Infraestructura i Tecnologia de Xarxes
Curs 2016-2017

Pràctica 4: *Traffic Graphers*

Introducció

Els *traffic graphers* són unes eines molt específiques que serveixen per mesurar i monitoritzar la càrrega (quantitat de tràfic) que suporten els diferents elements d'una xarxa. Normalment no estan orientats a experts en l'administració de xarxa, per tant, presenten la informació de forma molt gràfica i no ofereixen tantes funcionalitats com els monitors de xarxa.

Aquest tipus d'eina és útil per descobrir pics (horaris, setmanals, mensuals, etc...) de càrrega en una xarxa, comprovar quins són els elements més crítics d'aquesta, saber quins elements són utilitzats al límit de les seves capacitats, etc...

1 Eina utilitzada

1.1 Traffic Graphers

Un *traffic grapher* s'instal·la sobre un node qualsevol de la xarxa i utilitza SNMP per obtenir informació d'altres dispositius. Aleshores utilitza aquesta informació per generar gràfics i els presenta a l'usuari de forma senzilla a través d'una pàgina web personalitzada. Per aquests motius, per funcionar necessita tant un servidor web (apache2, per exemple) com que els nodes a monitoritzar disposin d'un agent SNMP.

Les funcionalitats que un *traffic graphic* sól proporcionar són:

- Mesura els valors d'entrada i de sortida de cada objecte i calcula els valors màxim, mitjà i actual de càrrega.
- Obté dades a través d'un agent SNMP.
- Pot ser configurat per a recollir dades de forma periòdica.
- Crea una pàgina HTML per a cada objecte i mostra els diferents gràfics de càrrega.

1.2 SNMP

SNMP [3] és un protocol d'aplicació per administració de xarxes. SNMP està dissenyat perquè els administradors puguin supervisar el funcionament d'una xarxa, buscar i resoldre problemes i planificar el seu creixement.

El funcionament de SNMP es basa en l'agent SNMP. Un agent és un mòdul de software que resideix en el dispositiu administrat, l'agent disposa d'informació local, l'organitza de forma jeràrquica, l'emmagatzema en una MIB (Management Inforamtion Base) i la posa a disposició de l'administrador de la xarxa a través del port UDP 161.

2 Guió de la pràctica.

En aquesta sessió pràctica monitoritzareu en temps real la xarxa de la UAB, per fer-ho, utilitzarem Cricket [1]. Obriu el vostre navegador i accediu a `http://monitor.uab.es/monitor/`.
És molt important que a l'informe de la pràctica hi afegiu captures de pantalla amb els gràfics que justifiquen cadascuna de les vostres respostes.

2.1 Actius de xarxa i tràfic

1. **(0.5 punts)** Consulteu el mapa de la xarxa. Quins són els enllaços que estan més carregats? Consulteu les dades d'aquests enllaços i trobeu si hi ha alguna relació entre el dia de la setmana i el tràfic que circula a través d'aquests enllaços.

2. **(0.5 punts)** L'ús de tots els enllaços és simètric o hi ha alguns en els que hi ha molt més tràfic de pujada que de baixada (o a l'inrevés)? En quins casos es dona aquesta situació?

3. **(0.5 punts)** Al mapa hi ha dos elements que centralitzen les connexions en forma d'estrella. Compareu la quantitat de tràfic que suporten les línies que

hi ha entre cada facultat i l'element de l'esquerra amb el tràfic que suporten les línies que hi ha entre cada facultat i l'element de la dreta. Expliqueu les diferències i justifiqueu l'existència d'aquests dos elements.

4. **(0.5 punts)** Feu click a sobre de la línia que connecta "FTI" amb el router que dóna accés a Internet per accedir a la informació relativa a **gigabitethernet7_13**. En quins períodes de l'any el tràfic d'entrada és més gran que el de sortida? Veus alguna relació amb el calendari docent?

5. **(0.5 punts)** Entreu a "Monitorització dels actius de xarxa" → "Routers" → "Sabadell". Consulteu la informació relativa a la "Connexió Sabadell". En quina hora creieu que es realitza, diàriament, el procés de backup de les dades a un servidor extern? Justifiqueu la resposta.

2.2 Monitorització dels serveis d'usuari

1. **(0.75 punts)** Trobeu la informació referent als missatges d'spam, hi ha algun patró referent a la quantitat de missatges d'spam per dia de la setmana? Quin dels tres servidors de correu ha processat més missatges d'aquest tipus aquesta setmana?

2. **(1 punt)** Consulteu la informació relativa al servidor PaloAlto. Trobeu dos gràfics de mètriques diferents que siguin molt semblants. Expliqueu a què es deu aquesta correlació.

2.3 Monitorització de línies Anella

1. **(0.75 punts)** Consulta el tràfic d'entrada i sortida del Campus de Bellaterra. Quan va ser la última vegada que es va produïr un tall en el funcionament de la xarxa?

2. **(0.75 punts)** En general, el Campus de Bellaterra genera més tràfic d'entrada o de sortida? En algun moment succeeix a l'inrevés?

3. **(1 punt)** A quina època de l'any el Campus de Sabadell genera més tràfic d'entrada que de sortida? Quins són els dies de la setmana en que també succeeix això? (per tal de resoldre aquesta pregunta haureu de triar vosaltres mateixos les característiques del gràfic que voleu generar).

2.4 General

1. **(0.75 punts)** Trobeu la monitorització del router de la **unitat docent** de la Vall d'Hebron. Digues a quines hores comença i acaba la jornada laboral, justifica aquesta resposta. (**NOTA:** tot i que a l'enllaç de la pàgina principal a la informació sobre la Vall d'Hebron està restringit, hi ha una altra forma d'accedir a la informació **del seu router**).

2. **(0.75 punts)** Esmenteu 6 mètriques diferents que heu pogut monitoritzar a `http://monitor.uab.es/monitor/` (com a mínim dues d'aquestes mètriques **no han de ser de xarxa**).

3. **(1.75 punts)** Dibuixeu un diagrama de xarxa referent al procés de monitorització on apareguin com a mínim: 1) l'ordinador on esteu treballant, 2) el servidor de `http://monitor.uab.es/monitor/`, 3) un servidor de correu del qual esteu consultant l'ús de la seva CPU i 4) algun router si tots aquests elements no estan a la mateixa xarxa. Indiqueu en quins nodes resideixen: a) el client de Cricket, b) el dimoni de Cricket. Finalment, indiqueu també entre quins nodes hi ha tràfic: I) SNMP sobre UDP i II) HTTP sobre TCP.
NOTA: per simplicitat, podeu assumir que a la xarxa que esteu dibuixant hi ha un sol router.

3 TOP Enginyeria

Tots els alumnes que obtinguin més del 75% de la puntuació possible als dos apartats identificats amb la icona de TOP Enginyeria [2], obtindran el mèrit mitjà "Network Forensic", que reconeix el seu domini utilitzant *traphic graphers*.

4 Calendari i fites importants

A continuació es descriu el calendari de les fites relatives a la pràctica:

- **Sessió pràctica**: 20/03/17 i 23/03/17.
- **Entrega**: Un dia abans de la pròxima pràctica (26/03/17 i 29/03/17).

5 Condicions de lliurament

- L'entrega de la pràctica es farà a través del campus virtual.
- Cada grup ha d'entregar un informe en format pdf que contingui la resposta a totes les preguntes del guió de la pràctica, adjuntant captures de pantalla sempre que sigui necessari.
- No s'acceptarà cap informe lliurat fora de plaç.

Referències

[1] Terje Bless. Cricket Home. `http://cricket.sourceforge.net/`.

[2] Departament d'Enginyeria de la Informació i les Comunicacions. TOP Enginyeria. `http://top.uab.cat`.

[3] Wikipedia. Simple Network Management Protocol. `http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol`.