Gestió d'Infraestructures per al Processament de Dades

Revisió Xarxes i Proxies

Departament Arquitectura d'Ordinadors i Sistemes Operatius
UAB (Remo.Suppi@uab.cat)

Què veurem?

Conceptes essencials d'infraestructures 'aplicats' a xarxes i serveis:

NAT, SSH, DHCP, DNS, NIS, NFS,

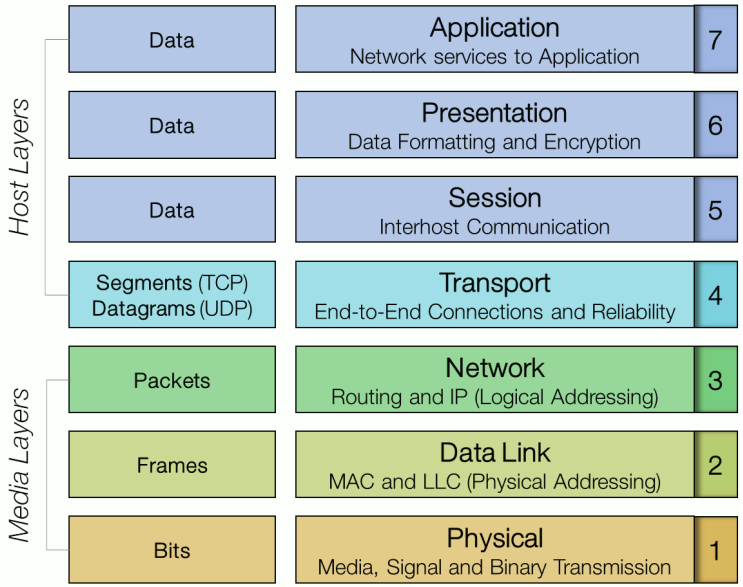
Iptables

WWW

Proxies

Xarxes

El protocol TCP/IP és en realitat un conjunt de protocols bàsics ques'han anat agregant al principal per a satisfer les diferents necessitatsen la comunicació ordinador-ordinador, com són TCP, UDP, IP, ICMP, ARP.



Utilització típica de TCP/IP remote login (actualment, per qüestions de seguretat, telnet ha estat substituït per ssh):

ssh user@remote_host

GNU/Linux 5.10-generic x86_64
Last Login: Fri Sep 08 08:00:03 2021 from sys.nteum.org
$

Conceptes de xarxes

Internet/intranets: el terme intranet es refereix a l'aplicació de tecnologies d'Internet (xarxa de xarxes) dins d'una organització. Si és necessari que algun d'aquests serveis tingui accés des de fora de la institució, és necessari posar serveis de Proxy o encaminadors que puguin redireccionar els paquets cap al servidor intern.

Node: es denomina node (amfitrió) una màquina que es connecta a la xarxa (en un sentit ampli, un node pot ser un ordinador, una tauleta, un telèfon,una impressora, una torre (rack) de CD, etc.), és a dir, un element actiu i diferenciable a la xarxa que reclama o deixa algun servei o comparteix informació.

Adreça de (física) xarxa (**Ethernet address o MAC address**): un número de 48 bits (per exemple 00:88:40:73:AB:FF –en octal–, o 0000 0000 10001000 0100 0000 0111 0011 1010 1011 1111 1111 –en binari–) que es troba en el dispositiu físic (maquinari) del controlador (NIC) de xarxa i és gravat pel fabricant (aquest número ha de ser únic al món, per la qual cosa cada fabricant de NIC té un rang preassignat). S'utilitza en la capa 2 del model OSI i és possible tenir-ne 2^{48}; és a dir, 281.474.976.710.656 MAC (Media access control)

Conceptes de xarxes

Nom de l'amfitrió: cada node ha de tenir a més un únic nom a la xarxa. Poden ser només noms o bé utilitzar un esquema de noms jeràrquic basat en dominis (hierarchical domain naming scheme). Els noms dels nodes han de ser únics, la qual cosa resulta fàcil en petites xarxes, i més dificultós enxarxes extenses, i impossible a Internet si no es fa algun control. Els noms han de ser d'un màxim de 32 caràcters, han d'usar a-zA-Z0-9.-, no han de contenir espais o # i han de començar per un caràcter alfabètic.

Adreça d'Internet (IP address): està compost per un conjunt de nombres i dependrà de la versió del protocol IP i s'utilitza universalment per a identificar els ordinadors sobre una xarxa o Internet. Per a la **versió 4 (IPV4**) està format per quatre nombres en el rang 0-255 (32 bits) separats per punts (per exemple, 192.168.0.1), la qual cosa possibilita 4.294.967.296 (2^{32}) adreces de host diferents, cosa que s'ha mostrat insuficient sobretot perquè cada individu disposa de més d'un ordinador, tauleta, telèfon, PDA, etc.

Per a la **versió 6 (IPv6)** l'adreça és de 128 bits i s'agrupen en quatre dígits hexadecimals formant vuit grups. Per exemple,fe80:0db8:85a3:08d3:1319:7b2i:0470:0534 és una adreça IPv6 vàlida. Espot comprimir un grup de quatre dígits si aquest és nul (0000). Per exemple: fe80:0db8:0000:08d3:1319:7b2i:0470:0534=fe80:0db8::08d3:1319:7b2i:0470:0534

Seguint aquesta regla, si dos grups consecutius són nuls es poden agrupar, per exemple fe80:0db8:0000:0000:0000:0000:0470:0534=fe80:0db8::0470:0534.

S'ha d'anar amb compte, ja que per exemple fe80:0000:0000:0000:1319:0000:0000:0534 no es pot resumir com afe80::1319::0534 perquè no se sap la quantitat de grups nuls de cada costat. També els zeros inicials es poden ometre quedant fe80:0db8::0470:0534 com fe80:db8::470:534.

Conceptes de xarxes

Per tant, en IPv6 s'admeten 340.282.366.920.938.463.463.374.607.431.768.211.456 adreces (2^{128} o 340 sextilions d'adreces), la qual cosa significa aproximadament 6,7 × 1017(670 mil bilions) adreces per cada mil·límetre quadrat de la superfície de la Terra.

La translació de noms en adreces IP la fa un servidor DNS (domain name system) que transforma els noms de node (llegibles per humans) en adreces IP

Port: identificador numèric de la bústia en un node que permet que un missatge (TCP, UDP) pugui ser llegit per una aplicació concreta dins d'aquest node (per exemple, dues màquines que es comuniquin per ssh ho faran pel port 22, però aquestes mateixes màquines poden tenir una comunicació http pel port 80).

Node encaminador (passarel·la o gateway): és un node que fa encaminaments (transferència de dades routing). Un encaminador o router, segons les seves característiques, podrà transferir informació entre dues xarxes de protocols similars o diferents. Cada node tindrà **un default gateway**.

Conceptes de xarxes

Domain name system (DNS): permet assegurar un únic nom i facilitar l'administració de les bases de dades que fan la translació entre nom i adreça d'Internet, i s'estructuren en forma d'arbre. Per a això, s'especifiquen dominis separats per punts, el més alt (de dreta a esquerra) dels quals descriu una categoria, institució o país (com, comercial; edu, educació; gov, governamental; mil, militar (govern); org, sense finalitat de lucre; dues lletres per a un país, o en casos especials tres lletres, com cat, llengua i cultura catalana...).

El segon nivell representa l'organització, el tercer i els restants els departaments, seccions o divisions dins d'una organització (per exemple, www.uab.cat o pirulo@nteum.remix.cat). Els dos primers noms (de dreta a esquerra, uoc.edu en el primer cas, remix.cat en el segon, han de ser assignats (aprovats) per l'Internet Network Information Center (NIC,òrgan mundial gestor d'Internet) i els restants poden ser configurats o as-signats per la institució. Una regla que regeix aquests noms és la FQDN (*fully qualified domain name*), que inclou el nom d'un ordinador i el nom de domini associat a aquest equip.

Conceptes de xarxes

Mask: Una subxarxa és una subdivisió lògica d'una xarxa IP. Els ordinadors que pertanyen a una subxarxa s'adrecen amb un grup de bits més significatiu de les seves adreces IP (per exemple totes les màquines d'un departament). Això resulta en la divisió lògica d'una adreça IP en dos camps: la part de xarxa i la part de la màquina. Per a totes les màquines que coincideixen aquest bits de xarxa es podran comunicar directament (estaran directament connectades). La que no, el paquet haurà de ser 'encaminat' per altres xarxes.

Es per això que subxarxes significa subdividir la IP en xarxes dins de la mateixa xarxa, per exemple, per a millorar el trànsit. El nombre de bits que són interpretats com a identificador de la subxarxa és donat per una màscara de xarxa (o netmask) que és un nombre de 32 bits (igual que la IP).

Per exemple si tenim una màquina en la IP 172.16.1.10 i altre en la 172.16.1.20 i la màscara és 255.255.255.0 en format llarg o 24 en format abreujat (vol dir 24 nombres 1) com sabem si estan en la mateixa xarxa?

S'haurà de fer una operació lògica AND entre la màscara i la IP, la qual cosa donarà la IP de la subxarxa. Tenint en compte que 255 és igual a 1111 1111 en binari, 172.16.1.10 AND 255.255.255.0 ens donarà 172.16.1.0 que serà el ID de la xarxa. En la segona IP 172.16.1.20 AND 255.255.255.0 ens donarà 172.16.1.0 per tant poden concloure que les dos màquines estan en la mateixa xarxa i es poden comunicar directament sense 'encaminament' (routing).

Si la mascara es 255.255.255.0 (que indica 24 nombres 1), vol dir que les màquines solament poden canviar l'ultim dígit i per tant les IP d'aquestes màquines seran en el rang: 172.16.1.0 fins a 172.16.1.255, es a dir 256 IP diferents en aquesta subxarxa.

Conceptes de xarxes

Per tan es pot especificar la IP d'una maquina i la màscara com 172.16.1.20 i màscara 255.255.255.0 o també 172.16.1.20/24 (això ens dirà que tenim 3 dígits o 24 bits assignats per al prefix de xarxa i dígit restant o 8 bits a l'adreça de node.

En les IP públiques la part de xarxa és assignada per l'ICANN (organisme gestor de gestió de IP), i la part del node és assignada per la institució o el proveïdor.

Per exemple la UAB té assignada pel ICANN una xarxa classe B amb la IP 158.109.0.0/16 que significa que després la UAB pot assignar el tercer i quart dígit de les Ips internament per tant té la possibilitat de tenir 256 x 256 IP es a dir 65536 IP diferents.

Hi ha algunes restriccions: 0 (per exemple, 0.0.0.0) en el camp de xarxa és re-servat per a l'encaminament per defecte i 127 (per exemple, 127.0.0.1) és reservat per a l'autoreferència (local loopback o local host), 0 en la part de node es re-fereix a aquesta xarxa (per exemple, 192.168.0.0) i 255 és reservat per a paquets de tramesa a totes les màquines (difusió) (per exemple, 198.162.255.255).

Hi ha un conjunt d'adreces IP que no es fan servir externament, es reserven per xarxes privades (per exemple dintre de casa) i es coneixen com IP privades. Els paquets solament poden moure dintre d'aquesta xarxa i si necessitem que vagin a una xarxa pública han de passar por un router que tindrà un IP publica, el paquet farà servir aquesta IP i quan torni, agafarà novament la IP privada. Aquest procediment s'anomena NAT i es veurà després.

Conceptes de xarxes

En les diferents assignacions es poden tenir diferents tipus de xarxes o adreces:

ClasseA (xarxa.amfitrió.amfitrió.amfitrió): 1.0.0.1 a 126.254.254.254 (126 xarxes, 16 milions de nodes); defineixen les grans xarxes.

ClasseB (xarxa.xarxa.amfitrió.amfitrió): 128.1.0.1 a 191.255.254.254 (16K xarxes, 65K nodes); generalment s'utilitza el primer byte de node per a identificar subxarxes dins d'una institució).

ClasseC (xarxa.xarxa.xarxa.amfitrió): 192.1.1.1 a 223.255.255.254 (2 milions de bits de xarxes, 254 de nodes).

Classe D i E (xarxa.xarxa.xarxa.amfitrió): 224.1.1.1 a 255.255.255.254, reservat per a multidestinació (des d'un node a un conjunt de nodes que formen part d'un grup) i propòsits experimentals.

Alguns rangs d'adreces han estat reservats perquè no corresponguin a xarxes públiques, sinó a **xarxes privades**, i els missatges no seran encaminats per mitjà d'Internet, cosa que es coneix com a intranets. Aquestes són:

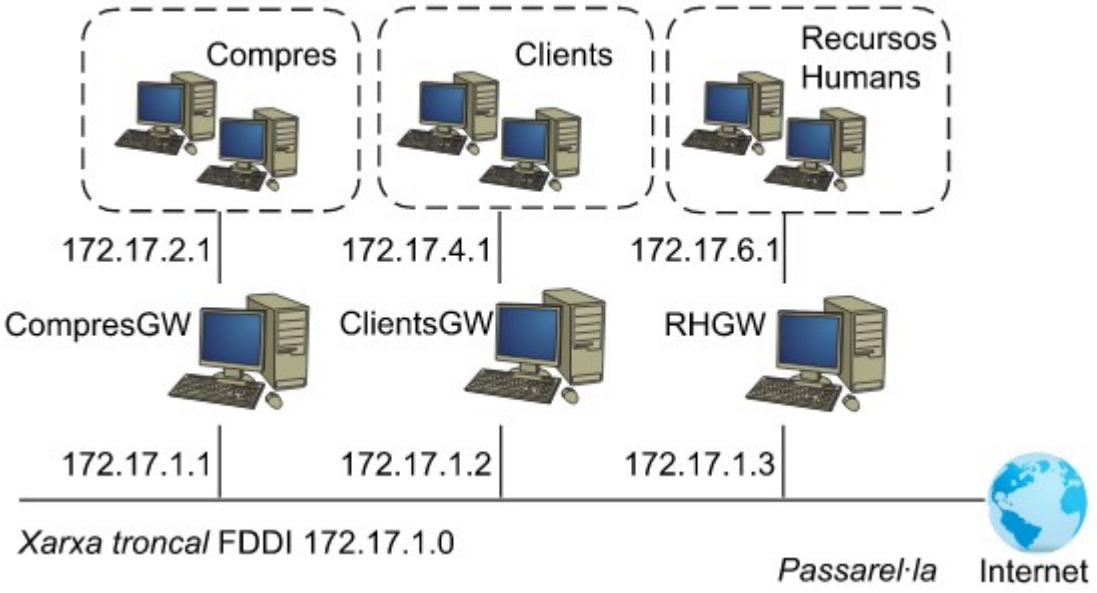
ClasseA des de 10.0.0.0 fins a 10.255.255.255

ClasseB des de 172.16.0.0 fins a 172.31.0.0

ClasseC des de 192.168.0.0 fins a 192.168.255.0

Conceptes de xarxes: Routing

El punt que connecta totes aquestes subxarxes (xarxa troncal) té la seva pròpia adreça, com per exemple 172.17.1.0. Aquestes subxarxes comparteixen la mateixa IP de xarxa, mentre que la tercera és utilitzada per a identificar cada una de les subxarxes que hi ha a dins (per això s'utilitzarà una màscara de xarxa 255.255.255.0) o també especificada com /24.



Adreça	Màscara	Passarel·la
172.17.1.0	255.255.255.0	-
172.17.4.0	255.255.255.0	172.17.1.2
172.17.6.0	255.255.255.0	172.17.1.3
0.0.0.0	0.0.0.0	172.17.2.1
172.17.2.0	255.255.255.0	-

Conceptes de xarxes

NAT: mètode que permet canviar l'adreça origen o destinació d'un paquet IP per canviar-ho de xarxa. És la forma habitual que un paquet pot passar d'una xarxa privada a una pública i retornar al node que ho ha enviat. El dispositiu que fa aquest canvi normalment es coneix com router.

DHCP (Dynamic Host Configuration Protocol): és un protocol que permet a un node obtenir el paràmetres de xarxa sense tenir cap configuració de la xarxa (es fa fent servir Broadcast).

NIS o YP: El servei d'informació de xarxa (originalment anomenat Yellow Pages), és un protocol de servei de directori client-servidor per distribuir dades de configuració del sistema, com ara noms d'usuari entre ordinadors d'una xarxa informàtica.

Un sistema NIS/YP manté i distribueix un directori central d'informació d'usuaris i grups, noms d'amfitrió, àlies de correu electrònic i altres taules d'informació basades en text en una xarxa informàtica. D'aquesta forma un administrador no ha de crear un compte d'usuari en cada màquina sinó la crea ene l servidor i els usuaris es podran connectar en qualsevol màquina del domini.

Conceptes de xarxes

ARP, RARP: en algunes xarxes (com per exemple IEEE 802 LAN, l'estàndard per a Ethernet), les adreces IP són descobertes automàticament per mitjà de dos protocols: ARP i RARP. ARP utilitza missatges de difusió (broadcast messages) per a determinar l'adreça MAC (especificació MAC de la capa 3 del model OSI) corresponent a una adreça de xarxa particular (IP). RARP utilitza missatges de difusió (missatge que arriba a tots els nodes) per a determinar l'adreça de xarxa associada amb una adreça de maquinari en particular. RARP és especialment important en màquines que no tenen IP en el moment de l'inici (boot).

NFS (Network File System): sistema de fitxers de xarxa (NFS) és un protocol de sistema de fitxers distribuït desenvolupat originalment per Sun Microsystems (Sun) el 1984, que permet a un usuari d'un equip client accedir a fitxers a través d'una xarxa de la mateixa manera que s'accedeix a l'emmagatzematge local. El NFS és un estàndard obert definit en una sol·licitud de comentaris (RFC), que permet a qualsevol persona implementar el protocol.

DFS (Distributed File System): sistema client servidor que permet definir un sistema d'emmagatzematge a partir de particions de discs o discs sencers (brics) en altres nodes i que un arxiu estigui distribuït/replicat en els diferents nodes.

RAID (Redundant Array of Independent Disks): sistema d'arxius redundant que permet la fallida dels dispositius sense perdre la informació (nivell 1 a 6, més utilitzats 1,5,6 o combinacions)

Pràctica 1: Cas d'ús d'infraestructura de xarxa

Objectiu: Considerant un sistema informàtic com la de la figura, definir per a les tres màquines tots els aspectes relacionats als conceptes mostrats fent servir MV el cloud OpenNebula. Trobareu al CV l'enunciat detallat i quan lliurar l'informe.

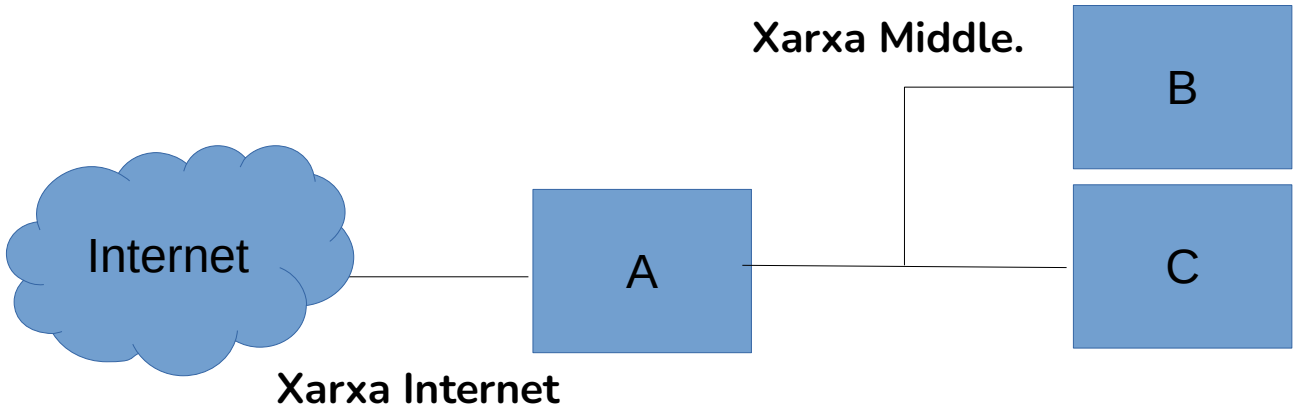
Aspectes a considerar:

1. les MV B, C no tenen connexió a Internet per tant hauran d'enviar el paquets de comunicació a MV A i aquesta cap Internet.

2. El rol de MV A es el de Router: rep els paquets de B i C que va cap a Internet, els canvia de interface de xarxa, fa un NAT i els envia a Internet. Quan el paquet torna fa el procediment invers (és el mateix rol del router que tenim a casa).

3. Aquestes màquines no tenen nom FQDN per tant s'haurà de posar un servei de noms (DNS).

4. Tampoc tenen cap serveix i s'hauran de instal·lar i configurar (NFS, SSH, Apache).



DNS (*Domain Name System*)

Objectiu: disposar d'un servir que pugui resoldre nom -> IP d'una xarxa pròpia (i viceversa) i fer de DNS-cache

Bind és probablement el més utilitzat per la seva versatilitat i prestacions però es complex de configurar.

Dnsmaq es un servei de DNS i DHCP de molt bones prestacions i característiques per a xarxes petites/mitjanes.

És possible atendre peticions de noms de màquines que no estan en els DNS globals i a més suporta gestió d'IP dinàmiques i estàtiques.

La forma de configurar ràpidament un DNS per a màquines de domini propi i que faci de forwarder per als dominis externs és fent servir:

apt-get update; apt-get install dnsmasq

Si el que es desitja és un simple DNS, ja està configurat tenint en compte que en /etc/resolv.conf tindrem alguna cosa com nameserver 8.8.8.8 (en el cas de ONE ja estan posat els DNS de la UAB). Amb això, podem provar els externs utilitzant la instrucció `dig` o l'ordre `hosts`

També respondrà a les totes les màquines que tinguem definides en */etc/hosts*. Per exemple, si tenim una línia com *172.16.1.10 nteum.remix.org nteum* podrem executar **dig nteum.remix.org** ens respondrà amb l'IP corresponent.

Per aquest motiu, si la xarxa és simple podem agregar les màquines en aquest arxiu, però si és més complexa, podem utilitzar l'arxiu de configuració */etc/dnsmasq.conf* que inclou una gran quantitat d'opcions per a organitzar els dominis interns i altres paràmetres no només per a la configuració del DNS, sinó també per al servidor de DHCP.

Sobre els host de la xarxa interna solament hem de posar en /etc/resolv.conf una línia

nameserver IP_our_server_DNS

En el */etc/resolv.conf* s'ha de afegir *nameserver 127.0.0.1* com primer nameserver (sobre ONE tindrem que veure com podem evitar que quan es faci un boot de la MV aquest línia no desaparegui).

NFS (*Network File System*)

Objectiu: Servei de disc que permet accedir des de un clinet a arxius en el servidor on-line.

Protocol de sistema de fitxers distribuït desenvolupat originalment per Sun (1984) que permet a un usuari d'un ordinador client accedir a fitxers a través d'una xarxa igual que s'accedeix a l'emmagatzematge local. Es basa en Remote Procedure Call (RPC) i és un estàndard obert definit en una RFC, que permet a qualsevol persona implementar el protocol..

apt-get install nfs-common sobre el client

apt-get install nfs-kernel-server sobre el servidor.

Gestió: **systemctl start|restart|stop nfs-kernel-server rpcinfo -p**

Permisos: Editar l'arxiu /etc/exports sobre el server que serveix d'ACL (llista de control d'accés) dels sistemes d'arxiu que poden ser exportats als clients.

```
/               master(rw)
/               trusty(rw,no_root_squash)
/projects       proj*.local.domain(rw)
/usr            .local.domain(ro) @trusted(rw)
/pub    *(ro,insecure,all_squash)
/home           20.20.20.0/24(rw,sync,no_root_squash,no_subtree_check)
```

Sobre el client (o un altre usuari fent servir sudo), el root pot muntar el sistema remot a través de l'ordre:

mount -t nfs Ipserver:directori-remot directori_local

A partir d'aquest moment, el directori-remot es veurà dins del directori_local (aquest ha d'existir abans d'executar el mount). Aquesta tasca en el client es pot automatitzar utilitzant l'arxiu de mount automàtic (/etc/fstab) incloent una línia. per exemple:

```
20.20.20.X:/nfsdir      /mnt        nfs         defaults    0       0
```

SSH (*Secure Shell*)

Objectiu: interconnexió interactiva segura (encriptada) entre màquines fent servir PKI i forwarding del protocol X11.

El ssh és un programari client -servidor disponible en tot el sistema operatius (W fer servir Mobaterm o Putty) i permet fer tunnels, *forwarding* de protocols, *proxies SOCKS* i altres funcionalitats més. Nosaltres farem servir openssh-server (el client ja està instal·lat per defecte normalment en Linux i MacOS)

Sobre el server: **apt install openssh-server**

Sobre el client: **ssh** **user@ip_server** **sol·licitara** usuari i passwd

Configuració: */etc/ssh/ssh_config* i */etc/ssh/sshd_config* (el root per seguretat no està permés com usuari de connexió i s'ha de canviar la configuració *PermitRootLogin yes*)

Com mètode d'autentificació es pot fer servir PKI (clau pública i privada):

ssh-keygen -t rsa|dsa es poden crear les claus d'identificació d'usuari.

L'ordre crea en el directori del $HOME/.ssh de l'usuari els fitxers *id_rsa i id_rsa.pub*, les claus privada i pública, respectivament. L'usuari podria copiar la clau pública (id_rsa.pub) en l'arxiu $HOME/.ssh/authorized_keys de la

màquina fent servir l'ordre:

ssh-copy-id usuari@màquina

Sobre màquines sense terminal gràfic (GUI) es poden redireccionar les sortides aplicacions d'aplicacions (Xwindow) cap a la màquina client que inicia la connexió i que tingui GUI (molt útil en l'administració remota de servidors):

ssh -X usuari@host_per_a_administrar

SSH també és molt útil per a crear túnels i VPN sobre SSL a través d'interfases virtuals.

Altres utilitats: **scp** (per copiar arxisu en forma segura), **sftp/zssh** per transferir arxius en forma segura, **sshfs** per muntar un directori remot sobre la màquina local.

Apache2 (*Web Server*)

Objectiu: disposar d'un servir web server basat en APache2 (alternativa Nginx)

Apache2 és probablement el més utilitzat per la seva versatilitat i prestacions però per moltes transaccions es recomana Nginx.

Instal·lació: **apt install apache2** -> URL: localhost/IP/nom_MV si tenim DNS obtindrà */var/www/html/index.html*
*DocumentRoot: /var/*www/*html*

Configuració: */etc/apache2* hi ha **-available *-enabled* i ordres com **a2(en|dis)site nom.conf** (per defecte 000-default.conf)

```
<VirtualHost *:80>
        #ServerName www.example.com
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Com fer una redirecció des de un server a un altre: podem agafar els paquets en capa 3 i canviar-les l'IP del nou server.
iptables -t nat -A PREROUTING -i ens3 -p tcp --dport 80 -j DNAT --to 20.20.20.X:80
Com configurar https: http://openaccess.uoc.edu/webapps/o2/handle/10609/60685
(link a la pàgina 31 d'adm. servidors)

Proxies

Un proxy, és un programa o dispositiu que realitza una acció en representació d'un altre, és a dir, actua com a intermediari entre dues màquines que desitgin connectar-se:

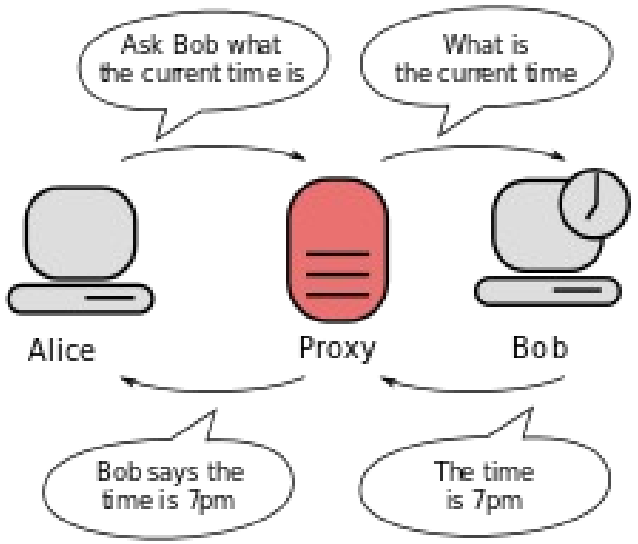
La ubicació estratègica de punt intermedi s'aprofita per a una sèrie de funcionalitats: proporcionar memòria cau, control d'accés, registre de trànsit, prohibir cert tipus de trànsit, etc.

L'objectiu més general és la de servidor intermediari (proxy server), que consisteix a interceptar les connexions de xarxa.

Motius: seguretat, rendiment, anonimat, etc.

En l'actualitat la funció més utilitzada és com web proxies, que permeten i/o faciliten l'accés a continguts de la World Wide Web.

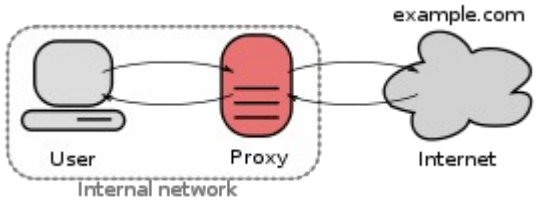
NO confondre amb NAT.



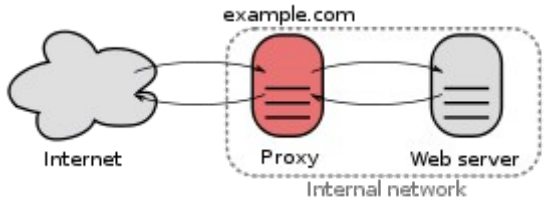
Proxies

Un Proxy server pot ser ubicat en diferents punts de la xarxa i rebrà diferents noms:

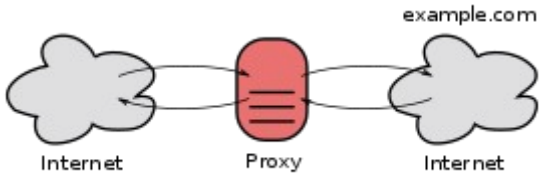
Forward: (són els més habituals) s'utilitza com concentrador de les peticions dels usuaris per obtenir recursos de qualsevol lloc (p.e. Internet).



Reverse proxy: és (generalment) un proxy utilitzat com front-end per controlar i protegir l'accés a una xarxa privada realitzant a més les tasques de load-balancing, authentication, decryption o caching.



Open proxy: Un tipus especial de forward proxy el qual és accessible a qualsevol usuari en Internet. S'estima que hi ha "cent de milers" de open proxies on the Internet. Un anonymous open servidor intermediari permet als usuaris escoder la seva IP quan accedeixen per la web o usant altres serveis (veure TOR)



Proxies: avantatges i desavantatges

Els proxies permeten:

Control/seguretat: pot limitar i restringir les connexions d'usuaris, i pot amagar web server dintre d'una xarxa interna.

Estalvi: Només el proxy ha de tenir els recursos necessaris (per exemple direcció pública, memòria, potència de còmput, ample de banda, ...) i no tots els usuaris de la xarxa interna.

Velocitat: Si diversos usuaris sol·liciten el mateix recurs el proxy pot fer memòria cau guardant la petició per donar-la després a l'usuari que la demani guanyant en velocitat i reduint l'ample de banda necessari per satisfer la petició.

Filtrat: El proxy pot negar-se a respondre algunes peticions si elles estan prohibides o analitzar el contingut per evitar que malware /dades privades que entran/surten de la xarxa.

Modificació: Com intermediari un proxy pot canviar la informació seguint unes regles o un algoritme predeterminat (per exemple traduint el contingut o adaptant el format d'acord a el dispositiu d'on es realitza la petició)

També (possibles) desavantatges:

Anonimat: El recurs destí només veurà a l'intermediari com a única direcció i no serà possible identificar l'usuari que la va realitzar i pot significar un problema si és necessari saber qui fa la petició.

Abús: atès que ha de rebre peticions i respondre a elles, és possible que rebi peticions no permeses i haurà de controlar qui té accés i qui no als seus serveis.

Càrrega: Com és el coll d'ampolla de totes les peticions serà generalment una màquina molt carregada i s'haurà de dimensionar per a això.

Privacitat/Intromissió: com és el pas obligat entre origen i destinació es tindrà registre de què entra i surt per la qual cosa algunes qüestions de privacitat poden quedar compromeses i sobretot si fa de memòria cau i guarda còpies dels dades.

Incoherència: Si és proxy cache, pot ser possible que la còpia local de el recurs sigui més vella que l'original però en els servidors actuals no existeix aquest problema pels mecanismes de coherència i control de versions que disposen.

Inseguretat aparent: Com el proxy representa més d'un server/usuari dóna problemes en molts escenaris com ara els que pressuposen una comunicació directa entre un emissor i un receptor (p.e. validació d'un certificat de servidor de domini en https).

Apache2 Reverse Proxy

Per configurar un reverse proxy (es a dir que les peticions que arribin a MV A les atendrà MV B): Instal·lar Apache2 en MV A i en MV B i modificar els index.html corresponents.

Carregar els mòduls corresponents: **a2enmod** ....

Per verificar els mòduls instal·lats: **apache2ctl -M**

Crear la configuració per a un virtual host: reverse.conf

```
<VirtualHost *:80>
        DocumentRoot /var/www/html
        ServerName proxy.gixpd.org
        ProxyRequests Off
        ProxyPreserveHost On
        ProxyPass / http:20.20.20.164/
        Proxyreverse / http://20.20.20.164/
</VirtualHost>
```

Test funcional: sobre A posar la URL de A (FQDN) i es veurà el index.html de B.

Test de càrrega: instal·lar el paquet apache2-utils per fer servir ab - Apache HTTP server benchmarking tool

p.e. **ab -c 100 -n 100 -r http://proxy.gixpd.org/**

[+ info, pag 36]

Administració de sistemes GNU/Linux (2016). Jorba i Esteve, Josep & Suppi Boldrito, Remo
http://openaccess.uoc.edu/webapps/o2/handle/10609/60687