Plan Estratégico
de Desarrollo 2025 - 2035
visión de futuro 2045

Por la universidad que soñamos
¡Participa!

Fundamentos de Redes

MBA Jorge Andrés Ángel Salazar
Esp. Gestión y Seguridad de Bases de Datos
Ingeniero de Sistemas y Computación
Tecnólogo en Sistemas de Información

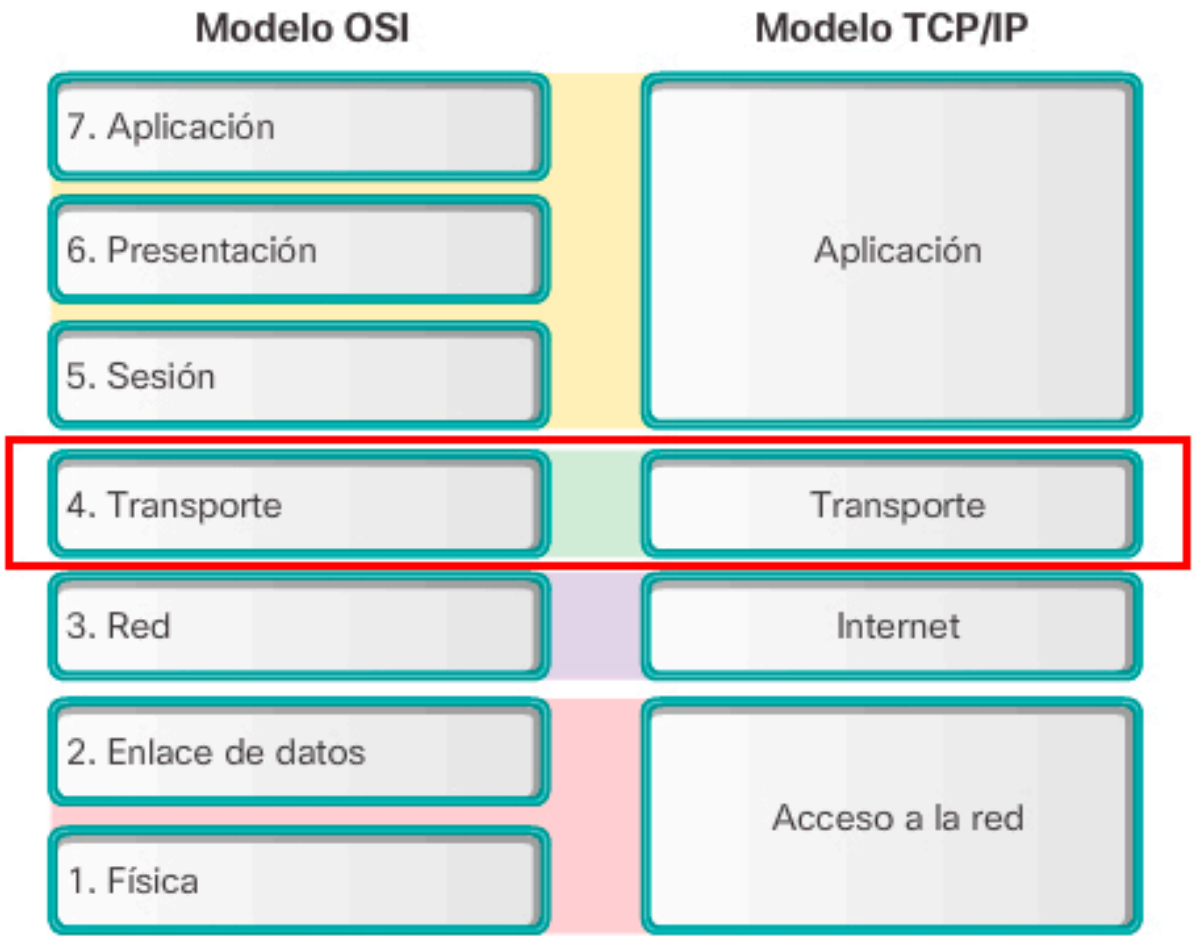
Cronograma

Fecha	Tema
21 – Octubre (Semana 11)	Capa de Transporte
28 – Octubre (Semana 12)	Capa Red
04 – Noviembre (Semana 13) - F	Ejercicios de Subneting
11 – Noviembre (Semana 14) - F	
18 – Noviembre (Semana 15)	Capa de Acceso a la Red
25 – Noviembre (Semana 16)	Parcial 2
02 – Diciembre (Semana 17)	Opcional 2 - Trabajo Final
09 – Diciembre (Semana 18)	Habilitacion

Sesión 11. Capa de Transporte

- ✓ Definición.
- ✓ Conversaciones.
- ✓ Segmentación y reemsamble.
- ✓ Identificación.
- ✓ Propósitos.
- ✓ Multiplexación.
- ✓ Control de conversaciones Soporte.
- ✓ Confiabilidad.
- ✓ Funciones de la capa.
- ✓ Protocolos TCP y UDP.
- ✓ Direccionamiento de puertos.
- ✓ Tipos de puerto.
- ✓ Segmentación.
- ✓ Reemsamble.
- ✓ Diferencias TCP y UDP.
- ✓ Confiabilidad.
- ✓ Procesos servidor TCP.
- ✓ Ensamble segmentos TCP.
- ✓ Verificación de errores.
- ✓ Control de flujo.
- ✓ Ventana de sesión.
- ✓ Confiabilidad.
- ✓ Sobrecarga.
- ✓ Procesos y solicitudes UDP.
- ✓ Actividades de seguimiento en simulador a los datagramas.

Sesión 11. Capa de Aplicación.



Capa de Transporte

- ✓ Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que esté utilizando.
- ✓ Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión
- ✓ La Unidad de Protocolo de Datos de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP..
- ✓ Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP: Puerto (191.16.200.54:80).

Capa de Transporte

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:

- ✓ seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino
- ✓ segmentación de datos y gestión de cada porción
- ✓ reensamble de segmentos en flujos de datos de aplicación
- ✓ identificación de las diferentes aplicaciones.

Capa de Transporte

Seguimiento de Conversaciones individuales

Cualquier host puede tener múltiples aplicaciones que se están comunicando a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de Transporte mantener los diversos streams de comunicación entre estas aplicaciones.

Segmentación de datos

Debido a que cada aplicación genera un stream de datos para enviar a una aplicación remota, estos datos deben prepararse para ser enviados por los medios en partes manejables. Los protocolos de la capa de Transporte describen los servicios que segmentan estos datos de la capa de Aplicación. Esto incluye la encapsulación necesaria en cada sección de datos. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de Transporte para indicar la comunicación a la cual está asociada.

Capa de Transporte

Reensamble de segmentos

En el host de recepción, cada sección de datos puede ser direccionada a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar un stream completo de datos que sea útil para la capa de Aplicación. Los protocolos de la capa de Transporte describen cómo se utiliza la información de encabezado de dicha capa para reensamblar las secciones de datos en streams y enviarlas a la capa de Aplicación.

Identificación de las aplicaciones

Para poder transferir los streams de datos a las aplicaciones adecuadas, la capa de Transporte debe identificar la aplicación de destino. Para lograr esto, la capa de Transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en ese host. Este número de puerto se utiliza en el encabezado de la capa de Transporte para indicar con qué aplicación está asociada esa sección de datos.

Capa de Transporte

Puertos

Los puertos en las redes de datos son números de identificación que se utilizan para dirigir el tráfico de datos a servicios y aplicaciones específicas en un dispositivo o servidor dentro de una red. Estos puertos se utilizan para organizar y distinguir diferentes tipos de comunicaciones en una red y garantizar que los datos lleguen al servicio o programa correcto.

Tanto en TCP como en UDP tenemos un total de **65535** puertos disponibles, tenemos una clasificación dependiendo del número de puerto a utilizar, ya que algunos puertos son los comúnmente llamados «conocidos», y que están reservados para aplicaciones específicas, aunque hay otros muchos puertos que se utilizan habitualmente por diferentes software para comunicarse tanto a nivel de red local o a través de Internet. También tenemos los puertos registrados, y los puertos efímeros.

Puertos conocidos: los puertos conocidos (well-known en inglés) van desde el puerto 0 hasta al 1023, están registrados y asignados por la Autoridad de Números Asignados de Internet (IANA). Por ejemplo, en este listado de puertos está el puerto 20 de FTP-Datos, el puerto 21 de FTP-Control, el puerto 22 de SSH, puerto 23 de Telnet, puerto 80 y 443 para web (HTTP y HTTPS respectivamente), y también el puerto de correo entre otros muchos protocolos de la capa de aplicación.

Capa de Transporte

Universidad del Valle

Puertos registrados: los puertos registrados van desde el puerto 1024 hasta al 49151. La principal diferencia de estos puertos, es que las diferentes organizaciones pueden hacer solicitudes a la IANA para que se le otorgue un determinado puerto por defecto, y se le asignará para su uso con una aplicación en concreto. Estos puertos registrados están reservados, y ninguna otra organización podrá registrarlos nuevamente, no obstante, normalmente están como «semireservados», porque si la organización deja de utilizarlo podrá reutilizarse por otra empresa. Un claro ejemplo de puerto registrado es el 3389, se utiliza para las conexiones RDP de Escritorio Remoto en Windows.

Capa de Transporte

Puertos efímeros: estos puertos van desde el 49152 hasta el 65535, este rango de puertos se utiliza por los programas del cliente, y están constantemente reutilizándose. Este rango de puertos normalmente se utiliza cuando está transmitiendo a un puerto conocido o reservado desde otro dispositivo, como en el caso de web o FTP pasivo. Por ejemplo, cuando nosotros visitamos una web, el puerto de destino siempre será el 80 o el 443, pero el puerto de origen (para que los datos sepan cómo volver) hace uso de un puerto efímero.

Capa de Transporte

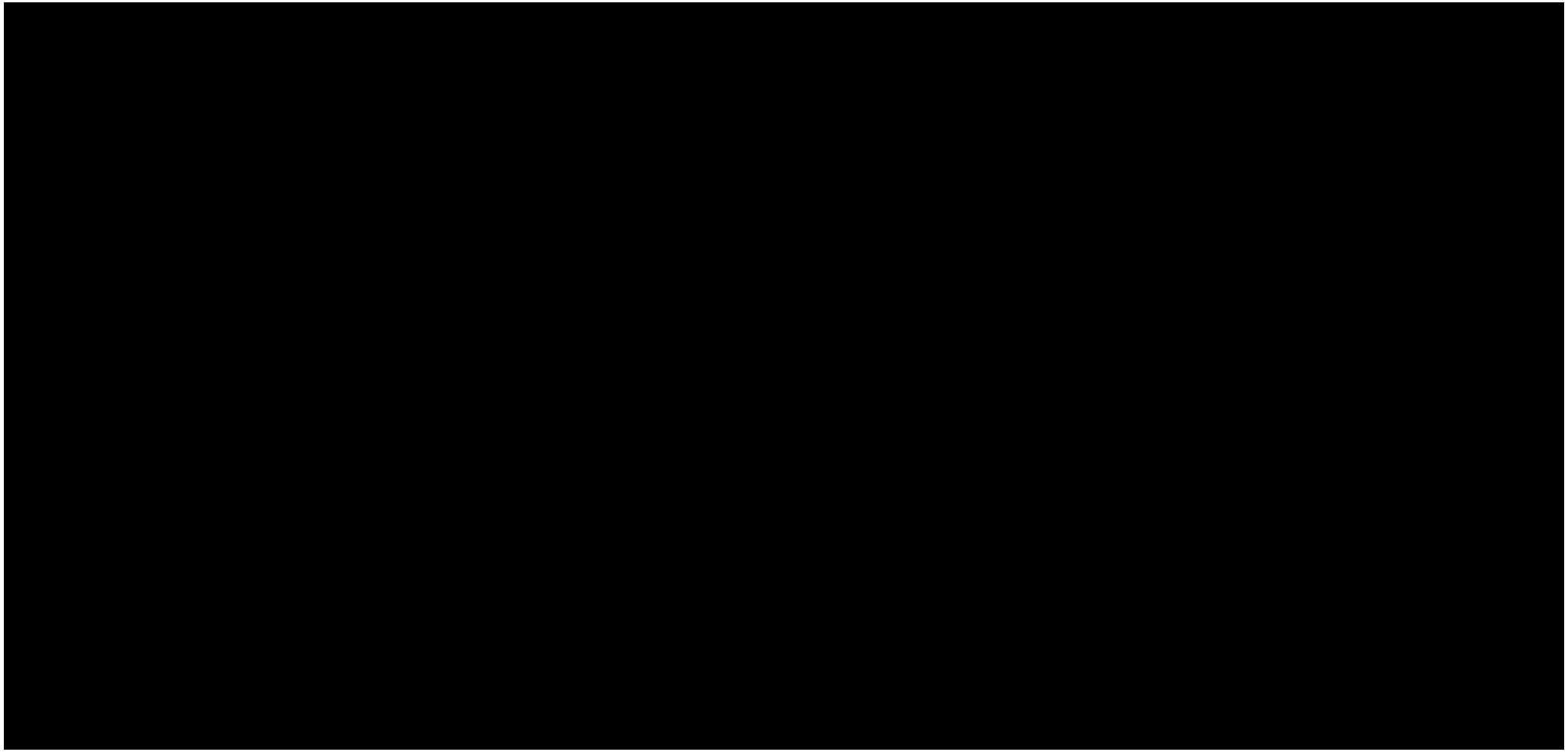
Para determinar el estado de los puertos, podemos utilizar tres términos los cuales varían en función de la configuración de los mismos.

Puertos cerrados: Cuando la comunicación es rechazada completamente, por lo cual no generan ningún tráfico entrante o saliente.

Puertos filtrados: Todo el tráfico que transcurre por estos, es filtrado por aplicaciones de seguridad como los firewall.

Puertos abiertos: Cuando un servicio está escuchando en este puertos, y es accesible desde el exterior.

Capa de Transporte



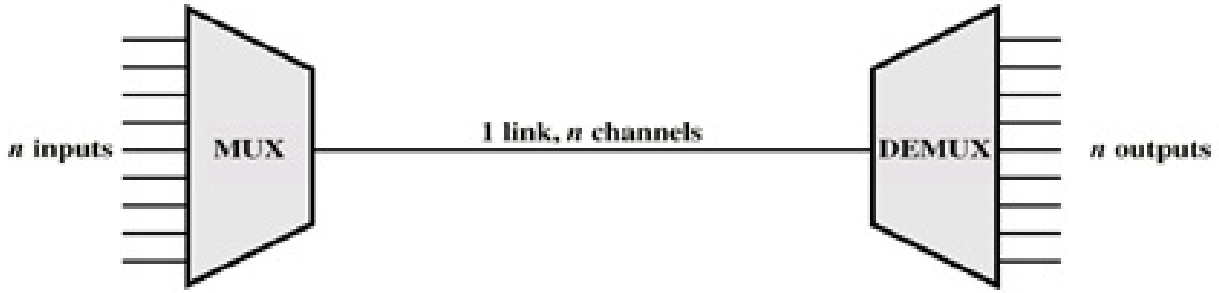
Multiplexación

La Multiplexación es una técnica utilizada en comunicaciones mediante la cual en un canal pueden convivir señales procedentes de distintos emisores y cuyo destino son diferentes receptores. Es decir, se comparte un canal físico, estableciendo sobre él varios canales lógicos

En la Multiplexación de diferentes conexiones intervienen dos dispositivos: el multiplexor y el demultiplexor. El multiplexor combina (multiplexa) los datos de las n líneas de entrada y los transmite a través del canal. Mientras que el demultiplexor capta la secuencia de datos multiplexados, separa (demultiplexa) los datos de acuerdo con el canal, y los envía hacia las líneas de salida correspondientes.

Capa de Transporte

Multiplexación



EL MULTIPLEXOR:

- Combina (multiplexa) los datos de las líneas de entrada.
- Los transmite a través del enlace de mayor
- capacidad.

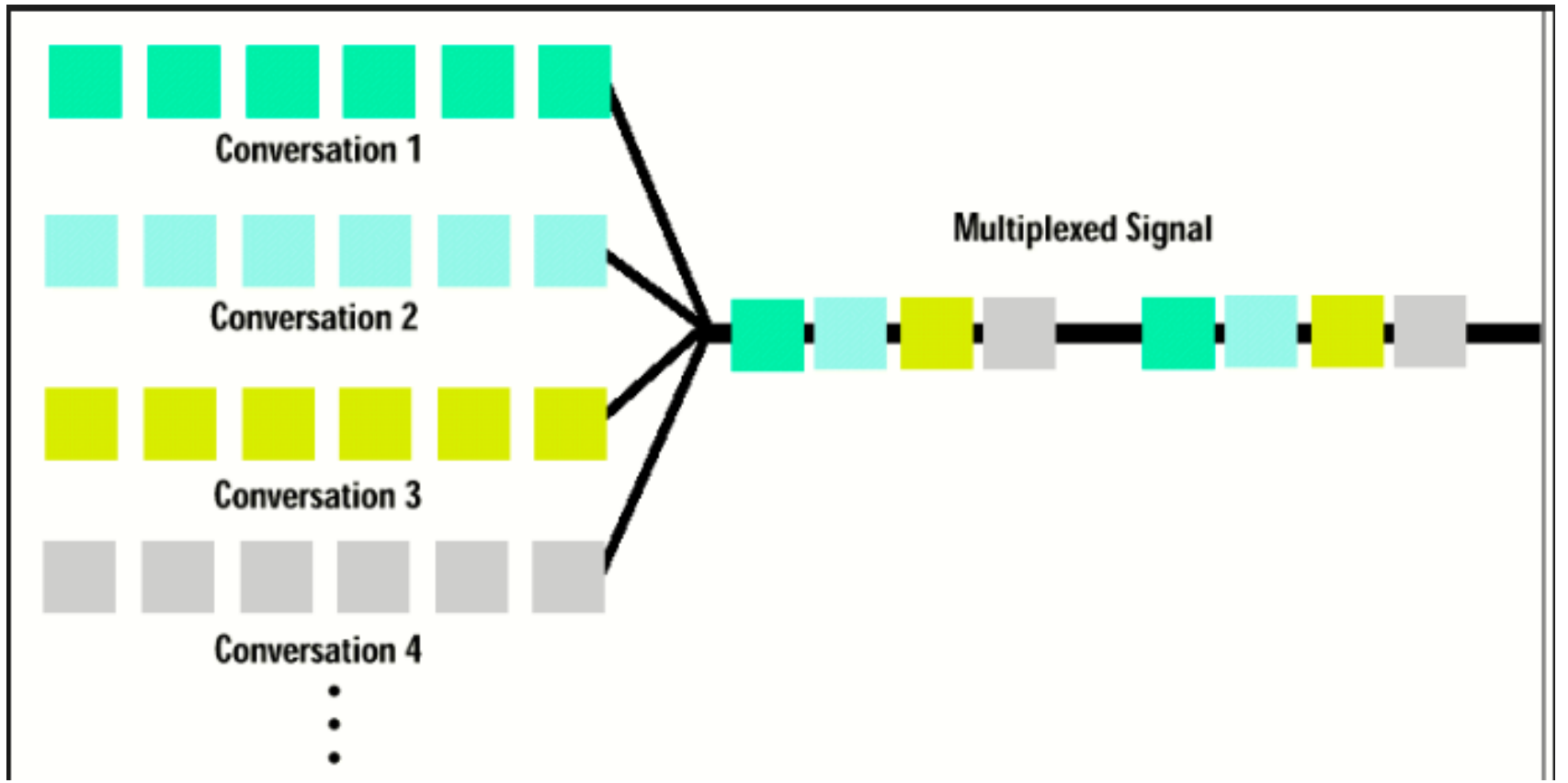
EL DEMULTIPLEXOR:

- Acepta la cadena de datos multiplexada.
- Separa (demultiplexa) los datos conforme al canal al que pertenecen.
- Los distribuye a la línea apropiada de salida.

Capa de Transporte

Universidad del Valle

Multiplexación

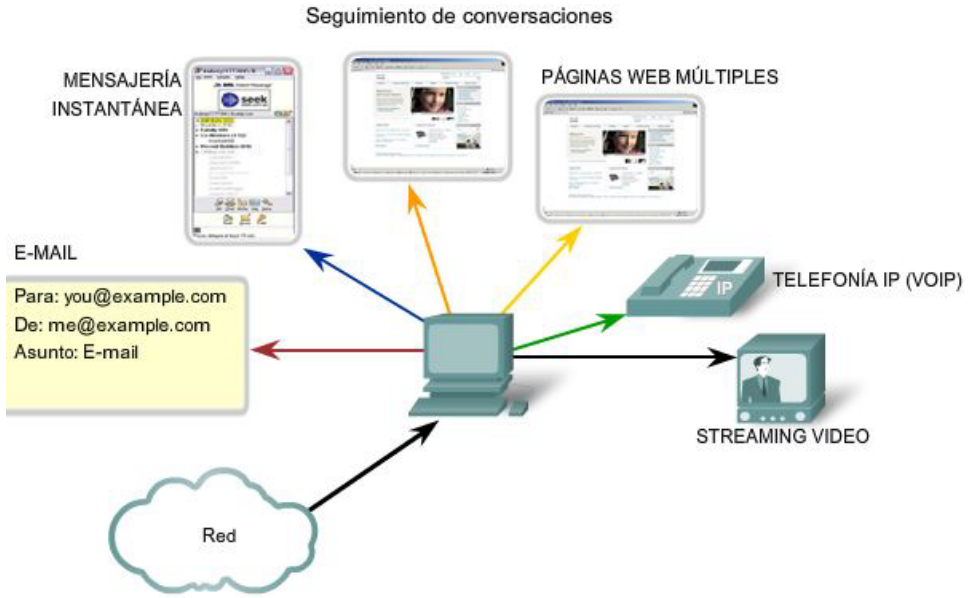


Capa de Transporte

Universidad del Valle

Separación de comunicaciones múltiples – Multiplexación

Considere una computadora conectada a una red que recibe y envía e-mails y mensajes instantáneos, explora sitios Web y realiza una llamada telefónica de VoIP de manera simultánea. Cada una de estas aplicaciones envía y recibe datos en la red al mismo tiempo. Sin embargo, los datos de la llamada telefónica no se direccionan al explorador Web y el texto de un mensaje instantáneo no aparece en el e-mail.



Capa de Transporte – TCP

Universidad del Valle

Protocolo TCP

TCP (que significa Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

El fin de TCP es proveer un flujo de bytes confiable de extremo a extremo sobre una internet no confiable. TCP puede adaptarse dinámicamente a las propiedades de la internet y manejar fallas de muchas clases.

Protocolo TCP

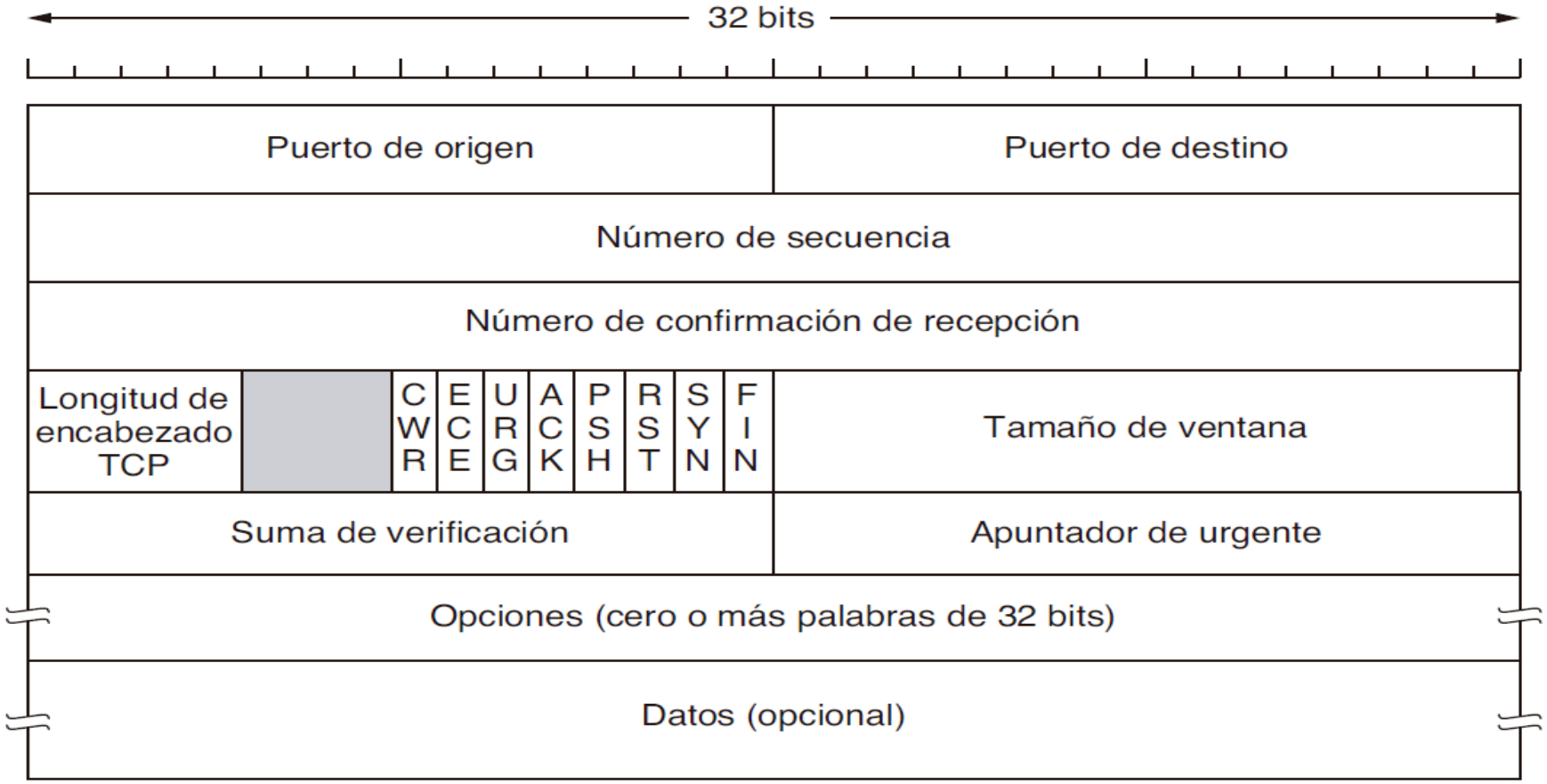
Las principales características del protocolo TCP son las siguientes:

- ✓ TCP permite colocar los segmento nuevamente en orden cuando vienen del protocolo IP.
- ✓ TCP permite que el monitoreo del flujo de los datos y así evita la saturación de la red.
- ✓ TCP permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.
- ✓ TCP permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.
- ✓ Por último, TCP permite comenzar y finalizar la comunicación amablemente.

Capa de Transporte – TCP

Universidad del Valle

Un segmento TCP está formado de la siguiente manera:



Capa de Transporte – TCP

- ✓ **Puerto de origen (16 bits) :** Este campo contiene el número de puerto asociado con la aplicación del dispositivo emisor. Es un número que identifica la conexión específica a nivel de aplicación, como por ejemplo el puerto 80 para HTTP

- ✓ **Puerto de destino (16 bits) :** Similar al puerto de origen, pero en este caso identifica el número de puerto del dispositivo receptor. Esto permite que el receptor sepa qué servicio o aplicación debe manejar el segmento recibido.

- ✓ **Número de secuencia (32 bits) :** Este es un número único asignado a cada byte de datos enviado en una conexión. El número de secuencia permite a TCP asegurarse de que los datos se reciban de manera ordenada y sin pérdida. Cada byte transmitido tiene un número de secuencia asociado.

Capa de Transporte – TCP

- ✓ **Número de acuse de recibo (32 bits) :** El campo de número de confirmación se usa para indicar que se ha recibido correctamente un segmento. Este número indica el siguiente número de secuencia que espera recibir el dispositivo. Es parte del mecanismo de control de flujo y de la confiabilidad de TCP.

- ✓ **Longitud de Cabecera (4 bits):** Este campo indica el tamaño de la cabecera TCP. Es necesario porque la cabecera puede variar de tamaño debido a la presencia de opciones TCP. El tamaño se expresa en términos de número de palabras de 32 bits (4 bytes)

- ✓ **Reservado (6 bits) :** Estos bits están reservados para uso futuro o extensiones, y no se utilizan en las versiones estándar de TCP.

Capa de Transporte – TCP

- **Bits de código (8 bits):** Está formado por 8 banderas de 1 bit cada una. Cuando vale 1 representa que la bandera correspondiente está activa. Las diferentes banderas se describen a continuación

  - **URG (Urgent):** Indica que hay datos urgentes en el segmento que deben ser tratados de inmediato.
  - **ACK (Acknowledgment):** Indica que el número de confirmación es válido y que los datos han sido recibidos correctamente.
  - **PSH (Push):** Señala que los datos deben ser entregados a la aplicación de inmediato sin esperar más datos.
  - **RST (Reset):** Reinicia la conexión en caso de error o si un dispositivo no puede continuar la comunicación.
  - **SYN (Synchronize):** Se usa durante el apretón de manos de tres vías (three-way handshake) para establecer una conexión y sincronizar números de secuencia.
  - **FIN (Finish):** Indica que el remitente ha terminado de enviar datos y quiere cerrar la conexión.
  - **ECE (Explicit Congestion Notification Echo**) – Notificación de congestión:Este bit se utiliza para señalar que el receptor ha recibido una señalización de congestión desde la red (cuando el bit CWR está activo) o para informar que el emisor está notificando sobre la congestión.
  - **CWR (Congestion Window Reduced)** – Ventana de congestión reducidaEl bit CWR es utilizado por el emisor para indicar que ha recibido una señal de congestión (como el bit ECE) y que ha reducido su ventana de congestión como respuesta.

Capa de Transporte - TCP

- ✓ **Ventana (16 bits) :** Este campo es crucial para el **control de flujo**. Especifica cuántos bytes de datos está dispuesto a recibir el dispositivo receptor sin desbordarse. Este valor es dinámico y ayuda a evitar la congestión

- ✓ **Suma de Verificación (CRC) :** El checksum es un mecanismo de verificación de errores. Se genera en el remitente y se revisa en el receptor para asegurarse de que los datos no se hayan corrompido durante el tránsito. Si el checksum no coincide, el segmento se descarta.

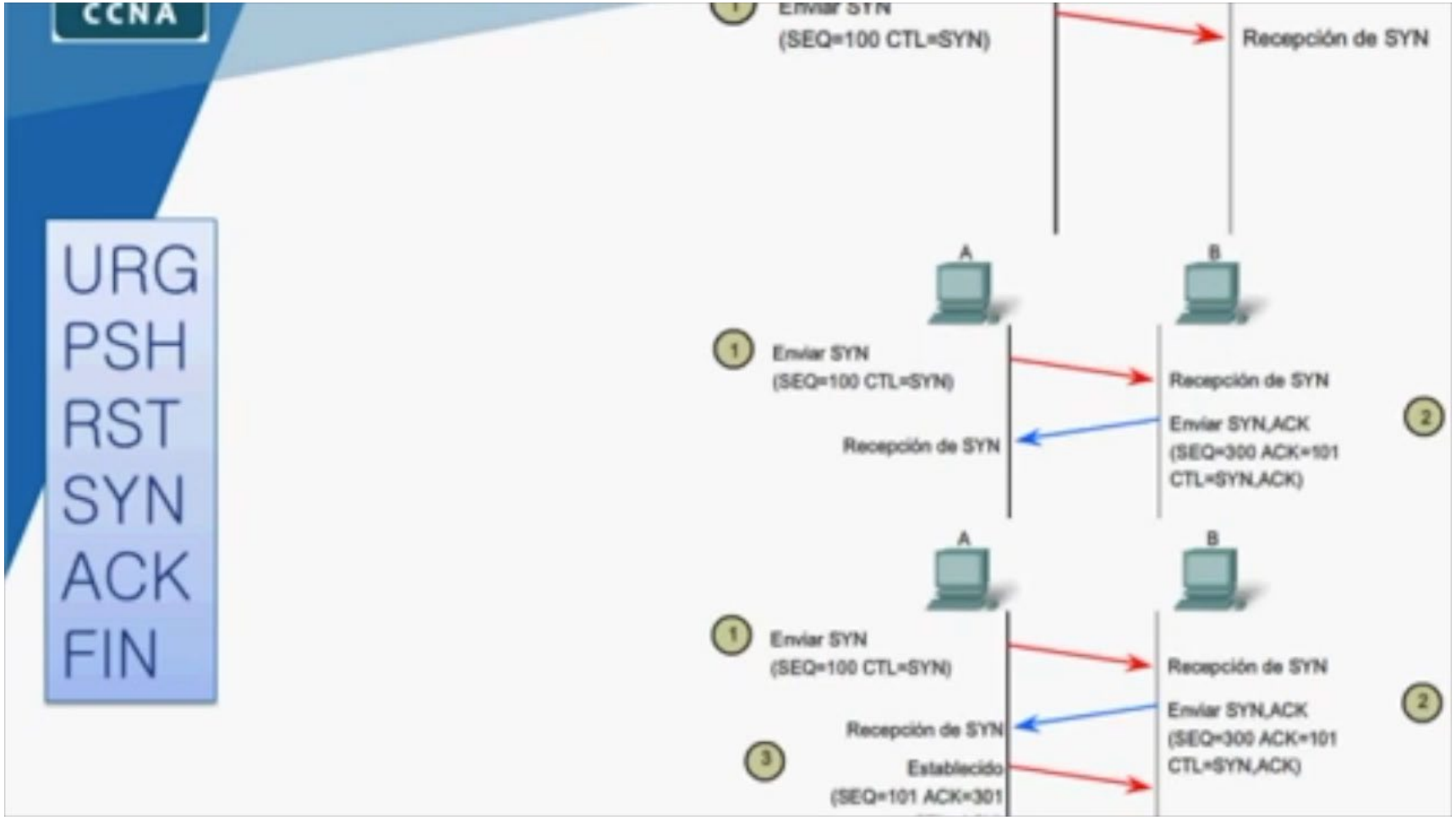
- ✓ **Puntero urgente (16 bits) :** Este campo se usa en conjunto con la bandera **URG**. Indica la posición dentro del segmento donde terminan los datos urgentes. Es útil para manejar información que debe ser procesada inmediatamente, ignorando el flujo normal de datos.

Capa de Transporte - TCP

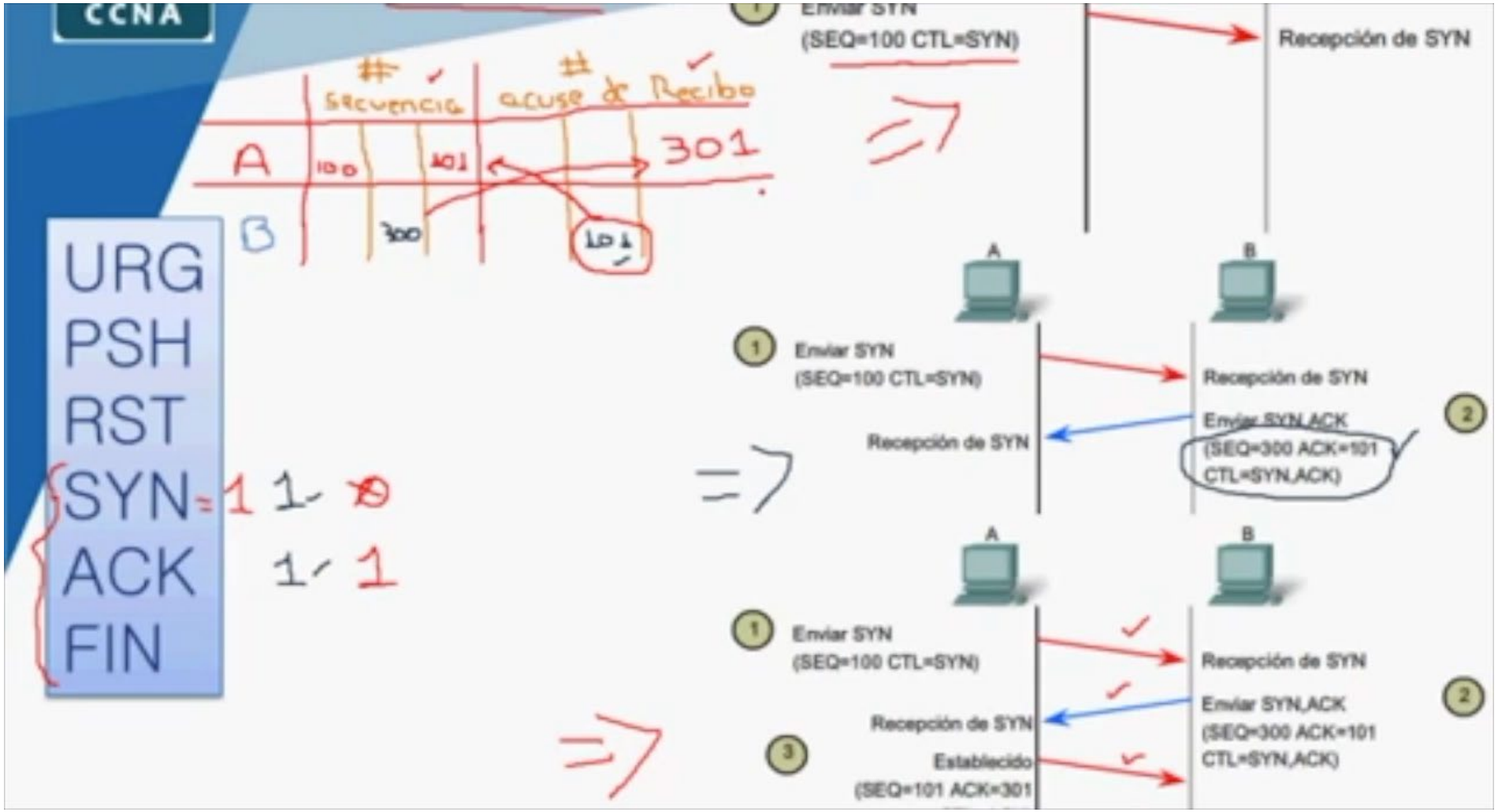
- ✓ **Opciones (tamaño variable):** El campo de opciones permite incluir información adicional como el **Tamaño de la Ventana de TCP** o la **Marca de Tiempo**. Esto puede mejorar la eficiencia o añadir funcionalidades, pero no siempre está presente en todos los segmentos.

- ✓ **Datos:** Finalmente, el segmento TCP contiene el **bloque de datos** que está siendo transmitido. La longitud de estos datos puede variar, y si no hay datos en el segmento (por ejemplo, durante la fase de establecimiento de la conexión), el campo de datos puede estar vacío.

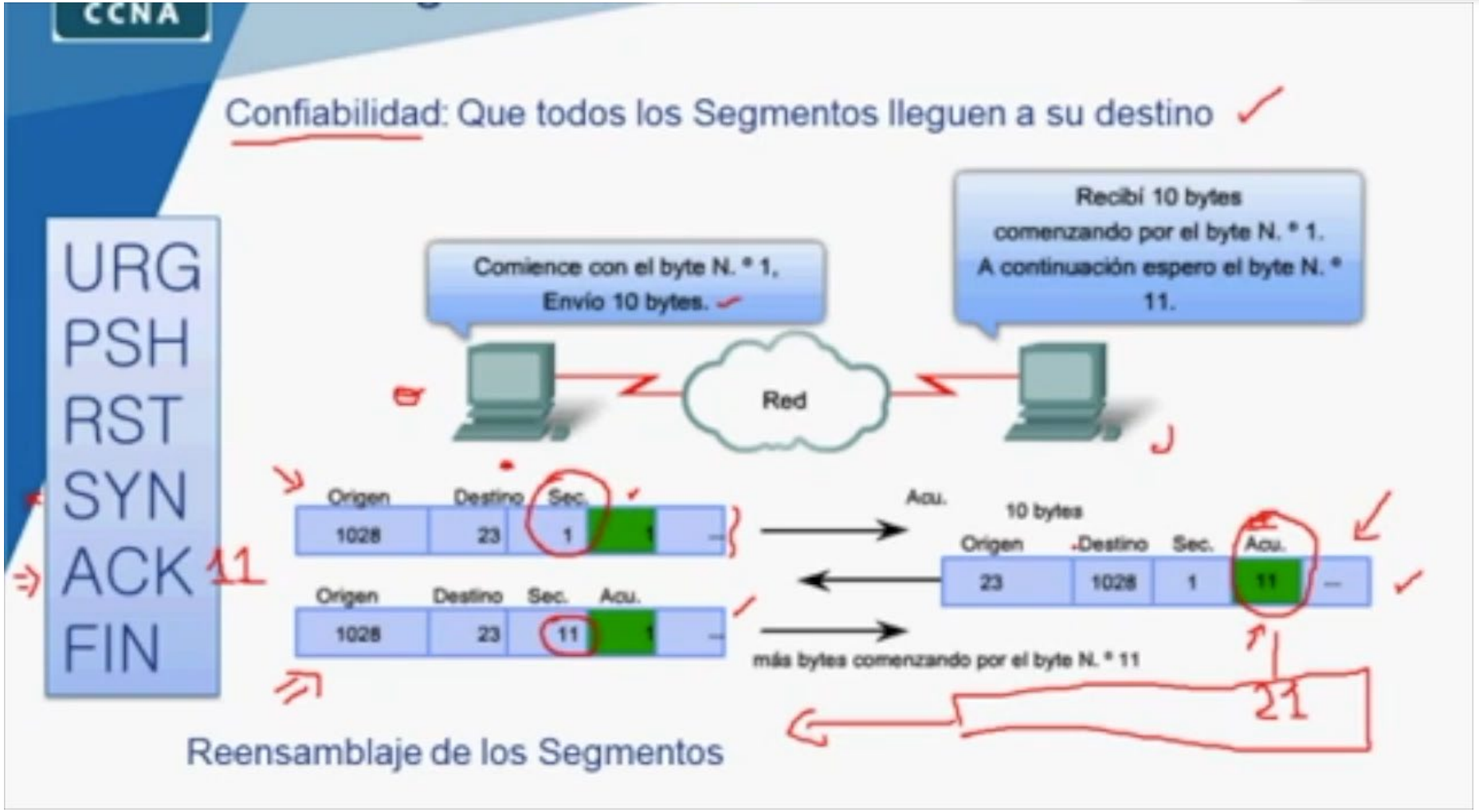
Capa de Transporte – Conexión TCP



Capa de Transporte – Segmentación TCP



Capa de Transporte – Flujo TCP



Capa de Transporte - TCP

Universidad del Valle

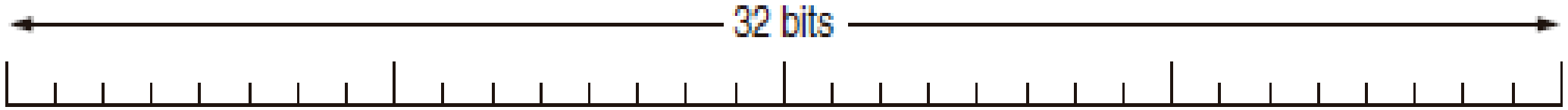
Funcionamiento del Segmento TCP

- ✓ **Establecimiento de Conexión:** TCP utiliza un "apretón de manos de tres vías" (three-way handshake) para establecer una conexión entre dos dispositivos. Durante este proceso, los segmentos TCP con los flags SYN y ACK son esenciales para sincronizar y confirmar los números de secuencia.
- ✓ **Transmisión de Datos:** Una vez establecida la conexión, los datos se envían en segmentos. Cada segmento tiene un número de secuencia que permite que los datos lleguen de manera ordenada y sin duplicados.
- ✓ **Control de Flujo:** TCP ajusta dinámicamente la cantidad de datos que puede enviar mediante el campo de ventana de recepción, evitando así la congestión o sobrecarga de los dispositivos.
- ✓ **Cierre de Conexión:** El cierre de la conexión también sigue un proceso de intercambio de segmentos utilizando el flag FIN para indicar que no se enviarán más datos.

Capa de Transporte - UDP

Universidad del Valle

Un Datagrama UDP está formado de la siguiente manera:



Puerto de origen	Puerto de destino
Longitud de UDP	Suma de verificación de UDP

Capa de Transporte - UDP

- ✓ **Puerto de origen (16 bits) :** Este campo contiene el número de puerto asociado con la aplicación del dispositivo emisor. Al igual que en TCP, el puerto de origen identifica la aplicación que está enviando los datos. Este campo es opcional; si no se usa, se rellena con ceros.

- ✓ **Puerto de destino (16 bits) :** Este campo indica el número de puerto del dispositivo **receptor**, permitiendo que los datos lleguen a la aplicación correcta. El puerto de destino es necesario para que el receptor sepa a qué aplicación o servicio entregar los datos.

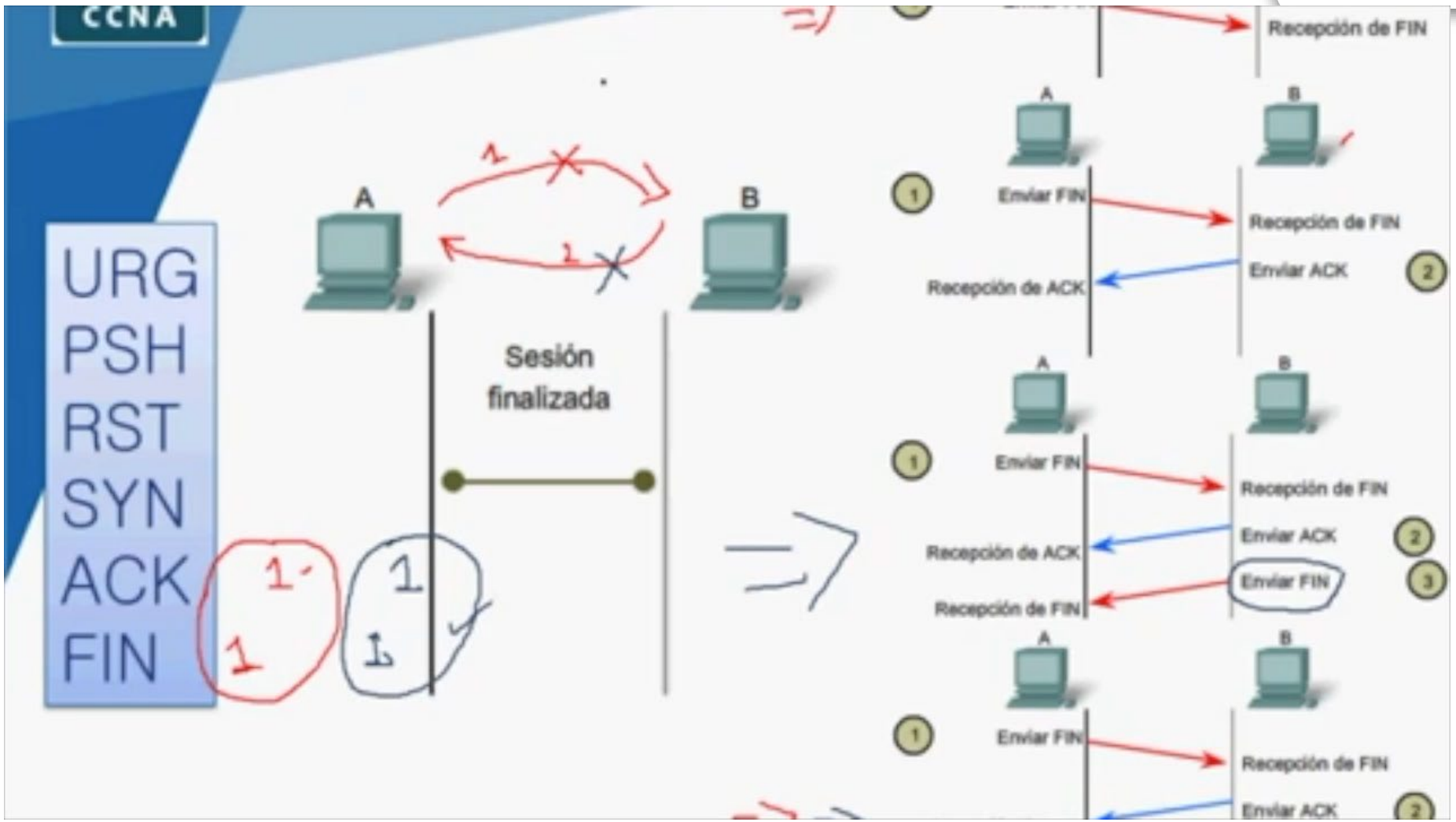
- ✓ **Longitud UDP (16 bits) :** Este campo especifica la longitud total del datagrama UDP, incluyendo tanto la cabecera como los datos (payload). El tamaño mínimo de un datagrama UDP es de 8 bytes (sólo la cabecera), aunque puede crecer dependiendo de la cantidad de datos transmitidos. La longitud máxima permitida es de 65.535 bytes.

Capa de Transporte - UDP

- ✓ **Suma Verificación (16 bits) :** El checksum es un valor usado para verificar la **integridad de los datos** durante la transmisión. Aunque este campo es opcional, se utiliza para detectar errores en los datos o en la cabecera. Si no se usa, se rellena con ceros. El valor del checksum es calculado por el emisor antes de enviar el datagrama y es verificado por el receptor.

- ✓ **Datos (Payload):** Este campo contiene los datos que la aplicación quiere transmitir. La cantidad de datos puede variar según la longitud especificada en el campo anterior. Si no hay datos que enviar, el datagrama tendrá una longitud mínima de 8 bytes (sólo la cabecera).

Capa de Transporte – UDP



Funcionamiento del Datagrama UDP

A diferencia de TCP, **UDP** no utiliza mecanismos para asegurar que los datos lleguen correctamente o en orden. Es un protocolo "best effort" (de mejor esfuerzo), por lo que no retransmite los paquetes perdidos ni controla el flujo de datos. Esto lo hace adecuado para aplicaciones que priorizan la **velocidad** sobre la **fiabilidad**, como:

- Streaming de video y audio en tiempo real.
- Juegos en línea.
- Servicios de DNS (Domain Name System).
- Protocolo de VoIP (Voice over IP).

Plan Estratégico
de Desarrollo 2025 - 2035
visión de futuro 2045

Por la universidad que soñamos
¡Participa!

Fundamentos de Redes

MBA Jorge Andrés Ángel Salazar
Esp. Gestión y Seguridad de Bases de Datos
Ingeniero de Sistemas y Computación
Tecnólogo en Sistemas de Información

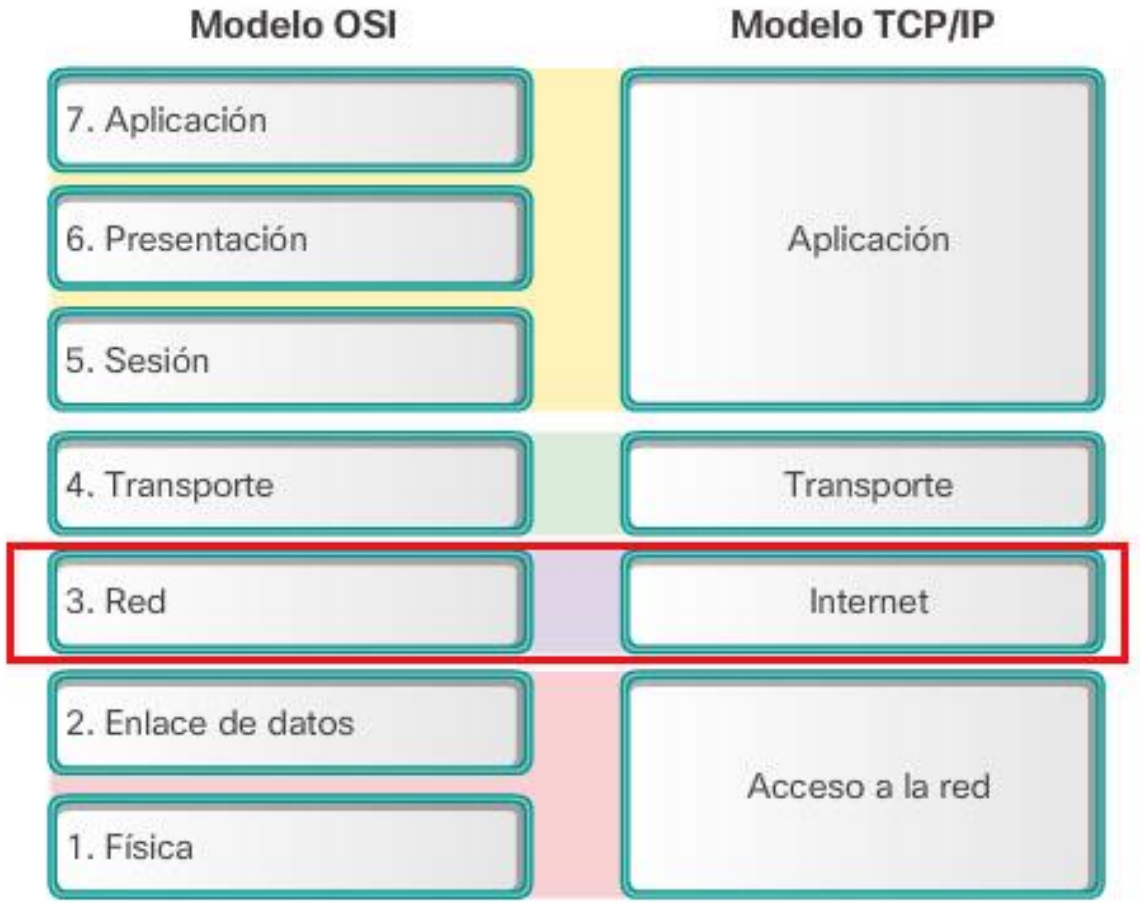
Sesión 12 - Capa de Red - Internet

- ✓ Definición.
- ✓ Propósitos.
- ✓ Procesos básicos.
- ✓ Comunicación host-host.
- ✓ Protocolos en IPV4 IPV6.
- ✓ Roles IPV4.
- ✓ Independencia de medios.
- ✓ Paquetes y encabezados.
- ✓ Administración de la red.
- ✓ Seguridades.
- ✓ Niveles.
- ✓ División.
- ✓ Rendimiento.
- ✓ Paquetes y encabezados.
- ✓ Dominios de broadcast.

Contenido

Universidad del Valle

Sesión 12 - Capa de Red - Internet



Importancia de la Capa de Red en el Modelo TCP/IP

La capa de red en el modelo TCP/IP es esencial para el funcionamiento de Internet, ya que permite la comunicación entre dispositivos en distintas redes. Sin esta capa, la red no podría escalar y conectar millones de dispositivos en diferentes ubicaciones alrededor del mundo. Al gestionar el direccionamiento, enrutamiento y control de errores básicos, la capa de red asegura que los datos puedan moverse de manera eficiente y efectiva en una arquitectura tan extensa y compleja como Internet.

Capa de Red - Direccionamiento

Protocolos Principales de la Capa de Red

La capa de red del modelo TCP/IP utiliza varios protocolos para realizar sus funciones:

IP (Internet Protocol):

- ✓ Es el **protocolo central** de esta capa, encargado del direccionamiento y enrutamiento de paquetes. Define cómo se estructuran y transmiten los paquetes entre el origen y el destino.
- ✓ Versiones: **IPv4** es la versión más ampliamente utilizada; **IPv6** se diseñó para solucionar la escasez de direcciones IPv4, ampliando el espacio de direccionamiento.

ICMP (Internet Control Message Protocol):

- ✓ Protocolo usado principalmente para **diagnóstico y control** de errores en la transmisión de paquetes IP. ICMP es el protocolo detrás de herramientas de red como **ping** y **traceroute** que ayudan a verificar la conectividad y la ruta de los paquetes en una red.

Capa de Red - Direccionamiento

Universidad del Valle

Protocolos Principales de la Capa de Red

ARP (Address Resolution Protocol):

- ✓ Este protocolo convierte las **direcciones IP en direcciones MAC**, que son necesarias para que los dispositivos puedan comunicarse en una red local (LAN). Es fundamental para que los routers y switches puedan enviar paquetes en redes de área local.

RARP (Reverse Address Resolution Protocol):

- ✓ RARP es el inverso de ARP y permite que un dispositivo obtenga su dirección IP a partir de su dirección MAC. Esto se usa típicamente en redes donde un dispositivo, como una computadora sin disco, no tiene una dirección IP asignada y la solicita a través de la red.

IGMP (Internet Group Management Protocol):

- ✓ Protocolo que facilita la transmisión de **datos en grupo o multicast**, permitiendo que un dispositivo envíe un solo paquete a múltiples dispositivos en una red. Es común en aplicaciones como transmisión de video en vivo.

Capa de Red - Direccionamiento

Universidad del Valle

Funciones de la Capa de Red en TCP/IP

Fragmentación y Reensamblaje:

A veces, los datos son demasiado grandes para ser enviados en un solo paquete debido a limitaciones en las redes intermedias. En estos casos, la capa de red fragmenta los paquetes y los reensambla en el dispositivo de destino, asegurando que se reciban correctamente.

Control de Errores Básico:

Aunque no ofrece la misma confiabilidad que la capa de transporte, la capa de red cuenta con mecanismos básicos para detectar errores en la transmisión y toma decisiones para reenviar o desechar paquetes si se identifican problemas de integridad.

Capa de Red - Direccionamiento

Funciones de la Capa de Red en TCP/IP

Encaminamiento de Paquetes (Routing):

La capa de red se encarga de determinar la ruta óptima que los datos deben seguir para llegar al dispositivo de destino. Este proceso, llamado enrutamiento o routing, permite que los paquetes atraviesen diferentes redes mediante routers, optimizando el camino y el tiempo de llegada.

Direccionamiento IP:

Los dispositivos se identifican en la red mediante direcciones IP. Esta capa administra y utiliza direcciones IP para identificar de manera única cada dispositivo y cada red, asegurando que los paquetes lleguen al receptor correcto. Las direcciones pueden ser IPv4 (32 bits) o IPv6 (128 bits).

Capa de Red - Direccionamiento

La dirección IP es el identificador de cada equipo dentro de su red de redes. Cada equipo conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el equipo.

Una dirección IP es un número binario de 32 bits, es decir, (XXXXXX) posibilidades o direcciones distintas a construir. El conjunto de todas ellas se conoce como espacio de direcciones.

Como las personas no manejan fácilmente los número binarios, y menos los especialmente largos, se inventó una forma de escribir las direcciones IP más cómoda: la notación decimal o de puntos. Consiste en dividir los 32 bits en cuatro grupos de 8 bits (4 octetos o bytes). Cada uno de estos octetos se escribe en forma decimal, separando un octeto del siguiente por un punto.

Cada uno de los octetos de una dirección IP será siempre un número decimal entre 0 (00000000) y 255 (11111111)

Capa de Red - Direccionamiento

Universidad del Valle

Dirección IP binaria de 32 bits

11000000 • 10101000 • 00100010 • 00001011

Ejemplo: 11000000.10101000.01100100.00001111 = XXX.XXX.XXX.XXX

Recordemos que para pasar un número decimal a binario se realiza el sumatorio de la base (2) elevada a la posición del dígito y multiplicado por el valor binario correspondiente de dicho dígito. La posición de cada dígito es, empezando de derecha a izquierda el primer dígito ocupa la posición 0, el segundo la posición 1 y así hasta el octavo que ocupa la posición 7. Así, para el último octeto o el de más a la derecha sería:

0 0 0 0 1 0 1 1

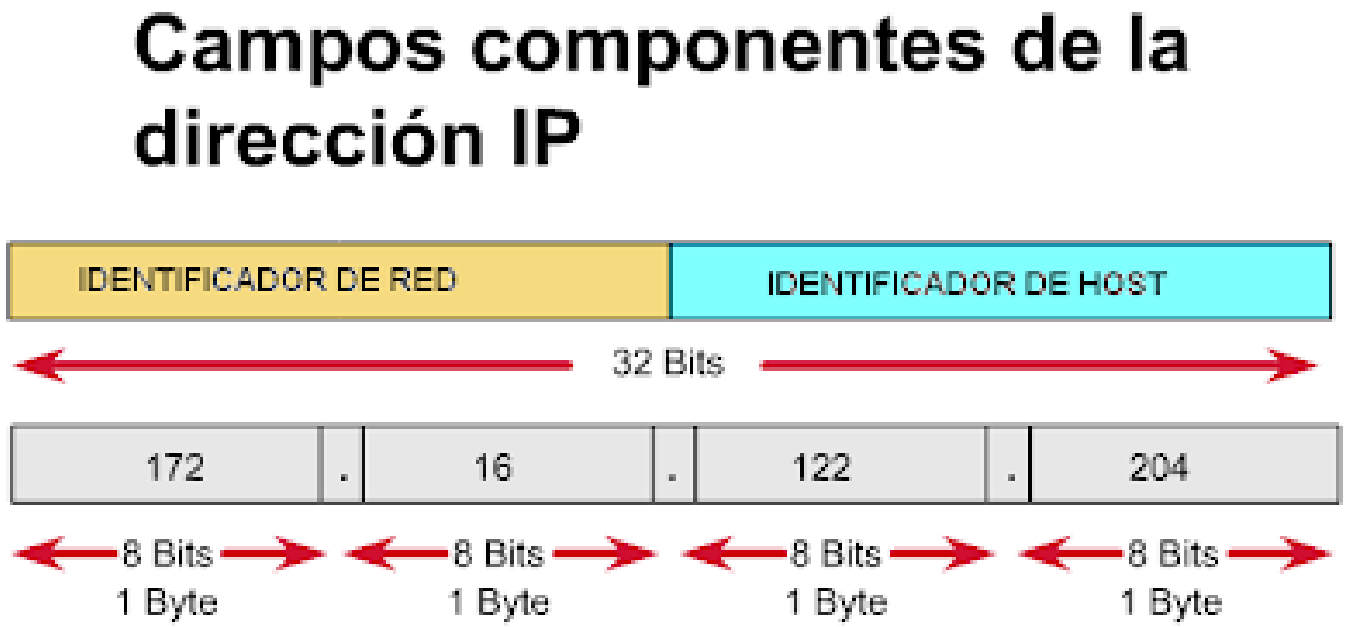
$2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$

Octeto (8 bits)

Capa de Red - Direccionamiento

La dirección IP de un dispositivo está estructurada en dos partes:

- Identificador de red a la que está conectado el dispositivo,
- host u ordenador. Identificador del dispositivo, host u ordenador dentro de la red.



Capa de Red - Direccionamiento

Universidad del Valle

Para facilitar la administración, los diseñadores del esquema de direccionamiento IP determinaron la existencia de cinco únicas clases de direcciones, es decir, clase A, clase B, clase C, clase D y clase E.

Direcciones clase A

- Lo que caracteriza una red clase A es que el primer bit (el que se encuentra más a la izquierda) tomará siempre el valor 0, es decir, el primer octeto tendrá un valor decimal entre 0 y 126, ya que la red 127.0.0.0, aunque su primer octeto también empieza por el valor binario 0, no puede utilizarse por estar reservada para pruebas del adaptador de red. Un ejemplo de una dirección IP clase A sería 124.95.44.15 y pertenecería a la red 124.0.0.0.

- Todas las direcciones IP clase A utilizan solamente los 8 primeros bits para identificar la parte de red de la dirección, el resto (tres octetos) se utilizan para especificar la parte de host de la dirección, es decir, 24 bits se reservan para identificar cada una de las conexiones dentro de la red, por lo que el número de conexiones posibles en dicha red será de 224, es decir, 16.777.216, aunque siendo precisos, se debe indicar que de todo ese rango de direcciones hay dos que no se pueden utilizar, por lo que el número real de conexiones será 224 – 2, es decir, 16.777.214.

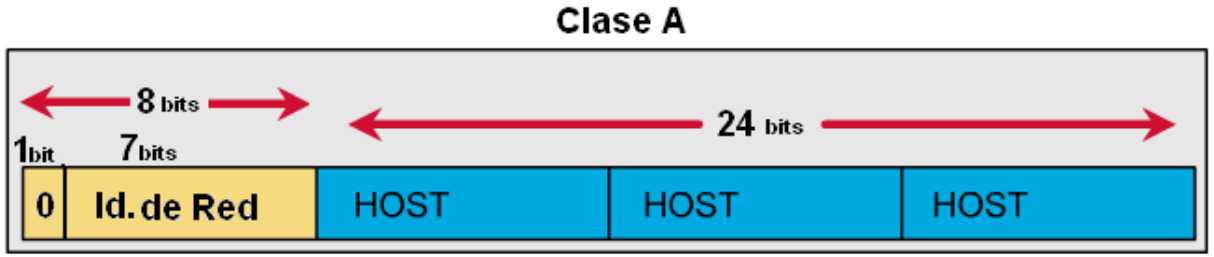
Capa de Red - Direccionamiento

Direcciones clase A

Las direcciones que no se pueden utilizar son:

- Una primera dirección IP para el identificador de la red, que como ya vimos anteriormente estará formada por el primer octeto con el valor de la red correspondiente y el resto de octetos con sus bits a valor cero. (Ejemplo: Identificador de red 124.0.0.0).

- Una dirección IP para difusión o broadcast, que tendrá el primer octeto con el valor de la red y el resto de octetos con los bits a valor 1, es decir 255 en decimal. (Ejemplo: Identificador de red 124.0.0.0 y dirección de broadcast de dicha red 124.255.255.255).



Direcciones clase A

Las direcciones clase A están reservadas a los gobiernos de todo el mundo, aunque en un primer momento de creación de Internet, y sin tener en cuenta las futuras repercusiones, la direcciones clase A fueron asignadas a grandes empresas multinacionales, como Microsoft, Hewlett Packard (HP), etc.

Capa de Red - Direccionamiento

Universidad del Valle

Direcciones clase B

- Lo que caracteriza una red clase B es que sus dos primeros bits (los que se encuentran más a la izquierda) tomarán siempre el valor binario 10, es decir, el primer octeto tendrá un valor decimal entre 128 y 191, además las direcciones clase B utilizan los dos primeros octetos para el identificador de red, por lo que restan los dos últimos octetos para el identificador de host. Un ejemplo de una red de clase B será 151.23.45.76.

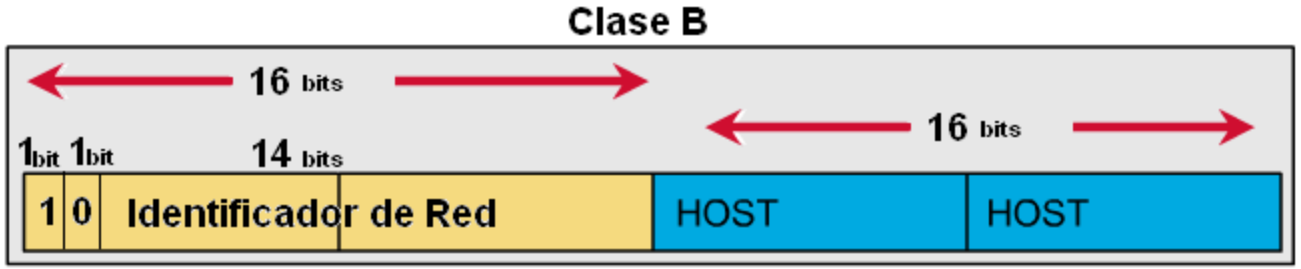
- Como se pueden utilizar los dos últimos octetos para identificador de host, en una red clase B existirán un máximo 216 conexiones, es decir, 65.536 conexiones distintas, de las cuales, igual que en el caso anterior, dos están reservadas para la red y para el broadcast, por lo tanto, el número máximo de conexiones reales será de 216 – 2 = 65.534.

- Una dirección identificativa de red clase B tendrá los dos primeros octetos con cualquier valor siempre que comiencen por 10 binario y el resto de los octetos tendrán sus bits a valor cero. (Ejemplo: Identificador de red 151.23.0.0)

Capa de Red - Direccionamiento

Direcciones clase B

- La dirección de broadcast de una red de clase B tendrá los dos primeros octetos con cualquier valor siempre que comience por 10 binario y el resto de los octetos tendrán sus bits a valor uno. (Ejemplo: Identificador de red 151.23.0.0 y dirección de broadcast de la red 151.23.255.255)



Las direcciones clase B se asignan a empresas de tamaño medio. Si la empresa fuera tan grande como para necesitar un rango de direcciones mayor que el proporcionado por la clase B, se le asignarían 2 o más clases B.

Capa de Red - Direccionamiento

Universidad del Valle

Direcciones clase C

- Lo que caracteriza una red clase C es que sus tres primeros bits (los que se encuentran más a la izquierda) tomarán siempre el valor binario 110, es decir, el primer octeto tendrá un valor decimal entre 192 y 223, además las direcciones clase C utilizan los tres primeros octetos para el identificador de red, por lo que únicamente queda el último octeto para el identificador de host. Un ejemplo de una red de clase C será 192.21.45.9.

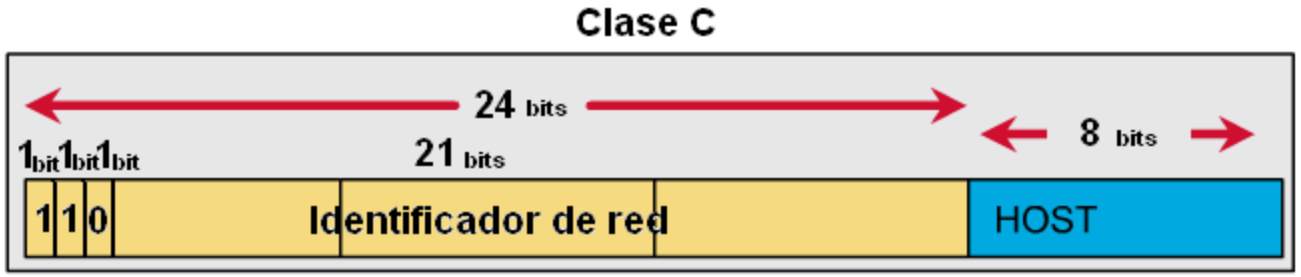
- Al quedar únicamente el último octeto para identificador de host, en una red de clase C existirá un máximo de 28 conexiones, es decir, 256 conexiones distintas, de las cuales, igual que en los casos anteriores, dos están reservadas para la red y para el broadcast, por lo tanto, el número máximo de conexiones reales será de 28 – 2 = 254.

- Una dirección identificativa de red clase C tendrá los tres primeros octetos con cualquier valor siempre que comiencen por 110 binario y en el último octeto tendrán sus bits a valor cero. (Ejemplo: Identificador de red 192.21.45.0)

Capa de Red - Direccionamiento

Direcciones clase C

- La dirección de broadcast de una red de clase C tendrá los tres primeros octetos con cualquier valor siempre que comience por 110 binario y el último octeto tendrán sus bits a valor uno. (Ejemplo: Identificador de red 192.21.45.0 y dirección de broadcast de la red 192.21.45.255)



Las direcciones clase C son asignadas a organizaciones pequeñas y si fuera necesario se le asignarían varias direcciones de clase C.

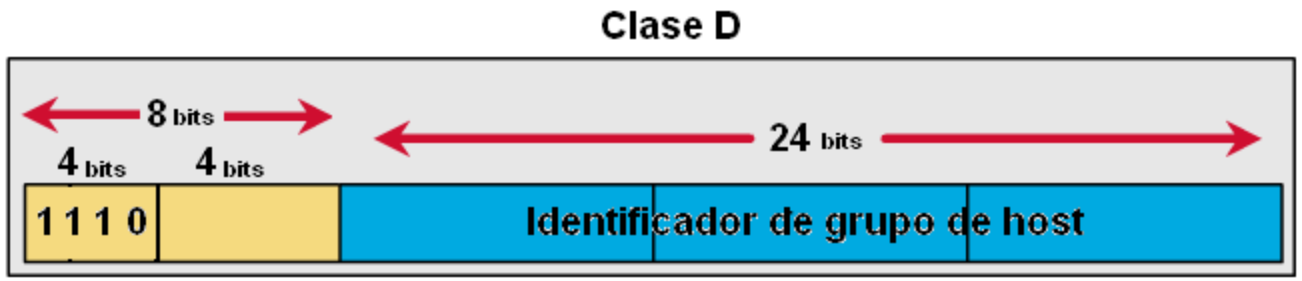
Capa de Red - Direccionamiento

Universidad del Valle

Direcciones clase D

- Las direcciones de clase D son direcciones de multicast o multienvío. El multicast consiste en que un datagrama sea entregado a varios host dentro de la red en lugar de todos (broadcast) o uno sólo (unicast).Se puede decir que una dirección de clase D o multicast identifica un grupo de host dentro de la red.

- Lo que caracteriza a las direcciones clase D es que sus cuatro primeros bits (los que se encuentran más a la izquierda) tomarán siempre el valor binario 1110, es decir, el primer octeto tendrá un valor decimal entre 224 y 239, además las direcciones clase D utilizan únicamente el primer octeto como identificativo de red y los tres octetos restantes se utilizan como identificativo de grupo de host.

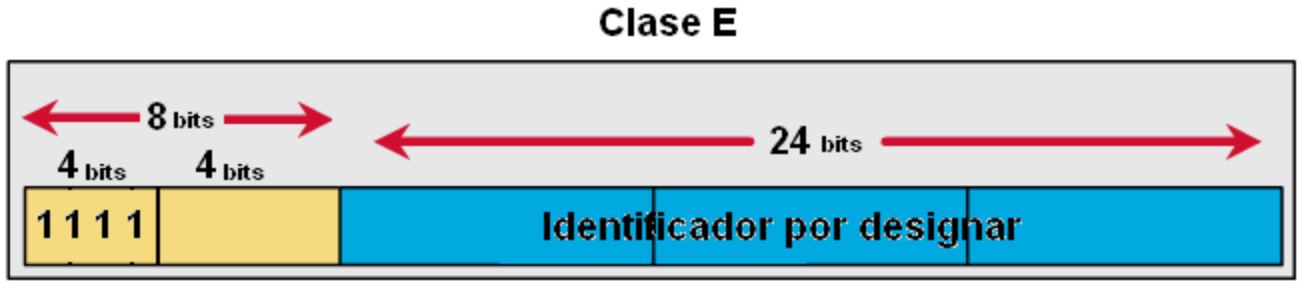


Capa de Red - Direccionamiento

Direcciones clase E

- Las direcciones de clase E están reservadas para uso experimental en proyectos de investigación en la red.

- Lo que caracteriza a las direcciones clase E es que sus cuatro primeros bits (los que se encuentran más a la izquierda) tomarán siempre el valor binario 1111, es decir, el primer octeto tendrá un valor decimal entre 240 y 255, además las direcciones clase D utilizan únicamente el primer octeto como identificativo de red y los tres octetos restantes están por designar para futuros proyectos y experimentaciones.



Capa de Red - Direccionamiento

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, 7 de modo que la cantidad máxima de hosts es 224 - 2 (se excluyen la dirección reservada para broadcast (últimos octetos a 1) y de red (últimos octetos a 0)), es decir, 16 777 214 hosts.

- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts,7 de modo que la cantidad máxima de hosts por cada red es 216 - 2, o 65 534 hosts.

- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts,7 de modo que la cantidad máxima de hosts por cada red es 28 - 2, o 254 hosts.

Capa de Red - Direccionamiento

Clase	Bits iniciales	Intervalo (*)	N.º de redes	N.º de direcciones por red	N.º de hosts por red(‡)	Máscara de red	Dirección de *broadcast*
A	0	0.0.0.0 - 127.255.255.255	126	16 777 216	16 777 214	255.0.0.0	x.255.255.255
B	10	128.0.0.0 - 191.255.255.255	16 384	65 536	65 534	255.255.0.0	x.x.255.255
C	110	192.0.0.0 - 223.255.255.255	2 097 152	256	254	255.255.255.0	x.x.x.255
D (Multicast)	1110	224.0.0.0 - 239.255.255.255					
E (experimental)	1111	240.0.0.0 - 255.255.255.255					

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
1111111.00000000.00000000.00000000	255.0.0.0	/8	16.777.214	16.777.216	A
11111110.00000000.00000000.00000000	254.0.0.0	/7	33.554.430	33.554.432	
11111100.00000000.00000000.00000000	252.0.0.0	/6	67.108.862	67.108.864	
11111000.00000000.00000000.00000000	248.0.0.0	/5	134.217.726	134.217.728	
11110000.00000000.00000000.00000000	240.0.0.0	/4	268.435.454	268.435.456	
11100000.00000000.00000000.00000000	224.0.0.0	/3	536.870.910	536.870.912	
11000000.00000000.00000000.00000000	192.0.0.0	/2	1.073.741.822	1.073.741.824	
10000000.00000000.00000000.00000000	128.0.0.0	/1	2.147.483.646	2.147.483.648	
00000000.00000000.00000000.00000000	0.	/0	4.294.967.294	4.294.967.296	

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
11111111.11111111.00000000.00000000	255.255.0.0	/16	65.534	65.536	B
11111111.11111110.00000000.00000000	255.254.0.0	/15	131.070	131.072	
11111111.11111100.00000000.00000000	255.252.0.0	/14	262.142	262.144	
11111111.11111000.00000000.00000000	255.248.0.0	/13	524.286	524.288	
11111111.11110000.00000000.00000000	255.240.0.0	/12	1.048.574	1.048.576	
11111111.11100000.00000000.00000000	255.224.0.0	/11	2.097.150	2.097.152	
11111111.11000000.00000000.00000000	255.192.0.0	/10	4.194.302	4.194.304	
11111111.10000000.00000000.00000000	255.128.0.0	/9	8.388.606	8.388.608	

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
11111111.11111111.11111111.00000000	255.255.255.0	/24	254	256	C
11111111.11111111.11111110.00000000	255.255.254.0	/23	510	512	
11111111.11111111.11111100.00000000	255.255.252.0	/22	1.022	1.024	
11111111.11111111.11111000.00000000	255.255.248.0	/21	2.046	2.048	
11111111.11111111.11110000.00000000	255.255.240.0	/20	4.094	2.096	
11111111.11111111.11100000.00000000	255.255.224.0	/19	8.190	8.192	
11111111.11111111.11000000.00000000	255.255.192.0	/18	16.382	16.384	
11111111.11111111.10000000.00000000	255.255.128.0	/17	32.766	32.768	

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
11111111.11111111.11111111.11111111	255.255.255.255	/32		0	C
11111111.11111111.11111111.11111110	255.255.255.254	/31		2	
11111111.11111111.11111111.11111100	255.255.255.252	/30	2	4	
11111111.11111111.11111111.11111000	255.255.255.248	/29	6	8	
11111111.11111111.11111111.11110000	255.255.255.240	/28	14	16	
11111111.11111111.11111111.11100000	255.255.255.224	/27	30	32	
11111111.11111111.11111111.11000000	255.255.255.192	/26	62	64	
11111111.11111111.11111111.10000000	255.255.255.128	/25	126	128	

Plan Estratégico
de Desarrollo 2025 - 2035
visión de futuro 2045

Por la universidad que soñamos
¡Participa!

Fundamentos de Redes

MBA Jorge Andrés Ángel Salazar
Esp. Gestión y Seguridad de Bases de Datos
Ingeniero de Sistemas y Computación
Tecnólogo en Sistemas de Información

Capa de Red - Segmentación

La segmentación de una red de datos es el proceso de dividir una red grande en múltiples redes más pequeñas o "segmentos". Esta práctica permite mejorar la organización, seguridad, eficiencia y administración de los recursos en una red. Cada segmento de la red actúa como una subred independiente, lo que puede limitar el tráfico de datos a un área específica y reducir la congestión en la red general.

Beneficios de la Segmentación de Redes

Reducción del Congestionamiento:

Al dividir una red en segmentos, el tráfico de datos se mantiene dentro de cada subred siempre que sea posible, lo cual reduce la congestión general y mejora el rendimiento de la red.

Beneficios de la Segmentación de Redes

Mejora de la Seguridad:

Los segmentos pueden ser aislados entre sí, limitando el acceso entre diferentes áreas de la red. Esto permite aplicar políticas de seguridad específicas y proteger los datos sensibles de usuarios no autorizados.

Beneficios de la Segmentación de Redes

Facilita la Administración de la Red:

Con segmentos más pequeños, es más fácil gestionar y supervisar el tráfico, detectar problemas y aplicar configuraciones de manera específica sin afectar a toda la red.

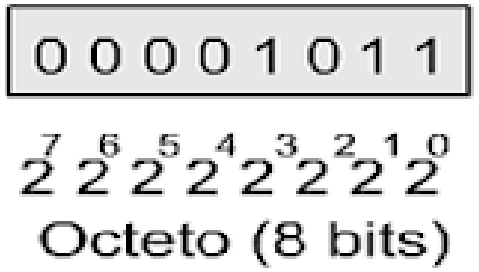
Beneficios de la Segmentación de Redes

Escalabilidad:

Segmentar una red permite un crecimiento más organizado. Es posible agregar nuevos segmentos según sea necesario sin afectar el rendimiento del resto de la red.

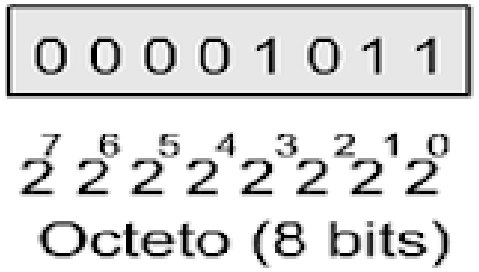
Capa de Red - Segmentación

Ejemplo 1: 11000000.10101000.00000001.00000001 = XXX.XXX.XXX.XXX
Ejemplo 2: 00001010.00000000.00000000.00000001 = XXX.XXX.XXX.XXX
Ejemplo 3: 10101100.00010000.00000000.00000001 = XXX.XXX.XXX.XXX
Ejemplo 4: 11111111.11111111.11111111.00000000 = XXX.XXX.XXX.XXX
Ejemplo 5: 01111111.00000000.00000000.00000001 = XXX.XXX.XXX.XXX
Ejemplo 6: 11000000.00000000.00000010.10010010 = XXX.XXX.XXX.XXX
Ejemplo 7: 11001011.00000000.01110001.00000000 = XXX.XXX.XXX.XXX



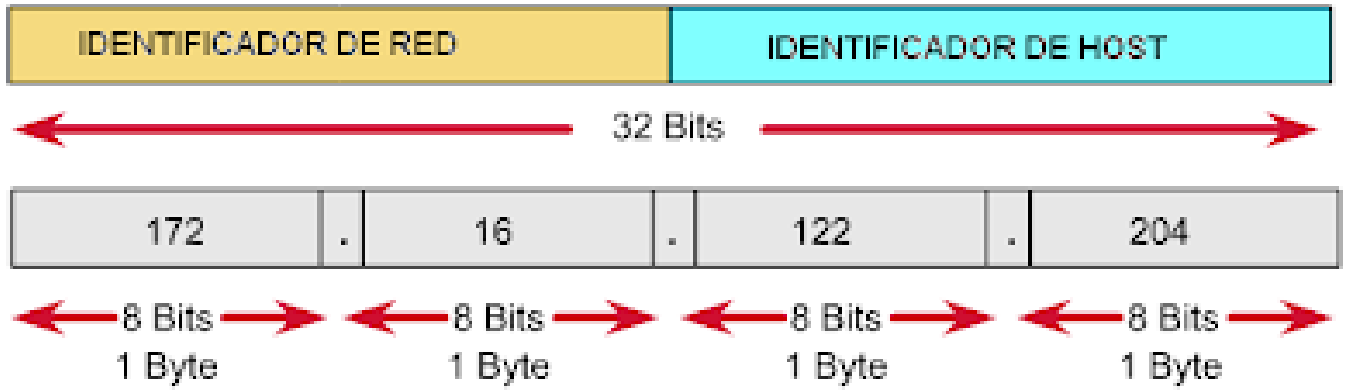
Capa de Red - Segmentación

Ejemplo 1: 11000000.10101000.00000001.00000001 = **192.168.1.1**
Ejemplo 2: 00001010.00000000.00000000.00000001 = **10.0.0.1**
Ejemplo 3: 10101100.00010000.00000000.00000001 = **172.16.0.1**
Ejemplo 4: 11111111.11111111.11111111.00000000 = **255.255.255.0**
Ejemplo 5: 01111111.00000000.00000000.00000001 = **127.0.0.1**
Ejemplo 6: 11000000.00000000.00000010.10010010 = **192.0.2.146**
Ejemplo 7: 11001011.00000000.01110001.00000000 = **203.0.113.0**



Capa de Red - Segmentación

Campos componentes de la dirección IP



Capa de Red - Segmentación

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, 7 de modo que la cantidad máxima de hosts es 224 - 2 (se excluyen la dirección reservada para broadcast (últimos octetos a 1) y de red (últimos octetos a 0)), es decir, 16 777 214 hosts.

- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts,7 de modo que la cantidad máxima de hosts por cada red es 216 - 2, o 65 534 hosts.

- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts,7 de modo que la cantidad máxima de hosts por cada red es 28 - 2, o 254 hosts.

Capa de Red - Segmentación

Clase	Bits iniciales	Intervalo (*)	N.º de redes	N.º de direcciones por red	N.º de hosts por red(‡)	Máscara de red	Dirección de *broadcast*
A	0	0.0.0.0 - 127.255.255.255	126	16 777 216	16 777 214	255.0.0.0	x.255.255.255
B	10	128.0.0.0 - 191.255.255.255	16 384	65 536	65 534	255.255.0.0	x.x.255.255
C	110	192.0.0.0 - 223.255.255.255	2 097 152	256	254	255.255.255.0	x.x.x.255
D (Multicast)	1110	224.0.0.0 - 239.255.255.255					
E (experimental)	1111	240.0.0.0 - 255.255.255.255					

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
1111111.00000000.00000000.00000000	255.0.0.0	/8	16.777.214	16.777.216	A
11111110.00000000.00000000.00000000	254.0.0.0	/7	33.554.430	33.554.432	
11111100.00000000.00000000.00000000	252.0.0.0	/6	67.108.862	67.108.864	
11111000.00000000.00000000.00000000	248.0.0.0	/5	134.217.726	134.217.728	
11110000.00000000.00000000.00000000	240.0.0.0	/4	268.435.454	268.435.456	
11100000.00000000.00000000.00000000	224.0.0.0	/3	536.870.910	536.870.912	
11000000.00000000.00000000.00000000	192.0.0.0	/2	1.073.741.822	1.073.741.824	
10000000.00000000.00000000.00000000	128.0.0.0	/1	2.147.483.646	2.147.483.648	
00000000.00000000.00000000.00000000	0.	/0	4.294.967.294	4.294.967.296	

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
11111111.11111111.00000000.00000000	255.255.0.0	/16	65.534	65.536	B
11111111.11111110.00000000.00000000	255.254.0.0	/15	131.070	131.072	
11111111.11111100.00000000.00000000	255.252.0.0	/14	262.142	262.144	
11111111.11111000.00000000.00000000	255.248.0.0	/13	524.286	524.288	
11111111.11110000.00000000.00000000	255.240.0.0	/12	1.048.574	1.048.576	
11111111.11100000.00000000.00000000	255.224.0.0	/11	2.097.150	2.097.152	
11111111.11000000.00000000.00000000	255.192.0.0	/10	4.194.302	4.194.304	
11111111.10000000.00000000.00000000	255.128.0.0	/9	8.388.606	8.388.608	

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
11111111.11111111.11111111.00000000	255.255.255.0	/24	254	256	C
11111111.11111111.11111110.00000000	255.255.254.0	/23	510	512	
11111111.11111111.11111100.00000000	255.255.252.0	/22	1.022	1.024	
11111111.11111111.11111000.00000000	255.255.248.0	/21	2.046	2.048	
11111111.11111111.11110000.00000000	255.255.240.0	/20	4.094	2.096	
11111111.11111111.11100000.00000000	255.255.224.0	/19	8.190	8.192	
11111111.11111111.11000000.00000000	255.255.192.0	/18	16.382	16.384	
11111111.11111111.10000000.00000000	255.255.128.0	/17	32.766	32.768	

Capa de Red - Segmentación

Universidad del Valle

Binario	Decimal	CIDR	Nº hosts Utilizados	Nº hosts Encontrados	Clase
11111111.11111111.11111111.11111111	255.255.255.255	/32		0	C
11111111.11111111.11111111.11111110	255.255.255.254	/31		2	
11111111.11111111.11111111.11111100	255.255.255.252	/30	2	4	
11111111.11111111.11111111.11111000	255.255.255.248	/29	6	8	
11111111.11111111.11111111.11110000	255.255.255.240	/28	14	16	
11111111.11111111.11111111.11100000	255.255.255.224	/27	30	32	
11111111.11111111.11111111.11000000	255.255.255.192	/26	62	64	
11111111.11111111.11111111.10000000	255.255.255.128	/25	126	128	

Plan Estratégico
de Desarrollo 2025 - 2035
visión de futuro 2045

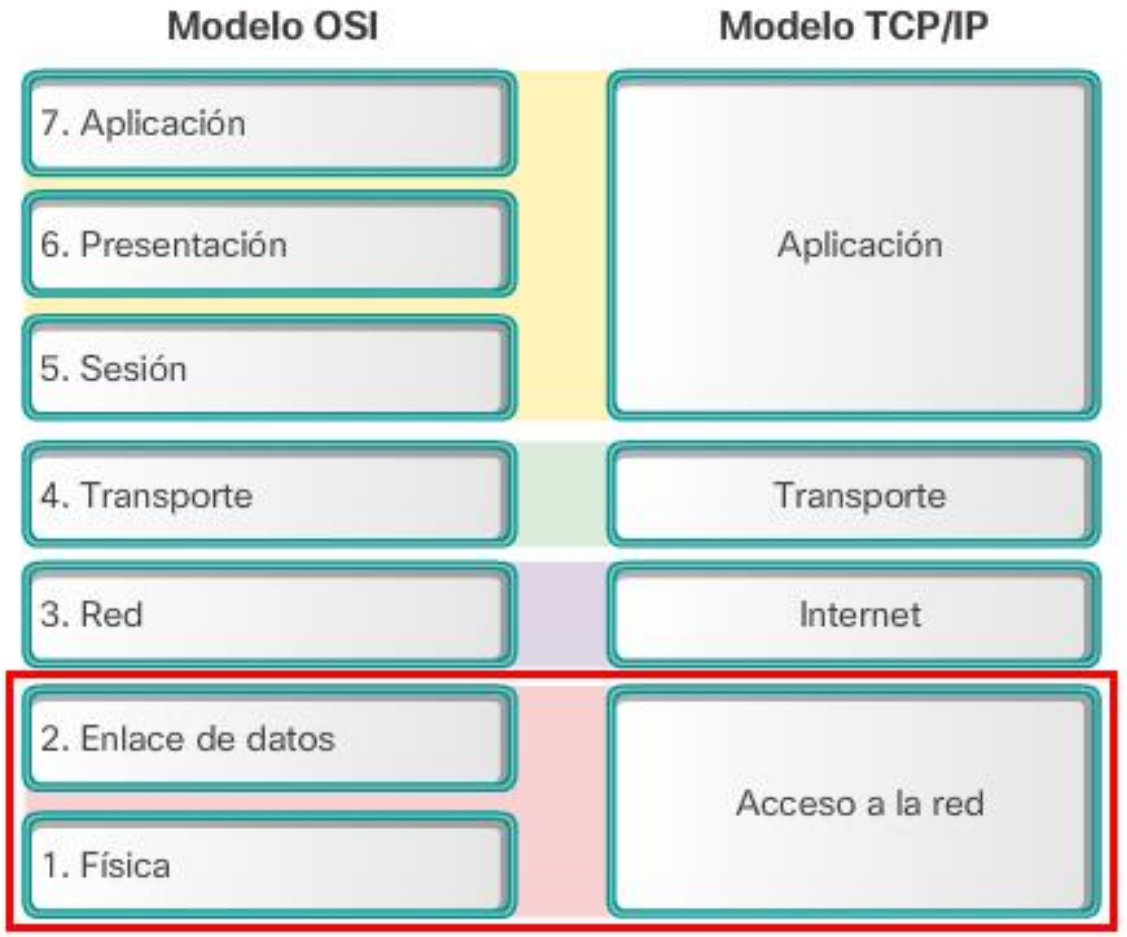
Por la universidad que soñamos
¡Participa!

Fundamentos de Redes

MBA Jorge Andrés Ángel Salazar
Esp. Gestión y Seguridad de Bases de Datos
Ingeniero de Sistemas y Computación
Tecnólogo en Sistemas de Información

Contenido

Sesión 15 - Capa Física – Enlace Datos (Acceso Red)



Capa Acceso a la Red – TCP/IP

La Capa de Acceso a la Red en el modelo TCP/IP (también conocida como Host-to-Network Layer) es la más baja de las capas y se encarga de las funciones físicas y de enlace de datos necesarias para transmitir datos entre dispositivos en una red local o a través de medios físicos de transmisión.

Capa Acceso a la Red – TCP/IP

Universidad del Valle

Componentes clave de la Capa de Acceso a la Red

Protocolos de Enlace de Datos: Establecen reglas para la transferencia de datos entre dispositivos en una red local.
Ejemplos: Ethernet, Wi-Fi (IEEE 802.11), PPP (Protocolo Punto a Punto).

Protocolos de Control de Acceso al Medio (MAC): Determinan cómo los dispositivos comparten el medio de transmisión.
Ejemplos: CSMA/CD (Ethernet), CSMA/CA (Wi-Fi).

Hardware: Incluye los componentes físicos que permiten la conexión y transmisión de datos.
Ejemplos: NICs, switches, routers, puntos de acceso.

Direcciones físicas: Identifican de manera única a cada dispositivo en la red local.
Ejemplo: Dirección MAC de una tarjeta de red.

Capa Acceso a la Red – TCP/IP

Universidad del Valle

Funciones principales de la Capa de Acceso a la Red

Encapsulación y des-encapsulación de datos: Los datos provenientes de la capa de Internet (por ejemplo, un paquete IP) se encapsulan en tramas para ser enviados a través de los medios físicos.
En el receptor, las tramas son des-encapsuladas para recuperar los datos.

Acceso al medio: Define cómo los dispositivos acceden al medio físico de transmisión (cableado, inalámbrico, fibra óptica, etc.).Esto incluye técnicas como CSMA/CD en Ethernet o CSMA/CA en redes inalámbricas.

Dirección física: Utiliza direcciones físicas como las direcciones MAC para identificar dispositivos en una red local.

Capa Acceso a la Red – TCP/IP

Universidad del Valle

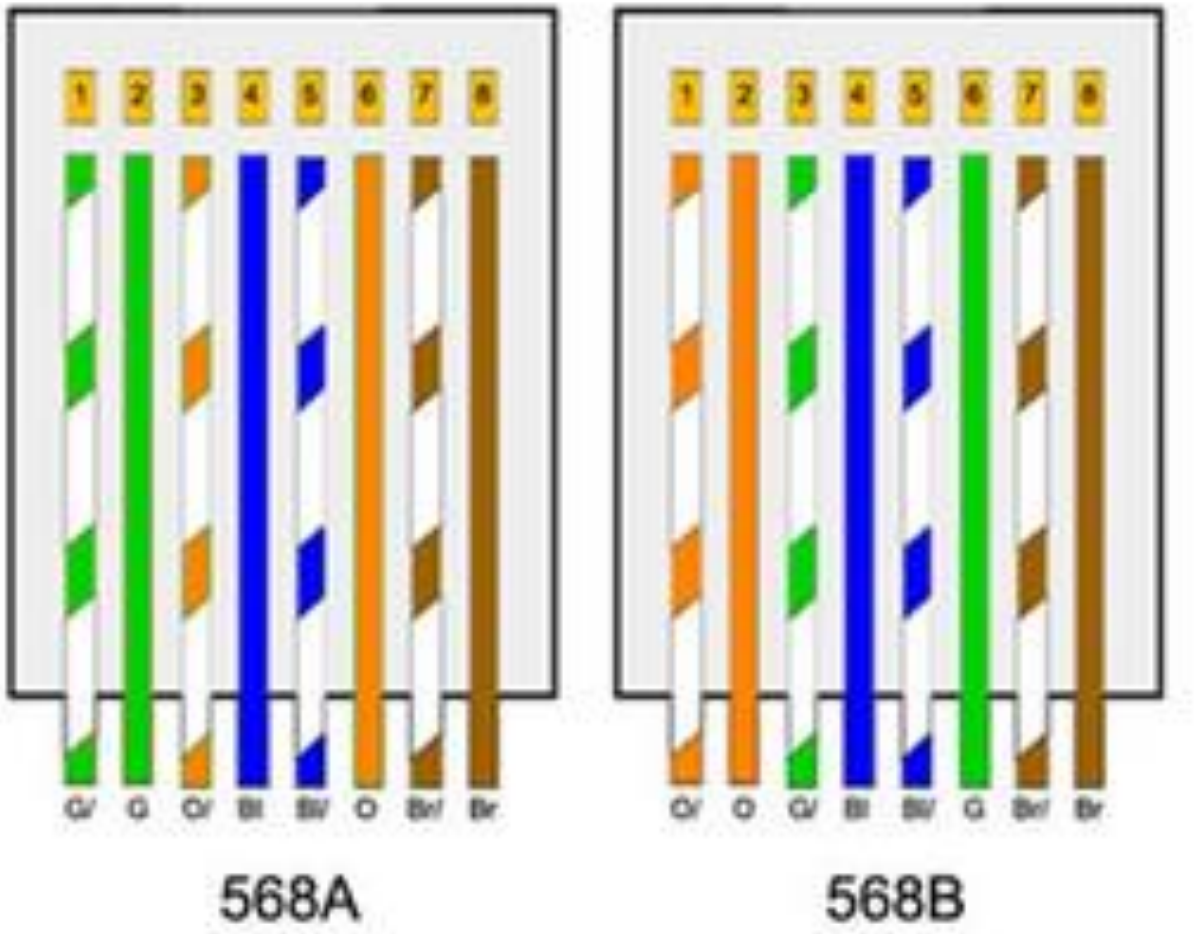
Funciones principales de la Capa de Acceso a la Red

Detección y corrección de errores: Implementa mecanismos para detectar errores en las tramas transmitidas. Por ejemplo, los protocolos como Ethernet utilizan CRC (Cyclic Redundancy Check) para verificar la integridad de los datos.

Gestión de hardware: Coordina el hardware de red, como tarjetas de red (NIC), cables y dispositivos de interconexión (switches, hubs).

Interoperabilidad con diferentes tecnologías: Permite que los protocolos de las capas superiores funcionen independientemente del tipo de red física utilizada.

Capa Acceso a la Red – TCP/IP



Capa Acceso a la Red – TCP/IP

Las normas **568A** y **568B** son estándares definidos por la organización **TIA/EIA (Telecommunications Industry Association / Electronic Industries Alliance)**, utilizados para establecer la disposición de los cables de par trenzado en conectores RJ-45 para redes de datos. Estas normas aseguran la interoperabilidad entre dispositivos y facilitan la instalación de infraestructuras de red.

Objetivo de las Normas

- Especificar el orden de los colores de los hilos dentro del conector RJ-45.
- Garantizar una conexión adecuada para transmitir datos y señales de red (Ethernet).
- Permitir que los cables sean compatibles con diferentes dispositivos y estándares de red.

Capa Acceso a la Red – TCP/IP

Pin	Color T568A	Color T568B	Función
1	Blanco-Verde	Blanco-Naranja	Transmisión de datos (+)
2	Verde	Naranja	Transmisión de datos (-)
3	Blanco-Naranja	Blanco-Verde	Recepción de datos (+)
4	Azul	Azul	No usado (PoE positivo)
5	Blanco-Azul	Blanco-Azul	No usado (PoE positivo)
6	Naranja	Verde	Recepción de datos (-)
7	Blanco-Marrón	Blanco-Marrón	No usado (PoE negativo)
8	Marrón	Marrón	No usado (PoE negativo)

Capa Acceso a la Red – TCP/IP

Universidad del Valle

Funciones en Detalle

1.Pares de datos (1-2 y 3-6):

1. Los pines 1 y 2 (Transmisión) y 3 y 6 (Recepción) son los únicos utilizados en Ethernet de **10 Mbps y 100 Mbps**.
2. En estas configuraciones, solo se usan dos pares de los cuatro disponibles.

2.Pares adicionales (4-5 y 7-8):

1. En configuraciones de **Gigabit Ethernet (1000BASE-T)**, se usan los 4 pares para transmitir y recibir datos simultáneamente.
2. En redes PoE, pueden transportar alimentación eléctrica.

3.Power over Ethernet (PoE):

1. Algunos estándares PoE (como IEEE 802.3af y 802.3at) utilizan los pares no empleados (4-5 y 7-8) para suministrar corriente eléctrica.
2. Otros estándares avanzados, como **PoE+**, pueden utilizar todos los pares para alimentación.

Contenido

Capa Acceso a la Red – TCP/IP