

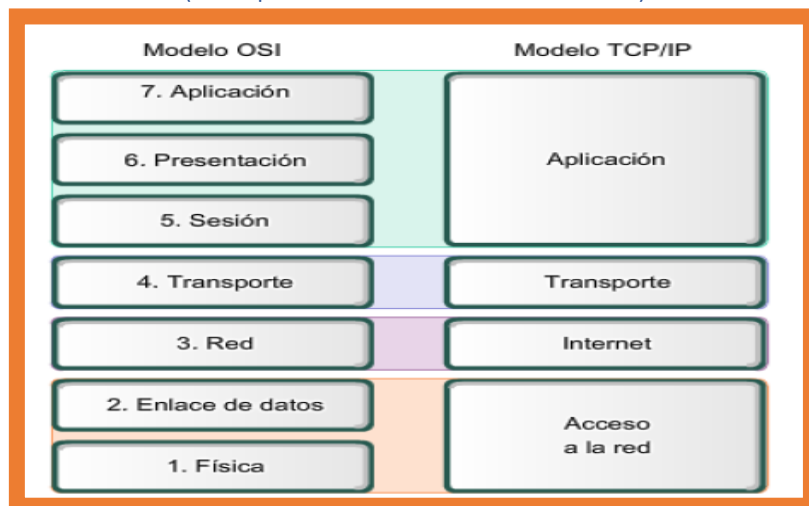
## Unidad 4 – PROTOCOLOS

### Protocolo TCP/IP:

Protocolo de Control de Transacciones / Protocolo de Internet

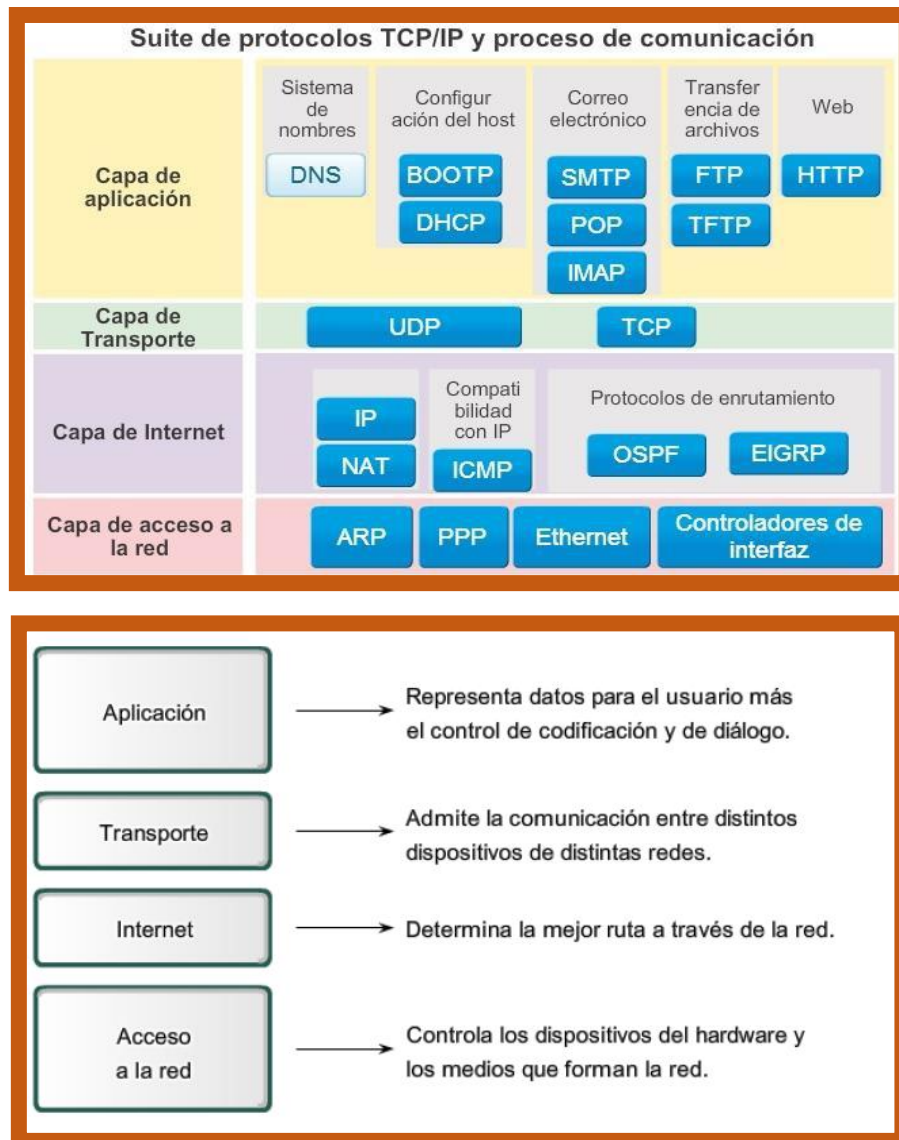
- Es un conjunto de protocolos desarrollado en los 70 y se convertido en norma para ARPANET en 1983
  - UNIX lo incorpora para su amplia difusión
  - Acompaña la evolución de internet IPV4/Internet 2/ IPV6
  - Muchos programas dentro de una red de datos compuesta por [computadoras](#) pueden usar TCP para crear *conexiones* entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de [puerto](#).
  - TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas [HTTP](#), [SMTP](#), [SSH](#) y [FTP](#).
- 
- IP Basica como una red sin conexiones
  - Una red IP Networking hace más fácil el escalamiento
    - Servicios y aplicaciones no estáticamente vinculadas con la infraestructura de la red
      - Mantiene la complejidad fuera del nucleo de la red
      - Permite la rápido creación de nuevos servicios
    - Diseñada para compartir información
  - Permiso para decisiones autónomas mediante nodos de red procesando cada paquete
    - Los paquetes transportan globalmente direcciones con sentido
    - Procesamiento distribuido a través de toda la red
    - Provee redundacia, mejora la escalabilidad

### Modelo de Protocolo de Internet (Comparación con el modelo OSI)



- Capa de Acceso a RED:
  - Se encarga del intercambio entre un host y la red y entre los dispositivos de la misma red
  - Proporciona el mecanismo abstracto de direcciones para la entrega de datos
- Capa Internet:
  - Encamina los mensajes a través de las redes e interredes.
  - Interactúa con los Routers y Gateways.
  - Utiliza el protocolo IP y ARP
  - Implementa un diagrama de direcciones lógicas de Hosts denominadas Direcciones IP
- Capa Host a Host

- Se encarga del control de integridad de datos (control de calidad)
- Utiliza protocolos TCP y UDP
- TCP => Fiable
- UDP => No fiable
- Capa Proceso/Aplicación:
  - Abarca las funciones de las capas sesión, presentación y aplicación.
  - Incluye los protocolos FTP, TELNET, SMTP, SNMP, NFS.



Esquema TCP/IP

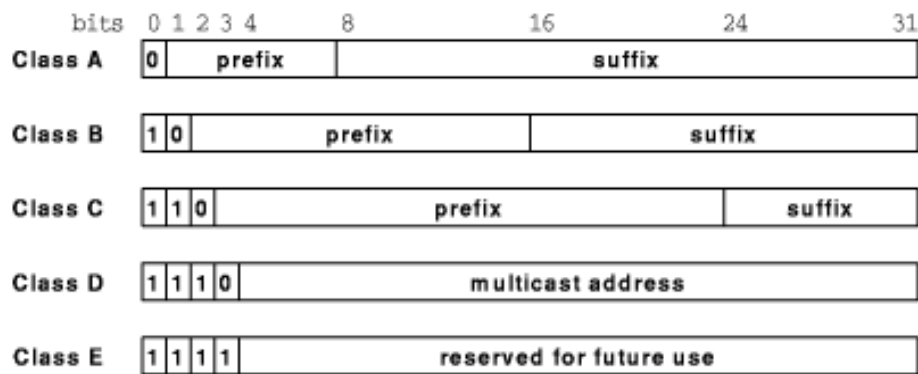
- **Computadora Host** : Cualquier Sistema de Computo conectado que ejecute una aplicación (dentro de este esquema).
- **Routers** : Encargados de Enrutar a través de los medios físicos los paquetes en las red.
- **TCP/IP** : Provee el Software para realizar esta Comunicación/Intercambio de paquetes.

#### Direccionamiento IPV4:

- **Oculto detalles de Redes Físicas y ofrece las características de una Red Virtual (Heterogénea).**
- **Define un Esquema de Direccionamiento Abstracto que asigna a cada Host una Dirección UNICA.**
- **Los usuarios, los programas de aplicación y las capas superiores del protocolo usan las direcciones abstractas para comunicarse.**

- **Dirección IP :** Es un número de 32 Bits asignado a un Host y usado para todas las comunicaciones con El.
- **Jerarquía de Direcciones :**
  - **Prefijo :** Identifica a la Red Física que está conectada la computadora.
  - **Sufijo :** Identifica a cada Host de la Red.
- **Ventaja :** Facilita el Enrutamiento de los usuarios asegurando:
  - A cada computadora se le asigne una dirección única.
  - Aunque las Direcciones se coordinen globalmente los sufijos pueden asignarse de manera Local.
- **Capas – Direcciones de protocolo**
  - Se esconden las capas físicas para utilizar las capas superiores ➤ ➤ **Direcciones Lógicas (Heterogeneidad)**
- **Direccionamiento IPv4 Estático**
  - Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host, como se muestra en la figura. Como mínimo, esto implica ingresar la dirección IP del host, la máscara de subred y el 208ersión por defecto. Las direcciones estáticas tienen algunas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos de red que deben ser accesibles a los clientes de la red. Al utilizar direccionamiento IP estático, es necesario mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Éstas son direcciones permanentes y normalmente no vuelven a utilizarse. Cualquier recurso de red como un servidor o una impresora debe tener una dirección Ipv4 estática, como se muestra en la figura. Los hosts clientes acceden a estos recursos utilizando las direcciones Ipv4 de estos dispositivos. Por lo tanto, son necesarias direcciones predecibles para cada uno de estos servidores y periféricos. Utilizar un sistema de numeración consistente para estos dispositivos facilita la identificación
- **Direccionamiento Dinámico**
  - El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de subred, el 209ersión por defecto y otra información de configuración. La configuración del sevidor DHCP requiere que un bloque de direcciones, llamado conjunto de direcciones, sea definido para ser asignado a los clientes DHCP en una red. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos. Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la “alquila” durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.

## Clases de direcciones:



- Las Clases A, B, y C se llaman Clases Primarias porque contienen direcciones de Host (Sufijos).
- La Clase D se utiliza para multitransmisión IP, permitiendo entregar paquetes a un Grupo de Computadoras.
- De acuerdo a los primeros 4 Bits de la Dirección se define la CLASE.
- 

32-bit Binary Number				Equivalent Dotted Decimal
10000001	00110100	00000110	00000000	129 . 52 . 6 . 0
11000000	00000101	00110000	00000011	192 . 5 . 48 . 3
00001010	00000010	00000000	00100101	10 . 2 . 0 . 37
10000000	00001010	00000010	00000011	128 . 10 . 2 . 3
10000000	10000000	11111111	00000000	128 . 128 . 255 . 0

Clase de Dirección				
A				
B	14	16384	16	65536
C	21	2097152	8	256

## Direcciones Privadas:

- Set de direcciones para uso p...
- Estas direcciones no son rute...
- Los routers no distinguen las...

Class	Range of Values
A	0 through 127
B	128 through 191
C	192 through 223
D	224 through 239
E	240 through 255

ntes del interior.  
arla traducción.

Clase	Desde	Hasta
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.16.255.255
C	192.168.0.0	192.168.255.255

## Mascara de Red

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. En formato binario todas las máscaras de red tienen los "1" agrupados a la izquierda y los "0" a la derecha

- *Numero de 32 Bits Igual a una Dirección IP.*
- *Delimitar el ámbito de una red de computadoras.*
- *Sirve para distinguir cuando una máquina determinada pertenece a una subred dada.*
- *Indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al Host.*

Clase	Máscara (decimal)	Máscara (binario)	Prefijo
A	255.0.0.0	11111111.00000000.00000000.00000000	/8
B	255.255.0.0	11111111.11111111.00000000.00000000	/16
C	255.255.255.0	11111111.11111111.11111111.00000000	/24

- *Algunos ejemplos:*
- 1- Red de Clase C                      192.168.1.0      255.255.255.0
- 2- Red de Clase B                      172.17.0.0      255.255.0.0
- 3- Red de Clase A                      10.0.0.0      255.0.0.0
- 4- Host de Clase B                      172.17.1.0      255.255.0.0
- 5- Host de Clase A                      10.1.0.0      255.0.0.0

## Routers y Direccionamiento

- *Los Routers tienen conexiones a varias redes físicas*
- *Cada Dirección IP tiene un prefijo que especifica una Red Física*
- *Los Routers manejan una Tabla de Enrutamiento entre Redes*

## Host Multibase

- *Host que se conecta a varias conexiones de Red.*
- *Suelen utilizarse para aumentar la confiabilidad, Aumentar el rendimiento o ancho de banda.*
- *Evita la congestión de Tráfico.*
- *Cambia la configuración de los Enrutadores*
- *Solución aplicada a la falta de ancho de banda (conexión excesivamente lenta) para cumplir con el Servicio de conexión de Internet respecto de Nuestro ISP . Se puede suplir con :*
  - **Aumento de Ancho de Banda (Análisis de Costo).**
  - **Cambio de Políticas en el Uso de Internet.**

- **Adquisición de Herramientas que controlen Servicios, Accesos, Correo electrónico, Etc.**

- *Solución Necesaria para evitar la salida de servicio de nuestro Nodo (Aumento de Confiabilidad).*

#### 24 HS porque es vital para nuestro Negocio

- Un Único Router debe tener las dos o mas conexiones y poder balancearlas soportando el uso del Protocolo BGP.

#### Border Gateway Protocol.

- NO confundir con un Host con dos canales de Internet con Routers independientes (Direcciones IP Diferentes).

#### Sin Balanceo de Carga.

#### Direcciones de Protocolo

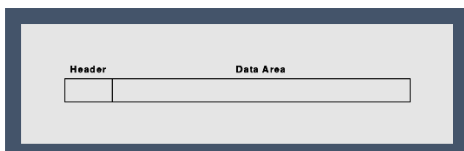
- *Son Abstracciones ofrecidas por Software que permite, antes de enviar el paquete, traducir la dirección del protocolo del siguiente salto equivalente a una Dirección Física.*
- *La correlación entre Dirección de Protocolo y Dirección de Hardware se llama **Resolución de Dirección.***

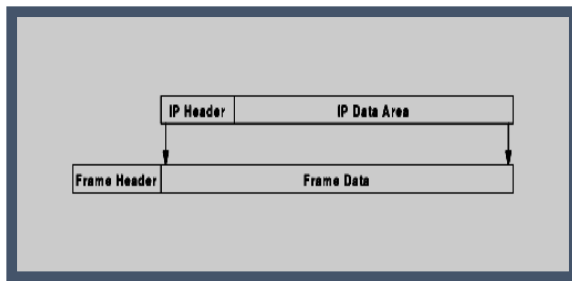
#### Resolución de Dirección

- *Los hosts y los routers sirven para la Resolución de la Dirección en transmisiones de datos entre computadoras*
- *Técnicas de resolución:*
  - *Búsqueda en una Tabla ➡ Resolver direcciones IP a través de una WAN y con el uso de Routers.*
  - *Calculo en forma cerrada ➡ Se utiliza en redes Configurables.*
  - *Intercambio de Mensajes ➡ Se emplea con Hardware de Lan que tiene Direccionamiento Estático.*
  - *ARP( Protocolo de resolución de direcciones)*
    - *Se utiliza en redes LAN TCP/IP homogéneas que tengan el mismo formato de mensajes para resolver todas las Direcciones.*
    - *Cada Computadora recibe la solicitud y examina la dirección IP, la computadora mencionada en la solicitud transmite la respuesta.*
    - *Maneja un Cache con las Respuestas (Direcciones Recibidas) para evitar congestión de tráfico ➡ Reduce el Numero de Solicitudes.*

#### Datagrama IP

- *Nace con la necesidad de trabajar con redes Heterogéneas.*
- *Permite el paso del cuadro de una red a otra.*
- *Formato de paquete independiente del Hardware*



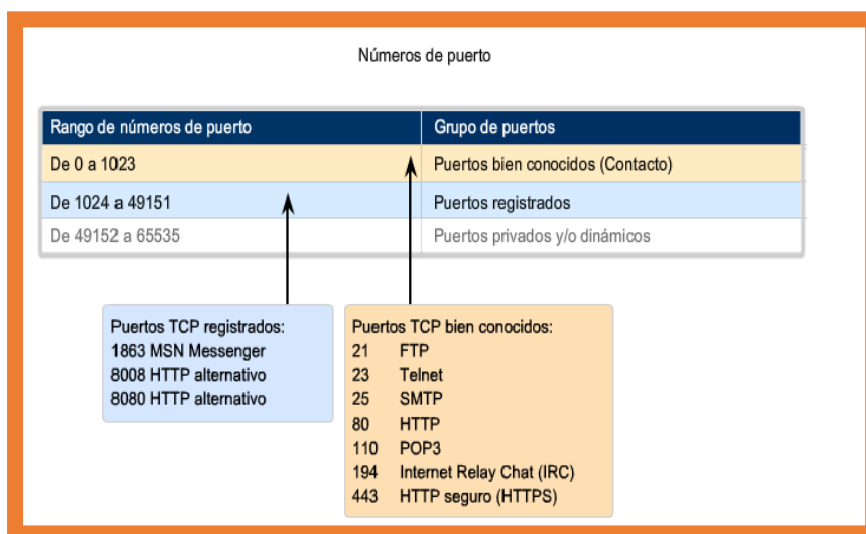


- Encapsulado de datos y la pila de protocolo TCP/IP. El paquete es la unidad de información básica que se transfiere a través de una red. ... Cuando un protocolo del sistema de envío agrega datos al encabezado del paquete, el proceso se denomina encapsulado de datos.

## SEGUNDO POWER POINT

### Puertos:

- **Los Sistemas Operativos establecen servicios, a través de localizaciones lógicas materializadas en direcciones físicas, en donde colocan los mismos para ser accedidos desde otras localizaciones físicas**
- **Estas direcciones se los denomina Puerto.**
- **Son controlados para otorgar y negar servicios.**
- **Los puertos son elementos que se mantienen en permanente escucha de las solicitudes de los clientes.**
- **Todos los servicios disponibles en los computadores tienen asociado un puerto.**
- **Cuando el usuario externo de Internet invoca a una Web o servicio el puerto queda implícito en dicha dirección**
- **Abierto: Acepta conexiones. Hay una aplicación escuchando en este puerto. Esto no quiere decir que se tenga acceso a la aplicación, sólo que hay posibilidad de conectarse.**
- **Cerrado: Se rechaza la conexión. Probablemente no hay aplicación escuchando en este puerto, o no se permite el acceso por alguna razón. Este es el comportamiento normal del sistema operativo.**
- **Bloqueado o Sigiloso: No hay respuesta. Este es el estado ideal para un cliente en Internet, de esta forma ni siquiera se sabe si el ordenador está conectado. Normalmente este comportamiento se debe a un cortafuegos de algún tipo, o a que el ordenador está apagado.**



### SOCKETS:

- **Interfaz de programación de aplicaciones que interactúa con los Protocolos .**
- **Es una norma por Defecto originada en el S.O. Unix versión B (Berkeley).**
- **Existen múltiples API en bibliotecas provistas para distintos sistemas operativos.**

- *Se diseñan para trabajar con aplicaciones concurrentes utilizando un grupo de protocolos y el servicio deseado.*
- *Pueden transferir, recibir y escribir datos (E/S).*

#### CONCEPTOS:

- *Todo dispositivo que se conecte a Internet necesita una dirección IP válida (Pública).*
- *Toda aplicación se identifica, hacia el mundo de las comunicaciones TCP/IP, con un número de puerto (TCP o UDP).*
- *Protocolos comunes de la capa de aplicación son:*
  - *8080 HTTP Protocolo HTTP.*
  - *443 HTTPS Protocolo HTTP sobre TLS/SSL*
  - *DNS 53 Resolución de Nombres de Dominio.*
  - *FTP 20/21 Transferencia de Archivos.*
  - *SMTP 25 Transmisión de e-mail.*
  - *POP3 110 Descarga de e-mail servidor a PC.*
- *El dispositivos de Seguridad (Firewall de red) puede realizar:*
  - *Filtrado de Paquetes,*
  - *Inspección los campos correspondientes a las direcciones IP (origen y destino)*
  - *Inspección del Protocolo.*
  - *Puertos de aplicación (origen y destino).*
  - *Tipo conexión (entrante o saliente).*
  - *Secuencias de paquetes en base a criterios más sofisticados.*
- *→ En un Terminal (Firewall Personal), pueden filtrarse los paquetes en base a las aplicaciones que se están ejecutando.*

#### ICMP (Internet control message protocol)

- *Protocolo de mensajes de control de Internet.*
- *Transmite mensajes de error o informativos cuando estos ocurren.*
- *Utiliza la Cifra de Comprobación CRC para verificar los errores.*
- *Si se produce el calculo de verificación con error en el Router se genera y transmite el mensaje respectivo.*
- *El mensaje encapsulado en formato IP es transportado a través de la Red a destino.*
- *Es utilizado por programas o servicios de Internet para distintos Objetivos.*
  - *Ping ➡ Solicitud de contestación de computadora destino.*
  - *Traceroute ➡ Calculo de mejor trayectoria a destino.*
- *Mensajes Informativos:*
  - *Echo Request /Reply*
  - *➡Solicitud/ Regreso de Contestación.*



- *A cualquier computadora.*
- *Address Mask Request /Reply*
- ➡ *Solicitud de Regreso de Máscara de Dirección.*
- *Los Routers responde con su Mascara.*
- *Mensajes de error*
  - *Source Quench ➡ Alivio de fuente .*
  - *Rebasado – Falta de Espacio de Buffer.*
  - *Time Exceeded ➡ Tiempo Excedido (vida).*
  - *Destination Unreachable ➡ Destino Inalcanzable.*
  - *Redirect ➡ Redirigir (Cambio de Ruta).*
  - *Fragmentation Required ➡ Fragmentación Requerida* *Depende de la MTU*
  - *MTU ➡ Cantidad máxima transportable por paquetes en la red.*

SNMP( Protocolo de monitorización ) Protocolo simple de gestion de red:

Version 1:

- *Gestión de Red a través de MIB.*
- *Los fabricantes de componentes permitían el monitoreo simple de funcionamiento.*
- *Deficiente en la Información y falta de una herramienta de seguridad.*

Version 2:

- *Gestión de Red a través de una estructura de gestión de información (SMI – Varios MIB). ➡ Gestión Centralizada o Distribuida*
- *Gestión Jerarquizada (Superior y Delegado)*
- *Permite Varias Estaciones (Redundancia)*
- *Tráfico de Red*
- *Gestión de Fallos*
- *Monitorización de Rendimiento*
- *Contabilización de Tiempo*

Version 3:

- *Corrige deficiencias de seguridad existentes de las dos versiones anteriores*
- *Conjunto de capacidades de Seguridad*
  - *Autenticación (Seguridad en Usuarios)*
  - *Privacidad (Seguridad en Usuarios)*
  - *Control de Acceso (Consideraciones)*
- *Seguridad ➡ Identidad de usuario*
  - *Director*
  - *Individuo*
  - *Grupo (Individuo o Aplicaciones)*
- *Mecanismo de Autenticación (USM)*
  - *Verifica y Asegura*
    - *Identidad*

- **Integridad**
- **Retardo**
- **Código de Autenticación en el mensaje**
  - **Trabaja con mecanismo de claves secretas (Simétrico) distribuidas en toda la red para gestores y agentes.**
  - **La clave secreta puede estar preconfigurada.**
  - **Sistema de Privacidad**
    - **Habilita el Sistema de encriptación (DES).**

#### Funcionamiento SNMP:

- **Mecanismo Básico y Directo para intercambiar información entre gestor y agente.**
- **Mensaje ➔ Unidad Básica de Intercambio**
  - **Envoltorio Exterior**
    - **Cabecera ➔ Seguridad.**
  - **Unidad de datos interior (PDU).**
- **Unidad de datos interior (PDU).**

#### 7 Tipos de mensajes PDU

- **Get Request - Solicitud de Valores a Objeto.**
- **Get Response - Respuesta a esa Solicitud.**
- **Get Next Request - Solicitud de Valores a varios objetos**
- **Get Bulk Request – Minimizar números de intercambios**
- **Set Request - Modificación de Valores**
- **Inform Request – Solicitud a una aplicación**
- **PDU Response – Respuesta a la Anterior**

#### Sistema de gestión de red

##### Componentes:

- **Estación de Gestión o Gestor**
- **Agente**
- **Base de información de gestión**
- **Protocolo de Gestión de red**

##### Estación de gestión de red:

- **Aplicaciones de Gestión para análisis de datos, recuperación de fallos, etc.**
- **Interfaz para monitorizar y controlar la Red.**
- **Capacidad de Trasladar los requisitos del gestor de red a la monitorización y control real de los elementos de la Red (Conexiones y Reglas de Seguridad).**
- **Base de datos de gestión (MIB)**

Agente:

- **Elemento Activo que responde a las solicitudes de gestión del sistema.**
- **Devuelve la información en forma asíncrona a la RED.**
- **Plataformas Claves :**
  - **Switches ,Hubs , Routers, Bridges**

## PROTOCOLOS DE PASARELA DE FRONTERA

Encaminamiento en internet:

- **Routers ➔ Decisión de Ruteo y Funciones de Encaminamiento en Base a :**
  - **Topología**
  - **Retardo (Latencia)**
  - **Algoritmos de Ruteo**

Sistema autónomo (AS) Host Multibase:

- **Características :**
  - **Conexión a un Grupo de Routers para Intercambio de Información través de Protocolo.**
  - **Conjunto de Redes y Dispositivos Routers gestionados en única organización.**
  - **Excepto en Fallos, un AS esta conectado como mínimo a un par de nodos.**

IRP(Interior Router Protocol) y ERP (Exterior Router Protocol):

- **Protocolo Interior entre dispositivos de Encaminamiento (Dentro de una LAN , ISP o AS).**
  - **Modelo detallado de conexiones para el calculo de la menor distancia.**
- **Protocolo Exterior entre dispositivos de Encaminamiento (Diferentes LAN , ISP o AS).**
  - **Resumen de Información de Accesibilidad**

Border Gateway Protocol:

### **Objetivo**

**Permitir la cooperación en el Intercambio de información en el encaminamiento entre Routers , llamados pasarelas en el estándar, en sistemas autónomos de diferente proveedor (ISP) .**

- **Desarrollado para su uso en conjunción con conjuntos de redes que emplean Arquitectura de Protocolos TCP/IP .**
- **Protocolo de Dispositivo de encaminamiento exterior estándar de Internet .**
- **BGP- 4 (RFC 1771).**
- **Presupone tres procedimientos funcionales entre encaminadores :**
  - **Adquisición del Vecino**
  - **Detección del Vecino Alcanzable**
  - **Detección de Red Alcanzable**
- **Dos dispositivos encaminadores se consideran vecinos si están conectados a la misma subred.**
- **Mensajes BGP**

- **Open - Establecer relación de vecindad (AD).**
- **Update - Transmisión y actualización de posibles y múltiples rutas (RA).**
- **Keepalive - Conformar OPEN y confirmar periódicamente relación de vecindad. (AD) (VA).**
  - **(Mantener Viva periódicamente - Tiempo) .**
- **Notification - Enviado cuando se detecta condición de error.**

#### PROTOCOLO X500:

- **Desarrollo conjunto entre :**
  - **Comité Consultivo Internacional Telegráfico y Telefónico (CCITT), conocido ahora como la Unión de Telecomunicaciones Internacional (ITU),**
  - **Organización Internacional para la Estandarización (ISO).**
- **Definir un estándar de directorio de uso general para distintas y variadas aplicaciones.**

#### PROTOCOLO LDAP(Lightweight Directory Access Protocol)

- **Protocolo que implementa un Servicio de Directorio Jerárquico y Distribuido para acceder depósitos de información.**
- **Opera sobre usuarios, contraseñas y otras entidades en un entorno de red, ofreciendo una amplia capacidad de filtrado sobre la información que está siendo solicitada.**
- **Define el “lenguaje” utilizado por los programas cliente para comunicarse con los servidores.**
- **El cliente, puede ser de mail, una impresora, una libreta de contactos.**
- **LDAP no incluye seguridad o encriptación en la escritura o actualización de información, por lo que requiere comunicación encriptada**
- **Permite definir permisos para permitir el acceso a ciertos usuarios a la base de datos, y mantener información en privado - “Control de Acceso” .**
- **Es útil para información que pueda estar en un directorio, y que necesite búsquedas rápidas y actualizaciones poco frecuentes.**
- **Funcionamiento:**
  - El servicio de directorio se implementa mediante el modelo de cliente-servidor de manera que una aplicación que desea acceder al directorio no accede directamente a la base de datos sino a una serie de funciones de interface (API) que por medio de mensajes se comunica con el proceso corriendo en el servidor. Este proceso accede a la base de datos y devuelve la información. En casos en los que el servidor consultado no tenga los datos solicitados pero sepa de otro servidor de directorios que si tenga ese dato se convierte en cliente del segundo servidor, le solicita la información y se la devuelve al usuario inicial, todo esto de forma transparente al usuario
- **Tecnología apropiada para compartir información centralizada estructurada en forma de árbol jerárquico y no necesite constante actualización y sea accedida primordialmente para obtención de datos.**
- **Entre otras aplicaciones prácticas podemos nombrar:**
  - **Cuentas de usuario**
  - **Autenticación centralizada**
  - **Directorio de correo**
  - **Libreta de direcciones de correo, direcciones y teléfonos.**
  - **Repositorio de certificados digitales.**
  - **Distribución de correo.**

- *Sustitución de NIS*
- *Integración de todos los recursos de la organización*
- *Personal*
- *Salas de Reuniones*
- *Modelos sobre los cuales está basado:*
  - *Información: describe la estructura de información almacenada en un directorio.*
  - *Nombramiento: organización e identificación de la información en un directorio.*
  - *Funcional: Describe que operaciones pueden ser realizadas un directorio LDAP.*
  - *Seguridad: Describe como la información debe ser protegida del acceso no autorizado.*
- *Control de Acceso*
- *Comunicar las peticiones y respuestas entre el cliente y el servidor.*
- *LDAP usa SSL para Autenticación:*
  - *No Autenticación ⇒ Datos Públicos*
  - *Autenticación básica ⇒ Nombre y Contraseña*
  - *Simple Authentication and Security Layer (SASL) Nombre, Contraseña y Encriptación.*
- *RFC2254 Conformación de strings de filtros de búsqueda.*
- *RFC2255 Formato de la URL LDAP.*
- *RFC2256 Un resumen del protocolo X.500, Esquemas de usuarios para usar con LDAPv3.*
- *RFC2829 Métodos de autenticación.*
- *RFC2830 LDAP(v3) - Extensión de seguridad para la capa de transporte.*
- *RFC3377 Especificaciones técnicas.*

## Control de Flujo

- *Control de Flujo y Parada*
  - *Acuso recibo por cada Paquete*
- *Ventana Deslizante*
  - *Acuso recibo por Ventana*
    - *Varios Paquetes preestablecidos.*

## Congestionamientos:

- *Protocolos de Supervisión de Red.*
  - *Conmutadores informan a los transmisores cuando hay congestionamiento.*
  - *Tomar la pérdida de paquetes como estimación de congestionamiento (Cronometraje y Retransmisión).*

## TERCER POWER POINT

### PROTOCOLO IPV6

- **IPv4 permitió :**
  - **Manejo de Redes Heterogéneas.**
  - **Cambios Drásticos de Tecnología en Hardware y Software.**
  - **Modelo de Direcciones Independiente del Hardware.**
  - **Espacio de Direcciones Limitado. (1.000.000 de redes Aprox )**
- **IPv4 Balanceaba :**
  - **Cantidad Redes**
  - **Cantidad de Host Por Redes**
  - **Aplicaba el Concepto de Clases**
  - ➔ **Limitaba Espacio de Direcciones**
- **IPv4 El Protocolo es limitado para el crecimiento exponencial de las direcciones IP que se duplica año a año.**
- **¿Por qué IPV6?**
  - **Apertura comercial de Internet**
  - **Nuevos dispositivos con conexión**
  - **Aumento de la población conectada**
  - **Mayor Necesidad de Direccionamiento**
- **IPV4 => 2e32 direcciones disponibles**
- **IPV6=> 2e128 direcciones disponibles**
- **IPV brindaba: SIMPLIFICACION DE LA CABECERA IP, ESPACIO DE DIRECCIONES EXTENDIDO, SOPORTE PARA OPCIONES MEJORADO(MULTIMEDIA) Y SEGURIDAD INTRINSECA**

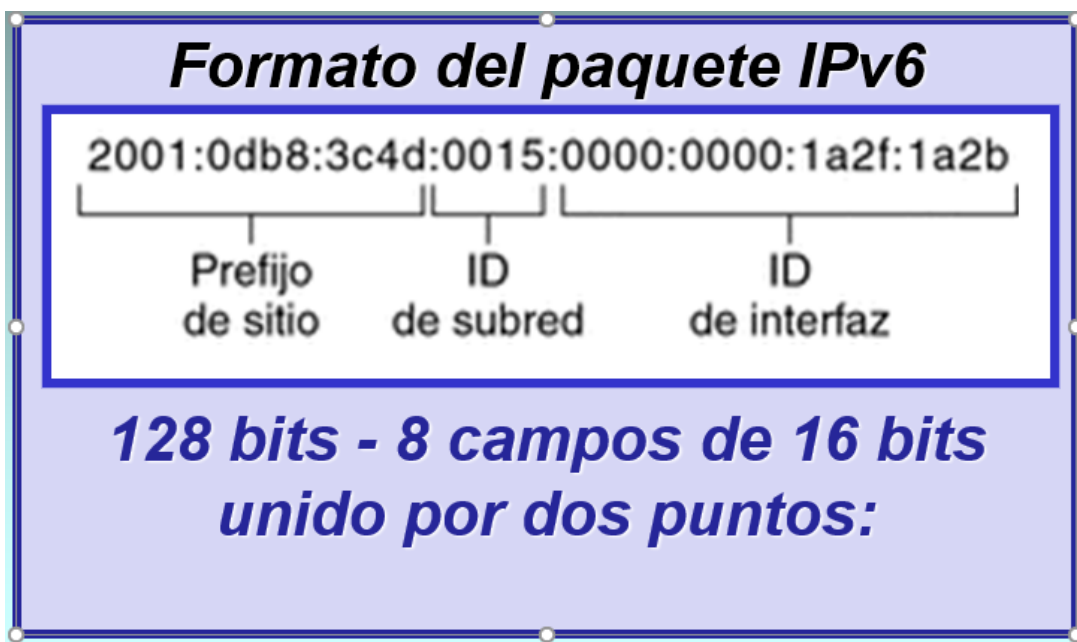
### FORMATO DATAGRAMA IPV4:

Bit 0	4	8	16	19	31
Versión	IHL	Tipo de servicio	Longitud total		
Identificador				Indicadores	Desplazamiento del fragmento
Tiempo de vida		Protocolo		Suma de comprobación de la cabecera	
Dirección origen					
Dirección destino					
Opciones + relleno					

0	Red (7 bits)		Máquina (24 bits)										Clase A
1	0	Red (14 bits)						Máquina (16 bits)					Clase B
1	1	0	Red (21 bits)							Máquina (8 bits)			Clase C

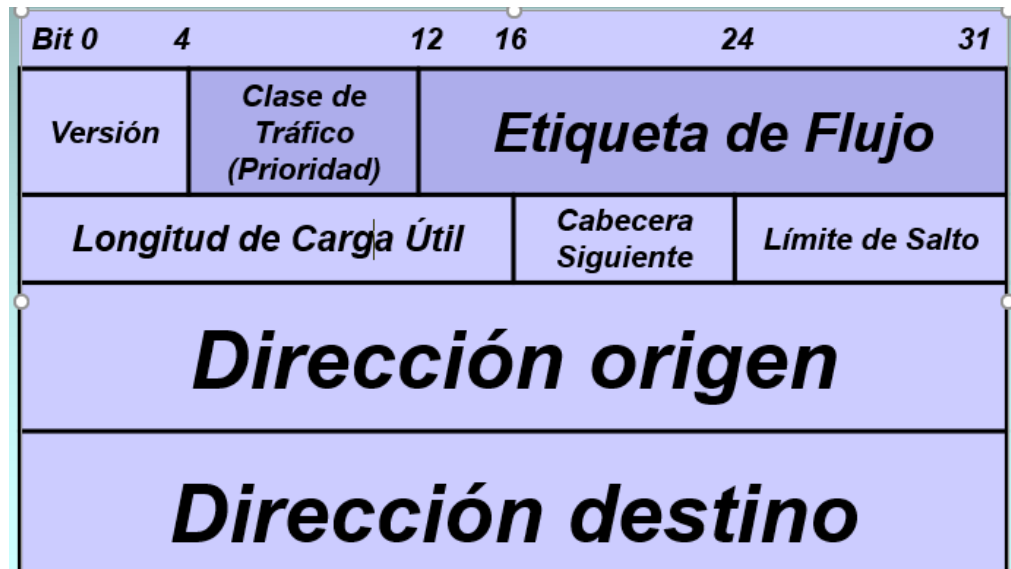
## COMPARACION IPV6 IPV4

IPv6 (128 bits)	IPv4 (32 bits)
2004 : 0401 : <u>beef</u> : 85af : 3952 : <u>cafe</u> : 0000 : 0001	209.185.204.232
16 + 16 + 16 + 16 + 16 + 16 + 16 + 16	8 + 8 + 8 + 8



- PREFIJO:
  - Primeros (48 bits) contienen el **prefijo de sitio**.
  - **Topología pública** que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.
- ID de la subred:
  - **ID de subred** de 16 bits que usted (u otro administrador) asigna al sitio.
  - Describe la **topología privada** denominada **topología del sitio**
  - Es interna del sitio.
- ID de la interfaz
  - Los cuatro campos situados más a la derecha (64 bits) contienen el ID de interfaz, también denominado Token.

- El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.
- NOTA: Si tengo FFFF:0000:0000:0000:A123 es equivalente a poner FFFF:::A123



Datos de IPV4 y IPV6 comparativa.

	IPv4	IPv6
Antigüedad	25 años.	10 años.
Direcciones únicas	4.300 millones. Menos que la población mundial.	340 sextillones. (665.000 trillones/m <sup>2</sup> )
Necesidad de NAT	Sí. Es imposible entregar varias direcciones IP a todos los clientes que la necesiten.	No. Cada dispositivo del planeta puede tener su propia dirección pública.
Direcciones estáticas	Costosas. No pueden ser asignadas a todos los clientes.	Ampliamente disponibles para todos los clientes y dispositivos.
Eficiencia de ruteo	Baja.	Alta.
Encriptación de tráfico	Varios métodos disponibles, pero ninguno integrado.	Soporte integrado y estandarizado para IPsec.
Soporte para QoS	Disponible, pero no integrado.	Integrado, estandarizado y compatible con IPsec.

IPV6 ROUTING MAS EFICIENTE – ABUNDAN IP, CADA EQUIPO TIENE SU IP PUBLICA, SEGURIDAD INTEGRADA YA QUE INCLUYE AUTENTICACION Y CIFRADO mediante Ipsec.

Mejor control de flujo y de prioridades.

Autoconfiguración de la dirección.

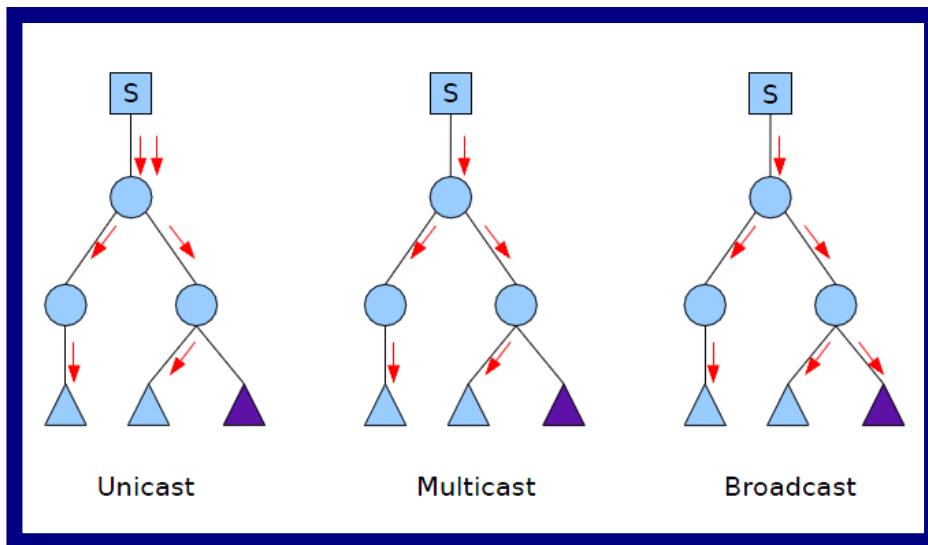
Gran avance en la transmisión multimedia.

## FORMAS DE DIRECCIONAMIENTO IPV4

- **Unicast - Un único destino**
- **Broadcast –copias a muchos destinos (red, subred)**
- **Limitado**



- **Dirigido**
- **Multicast**
  - *Sólo a los que explícitamente deseen recibirlo (protocolo de gestión de grupos -IGMP)*
- **Anycast (IPv6) –Al mejor de los destinos**



#### MULTICAST:

- **Envío de un datagrama a un grupo de hosts que previamente han solicitado su unión al grupo de multicast.**
- **Orientado a no conexión, entrega y orden no garantizado (UDP).**
  - **Diferencia de paquetes unicast/multicast**
    - **Destination Address = dirección de un grupo (clase D).**
- **Individuos libres de unirse o dejar el grupo multicast sin restricción en nº de miembros o nº de grupos.**
- **Enviar a un grupo de multicast no implica pertenencia a él.**

#### FORMAS DE DIRECCIONAMIENTO IPV6

- **UNITRANSMISIÓN (UNICAST)**
- **MONODISTRIBUCIÓN(ANYCAST)**
- **MULTITRANSMISIÓN(MULTICAST)**

#### UNICAST:

- **Un Identificador para una Interfaz Individual.**
- **El Paquete se entrega a la Interfaz identificada solo por esa dirección.**
- **Es equivalente a las Direcciones IPv4.**

#### ANYCAST:

- **Un Identificador para un conjunto de Interfaces (Normalmente pertenecientes a diferentes nodos).**
- **El Paquete se entrega a una de las Interfaces identificadas por esa Dirección. (La mas Cercana de acuerdo al protocolo de encaminamiento).**
- **Permite crear ámbitos de Redundancia para que varias maquinas se ocupen del mismo tráfico según una secuencia determinada (Routing).**

## MULTICAST:

- **Un Identificador para un conjunto de Interfaces (Normalmente pertenecientes a diferentes nodos).**
- **El paquete es enviado a una dirección de multidistribución se entrega a todas las interfaces identificadas por esa dirección.**
- **La misión de este tipo de paquete es evidente: aplicaciones de retransmisión múltiple.**

## Migración de IPv4 a IPv6

- Pila Doble
- Traducción
- Tunneling

### PILA DOBLE:

Un nodo IPv4/IPv6 con una dirección IPv4 compatible, utiliza esa misma dirección como una dirección IPv6 incluyéndola en los **últimos** 32 bits .

### TRADUCCION:

Es la conversión directa de protocolos (entre IPv4 e IPv6) de manera bidireccional .

### TUNNELING:

**Este mecanismo de transición permite crear un “puente” entre redes no compatibles y se desarrolla de manera punto-a-punto.**

**PRO: Permiten la coexistencia de ambas versiones de protocolo.**

**CONTRA: El encapsulado de paquetes es perjudicial para el rendimiento de las conexiones.**

- **Tipos de Tunneling:**

**Tunneling puede ser utilizado en una variedad de formas:**

- **TUNNELING CONFIGURADO**

- » **Router-a-Router**
- » **Usuario-a-Router**

- **TUNNELING AUTOMÁTICO**

- » **Usuario-a-usuario**
- » **Router-a-usuario**

- **6over4 (RFC 2529)**
  - **Realiza el tunneling dentro de una sola organización o sitio, requiere que IPv4 soporte ruteo Multicast.**
  - **Incluye seguridad punto-a-punto y configuración estática**
- **6to4 ⇒ Tunneling Automático**
  - **Mecanismo más utilizado y crea túneles IPv6 para tráfico del mismo tipo sobre redes IPv4 entre redes aisladas de 6to4.**
- **6to4 ISATAP**
  - **Método para generar una dirección IPv6 local a partir de una dirección IPv4.**
  - **No requiere que la red IPv4 subyacente soporte Multicast.**
  - **La dirección local se determina mediante la concatenación de fe80:0000:0000:0000:5efe: con los 32 bits de la dirección IPv4.**
- **Teredo (RFC 4380)**

- *Provee asignación de direcciones y tunneling automático para tráfico Ipv6 cuando los hosts.*
- *Están situados detrás de uno o múltiples NATs.*
- *Encapsula el paquete Ipv6 como un mensaje UDP Ipv4. Estos pueden ser traducidos universalmente por NATs y pueden atravesar múltiples capas de NATs.*

## CUARTO POWER POINT

### PROTOCOLOS PARA VoIP(Voice over IP):

Anda a la hoja 2 del power point 4 de la unidad 4. Mucho texto xd

### TELEFONIA IP – PROTOCOLO H323

- *Provee servicio de comunicaciones multimedia sobre redes que emplean conmutación de paquetes .*
- *Diseñado por la ITU ⇒ **Union internacional de Telecomunicaciones***
- *Las **entidades H323** pueden proveer en tiempo real comunicaciones de datos, video o audio.*
- *Es una pila de protocolos que trabaja sobre IP*
- *Puede proveer calidad de servicio garantizada (QoS).*
- *Dentro de este modelo se definen 5 tipos de **dispositivos**:*
  - **Terminal** ➔ *Iniciador de la Llamada.*
  - **MCU** ➔ *Unidad de Control Multipunto.*
  - **Gatekeeper** ➔ *Autoriza y Rutea la Llamada.*
  - **ATA** ➔ *Conversor Analógico /Digital.*
  - **Gateway** ➔ *Conversión de Paquetes IP a Paquetes de Voz.*

### RTP (Real Time Protocol):

- ***Permite la administración de flujos multimedia (voz, video) sobre IP.***
- ***Se encuentra en un Nivel de Aplicación y utiliza los protocolos de transporte subyacentes TCP o UDP.***
- ***Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.***
- ***Es usado a través del protocolo UDP/IP para identificación de carga útil, sincronización numeración secuencial y monitoreo.***

### RTCP ( RT Control Protocol):

- ▶ ***Permite transmitir información básica sobre los participantes de la sesión y la calidad de servicio.***
- ▶ ***RTCP es un protocolo de control asociado con RTP.***
- ▶ ***Entrega retroalimentación sobre la calidad de la transmisión de datos.***
- ▶ ***El encabezado de RTP puede ser comprimido para reducir el tamaño de archivos en la red.***
- ▶ ***RTCP se encuentran en un nivel de aplicación y utilizan los protocolos de transporte subyacentes TCP o UDP.***

## PROTOCOLO SIP:

- ▶ *Protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea.*
- ▶ *Desarrollado por IETF en 1999.*
- ▶ *Modelo cliente-servidor.*
- ▶ *Objetivo: Establecer sesiones multimedia entre 2 agentes de red.*
- ▶ *Transmisión de la voz a través de datagramas IP.*
- ▶ *Independiente de la topología de red utilizada.*
- ▶ *Aplicación inmediata de la VoIP.*
- ▶ *Organizaciones internacionales estandarizan su funcionamiento.*
- ▶ *Noviembre 2000, aceptado como protocolo de señalización para 3GPP.*
- ▶ *Principal Ventaja ⇨ Reducido costo operacional y de implementación.*
- ▶ *Servicios:*
  - ▶ *Llamada en espera (on-hold)*
  - ▶ *Desvío de llamadas (ocupado, no contesta, incondicional)*
  - ▶ *Conferencias de voz y video*
  - ▶ *Transferencia de llamadas*
  - ▶ *Traducción de Número de Origen y Destino*
- ▶ *SIP está más integrado con las aplicaciones y servicios de Internet.*
- ▶ *Es más flexible a la hora de incorporar nuevas funcionalidades (servicios).*
- ▶ *Su implementación es más simple.*
  - ▶ *(Ejemplo: para subredes con IP Privada y Firewall)*
- ▶ *La sintaxis es similar a HTTP.*
- ▶ *Es mas fácil de leer el call flow de la llamada.*
- ▶ *Hace uso del protocolo SDP para la descripción de las capacidades multimedia de sus agentes.*
- ▶ *RTP transporta la voz (o video) digitalizado.*
- ▶ *Utiliza Protocolos de transporte UDP y TCP.*
- ▶ *Codecs de audio: G711 alaw (PCMA), G711 ulaw (PCMU), G729, GSM, Speex e iLBC .*
- ▶ *Codecs de video: H263 y MPEG.*

## ELEMENTOS DE RED – PROTOCOLO SIP:

- ▶ *Agentes de Usuario*
  - ▶ *Clientes (User Agent Client, UAC): generador de solicitudes SIP.*
  - ▶ *Servidores (User Agent Server, UAS): encargado de responder las solicitudes SIP.*
- ▶ *Servidores de Red:*
  - ▶ *Servidor de Redirección (Redirect Server).*

- ▶ ***Servidor Proxy (Proxy Server).***
- ▶ ***Servidor de Registro (Register Server).***

#### REGISTRAR SERVER O LOCATION SERVER:

- ***Registran las direcciones SIP (SIP – URL) y sus direcciones IP asociadas.***
- ***Garantizan el “mapping” entre direcciones SIP y direcciones IP.***

#### REDIRECT SERVER:

- ***Procesan solicitudes SIP (Invite) y retoman la dirección IP del Corresponsal al que pertenece la URI( Uniform Resource Identifiers).***

#### PROXY SERVER:

- ***Re-envia paquetes modificando o no los datos del mismo.***
- ***Desarrollan el “routing” de los mensajes de solicitudes y respuestas SIP.***
- ***Trabajan en estado “statefull” o “stateless”.***

#### CAPACIDADES DE SIP:

- ▶ ***Servicios de telefonía tradicional***
- ▶ ***SIMPLE (mensajería instantánea).***
- ▶ ***PRESENCE.***
- ▶ ***S/MIME (segurización de la mensajería).***
- ▶ ***Compresión de la señalización.***
- ▶ ***Soporte de UDP, TCP y SCTP.***
- ▶ ***SBC (Session Border Controller).***
- ▶ ***IPv6.***

#### NAT TRAVERSAL:

- ▶ ***Modos de funcionamiento de Firewalls:***
  - ▶ Full cone NAT
  - ▶ Restricted cone NAT
  - ▶ Port Restricted cone NAT
  - ▶ Symmetric NAT
- ▶ ***Soluciones:***
  - ▶ Señalización y RTP Simétricos
  - ▶ RTP Proxy
  - ▶ Gateways de Aplicación
  - ▶ STUN (Simple Traversal of UDP through NATs)
  - ▶ TURN (Traversal Using Relay NAT)

## TP N4 PARTE 1

**1) Dentro del Modelo de Protocolo Internet, los protocolos de transporte utilizados en la capa Host a Host son IP y UDP.**

FALSO

**2) Dentro del Esquema del Protocolo TCP/ IP el/los componentes que intervienen en el proceso de la comunicación son:**

TODAS LAS ANTERIORES SON CORRECTAS.

**3) En red LAN, la agrupación lógica de dispositivos y usuarios que están agrupados por función, aplicación o departamento sin tener en cuenta la ubicación del segmento físico se la denomina:**

VLAN.

**4) Dentro del Esquema del Protocolo TCP/ IP v4, el esquema de direccionamiento abstracto tiene como Objetivo:**

AMBAS B Y C.

**5) Dentro del Esquema del Protocolo TCP/ IP, cuando nos referimos a ARP estamos haciendo mención de:**

EL PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN.

**6) Dentro del Esquema del Protocolo TCP/ IP, cuando hablamos de un Puerto nos referimos a:**

IDENTIFICADOR ÚNICO DE UN SERVICIO

**7) Dentro del Modelo de Protocolo TCP/IP v4, la capa Internet cumple con las siguientes funciones:**

TODAS LAS ANTERIORES SON CORRECTAS.

**8) Dentro del Esquema del Protocolo TCP/ IP, el Router utiliza un protocolo que le permite informar a los Routers vecinos que se encuentra fuera de servicio o congestionado. Dicho protocolo corresponde a:**

NINGUNA DE LAS ANTERIORES ES CORRECTA.

**9) El Esquema de Datagrama IP nace con la necesidad de trabajar con redes heterogéneas, y permite el paso de un cuadro de una red a otra respetando el paquete original de manera tal de encapsularlo y que el mismo no sea modificado mientras se realice la transmisión:**

VERDADERO

**10) Una red que tiene una combinación de Hardware y Software Heterogéneo, que**

entrega al usuario la apariencia de un sistema de comunicación integrado y uniforme al cual se conectan muchas computadoras se lo denomina:

RED VIRTUAL.

### **TP N4 PARTE 2**

1) Un Cuadro de Tipo Identificable como unidad de transmisión de paquetes en una LAN está compuesto por una cantidad limitada de Bits, que tienen sus formatos de campos como:

TODAS LAS ANTERIORES SON CORRECTAS.

2) El protocolo simple de Gestión de Red utilizado por los monitores de red para relevar y controlar el desempeño de terminales en la misma se lo denomina:

SNMP.

3) Algunos cuadros no identificables se caracterizan por no incluir un campo de Tipo de cabecera de cuadro, por lo tanto, establecen previamente:

ACUERDO ENTRE EMISOR Y RECEPTOR EN EL FORMATO DE DATOS A ENVIAR.

4) Dentro del Esquema del Protocolo TCP/ IP V4, cuando nos referimos a un host multibase o sistema autónomo estamos hablando de:

UN HOST QUE SE CONECTA A VARIAS CONEXIONES DE RED.

5) Dentro de una red de dominio con recursos compartidos, la acción de copiar los cuadros en las interfaces de red realizada por un concentrador se la denomina:

DIFUSIÓN.

6) Dentro del Esquema del Protocolo TCP/ IPV4, la dirección IP corresponde a un número de 32 Bits asignado a un Host y usado para todas las comunicaciones con él; a su vez aplica un esquema de jerarquía de direcciones utilizando el prejo, para identificar a la red física que está conectada y el sujo para identificar a cada host de la red.

VERDADERO

7) Una Red compartida topología estrella con un conmutador de capa 2 del modelo OSI se vale de direcciones para ltrar los cuadros de entrada a las distintas estaciones; para ello los formatos de direcciones corresponden a:

DIRECCIONES FÍSICAS.

8) El Router fronterizo (intranet–extranet) que tiene dos o más conexiones balanceadas, dentro de un host o nodo multibase trabaja soportando bajo el protocolo:

BGP.

9) Dentro del Esquema del Protocolo TCP/ IP V4 De acuerdo con la cantidad máxima de redes y cantidad máxima de hosts por red se dene la clase de la red que estamos

evaluando para ver si es clase A, B o C.

VERDADERO

10) La Interfaz de programación de aplicaciones que interactúa entre el Sistema Operativo y los Protocolos, que se diseñan para trabajar con aplicaciones concurrentes utilizando un grupo de protocolos y el servicio deseado se lo denomina:

API DE SOCKETS.

### **TP N4 PARTE 3**

1) Los Protocolos más utilizados en Telefonía sobre IP corresponden a:

AMBAS B Y D.

2) Dentro Protocolo de Internet Versión 6 Ipv6, la dirección posee 3 campos de elementos hexadecimales que corresponden a.

AMBAS A, C Y E.

3) El Protocolo de Internet Versión 6 Ipv6 posee un espacio de direcciones de 128 Bits.

Los cambios en las cabeceras del Datagrama (Flujo Continuo de datos) permiten mejorar la calidad de transmisión de audio y video.

VERDADERO

4) El Esquema de Datagrama IP nace con la necesidad de trabajar con redes homogéneas, y permite el paso de un cuadro de una red a otra respetando el paquete original de manera tal de encapsularlo y que el mismo sea modificado mientras se realice la transmisión:

FALSO

5) Dentro del Esquema del Protocolo TCP/ IP V4 de acuerdo a la cantidad mínima de redes y cantidad mínima de hosts por red se define la clase de la red que estamos evaluando para ver si es clase A, B o C.

FALSO

6) El Protocolo de Internet versión 4 Ipv4 con los cambios tecnológicos permitió:

AMBAS B Y C.

7) El Proxy WAP traduce las peticiones WAP a peticiones Web, de forma que el cliente WAP (el terminal inalámbrico) pueda realizar peticiones de información al servidor Web. Adicionalmente este Proxy codifica las respuestas del servidor Web en un formato binario compacto, que es interpretable por el cliente.

VERDADERO

8) Dentro de la estructura del Protocolo H323 para telefonía IP, podemos decir que el Gatekeeper tiene la función de:



AUTORIZAR Y RUTEAR LA LLAMADA.

9) Dentro del Esquema del Protocolo TCP/ IP V4, la dirección IP corresponde a un número de 34 Bits asignado a un Host y usado para todas las comunicaciones con él; a su vez aplica un esquema de jerarquía de direcciones utilizando el prejo, para identificar a la red física que está conectada y el sujo para identificar a cada host de la red.

FALSO

10) El protocolo estándar utilizado para mostrar información en pequeñas pantallas a través de conexiones celulares, basado en Wireless Markup Language (WML) (similar al HTML), preparado para que el cliente y no requiera en sus dispositivos teclado o Mouse se lo denomina:

WAP

#### **TP N4 PARTE 4**

1) Dada la dirección 157.89.0.64 y la máscara 255.255.0.0 ¿qué parte representa la porción de host?

NINGUNA DE LAS ANTERIORES ES CORRECTA.

2) El Siguiendo Rango de direcciones IPv4 172.16.0.0 — 172.31.0.0 Representa a:

DIRECCIONES PRIVADAS.

3) ¿Sobre qué Subnet está el host 200.1.1.99/27?

200.1.1.96

4) ¿Cuál es el rango de direcciones válidas para la dirección IP 222.37.2.50/24?

222.37.2.1 — 222.37.2.254

5) Identifique la dirección de broadcast, dada la dirección IP 201.100.178.36

255.255.255.224

201.100.178.63

6) Dada una dirección clase B y máscara 255.255.255.240 ¿cuál es el máximo número de hosts y subredes útiles?

REDES = 4094; HOSTS = 14

7) ¿Qué clase de dirección tiene la menor cantidad de hosts para direccionar?

CLASE C.

8) ¿Qué clase de dirección IP me brinda la mayor cantidad de redes?

CLASE C.

9) Cuáles son los host válidos para 199.37.2.33/29?

199.37.2.33 — 199.37.2.38

