

桃園區網 維運工作報告

中央大學電算中心 楊素秋

May 8th 2014



報告大綱

- ❑ 1. 連網維運重點工作
 - 連外網路問題排除 (Fdns, Ips Loading)
- ❑ 2. Apache Hadoop (Cloud Computing)
 - Hadoop Maven Package
 - Hadoop Mongo Connector
- ❑ 3. Cloud-based 異常流量偵測
- ❑ 4. UDP Flooding 流量偵測
- ❑ 5. Pandora 異常流量



1. 連網維運重點工作

□ PaloAlto 5060 IPS

➤ 2013-03 設定超量攻擊 threshold

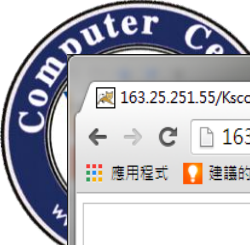
- 當 **Cpu Load** (Data-plane) > **70%** , 影響網路傳輸狀況
 - Dns, ssh, MS_rdp (2012-12, 2013-03 調整threshold)
 - MySql, MsSql, Pop3 (2013-03-28)

➤ 2014-03 overload

- Cpu Load (Manage-plane) 持續衝高
 - **TANet Backbone ISIS routing** 交換狀況不穩
 - 聯絡 IPS 設備廠商抓錯, ACL 阻擋 異常流量
 - » 捨棄 url content, spyware detection

➤ 2014-04 overload

- Google 相關網站不通



163.25.251.55/Kscore/Di x

163.25.251.55/Kscore/Demo.zul

應用程式 建議的網站 網管工具箱 網頁快訊圖庫 Map Reduce Seco... download Invoice - Sample In... (Part 1) Configurin... Spring Hibernate jazon.com/histor... Text File to JPG file ... 其他書籤



臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router

PaloAlto 5060 IPS

區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢

網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢

Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢

連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統

桃園區網 KSCORE 紀錄查詢

中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群

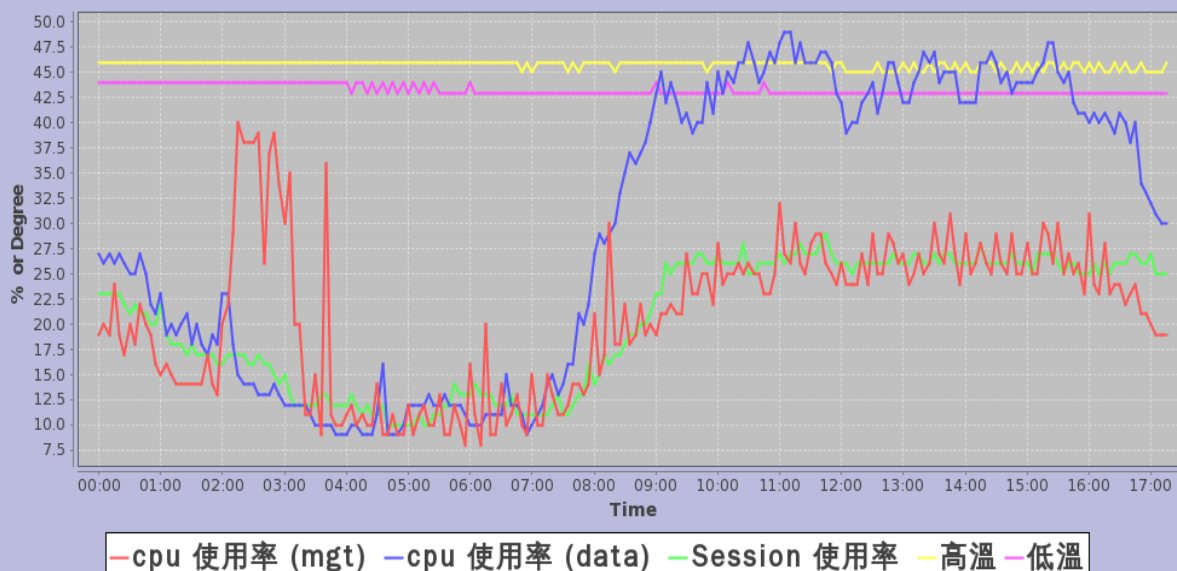
中央大學 伺服器主機群

Service Usage Statistics

區網 PaloAlto 5060 IPS

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-10-25)

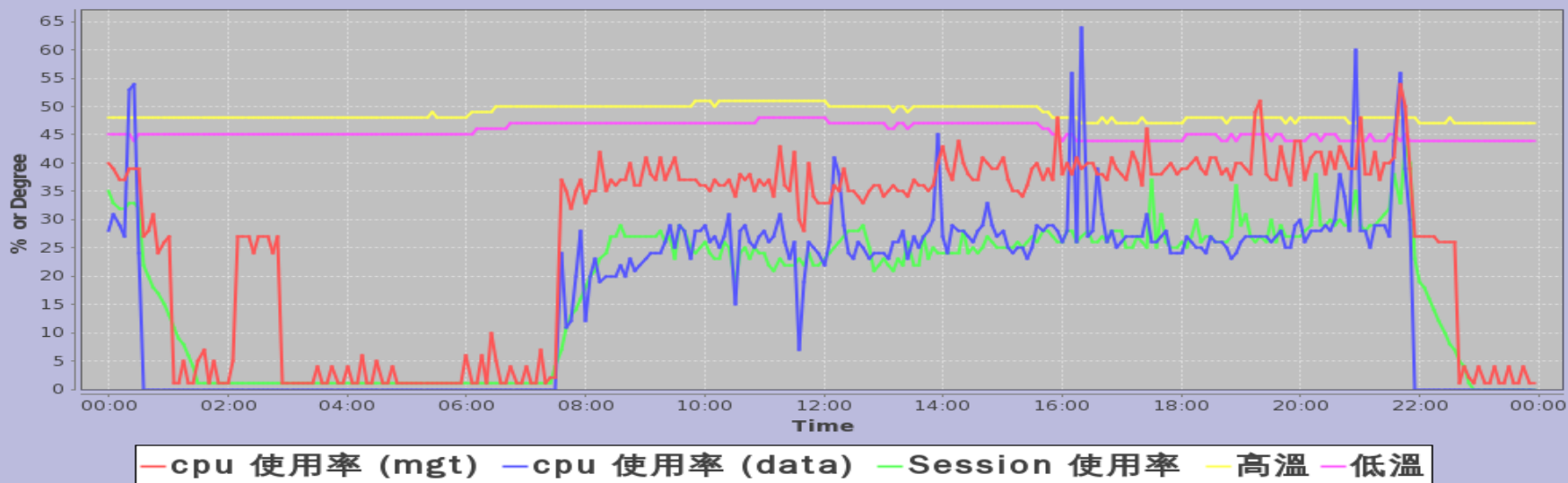
系統運作溫度 不可過高, Session使用率 不可過高



國立中央大學 電算中心

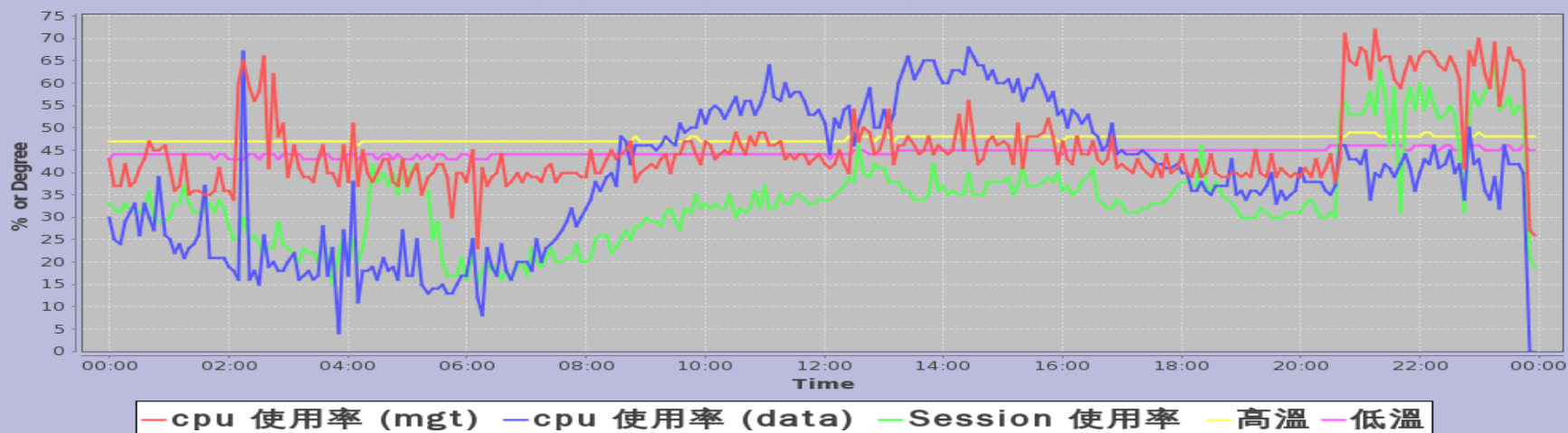
桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2014-03-29)

系統運作溫度 不可過高, Sesssion使用率 不可過高



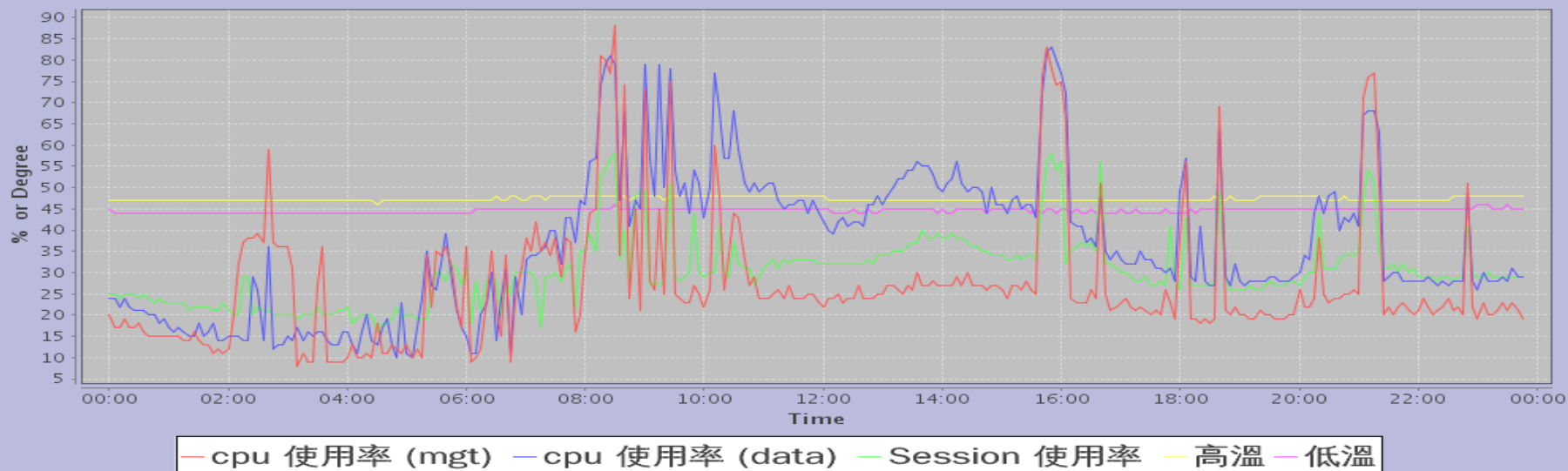
桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2014-04-01)

系統運作溫度 不可過高, Sesssion使用率 不可過高



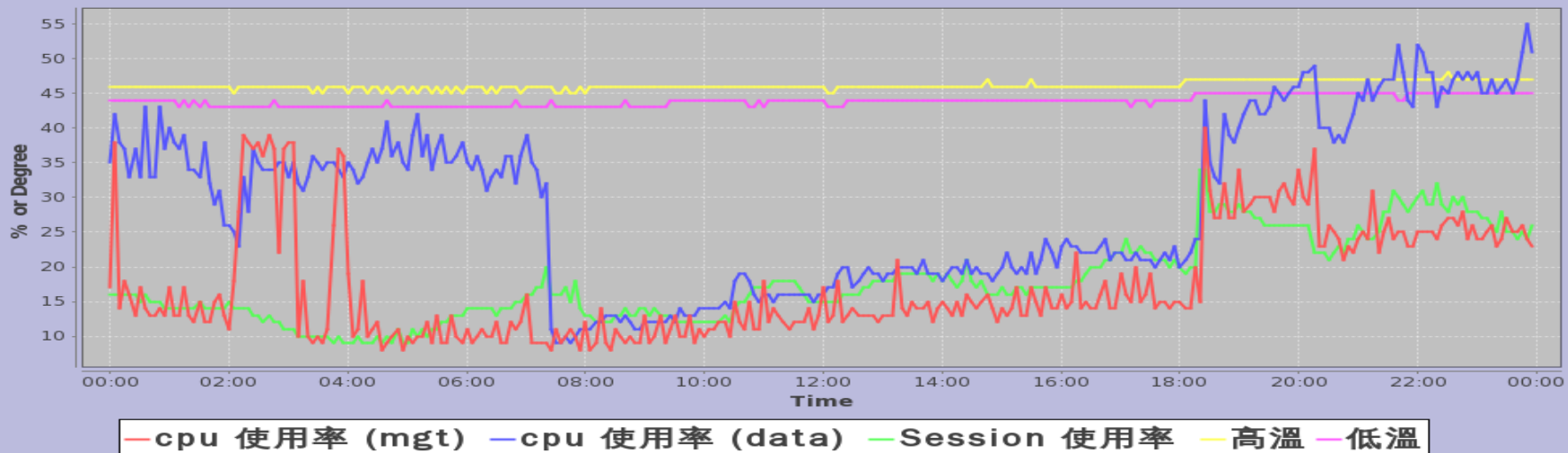
桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-09-23)

系統運作溫度 不可過高, Sessstion使用率 不可過高



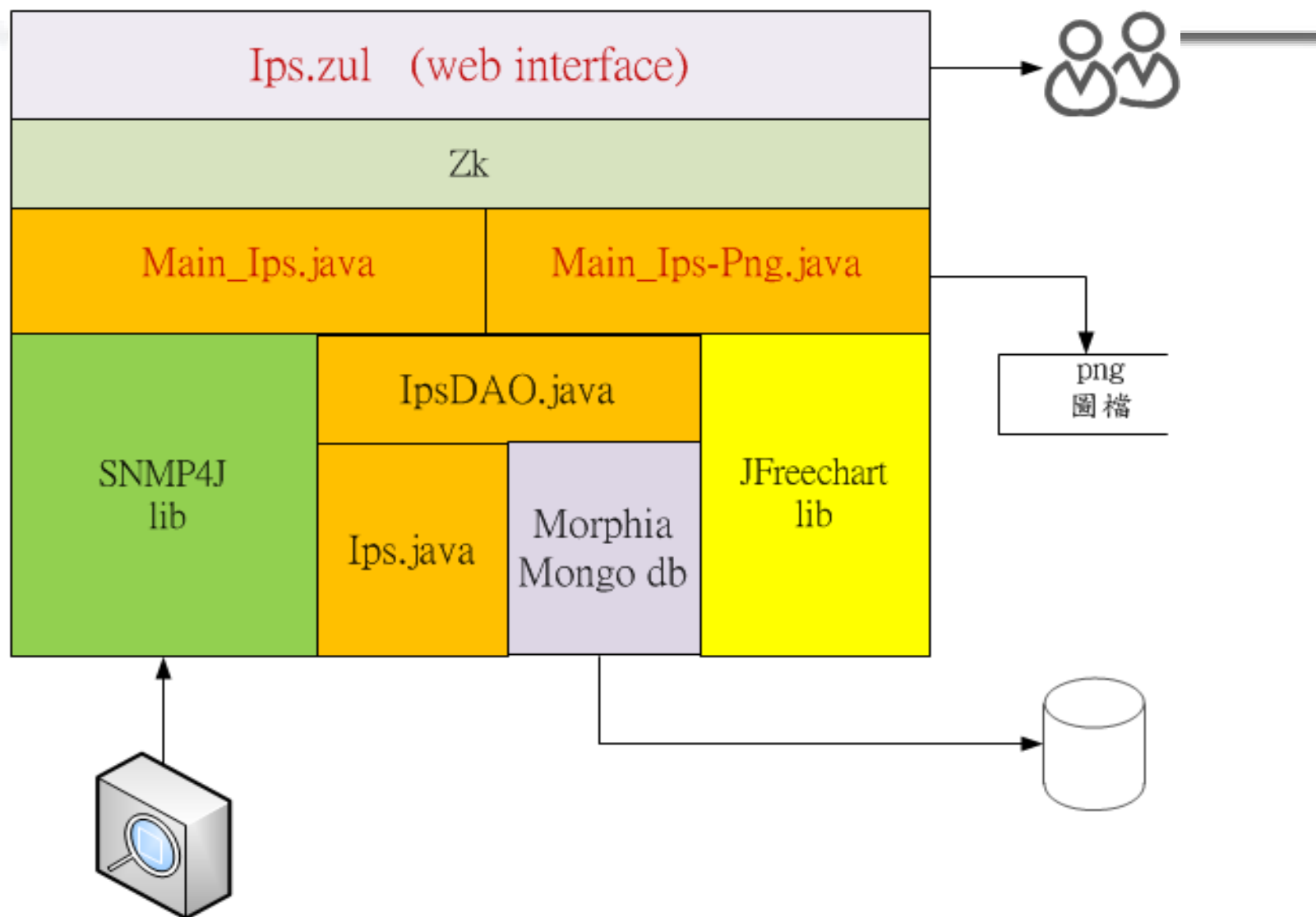
桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-10-27)

系統運作溫度 不可過高, Sessstion使用率 不可過高





區網 IPS 系統資源使用比率監看 處理程序





1. 連網維運重點工作 (cont.)

☐ Botnet 紀錄與自動通報

- <http://kscore.tyc.edu.tw/Kscore/searchBotnetMvc.zul>

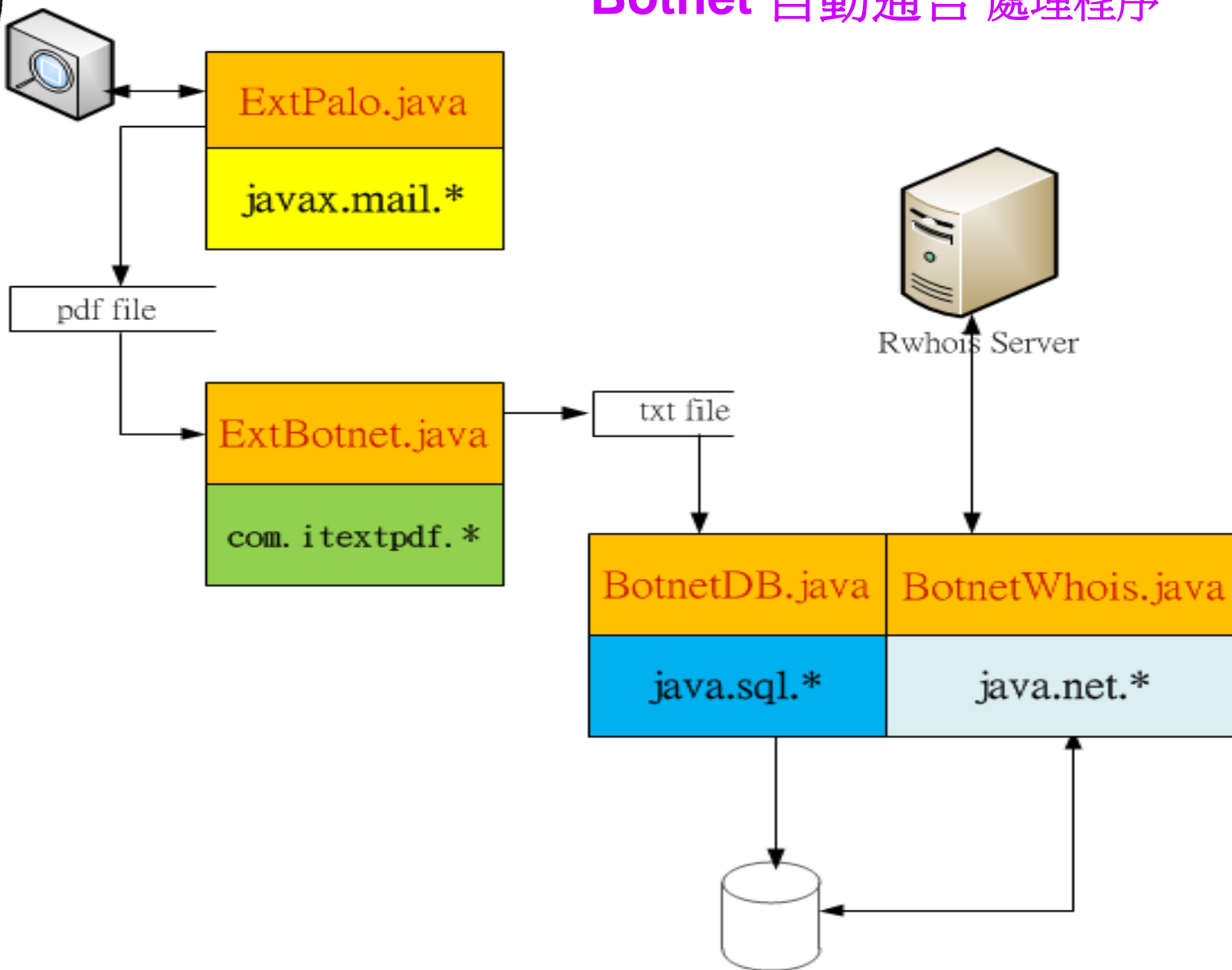
☐ Asoc 資安事件紀錄與自動通報

- <http://kscore.tyc.edu.tw/Kscore/searchAsocMvc.zul>

☐ 異常流量偵測 / 監看

- <http://hadoop.tyc.edu.tw/Fdns>
- Top UDP 流量 (10-minute, hour, day)
- PortScan 流量 (day, 10-minute)
- TopN 流量, Top Connection (day)
- Kscore 篩選 **, Pandora 異常流量

Botnet 自動通告 處理程序





Botnet 通告紀錄查詢 網頁

網路設備運作狀況

Cisco 8509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群
中央大學 伺服器主機群

桃園區網 Botnet 通告紀錄查詢

Keyword:

Search

Botnet_信度	Botnet IP	Botnet 判別依據	Botnet 管理者 Email	通告日期
4	140.115.20.48	vsys1 Repeatedly visited (54) the same malicious URL \secure-content-delivery.com\	hsuhm@cc.ncu.edu.tw,wangcy@cc.ncu.edu.tw	2013-10-24 00:00:00
4	140.115.43.92	vsys1 Repeatedly visited (24) the same malicious URL \secure-content-delivery.com\	gracelin@ncu.edu.tw,hhtsai@cc.ncu.edu.tw	2013-10-23 00:00:00
4	140.115.231.108	vsys1 Repeatedly visited (64) the same malicious URL \api.idown.org/api/update_server.php\	center9@cc.ncu.edu.tw	2013-10-23 00:00:00
4	120.124.62.204	vsys1 Repeatedly visited (30) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	tychiu@mail.vnu.edu.tw,cysung@mail.vnu.edu.tw	2013-10-23 00:00:00
4	140.115.230.9	vsys1 Repeatedly visited (32) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	center9@cc.ncu.edu.tw	2013-10-23 00:00:00
4	140.115.53.122	vsys1 Repeatedly visited (30) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	jjhuang@cc.ncu.edu.tw,wjwang@csie.ncu.edu.tw	2013-10-22 00:00:00
4	140.115.219.57	vsys1 Repeatedly visited (28) the same malicious URL \api.luckyleap.net\	center9@cc.ncu.edu.tw	2013-10-22 00:00:00
4	140.135.31.2	vsys1 Repeatedly visited (20) the same malicious URL \api.luckyleap.net\	yeh@cycu.edu.tw,wenhan@cycu.edu.tw,anpin	2013-10-22 00:00:00
4	140.115.66.145	vsys1 Repeatedly visited (22) the same malicious URL \api.webconnect.co/rs\	opcwl@ncu.edu.tw,tlyeh@cc.ncu.edu.tw,howa	2013-10-22 00:00:00
4	140.135.26.155	vsys1 Repeatedly visited (33) the same malicious URL \secure-content-delivery.com\	yeh@cycu.edu.tw,wenhan@cycu.edu.tw,anpin	2013-10-21 00:00:00
4	140.138.225.90	vsys1 Repeatedly visited (32) the same malicious URL \www.searchto.kr/ocs/intro_proc.php\	joejoe@saturn.yzu.edu.tw,c7ht@saturn.yzu.edu.tw	2013-10-21 00:00:00

國立中央大學 電算中心



1.連網維運重點工作 (cont.)

➤ 桃園區網 ASOC ABUSE轉通報系統

http://ncusvr.ncu.edu.tw/Contact_Tiles (停用)

<http://kscore.tyc.edu.tw/Kscore/searchAsocMvc.zul>

桃園區網中心

Asoc ABUSE TYC List

通告編號	主機 IP	所屬學校	網管人員	事件類型	通告日期
AISAC-13522	192.192.250.192	開南大學	吳世彥	殭屍電腦(Bot)	2012-10-19 11:35:57.0
AISAC-13507	140.115.219.120	中央大學	戴元任	對外攻擊	2012-10-19 07:35:56.0
AISAC-13502	203.68.248.248	新興高中	林燦堂	殭屍電腦(Bot)	2012-10-19 07:15:56.0
AISAC-13415	140.132.27.183	中正理工學院	張凱威	殭屍電腦(Bot)	2012-10-16 14:15:53.0
AISAC-13413	120.125.84.170	銘傳大學	游象勇	殭屍電腦(Bot)	2012-10-16 12:55:53.0
AISAC-13363	203.68.248.248	新興高中	林燦堂	殭屍電腦(Bot)	2012-10-16 07:15:53.0
NTUSOC-EWA-201210-0015	210.60.239.13	青輔會青年職訓中心	蔡宏松	疑發起對外攻擊	2012-10-16 07:04:28.0
AISAC-13353	140.115.113.150	軟體中心	王耀強	殭屍電腦(Bot)	2012-10-15 13:45:53.0
AISAC-13351	120.124.199.253	清雲科技大學	林大為	殭屍電腦(Bot)	2012-10-15 13:25:53.0
AISAC-13339	210.59.41.252	敬城高中	宋清風	垃圾郵件(Spam)	2012-10-15 09:46:00.0
AISAC-13332	140.115.14.178	電算中心	戴元任	對外攻擊	2012-10-15 09:05:53.0
AISAC-13327	140.115.120.128	太空	呂凌霄	對外攻擊	2012-10-15 08:35:53.0



Asoc 資安通報紀錄查詢 網頁

163.25.251.55/Kscore/Demo.zul

應用程式 建議的網站 網管工具箱 網頁快訊圖庫 Map Reduce Seco... download Invoice - Sample In... (Part 1) Configurin... Spring Hibernate jazon.com/histor... Text File to JPG file ... 其他書籤

臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群
中央大學 伺服器主機群

區網 Asoc Abuse紀錄查詢

Keyword:

Asoc_ID	IP	School	AbuseType	Date
AISAC-28522	192.192.250.155	開南大學資訊科技中心	對外攻擊	2013-10-23 11:16:31
AISAC-28283	140.135.198.35	中原大學電算中心	對外攻擊	2013-10-21 08:56:54
AISAC-28251	210.60.0.2	國立體育大學	殭屍電腦(Bot)	2013-10-21 08:26:22
ASOC-EWA-201310-0645	140.135.25.98	中原大學電算中心	對外攻擊	2013-10-17 16:02:10
AISAC-28124	192.83.181.124	國立體育大學	網頁置換	2013-10-16 22:26:26
AISAC-28110	192.192.250.94	開南大學資訊科技中心	對外攻擊	2013-10-16 17:36:05
AISAC-27968	140.115.71.237	中央大學電機	對外攻擊	2013-10-15 14:27:08
AISAC-27966	140.115.152.210	中央大學通訊	對外攻擊	2013-10-15 14:26:58
AISAC-27875	140.115.5.32	中央大學教職員宿舍	對外攻擊	2013-10-12 22:36:32
AISAC-27855	140.115.65.65	中央大學機械	對外攻擊	2013-10-11 11:56:30
AISAC-27789	140.115.185.82	總務處	對外攻擊	2013-10-08 15:26:05
AISAC-27641	210.60.0.2	國立體育大學	殭屍電腦(Bot)	2013-10-03 14:56:32
AISAC-27470	140.135.24.101	中原大學	對外攻擊	2013-09-28 13:46:17
AISAC-27339	120.124.129.31	健行科技大學	對外攻擊	2013-09-25 08:36:27
AISAC-27294	140.135.50.72	中原大學	殭屍電腦(Bot)	2013-09-24 13:53:05
AISAC-26791	140.135.56.124	中原大學	對外攻擊	2013-09-09 17:48:01
AISAC-26599	140.138.31.199	元智大學	殭屍電腦(Bot)	2013-09-05 10:27:26
AISAC-26458	140.115.65.65	中央大學機械	對外攻擊	2013-09-03 09:28:42
NTUSOC-EWA-201308-0094	120.124.74.210	萬能科技大學	可疑連線	2013-08-30 11:40:55
AISAC-26247	140.115.49.1	中央大學生資	對外攻擊	2013-08-27 15:57:33

國立中央大學 電算中心

©2012 Computer Center, National Central University.



2. Cloud Computing

- ❑ Hadoop
 - javac (compile)
 - java jar (execution)
- ❑ Hadoop + **Maven**
 - Input/output to text files
- ❑ **Hadoop + MongoDB + Maven**
 - Input/output to mongoDB **

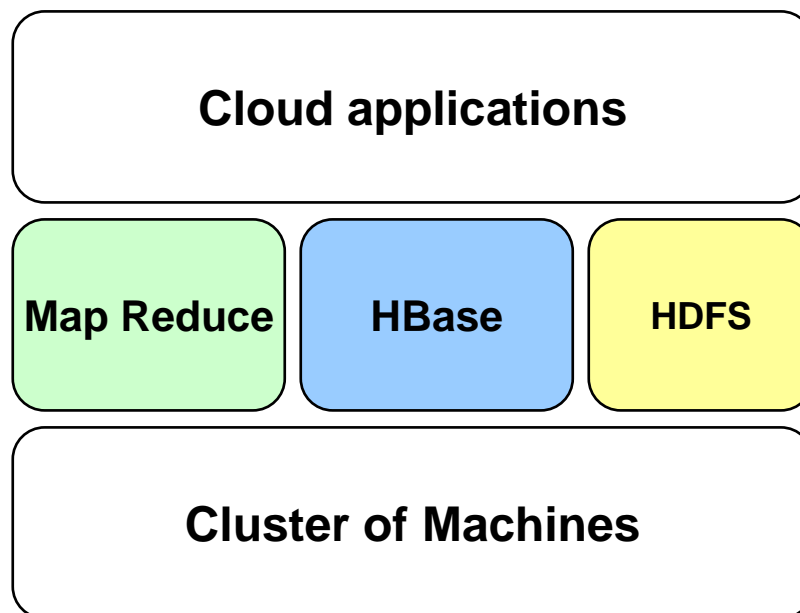


2. Cloud Computing (cont.)



- ☐ provides a framework for large scale parallel processing
 - distributed file system
 - map-reduce programming paradigm.

- ☐ **Open source project**
- ☐ Written by Java
- ☐ Runs on
 - **Linux**, Mac OS/X,
 - Windows, Solaris
 - Commodity hardware

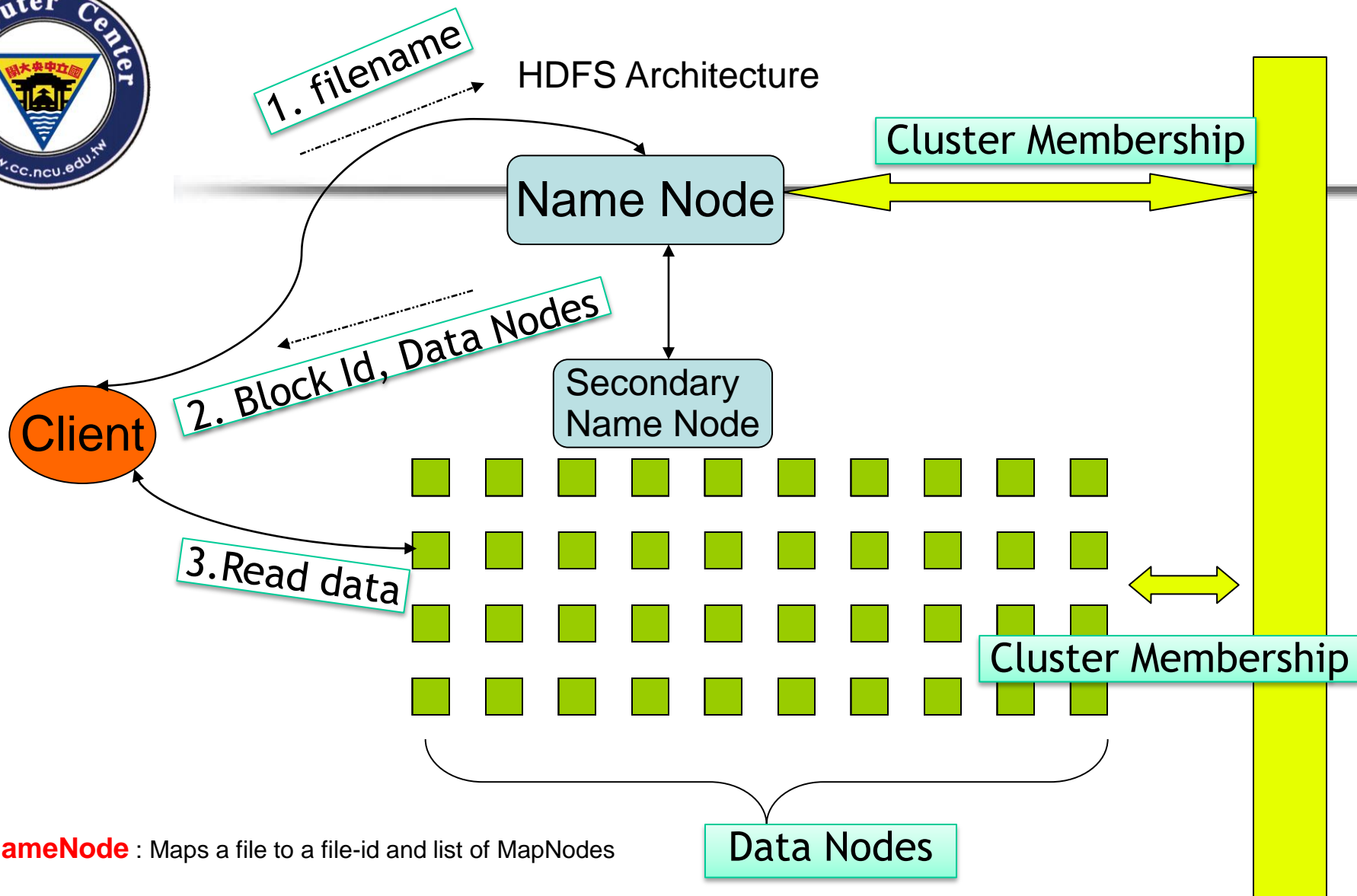




2. Cloud Computing (cont.)

❑ Hadoop installation

- Hadoop tutorial
 - http://trac.nchc.org.tw/cloud/wiki/Hadoop_Lab1
- `cd /opt`
- `yum -y install openssh rsync`
 - `vim /etc/ssh/ssh_config`
 - `ssh-keygen -t rsa -f ~/.ssh/id_rsa -P ""`
 - `cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys`
- `wget http://apache.mesi.com.ar/hadoop/common/hadoop-1.2.1/hadoop-1.2.1.tar.gz`
- `tar zxvf hadoop-1.2.1.tar.gz`
- `mv hadoop-1.2.1 hadoop`
- `/opt/hadoop/conf`
 - `core-site.xml`, `hadoop-env.sh`, `mapred-site.xml`
- **`hadoop namenode -format`**
 - **`Hadoop dfsadmin -safemode leave`**
- `/opt/hadoop/bin`
 - `start-all.sh`, `stop-all.sh`



NameNode : Maps a file to a file-id and list of MapNodes

DataNode : Maps a block-id to a physical location on disk

SecondaryNameNode: Periodic merge of Transaction log



2. Cloud Computing (cont.)

□ Hadoop

➤ Mapreduce 程式

➤ Compile

- **javac** -classpath /opt/hadoop/hadoop-core-1.0.1.jar:/opt/hadoop/hadoop-tools-1.0.1.jar -d flood_min flood_min.java
- **jar** -cvf **flood_min.jar** -C flood_min/ .

➤ Execute

- **hadoop jar flood_min.jar** flood_min input_dir output_dir



2. Cloud Computing (cont.)

□ Hadoop + Maven

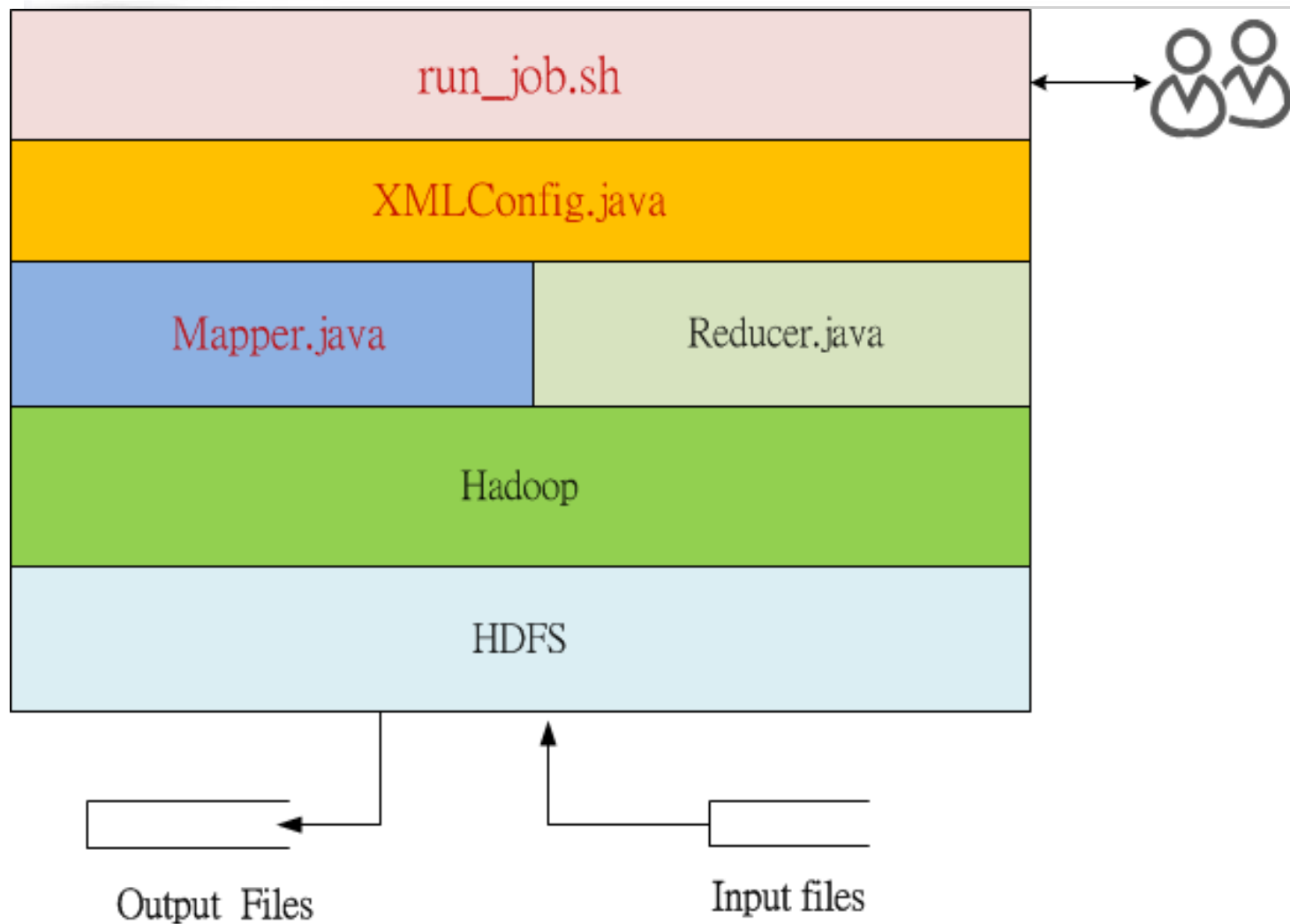
➤ Mapreduce 程式

➤ Compile

- `mvn clean compile package`
 - `target/project_name.war`

➤ Execute

- `run_job.sh`
 - `org.apache.hadoop.util.Tool;`
 - `org.apache.hadoop.util.ToolRunner;`





run_job.sh

```
#!/bin/sh
source /etc/profile
mday=`/bin/date '+%m%d'`
min=$(date --date='10 minute ago' +%H%M)

export HADOOP_HOME="/opt/hadoop"
JARNAME="tyrc_hadoop-1.0.jar"

HERE="$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )"

declare -a job_args
job_args=("jar" "$HERE/target/$JARNAME")

# INPUT SOURCE -
job_args=(${job_args[@]} "flood.flood_min")
job_args=(${job_args[@]} "flow_min")
job_args=(${job_args[@]} "output_flood")

$HADOOP_HOME/bin/hadoop "${job_args[@]}"

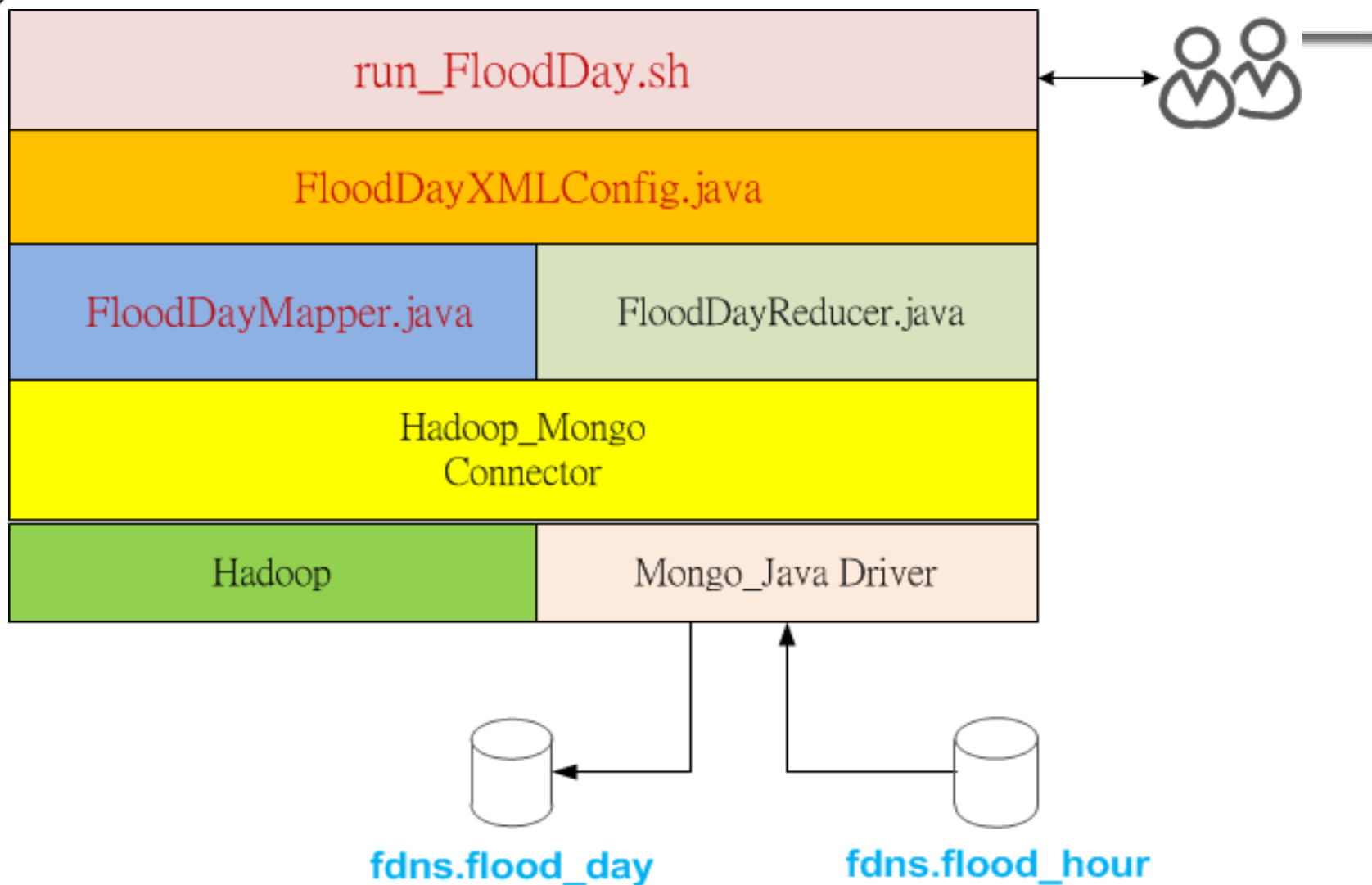
cd /home2/tyrc/Data/flood
hadoop fs -get output_flood/part-r-00000 $mday$min
```



2. Cloud Computing (cont.)

□ Hadoop + MongoDB + Maven

- Install Hadoop
- Install Hadoop Mongo Connector
 - lib
- Modify pom.xml
 - <resource>
 - <directory>\${basedir}/lib</directory>
 - </resource>
- run_job.sh





pom.xml

```
...  
<build>  
  <plugins>  
    <plugin>  
      <groupId>com.googlecode.addjars-maven-plugin</groupId>  
      <artifactId>addjars-maven-plugin</artifactId>  
      <version>1.0.5</version>  
      <executions>  
        <execution>  
          <goals>  
            <goal>add-jars</goal>  
          </goals>  
          <configuration>  
            <resources>  
              <resource>  
                <directory>${basedir}/lib</directory>  
              </resource>  
            </resources>  
          </configuration>  
        </execution>  
      </executions>  
    </plugin>  
  </plugins>  
</build>
```

...



run_mongo_job.sh

```
#!/bin/sh
cd /home2/tyrc/mongo_hadoop.
export HADOOP_HOME="/opt/hadoop"
INPUT_URI="mongodb://localhost:27017/fdns.flood_hour"
OUTPUT_URI="mongodb://localhost:27017/fdns.flood_day"
JARNAME="mongo_hadoop-1.0.jar"
HERE="$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )"
declare -a job_args
job_args=("jar" "$HERE/target/$JARNAME")
job_args=(${job_args[@]} "tyrc.FloodDayXMLConfig")
job_args=(${job_args[@]} "-D" "mongo.job.verbose=true")
job_args=(${job_args[@]} "-D" "mongo.job.input.format=com.mongodb.hadoop.MongoInputFormat")
job_args=(${job_args[@]} "-D" "mongo.input.uri=$INPUT_URI")
job_args=(${job_args[@]} "-D" "mongo.input.split_size=8")
job_args=(${job_args[@]} "-D" "mongo.job.mapper=tyrc.FloodDayMapper")
job_args=(${job_args[@]} "-D" "mongo.job.reducer=tyrc.FloodDayReducer")
job_args=(${job_args[@]} "-D" "mongo.job.output.key=org.apache.hadoop.io.Text")
job_args=(${job_args[@]} "-D" "mongo.job.output.value=com.mongodb.hadoop.io.BSONWritable")
job_args=(${job_args[@]} "-D" "mongo.job.mapper.output.key=org.apache.hadoop.io.Text")
job_args=(${job_args[@]} "-D" "mongo.job.mapper.output.value=org.apache.hadoop.io.Text")
job_args=(${job_args[@]} "-D" "mongo.output.uri=$OUTPUT_URI")
job_args=(${job_args[@]} "-D" "mongo.job.output.format=com.mongodb.hadoop.MongoOutputFormat")
echo "${job_args[@]}" "$1"
$HADOOP_HOME/bin/hadoop "${job_args[@]}" "$1"
```



3. Cloud-based 異常流量偵測

□ Cloud-based 異常流量偵測系統

➤ 桃園區網 FDNS (舊)

- <http://hadoop5.tyc.edu.tw>
 - TopN 流量排行, Top 連結 排行 (file)
 - Top UDP 排行 (mysql DB)
 - Kscore 異常監看 (mysql DB)

➤ 桃園區網 FDNS (新)

- <http://hadoop.tyc.edu.tw>
 - Mongo DB Collections
 - SEARCH 功能

桃園區網中心

ASOC_Abuse 通報

服務台

連線檢查

網管好幫手

區網異常連結

流量異常偵測

網管平台

FDNS 異常流量監測

* FDNS 首頁

* FDNS 異常監看

* TopN 流量排行

* TopN 連結排行

* 連線單位 單日流量

* 網路應用 單日流量

* 連線單位流量分布

* 網路應用流量分布

* TopN Udp 流量排行

* 單日 UDP Flood Traffic

* 單時 UDP Flood Traffic

* 詳細 UDP Flood Traffic

* UDP Traffic 指數

UDP Kscore

Enter IP Address

搜尋

Id	主機 IP	rate_in (MB)	rate_out	pkz_in(B)	pkz_out	flow_in	flow_out	Kscore	紀錄時間
72551	94.125.182.255	1024	0	1379	0	37954	0	21	2013-10-28 07:30:00.0
72445	94.125.182.255	13431	0	1383	0	216583	0	16	2013-10-28 05:50:00.0
72773	93.115.210.72	644	0	653	0	562474	0	14	2013-10-28 10:10:00.0
72550	91.236.182.1	9190	0	1382	0	222346	0	21	2013-10-28 07:30:00.0
72766	89.43.74.6	30	0	49	0	599493	0	8	2013-10-28 11:00:00.0
72767	89.43.74.6	27	0	49	0	548980	0	9	2013-10-28 10:50:00.0
72768	89.43.74.6	30	0	49	0	599893	0	10	2013-10-28 10:40:00.0
72769	89.43.74.6	28	0	49	0	566037	0	11	2013-10-28 10:30:00.0
72770	89.43.74.6	28	0	48	0	576577	0	12	2013-10-28 10:20:00.0
72771	89.43.74.6	33	0	49	0	665774	0	13	2013-10-28 10:10:00.0
72772	89.43.74.6	35	0	49	0	699709	0	14	2013-10-28 10:00:00.0



TopN 流量排行 查詢

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://163.25.255.31/Fdns/ 20140402.png (PNG Image, 1000 x... x) TopN 連結查看

163.25.255.31/Fdns/ Yahoo

Most Visited Getting Started

TAnet 桃園區網 異常流量監測

TopN 流量監測

- TopN 流量排行
- Top 連接數量排行
- UDP 流量排行

Pscan 異常偵測

- Pscan 異常流量排行
- Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

- Udp 流量 (10分鐘)
- Udp 流量 (小時)

UDP Flooding 流量監看

- UDP Flooding 異常流量

Tyrc TopN 流量排行

Keyword:

Oid	Hostip	Sum (MB)	Sum_in	Sum_out	Psz_in	Psz_out	Sum_dur (Hour)
1	202.169.175.79	391696	3343	388353	52	1482	17
2	202.169.173.204	356278	3323	352955	50	1482	17
3	202.169.175.80	353407	2890	350517	50	1482	17
4	202.169.173.207	351020	2551	348469	51	1482	17
5	202.169.173.205	346050	3054	342996	51	1482	17
6	202.169.173.210	342072	2871	339201	50	1481	17
7	202.169.175.77	338562	2330	336232	51	1481	17
8	202.169.175.81	335845	2561	333284	51	1479	17
9	202.169.173.209	324979	2661	322318	51	1481	17
10	202.169.173.208	321074	2855	318219	51	1482	17
11	202.169.175.78	316795	2356	314439	51	1482	17
12	202.169.173.211	313393	2689	310704	51	1480	17
13	202.169.173.206	312774	2346	310428	51	1479	17
14	202.169.175.76	309776	2201	307575	51	1479	17
15	140.115.17.45	273703	190	273513	49	1460	17
16	163.28.5.32	176386	3410	172976	53	1464	17
17	210.60.0.2	163829	155464	8365	1303	135	17
18	163.28.5.17	138713	3113	135600	58	1453	17
19	163.28.5.34	133038	2763	130275	57	1462	17
20	120.125.11.230	128768	115510	13258	1290	268	17

國立中央大學 電算中心





Udp Flooding 流量異常查詢

Mozilla Firefox
http://163.25.255.31/Fdns/
163.25.255.31/Fdns/

TANet 桃園區網 TopN 流量監測

UDP 流量排行

Keyword:

Oid	Hostip	Sum (MB)	Sum_in	Sum_out	Cnt_in	Cnt_out	Psiz_in	Psiz_out	Sum_dur (Hour)
1	192.186.208.165	177453	177453	0	506	0	1052	46	2
2	140.115.126.110	161350	0	161350	0	137	0	1052	2
3	162.212.252.47	154238	154238	0	349	0	1052	65	1
4	212.90.148.51	149669	149669	0	720	0	1052	332	2
5	120.124.40.98	129381	0	129381	23	657	137	1052	5
6	120.124.16.105	125480	0	125480	0	849	0	1054	5
7	198.251.80.166	94059	94059	0	154	0	1052	65	1
8	162.212.252.235	93630	93630	0	133	0	1052	65	1
9	198.251.80.221	53463	53463	0	128	0	1052	65	1
10	163.25.26.150	34036	55	33981	382	480	45	468	6
11	80.80.160.8	17597	17597	0	42	0	1052	46	1
12	96.45.82.133	17294	17294	0	31	0	1052	476	1
13	120.125.94.225	16998	5589	11409	41507	69354	581	985	9
14	140.135.13.130	15975	1106	14869	7993	7957	65	1059	10
15	140.135.9.120	15703	2861	12842	53648	52246	183	888	10

國立中央大學 電算中心



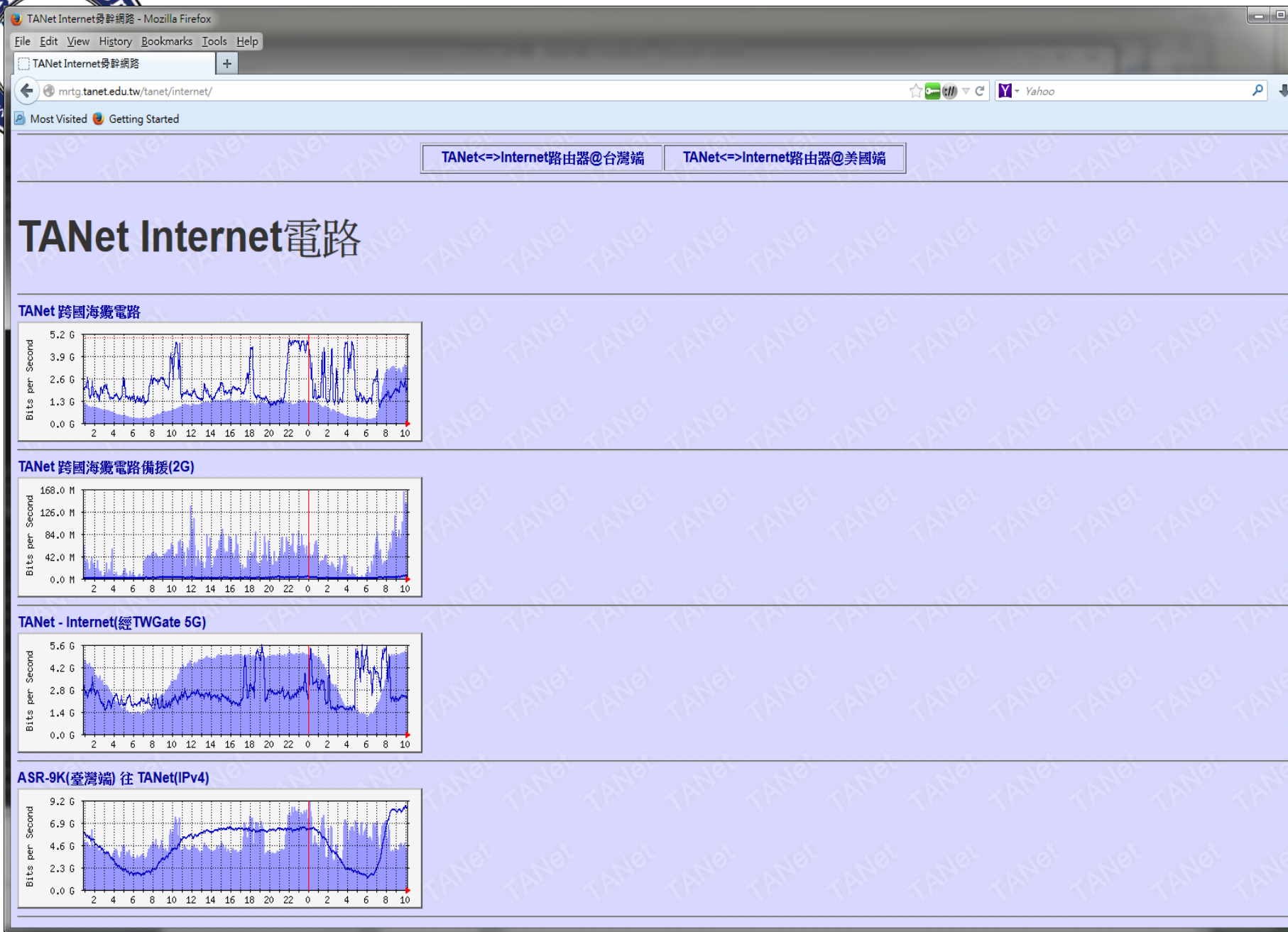
TANet 桃園區網 TopN 流量監測

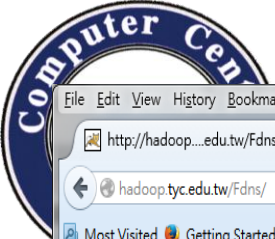
UDP Flooding 偵測 (Kscore)

Keyword:

Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
140.115.126.110@	0	18015	0	12	130	1052	04-21 08:20
140.115.126.110@	0	14150	0	17	115	1052	04-21 08:10
120.124.16.105@1	0	5381	0	51	214	1052	04-21 07:50
120.124.40.98@17	0	7465	0	58	49	1052	04-21 07:50
140.115.126.110@	0	12347	0	24	131	1052	04-21 07:50
120.124.40.98@17	0	6614	1	31	137	1052	04-21 07:40
140.115.126.110@	0	17309	0	10	137	1052	04-21 07:40
120.124.40.98@17	0	5134	1	37	137	1052	04-21 07:30
140.115.126.110@	0	29218	0	28	124	1052	04-21 07:30
120.124.40.98@17	0	6186	0	18	46	1052	04-21 07:20






File Edit View History Bookmarks Tools Help

http://hadoop...edu.tw/Fdns/ +

hadoop.tyc.edu.tw/Fdns/ Yahoo

Most Visited Getting Started



TANet 桃園區網 TopN 流量監測

[連線學校 MRTG流量] [IPv6 MRTG流量] [Links 連線狀態偵測] [網管工具箱] [伺服器主機檢客系統] [NCU 伺服器主機檢客系統] [NCU

TopN 流量監測

TopN 流量排行
TopN 流量 (小時)
Top 連接數量排行

Pscan 異常偵測
Pscan 異常流量排行
Pscan 異常流量 (小時)
Pscan 異常流量 (10分鐘)

UDP 詳細流量監看
UDP 流量排行
Udp 流量 (小時)
Udp 流量 (10分鐘)

UDP Flooding 流量監看
UDP Flooding 流量

TCP 異常流量偵測
密碼猜測 流量
Pandora 流量 (111.111.111.111)

UDP 流量排行

Keyword:

Oid	Hostip	Sum (MB)	Sum_in	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Sum_dur (Hour)
1	198.50.130.224	115780	115780	0	698	0	1052	46	2
2	120.125.114.3	40861	0	40861	0	167	0	1052	2
3	198.50.130.227	30568	30568	0	217	0	1052	46	1
4	120.125.115.22	23639	0	23639	0	99	0	1052	1
5	37.187.40.140	23307	23307	0	84	0	1052	73	1
6	94.23.197.146	21779	21779	0	130	0	1052	46	1
7	176.31.228.8	20945	20710	235	3132	218	1480	73	3
8	162.218.53.138	18130	18130	0	72	0	1052	73	1
9	91.121.182.86	11018	11018	0	48	0	1052	73	1
10	163.25.20.177	7642	7311	331	64782	88381	1162	85	6
11	210.60.0.2	5412	3010	2402	79221	77813	419	337	7
12	162.218.53.228	5101	5101	0	17	0	1052	73	1
13	120.124.84.34	4174	3358	816	37616	42996	556	203	8
14	162.218.53.254	4036	4036	0	12	0	1052	73	1
15	37.187.199.115	3937	3937	0	21	0	1052	73	1
16	163.25.26.150	3443	0	3443	6	11	76	468	1
17	120.124.160.116	3337	2	3335	16	67	73	1493	2

國立中央大學 電算中心


Computer Center

File Edit View History Bookmarks Tools Help

http://hadoop....edu.tw/Fdns/

hadoop.tyc.edu.tw/Fdns/

Most Visited Getting Started



TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器主機檢查系統\]](#) [\[NCU 伺服器主機檢查系統\]](#) [\[NCU TopN 流量監測\]](#)

TopN 流量監測

TopN 流量排行

TopN 流量 (小時)

Top 連接數量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (小時)

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

UDP 流量排行

Udp 流量 (小時)

Udp 流量 (10分鐘)

UDP Flooding 流量監看

UDP Flooding 流量

TCP 異常流量偵測

密碼猜測 流量

Pandora 流量 (111.111.111.111)

Tyrc UDP 流量排行 (10分鐘)

Keyword: 120.125.114.3 Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.125.114.3@17	0	3239	0	12	0	1052	05-07 04:10
120.125.114.3@17	0	4164	0	21	0	1052	05-07 04:00
120.125.114.3@17	0	7956	0	43	0	1052	05-07 03:50
120.125.114.3@17	0	3149	0	11	0	1052	05-07 03:40
120.125.114.3@17	0	2578	0	9	0	1052	05-07 03:30
120.125.114.3@17	0	4278	0	10	0	1052	05-07 03:20
120.125.114.3@17	0	2179	0	9	0	1052	05-07 02:30
120.125.114.3@17	0	1304	0	5	0	1052	05-07 02:20
120.125.114.3@17	0	3205	0	9	0	1052	05-07 01:40
120.125.114.3@17	0	3391	0	31	0	1052	05-06 23:30
120.125.114.3@17	0	5099	0	35	0	1052	05-06 23:20
120.125.114.3@17	0	4604	0	31	0	1052	05-06 23:10
120.125.114.3@17	0	4597	0	27	0	1052	05-06 23:00
120.125.114.3@17	0	6079	0	32	0	1052	05-06 22:50

國立中央大學 電算中心

2014/5/12

©2012 Computer Center, National Central University.

33



TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器主機檢察系統\]](#) [\[NCU 伺服器\]](#)

主機檢察系統 INCU TopN 流量監測

TopN 流量監測

[TopN 流量排行](#)[TopN 流量 \(小時\)](#)[Top 連接數量排行](#)

Pscan 異常偵測

[Pscan 異常流量排行](#)[Pscan 異常流量 \(小時\)](#)[Pscan 異常流量 \(10分鐘\)](#)

UDP 詳細流量監看

[UDP 流量排行](#)[Udp 流量 \(小時\)](#)[Udp 流量 \(10分鐘\)](#)

UDP Flooding 流量監看

[UDP Flooding 流量](#)

TCP 異常流量偵測

[密碼猜測 流量](#)[Pandora 流量 \(111.111.111.111\)](#)

Tyrc UDP 流量排行 (10分鐘)

Keyword: 120.125.115.22

Q Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.125.115.22@17	0	2415	0	4	0	1052	05-07 06:10
120.125.115.22@17	0	2124	0	9	0	1052	05-07 05:10
120.125.115.22@17	0	4654	0	16	0	1052	05-07 05:00
120.125.115.22@17	0	1502	0	4	0	1052	05-07 04:30
120.125.115.22@17	0	2412	0	4	0	1052	05-07 04:10
120.125.115.22@17	0	5482	0	25	0	1052	05-07 03:50
120.125.115.22@17	0	4839	0	22	0	1052	05-07 03:40
120.125.115.22@17	0	4796	0	19	0	1052	05-07 03:20
120.125.115.22@17	0	3393	0	9	0	1052	05-07 02:30
120.125.115.22@17	0	2493	0	9	0	1052	05-07 02:20
120.125.115.22@17	0	3866	0	17	0	1052	05-07 01:40
120.125.115.22@17	0	2613	0	14	0	1052	05-06 23:30
120.125.115.22@17	0	1453	0	7	0	1052	05-06 23:20
120.125.115.22@17	0	860	0	4	0	1052	05-06 23:10
120.125.115.22@17	0	1454	0	6	0	1052	05-06 23:00

國立中央大學 電算中心

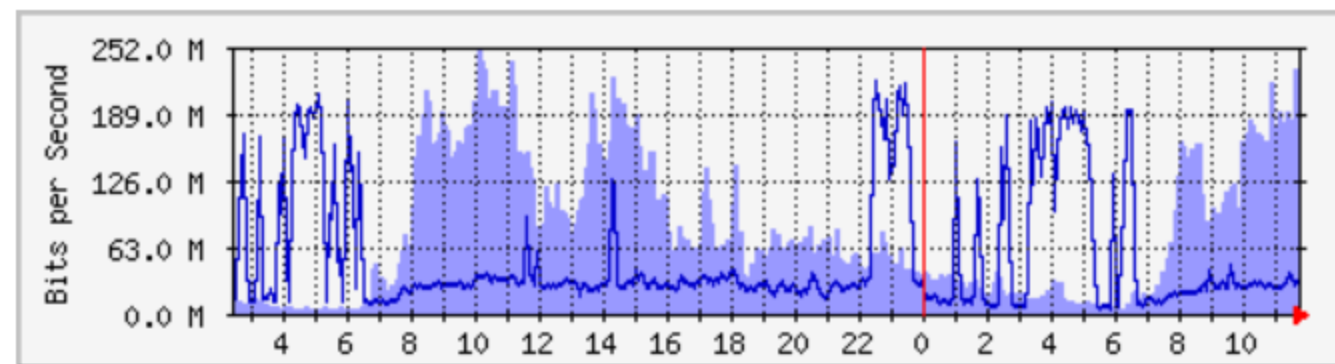
即時流量分析:(桃園區網) ---> 金門縣網

Description: (桃園區網) ---> 金門縣網

Max Speed: 300 Mbps

上次統計更新時間: 2014 年 五 7 日 星期三 11:45

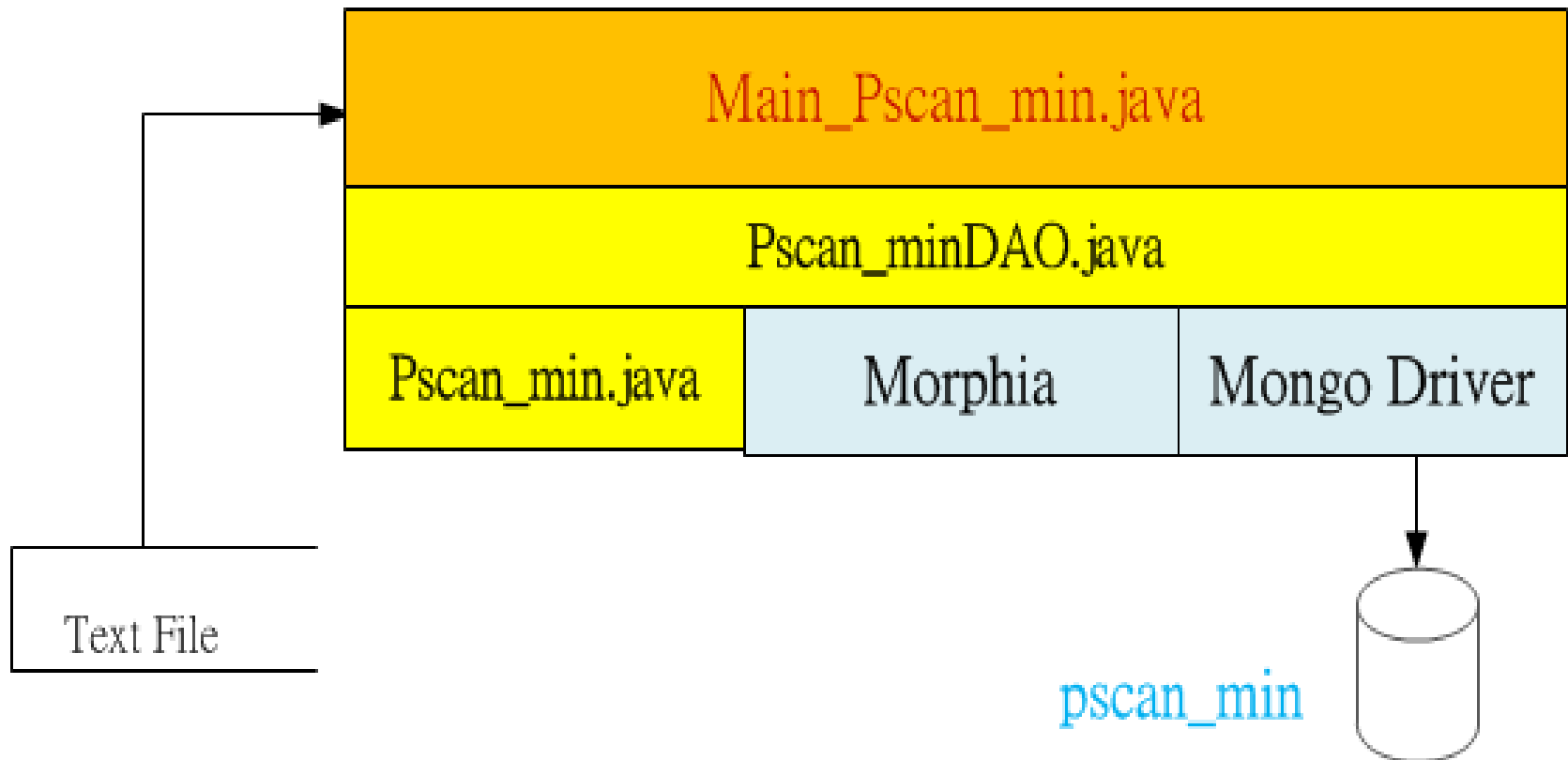
每日 圖表 (5 分鐘 平均)

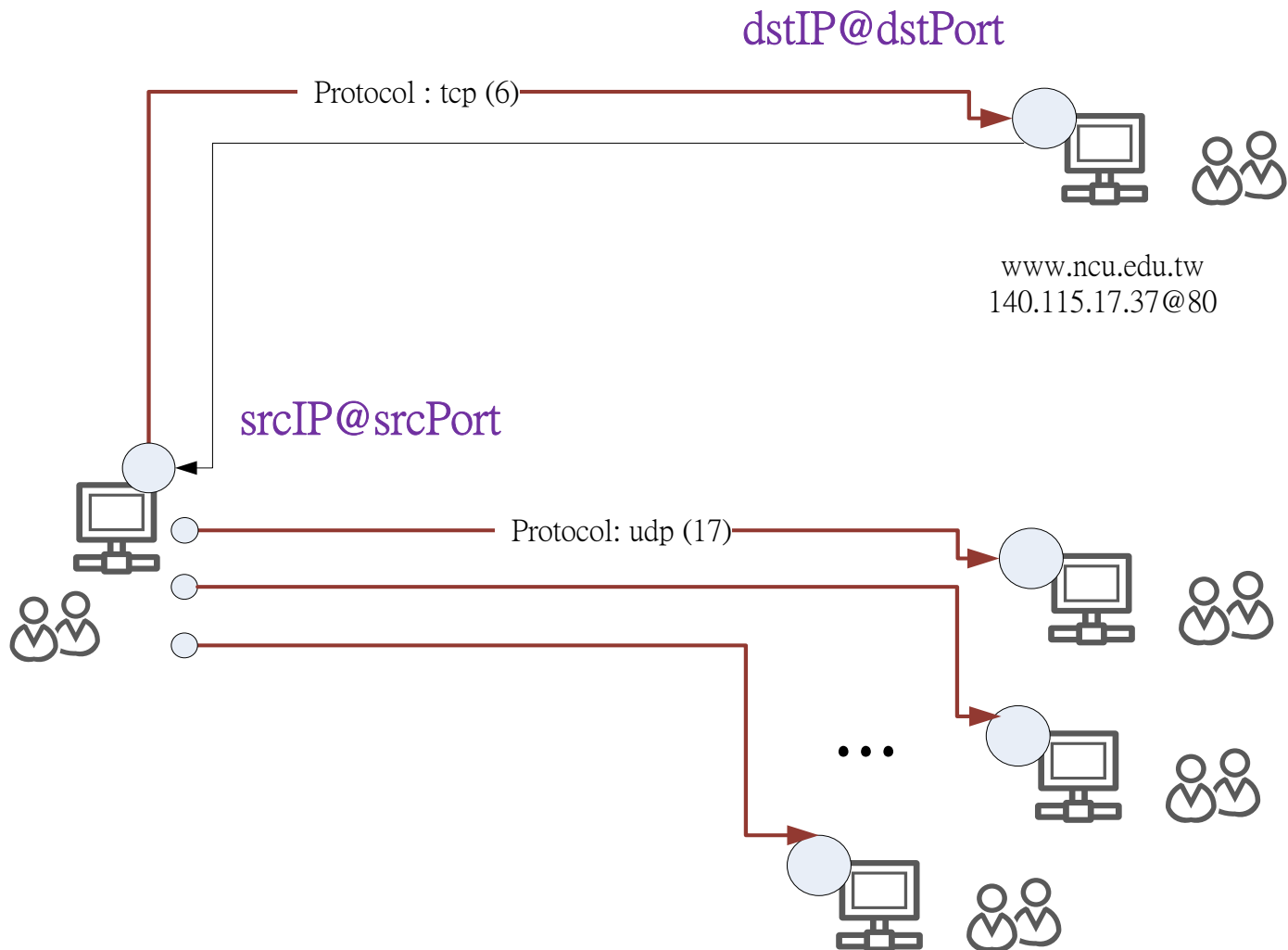


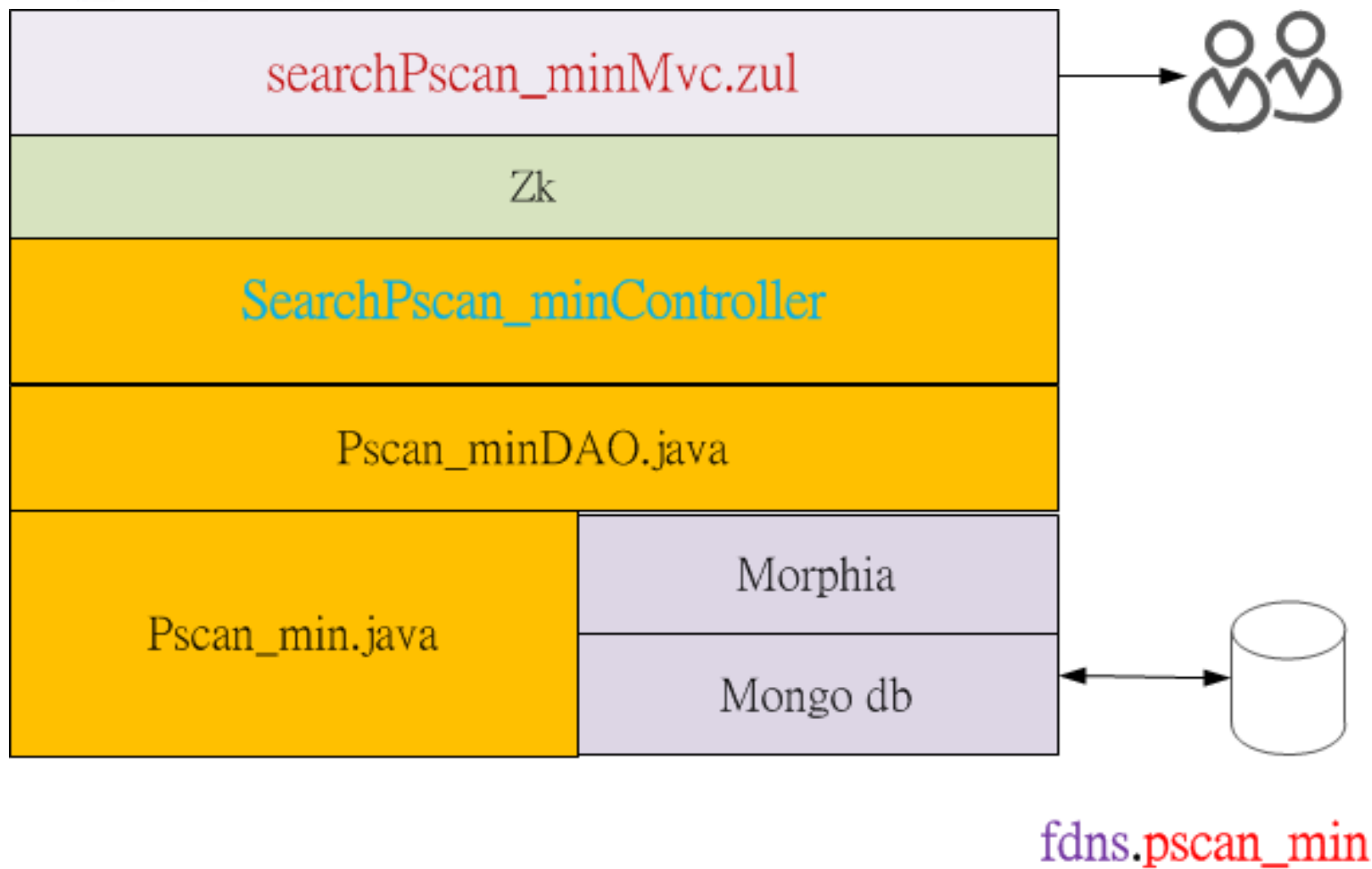
	最大	平均	目前
區網 ==> 縣網:	249.3 Mb/秒 (83.1%)	75.3 Mb/秒 (25.1%)	188.2 Mb/秒 (62.7%)
縣網 ==> 區網:	217.5 Mb/秒 (72.5%)	51.0 Mb/秒 (17.0%)	30.0 Mb/秒 (10.0%)



Fdns 架構 (Pscan_min 例)









TopN 流量監測

TopN 流量排行

Top 連接數量排行

UDP 流量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

Udp 流量 (10分鐘)

Udp 流量 (小時)

UDP Flooding 流量監看

UDP Flooding 異常流量

PortScan 流量 (per-10分鐘)

Keyword:

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.124.84.36@443	540	48	12056	17321	1171	122	04-22 15:00
120.124.84.36@80	2857	29	6114	10285	1401	80	04-22 15:00
120.125.11.202@443	794	202	16836	24421	1073	418	04-22 15:00
120.125.11.202@80	1807	56	12577	18376	1442	84	04-22 15:00
120.125.11.230@443	1286	503	47130	67390	915	366	04-22 15:00
120.125.11.230@80	4527	129	33772	47080	1438	86	04-22 15:00
120.125.120.115@25	3	3	10064	16762	81	50	04-22 15:00
163.25.155.5@443	192	18	3867	7555	1172	118	04-22 15:00
163.25.34.254@443	267	61	12619	25775	1048	189	04-22 15:00
163.25.34.254@80	1405	48	7880	17372	1389	68	04-22 15:00
163.25.34.50@443	549	625	6323	14408	872	795	04-22 15:00
163.25.34.50@80	6466	110	5336	13451	1493	54	04-22 15:00
163.30.178.45@443	120	13	4280	5322	1160	146	04-22 15:00

國立中央大學 電算中心



4. UDP Flooding 流量偵測

□ Target UDP Flooding

- appServ flooding (per-10-minute)
 - Output Packet Size \sim 1500 B/pkt
 - Output flow count > 10000
- Bandwidth Flooding
 - Output Udp Traffic > 5 GB
- Resource Flooding
 - Output Packet Size < 80 B/pkt
 - Output flow count > 100000
- Connection Flooding
 - Output flow count > 100000
- Packet Flooding
 - Output packet count > 1000000



Mongo/Morphia 篩選規則例

(10-minute Udp Traffic)

```
public static List<Udp_min> getAllKscore() throws
UnknownHostException {
    // Datastore ds = getDatastore();
    Query<Udp_min> q= ds.createQuery(Udp_min.class);
    q.or(
        q.and(
            q.criteria("psz_out").greaterThan(1495),
            q.criteria("cnt_out").greaterThan(10000)
        ),
        q.and(
            q.criteria("cnt_out").greaterThan(10000),
            q.criteria("psz_in").lessThanOrEqualTo(80),
            q.criteria("psz_out").lessThanOrEqualTo(80)
        ),
        q.criteria("sum_out").greaterThan(5000),
        q.criteria("cnt_out").greaterThan(100000)
    );
    return q.asList();
}
```

TANet 桃園區網 異常流量監測

Tyrc UDP Flooding 偵測

Keyword: 163.30.154

🔍 Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
163.30.196.253@17	0	6	0	126270	46	50	04-13 20:20
163.30.196.253@17	0	9	0	181984	176	50	04-13 20:30
120.125.2.67@17	0	8993	0	20	245	600	04-13 21:20
163.25.26.150@17	12	6159	5	10	46	468	04-13 01:40
140.115.30.31@17	0	3175	0	300064	125	1304	04-13 02:00
140.115.30.31@17	0	3987	0	303333	64	1299	04-13 02:10
163.25.26.150@17	12	6364	7	8	46	468	04-13 02:10
140.115.30.31@17	0	1579	0	142819	70	1303	04-13 02:20
163.25.26.150@17	4	5572	31	31	46	468	04-13 02:50
163.25.26.150@17	1	5075	28	50	46	468	04-13 05:30
140.115.170.248@17	0	5165	0	71	426	468	04-13 12:10
120.125.2.67@17	0	6433	0	20	270	600	04-13 12:50
163.25.131.1@17	0	20193	0	12	70	1028	04-13 15:10
163.25.131.1@17	0	6214	0	16	64	1028	04-13 15:20


Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://163.25.255.31/Fdns/ 20140402.png (PNG Image, 1000 x... x) TopN 連結監看

163.25.255.31/Fdns/ ☆ Yahoo

Most Visited Getting Started



TANet 桃園區網 異常流量監測

TopN 流量監測

TopN 流量排行

Top 連接數量排行

UDP 流量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

Udp 流量 (10分鐘)

Udp 流量 (小時)

UDP Flooding 流量監看

UDP Flooding 異常流量

Tyrc UDP Flooding 偵測

Keyword: 163.30.154

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
163.30.154.129@17	0	25	0	232940	69	108	04-13 17:50
163.30.154.129@17	0	25	0	501966	97	50	04-13 18:20
163.30.154.129@17	0	125	0	1151491	131	108	04-13 18:30
163.30.154.129@17	0	77	0	714677	1148	108	04-13 18:40
163.30.154.129@17	0	132	0	1214887	565	108	04-12 06:10
163.30.154.129@17	0	13	0	122804	565	108	04-12 06:20
163.30.154.129@17	0	37	0	341436	143	108	04-12 16:30
163.30.154.129@17	0	156	0	1433489	132	108	04-12 00:20

國立中央大學 電算中心

TANet 桃園區網 TopN 流量監測

[\[區網連線學校 MRTG流量\]](#)
[\[區網 IPv6 MRTG流量\]](#)
[\[區網 Links 連線狀態偵測\]](#)
[\[網管工具箱\]](#)
[\[區網伺服器主機檢索系統\]](#)

UDP Flooding 偵測 (Kscore)

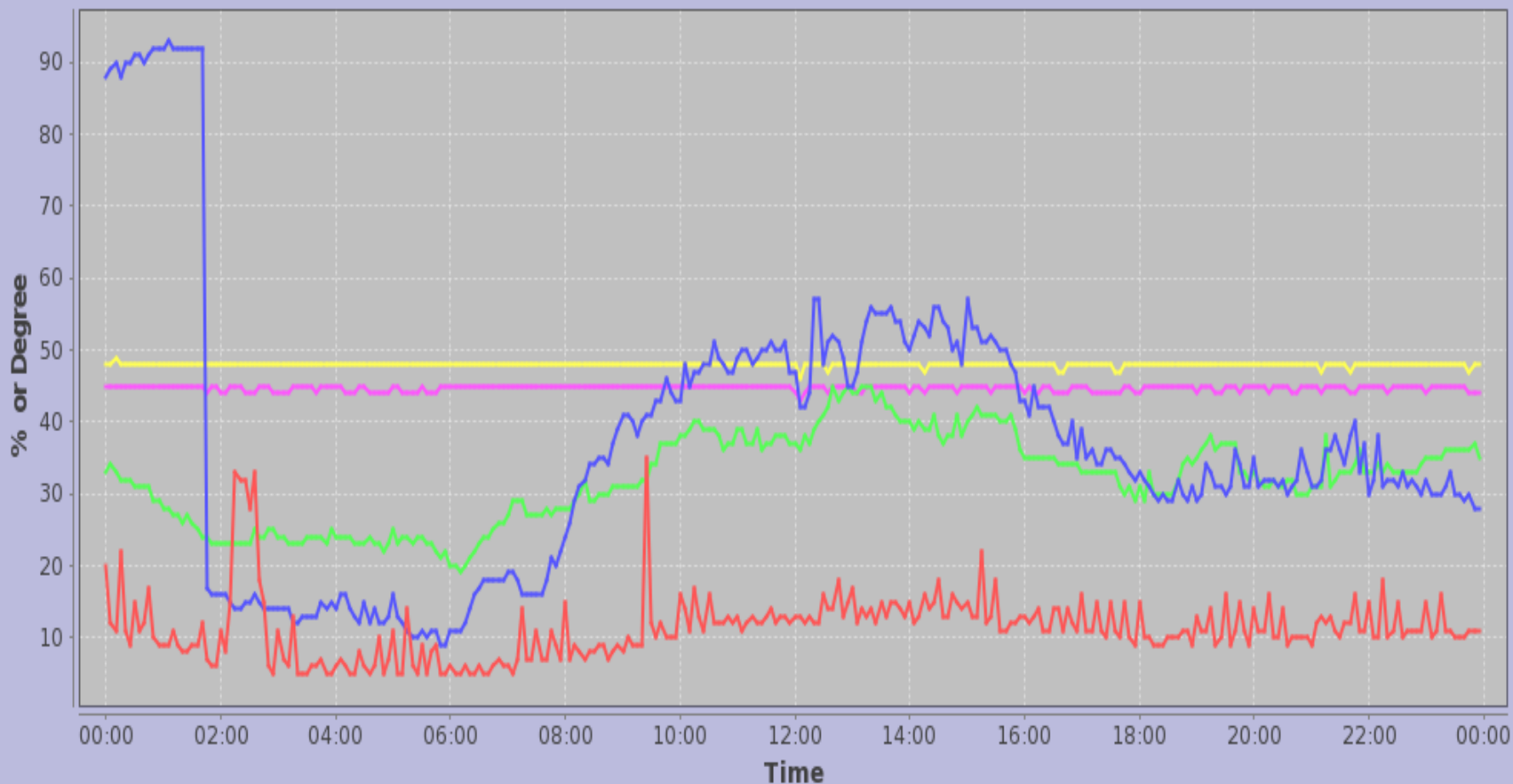
Keyword:

Q Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.125.85.166@17	0	1804	0	71219	0	1393	05-01 04:50
120.125.85.166@17	0	4685	0	81128	0	1376	05-01 04:40
120.125.85.166@17	0	3268	0	80847	0	1382	05-01 04:30
120.125.85.166@17	0	3255	0	76953	0	1381	05-01 04:10
120.125.85.166@17	0	2472	0	70559	0	1385	05-01 04:00
120.125.85.166@17	0	3354	0	79880	0	1381	05-01 03:50
120.125.85.166@17	0	295	0	49251	0	1500	05-01 03:40
140.115.8.220@17	0	4446	0	103938	0	1317	05-01 01:30
140.115.8.220@17	0	2327	0	111485	0	1325	05-01 01:20
140.115.8.220@17	0	2326	0	104407	0	1324	05-01 01:10
140.115.8.220@17	0	4434	0	98618	0	1317	05-01 01:00
140.115.8.220@17	0	2295	0	89948	0	1322	05-01 00:50
140.115.8.220@17	0	3309	0	90727	0	1319	05-01 00:40
140.115.8.220@17	0	4405	0	76696	0	1316	05-01 00:30

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2014-05-01)

系統運作溫度 不可過高, Session使用率 不可過高



—cpu 使用率 (mgt) —cpu 使用率 (data) —Session 使用率 —高溫 —低溫



5. Pandora 異常流量

☐ KMPlayer 安裝

- 未 unmask “Pandora tv” 選項
- Malwarebytes starts blocking 111.111.111.111 about every 60 seconds.

☐ hook up with something called Pandora

- The player has added a directory,
 - Pandora TV
 - KMPlayerservice.exe

☐ Uninstall “Pandora tv”

桃園區網 TopN 流量監測

[\[桃園區網 TopN 流量偵測\]](#)
[\[中央大學 TopN 流量偵測\]](#)
[\[桃園區網 Links 連線狀態偵測\]](#)
[\[網管工具箱\]](#)
[\[桃園區網\]](#)

輸入量(MB)	輸出量	輸入連結量	輸出連結量	輸入封包長度	輸出封包長度	紀錄時間
0	42252	0	678	0	50	04-29 10:00
0	44328	0	707	0	50	04-29 10:00
0	42844	0	696	0	50	04-29 10:00
0	42536	0	696	0	50	04-29 10:00
0	85240	0	1410	0	50	04-29 10:00
0	49228	0	867	0	49	04-29 10:00
0	127964	0	2310	0	49	04-29 10:00
0	232848	0	4411	0	48	04-29 10:00
0	41664	0	638	0	48	04-29 10:00
0	39744	0	631	0	48	04-29 10:00
0	54436	0	780	0	50	04-29 10:00
0	44408	0	659	0	52	04-29 10:00



6. 結語

□ 校園網路（中央大學例）

- Resource 耗損
 - IPS/Router/Firewall Overload
- 連線速度超級慢
 - BW, Connections,
- 校內主機 大量 crack 成群主機 accounts

□ 區域聯防

- 連線 機關/學校
- 外部攻擊(非 tw. Domian)
 - 即時攔阻 Blocking, 自動開單 Notification (Auto.)





6. 結語 (cont.)

□ TANET 整體 布局

➤ TANET 出國連網 ***

- IPS/Router/Firewall Resource 耗損
- 連線速度超級慢
- 外部超量攻擊 攔阻 (非 tw. Domian)

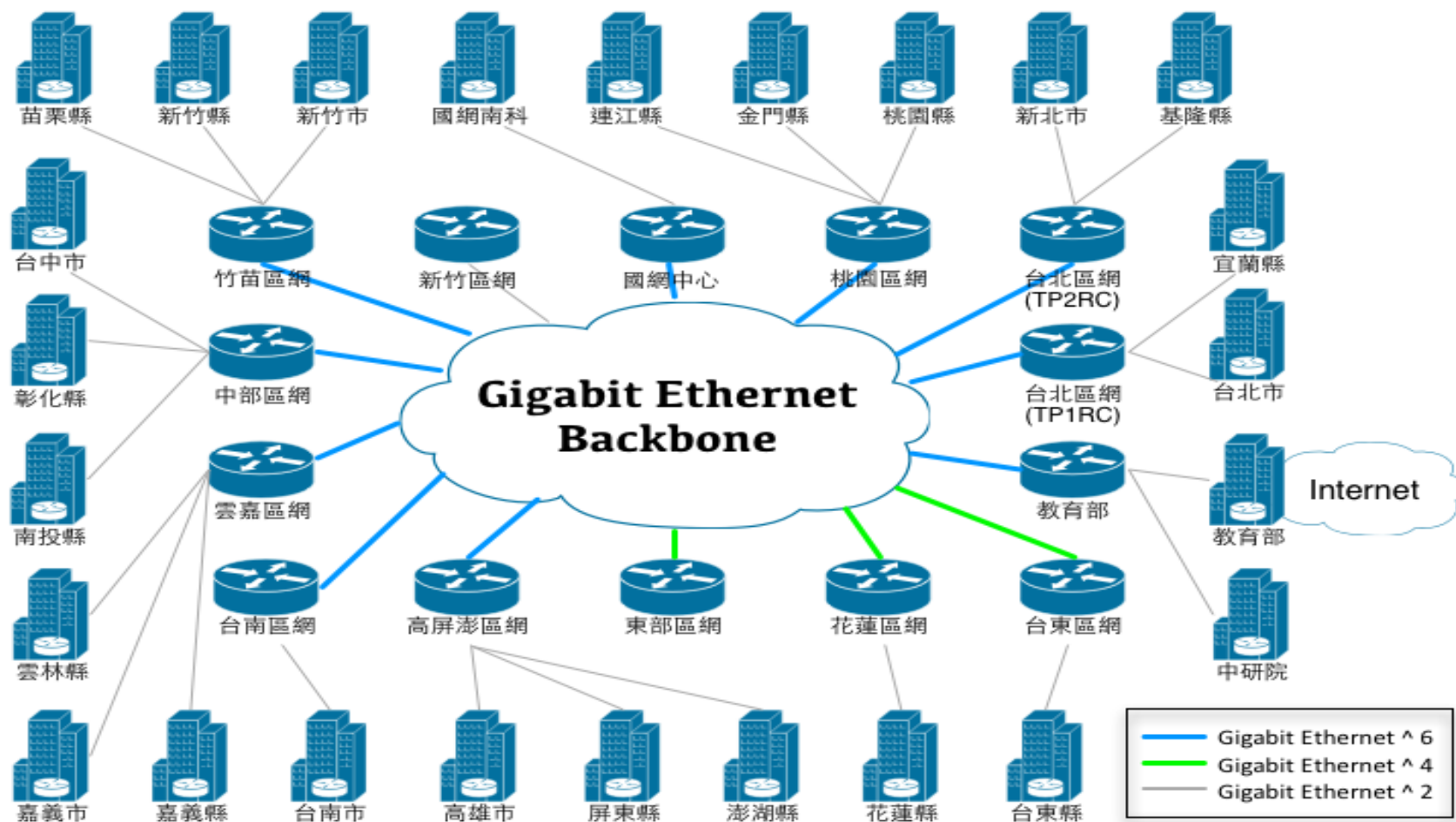
➤ 主要 區網/縣網中心

- Mongo DB cluster
 - Shard_tyrc, shard_moe,
- Data Mining
 - 即時攔阻 Blocking, 自動開單 Notification (Auto.)

6. 結語 (cont.)

TANet 骨幹網路架構圖

August, 2012





附錄

□ A1. Preparation

- Hadoop installation, Mongo installation
- Maven installation, Tomcat installation
- Integrate Spring, zk

□ A2. NetFlow 轉送紀錄

- srcIP, dstIP, srcPort, dstPort, protocol
- Flow_count, Packet count

□ A3. FDNS Traffic Aggregation

- Port scan, Udp flooding
- TopN Traffic List

A1. Preparation

- Xen Server (6.1 version)
 - On PC
 - On Blade server
- XenCenter
 - new VM
 - export VM
 - import VM
- Virtual machine
 - CentOS 64-bits (6.3 version)

A1. Preparation (cont.)

– JDK installation

- cd /opt
- Download jdk-7u51-linux-x64.tar.gz
 - <http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html>
- tar zxvf jdk-7u51-linux-x64.tar.gz
- vi **/etc/profile** or **/etc/bashrc**
 - **\$JAVA_HOME**
 - **\$PATH**
 - **\$CLASSPATH**

A1. Preparation (cont.)

/etc/profile

...

HADOOP_HOME=/opt/hadoop

TOMCAT_HOME=/opt/apache-tomcat-7.0.50

MAVEN_HOME=/opt/apache-maven-3.1.1

JAVA_HOME=/opt/jdk1.7.0_51

CLASSPATH=/opt/jdk1.7.0_51/lib:/opt/jdk1.7.0_51/jre/lib:/opt/apache-tomcat-7.0.50/lib:/opt/zk:/opt/hadoop/lib:.

PATH=\$PATH:/usr/sbin:/opt/jdk1.7.0_51/bin:/opt/apache-maven-3.1.1/bin:/opt/apache-tomcat-7.0.50/bin:/opt/hadoop/bin:.

export PATH USER LOGNAME JAVA_HOME TOMCAT_HOME ANT_HOME LOG4J_HOME HADOOP_HOME CLASSPATH

export TMOUT DISPLAY MAVEN_HOME

export LANG=zh_TW.UTF-8

export LC_CTYPE=zh_TW.UTF-8

...

A1. Preparation (cont.)

- **Hadoop** installation

- Hadoop tutorial

- http://trac.nchc.org.tw/cloud/wiki/Hadoop_Lab1

- `cd /opt`

- `yum -y install openssh rsync`

- `vim /etc/ssh/ssh_config`
 - `ssh-keygen -t rsa -f ~/.ssh/id_rsa -P ""`
 - `cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys`

- `wget http://apache.mesi.com.ar/hadoop/common/hadoop-1.2.1/hadoop-1.2.1.tar.gz`

- `tar zxvf hadoop-1.2.1.tar.gz`

- `mv hadoop-1.2.1 hadoop`

- `/opt/hadoop/conf`

- `core-site.xml, hadoop-env.sh, mapred-site.xml`

- **`hadoop namenode -format`**

- **`Hadoop dfsadmin -safemode leave`**

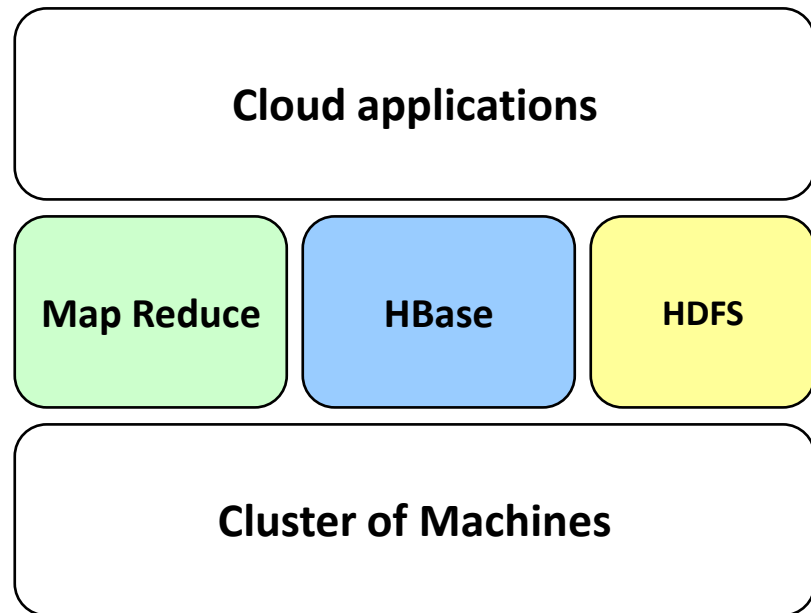
- `/opt/hadoop/bin`

- `start-all.sh, stop-all.sh`

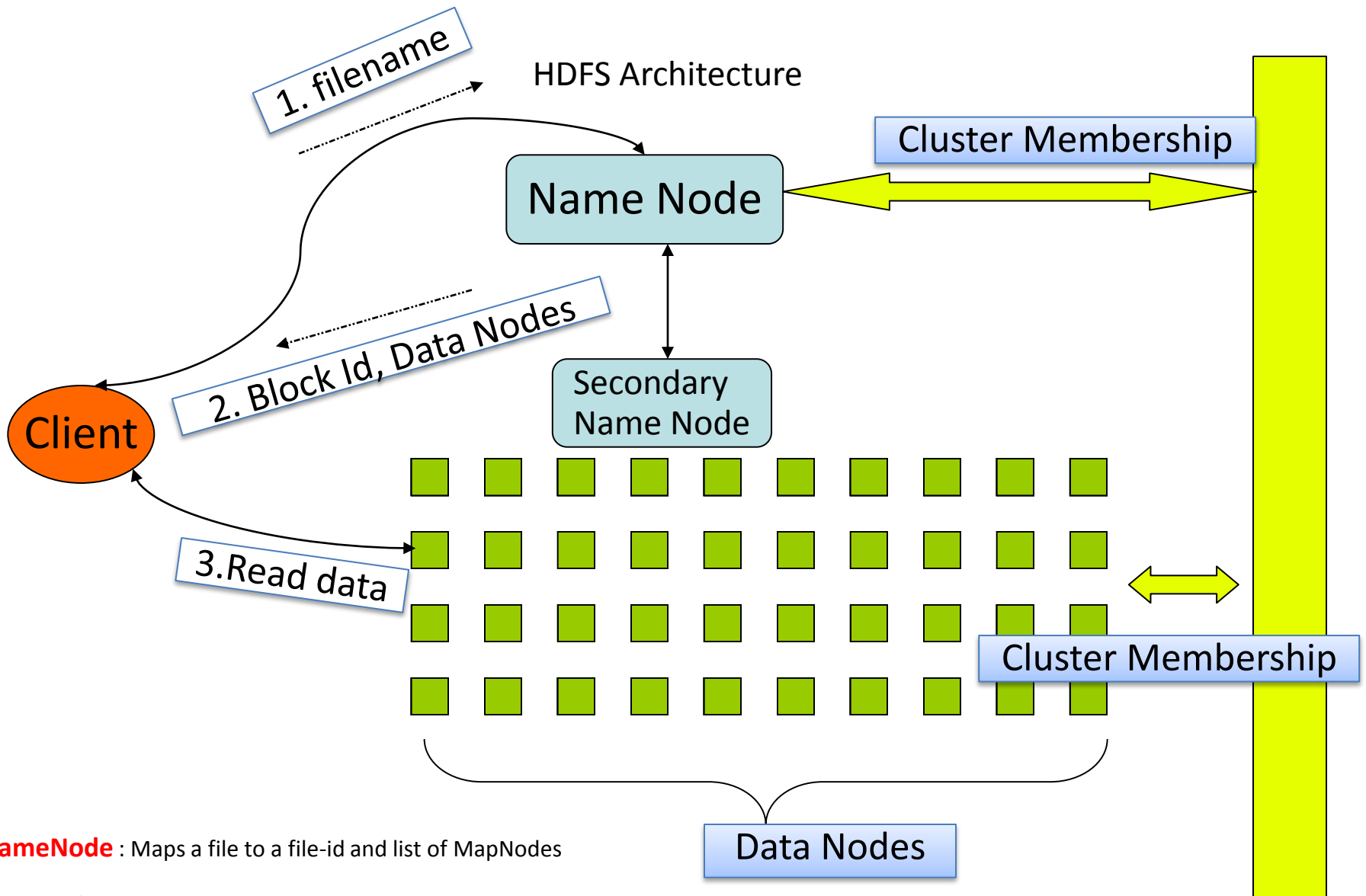
A1. Preparation (cont.)



- provides a framework for large scale parallel processing
 - distributed file system
 - map-reduce programming paradigm.
- **Open source project**
- Written by Java
- Runs on
 - **Linux**, Mac OS/X,
 - Windows, Solaris
 - Commodity hardware



HDFS Architecture



NameNode : Maps a file to a file-id and list of MapNodes

DataNode : Maps a block-id to a physical location on disk

SecondaryNameNode: Periodic merge of Transaction log

A1. Preparation (cont.)

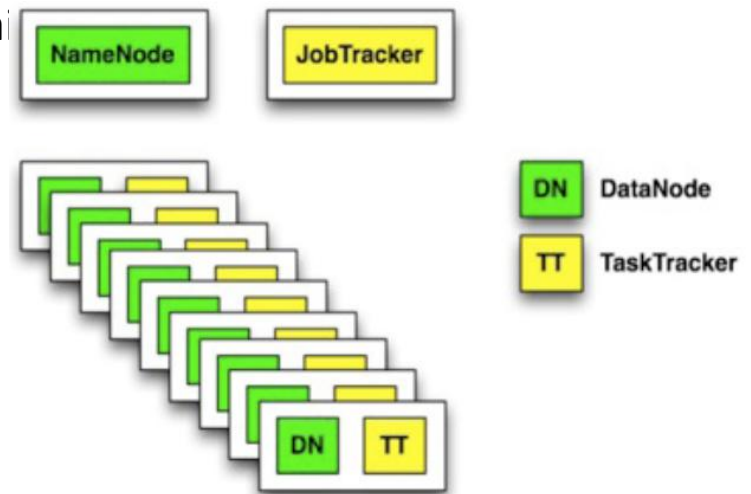
- **# /opt/hadoop/bin/start-all.sh**
 - starting namenode, logging to /opt/hadoop/logs/hadoop-yang-namenode-centos-2-31.out
 - 140.115.2.31: starting datanode, logging to /opt/hadoop/logs/hadoop-root-datanode-centos-2-31.out
 - 140.115.2.31: starting secondarynamenode, logging to /opt/hadoop/logs/hadoop-root-secondarynamenode-centos-2-31.out
 - starting jobtracker, logging to /opt/hadoop/logs/hadoop-yang-jobtracker-centos-2-31.out
 - 140.115.2.31: starting tasktracker, logging to /opt/hadoop/logs/hadoop-root-tasktracker-centos-2-31.out
- **# jps**
 - **28844 DataNode**
 - 28974 SecondaryNameNode
 - **27588 NameNode**
 - **29193 TaskTracker**
 - 29272 Jps
 - **27936 JobTracker**
 - 24521 Bootstrap
- **# /opt/hadoop/bin/stop-all.sh**

A1. Preparation (cont.)

- **MapReduce**
 - Software framework introduced by Google
 - Support distributed computing on large data sets on clusters of computers.
 - computing certain kinds of distributable problems using a large number of computers (nodes), collectively referred to as a cluster.
- Examples
 - Large data processing
 - Search, Indexing, Sorting
 - Data mining and machine learning in large data set
 - Huge access logs analysis in large portals

A1. Preparation (cont.)

- MapReduce framework consists of
 - master JobTracker
 - slave TaskTracker per cluster node.
- JobTracker is responsible for
 - **scheduling** the jobs' component tasks on the slaves
 - **monitoring** them and re-executing the failed tasks
- TaskTrackers execute the tasks

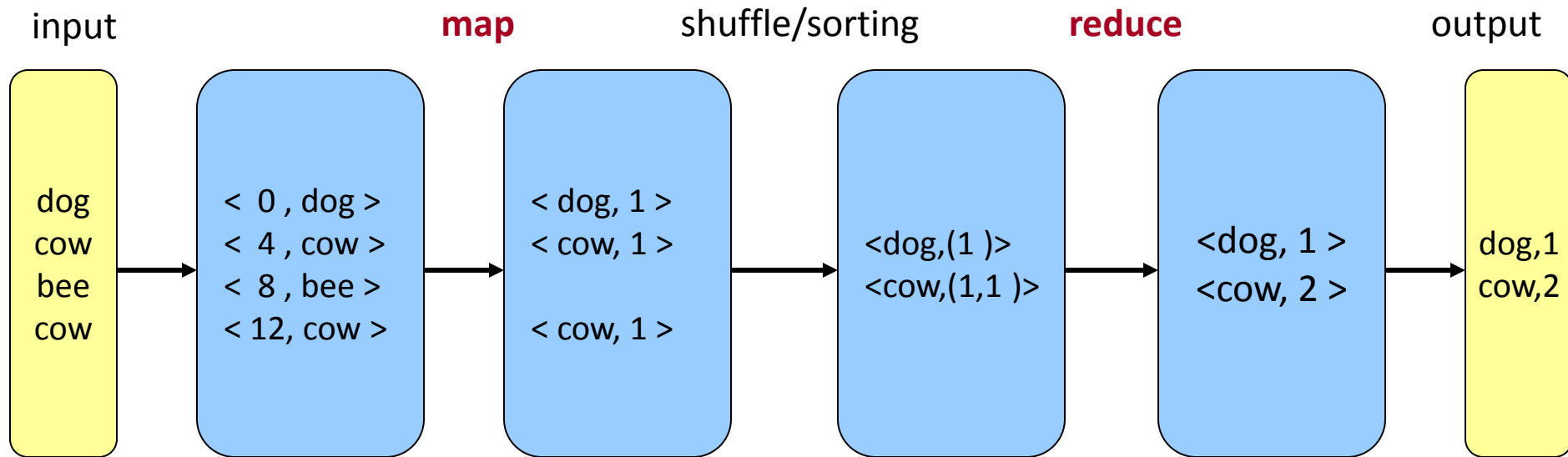


A1. Preparation (cont.)

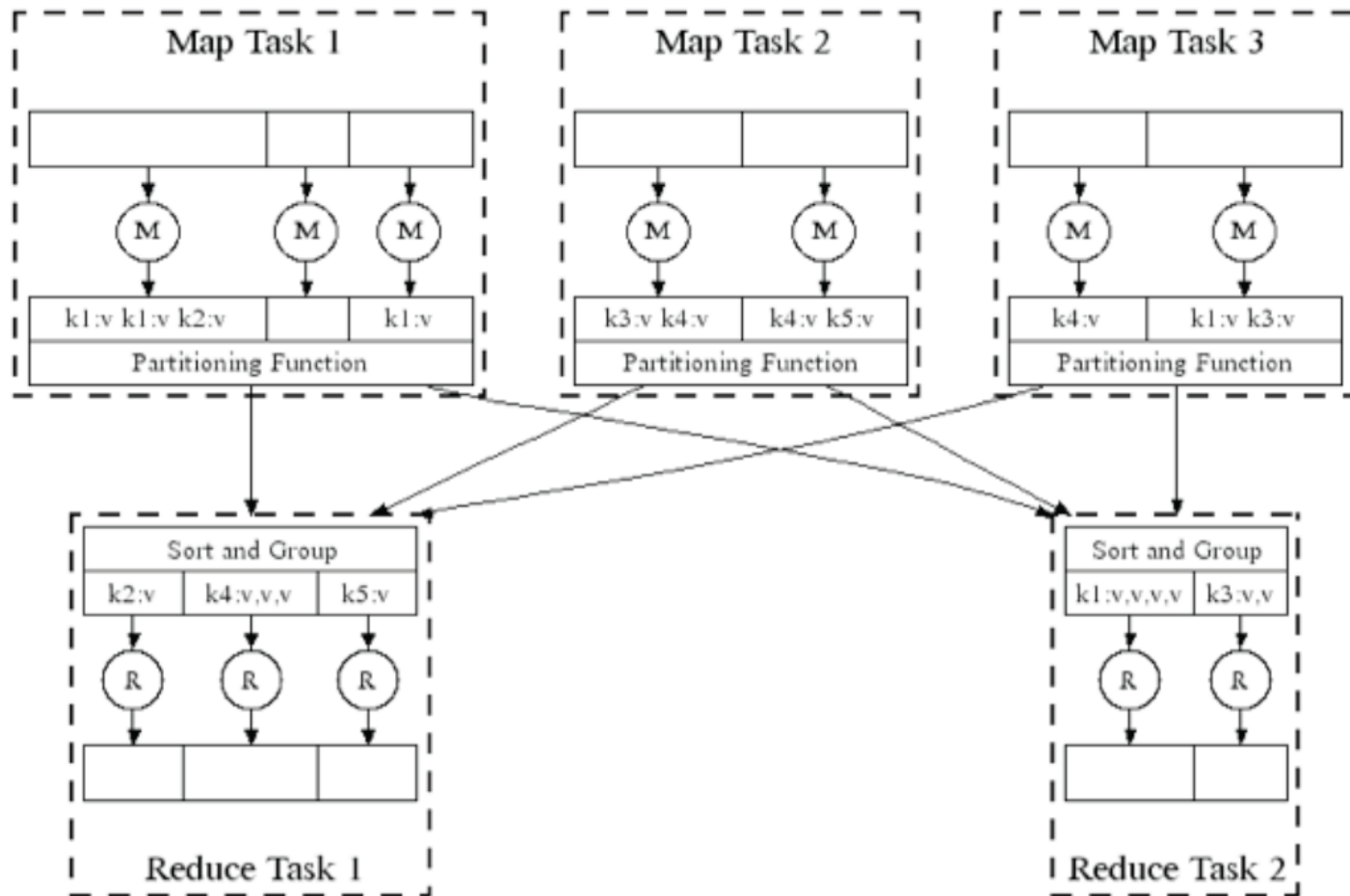
- **MapReduce Programming Model**

- User define two functions
- **map** $(K1, V1) \rightarrow \text{list}(K2, V2)$
 - takes an input pair
 - produces a set of intermediate key/value
- **reduce** $(K2, \text{list}(V2)) \rightarrow \text{list}(K3, V3)$
 - accepts an intermediate key and a set of values
 - merges together these values to form a possibly smaller set of values

A1. Preparation (cont.)



Execution flow of a MapReduce



A1. Preparation (cont.)

- `hadoop fs -ls`
 - 與Linux裡面的ls類似
- `hadoop fs -put src_name dst_name`
 - 把檔案src上傳到HDFS並取名為dst_name
- `hadoop fs -get src_name dst_name`
 - 從HDFS上面下載檔案回來
- `hadoop jar XX.jar <input_file> <out_dir>`
 - 執行hadoop任務

A1. Preparation (cont.)

```
import java.io.IOException;
import java.util.*;
import org.apache.hadoop.fs.Path;
import org.apache.hadoop.conf.*;
import org.apache.hadoop.io.*;
import org.apache.hadoop.mapred.*;
import org.apache.hadoop.util.*;
```

```
public class WordCount
```

```
{
    public static class Map extends MapReduceBase implements Mapper<LongWritable, Text, Text,
    IntWritable> { ... }

    public static class Reduce extends MapReduceBase implements Reducer<Text, IntWritable, Text,
    IntWritable> { ... }

    public static void main(String[] args) throws Exception { ... }
}
```

A1. Preparation (cont.)

```
public static void main(String[] args) throws Exception
{
    JobConf conf = new JobConf(WordCount.class);
    conf.setJobName("wordcount");
    conf.setOutputKeyClass(Text.class);
    conf.setOutputValueClass(IntWritable.class);
    conf.setMapperClass(Map.class);
    conf.setCombinerClass(Reduce.class);
    conf.setReducerClass(Reduce.class);
    conf.setInputFormat(TextInputFormat.class);
    conf.setOutputFormat(TextOutputFormat.class);
    FileInputFormat.setInputPaths(conf, new Path(args[0]));
    FileOutputFormat.setOutputPath(conf, new Path(args[1]));
    JobClient.runJob(conf);
}
```

```
private final static IntWritable one = new IntWritable(1);
private Text word = new Text();
public void map(LongWritable key, Text value, OutputCollector<Text, IntWritable> output,
    Reporter reporter) throws IOException
{
    // 從分派的input之中擷取一行
    String line = value.toString();
    //tokenize
    StringTokenizer tokenizer = new StringTokenizer(line);
    while (tokenizer.hasMoreTokens())
    {
        //把此token包成一個word
        word.set(tokenizer.nextToken());
        //再把word與權重(這邊是出現次數)包成<key, value>的型式
        output.collect(word, one);
    }
}
```

A1. Preparation (cont.)

```
public void reduce(Text key, Iterator<IntWritable> values, OutputCollector<Text,
    IntWritable> output, Reporter reporter) throws IOException
{
    int sum = 0;
    while (values.hasNext())
    {
        // 將mapper或別的reducer傳來的value加總
        sum += values.next().get();
    }
    // 輸出<key, value>的結果
    output.collect(key, new IntWritable(sum));
}
```

```

import java.io.IOException;
import java.util.*;
import org.apache.hadoop.fs.Path;
import org.apache.hadoop.conf.*;
import org.apache.hadoop.io.*;
import org.apache.hadoop.mapred.*;
import org.apache.hadoop.util.*;

public class WordCount {
    public static class Map extends MapReduceBase implements Mapper<LongWritable, Text, Text, IntWritable> {
        private final static IntWritable one = new IntWritable(1);
        private Text word = new Text();
        public void map(LongWritable key, Text value, OutputCollector<Text, IntWritable> output, Reporter reporter) throws IOException {
            String line = value.toString();
            StringTokenizer tokenizer = new StringTokenizer(line);
            while (tokenizer.hasMoreTokens()) {
                word.set(tokenizer.nextToken());
                output.collect(word, one);
            }
        }
    }

    public static class Reduce extends MapReduceBase implements Reducer<Text, IntWritable, Text, IntWritable> {
        public void reduce(Text key, Iterator<IntWritable> values, OutputCollector<Text, IntWritable> output, Reporter reporter) throws IOException {
            int sum = 0;
            while (values.hasNext()) {
                sum += values.next().get();
            }
            output.collect(key, new IntWritable(sum));
        }
    }

    public static void main(String[] args) throws Exception {
        JobConf conf = new JobConf(WordCount.class);
        conf.setJobName("wordcount");
        conf.setOutputKeyClass(Text.class);
        conf.setOutputValueClass(IntWritable.class);
        conf.setMapperClass(Map.class);
        conf.setCombinerClass(Reduce.class);
        conf.setReducerClass(Reduce.class);
        conf.setInputFormat(TextInputFormat.class);
        conf.setOutputFormat(TextOutputFormat.class);
        FileInputFormat.setInputPaths(conf, new Path(args[0]));
        FileOutputFormat.setOutputPath(conf, new Path(args[1]));
        JobClient.runJob(conf);
    }
}

```

A1. Preparation (cont.)

```
## make.sh
```

```
#!/bin/sh
```

```
cd /home1/wordcount
```

```
mkdir bin
```

```
javac -classpath /opt/hadoop/hadoop-core-1.2.1.jar -d bin WordCount.java
```

```
jar -cvf wc.jar -C bin/ .
```

A1. Preparation (cont.)

```
## run.sh
```

```
#!/bin/sh
```

```
cd /home1/wordcount
```

```
rm -fr output/*
```

```
hadoop dfs -rmr output
```

```
hadoop dfs -mkdir input
```

```
hadoop fs -put file* input
```

```
hadoop jar wc.jar WordCount input output
```

```
hadoop fs -get output/* output
```

```
cat output/*
```

A1. Preparation (cont.)

```
# cat output/part-00000
```

```
2014-02-05    1
Happy  4
again  4
hadoop 1
ncu    1
new    4
test   5
yang   1
year   4
```

察看 wordcount 執行結果

A1. Preparation (cont.)

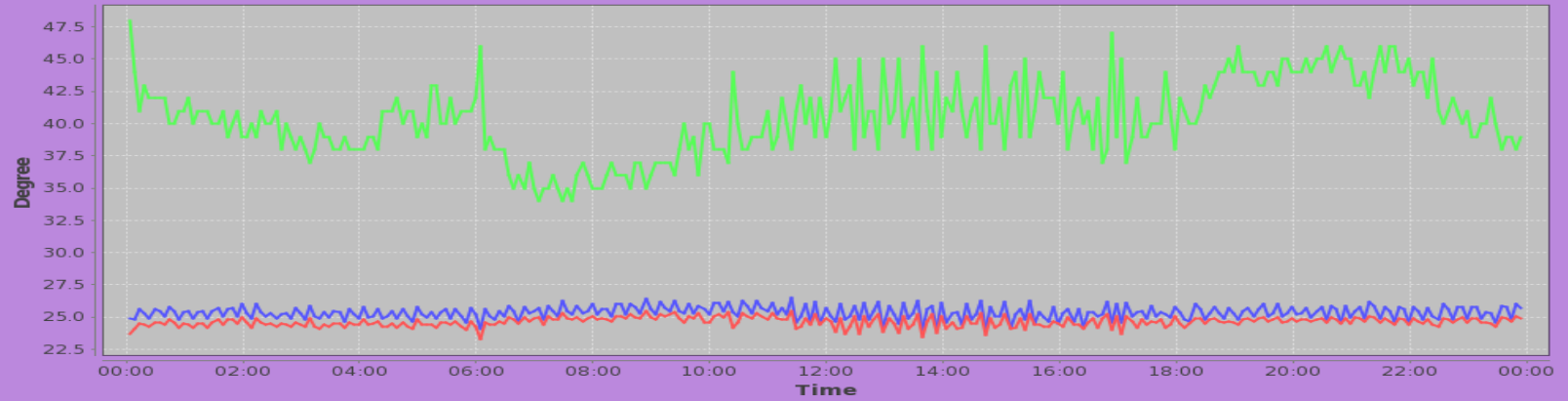
- **mongo** db installation
 - vi /etc/yum.repos.d/mongodb.repo
 - [10gen]
 - name=10gen Repository
 - baseurl=http://downloads-distro.mongodb.org/repo/redhat/os/x86_64
 - gpgcheck=0
 - enabled=1
 - yum install mongo-10gen **mongo-10gen-server**
 - service mongod start
 - service mongod stop
 - chkconfig mongod on

A1. Preparation (cont.)

- Mongo shell command
 - **show dbs**
 - **use ncu**
 - `db.foo.find()`
 - `db.foo.save({a: 1})`
 - `db.foo.save({b: 4})`
 - `db.foo.save({c: 3})`
 - `db.foo.find()`
 - `{ "_id" : ObjectId("52e76ff01f71cd57cbd192da"), "a" : 1 }`
 - `db.foo.update({a: 1}, {a: 5})`
 - `db.foo.find()`
 - `{ "_id" : ObjectId("52e76ff01f71cd57cbd192da"), "a" : 5 }`
 - `db.foo.remove({a: 5})`
 - `db.foo.find()`

桃園區網機房 溫度/濕度 監看 (2013-11-09)

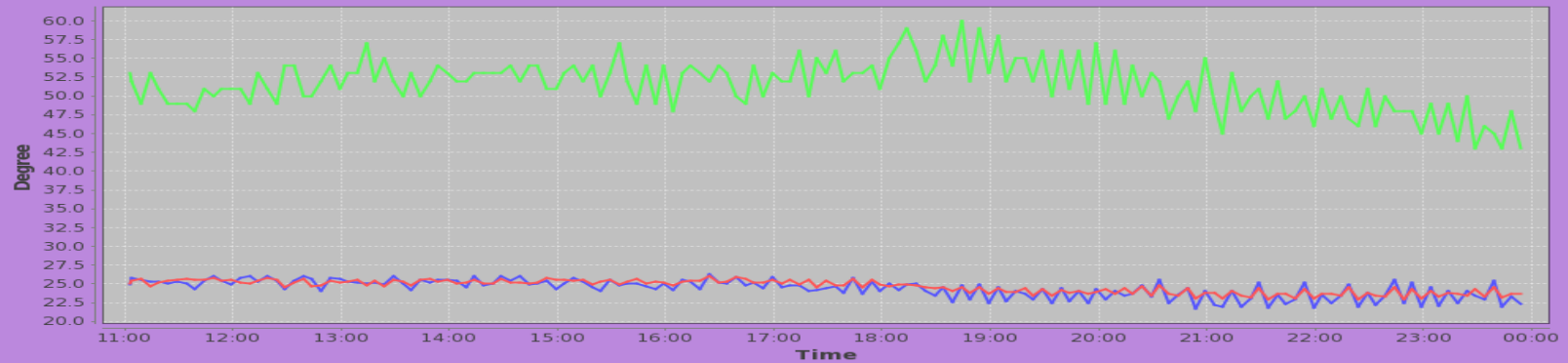
連網機房溫度 不可過高



— 溫度 (前半部) — 溫度 (後半部) — 濕度

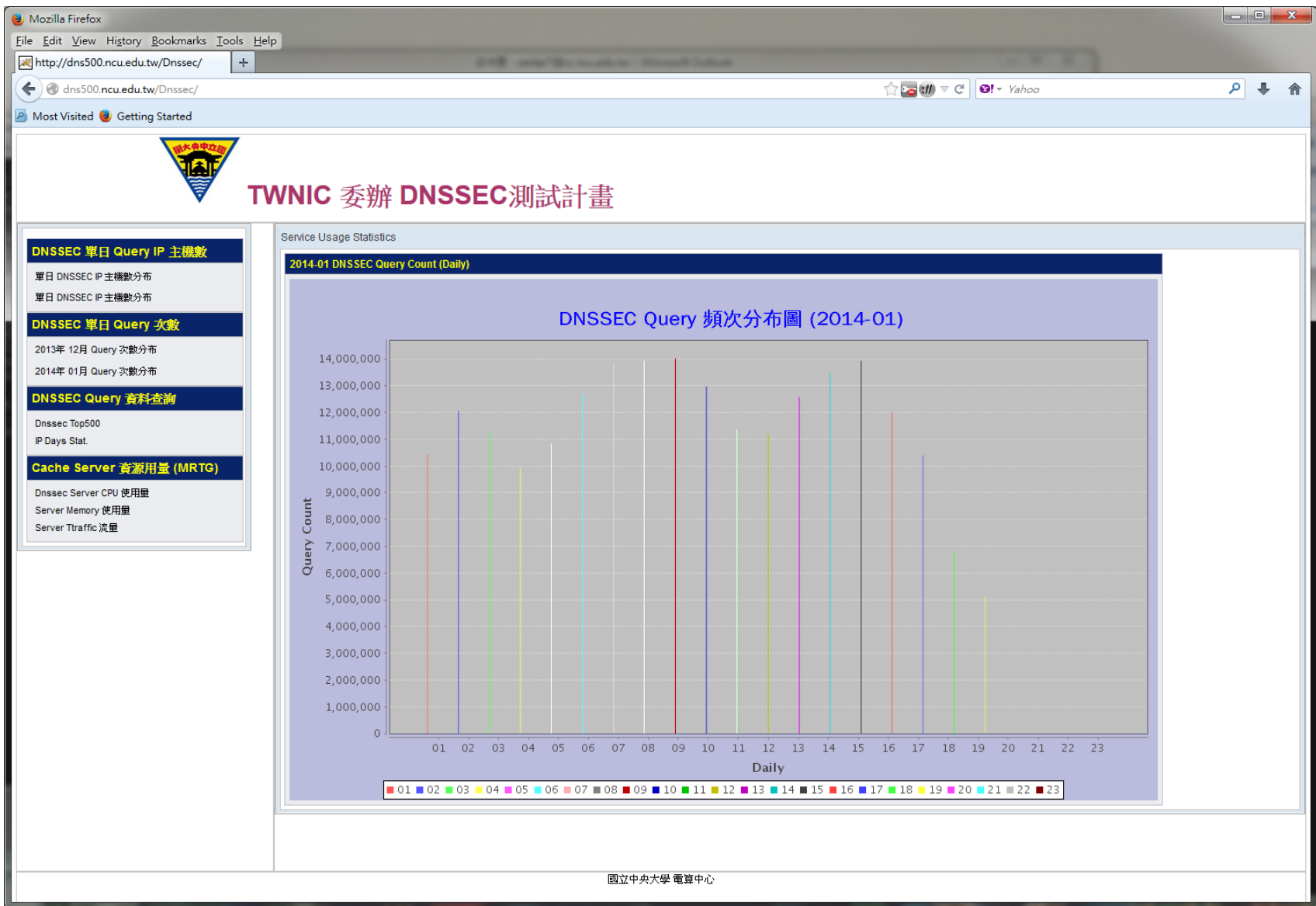
桃園區網機房 溫度/濕度 監看 (2013-12-09)

連網機房溫度 不可過高



— 溫度 (前半部) — 溫度 (後半部) — 濕度

<http://dns500.ncu.edu.tw/Dnssec/>



A1. Preparation (cont.)

- Mongo shell command
 - use todo
 - **db.dropDatabase()**
 - show collections
 - db.dnssec.remove (), db.dnssec.drop()
 - **db.dnssec.find()**
 - db.dnssec.find({dnsdate:"2013-12-10-21"})
 - db.top500.find({"secip":{"\$gte: "140.115.211"}})
 - **db.top500.remove()**
 - db.top500.remove({"secip":{"\$gte: "140.115.211"}})
 - db.dnssec.remove({"dnsdate":{"\$gte: "2013-12-25-20"}})
 - **db.top500.ensureIndex({"queryday":1})**

A1. Preparation (cont.)

- **mongoDB Backup (備份)**

- **# mongodump --db todo**
 - `ls -l ~yang/Mongo*/dump/todo`
 - `-rw-r--r--. 1 root root 163374798 2014-01-23 18:48 dnssec.bson`
 - `-rw-r--r--. 1 root root 93 2014-01-23 18:48 dnssec.metadata.json`
 - `-rw-r--r--. 1 root root 776661 2014-01-23 18:48 dormip.bson`
 - `-rw-r--r--. 1 root root 93 2014-01-23 18:48 dormip.metadata.json`
 - `-rw-r--r--. 1 root root 29452693 2014-01-23 18:48 ipinfo.bson`
 - `-rw-r--r--. 1 root root 93 2014-01-23 18:48 ipinfo.metadata.json`
 - `-rw-r--r--. 1 root root 607 2014-01-23 18:48 system.indexes.bson`
 - `-`

- **mongoDB Restore (還原)**

- **# mongorestore --collection thank --db todo dump/todo/task.bson**
- **# mongorestore --collection dormip --db todo Mongo_DB/dump/todo/dormip.bson**
 - `connected to: 127.0.0.1`
 - `Wed Feb 5 17:53:52.846 Mongo_DB/dump/todo/dormip.bson`
 - `Wed Feb 5 17:53:52.846 going into namespace [todo.dormip]`
 - **5529 objects** found
 - `Wed Feb 5 17:53:52.957 Creating index: { key: { _id: 1 }, ns: "todo.dormip", name: "_id_" }`

A1. Preparation (cont.)

- **Tomcat** installation

- Download Apache Tomcat

- cd /opt
 - wget <http://apache.mesi.com.ar/tomcat/tomcat-7/v7.0.50/bin/apache-tomcat-7.0.50.tar.gz>

- Tar zxvf apache-tomcat-7.0.50.tar.gz

- ls -l apache-tomcat-7.0.50
 - drwxr-xr-x. 2 root root 4096 2013-12-18 09:43 **bin**
 - drwxr-xr-x. 2 root root 4096 2013-10-18 18:21 **conf**
 - drwxr-xr-x. 2 root root 4096 2013-12-18 09:43 lib
 - drwxr-xr-x. 2 root root 4096 2013-10-18 18:10 logs
 - drwxr-xr-x. 2 root root 4096 2013-12-18 09:43 temp
 - drwxr-xr-x. 7 root root 4096 2013-10-18 18:19 **webapps**
 - drwxr-xr-x. 2 root root 4096 2013-10-18 18:10 work
 - /opt/apache-tomcat-7.0.50/bin/startup.sh
 - /opt/apache-tomcat-7.0.50/bin/shutdown.sh

Apache Tomcat/7.0.50 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://kscore.tyc.edu.tw/Kscore/ x Apache Tomcat/7.0.50 x +

140.115.2.31:8080


☆ Yahoo

Most Visited Getting Started

Home Documentation Configuration Examples Wiki Mailing Lists


Find Help

Apache Tomcat/7.0.50



The Apache Software Foundation
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:
[Security Considerations HOW-TO](#)
[Manager Application HOW-TO](#)
[Clustering/Session Replication HOW-TO](#)

Server Status

Manager App

Host Manager

Developer Quick Start

[Tomcat Setup](#)
[First Web Application](#)

[Realms & AAA](#)
[JDBC Data Sources](#)

[Examples](#)

[Servlet Specifications](#)
[Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 7.0 access to the manager application is split between different users.
[Read more...](#)

[Release Notes](#)
[Changelog](#)
[Migration Guide](#)
[Security Notices](#)

Documentation

[Tomcat 7.0 Documentation](#)
[Tomcat 7.0 Configuration](#)
[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

[Tomcat 7.0 Bug Database](#)
[Tomcat 7.0 JavaDocs](#)
[Tomcat 7.0 SVN Repository](#)

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

announce@tomcat.apache.org
Important announcements, releases, security vulnerability notifications. (Low volume).

users@tomcat.apache.org
User support and discussion

taglibs-user@tomcat.apache.org
User support and discussion for [Apache Taglibs](#)

dev@tomcat.apache.org
Development mailing list, including commit messages

Other Downloads

[Tomcat Connectors](#)
[Tomcat Native](#)
[Taglibs](#)
[Deployer](#)

Other Documentation

[Tomcat Connectors](#)
[mod_jk Documentation](#)
[Tomcat Native](#)
[Deployer](#)

Get Involved

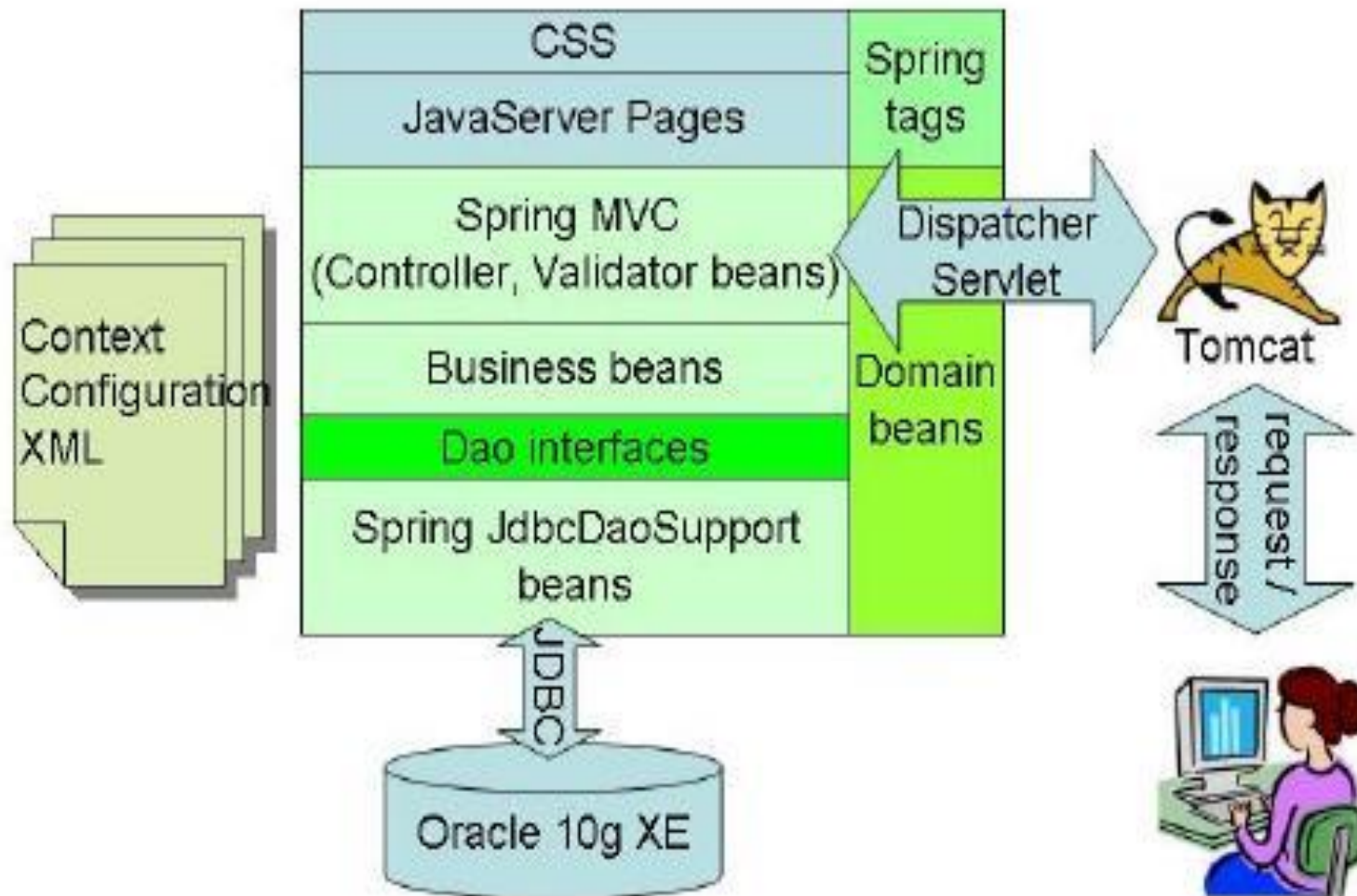
[Overview](#)
[SVN Repositories](#)
[Mailing Lists](#)
[Wiki](#)

Miscellaneous

[Contact](#)
[Legal](#)
[Sponsorship](#)
[Thanks](#)

Apache Software Foundation

[Who We Are](#)
[Heritage](#)
[Apache Home](#)
[Resources](#)



A1. Preparation (cont.)

- **maven** installation

- **Download Apache Maven 3.1.1**

- [cd /opt](#)

- wget <ftp://mirror.reverse.net/pub/apache/maven/maven-3/3.1.1/binaries/apache-maven-3.1.1-bin.tar.gz>

- tar zxvf apache-maven-3.1.1-bin.tar.gz

- ls -l apache-maven-3.1.1/bin

- -rw-r--r--. 1 root root 228 2013-09-17 23:24 m2.conf

- -rwxr-xr-x. 1 root root 5806 2013-09-17 23:24 **mvn**

A1. Preparation (cont.)

– Maven command

- mvn clean
- mvn compile
- mvn package
- mvn test

- **mvn** archetype:generate -DgroupId=ncu.app -DartifactId=ncu_app -DarchetypeArtifactId=maven-archetype-quickstart
 - ls -l ncu_app
 - -rw-r--r--. 1 root root 634 2014-01-28 14:51 **pom.xml**
 - drwxr-xr-x. 4 root root 4096 2014-01-28 14:51 src
 - ls -l ncu_app/src/main/java/ncu/app
 - -rw-r--r--. 1 root root 170 2014-01-28 14:51 App.java

A1. Preparation (cont.)

- more ncu_app/src/main/java/ncu/app/App.java
 - package ncu.app;
 - public class App {
 - public static void main(String[] args) {
 - **System.out.println("Hello World!");**
 - }
 - }
 - **mvn clean compile package**
 - ls -l target
 - » drwxr-xr-x. 3 root root 4096 2014-01-28 15:02 classes
 - » drwxr-xr-x. 2 root root 4096 2014-01-28 15:02 maven-archiver
 - » -rw-r--r--. 1 root root 2041 2014-01-28 15:02 **ncu_app-1.0-SNAPSHOT.jar**
 - » drwxr-xr-x. 2 root root 4096 2014-01-28 15:02 surefire-reports
 - » drwxr-xr-x. 3 root root 4096 2014-01-28 15:02 test-classes
 - Execution
 - **java** -cp target/ncu_app-1.0-SNAPSHOT.jar ncu.app.App
 - » Hello World!
 - **mvn exec:java** -Dexec.mainClass="ncu.app.App"
 - » Hello World!



A2. Netflow data

➤ NetFlow data

- 5-tuple record

-	srcIP	dstIP	prot	sPort	dPort	oct	pkt
-	-----						
-	96.244.49.242	140.135.230.123	6	3618	445	64	1
	96.244.49.242	140.135.59.95	6	3619	445	64	1
	96.244.49.242	140.135.148.61	6	3772	445	64	1



fetch.sh

```
#!/bin/bash
mday=`/bin/date '+%m%d'`
yday=$(date --date='1 day ago' +%m%d%H)
min=$(date --date='16 minute ago' +%H%M)
min=`expr $min / 10`
min=`expr $min \* 10`
len=${#min}
if [ $len -lt 4 ]
    then min=0$min
fi

cd /home1/Flood/rawdata

ftp -v -n lisa.tyc.edu.tw << END
user yang test_passwod
prompt off
cd /home1/rawdata
mget $mday$min
exit
END

/opt/hadoop/bin/hadoop fs -put $mday$min .
```

A3. FDNS Traffic Aggregation

➤ PortScan 特徵

- Index key

- srcIP@dstPort
- [140.115.11.11@22](#)
- 140.115.11.11@25

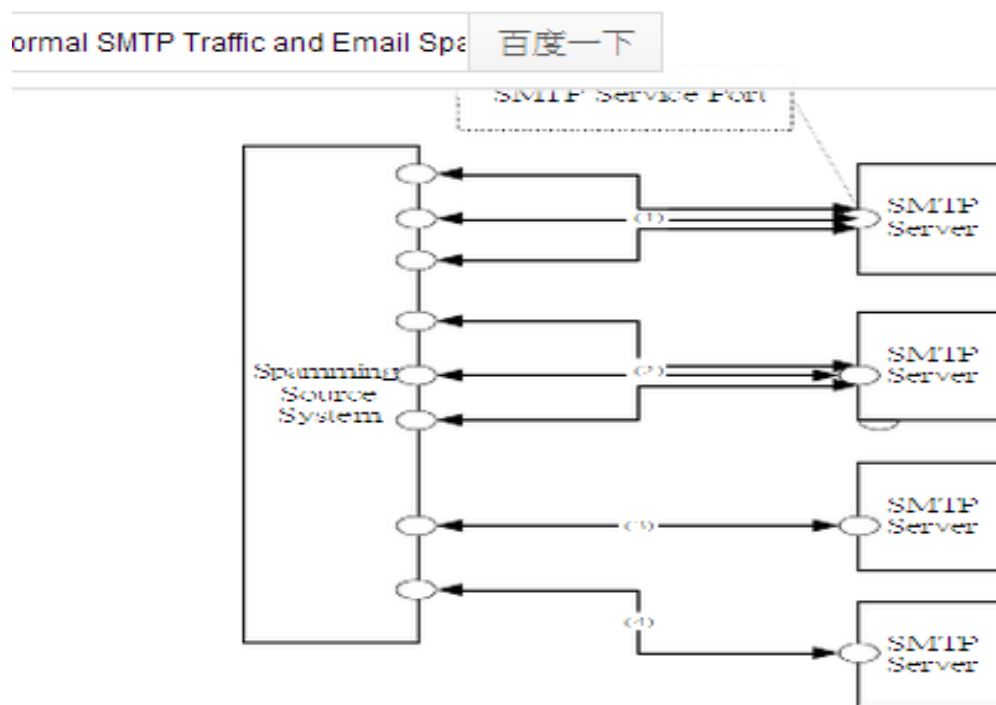


Fig. 1. SMTP flooding model.



Class map

```
public static class Map1 extends MapReduceBase implements Mapper<LongWritable, Text, Text, Text>
{
    public void map(LongWritable id, Text input, OutputCollector<Text, Text> output, Reporter reporter)
    throws IOException
    {
        StringTokenizer tokenizer = new StringTokenizer(input.toString());
        int cc = 0;
        String temp[] = new String[7];
        for (cc = 0; tokenizer.hasMoreTokens(); cc++)
        {
            temp[cc] = tokenizer.nextToken(" ");
        }

        if ( temp[0].matches("[0-9. ]+") && !temp[3].equals("53") && !temp[4].equals("53"))
        {
            output.collect( new Text(temp[0] + "@" + temp[2]), new Text("0:" + temp[5] + ":0:1:0:" + temp[6]) );
            output.collect( new Text(temp[1] + "@" + temp[2]), new Text(temp[5] + ":0:1:0:" + temp[6] + ":0") );
        }
    }
}
```



Class reduce

```
public static class Reduce1 extends MapReduceBase implements Reducer<Text, Text, Text, Text>
{
    public void reduce(Text k1, Iterator<Text> v1, OutputCollector<Text, Text> output, Reporter
reporter) throws IOException {
        Long sum_in = 0L; sum_out = 0L;
        Long pkt_in = 0L; pkt_out = 0L;
        Integer cnt_in = 0; cnt_out = 0;
        while (v1.hasNext()) {
            String[] token = v1.next().toString().split(":");
            sum_in += Long.parseLong(token[0]);
            sum_out += Long.parseLong(token[1]);
            cnt_in += Integer.parseInt(token[2]);
            cnt_out += Integer.parseInt(token[3]);
            pkt_in += Long.parseLong(token[4]);
            pkt_out += Long.parseLong(token[5]);
        }
        if ( (sum_in >= 10000 || sum_out>=10000) && (cnt_in + cnt_out) >5 ) {
            output.collect( k1, new Text( Long.toString(sum_in) + ":" + Long.toString(sum_out) + ":"
                + Integer.toString(cnt_in) + ":" + Long.toString(cnt_out) + ":"
                + Long.toString(pkt_in) + ":" + Long.toString(pkt_out)) );
        }
    }
}
```



Flood_min.sh

```
#!/bin/bash
```

```
mday=`/bin/date '+%m%d'`
```

```
yday=$(date --date='1 day ago' +%m%d)
```

```
min=$(date --date='20 minute ago' +%H%M)
```

```
...
```

```
/opt/hadoop/bin/hadoop fs -rmr flood_min
```

```
/opt/hadoop/bin/hadoop jar /home/Flood/flood_min.jar flood_min  
$mday$min flood_min
```

```
cd /home/Flood/result
```

```
rm /home/Flood/result/$mday$min
```

```
sleep 2
```

```
/opt/hadoop/bin/hadoop fs -get flood_min/part-00000  
/home/Flood/result/$mday$min
```



A3. FDNS Traffic Aggregation (cont.)

□ a. Map

- 讀入 資料檔
- 輸出

□ b. Reduce

- 加總 src_ip 之 flow, byte, packet 數量
- 輸出

□ Execution

- flood_min.java
 - Execution shell script
 - Flood_min.sh



Result data (per 10-minutes for topN)

...

140.11x.xx.110@6	1212220:135902:93:92:1420:946
140.11x.xx.115@6	238590:16639:13:5:219:69
140.11x.xx.132@6	71076901:2117573:186:191:51519:37743
140.11x.xx.136@6	107746:367424:86:43:867:418
140.11x.xx.137@6	20404:46492:63:96:413:764
140.11x.xx.150@6	12454:0:4:0:127:0
140.11x.xx.154@6	95425:3510:13:8:221:26
140.11x.xx.161@6	178337:5415:63:11:1931:53
140.11x.xx.166@6	1608698:40227:13:11:1133:594
140.11x.xx.16@6	92836:46:26:1:1136:1
140.11x.xx.170@17	1262:18994:3:8:19:321
140.11x.xx.170@6	39745:1189:7:8:404:21
140.11x.xx.191@17	51227:56918:622:737:643:755
140.11x.xx.195@6	76663:46:20:1:787:1

...



Result data (per 10-minutes for portscan)

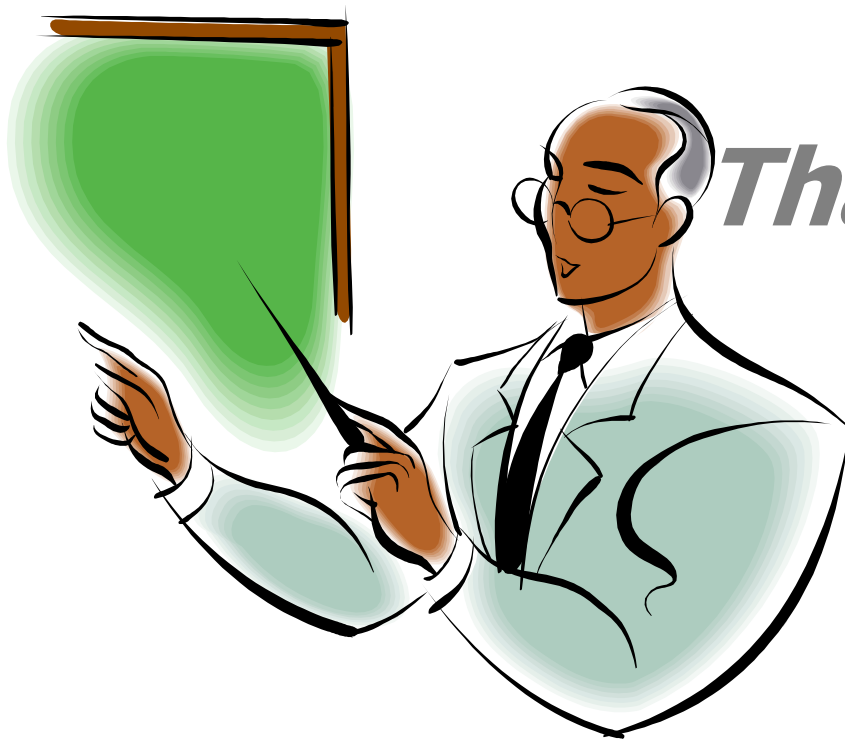
...

140.11x.xx.227@80	300782:223288:115:207:367:2138
140.11x.xx.56@443	376723:73189:24:55:298:291
140.11x.xx.56@80	4870479:168291:273:462:3617:1381
140.11x.xx.64@80	4195419:13832:12:3:2839:274
140.11x.xx.69@443	150323:100472:2:25:123:459
140.11x.xx.75@16884	0:42462:0:194:0:563
140.11x.xx.75@443	2516001:164203:46:32:2143:923
140.11x.xx.75@6881	635:200603:8:836:8:2582
140.11x.xx.75@80	3138670:119936:13:36:2174:1327
140.11x.xx.78@80	1475858:237246:53:69:1295:1020
140.11x.xx.89@80	25242266:1576:52:5:17082:18
140.11x.xx.8@80	471063:99851:12:20:473:488
140.11x.xx.100@443	2524:690:7:5:32:15
140.11x.xx.100@80	156667:82260:5:45:132:403

...



Computer Center, National Central University.



Thank You!