



*Figura 28.* Esquema del Funcionamiento de Telnet. Fuente: Palet, 2007.

El cliente *telnet* abre una conexión de TCP con el servidor *telnet*, al que se accede por el puerto público 23. El servidor *telnet* interacciona con las aplicaciones y asiste en la emulación de un terminal nativo.

Para conseguir iniciar una sesión, ambos extremos intercambian información utilizando un protocolo muy sencillo llamado terminal virtual de red NVT (Network Virtual Terminal). El protocolo de NVT se modeló en un antiguo teclado semidúplex y una impresora funcionando línea a línea. NVT posee unas características bien definidas:

- Los datos del NVT se componen de caracteres USASCII de 7 bits aumentados a 8 bits por medio de una 0 inicial.
- Los datos se envían línea a línea.
- Cada línea termina con una combinación de caracteres ASCII de retorno de carro (CR - Carriage Return) y salto de línea (LF - Linefeed).
- Los bytes cuyo bit inicial (más significativo) es 1 se usan para códigos de comandos.

Los terminales ASCII se usan con computadoras UNIX y VAX. Los terminales ASCII se caracterizan por:

- Eco remoto de cada carácter. Esto es, cada carácter se envía al ordenador remoto y se reenvía de vuelta antes de aparecer en la pantalla del usuario. Es muy duro para la red.
- Transmisión dúplex. Los caracteres viajan en las dos direcciones simultáneamente. El servidor no necesita enviar códigos de control de <<Adelante>>.
- Soporte para aplicaciones interactivas de pantalla completa (con mucha carga de red).
- Conjunto de caracteres ASCII mayor que el de NVT.

A diferencia de los terminales ASCII, los terminales de IBM están optimizados para aplicaciones de procesado de datos que operaban en “modo de bloque”, lo que significa que un usuario trabaja con una pantalla de datos cada vez. Cuando el usuario pulsa INTRO u otra tecla de función, se envía al ordenador la información de la pantalla. El teclado se bloquea y el ordenador procesa los datos. A continuación, el ordenador envía de vuelta una o más pantallas de datos. Cuando el ordenador termina, desbloquea el teclado. Los 3270 se caracterizan por:

- Códigos EBCDIC de 8 bits.
- Comunicación semidúplex.

- Modo de bloque.

Los aspectos más destacados de la copia de terminales se establecen mediante instrucciones comerciales que organizan alternativas de telnet. Una vez más, el reportero puede reconocer o no. Hay cuatro intercambios de solicitud / reacción que generalmente ocurren durante el intercambio de alternativas:

Tabla 19
*Opciones de la negociación de una conexión telnet*

| Opción | Definición |
|---|---|
| DO | Solicita que acepte la opción. |
| WILL | Se acepta y se realiza la opción. |
| DO | Solicita nuevamente una opción. |
| WONT | El destinatario acepta y su estado no varía. |
| WILL | Revela el afán de iniciar opción. |
| DO | Se da el permiso, la opción se realiza. |
| WILL | Inica deseo de comenzar nuevamente una opción. |
| DONT | Se rehusa a aceptar la opción. |
| WONT | Confirma que no cambiará el estado de rehusa. |

*Nota:* Comandos de control para consola en una conexión telnet. Fuente: Palet, 2007.

Al inicio de la conexión, hay muchas peticiones de opciones que van y vuelven entre los interlocutores. A veces, también se intercambian opciones en mitad de una sesión. Algunas opciones señalan el comienzo de sus multiples subnegociaciones, en las cuales se intercambia información adicional. ¿Qué ocurre si ambas partes rechazan todas las peticiones de opciones? La sesión se mantendrá en modo NVT (Palet, 2007, p.78).

Las solicitudes de alternativas de arreglo y subnegociación están codificadas con tres bytes: un código IAC, un octeto de solicitud y un código de elección. Por ejemplo, la representación del arreglo para tipo de terminal de voluntad es: 0xFF 0xFB 0x18. Las tablas adjuntas demuestran los códigos de intercambio y subnegociación y. los números de código relacionados probablemente con las alternativas más utilizadas (Perez, 2001).

Tabla 20
*Codificación de las peticiones de negociación de una conexión telnet*

| Petición de negociación | Código |
|---|---|
| WILL | 251 |
| WONT | 252 |
| DO | 253 |
| DONT | 254 |
| SB | 250 |
| SE | 240 |

*Nota:* Comandos de control para consola en una conexión telnet. Fuente: Palet, 2007.

Tabla 21
*Códigos de opciones de una conexión telnet*

| Códigos de opción del comando | Código |
|---|---|
| Transmit binary | 0 |
| Echo | 1 |
| Suppress go | 3 |
| Status | 5 |
| Timing mark | 6 |
| Output Line width | 8 |
| Output page size | 9 |
| Extended ASCII | 17 |
| Data entry terminal | 20 |
| Terminal type | 24 |

*Nota:* Códigos de opciones de control para consola en una conexión telnet. Fuente: Palet, 2007.

Se han escrito más de 30 RFC que detallan opciones para definir características especializadas. Algunas opciones interesantes incluyen:

- La capacidad de sondear al corresponsal para saber los parámetros de la opción actual. Se envía una petición de estado y se recibe una respuesta por medio de una subnegociación.
- La negociación del tamaño de la ventana. Los corresponsales acuerdan que el cliente puede realizar una subnegociación para informar al servidor del alto y ancho de la ventana que se va a usar para la sesión de telnet. Esta característica es útil cuando se ejecuta una sesión de telnet en una estación basada en ventanas.

No es necesario que una implementación permita todas, ni siquiera la mayoría, de las opciones definidas. Dos de las opciones que se utilizan para la emulación del 3 270 tienen características especiales:

- Transmitir en binario (Transmit Binary). Comenzar a transmitir datos binarios de 8 bits. Recuerde que las sesiones del 3 270 de IBM se realizan en binario.
- Fin de registro (End of Record). El interlocutor que recibe la orden de fin de registro (DO END-OF-RECORD) usará un código de control estándar de IAC 239 para señalar un fin de registro de flujo de datos.

Recuerde que, incluso después de pasar a modo binario, se pueden enviar los comandos de *telnet* al interlocutor duplicando los caracteres de escape de IAC.

En el discurso de ejemplo que persigue, se ejecuta telnet y se ingresan opciones de cambio para que telnet nos demuestre sus arreglos. En ese punto, se utilizan abiertos para iniciar una asociación. Los cómplices organizan una imitación ASCII VT100 eligiendo las cualidades que lo acompañan:

- El servidor no avanzará (Adelante) a la luz del hecho de que la sesión será dúplex.
- Se utilizará una subnegociación del tipo de terminal, velocidad de movimiento, para demostrar el tipo particular de terminal ASCII a imitar.
- El servidor hará resonar los caracteres del cliente.

Ninguna de las partes debe esperar una reacción a una solicitud de elección antes de enviar otra solicitud. En ningún caso un árbitro necesita reaccionar a las elecciones en una solicitud similar que recibió. Por lo tanto, aquí y allá para comprender una progresión de arreglos, necesita desentrañarlo.

#### *6.1.1.4 Características de NVT.*

Después de completar la negociación de opciones, una emulación de terminal particular puede proporcionar un abundante repertorio de caracteres y símbolos gráficos para la interacción entre un usuario y una aplicación, abandonando el modo de terminal NVT. Sin embargo, cuando se usa *telnet* para construir aplicaciones cliente/servidor, a menudo la mayoría o todas las interacciones ocurren simplemente en modo NVT. Por lo cual, es interesante resaltar las características de una sesión NVT.

Tabla 22
*Juego de caracteres de ASCII de control de una sesión NVT*

| Descripción | Código ASCII |
|---|---|
| Nulo | 0 |
| Timbre | 7 |
| Retroceso | 8 |
| Tabulador | 9 |
| Salto de línea | 10 |
| Tabulador vertical | 11 |
| Salto de página | 12 |
| Retorno de carro | 13 |

*Nota:* Códigos de opciones de control para consola en una conexión NVT. Fuente: Palet, 2007.

Recuerde que una interacción de NVT es semidúplex, lo que significa que, en un momento dado, o bien el cliente de *telnet* o bien el servidor de *telnet* está al mando:

- En cuanto el cliente de *telnet* envía una línea terminada con CR y LF, el control pasa al servidor.
- El servidor envía líneas de salida al cliente. Al final de cada línea de salida, el servidor utiliza CR y LF para pasar a la siguiente línea de la pantalla del cliente.
- El cliente de *telnet* acepta la salida del servidor y puede volver a introducir una entrada después de recibir del servidor la secuencia de códigos de control adelante (Go Ahead).

Observe que las líneas que se envían a través de la sesión de *telnet* terminan con CR LF, independientemente de lo que usen los ordenadores cliente y servidor como caracteres

locales de fin de línea. Cada ordenador traduce sus caracteres de fin de línea a, y desde, los caracteres de fin de línea de *telnet*.

#### *6.1.1.5 Control de un cliente telnet de texto.*

En ciertas ocasiones, es necesario interaccionar con un cliente *telnet* para establecer o mostrar sus parámetros. ¿Podemos obtener información de nuestra implantación ejecutando telnet y tecleando <<?>> o <<help>> para averiguar los comandos locales.

¿Cómo puede cambiar un usuario las características de una sesión activa o abortar una sesión? Siempre se reserva una secuencia de control del teclado que significa salida al modo de comandos de telnet. La secuencia de escape por defecto habitual es CONTROL y ], que se suele representar por ^]. Esta secuencia de escape la puede definir el usuario. Observe el comentario que aparece en la última conexión realizada a faeton.irobot.uv.es en la tercera línea:

Escape character is '^]'.

Continuemos el diálogo a partir de este punto. Después de introducir la secuencia de escape, aparece un curso de telnet y podemos observar el estado de la sesión actual, los atributos, etc. Después de ejecutar un comando, se vuelve de forma automática al modo de emulación de terminal. Por ejemplo, si en la conexión a faeton.irobot.uv.es introducimos la secuencia de escape y preguntamos el estado de la sesión (status), obtenemos:

Antes de que las redes fueran algo habitual, los terminales se unían directamente a las computadoras. El sistema operativo de la computadora interpretaba inmediatamente las teclas que había pulsado el usuario.

Durante una sesión de telnet, es necesario traducir los códigos de control a comandos de telnet y pasarlos al sistema operativo del extremo remoto de la conexión de red. Por lo tanto, el programa cliente de telnet tiene que manejar en bruto todas las teclas pulsadas por

el usuario, traducir las teclas especiales de control a comandos de telnet y pasar estos comandos al servidor de telnet.

El cliente de telnet envía secuencias de comandos al servidor para realizar funciones útiles, como puede verse en la figura siguiente:

Tabla 23
*Secuencias de comandos del cliente telnet al servidor*

| Comando. | Descripción. |
|---|---|
| Pausa (BRK) | Envía una pausa o señal de atención al proceso de la aplicación remota. |
| Interrumpir proceso (IP) | Indica al sistema operativo remoto que detenga el programa de la aplicación remota que está en ejecución, por ejemplo, para detener un programa que está en un bucle. |
| Abortar la salida (AO) | Pide a la aplicación del servidor que no envíe el resto de la salida de la operación actual. |
| ¿Estás ahí? (AYT) | Solicita al servidor que muestre una indicación de que el servidor continúa en funcionamiento. |
| Borrar carácter (EC) | Un usuario que teclea un carácter erróneo al escribir una línea de datos normalmente lo corrige utilizando la tecla de retroceso (Backspace) o de borrado (Del). Al operar en modo ASCII carácter a carácter, los caracteres ya se han enviado a la aplicación remota, por lo que debe enviarse el comando EC a través de la conexión. |
| Borrar línea (EL) | Pide a la aplicación remota que borre la línea actual. |

*Nota:* Secuencia de comandos para consola en una conexión telnet. Fuente: Palet, 2007.

Se pueden enviar los comandos incluso después de la negociación, cuando los interlocutores ya no están en modo NVT básico. Pero supongamos que la negociación permite a los interlocutores enviar datos binarios. ¿Cómo se puede reconocer una

secuencia de comandos? La forma de hacerlo consiste en que cada vez que aparece 0xFF como dato, el emisor lo duplica. El receptor elimina el duplicado. Cuando el receptor ve llegar un único 0xFF, o un número impar de ellos, detecta que se trata de un comando.

Tabla 24

*Acrónimos de los comandos más comunes en una conexión telnet*

| Acrónimo | Comando | Código |
|---|---|---|
| EOF | Endo of file | 236 |
| SUSP | Suspend current process | 237 |
| ABORT | Abort process | 238 |
| EOR | Endo f record | 239 |
| NOP | No operation | 241 |
| DM | Data mark | 242 |
| BRK | Break | 243 |

*Nota:* Códigos de opciones de control para consola en una conexión telnet. Fuente: Palet, 2007.

Cuando llega el segmento de señal de sincronismo, el servidor extrae del flujo de datos los comandos de NVT y desecha el resto, hasta que llega la marca de datos. El servidor ejecuta los comandos de NVT. Después de la marca de datos, continúa el funcionamiento normal. En la tabla siguiente puede verse la lista de acrónimos de los comandos más comunes, todos ellos van precedidos del valor 255 (0xFF) cuando se envían a través de la conexión de *telnet*.

### 6.1.2 La world wide web.

#### *6.1.2.1 Introducción.*

La World Wide Web (WWW) es un sistema de composición para acceder a los registros conectados que circulan en una gran cantidad de máquinas a través de Internet; En cinco años pasó de ser un método para dispersar información sobre ciencia de materiales de alta vitalidad a la aplicación que un gran número de personas cree que es Web (Stalling, 2000, p.67).

"La Web comenzó en 1989 en el CERN, el Centro Europeo de Investigación Nuclear. Los comportamientos del CERN exploran la ciencia de los materiales moleculares con investigadores de diferentes naciones europeas" (Stalling, 2000, p.89).

Estos exámenes incluyen grupos enmarcados por individuos de aproximadamente seis naciones o más.

### *6.1.2.2 El lado del cliente.*

Desde la perspectiva del cliente, la web se compone de una colosal disposición general de archivos, llamados páginas. Stalling (2008) afirma:

> Las páginas se ven a través de un programa llamado vigilante, programa o programa. Los dos más generales son netscape y explorer. el observador obtiene la página mencionada, traduce el contenido y organiza las direcciones que la página contiene y muestra, adecuadamente diseñadas, en la pantalla (p.90).

Un ejemplo de página Web puede verse a continuación:


*Figura 29.* Ejemplo de web. Fuente: Recuperado de http://www.uv.es.

Como la mayoría de las páginas web, comienza con un título y contiene cadenas de contenido que son conexiones a diferentes páginas, llamadas hipervínculos. Estas cadenas

se presentan, ya sea por subrayado, introducción de sombreado extraordinario, o ambos. Para buscar una conexión, el cliente coloca el cursor en el territorio destacado (utilizando el mouse o las teclas de bloqueo) y lo elige (haciendo clic con un mouse o presionando ENTER). La mayoría de los observadores tienen capturas y aspectos destacados que desenredan la lectura de la web.

### *6.1.2.3 El lado del servidor.*

Cada establecimiento de la Web tiene un procedimiento de servidor que sintoniza el puerto TCP 80, que se adapta a las asociaciones de los clientes (generalmente observadores). Después de que se crea una asociación, el cliente envía una solicitud y el servidor envía una reacción. En ese punto, la asociación se descarga. La convención que caracteriza las solicitudes y reacciones legítimas se llama HTTP y la contemplaremos en detalle a continuación. Un caso directo de utilización puede dar una idea sensata sobre la actividad de los servidores web. Veamos la figura siguiente:

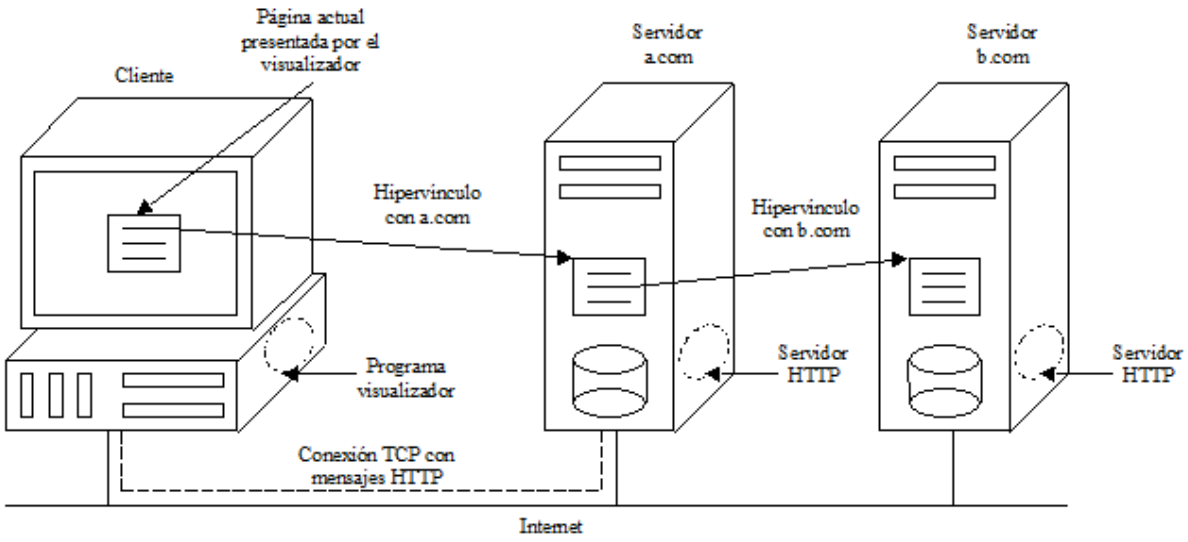



*Figura 30*. Esquema de Funcionamiento del WWW. Fuente: Perez, 2001.

Suponga que el cliente recientemente hizo clic en algún lugar del contenido o en un símbolo que se enfoca en una página cuya URL (Localizador Uniforme de Recursos) es http://www.uv.es/index.html.

> Numerosos observadores presentan la progresión que están ejecutando cada vez en una línea de estado en la base de la pantalla, con el objetivo de que el cliente pueda percibir lo que está haciendo y si ocurre un error a la luz del hecho de que se espera. Es importante destacar que para cada imagen en línea (símbolo, dibujo, foto, etc.) de una página, el escaparate crea otra asociación TCP con el servidor, de modo que si una página contiene numerosos símbolos, todos en un similar servidor, configurar, utilizar y descargar otra asociación para cada uno no es competente, pero reorganiza el uso (Palet, 2007, p.56).

*6.1.2.3.1 HTTP: Protocolo de transferencia de hipertexto.*

La convención de movimiento web estándar es HTTP (Protocolo de transferencia de hipertexto). Cada cooperación se compone de una solicitud ASCII perseguida por una reacción de tipo MIME RFC 822, a pesar de que la utilización de TCP para la asociación de vehículos es normal, el estándar no lo exige oficialmente (Perez, 2001, p.56).

Se utilizan algunas versiones y se están creando otras. Las adaptaciones se indican mediante una disposición de numeración de tipo <major>. <menor> para mostrar las representaciones de la convención. En este sentido, el remitente puede demostrar la configuración del mensaje y su capacidad para comprender futuros intercambios HTTP (Palet, 2007, p.34).

*6.1.2.3.2HTTP-Versión: HTTP/1.0.*

Si no se determina la adaptación de la convención, el beneficiario del mensaje espera que el mensaje tenga la configuración HTTP / 1.0.

Las dos formas principales a las que ahora se puede acceder son HTTP / 1.0 y HTTP / 1.1. El contraste fundamental entre los dos es que, mientras que la versión 1.0 impulsa cada solicitud que un cliente realiza a un servidor para producir una asociación TCP alternativa, la adaptación 1.1 permite una asociación con el host de varios intercambios de solicitudes y reacciones (Stalling, 2000, p.56).

Tabla25

*Método existentes en HTTP*

| Métodos | Descripción |
|---|---|
| OPTIONS | Verifica las opciones para la comunicación. |
| GET | Genera una página web. |
| HEAD | Genera la cabecera de la página web. |
| POST | Añade recursos como páginas. |
| PUT | Gestiona el almacenamiento web. |
| DELETE | Quita una o más páginas web. |
| TRACE | Genera la devolución de la solicitud. |

*Nota:* El método http fue uno de los primeros en usarse hasta que llegó su predecesor y más seguro https. Fuente: Stalling, 2000.

La técnica OPTIONS se acerca al servidor para obtener datos sobre las alternativas de correspondencia accesibles para el activo indicado por una URL, generalmente un tipo MIME (contenido / html, etc.). En este sentido, el cliente puede decidir los resultados concebibles que tiene el servidor o las alternativas relacionadas con un activo específico (Perez, 2001, p.78).

La estrategia GET solicita que el servidor envíe la página codificada adecuadamente en MIME. Sea como fuere, si la solicitud GET es rastreada por un encabezado If-Modified-Since, el servidor posiblemente envía la información en caso de que se haya ajustado después de la fecha indicada. Al utilizar este sistema, un observador que

mencionó una página que está almacenada puede exigirla restrictivamente al servidor (Stalling, 2000, p.89).

La técnica PUT es el reverso de GET, en lugar de leer una página, la compones. Esta técnica hace posible la fabricación de muchas páginas en un servidor remoto. El cuerpo de la solicitud contiene la página y puede codificarse utilizando MIME, en cuyo caso las líneas que persiguen PUT podrían incorporar encabezados de aprobación de tipo de contenido e identificación, para demostrar que el candidato tiene autorización para ejecutar la actividad (Andrew, 2003, p.114).

La estrategia DELETE borra la página. Del mismo modo que con PUT, la aprobación de prueba reconocible y las licencias asumen un trabajo principal. No hay certificación de que DELETE tenga éxito, ya que independientemente de si el servidor HTTP remoto está feliz de borrar la página, el registro fundamental puede tener un modo que impida el cambio o la cancelación del servidor HTTP (Palet, 2007, p.31).

"Por fin, la metodología TRACE se utiliza para investigar aplicaciones. El último servidor debe restablecer el mensaje de solicitud, reflejando que ha recibido exactamente el mensaje o el tipo de error reconocido" (James, 2001, p.67).

Cada solicitud obtiene una reacción que comprende una línea de estado y posiblemente datos adicionales (por ejemplo, todo o parte de una página del sitio), la línea de estado contiene un código que consta de un número de tres dígitos (Stalling, 2000).

Un ejemplo de línea de estado es el siguiente:

HTTP/1.0 200

**Aplicación didáctica**

**I.E.P. VIRGEN DEL ROSARIO DE YUNGAY. EIRL**

# PLAN DE LECCIÓN Nº 1

**Actividad:** Aplicando el protocolo TCP/IP en la configuración de una cámara IP.

I. DATOS INFORMATIVOS

1.1. INSTITUCIÓN EDUCATIVA : VIRGEN DEL ROSARIO DE YUNGAY

1.2 DIRECTOR : ELMIRA VÁZQUEZ MELÉNDEZ

1.3 NIVEL : SECUNDARIO

1.4 GRADO : QUINTO

1.5 DURACIÓN : 45 MINUTOS

1.6 DOCENTE : SÁNCHEZ LUIS, CARLOS MARX

1.7 FECHA : 13 DE SETIEMBRE DE 2018

II. CAPACIDAD FUNDAMENTAL:

- Solución de problemas

III. APRENDIZAJE ESPERADO: Aplica el protocolo TCP/IP configurando la cámara IP

IV. VALORES:

- Puntualidad
- Responsabilidad
- Laboriosidad

V. ESTRATEGIAS METODOLÓGICAS:

| SITUACIÓN DE APRENDIZAJE | ESTRATEGIAS Y ACTIVIDADES | RECURSOS | TIEMPO |
|---|---|---|---|
| INICIO:<br>• Motivación<br>• Recojo de saberes previos | Ingreso al aula de clases, saludo a los estudiantes y comienzo mi clase. Realizo una breve presentación sobre la demanda de módulos de vigilancia para la seguridad y el impacto de estos en la reducción de robo y asaltos. Recojo los saberes previos preguntando: ¿Qué conocen sobre redes e IP? ¿conocen del programa alto al crimen? ¿Cuál creen que será el objetivo del protocolo TCP/IP? | • Laptop<br>• Parlante<br>• Proyector multimedia | 5 min |

| | | | |
|---|---|---|---|
| PROCESO:<br>• Análisis de la nueva información<br>• Aplicación de la nueva información<br>• Evaluación de los aprendizajes | Expongo los temas de las diapositivas del protocolo tcp/ip desde conceptos, clasificación, tipos, entre otros temas importantes.<br>Entrego las hojas de información a los estudiantes, para que lo analicen y respondan la pregunta del cuestionario.<br>Entrego a los estudiantes la hoja de practica para que ejecuten la tarea programada<br>Asesoro y respondo las preguntas de los estudiantes.<br>Evaluó a los estudiantes en el desarrollo de la práctica. | • Laptop<br>• Proyector multimedia<br>• Hoja de información<br>• Hoja de práctica | 30 min |
| SALIDA:<br>• Metacognición | Los estudiantes responden a las preguntas de la ficha de metacognición. | • Ficha de metacognición | 10 min |

VI. EVALUACIÓN.

| CRITERIO | INDICADOR | INSTRUMENTO |
|---|---|---|
| Aplicación de los procesos | Aplica el protocolo TCP/IP, configurando la cámara IP para el módulo de seguridad. | Lista de cotejo |

# VII. REFERENCIA


- http://www.ipv6tf.org/pdf/the_choice_ipv4_exhaustion_or_transiti on_to_ipv6_v4.4.pdf.
- http://www.ipv6tf.org/pdf/the_choice_ipv4 pv6_v4.4.pdf.


Carlos Marx Sánchez Luis
DOCENTE

Elmira Vázquez Meléndez
DIRECTORA

**HOJA DE INFORMACIÓN Nº1**

**I. Título**: Introducción al protocolo TCP/IP para la configuración de una cámara IP.

**II. Propósito**: Al término de la lectura el estudiante comprenderá el protocolo TCP/IP aplicado a la configuración de una cámara IP.

**III. Contenido:**

**Principios y generalidades del protocolo TCP/IP**

**¿Qué es el protocolo TCP/IP?**

La Agencia de Investigación de Proyectos Avanzados de 1968 del Departamento de Defensa de los Estados Unidos (DARPA) inicia un programa de mejora que permitiría la transmisión de datos entre sistemas de diversos tipos y calidades Se ejecutó un sistema punto a punto de líneas telefónicas llamado ARPANET, utilizando un conjunto de convenciones que luego se llamarían TCP / IP. Este sistema enmarcado por instructivos, militares y de investigación se convirtió en el centro de Internet alrededor de 1980, y en 1983, todos los hosts ARPANET utilizaron dicho conjunto de convenciones (Stalling, 2000, p.56).

Como hemos encontrado en la parte anterior, los elementos de un sistema de PC pueden basarse en los siete. Niveles del modelo OSI, a pesar del hecho de que el uso real de un sistema puede contrastar en el grado pragmático de ese modelo. No Existe una concesión general sobre cómo exhibir la disposición de las convenciones TCP / IP con un modelo de capa. Como una regla. En algún lugar en el rango de tres y cinco niveles prácticos se muestran como sustanciales en la ingeniería de convenciones.

**Nivel de acceso a la red**

Este es el nivel inferior del orden jerárquico de la convención TCP / IP. Las convenciones de esta capa dan

Los métodos para que el marco transmita la información a diferentes dispositivos directamente asociados con el sistema. Caracterizar cómo

Utilice el sistema para transmitir un datagrama IP.

En este nivel, los datagramas IP son epitomizados que dan forma a las cajas que se transmiten al sistema y cambian IP entrega a lo físico tiende a utilizarse en el sistema. Una convención modelo de este nivel sería ARP (Dirección El Protocolo de objetivos) en LAN y SLIP (Serial Line Ip) o PPP (Protocolo punto a punto) se organizan en sistemas WAN. Diciendo la convención da.

Curso de administrador de servidor web / extranet / intranet

Sistemas TCP / IP

**Nivel internet**

Este nivel controla la correspondencia entre grupos, eligiendo el curso más adecuado para perseguir los paquetes de información para llegar a su objetivo. Realice la administración de transporte de paquetes fundamental sobre la cual se construye un sistema TCP/IP.

El protocolo más importante de este nivel es IP (Internet Protocol).

**Nivel de transporte**

Insta a la correspondencia punto a punto que comienza con un programa de aplicación y luego con el siguiente, garantizando que así sea. Es fundamental que los datos entren en contacto con la base sin errores y en el plan de juego correcto. Haga una suma de verificación para afirmar asimismo que la información no ha cambiado durante la transmisión.

TCP (Protocolo de control de transmisión) y UDP (Protocolo de datagramas de usuario) serían espectáculos de nivel de sustancia.

**Nivel de aplicación**

Encontramos en este nivel cada uno de los procedimientos que utilizan las convenciones de nivel de vehículo. Entre cada convención existente en este nivel, podemos demostrar FTP (Protocolo de movimiento de archivos), HTTP (Protocolo de transferencia de hipertexto), SMTP (Protocolo simple de transferencia de correo), DNS (Servidor de nombres de dominio), NFS (Archivo de red

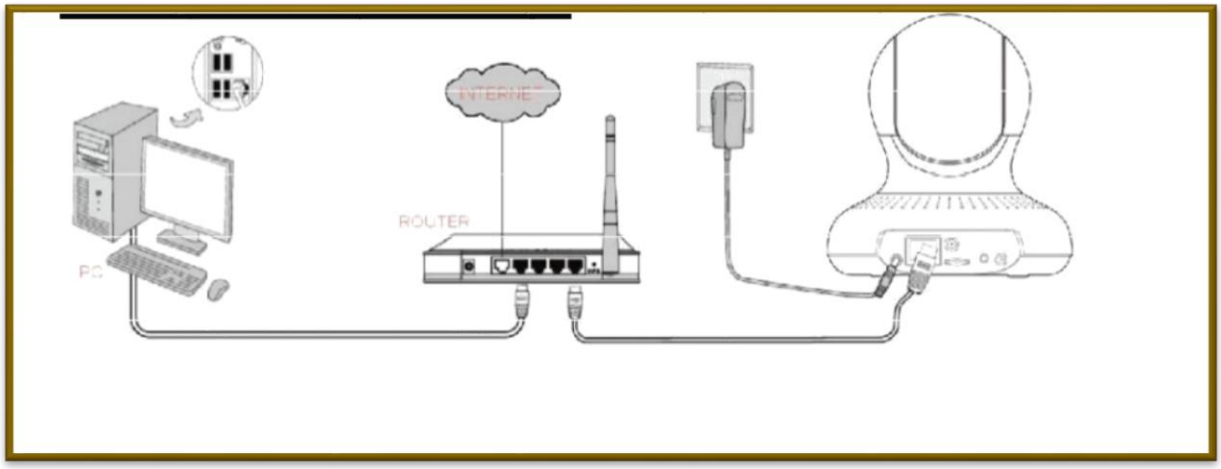
Framework), telnet,etc...

**¿Qué es una cámara IP?**

Una cámara de sistema, también llamada cámara IP, se puede representar como una cámara y una PC consolidada para dar forma a una unidad solitaria. Los segmentos principales que incorporan este tipo de cámaras del sistema incorporan un punto focal, un sensor de imagen, al menos un procesador y memoria. Al igual que una PC, la cámara del sistema tiene su propia dirección IP, está legítimamente asociada con el sistema y se puede colocar en cualquier área donde haya una asociación del sistema. Este componente es la distinción de una cámara web, que debe ejecutarse cuando se asocia con una (PC) a través del puerto USB o IEE 1394

**¿Cómo se conecta una cámara IP?**

La cámara Ip viene con dos puertos, uno para el conector RJ45 y otro para la fuente de Poder. Y se conectan de la siguiente manera:




**Sintetice:** _____

_____

_____

_____

_____

_____

# HOJA DE PRACTICA Nº1

**IV. TÍTULO**: Aplica el protocolo TCP/IP en la configuración de una cámara IP.

**V. PROPÓSITO**: Al término de la práctica el estudiante aplicará el protocolo TCP/IP para configurar una cámara IP.

**VI. PROCEDIMIENTO:**

La cámara IP puede interactuar con NVR y la PC legítimamente sin NVR para ahorrar archivos de video en la PC. En el caso de que la cámara esté asociada con el NVR, sería ideal si aludiera al manual del NVR. En el caso de que la cámara se asocie directamente a la PC, si no le importa aludir a esto.

**Parte I: conexión de LAN**

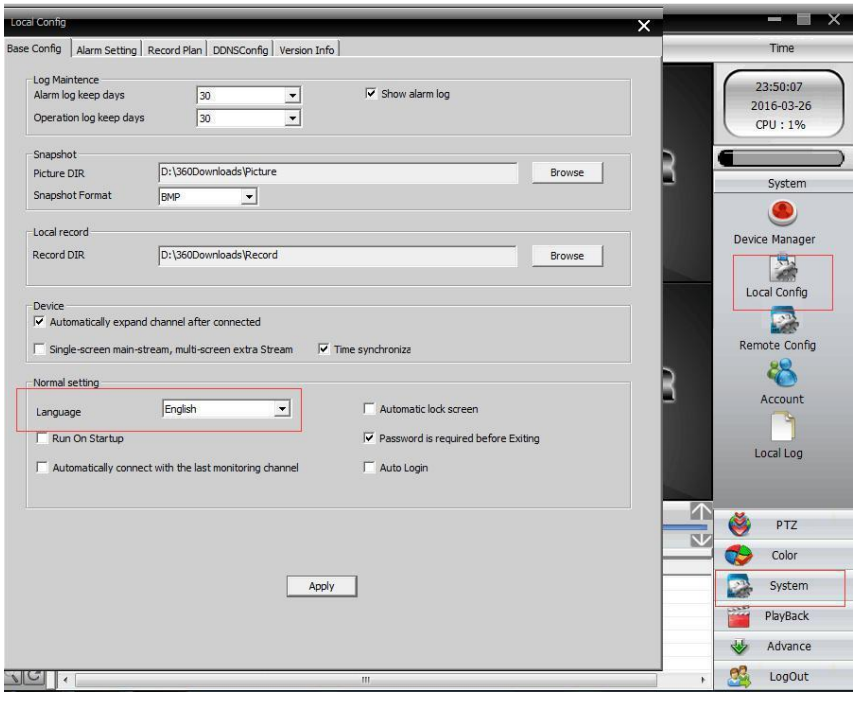
"Antes de la actividad, debemos familiarizarnos con la cámara IP (cuyo inicio tarda aproximadamente 90 segundos) y, simultáneamente, asociar la cámara IP y la PC a un interruptor o interruptor similar, manteniendo el sistema líquido. Después del inicio típico del hardware, la cámara, la PC y el conmutador estructuran una LAN sencilla a través de las líneas" (Perez, 2001, p.67).

Notas: La dirección IP predeterminada al momento del transporte es 192.168.1.10 de China, debe modificarla al área residencial.

Abra General-CMS-Chn y pulse dos veces para introducir, y formará un símbolo de cámara en el área de trabajo de la PC después del establecimiento: CMS.

1. Ingresar al software CMS, se requiere seleccionar idioma a la primera vez. El usuario predeterminado por defecto es "super", y la contraseña predeterminada es vacía.

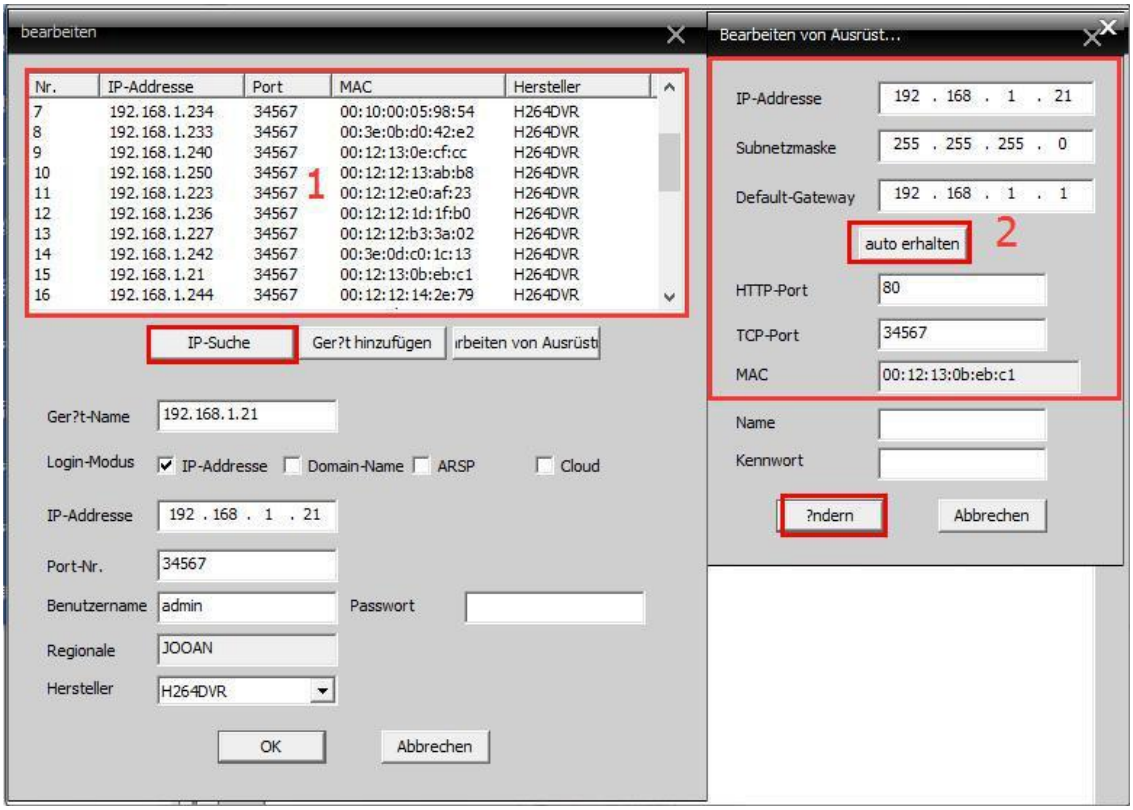
2.



**3.** En ese punto, ingrese al CMS para diseñar: haga clic en la configuración del marco a un lado debajo - organización de los enfoques de reconocimiento - incluya zonas - fabrique una zona de organización. Seleccione la zona adicional, haga clic en incluir gadget - búsqueda de IP - seleccione la dirección IP del gadget que se ajustará - altere el equipo - seleccione el logro programado, en ese momento el gadget cambiará la dirección IP de la cámara en consecuencia como lo indica la PC de flujo y reflujo - cambio como apareció en el adjunto figura:

**4.** El segmento resaltado como bloque "1" es lista de equipos, y todas las direcciones IP buscadas, se muestran en forma de lista.

**5**. El segmento resaltado con el numero "2" es lista de información de los equipos que muestra dirección IP de equipos, su máscara de subred, portal, terminal y dirección física o dirección MAC. Aquí se puede modificar información de dirección de equipos.

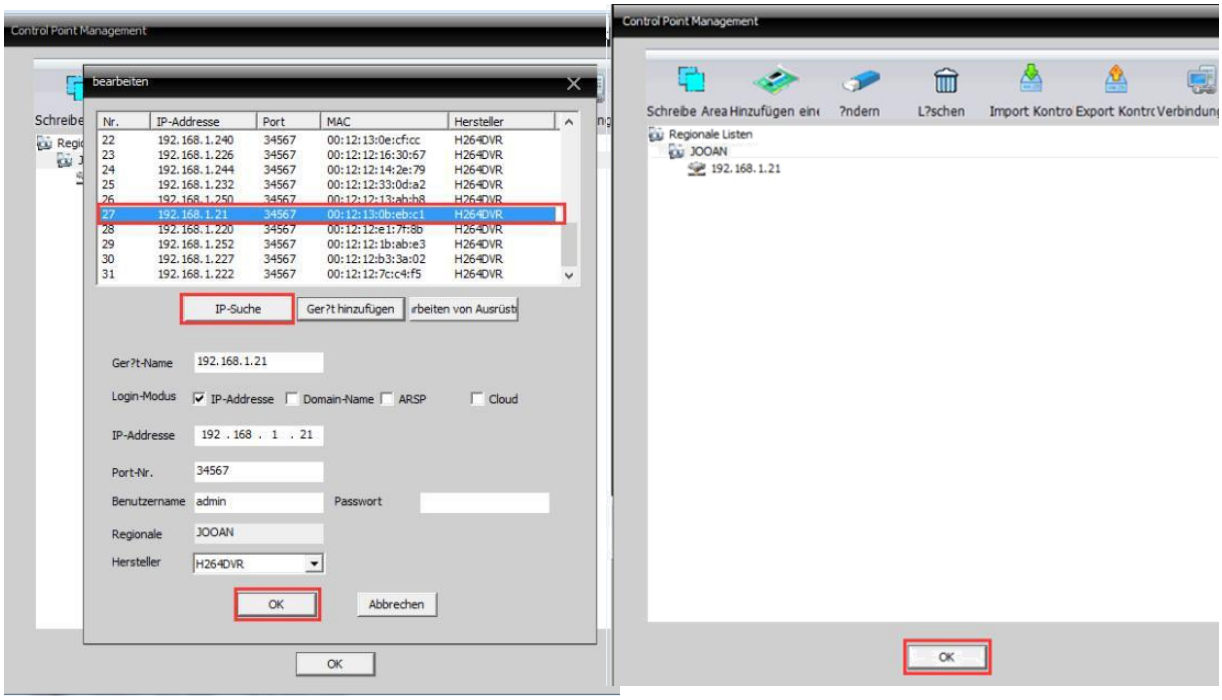


1. **Conexión vía página web.**

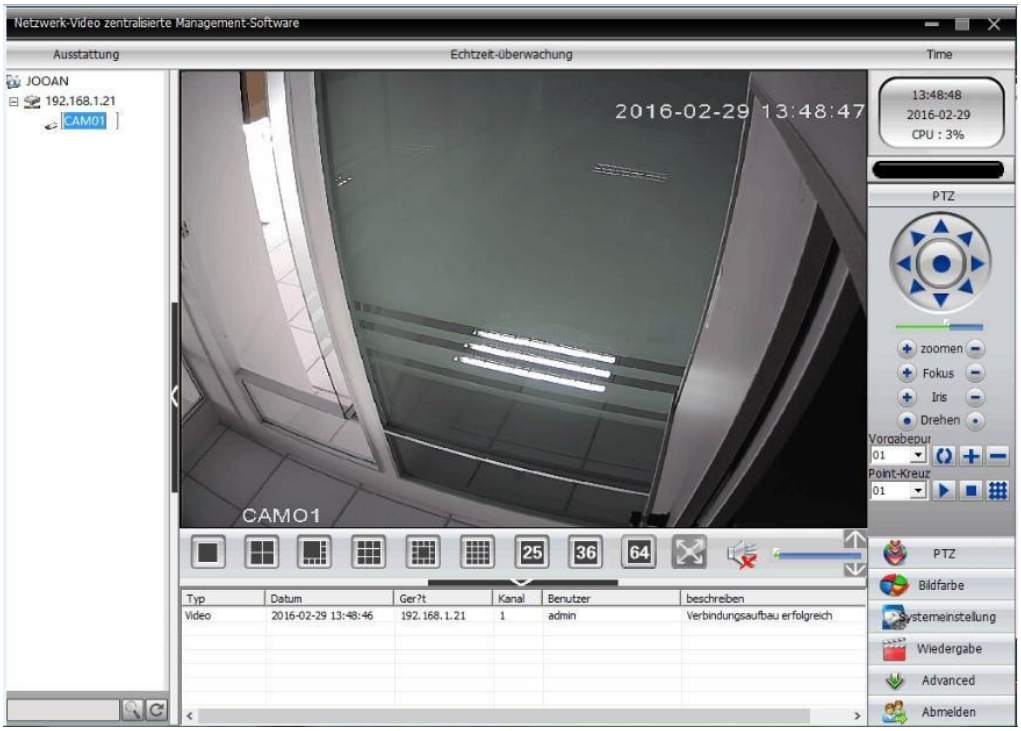
Ingrese la dirección IP del gadget en la barra de direcciones del programa para la interfaz, que mostrará la página de inicio de sesión cuando se asocie directamente. (Nota: solo el programa IE es apropiado). Ingrese el nombre de usuario y la clave secreta - haga clic en Intro - seleccione flujo (flujo real: imágenes claras, enorme paquete de información, interés extremo en el sistema y no líquido en el control remoto. Menos flujo: al revés). Snap afirma ingresar las imágenes para verlo. Nombre de usuario predeterminado: administrador, clave secreta: sin completar, como aparece en la figura

2. **CMS, software de administración concentrada de cámaras web.**

Abra el CMS, debe elegir el idioma en la primera ejecución, en ese punto ingrese el CMS para diseñar: haga clic en la configuración del marco a un lado debajo - organización de los enfoques de reconocimiento - incluye zonas - fabrique una zona de organización. Seleccione la zona adicional y seleccione para incluir gadgets, haga clic en la búsqueda de IP en la página mostrada - busque dispositivos en línea y seleccione los descubiertos, seleccione para incluir, como se muestra en la figura:




Pueden ver los equipos añadidos en el lado izquierdo superior de la interfaz de CMS después de haber añadido, doble click en el equipo IP para ver imágenes. Como se muestra en la siguiente imagen:




Para poder conectar a múltiples equipos, debe de repetir todos los pasos anteriormente mencionados. También se puede conectar a un NVR así se puede almacenar el video de todas las cámaras conectadas y configuradas, estos equipos llevan discos duros de 1tb a más y dependerá de la calidad en pixeles de las cámaras ya que mientras más alta es la calidad más capacidad de almacenamiento requerirá el NVR.

# I.E.P. VIRGEN DEL ROSARIO DE YUNGAY. EIRL

- NIVEL: SECUNDARIO
- GRADO: QUINTO
- DOCENTE: SÁNCHEZ LUIS, CARLOS MARX

## LISTA DE COTEJO

| | INDICADORES / APELLIDOS Y NOMBRES | Conoce los procedimientos de | Identifica los hosts a configurar y conectar. | Aplica el direccionamiento IP | Sigue de manera puntual el | Configuro correctamente la | TOTAL |
|---|---|---|---|---|---|---|---|
| 01 | Alvarado Balcázar, Alison | | | | | | |
| 02 | Huarca Cusihuamán, Kevin | | | | | | |
| 03 | Bulnes Montenegro, Sebastián | | | | | | |
| 04 | Cornejo Leveratto, Sofia | | | | | | |
| 05 | León Rioja, Fiorella | | | | | | |
| 06 | Gamboa Velásquez, Nelly | | | | | | |
| 07 | Linares Cuevas, Mayra | | | | | | |
| 08 | Mengoni Reátegui, Francesco | | | | | | |
| 09 | Meza Calle, Marcelo | | | | | | |
| 10 | Paez Torres, Bridggite | | | | | | |
| 11 | Romero Guerrero, Matías | | | | | | |
| 12 | | | | | | | |

_____

FIRMA

# I.E.P. VIRGEN DEL ROSARIO DE YUNGAY. EIRL

- NIVEL: SECUNDARIO
- GRADO: QUINTO
- DOCENTE: SÁNCHEZ LUIS, CARLOS MARX

## HOJA DE EVALUACIÓN

**1) Reconoce las partes del dispositivo y escríbelo en el espacio. (2 pts cada una)**


**2) Marca la alternativa correcta. (2 pts. cada una)**

**a) ¿Qué es significan las siglas TCP?**

Tecnología Comunicación Privada ☐

Transmission Control Protocol ☐

Terry's Computer Pops ☐

**b) ¿Qué significan las siglas de nuestra querida asignatura TIC?**

Televisión Intercomunicación configuración ☐

Tecnologías de la Información y la Comunicación ☐

Tecno Info Clara ☐

**c) ¿Qué significa las siglas NIC?**

Nickname ☐

No Información Conocida ☐

Network Interface Card ☐

**3) Señale verdadero o falso en la elipse. (2 pts. cada una)**

b) El router es un dispositivo que distribuye tráfico entre redes ◯

a) La dirección Ip v4 está formada por 4 octetos y mide 32 bits? ◯

**FICHA DE METACOGNICIÓN**

¿QUÉ APRENDI LA CLASE DE HOY?

---
---
---
---
---
---

¿CÓMO ME SENTI EN LA CLASE?

---
---
---
---
---
---

¿QUÉ DIFICULTADES TUVE?

---
---
---
---
---
---

¿CÓMO FUE QUE APRENDI?

---
---
---
---
---
---
---
---

## Síntesis

La Agencia de Investigación de Proyectos Avanzados de 1968 del Departamento de Defensa de los Estados Unidos (DARPA) inicia el programa de mejora que permitiría la transmisión de datos entre sistemas de diversos tipos y atributos. Se actualizó un sistema de línea telefónica punto a punto llamado ARPANET, utilizando muchas convenciones que luego se llamarían TCP / IP. Este sistema enmarcado por asociaciones instructivas, militares y de investigación se convirtió en el centro de Internet alrededor de 1980, y en 1983, todos los anfitriones de ARPANET utilizaron este arreglo de convenciones.

Como hemos encontrado en la sección anterior, los elementos de un sistema de PC pueden fundarse en los siete grados del modelo OSI, a pesar de que el uso real de un sistema puede contrastar en el grado de sentido común de ese modelo. No existe una amplia concurrencia sobre la mejor manera de mostrar la disposición de las convenciones TCP / IP con un modelo de capas. En su mayor parte, en algún lugar en el rango de tres y cinco niveles útiles se exhiben como sustanciales en la ingeniería de convenciones.

**Nivel primero o de acceso a la red**

Para Andrew (2003):

> Este es el nivel inferior de la cadena de comando de la convención TCP / IP. Las convenciones en esta capa dan paso al marco para transmitir la información a diferentes dispositivos directamente asociados con el sistema. Caracterice cómo utilizar el sistema para transmitir un datagrama IP (p.176).

En este nivel, los datagramas de IP son carcasas de configuración incorporadas que se transmiten al sistema y cambian las entregas de IP a las formas físicas que se utilizan en el sistema. Un caso de una convención de este nivel sería ARP (Protocolo de

resolución de direcciones) en LAN y SLIP (Serial Line Ip) o PPP (Protocolo punto a punto) se organiza en sistemas WAN.

**Nivel segundo o de internet**

Para Ross (2001) afirma:

> Este nivel controla la correspondencia entre los grupos, escogiendo el curso más adecuado que los paquetes de información deben seguir para llegar a su objetivo. Es la administración esencial de transporte de paquetes en la que se fabrica un sistema TCP / IP (p. 278).

El protocolo más importante de este nivel es IP (Internet Protocol).

**Nivel tercero o de transporte**

Fomenta la correspondencia punto a punto, comenzando con un programa de aplicación y luego con el siguiente, asegurando que es esencial que la información toque la base sin errores y en la sucesión correcta. Haga una suma de verificación para confirmar igualmente que los datos no han sido alterados durante la transmisión (Stallings, 2008).

Los protocolos de este nivel son TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

**Nivel cuarto o de aplicación**

Es el nivel o capa final donde el usuario puede palpar toda la información ya descifrada y visual, auditiva también encontramos aquí los protocolos o lenguajes HTTP, FTP, SMTP, NFS, etc.

## Apreciación crítica y sugerencias

Cuando hacemos clic en un link, se produce un flujo de información dentro del computador, el cual es empaquetado, etiquetado y es puesto en camino; todo lo hace la IP.

Una red LAN no es nada controlado y pueden ocurrir accidentes.

La disposición de las convenciones TCP / IP ha sido de importancia esencial para el avance de los sistemas de correspondencia, particularmente para Internet.

El ritmo de la extensión de Internet es también el resultado de estas convenciones, sin las cuales los sistemas de interfaz de varias naturalezas (hardware distintivo, marco de trabajo, etc.) habrían sido sustancialmente más problemáticos, si es que fuera posible.

Las convenciones de TCP / IP fueron y son el motor vital para que los sistemas en general, y específicamente Internet, mejoren y se pueda lograr un "camino de datos" decente.

Para beneficiarse de este tipo de cámaras, se prescribe profundamente comprar una grabadora NVR, con el objetivo de que la cámara no solo nos muestre lo que está sucediendo en un lugar específico, sino que se grabará en el círculo rígido incorporado en la grabadora.

Dentro de las cámaras avanzadas podemos elegir, entre algunos modelos, en los que los ángulos, por ejemplo, los objetivos de la imagen, la estrategia de grabación fluctuará, independientemente de si tiene infrarrojos, sonidos, alertas, etcétera.

Se recomienda la instalación de cámaras IP.

Dentro de las aulas: Se elimina el desorden, falta de respeto de los estudiantes y aumenta la productividad tanto del profesor como de los estudiantes.

Además, ayudan con el reconocimiento y el control de seguridad fuera de estos lugares para evitar y controlar robos y peligros por parte de personas fuera de la base instructiva.

Tener la opción de "filtrar" su hogar, negocio, organización, personas mayores, jóvenes o bebés, y hacerlo desde su trabajo, desde su lugar de escape, desde cualquier lugar con una asociación de Internet.

## Referencias

Andrew, S. (2003), *Computer Networks*. New Jersey, USA: Prentice Hall.

Andrew, S. (2003), *Redes de computadores.* New Jersey, USA: Prentice Hall.

James, F. y Keith, W. (2001), *Redes de Computadores. A top-down approach featuring the Internet.* Massachusetts, USA: Addison Wesley.

Palet, J. (2007). *The Choice: IPv4 Exhaustion or Transition to IPv6*. Recuperado de http://www.ipv6tf.org/pdf/the_choice_ipv4_exhaustion_or_transition_to_ipv6_v4.4.pdf.

Pérez, G. y Silva, M. (2001). *Rain Attenuation Considerations in Broadband Wireless Systems Operating at Frequencies Above 10 GHz*. Recife, Brazil.

Stallings, W. (2008). *Data and computer communications*. New Jersey, USA: Prentice Hall.

Stallings, W. (2000), *Comunicaciones y redes de computadores*. Madrid, España: Prentice-Hall.

# Apéndices

## Apéndice A: Glosario

**DVR**: Un grabador de vídeo digital (DVR por las siglas en inglés de Digital Video Recorder) es un aparato electrónico que permite grabar y almacenar todas la imágenes en video de las cámaras instaladas y conectadas a él.

**PAL (Phase-Alternating Line):** Es el marco de codificación utilizado en la transmisión de la bandera de TV de sombreado simple en muchas partes del mundo. Se utiliza en la mayoría de las naciones africanas, asiáticas y europeas, a pesar de Australia y algunas naciones americanas. Su particular es 625 líneas a 50Hz.

**ARP (Address Resolution Protocol:** Protocolo de resolución de direcciones)
Esta convención se utiliza para relacionar una dirección IP con una dirección MAC del equipo. Se transmite una solicitud en el sistema del vecindario para encontrar la dirección MAC de una dirección IP.

**DHCP (Dynamic Host Configuration Protocol:** Protocolo de configuración dinámica de hosts): Es una convención que permite organizar a los supervisores para que se mecanicen y se ocupen a medias de la tarea de las direcciones IP (Protocolo de Internet) con los dispositivos del sistema.

**FTP (File Transfer Protocol, Protocolo de transferencia de archivos):** Es una convención de aplicaciones que utiliza las convenciones TCP / IP, utilizadas para intercambiar documentos entre PC o dispositivos en sistemas.

**HTTP (Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto):** HTTP es la disposición de principios utilizados para intercambiar registros (documentos de contenido,

diseños, imágenes, sonido, grabaciones y otros registros de medios) en la Web. La convención HTTP sigue corriendo sobre la disposición de las convenciones TCP / IP.

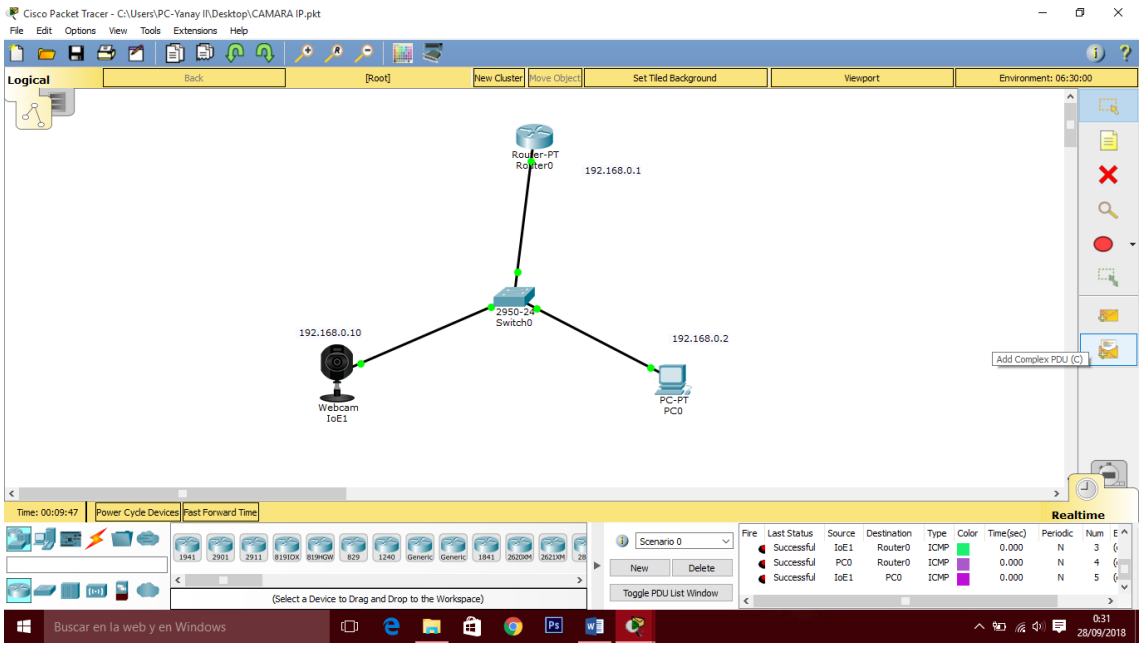
**PPTP (Point-to-Point Tunneling Protocol, Protocolo de túneles punto a punto):** Convención (conjunto de corridas de correspondencia) que permite a las organizaciones expandir su propio sistema corporativo a través de "madrigueras" privadas en el arreglo abierto de Internet. En este sentido, una organización puede utilizar una WAN (Red de área amplia) como una LAN (Red de área local) enorme y solitaria. Este tipo de interconexión se llama sistema privado virtual (VPN

**SOCKETS**: Los sockets son una técnica para la correspondencia entre un programa de cliente y un programa de servidor a través de un sistema. Un archivo adjunto se caracteriza como "la parte del trato". Los archivos adjuntos se hacen y utilizan con muchas solicitudes de programación o "llamadas de capacidad", que a veces se denominan "interfaz de programación de aplicaciones (API) de archivos adjuntos".

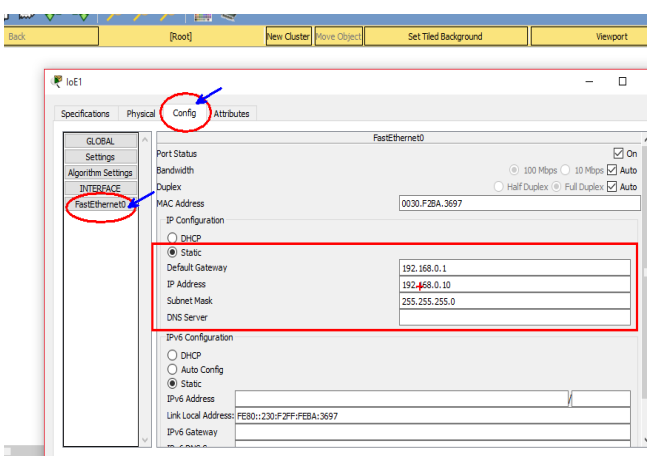
**UDP (User Datagram Protocol, Protocolo de datagramas de usuario)**: Es una convención de intercambios que ofrece un soporte limitado de información comercial en un sistema que utiliza el Protocolo de Internet (IP). UDP es una opción en contraste con el Protocolo de Control de Transmisión (TCP).

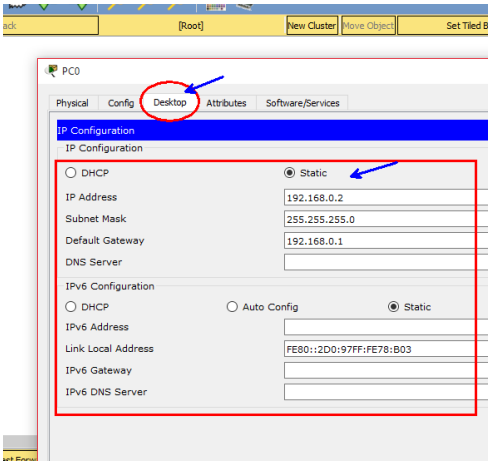
# Apéndice B: Programa Cisco Packet Tracer

- **Diseño del proyecto**

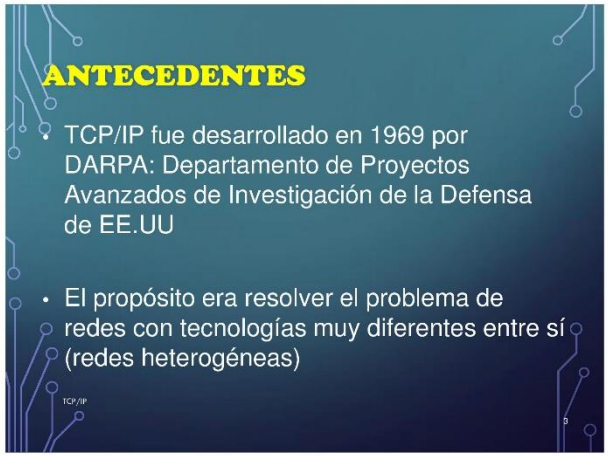


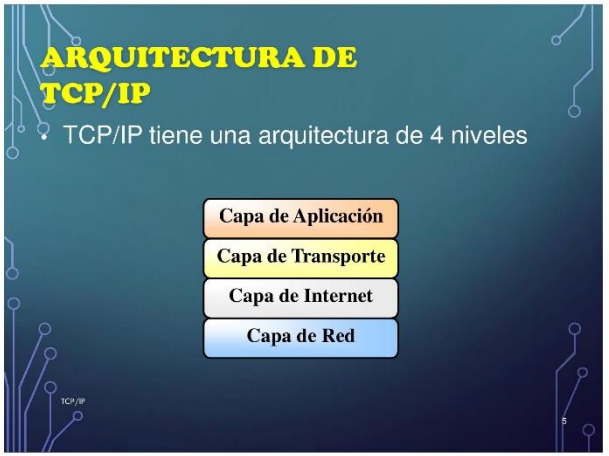

- **Configuración de la IP en los dispositivos**

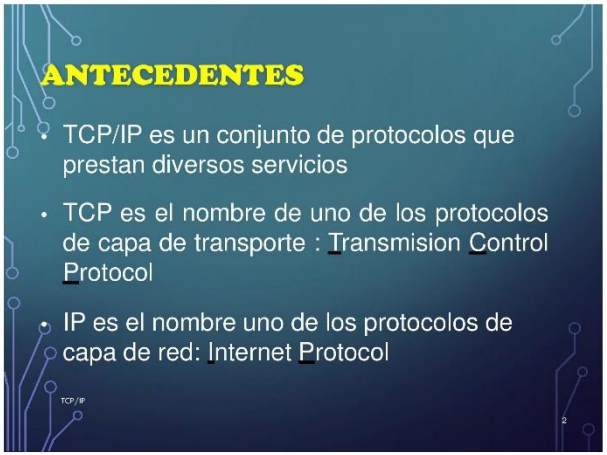


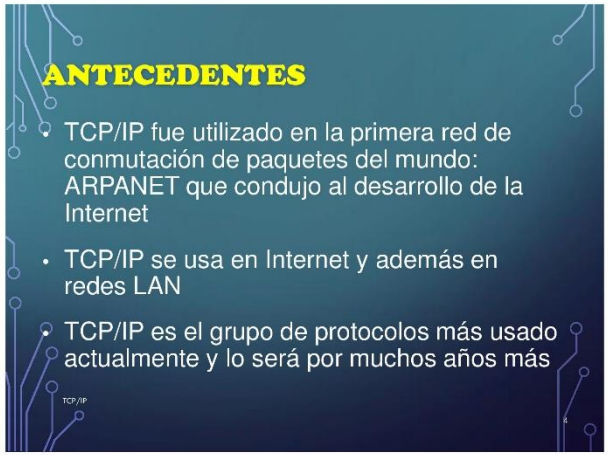



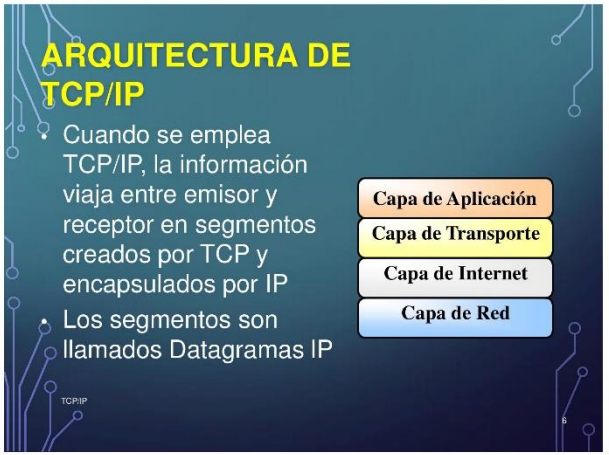
## Apéndice C: Diapositivas

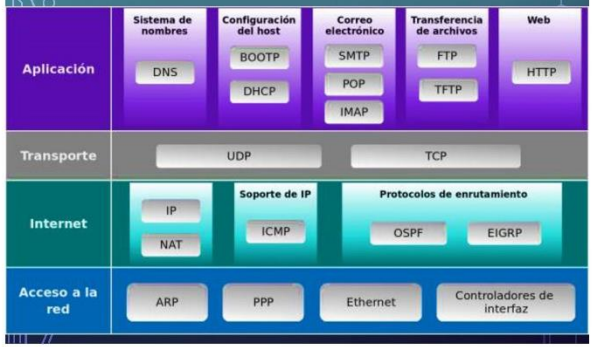



## ARQUITECTURA DE TCP/IP




## COMUNICACIÓN ENTRE REDES

- Dos redes diferentes, que utilizan el mismo protocolo de comunicaciones TCP/IP, pueden comunicarse entre sí, sin que los equipos tengan que ser de la misma marca o fabricante
- Por ejemplo una estación con Windows NT de Microsoft puede intercambiar datos con una computadora Sun con Solaris

TCP/IP 8

## PROTOCOLOS DE COMUNICACIÓN

- Pueden existir dos grandes tipos de protocolos:
  - Protocolos orientados a conexión
  - Protocolos no orientados a conexión

TCP/IP 9

## PROTOCOLO ORIENTADO A CONEXIÓN

- Un protocolo orientado a conexión proporciona un servicio similar al provisto por el servicio telefónico, tiene 3 fases distintas:
  - Establecer la conexión
  - Transferencia de datos
  - Terminar la conexión

TCP/IP 10

## PROTOCOLO NO ORIENTADO A CONEXIÓN

- Un protocolo no orientado a conexión proporciona un servicio similar al provisto por el servicio de correo postal
- La comunicación tiene solo una fase simple pues no requiere establecer la conexión
- El mensaje se identifica con la dirección de fuente y la del destino
- No es un servicio confiable

TCP/IP 11

## ENRUTAMIENTO EN TCP/IP

- El enrutamiento es el proceso a través del cual dos estaciones que se comunican se encuentran y usan la mejor trayectoria de una red TCP/IP sin importar la complejidad
- Componentes del enrutado:
  - Determinar las trayectorias disponibles
  - Seleccionar la mejor trayectoria
  - Enviar el paquete por la mejor ruta

TCP/IP 12

## DIRECCIONAMIENTO TCP/IP

- Una dirección IP es un conjunto de cuatro números decimales cada uno formado por un byte y que se escriben separados por un punto, en total son 32 bits; por ejemplo:

  200.10.4.8

- Cada host debe tener una dirección IP única



## DIRECCIONAMIENTO IP

- La máscara contiene unos (1) en la parte correspondiente a la red y ceros (0) en la parte correspondiente al host




## DIRECCIONAMIENTO IP

Clases de redes

| Clase de red | 1er byte | máscara | Total redes | Host por red |
|---|---|---|---|---|
| A | 1 .. 126 (01…) | 255.0.0.0 | 126 | 2**24-2 = 16777214 |
| B | 128 .. 191 (10…) | 255.255.0.0 | 64*256= 16384 | 2**16-2 = 65534 |
| C | 192 .. 223 (110…) | 255.255.255.0 | 32*256* 256=2097152 | 254 |
| D | 224 .. 239 | N/A | 16 | |
| E | 240 .. 254 | N/A | 7 | |



## DIRECCIONAMIENTO IP

- Una dirección IP consta de dos partes:
  - La dirección de red
  - El número de host


- La red se distingue del host por medio de la máscara

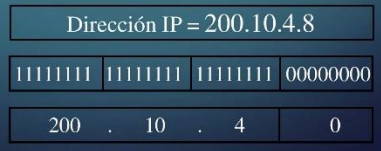


## DIRECCIONAMIENTO IP

- Ejemplo:

  Dirección IP = 200.10.4.8

  Máscara = 255.255.255.0






## DIRECCIONAMIENTO IP

Tipos de direcciones IP

- Direcciones IP públicas

  (administradas por NIC o por sus representantes, los proveedores de servicios)

- Direcciones IP privadas

  (pueden ser usadas sin requerir permiso por cualquiera)

## DIRECCIONAMIENTO IP

Direcciones IP privadas

| Clase de red | redes | máscara | Total redes | Host por red |
|---|---|---|---|---|
| A | 10.0.0.0 | 255.0.0.0 | 1 | 256*256*254 = 16.646.144 |
| B | 172.16.0.0 a 172.31.0.0 | 255.255.0.0 | 16 | 256*254 = 65.024 |
| C | 192.168.0.0 a 192.168.255.0 | 255.255.255.0 | 256 | 254 |



## DIRECCIONAMIENTO IP

Conversión binario a decimal

- La numeración binaria es posicional (como la decimal) pero tiene solo dos valores 0 y 1

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |

128+ 0+ 32+ 16+ 0+ 4+ 2+ 0 = 182

- Todos los bits en 1 equivalen a 255



## DIRECCIONAMIENTO IP

De los bits a los bytes

- Bit : 1 ó 0 (unidad básica de información)
- Byte (8 bits)

| 1 | | | | | | | |
|---|---|---|---|---|---|---|---|