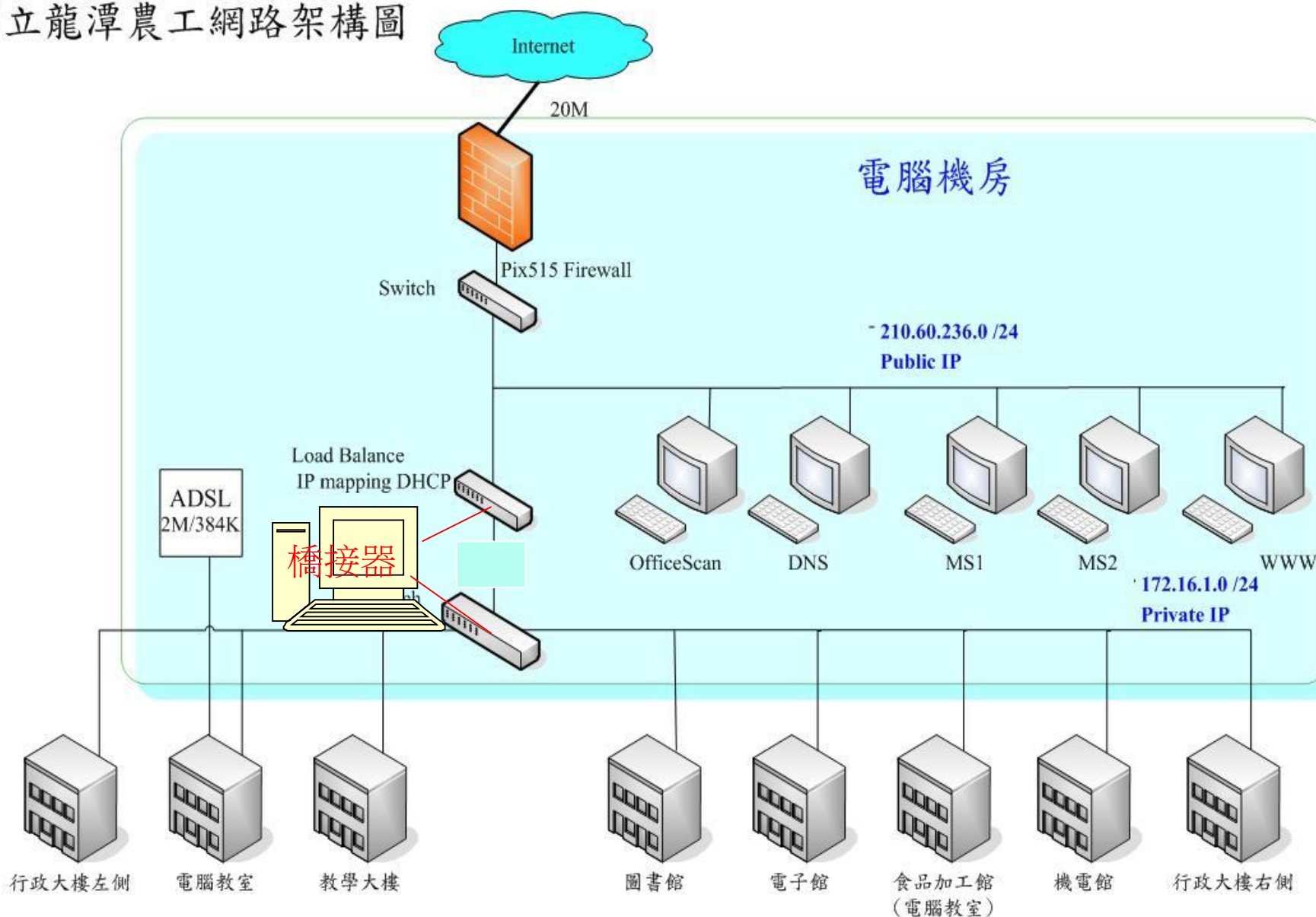




龍潭農工網路現況報告

報告人：黃仁和
2008/11/11

國立龍潭農工網路架構圖



橋接器的目的

- 以個別機器的mac碼鎖定，控制個別電腦接觸網路

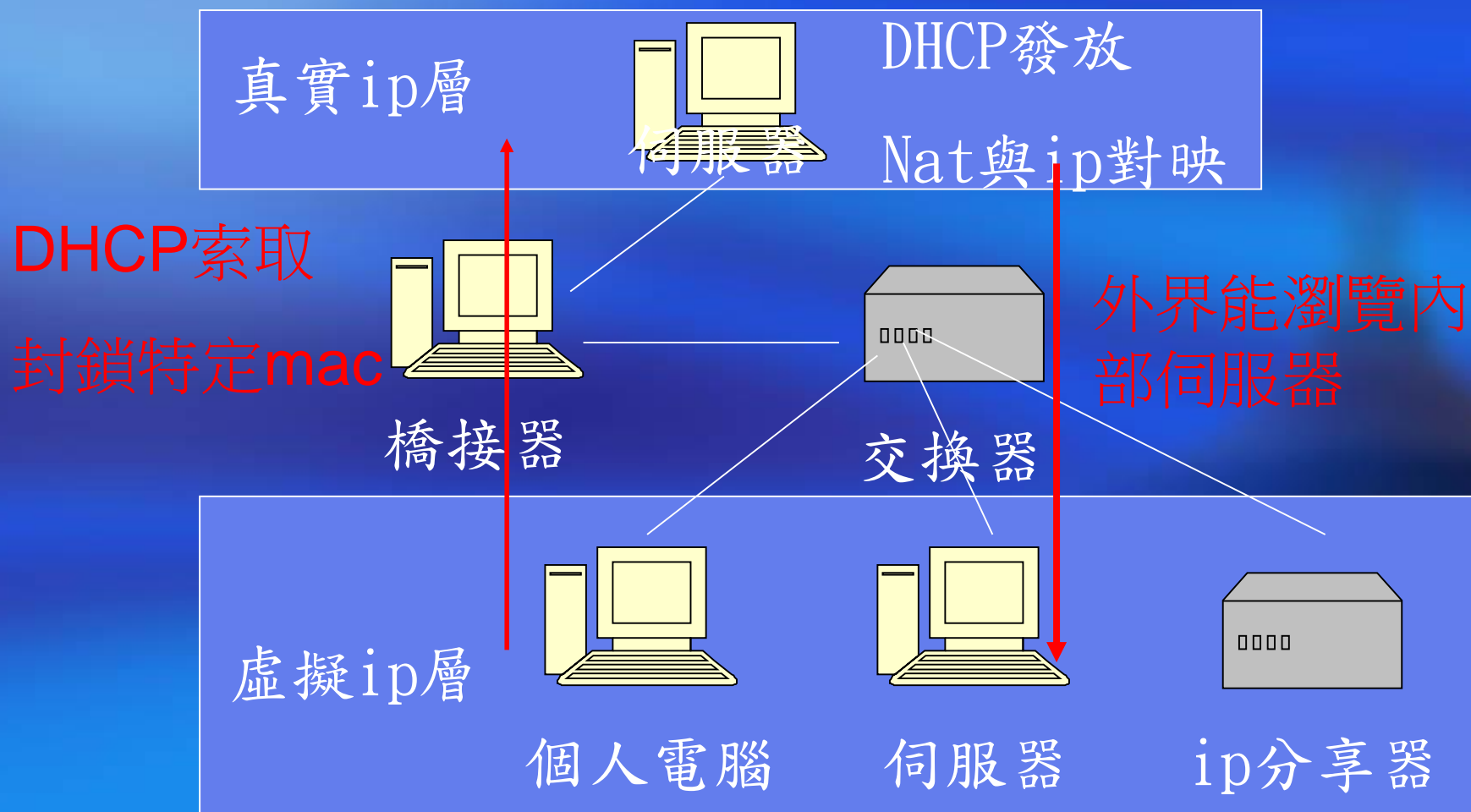
內部網路的問題1

39.540324	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.231?
39.555861	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.232?
39.571484	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.233?
39.587148	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.234?
39.602738	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.235?
39.618356	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.236?
39.635727	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.237?
39.649677	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.238?
39.665250	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.239?
39.680871	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.240?
39.696492	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.241?
39.712114	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.242?
39.727761	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.243?
39.743385	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.244?
39.759029	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.245?
39.774636	Giga-Byt_3b:ab:6f	Broadcast	ARP	Who has 172.16.1.246?

內部網路的問題2

Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f
Giga-Byt_3b:ab:6f	00:22:15:6a:a6:b1	ARP	172.16.1.254	is	at	00:0d:61:3b:ab:6f

預想網路架構



準備工作

- Linux安裝bridge套件
- iptables的FORWARD鏈預設規則DROP
- 偷偷掃描校內電腦的mac碼

問題與解決1

- DHCP發放ip
- 橋接器應能讓所有DHCP的UDP封包通過(埠號67/68)

問題與解決2

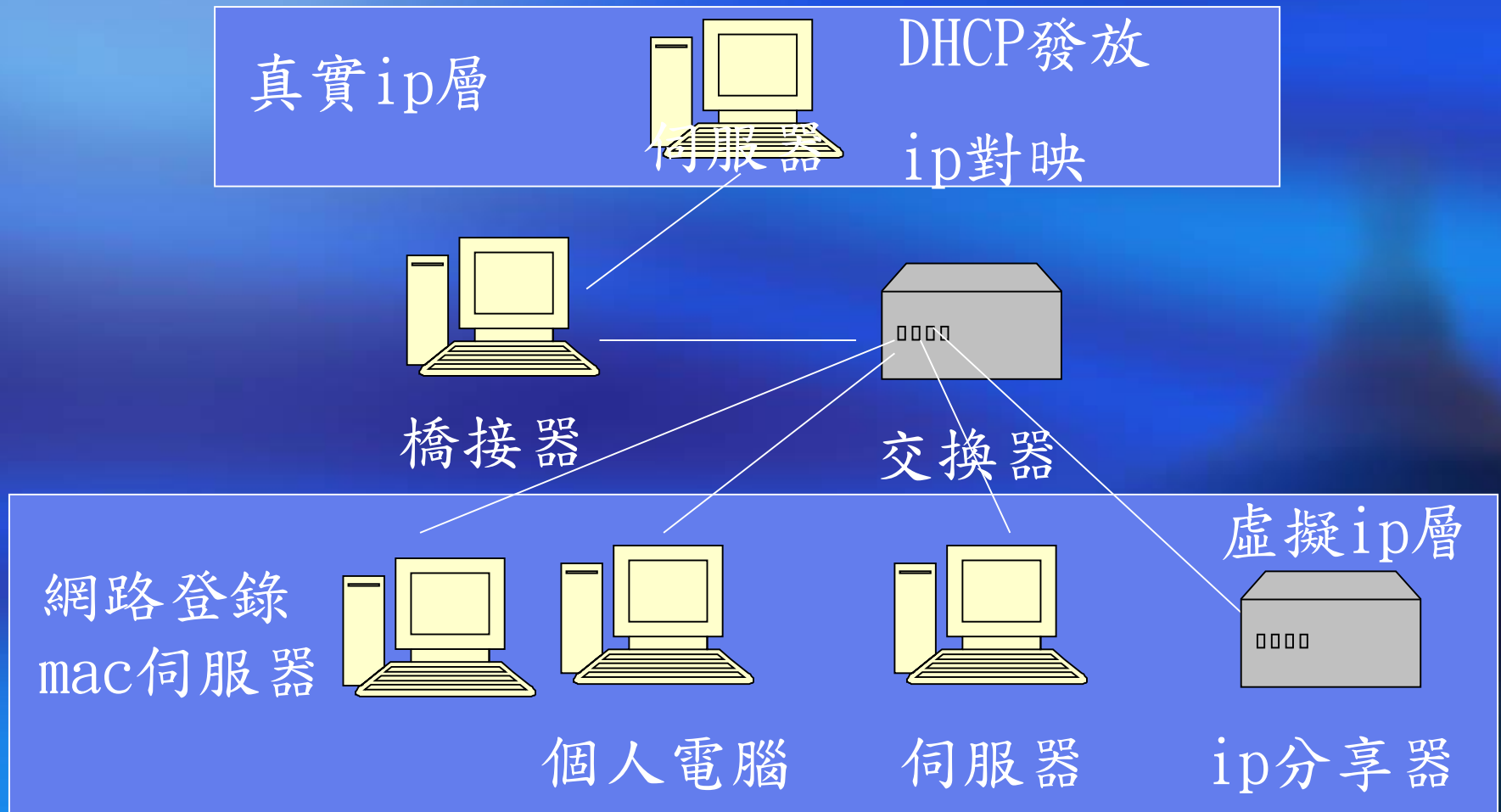
- 允許虛擬ip層架設伺服器(固定虛擬ip發放並以真實ip對映虛擬ip)
- 橋接器對特定目的地的ip位置開放

或直接允許DHCP伺服器的mac

準備白名單

- 一般使用者會不會查mac?
- 伺服器，ip分享器，網路印表機的mac?

內部mac登錄伺服器



在虛擬ip層架設網頁伺服器讓使用者登錄

請輸入使用人、電腦位置描述及校內分機號碼

請在個人所使用的電腦上網,因為會紀錄電腦的ip172.16.1.217;與mac碼00:22:15:6A:A6:B1

在別人的電腦上登錄,會被視為另一部電腦,請記得所有欄位必須填寫

請輸入使用人：

請輸入電腦所在辦公室：

請輸入使用人校內電話分機號碼：

請輸入電腦位置描述：(30個字以內，任何人都可以輕易找到這台電腦的描述)

確認送出

完成

網際網路

對伺服器及ip分享器測ip及mac

ip爲172.16.1.20

mac爲00:05:07:02:19:83

負責人爲123

機器所在辦公室123

機器位置爲456

感謝您的合作...資料已登錄...謝謝

後續處理

- 如放棄上一層機器的mac認同
則需對每一台虛擬層的伺服器均設開放規則
- 橋接器本身的防火牆設定(INPUT鏈)需重新設定?

但丁：

道德常能彌補智慧的缺陷

智慧卻往往無法彌補道德的缺陷

The background of the slide is a photograph of the Temple of Heaven in Beijing at night. The main structure, the Circular Hall, is visible in the lower half, its dark silhouette contrasting with the deep blue night sky. A bright, full moon is positioned in the upper center of the frame, casting a soft glow. The overall mood is serene and traditional.

報告完畢，敬請指正