********** RESUMEN DE ÓRDENES PARA CONFIGURACIÓN DE RED EN EQUIPOS UNIX (disponibles en NetGUI) **********

ifconfig -a	Muestra las interfaces de red e IPs
ifconfig <interfaz> <dirIP> netmask <máscara> Ej.: ifconfig eth0 10.0.0.1 netmask 255.255.255.0	Configura la dirección IP a <interfaz>
ifconfig <interfaz> [up|down] Ej.: ifconfig eth0 up	Inicia o Para <interfaz>. Equivalente a (ifup/ifdown <interfaz>)
ifconfig <interfaz> [promisc|-promisc] Ej.: ifconfig eth0 -promisc	Activa/desactiva el modo promiscuo en <interfaz>
ip [-6] addr show [interfaz]	Muestra información detallada sobre todas las interfaces o sólo sobre <interfaz> (-6 = **IPv6**).
ip addr add <dirIPv4/máscara> dev <interfaz> broadcast + Ej.: ip addr add 10.0.0.1/24 dev eth0 broadcast +	Añade la dirección <dirIPv4> a <interfaz> con máscara (CIDR)
ip addr add <dirIPv6/prefijo> dev <interfaz> Ej.: ip addr add 2002:c000:0203::1/16 dev eth0	Añade la dirección **IPv6** a <interfaz> con dirIPv6 y prefijo (CIDR)
ip addr del <dirIP/máscara> dev <interfaz> Ej.: ip addr del 10.0.0.1/24 dev eth0	Elimina una dirección IPv5 (ó v6) a <interfaz>. Con ifconfig esto no se puede hacer.
ip link set <interfaz> { up | down | arp { on | off } } Ej.: ip link set eth0 up Ej.: ip link set eth0 down	Inicia (up), para (down), activa o desactiva (arp on|off) el flag NOARP de <interfaz> Inicia (o activa) la interfaz eth0 Para (o desactiva) la interfaz eth0
ip [-6] route show	Muestra la tabla de encaminamiento (-6=**IPv6**).
ip neigh show	Muestra la caché de vecinos (“arp -a”).
ip [-6] route add <dirIP/máscara> via <gateway> **ip [-6] route add default via <gateway>** Ej.: ip route add 12.0.0.0/24 via 10.0.0.1 Ej.: ip route add default via 10.0.0.2 Ej.: ip -6 route add 2001:db8:100::/48 dev eth0 metric 1	Añade una ruta a una red o host (IPv4/**IPv6** y máscara en formato CIDR) y también ruta por defecto.
ip [-6] route del <dirIP/máscara> via <gateway> **ip [-6] route del default via <gateway>** Ej.: ip route del 12.0.0.0/24 via 10.0.0.1 Ej.: ip route del default via 10.0.0.2 Ej.: ip -6 route del 2001:db8:100::/48 dev eth0 metric 1	Borra una ruta a una red o host (IPv4/**IPv6** y máscara en formato CIDR) y también ruta por defecto.
ifup <interfaz>, ifdown <interfaz> Ej.: ifup eth0	Inicia (ifup) ó Para (ifdown) la <interfaz> de acuerdo con /etc/network/interfaces
arp -a	Muestra la tabla ARP
arp -d <máquina> Ej.: arp -d 172.20.0.1	Elimina la entrada de la tabla ARP correspondiente a <máquina>
route	Muestra la tabla de encaminamiento
route add [-net|-host] dirIP [opciones] **route add default gw <gateway> [opciones]** Ej.: *route add -net 10.0.0.0 netmask 255.0.0.0 gw 10.0.0.9* Ej.: *route add default gw 10.0.0.1*	Añade una ruta a una red o host o una ruta por defecto. Opciones: máscara de subred (netmask), puerta de enlace (gw), interfaz (dev) y métrica (metric).
route del [-net|-host] dirIP [opciones] **route del default gw <gateway> [opciones]** Ej.: *route del -net 10.0.0.0 netmask 255.0.0.0 gw 10.0.0.9* Ej.: *route del default gw 10.0.0.1*	Borra una ruta a una red o host o una ruta por defecto. Opciones: máscara de subred (netmask), puerta de enlace (gw), interfaz (dev) y métrica (metric).
netstat -a	Muestra las conexiones de red entrantes y salientes
netstat -nr	Muestra la tabla de encaminamiento
netstat -i	Muestra estadísticas del protocolo de red
netstat –sp tcp|udp	Muestra estadísticas del protocolo tcp/udp
netstat -ntlu6	Procesos servidores que utilizan IPv6 (en Windows **netstat –anop TCPv6|UDPv6)**

lsof -Pni	Muestra los puertos asociados a los servicios *daemon* en ejecución: -i Lista los sockets -n No resuelve nombres de máquina (no DNS) -P No resuelve números de puerto (services)
ping [opciones] [salto1 salto2 ...] <destinatario> Ej.: ping -c 2 -s 250 -i 5 ftp.rediris.es	Comprueba la alcanzabilidad de un destinatario a partir de su dirección IP o nombre. En el ejemplo comprueba la alcanzabilidad de la máquina ftp.rediris.es enviando dos solicitudes ICMP de eco (-c 2) de un tamaño de 250 bytes (-s 250) y con una espera de 5 segundos entre cada una (-i 5).
ping6 [opciones] <destinatario> Ej.: ping6 2001:db8:100:100:214:22ff:feaa:aa22 Ej.: ping6 -I eth0 fe80::214:22ff:feaa:aa22	Comprueba la alcanzabilidad de un destinatario con IPv6. En caso de direcciones IPv6 locales es necesario utilizar -I <interfaz> por la que enviar los mensajes (una máquina podría tener en distintas interfaces vecinos con la misma IPv6 local de enlace).
traceroute [opciones] <destinatario> [tamaño] Ej.: traceroute -n -u ftp.rediris.es	Muestra la ruta seguida para alcanzar el destinatario a partir de su dirección IP o nombre.
telnet <máquina> [puerto] Ej.: telnet www.usal.es 80	Realiza una conexión TCP al puerto [puerto] en <máquina>. Si no se especifica [puerto] por defecto coge el 23 (telnetd).
nslookup [nombre/dirIP] Ej.: nslookup roble.usal.es Ej.: nslookup 212.128.144.90 Ej.: nslookup –type=ANY ipv6.l.google.com	Realiza resoluciones de DNS en modo interactivo o en línea de órdenes. Preferible dig o host. Con la opción –type=ANY resuelve todo tipo de direcciones (incluidas IPv6).
dig [opciones] <nombre/dirIP> Ej.: dig informatica.usal.es Ej.: dig -t AAAA ipv6.l.google.com Ej.: dig informatica	Realiza resoluciones directas/inversas de DNS. La opción -6 –t AAAA es para registro de recursos de direcciones IPv6. Para resolver nombres sin sufijo se requiere en el fichero $HOME/.digrc la siguiente clave: +domain=usal.es
host [opciones] <nombre/dirIP> Ej.: host roble.usal.es Ej.: host 212.128.144.90 Ej.: host –t AAAA ipv6.l.google.com	Realiza resoluciones directas/inversas de DNS. Con la opción –t AAAA resuelve direcciones IPv6
wget [opciones] <url> Ej.: wget informatica.usal.es/descargas/software-base.sh Ej.: wget --no-check-certificate https://diaweb.usal.es	Descarga de forma no interactiva recursos de la web (http, https y ftp). Por defecto usa http. Soporta proxies.
dhclient [-4|-6] [opciones] Ej.: dhclient -s <ip_servidor_dhcp> Ej.: dhclient -r	Programa cliente DHCP (compatible IPv4 e IPv6) que se apoya en /etc/network/interfaces. Dirige las peticiones al DHCP especificado Libera la IP que nos ha concedido el DHCP
tail [opciones] <fichero> Ej.: tail -f /var/log/syslog Ej.: tail -20 /var/log/daemon.log	Muestra las últimas líneas de <fichero>. Muestra las últimas 10 líneas y continua con las líneas incorporadas en syslog (log del sistema (-F para logs rotativos). Muestra las últimas 20 líneas del log daemon.

********** SNIFFERS **********

cd X/linux **./arranca_tcpdump**	Inicia tcpdump en el Fedora del laboratorio (ejecutar desde un terminal). En casa simplemente ejecutar “tcpdump”
Ej.: tcpdump -i eth0 -s 0 -w /hosthome/r1.cap	Captura paquetes completos por eth0 y lo guarda en “/hosthome/r1.cap”.
Ej.: tcpdump ip proto \\udp	Captura paquetes udp
Ej.: tcpdump ip broadcast	Captura paquetes de difusión
Ej.: tcpdump ip multicast	Captura paquetes de difusión multicast
Ej.: tcpdump ether proto \\arp	Captura tramas ARP (preguntas y respuestas)
Ej.: tcpdump ether broadcast	Captura tramas de difusión
Ej.: tcpdump ether multicast	Captura tramas de difusión multicas
Ej.: tcpdump tcp and port 80	Captura el tráfico web
Ej.: tcpdump tcp and \(port 22 or port 23\)	Captura el tráfico de telnet y ssh
cd X/linux **./arranca_wireshark**	Inicia wireshark en el Fedora del laboratorio (ejecutar desde un terminal). En casa simplemente ejecutar “wireshark”
Ej.: wireshark r1.cap	Abre el entorno gráfico de wireshark con el fichero de captura “r1.cap”.

********** NetGUI: UTILIDADES **********

cd X/linux **./arranca_netgui**	Secuencia de órdenes que inicia NetGUI en el Fedora del laboratorio. En casa simplemente ejecutar “netgui.sh”. Con la opción “regenera” reinstala netgui en las aulas: cd X/linux ./arranca_netgui regenera
clean-netgui.sh	Shell script que limpia el entorno de NetGUI. Ejecutar si ha habido ejecuciones previas o terminaciones abruptas.
clean-vm.sh <máquina>	Shell script que termina abruptamente la ejecución de la máquina virtual <máquina> del escenario cargado en NetGUI. A continuación ejecutar “clean-netgui.sh”
for MV in `$NETKIT_HOME/bin/vlist | awk '{ print $2; }' \| sed '1d' \| sed '$d' | sed '$d' \| sed '/^$/d'`; do clean-vm.sh $MV; done	Combinación de órdenes que termina abruptamente todas las máquinas virtuales del escenario. Requiere la variable de entorno NETKIT_HOME apuntando a la carpeta de instalación de NetKIT (/usr/local/netkit).
./reset-lab [nombre-máquina] Ej.: ./reset-lab pc1	Shell script que retorna todo un escenario a su situación inicial o sólo la máquina <nombre-máquina>. Se pierden todos los cambios de configuración que se hubieran hecho dentro de la/s máquina/s. Esta Shell está dentro de la carpeta del escenario en cuestión.

********** NetGUI: ESCENARIOS **********

halt	Termina ordenadamente la ejecución de una máquina virtual de NetGUI.
reboot	Termina y arranca de nuevo una máquina virtual. Los cambios que se hicieran en los ficheros de la máquina virtual se mantienen.
/hosthome	Carpeta de intercambio de archivos entre las máquinas virtuales de NetGUI y el host anfitrión. **Enlaza con la carpeta HOME del usuario que ha ejecutado NetGUI (/home/usuario ó /root).** Ejemplo de uso: pc1:~# tcpdump -s 0 -w /hosthome/r1.cap
/hostlab	Carpeta de intercambio de archivos entre las máquinas virtuales de NetGUI y el host anfitrión. **Enlaza con la carpeta donde reside el escenario de NetGUI** en el host anfitrión (en las aulas **/redesII/escenario**).

********** SERVICIO DE RED **********

/etc/init.d/networking restart	Reinicia, inicia o para los servicios de red y borra la configuración del proxy ARP de un router. En caso de restart (o start) es necesario previamente parar las interfaces afectadas con “ifconfig eth0 down”
Ficheros de configuración:	
a) /etc/hosts	Asocia direcciones IPv4/IPv6 con un nombre
a.1) Direcciones locales:	127.0.0.1 localhost 127.0.1.1 mydebian ::1 ip6-localhost ip6-loopback fe00::0 ip6-localnet ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip6-allrouters
b) /etc/network/interfaces	Configuración de las interfaces de red
b.1) Interfaz eth0 con IP dinámica:	auto eth0 iface eth0 inet dhcp
b.2) Interfaz eth1 con IP fija e indicaciones para el inicio y parada:	auto eth1 iface eth1 inet static address 192.168.0.101 # dirección IP network 192.168.0.0 # dirección de la subred netmask 255.255.255.0 # máscara de la subred broadcast 192.168.0.255 # dirección de difusión (opcional) up route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.2 up route add default gw 192.168.1.200 # o bien: gateway 192.168.0.1 down route del default gw 192.168.1.200 down route del -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.2
b.3) Interfaz eth2 con IPv6 fija:	auto eth2 iface eth0 inet6 static address 2002:c000:0203::1 netmask 16
Logs afectados	/var/log/syslog

********** SERVICIO DE DNS **********

/etc/init.d/bind restart	Reinicia, inicia o para el servicio de DNS (bind9). Se puede revisar la sintaxis de los archivos de configuración con los programas: named-checkconf y named-checkzone. Ej.: named-checkconf /etc/bind/named.conf Ej.: named-checkzone localhost /etc/bind/db.local
Ficheros de configuración:	
a) /etc/bind/named.conf	Fichero con la configuración general del servidor de DNS (dominios maestro, esclavo, etc.) y ficheros que contienen los mapas de dominio.
b) /etc/bind/db.root	Fichero con las direcciones IP de los servidores del dominio raíz.
c) /etc/bind/named.conf.local	Fichero de configuración para incluir dominios locales.
d) /etc/bind/db.*	Ficheros con los mapas de dominio (resolución directa e inversa).
e) /etc/resolv.conf	Fichero con los DNS primario y secundarios de un computador (también en todo cliente).
Logs afectados	/var/log/syslog, /var/log/daemon.log

********** SERVICIO DE DHCP **********

/etc/init.d/dhcp3-server restart	Reinicia, inicia o para el servicio del servidor DHCP (dhcp3-server).
Ficheros de configuración: a) /etc/dhcp3/dhcpd.conf	Fichero con la sección de configuración genérica y secciones de tipo subnet (rangos de cesión) y host (cesión a una máquina en particular).
b) /etc/default/dhcp3-server	Fichero con las interfaces en las que se actúa como servidor DHCP
Logs afectados	/var/log/syslog, /var/log/daemon.log /var/lib/dhcp3/dhcpd.leases (direcciones IP cedidas en todo momento)

********** SERVICIO DE ENCAMINAMIENTO **********

/etc/init.d/quagga restart	Reinicia, inicia o para el servicio *quagga* de gestión de tablas de encaminamiento según diversos protocolos (RIP y OSPF).
telnet localhost ripd	VTY del daemon ripd
show ip rip	Tabla de encaminamiento según protocolo RIP
telnet localhost ospfd	VTY del daemon ospfd
show ip ospf route	Tabla de encaminamiento según protocolo OSPF
show ip ospf neighbor	Vecinos que conoce el router (OSPF)
show ip ospf database router	Base de datos del Router Link States (OSPF)
show ip ospf database network	Base de datos del Network Link States (OSPF)
show ip ospf database summary	Resumen de la base de datos (OSPF)
Ficheros de configuración:	
a) /etc/quagga/daemons	Configuración genérica y protocolos activados
b) /etc/quagga/ripd.conf	Configuración de RIP
c) /etc/quagga/ospfd.conf	Configuración de OSPF
Logs afectados	/var/log/syslog, /var/log/daemon.log, /var/log/quagga /var/log/ripd.log ó /var/log/ospfd.log

********** SERVICIO CONFIGURACIÓN AUTOMÁTICA DE DIRECCIONES IPv6 **********

/etc/init.d/radvd restart	Reinicia, inicia o para el demonio radvd.
Ficheros de configuración:	
a) /etc/sysctl.conf	Fichero con los parámetros de configuración del kernel que se carga en el arranque. Para IPv6 se requiere "net.ipv6.conf.all.forwarding=1". Cualquiera de estos cambios también se pueden realizar escribiendo directamente sobre los archivos en el directorio /proc/sys, por ejemplo: `echo 1 > /proc/sys/net/ipv6/conf/all/forwarding` Para cargar una nueva configuración sobre el kernel en ejecución se usa la orden: sysctl –a.

b) /etc/radvd.conf	Fichero de configuración del demonio radvd. Campo prefix requerido.
	
	Ejemplo:
	interface eth0 {
	AdvSendAdvert on;
	MinRtrAdvInterval 3;
	MaxRtrAdvInterval 10;
	prefix 2001:0db8:0100:f101::/64 {
	AdvOnLink on;
	AdvAutonomous on;
	AdvRouterAddr on;
	};
	};

Logs afectados	/var/log/syslog, /var/log/kern.log, /var/log/daemon.log

********** SERVICIO DEL SUPERSERVIDOR INETD **********

/etc/init.d/inetd restart	Reinicia, inicia o para el superservidor inetd.
Ficheros de configuración:	
a) /etc/inetd.conf	Fichero de configuración con los servicios gestionados por inetd.
b) /etc/services	Correspondencia entre servicios, puertos y protocolo transporte
Logs afectados	/var/log/syslog, /var/log/daemon.log

********** RESUMEN DE ÓRDENES PARA DIAGNÓSTICO/CONFIGURACIÓN DE RED EN EQUIPOS WINDOWS **********

ipconfig /all	Muestra información sobre todas las interfaces de red (con todo detalle)
route print	Muestra información sobre la tabla de encaminamiento
route add <destino> mask <máscara> <pasarela> metric <n> if <n> Ej.: route add 10.0.0.0 mask 255.0.0.0 10.0.0.9 metric 3 if 2	Añade una ruta al destino (red/host). Opciones: máscara de subred (mask), puerta de enlace (pasarela), interfaz (if) y métrica (metric).
route delete <destino> Ej.: route delete 10.0.0.0	Borra una ruta a una red o host.
netsh interface ipv6 show interface [numinterfaz]	Muestra información sobre todas las interfaces de red o una en particular
netsh interface ipv6 show neighbors [numinterfaz]	Muestra la caché de vecinos de todas las interfaces de red o una en particular
netsh interface ipv6 show route	Muestra la tabla de encaminamiento
netsh interface ipv6 add address	Agrega una ruta IPv6 en una interfaz
netsh interface ipv6 add route	Agrega una ruta IPv6 sobre una interfaz
ping destinoIPv4	Comprueba la alcanzabilidad de un destinatario con IPv4.
ping6 destinoIPv6%interfaz	Comprueba la alcanzabilidad de un destinatario con IPv6.
tracert [-d] [-h saltos] [-j hosts] [-w tiempo] destinoIPv4	Muestra la ruta seguida para alcanzar un destinatario con IPv4
tracert6 [-d] [-h saltos] [-j hosts] [-w tiempo] destinoIPv6	Muestra la ruta seguida para alcanzar un destinatario con IPv6
netstat -an	Muestra las conexiones de red entrantes y salientes con los números de puerto y direcciones en formato numérico (
netstat –p <proto>	Muestra conexiones del protocolo "proto", que puede ser TCP, UDP, TCPv6 o UDPv6.
netstat -r	Muestra la tabla de encaminamiento
netstat -s	Muestra estadísticas del protocolo de red
netstat –o	Muestra el identificativo de proceso asociado con cada conexión
netstat –b	Muestra el ejecutable que crea cada conexión o puerto de escucha
Algunos ejemplos combinados: Ej.: netstat –anobp TCP Ej.: netstat –anobp UDP Ej.: netstat –anobp TCPv6 Ej.: netstat –anobp UDPv6	Ejemplos combinados que muestran: [-a] conexiones de red entrantes y salientes [-n] puertos y direcciones en formato numérico [-o] identificativo de proceso asociad [-b] Muestra el ejecutable [-p proto] filtra por el protocolo <proto>
nslookup [–opcion] <máquina> Ej.: nslookup roble.usal.es Ej.: nslookup 212.128.144.90 Ej.: nslookup –type=any ipv6.l.google.com	Realiza resoluciones directas/inversas de DNS. Con la opción –type=any resuelve direcciones IPv6.