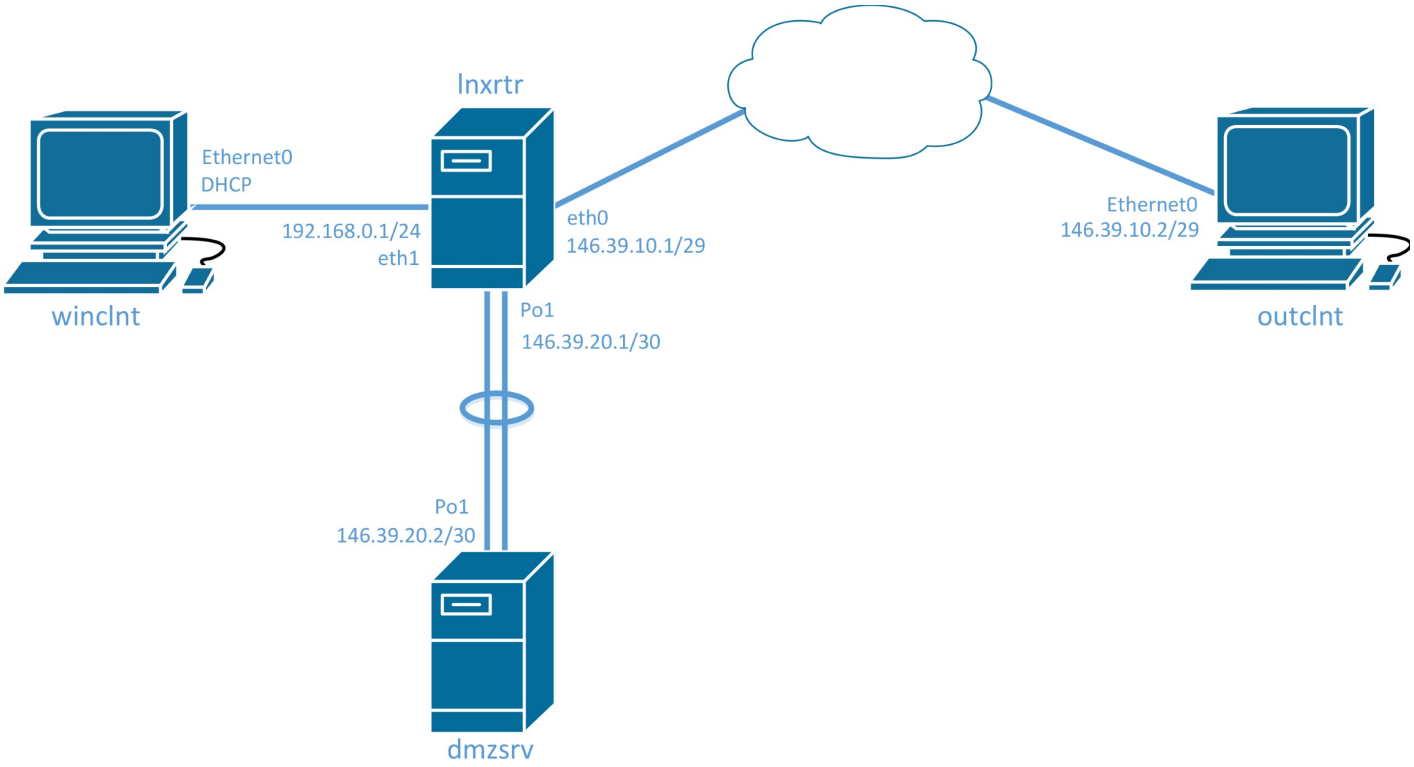
46th TWSkills

39 | IT Network Systems Administration

Test Project - Day 1

PROJECT TASKS

Diagram



Introduction & Description

- 本競賽為固定式起訖時間，請選手自行掌握工作流程，並依據試題敘述完成要求
- 評分時，將盡可能採用功能測試，項目之區隔以評分表所列為主，個別項目完全符合試題之敘述即得分，無部份給分
- 除了必須以檢視設定值的方式進行評分的項目外，所有面向用戶的服務一律由用戶端系統進行測試，否則該項目不予計分
- 工作項目中需設定密碼之處，若試題未明確指定，則一律使用Skills39

VMware Workstation Pro

- Windows Server虛擬機須能以Ctrl + Alt + Del組合鍵解除登入畫面的鎖定
- 關閉Linux虛擬機在未安裝虛擬音效卡時，於CLI進行Tab鍵自動完成等操作所發出的音效(嗶聲)

lnxrtr

- 於PC1建立Debian 8虛擬機lnxrtr
- 設定DNS服務，管理gotowsc2017.tw網域的資源紀錄(Resource Records)
- 在連接dmzsrv的兩個介面設定Link Aggregation，以IEEE公開標準協定進行協商
- 啟用IP封包轉送服務
- 為來自內部網路的流量設定NAT，可經由146.39.10.1位址對外連線
- 設定DHCP Relay Agent，讓用戶端自dmzsrv取得IP位址
- 以SMB協定提供網路資料夾ccs_crts，用戶端可輸入UNC Path進行存取，僅供dmzsrv以Administrator帳戶使用

dmzsrv

- 於PC1建立Windows Server 2012 R2虛擬機dmzsrv
- 設定Active Directory Domain Services，網域名稱為gotowsc2017.tw
- 將Active Directory服務所需的DNS紀錄註冊於lnxrtr下
- 在連接lnxrtr的兩個介面設定IEEE Link Aggregation
- 設定DHCP服務，配發192.168.0.21 ~ 192.168.0.220範圍內的IP位址
- 以HTTPS協定提供網路資料夾private_share，供網域帳戶使用，用戶端可輸入E-Mail Address進行存取，每位使用者擁有個人專屬的資料夾，並禁止存取他人的資料
- 建立Root CA，為所有Web站台 個別核發包含相應FQDN資訊的憑證
- 安裝IIS，以HTTP與HTTPS協定，提供www.gotowsc2017.tw與support.gotowsc2017.tw網頁，並使用隨身碟內所附的檔案作為首頁內容
- 為增進服務可攜性並便於統一管理，所有網頁站台的憑證均須存放於\\lnxrtr\ccs_crts上，dmzsrv本機的憑證儲存區內不保存憑證與私鑰副本

Active Directory Tasks

- 依附表建立使用者與群組
- 建立名為StdComputers的OU(組織單位)，新加入網域的PC須自動置於此OU內
- 關閉所有網域電腦的休眠與睡眠功能
- 禁止所有網域電腦操作系統保護(System Protection)相關設定
- 所有網域PC以檔案總管瀏覽資料時，須在視窗標題上顯示完整的工作路徑
- dmzsrv可主動發布群組原則設定至網域中所有的電腦
- 使用者登入後，將自動連結至dmzsrv所提供的網路資料夾，並啟用同步功能，如同Google.Dropbox.OneDrive等常見雲端硬碟服務的使用模式，使用者於本機相應目錄進行操作後，將自動反映至伺服器上

WinClnt

- 於PC2建立Windows虛擬機winclnt
- 加入gotowsc2017.tw網域

OutClnt

- 於PC2安裝Windows 10虛擬機outclnt
- 在Manager使用者的桌面上放置回收桶、控制台與Edge瀏覽器的捷徑

APPENDIX

Active Directory Users

Username	Group
User01 – User50	Domain Users

Device Specifications

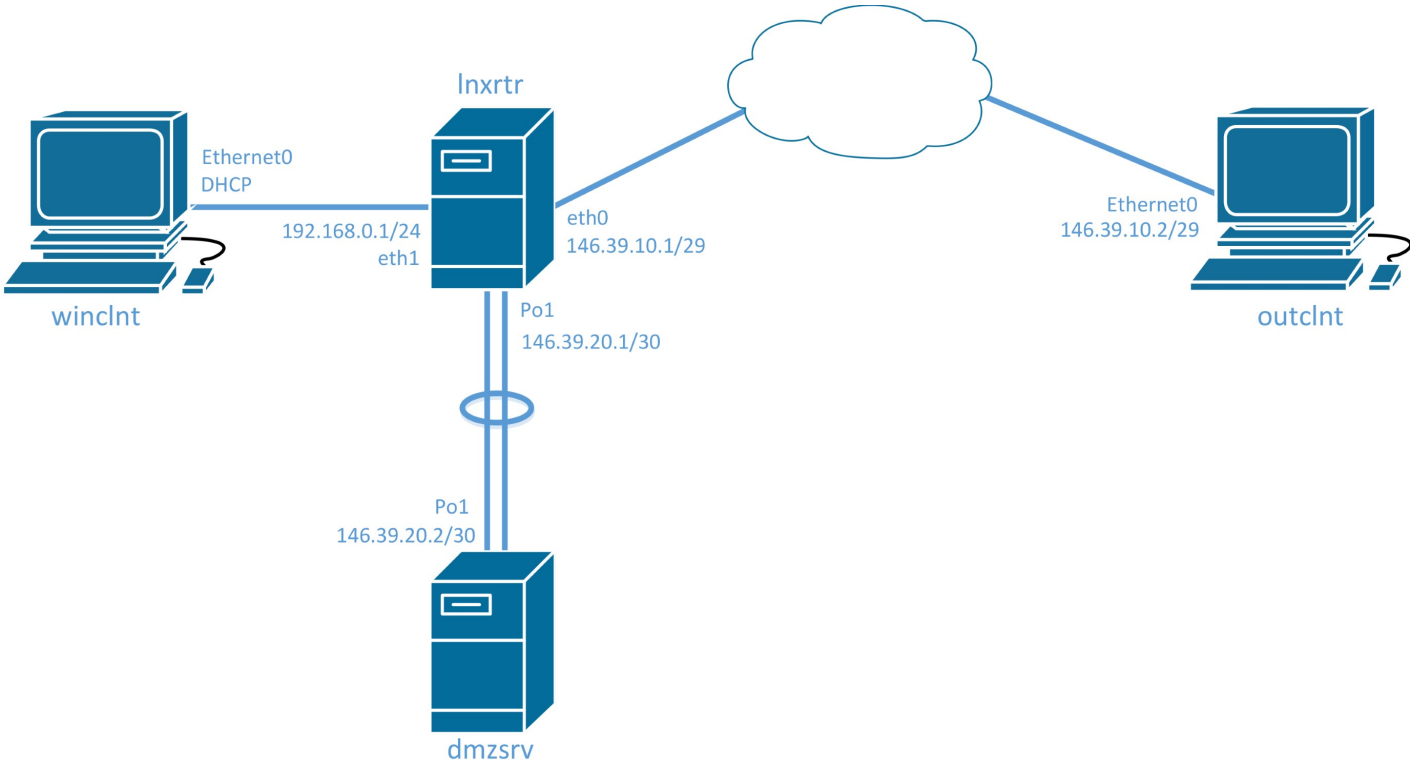
Device	Management User
winsrv	Administrator
lnxrtr	root
outclnt	Manager

46th TWSkills

39 | IT Network Systems Administration

Test Project - Day 2

PROJECT TASKS

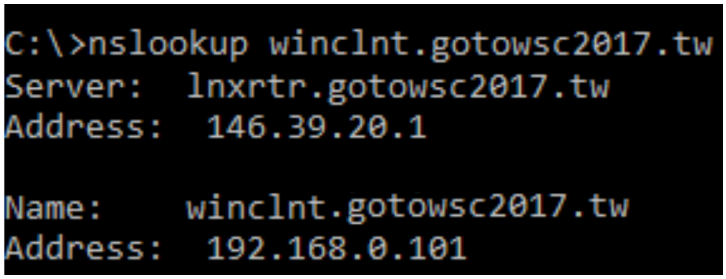


Introduction & Description

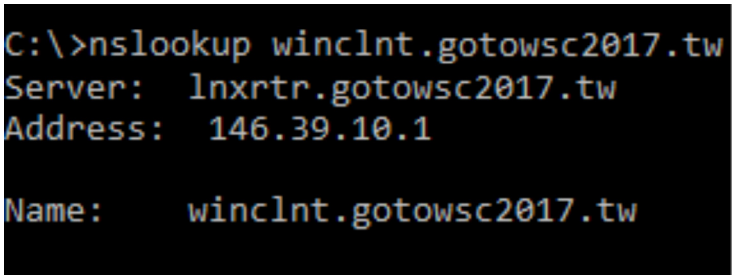
- 今日工作項目將延續昨日之情境，部分資訊請選手自行參考前一日的試題

Security - Access Control

- 查閱隨身碟所附之文檔，於lnxrtr設定Access Control，僅允許檔案中所列的來源IP存取dmzsrv，為提升效能，只有來自外部的封包需要進行此項比對
- 實務上，ISP不會協助轉送來源或目的為Private IP的封包，在本次競賽的模擬情境中並沒有這樣的機制，因此，若outclnt發送目的為192.168.0.0/24的封包，將會順利被轉送至GoToWSC2017內部網路，請思考並實作一個符合Netfilter正確施作建議、且不會對既有的網路環境(例：NAT)造成影響的解決方案
- 為避免內網的DNS記錄流向Internet，若DNS查詢來自外部且查詢結果對應至192.168.0.0/24下的IP位址，則回應「記錄存在但查無所要求的內容」的訊息，見下圖：



dmzsrv OR winclnt



Outclnt

Security - VPN

- 於dmzsrv上提供Remote Access VPN供漫遊使用者存取內部資源，提供SSL與IPsec Tunnel Mode兩種加密方式
- 為提升安全性，IPsec VPN協商過程，需使用基於橢圓曲線密碼學(Elliptic curve cryptography)的金鑰交換演算法
- 使用者連線至VPN後，將取得192.168.255.0/24範圍內的IP位址，並可與內網PC (例：winclnt)相互連線
- 為提升使用上的便利性，於outclnt上開啟IE或Edge瀏覽器時，將自動連線至VPN服務
- 連線至VPN後，須可使用VPN驗證身分，存取dmzsrv的網路資料夾，評分時將以Domain Users中任意使用者進行測試

Network Monitoring

- 於dmzsrv與lnxrtr上進行設定，當網域使用者登入失敗時，dmzsrv將以SNMP協定知會lnxrtr，並將於lnxrtr本機/var/log/failed_ad_attempts.log產生紀錄

Diagnostic

Introduction & Description

。在本階段的競賽，選手將擔任網路技術顧問，分別協助診斷或排除數個網路環境的障礙

。本階段說明如下：

1. 共有 4 個完全獨立的情境
2. 針對每個情境，選手將獲得該狀況的整體說明或求助的電子郵件，並附有架構圖與設備的記錄檔等資訊
3. 選手沒有任何設備的操作權，僅可依據對方提供的既有資訊，判斷網路或服務的問題所在
4. 每個情境將會附有數個提問，請自行依觀察與診斷的結果進行作答

Discovery

Introduction & Description

。在本階段的競賽，選手僅會被提供有限的資訊，並須倚靠網路檢修與觀察的技巧，探索並推理出完整的網路拓樸

。評分時完全以答案紙上的作答內容為依據，所有設備的設定狀態均不會影響選手的得分

。關於本階段競賽的「事實」如下：

1. 共有 8 台設備，選手將獲得 1 台設備的 Console 存取 (TR1)
2. 所有設備的介面 IP 位址都是設定完成、且設定正確的
3. 所有設備都能夠被 Telnet 連線，用以連入 VTY 管理介面
4. 所有設備上所設定的介面 IP 都是有意義的 (一定有連接對象)
5. 所有設備可能事先被進行任何設定，除了 IP 位址之外，其餘的預先設定均不保證合理性與正確性
6. 選手將無法成功的以 Broadcast 或 Multicast Ping 獲得相鄰設備的資訊，請使用其他方式進行本階段試題
7. 除第 6 點所列出的內容外，所有設備上均**沒有**設定任何會明確導致封包遭到丟棄的過濾機制 (例如 ACL、防火牆等)

。請於答案紙上繪製出網路的拓樸，並記錄所有影響到設備連線的設定錯誤，完成後，所有設備應能與相鄰的設備互通