Gestió de xarxa

Pere Barberán Agut
Manel Mendoza Flores

PID_00240340

Temps de lectura i comprensió: **5 hores**

UOC
Universitat Oberta de Catalunya

Índex

Introducció 5

Objectius 6

1. Introducció a la gestió de xarxa 7
1.1. Fonaments de la gestió de xarxa 8
1.1.1. Operacions en la gestió de xarxes 8
1.1.2. FCAPS 8
1.2. Components de la gestió de xarxa 12

2. Gestió de xarxa SNMP 14
2.1. Orígens de la gestió de xarxa SNMP 14
2.2. Arquitectura de gestió de xarxa SNMP 15
2.3. La base de dades d'informació a SNMP 16
2.3.1. Estructura de dades d'informació. Model d'informació 17
2.3.2. Estructura de la MIB 18
2.3.3. Definició dels objectes 20
2.3.4. Les MIB privades 21
2.4. **El protocol SNMP** 21
2.4.1. Operacions en SNMP 22
2.4.2. Les comunitats SNMP 22
2.4.3. Identificació d'instàncies 23
2.4.4. Format del paquet SNMP 26
2.5. Limitacions del protocol SNMP 27

3. SNMPv2 28
3.1. Millores en la gestió 28
3.2. Estructura de la informació de gestió 28
3.3. El protocol SNMPv2 29

4. SNMPv3 30
4.1. Marc de referència 30
4.2. Objectius de seguretat d'SNMPv3 31
4.3. Arquitectura d'SNMPv3 31
4.3.1. Model basat en usuari 33
4.3.2. Model basat en vistes 33

5. RMON (*remote network monitoring*) 35
5.1. Objectius del disseny d'RMON 35
5.2. Control de la sonda RMON 35
5.2.1. Configuració de la sonda 36

5.3. RMON1 i RMON2 37
5.3.1. La MIB RMON 38
5.3.2. RMON2 39

6. Eines i protocols en la gestió de xarxes 41
6.1. Internet control message protocol (ICMP) 41
6.2. *Traceroute* 44
6.3. Analitzador de xarxes 46
6.4. Monitoratge de xarxes 47

7. Gestió TMN 51
7.1. Arquitectura TMN 53
7.1.1. Arquitectura funcional del TMN 53
7.1.2. Arquitectura física del TMN 54
7.1.3. Arquitectura d'informació del TMN 54

Resum 55

Activitats 57

Exercicis d'autoavaluació 58

Solucionari 59

Glossari 61

Introducció

L'imparable creixement els últims vint-i-cinc anys en les necessitats de processament de la informació ha anat acompanyat del ràpid desenvolupament en els ordinadors i de la tecnologia de xarxa per a suportar aquestes necessitats. Lligat a aquesta demanda hi ha hagut una explosió en la varietat d'equips i xarxes ofertes pels venedors. Queden lluny els dies en què les empreses confiaven en un únic venedor i en conseqüència en una arquitectura que suportés les seves necessitats.

Avui en dia les organitzacions creixen ràpidament i la seva arquitectura de xarxa pot estar formada per diverses LAN, WAN, suportades per commutadors (*switchs*), encaminadors (*routers*), diferents tipus de computadors, serveis, etc. Per gestionar aquests sistemes i xarxes calen eines, metodologies, estàndards i aplicacions que treballin de manera automatitzada. La base d'aquestes eines en un entorn multivenedor és que hi hagi tècniques estandarditzades tant per a representar com per a intercanviar la informació de gestió de xarxes.

Així, en el món d'Internet destaquen els següents protocols per a aquesta finalitat; l'*Internet control message protocol* (ICPM), el *simple network management protocol* (SNMP) i l'especificació relacionada *Remote network monitoring* (RMON). Aquests estàndards inicials han estat revisats i actualitzats amb diverses versions en els últims anys i estan plenament vigents en l'actualitat.

Juntament amb els protocols estàndards existeixen una sèrie de metodologies i processos àmpliament utilitzats per a la gestió de xarxa. En aquest aspecte cal destacar la metodologia FCAPS (*fault*, *configuration*, *accounting*, *performance*, *security*), que estudiarem a fons en aquest mòdul.

Dintre del món de les telecomunicacions el procés ha estat similar quant a creixement. Actualment és molt competitiu, atesa la liberalització i globalització del mercat de les telecomunicacions. Els estàndards TMN estan creixent en importància com un medi per a proporcionar un avantatge als proveïdors de serveis de telecomunicacions.

En aquest mòdul didàctic es vol donar una visió dels conceptes associats a la gestió de xarxa, els seus processos, eines més utilitzades i els protocols més àmpliament acceptats, com són SNMP, ICMP i TMN.

Objectius

Els materials didàctics d'aquest mòdul han de permetre que l'estudiant assoleixi els objectius següents:

1. Entendre la necessitat de la gestió de xarxa, els seus requeriments i l'arquitectura bàsica de la gestió.

2. Conèixer els elements de la gestió de xarxa SNMP aprofundint en cadascun d'aquests elements i veient els avantatges i les limitacions de les diverses versions del protocol.

3. Prendre una consciència crítica dels aspectes de seguretat en la gestió de les xarxes de telecomunicacions.

4. Conèixer la metodologia de gestió de xarxa FCAPS i els seus processos associats per a la seva aplicació en la gestió de xarxes.

5. Aprendre l'estructura de la MIB-II i ser capaç de fer peticions SNMP als dispositius gestionats.

6. Aprendre els detalls del protocol ICMP i les eines que implementen aquest estàndard per a realitzar funcions de gestió de xarxa.

7. Entendre els objectius del monitoratge remot RMON, com es configura i com s'accedeix als recursos emmagatzemats en les sondes.

8. Diferenciar les necessitats de les operadores de telecomunicacions respecte a les xarxes convencionals.

9. Entendre gràfiques de rendiment obtingudes a partir d'SNMP.

10. Conèixer i aprendre a utilitzar l'analitzador de xarxes *Wireshark* com a eina clau per al diagnòstic de xarxes.

11. Conèixer l'arquitectura bàsica de gestió TMN per a infraestructures de telecomunicacions.

1. Introducció a la gestió de xarxa

Igual que les xarxes porten informació, aquesta informació necessita ser transmesa de manera eficient, efectiva i fiable. Hi ha moltes raons que fan que calgui una gestió de xarxa:

- Les xarxes actuals són una col·lecció de hardware i software de fabricants diversos i que cal configurar perquè funcionin conjuntament. Cada venedor a la vegada té les seves eines per a gestionar els seus equips de la forma més adequada possible.

- Les noves tecnologies han de conviure amb tecnologies antigues abans que aquestes siguin actualitzades. Cal, per tant, configurar xarxes amb tecnologies de diverses "generacions".

- La gestió de xarxa és un factor de cost. Les empreses intenten que la planificació, el suport, la detecció, la correcció de problemes, l'operació i l'administració siguin tasques que tinguin una component el més automatitzada possible.

- La seguretat és un altre aspecte molt important en les xarxes actuals.

- Altres aspectes relacionats amb la gestió són la planificació i el disseny, la gestió de polítiques, la gestió de sistemes, la gestió de serveis que es fan amb eines normalment propietàries.

Així, el marc de treball de la gestió de xarxa ha d'estar dirigit a resoldre aquests temes dintre dels límits funcionals i de cost. El cost de la gestió de xarxa no es refereix només al preu de compra dels equips, sinó que s'ha de veure des d'un punt de vista més ampli i ha de preveure aspectes humans, actualitzacions, utilització dels sistemes, etc.

Es pot dir, per tant, que la gestió de xarxa optimitza la capacitat funcional de la xarxa. Algunes connotacions que se'n poden derivar són les següents:

- Manté la xarxa operant a rendiment màxim.

- Informa a l'operador de qualsevol anomalia i intenta acotar el lloc on s'ha produït.

- Possibilita examinar el rendiment de la xarxa en temps real.

- Proporciona funcions de gestió de la configuració.

L'objectiu i els beneficis de les plataformes actuals de gestió de xarxa són els següents:

- Millorar en el procés de la presa de decisions.
- Millorar en l'eficàcia de les operacions.
- Alliberar els gestors de les feines rutinàries per poder-se dedicar a l'anàlisi, el control i la planificació. Gran part de les falles solen ser rutinàries o per errors humans.
- Assolir el ràpid retorn de la inversió.

1.1. Fonaments de la gestió de xarxa

Què és la gestió de xarxa?

> La ISO defineix la gestió de xarxa com el conjunt d'elements de control i supervisió dels recursos que permeten que la comunicació tingui lloc sobre la xarxa.

1.1.1. Operacions en la gestió de xarxes

La gestió de xarxes és una de les problemàtiques àmpliament estudiada i documentada en els diferents organismes d'estandardització.

Existeixen diverses metodologies com ITIL, FCAPS, TMN o PPDIOO que permeten la gestió de serveis i xarxes IT. A continuació estudiarem detalladament la més utilitzada per la indústria en relació a la gestió de xarxes, juntament amb els seus processos principals.

Enllaç d'interès

Per aprofundir en les diferents metodologies es pot consultar el següent document http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-453503.html

1.1.2. FCAPS

La metodologia de gestió de xarxes FCAPS (*fault*, *configuration*, *accounting*, *performance*, *security*) consisteix en unes recomanacions de gestió que s'han estandarditzat mitjançant una normativa ISO i es componen de cinc processos que es consideren crítics en la bona gestió de xarxa.

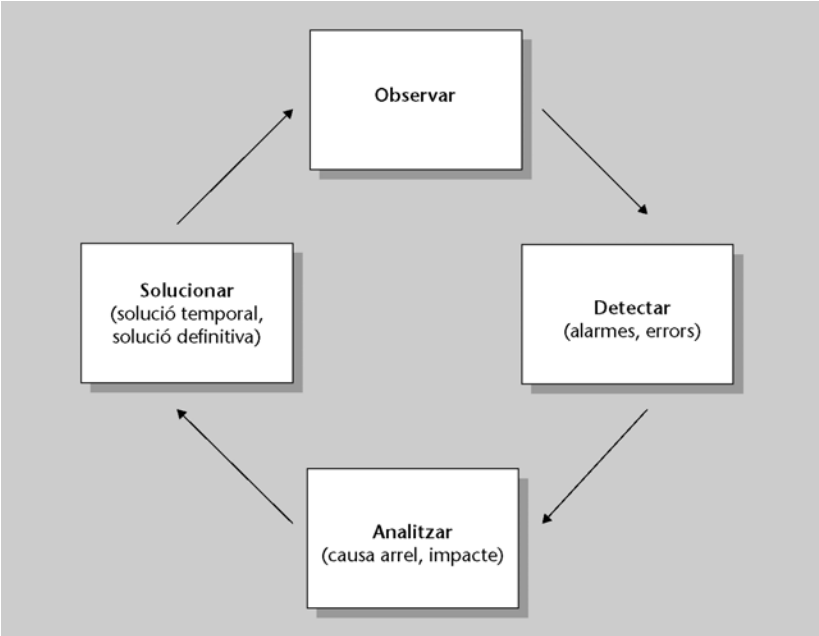
1) Gestió de fallades (*fault management*): el procés de gestió de fallades, segons la definició de l'estàndard FCAPS, consisteix a detectar, aïllar i resoldre els problemes de xarxa. És obligatori ser proactius per minimitzar els temps mitjans de reparació (MTTR, *mean time to repair*) i maximitzar els temps mitjans entre fallades (MTBF, *mean time between failures*). Per aconseguir aquest objectiu l'estàndard cita mecanismes de notificació com SNMP (*simple network managment protocol*) que permeten mesurar i controlar l'estat actual de la infraestructura de xarxa i d'aquesta forma anticipar-se a possibles anomalies de funcionament.

L'estàndard recomana realitzar un cicle periòdic per a la gestió de fallades. Molts d'aquests processos defineixen una metodologia comuna basada en les millors pràctiques del mercat. En concret el cicle es basa en els següents punts:

- Detecció de l'anomalia.
- Anàlisi de la causa arrel.
- Determinar les accions a prendre per a la seva solució.
- Observar l'efectivitat de la solució amb la situació esperada.

De forma gràfica ho podem observar en la figura 1.

Figura 1. Procés de gestió de fallades

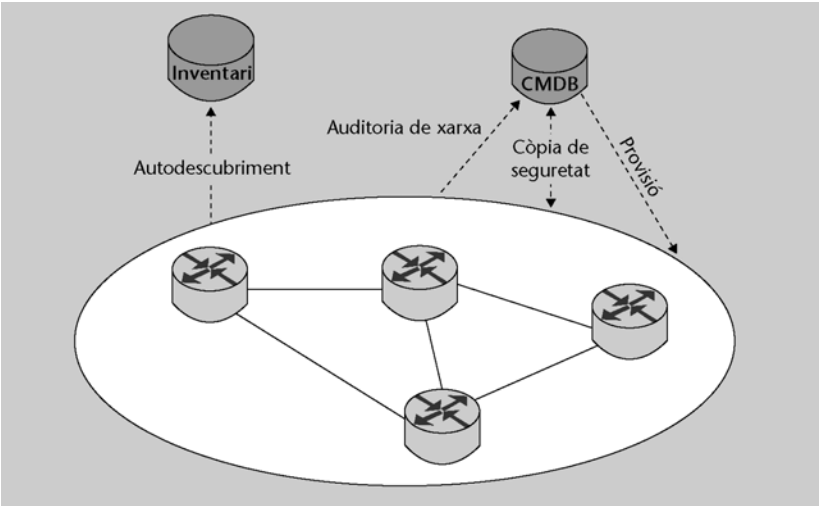


2) Gestió de la configuració (*configuration management*): aquest procés es basa en l'obtenció i emmagatzematge de la configuració dels sistemes i de la xarxa, tenint en compte les diferents versions i simplificant la gestió de canvis. A més, inclou les tasques d'instal·lació i configuració de maquinari, com també la gestió de *firmware* i inventariat. Aquest procés és de vital importància com més gran sigui la xarxa a gestionar.

Com a recomanació a l'hora de realitzar aquest procés es recomana tenir un inventari centralitzat de tots els elements de la xarxa i comprovar que es disposa de la configuració de tots els actius de la xarxa.

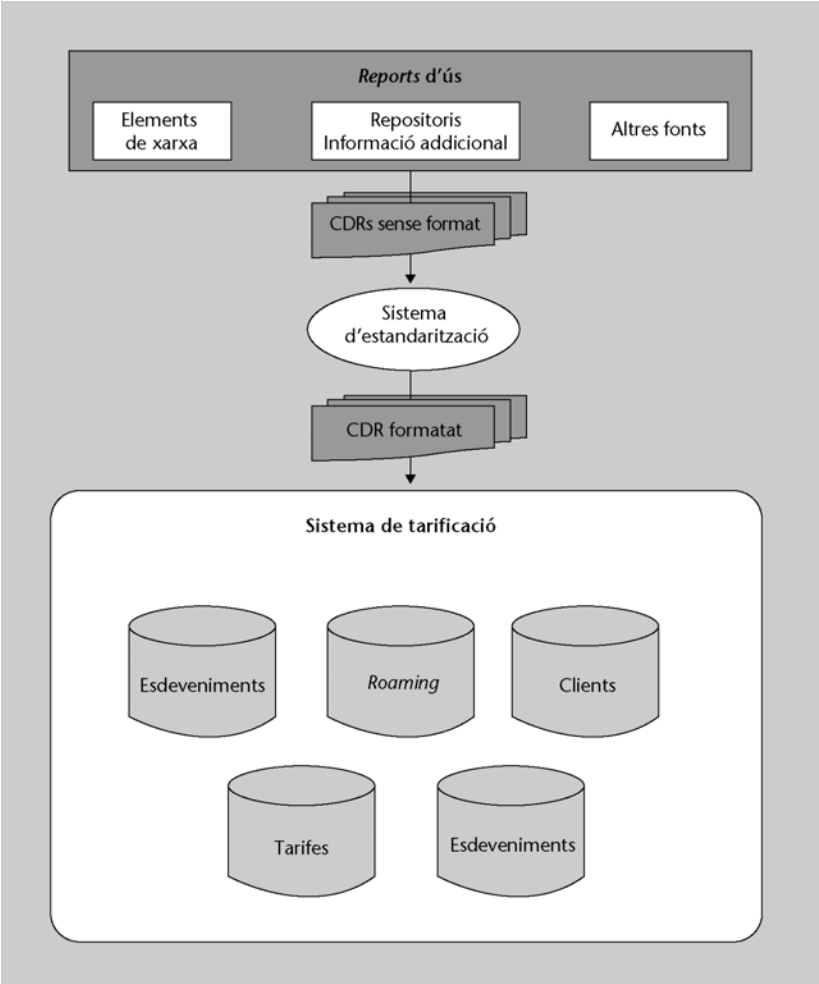
Un altre dels aspectes crucials a l'hora de gestionar la configuració i especialment a l'hora de diagnosticar errors és la capacitat de poder referenciar temporalment els canvis realitzats en una xarxa. Cal remarcar que la majoria dels errors de xarxa vénen provocats per canvis en la configuració dels sistemes o errors humans. En una xarxa amb diversos elements és habitual centralitzar les còpies de seguretat de les configuracions en una base de dades de configuració CMDB (*configuration managment data base*), per referenciar possibles incidents amb els canvis realitzats en l'arquitectura de xarxa. Aquest punt pren especial rellevància a mesura que les xarxes es tornen complexes i amb molts elements.

Figura 2. Procés de gestió de la configuració



3) Gestió de la comptabilitat (*accounting management*): aquest procés es focalitza a conèixer els recursos utilitzats per usuaris i/o serveis suportats per la xarxa per obtenir diversos indicadors de costos operacionals de la xarxa. Amb aquests indicadors es pot obtenir el cost en un determinat moment del dia, ajudant a planificar els manteniments o talls de la xarxa o ampliacions de la xarxa quan es requereixi. Aquestes dades són molt importants per gestionar el risc en intervencions i poder calcular l'impacte econòmic en interrupcions de servei.

Figura 3. Sistema de tarificació típica d'una xarxa mòbil



4) Gestió d'indicadors de rendiment (*performance management*): la gestió del rendiment consisteix en monitoritzar la xarxa per conèixer el seu estat de salut, a través d'uns indicadors tècnics, i avançar-nos als futurs problemes de xarxa, assegurant la disponibilitat del servei i els nivells òptims de xarxa.

Existeixen molts paràmetres per mesurar el rendiment en una xarxa de comunicacions però entre els més habituals i definits en els diferents estàndards tenim:

a) Mètriques a nivell de xarxa

- *Throughput* en bytes/segon o paquets/segon
- A nivell d'aplicació: trucades/segon
- Retards
  - Retard d'anada i tornada RTT (*round trip time*)
  - Variació del retard entre paquets consecutius (*jitter*)

b) Fiabilitat

- Percentatge de paquets perduts
- Taxa d'error de bit (BER)

5) Gestió de xarxa (*security management*): un altre dels aspectes crítics en la gestió de xarxa és la seguretat dels processos de gestió i els elements de xarxa. Aquest procés es focalitza en la confidencialitat dels usuaris i del negoci, protegeix la xarxa d'usuaris no autoritzats i s'asseguren les dades mitjançant l'autenticació i el xifrat, a més d'utilitzar tècniques de prevenció i detecció d'intrusos.

Aquest procés està prenent cada dia més rellevància donada la importància que té la seguretat en les comunicacions.

A mode de resum adjuntem la següent taula amb les funcions.

	Funcions	Tasques Detallades
Gestió de Fallades	Vigilància d'alarmes Localització d'avaries Reparació d'avaries Proves d'alta disponibilitat Administració d'anomalies	Detecció de fallades Correcció de fallades Aïllament de fallades Recuperació de xarxa Gestió d'alarmes Filtrat d'alarmes Generació d'alarmes Test de diagnòstics Registre d'errors Gestió d'errors Estadístiques d'errors

	Funcions	Tasques Detallades
Gestió de la Configuració	Planificació i enginyeria de la xarxa Instal·lacions Planificació de serveis Provisió Situació i control	Aprovisionament de xarxa Auto-descobriment Còpies de seguretat i restauració Eliminar elements de xarxa Gestió de canvis Pre-aprovisionament Maneig d'inventari/actius Còpia de configuració Configuració remota Distribució automàtica de programari Iniciació de treballs, seguiment i execució
Gestió de la Comptabilitat	Mesurament de la utilització Tarificació/fixació de preus Cobraments i finances Control de l'empresa	Costos per serveis Ús de quotes per servei Auditories Reportar fraus Combinació de costos de múltiples recursos Anàlisi de dades de rendiment Reportar problemes Planificació de capacitat Generació de reports Manteniment i avaluació de *logs* històrics
Gestió de Indicadors de rendiment	Assegurament de la qualitat de funcionament Supervisió de la qualitat de funcionament Control de la gestió de la qualitat de funcionament Anàlisi de la qualitat de funcionament	Percentatge d'utilització i relació d'errors Recol·lecció de dades de rendiment Anàlisi de dades d'indicadors Reportar problemes Planificació de capacitat Generació d'informes de rendiment Manteniment i avaluació de *logs* històrics
Gestió de la Seguretat	Prevenció Detecció Continència i recuperació Administració i operacions de la seguretat	Accés selectiu a recursos *Logs* d'accés Privadesa de dades Revisió dels privilegis de accés d'usuari Auditoria de seguretat Seguiment de *logs* Alarmes de seguretat/reportar esdeveniments Protecció de bretxes de seguretat i d'intents d'intrusió Seguretat relacionada amb la distribució d'informació

1.2. Components de la gestió de xarxa

La gestió de xarxa està formada bàsicament per quatre components (figura 4):

Funció del gestor de la xarxa

Si el gestor no fes un filtrat de la informació que realment és útil, la gestió de xarxa acabaria no resultant interessant atès l'excés d'informació. Cal, per tant, que el gestor elimini la informació supèrflua.

1) **Plataforma de gestió o element que supervisa**. Aquest component s'anomena *network management server* (NMS) i s'usa per a gestionar tota la xarxa. Rep tota la informació i la mostra un cop **filtra** el que realment és important.

2) L'element per gestionar. Aquest element s'anomena *network management agent* (NMA). L'NMA és un element de la xarxa com poden ser els encaminadors, commutadors, *hosts*, etc. A la vegada, cada node de xarxa conté una col·lecció de software encarregat de les tasques de gestió. Aquest software s'anomena NME (*network management entity*).

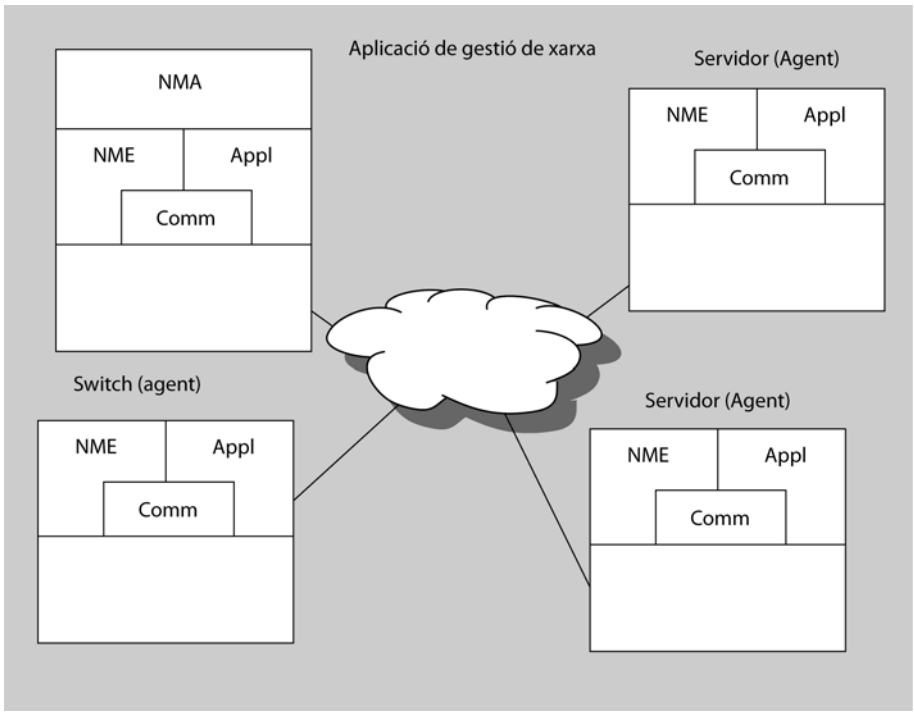
3) El protocol de diàleg entre l'agent i el servidor. El protocol més comú és SNMP (*simple network management protocol*). Genèricament seria el software de comunicació.

Exemples d'objectes per gestionar

Alguns exemples d'objectes per gestionar poden ser les taules d'encaminament d'un encaminador, l'última vegada que es va reiniciar un equip, etc.

4) Els objectes per gestionar. Aquests objectes són els recursos dels dispositius per gestionar. S'agrupen normalment en una mena de base de dades anomenada MIB (*management information base*).

Figura 4. Elements d'un sistema de gestió



2. Gestió de xarxa SNMP

La gestió de xarxa SNMP (*simple network management protocol*) engloba tot un grup d'especificacions de gestió de xarxa que inclouen el **protocol**, la **definició de l'estructura de dades** i altres conceptes associats.

2.1. Orígens de la gestió de xarxa SNMP

Als inicis del que coneixem com Internet no existien els protocols de gestió com a tal. L'única eina que es feia servir per "gestió" era el protocol ICMP (*Internet control message protocol*). ICMP està disponible en tots els dispositius IP i en els seus inicis era un mecanisme que servia per a testejar (*echo/reply*) la comunicació entre parelles de dispositius. El receptor del missatge "echo" està obligat a respondre a qui li fa la petició. A la vegada, també és útil per a obtenir altres informacions molt interessants, com són el retard en la xarxa.

L'exemple més conegut de l'ús del protocol ICMP és el programa **ping** (*packet Internet grouper*). Amb aquesta senzilla eina es poden observar, entre altres, les variacions en el retard extrem a extrem, la pèrdua de paquets, de manera que pot ajudar entre altres coses a determinar àrees de congestió i punts de fallada.

Figura 5. Captura d'una petició ping des de *cmd*

```
Z:\>ping 147.83.245.4

Haciendo ping a 147.83.245.4 con 32 bytes de datos:

Respuesta desde 147.83.245.4: bytes=32 tiempo=1ms TTL=255
Respuesta desde 147.83.245.4: bytes=32 tiempo=1ms TTL=255
Respuesta desde 147.83.245.4: bytes=32 tiempo=44ms TTL=255
Respuesta desde 147.83.245.4: bytes=32 tiempo=1ms TTL=255

Estadísticas de ping para 147.83.245.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 44ms, Media = 11ms

Z:\>
```

Aquesta eina juntament amb altres eines senzilles van ser solucions prou vàlides per a la gestió de xarxa fins a mitjan anys vuitanta. A partir de llavors, amb el creixement exponencial d'Internet es va fer necessari plantejar noves eines per a la gestió.

Les propostes més interessants van ser:

- *Simple network management protocol* (SNMP)
- CMIP sobre TCP/IP (CMOT)

El 1988 Internet Architecture Board (IAB) va revisar les propostes i va aprovar que SNMP fos desenvolupat com una solució a curt termini mentre que es plantejava CMOT com la solució cap a on s'havia d'anar. La simplicitat del protocol SNMP va fer que aviat fos el protocol escollit pels fabricants.

Fent una breu cronologia de l'evolució d'SNMP tenim el següent:

1) SNMPv1. Sorgeix i introdueix les bases a la gestió de xarxes.

2) SNMPv2. Millora capacitats de transferència de dades i intercanvi d'informació entre gestors. (*getbulkrequest*, *informrequest*) i millora la manera de gestionar les taules.

3) RMONv1. Permet la monitorització remota d'un segment de xarxa.

4) RMONv2. Amplia la MIB-II d'RMON i permet un monitoratge de segments de xarxes LAN i un seguiment del trànsit a nivell de xarxa i aplicació.

5) SNMPv3. Introdueix capacitats de seguretat (control d'accés, autenticació i privacitat).

2.2. Arquitectura de gestió de xarxa SNMP

El model de gestió de xarxa TCP/IP té els elements clau següents:

- L'estació de gestió o gestor
- Els agents gestionats
- La base de dades de gestió (*managament information base*, MIB)
- El protocol de gestió de xarxa

L'**estació de gestió** pot ser o un o un grup de dispositius distribuïts. L'estació de gestió serveix d'interfície entre el gestor i el sistema de gestió de xarxa.

Si us hi fixeu, els elements de la xarxa TCP/IP són els mateixos ja comentats en el subpartat 1.1.2.

Els **agents gestionats** són l'equipament lògic allotjat en els dispositius per gestionar de la xarxa. Emmagatzema dades de gestió i respon a les peticions associades a aquestes dades. De forma asíncrona (*traps*) –dels quals parlarem més endavant– poden proporcionar informació al gestor sense que aquest ho sol·liciti.

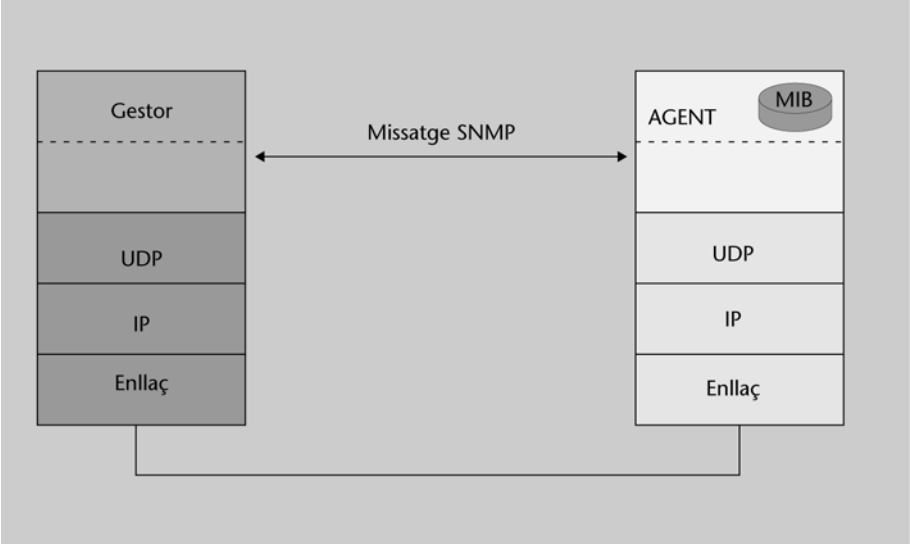
La **base de dades de gestió (en anglès *managament information base,* MIB)** és una base de dades virtual dels recursos per gestionar, els quals es representen com a objectes. Aquests objectes de la MIB estan **estandarditzats**, són accessibles per l'agent i poden ser manipulats via SNMP per realitzar la gestió de xarxa.

En el subapartat 2.3 tractarem en detall la MIB i els seus objectes.

Finalment, l'últim element bàsic dintre de l'arquitectura és el protocol de comunicació, el qual permet comunicar l'estació de gestió amb els agents. En aquest cas és el protocol SNMP. És un protocol que es basa en el paradigma **petició-resposta**.

En la figura 6 tenim l'esquema bàsic amb els quatre elements descrits.

Figura 6. Model d'arquitectura de gestió SNMP



Protocol SNMP

El protocol SNMP està muntat sobre UDP, que és un protocol de capa de transport no orientat a connexió.

2.3. La base de dades d'informació a SNMP

La base de dades d'informació s'anomena MIB (*management information base*) i conté la informació del elements per ser gestionats.

La MIB està estructurada en forma **jeràrquica**, on cada recurs està representat per un objecte.

En el subapartat 2.3.2 podeu veure com està formada l'estructura jeràrquica de la MIB.

La MIB ha de complir un parell de regles bàsiques:

1) L'objecte u objectes utilitzats per a representar un recurs particular ha de ser el mateix per a tots els sistemes.

> Seria impossible crear un protocol per adquirir informació si aquesta informació depengués del sistema per gestionar.

2) Ha d'existir un esquema comú de representació per suportar interoperabilitat. Aquest esquema comú és l'**estructura de dades d'informació (SMI).**

2.3.1. Estructura de dades d'informació. Model d'informació

L'SMI defineix el tipus de dades que es poden utilitzar i especifica com es poden representar i anomenar els recursos.

SNMP usa com a notació un subconjunt d'*abstract syntax notation one* (ASN.1) per a acomodar la comunicació entre sistemes heterogenis.

ASN.1 és un format de dades que és comú a totes les màquines i, per tant, que és independent del hardware, sistema operatiu. Per fer aquesta representació de les dades es podia haver agafat algun llenguatge d'alt nivell ja existent, com C, però el que s'ha volgut és que sigui independent del llenguatge.

Implementació de l'ASN.1

L'ASN.1 és una notació comuna per a representar les dades, però la seva implementació es pot fer en el llenguatge que es vulgui.

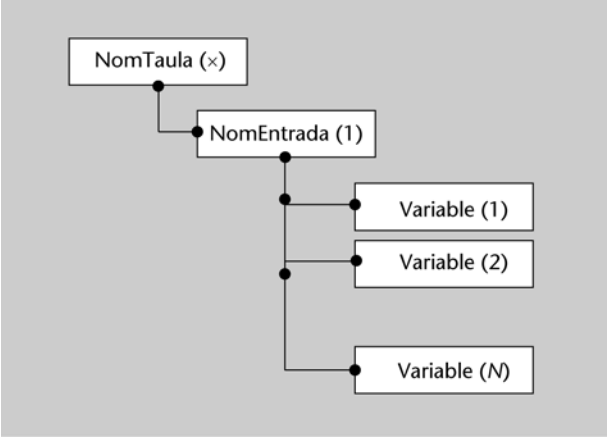
La MIB SNMP emmagatzema, de tots els tipus definits per l'ASN.1, només els tipus de dades simples, entenent per simples el següent:

- **Escalars**. Així les possibles variables són les que es mostren en la taula següent.

Nom	Tipus	Bytes	Significat
INTEGER	Numeric	4	Enter 32 bits
Counter32	Numeric	4	Unsigned 32 bits counter that wraps
Gauge32	Numeric	4	Unsigned value that does no wrap
Integer32	Numeric	4	32 bits
Unteger32	Numeric	4	Like integer32 but unsigned
Counter64	Numeric	8	A 64 bit counter
TimeTicks	Numeric	4	
BIT STRING	String	4	Bit map of 1 to 32 bits
OCTET STRING	String	0	Variable length byte string
Opaque	String	0	Obsolete
OBJECT IDENTIFIER	String	> 0	A list of integers
ipAddress	String	4	A dotted decimal integer address
NsapAddress	String	< 22	An OSI NSAP address

- ***Arrays* bidimensionals d'escalars (taules)**. La manera de definir una taula, que és usada per totes les taules de la MIB, és mitjançant dos tipus ASN.1, que són: SEQUENCE i SEQUENCE OF. SEQUENCE és comparable al que entenem per un *array* en programació, mentre que SEQUENCE OF seria comparable a una estructura. D'aquesta manera, la taula es crea a partir d'un *array* on cada element de l'*array* és una estructura d'escalars. La forma es mostra en la figura 7.

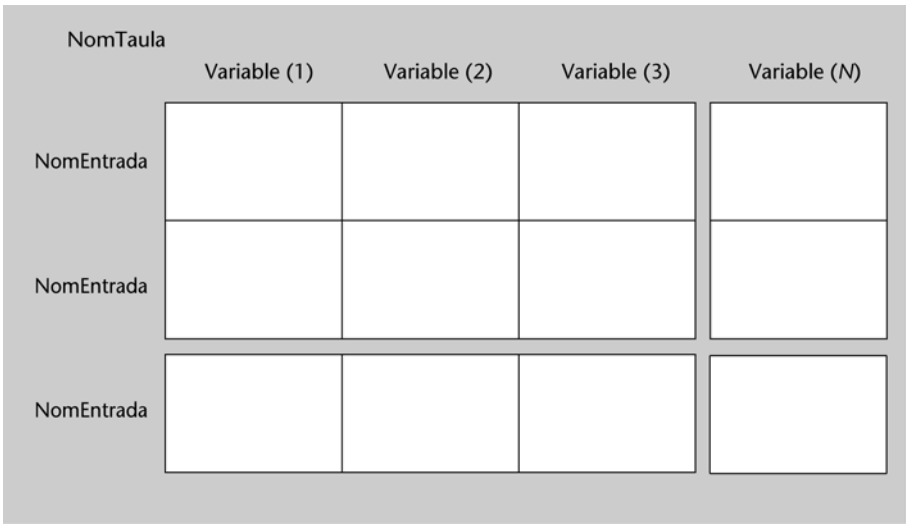
Figura 7. Exemple de taula genèrica SNMP



Les fileres de la taula estaran formades per elements *NomEntrada* els quals són una SEQUENCE. A la vegada hi haurà una de les variables o diverses que seran els índex. Aquests índex permetran distingir cada una de les fileres dintre de la taula (figura 8).

Parlarem més endavant de l'ús dels índexs.

Figura 8. Representació d'una taula SNMP



2.3.2. Estructura de la MIB

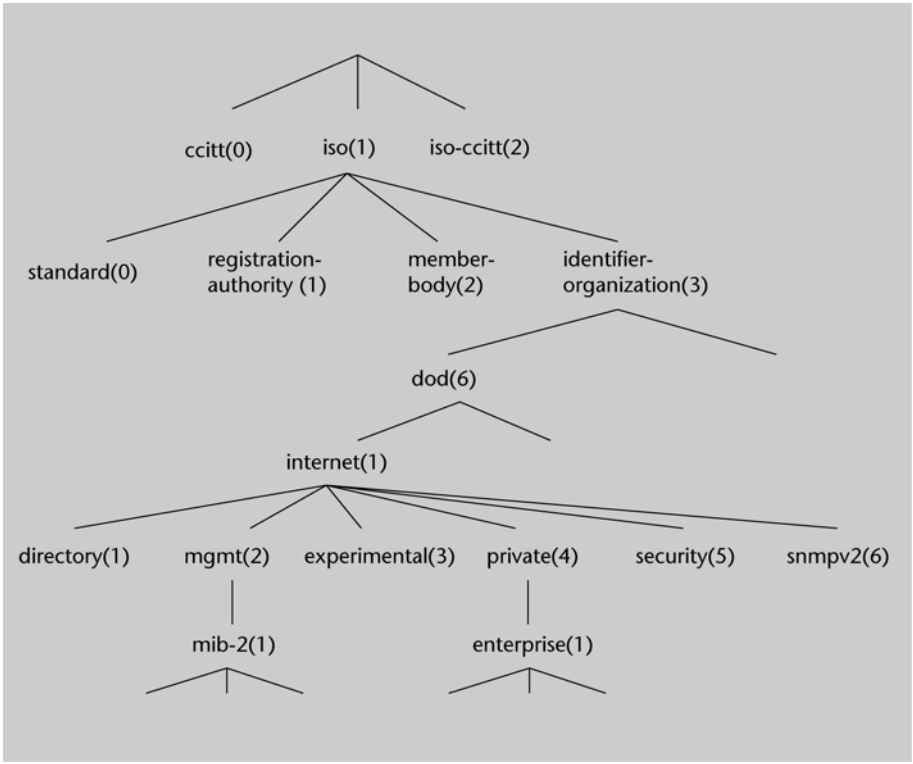
Per a definir l'estructura de la MIB el primer que cal fer és tenir clar com se'n volen definir els objectes. Així l'estructura utilitzada segueix les regles bàsiques següents:

- Identificació no ambigua i universal dels objectes a través d'una arquitectura en forma d'arbre.
- Aquesta estructura està basada en l'esquema d'identificació d'objectes definit per l'OSI.

Seguint aquest esquema de l'OSI els objectes gestionats a l'entorn SNMP estan ordenats en una arquitectura d'arbre on les branques són els diversos objectes.

Associat a cada tipus d'objecte hi ha un identificador de tipus ASN.1 (*object identifier*) que serveix per a anomenar els objectes i per a situar-se dintre de l'estructura de l'arbre. La jerarquia MIB es pot veure com un arbre amb una arrel sense nom i on tenim diversos nivells, que estan assignats per diverses organitzacions (figura 9).

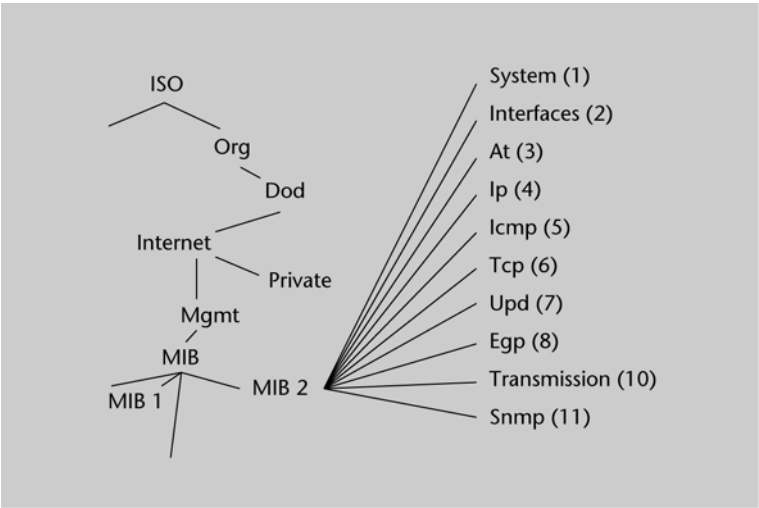
Figura 9. Representació de forma jeràrquica de la MIB



Un aspecte molt important en la comunicació entre dispositius heterogenis és que hi hagi una representació de les dades que sigui comuna. Així aquesta tasca, com ja s'ha dit, la fa la notació estandarditzada ASN.1.

Dintre de la MIB-II trobem els grups que es mostren en la figura 10.

Figura 10. Grups de la MIB 2 dintre de l'estructura jeràrquica



En la taula següent es mostren els deu grups administrats amb una breu descripció de cadascun d'ells.

Grup	Objectes	Descripció
System	7	Nom, localització i descripció de l'equip
Interfaces	23	Interfícies de xarxa i estadístiques de trànsit
At	3	Translació d'adreces (no usat)
Ip	42	Estadístiques dels paquets IP
Icmp	26	Estadístiques de paquets ICMP rebuts
Tcp	19	Algorismes, paràmetres i estadístiques de trànsit TCP
Udp	6	Estadístiques de trànsit UDP
Egp	20	Estadístiques de trànsit EGP
Transmission	0	Reservat
snmp	29	Estadístiques de trànsit SNMP

2.3.3. Definició dels objectes

Una MIB està formada per objectes. Cada objecte definit té associat un tipus i un valor. Així, com podeu imaginar, hi ha molts tipus diferents en funció de la informació dels objectes.

Per senzillesa s'usa una macro per a crear els diferents objectes. Aquesta macro defineix la sintaxi per als diferents conjunts de tipus relacionats.

```
OBJECT-TYPE MACRO ::=
BEGIN
  TYPE NOTATION ::= "SYNTAX" type (TYPE ObjectSyntax )
        "ACCESS" Access
        "STATUS" Status
  VALUE NOTATION ::= value (VALUE ObjectName)
  Access ::= "read-only"
      | "read-write"
      | "write_only"
      | "non-accessible"
  Status ::= "mandatory"
      | "optional"
      | "obsolete"
END
```

A partir d'aquesta es creen els tipus específics, el que anomenem "instàncies macro".

```
OBJECT:
  object descriptorobject identifier
SYNTAX:
  sintaxi ASN.1 dels objectes
DEFINITION:
  descripció de l'objecte
ACCESS:
  només lectura, lectura-escriptura o no accessible
STATUS:
  obligatori, opcional o obsolet
```

Exemple de definició d'objecte

A continuació teniu un exemple de definició d'objecte que proporciona l'RFC 1212

```
ifNumber OBJECT-TYPE
         SYNTAX  INTEGER
         ACCESS  read-only
         STATUS  mandatory
         DESCRIPTION
               "The number of network interfaces (regardless of
               their current state) present on this system."
         ::= { interfaces 1 }
```

Web recomanada

Els RFC (*request for comments*) contenen informació tècnica i documents associats a Internet que inclouen especificacions tècniques i documents polítics produïts per l'Internet Engineering Task Force (IETF). Els podeu consultar a http://www.rfc-editor.org.

En el cas de l'exemple, quan es vol anomenar aquest objecte concret cal fer: *Iso (1) identified-organization (3) dod (6) internet (1) mgmt(2) mib-2(1) interfaces (2) IfNumber (1)* o la forma com s'expressa habitualment 1.3.6.1.2.1.2.1.

Per a poder demanar la informació concreta de la variable associada a aquest objecte llavors cal incloure un 0: 1.3.6.1.2.1.2.1.0

En el subapartat 2.4.3 podeu veure en detall com es fa la petició a objectes concrets (instàncies).

Un tipus d'objecte que cal tractar a part són les taules. SMI suporta només una forma d'estructura de dades: **taules bidimensionals d'escalars**.

2.3.4. Les MIB privades

Una de les característiques més importants d'SNMP és el fet que la MIB ha estat dissenyada de manera que pot anar creixent i així proporciona flexibilitat per a incorporar nous objectes. Si us fixeu en la figura 7, on es mostra l'estructura MIB hi ha una branca *private* en què es poden afegir extensions. Això permet als fabricants incorporar objectes associats a la gestió específica dels seus productes. Gràcies a l'estandardització de l'SMI encara que creem objectes privats aquests es poden gestionar des de qualsevol plataforma de gestió, és a dir, hi ha d'haver una interoperabilitat que arribi fins a les extensions privades de la MIB.

Per defecte, les estacions de gestió només coneixen la MIB estàndard. Per tant, per poder gestionar objectes MIB privats cal que prèviament es carregui l'estructura de la MIB privada en la plataforma de gestió.

Les plataformes de gestió actuals permeten compilar noves MIB per a gestionar recursos privats.

2.4. El protocol SNMP

Hi ha uns conceptes bàsics relacionats amb les operacions del protocol SNMP:

- Les operacions que suporta SNMP
- Les comunitats
- La identificació d'instàncies

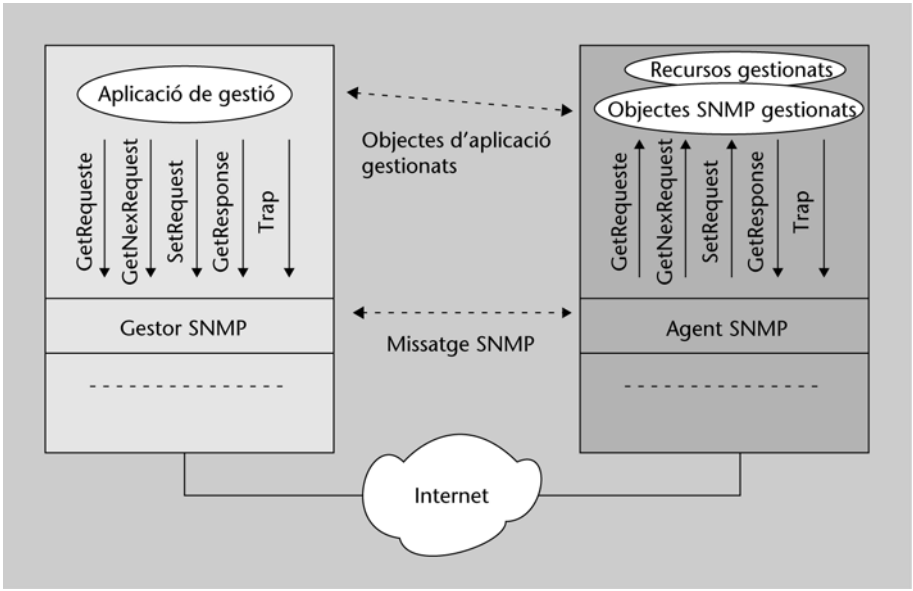
2.4.1. Operacions en SNMP

Totes les operacions que suporta el protocol SNMP estan relacionades amb la modificació i inspecció de variables. En els objectes escalars es poden agrupar en tres tipus d'operacions bàsiques:

- **Get**. L'estació de gestió demana un objecte escalar a l'estació gestionada.
- **Set**. L'estació de gestió actualitza un objecte escalar d'una estació gestionada.
- ***Trap***. L'estació gestionada envia el valor d'un objecte escalar al gestor sense sol·licitud prèvia.

Hi ha cinc tipus de missatges usats per SNMP, com mostra la figura 11.

Figura 11. Accions SNMP



Accés a un únic objecte cada cop

L'accés a un únic objecte cada cop és una restricció que simplifica la implementació d'SNMP però limita la capacitat del sistema de gestió.

No és possible accedir a una taula sencera amb una única acció.

2.4.2. Les comunitats SNMP

La comunitat SNMP és una relació entre agent i gestor que defineix bàsicament **autenticació** i **control d'accés**.

Una comunitat SNMP és una **relació** entre l'**agent SNMP** i els **gestors SNMP**. El concepte de comunitat és **local** i es defineix en el sistema gestionat. Aquest crea una comunitat per a cada combinació d'autenticació i control d'accés. A cada comunitat se li dóna un nom de comunitat únic (dintre de l'agent), el qual es proporciona a l'estació de gestió. Aquesta estació, a la vegada, ha d'usar aquest nom cada cop que fa una operació *get* o *set*. L'agent pot establir diverses comunitats en funció dels permisos dels gestors.

Llavors, **com fa l'autenticació?** Cada missatge que genera el gestor cap a l'agent ha d'incloure el nom de comunitat (*community name*).

Autenticació i control d'accés

Entenent per autenticació el cas en què el missatge és autèntic.

Control d'accés = diferents privilegis en funció del gestor.

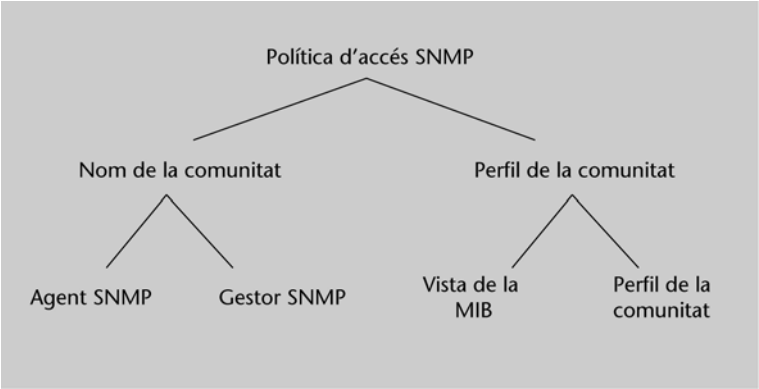
I com funciona la política d'accés? L'agent pot crear diferents categories d'accés a la MIB en funció de qui sigui el gestor. El que fa és crear diferents perfils lligats al nom de comunitat que tenen accés a les diferents parts de la MIB amb permisos concrets de lectura o lectura/escriptura (mode d'accés).

Així, la figura 12 intenta mostrar tot el que serien les polítiques d'accés a SNMP. Per una banda, tenim el nom de comunitat que coneixen tant l'agent com el gestor. Per l'altra, el que tenim és que cada comunitat té associat un perfil que li permet tenir accés a unes parts de la MIB concretes.

Noms de comunitat dels dispositius

Els dispositius per defecte solen portar dos noms de comunitat coneguts per tothom: *public* (lectura) i *private* (lectura/escriptura). Cal tenir cura d'eliminar-los.

Figura 12. Conceptes administratius



2.4.3. Identificació d'instàncies

Cada objecte a la MIB té un únic identificador d'objecte, que està definit per la posició que ocupa dintre de l'arbre MIB. No obstant això, quan es fa un accés a la MIB via SNMP el que es vol no és el tipus de l'objecte sinó una instància concreta (el valor de la variable). Vegem com es fa.

Cal que recordeu la diferència entre objecte i instància de l'objecte.

Cas d'objectes escalars

Per a obtenir la instància d'un objecte escalar cal posar el camí per a arribar a l'objecte i incloure al final sempre **.0.**

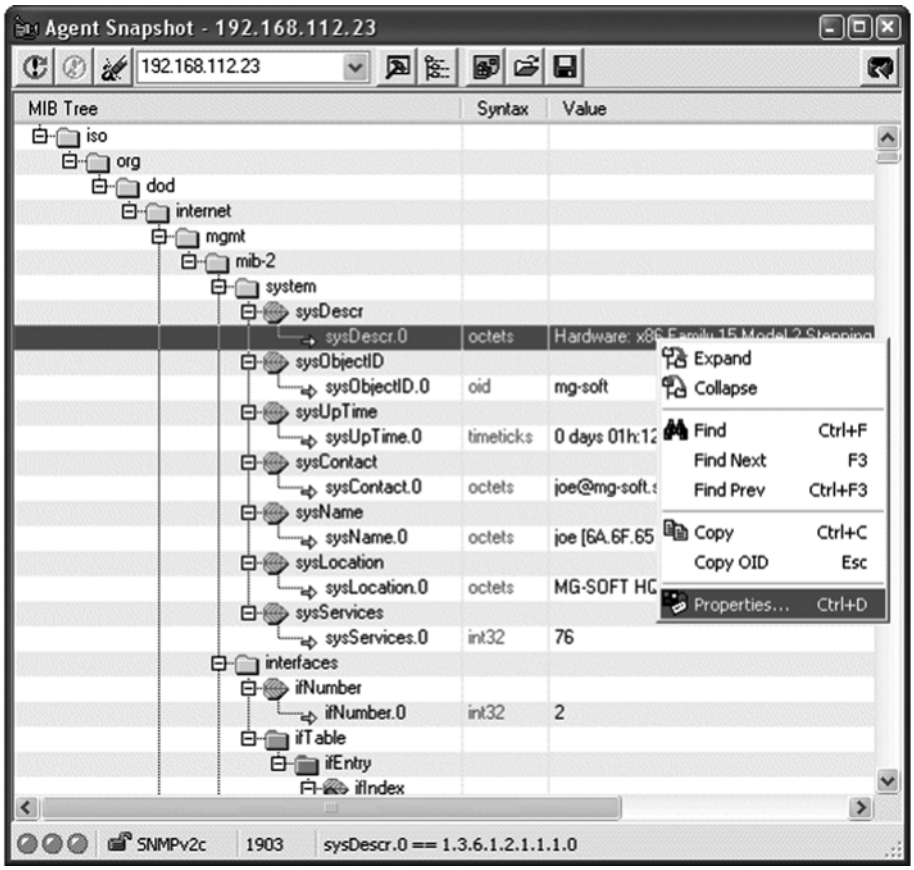
El 0 es posa per diferenciar entre fer una referència a un objecte i fer-la a la variable associada a aquest objecte.

Per exemple tenim,

	OBJECT IDENTIFER
Snmp subtree	1.3.6.1.2.1.11
snmpInBadValues	1.3.6.1.2.1.11.10
instància de snmpInBadValues	1.3.6.1.2.1.11.10.0

En la figura 13 es mostra l'arbre mib-2 i unes peticions als diversos objectes del grup *system*.

Figura 13. Resultat obtingut del grup *system* amb una aplicació de gestió



Objectes de tipus taula

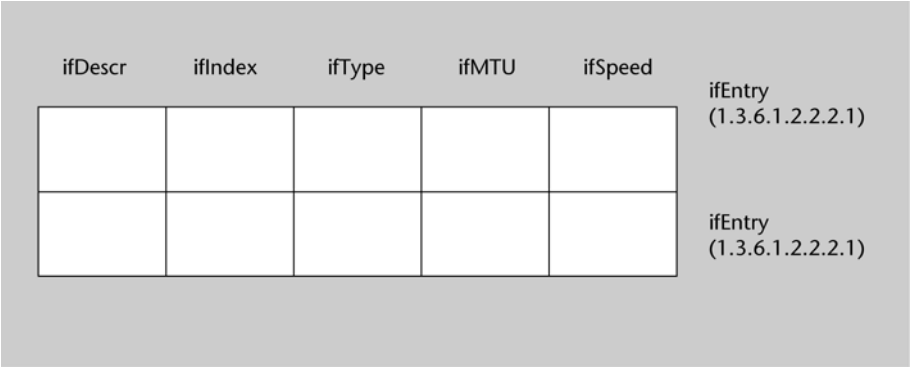
L'accés a les instàncies dintre d'una taula, encara que el mecanisme és senzill, resulta una mica complicat d'explicar. El millor és veure-ho mitjançant un exemple.

Exemple

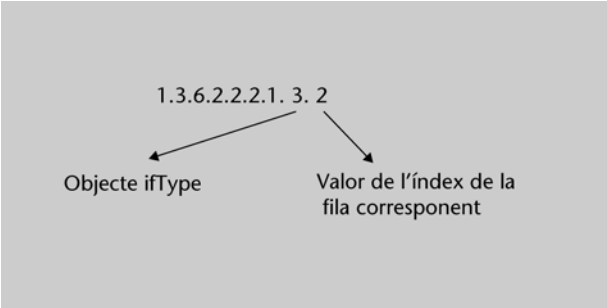
Suposem un dispositiu amb dos interfícies i volem informació del grup dintre de la mib-2 anomenada *interface*. Aquest grup té la forma següent:

```
Interfaces
  ifTable
         ifEntry
                ifDescr
                IfIndex
                ifType
                ifMTU
                ifSpeed
```

En aquest cas tindríem una taula amb dos files i cinc columnes de la forma següent:



A partir d'aquesta informació, si el que volem fer és una instància concreta, per exemple d'*ifType*, haurem de fer:



En cas que tinguem una taula amb més d'un índex caldria fer:

Ruta.objecte.valor_index1.valor_index2_..valor_index*n*

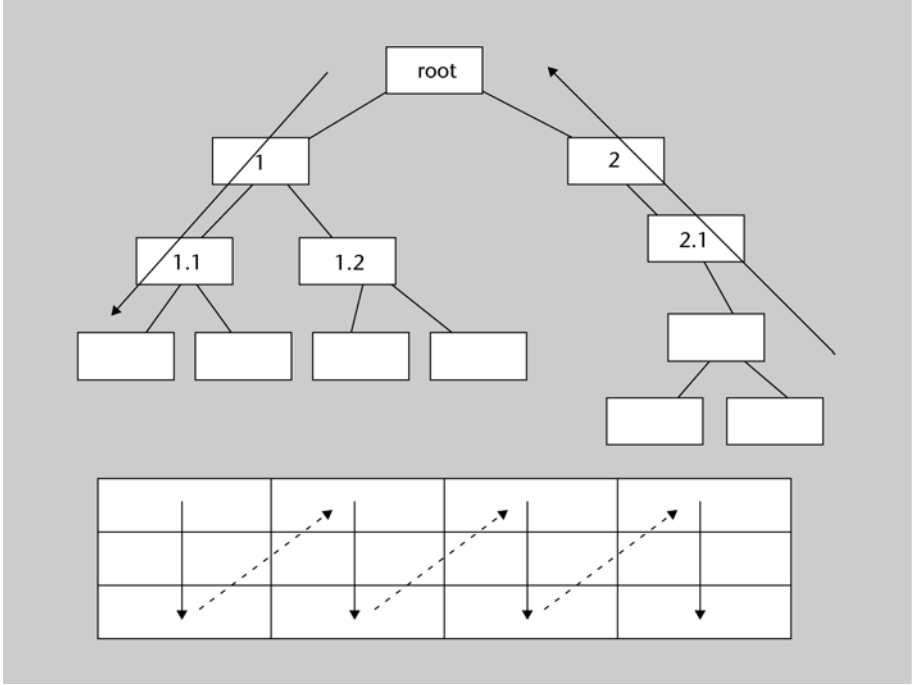
Aquesta és l'única forma d'identificar correctament la filera exacta on es troba la instància de l'objecte sol·licitat.

Cal que tingueu present que els índex poden tenir qualsevol valor en funció de l'objecte que representin.

Es molt interessant tenir clar l'ordre lexicogràfic en un arbre d'objectes, tant escalars com en una taula.

En la figura 14 es mostra com ens movem dintre de l'arbre jeràrquic i a la vegada dintre d'una taula concreta si anem sol·licitant els valors dels objectes un darrere l'altre.

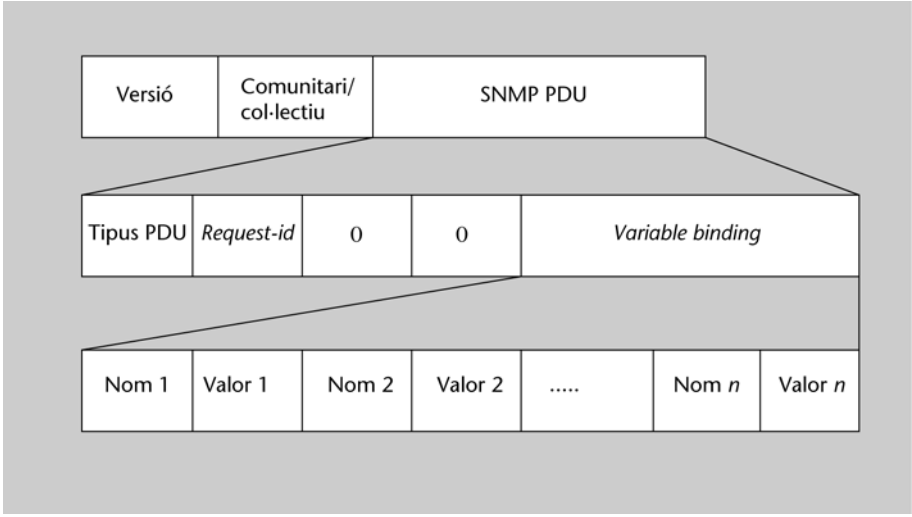
Figura 14. Ordre d'accés a les instàncies dels objectes dintre de les taules SNMP



2.4.4. Format del paquet SNMP

En la figura 15 es mostra el format del paquet SNMP. Com podem veure tots els missatges inclouen el número de versió d'SNMP, nom de la comunitat per utilitzar en l'intercanvi i tipus de missatge.

Figura 15. Format dels paquets SNMP



Cal saber que en un mateix missatge SNMP es poden incloure diverses operacions del mateix tipus.

Un cas interessant és *GetNextRequest*. Es similar a *GetRequest* però amb la diferència que permet veure el valor següent dintre de l'estructura de l'arbre, és a dir, quan sol·licitem una instància no obtenim el valor de la mateixa instància

sinó el valor corresponent a l'objecte immediatament posterior al sol·licitat. Es molt útil en el cas que es vulgui accedir als valors d'una taula. Si recordeu, hem explicat que per a accedir a les instàncies d'una taula calia posar els valors de les instàncies índex d'aquesta taula, la qual cosa és complicada *a priori*, ja que no sabem aquests valors. En aquest cas, el que fem és demanar el valor justament anterior dintre de l'arbre d'objectes i el que l'agent ens retorna és el primer valor de la taula.

Exemple

Si recordem l'exemple anterior a la petició següent: GetNext (1.3.6.1.2.2.1.0), la resposta que obtindrem serà:

GetReponse = 1.3.6.1.2.2.2.eth0.1

En aquest cas ens retorna el valor d'*IfDescr* i a la vegada el valor que té l'índex de la primera fila.

2.5. Limitacions del protocol SNMP

Un cop vist el funcionament bàsic del protocol SNMP, cal que tingueu present algunes de les seves limitacions:

- SNMP no és adequat per a la gestió de xarxes molt grans ateses les limitacions de rendiment lligades al paradigma petició-resposta.
- SNMP no està ben dissenyat per a grans volums de dades com són les taules.
- Els *traps* no tenen reconeixement, la qual cosa pot provocar que *traps* crítics es puguin perdre sense que arribin al gestor. Recordeu que els *traps* permeten a l'agent generar un missatge cap al gestor sense petició prèvia.
- L'autenticació, com s'ha vist, és molt trivial.
- La MIB té limitacions.
- SNMP no suporta comunicació entre gestors.

Per què els *traps* no tenen reconeixement

Doncs, com s'ha dit, perquè SNMP té UDP com a protocol de capa de transport.

3. SNMPv2

L'SNMPv2 és una evolució de la versió inicial d'SNMP, la qual inclou tota una sèrie de millores respecte a la versió anterior.

3.1. Millores en la gestió

Cal que tingueu present que el primer que cal destacar és el canvi en la filosofia de treball d'aquesta nova versió. SNMPv2 pot suportar tant **gestió centralitzada** com **distribuïda**. En aquest cas alguns gestors faran el paper de gestor i agent simultàniament. Com a agents acceptaran comandes d'un gestor de categoria superior. Aquestes peticions poden ser per a obtenir informació del gestor intermedi o per a demanar informació en aquest gestor un informe dels agents que hi estan subordinats. De la mateixa manera, el gestor intermedi pot enviar *traps* al superior.

Les millores d'SNMPv2 s'agrupen en tres categories:

- Estructura de la informació de gestió
- Capacitat gestor-gestor
- Operacions del protocol

3.2. Estructura de la informació de gestió

L'estructura de la informació de gestió (SMI) creix respecte a l'SMI de la versió 1. Trobem una estructura amb més tipus de dades, millora en la documentació associada a cada objecte i un aspecte molt important que és una nova convenció per a crear i esborrar fileres en les taules de la MIB.

Si hem de resumir breument com queda aquesta estructura es pot reduir a quatre conceptes clau:

1) Definició d'objectes. Es crea una nova macro que permet incloure nous tipus de dades i millorar la documentació associada a cada objecte.

2) Taules conceptuals. SNMPv2 millora el mecanisme usat tant a l'RFC 1212 com a l'especificació RMON per a facilitar la creació, eliminació i accés a les fileres de les taules.

3) Definicions de notificació. Es crea una macro específica que defineix la informació enviada per una entitat SNMPv2 quan hi ha un esdeveniment excepcional en l'entitat.

4) Mòduls d'informació. SNMPv2 introdueix el concepte de mòdul d'informació, que especifica un grup de definicions que estan relacionades.

3.3. El protocol SNMPv2

Quant a les operacions del protocol, aquest inclou dos nous tipus de PDU:

- *GetBulkRequest*. Permet obtenir un gran nombre de blocs de dades de forma eficient, com són la possibilitat d'obtenir diverses fileres d'una taula.

- *InformRequest*. Amb aquesta PDU el gestor intermedi pot enviar *traps* a un altre gestor.

4. SNMPv3

Una de les grans mancances dels protocols SNMPv1 i SNMPv2 és la seguretat en les comunicacions. Com ja hem analitzat el protocol SNMP representa els aspectes de gestió de les xarxes i si aquest protocol és vulnerable podem afirmar per extensió que la xarxa sencera és vulnerable a atacs.

El protocol SNMPv3 és l'evolució del protocol SNMPv2, que millora i soluciona diversos aspectes relacionats amb la seguretat, incloent autenticació, privadesa i control d'accés.

El protocol SNMPv3 va aparèixer el 1997, estant descrit en les RFC 1902-1908 i 2271-2275. Cal destacar que SNMPv3 no es tracta d'un estàndard que reemplaça a SNMPv1 i/o SNMPv2, sinó que defineix una sèrie de capacitats addicionals de seguretat i administració a ser utilitzades en conjunció amb SNMPv2 (preferiblement) o SNMPv1. Aquestes millores faran que SNMPv3 s'aconselli com el protocol de gestió per ser utilitzat amb altes prestacions i seguretat en tot tipus de xarxes.

4.1. Marc de referència

Com ja hem indicat, SNMP consisteix en diversos estàndards realitzats pel IETF i adoptats per la indústria. A continuació indiquem la referència dels estàndards i una breu descripció:

- **RFC 3410**: defineix el protocol d'administració senzilla de xarxa (SNMPv3) que és un protocol utilitzat per accedir a una xarxa d'objectes administrats i recepció d'avisos de canvi.
- **RFC 3411**: descriu l'arquitectura per al protocol d'administració senzilla de xarxa SNMPv3.
- **RFC 3412**: descriu el processament i enviament de missatges per al protocol d'administració senzilla de xarxa SNMPv3.
- **RFC 3413**: descriu les aplicacions per al protocol d'administració senzilla de xarxa SNMPv3.
- **RFC 3414**: descriu el model de seguretat basat en usuaris (USM) versió 3 per al protocol d'administració senzilla de xarxa SNMPv3.
- **RFC 3415**: descriu el model de control d'accés basat en vistes (VCAM) per al protocol d'administració senzilla de xarxa SNMPv3.

El Terme RFC

El terme RFC (*request for comments*) consisteix en els estàndards desenvolupats per l'IETF. Per a més informació consulteu https://www.ietf.org/rfc.html.

4.2. Objectius de seguretat d'SNMPv3

Els principals objectius des del punt de vista de seguretat que SNMPv3 aborda són els següents:

- **Autenticitat**: és el missatge enviat des d'un usuari vàlid?
- **Integritat**: s'ha modificat el missatge SNMP durant la seva transmissió per la xarxa?
- **Confidencialitat**: s'ha mantingut el secret de la informació durant la seva transmissió per la xarxa?
- **Disponibilitat**: està el servici de monitoratge SNMP disponible per a l'usuari?
- **Autorització**: té l'usuari que ha sol·licitat la lectura d'un valor SNMP permisos per a l'operació en aquest objecte?

4.3. Arquitectura d'SNMPv3

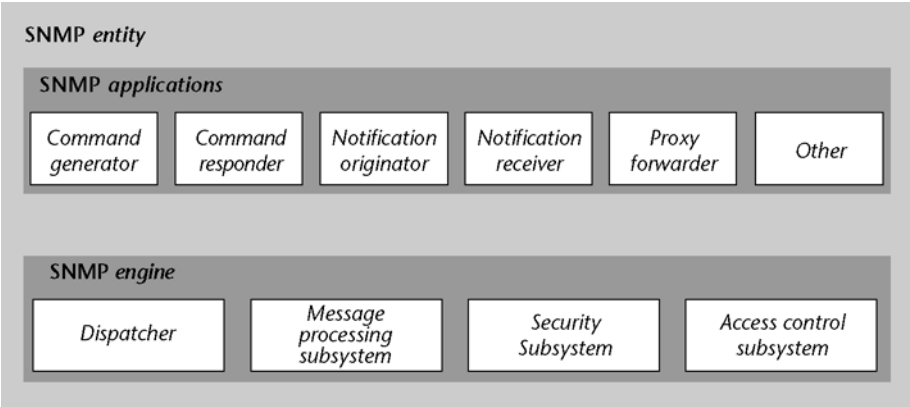
El canvi més significatiu d'aquesta versió en referència a l'arquitectura és que abandona la noció d'estacions i agents. Ambdós són denominats entitats SNMP. Cada entitat consisteix d'un motor (*engine*) i una o més aplicacions, i permeten definir una arquitectura més que un simple conjunt de missatges; l'arquitectura genera una autonomia de les peces d'un sistema SNMP, la qual cosa fa possible implementar aspectes de seguretat.

Un altre dels aspectes que més ha canviat en SNMPv3 és la implementació del motor (peça que s'encarrega de processar les peticions) que rep les transaccions d'SNMP. Així en SNMPv3 en augmentar la complexitat s'han hagut de redissenyar els diferents mòduls.

En la versió SNMPv3 els diferents agents es denominen *entity* i corresponen als diferents elements de la solució. Cada *entity* implementa diferents mòduls en funció de les capacitats que aquesta necessiti implementar.

A continuació representem gràficament, en la figura 16, els mòduls i components que componen una entitat SNMPv3.

Figura 16. Esquema de l'arquitectura d'SNMPv3



Com podem observar en la figura anterior cada entitat es composa de dos apartats:

1) Aplicacions: corresponen als aspectes funcionals del protocol SNMP. Així podem trobar les següents tipologies:

- *Command generator*. Corresponen a les trucades *Get*, *Getnext*, *Getbulk* i *Set*, i a més processa les respostes. Aquesta aplicació la implementa una estació, i d'aquesta manera pot monitorejar i configurar equips de xarxa (encaminador, *switch*, *hosts*, etc.).

- *Command reponder*. Es tracta de l'aplicació que rep les trucades de l'aplicació anterior i prepara les trames *Response*.

- *Notification orginator*. Igual que en SNMPv1 i v2 aquesta aplicació és l'encarregada de generar els *traps* i les notificacions (*Inform-Request*).

- *Notification receiver*. Aquesta aplicació és l'encarregada de rebre els missatges anteriors (*Inform*) i generar un missatge de resposta (*Response*).

- *Proxy forwarder*. Aquesta aplicació s'usa per reexpedir les peticions SNMP a altres entitats podent realitzar alguna modificació en aquesta aplicació.

2) Motors (*Engine*). Els motors actuen com a peces auxiliars a les aplicacions i que doten a l'arquitectura de capacitats d'enviament i recepció de missatges, encriptació i desencriptació, control d'accés i verificació de permisos. Podem destacar els següents motors:

- *Dispatcher*: Aquest motor és l'encarregat de realitzar les funcions de passarel·la entre l'aplicació i els diferents mòduls auxiliars. Igualment, és el mòdul que interactua amb les capes de xarxa i amb el sistema de procés de missatges.

- *Message processing subsytem*: Aquest sistema prepara els missatges per ser enviats (en cas de consultes a altres entitats) o extreu les dades d'aquells missatges que són rebuts des d'alguna entitat en particular. Aquesta etapa conté múltiples mòduls de processament de missatges. Per exemple, un subsistema pot tenir mòduls per processar consultes SNMPv1, SNMPv2c i SNMPv3. També pot tenir un mòdul per processar altres models que puguin ser definits en un futur.

- *Security Subsystem*: proveeix serveis d'autenticació i privadesa. L'autenticació pot ser basada en comunitats (v1 i v2c) o en usuaris (v3). L'autenticació basada en usuaris usa els algorismes MD5 o SHA i així evita enviar una contrasenya en text pla. Per a encriptar i desencriptar missatges SNMP (concepte de privadesa) s'usa l'algorisme DES i AES.

- *Access control subsystem*: és responsable de controlar l'accés cap a objectes MIB. És possible definir quins objectes pot accedir un determinat usuari, i a més quina operació té permesa fer sobre aquests objectes.

Amb l'arquitectura anterior i per aconseguir els reptes de seguretat citats als apartats previs SNMPv3 implementa dos models de seguretat: USM (*User-based security model*) i VACM (*Views- access control model*). A continuació passem a descriure cada model.

4.3.1. Model basat en usuari

El model de seguretat basat en usuari o USM (*User-based security model*) proporciona els serveis d'autenticació i privadesa en SNMPv3.

El mecanisme d'autenticació en USM assegura que un missatge rebut va ser transmès per l'entitat indicada autenticant en el camp corresponent a la font en la capçalera del missatge. Igualment, garanteix que el missatge no va ser alterat durant el seu trànsit i que no va ser retardat o repetit.

Per aconseguir l'autenticació, el gestor i l'agent que desitgen comunicar-se han de compartir la mateixa clau d'autenticació secreta (Usuari/*Password*) configurada prèviament fora de SNMPv3 (no està emmagatzemada en la MIB i no és accessible mitjançant SNMP). El protocol d'autenticació utilitzat pot ser l'HMAC-MD5-96 o l'HMAC-SHA-96.

En referència a la privadesa el model USM possibilita als gestors i als agents encriptar missatges per prevenir que siguin analitzats per intrusos. De nou, el gestor i l'agent han de compartir una clau secreta configurada prèviament. L'algorisme d'encriptació utilitzat és el CBC (*Cipher block chaining*) de DES (*Data Encryption Standard*), conegut també per DES-56.

Algoritmes HMAC-MD5-96 i HMAC-SHA-96

Els algoritmes HMAC-MD5-96 i HMAC-SHA-96 són operacions matemàtiques que es realitzen sobre el conjunt de dades i la seva sortida representa una empremta digital singular. Si la destinació de la informació realitza el mateix còmput amb les mateixes dades pot comparar les petjades resultants i així validar la seva autenticitat.

DES (*Data Encryption Standard*)

DES és l'algoritme de xifrat per blocs que pren un text en clar d'una longitud fixa de bits i ho transforma mitjançant una sèrie d'operacions matemàtiques bàsiques en un altre text xifrat de la mateixa longitud, utilitzant una clau de xifrat coneguda per ambdues parts. D'aquesta forma s'aconsegueix mantenir la privadesa si es transmet el missatge codificat per la xarxa.

4.3.2. Model basat en vistes

Existeix un segon mecanisme que permet el filtrat condicional de parts de la MIB. Aquest model es denomina VACM (*Views-based access control model*) i permet proporcionar nivells d'accés a les MIB dels agents en funció dels diferents gestors en SNMPv3 o usuaris del sistema. Un agent pot restringir l'accés de certs gestors a part del contingut de la seva MIB o bé limitar les operacions susceptibles de realitzar per certs gestors sobre una part de la seva MIB.

Existeixen tres tipus de maneres d'accés (lectura, escriptura i notificació). Cada model del VACM té els següents atributs:

- Grup o nom de seguretat del model VACM.

- Nivell de seguretat en referència a l'autenticació i privadesa.
- Part de la MIB a la qual fa referència aquest grup.
- Permisos per al grup i MIB indicada anteriorment (lectura/escriptura/notificació).

5. RMON (*remote network monitoring*)

L'objectiu d'RMON és proporcionar informació a la plataforma de gestió dels diferents segments de xarxa però sense canviar el protocol SNMP. Per a fer-ho, podem considerar que dintre de la xarxa tindrem una sèrie de dispositius que seran capaços de monitoritzar la informació, analitzar-la i comunicar-se de forma adequada amb el gestor. Això, d'entrada, evita la necessitat de conèixer el trànsit d'entrada i sortida de cadascun dels dispositius, la qual cosa en la majoria de casos no és interessant.

Tradicionalment els equips que han analitzat el trànsit han estat els analitzadors de xarxa o en ocasions anomenats detectors (*sniffers*).

Actualment molts dels commutadors (*switchs*) de gamma mitjana i alta incorporen prestacions RMON.

5.1. Objectius del disseny d'RMON

Els objectius del disseny d'RMON estan especificats en l'RFC 1757 i són bàsicament els següents:

- **Limitar el sondeig (*polling*) permetent fer operacions fora de línia**. Aconseguim millorar el rendiment, continuar recollint informació del segment en cas que caigui la línia entre gestor i monitor, i quan aquesta es recupera enviar la informació.

- **Monitoratge proactiu**. Si el monitor té prou recursos és interessant que pugui treure diagnosis i informes de rendiment de la xarxa.

- **Detecció de problemes i tramesa d'informes (*reports*)**.

- **Possibilitat de diàleg amb més d'un mànager**. Això millora la fiabilitat.

- **Anàlisi del trànsit recollit.**

5.2. Control de la sonda RMON

El dispositiu que suporta RMON s'anomena normalment sonda RMON o simplement **sonda**.

La sonda RMON té alguna característica pròpia a l'hora de ser gestionada, ja que és capaç de fer feines més complexes que un agent amb MIB-2. Aquestes característiques estarien associades a la **configuració de la sonda** i a la **invocació d'accions**.

5.2.1. Configuració de la sonda

Una sonda necessita ser configurada per a recollir dades. En funció de la configuració que fem ens permetrà decidir el tipus i la forma de les dades recollides. La forma de fer-ho s'explica a continuació.

La MIB RMON està estructurada en grups com a MIB-2, però amb la particularitat que tots els grups estan formats per taules. Així per a cada grup hi ha **taules de control** i **taules de dades**. Les taules de control són taules de lectura/escriptura i contenen paràmetres que descriuen les dades. Les taules de dades són només de lectura. Si ho penseu té sentit que aquestes taules només siguin de lectura. El que fa l'estació de gestió és configurar els paràmetres de control apropiats perquè la sonda reculli les dades que interessen al gestor en cada moment.

Sembla lògic que la MIB tingui només taules, ja que el que fa és obtenir informació dels segments de xarxa.

Els paràmetres es posen incloent una nova fila o modificant una fila de la taula de control. Per tant, les funcions que ha d'efectuar una sonda estan definides i implementades en termes de files d'una taula.

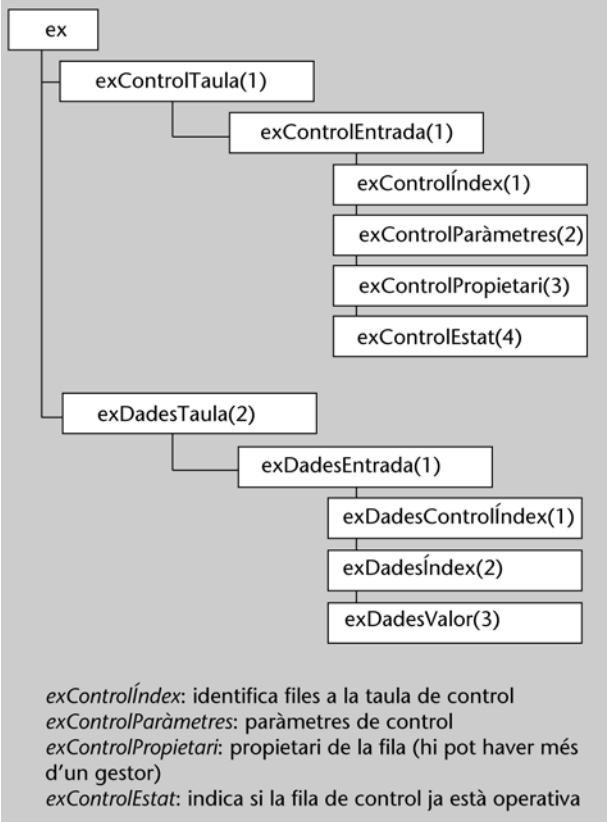
Per exemple, en la taula de control es poden indicar paràmetres com origen de les dades, tipus, temps entre captures, etc. Així l'índex en la taula de control serveix per a accedir a la taula de dades, i a l'inrevés.

La millor manera d'entendre el funcionament és mitjançant un exemple.

Exemple de configuració d'una sonda

Suposem el grup fictici *ex* (exemple) amb l'estructura que es mostra en la figura 17.

Figura 17. Representació d'un grup genèric seguint el format RMON



La taula de dades té dos índex, on *exDadesControlIndex* coincideix amb *exControlIndex*.

Així, una possible configuració de les taules es mostra en la figura 18.

Figura 18. Valors concrets d'una possible taula resultant

exControlÍndex	exControlParam	exControlPropiet	exControlEstat
1	5	gestor1	valid(1)
2	26	gestor2	valid(1)
3	19	gestor2	valid(1)

exDadesControlÍndex	exDadesÍndex	exDadesValor
1	1	25
2	1	34
2	2	45
2	3	12
3	1	11
3	2	19
3	3	23

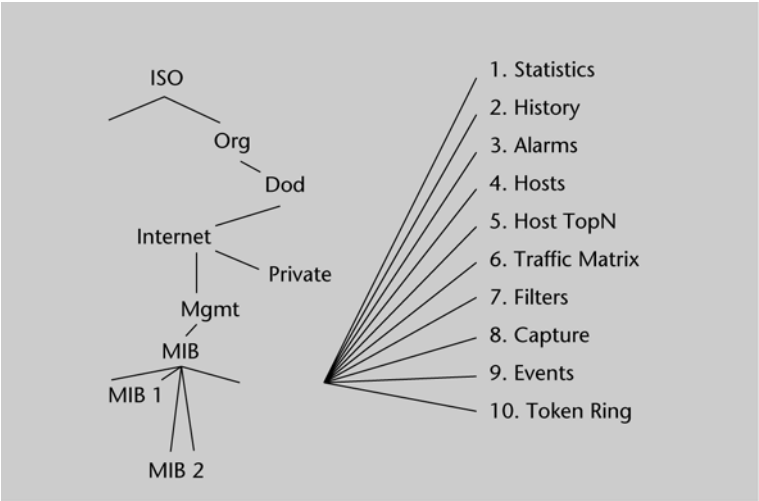
Cada filera de la taula de control crida unes taules que guarden els valors.

L'índex comú de les dues taules permet identificar les files de dades associades a un gestor concret creat en la taula de control.

5.3. RMON1 i RMON2

Inicialment RMON va ser desenvolupat per a xarxes LAN Ethernet i Token Ring de manera que divideix les funcions de monitoratge en nou grups associats a topologies Ethernet i un grup deu per a Token Ring. En la figura 19, es veuen els deu grups que formen part de la branca MIB.

Figura 19. Grups RMON1 dintre de l'estructura MIB



L'estàndard RMON està acceptat extensament per les empreses de *networking* i comunicacions.

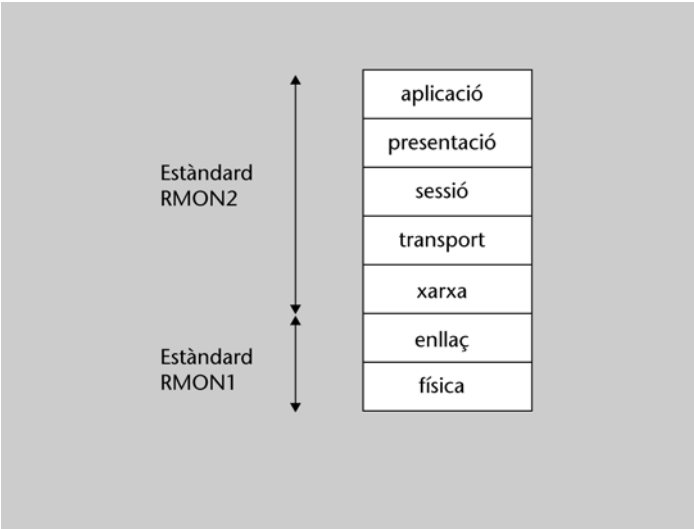
Una limitació important d'RMON1 és que especifica només monitoratge i diagnòstic de trànsit de xarxa a nivell de capa d'enllaç i no fa el monitoratge de trànsit a nivell d'aplicacions extrem a extrem.

Com a conseqüència d'aquesta limitació ens trobem que RMON1 no pot identificar dispositius que estiguin fora de la seva subxarxa, és a dir, darrere de l'encaminador.

Penseu atentament en el que això implica.

RMON2 respon a la necessitat d'analitzar el trànsit de les capes superiors. Es pot considerar una extensió d'RMON1 i són tecnologies complementàries com es pot veure en la figura 20.

Figura 20. Capes OSI on aplica cadascun dels protocols RMON1 i RMON2



En la taula següent podem veure com es complementen ambdós estàndards per a cobrir els diferents temes de monitoratge de xarxa.

Aspectes de la gestió	Nivell OSI	Estàndard RMON
Utilització i errors físics	Control d'accés al medi	RMON1
Segmentació LAN	Enllaç	RMON1
Interconnexió de xarxes	*Network*	RMON2
Ús d'aplicació	Aplicació	RMON2

5.3.1. La MIB RMON

Com s'ha dit, la MIB RMON està dividida en deu grups. En la taula següent es mostra una descripció de cadascun dels grups.

Grup	Descripció
Statistics	Manté estadístiques d'utilització i errors dels nivells baixos per a cada subxarxa monitoritzada.
History	Guarda mostres d'estadístiques de forma periòdica. Les extreu del grup *statistics.*
Alarm	Permet al gestor configurar intervals de mostratge i llindars d'alarma associats als valors obtinguts per la sonda.
Host	Conté comptadors de diversos tipus de trànsit dels *hosts* de la subxarxa.
hostTopN	Conté estadístiques dels *hosts* ordenades.
Matrix	Ensenya informació d'errors i utilització en forma de matriu.
Filter	Permet veure certs paquets a partir d'un filtre concret.
Capture	Controla com s'envien les dades a la consola de gestió.
Event	Dóna una taula amb els esdeveniments generats en la sonda.
TokenRing	Manté estadístiques i informació de configuració per a les subxarxes Token Ring.

A la vegada, els grups RMON els podem agrupar en funció de la tasca que fan. Podem trobar dos grups de tasques bàsiques:

- Estadístiques de trànsit
- Alarmes, filtres i captura de paquets

Alarmes, filtres i captura de paquets

Encara que dintre del grup d'alarmes, filtres i captura de paquets hi ha tres tasques, veurem que depenen unes de les altres pel seu correcte funcionament.

Tots els grups són opcionals en la seva implementació, però hi ha dependències entre alguns d'ells. Així, les dependències principals són les següents:

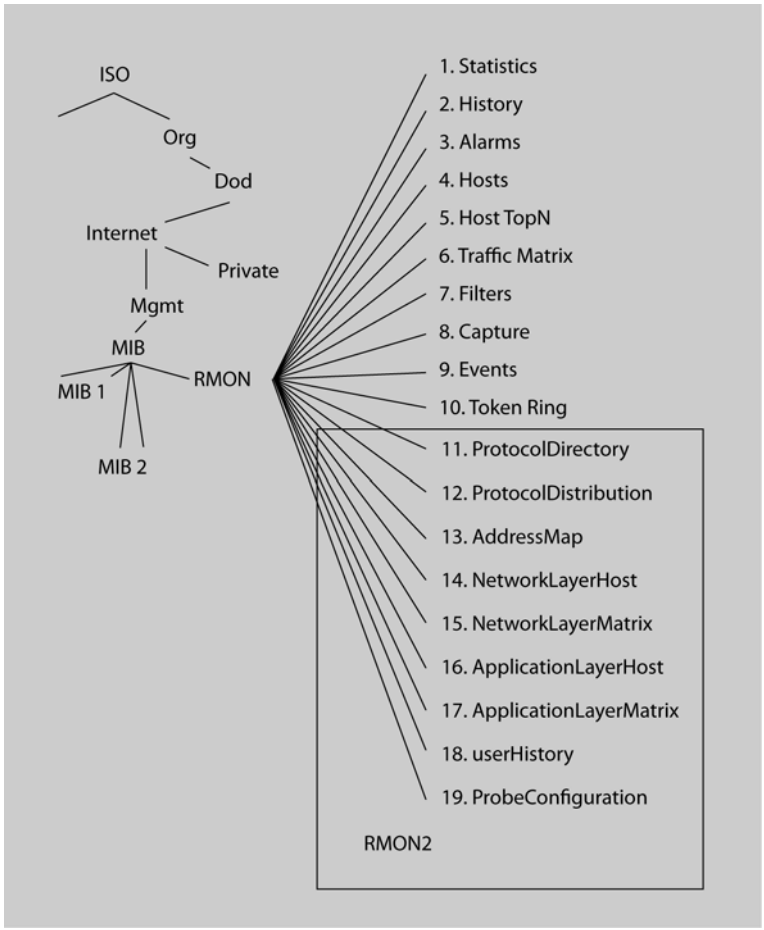
- El grup *alarm* requereix la implementació del grup *event*.
- El grup *hostTopN* requereix la implementació del grup *host*.
- El grup *capture* requereix la implementació del grup *filter*.

5.3.2. RMON2

Com hem dit anteriorment **RMON2** descodifica paquets de **nivell 3 a 7** de la pila OSI. Això vol dir que pot fer **monitoratge de trànsit a nivell IP** i, per tant, no està limitat a un segment Ethernet com passava en RMON1. Podem saber cap on va el trànsit que va cap a fora de la pròpia subxarxa i el mateix succeeix amb el trànsit entrant. Fins ara aquest trànsit a nivell 2 sempre tenia l'adreça MAC de l'encaminador per defecte. El mateix passarà amb la descodificació a nivell d'aplicació. Podrem saber cap a quina aplicació es genera el trànsit de cadascuna de les subxarxes.

Tal com es pot veure en la figura 21, la MIB RMON2 és una extensió de la MIB RMON.

Figura 21. Grups RMON2 dintre de l'estructura MIB



Altres característiques d'RMON2

Les noves característiques d'RMON2 estan associades a la forma d'**indexar de les taules**. Un gestor el que fa és sol·licitar la informació de les sondes de forma periòdica amb l'inconvenient quant a eficiència que implica el fet que cada cop retorna els nous valors a més dels antics. El que incorpora RMON2 és un índex temporal que permet enviar només el valors dels objectes que han canviat des de l'última petició a la sonda RMON.

RMON2 no envia tantes dades i per tant fa un ús més eficient de l'amplada de banda.

6. Eines i protocols en la gestió de xarxes

Inicialment en la concepció de les comunicacions de les xarxes IP es va veure la necessitat de crear un protocol auxiliar per realitzar tasques de control i gestió de les comunicacions. En aquest sentit s'ha definit el protocol ICMP (*Internet control message protocol*) que a continuació passem a detallar i que constitueix un dels pilars de la senyalització de control a les xarxes IP.

6.1. Internet control message protocol (ICMP)

El protocol ICMP es tracta d'un protocol que realitza funcions de control i gestió de xarxes IP. L'ICMP està definit en l'RFC 792 i posteriorment actualitzat en els RFC 950, 4884, 6633, 6918. Aquest protocol pertany als inicis de la creació de la xarxa internet i la seva funció principal és proporcionar informació de control a la capa de transmissió IP.

Per definició el protocol IP no garanteix que un datagrama sigui lliurat o que es retorni un missatge de control en cas que detecti alguna anomalia. Dit això, existeix la possibilitat que alguns datagrames no siguin lliurats correctament a la seva destinació per problemes a la xarxa de comunicacions entre origen i destinació. Típicament, els missatges ICMP informen d'errors en el processament de datagrames.

Els missatges ICMP tenen un entramat de 8 bytes de capçalera seguit de dades variables. Aquests bytes es combinen formant una capçalera que constitueix la capçalera tipus dels missatges ICMP.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Tipus     |      Codi     |        Suma de Control        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             sense utilitzar                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Capçalera Internet + 64 bits de dades del datagrama original  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

En el camp *Tipus* es codifica la tipologia de transacció ICMP del datagrama en qüestió. Dins dels possibles codis de tipus trobem:

0 Echo Reply
3 Destination Unreachable
4 Source Quench
5 Redirect Message
8 Echo Request
11 Time Exceeded
12 Parameter Problem
13 Timestamp Request
14 Timestamp Reply

15 Information Request (No Longer Used)
16 Information Reply (No Longer Used)
17 Address Mask Request
18 Address Mask Reply

Existeixen més codis definits en l'RFC 792 però posteriorment en l'RFC 6918 s'han proposat per a la seva anul·lació degut a la seva falta d'ús.

El protocol ICMP és la base per a la implementació de la coneguda eina *ping* que permet la comprovació de la connectivitat entre dos extrems de xarxes IP. Mitjançant l'eina *ping* els sistemes operatius llancen un datagrama del tipus Echo Request (codi 8) cap a la destinació. Si tot ha funcionat correctament, i una vegada el receptor rep aquest paquet, retorna la resposta mitjançant un reply (0) a l'adreça IP que ha iniciat la transacció.

Figura 22. ICMP request

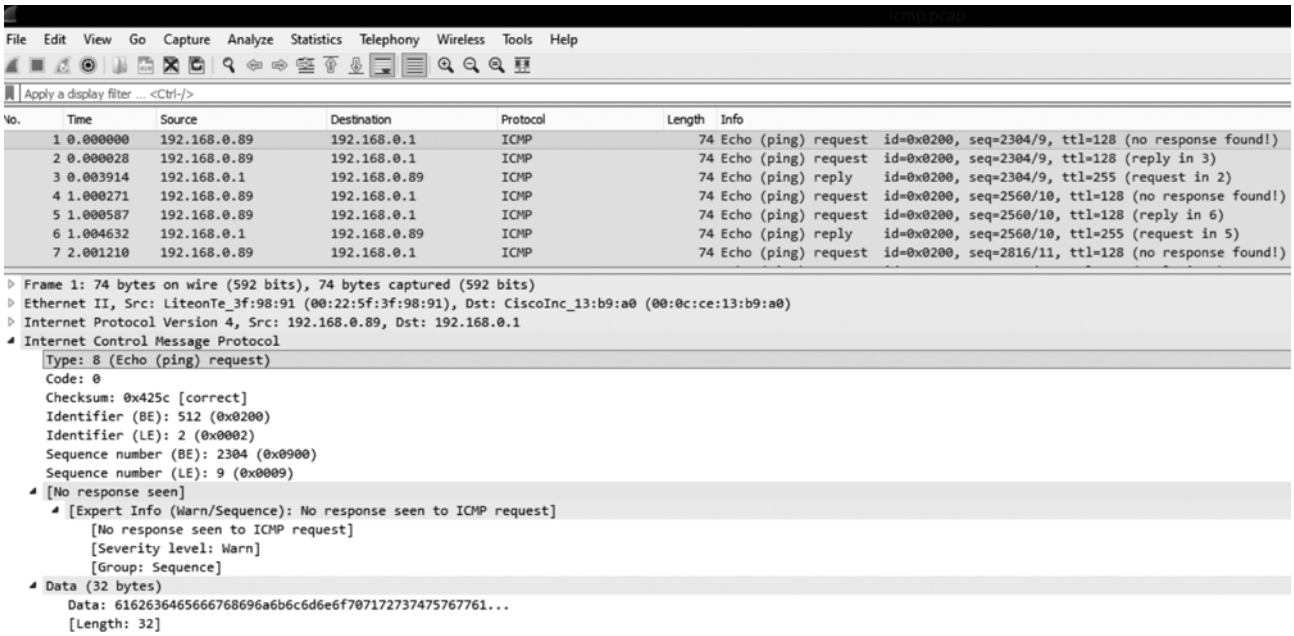
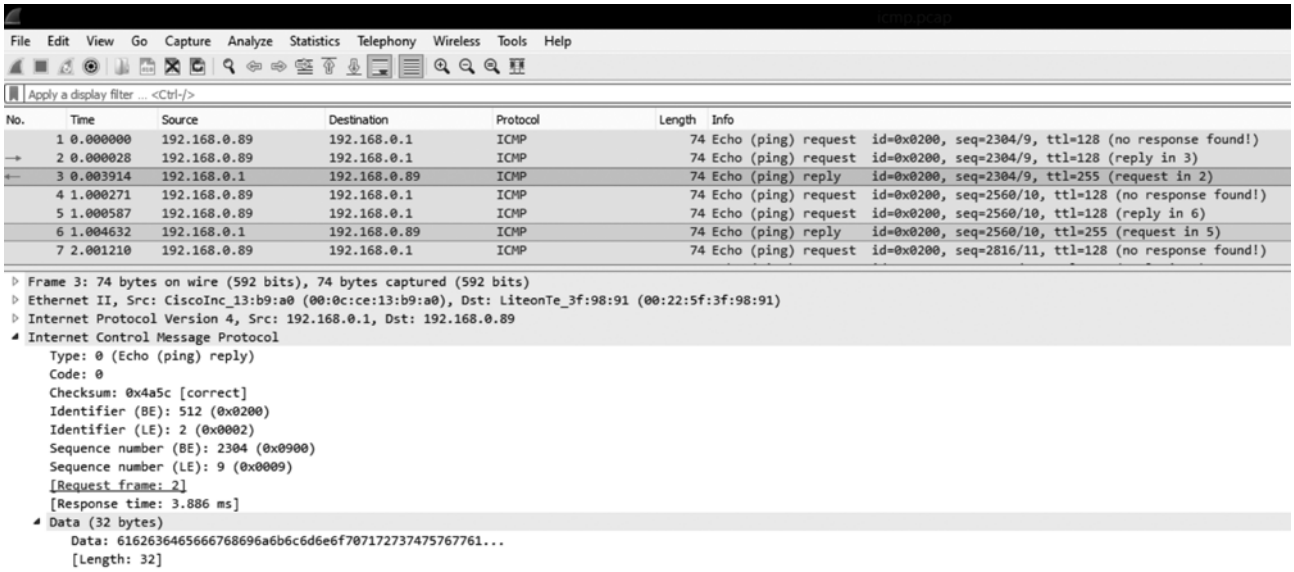


Figura 23. ICMP reply



Com podem observar en la figura anterior, s'ha realitzat una petició tipus ICMP amb adreça IP origen: 192.168.0.89 fins l'adreça 192.168.0.1. Es poden observar els diferents camps del protocol ICMP tal com s'han definit prèviament.

Igualment veiem, en aquesta mateixa figura, que aquest paquet s'ha transportat sobre el protocol ICMP que viatja sobre la mateixa xarxa IP, sent el protocol ICMP un protocol amb senyalització dins de banda.

Per a major detall sobre la senyalització dins de banda es pot consultar el primer mòdul de l'assignatura.

A tall d'exemple podem observar diferents opcions de tornada de l'ordre *ping*, corresponent a diferents casuístiques.

Ping correcte

```
C:\Users\Manel>ping 192.168.1.1

Fent ping a 192.168.1.1 amb 32 bytes de dades:
Resposta des de 192.168.1.1: bytes=32 temps=20ms TTL=63
Resposta des de 192.168.1.1: bytes=32 temps=20ms TTL=63
Resposta des de 192.168.1.1: bytes=32 temps=19ms TTL=63

Estadístiques de ping per 192.168.1.1:
  Paquets: enviats = 3, rebuts = 3, perduts = 0
  (0% perduts),
Temps aproximats d'anada i tornada en milisegons:
  Mínim = 19ms, Màxim = 20ms, Mitjana = 19ms
```

En aquest primer exemple podem observar que el *ping* s'ha realitzat correctament amb els temps de retard correctes (tenen una variació de retard *jitter* molt baixa) entre origen i destinació. Igualment podem observar que el camí entre origen i destinació és constant al no variar el TTL, amb un valor de 63 salts o elements de xarxa intermedis.

Ping amb resposta en l'últim element d'encaminat

```
C C:\Users\Manel>ping 10.91.158.66

Fent ping a 10.91.158.66 amb 32 bytes de dades:
Resposta des de 172.25.53.245: Host de destinació inaccessible.
Resposta des de 172.25.53.245: Host de destinació inaccessible.
Resposta des de 172.25.53.245: Host de destinació inaccessible.
Resposta des de 172.25.53.245: Host de destinació inaccessible.

Estadístiques de ping per 10.91.158.66:
  Paquets: enviats = 4, rebuts = 4, perduts = 0
  (0% perduts)
```

Podem observar que el *ping* ha fallat però l'encaminador amb adreça IP 172.15.53.245 retorna un missatge de control cap a la font indicant en el missatge que el *host* de destinació no està accessible. Típicament, això denota que el dispositiu de xarxa no posseeix la ruta per arribar a la destinació en el moment de l'execució del *ping*.

Ping sense resposta

```
C:\Users\Manel>ping 192.168.0.1

Fent ping a 192.168.0.1 amb 32 bytes de dades:
Temps d'espera esgotat per a aquesta sol·licitud.

Estadístiques de ping para 192.168.0.1:
Paquets: enviats = 1, rebuts = 0, perduts = 1
  (100% perduts),
```

A diferència del missatge anterior, aquí no s'observa cap missatge de tornada i pot indicar que el *host* destinació està filtrant els missatges d'ICMP.

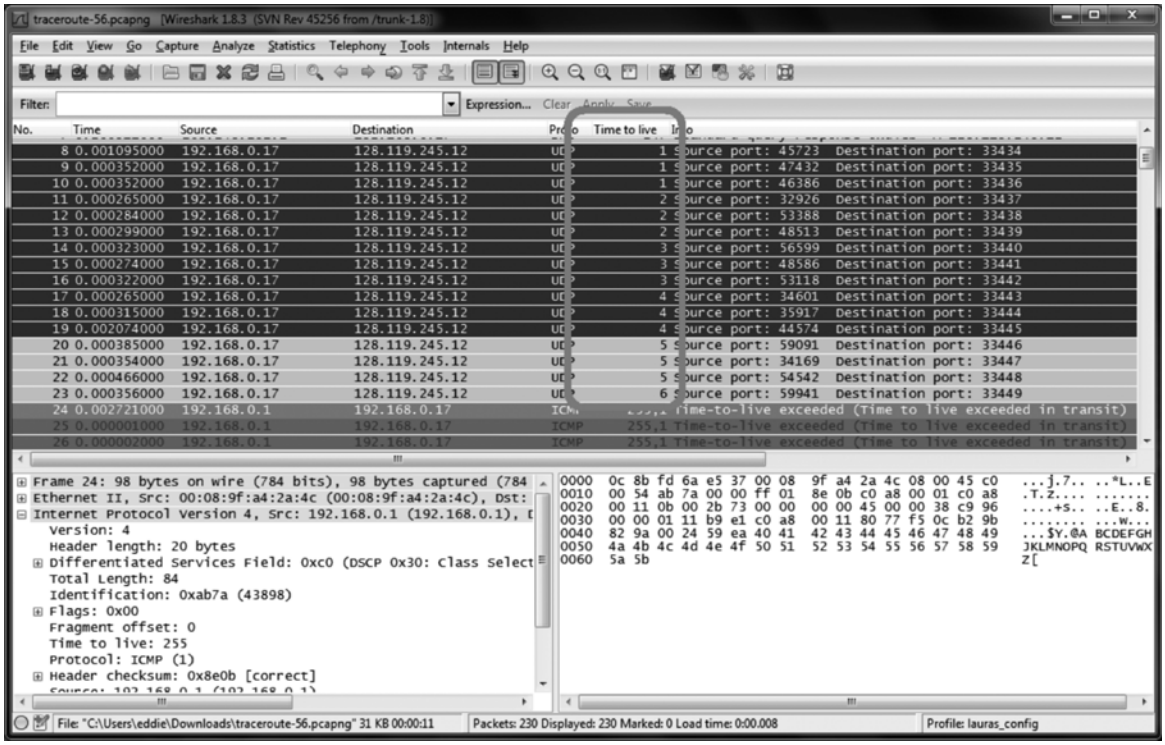
6.2. *Traceroute*

Una altra de les eines de gran utilitat en la gestió de xarxes i que està basada en missatges de control ICMP és el *traceroute*. Aquesta utilitat ens permet deduir els encaminadors de xarxa intermedis que existeixen entre una adreça o *host* origen i un *host* destinació. Aquesta eina existent en plataformes Windows i Unix és de gran utilitat per diagnosticar errors d'encaminat, proporcionant informació molt útil com el temps que pren cada enllaç entre encaminadors.

Per realitzar aquesta funció, la comanda *traceroute* realitza un enviament incremental de paquets IP incrementant el camp TTL de forma unitària, començant amb el TTL en 1 i acabant amb un valor de TTL igual al nombre màxim de salts fins a arribar al host destinació. Els encaminadors intermedis, després d'haver disminuït el TTL, i en el supòsit que el TTL sigui 0, descarta el paquet i envia a l'origen un paquet ICMP de tipus *Time Exceeded*. D'aquesta manera el host que executa el *traceroute* identifica les adreces IPs dels encaminadors intermedis i el temps en anar i tornar del paquet (RTT).

Després repeteix el procés incrementant en una unitat el TTL (TTL nou = TTL anterior +1) i així conèixer quin és el següent encaminador en la ruta cap al host destinació o a falta de destinació fins a un TTL màxim. D'aquesta manera mitjançant l'ordre *traceroute* es pot conèixer tots els encaminadors en el camí entre origen i destinació. Finalment, quan el paquet arriba a la destinació el host informa a l'origen la correcta recepció enviant un paquet ICMP de tipus *Echo Replay*.

En la següent figura es poden apreciar els enviaments de paquets IP/UDP amb els valors incrementals en el TTL i que provoquen els posteriors missatges d'ICMP de tornada.



Aquesta funcionalitat resulta molt útil per diagnosticar de forma clara els encaminadors o salts intermedis per on les trames IP s'estan encaminant.

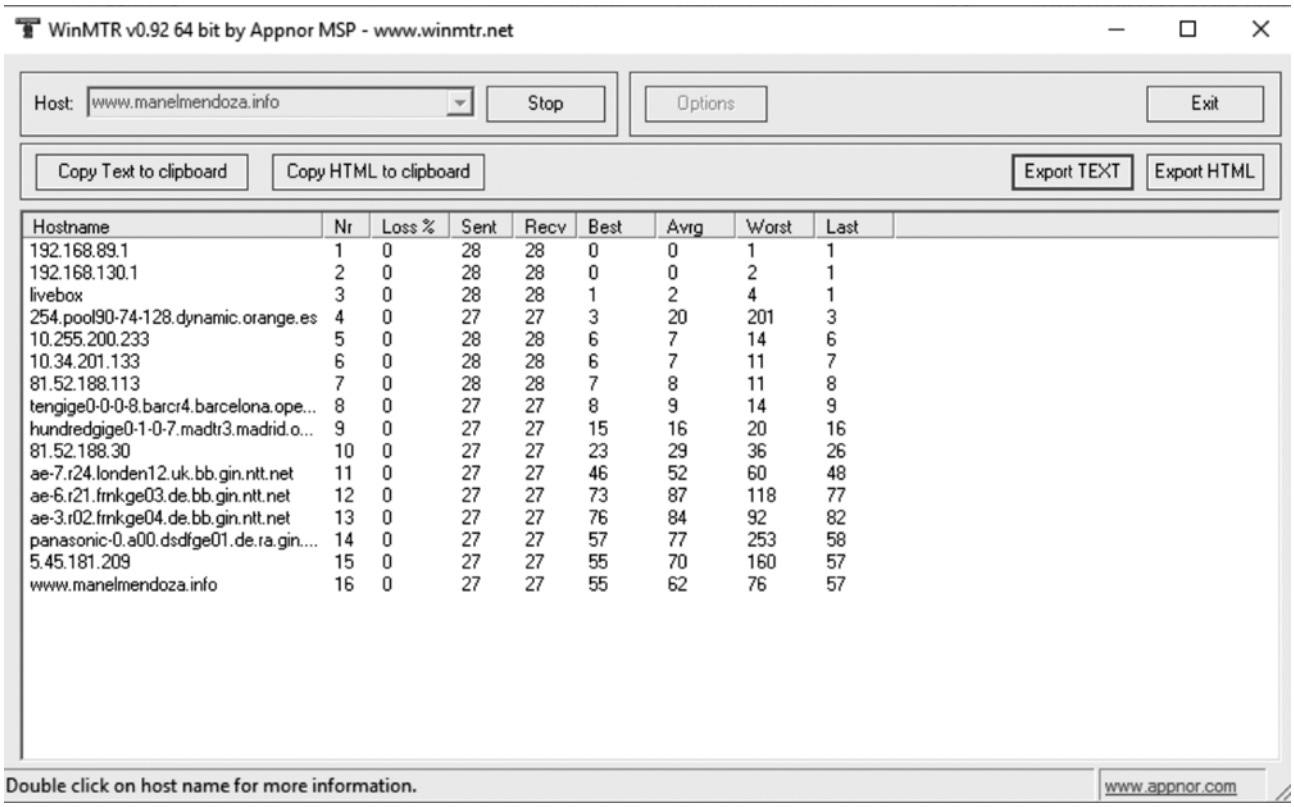
```
root@v01:~# traceroute www.lacaixa.es
traceroute to www.lacaixa.es (192.229.182.219), 30 hops max,
60 byte packets
 1 31.170.105.1 (31.170.105.1) 0.523 ms 0.483 ms 0.476 ms
 2 5.45.181.222 (5.45.181.222) 0.882 ms 0.950 ms 0.999 ms
 3 fa-0-0.a00.dsdfge01.de.ra.gin.ntt.net (213.198.77.65)
3.901 ms 4.047 ms 4.061 ms
 4 ae-4.r21.frnkge03.de.bb.gin.ntt.net (129.250.4.53) 3.873
ms 3.878 ms ae-3.r20.frnkge04.de.bb.gin.ntt.net
(129.250.3.93) 3.548 ms
 5 ae-3.r03.frnkge03.de.bb.gin.ntt.net (129.250.6.249) 4.452
ms 4.804 ms ae-2.r03.frnkge03.de.bb.gin.ntt.net
(129.250.6.217) 6.090 ms
 6 213.198.77.238 (213.198.77.238) 3.966 ms 4.000 ms 3.958 ms
 7 192.229.182.219 (192.229.182.219) 3.982 ms 3.959 ms 3.933
ms
root@v01:~#
```

En la figura anterior podem observar els camins i enllaços que s'utilitzen, al costat del retard de cada enllaç. Igualment, podem observar que al tercer enllaç (salt 3) existeixen gairebé 4 segons de retard pel que pot denotar un enllaç saturat o de baixa velocitat.

Aquesta eina pot ser de gran utilitat per a realitzar comparacions temporals i poder arribar a deduir possibles enllaços amb problemes. Aspectes com la variació dels temps (*jitter*) o temps elevats respecte a una línia base de retards poden denotar comportaments anòmals o sospitosos. A diferència de l'eina *ping* el *traceroute* permet segmentar la xarxa en salts i discriminar segment a segment per trobar els errors.

Existeixen multitud d'eines (*Pathping*, *mtr*, *winMtr*, etc.) que combinen les tècniques anteriors amb capacitat estadística obtenint dades estadístiques per a cada commutador de xarxa. A continuació, en la figura 24, es poden observar els retards, desviacions i millors temps per a la destinació fixada. Analitzant amb detall aquests paràmetres es pot procedir a la resolució d'anomalies a la xarxa.

Figura 24. Exemple de *traceroute* estadístic



Hostname	Nr	Loss %	Sent	Recv	Best	Avrg	Worst	Last
192.168.89.1	1	0	28	28	0	0	1	1
192.168.130.1	2	0	28	28	0	0	2	1
livebox	3	0	28	28	1	2	4	1
254.pool90-74-128.dynamic.orange.es	4	0	27	27	3	20	201	3
10.255.200.233	5	0	28	28	6	7	14	6
10.34.201.133	6	0	28	28	6	7	11	7
81.52.188.113	7	0	28	28	7	8	11	8
tengige0-0-0-8.barcr4.barcelona.ope...	8	0	27	27	8	9	14	9
hundredgige0-1-0-7.madtr3.madrid.o...	9	0	27	27	15	16	20	16
81.52.188.30	10	0	27	27	23	29	36	26
ae-7.r24.londen12.uk.bb.gin.ntt.net	11	0	27	27	46	52	60	48
ae-6.r21.frnkge03.de.bb.gin.ntt.net	12	0	27	27	73	87	118	77
ae-3.r02.frnkge04.de.bb.gin.ntt.net	13	0	27	27	76	84	92	82
panasonic-0.a00.dsdfge01.de.ra.gin....	14	0	27	27	57	77	253	58
5.45.181.209	15	0	27	27	55	70	160	57
www.manelmendoza.info	16	0	27	27	55	62	76	57

6.3. Analitzador de xarxes

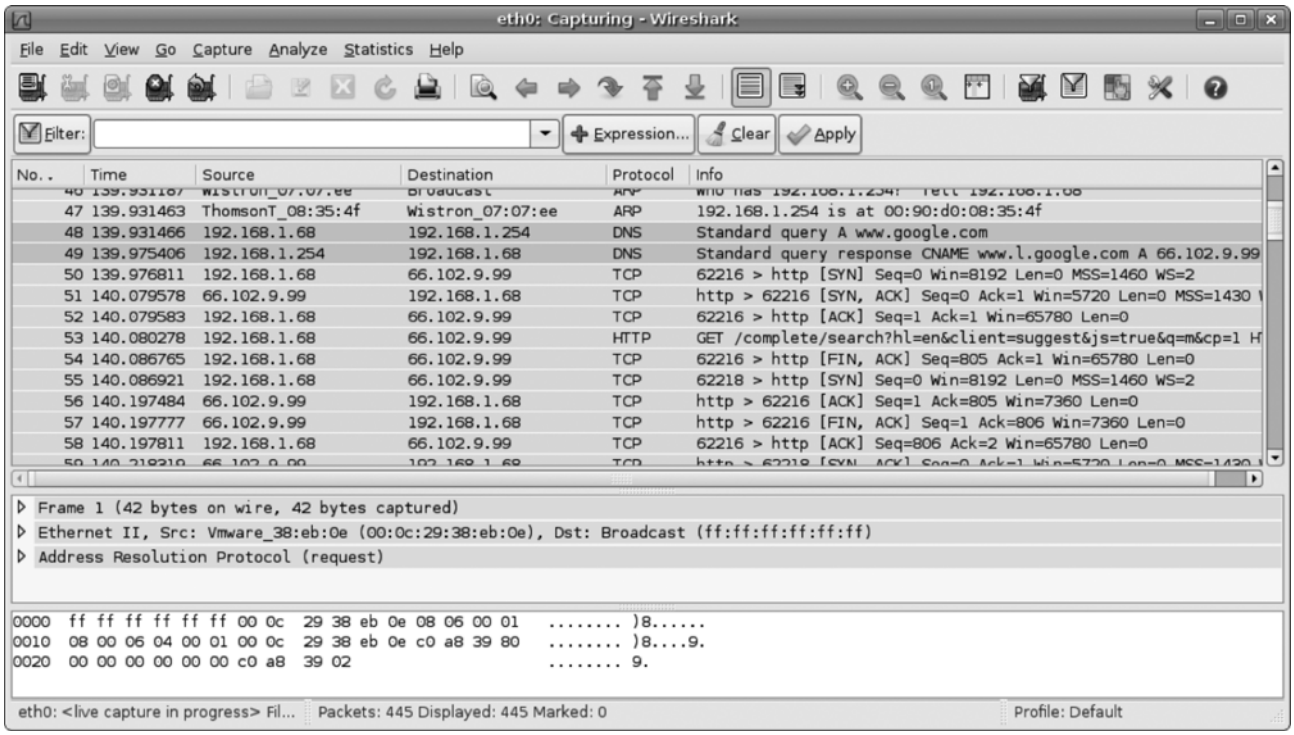
Unes altres de les eines i funcionalitats molt importants que tenim disponibles en les xarxes per a realitzar la gestió són les eines de captura de trames a baix nivell. Aquest tipus d'eines permeten capturar les trames que viatgen per la xarxa i comparar el comportament observat amb el funcionament dels protocols que estan definits en l'RFC. En aquest sentit existeix un programari *open source* per excel·lència anomenat *wireshark* que permet realitzar aquestes funcions.

Aquesta utilitat de gestió permet investigar successos o errors més complexos i especialment és possible realitzar les següents accions:

- Detecció de pèrdues de paquets. Això és possible gràcies a que els protocols posseeixen nombres de seqüència i es poden detectar les pèrdues dels mateixos.
- Detecció del diàleg entre emissor i receptor, estimant retards entre paquets, volumetries, etc.
- Possibles errors en la implementació dels protocols, gràcies el desentramat del propi programari.

Aquesta eina constitueix una de les formes més avançades i complexes de realitzar la gestió d'un problema en xarxes, però és la forma més eficaç de diagnòstic quan es vol analitzar amb detall algun comportament anòmal.

Figura 25. Exemple de l'eina de captura de paquets



No existeix una metodologia definida per a la gestió de problemes mitjançant aquesta eina però de forma genèrica podria aproximar-se amb els següents aspectes:

- Utilitzar tècniques comparatives de captures realitzades al moment d'anàlisi amb captures realitzades quan la xarxa estava en funcionament estable. Així es podrien detectar canvis de tendències o anomalies generals.

- Realitzar un escaneig general de la captura i identificar possibles anomalies en els protocols de control (ICMP, retransmissions de TCP, etc.).

- Analitzar de forma comparativa les comunicacions d'un flux que no funcioni correctament amb un altre que sí funcioni o que es tingui la captura guardada com a línia base.

- Realitzar comprovacions del funcionament estàndard del protocol amb la captura en l'analitzat de paquets i verificar la informació enviada en les trames.

6.4. Monitoratge de xarxes

Uns dels aspectes més crítics a l'hora de poder determinar el bon funcionament de les xarxes de comunicacions recau en el monitoratge actiu del seu funcionament i poder analitzar de forma empírica que els valors de rendiment dels elements que componen la xarxa estan dins dels valors esperat i per sota de les capacitats màximes del sistema.

Els paràmetres més habituals de monitoratge en xarxes s'han citat als apartats anteriors, però moltes de les eines habituals de monitoratge ja incorporen d'una bona base de plantilles per agilitzar el desplegament.

Entre les eines més habituals de monitoratge trobem multitud de programari lliure que ens permeten obtenir els paràmetres necessaris per obtenir una visió de l'estat de salut. Entre les més populars podem trobar (Nagios, Cacti, Zenoss). Si analitzem el seu funcionament totes tenen un funcionament similar:

- Mòduls encarregats de captar les dades i/o esdeveniments. Aquests mòduls estan basats en la seva majoria en SNMP, o en petits programes que realitzen comprovacions de forma periòdica.

- Base de dades que emmagatzema les dades anteriors i processa els valors anòmals, generant una alarma.

- Capa de representació de dades de forma visual, per poder ser interpretats de forma ràpida i clara.

- Mòdul d'alertes i avisos sobre la base dels paràmetres establerts.

Enllaços d'interès

Nagios:
https://www.nagios.org/
Cacti:
http://www.cacti.net/
Zenoss:
http://www.zenoss.org/

Amb les anteriors eines tindrem la base per a executar els procediments típics de diagnòstics de xarxes, que, tenen en compte les següents variables:

1) Relació d'esdeveniments que poden haver afectat la disponibilitat dels elements de comunicació (fallades elèctriques, cablejats, intervencions programades, etc.).

En aquest aspecte és molt important que els esdeveniments o la generació dels mateixos en el sistema tinguin en compte els següents aspectes:

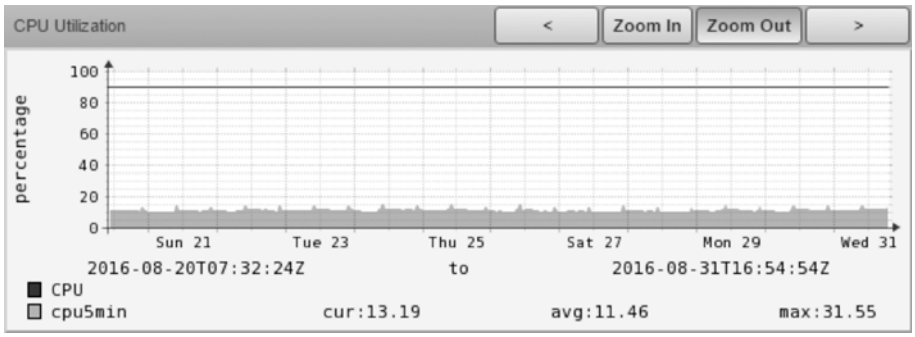
- Element o actiu que ha sofert l'esdeveniment
- Hora d'inici de l'esdeveniment
- Hora de finalització de l'esdeveniment
- Tipologia de l'esdeveniment i criticitat
- Acció correctora

A continuació, veiem un exemple en el qual es reflecteixen els esdeveniments de caiguda i de recuperació d'un element de xarxa. Es pot observar com s'utilitza l'eina Ping per monitoritzar la disponibilitat de l'element i reportar així la seva disponibilitat, indicant l'hora d'inici i fi.

Status	Severity	Component	Event Class	Summary	First Seen	Last Seen	Count
...	...						
			/Status/Ping	172.27.9.3 is DOWN!	2016-08-31 13:53:47	2016-08-31 13:53:47	1
			/Status/Ping	172.27.9.3 is UP!	2016-08-31 13:54:47	2016-08-31 13:54:47	1

2) Canvi en els paràmetres de funcionament de rendiment dels equips. Aquests indicadors són aspectes molt importants per diagnosticar anomalies a la xarxa i especialment el canvi d'aquests paràmetres pot indicar una situació anòmala. Entre els indicadors més importants tenim els valors de CPU, memòria i capacitat dels enllaços de l'equip.

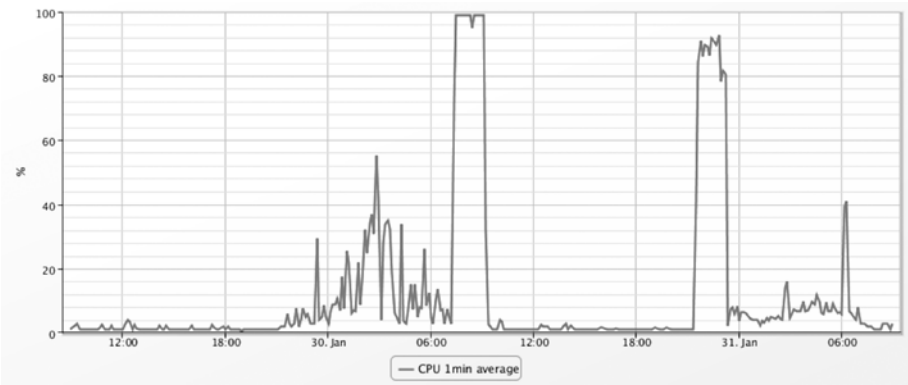
Figura 26. Exemple de CPU d'encaminador estable



En la figura anterior podem observar la gràfica de CPU d'un encaminador la qual es manté constant i no té pics de treball elevats. Igualment, es pot observar com la càrrega mitjana és d'un 11%, valor molt per sota del màxim i que garanteix un correcte funcionament del sistema. Aquests valors formen part de la línia base de modelatge de capacitat de la xarxa i són de vital importància per detectar accions anòmales, etc.

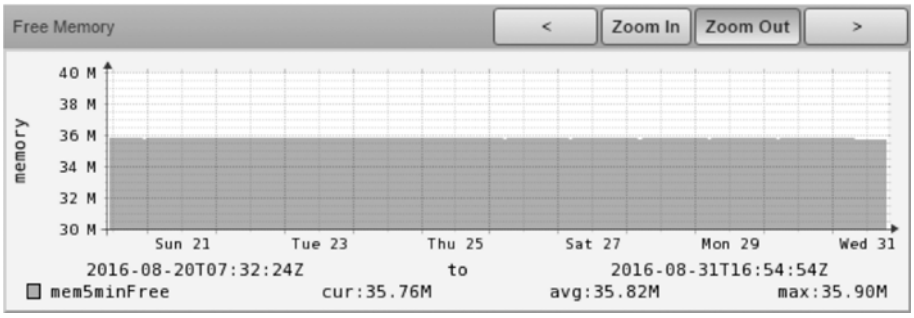
En l'exemple següent s'observa un comportament anòmal de CPU, arribant al 100% en una franja horària de 8:00 a 10:00 hores aproximadament. Aquests valors tan elevats poden comprometre l'estabilitat de la xarxa durant aquest període. Clarament, es pot comprovar com es tracta d'un procés puntual i asíncron, atès que el creixement de CPU té un pendent molt elevat i puntual.

Figura 27. Exemple d'esdeveniment anòmal en la CPU d'encaminador



De la mateixa manera, en el següent exemple, es pot observar el comportament de la memòria que és estable al llarg de les diverses setmanes. D'aquesta manera es pot comprovar que els valors són estables i que no s'aprecien canvis de càrrega en el sistema.

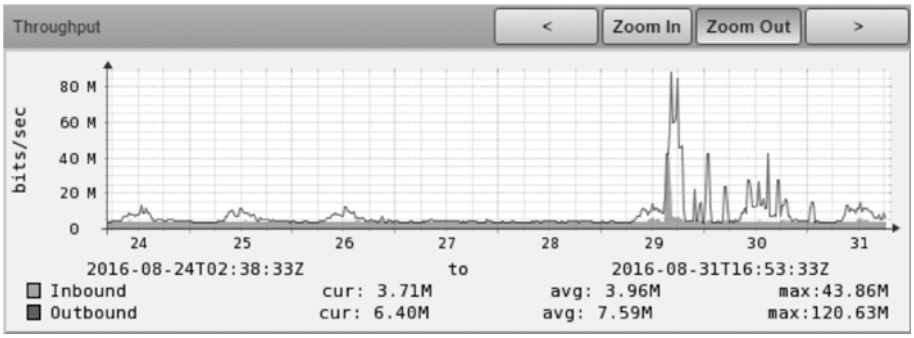
Figura 28. Exemple d'estabilitat de memòria



3) Canvis bruscs de tendències en el perfil de tràfic dels equips. Un altre dels aspectes crítics recau en el monitoratge de la capacitat dels enllaços per comprovar que no estan a la vora de la seva capacitat màxima i detectar patrons de comportaments anòmals.

A tall d'exemple, en la figura 29, podem apreciar un increment considerable de tràfic de l'enllaç sobre el dia 29. A partir d'aquestes dades es pot estimar si el tràfic de 80 Mbps està dins dels valors de disseny inicial o per contra representa un risc no planificat en termes de gestió de capacitat de xarxa.

Figura 29. Monitoratge d'ús d'interfícies de xarxa



7. Gestió TMN

Les operadores de telecomunicacions requereixen una infraestructura de gestió singular. Aquest entorn de gestió ha de preveure com a objectiu últim la prestació de servei de manera flexible i dinàmica. El model clàssic de gestió orienta les seves tasques cap a la xarxa, és a dir, configuració, manteniment i si és possible anàlisi de rendiment. La necessitat de les capacitats de gestió cap a la banda dels clients i els serveis ha provocat l'aparició de models de referència per a desenvolupar la gestió TMN.

Fa uns anys la indústria de les "telecos" usava solucions propietàries per a la gestió. Les operadores donaven nous serveis en funció de les seves possibilitats i per tant anaven millorant el seu sistema de gestió Actualment, amb la desregularització del sector l'increment de la competència i nous serveis les operadores s'han trobat que la gestió propietària no proporciona interoperabilitat entre les diverses tecnologies i les solucions de gestió que incorporen. Un altre aspecte que han de tenir en compte és la coexistència de les noves solucions amb sistemes "antics".

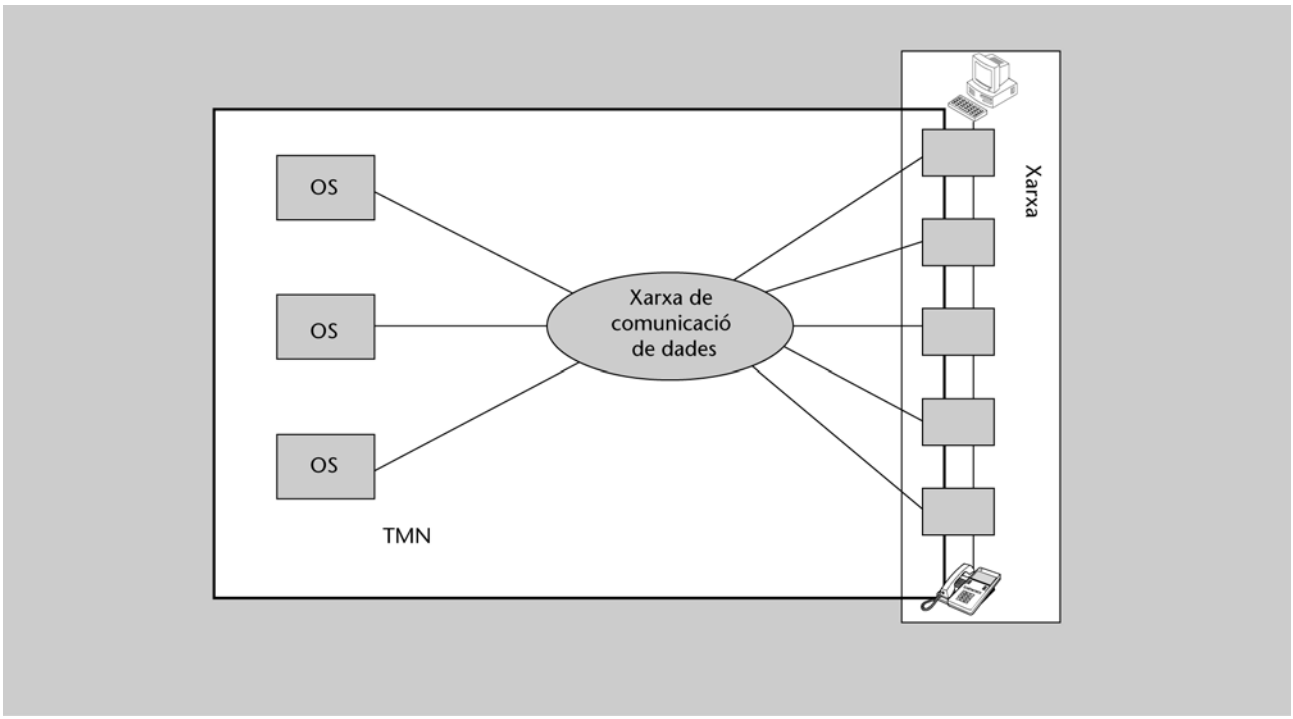
Així, com a resum podem dir que la motivació de l'arquitectura TMN ha estat, d'una banda, l'heterogeneïtat de les xarxes de telecomunicacions i, de l'altra, les demandes sobre aspectes com els següents:

- Possibilitat d'introduir nous serveis
- Alta qualitat dels serveis
- Possibilitat de reorganitzar les xarxes
- Mètodes eficients de treball per a operar les xarxes
- Competència entre operadores

Els principis del TMN (*telecomunications management networks*) es tracten en la recomanació M.3010 de la ITU-T, que **defineix un model d'operació per capes**: capes d'operació. Té una forta relació amb el model de gestió OSI.

L'**objectiu de TMN** és proporcionar una estructura de xarxa organitzada per aconseguir la interconnexió dels diversos tipus de sistemes d'operació i equips de telecomunicació usant una arquitectura estàndard i interfícies normalitzades.

Figura 30. Relació de TMN en una xarxa de telecomunicacions



A diferència del model OSI que definia cinc àrees funcionals, l'estàndard TMN no entra en consideracions sobre aplicacions de la informació gestionada. Per contra, es defineixen les funcions següents:

Podeu consultar les cinc àrees funcionals del model OSI en el subapartat 1.1.1 d'aquest mòdul.

- L'intercanvi d'informació entre la xarxa gestionada i la xarxa TMN
- L'intercanvi d'informació entre xarxes TMN
- La conversió de formats d'informació per un intercanvi consistent de la informació
- La transferència d'informació entre punts d'una TMN
- L'anàlisi de la informació de gestió i la capacitat d'actuar en funció seva
- La manipulació i presentació de la informació de gestió en un format útil per a l'usuari de la mateixa informació
- El control d'accés a la informació de gestió per part dels usuaris autoritzats

No oblideu que el significat de gestió de xarxa per TMN és més ampli que el que havíem considerat en el cas d'SNMP. En ambdós casos, gestió de xarxa significa gestió de xarxes i serveis, però en TMN està focalitzat en xarxes de telecomunicacions, equips i serveis proporcionats als clients.

Protocols que cobreix TMN

Alguns exemples de protocols o tecnologies que cobreix TMN serien: ATM, SDH, SONET o XDSL.

En la indústria de les telecomunicacions, els serveis i configuracions dels usuaris finals (clients) estan inclosos com a part de TMN. Així, apareixen dos termes nous, com són **servei** i **aprovisionament de recursos**.

TMN proporciona el suport de gestió per a la planificació, aprovisionament, instal·lació, manteniment, operació i administració de xarxes i serveis de telecomunicacions.

Una xarxa de telecomunicacions pot incloure una gran varietat de components, com són equips per a transmissió analògica, digital o sense fils (*wireless*), etc.

7.1. Arquitectura TMN

L'arquitectura TMN està dividida en tres blocs. La recomanació M.3010 defineix els blocs següents:

- **Arquitectura física**. Estructura i entitats de la xarxa: com s'implanten les funcions de gestió en els equips físics.
- **Arquitectura funcional**. Components i funcions de gestió.
- **Arquitectura de la informació**. Nivells de gestió: la gestió s'estructura segons responsabilitats.

Adreça recomanada

Podeu trobar un interessant *tutorial* sobre l'arquitectura TMN a http://www.simpleweb.org/tutorials/tmn/

7.1.1. Arquitectura funcional del TMN

L'arquitectura funcional TMN divideix el domini TMN en diferents blocs funcionals. Cada bloc funcional executa una funció específica de gestió. Els blocs són els següents:

- ***Operations system function*** **(OSF)**. Proporciona les funcions de planificació i gestió per a la xarxa de telecomunicacions i per als mateixos components.
- ***Network element function*** **(NEF)**. Monitoritzat i controlat per TMN.
- ***Workstation function*** **(WSF)**. Permet que l'usuari pugui veure la informació.
- ***Mediation function*** **(MF)**. Una mena de passarel·la per a l'intercanvi d'informació de gestió quan els blocs funcionals tenen diferents punts de referència.
- ***Q adaptor function*** **(QAF)**. Per a traslladar informació de gestió entre punts de referència TMN i no TMN.

Un element important que ha sortit referenciat i que encara no s'ha comentat són els punts de referència (*reference points*). Aquests punt són els límits conceptuals dels diferents blocs.

7.1.2. Arquitectura física del TMN

L'arquitectura física explica la implementació dels blocs funcionals en sistemes físics i la interfície entre ells. Els components de l'arquitectura física són:

- ***Operations sytem*** **(OS)**. És l'equivalent al gestor. Dóna suport per al processament d'informació relacionat amb operacions, administració, manteniment i aprovisionament de les xarxes de telecomunicacions.

- ***Data communications network*** **(DCN)**. Capacitat d'encaminament i transport per a l'intercanvi d'informació entre OS i OS, OS i NE, WS i OS, i WS i NE.

- ***Mediation device*** **(MD)**. Té funcions de retransmissió o passarel·la.

- ***Workstation*** **(WS)**. Punt d'entrada o sortida que permet als operadors del sistema accedir a les dades de gestió.

- ***Network element*** **(NE)**. El que coneixem per agent.

- ***Q adaptor*** **(QA)**. Converteix les dades no TMN en dades TMN, i viceversa.

7.1.3. Arquitectura d'informació del TMN

L'arquitectura d'informació explica com els sistemes de gestió OSI i els principis X.500 poden ser aplicats a TMN. L'arquitectura d'informació descriu els recursos que han de ser gestionats per TMN usant les guies de referència per a la definició dels objectes gestionats i la sintaxi ASN.1

Resum

En aquest mòdul didàctic s'ha intentat donar una breu visió del conceptes bàsics de la gestió de xarxa i el perquè de la seva necessitat en un entorn com l'actual. Per fer-ho, s'han explicat els conceptes generals de la gestió i posteriorment s'ha aprofundit en els protocols i metodologies més usades. En aquest sentit, la metodologia FCAPS és l'estàndard més acceptat per la indústria i que defineix àmpliament els processos per a una bona gestió de xarxa.

S'ha intentat separar el que és la gestió de xarxa, en el que hem anomenat xarxes Internet, del que són les xarxes de les operadores o xarxes de telecomunicacions.

Com s'ha vist, el protocol dominant en el món Internet és el protocol SNMP, juntament amb l'ICMP, el qual ha anat evolucionant per cobrir les diferents necessitats que han anat sortint. En aquest aspecte s'han analitzat diferents eines àmpliament utilitzades per al diagnòstic i gestió de xarxes com el *ping*, *traceroute* o *wireshark*.

Inicialment SNMPv1 era un protocol senzill que treballava de forma centralitzada amb el paradigma petició-resposta. Posteriorment, de la mateixa manera que les xarxes es fan més complexes, el protocol ha hagut d'evolucionar per solucionar altres aspectes no plantejats inicialment. Així SNMPv2 inclou mecanismes que permeten optimitzar la informació emmagatzemada en les taules dels diversos agents. Les diferents debilitats de l'SNMPv2 han provocat l'aparició d'una nova definició de l'estàndard en la seva versió 3 (SNMPv3), millorant els aspectes de seguretat d'aquest protocol. Igualment, s'han introduït i analitzat gràfics obtinguts a partir de monitorització SNMP i s'ha realitzat una breu interpretació.

Paral·lelament dintre de la MIB s'ha incorporat RMON, que com ja s'ha vist permet monitoritzar les xarxes sense haver de recorre a sol·licitar informació de cadascun dels dispositius via SNMP.

Finalment, per acabar el mòdul s'han vist les necessitats de les operadores de telecomunicacions i les possibilitats que els ofereix l'estàndard TMN per a cobrir les seves necessitats de gestió, que en la majoria de casos són bastant diferents de les necessitats de les xarxes convencionals.

Activitats

1. Descarregueu d'Internet l'RFC 1212 i l'RFC 1213 i familiaritzeu-vos amb la notació ASN.1 utilitzada per a definir les diferents MIB.

2. Realitzeu un *ping* en un dispositiu de la xarxa on us trobeu i intenteu determinar els valors obtinguts.

3. Amb l'ajuda d'MG SOFT MIB Browser intenteu determinar els diferents objectes de la MIB-II. Podeu trobar una versió d'avaluació d'aquest programa a http://www.mg-soft.com

4. Penseu el motiu pel qual hi ha taules SNMP que necessiten més d'un índex.

5. Esbrineu quines són les plataformes de gestió de dos fabricants com poden ser HP i Cisco.

6. Raoneu per quin motiu es va optar per treballar amb UDP i no TCP en gestió SNMP.

Exercicis d'autoavaluació

1. Tenim les peticions del grup *rs232* següents:

GetNext rs232.rs232Number.0
Response: rs232.rs232InSigTable.rs232InSigEntry.rs232InSigPortIndex.1.1 = 1

Getnext rs232.rs232InSigTable.rs232InSigEntry.rs232InSigPortIndex.1.1
Response rs232.rs232InSigTable.rs232InSigEntry.rs232InSigPortIndex.2.2 = 2

Getnext rs232.rs232InSigTable.rs232InSigEntry.rs232InSigPortIndex.2.2
Response: rs232.rs232InSigTable.rs232InSigEntry.rs232InSigState.1.1 = 2

Getnext rs232.rs232InSigTable.rs232InSigEntry.rs232InSigState.1.1
Response rs232.rs232InSigTable.rs232InSigEntry.rs232InSigState.2.2 = 2

Getnext rs232.rs232InSigTable.rs232InSigEntry.rs232InSigState.2.2
Reponse rs232.rs232InSigTable.rs232InSigEntry.rs232InSigChanges.1.1 = 3

Getnext rs232.rs232InSigTable.rs232InSigEntry.rs232InSigChanges.1.1
Response Reponse rs232.rs232InSigTable.rs232InSigEntry.rs232InSigChanges.2.2 = 4

A partir de la informació donada per aquestes peticions us demanem el següent:

a) Forma de la taula (contingut de la taula).
b) Quins són els objectes índex?
c) Si fem un *GetNext* a partir de l'últim valor obtingut, quin objecte obtindrem?
d) Construïu l'arbre de l'objecte definit.

Nota: El nom del segon índex és rs232InSigIndex.

2. Cerqueu l'RFC 1213 on està definida la MIB-2 i a partir d'aquesta determineu l'arbre del grup UDP.

Solucionari

1.

a) En aquest exercici el que veiem és que es fa un *Getnext*. Es fa perquè volem accedir a una taula SNMP. Com s'ha explicat, per fer la petició cal saber el valor dels índex corresponents. Com això no és així, amb el *Getnext* la resposta ens dóna el primer valor de la taula i de forma indirecta els valors (contingut) dels índexs de la primera filera de la taula.

La primera resposta

Response: rs232.rs232InSigTable.rs232InSigEntry.rs232InSigPortIndex.1.1 = 1

Ens diu:

Primer valor de la taula *rs232InSifPortIndex = 1* i a més ens diu que la taula té dos índex amb valors 1 i 1.

A partir d'aquí els successius *Getnext* van recorrent tota la taula de la mateixa manera que es mostra en la figura 11. El resultat és el següent:

InSIgPortIndex	InSigState	InSigChanges	InSigIndex
1	2	3	1
2	2	4	2

b) Els objectes índex són *InSIgPortIndex* i *InSigIndex*.

c) S'obtindria el valor *d'InSigIndex* de la primera filera de la taula.

d)
```
rs232
    rs232InSigTable
        rs232InSigEntry
            rs232InSigPortIndex (1)
            rs232InSigState (2)
            rs232InSigChanges (3)
            rs232InSigIndex (4)
```

2. El grup UDP en l'RFC 1213 té la forma següent:

```
udpInDatagrams OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The total number of UDP datagrams delivered to
            UDP users."
    ::= { udp 1 }

udpNoPorts OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The total number of received UDP datagrams for
            which there was no application at the destination
            port."
    ::= { udp 2 }

udpInErrors OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The number of received UDP datagrams that could
            not be delivered for reasons other than the lack
            of an application at the destination port."
    ::= { udp 3 }
```

```
udpOutDatagrams OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The total number of UDP datagrams sent from this
            entity."
    ::= { udp 4 }

-- the UDP Listener table

-- The UDP listener table contains information about this
-- entity's UDP end-points on which a local application is
-- currently accepting datagrams.

udpTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF UdpEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
            "A table containing UDP listener information."
    ::= { udp 5 }

udpEntry OBJECT-TYPE
    SYNTAX  UdpEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
            "Information about a particular current UDP
            listener."
    INDEX   { udpLocalAddress, udpLocalPort }
    ::= { udpTable 1 }

UdpEntry ::=
    SEQUENCE {
        udpLocalAddress
            IpAddress,
        udpLocalPort
            INTEGER (0..65535)
    }

udpLocalAddress OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The local IP address for this UDP listener.  In
            the case of a UDP listener which is willing to
            accept datagrams for any IP interface associated
            with the node, the value 0.0.0.0 is used."
    ::= { udpEntry 1 }

udpLocalPort OBJECT-TYPE
    SYNTAX  INTEGER (0..65535)
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The local port number for this UDP listener."
    ::= { udpEntry 2 }
```

Si resseguim cadascun dels objectes d'aquest grup ens queda una estructura com la següent:

```
  udp
    udpInDatagrams (1)
    udpNoPorts (2)
    udpInErrors (3)
    udpOutDatagrams (4)
    udpTable (5)
        udpEntry (1)
            udpLocalAddress (1)
            udpLocalPort (2)
```

Glossari

agent *m* En SNMP, mòdul programari que executa les funcions de gestió de xarxa que li demana el gestor. Gestor i agent es comuniquen via SNMP.

abstract syntax notation one *m* Llenguatge formal usat per a definir sintaxi. En el cas d'SNMP, la notació ASN.1 s'usa per a definir els objectes i el format del protocol.
sigla **ASN.1**

ASN.1 *m* Vegeu ***abstract syntax notation one***.

comunitat *f* En el context SNMP, relació entre agent i un grup de gestors que defineix característiques de seguretat. El concepte de comunitat és local i es defineix en l'agent.

base de dades d'informació *f* En el context SNMP, contenidor de la informació dels objectes per gestionar de forma estructurada on cada variable representa un recurs.
sigla **MIB**

estació de gestió *f* Mòdul programari que executa aplicacions de gestió per al control i monitorització d'elements de xarxa.
sin. **gestor**

gestor *m*
sin. **estació de gestió**

instància d'un objecte *f* Instància específica d'un tipus d'objecte que està vinculat a un valor específic.

MIB *f* Vegeu ***base de dades d'informació***.

objecte *m* Variable que representa algun recurs o altres aspectes del dispositiu gestionat.

remote network monitoring *m* Especificació de monitorització per a analitzar i monitoritzar protocols de xarxa.
sigla **RMON**

RMON *m* Vegeu ***remote network monitoring***.

sonda *f* En el context RMON, dispositiu de monitorització remota.

simple network management protocol *m* Col·lecció d'especificacions per a la gestió de xarxa que inclou el protocol, la definició de l'estructura de dades i altres conceptes associats.
sigla **SNMP**

SNMP *m* Vegeu ***simple network management protocol***.

telecomunication management network *m* Conceptualment, xarxa separada que interactua amb la xarxa de telecomunicacions a través de diversos punts. El concepte de TMN està definit per la recomanació M.3010.
sigla **TMN**

TMN *m* Vegeu ***telecomunication management network***.

trap *m* Missatge enviat per l'agent cap a l'estació de gestió sense que l'hagi sol·licitat.

Bibliografia

Mauro, D.R.; Schmidt, K. J. (2001). *Essential SNMP*. Sebastopol (EUA): O'Really.

(Disponible a http://www.unix.org.ua/orelly/networking_2ndEd/snmp)

Stalling, W. (1998). *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*. Reading (Massachussets): Addisson-Wesley.

Subramanian, M. (2000). *Network Management: Principles and Practice*. Reading (Massachussets): Addison-Wesley.

Udupa, D. (1999). *TMN Telecomunications Management Network*. McGraw-Hill