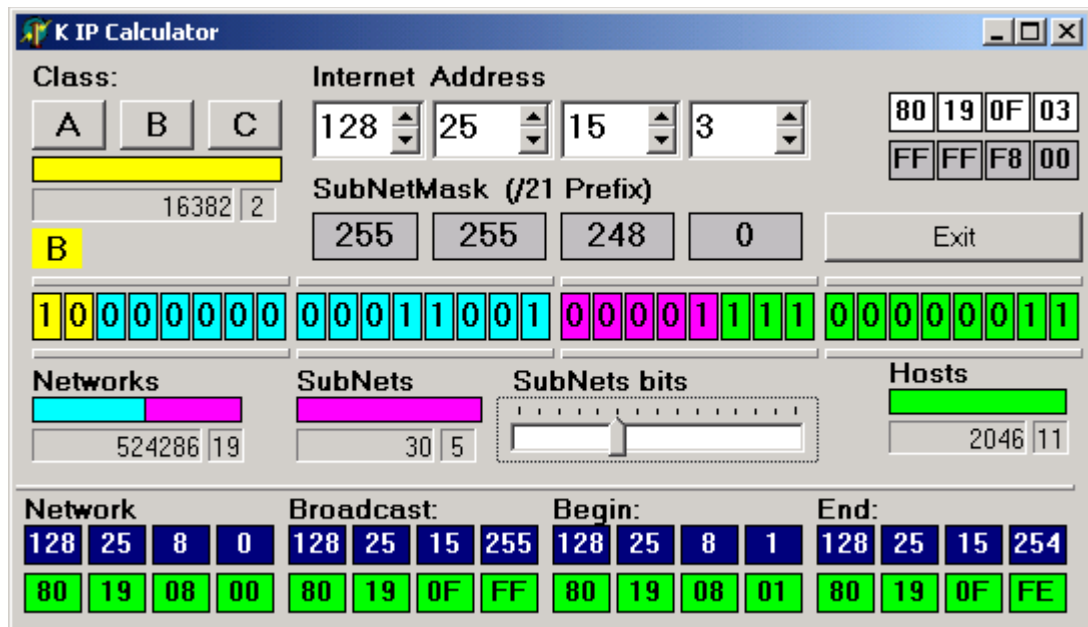


RAL 6_3: Calculadora IP, TCP/UDP Puertos, Firewall, FTP/Telnet/RSH, Protocolos de Microsoft, Simbología CISCO y Simulación de Redes

TCP/IP, Puertos:

1. Abra el programa Calculadora IP (KIPCalculator.exe) e identifica cada uno de los elementos de la ventana del programa:



2. Usando la calculadora IP resuelva los problemas del boletín RAL6_1
3. Una empresa tiene reservado el rango 192.168.5.0 – 192.168.5.255 para nuestra delegación y deseamos crear 5 subredes. Determine la máscara/máscara de red a usar y las direcciones de las subredes, así como las direcciones que podremos usar para los nodos dentro de cada subred.
4. Consultando Wikipedia determine:
 - ¿Cuál es la utilidad de emplear subredes?
 - ¿Cómo pueden conectarse dos subredes entre sí?
5. Repasa tus conocimientos de IP leyendo el resumen disponible en <http://gsyc.escet.urjc.es/docencia/asignaturas/redes/transpas/node5.html> y completando correctamente las siguientes frases:
 - El campo TTL indica el número máximo de que el datagrama puede atravesar (hubs, switches, routers, pasarelas)
 - Para ver la tabla de encaminamiento podemos ejecutar el comando -nr

- Las siglas ICMP corresponden a las siglas y se usa para entre máquinas.
 - La orden ping está asociada al protocolo
 - Las siglas NAT hacen referencia a que básicamente consiste en convertir IP en IP
6. Repasa tus conocimientos de UDP y TCP leyendo el resumen disponible en <http://gsync.escet.urjc.es/docencia/asignaturas/redes/transpas/node6.html> y <http://gsync.escet.urjc.es/docencia/asignaturas/redes/transpas/node7.html> y completando correctamente las siguientes frases:
- UDP es un protocolo que implementa un nivel de transporte..... orientado a conexión yfiable. (Sí/No)
 - TCP es un protocolo que implementa un nivel de transporte orientado a conexión yfiable. (Sí/No)
 - Si una máquina multiprocesos con IP 199.199.199.199 ejecuta simultáneamente un cliente web (Internet Explorer) y un programa de correo (Outlook Express), de forma que ambas aplicaciones realizan una comunicación con el servidor (servidor de correo y Web) con IP 191.191.191.191, la capa de transporte gracias a los..... puede asociar cada flujo de comunicación de cada aplicación con el proceso correspondiente.
 - El puerto 7 TCP y el 7 UDP son puertos (iguales /distintos)
 - La unidad de datos de TCP suele denominarse
 - Los números de secuencia del protocolo TCP numeran (bytes/segmentos).
 - Para coordinar el envío de segmentos y asentimientos se emplea la técnica de
 - Si en un segmento el bit SYN está a uno indica que estamos en fase de
 - Si en un segmento el bit FIN está a uno indica que estamos en fase de
7. ¿Qué se obtiene de la ejecución del comando **netstat -no**? ¿Qué nos indica el campo PID?
8. Descarga la aplicación de administración **TCPView** <http://www.microsoft.com/technet/sysinternals/Utilities/TcpView.msp>. Instale y observe qué procesos están asociados a qué conexiones de transporte, y las operaciones que puede realizar con dicha aplicación, ¿Cuáles son los posibles

estados de un puerto y qué significan? ¿Para qué podría servir esta aplicación desde el punto de vista de la seguridad?

FIREWALLS

9. Como sabes, los **requisitos mínimos-mínimos de seguridad** en cualquier máquina son:

- Tener **actualizado el sistema operativo y las aplicaciones**, con al menos, los Service Pack correspondientes y las actualizaciones críticas de seguridad.
- Un **antivirus (Anti-malware) actualizado** y adecuadamente configurado.
- Realización de **copias de seguridad**, adecuadamente planificadas.
- **Cortafuegos** o firewall adecuadamente configurado (local y/o de red).

Aunque se desarrollará el tema de la seguridad en el tema 9 ahora podemos resumir que, un cortafuegos (o firewall), definido en la RFC 2979, es **un elemento de hardware o software** utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Los Firewall se pueden clasificar según su tecnología en :

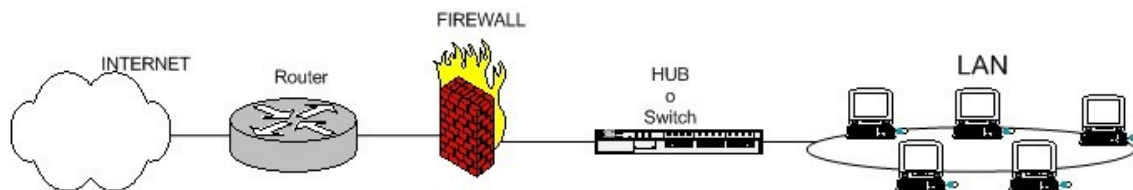
- **Filtros de paquetes:** (Nivel 3 y 4) Filtra por direcciones IP origen/destino y puertos TCP/UDP origen/destino.
 - PROS: Independencia de las aplicaciones. Son muy rápidos y escalables
 - CONTRAS: Menor nivel de seguridad. No examinan el tráfico ni entienden el contexto.
- **Proxy de aplicación** (Nivel Aplicación) No permiten tráfico entre las dos redes, si no es mediante un **proxy a nivel de aplicación**.
 - PROS: Alto nivel de seguridad. Examinan información a nivel de aplicación. Toman decisiones basadas en datos de cada aplicación
 - CONS: Menor rendimiento y escalabilidad. Rompe el modelo cliente/servidor (requiere dos conexiones).
- **Inspección de estados (statefull inspection)** (Varios niveles) Realizan filtros en base a las cabeceras, el paquete se intercepta a nivel de red, pero extrae información de los datos para analizar en función de la aplicación.
 - PROS: Alta seguridad, velocidad y escalabilidad. Inspecciona los datos a nivel aplicación.
 - CONS: No se rompe la conexión totalmente.
- **Híbridos:** Incorporan mezcla de varias tecnologías anteriores.

Según la ubicación y el uso los cortafuegos los podemos clasificar en:

- **Personales.** Software utilizables en PC en LAN, Modem, ADSL...
- **Cortafuegos para pequeñas oficinas:** Suelen ser pequeños equipos instalados antes del router o integrados en éste. Muy utilizable para el acceso con ADSL (3-50 usuarios).

- **Cortafuegos corporativos:** Ubicados en el punto central de accesos a Internet de una empresa mediana-grande. Suelen ser software que se instala en grandes servidores con configuraciones tolerantes a fallos o equipos (hardware) dedicados.

Abajo aparece el esquema típico de firewall para proteger una red local conectada a Internet a través de un router. El firewall debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN)



Clasifique los siguientes firewalls conforme la clasificación anterior, indicando además si se trata de un producto hardware o software, y si es software sobre qué sistema operativo puede ser instalado:

- **Isa Server**
 - **Kerio**
 - **Zone Alarm**
 - **Cisco PIX**
 - **Firestarter**
 - **Checkpoint Firewall-1**
10. **Windows XP SP2** cuenta con un Firewall Personal. Lee el artículo técnico de Microsoft en <http://www.microsoft.com/spain/empresas/seguridad/articulos/cfgfwall.msp> y determina como es posible (Captura las pantallas). Recuerde que deberá usar un usuario administrador de la máquina:
- Habilitar/deshabilitar el Firewall.
 - Habilitar/deshabilitar las notificaciones cada vez que el firewall bloquee un acceso.
 - Permitir el acceso a la red a la aplicación de Escritorio Remoto a los equipos de mi subred. (Excepciones)
 - Abrir el puerto de FTP (Excepciones).
 - Configura el Firewall de forma que su equipo no responda a los comandos ping. (ICMP)
 - Restaure los valores por defecto.
11. **Iptables** es una aplicación en línea de comandos que gestiona el filtrado de paquetes en sistemas **Linux** (kernels 2.4.x), en base a las reglas que hayamos definido. Usando la ayuda (**man**) del terminal de comandos de **Guadalinex 2004** determine que efecto produciría la ejecución del siguiente comando (como root):

```
/sbin/iptables -I INPUT -p tcp --destination-port 6881:6889 -j ACCEPT
```

12. Accede a la simulación de configuración del router DI604 en http://support.dlink.com/emulators/di604_reve/ y verifica si dicho router posee la función de firewall incorporada. Si es así, crea una regla para filtrar (denegar) todo lo que provenga desde Internet (WAN) destinado a cualquier equipo de la LAN y accedan por los puertos TCP del 8000 al 9000, durante las horas de trabajo (Captura pantalla)

Cientes FTP, TELNET,...

13. Usando Wikipedia, determina:

- ¿Qué es FTP, para qué sirve?
- ¿En qué nivel de OSI lo situarías?
- ¿Qué puerto está asociado a FTP?
- ¿Qué tipos de transferencia existen?
- Observa la lista de comandos de FTP, ¿Qué comando nos permite cambiar de directorio en el ordenador remoto?
- Observa la lista de comandos de FTP, ¿Qué comando nos permite cambiar de directorio en el ordenador local?
- Para mejorar la seguridad, ¿qué protocolo de aplicación debe usarse en lugar de ftp y telenet?

14. Desde el terminal de comandos de Windows XP y empleando el comando ftp conéctese un ordenador de la Universidad de Helsinki (Finlandia) llamado (o con alias) ftp en el dominio funet.fi. A continuación copia el archivo README que se encuentra en la carpeta /pub a tu disco duro.

* Quizás, si todo está adecuadamente configurado el Firewall de Windows XP SP2 te impedirá por defecto usar el puerto de FTP, deberás abrir el puerto para ello ir al Firewall/Opciones avanzadas/ Conexión de red/Configuración localiza Servidor de FTP y Modifica añadiendo la IP del servidor.

15. Busca y descarga la aplicación WS_FTP y conéctate al servidor FTP de la Universidad de Buenos Aires (<ftp.ccc.uba.ar>), y descarga en tu disco duro el archivo README.txt

16. Realiza la operación anterior empleando un navegador Web (Firefox o Internet Explorer).

17. Consultando la de soporte técnico de Microsoft (<http://support.microsoft.com/>) determina cómo es posible usar el navegador Web como cliente de FTP en caso de que exista un usuario y una clave (Acceso no anónimo).

18. Ya has visto que es posible usar Windows XP como cliente de FTP, ahora usando la página de recursos técnicos de Microsoft determina si es posible usar un PC con Windows XP como servidor FTP. (IIS)

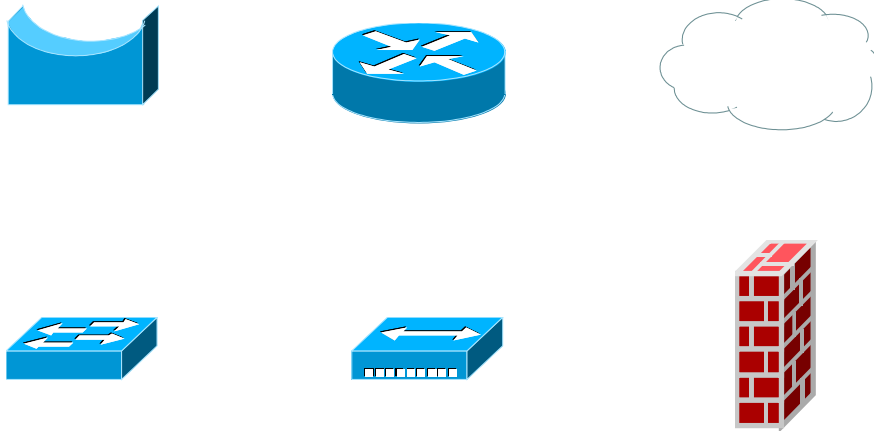
19. Preguntar lo que no se sabe a alguien más experto y de confianza, es una fuente importante del administrador de sistemas. Emplea el foro técnico de Microsoft en España, ver sitio Web <http://forums.microsoft.com/TechNet-ES>, para determinar si es seguro instalar un servidor telnet en un equipo con Windows XP, en caso negativo indique cual puede ser una alternativa para establecer una sesión remota con Windows XP.

20. ¿Qué es telnet (TELEtype NETwork)?

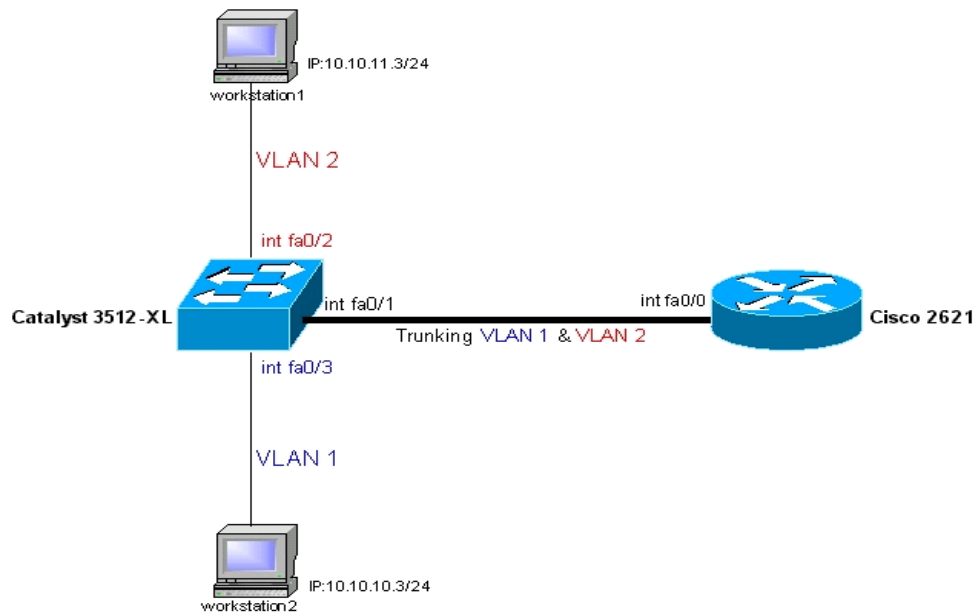
21. ¿Qué puerto usa Telnet? ¿TCP o UDP?
22. En un PC (PC1) con Windows XP crea un nuevo usuario en un equipo (usu/usu) e inicia el servicio telnet. Desde otro PC (PC2) abre una sesión de telnet y conéctate a este equipo y crea un directorio de nombre REMOTO en el disco duro del PC remoto (PC1).
23. La aplicación telnet es usada frecuentemente para la configuración remota por lenguaje de comandos de equipos de interconexión de redes (switchs, routers,...). Conéctese vía telnet al Switch de la clase y observa su configuración (pregunta al profesor un usuario y clave válidos).
24. Conéctate usando telnet a alguno de los servidores telnet que aparecen en la listas <http://www.telnet.org/htm/places.htm> o en http://conecta2.thebbs.org/pucela_bbs/listabbs.htm
25. ¿Para qué sirve el comando rsh? ¿y el comando rexec?
26. ¿Dispone Windows XP del servicio rexec?
27. Arranca un computador con Guadalinex (usu/usu), y desde un PC con Windows XP crea una carpeta llamada REMOTA en /home/usuario. Nota: usa rsh o rexec.
28. ¿Qué es rshsvc.exe?

DIAGRAMAS DE REDES CISCO

29. Abre el documento “ELEMENTOS GRAFICOS PARA DIAGRAMAS DE RED DE CISCO” (CISCO_ico.ppt) e identifica los siguientes elementos de red:



30. Empleando DIA (o Visio) y observa los diferentes elementos para realización de diagramas de Cisco. Usando esta herramienta cree el siguiente diagrama: (Recuerde que DIA es software libre disponible tanto para Windows como para Linux, además



es un software incluido en Guadalinex).

PROTOCOLOS DE REDES MICROSOFT

31. ¿Qué protocolos de transporte pueden utilizarse para crear una red con equipos con S.O. de Microsoft?
32. ¿Puede crearse una red Microsoft sin utilizar el protocolo TCP/IP?
33. ¿Cuál es el conjunto de protocolo típicos en una LAN Novell?
34. ¿A qué nivel OSI situaría NETBIOS?
35. ¿Qué es NETBEUI? ¿A que nivel OSI lo situarías?
36. Consultando la base de conocimiento de Microsoft determina de qué habla el artículo técnico 301041, ¿Qué conclusión obtiene de la lectura de este artículo?
37. ¿Permite encaminar Netbeui? ¿Qué protocolo sustituyó a NETBEUI?

SIMULACIÓN DE REDES

38. Instale el simulador de redes Packet Tracer y realice el Lab 5.1.13b