Introducción a Networking TCP/IP

Introducción

Para mantener una comunicación efectiva y conectarse con locaciones remotas, las organizaciones necesitan configurar y administrar redes de computadoras. Con Windows 2000 encontrará un conjunto de servicios de redes basados en protocolos de networking estándar y de tecnologías que ofrecen fiabilidad y una infraestructura de red ínter operable.

Los productos de Windows 2000 cuentan con servicios y herramientas para la instalación, configuración, administración y soporte para hacer más sencilla la infraestructura de su red. Una infraestructura de red cuenta con los siguientes elementos:

Intranet: Se refiere a la red privada dentro de una organización que usualmente cuenta con distribución de información interna. Una Intranet también puede ser llamada LAN. Incluye servicios como la distribución de documentos y software, accesos a bases de datos y entrenamiento. Además de servicios de archivos e impresoras compartidas, una Intranet usualmente utiliza aplicaciones asociadas con Internet como páginas Web, navegadores para Internet, sitios FTP, e-mail, newsgroups y listas de correo a las que sólo las organización tiene acceso.

Accesos Remotos: Provee de trabajo en red remoto para las telecomunicaciones, trabajadores móviles y administradores de sistemas que necesitan monitorear y administrar servidores de múltiples sucursales. Todos los servicios deben estar disponibles para los usuarios conectados en la LAN remota, incluye por supuesto compartir archivos e impresoras, acceso Web y mensajería a través de la conexión remota.

Oficinas Remotas: Parte de una organización se encuentra ubicada geográficamente en un área separada. Una LAN de una oficina remota conectada a una red corporativa forma una WAN. La conexión WAN es una conexión remota compartida a la red que habilita a usuarios en la oficina remota la comunicación y el uso de los recursos compartidos a la organización entera. Los enlaces WAN son persistentes, lo que involucra disponibilidad conectarse cuando se necesita y desconectarse cuando no se requiere.

Internet: La colección de redes mundiales y routers que utiliza la suite de TCP/IP para comunicarse una con otra. Internet comprende líneas para la comunicación de alta velocidad entre la mayoría de los nodos o computadoras, que se clasifican en comerciales, educacionales de gobierno, milicia, etc.

Extranet: Una extranet es una red “colaborativa” que utiliza tecnologías de Internet para facilitarse las relaciones de confianza entre empresas con proveedores clientes u otra relación de negocio. Esta compuesta por un lado de la Intranet o red corporativa y por otro lado las compañías que pueden accederla o también puede ser una red compartida de varias compañías que colaboran entre si. La información compartida debe estar disponible solo para las partes que colaboran y en algunos casos la información puede ser publica.

Para levantar una infraestructura de red adecuada, requiere de los conocimientos y la configuración de los protocolos de red necesarios, ***settings*** y servicios que serán utilizados para cada elemento dentro de la estructura de red.

TCP/IP provee de la conectividad básica para su red, es una industria estándar que comprende un set de protocolos de red y los servicios más importantes. Hoy en día se ha convertido en el protocolo por excelencia para las telecomunicaciones y la ínter conectividad. Existen actualmente diferentes versiones de ésta ***suite*** de protocolos para diferentes sistemas operativos y para diferentes proveedores de hardware, todos por supuesto; orientados a la comunicación y siguiendo los estándares establecidos.

La escalabilidad de TCP/IP se adapta a todos los tamaños de redes. Windows 2000 incluye todas las implementaciones y requerimientos estándar de la IETF para hosts y servidores TCP/IP.

TCP/IP depende de la resolución de nombres para trabajar apropiadamente. La resolución de nombres es un proceso que ofrece a los usuarios una manera sencilla de recordar los nombres de los servidores en vez de utilizar direcciones numéricas para identificarlos dentro de la red.

TCP/IP se ha convertido en el protocolo de red por defecto para Windows 2000 y se instala dentro del proceso del setup.

Antecedentes Históricos

Las redes están compuestas generalmente por un pequeño numero de máquinas localizadas en el mismo edificio, o incluso en una sola planta que están interconectadas para proporcionar un entorno de trabajo homogéneo. Es típico que se quiera compartir archivos entre estos nodos, o ejecutar aplicaciones distribuidas en diferentes máquinas.

Estas tareas requieren una aproximación completamente diferente a las redes. En lugar de reenviar archivos completos con una descripción del trabajo, todos los datos se fragmentan en pequeñas unidades (paquetes), que se envían inmediatamente al nodo destino, donde son reensamblados. Este tipo de redes son llamadas redes de intercambio de paquetes. Entre otras cosas, esto permite ejecutar aplicaciones interactivas a través de la red. El costo de esto supone, por supuesto, una complejidad adicional al software.

La solución que han adoptado los sistemas es conocida como TCP/IP. El TCP/IP tiene sus orígenes en un proyecto de investigación fundado en Estados Unidos por el DARPA (Defense Advanced Research Projects Agency, Agencia de Proyectos Avanzados de Investigación en Defensa) en 1969. Una vez comprobado el éxito, esta red ARPANET fue operativa en 1975.

En 1983, fue adoptado como estándar el nuevo conjunto de protocolos TCP/IP, y todos los nodos de la red empezaron a utilizarlo. Cuando ARPANET por fin dio paso a Internet (con la propia ARPANET integrándose en su existencia en 1990), el uso del TCP/IP se había extendido a redes más allá de la propia Internet. Las más destacables son las redes locales UNIX, pero con la llegada de los equipos telefónicos digitales rápidos, como la RDSI, también tiene un futuro prometedor como transporte en redes telefónicas.

Comprendiendo TCP/IP

Actualmente los sistemas de redes están construidos sobre un concepto de “niveles o capas de servicio” cuando nosotros tratamos de mandar información de un lugar a otro corremos el peligro de perder algunos bits en el trayecto. Definiendo cuales serían los diferentes niveles en este proceso tenemos que:

La primera capa de nuestro sistema lo compone el hardware, es decir, la computadora, tarjeta de red y algunos cables que no son precisamente muy confiables. Después, una capa de software básico que nosotros agregamos y que nos permite aislar los problemas del hardware. Se incorpora otra capa más de software para dar al software básico algunas características deseadas y continuamos agregando funcionalidad e inteligencia a la red, capa por capa, hasta que se obtiene algo amigable y útil.

Bien, con esta sencilla explicación se comenzará la descripción de uno de los protocolos de comunicación mas usado en el mundo por cientos de diferentes empresas que elaboran tanto software como hardware para las telecomunicaciones. La descripción de éste sistema de protocolos inicia con una sencilla analogía desde como funciona y como es el flujo de la información en los diferentes niveles o capas que lo componen. Igualmente, sigue la misma ruta de transmisión.

Un modelo excelente para describir el funcionamiento de TCP/IP es el Servicio Postal. El Servicio Postal es una red de conmutación de paquetes, donde nosotros contamos con una red dedicada a enviar información que se mezcla con los mensajes de otras personas, se ponen en un conducto, se transfieren a otra oficina postal y se clasifica todo nuevamente. Aunque las tecnologías son completamente diferentes, el Servicio Postal es sorprendentemente similar.

Un cable puede llevar información de un lugar a otro, pero cómo lo hace? Las redes son un conjunto de computadoras que están conectadas por todo el mundo por unos dispositivos llamados routers (mejor conocidos como ruteadores o enrutadores) que su función principal es interconectar fragmentos físicos de redes, las cuales pueden ser Ethernets, token rings, etc.

Las líneas telefónicas y las redes Ethernets son el equivalente a los camiones y aviones del Servicio Postal, es decir, el medio a través del cual el correo va de un lugar a otro. Los routers son las sucursales postales; estos equipos deciden cómo dirigir la información " o los paquetes de información", de la misma forma que una oficina postal decide cómo distribuir los sobres por correo.

No todas las oficinas de correos o todos los routers cuentan con una conexión a cada uno de los otros destinos de la red; es decir, si se envía un sobre por correo desde Mérida con destino a Tijuana, el sistema no reserva un avión especial para llevarlo, sino que envía el sobre a una sucursal de correo y ésta a su vez lo envía a otra, y así sucesivamente hasta alcanzar su destino final. Esto significa que cada sub estación sólo necesita conocer las conexiones con las que cuenta y cuál es el mejor "siguiente salto" para acercar el paquete a su destino. El protocolo trabaja de una manera similar: un router se fija en el destino de la información y decide a dónde enviarla. El router elige cuál es el enlace más apropiado para enviar el paquete.

Si se quiere enviar una carta, no basta con poner el papel escrito en el buzón y esperar a que sea entregado. Es necesario poner el papel con la información dentro de un sobre, escribir el domicilio del destinatario y pegar los timbres postales. De esta misma manera que el servicio postal tiene sus reglas que definen la operación de su red, también existen reglas que definen la operación de Internet. Las reglas son los llamados protocolos.

Uno de los más importantes de nuestro esquema es el Protocolo Internet (IP) que se encarga de establecer domicilios o se asegura que los routers sepan qué hacer con la información que les llega; continuando con nuestro ejemplo, el protocolo IP tiene la función del sobre donde enviamos una carta.

Una parte de la información del domicilio va al principio del mensaje; estos datos dan a la red información suficiente para hacer la entrega del paquete. Las direcciones IP, constan de cuatro cifras de números, cada uno de ellos menor que 256 y cuando se escriben, se separan por puntos, como se muestra a continuación: 192.112.36.5. Así como los domicilios están compuestos por varias partes y son únicos en el mundo. El protocolo IP le da a todas las computadoras de la red una dirección que es única en el mundo y que como ya dijimos se divide en cuatro segmentos.

Los primeros números de la dirección IP indica a los ruteadores cuál es la red a la que pertenece el paquete y los últimos números indican qué computadora personal o equipo anfitrión de la red debe recibir la información. Consideremos la siguiente dirección:

Priv. De San Enrique 976
Col. Chapalita 04590
Guadalajara, Jal.

En este caso, la ciudad es como la parte de la dirección IP que permite que el sobre llegue a la oficina postal correcta; el código postal indica el segmento de la red y el domicilio el buzón particular en el área de servicio de la oficina de correos. El sistema concluye su trabajo cuando entrega el paquete en la oficina correcta y ésta la pone en el buzón correcto. De la misma manera, el protocolo de comunicación concluye su trabajo cuando entregó la información en el ruteador correcto y éste a su vez en el equipo correcto localizados en la red.

Por muchas razones prácticas, la información enviada a través de las redes IP se divide en fragmentos de distintos tamaños llamados paquetes. La cantidad de información en un paquete normalmente se encuentra entre 1 y aproximadamente 1500 caracteres de largo. Esto previene que cualquier usuario monopolice la red, permitiendo que todos tengan un acceso equitativo.

Una de las propiedades más impresionantes de Internet es que, en un nivel básico, el protocolo IP es todo lo que se necesita para participar en la red. No será muy amigable, pero sí suficientemente capaz, siempre y cuando la información se ponga en un sobre IP. Con esto, la red tiene toda la información necesaria para llevar el paquete hasta su destino. No obstante, habrá que resolver varios problemas:

La mayoría de las transferencias de información es mayor que 1500 caracteres. El servicio postal no sería realmente funcional, si sólo recibiera tarjetas postales y no paquetes o sobres más grandes.

En ocasiones se pueden presentar errores; así como el Servicio Postal puede perder una carta, algunas veces las redes pierden paquetes o pueden dañarse durante la transmisión. A diferencia de lo que sucede con el servicio del correo, TCP/IP puede resolver estos problemas exitosamente.

Los paquetes de información pueden llegar en desorden. Si se envían dos cartas al mismo lugar en días consecutivos no existe la garantía de que viajarán por la misma ruta o llegarán en el mismo orden. Lo mismo sucede con Internet.

Para evitar esto, la siguiente capa de la red nos permitirá enviar grandes cantidades de información y corregirá todas las alteraciones que puedan ser causadas por la red. El Protocolo de Control de Transmisión (TCP) es el protocolo que se utiliza para resolver los problemas mencionados.

¿Qué pasaría si usted deseara enviar un libro a alguien y el Servicio Postal sólo aceptara cartas? ¿Cómo podría solucionar este problema? Una de las soluciones sería arrancar todas las hojas del libro, ponerlas en un sobre cada una y depositarías en un buzón. La persona que reciba las cartas tendrá que asegurarse de recibirlas todas y volverlas a empastar en el orden original. Esto es lo que hace el protocolo TCP.

TCP toma la información que se desea enviar y la divide en segmentos, además enumera cada uno de ellos para que el receptor pueda verificar la información y ponerla en el orden adecuado.

Para que el protocolo TCP pueda enviar esta secuencia de números a través de la red, cuenta con su propio sobre que le permite "escribir" en él la información requerida para su re-ordenamiento. Un segmento de la información a transmitir se coloca en el sobre del protocolo TCP. Este sobre es puesto, a su vez, dentro del sobre del protocolo IP y posteriormente es transmitido a la red. Una vez que se pone algo en un sobre IP, la red lo puede transmitir.

Del lado del destinatario, una parte del software del TCP reúne los sobres, extrae la información de ellos y la pone en el orden adecuado. Si algún sobre se pierde en la transmisión, el receptor solicita su retransmisión al emisor. Una vez que el protocolo TCP tiene toda la información en el orden adecuado, la pasa a la aplicación del programa que esté utilizando sus servicios.

En realidad los paquetes de información no sólo se pierden en una transmisión, sino que además de esto, pueden ser modificados por el mal funcionamiento de las líneas telefónicas. TCP también resuelve este tipo de problemas. Así como coloca la información en un sobre, el protocolo calcula algo llamado número de verificación (*checksum*). Este número de verificación es un número que permite que el receptor TCP detecte errores en el paquete transmitido. Cuando un paquete llega a su destino, el receptor calcula el número de verificación y lo compara con el enviado por el transmisor. Si no coinciden, significa que ocurrió un error en la transmisión. El receptor deshecha el paquete y solicita la retransmisión.

El protocolo TCP crea la apariencia de que existe una conexión permanente entre dos aplicaciones, garantizando de esta forma que lo que se transmite de un lado llegue al otro.

Ahora bien, en el caso de que sea poca la información que estamos enviando TCP pueda llegar a ser demasiado complicado y no necesario; para estos efectos,

contamos con un protocolo más llamado “Protocolo de Datagramas de Usuario” ó UDP que es utilizado por algunas aplicaciones en lugar del TCP. Lo cual sería, en lugar de tomar la información y ponerla en un sobre TCP para después ponerla en un sobre IP, esta aplicación pone la información en un sobre UDP y después en un sobre IP.

El protocolo UDP es mucho más sencillo porque no se preocupa por que los paquetes se pierdan, ni por que la información llegue en orden o cualquier situación de ese tipo. El UDP se usa comúnmente en programas que envían mensajes cortos y que sólo reenvían la información si no reciben una respuesta en un tiempo determinado.

Ahora que se tiene la habilidad de transferir información entre dos nodos, es posible trabajar en una capa mas que hace que la red sea más amigable. Esto es utilizando el software adecuado para la tarea que se quiera realizar y poniendo nombres con letras en lugar de sólo números para referirse a las computadoras.

La mayor parte de la gente no se emociona cuando tiene o cuenta con un flujo garantizado de bits entre dos máquinas, sin importar lo veloz que éste sea o lo exótico de la tecnología que lo hace posible. Generalmente desean usar ese flujo de bits para hacer algo útil, ya sea mover un archivo, obtener información o divertirse. Las aplicaciones son partes del software que permiten que lo anterior suceda fácilmente. De hecho son otra "capa" del software, que actúa por encima de los servicios de TCP o UDP. Las aplicaciones ofrecen al usuario una forma de realizar la tarea que se requiera.

Las aplicaciones pueden variar desde un programa hecho en casa hasta un programa propietario proporcionado por una compañía de software. Hay tres aplicaciones "básicas" sesión de trabajo remota, transferencia de archivos y correo electrónico (Telnet, Gopher, FTP, SNMP, etc.) así como otras usadas comúnmente, pero que no son estandarizadas.

Como hemos descubierto hasta ahora, TCP/IP no es otra cosa mas que una suite de diferentes protocolos de comunicación que se divide en diferentes capas y que igualmente incluye aplicaciones.

Sección 1: Definición y Arquitectura de TCP/IP

Sección 1: Definición y Arquitectura de TCP/IP

Introducción

Esta sección presenta en detalle los conceptos y definiciones de los protocolos de TCP/IP, así como sus antecedentes históricos y documentos que lo regulan.

Objetivos Particulares

Al finalizar esta sección, Usted podrá:

- Comprender y describir la función de TCP/IP
- Identificar y describir las capas del Modelo DoD
- Comparar el modelo de TCP/IP con el modelo OSI
- Identificar y describir los principales protocolos y aplicaciones con TCP/IP y sus grupos
- Terminología de paquetes

Qué es TCP/IP?

Últimamente hemos escuchado demasiado de TCP/IP y no es extraño, si es el protocolo asignado para la integración de redes de tipo WAN y por consiguiente de Internet.

Si queremos definir TCP/IP, podemos decir que es un conjunto de protocolos de red que proporcionan comunicaciones a través de redes interconectadas de computadoras con diversas arquitecturas hardware y variados sistemas operativos. Por ser un sistema abierto, TCP/IP incluye estándares de cómo se han de comunicar las computadoras y reglas para conectar redes y encaminar el tráfico. Las siglas significan: Protocolo de Control de Transmisiones/Protocolo Internet y se deben a los dos protocolos más importantes los cuales quedaron definidos en 1982.

Cuando se inició este experimento a finales de la década los 60's, fue conducido por el Departamento de Defensa de los Estados Unidos de Norteamérica y por muy pocas universidades; el origen de su investigación fue de fines bélicos principalmente por la llamada "Guerra Fría" y fue la Agencia de Recursos de Proyectos Avanzados del DoD, (DARPA), quien llevó la batuta en el proyecto. El experimento fue un éxito y surgió de él, una pila de protocolos relacionados entre sí con un solo objetivo: Conectividad entre diferentes tipos de computadoras. Rápidamente se convirtió en el estándar para redes de tipo UNIX y se extendió por todo el mundo su uso. Hoy en día, se puede encontrar en versiones comerciales y públicas de TCP/IP para todo tipo de procesador. A continuación, tenemos una lista de fechas significativas del proceso:

En 1970, los host de ARPANET empezaron a usar el Protocolo de Control de Redes (NCT).

En 1972 se dieron a conocer las primeras especificaciones de Telnet.

En 1973, se introdujo el Protocolo de Transferencia de Archivos FTP.

En 1974, TCP se dio a la luz como el Programa de Control de Transmisiones.

En 1981, se publico por primera vez el estándar del Protocolo de Internet IP.

En 1982, la Agencia de comunicaciones de la Defensa DCA y la ARPA, establecieron el Protocolo de Control de Transmisiones TCP y el Protocolo de Internet IP; como la suite de protocolos TCP/IP.

En 1983, la ARPANET emigro de NTC a TCP/IP y se convirtió en el protocolo estándar de los organismos militares para el trabajo en redes y de inter-redes.

En 1984, el Sistema de Nombres de Dominio DNS, fue introducido.

Son varias las asociaciones y organismos que intervienen en la regulación de TCP/IP, entre ellas podemos identificar a la ISOC**,** *Internet Society* como la más importante; ya que son los responsables de aprobar las tecnologías que aplican a su desarrollo. A su vez, esta es integrada por:

IAB, Internet Arqchitecture Board; le corresponde la aprobación de los RFC's

IANA, Internet Assigned Number Authority

IRFT, Internet Research Task Force

IETF, Internet Eingeener Task Force

RFC´s, Request for Comments

Son los documentos oficiales del IETF, que definen los estándares de TCP/IP. Su propósito es proporcionar un medio a un grupo diverso de usuarios de Internet para comunicarse y conciliarse dentro de la arquitectura y funcionalidad de Internet.

Hay mucho tipos de RFC's pero todos tienen la misma intención y algún aspecto similar en su formato, algunos son proyectos que ambicionan llegar a ser estándares, otros tienen naturaleza de tutorial o los hay bastante técnicos; pero todos los RFC son de hecho, el medio para que Internet pueda ser organizada y permitir a sus usuarios comunicarse. En general, se clasifican en cinco categorías; Requeridos, Recomendados, Electivos, Uso limitado y No recomendados.

Si alguno de estos documentos se puede considerar como un estándar, entonces sigue un proceso de desarrollo, prueba y aceptación, que igualmente contamos con tres niveles de maduración: Propuesta de Estándar, Borrador Estándar e Internet Estándar.

Cuando un RFC's es aprobado y publicado se le asigna un número, un documento nunca es actualizado, más bien es publicado en un nuevo RFC y se le asigna un número nuevo. Encontramos una lista que hace referencia a los documentos que parece son los más importantes, todos ellos se pueden consultar por Internet y están al alcance de cualquier usuario que desee profundizar en la investigación.

RFC 791	Protocolo Internet (IP)
RFC 792	Protocolo de mensajes de control de Internet (ICMP)
RFC 793	Protocolo de control de transmisiones (TCP)
RFC 768	Protocolo de datagrama de usuario (UDP)
RFC *854*	Protocolo de Telnet
RFC 959	Protocolo de transferencia de archivos (FTP)
RFC 821	Protocolo simple de transferencia de correo (SMTP)
RFC 822	Estándar para el formato de los mensajes de texto ARPA de Internet
RFC 1117	Números asignados
RFC 991	Protocolo oficial de ARPA en Internet
RFC 1034	DNS - conceptos y facilidades
RFC 1035	DNS - implementación y especificaciones

Una vez aclarado, vamos a describir a continuación cada una de las capas de TCP/IP y de que protocolos se componen.

TCP/IP esta dividido en cuatro capas que definen el llamado Modelo DOD, cada una de éstas, se encarga de realizar una función o tarea especifica dentro de una red y también puede incluir diferentes protocolos. *Figura no. 1.*

Capas del Protocolo

Vamos a presentar una breve descripción de las capas y cómo es la comunicación entre ellas cuando se entrega o se recibe un paquete.

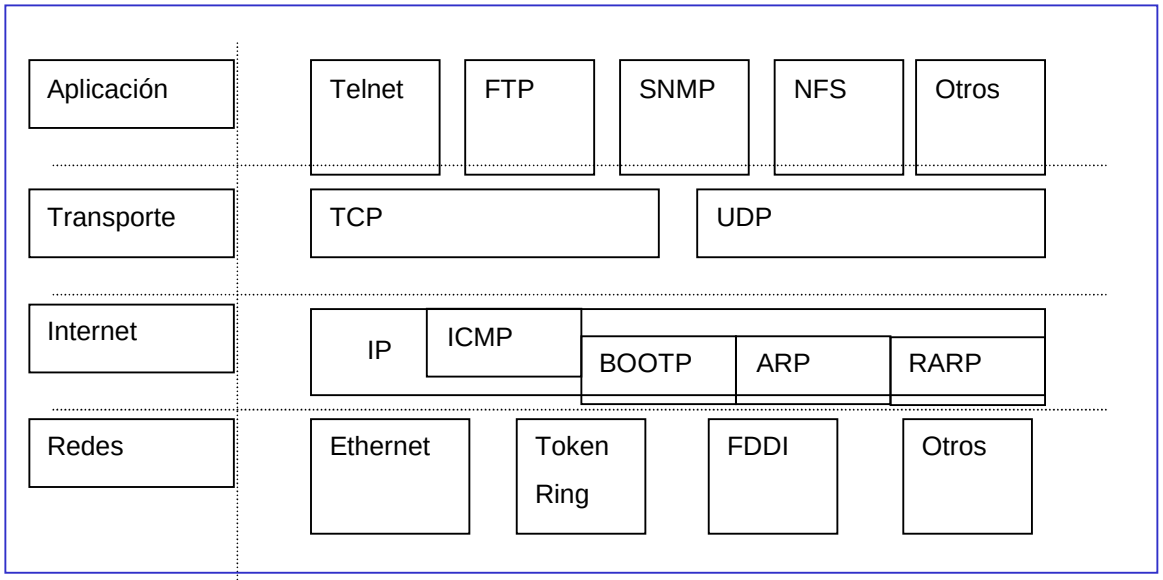


Figura no. 1. Descripción del modelo DOD y su referencia con TCP/IP

Capa Interfaz de Redes

Es la base del modelo y el nivel mas bajo. Esta capa es responsable de poner los frames dentro de los cables y fuera de ellos; es decir, es responsable de la transmisión de los datagramas sobre la capa física de la red y hasta el destino.

Cuando llega el paquete a esta capa, se agrega un CRC y un *preamble*; al recibirse en el host destino se descarga el *preamble* y se calcula el CRC si esta correcto la dirección MAC es examinada.

- ***CRC***: Cyclic Redundancy check, cálculo matemático que se añade para verificar que no ha sido corrupto el paquete.
- ***Preamble***: Secuencia de bits que identifican el inicio del paquete.
- ***MTU, Unidad Máxima de Transferencia***: Cada tipo de medio físico tiene un tamaño máximo de trama que no se puede superar, el nivel de redes o el nivel de enlace (modelo OSI) es el responsable de obtener esta unidad y de informar a los protocolos situados por encima.

  Cuando se establece una conexión, los dos hosts involucrados intercambian sus valores MSS (tamaño de segmento máximo), y que para la conexión se utiliza el valor más pequeño de los dos MSS, el cálculo es él siguientes: MTU menos 40 bytes para los encabezados de IP y TCP.

Capa de Internet

Es el segundo nivel y es el responsable proveer la comunicación hots-to-host. Aquí es donde el paquete es encapsulado en un datagrama de Internet, los algoritmos de ruteo son cargados (ya sea estático o dinámico) y el datagrama es enviado a la capa de Redes para su transmisión. Los protocolos mas importantes son:

- ***ARP***: que es usado para obtener la dirección física de los *hosts* localizados en la misma red física.
- ***ICMP***: envía mensajes y reportes de error de los paquetes.
- ***IP***: es el principal responsable de la dirección y ruteo de los paquetes entre *hosts* y redes. IP para enviar un paquete le agrega su propio encabezado con las direcciones IP del host origen y del host destino, el protocolo que lo entrega, checksum y el TTL. Si el host esta en el mismo segmento de red lo envía directamente si no es el caso, el paquete es enviado al router.

Capa de Transporte

Provee la comunicación entre computadoras, El método deseado para la entrega de paquetes lo define el protocolo, de los cuales tenemos:

- ***TCP*** que es orientado a conexión, establece comunicación para aplicaciones de transferencia larga y que requiere un mensaje de conocimiento de la información enviada.
- ***UDP*** no es orientado a la comunicación por lo que no garantiza que los paquetes hayan sido entregados. Las aplicaciones que utilizan UDP son pequeñas y es su responsabilidad la entrega de los paquetes.

Son cuatro las características que hay que considerar cuando se habla de un protocolo orientado a conexión:

1. El camino para los paquetes se establece por adelantado
2. Los recursos necesarios para la conexión se establecen por adelantado.
3. Se asegura la reserva de los recursos durante toda la conexión
4. Cuando la transferencia de datos se ha completado, la conexión finaliza y se liberan los recursos.

Capa de Aplicaciones

Es la capa más alta, es donde las aplicaciones inician la cadena hacia el acceso por la red. Esta capa es la interfase con el usuario, contiene aplicaciones especificas. Entre las cuales tenemos: FTP, Telnet y SNMP, lo que son transferencias de Archivos y correos electrónicos, entre otras y varían de acuerdo al sistema operativo con el que estamos trabajando. Estas aplicaciones usualmente incluyen un cliente y un programa de servidores. A este programa se le refiere como daemon, que en la mitología griega significa “espíritu guardián”

La importancia de los números de puerto

Cada máquina en una red IP tiene al menos una dirección IP. Además, cada máquina tiene muchos procesos individuales en ejecución. Cada proceso puede llegar a ser un cliente de red, un servidor de red, o ambos. Obviamente, si el destino de un paquete se identifica sólo con la dirección IP, el sistema operativo no tiene forma de saber a qué proceso se envían los contenidos del paquete. Para resolver este problema, TCP/IP añade un componente identificado como puerto TCP o UDP. Cada conexión de una máquina a otra tiene un puerto de origen y un puerto destino. Cada puerto se etiqueta con un número entero del 0 al 65,535.

A fin de identificar cada conexión única posible entre dos máquinas, el sistema operativo tiene cuatro fuentes de información: la dirección IP origen, la dirección IP destino, el número e puerto origen y el número de puerto destino. La combinación de estos cuatro valores se garantiza que es única para todas las conexiones entre máquinas.

Una máquina inicia una conexión especificando la dirección IP y el número de puerto destino. Obviamente, la dirección IP origen ya se conoce. Pero el número de puerto origen, el valor que hará que la conexión sea única, se la asigna el sistema operativo origen. Por convención, el número es mayor a 1024 (los números de puerto del 0 al 1023 se reservan para usos del sistema). Técnicamente, la máquina origen también puede seleccionar su número de puerto origen. Sin embargo, para hacer esto ningún otro proceso puede ocupar ese puerto. Generalmente, muchas aplicaciones dejan que el sistema operativo gestione el número de puerto origen por ellas.

Conociendo esta disposición, podemos ver cómo la máquina origen A puede abrir varias conexiones para un solo servicio hacia la máquina destino B. La dirección IP y el número de puerto B siempre es constante, pero el número de puerto A será diferente en cada conexión. La combinación de IP y números de puerto origen y destino (4 datos) es única, y ambos sistemas pueden tener muchos flujos de datos (conexiones) entre ellas.

Para que un servidor ofrezca servicios, debe ejecutar programas que escuchen en un número de puerto específico. Muchos de esos números de puertos se llaman servicios bien conocidos, porque el número de puerto asociado con el servicio es un estándar aprobado. Por ejemplo, el puerto 80 es un puerto de servicio bien conocido para el protocolo http.

Más sobre Puertos

Los puertos se pueden ver como puntos de anclaje para conexiones de red. Si una aplicación quiere ofrecer un cierto servicio, se engancha a un puerto y espera a los clientes (a esto también se le llama escuchar en un puerto). Un cliente que quiera usar este servicio consigue un puerto libre en su nodo local, y se conecta al puerto del servidor en el nodo remoto.

Una propiedad importante de los puertos es que una vez que se ha establecido una conexión entre el cliente y el servidor, otra copia del servidor puede engancharse al puerto servidor y esperar a mas clientes. Esto permite, por ejemplo, varios accesos remotos simultáneos al mismo nodo, usando todos ellos el mismo puerto 513. TCP es

capaz de distinguir unas conexiones de otras, ya que todas ellas provienen de diferentes puertos o nodos. Por ejemplo, si accede dos veces a la Computadora A desde la Computadora B, entonces el primer cliente rlogin usará el puerto local 1023, y el segundo usara el puerto número 1022; sin embargo, ambos se conectarán al mismo puerto 513 de Computadora A.

Este ejemplo muestra el uso de puertos como puntos de encuentro, donde un cliente contacta con un puerto especifico para obtener un servicio especifico. Para que un cliente sepa el número de puerto adecuado, se ha tenido que llegar a un acuerdo entre los administradores de los dos sistemas para asignar estos números. Para servicios ampliamente usados, como rlogin, estos números tienen que administrarse centralmente. Esto lo realiza el IETF (o Internet Engineering Task Force), que regularmente publica un RFC denominado Assigned Numbers (Números Asignados). Describe, entre otras cosas, los números de puerto asignados a servicios reconocidos.

Nota: Vale la pena indicar que aunque las conexiones TCP y UDP se basan en puertos, estos números no entran en conflicto. Esto significa que el puerto TCP 513, por ejemplo, es diferente del puerto UDP 513. De hecho, estos puertos sirven como puntos de acceso para dos servicios diferentes, como rlogin (TCP) y rwho (UDP).

La Librería de Sockets

En sistemas operativos como UNIX, el software que realiza todas las tareas y protocolos descritos anteriormente es generalmente parte del kernel, y por tanto también del de Linux. La interfaz de programación más común en el mundo UNIX es la Librería de Socket de Berkeley, *Berkeley Socket Library*. Su nombre proviene de una analogía popular que ve los puertos como enchufes, y conectarse a un puerto como enchufarse. Proporciona la llamada bind(2) para especificar un nodo remoto, un protocolo de transporte, y un servicio al que un programa pueda conectarse o escuchar (usando connect(2), listen(2), y accept(2)). La librería de sockets, sin embargo, es algo mas general, ya que proporciona no solo una clase de sockets basados en TCP/IP (los sockets AF_INET), sino también una clase que maneja conexiones locales a la máquina (la clase AF_UNIX). Algunas implementaciones pueden manejar también otras clases, como el protocolo XNS ((Xerox Networking System), o X.25.

El modelo OSI

Los sistemas abiertos son sistemas diseñados para incorporar a cualquier dispositivo independientemente de su origen y aceptar también de otros fabricantes, para esto se generan los llamados estándares.

Los estándares se catalogan de dos maneras: estándares de facto y estándares de jure. Los estándares de jure los respalda un organismo como la ISO, ANSI, IEEE, etc. y como ejemplo tenemos: el código ASCII, POSIX, y el modelo OSI. Los estándares *de facto* existen porque cubren los huecos dejados por las especificaciones de los estándares *de jure*.

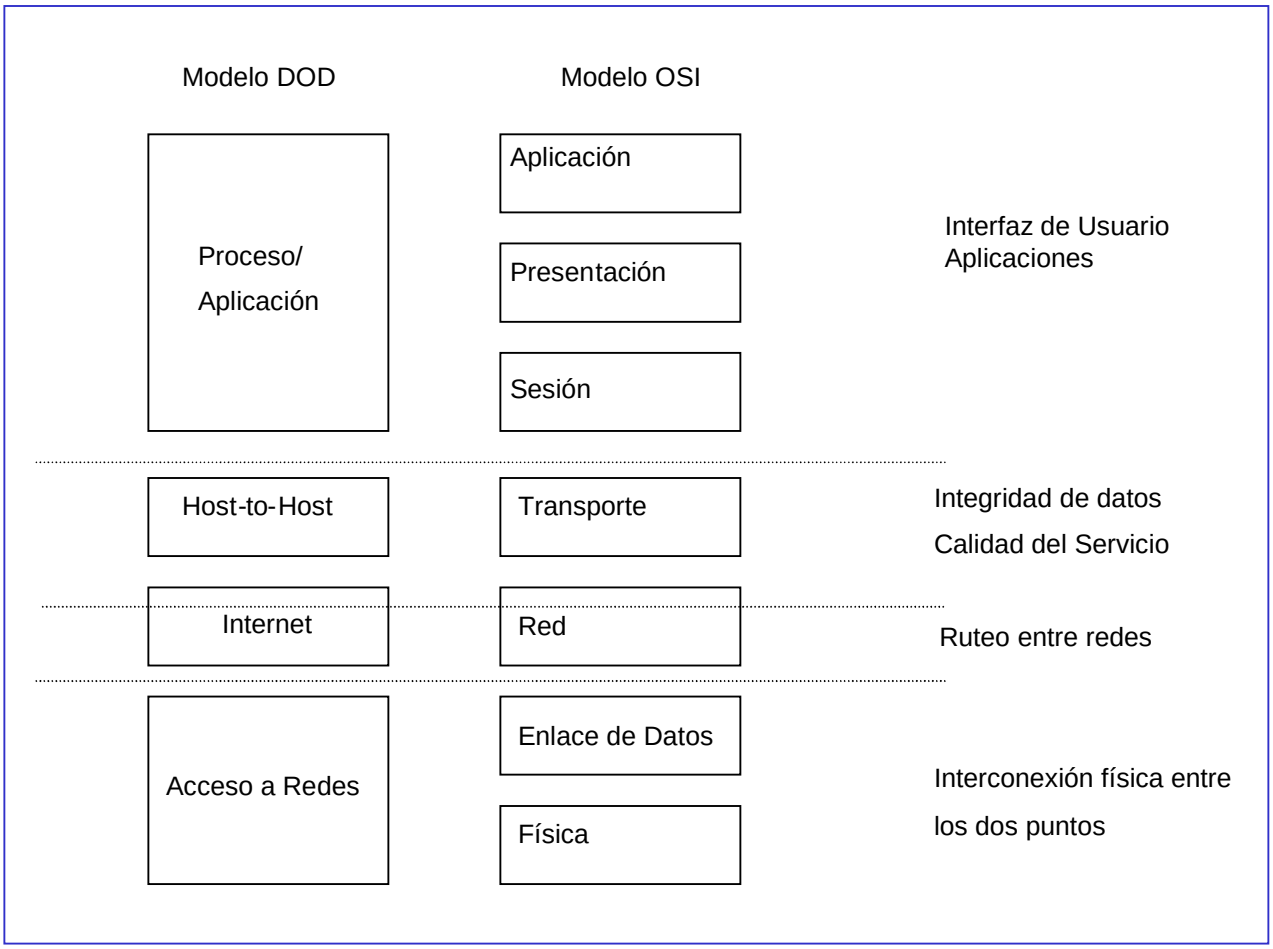


Figura no. 2. Cuadro comparativo entre el Modelo DOD y el Modelo OSI

En 1978 fue introducido por la organización Internacional de Estándares (ISO), sus siglas OSI indican: Open System Interconnect. Se puede ver como un modelo funcional divido en módulos que contiene las reglas que se requieren para el intercambio de información entre redes y permite la solución para múltiples proveedores. Realmente no es mas que un concepto que describe como la comunicación de datos debería tener lugar y lo dividen en siete capas. Las cuales están descritas en la siguiente tabla.

El concepto básico de la responsabilidad de cada capa es que individualmente agregan valor a los servicios proporcionados por los conjuntos de capas inferiores. De esta manera para el nivel mas alto se ofrecerá el conjunto completo de los servicios para correr una aplicación de datos distribuida.

Cada capa es esencialmente independientemente de cada una de las otras capas. Por lo tanto, muchas de las funciones realizadas en las capas inferiores se removieron completamente de las tareas de software para reemplazarlas con hardware. La desventaja principal de la arquitectura de siete capas es la tremenda cantidad de sobrecarga requerida al agregar encabezados a la información que transmite.

Terminología TCP/IP y Protocolos

Antes de intentar entender como se establecen las bases del direccionamiento IP y las clases de redes vamos a dar un recorrido entre los protocolos más importantes en cada una de las capas además de familiarizarnos con la terminología de paquetes.

Llamamos paquete a la unidad de transmisión de tamaño máximo fijo que consta de información binaria que representa datos y una cabecera que contiene un número ID, direcciones origen y destino y datos de control de errores.

Un paquete de datos se mueve de una capa a otra dentro del stack de TCP/IP, cada protocolo agrega al paquete su propia información. El paquete con la información que se le va agregando recibe diferentes nombres técnicos como identificación a los protocolos. Estos nombres son:

- ***Segmento***: un segmento es la unidad de transmisión en TCP. Este contiene un encabezado y datos aplicación.
- ***Mensaje***: un mensaje es una unidad de transmisión de protocolos no-fiables como: ICMP, UDP, IGMP. Este contiene un encabezado del protocolo y datos aplicación o datos-protocolo.
- ***Datagrama***: es la unidad de transmisión IP. Contiene un encabezado IP acompañado de datos de la capa de transporte y también se considera como no fiable.
- ***Frame***: un frame es una unidad de transmisión en la capa de interfaz de redes y consiste de un encabezado agregado por la capa de interfaces de red acompañado de datos capa IP.

El propósito de toda la información que contienen estos encabezados es ayudar a la red a que dirija los paquetes desde la máquina origen a la máquina destino. Una vez de que llega a la máquina destino, permite a la máquina decidir si quiere aceptarlo. El encabezado IP especifica qué máquina debería recibirlo y el encabezado TCP especifica qué aplicación de la máquina destino tomará los datos.

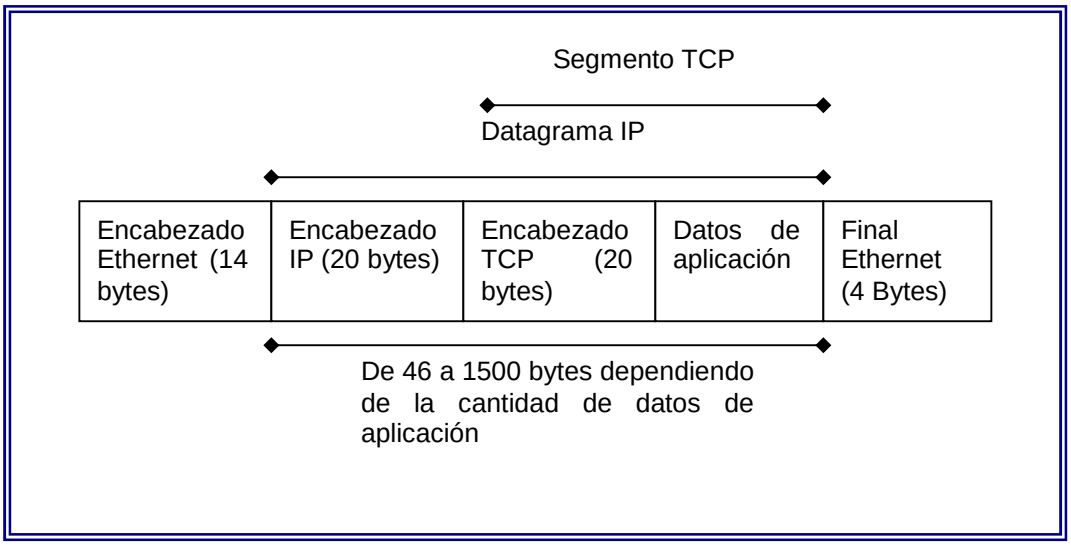


Figura no. 3. Un frame Ethernet con los encabezados de todos los componentes de un paquete TCP

Revisando los encabezados IP y TCP, vemos los campos que podemos usar para decidir si queremos aceptar un paquete. Los campos más interesantes son: Direcciones IP origen /destino y números de puertos origen / destino.

Los números de origen y destino son obvios (dónde va el paquete y de dónde viene). Comprobar contra qué números de puerto origen y destino se conecta nos permite elegir que servicios queremos permitir.

Notas: Como el nombre de UDP (Protocolo de datagramas de usuarios) sugiere igual que se le refiera como datagrama. No hay que confundir aunque de cualquier manera, es aceptable el término para un mensaje de UDP. El término de segmento es aplicable cuando un dispositivo físico es utilizado para dividir una red. En el contexto de paquetes, el término de segmento hace referencia generalmente a un segmento TCP.

Componentes del Frame

Un frame que es el término para un paquete de datos en la capa de Interfaz de redes contiene tres componentes principales: el encabezado, datos y *trailer*.

- ***Encabezado***: incluye una señal de alerta para indicar que el paquete es transmitido, la dirección fuente y la dirección destino.
- ***Datos***: esta es la información actual enviada por la aplicación. Este componente varía en tamaño dependiendo de los límites configurados por la red. La sección de datos en la mayoría de las redes varia desde los .5 Kb hasta 4 Kb. En redes Ethernet el tamaño de los datos es aprox. 1.5 Kb.
- ***Trailer***: El contenido exacto varía dependiendo de la capa de interfaz de redes. Contiene un CRC (*cyclical redundancy check*) que es un número que se produce de un cálculo matemático en la fuente. Cuando el paquete llega al destino, el cálculo se hace de nuevo, si el resultado es el mismo indica que el paquete se ha mantenido estable.

ARP, Address Resolution Protocol

Para que los host de una red se puedan comunicar, es necesario que entre ellos se conozcan sus direcciones físicas, la resolución de direcciones es el proceso del mapeo entre las IP de los hosts y sus direcciones físicas.

ARP, es el responsable de esta función y lo hace a través del envió de broadcast a los hosts si están en una red local o al ruteador si es remoto. Una vez que se obtiene un mapeo se guarda una entrada en su caché, así, cada vez que requiere de una dirección primero checa si no la ha resuelto ya.

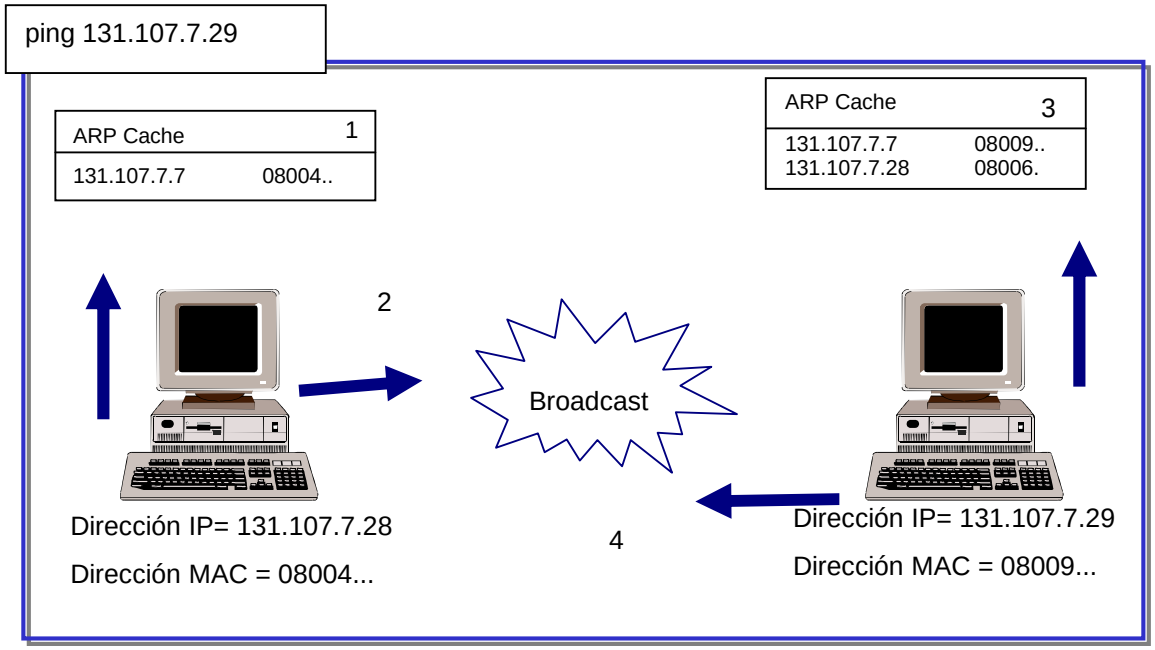


Figura no. 5. Proceso de resolución de direcciones en una red remota

El proceso ARP, incluye dos fases un ARP *request* y un ARP *replay*, y va como sigue:

1. Una petición ARP es iniciada cada vez que un host intente conectarse a otro host. Primero IP determina si esta en su mismo segmento de red para que el host cheque su caché y busque la dirección física del host.
2. Si no cuenta con el mapeo, ARP construye un mensaje solicitando “Quien es esta IP y cual es su dirección física”. Es enviado como una señal de tipo broadcast y es para todos los hosts de la red
3. Todos los hosts escuchan el mensaje y revisan si no es su dirección, en caso de no ser para ellos, ignoran la solicitud.
4. Cuando el host destino reconoce su IP entonces envía un *replay* (respuesta) directamente al host origen con su dirección MAC. Por supuesto, actualiza su

caché con la información del host y al enviar su respuesta se establece la comunicación.

Si el host destino se encuentra en otra red, el proceso varía un poco porque el mensaje broadcast va dirigido al ruteador, él a su vez, envía un datagrama al host destino.

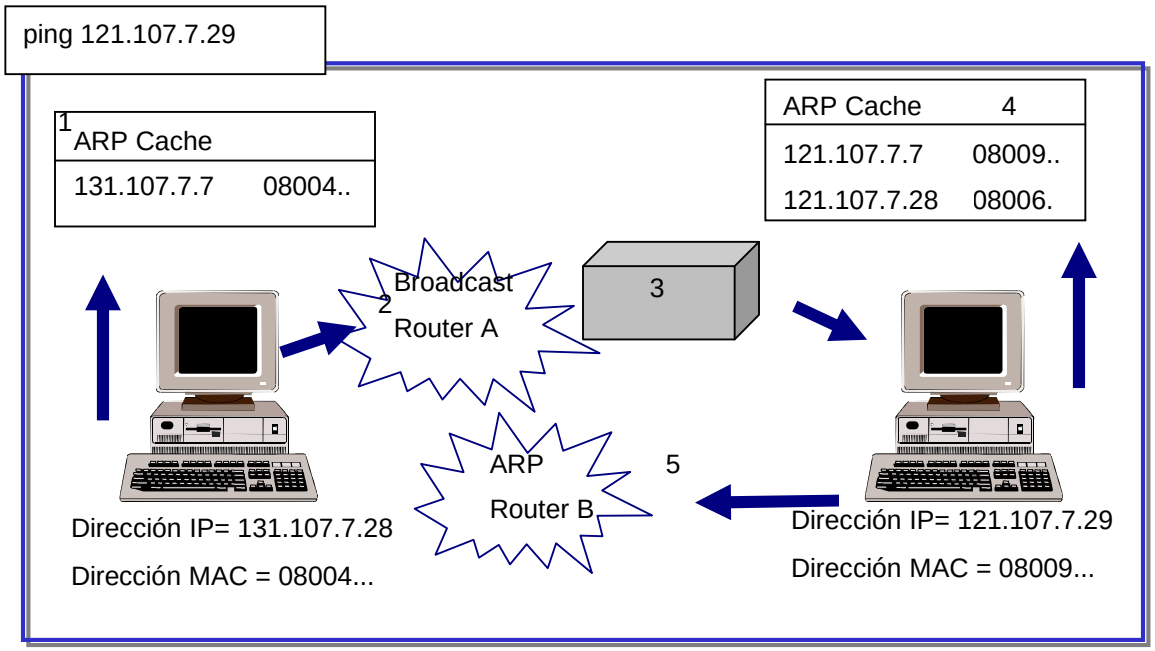


Figura no. 5. Proceso de resolución de direcciones en una red remota

Cuando el host destino esta en una red remota el proceso es diferente; el broadcast que envía ARP es dirigido al router y este envía un datagrama directo al host, veamos:

1. Se inicia el proceso, primero checa el host su caché pare verificar si cuenta con el mapeo del host o de la red. Si no lo tiene, entonces revisa su caché para localizar el mapeo que corresponde al ruteador.
2. En caso de no contar con él, envía un broadcast solicitando la IP del router, mismo que le responde con su dirección IP y Física, una vez recibido el mensaje por el host inicio, éste le libera el paquete con el mensaje para el host destino y el router lo retransmite de nuevo a la computadora remota.
3. En el router, IP es el que determina si la dirección IP es remota o local, por supuesto el router utiliza ARP (Caché o Broadcast) para obtener la dirección física del próximo destino. En el caso de una red remota, checa su tabla de ruteo para obtener la dirección del Gateway.

4. Después de que el destino recibe el paquete, este formula una respuesta eco ICMP. Como el host es remoto, verifica su tabla local de ruteo para identificar la IP del router, cuando es encontrada ARP se encarga de resolver a la dirección IP.
5. En cuanto es resuelta la dirección física, la respuesta ICMP es enviada al gateway y este la envía al host inicio.

La Caché ARP

La caché ARP mantiene entradas estáticas y dinámicas, las dinámicas se crean y se borran automáticamente cuando estamos resolviendo a direcciones IP y tienen un tiempo de vida de 10 minutos.

Las entradas estáticas se ingresan manualmente y se conservan hasta que la máquina es re-iniciada, o cuando se borran manualmente y cuando ARP recibe una dirección diferente, entonces se convierte en dinámica y reemplaza la anterior.

Nota: Cuando ingresamos entradas estáticas en la caché ARP, las direcciones IP hay que ingresarla con los guiones.

Adicionalmente, tenemos una entrada permanente que no se despliega cuando queremos ver los mapeos existentes en la caché, nos referimos a la dirección física para la red local.

Estructura de los paquetes ARP

Dentro de este proceso de resolución se generan dos tipos de paquetes, uno de petición (query) y uno más de respuesta, el primero es un paquete de difusión. La estructura de los paquetes ARP cuenta con los siguientes campos:

Campo	Función
Hardware Type	El tipo de tarjeta del host destino
Protocol Type	El tipo de protocolo que fue designado para el proceso de resolución
Hardware Address Length	Longitud en bytes de la dirección física
Protocol Address Length	Longitud en bytes de la dirección de protocolo
Operation (Opcode)	La operación performada
Sender´s Hardware Address	Dirección MAC del que envía
Sender´s Protocol Address	Dirección IP del que envía
Target´s Hardware Address	Dirección MAC del que destino
Target´s Protocol Address	Dirección IP del que recibe

ICMP, Internet Control Message Protocol

El protocolo de mensajes de control de Internet es un protocolo de mantenimiento especificado en el RCF 792. Los mensajes ICMP se encapsulan dentro de los datagramas de IP para que puedan encaminarse entre varias redes interconectadas. Se utiliza para:

- Construir y mantener tablas de ruteo
- A descubrir la Unidad de Transferencia (PMTU); se basa en los mensajes del destino no alcanzables RFC 1,191.
- Diagnosticar problemas (Ping y Tracert)
- Ajustar el control de flujo para prevenir la saturación de enlace de encaminadores

Estructura del paquete ICMP

Todos los paquetes ICMP tienen la misma estructura y los siguientes campos:

Campo	Función
Type	Indica el tipo de paquete que es, echo request o echo replay
Code	8 bit que Indica una de las múltiples funciones
Checksum	Número de 16 bit
Type-sepecific Data	Datos adicionales que varían para cada tipo diferente

Nota: ICMP es definido en el RFC´s 792.

IP, Internet Protocol

Es el protocolo primeramente responsable del direccionamiento y ruteo de los paquetes entre los hosts. Protocolo de mensajería proporciona un sistema de envío de mínimo esfuerzo.

No esta orientado a la conexión, lo que quiere decir es que no establece una sesión antes del intercambio de datos. No garantiza la entrega de paquetes, Siempre hace su mejor esfuerzo pero por el camino puede ser extraviado, fuera de secuencia o duplicado.

Si IP identifica la dirección destino en una red local, transmite el paquete directamente al host. Si lo identifica en una red remota, entonces IP checa la tabla de ruteo para enviarlo al router que corresponde el *host* remoto.

Nota: Encontramos la definición de IP en el RFC 791.

Estructura del paquete IP

Campo	Función
Version	4 bits son usados para indicar la versión de IP
Header Length	4 bits para indicar él numero de 32 bits en el encabezado IP
Type of service	8 bits que son usados para indicar la calidad deseada del servicio por este datagrama en la entrega a través de los routers en la red
Total Length	13 bits usados para indicar el total de la longitud del datagrama
Identification	16 bits son usados como identificador para este específico paquete. Si el paquete es fragmentado, todos los fragmentos tienen el mismo numero de identificador
Fragmentation Flags	3 bits para las banderas del proceso o de fragmentación
Fragmentation Offset	13 bits para un contador que indica la posición del fragmento
TTL	8 bits para indicar el TTL o brincos antes de ser descargado
Protocol	8 bits para identificar el protocolo IP del cliente
Header Checksum	16 bits usados como checksum
Source Address	32 bits para almacenar la IP del host origen
Destination Address	32 bits para la dirección destino
Options and Padding	Un múltiple de 31 bits usado para almacenar las opciones de IP

TCP, Transmission Control Protocol

Es un protocolo de Internet orientado a conexión responsable de fragmentar los datos en paquetes que el protocolo IP envía a la red. Este protocolo proporciona un flujo de comunicación fiable y secuenciado para la comunicación de red.

El protocolo de control de Transmisión suministra a los programas un servicio orientado a conexión, fiable y de flujos de bytes. Los servicios de red se basan en el transporte TCP para iniciar la sesión, compartir archivos e impresión, duplicar la información entre controladores de dominio, transferencia de listas de examinadores y otras funciones comunes. Sólo puede utilizarse TCP para comunicaciones de uno a uno. TCP utiliza una suma de comprobación en ambas cabeceras y en los datos de cada segmento para reducir las probabilidades de corrupción que no se detecte en los datos.

Un mensaje de ACK (*acknowledgment*) es usado para verificar que los datos hayan sido recibidos por los otros hosts. Por cada segmento enviado, el host que recibe debe enviar un ACK.

Cuando no se recibe el mensaje de ACK, la información es retransmitida, igualmente, cuando un segmento es dañado se vuelve a enviar.

TCP Ports: Los ports de TCP proveen un especifico punto para entregar mensajes. Son alrededor de 256 port los que estas definidos como uso común. A continuación unos cuantos para referencia: FTP, 21; Telnet, 23; DNS, 53; NetBios, 139. TCP este definido en el RFC 793.

Estructura del paquete de TCP

Todos los paquetes de TCP tienen dos partes, una de datos y otra el encabezado. Los campos que contiene el encabezado son los siguientes:

Campo	Función
Source Port	Port del host que envía 16 bits
Destination Port	Port del host destino. 16 bits
Sequence Number	La secuencia en bits transmitidos por segmento. El número de secuencia es usado para verificar que todos los bytes fueron recibidos 32 bits
Acknowledgment Number	El número de secuencia de los bytes que host local espera recibir. 32 bits
Data Length	Longitud del encabezado 4 bits
Reserved	Reservado para uso futuro 6 bits
Flags	Este campo especifica el contenido del segmento
Windows	Que espacio esta disponible en la ventana TCP
Checksum	Verifica que el encabezado no este corrupto 16 bits
Urgent Pointer	Cuando un dato urgente es enviado (se especifica en el campo Flag). 16 bits

UDP, User Datagrama Protocol

El protocolo de datagramas de usuarios suministra un servicio no orientado a la conexión y no fiable. Se utiliza frecuentemente en comunicaciones de datagramas IP de difusión. Puesto que no esta garantizada la recepción de los datagramas UDP, los programas que lo utilizan deben elaborar sus propios mecanismos de fiabilidad.

UDP Ports: Para uso de UDP, la aplicación debe contar con la dirección IP y el número de puerto de la aplicación destino. Un port es la entrada por donde se reciben los mensajes. Por mencionar algunos ejemplos: Netstat,15; Domain, 53; TFTP,69; SNMP, 161.

Nota: El RFC 768 define el protocolo UDP.

Estructura de un paquete UDP

Los siguientes campos son parte del encabezado de un paquete UDP:

Campo	Función
Source Port	Port UDP del host que envía, es un valor opcional si no se usa es igual a cero.
Destination Port	Port UDP del host destino.
Message Length	El tamaño del mensaje UDP
Checksum	Verifica que el encabezado no este corrupto

Sección 2: *Classfull IP Addressing*

Sección 2: *Classfull IP Addresing*

Introducción

Este capítulo es la introducción a los conceptos de direccionamiento IP, incluye términos como: clases de redes y mascaras. Identificará direcciones inválidas para determinadas clases de redes y situaciones, identificará los problemas más comunes de direccionamiento IP.

Objetivos Particulares

Al finalizar esta sección, Usted podrá:

- Definir que es una dirección IP y su estructura
- Identificar de las direcciones IP las diferentes clases de redes
- Identificar el ID de la red y el ID del host, dentro de las redes de clase A, B, C
- Distinguir direcciones IP válidas entre las diferentes clases de redes

Qué son las Direcciones IP?

Internet es un gran grupo de redes interconectadas. Todas estas redes se ponen de acuerdo para conectarse con otras redes, permitiendo a cualquiera conectarse a otro. Cada uno de estos componentes de red se asignan a una dirección de red.

Cada host en una red TCP/IP es identificada por una dirección IP. Cada uno de los componentes de una red TCP/IP debe tener una dirección IP para que se comuniquen entre ellos.

Las direcciones IP son una cadena de 32 bits que se dividen en octetos; los cuales están separados por puntos entre cada uno de ellos. Los octetos están representados por un número decimal que esta dentro del rango del 1 al 255, esto es a lo que se le llama notación decimal pero igual tenemos la notación binaria que es de donde parte este formato de direcciones. Ejemplo:

Formato Binario:	Formato Decimal:
10000011.01101011.00000011.00011000	131.107.3.24

Cada dirección define un número de red (Network ID) y un número de Hots (Host ID), el ID de la red es el número que identifica en el sistema que están localizadas en el mismo segmento físico de una red, por supuesto, todos los hosts en esta red tienen el mismo número de ID y que debe ser único en una Internetwork.

El host ID identifica la estación de trabajo, servidor, router o algún otro host de TCP/IP en un mismo segmento. La dirección para cada uno de los hosts debe ser única para el network ID.

Nota: un octeto son 8 bits, lo que en una notación decimal típica significa el primer conjunto de números. Por ejemplo: en la dirección IP 192.168.1.42 el primer octeto es el 192.

Convirtiendo direcciones IP

Recordando un poco, en el formato binario contamos nada más con dos valores: 0 / 1 que dependiendo de su posición dentro del octeto, cada número 1 tiene un valor decimal. Cuando tenemos un bit 0, su valor siempre es cero.

En la tabla que relatamos a continuación tenemos un ejemplo: todos los número 1 tienen un valor diferente siendo el mas alto el 128 y el mas bajo el 1. Para sacar el valor en notación decimal se requiere sumar la cantidad de cada uno de ellos, es decir: 1+2+4+8+16+32+64+128=255

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

Siguiendo lo anterior, tenemos la siguiente tabla:

Binario	Valores de los Bits	Notación Decimal
00000000	0	0
00000001	1	1
00000011	1+2	3
00000111	1+2+4	7
00001111	1+2+4+8	15
00011111	1+2+4+8+16	31
00111111	1+2+4+8+16+32	63
01111111	1+2+4+8+16+32+64	127
11111111	1+2+4+8+16+32+64+128	255

Examen 2-1

Convertir de Binario a Decimal y viceversa

Valores en Binario	Decimal
10001011	_____
10101010	_____
10111111.11100000.00000111.10000001	_____
01111111.00000000.0000000.00000001	_____

Decimal	Binario
250	_____
19	_____
109.128.255.254	_____
131.107.2.89	_____

Clases de Redes

La comunidad de Internet decidió que las direcciones IP se dividieran en diferentes clases de redes, (A, B, C, D y E); de los cuales trabajamos con tres nada mas ya que los otros rangos están asignados a usos experimentales e investigaciones.

Para organizar mejor las clases de red, se decidió desde los primeros días de vida de IP, que los primeros bits deberían decidir la clase a la que pertenecían. Esto quiere decir que el primer octeto de la dirección IP especifica la clase.

TCP/IP soporta las clases A, B y C; las clases de redes se definen por el número de bits que son utilizados para identificar la red (Network *ID*) y los bits restantes son asignados a los dispositivos que componen la red. Igualmente define los posibles números de redes que hay dentro de cada clase y los números de hosts que puede haber por cada red.

Nota: Observará que algunos huecos en los rangos, esto se debe a que hay algunas direcciones especiales que se reservan para usos especiales. La primera dirección especial es una que ya le es familiar: 127.0.0.1. Está se conoce como la dirección de loopback o de bucle local. Se configura en cada máquina que usa IP para que se refiera a sí misma. Otros rangos importantes: cada IP de la red 10.0.0.0, de las redes 172.16 a 172.31 y de la red 192.168 se consideran como IP privadas. Estos rangos no se permiten reservar a nadie de Internet, y por tanto, puede usarlos para sus redes internas.

Definimos redes internas como redes que están detrás de un firewall, no conectadas realmente a Internet, o que tienen un enrutador que realiza el enlace de las redes.

Redes Clase A

Network	Host	Host	Host

En una red clase A, el primer octeto identifica la red y los tres octetos últimos el número de nodo.

El primer bit debe ser: 0xxxxxxx

Valor mínimo:	00000000	Decimal: 0
Valor máximo:	01111111	Decimal: 127
Rango:	1 –126	

Hay 126 redes de clase A, cada una tiene 16,777,214 hosts.

Redes Clase B

Network	Network	Host	Host

En redes clase B, los dos primeros octetos son para identificar la red y los demás para el número de host.

Los primeros bits deben ser: 10xxxxxxx

Valor mínimo: 10000000 Decimal: 128
Valor máximo: 10111111 Decimal: 191
Rango: 128 –191

Hay 16,384 redes de clase B, cada una tiene 65,534 hosts.

Redes Clase C

Network	Network	Network	Host

Los primeros bits deben ser: 110xxxxxx

Valor mínimo: 11000000 Decimal: 192
Valor máximo: 11011111 Decimal: 223
Rango: 192 –223

Hay 2'097,152 redes de clase c y cada una tiene 254 hosts.

Redes Clase D

Las direcciones de las redes clase D están dentro del rango de 224.0.0.0 al 239.255.255.255 son usadas para paquetes multicast.

Los paquetes multicast usan muchos protocolos para alcanzar el grupo de hosts. IGMP *Router Discovery* es un ejemplo de un protocolo que utiliza paquetes multicast.

Redes Clase E

Igualmente, las direcciones de esta clase se encuentran dentro del rango del 240.0.0.0 al 255.255.255.255 y que están reservadas para futuros nodos de direcciones. Direcciones de las clases D y E no están asignadas a hosts individuales y más bien son para fines de investigación.

La siguiente tabla es un sumario de las diferentes clases de Redes y algunos valores a considerar.

Clase	Octetos	Inicia con Bits:	Número de Bits para identificar la red	Número de bits para identificar los host	Valor	Máscara de Red
A	NHHH	0xx	7	24	1 - 126	255.0.0.0
B	NNHH	10x	14	16	128 - 191	255.255.0.0
C	NNNH	110	21	8	192 - 223	255.255.255.0
D		1110	20	8	224 - 239	
E		1111	20	8	240 - 255	

Guía de Direcciones IP

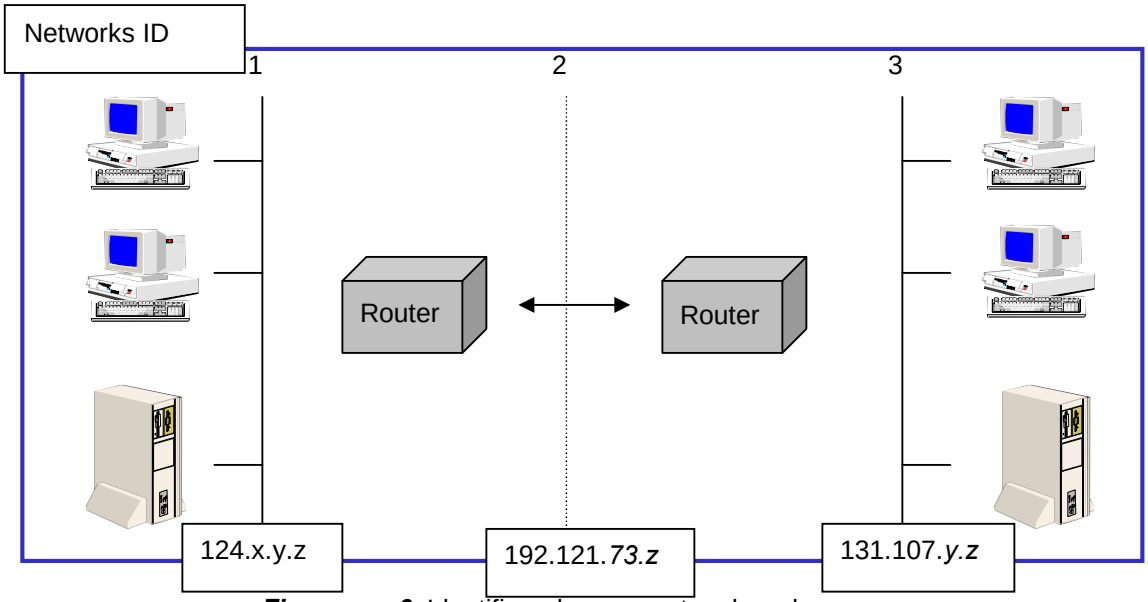


Figura no. 6. Identificando segmentos de redes

Si esto no fuera suficiente, aún contamos con ciertas reglas que debemos tener siempre en cuenta:

- El ID de una red no puede ser 127, ya que esta reservada para funciones de Loopback
- El ID de la red y el ID del host, nunca pueden ser todos 0´s o sea que no puede ser 0 porque se considera como en esta red nada mas.
- El ID de la red y el ID del host, nunca pueden ser todos 1´s o sea que no puede tener el valor de 255 ya que se considera como un broadcast a la dirección.
- El número ID de un host debe ser único en una red local

Todos los hosts incluyendo interfaces como routers, requieren una dirección única dentro de la red. Ya sabemos que él ID de una red nos define un segmento físico, pero cuales son los rangos válidos de direcciones para los hosts?

Clase de Red	Rango de Inicio	Rango Final
A	w.0.0.1	w.255.255.254
B	w.x.0.1	w.x.255.254
C	w.x.y.1	w.x.y.254

Como orden, dos recomendaciones:

- Asignar a los hosts sus ID´s de acuerdo al segmento de red
- Asignar a los routers las primeras direcciones IP

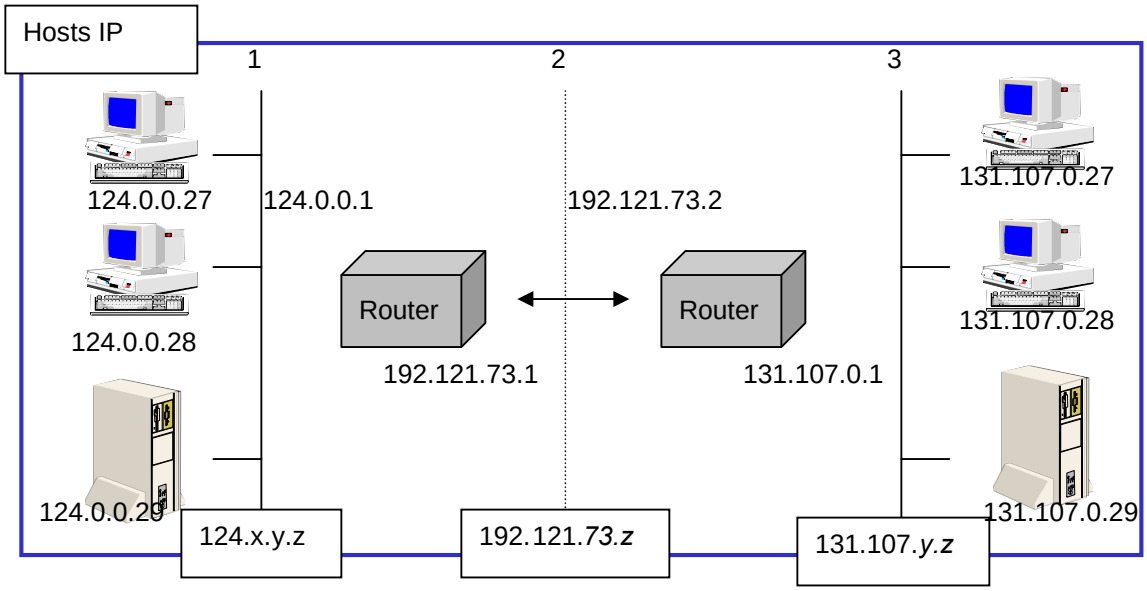


Figura no. 7. Identificando direcciones de *hosts*

Examen 2-2

Identificando direcciones IP válidas. Revisar las siguientes direcciones IP e identificar cuales son válidas y porque.

131.107.256.80	
222.222.255.222	
231.200.1.1	
126.1.0.0	
0.127.4.100	
190.7.2.0	
127.1.1.1	
198.121.254.255	
255.255.255.255	

Máscara de Red

Como mencionamos antes, las direcciones IP se dividen en dos partes, la dirección de red y la dirección de la máquina. Dependiendo de la clase de la dirección hay de 254 a 16 millones de direcciones disponibles para los hosts de la red.

Una máscara de red, es una dirección de 32 bits, que:

- En primer lugar le dice al sistema que bits de la dirección IP corresponden al componente de red y qué bits corresponden al componente máquina.
- Sirve para bloquear una porción de la dirección IP para distinguir él ID de la Red del número de los hosts.
- Especificar cuando un host destino esta en una red local o remota.

Cada hosts en una red basada en TCP/IP requiere de una máscara, ya sea una máscara por defecto cuando la red no esta subdividida o una personalizada de acuerdo a los segmentos en que se haya dividido la red.

Volviendo un poco atrás, cuando en formato binario realizamos una operación AND tenemos que:

1	AND	1	=1
1	AND	0	=0
0	AND	1	=0
0	AND	0	=0

Este es el mismo proceso que TCP/IP utiliza para saber a donde debe enviar los paquetes que van de una red a otra, veamos. Si mi dirección IP es de una clase B, tenemos que:

Dirección Host	10011111	11100000	00000111	10000001
Máscara	11111111	11111111	00000000	00000000
Resultado:	10011111	11100000	00000000	00000000

Es de esta manera que la máscara bloquea la porción del Network ID para indicarnos de que clase de red estamos hablando. Las máscaras por default, las tenemos indicadas en una tabla anterior, para ser compatible con direcciones IP en notación binaria, la subnet mask también es convertida en binario.

Subnet Mask Bits

Representación Binaria	representación decimal
11111111	255
11111110	254
11111100	252
11111000	248
11110000	240
11100000	224
11000000	192
10000000	128
00000000	0

En notación binaria, una máscara de subred es representada por cuatro octetos tal y como la dirección IP. La siguiente tabla le muestra las máscaras en notación decimal y binario utilizadas en el classfull método.

reprsentacion DECIMAL	REPRESENTACIÓN binaria
255.0.0.0	111111111.00000000.00000000.00000000
255.255.0.0	11111111.11111111.00000000.00000000
255.255.255.0	11111111.11111111.11111111.00000000

Utilizando la representación en binario de la mascara usted puede manipular los 32 números. Esto incrementa la capacidad de proveer una mayor selección de redes comparado con el *classful-method.*

Examen 2-3

Escenario 1. Convertir las direcciones IP de la siguiente tabla en binario. En la primera columna el número decimal convertir en porción binaria y en la segunda columna completar la dirección IP en binario.

IP DECIMAL	Porción en binario	IP en Binario
122.131.25.64	1111010,10000011,1101,1000000	01111010.10000011.00001101.0100000
215.34.211.9		
97.49.153.122		
64.144.25.100		
176.34.68.78		
42.89.215.61		
71.73.65.166		
47.245.235.84		
156.213.67.23		
124.87.235.87		
7.23.87.2		
223.12.7.8		

Escenario 2. En este ejercicio usted deberá identificar la clase de red de la dirección IP, separar el network ID del Host ID.

IP Address	Class/Subnet mask	Network ID	Host ID
129.102.197.23	B/255.255.0.0	129.102.0.0	197.23
131.107.2.1			
199.32.123.54			
32.12.54.23			
1.1.1.1			
221.22.64.7			
93.44.127.235			
23.46.92.184			
152.79.234.12			
192.168.2.200			
168.192.3.26			
224.224.224.224			
200.100.50.25			
172.71.243.2			
163.37.121.32			
76.35.61.23			

Para una red de más de 1,000 hosts, que clases de redes se necesitan?

_____

Si tengo 64 hosts, que clase de red debe solicitar?

_____

Sección 3: Subnetting/Supernetting

Sección 3 Subnetting / Supernetting

Introducción

Como parte de esta sección, veremos los conceptos y procedimientos fundamentales del subnetting y supernetting. Incluyendo cuando es necesario un subnetting y que se requiere, como y cuando utilizar una máscara de sub redes y como crear los rangos de direcciones válidas dentro de cada segmento.

Objetivos Particulares

Al finalizar esta sección, usted podrá:

- Explicar la función de una máscara de Sub-Red
- Definir una máscara de subredes común para una red WAN que contiene múltiples subredes.
- Definir los rangos de ID válidos de los hosts para múltiples sub- redes
- Explicar qué es el *Supernetting*

Definiendo Subnetting

Una Subnet o sub-red, es un segmento físico en un ambiente de TCP/IP que usa direccionamiento IP derivadas de una sola network ID.

Por lo general, las organizaciones adquieren su Network ID de parte del InterNIC, dividirla en segmentos requiere que cada segmento utilice un número diferente de network ID o digamos un Subnet ID. Este ID se crea dividiendo los bits que corresponden para identificar al host en dos partes, una parte se agrega a los bits que corresponden al ID de la red y la otra parte es para el ID de los hosts.

Para las organizaciones que aplican el subneteo, de una sola red crean múltiples segmentos; lo que les permite:

- Mezclar diferentes tecnologías como: Ethernet y Token Ring
- Reducir la congestión de la red, re-direccionando el tráfico y reduciendo los broadcast.
- Una administración más comoda de las direcciones IP
- Conectar sucursales y tolerancia a fallas

Nota: El Subnetting, esta definido en el RFC´s: 950.

Implementando una Sub-red

Antes de crear un esquema de Sub redes, necesitamos determinar los requerimientos actuales y considerar el crecimiento de la organización.

- Determinar el número de segmentos físicos que se requieren en la red
- Determinar el número de hosts para cada segmento físico. Recordemos que cada uno de los hosts requieren una dirección IP.
- En base a estas necesidades definir:

  Una Máscara de Sub red para toda la red.

  Un único ID para cada segmento físico

  Un rango de hosts ID´s para cada sub-red

Cómo se crean las máscaras de subredes

Ejemplo para una red de Clase B

Número de Sub-redes 0….. 254 Número de Hosts 254

Network ID			Host Id
10xxxxxx	Xxxxxxxx	**111**xxxxx	xxxxxxxx

Número de Hosts Posibles: 65,534

En la gráfica anterior, se ilustra como se toman bits extras de los asignados al host ID para formar una máscara de red. Por supuesto, podemos tomar más bits para más segmentos en el caso de necesitar más de 254; pero nos queda un número más pequeño de bits para combinar y crear los hosts ID. Por esta razón es muy importante una buena planeación.

Pasos para definir las nuevas subnet mask:

1. Determinar el número de segmentos que se requieren y convertir este número en binario.
2. Determinar el número de bits que nos tenemos que robar y comprobar
3. Convertir en decimal y definir la nueva subnet mask
4. Definir los segmentos de subred
5. Definir los rangos de direcciones IP para cada unode los segmentos

Ejemplo para una Red de Clase B:

1. Requerimos 6 segmentos convertidos en Binario tenemos: 0000110.
2. Lo cual quiere decir que ocupamos 3 bits que vamos a tomar del tercer octeto comprobando: 2 a la 3 es igual a 8, menos dos combinaciones que nos son posibles (ni todos ceros ni todod unos) es igual a 6 que cumple con los 6 segmentos que necesitamos.
3. La Sub-máscara en binario queda así: 11111111.11111111.11100000.00000000
   Convirtiendo en decimal: 255. 255. 224. 0

4. Permutamos los bits que nos robamos para definir segmentos:

Tercer octeto:	000xxxxx	=	0	(no válido)
	001xxxxx	=	32	
	010xxxxx	=	64	
	011xxxxx	=	96	
	100xxxxx	=	128	
	101xxxxx	=	160	
	110xxxxx	=	192	
	111xxxxx	=	224	(no válido)

5. Definiendo los rangos de IP´s para cada segmento:

w.x.32.0	w.x.32.1 a la w.x.63.254
w.x.64.0	w.x.64.1 a la w.x.95.254
w.x.96.0	w.x.96.1 a la w.x.127.254
w.x.128.0	w.x.128.1 a la w.x.159.254
w.x.160.0	w.x.160.1 a la w.x.191.254
w.x.192.0	w.x.192.1 a la w.x.224.254

Cuando son pocos los bits que tenemos que combinar no representa un problema, pero que pasaría si son 7 ó 14?. Otro método que es un "***shortcut***" para la definición de los segmentos de red y de los rangos para las direcciones IP es:

1. Definir los bits que ocupamos para los segmentos, para este caso, requerimos 3.
2. Activar los bits en 1 de izquierda a derecha, esto es: 11100000
3. Seleccionamos el bit de menos valor, en este caso es el tercero y se convierte en decimal =32
4. Este es el valor que se debe incrementar para definir los segmentos, comparemos: 32 + 32 =64; 64+32 =96; 96+32=128; etc.

A continuación le relatamos una tabla de conversiones que le será bastante útil para planear su subnetting.

Clase A, considerar que se toma el segundo octeto para crear la máscara

Segmentos	Bits requeridos	Máscara Sub-red	Hosts por segmento
0	1	Inválida	Inválida
2	2	255.192.0.0	4,192.302
6	3	255.224.0.0	2,0972150
14	4	255.240.0.0	1,048,574
30	5	255.248.0.0	524,286
62	6	255.252.0.0	262,142
126	7	255.254.0.0	131,070
254	8	255.255.0.0	65,534

Clase B, en este caso es el tercer octeto que utilizamos para crear la máscara

Segmentos	Bits requeridos	Máscara Sub-red	Hosts por segmento
0	1	Inválida	Inválida
2	2	255.255.192.0	16,382
6	3	255.255.224.0	8,190
14	4	255.255.240.0	4,094
30	5	255.255.248.0	2,046
62	6	255.255.252.0	1,022
126	7	255.255.254.0	510
254	8	255.255.255.0	254

Clase C, recordar que es el cuarto octeto el que define la sub máscara

Segmentos	Bits requeridos	Máscara Sub-red	Hosts por segmento
0	1	Inválida	Inválida
2	2	255.255.255.192	62
6	3	255.255.255.224	30
14	4	255.255.255.240	14
30	5	255.255.255.248	6
62	6	255.255.255.252	2
126	7	Inválida	Inválida
254	8	Inválida	Inválida

Hasta ahora hemos subdividido redes en un solo octeto, pero igualmente si las necesidades son más segmentos, una clase A se puede definir hasta el tercer octeto; por ejemplo:

Network ID	Subnet Mask	Binario
10.0.0.0	255.255.248.0	11111111.11111111.11111000.00000000

Examen 3-1

Definiendo máscaras de Sub – Redes Válidas. En este ejercicio, usted va a definir una máscara para las sub-redes en diferentes situaciones:

1. Clase A, red local

2. Clase B, red local con 4,000 hosts

3. Clase C, red local con 254 hosts

4. Clase A, con 6 Sub-Redes

5. Clase B, con 126 sub-Redes

6. Clase A, actualmente cuenta con 30 sub-redes que en un año crecerán a 65. Cada una de las sub – redes no tendrán más de 50,000 hosts.

7. Usando la máscara del paso 6, hasta cuantas sub-redes nos permite crecer?

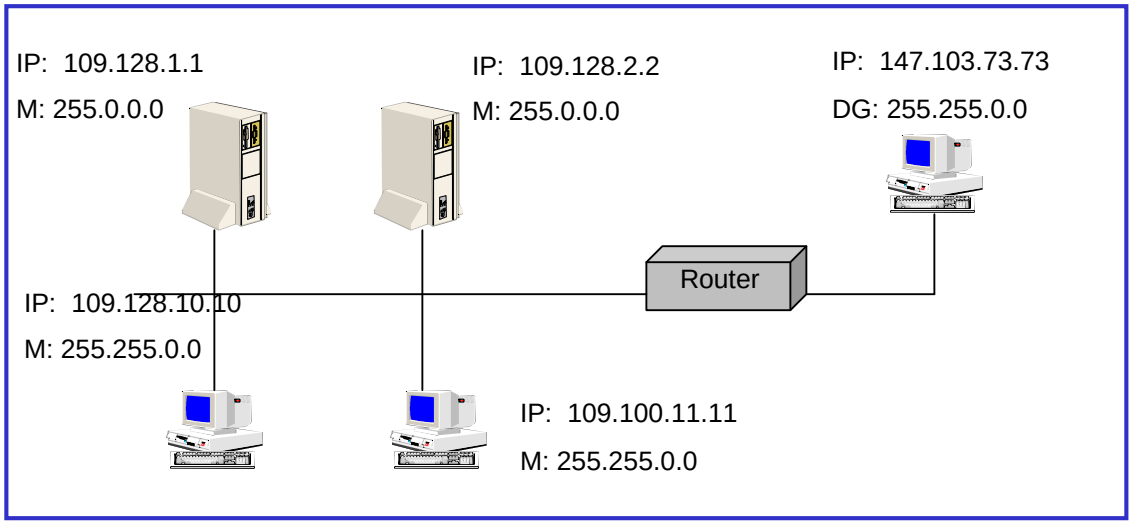
8. Clase B, Contamos con 14 sub – redes que crecerán al doble el próximo año; cada una de las sub – redes contaran con 1500 *hosts*.

9. Siguiendo con el paso anterior, con esa máscara de *subnetting* cuantas redes nos provee para un futuro crecimiento.

Examen 3-2

Identificando problemas de direcciones en sub – Redes . En este ejercicio, hay que observar los escenarios e identificar los problemas escondidos, cuales son los efectos ocasionados y explicarlos.

Escenario 1

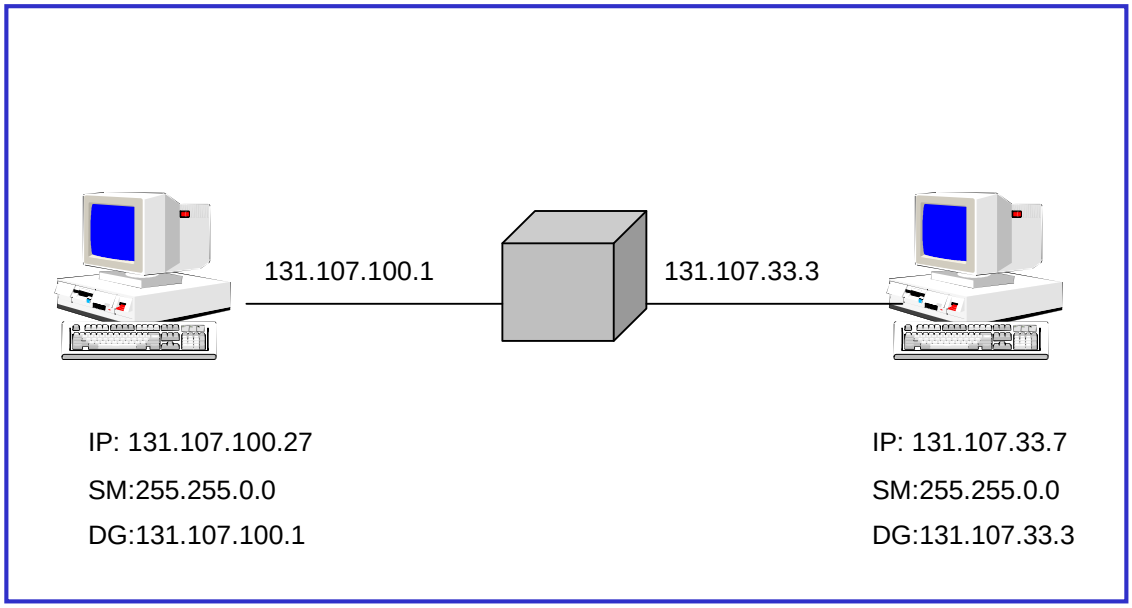


Qué hosts del diagrama tienen una máscara incorrecta?

Cuáles son los efectos para estos hosts?

Cuál es la máscara de sub-red correcta?

Escenario 2



Cuál es el problema en esta gráfica?

Cómo afecta en la comunicación?

Cuál es la máscara correcta?

Supernetting

Supernetting es el caso contrario que *subnetting*, esto es que teniendo varias redes de clase C, pueda crear una máscara que haga suponer que todas son un sólo segmento, es decir una sola red.

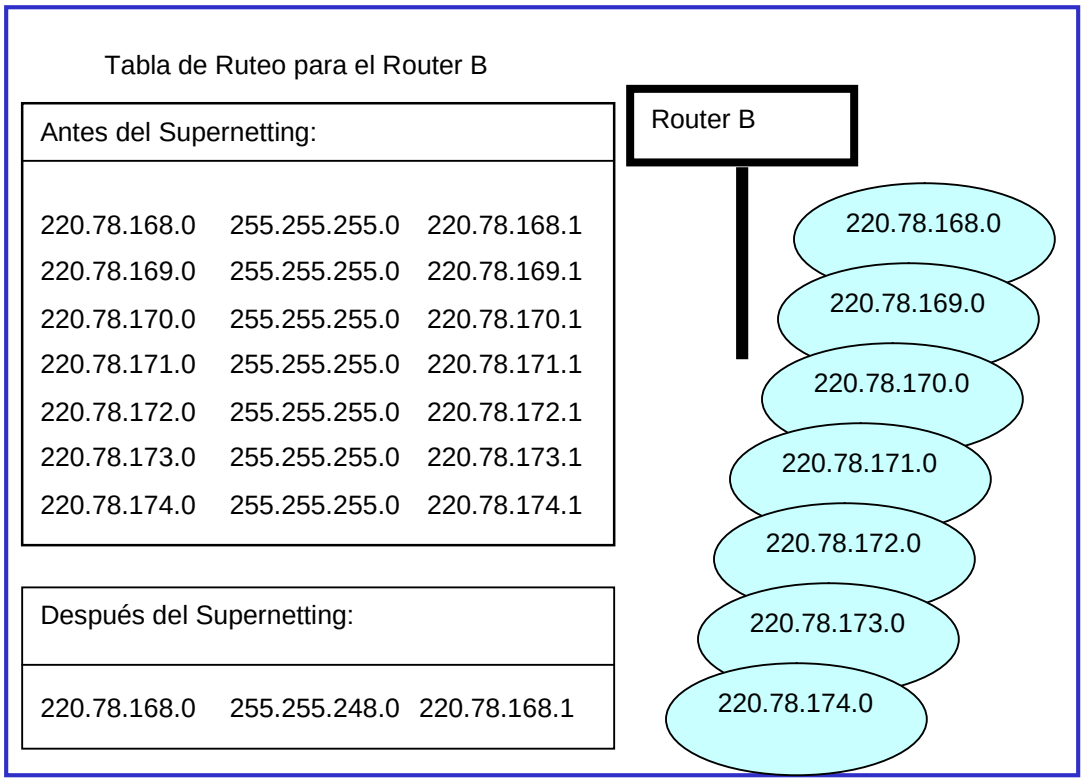


Figura no. 10. Supernetting con 7 redes de clase C

Tengo siete redes de Clase C, que van de los segmentos 220.78.168.0 al 220.78.174.0

Convierto cada uno de los octetos en binario y tomo los 3 últimos bits del octeto que me indica el segmento de red y les pongo valor de 0. Por último, convierto en binario y obtengo mi nueva máscara.

Network ID	Máscara	Binario
220.78.168.0	255.255.248.0	11111111.11111111.11111000.00000000

Examen 3 - 3

Definiendo Rangos para Sub – Redes. En este ejercicio, de acuerdo a los escenarios usted definirá los ID´s de la red y sus Sub-Redes.

Escenario 1.

Es una red de clase B y dos sub-redes; usando 2 bits para la máscara. Listar las combinaciones posibles de los bits, convertir en decimal para determinar los segmentos de red.

255	255	192	0
11111111	11111111	**11**00000	0000000

Inválida 00000000 = 0

Subnet 1 _____ =

Subnet 2 _____ =

Inválida _____ =

Listar el rango de los hosts ID para cada sub-Red

Subnet 1 w.x._____.1 w.x._____.254

Subnet 2 w.x._____.1 w.x._____.254

Escenario 2

En este escenario, se requieren 14 segmentos usando 4 bits, listar las combinaciones posibles, convertir en decimal y después marcar los rangos de los segmentos.

255	255	240	0
11111111	11111111	1111000	0000000

Inválida	00000000	=	0
Subnet 1	_____	=	_____
Subnet 2	_____	=	_____
Subnet 3	_____	=	_____
Subnet 4	_____	=	_____
Subnet 5	_____	=	_____
Subnet 6	_____	=	_____
Subnet 7	_____	=	_____
Subnet 8	_____	=	_____
Subnet 9	_____	=	_____
Subnet 10	_____	=	_____
Subnet 11	_____	=	_____
Subnet 12	_____	=	_____
Subnet 13	_____	=	_____
Subnet 14	_____	=	_____
Inválida	11110000	=	240

Listar los rangos de los diferentes segmentos

Subnet 1	_____	_____
Subnet 2	_____	_____
Subnet 3	_____	_____
Subnet 4	_____	_____
Subnet 5	_____	_____
Subnet 6	_____	_____
Subnet 7	_____	_____
Subnet 8	_____	_____
Subnet 9	_____	_____
Subnet 10	_____	_____
Subnet 11	_____	_____
Subnet 12	_____	_____
Subnet 13	_____	_____
Subnet14	_____	_____

Escenario 3

En este ejercicio va a determinar la máscara apropiada de sub-redes para los siguientes rangos de direcciones IP

1. Rango de la 128.71.1.1 hasta la 128.71.254.254

2. Rango de la 61.8.0.1 hasta la 61.15.255.254

3. Rango de la 172.88.32.1 hasta la 172.88.63.254

4. Rango de la 111.224.0.1 hasta la 111.239.255.254

5. Rango de la 3.64.0.1 hasta la 3.127.255.254

6. Tenemos 4 segmentos, los Networks ID son: 190.1.16.0, 190.1.32.0, 190.1.48.0 y 190.1.64.0 máscara: 255.255.248.0:

Examen 3–4

Definiendo el esquema de Direcciones para una Sub - Red

Escenario 1

Tiene usted asignada una red de clase B, 131.107.0.0. en estos momentos cuenta con 5 segmentos, cada segmento cuenta con 300 hosts. Para el próximo año tendremos el triple de redes y el número de hosts se incrementará a 1,000 hosts.

Cuántos bits necesita para elaborar la nueva máscara de redes?

Con esta, cuántas sub-redes le permitirá de desarrollo?

Cuántos hosts le permitirá adicionalmente de soporte?

Escenario 2

Tiene usted asignada una red de Clase A, 124.0.0.0 con 5 redes con 500,000 hosts. En un futuro en lugar de trabajar con 5 redes, se fragmentará a 25 más pequeñas y más manejables. El numero de los hosts sería en promedio de 300,000.

Cuántos bits requiere para crear la nueva máscara?

Cuántas subredes le permite adicionalmente para crecer?

Hasta cuantos hosts le soporta la nueva máscara?

Examen 3-5

Usted es un proveedor de servicios de Internet al cual le fueron asignadas un bloque de 2,048 redes de clase C iniciando en 192.24.0.0 y terminando con 192.31.255.0.

1. Si usted hiciera un superneteo de este bloque de redes, como cual dirección IP se debe ver? _____

2. Cuál es la máscara de red? _____

Los clientes que le han solicitado el servicio de Internet tienen los siguientes requerimientos:

- El cliente no. 1 no tendrá más de 2,023 hosts
- El cliente no. 2 no tendrá más de 4,047 hosts
- El cliente no. 3 no tendrá más de 1,011 hosts
- El cliente no. 4 no tendrá mas de 500 hosts

Conteste las siguientes opciones llenando con la IP correcta los espacios vacíos:

3. Cliente no. 1

Dirección de inicio	192.24.0.1
Dirección Final	192.24.7.8
Subnet Mask	_____

4. Cliente no. 2

Dirección de inicio	_____
Dirección Final	192.24.31.254
Subnet Mask	255.255.240.0

5. Cliente no. 3

Dirección de inicio	192.24.8.1
Dirección Final	_____
Subnet Mask	255.255.252.0

6. Cliente no. 4

Dirección de inicio	192.24.14.1
Dirección Final	192.24.15.254
Subnet Mask	_____

CIDR, Classless Inter.-Domain Routing

Las clases de redes IP proveen de un método simple para diferenciar hosts locales de hosts remotos y para ubicar las rutas hacia los hosts de redes remotas. De cualquier manera, este método permite muy pocas variaciones en los tamaños de la red lo cual le puede ocasionar varios problemas con una inapropiada asignación de direcciones a las redes. Para romper estas limitaciones tenemos un método conocido como *Classless Inter-Domain Routing* que fue desarrollado para romper las redes de grandes tamaños.

Incluso si tiene una clase de direcciones A o B, no es realista configurar su red como un gran grupo de máquinas. Aparte de resultar una pesadilla administrar, le retamos a que encuentre cualquier tipo de red capaz de tener tantas máquinas agrupadas juntas. Por ejemplo, Ethernet no puede tener más de 1024 máquinas por segmento debido a las colisiones.

Para resolver este problema, estas redes enormes se dividen en subredes más pequeñas. Esto se hace expandiendo el número de bits usados para representar la dirección de red, una técnica conocida como *Classless InterDomain Routing* (Enrutamiento Inter. dominio sin clases) debido a que viola la descripción de las redes A, B y C.

La notación CIDR nos pide especificar una notación en decimal con el número de bits que compone la máscara. Por ejemplo:

IP Address	10.		217.	123.		7	
Mask	11111111.11111111.11110000.00000000						
Bits activados:	8 +		8+	4	+	0=	20
Notación CIDR	10.217.123.7/20						

Nota: A la notación CIDR también se le conoce como *network prefix notation*.

CIDR y Clases de Redes

Las direcciones IP en la notación CIDR son comprendidas por el número de bits de la dirección IP que identifican al network ID y se representada como /*x*. Por ejemplo, un network ID de 10 bits se representado como /10.

En la notación CIDR, la IP que se representa con /20 puede ser una red de clase A, B o C. Los ruteadores que soportan CIDR no utilizan los tres primeros octetos de la dirección para determinar si el host destino es local o es remoto, como en el método *classful*. En vez de eso, descarga en la información de bits de la mascara provista con la ruta para hacer una determinación.

La siguiente tabla es una lista practica de *bits mask*, la subnet mask asociada y el número de *classfull networks* posibles para cada una.

Notación CIDR	*Subnetmask*	*Número de classful networks*
/8	255.0.0.0	256 clase B
/9	255.128.0.0	128 clase B
/10	255.192.0.0	64 clase B
/11	255.224.0.0	32 clase B
/12	255.240.0.0	16 clase B
/13	255.248.0.0	8 clase B
/14	255.252.0.0	4 clase B
/15	255.254.0.0	2 clase B
/16	255.255.0.0	1 clase B o 256 clase C
/17	255.255.128.0	128 clase C
/18	255.255.192.0	64 clase C
/19	255.255.224.0	32 clase C
/20	255.255.240.0	16 clase C
/21	255.255.248.0	8 clase C
/22	255.255.252.0	4 clase C
/23	255.255.254.0	2 clase C
/24	255.255.255.0	1 clase C
/25	255.255.255.128	½ clase C
/26	255.255.255.192	¼ clase C
/27	255.255.255.224	1/8 clase C
/28	255.255.255.240	1/16 clase C

Como nota aparte, esta versión de TCP/IP es la número 4, cuando se planteó el esquema de las direcciones IP nunca creyeron que en algún momento se fueran agotar las direcciones disponibles. Pues bien, el sistema esta por saturarse, por lo que se tiene ya contemplado una versión 6.0 para TCP/IP donde los números binarios se convierten a hexadecimales, es decir, que en vez de ser una cadena de 32 bits ahora su tamaño es de 128 bits, cuatro veces más grande.

Cuando usted configure direcciones IP en Windows 2000 debe teclear la dirección IP y la información de máscara de red en notación decimal. No acepta notación CIDR. Ahora que para calcular un network ID es mejor en notación binaria que en cualquiera de las dos (Notación Decimal o Notación CIDR). Veamos el siguiente ejemplo.

- **Para calcular el network ID cuando la dirección se especifica en notación CIDR.**

1. Convertir la IP en formato binario.
2. Utilice el bit mask para determinar el número de bits en la dirección IP que crean el network ID.
3. Agregue los 0´s que le hace falta para completar la máscara.

Ejemplo 1:

IP Address en Notación CIDR:		10.217.123.7/20		
IP Address	10.	217.	123.	7
Bin	00001010.	11011001.	01111011.	00000111
	255.	255.	240.	0
Mask	11111111.	11111111.	11110000.	00000000
Network ID	00001010.11011001.01110000.00000000			
Network ID CIDR	10.217.112.0/20			

- **Para calcular el network ID cuando la dirección y la máscara de red se especifican en notación decimal.**

1. Convertir la dirección IP en formato binario
2. Convertir la mascara de red en formato binario
3. Hacer un AND para calcular el Network ID.

Ejemplo 2:

IP:	10.217.128.7
Mask:	255.248.0.0
IP Address	00001010.11011001.01111011.00000111
Mask	11111111.11111000.00000000.00000000
Network ID	00001010.11011000.00000000.00000000

4. Después de calcular el Network ID en notación Binaria hacer el cálculo en notación decimal/CIDR. Recuerde que los usuarios usualmente no utilizan estos términos.

	Notación Binaria	Notación CIDR
Ejemplo 1	00001010.11011001.0111000.00000000	10.217.112.0/20
Ejemplo 2	00001010.11011000.0000000.00000000	10.216.0.0/13

IP´s disponibles para Hosts

El número de hosts soportados por network ID es calculado utilizando el número de 0´s que tenemos en la máscara de subred. Es decir, el número de 0´s es el exponente, siempre restándole 2 combinaciones que no son posibles (todos ceros y todos unos). Ejemplo:

IP	11000000	10101000	11000001	00000000
	192.	168.	193.	0
Mask:	11111111	11111111	11110000	00000000
	255.	255.	240.	0
Hosts ID			0000	00000000

2 exp 12 = 4,096 menos 2= 4,094 hosts ID.

Examen 3-6

Complete la siguiente tabla:

CIDR notación	*Subnetmask*	*Número de 0´s*	*Numero de hosts*
w.x.y.z/1	128.0.0.0	31	2´147,483,646
w.x.y.z/2			
w.x.y.z/3			
w.x.y.z/4			
w.x.y.z/5			
w.x.y.z/6			
w.x.y.z/7			
w.x.y.z/8			
w.x.y.z/9			
w.x.y.z/10			
w.x.y.z/11			
w.x.y.z/12			
w.x.y.z/13			
w.x.y.z/14			
w.x.y.z/15			
w.x.y.z/16			
w.x.y.z/17			
w.x.y.z/18			
w.x.y.z/19			
w.x.y.z/20			
w.x.y.z/21			
w.x.y.z/22			
w.x.y.z/23			
w.x.y.z/24			
w.x.y.z/25			
w.x.y.z/26			
w.x.y.z/27			
w.x.y.z/28			
w.x.y.z/29			
w.x.y.z/30			
w.x.y.z/31			
w.x.y.z/32			

Escenario 2. Usted es el encargado de telecomunicaciones de una universidad y cuenta con la red: 118.0.0.0/10. Esta red tiene que subdividirla en 8 segmentos para cada uno de los campus de la universidad, además de subdividir bajo las siguientes especificaciones:

a) El primer sub-segmento es asignado a la Facultad de Medicina, la cual tiene que dividirlo en 4 segmentos más pequeños.

b) El segundo sub-segmento corresponde a la Facultad de Ingeniería que cuenta con 15 laboratorios con salida a Internet. Dividir esta red en 15 más pequeños.

c) El tercer campus corresponde a las Areas Sociales-Administrativas que requiere dividir en 30 segmentos más pequeños

d) El cuarto sub-segmento corresponde a las oficinas administrativas que se ubican en dos edificios conectados entre si. (Dividir en dos redes)

e) El quinto sub segmento se va a dividir en 8 redes para las áreas públicas.

Debe indicar al elaborar los ejercicios, el NetId en notación CIDR, las direcciones inicio, final y de broadcast en cada uno de los casos e indicar el número de direcciones IP con las que cuentan.

Continuación para el escenario 2.