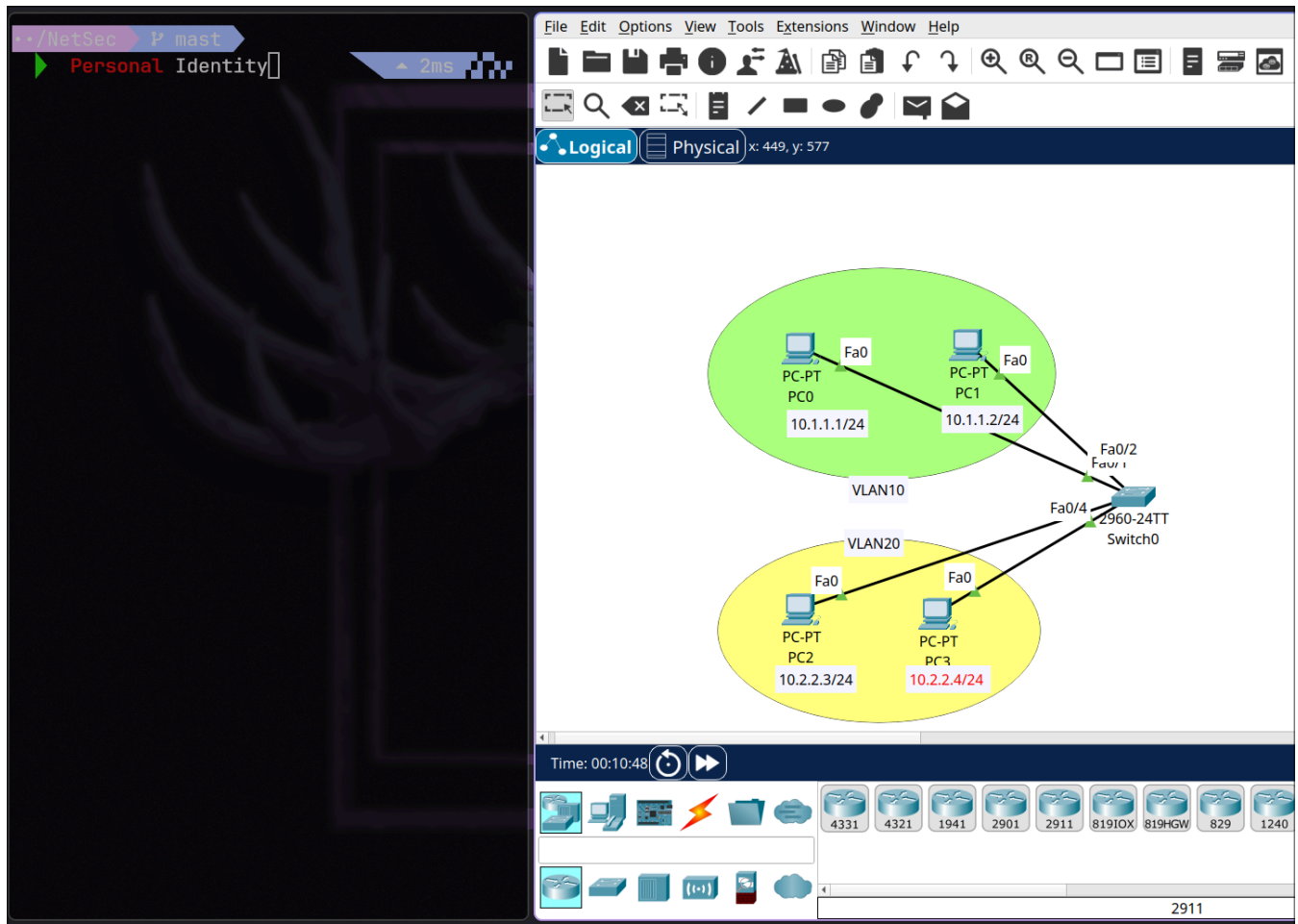


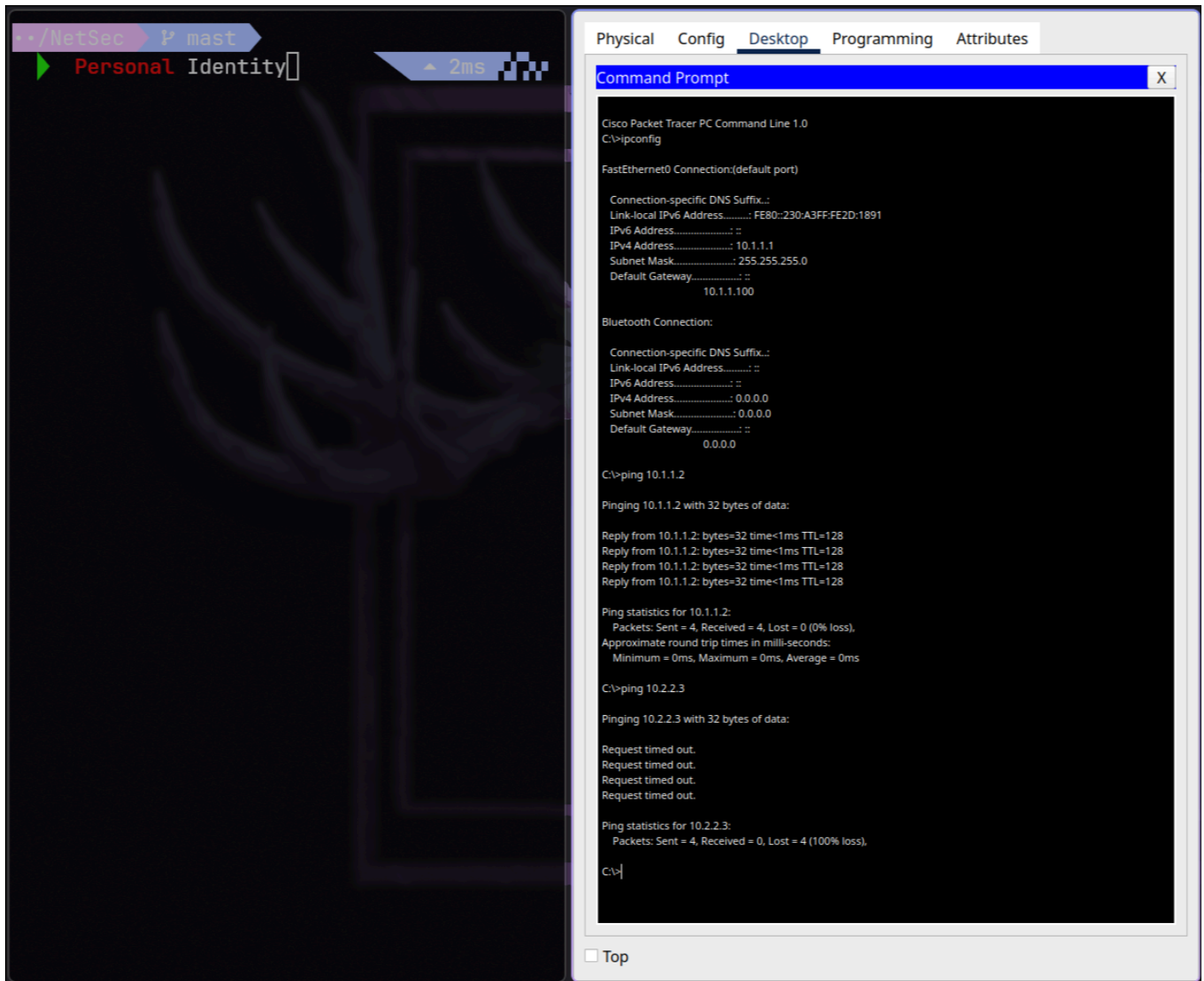
# Lab01 Report

1. Name: 林靖昀 Student ID: B12902116
2. Proof of your lab work (clearly label each screenshot)

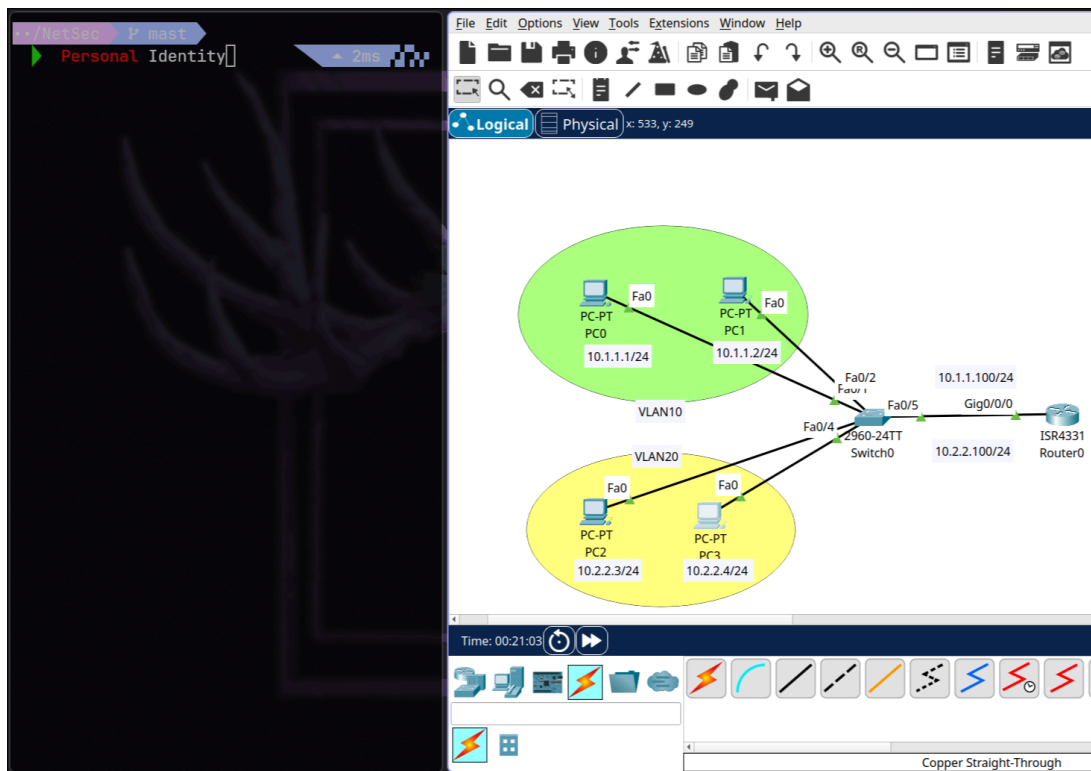
Screenshot-01: cisco network tracer VLAN架構圖 (5%)



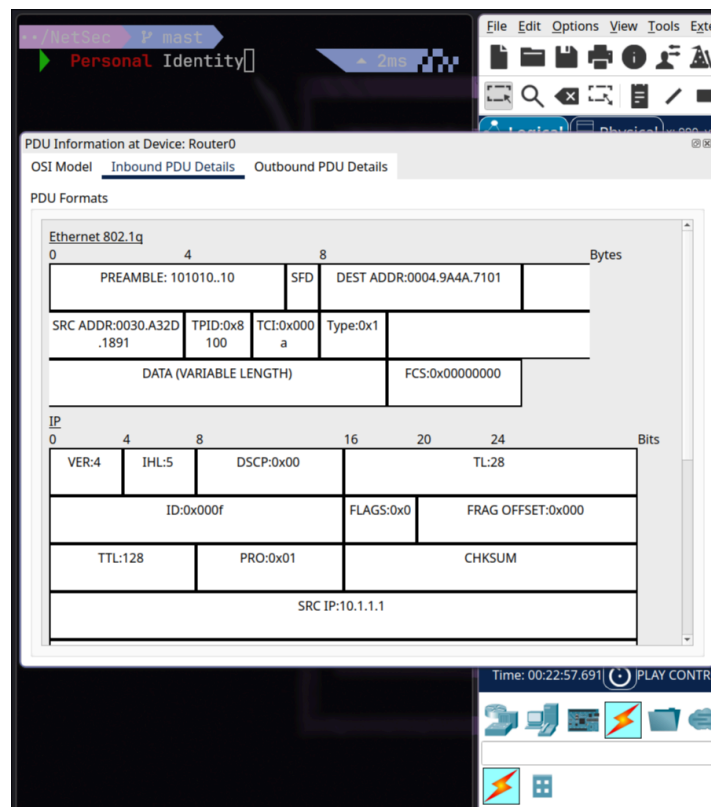
Screenshot-02: VLAN互PING (5%)



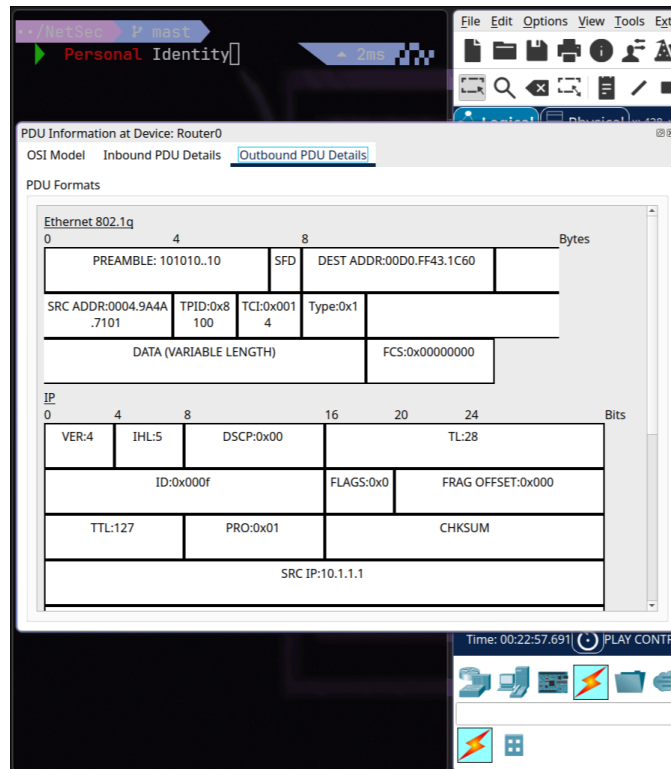
Screenshot-03: Inter-VLAN static Routing架構圖 (5%)



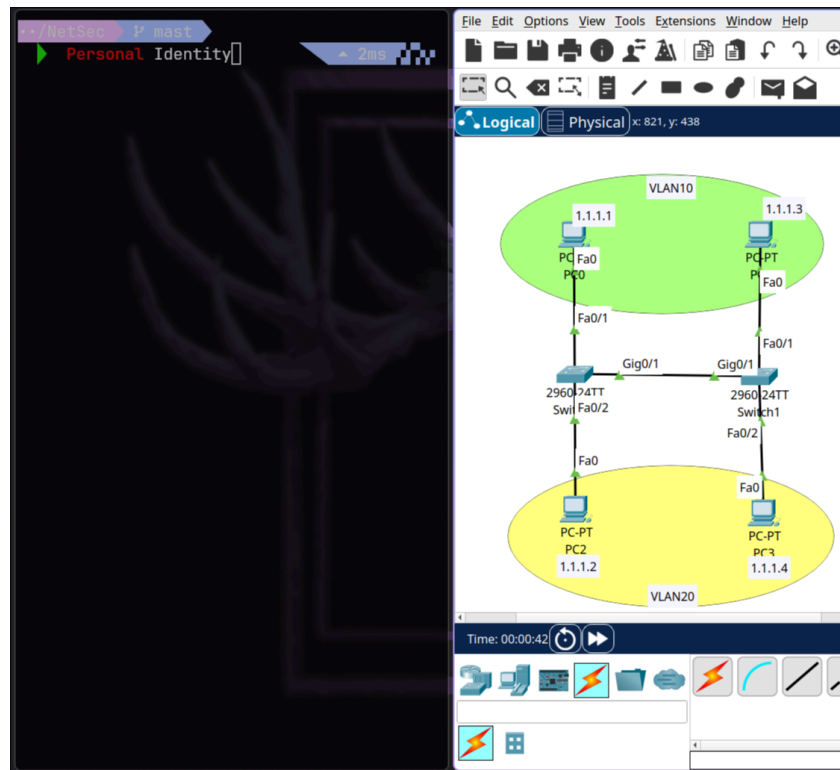
Screenshot-04: Inter-VLAN static Routing: From Switch to Router (5%)



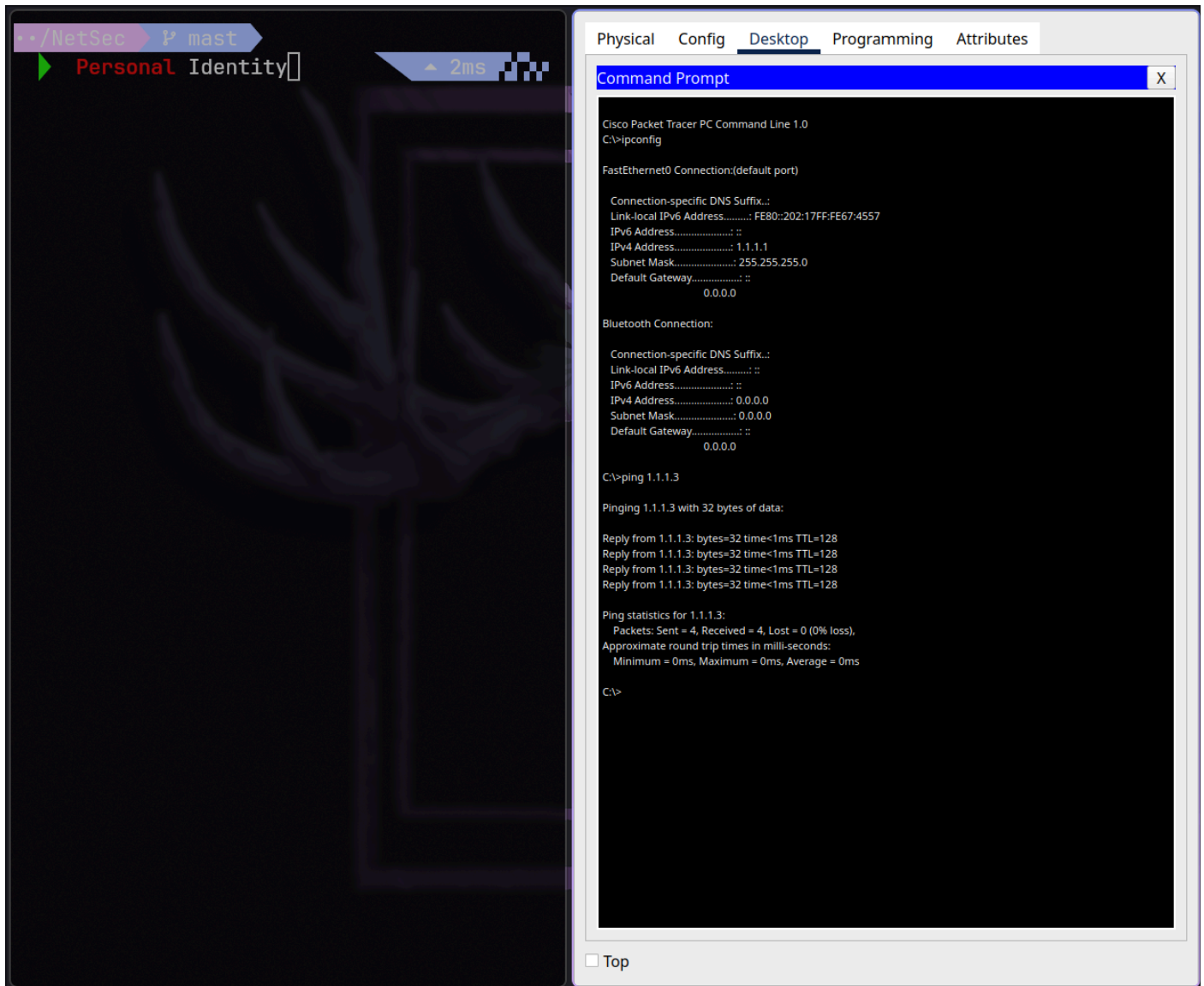
Screenshot-05: Inter-VLAN static Routing: From Router to Switch (10%)



Screenshot-06: VLAN in multiple Switches架構圖 (10%)

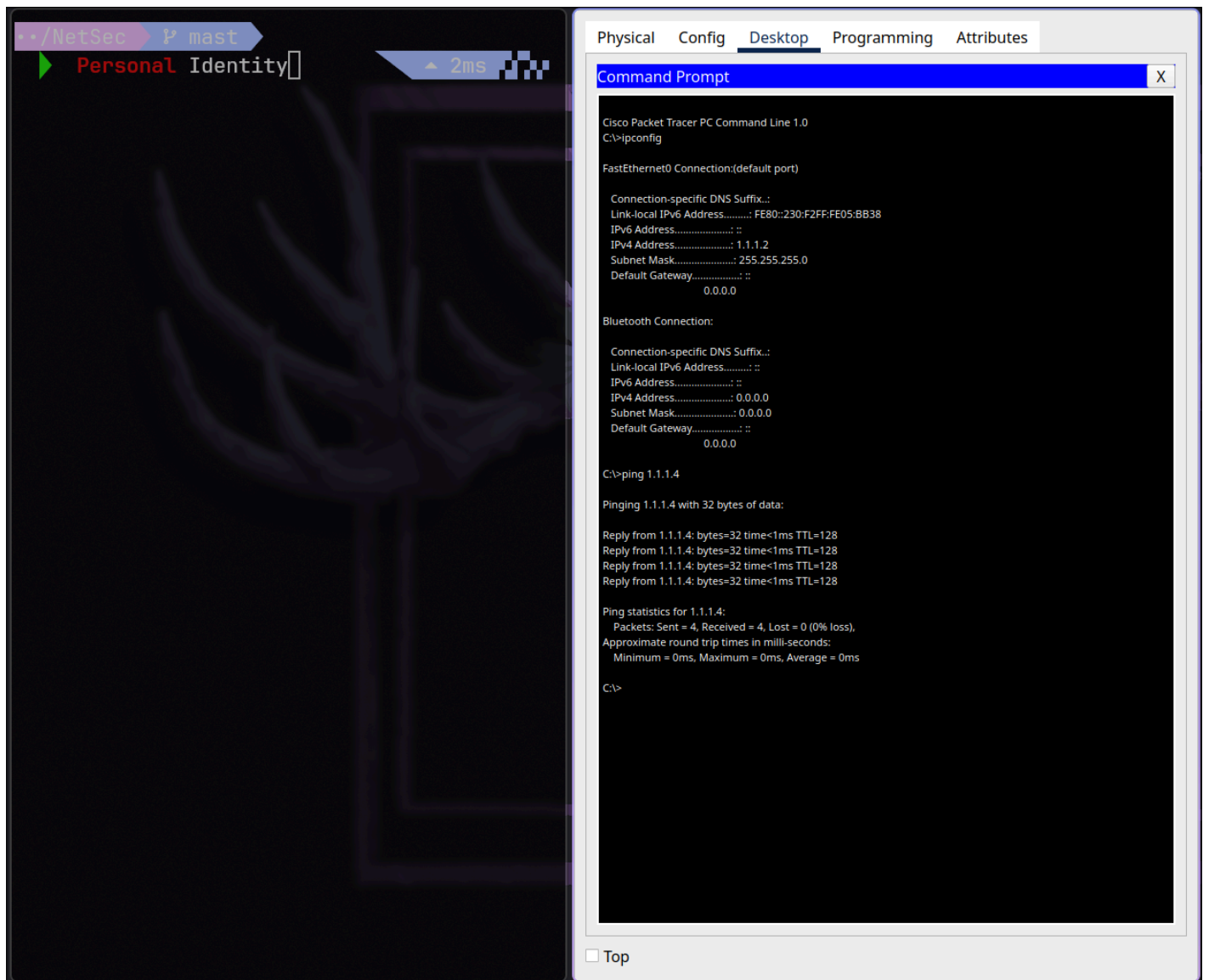


Screenshot-07: 1.1.1.1 Ping 1.1.1.3 相通(10%)





Screenshot-08: 1.1.1.2 Ping 1.1.1.4 相通(10%)



The screenshot displays a Cisco Packet Tracer simulation environment. On the left, a 'Personal Identity' window is visible. The central window shows the 'Cisco Packet Tracer' welcome screen with a 'Web Browser' tab open, displaying the URL 'http://2.2.2.2'. The right window shows a network diagram with two VLANs (VLAN10 and VLAN20) connected to a central 2960-24TT Switch0. VLAN10 contains PC-PT PC0 and PC1, while VLAN20 contains PC-PT PC2 and PC3. A 2960-24TT Switch1 is connected to Switch0 and a Server-PT. A Router is also connected to Switch0 and Switch1. The bottom status bar shows 'Time: 01:33:27' and 'Realtime' mode.

3. 以下為多重選擇題, 必須要全對該題才会有分

題目	答案
<p>在 Cisco Packet Tracer 環境中, 當兩台 Switch 之間需要透過 Trunk 連接 來允許不同 VLAN 的通訊時, 以下哪些設定是必要的?(可複選)(5%)</p> <p>A. 兩台 Switch 的連接埠必須都設為 <b>Access Mode</b></p> <p>B. 兩台 Switch 的連接埠必須都設為 <b>Trunk Mode</b></p> <p>C. 需要使用 <b>IEEE 802.1Q</b> 標準來標記 VLAN Tag</p> <p>D. 每個 VLAN 需要手動設定 <b>Static Route</b> 來確保通訊</p> <p>E. 兩台 Switch 的 <b>Native VLAN</b> 必須相同, 否則可能造成 VLAN 間的流量錯誤</p> <p>F. 只能使用 Cisco 交換器, 其他廠商的交換器無法進行 VLAN Trunking</p>	BCE
<p>當你的 Switch 網路拓撲發生 Broadcast Storm 時, 你應該如何解決?(可複選)(5%)</p> <p>A. 啟用 Spanning Tree Protocol(STP)</p> <p>B. 在所有 Switch 的連接埠啟用 BPDU Guard</p> <p>C. 在所有 Switch 的連接埠手動設定 PortFast</p> <p>D. 啟用 Root Guard 來防止 Switch 之間產生 Root 競爭</p> <p>E. 使用 EtherChannel 來將多條鏈路聚合為單一邏輯連接, 減少 STP 計算</p> <p>F. 手動設定 MAC Table 來阻擋不必要的封包</p>	ABDE
<p>當一台電腦第一次嘗試與同一網段內的另一台電腦通訊時, 以下哪些步驟會發生?(可複選)(5%)</p> <p>A. 來源端發送 ARP Request 來查詢目標端的 MAC Address</p> <p>B. Switch 會透過 MAC Table 來直接轉發封包, 而不需要廣播</p> <p>C. 目標端回應 ARP Reply, 並且 MAC Address 會被加入來源端的 ARP Cache</p> <p>D. 來源端會發送 ICMP Echo Request(Ping) 來確認目標端是否可達</p> <p>E. 如果 Switch 尚未學習目標 MAC Address, 它會將封包 Flood 到所有埠</p>	ABC
<p>假設內部 VLAN 10 的 PC 能夠存取外部 Server4, 而 VLAN 20 的 PC 無法存取, 可能的原因是?(可複選)(5%)</p>	ACEF



A. VLAN 20 沒有設定 NAT 轉譯規則	
B. VLAN 20 的 PC 沒有設定靜態路由	
C. VLAN 20 內部的 PC 沒有正確的 Default Gateway	
D. VLAN 10 的 NAT ACL 設定允許了 VLAN 20 的存取	
E. VLAN 20 內部的 IP 位址與外部網路產生 IP Address Overlap	
F. VLAN 20 的 Router 沒有啟用 NAT 設定	