

## **Conmutación de Paquetes (Facilidad Disponible) Todos tienen acceso con velocidad disminuida**

Es un método para dividir los archivos de datos en paquetes o porciones más pequeñas con el fin de enviarlos mejor a través de diferentes redes.

### **Ventajas:**

- Es el uso más eficiente del ancho de banda total de la red.
- Es más barato construirlos, ya que se necesita menos equipo.
- Es más fiable. Si se detecta que falta un paquete, el destino solicita que sea reenviado.
- Ofrece redireccionamiento automático en caso de que un nodo falle en su recorrido.
- No tiene líneas atadas y se puede mover fácilmente alrededor de las partes rotas de la red.
- A medida que los clientes aumentan, en comparación con la conmutación de circuitos, la red sólo tiene que expandirse lentamente.

### **Desventajas**

- Hay grandes retrasos en la recepción de mensajes debido al tiempo requerido para empaquetar y encaminar los paquetes. Pueden no ser significativos, pero no proporcionan calidad de servicio (QoS) para alcanzar algunos niveles de rendimiento requeridos.
- Los enlaces físicos compartidos pueden suponer una violación de la seguridad de la red.
- No es adecuado para paquetes de datos pequeños -si el paquete de datos en sí es de sólo 600 bytes, entonces es necesario utilizar dos paquetes de 512 bytes con la información de la dirección.
- Latencia impredecible.

## **Conmutación de circuitos (los usuarios que acceden primero ocupan los canales)**

### **Ventajas**

- Que exista un canal con el ancho de banda fijo, la comunicación es constante mientras dure la sesión.
- Al tratarse de un circuito fijo no hay margen para que se produzcan retrasos por el encadenado de los datos.
- Facilita la comunicación en tiempo real.
- Con ella se agiliza mucho los datos y los cambios que haya que reflejar en los procesos de trabajo, permitiendo que todo resulte más dinámico.
- Es un tipo de conmutación muy completa, útil.

### **Desventajas**

- Mientras dure la comunicación se consumirán muchos recursos del sistema, como ancho de banda.
- Es posible que se produzcan retrasos en el establecimiento de las llamadas y es posible que algunas llamadas sean intermitentes dependiendo de la estabilidad de los canales y de lo congestionados que se encuentren.
- Ausencia de canales alternativos físicos que permitan aumentar la efectividad y blindarse ante posibles carencias.
- Además, el establecimiento de la comunicación puede ser un poco más lento de lo esperado.
- Posibles fallas en el sistema físico, daños externos en estas plataformas.

## Protocolos

- Codificación del mensaje

Proceso mediante el cual la información se convierte en otra forma aceptable para la transmisión. La decodificación revierte este proceso para interpretar la idea

El host emisor, primero convierte en bits los mensajes enviados a través de la red. Cada bit se codifica en un patrón de sonidos, ondas de luz o impulsos electrónicos, según el medio de red a través del cual se transmitan los bits. El host de destino recibe y decodifica las señales para interpretar el mensaje

- Formato y encapsulamiento del mensaje

Cuando se envía un mensaje desde el origen hacia el destino, se debe utilizar un formato o estructura específicos. Los formatos de los mensajes dependen del tipo de mensaje y el canal que se utilice para entregar el mensaje

- Tamaño del mensaje

Las reglas pueden ser diferentes, de acuerdo con el canal utilizado.

Las tramas que son demasiado largas o cortas no se entregan.

Las restricciones de tamaño de las tramas requieren que el host de origen divida un mensaje largo en fragmentos individuales que cumplan los requisitos de tamaño mínimo y máximo. El mensaje largo se enviará en tramas independientes, cada trama contendrá una parte del mensaje original. Cada trama también tendrá su propia información de direccionamiento.

- Sincronización del mensaje

- **Método de acceso**

Determina en qué momento alguien puede enviar un mensaje.

Las computadoras deben definir un método de acceso. Los hosts de una red necesitan un método de acceso para saber cuándo comenzar a enviar mensajes y cómo responder cuando se produce alguna colisión.

- **Control de flujo**

Afecta la cantidad de información que se puede enviar y la velocidad con la que puede entregarse.

Los hosts de origen y destino utilizan métodos de control de flujo para negociar la sincronización correcta a fin de que la comunicación sea exitosa.

- **Tiempo de espera para la respuesta**

Los hosts de las redes también tienen reglas que especifican cuánto tiempo deben esperar una respuesta y qué deben hacer si se agota el tiempo de espera para la respuesta

- Opciones de entrega

Unicast      Multicast      Broadcast

- Reglas de comunicaciones (Suites de protocolos)

Es un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación. Los hosts y los dispositivos de red implementan las suites de protocolos en software, hardware o ambos.

## Modelo OSI (Open Systems Interconnection)

- Objetivo

Promover la creación de estándares independientes del fabricante.

Proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él.

- Capas

- **Aplicación**

- Sobre esta capa están las aplicaciones que utilizan los usuarios.
    - Cualquier aplicación que admita comunicación de red se desarrollará utilizando interfaces de programación de aplicaciones de red (API).
    - La API contiene código que le dice a la aplicación cómo hablar con la capa de la aplicación.
    - Envía los datos de usuario a la aplicación de destino usando los servicios de las capas inferiores
    - SMTP, POP, IMAP, HTTP, DNS, SSH, FTP

- **Presentación**

- Convierte los datos de la red al formato requerido por la aplicación. Es la presentación común de los datos transferidos
      - Los datos de la aplicación dependen de la máquina
      - Los datos de las capas bajas son independientes de la máquina
    - JPEG, ASCII, TIFF, GIF

- **Sesión**

- Sincroniza el intercambio de datos entre capas inferiores y superiores
      - Establece conexión
      - Cierra la conexión
    - Es en esta capa que los dispositivos acuerdan el tipo de comunicación que va a tomar.
      - Simplex
      - Half-duplex
      - Full-duplex
    - RPC, SQL, NetBIOS, Point-to-point tunneling protocol (PPTP)

- **Transporte**

- Define servicios para segmentar, transferir y reensamblar los datos.
      - Conexión extremo a extremo
      - Verifica que los datos se transmitan correctamente
    - TCP, UDP

- **Red**

- Proporciona servicios para intercambiar los datos individuales en la red.
    - Suministra la información sobre la ruta a seguir.
    - Es responsable del direccionamiento lógico de los dispositivos mediante el uso de direcciones IP.

- **Enlace de datos**

- Protocolos de la capa
      - IP
      - Internetwork Packet Exchange (IPX)
    - Describe los métodos para intercambiar tramas de datos entre dispositivos en un medio común.
      - Detecta y corrige Errores de transmisión
      - Provee el control de acceso a la capa física
    - Si los datos están destinados a un dispositivo dentro de la misma subred, el enlace será a ese dispositivo. Si los datos están destinados a un dispositivo fuera de la subred, el enlace será a la puerta de enlace predeterminada.
    - LogicalLink Control (LLC)

- Identifica que protocolo de capa de red se está utilizando (IP, IPX) y lo pone en el encabezado del marco
  - Media Access Control (MAC)
    - Controla cuando los datos se colocan en el medio.
    - 802.3 y 802.11
  - **Física**
    - Transmite datos en forma de bits.
    - Especifica los medios de transmisión mecánicos, eléctricos, funcionales, así como procedimientos.
    - No hay protocolos, pero si hay criterios y estándares.
- Encapsulamiento

Aplicación - Datos

Presentación - Datos

Sesión - Datos

Transporte - Segmentos

Red - Paquetes

Enlace de datos - Frames

Física – Bits

1. El rango de puertos del 0 al 1024, se conocen como bien conocidos.
2. NTP (Puerto 123)
3. Segundo paso del three-way handshake es SYNC/ACK
4. IANA asigna los puertos

## Modelo TCP/IP (Protocolo de Internet)

Conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

- Características
  - Protocolo de comunicación orientado a conexión y fiable del nivel de transporte.
  - Brinda al IP un servicio que permita que una comunicación entre dos dispositivos se efectúe libre de errores, sin pérdidas y con seguridad.
  - Divide los datos en paquetes
  - Su función es el envío de paquetes a nivel local y a través de redes, no es orientado a conexión por lo tanto se considera no fiable
  - Es la base del Internet
  - Sirve para enlazar computadoras que utilizan diferentes sistemas operativos sobre redes de área local y área extendida
- Protocolos de acuerdo con la capa
  - **Aplicación**
    - SSH, FTP, SMTP, DHCP, DNS, RIP, SNMP, HTTP
  - **Transporte**
    - TCP, UDP, DCCP, UTP, ICMP, FCP
  - **Internet**
    - IP, ICMP, IPSEC, IGMP
  - **Interfaz de red**
    - ARP, L2TP, NDP, ETHERNET

- Capa de aplicación

Actúa como interfaz entre las aplicaciones y la pila de red a través de API y biblioteca de programación.

- Formateo
- Compresión
- Cifrado de datos
- Protocolos

- Telnet (Más rápido que ssh) (23)

- Es un protocolo cliente-servidor, de emulación de terminal, utilizado para proporcionar acceso remoto a servidores y dispositivos de red. Especifica cómo se establece y termina una sesión virtual, y sus comandos asociados.
- Ventajas
  - Los servidores pueden tener múltiples clientes que solicitan información al mismo tiempo.
  - Telnet está disponible prácticamente en todos los sistemas operativos y facilita la interoperabilidad en redes heterogéneas
- Desventajas
  - No admite el transporte de datos encriptados, todos los datos intercambiados entre cliente y servidor, en una sesión telnet se transportan en texto plano (sin encriptar).

- SSH (22)

- Es un protocolo que se utiliza en el manejo de servidores de forma remota, permitiendo a un usuario realizar toda clase de tareas sobre el mismo.
- En estas conexiones, toda la información viaja de forma encriptada, lo cual lo convierte en uno de los medios más seguros a la hora de trabajar en un servidor.
- Requiere una herramienta, puede ser del tipo terminal o consola. La conexión SSH usa tres ítems: un usuario, un puerto y un servidor.
- La seguridad se logra mediante el uso de llaves y técnicas de cifrado.
- Cada server tiene su propia llave de cifrado
- Se genera una lista de servidores a los cuales es seguro conectarnos.

- DNS (53) UDP

- El servidor DNS, contiene bases de datos en las que se encuentran las direcciones IP y los nombres de dominio asociados a ellas.
- Se dedica a traducir las direcciones o nombres alfanuméricos que tecleamos en nuestro buscador en direcciones IP, de modo que se pueda localizar fácilmente el sitio web al que queremos acceder.

- FTP (21 y 20)

- It is used for exchanging files over the internet.
- Uses TCP
- Requires authentication
- It enables the users to upload and download the files from the internet.
- FTP is used for transferring one file at a time in either direction between the client and the server.

- TFTP (69)

- Uses UDP
- Trivial transfer protocol
- Does not require authentication
- Menos complejo
- Mainly used for transmission of configurations to and from network devices

- SMTP (25)
  - It is used for sending the emails efficiently and reliably over the internet.
  - SMTP is a push protocol.
  - SMTP uses TCP at the transport layer.
  - SMTP uses port number 25.
  - SMTP uses persistent TCP connections, so it can send multiple emails at once.
  - SMTP is a connection oriented protocol.
  - SMTP is an in-band protocol.
  - SMTP is a stateless protocol.
  - Does not require authentication
- SNMP(161/162)
  - SNMP is an application layer protocol which uses UDP port number 161/162. SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.
- DHCP(67)
  - Dynamic Host Configuration Protocol es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.
  - También asigna la máscara de subred, la dirección de puerta de enlace predeterminada, la dirección del servidor de nombres de dominio (DNS) y otros parámetros de configuración pertinentes.
- HTTP
  - It is mainly used for the retrieval of data from websites throughout the internet.
  - It works on the top of TCP/IP suite of protocols.
  - It is the protocol that allows web servers and browsers to exchange data over the web.
  - It is a request response protocol.
  - It uses the reliable TCP connections by default on TCP port 80.
  - It is stateless means each request is considered as the new request. In other words, server doesn't recognize the user by default.
- Capa de Transporte
  - TCP (Transmission Control Protocol)
    - Para crear “conexiones” entre sí a través de las cuales puede enviarse un flujo de datos.
    - Garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.
    - Proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.
    - Protocolos
      - MTP (Protocolo de transferencia multimedia)
      - FTP (Protocolo de transferencia de archivos) 20-21
      - TELNET (Protocolo cliente / servidor) 23
      - SMTP (Envío de mensajes de correo electrónico) 25
      - DNS (Resolución de nombre de dominio) 53
      - HTTP (Transferencia de hipertexto) 80
      - POP3 (Obtención de mensajes de correo electrónico en clientes locales) 110
      - IMAP (Acceso a correo electrónico) 143
      - HTTPS (Transferencia segura de hipertexto) 443
      - DHCP (Configuración automática de parámetros de red) 67-68
      - UDP (Intercambio de datagramas a través de una red) 113

➤ UDP (Datagrama de Usuario)

- Es un protocolo sin conexión que, como TCP, funciona en redes IP.
- UDP/IP proporciona muy pocos servicios de recuperación de errores, ofreciendo en su lugar una manera directa de enviar y recibir datagramas a través una red IP.
- Se utiliza sobre todo cuando la velocidad es un factor importante en la transmisión de la información

## Capa de Internet

➤ IP, Internet Protocol

- Porta datagramas de la fuente al destino.
- Es la base fundamental de la Internet.
- El nivel de transporte parte el flujo de datos en datagramas.
- Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino
- Características
  - Sin conexión
    - No establece conexión con el destino antes de enviar los paquetes de datos
    - Emisor
      - No sabe si el destinatario está presente
      - No sabe si el paquete llegó
      - No sabe si el receptor puede leer el paquete
    - Receptor
      - No sabe cuándo llegará el paquete
  - Servicio mínimo
    - No es confiable por naturaleza, la entrega de datos no está garantizada
  - Independiente de los medios
    - No importa el medio (cobre, fibra, aire)

➤ Utiliza 2 protocolos

- IPv4
- IPv6

➤ Capa IP

- Direccionamiento de terminales
  - Los terminales se deben configurar con una dirección IP única para identificarlos en la red.

➤ Brinda servicios para permitir que los terminales puedan intercambiar datos en la red. Para lograr el transporte completo, la capa de red utiliza cuatro procesos básicos:

- Direccionamiento de terminales
- Encapsulamiento
  - La capa de red encapsula la unidad de datos del protocolo (PDU) de la capa de transporte a un paquete. El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen (emisores) y de destino (receptores).
- Routing
  - Para transferir un paquete a otras redes, debe procesarlo un router.
  - La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino
  - Un paquete puede cruzar muchos dispositivos intermediarios antes de llegar al host de destino.
  - Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.
- Desencapsulamiento
  - Cuando el paquete llega a la capa de red del host de destino, el host revisa el encabezado IP del paquete.
  - Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete.

- Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene se transfiere al servicio apropiado en la capa de transporte.

#### ➤ Gateway

- Dispositivo de red que puede enrutar el tráfico a otras redes
- Puede enrutar el tráfico fuera de la red local
- La dirección IP de la interfaz del Router es la dirección de Gateway predeterminado para las PC

## Protocolo ARP

Es un protocolo de comunicaciones de la capa de red, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP

- Cada equipo conectado a una red tiene un número de 48 bits (6 bloques hexadecimales de 8 bits cada uno) que le identifica.
- Esta dirección es única para cada dispositivo.
- Los 24 primeros bits identifican al fabricante y los 24 últimos son los propios del equipo (tablet, smartphone, Arduino, Raspberry Pi, etc).
- La comunicación por Internet no utiliza directamente esta dirección (MAC), sino que utiliza direcciones IP, es decir, que tiene que haber relación entre direcciones físicas (MAC) y lógicas.

¿Cuándo se usa ARP?

- Existen 2 hosts en una misma red y uno quiere enviar un paquete a otro.
- Existen 2 hosts en redes diferentes y deben usar un router para llegar al otro host.
- Cuando un router necesita enviar un paquete a un host a través de otro router.
- Cuando un router necesita enviar un paquete a un host de la misma red.

## Cableado

- Área de trabajo.
- Cableado horizontal.
- Armario de telecomunicaciones (racks, closet).
- Cableado vertical.
- Sala de equipos.
- Backbone.
- Cable
  - Coaxial
    - Compuesto por dos conductores que se orientan de manera coaxial y son separados por una capa de aislamiento dieléctrico.
    - Diseñado para transportar señales de alta frecuencia y para protegerlas frente a las interferencias electromagnéticas de fuentes externas.
    - El conductor central es el encargado de llevar la información y el conductor exterior (malla) que sirve como referencia de tierra y retorno de las corrientes.
    - Puede transmitir información a 10 Mbps sobre distancias de casi 600 m, por lo que se utiliza en redes LAN de pequeña cobertura



- STP: blindado uno por uno
- FTP: todo blindado
- UTP: sin blindar
  - T-568 A
    - Verde/Blanco
    - Verde
    - Naranja/Blanco
    - Azul
    - Azul/Blanco
    - Naranja
    - Café/Blanco
    - Café
  - T-568 B
    - Naranja/Blanco
    - Naranja
    - Verde/blanco
    - Azul
    - Azul/blanco
    - Verde
    - Café/blanco
    - Café
- Fibra óptica
  - Es una delgada y flexible hebra de vidrio o silicio fundido que conduce la luz.
  - Son necesarios dos filamentos para una comunicación bidireccional: Txy Rx.
  - Puede utilizarse en una LAN y para lograr transmisiones de largo alcance
  - Al utilizar la luz como información, cuentan con una velocidad de transmisión mayor.
  - Mono-modo
    - Permite el paso de un solo haz de luz
    - Longitudes de onda comunes son: 1310 nmy 1550 nm
    - Se utiliza para largas distancias
    - Menor atenuación que multi-modo
  - Multi-modo
    - Permite el paso de varios haces de luz
    - Opera en longitudes de onda de 850 nmy 1300 nm
    - Se utiliza en distancias cortas o redes privadas
    - Presenta mayor atenuación que la fibra mono-modo

## Dispositivos

- **HUB (Envía todos los dispositivos) Física**
  - Permiten la interconexión de diferentes estaciones y segmentos de red.
  - Puede ser usado en una LAN convencional para crear una estructura estrella en la cual el concentrador se encuentra en el centro de la misma
- **Switch (Solo al que se busca conectar) Enlace de datos**
  - El switch es un dispositivo que se utiliza para conectar equipos en red, formando una red de área local (LAN) y se encargan de la interconexión de dispositivos cableados, que siguen las especificaciones técnicas.

- **Bridge Enlace de datos**
  - Se usan para interconectar dos o más subredes LAN separadas. Envía tramas de una subred LAN a otra. Algunos toman conocimiento de la dirección de las estaciones que se pueden alcanzar en cada subred de enlace de datos que ellos unen, de modo que pueden enviarse
  - Este opera en la subcapa de Control de Acceso al Medio de la capa de Enlace de Datos y es transparente al software que opera en las capas por encima de la subcapa de Control de Acceso al Medio
- **Router Red**
  - Es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar
  - Generalmente, se encuentra entre las puertas de enlace en el que se conecta a dos redes o más.
  - Usando encabezados y tablas de reenvío, el router determina la mejor ruta para reenviar los paquetes.

## IPv4

- Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.
- El sistema de direccionamiento IP consiste de números binarios de 32 bits. Están separados en 4 octetos (bytes) y se pueden representar también en forma decimal separados por puntos cada byte.
- Las direcciones IP están construidas de dos partes:
  - ID network: el identificador de red
  - ID host: el identificador del dispositivo.
- Tipos de direcciones:
  - Dirección de red: la dirección en la que se hace referencia a la red.
  - Dirección de broadcast: una dirección especial utilizada para enviar datos a todos los hosts de la red.
  - Direcciones host: las direcciones asignadas a los dispositivos finales de la red.
  - Gateway
    - Puerta de enlace es un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior.
- Direccionamiento con clase
  - No envían información de la subred en las actualizaciones de enrutamiento.
  - Primeros protocolos como RIP son con clase.
  - Las rutas se intercambian entre las redes y se suman a los límites de la clase.
- Direccionamiento sin clase
  - Incluyen la máscara de la subred con la dirección de la misma en las actualizaciones de enrutamiento.
  - Actualmente la mayoría de los protocolos lo requieren.
  - Admiten redes no contiguas.VLSM (Variable Length Subnet Masking)

- Tipos de direcciones
  - **Direcciones públicas:** Las direcciones IPv4 públicas constituyen el espacio de direcciones de Internet. El principal propósito de este espacio de direcciones es permitir la comunicación usando el IPv4 sobre Internet.
  - **Direcciones privadas:** Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet
- Direcciones pruvadas
  - Clase A 10.0.0.0 a la 10.255.255.255
    - 16,777,214 (224-2) direcciones IP para los hosts, pero está limitada a sólo 127 redes de clase A. Es utilizada para grandes corporaciones internacionales (e.g. carriers como AT&T, IBM, GM,...)
  - Clase B 172.16.0.0 a la 172.31.255.255
    - 16,384 redes supliendo todas ellas un total de 65,534 (216-2) direcciones IP para los hosts. La clase B es utilizada por grandes compañías que necesitan un gran número de nodos (e.g. universidades, GM, FORD, ..)
  - Clase C 192.168.0.0 a la 192.168.255.255
    - 2,097,152 redes con un máximo de 254 (28-2) hosts cada una. La clase C es utilizada por pequeñas redes
  - Clase D multicasting
  - Clase E investigación y desarrollo
- Asignación estática
- Asignación dinámica
  - Para utilizar esta opción es necesario que en la red exista un servidor DHCP
- CIDR Classless Inter-Domain Routing
  - El prefijo de red de la dirección CIDR indica cuántas direcciones IPv4 hay disponibles para los hosts de su red.
  - Si un host tiene más de una interfaz física, debe asignar una dirección de host para cada interfaz física que se utilice.
  - El prefijo de red de una dirección CIDR también define la longitud de la máscara de subred.
- Subnetting
  - Subdivisión de una red en varias subredes.
  - El Subneteo permite a los administradores de red, por ejemplo, dividir una red empresarial en varias subredes
  - Dividir un bloque de direcciones IP en subredes
  - Separa los dominios de broadcast
  - Extiende el número de bits asignados al ID de red en la máscara de red
- Máscara de red
  - Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, y qué parte es la correspondiente al host.
  - Es un número de 32 bits, separados en 4 grupos de bytes, asociados uno a uno a la dirección IP del host.
  - Es una sucesión continua de unos, seguida por una de ceros.
  - Cada bit en 1, indica que es un bit perteneciente a la dirección de red
  - Para definir las porciones de red y de host de una dirección, los dispositivos usan un patrón separado de 32 bits llamado máscara de subred.
  - Esta máscara se expresa con el mismo formato decimal punteado que la dirección IPv4.

- Ejemplo, para la dirección x.y.z.t /24, la máscara subred es: 255.255.255.0
- La máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host.

### Bloques de longitud variable

El espacio completo de direcciones (232) se divide en bloques de diferentes tamaños.

A cada organización se le asigna un bloque de tamaño adecuado para sus propósitos.

Hay restricciones para el buen funcionamiento de la arquitectura.