Identificació, diagnosi, resolució i documentació d'incidències. Eines de gestió (NMS)

Xavier Marchador Márquez

Índex

Introducció

Les xarxes són una peça clau en la infraestructura de les empreses, independentment del sector al qual pertanyen. Avui dia, una degradació del servei de xarxa pot provocar pèrdues multimilionàries i aquest és precisament un dels motius principals pels quals la monitorització dels serveis és tan important.

Les xarxes han crescut en dimensions i en complexitat; cada vegada hi ha més usuaris, dispositius de tot tipus i varietat de fabricants. Tots aquests factors fan que administrar una xarxa i supervisar-ne el funcionament correcte requereixi tenir coneixements i eines específics per realitzar aquestes tasques.

És important que conegueu els problemes més habituals de les xarxes i els mecanismes que teniu a l'abast per detectar-los i solucionar-los. Tot i que la documentació disponible a Internet és immensa, és possible que alguna vegada no pugueu accedir a un terminal amb connexió, de manera que cal que conegueu comandes bàsiques del sistema operatiu que us facilitaran informació vital per al diagnòstic de la incidència.

Quan una xarxa augmenta en complexitat esdevé necessari disposar d'eines especialitzades que permetin gestionar-la. Aquestes eines anomenades *sistemes de monitoratge de xarxa* (NMS), les veureu al primer apartat d'aquesta unitat "Detecció i diagnosi d'incidències en xarxes locals", permeten recollir informació sobre l'estat dels dispositius i, si escau, fer-ne modificacions de la configuració, tant si és per fer una millora del servei com per aplicar una mesura de contingència en el cas que hi hagi una incidència en curs.

Segons el tipus de documentació que té una empresa, pot ser susceptible de rebre atacs informàtics amb l'objectiu d'aconseguir informació classificada o causar destrosses en el seu sistema informàtic. Per lluitar contra aquestes amenaces, disposeu d'eines especialitzades a detectar aquests comportaments i, en alguns casos, afrontar-los. Aquestes eines, anomenades *sistemes de detecció i prevenció d'intrusions* (IDPS) són cada vegada més necessàries a causa de la facilitat de realitzar atacs des de terminals connectats a Internet i les, cada vegada més habituals, connexions de banda ampla. Al segon apartat d'aquesta unitat, "Monitoratge de la xarxa local per a detecció de situacions anòmales", es tracten aquest tipus d'eines.

Per treballar els continguts d'aquesta unitat, és convenient fer les activitats i els exercicis d'autoavaluació, i llegir els annexos del material web.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Identifica comportaments anòmals dels dispositius de la xarxa local, i els atén i resol seguint uns procediments determinats.
    - Identifica incidències i comportaments anòmals.
    - Identifica si la disfunció és deguda a maquinari o a programari.
    - Monitora els senyals visuals dels dispositius d'interconnexió.
    - Verifica els protocols de comunicacions.
    - Restitueix el funcionament substituint equips o elements.
    - Soluciona les disfuncions de programari (configurant o reinstal·lant).
    - Elabora un informe d'incidències.
    - Enumera els procediments i les eines utilitzats per detectar incidències dels elements de comunicacions de la xarxa local, segons les especificacions d'un pla de contingències definit.
    - En una xarxa local es simulen avaries en els dispositius de la xarxa, per solucionar-los segons els procediments següents: identificar els símptomes del funcionament anòmal; caracteritzar tenint en compte els efectes produïts; formular una hipòtesi de la possible causa de la disfunció; descriure el pla d'intervenció per resoldre l'anomalia; aplicar el pla descrit i reparar el mal funcionament detectat i documentar les activitats realitzades.
2. Descriu les tècniques i els procediments de monitoratge de la xarxa local segons unes especificacions donades.
    - Identifica els paràmetres que identifiquen el rendiment d'una xarxa local tenint-ne en compte l'arquitectura i la tecnologia de xarxa de suport.
    - Enumera les eines de maquinari i de programari utilitzades en el monitoratge d'una xarxa local tenint-ne en compte les especificacions tècniques.
    - Explica el funcionament de les eines de gestió de la xarxa per obtenir informació del trànsit i el rendiment de les comunicacions de la xarxa local, segons especificacions tècniques de les mateixes eines.
    - Explica el procés que cal seguir per monitorar el trànsit d'una xarxa local segons les topologies i els protocols de xarxa implementats.
    - Descriu els procediments de resolució d'incidències segons el pla de manteniment preventiu i periòdic.

1. Detecció i diagnosi d'incidències en xarxes locals

Una tasca habitual en el món de les xarxes de dades és diagnosticar problemes o mals funcionaments. Les xarxes estan formades per múltiples dispositius que en un moment o un altre es poden espatllar. Per tant, quan això passi caldrà que siguem capaços d'identificar quin o quins components funcionen d'una manera incorrecta.

No sempre serà fàcil localitzar els components o els dispositius defectuosos; per això caldrà tenir clar com funciona tota la xarxa per tal d'identificar els segments que presentin un comportament anòmal i fer-los servir com a punt de partida per analitzar-la minuciosament.

Disposem de diverses eines i procediments que ens proporcionaran les pautes que hem de seguir per analitzar minuciosament els components de la xarxa i la informació necessària per diagnosticar-ne l'estat.

1.1 Procediments de diagnòstic d'incidències en xarxes locals

Per saber diagnosticar si hi ha cap problema en la xarxa, de primer heu de tenir clar què considereu una incidència i sobre la base de quins indicis o registres històrics ho compareu.

El sistema base us permetrà tenir un punt de referència a l'hora de comparar l'activitat de la xarxa en un moment determinat amb registres anteriors.

No hi ha un procediment únic per diagnosticar un problema, ja que cada tècnic se'n va creant un de propi, fruit de l'experiència. No obstant això, hi ha certes pautes o comportaments recurrents en qualsevol departament de TIC a l'hora de supervisar una xarxa.

Una de les tasques més habituals és revisar els registres (*logs*) de les diferents aplicacions d'administració de xarxes (NMS), els quals indicaran si algun dispositiu ha deixat de funcionar o bé no funciona adequadament.

Una altra activitat habitual és revisar les gràfiques que mostren el trànsit que circula per la xarxa. Com que poden emmagatzemar registres anteriors, podreu comparar la utilització de l'enllaç de comunicacions en aquell moment amb la que s'ha fet en dies o setmanes anteriors.

Altres eines com els sistemes de detecció i prevenció d'intrusions us proporcionen molta informació sobre els esdeveniments que ocorren en la xarxa i poden mostrar diverses pautes de comportament susceptibles d'indicar l'existència d'un problema de seguretat. Entendre com funcionen aquests sistemes, familiaritzar-se

amb la informació que proporcionen i com la mostren i estar habituat a revisar-la i analitzar-la és un dels procediments o tasques que haureu de dur a terme per tal de diagnosticar problemes en la xarxa.

Finalment, i no per això menys important, és recomanable revisar de tant en tant les instal·lacions físiques (és a dir, el centre de dades on són els armaris de comunicació) i revisar de manera visual els equips que hi ha, mirant de localitzar indicadors de llum d'alarma, cables desconnectats i, en general, qualsevol degradació física que pugui afectar les comunicacions en aquell moment o en un futur proper.

1.2 Eines de diagnòstic d'incidències

Per tal de detectar i intentar trobar la font del problema d'un mal funcionament de la xarxa, teniu diverses eines, algunes de les quals seran programes i utilitats inclosos en el sistema operatiu i d'altres, eines en forma de dispositius o aparells.

Haureu d'analitzar la informació que obtindreu d'aquestes eines per fer-vos una idea del que succeeix en la xarxa. Veureu que no hi ha una eina universal i definitiva que us digui directament quin és el problema o com se soluciona, sinó que normalment haureu de fer servir diverses eines i utilitats amb el resultat de les quals podreu fer el vostre diagnòstic.

Com que no sempre tindreu totes les eines existents a l'abast i haureu d'intentar resoldre la incidència amb les eines de què disposeu en aquell moment, és important conèixer diverses eines que tinguin la mateixa funció o funcions similars.

1.2.1 Eines incloses en el sistema operatiu

Distribució

El sistema operatiu Linux, igual que l'Unix, està disponible amb el format de distribucions: un conjunt format pel nucli del sistema operatiu i un paquet de programari i biblioteques del sistema que pot variar segons la distribució.

Quan es treballa monitorant i diagnosticant incidents de xarxa, hi ha la possibilitat de fer servir un ventall de sistemes operatius més ampli que el que empra un usuari mitjà.

Els sistemes operatius d'entorn d'usuari més comuns avui en dia són principalment el Microsoft Windows i, cada vegada més, el GNU/Linux. En el cas del primer, en podeu trobar diferents versions, totes del mateix fabricant, i, en el cas del segon, en podeu trobar variacions segons la distribució. Cal destacar que també existeixen distribucions *Live* de GNU/Linux especialitzades en la diagnosi de les xarxes. Són distribucions capaces d'arrencar des del seu suport sense haver estat instal·lades a la màquina. També se les anomena distribucions Live CD o Live DVD o Live USB, segons el seu suport.

Altres sistemes operatius que podeu fer servir en entorns de xarxa són els Unix, també amb diferents distribucions com HP/UX, SCO Unix, Open BSD, Solaris, etc.

Les ordres més habituals dels sistemes operatius dependran del tipus de sistema operatiu que feu servir, si bé és probable que sobretot utilitzeu el Windows i el Linux, ja que actualment són molt populars i sovint apareixen noves versions i millores de les funcionalitats actuals.

Les ordres bàsiques que haureu de fer servir són les següents:

- ping
- telnet
- arp
- traceroute
- netstat
- nslookup
- tcpdump

ping

La utilitat PING (*Packet interNet Groper*) serveix per comprovar l'estat de la connexió entre un equip i un altre. Aquesta utilitat envia un paquet de sol·licitud d'eco (*echo request*) a un equip i espera que aquest respongui mitjançant un paquet de resposta (*echo reply*). Una dada que també ens proporciona aquesta utilitat és la latència que hi ha entre els dos equips, és a dir, el temps que triga a arribar la resposta.

Amb aquesta utilitat podeu detectar primer de tot si hi ha comunicació a nivell d'IP o si hi ha congestió a la xarxa, comprovant els valors de latència respecte dels valors habituals.

```
1 test@ioc:~$ ping -c 4 www.google.es
2 PING www.l.google.com (209.85.229.99) 56(84) bytes of data.
3 64 bytes from ww-in-f99.1e100.net (209.85.229.99): icmp_seq=1 ttl=252 time=85.1
      ms
4 64 bytes from ww-in-f99.1e100.net (209.85.229.99): icmp_seq=2 ttl=252 time=63.2
      ms
5 64 bytes from ww-in-f99.1e100.net (209.85.229.99): icmp_seq=3 ttl=252 time=80.9
      ms
6 64 bytes from ww-in-f99.1e100.net (209.85.229.99): icmp_seq=4 ttl=252 time=107
     ms
7 --- www.l.google.com  ping statistics ---
8 4 packets transmitted, 4 received, 0% packet loss, time 3005ms
9 rtt min/avg/max/mdev = 63.244/84.164/107.258/15.674 ms
```

Aquesta ordre ha enviat mitjançant el paràmetre "- C4" quatre peticions de tipus *echo request* al servidor web de google.es i segons els resultats obtinguts en les estadístiques del final, s'han rebut quatre respostes; no s'ha perdut cap paquet i es mostra per cada paquet el temps de resposta.

telnet

Aquesta ordre, a part d'utilitzar-se per establir connexions de terminal amb els equips de xarxa, també us permet comprovar si un servei determinat està accessible sondejant el port de comunicacions TCP que fa servir l'aplicació. El podeu emprar quan creieu que el servei en qüestió no està operatiu, o bé quan penseu que el servei està operatiu, però hi ha algun filtre de xarxa o tallafoc que impedeix que el servei sigui accessible.

```
test@ioc:~$ telnet www.ioc.cat 80
Trying 85.192.111.244...
Connected to ioc.cat.
Escape character is '^]'.
```

En aquesta ordre podeu veure com hem comprovat, mitjançant un telnet al port 80, que el servidor web està operatiu i és accessible correctament; per tant, no hi ha cap tallafoc que ens n'impedeixi l'accés.

És important que conegueu els ports més comuns que fan servir les aplicacions per tal de poder usar l'ordre correctament.

arp

Aquesta ordre permet manipular el registre d'entrada ARP (*Adress Resolution Protocol*) del sistema. És a dir, possibilita saber quina adreça física MAC té un equip de la mateixa xarxa local a partir de la seva adreça IP. Això es fa servir sobretot per conèixer si un equip està connectat a la xarxa i no respon al ping. Si l'equip no està en la mateixa xarxa, a nivell 2, l'ordre no mostrarà els valors, ja que no pot saltar de xarxa.

```
test@ioc:~# arp
Address                  HWtype  HWaddress           Flags Mask
    Iface
192.168.1.200                    (incomplete)                              eth0
192.168.1.90             ether   00:c0:f0:30:c9:7b   C                     eth0
192.168.1.1              ether   00:1b:11:99:54:d3   C                     eth0
```

L'adreça 192.168.1.200 no mostra cap adreça física perquè no existeix en la xarxa (*incomplete*), no hi ha cap equip que la tingui assignada. En canvi, les altres dues adreces sí que existeixen i estan operatives. La manera d'aconseguir veure si l'equip 192.168.1.200 està disponible és fer-li en primer lloc un ping i després consultar la taula ARP. Passada una estona, les entrades en la taula ARP que no són vàlides i les entrades d'adreces que no generen trànsit de dades desapareixeran.

Nombre de salts

Cada vegada que un paquet de dades arriba a un encaminador a través d'una de les seves interfícies de xarxa i aquest el reenvia una altra vegada per una interfície diferent es considera que hi ha hagut un salt. Així doncs, cada vegada que un paquet travessa un encaminador, el nombre de salts s'incrementa en un.

traceroute

Aquesta ordre permet veure pas per pas el recorregut dels paquets des de l'origen fins a l'equip de destinació. Podreu obtenir dades molt útils per veure els operadors de xarxa pels quals passen els paquets, el temps que triga a arribar a cada xarxa i el nombre de salts necessaris per arribar a la màquina de destinació.

```
test@ioc:~$ traceroute www.google.es
traceroute to www.google.es (209.85.229.99), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  12.808 ms  12.718 ms  11.919 ms
 2  1.14.221.87.dynamic.jazztel.es (87.221.14.1)  50.712 ms  50.581 ms  50.480
    ms
 3  * * *
 4  178.216.106.212.static.jazztel.es (212.106.216.178)
181.236 ms 162.216.106.212.static.jazztel.es (212.106.216.162)
180.256 ms 34.217.106.212.static.jazztel.es (212.106.217.34)  179.980 ms
 5  49.217.106.212.static.jazztel.es (212.106.217.49)  47.562 ms  63.532 ms
    63.622 ms
 6  195.81.199.61 (195.81.199.61)  46.136 ms  38.610 ms  38.496 ms
 7  xe-2-0-0-0.mil-cal-score-2-re1.interoute.net (217.118.118.230)
 50.379 ms  100.204 ms  101.497 ms
 8  ae0-0.mil-cal-score-1-re1.interoute.net (89.202.146.85)  89.484 ms
91.407 ms  108.304 ms
 9  74.125.50.69 (74.125.50.69)  101.136 ms  103.023 ms  106.183 ms
10  216.239.47.128 (216.239.47.128)  107.753 ms 209.85.249.54 (209.85.249.54)
107.574 ms 216.239.47.128 (216.239.47.128)  108.761 ms
11  209.85.251.113 (209.85.251.113)  110.526 ms  113.420 ms 209.85.249.234
(209.85.249.234)  68.674 ms
12  209.85.248.182 (209.85.248.182)  81.886 ms 72.14.232.208 (72.14.232.208)
81.650 ms 209.85.250.140 (209.85.250.140)  110.088 ms
13  72.14.232.130 (72.14.232.130)  84.359 ms  84.301 ms 209.85.255.212
(209.85.255.212)  81.087 ms
14  209.85.251.231 (209.85.251.231)  82.884 ms  95.714 ms  88.722 ms
15  ww-in-f99.1e100.net (209.85.229.99)  93.114 ms  96.392 ms  93.716 ms
```

Com a màxim, es poden veure 30 salts i no sempre obtindreu les dades que voleu, ja que aquest protocol també es basa en l'ICMP, igual que el ping, i és bastant habitual que els operadors de xarxa filtrin aquest tipus de paquets per evitar que aquesta informació s'obtingui. En la tercera línia podeu veure que apareixen uns asteriscos quan la informació està filtrada.

netstat

Aquesta utilitat us proporciona moltíssima informació de la xarxa associada a l'equip en què s'executa. Podeu obtenir informació de les connexions de xarxa (un equip pot pertànyer a més d'una xarxa segons les interfícies de xarxa i la configuració que tingui), la taula d'encaminament, estadístiques sobre les interfícies de xarxa i informació sobre l'estat dels ports de comunicacions.

Per exemple, per saber quina és la taula de rutes de l'equip heu de fer servir els paràmetres –nr.

```
test@ioc:~$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
```

Aquí podeu veure que pertany a la xarxa 192.168.1.0 255.255.255.0 i que la porta d'enllaç és la 192.168.1.1.

Amb uns altres paràmetres, podeu veure les connexions de xarxa que teniu establertes i els serveis locals que ofereix la màquina:

```
root@ioc:~#netstat -natp
```

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/
    Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2501/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1008/
    cupsd
tcp        0      0 192.168.1.114:55613     209.85.229.105:80       ESTABLISHED 2295/
    firefox
tcp        0      0 192.168.1.114:48763     74.125.77.91:443        ESTABLISHED 2295/
    firefox
tcp6       0      0 :::22                   :::*                    LISTEN      2501/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      1008/
    cupsd
```

SSH

El *secure shell* (SSH) és un protocol de xarxa segur que permet intercanviar dades entre dos dispositius de xarxa de manera xifrada, a diferència del Telnet, que ho fa en text pla.

Amb la informació proporcionada per aquesta ordre podeu veure que sobre el port 22 de TCP teniu escoltant el servei de SSH en totes les interfícies de xarxa del dispositiu (0.0.0.0:22), el qual acceptarà connexions entrants mitjançant aquest protocol.

També podeu veure que únicament el servei de gestió d'impressores CUPS escolta l'adreça de xarxa local 127.0.0.1 en el port 631.

Quant a connexions establertes, es mostra que hi ha una connexió entre l'adreça IP de la màquina, la 192.168.1.114, en el port 80 de la 209.85.229.105, que es correspon amb una pàgina web, i una segona connexió amb l'adreça 74.125.77.91 en el port 443, que es correspon amb una pàgina web xifrada.

És important veure que l'estat de la connexió és ESTABLISHED per a les connexions establertes o LISTEN per als serveis que estan disponibles per rebre connexions d'altres màquines remotes. El camp proto us indicarà el protocol que fa servir el procés, entre els quals podeu trobar tcp, udp, tcp sobre IPv6, etc.

Estats d'una connexió TCP/IP

A part de l'estat ESTABLISHED i LISTEN, hi pot haver molts altres estats, com, per exemple, SYN_SENT, FIN_WAIT1, TIME_WAIT,CLOSE, etc. Consulteu la documentació del NETSTAT corresponent al sistema operatiu que esteu fent servir per tal de saber què indica cada estat i quins són els paràmetres de funcionament corresponents.

nslookup

L'ordre *nslookup* permet consultar els servidors de noms (*DNS servers*). Diversos tipus de consulta permeten conèixer l'adreça IP d'un equip determinat a partir del nom, o conèixer el nom a partir de l'adreça IP, etc. Són bastant habituals els problemes de xarxa causats per errors en els servidors de DNS, ja que moltes aplicacions els fan servir i algunes no poden funcionar sense aquests servidors.

Els paràmetres més habituals de l'nslookup són els següents:

```
test@ioc:~$ nslookup www.ioc.cat
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.ioc.cat     canonical name = ioc.cat.
Name:   ioc.cat
Address: 85.192.111.244
```

En aquesta ordre hem preguntat al servidor de DNS per defecte (192.168.1.1) que ens digui quina adreça IP correspon a la màquina www.ioc.cat i ens ha contestat que l'adreça és 85.192.111.244.

Ara li preguntarem el contrari, que ens indiqui quin nom correspon a l'adreça IP 85.192.111.244.

```
test@ioc:~$ nslookup 85.192.111.244
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
244.111.192.85.in-addr.arpa     name = ioclabs.xtec.net.

Authoritative answers can be found from:
```

En aquest cas, podeu apreciar que el nom obtingut a partir de l'adreça IP (ioclabs.xtec.net) no es correspon amb el que inicialment havíem fet servir per cercar l'adreça IP (www.ioc.cat). Això de vegades és així perquè els registres de DNS directe i DNS invers es gestionen de manera independent i, segons les necessitats de cada xarxa, pot ser necessari que els valors siguin diferents. No obstant això, hi ha certes aplicacions que requereixen que els dos registres, directe i invers, tinguin els mateixos valors exactes, ja que, si no, l'aplicació no funcionarà correctament.

tcpdump

Aquesta utilitat està disponible en plataformes Linux/Unix i és un analitzador de paquets que permet capturar els paquets de dades segons els paràmetres que definiu. Podeu fer servir paràmetres com ara l'adreça IP d'origen, IP destinació, tipus de paquet TCP, UDP, IP, etc.

L'ordre següent permet capturar tots els paquets TCP que s'originen en l'adreça IP 192.168.1.103 i van destinats a la pàgina web del Google.

```
test@ioc:~# tcpdump  -nni eth0 src 192.168.1.103 and dst www.google.es and
    proto TCP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13:46:13.666083 IP 192.168.1.103.48740 > 209.85.229.104.80: Flags [S], seq
    1533389292,
win 5840, options [mss 1460,sackOK,TS val 185799 ecr 0,nop,wscale 6], length 0
13:46:13.738090 IP 192.168.1.103.48740 > 209.85.229.104.80: Flags [.], ack
    4192696082,
win 92, options [nop,nop,TS val 185817 ecr 60244455], length 0
13:46:13.748621 IP 192.168.1.103.48740 > 209.85.229.104.80: Flags [P.], seq
    0:386, ack 1,
win 92, options [nop,nop,TS val 185819 ecr 60244455], length 386
13:46:13.869517 IP 192.168.1.103.48740 > 209.85.229.104.80: Flags [.], ack
    1419, win 137,
options [nop,nop,TS val 185850 ecr 60244585], length 0
13:46:13.869654 IP 192.168.1.103.48740 > 209.85.229.104.80: Flags [.], ack
    2837, win 182,
options [nop,nop,TS val 185850 ecr 60244585], length 0
13:46:13.870784 IP 192.168.1.103.48740 > 209.85.229.104.80: Flags [.], ack
    4255, win 227,
options [nop,nop,TS val 185850 ecr 60244585], length 0
```

El *tcpdump* admet molts paràmetres en la línia d'ordres, però els més habituals són:

- SRC: indica l'adreça IP o *host* d'origen.
- DST: indica l'adreça IP o *host* de destinació.
- PROTO: indica el protocol que voleu capturar.
- And: serveix per unir diverses condicions.

1.2.2 Eines de diagnòstic especialitzades: analitzadors lògics i analitzadors de cablatge

Els analitzadors de cablatge us permeten comprovar si un cable és correcte o si té cap problema que n'impedeixi l'ús. És útil sobretot comprovar els cables abans d'instal·lar-los en les infraestructures, ja que moltes vegades s'han de fer tirades llargues i, per tant, cal fer obres per ubicar-los. No és gens recomanable descobrir que el cable no funciona una vegada finalitzada la instal·lació.

Si el cablatge que instal·leu és de tipus troncal, és a dir, un dels cables de dades principals de la infraestructura, és recomanable analitzar-lo mitjançant un analitzador lògic i certificar que compleix els requisits de les normatives vigents, ja que no sempre n'hi haurà prou que el cable funcioni més o menys, sinó que ho haurà de fer al cent per cent per garantir la integritat de les dades.

Temps de latència

El temps que triga un paquet de dades a viatjar des de l'origen fins a la destinació es coneix com a *temps de latència*. Aquest temps serà més elevat com més gran sigui la distància fins a la destinació i el nombre d'equips de xarxa existents en el camí.

Un dels problemes més habituals amb què us trobareu són les degradacions de serveis. Quan una xarxa o una part de la xarxa no funciona gens ni mica perquè no hi ha cap tipus de trànsit, és més senzill diagnosticar la font del problema; per a això teniu a disposició diverses eines de programari i de maquinari, com els analitzadors de cablatge, que us permetran comprovar si els enllaços funcionen o no. A més a més, els indicadors visuals de les llums d'estat dels connectors dels equips de xarxa també canvien de color si es detecta senyal o no; per tant, també podeu fer servir aquesta ajuda visual.

Quan el problema de la xarxa és la degradació del servei, les intermitències, les congestions o la velocitat molt lenta en moments determinats, haureu de fer servir eines avançades, com els analitzadors lògics, i dedicar més temps a analitzar la informació obtinguda per tal de deduir què causa el problema.

Les estadístiques proporcionades per utilitats com el *ping*, el *traceroute* i el *netstat* us serviran per veure quins enllaços són els que funcionen incorrectament gràcies als temps de latència i les pèrdues de paquets. A vegades diversos errors poden tenir símptomes similars, ja que al cap i a la fi el funcionament de la connexió depèn del cablatge, dels connectors, dels equips de xarxa, dels protocols de xarxa i dels protocols d'aplicació com el DNS, l'HTTP, etc.

La normativa de cables

Hi ha diverses normatives o estàndards de cables que defineixen les característiques que han de complir els cables i els connectors segons la llargària i l'ús. Les normatives per a cablatge estructural d'edificis més conegudes són l'ANSI/TIA EIA-568A i l'ANSI/TIA/EIA-568B.

No obstant això, els problemes ocasionats en els nivells inferiors, com el físic, tenen moltes possibilitats de ser-ne la causa i és recomanable comprovar-ho.

Si un cable té una llargària superior a la que estableix la normativa, si els connectors són de qualitat inferior als recomanats o si algun segment del cable està pinçat o malmès, es poden produir degradacions en comptes de talls complets.

Gràcies als analitzadors lògics podreu obtenir tota classe de dades relatives a les característiques del cable, com ara la llargària real, la potència de senyalització, l'estat del connector, etc. que us serviran per comparar-les amb els valors esperats. Si el cablatge no està en bones condicions caldrà substituir-lo.

1.3 Detecció i identificació d'incidències. Tipus d'incidència

Hi pot haver molts problemes en les xarxes i no sempre serà senzill classificar-los en un grup o en un altre, ja que a vegades un problema deriva en un altre i fa que es pugui classificar en més d'una categoria. No obstant això, simplificant al màxim els tipus d'incidències, us podreu trobar les següents:

- Degradacions del servei
- Talls en el servei

Tant si es tracta d'una degradació com d'un tall, pot afectar tota la xarxa o un segment. Això dependrà en bona part de la topologia física i lògica de la xarxa. Les causes que poden provocar un tipus d'incidència o un altre són les següents:

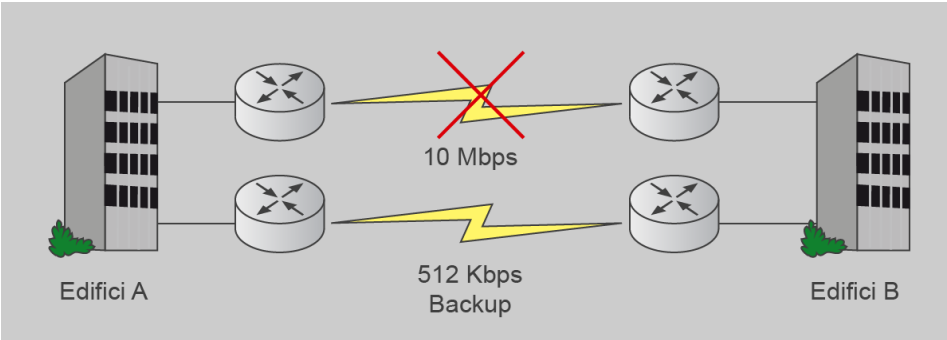
- Problemes físics en els components o dispositius (cables en mal estat, connectors incorrectes o defectuosos, equips de comunicació amb problemes de ventiladors, memòria, etc.).
- Equips de xarxa que funcionen per sobre de les seves possibilitats (enllaços sobrecarregats, falta de potència de commutació de paquets, manca de memòria, etc.).
- Mala configuració (filtres que bloquegen el trànsit, encaminament de paquets per rutes incorrectes, etc.).
- Altres causes (tallafocs, atacs informàtics, errors en el sistema operatiu del maquinari, etc.).

També es poden donar combinacions de diversos factors, com, per exemple, que una mala configuració en les taules d'encaminament d'un encaminador faci que el trànsit que, en teoria s'hauria de dividir per dos camins diferents, vagi tan sols per un i provoqui que aquest enllaç se sobrecarregui, o bé perquè l'equip secundari no té prou potència o bé perquè les línies de dades no són prou ràpides.

Podem trobar-ne un exemple en una empresa que té contractada una línia principal dedicada amb un operador perquè les dues seus de l'empresa que són en ciutats

diferents estiguin interconnectades amb una xarxa privada virtual. Aquesta línia principal té una capacitat de 10 Mbps (figura 1.1).

FIGURA 1.1. Línies principal i secundària entre seus diferents



Com que l'ús d'aquesta connexió és imprescindible, l'empresa opta per contractar una segona línia de seguretat (*backup*), però, com que aquest tipus de línies són costoses, s'opta per adquirir la secundària de menys capacitat; per exemple, de 512 kbps.

En condicions normals, si el trànsit regular de l'empresa és de 256 kbps, n'hi haurà prou amb la línia secundària en cas que caigui la primera. No obstant això, si la caiguda de l'enllaç primari es produeix a la nit, quan es fan les còpies de seguretat remotes de la seu B a les oficines principals, les quals necessiten una amplada de banda de 2 Mbps i el trànsit es deriva per l'enllaç secundari de 512 Kbps, aquest es col·lapsarà per falta de capacitat de la línia secundària i es produirà una degradació del servei.

1.4 Resolució d'incidències de la xarxa local. Substitució dels elements de maquinari i programari dels dispositius de xarxa

Abans de substituir un element de programari o maquinari d'un dispositiu de xarxa, heu de tenir clar el motiu pel qual feu el canvi o l'actualització. És a dir, què espereu aconseguir amb el canvi i si realment és imprescindible fer-lo, mirar si un cop fet pot afectar en res el funcionament de la resta de dispositius.

Quan es canvia una targeta de comunicacions per afegir més ports o millorar les prestacions respecte de les actuals, heu de considerar que és possible que a l'altre extrem de la connexió també s'hagi de canviar algun component, ja que potser no és compatible una targeta amb l'altra. Per exemple, no podeu posar en un extrem una targeta de comunicacions de fibra òptica monomode i en l'altre extrem una targeta multimode, ja que fan servir mètodes de transmissió diferents.

Fibra òptica monomode o multimode

Depenent de com es propaga el feix de llum dins un cable de fibra òptica, podeu trobar fibres monomode i multimode. La fibra monomode tan sols fa servir un feix de llum, mentre que la multimode n'empra diversos alhora. En distàncies curtes s'utilitzen principalment multimode, ja que és més econòmica pel fet que usa LED com a font de transmissió, mentre que la monomode sol fer servir làser.

L'actualització del programari del dispositiu de xarxa és un procés delicat pel fet que un problema durant l'actualització o una mala elecció de la versió del sistema operatiu que fareu servir pot deixar el dispositiu inoperatiu. A més a més, atesa la gran quantitat de versions de sistema operatiu que hi ha per a un mateix dispositiu, pot ser complicat encertar la versió idònia.

Tingueu en compte que, quan es fa una actualització, es pretén que, a part d'incorporar les noves prestacions, el sistema operatiu continuï integrant la resta de protocols i característiques que ja tenia l'altre sistema; si no, pot ser que alguns serveis de la xarxa deixin d'estar suportats amb la nova versió perquè han quedat obsolets. De fet, aquest problema és més freqüent del que sembla. Hi ha xarxes que fa molts anys que estan operatives amb protocols que en el moment que es van crear eren comuns o els més adients i que, amb el pas del temps, han quedat en desús o s'han substituït per d'altres que ofereixen millors prestacions. No és estrany, doncs, que en substituir la versió del sistema operatiu per una de més actual us trobeu que alguna característica que fèieu servir no estigui suportada amb la nova versió.

És important que, si detecteu problemes de xarxa estranys o que, aparentment, no pugueu associar a deficiències dels elements físics o a problemes de configuracions, reviseu si últimament s'ha fet alguna actualització del sistema operatiu d'un dispositiu de xarxa o si s'ha substituït alguna targeta.

Carregar el fitxer de configuració

Segons la marca i el model del dispositiu de xarxa, el procediment per carregar la configuració pot variar. No obstant això, habitualment n'hi haurà prou de transferir-la per TFTP o fer un "copia i enganxa" entre la finestra de terminal amb accés a la consola de l'equip de xarxa i el terminal on tingueu la còpia de la configuració en format text pla.

És interessant que, quan dugueu a terme les actualitzacions dels dispositius, feu còpia de la versió actual del sistema operatiu i de la configuració que utilitzeu. Una vegada feta l'actualització del sistema operatiu, haureu de restaurar la configuració de la versió anterior.

Quan feu una actualització a una versió nova del sistema operatiu d'un dispositiu de xarxa, és important que de primer us centreu a aconseguir que el nou sistema operatiu funcioni de la mateixa manera que ho feia l'anterior. És a dir, en primer lloc instal·lareu el nou sistema operatiu, després carregareu el fitxer de configuració i comprovareu que totes les ordres i instruccions continuen suportades. En cas que no sigui així, el sistema operatiu us mostrarà algun missatge que indica que aquesta característica no està disponible.

Una vegada el dispositiu està configurat i funciona amb el nou sistema operatiu i la configuració que ja teníeu desada, deixeu-lo en observació uns quants dies abans d'activar les noves funcionalitats per veure si el dispositiu és estable i es comporta com espereu. Quan considereu que tot funciona correctament, serà el moment de fer les modificacions pertinents en la configuració per activar les noves funcionalitats.

L'ordre dels passos que heu de seguir per minimitzar l'impacte en la xarxa que pot tenir l'actualització del sistema operatiu d'un dispositiu i així disposar de noves funcionalitats és el següent:

1. Fer una còpia de seguretat del sistema operatiu actual i de la configuració corresponent.
2. Instal·lar o actualitzar el nou sistema operatiu.
3. Carregar la configuració anterior del dispositiu i comprovar que totes les característiques i funcionalitats continuen disponibles.
4. Tenir uns quants dies el dispositiu en observació per tal de comprovar que no es produeix cap problema i que funciona tal com ho feia abans del canvi de sistema operatiu (o més bé).

5. Configurar el dispositiu amb les noves funcionalitats que voleu activar.

6. Tenir en observació uns quants dies el dispositiu i verificar que les noves funcionalitats no entren en conflicte amb el funcionament de la xarxa i que la resta de dispositius no es veuen afectats d'una manera negativa.

En definitiva, heu de comprovar l'impacte que produeix el canvi en la xarxa i l'efecte que té en la resta de components i dispositius. Documenteu acuradament tots els canvis i modificacions que feu per tal que, si es produeix cap incidència, sigui més fàcil fer-ne el seguiment i així solucionar el problema de la manera més ràpida possible.

1.5 Verificació posterior del funcionament correcte del maquinari dels dispositius de xarxa

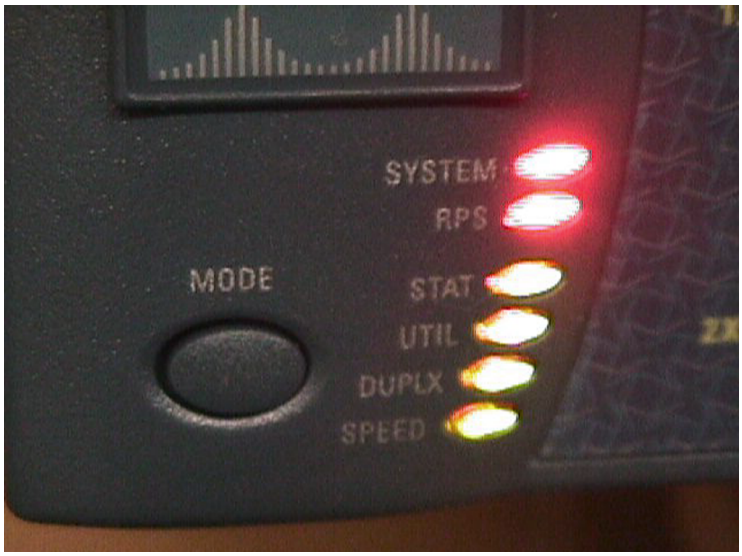
Per comprovar el funcionament correcte del maquinari una vegada fet el canvi d'elements de maquinari i de programari, serà important que verifiqueu *in situ* tots els elements que siguin visibles dels dispositius. Fixeu-vos principalment ens els dos extrems de la connexió.

LED

LED és l'acrònim de *light-emitting diode*, i és un dispositiu semiconductor que emet llum en un espai reduït.

Els LED d'estat us donaran informació important sobre l'estat de les connexions (figura 1.2). Segons la marca i el model del dispositiu, les combinacions de colors que indiquen l'estat poden ser diferents, però principalment us mostraran si l'enllaç està operatiu o si no ho està i, en cas d'estar-ho, si hi ha trànsit o si no n'hi ha. Altres informacions que us poden proporcionar és el percentatge d'utilització de l'enllaç.

Figura 1.2. Llums d'estat d'un commutador CISCO



Un enllaç no sempre té el mateix flux de dades; de fet, si la xarxa funciona correctament, el volum de trànsit no hauria de ser superior al 50% i, en cas d'estar permanentment al 100%, pot indicar que hi ha congestió. Un enllaç de xarxa ha

d'estar preparat per assolir puntes de trànsit: per aquest motiu sempre hi ha d'haver amplada de banda de sobres per poder absorbir aquests pics.

A part de les comprovacions visuals, és important verificar les connexions més habituals com ara Internet, que els servidors són accessibles, que hi ha connectivitat amb les seus externes de l'empresa, etc.

Depenent del dispositiu que actualitzeu, es podran veure afectats més o menys serveis. Si l'equip en qüestió és un equip troncal de la xarxa, del nucli de les comunicacions, serà relativament fàcil veure si hi ha cap problema important, ja que en cas de fallida molts serveis es veuran afectats de cop. No obstant això, si l'equip que heu actualitzat no és un equip principal de la xarxa i ofereix serveis secundaris o connectivitat a uns certs usuaris o serveis, és recomanable que dediqueu temps a revisar aquests serveis després de fer els canvis, ja que si no són d'ús habitual, és probable que no es detecti l'error fins que algú, en un moment donat, necessiti accedir al recurs. Si això es produeix uns quants dies després d'haver-ne fet l'actualització, és possible que ja no us recordeu detalladament del que vau fer o que el dia que es detecti el problema vosaltres no sigueu a l'oficina i la persona que hagi d'afrontar el problema no el sàpiga resoldre. Per això és tant important la documentació.

1.6 Verificació de la configuració, del funcionament correcte del programari dels dispositius de la xarxa i dels protocols de comunicació

Quan actualitzeu el sistema operatiu i carregueu la configuració anterior, reviseu amb molta cura els protocols de comunicacions. Comproveu que les versions del protocol que els diferents equips de la xarxa fan servir són les adequades, ja que alguns protocols disposen de diferents versions i, si en la xarxa no s'utilitzen les mateixes, hi pot haver inconsistències i problemes en el funcionament.

Protocols d'encaminament

Els encaminadors de xarxa fan servir el que es coneix com a *rutes* per prendre les decisions sobre el lloc cap on s'han d'enviar els paquets de dades que hi arriben segons la destinació. Per aprendre on estan situades les xarxes de destinació, es poden utilitzar protocols d'encaminament dinàmic com el RIP, l'EIGRP, l'OSPF, etc. Cadascun d'aquests protocols fa servir tècniques diferents per intercanviar informació de rutes entre els dispositius.

Comproveu que el TCP/IP està operatiu, reviseu que els protocols d'encaminament dinàmic, en cas d'estar actius, funcionen i que s'estan enviant i rebent actualitzacions. Comproveu que les taules d'encaminament són les correctes i que no s'han establert per error rutes secundàries com a principals o que determinades xarxes no són accessibles perquè falta la ruta o perquè hi ha hagut un error en l'establiment de la porta d'enllaç.

Si detecteu que alguna ruta no és la correcta o que els protocols de comunicacions no funcionen com esperàveu, activeu les funcions de depuració (*debug*) de l'equip que heu actualitzat i comproveu els valors que us mostra. Les opcions de depuració

són una eina molt útil que teniu a l'abast per poder trobar les causes del problema. Us mostrarà totes les operacions que fa l'equip amb la resta de dispositius, com ara l'intercanvi de paquets amb informació de l'estat de les connexions, les xarxes que hi ha disponibles, l'estat dels protocols d'encaminament com el RIP, l'EIGRP i l'OSPF, entre d'altres. També podreu veure l'estat i els ports que formen part de les diverses VLAN, camins redundants gestionats pel protocol arbre d'expansió (*spanning tree*), etc.

Spanning-tree

El protocol de xarxa arbre d'expansió (*spanning tree*) permet evitar que entre diversos commutadors es produeixin bucles que facin que la informació circuli d'una manera indefinida per la xarxa perquè hi ha camins redundants. Aquest protocol s'encarrega d'evitar això activant un camí i desbloquejant l'altre només quan el primer deixa d'estar disponible.

Tota aquesta informació us permetrà saber molt detalladament què passa dins l'equip de xarxa. No obstant això, activar aquestes funcions de depuració consumeix molts recursos de CPU i memòria de l'equip i, si activeu totes les opcions de depuració de cop, podeu provocar que l'equip se sobrecarregui i deixi de funcionar. Per tant, aneu activant i desactivant les funcions de depuració de mica en mica i descarteu problemes d'una manera selectiva. Activar totes les opcions de depuració de cop, a part de sobrecarregar l'equip i deixar-lo inoperatiu, no us servirà de res, ja que la quantitat d'informació que rebreu és tan gran que no sereu capaços de processar-la.

Sigueu selectius i aneu amb molta cura quan feu servir aquestes opcions de depuració i apreneu a interpretar la informació que rebeu. Per poder utilitzar aquesta informació i treure'n profit, caldrà que us familiaritzeu amb el format de les dades, que serà diferent segons el fabricant del dispositiu que empreu.

1.7 Elaboració d'informes d'incidències. Eines de disseny gràfic i documentació per a xarxes

Quan es produeix una incidència i se soluciona, cal redactar un informe que exposi els fets. Aquest informe pretén explicar com s'ha detectat la incidència, quines n'han estat les causes i quins serveis s'han vist afectats. La generació d'aquest informe ha de servir de guia per resoldre futurs problemes similars. Aquest informe ha d'anar acompanyat, sempre que sigui possible, de diagrames i gràfics que complementin el text explicatiu.

1.7.1 Elaboració d'informes d'incidències

Quan es produeix una incidència de xarxa, heu de redactar un informe que detalli el que ha passat. No hi ha un model únic ni un format obligatori per redactar aquest informe, ja que cada empresa pot tenir el seu propi model. No obstant això, en cas d'haver de dissenyar vosaltres el format de l'informe, assegureu-vos que conté com a mínim la informació següent:

- Nom i cognoms de la persona que ha detectat la incidència.
- Tipus d'incidència: seguretat, degradació del servei, caiguda total, etc.

- Equip(s)/servei(s) afectat(s): servidor, encaminador, ordinador usuari, aplicació, etc.
- Dia/hora de la incidència:
  - Dia/hora en què s'ha detectat.
  - Dia/hora en què es va produir la incidència.
  - Dia/hora en què es va resoldre o va finalitzar.
- Estat de la incidència: oberta/tancada/pendent.
  - Causa de la incidència: intencionada/accidental/desconeguda.
  - Àmbit de la incidència: local de l'empresa / extern en altres empreses.
  - Gravetat de la incidència: lleu/moderada/greu.
  - Descripció amb detalls de l'incident.
  - Procediment seguit per a la contingència/resolució.

Si es tracta d'un incident de seguretat en què heu patit una possible intrusió o s'ha fet alguna activitat maliciosa des dels equips de la vostra organització, caldria afegir-hi addicionalment la informació següent:

- Impacte de l'incident: denegació de servei / robatori d'informació / alteració d'informació / accés a dades confidencials / risc de reputació / altres.
- En cas que hi hagi altres empreses externes involucrades, cal especificar si necessiteu el seu suport.
- En cas que s'hagin produït pèrdues econòmiques a conseqüència de l'incident, cal quantificar-les.

1.7.2 Eines de disseny gràfic i documentació per a xarxes

Hi ha diverses eines que us serviran per documentar la xarxa, tant pel que fa a la ubicació dels equips de comunicació i servidors als armaris de tipus *rack* com pel que fa al disseny gràfic de la topologia física i lògica.

És igual d'important conèixer que l'encaminador A està connectat amb el commutador C mitjançant una fibra òptica com saber on estan físicament ubicats els dispositius, ja que en cas de perdre la gestió remota dels equips o haver d'actualitzar el maquinari, caldrà que hi accediu en persona, de manera que haureu de saber on estan situats. Com tot tipus de programes, n'hi ha de comercials i n'hi ha de programari lliure.

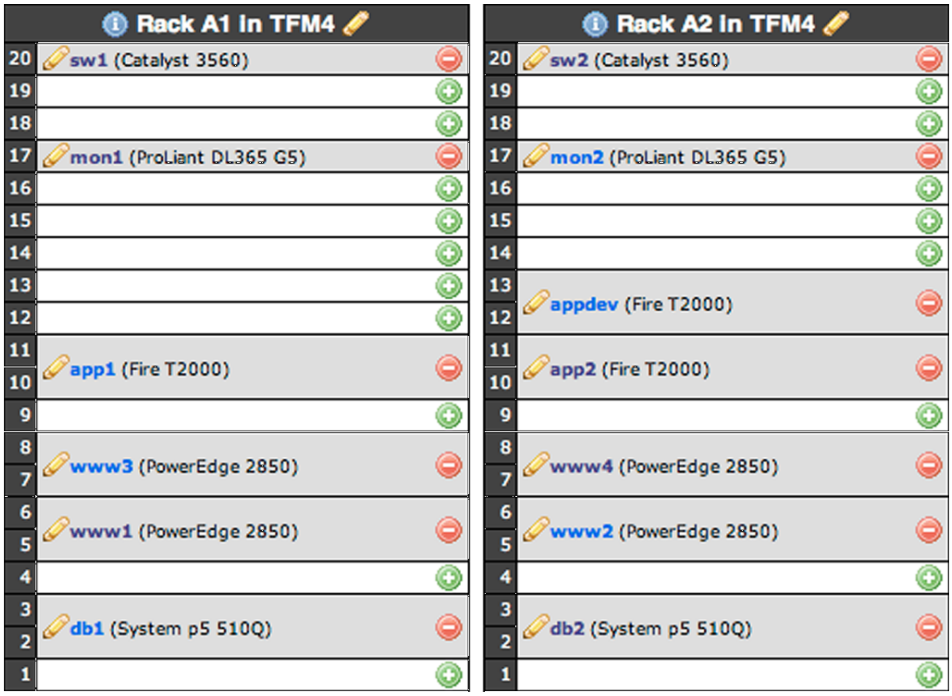
Armaris tipus rack

Els armaris *rack* són armaris metàl·lics que es fan servir en centres de dades per ubicar-hi a l'interior servidors i equips de comunicació, de manera que la manipulació quedi restringida al personal autoritzat. Aquests armaris divideixen l'espai en unitats anomenades *U*. El dispositiu pot ocupar diverses unitats de tipus U segons la mida que tingui.

Per dissenyar un esquema de xarxa manualment, és a dir, sense que ho faci un NMS de manera automàtica amb la informació obtinguda pels diferents sensors, podeu fer servir el programari comercial **Microsoft Visio** o programari lliure com el **Dia**, **Inkscape** o **Kivio**.

Per documentar els equips de xarxa podeu fer servir un programa de gestió documental, com, per exemple, el **Plone**, que permet generar documentació de tota classe, no únicament de xarxa, segons uns perfils que podeu escollir. També teniu el **RackMonkey**, el qual permet documentar tots els armaris *rack* (figura 1.3) que hi ha al centre de dades (CPD) i anotar quins equips o servidors hi ha en cada posició de l'armari i quines en són les característiques (fabricant, model, data de compra, venciment de la garantia, etc.).

Figura 1.3. Contingut de dos armaris rack documentats amb RackMonkey



1.8 Elaboració dels procediments per a la detecció d'incidències

Per poder detectar incidències, primer de tot cal que tingueu documentat el sistema base de la xarxa, és a dir, com es comporta habitualment en franges horàries diferents, i que conserveu un històric dels esdeveniments més rellevants que han succeït per poder comparar-los i poder discernir si una situació que *a priori* sembla anòmala ja ha passat amb anterioritat i quin va ser-ne el motiu. Igual d'important és que tingueu desplegat un mecanisme de monitoració amb sensors i una eina centralitzada NMS que s'encarregui de supervisar els equips i avisar en cas que es produeixi una incidència.

Els sistemes de detecció d'intrusions (IDS) i els sistemes de prevenció (IPS) són una eina complementària molt recomanable per a la detecció d'incidències. Els NMS habituals monitoren els equips intentant detectar problemes de mal funcionament, però no són capaços de fer servir tècniques heurístiques o fitxers de signatura per comprovar si els comportaments dels equips de la xarxa són normals o es corresponen amb un indici d'intrusió.

Els IDS haurien de ser una prioritat en la infraestructura de monitoratge i supervisió de la xarxa, atès que la informació que subministren és molt important.

Detectar un incident de seguretat a temps pot estalviar-vos molts problemes; minimitzarà l'impacte que aquest tindrà sobre la xarxa i, consegüentment, amb l'empresa, ja que al cap i a la fi una xarxa de comunicacions no deixa de ser una infraestructura de l'empresa per dur a terme la seva activitat comercial.

Quan tingueu tots els mecanismes de supervisió i monitoratge operatius, és important que definiu una línia d'actuació per comprovar la informació que rebeu de tots ells i així garantir el bon funcionament dels sistemes que administreu. Principalment, les tasques que heu de dur a terme d'una manera rutinària són:

Eines de monitoratge de trànsit

Les eines de monitoratge de trànsit, com el CACTI o l'MRTG, permeten mostrar d'una manera gràfica la quantitat de trànsit de xarxa que hi ha o l'amplada de banda utilitzada en un segment determinat. Aquestes eines recullen les dades estadístiques proporcionades pels equips de xarxa i generen les gràfiques corresponents.

- Revisar les gràfiques que proporciona l'NMS per revisar l'estat de salut dels dispositius de comunicacions i serveis.
- Comprovar les eines de monitoratge de trànsit com el CACTI, l'MRTG, etc., per veure si hi ha puntes de trànsit imprevistes o desconegudes.
- En cas de rebre alarmes d'avís o detectar qualsevol comportament estrany, reviseu els registres (*logs*) del sistema per veure si hi trobeu cap anotació sospitosa.
- En cas de detectar una incidència, preneu les mesures necessàries per minimitzar-ne l'impacte i notifiqueu la situació a qui escaigui (al vostre cap, als tècnics de xarxa d'una empresa externa involucrada, etc.).
- Finalment, feu una còpia dels *logs* que han enregistrat el comportament estrany per evitar que no se'n modifiqui el contingut d'una manera deliberada o accidental i no es pugui demostrar la veracitat de l'incident.

1.9 Simulació d'avaries

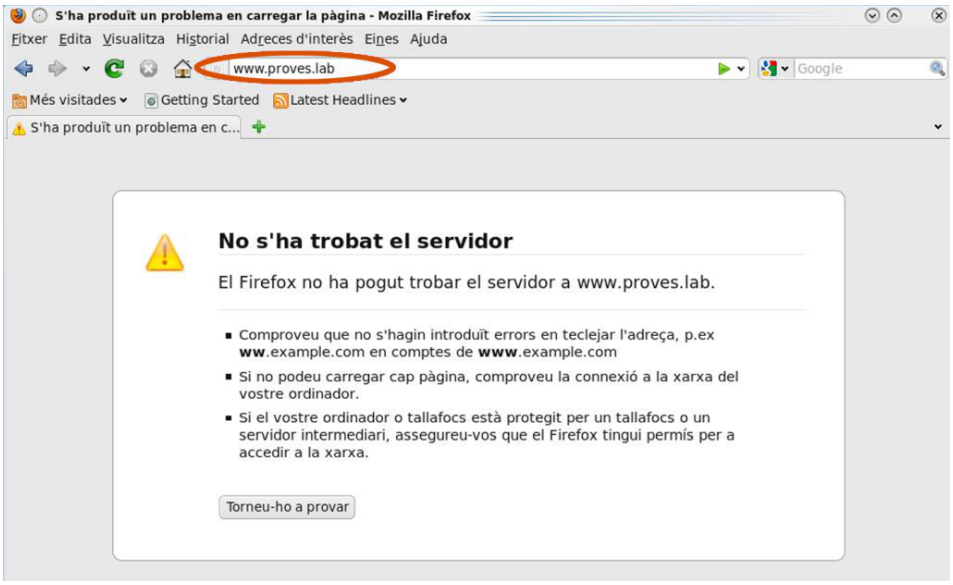
Quan es produeix un error o un problema en una xarxa, el temps que triguem a resoldre'l és fonamental. És clar que no podem preveure tots els tipus de contingències amb què ens podem trobar, però sí que podem aconseguir pràctica en la resolució de les incidències més habituals com, per exemple, que s'espatlli algun component de xarxa, patim un atac extern o detectem un ús de xarxa més elevat del que la xarxa és capaç de suportar. La pràctica i l'experiència que adquirim en la resolució d'aquests tipus d'incidències en laboratoris de proves ens beneficiaran quan es produeixi una incidència real.

1.9.1 Cas pràctic. Pèrdua de connectivitat

Teniu una topologia de xarxa com la de la figura 1.1.

Us informen que el servidor web ha deixat de funcionar de cop i us demanen que en reviseu la configuració per veure què ha passat i si el podeu deixar operatiu de nou.

FIGURA 1.4. Servidor Web inaccessible



El primer que heu de fer és intentar connectar-vos al servidor web, el qual té l'adreça www.proves.lab.

Intenteu connectar amb el navegador i obteniu el missatge següent (figura 1.4):

1. Quina en pot ser la causa? En teniu prou informació per saber-ho amb seguretat?

A continuació, comproveu que el servidor web és accessible mitjançant l'ordre *ping* per poder veure si respon correctament:

```
root@ioc:~# ping www.proves.lab
ping: unknown host www.proves.lab
root@ioc:~#
```

Fixeu-vos en la resposta "unknown host www.proves.lab".

2. Què indica aquesta resposta? De quin servei depèn aquesta resposta?

Comproveu que l'equip està configurat correctament, amb l'adreça IP, el servidor de DNS i la porta d'enllaç corresponent.

```
root@ioc:~# netstat –nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.200.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0

root@ioc:~# more /etc/resolv.conf
domain proves.lab
nameserver 192.168.200.30

root@ioc:~# /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0d:31:a8
          inet addr:192.168.200.5  Bcast:192.168.200.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0d:31a8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:863 errors:0 dropped:0 overruns:0 frame:0
          TX packets:796 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:113610 (113.6 KB)  TX bytes:86552 (86.5 KB)
          Interrupt:10 Base address:0xd020
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10032 (10.0 KB)  TX bytes:10032 (10.0 KB)
```

3. Què mostra el resultat de l'ordre *netstat –nr*? Hi ha res d'estrany?

4. Què mostra el resultat de l'ordre *more /etc/resolv.conf*?

5. Què mostra el resultat de l'ordre */sbin/ifconfig*?

En aquesta situació, és recomanable comprovar si el problema és local o del servidor de DNS, el qual no sap resoldre l'adreça IP del servidor **www.proves.lab**.

Primer de tot, comproveu si el servidor de DNS 192.168.200.30 està operatiu o, al contrari, no respon al ping.

```
root@ioc:~# ping –c 2 192.168.200.30
PING 192.168.200.30 (192.168.200.30) 56(84) bytes of data.
64 bytes from 192.168.200.30: icmp_seq=1 ttl=64 time=3.10 ms
64 bytes from 192.168.200.30: icmp_seq=2 ttl=64 time=3.61 ms

––– 192.168.200.30 ping statistics –––
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.108/3.359/3.611/0.258 ms
```

Com veieu, hem rebut resposta als dos pings enviats.

6. Què indica això?

Per comprovar les respostes del servidor de DNS quan fem la consulta al web, obrirem dues consoles d'ordres. En la primera, deixarem una captura del trànsit en temps real en què indicarem que es capturi tot el trànsit que vagi cap al servidor de DNS 192.168.200.30 i les seves respostes. Per fer-ho, executem l'ordre de *tcpdump* següent.

```
root@ioc:~# tcpdump –nni eth0 host 192.168.200.30 and UDP
tcpdump: unknown host 'UDP'
root@ioc:~# tcpdump –nni eth0 host 192.168.200.30 and proto UDP
tcpdump: verbose output suppressed, use –v or –vv for full protocol decode
listening on eth0, link–type EN10MB (Ethernet), capture size 96 bytes

20:47:08.134975 IP 192.168.200.5.53331 > 192.168.200.30.53: 3946+ A?
www.proves.lab. (32)
20:47:08.147625 IP 192.168.200.5.33805 > 192.168.200.30.53: 3946+ A?
www.proves.lab. (32)
```

Com podeu veure, no s'ha rebut cap resposta del servidor de DNS.

7. Vol dir això que l'adreça www.proves.lab no té cap adreça IP associada, o que el servei de DNS no funciona correctament?

Després d'una estona revisant la configuració del servidor de DNS, us adoneu que el servei està aturat i que no funciona. Així doncs, torneu a activar el servei i, una vegada més, comproveu si aquest resol correctament l'adreça.

```
root@ioc:~# ping -c2 www.proves.lab
PING www.proves.lab (192.168.200.100) 56(84) bytes of data.
64 bytes from 192.168.200.100: icmp_seq=1 ttl=64 time=5.14 ms
64 bytes from 192.168.200.100: icmp_seq=2 ttl=64 time=3.91 ms

--- www.proves.lab ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 5934ms
rtt min/avg/max/mdev = 3.917/4.529/5.141/0.612 ms
```

Ara sí que hi ha resposta. Comproveu, doncs, amb una nova captura de trànsit quan es fa la consulta al DNS, la resposta que es rep del servidor en connectar-vos de nou al servidor web. Per fer-ho, executem l'ordre anterior de *tcpdump*.

```
root@ioc:~# tcpdump -nni eth0 host 192.168.200.30 and proto UDP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:58:16.000552 IP 192.168.200.5.47299 > 192.168.200.30.53: 917+ A?
www.proves.lab. (32)
20:58:16.002889 IP 192.168.200.30.53 > 192.168.200.5.47299: 917* 1/1/1
A 192.168.200.100 (81)
```

En aquesta última captura tcpdump podeu veure que el vostre ordinador amb adreça 192.168.200.5 ha fet una consulta al port UDP/53 del servidor 192.168.200.30, li ha preguntat l'adreça IP de www.proves.lab i aquest li ha contestat que l'adreça IP és 192.168.200.100.

Podeu fer una última comprovació de la disponibilitat del servidor web fent un telnet al port 80 per comprovar que realment està operatiu. Tot i que ho heu provat amb el navegador web, a vegades mostren una versió anterior de la pàgina web emmagatzemada a la memòria cau. Amb aquesta altra comprovació, us assegureu que el servidor web està operatiu.

```
root@ioc:~# telnet www.proves.lab 80
Trying 192.168.200.100...
Connected to www.proves.lab.
Escape character is '^]'.
```

Ara ja podeu donar la incidència per tancada; només resta saber per quin motiu s'ha aturat el servidor de DNS i quan ha succeït. Per fer això, reviseu els registres del servidor i de les eines NMS de què disposeu.

1.9.2 Solucions a les preguntes plantejades al cas pràctic ("Pèrdua de connectivitat")

1. Hi ha diversos factors que ho poden provocar: una caiguda del servidor web, una caiguda del servidor de DNS, uns filtres de xarxa, un error de maquinari, etc. No teniu prou informació per saber-ho amb seguretat.

2. La resposta indica que l'ordinador no coneix l'adreça www.proves.lab. La resposta depèn del servei de DNS, el qual per algun motiu no ha estat capaç de resoldre l'adreça www.proves.lab en una adreça IP.

3. L'ordre mostra que l'ordinador pertany a la xarxa 192.168.200.0/24. Com a curiositat, no es mostra cap porta d'enllaç, la qual cosa indica que aquesta màquina només es podrà connectar amb altres ordinadors i servidors en el mateix segment de la xarxa.

4. L'ordre mostra que el servidor de DNS és el 192.168.200.30.

5. L'ordre mostra la configuració completa de la interfície de xarxa eth0, la qual té l'adreça IP 192.168.200.5.

6. Això indica que el servidor físicament funciona, i que, en cas d'haver-hi un problema, serà relatiu al servei de DNS i no a un problema de maquinari.

7. Si l'adreça www.proves.lab no tingués una adreça IP associada, sí que rebríem una resposta del servidor de DNS: ens diria que no té cap adreça. La falta de resposta indica que, o bé el servei no està operatiu, o bé l'accés està filtrat.

2. Monitoratge de la xarxa local per detectar situacions anòmales

Monitorar una xarxa és una tasca que implica entendre què passa i per què. Una xarxa no és comporta de la mateixa manera sempre; hi ha estones en què el volum de trànsit serà molt elevat, d'altres en què serà molt baix i d'altres en que serà regular. Conèixer les situacions en què us podeu trobar és important per saber diferenciar un comportament normal d'un altre d'estrany o fora de l'habitual.

Per conèixer el tipus de trànsit que circula per la xarxa no n'hi ha prou de conèixer els protocols més comuns, com el TCP/IP, i saber que la majoria d'usuaris només es connecta a Internet o a una base de dades. És important poder veure en primera persona tot el que hi circula, ja que sovint descobrireu que a la xarxa hi ha més protocols funcionant dels que us pensàveu.

Per tal d'analitzar els protocols que es fan servir en una xarxa, hi ha eines com els **analitzadors de protocols**, que us permetran capturar mostres de trànsit de la xarxa i en podreu fer l'anàlisi detallada.

2.1 Procediments d'anàlisi de protocols de comunicacions en xarxes locals

Hi ha diverses eines que permeten mostrar en temps real les dades de la xarxa i desar la informació en un fitxer per tal d'analitzar-les posteriorment. Els sistemes operatius GNU/Linux i Unix disposen de diverses eines de sèrie per dur a terme aquestes tasques. Tot i que el sistema operatiu de l'entorn Windows no en té, se n'hi poden instal·lar.

> Per conèixer l'estat de la xarxa, és important saber el tipus de dades que hi circulen, és a dir, els protocols de diferents nivells, les aplicacions que utilitzen els usuaris, els mecanismes de gestió i senyalització dels dispositius i la capacitat total i actual del conjunt de dispositius de la xarxa.

Les diverses eines que podem fer servir ens permeten analitzar els protocols que s'utilitzen a la xarxa, identificar els tipus de filtre que s'estan fent servir per accedir a uns recursos o uns altres i descobrir les aplicacions que s'estan executant en els servidors o clients, entre altres funcions.

2.1.1 Analitzadors de protocols

Els analitzadors de protocols us permeten capturar el trànsit que circula en un segment de la xarxa determinat i el podreu analitzar en temps real o posteriorment.

En una xarxa circulen molts paquets al mateix temps, paquets que corresponen a protocols i aplicacions diferents. En un moment donat, en la xarxa hi pot haver paquets de dades TCP corresponents a les consultes web dels usuaris, UDP de fluxos de vídeo, ARP de peticions d'adreces tipus MAC, intercanvi de rutes amb protocols d'encaminament dinàmic com l'EIGRP o l'OSPF, etc.

La quantitat de dades que podeu arribar a capturar en uns segons és molt elevada i cal que l'analitzador de protocols tingui prou potència per realitzar la captura. En cas que ho vulgueu, també podeu desar un registre de la captura per fer-ne l'anàlisi posterior.

Hi ha vegades en què només voldreu fer la captura, però no guardar-la, i d'altres en què ho voldreu capturar tot i després analitzar-ho amb calma per poder veure'n els detalls.

Observar el trànsit capturat en temps real és molt complicat, sobretot quan el trànsit de la xarxa és intens o quan hi ha diversos protocols. Per aquest motiu, el mètode d'anàlisi en temps real s'utilitza en casos puntuals en què simplement es vol saber si hi ha trànsit o no, en cas de voler saber si el segment de xarxa en qüestió funciona o quan es vol saber si un protocol determinat està permès. No obstant això, per a aquest últim cas habitualment definireu un filtre de captura per evitar que la resta de trànsit que no us interessa sigui descartat pel motor de captura i que només us mostri el que us interessa.

La resta de vegades, sobretot quan hi hagi un problema a la xarxa i no tingueu clar què el causa, probablement fareu una captura d'una mostra de trànsit i l'analitzareu posteriorment amb el mateix analitzador de trànsit o amb un altre programa específic d'anàlisi de captures. Aquest tipus de programa sol portar eines i utilitats que detecten comportaments anòmals, tant per un mal funcionament com per atacs de xarxa.

És important que us familiaritzeu amb aquest tipus d'eines, ja que la informació que se n'obté és vital per a la diagnosi i la resolució de problemes de xarxa.

2.1.2 Aplicació de filtres per a la captura de trànsit

Els filtres permeten filtrar d'entre tots els tipus de trànsit de la xarxa, el que ens interessa obtenir o descartar. Podeu indicar que voleu descartar tot el tipus de trànsit que no es correspongui amb el que heu indicat o fer el contrari: descartar un tipus de trànsit específic i capturar la resta.

Depèn de la situació que us porti a haver de capturar trànsit per analitzar-lo; segons el cas serà més convenient un tipus de filtre o un altre. De la mateixa manera, segons el moment, aplicareu els filtres en temps real, és a dir, durant la captura perquè el trànsit capturat ja estigui prèviament filtrat, o, si no, capturareu tot el trànsit i aplicareu els filtres més tard, en el moment de l'anàlisi.

```
root@ioc:~# tcpdump -nni eth0 host www.ioc.cat and tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
19:56:03.441982 IP 192.168.1.103.52861 > 85.192.111.244.80: Flags [S],
seq 2380512837, win 5840, options [mss 1460,sackOK,TS val 1037991 ecr 0,nop,
    wscale 6],
length 0
19:56:03.481061 IP 85.192.111.244.80 > 192.168.1.103.52861: Flags [S.],
seq 1709775399, ack 2380512838, win 5840, options [mss 1460], length 0
19:56:03.481170 IP 192.168.1.103.52861 > 85.192.111.244.80: Flags [.],
ack 1, win 5840, length 0
19:56:03.506395 IP 192.168.1.103.52861 > 85.192.111.244.80: Flags [P.],
seq 1:100, ack 1, win 5840, length 99
```

En aquest exemple heu pogut veure com hem fet una captura del trànsit de tipus TCP amb origen o destinació a la pàgina web de l'IOC www.ioc.cat. Aquesta captura ha aplicat els filtres en temps real, ja que només es captura el tipus de trànsit TCP i no es desa en cap fitxer per fer-ne l'anàlisi posterior.

Si voleu filtrar tot el trànsit de tipus TCP amb destinació la web de l'IOC, sense tenir en compte el trànsit de tornada i que, a més a més, es guardi en un fitxer per analitzar-lo més tard, hauríeu pogut fer servir la comanda següent:

```
root@ioc:~# tcpdump -nni eth0 -w captura.log dst host www.ioc.cat and tcp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

^C8 packets captured
12 packets received by filter
```

Fixeu-vos que, quan guardeu la captura en un fitxer, no la podreu veure en temps real; tanmateix, com que la teniu guardada en el fitxer captura.log, la podreu visualitzar en qualsevol moment.

```
root@ioc:~# tcpdump -r captura.log
reading from file captura.log, link-type EN10MB (Ethernet)
20:03:12.314148 IP ioc.local.33086 > ioclabs.xtec.net.www: Flags [S],
seq 516724778, win 5840, options [mss 1460,sackOK,TS val 1145209 ecr 0,nop,
    wscale 6],
length 0
20:03:12.343622 IP ioc.local.33086 > ioclabs.xtec.net.www: Flags [.],
ack 4138369611, win 5840, length 0
20:03:12.366237 IP ioc.local.33086 > ioclabs.xtec.net.www: Flags [P.],
seq 0:99, ack 1, win 5840, length 99
20:03:12.402008 IP ioc.local.33086 > ioclabs.xtec.net.www: Flags [.],
ack 176, win 6432, length 0
20:03:12.593392 IP ioc.local.33086 > ioclabs.xtec.net.www: Flags [P.],
seq 99:203, ack 176, win 6432, length 104
```

2.1.3 Anàlisi del trànsit a nivell de xarxa

El trànsit d'una xarxa està compost per diversos protocols, l'ús dels quals afegeix una sobrecàrrega (*overhead*) a la xarxa que disminueix l'ample de banda disponible per a les aplicacions dels usuaris.

No obstant això, no podeu suprimir aquests protocols de la xarxa, ja que precisament són necessaris perquè funcioni, la qual cosa està condicionada per la comunicació entre els dispositius.

La informació que es pot compartir, segons els protocols que s'utilitzen, són les rutes disponibles en la xarxa, les característiques dels enllaços, el sincronisme d'hora dels dispositius, l'informe d'activitat o registres, els protocols de senyalització de nivell físic que defineixen les característiques del medi pel qual es fa la transmissió d'informació, etc.

La quantitat de protocols que podeu arribar a detectar és immensa i cal ser conscient que detectar molts protocols diferents en la xarxa no ha d'implicar necessàriament que hi ha un problema, sinó que hi ha diversos mecanismes i serveis en funcionament que fan ús de la xarxa per realitzar les tasques corresponents.

Fins i tot en xarxes senzilles, de pocs usuaris i sense protocols d'encaminament, no és estrany que trobeu el protocol de nivell de xarxa IP, acompanyat del protocol de transport TCP i, en alguns casos, d'UDP. Altres protocols de nivell inferior com ARP són habituals en qualsevol segment de xarxa, de la mateixa manera que el trànsit ICMP. Aquest darrer, tot i que està filtrat, en alguns casos és molt habitual trobar-lo, ja que moltes aplicacions fan servir l'ICMP d'una manera nativa per dur a terme les seves tasques. Mitjançant filtres i tallafocs, podeu prevenir que qualsevol d'aquests protocols travessi la xarxa; tanmateix, si els protocols tenen com a origen i destinació equips de la mateixa xarxa, no els podreu filtrar (a nivell d'aplicació sí que podreu fer-ho, però continuarà havent-hi trànsit en la xarxa) i serà senzill que els captureu amb els programes de captura de trànsit.

A part d'aquests protocols, a nivell d'aplicació, gairebé en qualsevol entorn d'oficina podreu trobar HTTP, FTP, DNS, Netbios, SSH, IPSec, PPTP, L2TP, etc.

Principalment trobareu HTTP, FTP i DNS en qualsevol lloc on sigui permesa la navegació Web, tant per fer consultes a Internet com per accedir a aplicacions internes de l'empresa desenvolupades en un llenguatge de programació Web, com, per exemple, PHP o ASP i que requereixin un navegador per a la seva utilització.

El protocol Netbios és habitual dels entorns d'oficina que treballen amb Microsoft Windows, atès que és el protocol sobre el qual es duu a terme la resolució de noms d'equips locals de xarxa i compartició de fitxers.

Actualment el protocol Netbios es considera obsolet i està essent substituït per DNS inclús als sistemes Windows. No obstant això, per les xarxes amb equips Windows encara solen circular paquets d'aquest protocol.

Finalment, el protocol SSH és característic dels entorns Linux/Unix, ja que és el protocol d'administració remota per excel·lència i els protocols IPsec, PPTP o L2TP són propis d'entorns on hi ha accessos a seus remotes mitjançant enllaços de xarxes privades virtuals (VPN) o VPN d'accés per a teletreballadors.

Aquests protocols no són ni de bon tros tots els que us podeu trobar en una captura de trànsit; per tant, és important que us hi familiaritzeu i que estigueu al corrent de quin ús se'n fa en l'empresa on us trobeu.

2.1.4 Sondes de monitoratge remot i detecció d'intrusos

Monitorar una xarxa pot ser complex si és molt gran i està segmentada en diverses subxarxes.

Per poder monitorar xarxes grans, s'utilitzen sensors, els quals es distribueixen estratègicament per diversos punts de la xarxa i recullen informació sobre el trànsit en aquell punt.

Syslog

És un mecanisme format per un protocol de xarxa i una aplicació que permet que els dispositius de xarxa enviïn registres d'activitat a un punt centralitzat. Aquests registres que envien inclouen la data, l'hora i el tipus de succés. Amb aquest mecanisme, l'administrador de xarxa pot consultar els esdeveniments que han ocorregut en els diversos equips de la xarxa des d'un mateix equip.

Cadascun dels sensors envia informació sobre el trànsit capturat a un punt central, com, per exemple, un servidor de syslog, el qual concentra la informació de tots els sensors de la xarxa.

Hi ha programes especialment dissenyats per analitzar la informació de les sondes i cercar paràmetres de comportament típics d'atacs informàtics. Aquests programes són capaços de detectar molts comportaments estranys, els quals poden ser causats per un mal funcionament de la xarxa o un atac. De fet, aquests programes fan servir un fitxer de firmes, semblant als que utilitzen els programes antivirus, per aprendre nous tipus d'atacs o vulnerabilitats.

Hi ha dos tipus de programes especialitzats en l'anàlisi de la informació capturada per les sondes. En primer lloc, teniu els sistemes de detecció d'intrusions o IDS i, en segon lloc, els sistemes de detecció i prevenció d'intrusions o IDPS.

Els IDS analitzen la informació recollida per les sondes en busca d'indicis de comportaments anòmals. En cas de detectar algun possible incident ho notifica mitjançant un correu o una alarma a l'administrador de la xarxa.

Els IDPS, a part de monitorar la xarxa en busca de comportaments anòmals, quan detecten una situació que pot provocar un incident de seguretat, apliquen un canvi de política per tal de minimitzar l'impacte sobre la xarxa i evitar que l'incident vagi a més.

Per exemple, si un IDPS detecta que hi ha un ordinador no autoritzat connectat en un port d'un commutador i aquest està configurat per bloquejar els accessos no autoritzats, anul·larà el port del commutador on s'ha detectat l'accés indegut per evitar que des d'aquest port i ordinador s'accedeixi a altres recursos de la xarxa. A part de bloquejar el port, també ho notificarà a l'administrador de la xarxa perquè n'estigui al corrent.

La diferència principal entre IDS i IDPS és que el primer només notifica els comportaments anòmals i el segon actua segons una política definida per l'administrador per tal de contenir l'incident.

2.2 Gestió i control en els protocols de comunicacions

Una xarxa està formada per diversos elements físics que, segons el tram de la xarxa, poden patir més o menys càrrega i, per tant, poden tenir un ús més intensiu. Els protocols, la càrrega, el desgast, etc. són factors que influeixen en el rendiment de la xarxa i, per tant, cal que siguem capaços d'obtenir mètriques d'ús per veure en quin estat es troba la xarxa. Hi ha diverses eines que, mitjançant sondes, són capaces d'obtenir aquesta informació i generar informes que permeten avaluar la necessitat de modificar l'arquitectura de la xarxa o substituir equipament que està al límit de les seves possibilitats.

De la mateixa manera que la qualitat dels components físics que formen una xarxa són importants per garantir un funcionament correcte, els protocols de comunicacions són igualment rellevants, ja que, segons els protocols que hagin de circular per la xarxa, el trànsit generat serà més o menys intens i el rendiment de la xarxa se'n pot veure afectat.

2.2.1 Factors que determinen el rendiment d'una xarxa local

Una xarxa està formada per diversos elements, com ara els cables i els connectors, els equips de comunicació, els protocols de xarxa i els mateixos usuaris.

Perquè una xarxa funcioni de manera òptima cal en primer lloc garantir que els elements físics que la componen (cables, connectors, armaris de connexió, targetes de xarxa, etc.) són de qualitat i compleixen els estàndards i les normatives d'ús. Un cable de xarxa en bon estat, però més llarg que els límits recomanats, un equip de comunicació que no compleix els estàndards i fa servir un mecanisme de transmissió diferent o una targeta de xarxa de baixa qualitat poden tenir un impacte molt negatiu en el funcionament de la xarxa.

Protocols de gestió i monitoració

EL *CISCO discovery protocol* (CDP) és un protocol propietari de CISCO que proporciona informació sobre la interconnexió dels dispositius, com el model i les característiques. Hi ha aplicacions que, mitjançant aquesta informació, poden arribar a dibuixar un diagrama complet de la topologia de la xarxa. L'inconvenient principal és que no és compatible amb altres fabricants.

L'SNMP, a diferència del CDP, és un estàndard multifabricant que permet recollir informació dels dispositius i enviar-los instruccions o canviar-ne la configuració. Avui dia és àmpliament utilitzat per a aplicacions de gestió centralitzada de dispositius de xarxa.

Quan es dissenya una xarxa s'ha de tenir en compte l'ús que se n'haurà de fer, el nombre d'usuaris que s'estima, la disponibilitat dels serveis, el cost, etc. Tots els factors intervenen d'una manera o d'una altra en el resultat final. Una xarxa de baix cost dissenyada per donar servei a deu usuaris a nivell d'aplicacions d'ofimàtica, amb concentradors en comptes de commutadors, sense segmentar i amb targetes de xarxa 10/100 Mbps no serà gens escalable per donar servei a dos cents usuaris amb requeriments de telefonia IP i reproduccions de vídeo en temps real (*streamings*).

Els protocols de comunicació i el trànsit de la xarxa són igual d'importants. A part de les mateixes dades que els usuaris transmeten per la xarxa fent servir programes habituals, com les connexions Web, FTP, consultes al DNS, etc., hi ha tot un conjunt de protocols que generen trànsit de control per tal de poder fer la seva feina, com ara els protocols d'encaminament dinàmic (RIP, EIGRP...) o els protocols de gestió i monitoració (CDP, SNMP, etc.).

El rendiment de la xarxa es pot veure dràsticament reduït si algun d'aquests protocols d'encaminament o gestió no està configurat correctament o el sistema no està preparat per funcionar-hi per un mal disseny o per falta de prestacions en els dispositius.

Cal entendre que, perquè el rendiment de la xarxa sigui el volgut, no ha de ser l'usuari que utilitzi la xarxa segons les prestacions que aquesta li ofereix, sinó que la xarxa és la que ha de poder oferir els serveis que l'usuari necessita.

2.2.2 Mètriques

En xarxes mitjanes i grans on no és viable configurar totes les rutes a mà a causa de l'existència de diversos segments de xarxa i camins redundants, cal fer servir protocols d'encaminament dinàmic que vetllaran per configurar els equips de xarxa de manera que la ruta que segueixen els paquets de dades des de l'origen fins a la destinació sigui òptima.

Hi ha diversos protocols d'encaminament dinàmic que permeten que el trànsit pugui arribar a la destinació, cadascun dels quals amb un mecanisme de decisió de ruta propi.

Els protocols d'encaminament fan servir uns criteris per decidir quina de les possibles alternatives de rutes (en cas que n'hi hagi més d'una) és l'òptima per arribar a la destinació. Això es coneix com a *mètrica*. Hi ha protocols que basen la seva decisió en un simple factor com és el nombre de salts que ha de fer un paquet per arribar a la destinació i d'altres que la basen en la suma de diversos factors, com l'ample de banda del segment de xarxa, la latència, la fiabilitat de l'enllaç, etc.

Els protocols menys precisos són els que només fan servir un factor per al càlcul de la mètrica, com, per exemple, el protocol RIP. Els més precisos són els que fan servir diferents factors en el càlcul de la mètrica, com ara l'EIGRP o l'OSPF. No

obstant això, com més precís és el protocol, més complexa n'és la configuració i la supervisió.

Aquests protocols afegeixen un trànsit addicional a la xarxa per tal de sincronitzar la informació d'un equip amb la d'un altre i així poder avaluar millor la ruta que cal seguir. Si la xarxa és senzilla i s'implementa un protocol d'encaminament massa complex i pesant, com, per exemple, l'OSPF, a part de dificultar la tasca de supervisió de la xarxa, estareu afegint un trànsit excessiu a la xarxa que potser no és assumible pels equips a causa de les limitacions tècniques que aquests equips tenen.

És recomanable estudiar els diversos protocols d'encaminament disponibles i avaluar els avantatges i els inconvenients de cadascun abans de decidir quin es farà servir, ja que una vegada la xarxa està en funcionament i el protocol d'encaminament configurat i operatiu, acostuma a ser complex canviar de protocol d'encaminament.

2.2.3 Eines de mesurament

Per mesurar la qualitat i el rendiment dels enllaços podeu fer servir diverses eines, com ara els analitzadors de protocols, els analitzadors de cablatge, les eines per dur a terme proves de càrrega i, fins i tot, la mateixa informació subministrada pels mecanismes dels equips de xarxa.

La majoria d'equips de xarxa de gamma mitjana-alta inclouen mecanismes propis per comprovar la qualitat dels enllaços que estan directament connectats a una de les seves interfícies o ports de connexió i poden mostrar tota classe d'estadístiques, com ara el nombre de paquets que han passat per la interfície de xarxa, els segments defectuosos, les col·lisions, etc.

Si no disposeu de cap eina addicional, com a mínim és important que sapigueu que podeu fer servir aquesta informació subministrada pels equips de xarxa com a punt de partida per avaluar la qualitat d'un enllaç.

A continuació us mostrem les estadístiques d'ús d'una interfície de xarxa d'un dispositiu Cisco (s'obté amb l'ordre *show interfaces fastEthernet0/0*)

```
1  FastEthernet0/0 is up, line protocol is up (connected)
2    Hardware is Lance, address is 0002.177a.0201 (bia 0002.177a.0201)
3    Internet address is 192.168.1.1/24
4    MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255, txload
         1/255, rxload 1/255
5    Encapsulation ARPA, loopback not set
6    ARP type: ARPA, ARP Timeout 04:00:00,
7    Last input 00:00:08, output 00:00:05, output hang never
8    Last clearing of "show interface" counters never
9    Input queue: 0/75/0 (size/max/drops); Total output drops: 0
10   Queueing strategy: fifo
11   Output queue :0/40 (size/max)
12   5 minute input rate 121 bits/sec, 0 packets/sec
13   5 minute output rate 56 bits/sec, 0 packets/sec
14      63 packets input, 24768 bytes, 0 no buffer
15      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     52 packets output, 5252 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```

```
0 output buffer failures, 0 output buffers swapped out
```

2.2.4 Protocols de gestió

Per conèixer l'estat d'una xarxa, cal saber com funcionen els diversos equips de xarxa. Els equips de xarxa de gamma mitjana-alta acostumen a tenir diversos components redundants, com ara fonts d'alimentació, ventiladors, etc., perquè, en cas de fallada d'un d'ells, amb el component secundari l'equip pugui funcionar i continuar oferint el servei.

En tot moment heu de saber com estan els equips, ja que, si s'espatlla un component d'un equip i continua funcionant amb el de recanvi, pot ser que també s'espatlli el secundari i finalment deixi de funcionar. Per tant, cal que us assabenteu quan un component s'espatlla perquè el pugueu substituir i evitar que una segona fallada el deixi inoperatiu.

Hi ha protocols de gestió, com l'SNMP, que permeten obtenir informació de l'equip, com ara l'estat dels components, l'ús de CPU, la memòria, els ventiladors, etc. També permet obtenir la configuració de l'equip i canviar-la. Aquest protocol és un estàndard independent de fabricant, de manera que està disponible per a qualsevol fabricant i equip, sempre que l'equip disposi del protocol.

El protocol SNMP està format per tres components bàsics:

- Dispositiu o element que cal supervisar.
- Agent.
- Sistema d'administració de xarxa (NMS).

El dispositiu és l'element que voleu supervisar, com, per exemple, un encaminador, un commutador, un concentrador, un servidor, un ordinador, una impressora, etc. Qualsevol component de xarxa programable pot arribar a ser supervisat.

L'agent és el component de programari que s'instal·la en el dispositiu i que s'encarrega d'obtenir la informació de l'estat en què es troba i proporcionar-la al sistema d'administració de xarxa (NMS).

El sistema d'administració de xarxa és un dispositiu o aplicació que permet recollir tota la informació subministrada pels agents de SNMP i mostrar-la a l'administrador d'una manera gràfica (normalment) i intuïtiva. A més a més, des

d'aquest NMS es poden canviar les configuracions dels equips de manera remota i, fins i tot, més d'un dispositiu alhora.

Per fer totes aquestes funcions, l'NMS disposa d'una base de dades jeràrquica (MIB), que guarda tota la informació relativa als dispositius i els identifica de manera única en la xarxa.

Mitjançant una sèrie de paquets de dades, els agents es comuniquen amb l'NMS per proporcionar informació del dispositiu i, en cas que estigui configurat el sistema per fer-ho, es poden enviar instruccions als agents per tal de modificar les configuracions dels dispositius respectius.

MIB

MIB són les sigles de *management information base*, una base de dades jeràrquica que conté informació estructurada en forma d'arbre de tots els dispositius gestionats en una xarxa de comunicacions compatibles amb l'estàndard SNMP.

Es coneix com a *comunitat* (*community*) el conjunt d'agents i NMS que formen part d'un mateix grup. Només és possible l'intercanvi d'informació entre un agent i un NMS si aquests formen part de la mateixa comunitat.

Hi ha dos tipus de comunitat, de lectura i d'escriptura. En el primer tipus, els agents només subministren informació a l'NMS. En el segon tipus, a part d'aportar informació a l'NMS, aquest pot enviar instruccions als agents per tal de modificar la configuració dels dispositius.

El protocol SNMP viatja per la xarxa gràcies al protocol UDP i fa servir els ports 161 i 162 per intercanviar missatges. És important que, en cas que hi hagi tallafocs a la xarxa, aquests estiguin configurats per acceptar el trànsit d'aquest protocol, ja que, en cas contrari, no serà possible supervisar els equips mitjançant l'SNMP.

2.3 Execució de processos periòdics per identificar i diagnosticar deficiències de la xarxa local

Quan es crea un nou punt de connexió a la xarxa, és important comprovar si tots els elements i protocols que faran possible que l'enllaç estigui disponible operen correctament i que, per tant, l'enllaç funcionarà a ple rendiment.

Per fer aquesta comprovació, es realitza un test de càrrega, que consisteix a generar un trànsit de dades constant fent servir el nou enllaç i comprovar els diversos valors obtinguts, com ara l'ample de banda, la latència, la fiabilitat, etc. Amb tots aquests paràmetres podreu saber si l'enllaç funciona adequadament.

No cal fer aquest test de manera periòdica una vegada la xarxa està operativa, excepte quan creieu que els problemes de xarxa són ocasionats per un enllaç defectuós.

En canvi, sí que és important monitorar la xarxa mitjançant les dades obtingudes en els NMS i comprovar els resultats dels registres anteriors. Tot i que la xarxa no mostrarà els mateixos resultats idèntics, sí que us ha de ser possible establir un patró i definir un llindar a partir del qual considereu una cosa anòmala.

Es recomanable disposar d'eines que generin gràfiques d'ús de la xarxa, com, per exemple, el CACTI o l'MRTG, i que, gràcies a protocols de gestió com l'SNMP,

poden obtenir informació de trànsit dels enllaços dels equips. A vegades una imatge val més que mil paraules i la monitoració de xarxes no n'és una excepció. Si cada dia a la mateixa hora reviseu les gràfiques de consum d'ample de banda actual on indica que l'ús de la xarxa està entre un vint i un quaranta per cent i un dia concret veieu que hi ha hagut un consum del noranta per cent, de seguida us adonareu que passa alguna cosa fora del que és habitual.

2.4 Detecció dels problemes de seguretat de la xarxa local

Un problema de seguretat en la xarxa es pot convertir en un incident de seguretat, si alguna persona o aplicació aprofita aquesta vulnerabilitat per infringir la política de seguretat.

Es pot produir un problema de seguretat quan hi ha alguna vulnerabilitat en un component de programari de xarxa determinat, com ara el SO dels equips de comunicació, servidors o equips d'usuari. En el cas dels servidors i els ordinadors o dispositius dels usuaris, el perill és encara més gran, ja que la vulnerabilitat pot estar tant en el sistema operatiu com en les aplicacions de xarxa, com ara el navegador Web, o en els serveis que proporcionen els servidors (HTTP, DNS, BBDD, FTP, etc.).

Una altra font de problemes de seguretat pot ser un equip mal configurat, com, per exemple, un tallafocs o un encaminador.

2.4.1 Funcionament i configuració de les eines de monitoratge

Per posar en funcionament un sistema de monitoratge, en primer lloc cal conèixer la topologia de la xarxa i saber quins dispositius voleu monitorar. Com més dispositius s'hagin de supervisar, més complex serà configurar tot el sistema, de manera que avalueu si val la pena monitorar un sistema concret abans de fer-ho.

Habitualment, els dispositius que s'acostumen a monitorar són els equips de comunicació, els enllaços de VPN i els servidors de l'empresa, però, en realitat, es pot supervisar qualsevol dispositiu al qual es pugui instal·lar un agent de monitoratge.

No tots els equips de xarxa poden ser monitorats, ja que, per exemple, els commutadors petits d'escriptori no acostumen a tenir aquesta capacitat; en canvi, sí que es monitoren els commutadors troncals, els encaminadors i els punts d'accés sense fil.

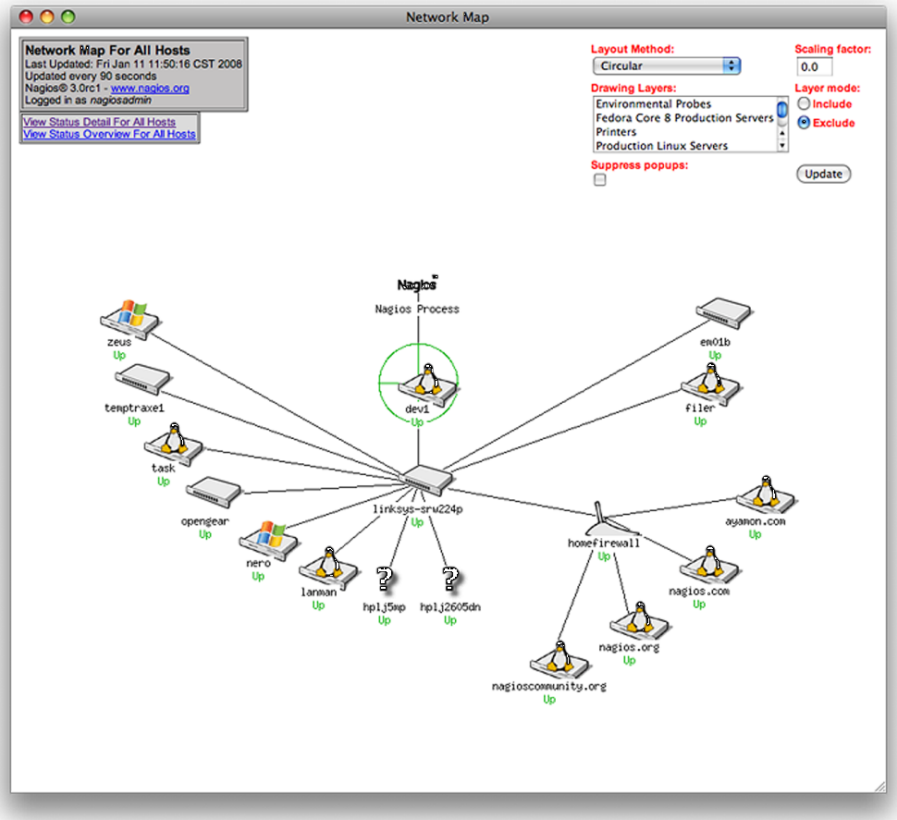
Quant als servidors, podeu escollir si monitoreu físicament la màquina, per exemple, que el servidor estigui engegat o aturat, o monitorar els serveis que ofereix. En el primer cas només podreu saber si el servidor està operatiu, però no si està actiu. És preferible que monitoreu els serveis del servidor, ja que es pot

produir un error en el programari que faci que el servei no estigui operatiu, tot i que el maquinari funcioni correctament.

El més habitual per monitorar els dispositius i serveis de xarxa és habilitar el protocol SNMP en els equips de xarxa i afegir els agents de SNMP en els dispositius i serveis que vulgueu monitorar. Tingueu present a permetre el trànsit UDP/161 i UDP/162 en els tallafocs i, si us és possible, habiliteu també l'ICMP a nivell intern perquè, mitjançant la utilitat PING, pugueu comprovar si un equip està actiu. Tot i que l'ICMP no és estrictament necessari, si està habilitat no serà sobrer disposar d'un doble mecanisme de comprovació.

Configureu un servidor de NMS, com, per exemple, l'aplicació NAGIOS, que s'encarregui de recollir la informació subministrada pels agents. Amb aquesta informació, l'NMS poblarà la seva MIB i generarà un diagrama de xarxa similar al de la figura 2.1.

FIGURA 2.1. Diagrama de xarxa generat per l'aplicació NAGIOS



Quan configureu el monitoratge mitjançant el protocol SNMP, haureu de definir el nom de la comunitat, perquè els agents es puguin comunicar amb la base de dades MIB. Considereu que el nom de la comunitat és com la contrasenya que han de conèixer els diferents dispositius per tal de formar part del mateix grup; per tant, és recomanable canviar el nom que ve per defecte, que sol ser públic, per un altre de més complex.

A continuació haureu de definir els permisos de lectura i d'escriptura en la comunitat. Si no esteu gaire familiaritzats amb aquest tipus d'eines i els equips

que formen part de la xarxa, és recomanable activar només el mode de lectura, per tal d'evitar que, per una mala manipulació de l'NMS, es canviï per error la configuració d'un equip i que això provoqui que algun servei o part de la xarxa resti inoperatiu.

Quan tot estigui configurat, comproveu que l'NMS és capaç de detectar tots els dispositius i, en el cas que algun d'aquests es mostri aturat o simplement no aparegui en el diagrama, comproveu que l'agent SNMP està actiu en l'equip i que no hi ha cap filtre o tallafocs en el recorregut que pugui afectar la comunicació.

Quan tots els equips estiguin representats correctament en el diagrama, configureu la política d'alarmes per tal de definir els llindars de criticitat i les línies d'actuació. Un NMS comprova cada cert temps si el servei o dispositiu està actiu i, en cas de no respondre correctament, llança una alarma que consisteix a mostrar en la pantalla un avís de caiguda del servei i a enviar un correu electrònic o un sms al mòbil a l'administrador de la xarxa per tal d'avisar-lo.

L'interval de temps de les consultes al servei i el nombre de respostes negatives que es consideren el límit de tolerància els definiu vosaltres. Els serveis poden tenir moments de càrrega puntual, de manera que, en el moment que l'NMS sondeja el dispositiu i aquest no respon, pot ser perquè aquest ha caigut o simplement perquè està sobrecarregat momentàniament. L'experiència que tingueu serà necessària per ajustar aquests valors segons la situació de la vostra xarxa.