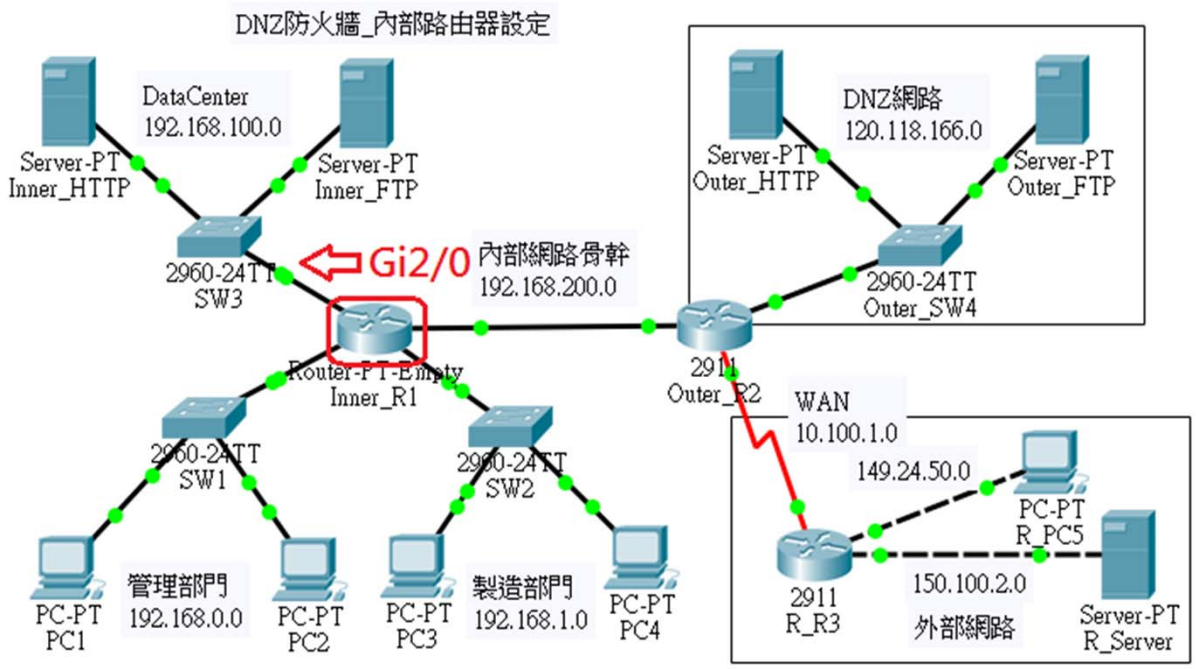
9-6-4 內部路由器 ACL 規劃 (一)

- 防火牆條件
  - (1) Gi2/0 (192.168.100.254) 管制內部伺服器的存取限制：
    - 1. 允許來源是 192.168.0.0/24與 192.168.1.1 存取 192.168.100.1:80 。
    - 2. 允許來源是 192.168.1.0 /24與 192.168.0.1 存取 192.168.100.2:22, 23。
    - 3. 允許 192.168.0.1 與 192.168.1.1 ping 192.168.100.1 與 192.168.100.2
    - 4. 允許 192.168.0.1 與 192.168.1.1 主機登入此埠口(192.168.100.254)。



9-6-4 內部路由器 ACL 規劃 (二)

Inner-ACL 條件 (Gi2/0)

- 1. 允許來源是 192.168.0.0/24與 192.168.1.1 存取 192.168.100.1:80 。
- 2. 允許來源是 192.168.1.0 /24與 192.168.0.1 存取 192.168.100.2:22, 23。
- 3. 允許 192.168.0.1 與 192.168.1.1 ping 192.168.100.1 與 192.168.100.2

Inner_R1(Gi2/0) 外部路由器：Inner-ACL								
編號	Permit/ deny	類型	來源		目的		方向	備註
			IP	port	IP	port		
1	permit	tcp	192.168.0.0/24	any	192.168.100.1	80	out	www
2	permit	tcp	192.168.1.1	any	192.168.100.1	80	out	www
3	permit	icmp-echo	192.168.0.1	any	192.168.100.1		out	ping
4	permit	tcp	192.168.1.0/24	any	192.168.100.2	20, 21	out	ftp
5	permit	tcp	192.168.0.1	any	192.168.100.2	20, 21	out	ftp
6	permit	icmp-echo	192.168.1.1	any	192.168.100.2		out	ping

9-6-4 內部路由器 ACL 規劃 (三)

- 設定 Inner-ACL 規則

```
Inner_R1>en
Inner_R1#config ter
Inner_R1(config)#ip access-list extended Inner-ACL
Inner_R1(config-ext-nacl)#permit tcp 192.168.0.0 0.0.0.255 host 192.168.100.1 eq
www
Inner_R1(config-ext-nacl)#permit tcp host 192.168.1.1 host 192.168.100.1 eq www
Inner_R1(config-ext-nacl)#permit icmp host 192.168.0.1 host 192.168.100.1 echo
Inner_R1(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 host 192.168.100.2 eq
ftp
Inner_R1(config-ext-nacl)#permit tcp host 192.168.0.1 host 192.168.100.2 eq ftp
Inner_R1(config-ext-nacl)#permit icmp host 192.168.1.1 host 192.168.100.2 echo
Inner_R1(config-ext-nacl)#deny ip any any
Inner_R1(config-ext-nacl)#
Inner_R1(config)#do show access-list Inner-ACL
Inner_R1(config)#int gi2/0
Inner_R1(config-if)#ip access-group Inner-ACL out
Inner_R1(config-if)#
```

- 測試網路功能
  - 測試 Inner_HTTP 連線
  - 測試 Inner_FTP 連線