Taller 2:

1.) Explique las estrategias de transición que se analizaron en clases.

En la actualidad existen miles de millones de dispositivos que utilizan IPv4. Así que pensar en una migración simultánea de IPv4 a IPv6 de todos estos dispositivos es inviable. En algunos casos, aunque se quiera migrar a IPv6, los dispositivos o el software pueden no admitir IPv6 o no tener soporte adecuado para IPv6. Por lo que la migración de IPv4 a IPv6 requerirá años incluso décadas. Entre estas destacamos 3 cosas buenas de esto: Pilas duales IPv4/IPv6, Túneles y Conversión entre IPv4 e IPv6 por medio de NAT-PT.

2.) Aplicaciones del protocolo H.323 , donde es usado comunmente.

H.323 es utilizado comúnmente para Voz sobre IP (VoIP, Telefonía de Internet o Telefonía IP) y para videoconferencia basada en IP. Es un conjunto de normas (recomendación paraguas) ITU para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP. No garantiza una calidad de servicio, y en el transporte de datos puede, o no, ser fiable; en el caso de voz o vídeo, nunca es fiable.

3.) ¿Existirá alguna vez la “killer application” para IPv6?, explique.

Las principales razones para que existirá “killer app” en IPv6, han sido ganar un espacio de direcciones más grande y evitar la obsolescencia tecnológica. Ha habido varias aplicaciones que pensamos que serían “killer app” para IPv6. Estos incluyen IPSec , Mobile IPv6 , Microsoft Three Degrees , Microsoft Direct Access y redes de sensores habilitadas con Stateless Address Auto-Configuration (SLAAC) . Sin embargo, estas tecnologías y productos no se han popularizado o no se han implementado rápidamente. Continúa la búsqueda de la única cosa que impulsará la rápida adopción de IPv6.

4.) Funcionalidad DNS-ALG, FTP-ALG (ejemplos)

- Permite que las aplicaciones cliente utilicen puertos TCP / UDP dinámicos para comunicarse con puertos conocidos usados por las aplicaciones de servidor, incluso si la configuración del firewall permite el tráfico a través de sólo un número limitado de puertos. Sin un ALG, los puertos serían bloqueados o el administrador de la red tendrían que abrir una gran cantidad de puertos en el firewall, provocando un debilitamiento de la red y permitiendo potenciales ataques en esos puertos.
- Reconoce comandos específicos de aplicación y ofrece controles de seguridad sobre ellos.
- Puede convertir la información de direccionamiento de la capa de red que se encuentra en la carga útil (payload) de la aplicación.
- Sincroniza múltiples flujos o sesiones entre hosts.

Ejemplo de DNS-ALG:

Solicitar un dominio al servidor DNS a una pasarela que va a descodificar su envío en términos de protocolo, y a continuación lo va a recodificar en IPv6 indicando como destino el servidor DNS del destinatario en IPv6.

Ejemplo de FTP-ALG:

Cuando vayamos a descargar archivos de un repositorio.