Departament de Llenguatges i Sistemes Informàtics
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Eina de monitorització de xarxes TCP / IP

Enginyeria en Informàtica

Autor: Iván Balañá Jiménez
Director: Ramon Sangüesa

28 de juny de 2007

Continguts

- ***Introducció***
- *Les xarxes actuals*
- *La llibreria libpcap*
- *Eina desenvolupada*
- *Proves realitzades*
- *Planificació*
- *Costos directes*
- *Anàlisi de desviacions*
- *Conclusions*
- *Línies futures*

Introducció: Ubicació del projecte

- Augment de l'ús d'Internet
  - Oci, negocis
- Augment de les xarxes connectades a Internet
  - Mòbils, empreses, universitats, xarxes sense fils als carrers
- Augment dels perills associats pels usuaris
  - Entorn més atractiu per hackers, spammers
- Necessitat d'exercir una sèrie de controls i auditories a les xarxes de dades IP
  - Racionalització dels recursos d'accés a la xarxa
  - Estimacions reals / estadístiques d'ús
  - Detecció de comportaments anòmals i problemes de seguretat

Introducció: Objectiu

- Estudiar i auditar xarxes IP de gran volum
- Presentar una arquitectura vàlida i viable per desenvolupar aquesta tasca
- Realitzar un prototip de la nostra arquitectura per tal de poder-la contrastar amb el món real

Introducció: Característiques principals

- L'eina ens permetrà
  - Conèixer i mesurar tràfic d'una LAN
  - Obtenir paràmetres de la LAN
  - Visualitzar possibles congestions
  - Preveure problemes
- Actuació passiva de l'eina
  - L'administrador obtindrà resultats sobre la Qualitat de Servei que podrem garantir
- Útil pels administradors de xarxa
- Basada en la llibreria *libpcap*

Introducció

- Anomenada *IPSS* (IP Surveillance Suite)
  http://gabriel.verdejo.alvarez.googlepages.com/ipss
- Desenvolupada amb i per a la comunitat de programari lliure
  - Alliberat amb llicència UPCFree / Creative Commons
- Multiplataforma. Funciona en:
  - Sistemes Linux
  - Sistemes BSD (FreeBSD, NetBSD i Mac OS X)
  - Sistemes Solaris

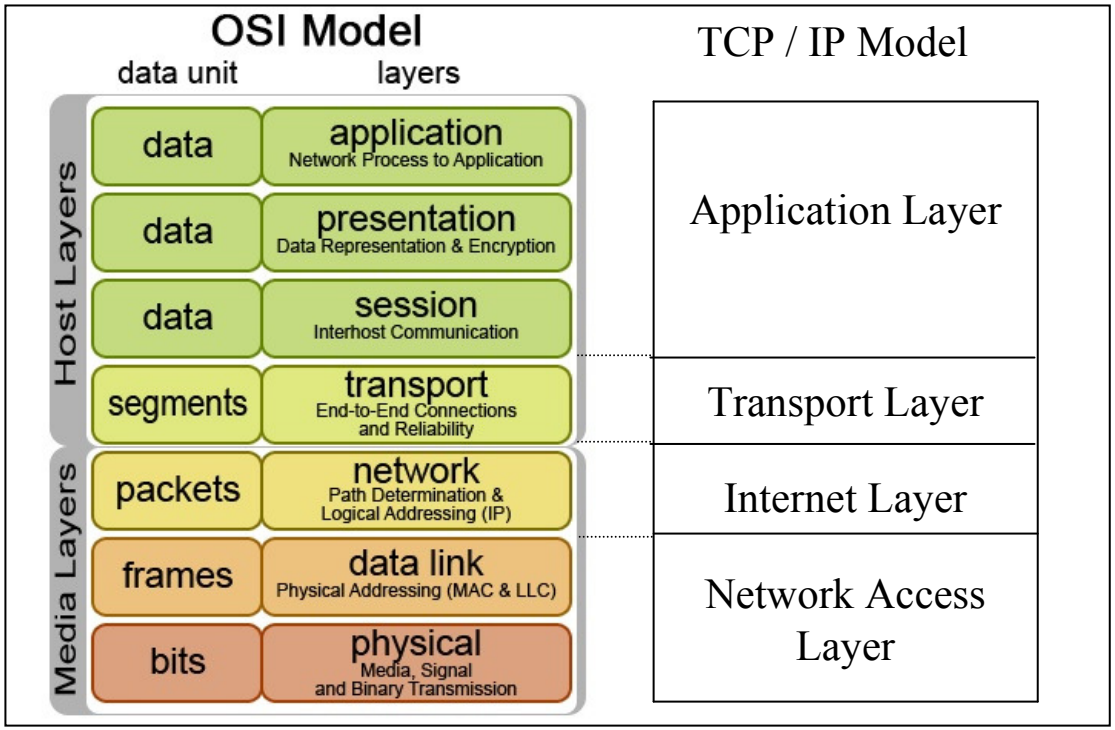
Continguts

- *Introducció*
- ***Les xarxes actuals***
- *La llibreria libpcap*
- *Eina desenvolupada*
- *Proves realitzades*
- *Planificació*
- *Costos directes*
- *Anàlisi de desviacions*
- *Conclusions*
- *Línies futures*

Les xarxes actuals: Estat de l'art

- Evolució constant de les xarxes físiques:
  - Més velocitat (ADSL, ADSL2, Myrinet)
  - Tipus de medi diferents (mòbils, PDAs, …)
- En canvi, hi ha hagut pocs canvis en els protocols de xarxa
  - Degut a l'estandardització realitzada per ISO/OSI per homogeneïtzar i posar ordre en tots els protocols
- El canvi més gran que es preveu pels propers anys (2010/2012) és el pas d'IPv4 a IPv6

Les xarxes actuals: Pila ISO/OSI



Les xarxes actuals: Protocols de transport

- Podem agrupar els protocols de transport en dos grans grups
  - Orientats a la connexió
    - Necessiten una fase d'establiment de la connexió
    - Garanteixen l'ordre de l'intercanvi de les dades
    - Garanteixen el reenviament de la informació en cas de pèrdua
    - Generalment, segueixen d'una fase de desconnexió
  - No orientats a la connexió
    - No presenten fases de connexió o desconnexió
    - No garanteixen per sí mateixos l'ordre en l'intercanvi de les dades ni el reenviament de la informació

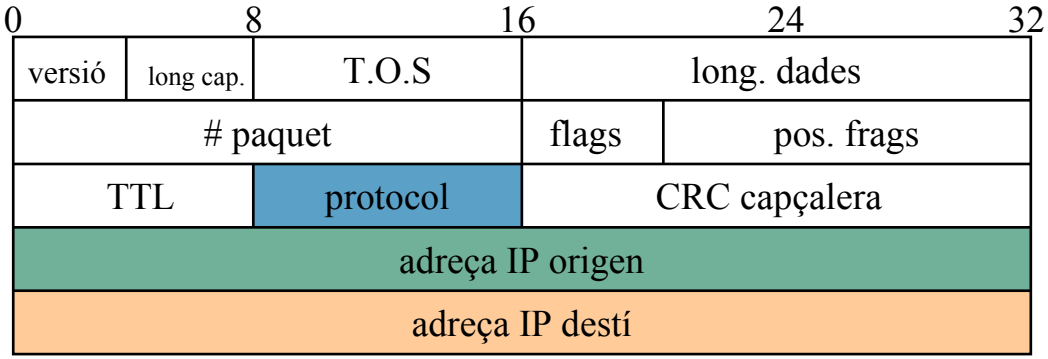
Les xarxes actuals: El protocol TCP

- Protocol orientat a la connexió
  - Reenviament de paquets en cas de pèrdua
  - Inici de connexió i finalització de la connexió marcats per sincronisme
    - *Three-way handshake* per l'inici de la connexió
    - *Four-way handshake* per la finalització de la connexió

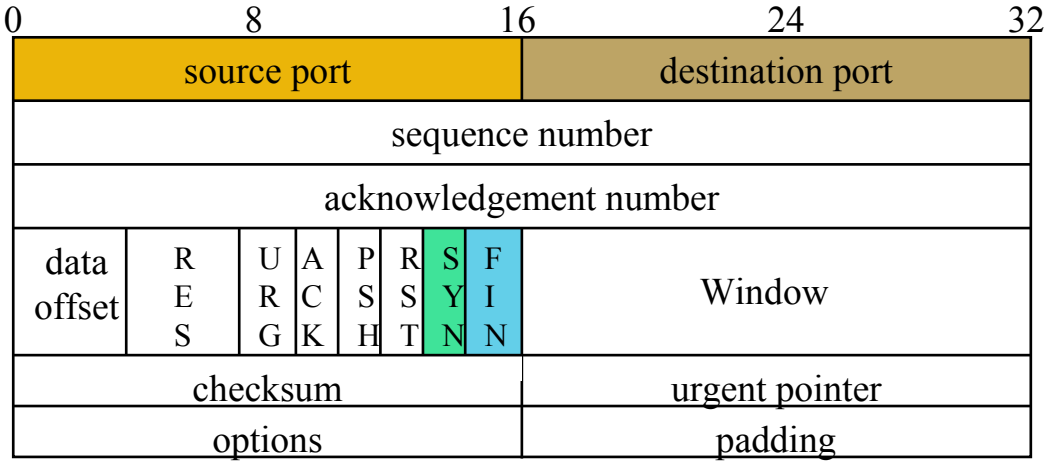
- La nostra eina seguirà aquests sincronismes de connexió i desconnexió per oferir informació més fidedigna de les connexions TCP capturades

Les xarxes actuals: Capçaleres TCP/UDP/IP

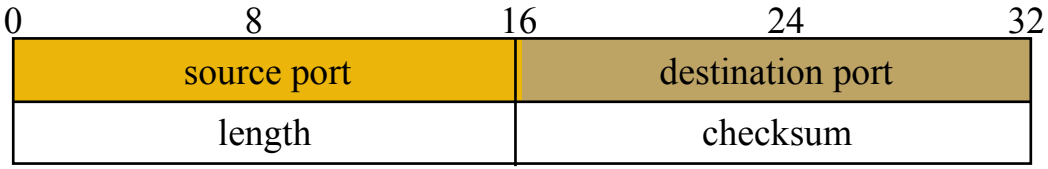
FORMAT DE LA CAPÇALERA IP



FORMAT DE LA CAPÇALERA TCP



FORMAT DE LA CAPÇALERA UDP

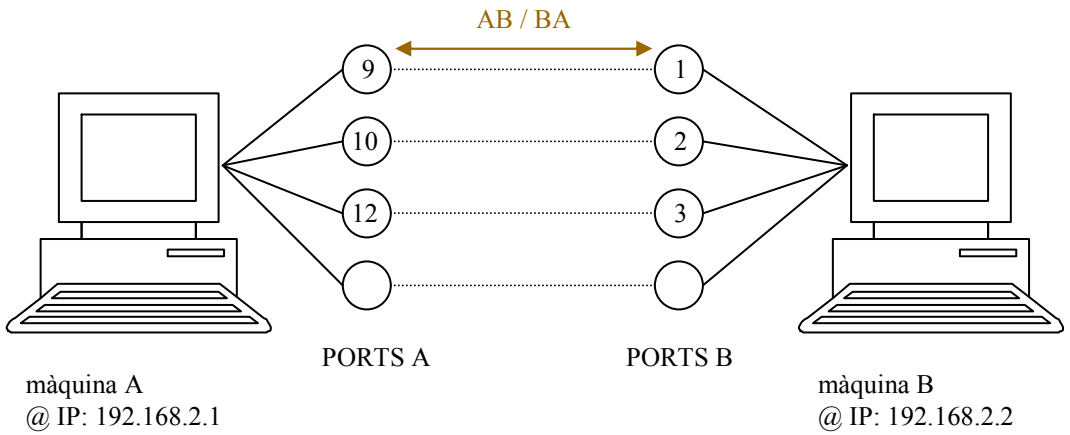


Les xarxes actuals: *Fluxos*

- Definirem un *flux* com un conjunt de paquets que s'intercanvien entre *dues màquines*, per un *mateix port origen* i *destí*, amb el *mateix protocol* i dintre d'una finestra de temps finita

- Tindrà sentit en protocols orientats a la connexió (com TCP) encara que també el farem servir per altres protocols com UDP

Les xarxes actuals: Exemple de *Flux*



La *màquina A* envia un paquet des del *port 9* a la *màquina B*, qui el rep pel *port 1*, fent servir el *protocol TCP*.

La *màquina B* contesta amb un paquet des del *port 1* a la *màquina A*, qui el rep pel *port 9*, fent servir el *protocol TCP*.

Aquest intercanvi d'informació pertany al mateix *flux*

Continguts

- *Introducció*
- *Les xarxes actuals*
- ***La llibreria libpcap***
- *Eina desenvolupada*
- *Proves realitzades*
- *Planificació*
- *Costos directes*
- *Anàlisi de desviacions*
- *Conclusions*
- *Línies futures*

La llibreria libpcap (1)

- Sorgeix per la necessitat d'uniformitzar i generalitzar els mètodes de captura de paquets existents en els diferents sistemes operatius
- Creada per l'equip de desenvolupament de l'eina *tcpdump*
- Suporta nombroses arquitectures
  - BSD
  - Linux
  - Solaris
  - AIX
  - Windows

La llibreria libpcap (2)

- Àmpliament reconeguda al món informàtic
  - TCPDUMP
  - Ethereal / Wireshark
  - Ntop
- Va superar satisfactòriament proves de rendiment, permetent la captura de més de 450Mbytes/s amb equipament hardware comú

La llibreria libpcap: Exemple d'aplicació

- En la nostra arquitectura, hem fet servir principalment, les següents crides:

```
pcap_open_live()                    Obre el dispositiu

pcap_loop(…, funcio,…)              Per a cada paquet rebut
                                    executa la funció indicada (thread)

                                    mentre no sortir fer
                                      esperar_paquet()
                                    fmentre

signal_sortir ()
{
      pcap_breakloop()              Avorta el bucle del pcap_loop
}
```

La llibreria libpcap

- La captura és un *procés crític*
- Minimització del temps d'execució de la funció de captura per tal de maximitzar-ne la captura de paquets
- Minimització de l'ús de recursos (RAM/CPU)
  - Trobar el punt entremig entre capturar tota la informació (consum de molta memòria) minimitzant l'ús del processador
  - Trobar el punt entremig entre compactar tota la informació (consum de molt processador) minimitzant l'ús de la memòria

Continguts

- *Introducció*
- *Les xarxes actuals*
- *La llibreria libpcap*
- ***Eina desenvolupada***
- *Proves realitzades*
- *Planificació*
- *Costos directes*
- *Anàlisi de desviacions*
- *Conclusions*
- *Línies futures*

Eina desenvolupada (1)

- Proposem un model de tres capes
  - Model que permet el desenvolupament de components independents
  - Model adaptatiu al hardware (*threads*)
  - Model incremental que permet preestablir una planificació i uns timings de desenvolupament
  - Model recolzat per nombrosa bibliografia

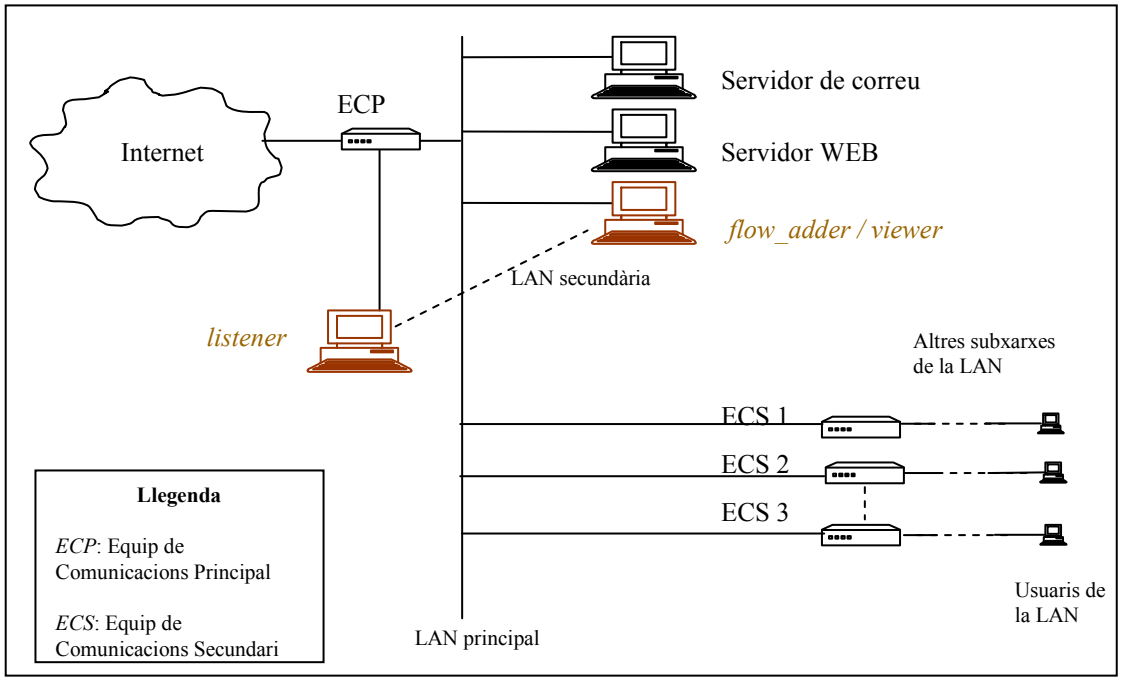
    [ROS06] [BAR03] i altres

Eina desenvolupada (2)

- Parts del model:
  - *Listener* : Guardarà la informació de la xarxa a disc
  - *Flow adder* : Agruparà els resultats obtinguts en el *listener*
  - *Viewer* : Generarà gràfiques i estadístiques per a la ràpida visualització dels resultats
- Aquesta divisió ens permet tenir una gran escalabilitat i alt rendiment especialment, en entorns amb molta càrrega

Eina desenvolupada (3)

- Un possible esquema d'implantació podria ser:



Eina desenvolupada: Altres productes (1)

- Exemples d'algunes solucions i productes amb un comportament similar:
  - Cisco netflow
    - Propietari de Cisco
    - Únicament funciona amb equips de xarxa fabricats per Cisco
    - No permet filtratges de les dades gaire complexos
  - Nprobe
    - Intenta eliminar el requisit hardware anterior (no cal equips Cisco per tal de poder monitoritzar)
    - No és un producte lliure ni tampoc gratuït
    - Té les mateixes limitacions que el Cisco netflow

Eina desenvolupada: Altres productes (2)

- IPAudit
  - Comportament molt similar al desitjat
  - Des del 2004 no ha aparegut cap nova versió, correcció o ampliació
  - Model no escalable

- Cap d'aquests productes acompleix amb tots els requisits que desitgem
  - Escalabilitat
  - Multiplataforma
  - Lliure i gratuït

Eina desenvolupada: *listener* (1)

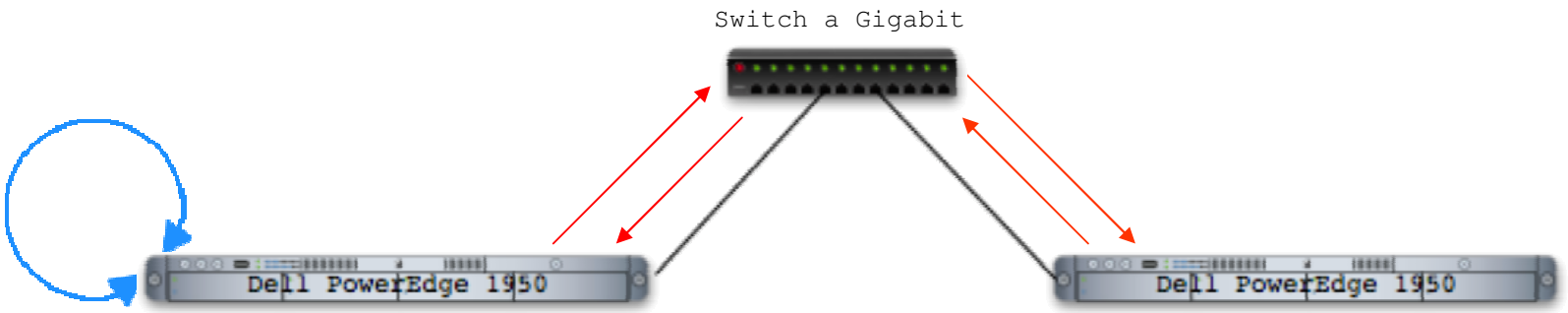
- És la part encarregada de recollir les dades de la xarxa
- Farà servir la llibreria *libpcap* comentada anteriorment
- Requeriments
  - Eficiència
  - Independència
  - Portabilitat

Eina desenvolupada: *listener* (2)

- Paràmetres de la captura
  - Temps inicial i final del flux
  - Protocol
  - Adreça i port origen
  - Adreça i port destí
  - Bytes i paquets intercanviats
  - Estat del flux

Eina desenvolupada: *listener* (3)

- Es van realitzar un parell de proves de rendiment



Prova 1

Llegint 12 Gbytes del dispositiu lògic */dev/zero* i enviant-los a l'altra màquina amb la utilitat *netcat*, es van aconseguir capturar 89.3 Mbytes per segon.

Prova 2

Transmetent un fitxer de disc a través de *netcat* i rebent-lo, a la mateixa màquina pel dispositiu de loopback, es van arribar a capturar 425.4 Mbytes per segon.

Eina desenvolupada: *flow_adder* (1)

- Serà l'encarregat de processar els fitxers de captura retornats pel *listener* i agrupar les dades per fluxos segons uns criteris preestablerts
  - Ordenació dels fluxos per temps
  - Temps d'expiració de flux (finestra de temps)

- Els intervals escollits d'agregació d'aquestes dades seran:
  - Cada 15 minuts fins a obtenir el diari (24h)
  - Setmanal, mensual i anual

Eina desenvolupada: *flow_adder* (2)

- Problema de la captura
  - Procés amb un període de temps entre resultats arbitrari
    - És el propi usuari qui el determina en el fitxer de configuració
  - Els fitxers de resultats no estan ordenats
- Aquests dos punts causaven problemes de temps amb grans volums de dades

- Part de la solució va passar per fer una ordenació parcial per temps en diferents taules de hash

Eina desenvolupada: *flow_adder* (3)

- Els resultats d'aquesta part són
  - Fitxers de dades agrupats per fluxos (tenint en compte el temps d'expiració indicat per l'usuari) i ordenats per temps de 15 minuts (de manera independent al temps indicat per l'usuari)
  - Fitxers d'estadístiques per tal de visualitzar, per a cada interval processat, quina quantitat de tràfic s'ha capturat i quines màquines o ports en són responsables. Es generaran fitxers d'estadístiques per
    - Cada interval de 15 minuts
    - Cada dia
    - Cada setmana
    - Cada mes
    - Cada any

Eina desenvolupada: *flow_adder* (4)

- Exemple d'agregació

Fitxer 1

```
1182678091.994204 0.0 6 81.44.213.27 192.168.0.2 4653 80 47 1290 3 9
```

Temps inicial
Temps final
Protocol
Adreça IP origen
Adreça IP destí
Port origen
Port destí

+

Fitxer 2

```
0.0 1182678991.994204 6 192.168.0.2 81.44.213.27 80 4653 117 120 7 5
```

Temps inicial
Temps final
Protocol
Adreça IP origen
Adreça IP destí
Port origen
Port destí

Resultat

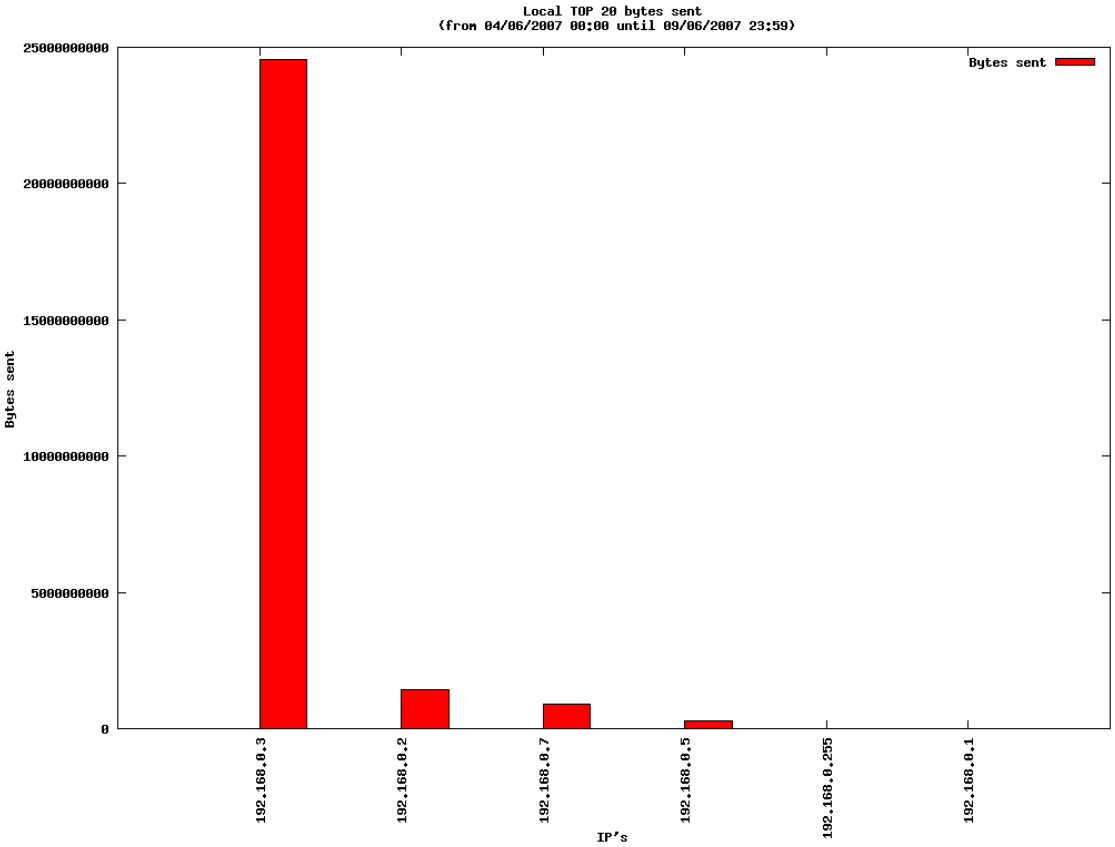
```
1182678091.994204 1182678991.994204 6 81.44.213.27 192.168.0.2 4653 80 167 1407 8 16
```

Eina desenvolupada: *viewer* (1)

- És la part encarregada de la visualització dels resultats
- S'ha realitzat una part molt senzilla per demostrar la validesa del model, encara que serà més extensa
- Es fa servir *gnuplot* per tal de generar les gràfiques

Eina desenvolupada: *viewer* (2)

- Exemple de gràfica obtinguda



Continguts

- *Introducció*
- *Les xarxes actuals*
- *La llibreria libpcap*
- *Eina desenvolupada*
- ***Proves realitzades***
- *Planificació*
- *Costos directes*
- *Anàlisi de desviacions*
- *Conclusions*
- *Línies futures*

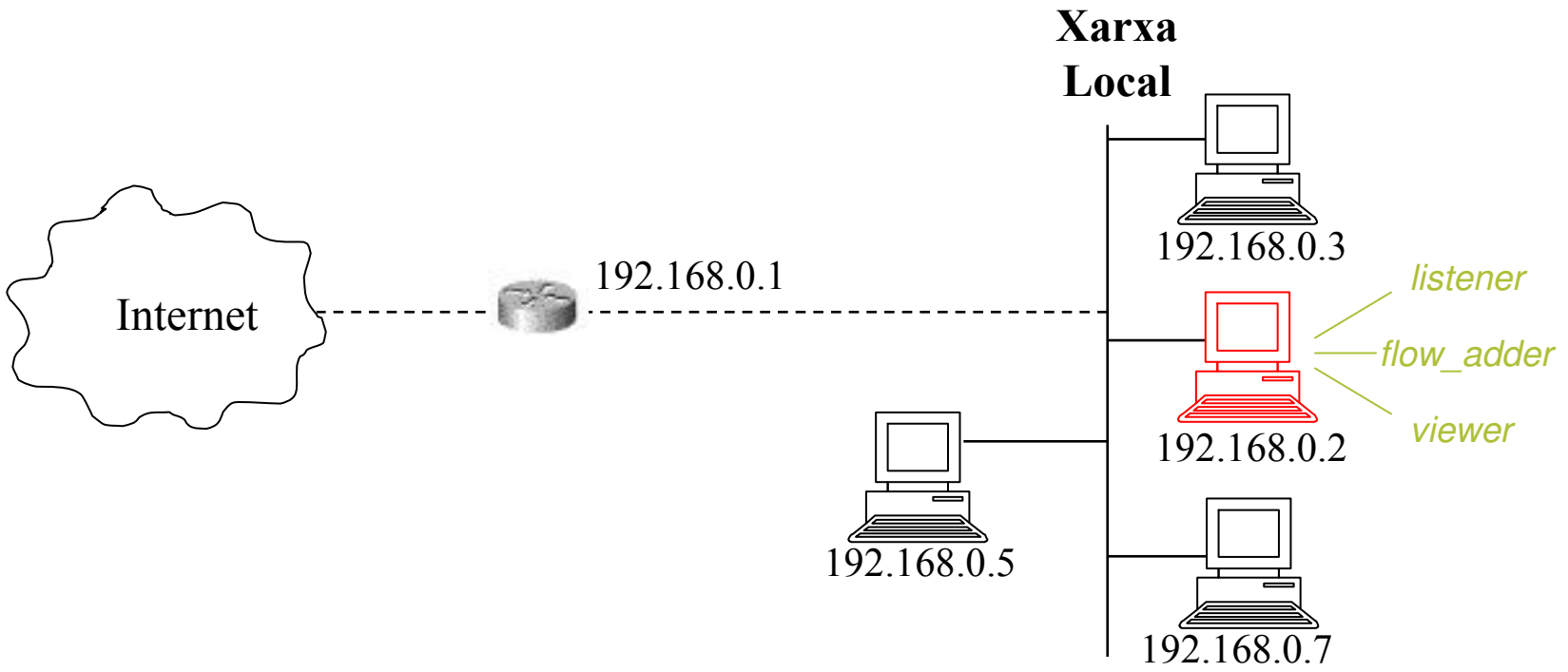
Proves realitzades (1)

- Degut a la limitació de duració d'un PFC i que el procés de desenvolupament i test és continu, aquest prototip encara no es troba en producció

- Adjuntem una mostra del resultat obtingut de realitzar unes proves en un entorn controlat en el transcurs d'una setmana

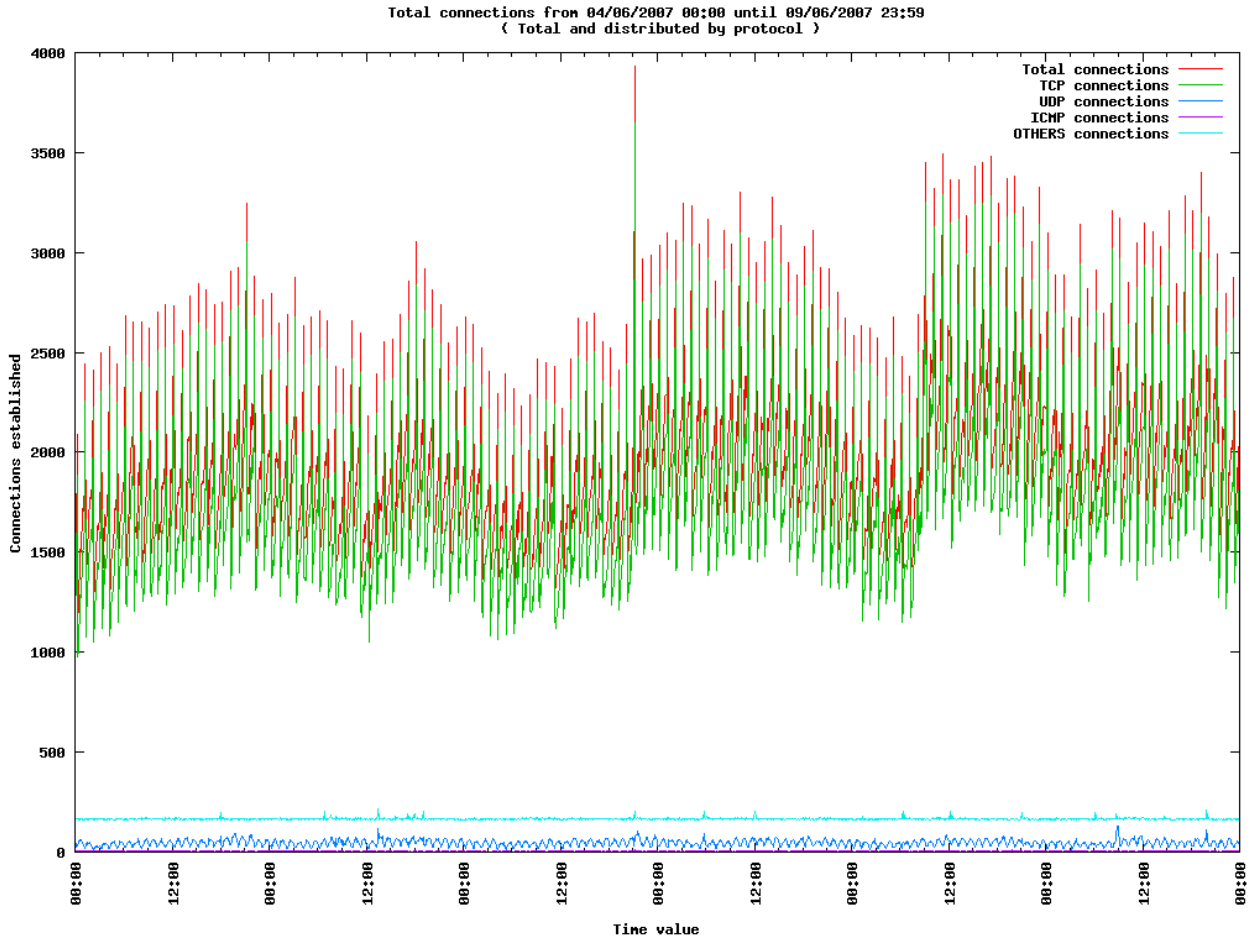
Proves realitzades (2)

- Xarxa on va estar funcionant l'eina



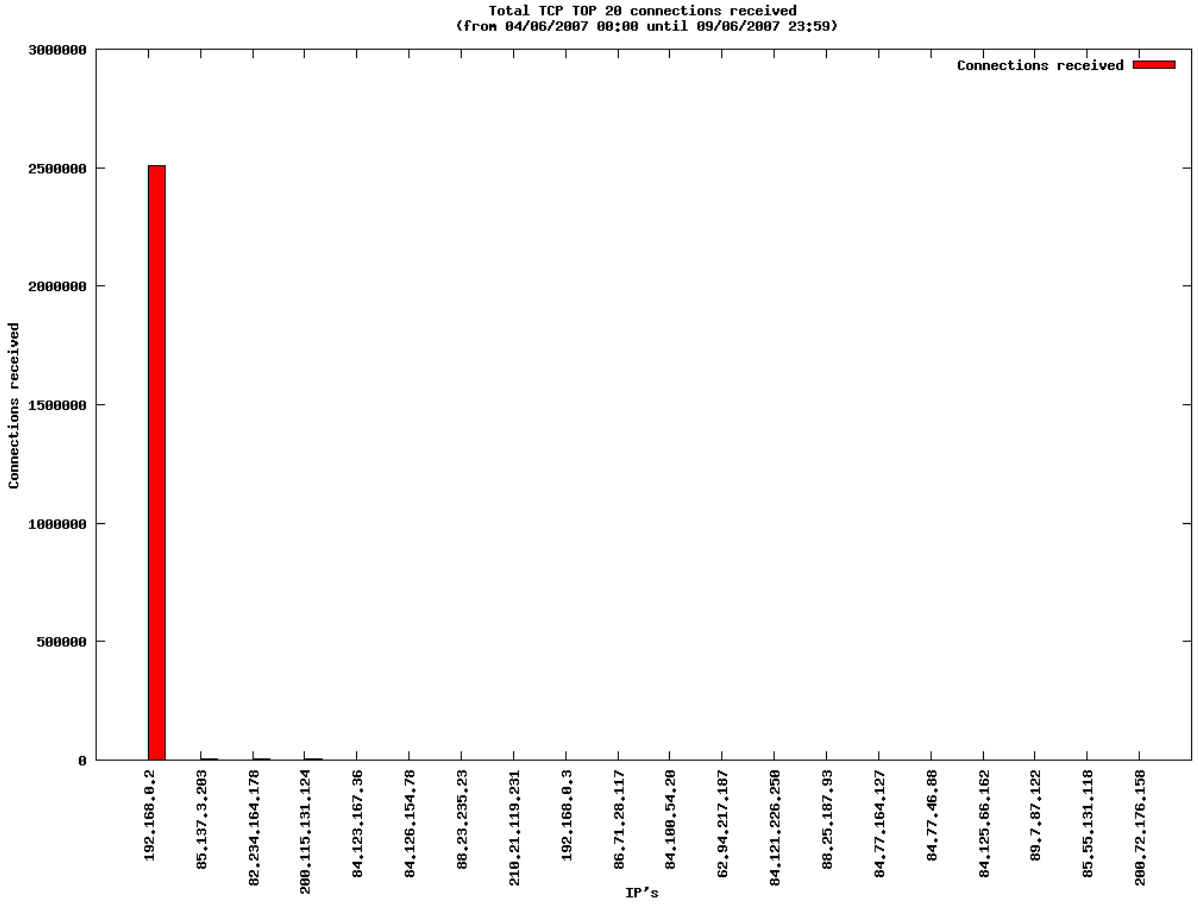
Proves realitzades (3)

Gràfica per conèixer el número de connexions totals



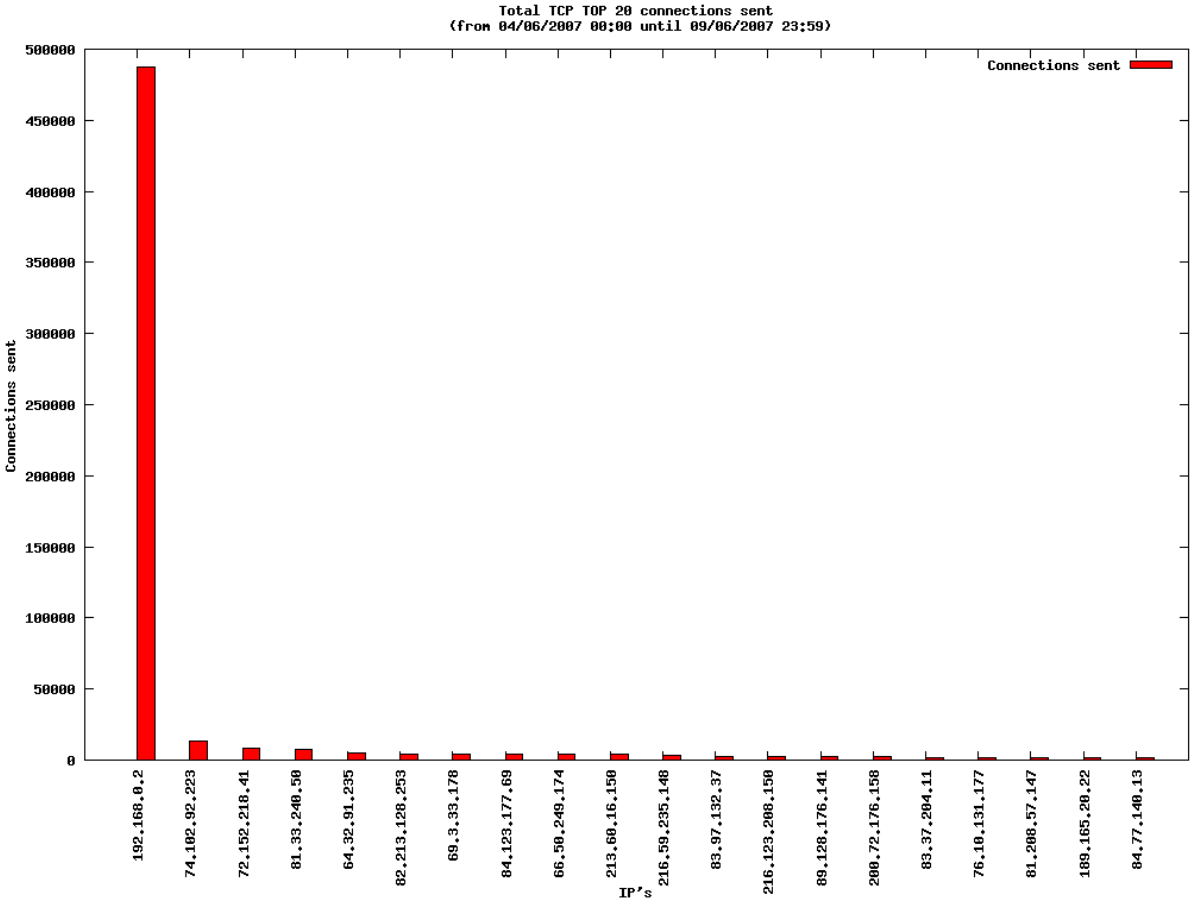
Proves realitzades (4)

Gràfica per conèixer el número de connexions TCP rebudes



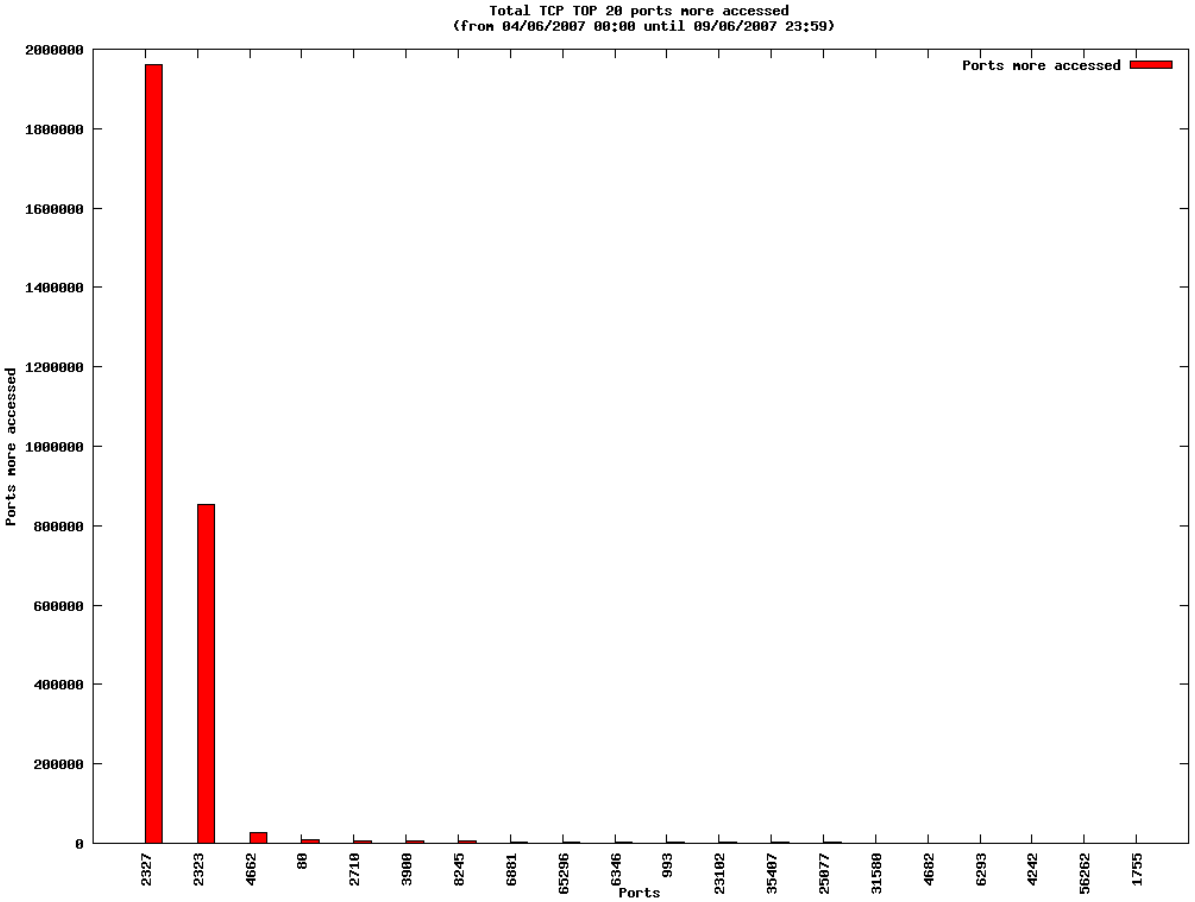
Proves realitzades (5)

Gràfica per conèixer el número de connexions TCP enviades



Proves realitzades (6)

Gràfica per conèixer el número de ports TCP més accedits



Continguts

- *Introducció*
- *Les xarxes actuals*
- *La llibreria libpcap*
- *Eina desenvolupada*
- *Proves realitzades*
- ***Planificació***
- *Costos directes*
- *Anàlisi de desviacions*
- *Conclusions*
- *Línies futures*

Planificació

Tasca	*Durada*	*Principi*	*Final*	*Hores dedicades*
Desenvolupament del *listener*	49 dies	16 de Febrer de 2007	5 d'Abril de 2007	203 hores
Investigació	17 dies	16 de Febrer de 2007	4 de Març de 2007	75 hores
Desenvolupament	29 dies	4 de Març de 2007	5 d'Abril de 2007	106 hores
Proves i optimitzacions	6 dies	18 de Març de 2007	23 de Març de 2007	22 hores
Desenvolupament del *flow_adder*	52 dies	6 d'Abril de 2007	3 de Juny de 2007	164 hores
Investigació	8 dies	6 d'Abril de 2007	13 d'Abril de 2007	32 hores
Desenvolupament	34 dies	14 d'Abril de 2007	31 de Maig de 2007	112 hores
Proves i Optimitzacions	10 dies	8 de Maig de 2007	18 de Maig de 2007	20 hores
Desenvolupament del *viewer*	5 dies	1 de Juny de 2007	5 de Juny de 2007	30 hores
Investigació	1 dia	1 de Juny de 2007	2 de Juny de 2007	8 hores
Desenvolupament	3 dies	2 de Juny de 2007	5 de Juny de 2007	17 hores
Proves	2 dies	3 de Juny de 2007	5 de Juny de 2007	5 hores
Documentació	22 dies	25 de Maig de 2007	15 de Juny de 2007	80 hores

Continguts

- *Introducció*
- *Les xarxes actuals*
- *La llibreria libpcap*
- *Eina desenvolupada*
- *Proves realitzades*
- *Planificació*
- ***Costos directes***
- *Anàlisi de desviacions*
- *Conclusions*
- *Línies futures*

Costos directes

Concepte		Cost
Equipament hardware		3.100 €
1 Equip de xarxa (*switch*) a Gigabit	900 €	
1 Equip enracable d'altes prestacions	2.200 €	
Anàlisi, Disseny i Implementació		10.440 €
1 analista (15 dies laborals, 8 hores diàries)	4.800 €	
1 dissenyador (6 dies laborals, 8 hores diàries)	1.288 €	
1 programador (28 dies laborals, 8 hores diàries)	4.032 €	
1 programador Web (2 dies laborals, 8 hores diàries)	320 €	

TOTAL	13.540 €

Continguts

- *Introducció*
- *Les xarxes actuals*
- *La llibreria libpcap*
- *Eina desenvolupada*
- *Proves realitzades*
- *Planificació*
- *Costos directes*
- ***Anàlisi de desviacions***
- *Conclusions*
- *Línies futures*

Anàlisi de desviacions

- Més temps de l'estimat inicialment en la part del *flow_adder*
  - Degut al gran volum de dades → Taules de hash
- Menys temps de l'estimat inicialment en la part del *viewer*
  - Ajustar planificació
  - Degut a la simplicitat amb la que es va fer
  - Era la part menys important per demostrar la viabilitat del model escollit

Continguts

- *Introducció*
- *Les xarxes actuals*
- *La llibreria libpcap*
- *Eina desenvolupada*
- *Proves realitzades*
- *Planificació*
- *Costos directes*
- *Anàlisi de desviacions*
- ***Conclusions***
- *Línies futures*

Conclusions (1)

- S'han assolit tots els objectius establerts en un principi
- Rendiment molt satisfactori de la llibreria *libpcap*
- Optimitzacions molt importants en l'eina de captura i en l'agregació de fluxos per tal de minimitzar el temps de procés i l'ús de memòria i processador.

Conclusions (2)

- Englobat dins del projecte de programari lliure
  - Codi accessible a tothom
  - Actualització de l'aplicació per una àmplia comunitat d'usuaris
- Eina útil per la utilització en un ISP (proveïdor de serveis d'Internet), un departament, una empresa, etc.
- S'aconsegueix
  - El 100% del tràfic real en una xarxa a 20Mbps
  - El 100% del tràfic generat de forma artificial entre dues màquines connectades en una xarxa a Gigabit
  - El 100% del tràfic generat de forma artificial en una màquina per la interfície de *loopback*

Continguts

- *Introducció*
- *Les xarxes actuals*
- *La llibreria libpcap*
- *Eina desenvolupada*
- *Proves realitzades*
- *Planificació*
- *Costos directes*
- *Anàlisi de desviacions*
- *Conclusions*
- ***Línies futures***

Línies futures (1)

- Fer servir *anonimització* d'adreces IP per garantir la privacitat de les dades recollides
- Creació d'un mòdul ARP per capturar dades per sota del protocol TCP/IP
- Creació de filtres d'usuari per restringir l'abast de les captures
- Suport de múltiples listeners a la xarxa
- Avaluar la viabilitat de fer servir una base de dades externa on desar les dades capturades / agregades

Línies futures (2)

- Ampliació de la part de visualització per tal d'integrar-la en un servidor web
- Provar la viabilitat de l'eina en sistemes Windows fent servir la llibreria *winpcap*
- *Adaptar-la a IPv6*

- Més informació

http://gabriel.verdejo.alvarez.googlepages.com/ipss

Bibliografia

- [BAR03] Barlet P., Domingo J., Solé J. (2003), *SMARTXAC: Sistemas de Monitorización y Análisis de tráfico para la Anella Científica*, RedIRIS: boletín de la Red Nacional de I+D RedIRIS, número 66-67, pàgines 27-33.

- [ROS06] Rossi D., Mellia M. (2006), *Real time TCP/IP analysis with common hardware*, IEEE ICC'2006.