

Curso Linux

UNIDAD V

[Unidad V@presentación]#

- 5.1 Configuración de la red
- 5.2 Firewall (IPTABLES), Proxy y enrutamiento
- 5.3 Herramientas de administración y monitoreo (SNMP, sniffers)

[Redes@Unidad V]\$

- Las redes de computadoras surgieron de la necesidad de compartir recursos informáticos como impresoras, unidades de cinta, etc., para posteriormente compartir información.
- Linux es un SO diseñado desde sus orígenes para permitir la conectividad entre diferentes máquinas al contrario de Windows.

[Redes@Unidad V]\$

- Linux nació con los protocolos TCP/IP inmersos en él, y dado que estos protocolos forman parte de Internet, Linux provee de buena manera servicios de Internet.
- Linux implementa los protocolos del modelo OSI.
- Direcciones físicas (direcciones MAC) y direcciones lógicas (direcciones IP)

[Redes@Unidad V]\$

- IP es una dirección de 32 bits separadas en 4 bytes y representadas en notación decimal:
 - 148.208.209.4
- Direcciones especiales divididas en 5 clases A, B, C, D y E.
- Las direcciones D y E no se pueden utilizar por que están reservadas para multicast y reservadas para su uso futuro.

[Redes@Unidad V]\$

- A 1.0.0.0 - 127.255.255.255
 - B 128.0.0.0 - 191.255.255.255
 - C 192.0.0.0 - 223.255.255.255
 - D 224.0.0.0 - 239.255.255.255
 - E 240.0.0.0 - 255.255.255.255
-
- Existen dos tipos de direcciones IP: públicas y privadas. Las direcciones privadas no tienen salida

[Redes@Unidad V]\$

- Clase A: 10.0.0.0 a 10.255.255.255
- Clase B: 172.16.0.0 a 172.31.255.255
- Clase C: 192.168.0.0 a 192.168.255.255

- Internet es una red de conmutación de paquetes, por lo tanto no existe una conexión física permanente (circuito dedicado) y los paquetes para llegar a su destino pueden seguir diversos caminos dependiendo de las rutas asignadas por el ruteador.

[Redes@Unidad V]\$

- El espacio de direcciones de 32 bits se está agotando, las direcciones IP dependen mucho de la red en la que este presente una máquina, han aparecido a últimas fechas muchos dispositivos que necesitan de espacio de direcciones mucho mayor, por este motivo surgió IPv6 que puede direccionar 2^{128} direcciones
- El Kernel de Linux ya soporta IPv6

[Redes@Unidad V]\$

- Todas las agencias federales de Estados Unidos para el 2008 deberán ser IPv6.
- 2001:0db8:85a3:08d3:1319:8a2e:0370:7334
- Se espera que hasta el 2025 este en amplio uso IPv6.

[Redes@Unidad V]\$

- Ejemplos de interfaces
- eth Ethernet
- lo loopback
- ppp redes punto a punto
- slip acceso telefónico

[Redes@Unidad V]\$

- Existen mecanismos para optimizar de mejor manera el uso de una dirección IP, entre ellos están las subredes.
- Las subredes consiste en determinar el mejor número para la cantidad de redes y máquinas para cada red.
- Se toman bits prestados ya sea de la parte del host o de la parte de red para obtener el resultado deseado.

[Redes@Unidad V]\$

- Una máscara es una dirección IP que aplicando un operador and a una dirección IP nos permite determinar la dirección de la red y el número de máquina.
- Una dirección de broadcast indica que el mensajes transmitido llegará a todas las máquinas de la red.
- Multicast (grupo) y unicast (única)

[Servicios de red@Unidad V]\$

- `netstat -natu`
- `/etc/rc.d/init.d/inet reload`
- `/etc/conf.modules`
- `Alias eth0 3c59x`
- `ifconfig eth0 1.1.1.1 netmask 255.255.255.0
broadcast 1.1.1.255`

[Configuración de red@Unidad V]\$

- `/etc/sysconfig/network-scripts/ifcfg-eth0`
- `DEVICE="eth0"`
- `IPADDR="192.168.1.1"`
- `NETMASK="255.255.255.0"`
- `NETWORK=192.168.1.0`
- `BROADCAST=192.168.1.25`
- `ONBOOT="yes"`
- `BOOTPROTO="none"`

[Configuración de red@Unidad V]\$

- `./ifdown ifcfg-eth0`
- `./ifup ifcfg-eth0`

- `ifconfig eth0:0 10.1.1.2 netmask
255.255.255.0 broadcast 10.1.1.255`

- `nslookup`
- `ping`

[Configuración de red@Unidad V]\$

- /etc/login.defs
- /etc/profile

- .bash_profile

- /etc/rc.d/init.d/network reload restart
- /etc/sysconfig/network

- arp -a

[Inetd.conf@Unidad V]\$

```
ftpstream    tcp nowait root    /usr/sbin/tcpd    in.ftpd -l -a
```

```
telnet  stream tcp nowait root    /usr/sbin/tcpd    in.telnetd
```

```
shell  stream    tcp    nowait root    /usr/sbin/tcpdin.rshd
```

```
login  stream    tcp    nowait root    /usr/sbin/tcpdin.rlogind
```

```
#exec  stream    tcp    nowait root    /usr/sbin/tcpdin.rexecd
```

```
talk   dgram udp    wait   nobody.tty    /usr/sbin/tcpdin.talkd
```

```
ntalk  dgram udp    wait   nobody.tty    /usr/sbin/tcpdin.ntalkd
```

```
[/etc/services@Unidad V]$
```

```
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp      fspd
ssh         22/tcp # SSH Remote Login Protocol
ssh         22/udp # SSH Remote Login Protocol
telnet      23/tcp
finger      79/tcp
www         80/tcp http# WorldWideWeb HTTP
www         80/udp# HyperText Transfer Protocol
link        87/tcp ttylink
kerberos    88/tcp kerberos5 krb5
```

[Unidad V@presentación]#

- 5.1 Configuración de la red
- 5.2 Firewall (IPTABLES), Proxy y enrutamiento
- 5.3 Herramientas de administración y monitoreo (SNMP, sniffers)

[Firewall@Unidad V]\$

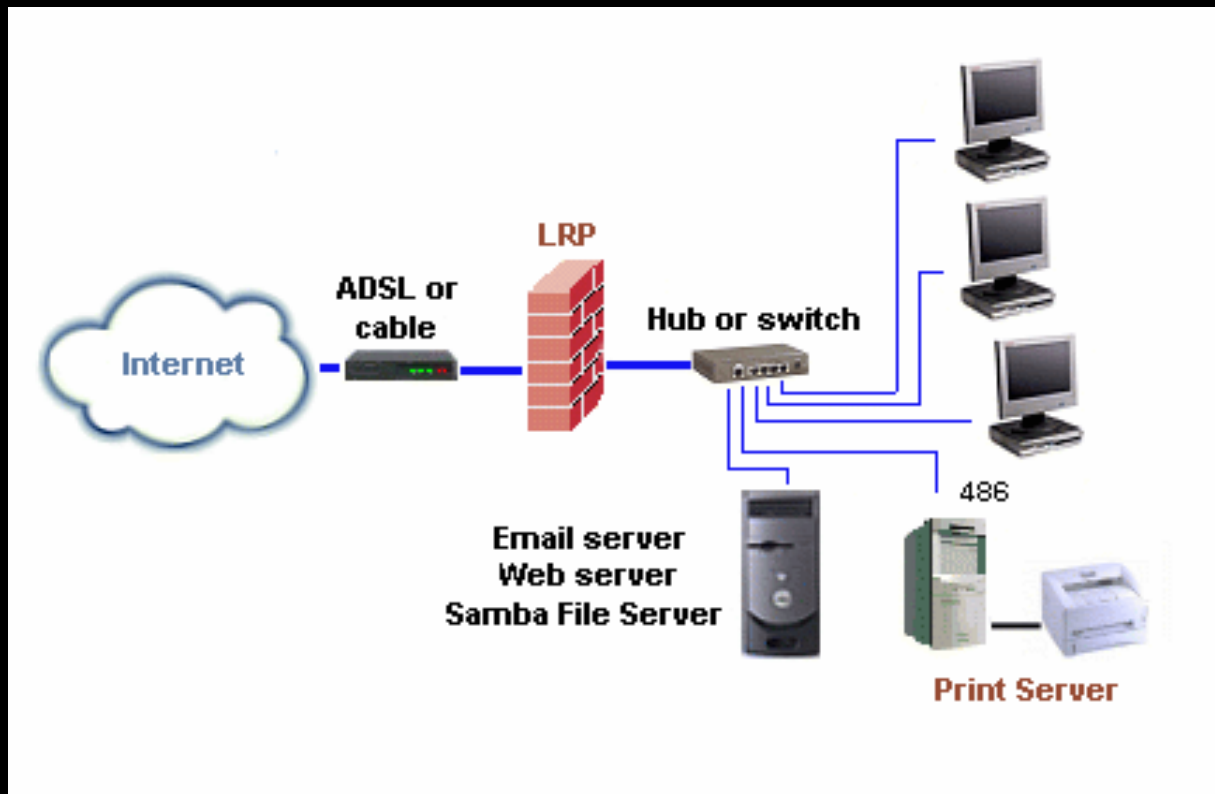
- Debido al auge de las redes de computadoras en donde muchos clientes pueden conectarse de manera remota a un servidor, los problemas de seguridad y control han aumentado haciendo que nuestra máquina sea más vulnerable y propensa a virus, infiltraciones y robo de información. Para ello se necesita un mecanismo que permita evitar esas infiltraciones, el cual recibe el nombre de Firewall.

[Firewall@Unidad V]\$

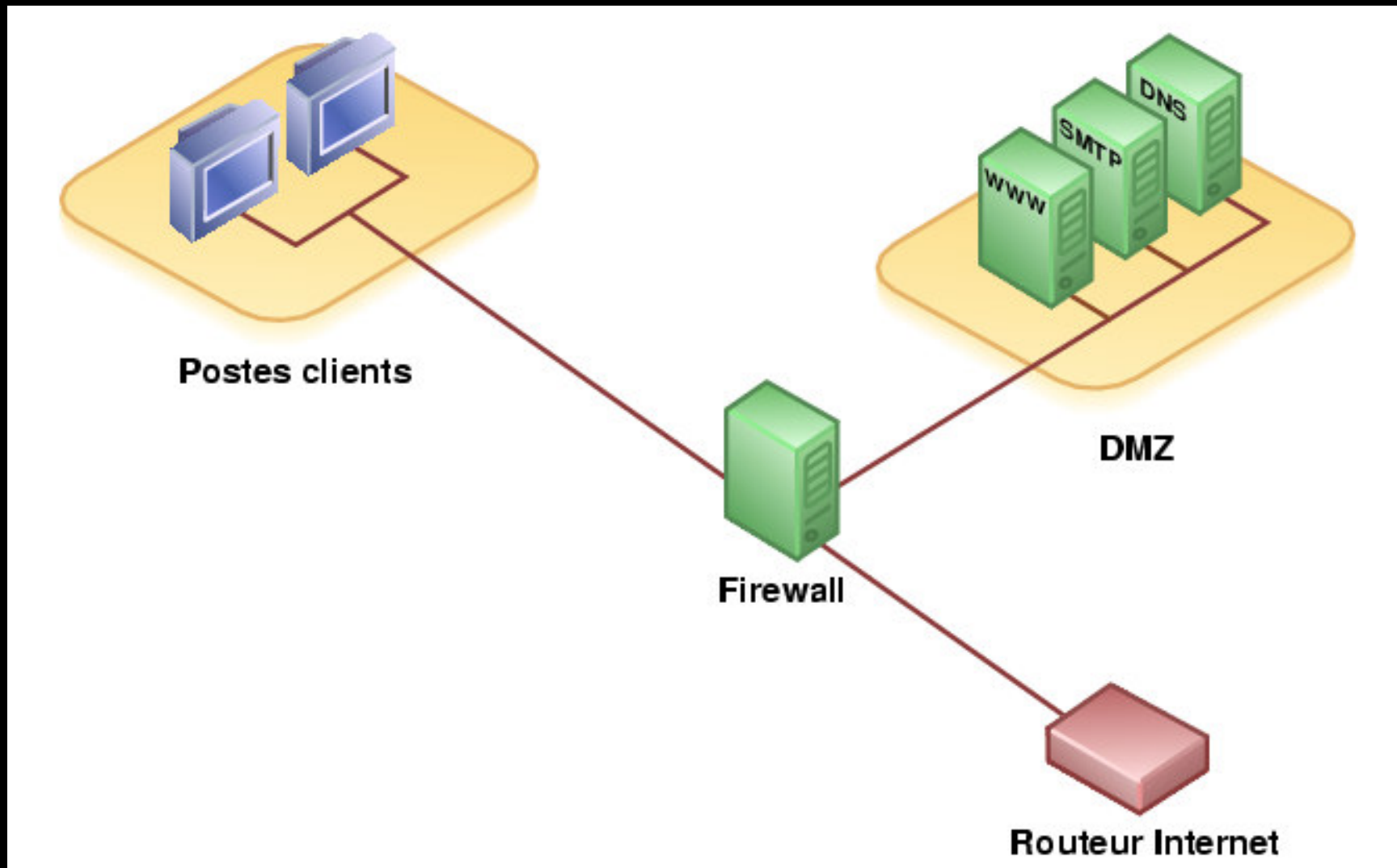
- Un Firewall es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

[Firewall@Unidad V]\$

- Netfilter/iptables www.netfilter.org
- Firewall Linux Project www.flinux.net



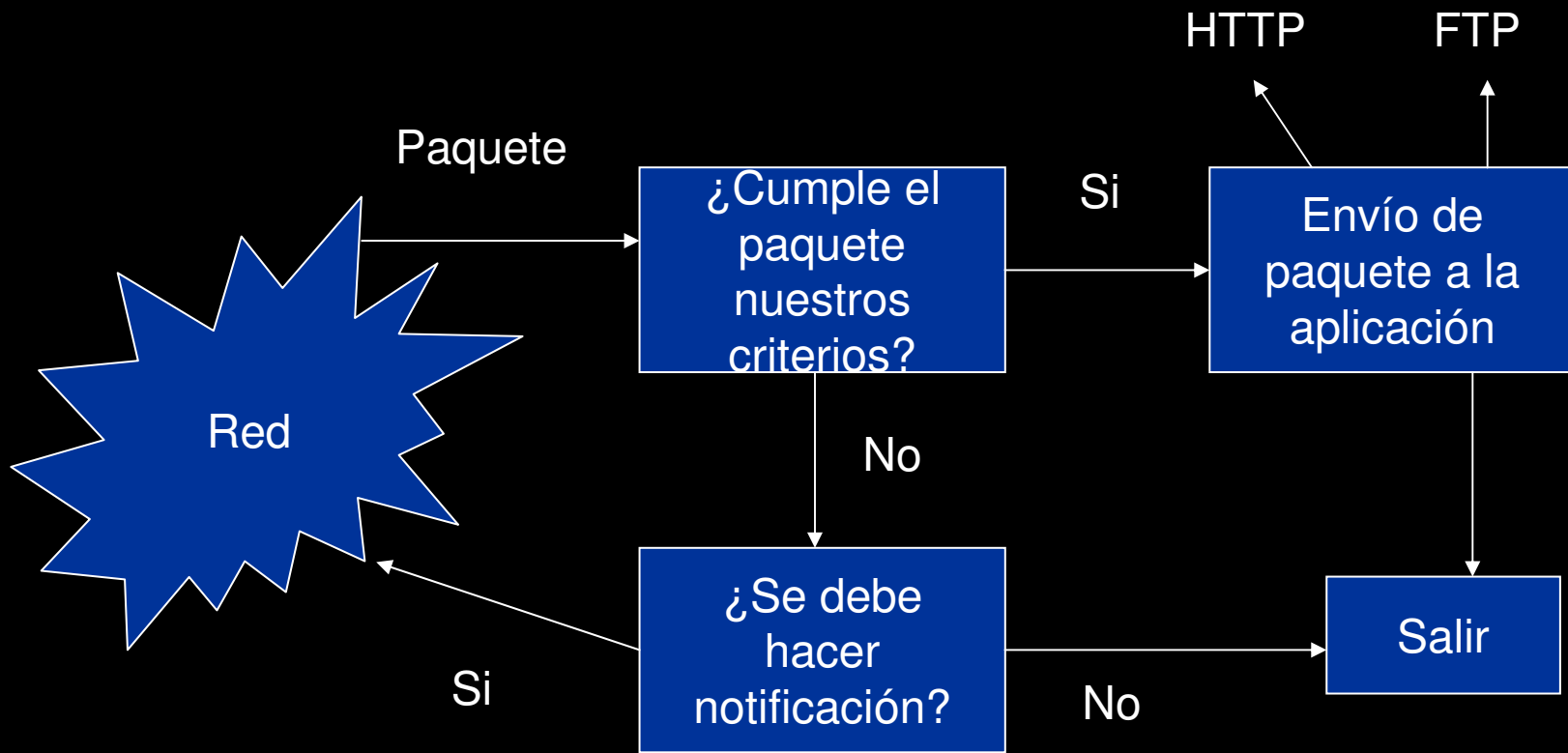
[DMZ@Unidad V]\$



[IPChains@Unidad V]\$

- El filtrado de paquetes consiste en revisar la información de los paquetes y aceptar o rechazar dichos paquetes.
- Para usar IPchains es necesario tener soporte en el kernel, así que deberías incluir las siguientes opciones:
- CONFIG_FIREWALL=y
- CONFIG_IP_FIREWALL=y

[IPChains@Unidad V]\$



[IPChains@Unidad V]\$

- Los comandos básicos de las IPchains son:
- -N Crea una nueva cadena
- -X Borra una cadena
- -P impone la política por defecto para la cadena
- -L Lista las reglas de una cadena
- -F Borra una cadena
- -A Añade una regla a la cadena.
- -I Introduce una regla en una cadena.
- -D Borra una regla de una cadena.

[IPChains@Unidad V]\$

- ipchains -A input -p udp -d 200.32.106.149 53 -j ACCEPT
- ipchains -A input -p tcp -d 200.32.106.199 110 -j ACCEPT
- ipchains -A input -s 200.34.108.241 -d 200.32.106.200 22 -j ACCEPT
- ipchains -P input DENY

[ipchains@Unidad V]\$



[ipchains@Unidad V]\$

- ipchains -A input -p tcp -s 192.168.1.8 -j DENY -y
- ipchains -A input -p tcp -destination-port 8080 -j DENY -I
- ipchains -P forward -j deny
- ipchains -A forward -s 192.168.1.0/24 -d 0/0 -j MASQ

[iptables@Unidad V]\$

- **Sustituto de IPChains. En una sola instrucción puede hacer varias de IPchains.**
- **iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT**
- **iptables -A INPUT -s 62.81.31.3 -p tcp -m tcp --dport 110 -j REJECT**

[iptables@Unidad V]\$

- **iptables -A OUTPUT -p icmp --icmp-type 0 -j DROP**
- **iptables -A OUTPUT -p tcp -j LOG --log-prefix "Conexion TCP en salida: "**

[scripts@Unidad V]\$

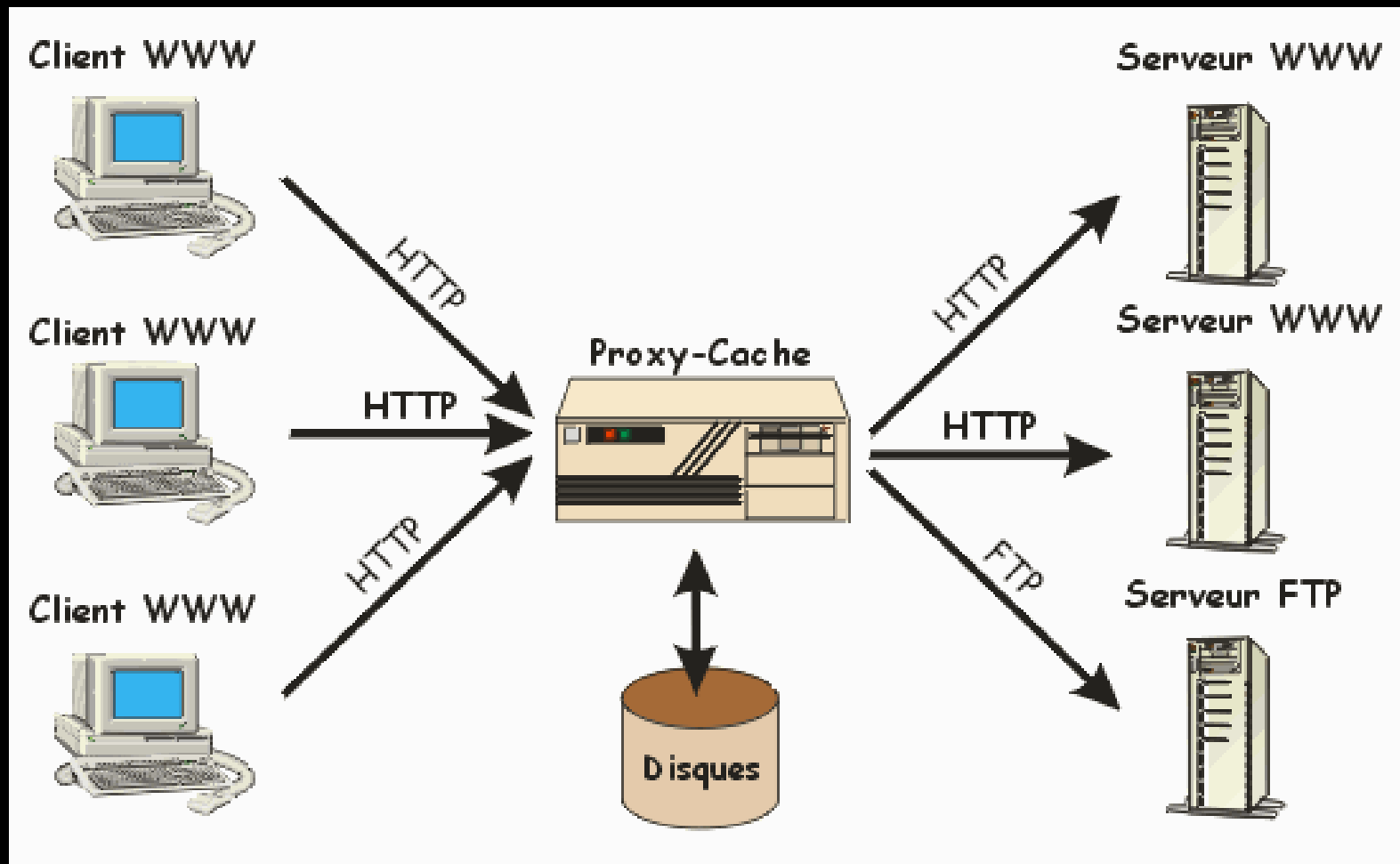
- FWM – Linux based Firewall Managment script (<http://jason.ihde.org/fwm.html>)
- GIPTables (<http://www.giptables.org>)
- Levy (<http://muse.linuxmafia.org/levy/>)

[Firewalls@Unidad V]\$

- PHIPtables
- Linux Routing Project
(<http://master-www.linuxrouter.org:8080/>)
 - Micro-distribución Linux
 - Centrada en redes
 - Cabe en un floppy

[Proxy@Unidad V]\$

- Squid www.squid-cache.org



[Proxy@Unidad V]\$

- Squid es el software para servidor Proxy más popular y extendido entre los sistemas operativos basados sobre UNIX. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios.

[Proxy@Unidad V]\$

- Squid es un servidor Web Proxy con caché, lo que permite agilizar el acceso a Internet de manera considerable.
- Para usar el servidor Proxy se debe configurar manualmente el navegador Web, o bien con un script de actualización automática.

[Proxy@Unidad V]\$

- Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado.

[Proxy@Unidad V]\$

- /etc/squid/squid.conf
- http_port 3128
- cache_dir ufs /usr/local/squid/cache 500 16 256
- reference_age 1 month
- maximum_object_size 4096 KB
- cache_peer 1.2.3.4 parent 8080 0 no-query
- nonhierarchical_direct off
- prefer_direct off

[Proxy@Unidad V]\$

- Es necesario establecer Listas de Control de Acceso que definan una red o bien ciertas maquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.
- **acl [nombre de la lista] src [lo que compone a la lista]**

[Proxy@Unidad V]\$

- `acl mynetwork src 192.168.27.0/255.255.255.0`
- `http_access [deny o allow] [lista de control de acceso]`
- `http_access allow mynetwork`
- `http_access deny !safe_ports`
`http_access deny CONNECT !SSL_ports`

[Proxy@Unidad V]\$

- Al menos una Lista de Control de Acceso
- Al menos una Regla de Control de Acceso
- Acelerar Web
 - httpd_accel_host
 - httpd_accel_port
 - httpd_accel_with_proxy

[Proxy@Unidad V]\$

- Proxy transparente, los navegadores no necesitan cambiar su configuración.
- `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128`
- `echo 1 > /proc/sys/net/ipv4/ip_forward`

[Proxy@Unidad V]\$

- `acl msn_messenger req_mime_type -i ^application/x-msn-messenger$`
- `http_access deny msn_messenger`
- `acl msn_url url_regex -i gateway.dll`
- `acl msn_port port 1863`
- `http_access deny msn_method msn_url`
- `http_access deny msn_port`
- `http_access deny CONNECT msn_port`

[Ruteo@Unidad V]\$

- El encaminamiento (ruteo o enrutamiento) es el mecanismo por el que en una red los paquetes de información se hacen llegar desde su origen a su destino final, siguiendo un camino o ruta a través de la red.
- El encaminamiento es jerarquizado y se hace a través de tablas que indican como enviar los paquetes.

[Ruteo@Unidad V]\$

- En una PC con diversas tarjetas de red e implementando algoritmos y tablas de ruteo se tiene un ruteador barato.
- RIP (Routing Information Protocol)
- OSPF(Open Shortest Path First)
- EIGRP(Enhanced Internet Gateway Routing Protocol)
- BGP(Border Gateway Protocol)

[Ruteo@Unidad V]\$

- `route add -net default gw 192.168.1.1 dev eth0`
- `route add -host 192.168.1.42 netmask 255.255.255.0`
- `route -n show`
- `traceroute` muestra la trayectoria de un paquete
- `pathping`

[Unidad V@presentación]#

- 5.1 Configuración de la red
- 5.2 Firewall (IPTABLES), Proxy y enrutamiento
- 5.3 Herramientas de administración y monitoreo (SNMP, sniffers)

[Administración y monitoreo de Redes@Unidad V]\$

- Debido a la gran importancia que juegan hoy en día las redes de computadoras ha hecho que su desempeño sea vital. De ahí la importancia de verificar que todos los procesos de la red hagan buen uso de la misma.
- A través del monitoreo es posible configurar hardware e instalar software.

[Herramientas de administración y monitoreo@Unidad V]\$

- nmap mapa de la red
- ntop visor de procesos de la red
- tcpdump sniffer básico
- snmp_walk muestra nodos en el árbol MIB

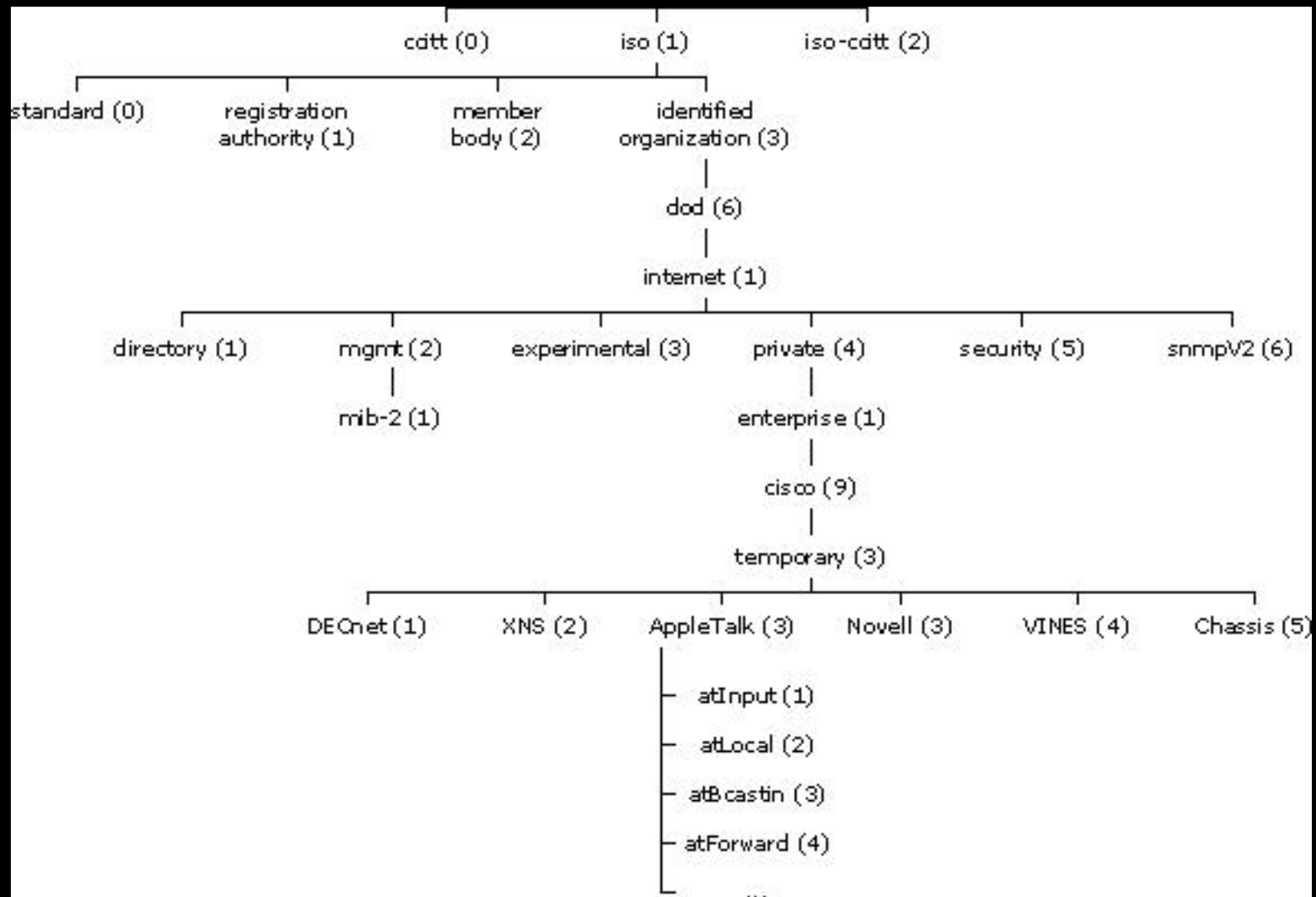
[SNMP@Unidad V]\$

- El Protocolo Simple de administración de red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.
- Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

[SNMP@Unidad V]\$

- SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.
- Una base de información de administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

[SNMP@Unidad V]\$



[SNMP@Unidad V]\$

- El objeto administrado atInput podría ser identificado por el 1.3.6.1.4.1.9.3.3.1.
- Utiliza el puerto 161 y el SNMP-trap el 162
- El corazón del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados mib-2. Los grupos son los siguientes:
 - System (1), Interfaces (2), AT (3), IP (4), ICMP (5), TCP (6), UDP (7), EGP (8), Transmission (10), SNMP (11)

[SNMP@Unidad V]\$

- GetRequest
- GetNextRequest
- SetRequest

- GetResponse
- Trap (Cold start, Warm start, Link down, Link up, Authentication failure, ...)
- GetBulkRequest
- InformRequest

[SNMP@Unidad V]\$

- service snmpd start
- chkconfig snmpd on

- **/usr/bin/snmpget**
- **/usr/bin/snmpgetnext**
- **/usr/bin/snmpset**
- **/usr/bin/snmpwalk**
- **/usr/bin/snmpnetstat**
- **/usr/bin/snmptrapd**
- **/usr/bin/snmpptest**

[SNMP@Unidad V]\$

- `snmpget localhost public interfaces.ifNumber.0`
- `snmpwalk -v 1 192.168.1.254 -c Cl4v3-d3-Acc3s0 system`
- `snmpwalk -v 1 192.168.1.254 -c Cl4v3-d3-Acc3s0 interfaces`
- `#snmpset -v 1 -c necromantux 192.168.1.35 system.sysContact.0 s ana@localhost`

[sniffers@Unidad V]\$

- Sniffer es un programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.
- Las LANs son redes de difusión en las cuales la información pasa por todas las máquinas. Si la tarjeta está en modo promiscuo puede leer esos paquetes.

[sniffers@Unidad V]\$

- Utilización de los sniffers
 - Captura automática de contraseñas enviadas en claro y nombres de usuario de la red.
 - Conversión del tráfico de red en un formato entendible por los humanos.
 - Análisis de fallos para descubrir problemas en la Medición del tráfico de la red.
 - Detección de intrusos

[sniffers@Unidad V]\$

- Ethereal (Wireshark) Gráfico
- tcpdump (Windump) Texto

- Ethereal es un analizador de protocolos, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación.

[tcpdump@Unidad V]\$

- *tcpdump -i eth0*
 - -n resuelve nombres
 - -s longitud
 - -x -X imprime contenido
- `tcpdump src host 192.168.1.1`
- `tcpdump host 192.168.1.2`
- `tcpdump ether dst 0:2:a5:ee:ec:10`
- `tcpdump dst net 192.168.1.0`

[tcpdump@Unidad V]\$

- tcpdump src net 192.168.1.0 mask 255.255.255.240
- tcpdump net 10.0.0.0/24
- tcpdump dst port 23
- tcpdump ip proto \\ip
- tcpdump udp
- tcpdump -n ether proto \\arp
- tcpdump tcp and port 80

[NIS@Unidad V]\$

- Una de las mayores problemáticas a la hora de administrar una red consiste en que existen diversas configuraciones tanto de usuarios como de otros recursos, dada la naturaleza centralizada de la administración se necesitan controlar esos recursos en un solo sistema. Esto se ha logrado gracias a NIS.

[NIS@Unidad V]\$

- NIS proporciona prestaciones de acceso a bases de datos genéricas que pueden utilizarse para distribuir, por ejemplo, la información contenida en los ficheros passwd y groups a todos los nodos de su red. Esto hace que la red parezca un sistema individual, con las mismas cuentas en todos los nodos.
- NIS está basado en RPC. Originalmente NIS se llamaba Páginas Amarillas (Yellow Pages), o YP, que todavía se utiliza para referirse a él.

[/etc/yp/Makefile@Unidad V]\$

- all: passwd group hosts rpc services netid protocols netgrp mail \
- shadow publickey networks ethers bootparams amd.home \
- auto.master auto.home passwd.adjunct

- /usr/lib/yp/ypinit -m

[NIS@Unidad V]\$

- /etc/yp.conf
- Domain dominio broadcast
- Domain dominio server servidor

- /etc/rc.d/init.d/ypbind start | stop
- /etc/nsswitch.conf
- Passwd: files nis

- Ypcat passwd

[NIS@Unidad V]\$

- Domainname nombre.dominio
- /etc/sysconfig/network
- NIS_DOMAIN=dominio
- /etc/rc.d/init.d/ypserv
- /etc/rc.d/init.d/ypserv start | stop

- /var/yp/Makefile

[NIS@Unidad V]\$

- Herramientas NIS
 - Ypcat
 - Ypwhich
 - Ypmatch

[Impresión@Unidad V]

- Una de las mayores problemáticas que se ha presentado en Linux es el tema de la impresión debido a que en muchas ocasiones no es tan fácil encontrar los controladores.
- /etc/hosts.lpd /etc/hosts.equiv
- borrándolos se autoriza la impresión remota para cualquiera.
- Printtool
- /etc/printcap

[Impresión@Unidad V]\$

- Impresora|lp: \
 - :sd=/var/spool/lpd/lp: \
 - sh: \
 - rm=intrepid: \
 - rp=engprint:
-
- Samba impresión smbprint

[Impresión@Unidad V]\$

/var/spool/lpd/NOMBRE-IMPRESORA/.config

Server=MAQUINA

Service=NOMBRE_IMPRESORA

Password="password"

Lpr archivo

Lpr -P impresora archivo

lprm

[Impresión@Unidad V]\$

- `/usr/sbin/lpc up betty`
- `/etc/printcap`
`betty|lp:lp=/dev/lp1:sd=/var/spool/lp1:sh:lf=/var/adm/lpd-errs:of=/etc/start-dj500:`
- `lpc`
- `/usr/spool`

[Redes inalámbricas@Unidad V]\$

- Las redes inalámbricas han llevado a que los usuarios logren la ansiada libertad de poder conectar sin cables y desplazarse.
- La gran popularidad de las redes inalámbricas de computadoras ha llevado a Linux a proveer soporte para esta tecnología. Desafortunadamente, no existen muchos drivers 100% compatibles con las NIC inalámbricas.

[Redes inalámbricas@Unidad V]\$

- iwconfig
- iface eth1 inet dhcp

- wireless_essid Nombre_de_red
- wireless_mode **ad-hoc**
- wireless_key s:mi_clave
- wireless_rate auto
- wireless_nick sofi

[VPN@Unidad V]\$

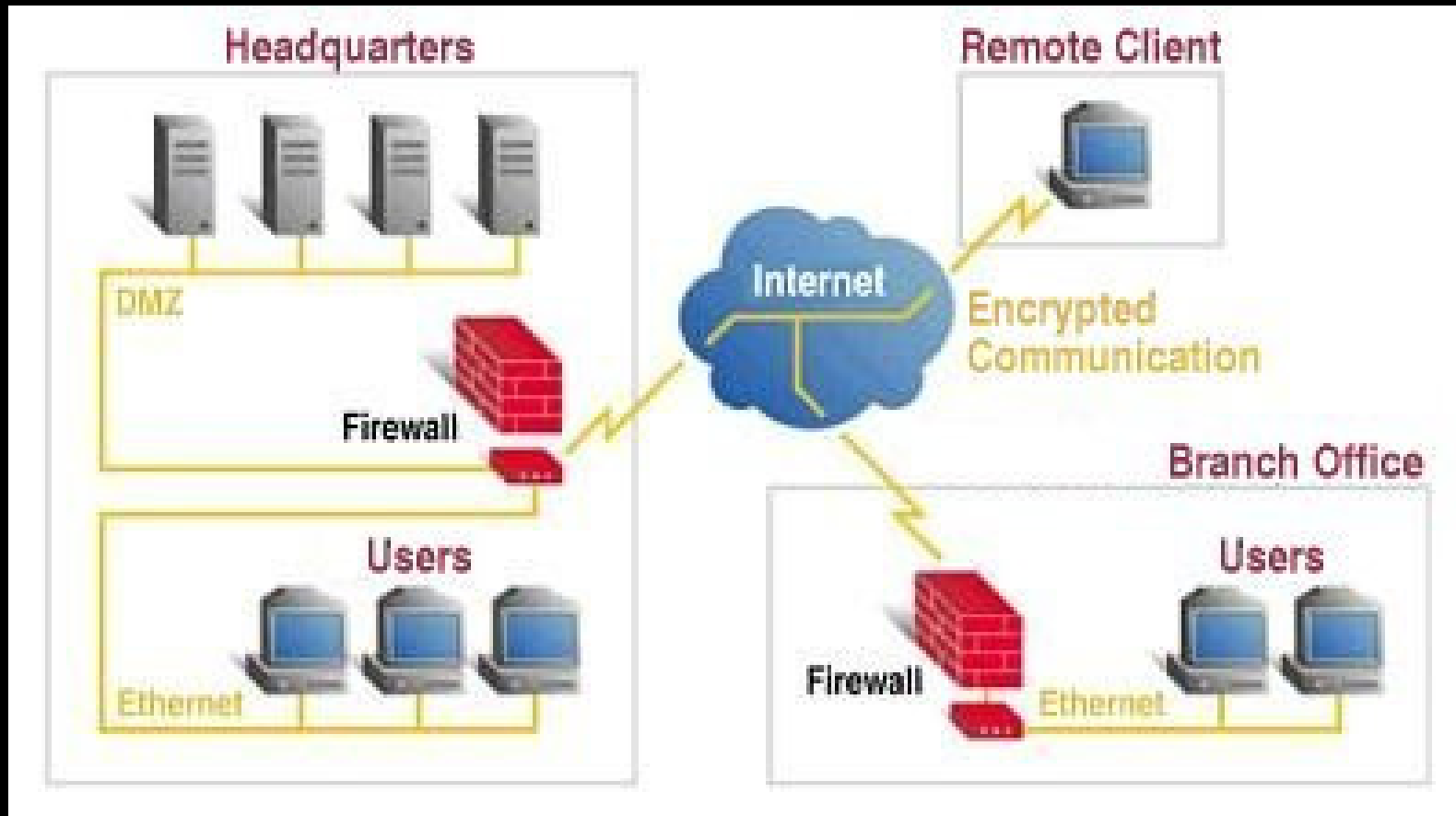
- La VPN es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.
- El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet.
- Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación

[VPN@Unidad V]\$

- Para realizar esa conexión virtual de redes sobre Internet, se necesita de cifrar los datos dado que Internet es totalmente seguro. A este proceso se le denomina tuneleo.
- Los algoritmos de cifrado son: IPSEC, PPTP, L2F, L2TP, SSL/TLS, SSH
- Con las VPN se logra una línea dedica virtual a un bajo costo.

[VPN@Unidad V]\$

- FreeSWAN www.freeswan.org
Cifrado y autenticación IPSEC



[VoIP@Unidad V]\$

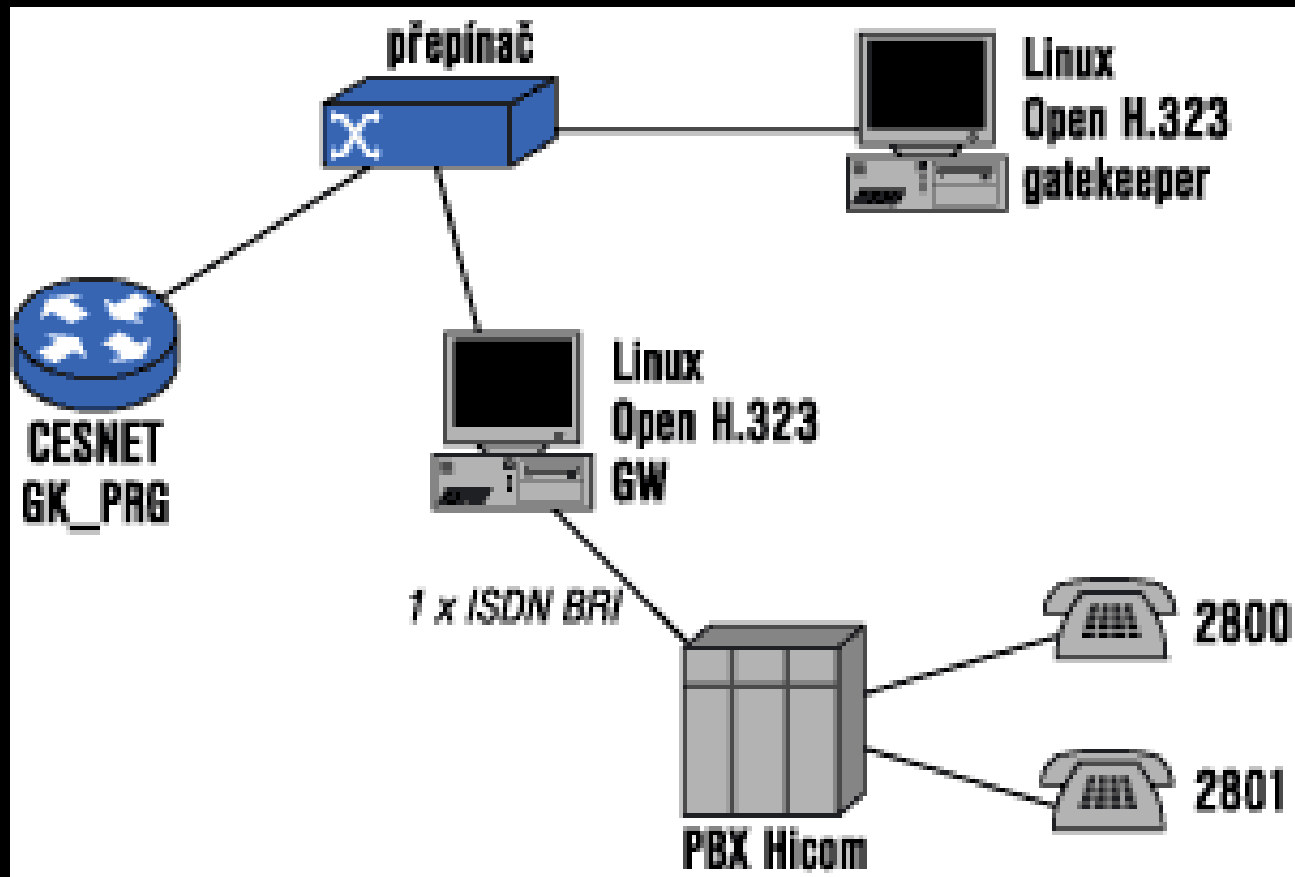
- La infraestructura de redes de computadoras se originó para enviar datos. Debido a la gran demanda de otros servicios como video y voz fue necesario modificar los esquemas de red para poder hacer frente a estas nuevas demandas.
- El poder compartir información de cualquier tipo es uno de los objetivos de las redes de telecomunicaciones.

[VoIP@Unidad V]\$

- Voz sobre IP (Telefonía IP, o Telefonía por Internet) es el enrutamiento de conversaciones de voz sobre Internet o a través de alguna otra red basada en IP.
- Es más barato*, movilidad. Latencia, baja calidad de servicio.
- Protocolos: H.323, SIP, Skype,

[VoIP@Unidad V]\$

- GnomeMeeting www.gnomemeeting.org
- OpenH323 www.openh323.org



[Asterisk@Unidad V]\$

- Asterisk es una aplicación de código abierto de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI tanto básicos como primarios.
- Asterisk incluye muchas características anteriormente sólo disponibles en caros sistemas propietarios PBX: buzón de voz, conferencias, IVR, distribución automática de llamadas, y otras muchas más. Los usuarios pueden crear nuevas funcionalidades escribiendo un dialplan en el lenguaje de script de Asterisk o añadiendo módulos escritos en lenguaje C o en cualquier otro lenguaje de programación soportado por Linux.

[Asterisk@Unidad V]\$

- Para conectar teléfonos normales analógicos hacen falta unas tarjetas telefónicas FXS o FXO fabricadas por Digium o por otros fabricantes, ya que para conectar el servidor a una línea externa no vale con un simple módem.
- Quizá lo más interesante de Asterisk es que soporta muchos protocolos VoIP como pueden ser SIP, H.323, IAX y MGCP. Asterisk puede interoperar con terminales IP actuando como un registrador y como gateway entre ambos.
- Las compañías de telecomunicaciones de todo el mundo empiezan a utilizar Asterisk como sistema nativo de VoIP junto con SER (Sip Express Router) en lugar de otras marcas que ofrecen PBX propietarios como Alcatel, Cisco , Avaya ó Nortel.