**Laboratorio de Hardware**

**Evaluación Unidad N°1 – Internet y Redes**

Luis Conforti – 6°2. Grupo Y.

1) ¿Cuáles son los cuatro procesos fundamentales de las redes informáticas? Explicar brevemente en que consiste cada uno de ellos

2) ¿Cuál es la diferencia entre arquitectura de red e infraestructura de red?

3) ¿Cuáles son los elementos que caracterizan la arquitectura de una red? Explique cada uno de ellos sintéticamente.

4) ¿Por qué decimos que desde el punto de vista lógico una red ethernet es un bus lógico?

5) ¿En un enlace entre dos nodos cuál de las dos direcciones (física y lógica) es más importante? Justifique la respuesta.

6) ¿Cómo haría un host para saber a qué dirección de red pertenece?

7) ¿Qué tipo de paquetes son utilizados para verificar la conectividad entre nodos?

8) ¿Qué se entiende por descartar un paquete?

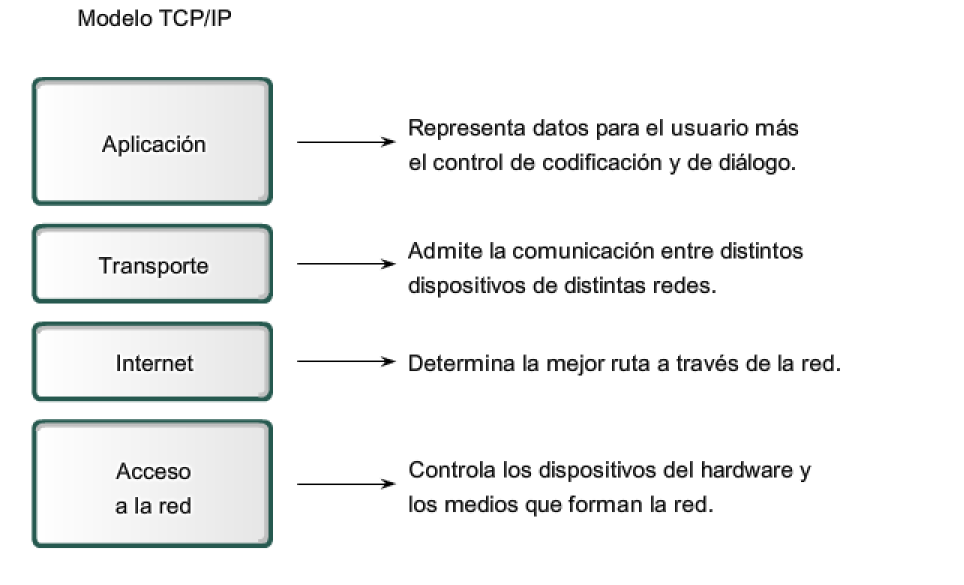
9) Dentro del modelo TCP/IP ubique el protocolo de servicio NAT.

10) ¿Qué institución se encarga regionalmente (nuestra) de administrar los nombres de dominio?

11) Explique de qué manera queda explicitado que una dirección IP presenta una estructura jerárquica, basarse en un ejemplo numérico.

1) En una red informática existen 4 procesos o capas de procesos (referidos al modelo TCP/IP). Estas capas son:

* Aplicación: Presenta en pantalla los datos para el usuario y el control y codificación del dialogo.
* Transporte: Comunica los dispositivos entre las redes, mandando los datos en forma de paquetes separados.
* Internet: Determina las mejores rutas para los paquetes en la red, y asigna las direcciones IP.
* Acceso a la red: Contiene protocolos para el control de los dispositivos de hardware y los medios que controlan la red.

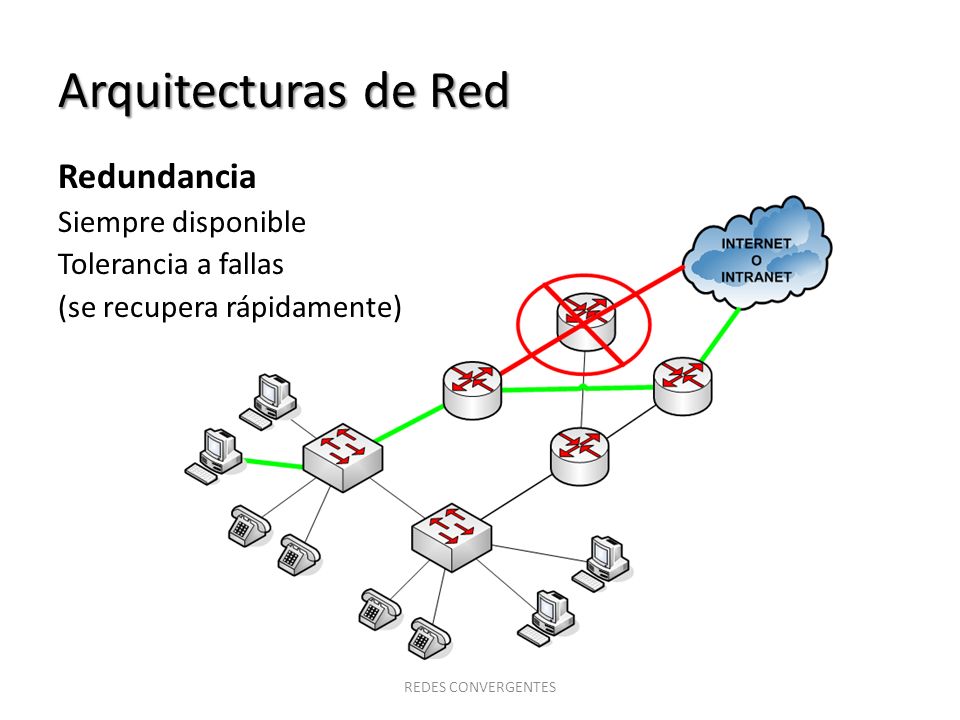


2) La infraestructura de red son todos los elementos de hardware (terminales, routers, switches, cableado, etc.) y software (controladores de dominio, software de servidor y de cliente, etc.) que la componen y son necesarios para el debido funcionamiento de la red. Por otro lado, la arquitectura de red son las tecnologías que le dan soporte a la infraestructura de la red para que funcione correctamente (protocolos de comunicación, estándares, servicios, y demás tipo de software).

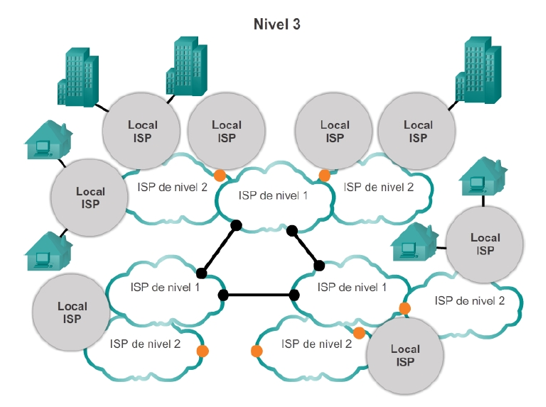


3) La arquitectura de red esta basada en cuatro pilares fundamentales: la tolerancia a fallas, la escalabilidad, la calidad del servicio, y la seguridad.

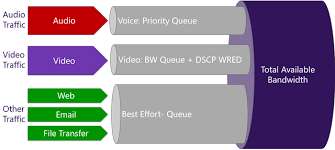
* Tolerancia a fallas: Para poder limitar y reducir la incidencia de posibles fallas y para poder recuperarse rápidamente de estas, se utiliza un concepto llamado “redundancia”. Sí ocurre un fallo en un router o en una línea, los demás routers pueden elegir una nueva ruta dinámicamente, ya que todas las rutas están conectadas entre sí.



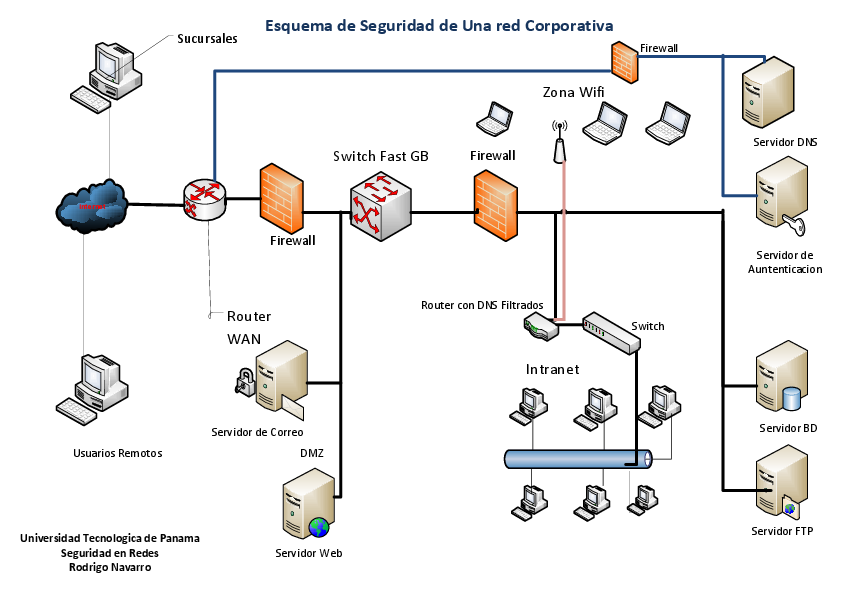
* Escalabilidad: Las redes como Internet tienen la característica de ser escalables. ¿A qué se refiere esto? La red debe ser capaz de admitir nuevos usuarios, aplicaciones, e ISP sin afectar el funcionamiento y rendimiento actual. ¿Cómo se logra esta “escalabilidad”? Generalmente se crean protocolos para la arquitectura de la red, volviéndola jerárquica, en varios niveles de relevancia (ISP nivel 1: grandes proveedores y sistemas que mantienen la red estable, nivel 2: proveedores regionales, nivel 3: proveedores locales, y, por último, usuarios domésticos o empresariales), permitiendo integrar nuevos niveles de menor importancia, y que estos niveles no interfieran con el tráfico central de la red, si no que transmitan datos en su propia red de la región.



* Calidad de servicio: Las redes conmutadas por paquetes son una gran opción para brindar una buena calidad en los servicios de red, pero eso no es suficiente, ya que aún así, los paquetes de la red pueden sobrepasar el ancho de banda y hacer colas, retrasando su entrega y bajando la calidad del servicio. Una buena solución para evitar esto, es el mecanismo de clasificación de los paquetes según su contenido: alta prioridad para comunicaciones audiovisuales y mensajería, mediana prioridad para transacciones comerciales y páginas web, baja prioridad para intercambio de archivos o entretenimiento. Con esto se organizan las colas y se dan más recursos a los paquetes de alta prioridad.

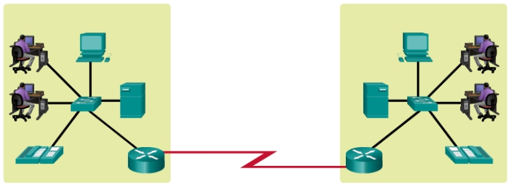


* Seguridad: Los dispositivos conectados a la red tanto como su información son extremadamente importantes, una falla de seguridad puede traer a: interrupciones, robo de propiedad intelectual, robo de información personal, perdida de recursos personales, perdida de datos irremplazables, y demás calamidades. Se debe asegurar seguridad tanto como para el hardware y el software de la infraestructura de la red, como también la información de los usuarios en la red. Para poder asegurar esto, se deben cumplir una serie de “requisitos de seguridad”, tales como asegurar la confidencialidad de los datos, con sistemas de verificación de usuarios y contraseñas para evitar agentes externos; mantener la información de los datos mientras se comunica un mensaje; como también ofreces servicios de antivirus y cortafuegos para minimizar el riesgo de ataques de seguridad.



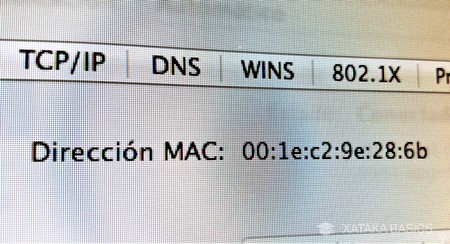
4) Podemos interpretar esta afirmación de dos maneras diferentes:

* En las redes de área local, se utiliza el protocolo ethernet para su conexión en la capa física, lo que podría definirlo como el “bus de datos lógico”.
* También puede interpretarse como el hecho de que las redes WAN están conformadas por miles de redes LAN ethernet, cuyas serían sus “buses de datos lógicos” por los cuales viaja la información.



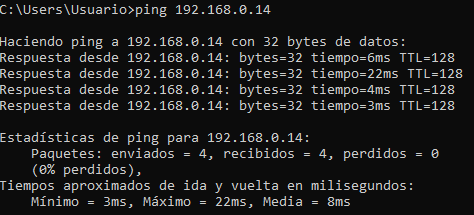
5) De las dos direcciones que posee un host; física (MAC) y lógica (IP) la dirección MAC es la más importante, por varios motivos. Estos son:

* La dirección MAC sirve como identificador irrepetible en el mundo entero; la dirección IP solo es irrepetible dentro de una red pública o dentro de una red privada aislada (muchas redes privadas aisladas pueden tener la misma dirección de red con las mismas direcciones de host sin causar conflictos).
* Los switches de capa 2 envían tramas de red utilizando la dirección MAC.

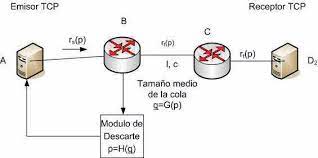


6) Un host puede determinar la dirección IP de la red utilizando la mascara de red. Se toma la dirección IP del host y la máscara de red para realizar la operación AND entre estas dos. Por ejemplo, si tenemos la IP 192.168.0.50 la máscara de red 255.255.255.0 y hacemos la operación AND con estas dos, nos dará como resultado la IP de la red, cuya sería 192.168.0.0.

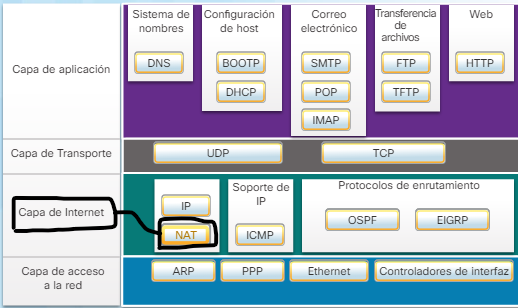
7) En una red que utiliza el modelo TCP/IP, se utiliza el comando “ping” para verificar la conectividad entre dos nodos. Al ejecutar este comando, se envían 4 paquetes de tipo ICMP al host destinatario; en caso de que los paquetes lleguen y se reciban correctamente, se mide su tiempo en milisegundos y la cantidad de saltos que tomaron para llegar a dicho host de destino. En caso de no llegar correctamente al host de destino o no encontrarlo, esto se informa.



8) Cuando la cantidad de paquetes es mayor a la que se puede transmitir con el ancho de banda disponible de una red, estos se ponen en cola esperando ser procesados y enviados. Si la cantidad de paquetes en cola aumenta, se empieza a descartar paquetes (eliminarlos de la cola) y a pedir su reenvío para alivianar la congestión.



9) En el modelo TCP/IP, el protocolo NAT se encuentra en la capa de Internet.



10) NIC Argentina (denominación que se le da a la Dirección Nacional Del Registro de Dominios de Internet) es el organismo que se encarga de registrar y administrar los nombres de dominio en Argentina (los terminados en .ar).



11) Una dirección IP es un identificador numerico de 32 bits, estos 32 bits se agrupan en 4 octetos y esos octetos se traducen a sistema decimal, lo que nos da una dirección decimal punteada (por ej: 192.168.10.78).

Esta dirección basa su jerarquía en una división de dos partes o “porciones”; una porción de red con la que se identifica a cada red, y una porción de host, con la que se identifica a los hosts de cada red. La cantidad de bits que abarca la porción de red depende del prefijo de red; este prefijo puede ir desde 1 a 30, y mientras mayor sea el prefijo, mayor será la cantidad de bits en la porción de red, por lo que habrá una mayor cantidad de redes; inversamente, habrá menor cantidad de bits en la porción de hosts, y menor cantidad de hosts por red.

El prefijo más común utilizado para esto es el 24, el cual brinda 24 bits de red y 8 bits de host, lo que da a la posibilidad de 254 hosts, ya que uno de estos se utiliza para identificar a la red y otro para identificar a todos los hosts para la multidifusión. Daremos un ejemplo:

Tenemos una dirección IP con la siguiente porción de red: **192.168.10**.x/24, la letra x representaría la porción de host de la IP. Como mencionamos anteriormente, no todos los bits de la porción de host se pueden usar para hosts específicos, ya que el 0 (192.168.10.0) identifica a la red y el 255 (en este caso, el mayor numero que se puede representar en binario con prefijo 24: 192.168.10.255) identifica a todos los hosts para el proceso de multidifusión. Excluyendo esas dos IP, las otras 254 se puede utilizar para los hosts (por ejemplo 192.168.10.45).

