

南投區域網路中心 期末審查

報告人：俞旭昇主任



大綱

- 1 網路基礎建置及營運
- 2 服務特色
- 3 服務滿意度
- 4 年度績效指標
- 5 104年度推動重點
- 6 綜合建議



大綱

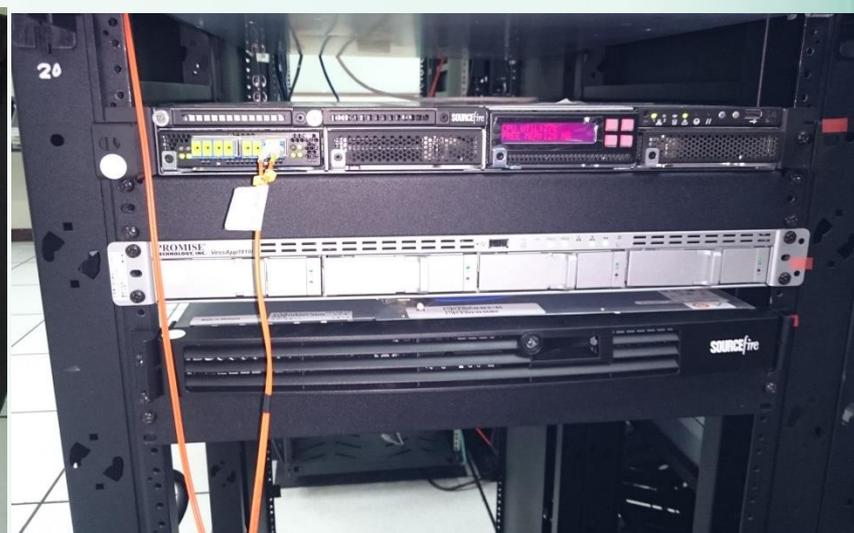
- 1 網路基礎建置及營運
- 2 服務特色
- 3 服務滿意度
- 4 年度績效指標
- 5 104年度推動重點
- 6 綜合建議

網路基礎建置及營運



防火牆

A-SOC Sourcefire 3D8120防火牆
Paloalto 5060頻寬管理



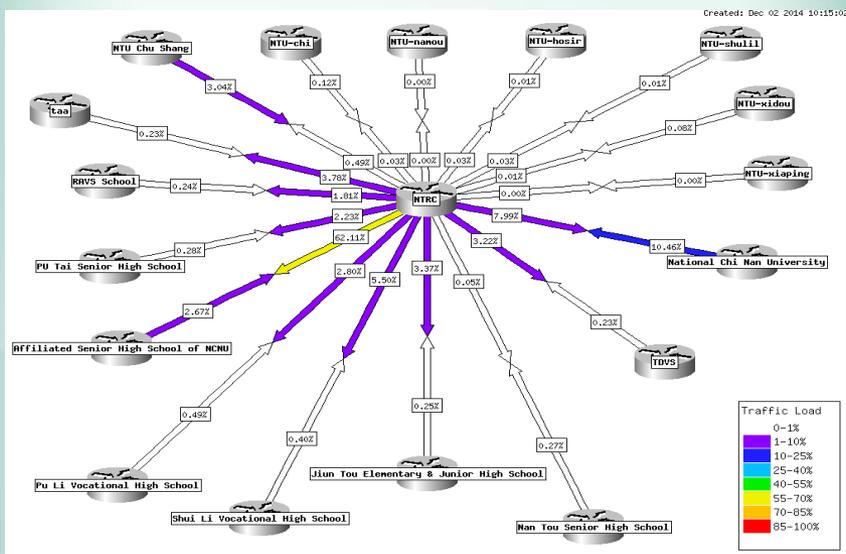
網路基礎建置及營運



網路管理機制

✓ 使用Mobile One Time Password:一次性密碼

✓ Cacti繪製流量圖供下游單位查詢



✓ 使用the dude監測設備可發出警報



網路基礎建置及營運



VoIP over IPv6推動及成效

- ✓ 推廣VoIP之成效：全校已全面改用網路電話系統，已建置3500門。
- ✓ 推廣IPv6之成效：全校皆使用雙協定(IPv4/ IPv6)網路電話環境。



網路基礎建置及營運-資安事件

102年度

103年度

1、2級
資安事件

- (1)自行通報數：0件。
- (2)非自行通報數：631件。
- (3)平均通報時數：18.38小時。

1、2級
資安事件

- (1)自行通報數：21件。
- (2)非自行通報數：538件。
- (3)平均通報時數：2.09小時。

3、4級
資安事件

- (1)自行通報數：0件。
- (2)非自行通報數：0件。
- (3)平均通報時數：0小時。

3、4級
資安事件

- (1)自行通報數：0件。
- (2)非自行通報數：0件。
- (3)平均通報時數：0小時。

平均時數

平均審核時數：3.97小時。
事件平均處理時數：18.59小時

平均時數

平均審核時數：0.35小時。
事件平均處理時數：2.09小時



大綱

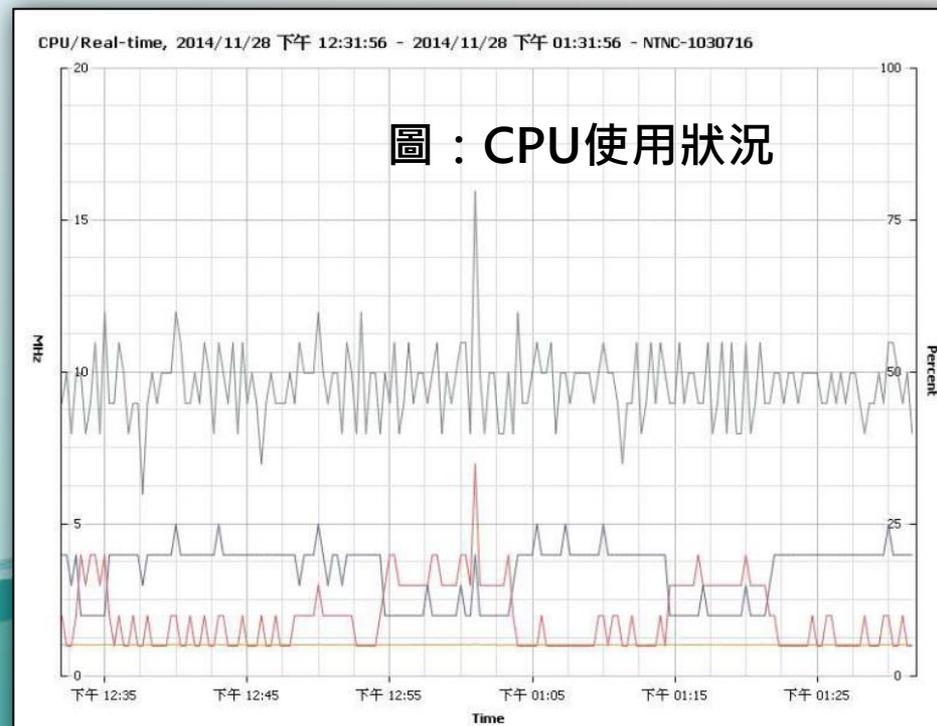
- 1 網路基礎建置及營運
- 2 服務特色
- 3 服務滿意度
- 4 年度績效指標
- 5 104年度推動重點
- 6 綜合建議

服務特色



資源共享

- ✓ 提供仁愛高農VM備份空間
- ✓ 提供縣網境內國中小網頁空間4T



服務特色



自由軟體推廣

✓ Ubuntu 正體中文站建置

下載 新聞 論壇 星球 Wiki

ubuntu[®] 正體中文

下載 Ubuntu Ubuntu 行為規範 Ubuntu@Taiwan 論壇規範 IRC 聊天室

ubuntu-tw 社群論壇規範調整，現在起開始實施。

下載

發行版

不同發行版具備不同的圖形環境與配套軟體。如果您不知道如何選擇，請選擇 Ubuntu 桌面版本。

- Ubuntu 桌面版本
- Ubuntu 伺服器版本

版本

最新版本是 14.04 LTS，提供桌面版三年支援（套件更新服務持續到 2017 年 4 月）、伺服器版五年支援（套件更新服務持續到 2019 年 4 月），以及其他版本：10.04 LTS、12.04 LTS、12.10、13.04、13.10

- 14.04 LTS
- 10.04 LTS (舊)
- 12.04 LTS (舊)
- 12.10 (舊)
- 13.04 (舊)
- 13.10 (舊)

電腦架構

一般電腦使用 32 位元的 Intel 架構，如果您的電腦可以使用 64 位元指令集，您也可以選擇安裝 64 位元版本。若您使用 Mac，您也可以使用其特殊版本，若不確定，請點選 32 位元版本。

- 32 位元版本
- 64 位元版本
- Mac 版本

下載選項

下載 BitTorrent 種子

開始下載

或是 至此瀏覽所有版本及檔案

✓ Ubuntu TW source list建置

```
File View VM
# deb cdrom:[Ubuntu-Server 14.04 LTS _Trusty Tahr_ - Release amd64 (20140416.2)]/ trusty main restrict
cted
#deb cdrom:[Ubuntu-Server 14.04 LTS _Trusty Tahr_ - Release amd64 (20140416.2)]/ trusty main restrict
ted
# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty main restricted
deb-src http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty main restricted
# Major bug fix updates produced after the final release of the
# distribution.
deb http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty-updates main restricted
deb-src http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty-updates main restricted
# N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty universe
deb-src http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty universe
deb http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty-updates universe
deb-src http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty-updates universe
# N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty multiverse
deb-src http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty multiverse
deb http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty-updates multiverse
deb-src http://ftp.ubuntu-tw.org/mirror/ubuntu/ trusty-updates multiverse
```

服務特色



貼心服務-協助連線單位資安通報查修

資安分析

- [資安通報 FILE-PDF Adobe Acrobat Reader msixec.exe file load exploit attempt](#)
- [資安通報 PUA-TOOLBARS Trackware funwebproducts mywebsearchtoolbar-funtools runtime detection](#)
- [資安通報 MALWARE-CNC Win.Trojan.Mudrop variant outbound connection attempt](#)
- [釣魚mail](#)
- [201404資安演練mial](#)
- [侵權 22-152478803 Notice of Unauthorized Use of Paramount Pictures Corporation Property](#)
- [OpenSSL OpenSSL heartbleed\(SERVER-OTHER OpenSSL *\)](#)
- [MALWARE-CNC Possible Zeus User-Agent - Mozilla 分析](#)
- [MALWARE-CNC Win.Trojan.Mevade variant outbound connection](#)
- [BLACKLIST User-Agent known malicious user agent - TrxDll - Win.Trojan.Adload.dyhq](#)
- [BLACKLIST User-Agent known malicious user-agent string http - Win.Trojan.Waski](#)
此通報http封包內容為User-Agent Http，內容的URL放到virustotal檢出率很低，但DN放到google上查確查不到資料，所以選擇封鎖URL
此通報還會有一個誤報就是gamania自給的軟體一樣會填入User-Agent: HTTP大小寫不同
- [MALWARE-CNC Win.Trojan.Necurs variant outbound detection](#)
連線多個IP(都沒DN) URL皆為/board/user.php
- [2014 10 29 科三實驗室區斷網事件](#)
- [2014/10/30人院無法上網](#)
- [2014/11/13 VLAN21 固定IP對外攻擊&系統置入檔案](#)

數: 2

開始時間	名稱	來源 IP	來源 Port	來源地國名	目的 IP	目的 Port	目的
2014/11/23 00:09:52	BLACKLIST User-Agent known malicious user agent - Post			Taiwan	101.199.109.143	80	C

Generate Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	IP Protocol	Application	Action	Rule	Bytes	Bytes Sent	Bytes Received	Device SN
11/23 00:11:55	end	TANET_V4_In	TANET_V4_Out		101.199.109.143	52031	80	tcp	360-safeguard-update	allow	TANET_V4_Outg...	2.3 K	1.5 K	869	NCNJ_PA-5060
11/23 00:11:55	end	Campus_NAT_In	Campus_NAT_Out		101.199.109.143	4490	80	tcp	360-safeguard-update	allow	Campus_NAT_In...	2.3 K	1.5 K	869	NCNJ_PA-5060
11/23 00:11:45	end	Campus_NAT_In	Campus_NAT_Out		101.199.109.143	4477	80	tcp	360-safeguard-update	allow	Campus_NAT_In...	2.2 K	1.3 K	869	NCNJ_PA-5060
11/23 00:11:44	end	TANET_V4_In	TANET_V4_Out		101.199.109.143	51992	80	tcp	360-safeguard-update	allow	TANET_V4_Outg...	2.0 K	1.2 K	819	NCNJ_PA-5060
11/23 00:11:44	end	Campus_NAT_In	Campus_NAT_Out		101.199.109.143	4479	80	tcp	360-safeguard-update	allow	Campus_NAT_In...	2.0 K	1.2 K	829	NCNJ_PA-5060

服務特色



防火牆阻擋攻擊事件

威脅/內容名稱	ID	威脅/內容類型	計數
Session Limit Event	8801	flood	23.91 M
DGA NXDOMAIN response Found	40040	vulnerability	1.47 M
NTP Denial-Of-Service Attack	40038	vulnerability	605.33 k
DNS ANY Queries Brute-force DOS Attack	40033	vulnerability	361.94 k
Sipivicious_Gen User-Agent Traffic	13272	spyware	180.14 k
Suspicious DNS Query (generic:oss.aliyuncc.com)	4045189	spyware	112.18 k
SSLv3 Found in Server Response	36815	vulnerability	67.79 k
Suspicious DNS Query (generic:gs4.playdr2.tw)	4002446	spyware	38.45 k
HTTP Unauthorized Brute-force Attack	40031	vulnerability	27.68 k
Suspicious DNS Query (generic:gs2.playdr2.tw)	4002447	spyware	25.39 k
Suspicious DNS Query (generic:gs3.playdr2.tw)	4002445	spyware	24.45 k
Morto RDP Request Traffic	13274	spyware	24.36 k
Suspicious DNS Query (generic:js.tv.itc.cn)	4082527	spyware	20.14 k
Suspicious DNS Query (generic:s.00oo00.com)	4045184	spyware	17.01 k
Suspicious DNS Query (generic:s.zampdsp.com)	4094235	spyware	15.93 k
Microsoft RPC <u>SystemActivator</u> bind	30846	vulnerability	15.67 k



大綱

- 1 網路基礎建置及營運
- 2 服務特色
- 3 **服務滿意度**
- 4 年度績效指標
- 5 104年度推動重點
- 6 綜合建議

服務滿意度

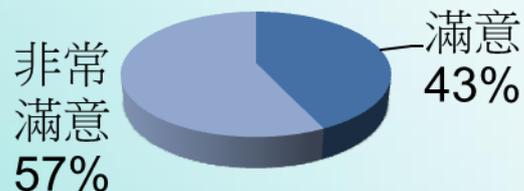
南投區網回覆比率：66.67%

整體區網回覆比率：66.92%

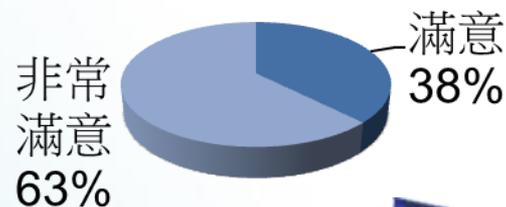


區網中心綜合整體服務的表現

102年整體滿意度



103年整體滿意度





大綱

- 1 網路基礎建置及營運
- 2 服務特色
- 3 服務滿意度
- 4 年度績效指標
- 5 104年度推動重點
- 6 綜合建議

年度績效指標

- ✓ 協助遠距課輔硬體維護，及維持網路品質。
- ✓ 舉辦兩次管理委員會
(預計12月15至19間舉行第二次管理委員會)
- ✓ 預計舉辦一場資安研討會。
- ✓ 針對連線單位進行一次期末滿意度調查，維持區網及電信業者服務品質。
- ✓ 完成至少五個連線單位進行網路健檢服務。

年度績效指標



協助遠距課輔硬體維護，及維持網路品質



舉辦兩次管理委員會

11/26舉辦第一次管理委員會

預計12月15至19間舉行第二次管理委員會

年度績效指標



預計舉辦一場資安研討會。

103/06/11舉辦『103年度第一梯次開源軟體教育應用研討會』

議題：

OpenOffice -開放好用的免費辦公室套裝軟體、開源軟體之美

103/11/26舉辦『103年度第二梯次開源軟體教育應用研討會』

議題：

網路著作權、挪威電腦教室裡的秘密（自由軟體發展協會）

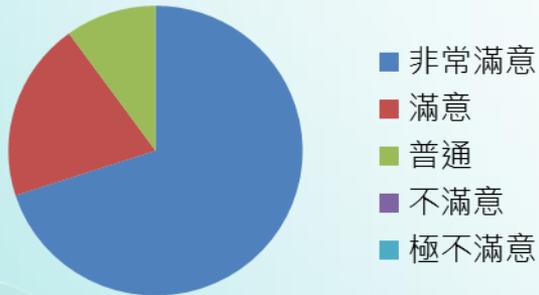


年度績效指標

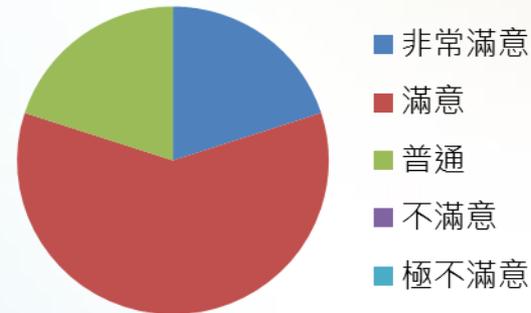


期末滿意度調查，確保服務品質

電信業者(ISP)線路穩定度



對研討會整體滿意度



完成至少五個連線單位進行網路健檢服務

本年2月13日至均頭國中、4月10日至暨大附中、
10月14日至普台高中、10月27日至三育高中、
10月29日至仁愛高農



大綱

- 1 網路基礎建置及營運
- 2 服務特色
- 3 服務滿意度
- 4 年度績效指標
- 5 **104年度推動重點**
- 6 綜合建議

104年度推動重點

- 威脅/防禦整合性服務
- 推廣開源軟體
- 協助偏鄉網路課輔計劃
- 提供連線單位VM空間
- 提供連線單位網路健檢及諮詢服務
- 引進多元社群服務，加速學術網路內資源共享





大綱

- 1 網路基礎建置及營運
- 2 服務特色
- 3 服務滿意度
- 4 年度績效指標
- 5 104年度推動重點
- 6 綜合建議

綜合建議

希望教育部可以持續提供維護經費來維運目前區網資安設備。

**簡報結束
謝謝**