

## Pràctica 3: Monitors de xarxa

---

### Infraestructura i Tecnologia de Xarxes

Daniel Morales (1391627)

Ramon Guimerà (1400214)

Laboratori - Grup B10

# Respostes:

## 2.3 Descobrir la xarxa:

1. Aneu a “Home” → “Details” → “Host Detail” i seleccioneu el node [www.uab.cat](http://www.uab.cat). En aquesta pagina podeu obtenir informació sobre l'estat del node, reconfigurar-lo, etc. . .

2. Seleccioneu “Traceroute to this host” i preneu nota dels routers que hi ha entre la vostra maquina i [www.uab.cat](http://www.uab.cat). Si no us apareix el nom de les màquines, podeu utilitzar la comanda ‘host’ per esbrinar-lo.

Es troben els routers següents amb els seus noms respectius utilitzant traceroute i host:

### Tracing Route To 158.109.95.225 ...

[Close This Window](#)

```
traceroute to 158.109.95.225 (158.109.95.225), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1)  0.421 ms  0.077 ms  0.064 ms
 2 158.109.79.65 (158.109.79.65)  0.276 ms  0.210 ms  0.183 ms
 3 158.109.64.1 (158.109.64.1)  2.913 ms  3.077 ms  3.413 ms
 4 158.109.1.1 (158.109.1.1)  0.838 ms  0.971 ms  1.100 ms
 5 158.109.95.225 (158.109.95.225)  0.997 ms  *  *
```

```
itx-b10@deic-dc18: /opt/vmware/nagiosxi2
File Edit View Search Terminal Tabs Help
itx-b10@deic-dc18: /opt/vmware/nagiosxi2$ host 192.168.1.1
Host 1.1.168.192.in-addr.arpa. not found: 3(NXDOMAIN)
itx-b10@deic-dc18: /opt/vmware/nagiosxi2$ host 158.109.79.65
65.79.109.158.in-addr.arpa domain name pointer triki-dc.uab.es.
itx-b10@deic-dc18: /opt/vmware/nagiosxi2$ host 158.109.64.1
1.64.109.158.in-addr.arpa domain name pointer etsesw-core.uab.es.
itx-b10@deic-dc18: /opt/vmware/nagiosxi2$ host 158.109.1.1
1.1.109.158.in-addr.arpa domain name pointer core-si-4001.uab.es.
itx-b10@deic-dc18: /opt/vmware/nagiosxi2$ host 158.109.95.225
225.95.109.158.in-addr.arpa domain name pointer www.uab.es.
225.95.109.158.in-addr.arpa domain name pointer www.uab.eu.
225.95.109.158.in-addr.arpa domain name pointer www.autonoma.cat.
225.95.109.158.in-addr.arpa domain name pointer www.autonoma.edu.
225.95.109.158.in-addr.arpa domain name pointer autonoma.cat.
225.95.109.158.in-addr.arpa domain name pointer autonoma.edu.
225.95.109.158.in-addr.arpa domain name pointer *.uab.eu.
225.95.109.158.in-addr.arpa domain name pointer *.autonoma.cat.
225.95.109.158.in-addr.arpa domain name pointer *.autonoma.edu.
225.95.109.158.in-addr.arpa domain name pointer uab.es.
225.95.109.158.in-addr.arpa domain name pointer uab.eu.
225.95.109.158.in-addr.arpa domain name pointer uab.cat.
itx-b10@deic-dc18: /opt/vmware/nagiosxi2$
```

3. Ara heu de repetir tots els passos de la secció anterior per cadascun dels elements que el 'traceroute' hagi trobat. Podeu realitzar aquest procés en paral·lel, posant en marxa més d'un 'discovery job' a la vegada.

- Poseu a cada node el seu nom. Podeu fer servir la comanda `host ip` per a esbrinar els noms que no conegueu.
- Quan arribeu al pas 6, seleccioneu qui és el 'Parent host' de cada node. Penseu que la informació que heu obtingut amb el 'traceroute' us pot servir per imaginar com es l'estructura jeràrquica de la xarxa. Si descobriu quin és el 'Parent host' d'un node després d'haver-lo configurat, podeu anar al "Host Detail" del node en qüestió i tornar-lo a configurar.
- Si aneu massa justos de temps, deixeu aquest pas per al final.

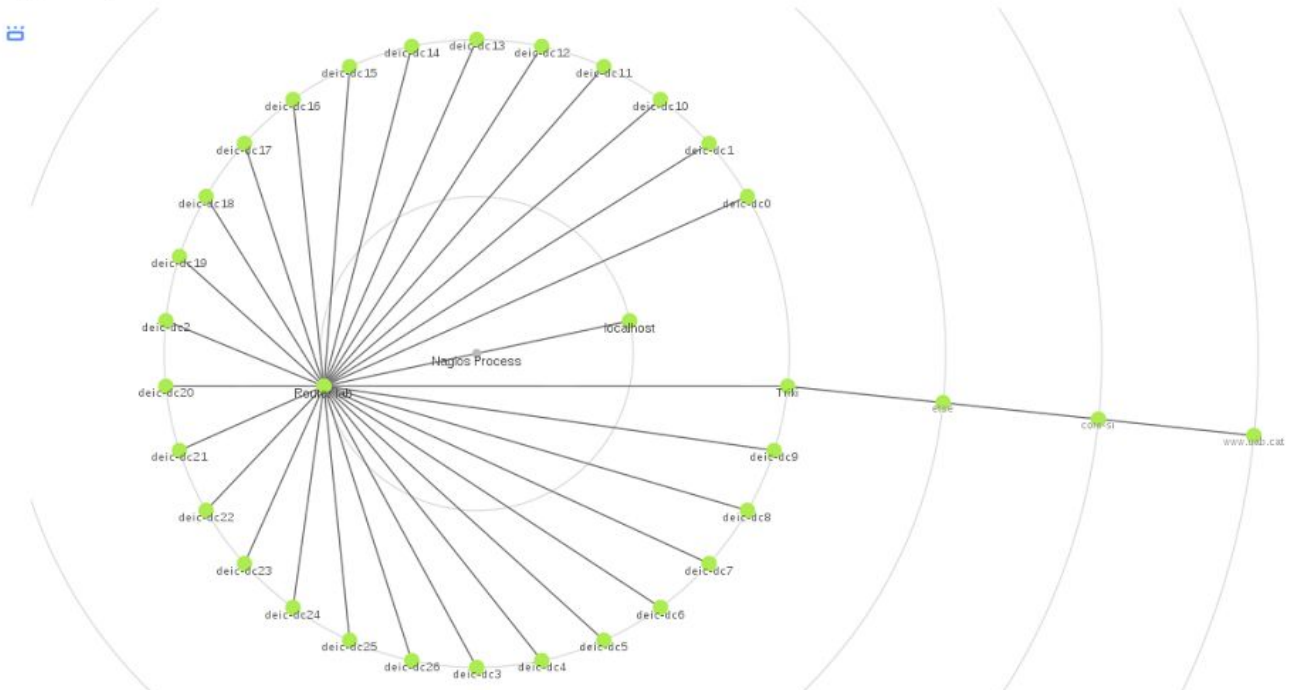
4. Aneu a "Configure" → "Advanced Configuration" → "Core Config Manager". Entreu amb l'usuari `nagiosadmin` i el password `welcome`. Aleshores aneu a "Monitoring" → "Host Groups" → "Add new" i creeu un nou grup de hosts anomenat `Laboratori-deic`.

5. Tornem al primer procés de descobriment, si ja ha acabat hauria d'haver trobat més d'un node, afegiu tots els nodes excepte el `158.109.79.65`.

Afegiu-los al hostgroup que heu creat al punt anterior. Anomeneu els nodes utilitzant la taula de l'enunciat.

6. (3 punts) Aneu a “Home” → “Maps” → “Hypermap”. Quan considereu que aquest s’ajusta a la realitat de la xarxa, preneu una captura de pantalla que adjuntareu a l’informe. Si creieu que hi ha alguna cosa malament, la podreu solucionar modificant els “parents” dels nodes afectats.

#### Hypermap



En el Hypermap generat, podem trobar en forma de cercle, totes les màquines del laboratori que van unides al Router-lab (punt central) a més a més del nostre localhost. Del router-lab, es va al router del deic Triki i d’allà al router de la ETSE. Quedan doncs només dos nodes més, core-si i www.uab.cat.

7. (1 punts) Expliqueu quin criteri heu utilitzat a l’hora de decidir els “parents” de cada node.

A l’hora d’utilitzar un criteri de decisió de parents, s’ha fet que a cada hop fet des de la màquina cap a [www.uab.cat](http://www.uab.cat) era un fill de l’anterior hop. És a dir, el router-lab té un fill, que és Triki.

8. Feu “Logout” al vostre navegador i utilitzeu “File” → “Power Off and Quit” per tancar la màquina virtual.

## 3.2 Informe d'activitat d'un node de la xarxa:

**1. Quan quedin 20 minuts, el professor escriurà a la pissarra una fórmula que haureu d'utilitzar per calcular X.**

Fòrmula entregada:  $X = 27 - \text{grup}$

El node monitoritzat en qüestió ha estat el deic-dc17.

**2. Dediqueu l'estona que queda a recollir informació sobre el node deic-dc17.uab.es.**

Es recull informació sobre el node durant la sessió de laboratori, a ser exactes, des de que es té el dashboard complert i se sap la resposta de la fórmula.

**3. Què ha succeït en aquest node durant la darrera hora. Podeu afegir gràfics, estadístiques, taules de notificacions, paràgrafs escrits, etc...**

Durant els aproximadament 20 minuts que s'ha analitzat el node deic-dc17, es pot veure que cada quatre minuts aproximadament passa per tres estats diferents.

Si es suposa que està en estat UP, on l'estat de la màquina és correcte, als pocs minuts passa a estar en estat DOWN, on no es pot accedir a la màquina des de la xarxa. Després d'aquest estat, sembla que la màquina es comença a recuperar i és accessible des de la xarxa, excepte els pings (UNREACHABLE).

Per últim, la màquina torna a entrar en estat UP, i de nou torna a començar el cicle.

Per aquest comportament, es pot deduir que la màquina es troba en estat de *flapping*[1], és a dir, que en un curt període de temps canvia molts cops el seu estat. Això es pot deure a una mala configuració, serveis problemàtics o problemes en la xarxa.

A continuació, es mostra una petita taula amb els estats obtinguts en certs moments.

Hora	Estat
14:39	DOWN
14:43	Host UP, ping critical (UNREACHABLE)
14:44	UP
14:46	DOWN
14:50	UNREACHABLE
14:52	UP
14:58	Tots els host tornen a estar UP

## Referències

[1]. Detection and handling of state flapping (online).

<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/flapping.html>