

習題與實驗解答

推理過程與評分規準

核心查閱：2026-10-03；LAN 補充：2026-10-06

修訂版 v1.2 | 2026-10-08 勘誤與一致性修訂

MD 原稿與本閱讀版共用正文。

目錄

單元 01 至 02 解答	3
單元 03 至 08 與基礎實驗解答	4
單元 09 至 16 解答	6
單元 17 至 24 解答與評量規準	8
實驗補充解答與報告示例	10
LAN 補充單元與實驗解答	12

單元 01 至 02 解答

單元 01

1. 拓撲圖應包含主機到出口的連線、AP / 交換 / 路由角色、位址設定來源及 DNS 解析位置。綜合裝置可以畫一個外框，框內列多種角色。評分重點是角色及資料路徑一致，不是裝置品牌。
2. 可以。TCP 與 UDP 使用不同協定的端點識別空間，相同數字的埠號不代表相同服務。IP、埠及傳輸協定須一起辨認。
3. 此例 DNS 轉送器在本地網道位址；若尚無鄰居快取，發出 DNS 查詢時就可能先觸發 ARP。不能無條件把 ARP 排在 DNS 回應之後。
4. IP 目的地描述遠端目的端點；訊框的目的鏈路位址描述本段交付的下一跳。路由器取出 IP 封包後，在下一段建立新的訊框。
5. HTTP 200 證明某個 HTTP 端點回覆成功狀態，但內容、端點身分及中間代理仍要分析。ping 成功只能佐證有相應 ICMP 回覆。Wi-Fi 已連線只能佐證鏈路接入狀態。不能把三者互相替代。

單元 02

1. $1200 \times 8 / 10,000,000 = 0.00096 \text{ s} = 0.96 \text{ ms}$ 。常見錯誤是少乘 8，或把 ms 與 s 混用。
2. 單一封包、兩段 store-and-forward、忽略處理與排隊： $2 \times (0.96 + 1) = 3.92 \text{ ms}$ 。若是多封包流水線或不同轉送模型，要重新計算。
3. $20,000,000 \times 0.1 = 2,000,000 \text{ bits} = 250,000 \text{ bytes}$ 。這是以 RTT 定義的 BDP，不是直接量測的佇列大小。
4. TCP 提供位元組串流，沒有保留應用訊息邊界。分段、合併及作業系統緩衝會影響每次 recv 回傳的資料量；應用須自行定義 framing，例如長度前綴或分隔符號。
5. 對大檔案量測穩態有效資料率，對小請求分別分析名稱解析、建連、驗證與第一個回應時間。保持其他條件相同，避免把工作負載差異當成協定差異。
6. 利用率不足以描述到達尖峰、封包大小、服務變異、緩衝區、排程與流量相關性。特定排隊公式只在其假設內適用。

L01 判讀

本機客戶端與服務端都使用 127.0.0.1，端點以不同的埠區分。成功紀錄中，服務端看到的來源埠應等於客戶端紀錄。Content-Length 是編碼後的 bytes，不是中文字元數。404 與 connection refused 分別位於應用回應與建連失敗的不同環節。loopback 的路徑不經過家庭 AP、外部 DNS、家庭 NAT 或遠端路由，也沒有使用 TLS。

本機量測包含連線、程式處理、排程及回應讀取；單次時間差不能證明鏈路速率或單向傳播延遲改變。

單元 03 至 08 與基礎實驗解答

單元 03

1. /27 每塊 32 位址，網路位址 .160、廣播位址 .191；一般主機 .161 至 .190，遮罩 255.255.255.224。
2. .200 落在 /25，下一跳 192.0.2.66；203.0.113.9 用預設路由 192.0.2.65。
3. IP 目的識別最終 IP 端點，鏈路目的識別下一跳。本例假設沒有先做 DNAT 且路由正常。
4. PMTU/必要 ICMP 被阻擋、伺服器大回應處理失敗或 timeout 皆為假設；查封包大小、錯誤日誌與可重現負載再區分。

單元 04

1. VLAN 代表鏈路域；IP 需要正確路由 / 子網 / 政策。不同子網可能經路由器可達，不能僅以 VLAN 決定。
2. 路由判為 on-link 時 ARP 找 B；遠端選閘道時找閘道，不找遠端 C。政策路由、proxy ARP 屬另外情境。
3. 路由器移除入口鏈路封裝、為下一條鏈路重新封裝。IP 位址正常不變，TTL 變小；NAT 另列。
4. MAC 可修改，交換學習不提供密碼學身分驗證。

單元 05

1. 經 150 秒，剩 450 秒（假設沒有預取、serve-stale 等另行機制）。
2. DHCP 給設定和租約；遞迴解析器替客戶查詢及快取；權威伺服器維護 zone 的回答。
3. NXDOMAIN 表示名稱不存在；無 AAAA 只表示該名稱缺該型別；timeout 不能判定名稱不存在。
4. 已快取：stub→遞迴→快取回應；未快取：遞迴從委派鏈找到權威，再回客戶。根 / TLD 委派也可能已快取。

單元 06

1. recv 只給目前可交付且不超過上限的 bytes，不保證填滿或對齊應用訊息。
2. 報中途 EOF，拒絕交付完整 100-byte 訊息；不能把 60 當成成功。
3. TCP ACK 由傳輸接收端回報，不證明業務處理、存檔或交易提交。
4. 先檢查長度上限，採有限 buffer、timeout 與中途 EOF 處理，再讀 payload。

單元 07

1. ACK 遺失令 sender 無法知悉成功、因而重傳；receiver 用序號記錄去重，只重新確認。
2. $8000/0.0808 \approx 99010$ bit/s，約 99.01 kb/s。
3. 最大 8，避免新視窗與舊視窗在序號環上重疊。
4. 可靠串流只保障傳輸語義；業務一次執行還需請求 ID、持久化狀態、交易與去重等。

單元 08

1. SYN 後 1001 起，送 300 bytes，下一期待 byte 為 1301。

2. cwnd 若限制在途量，增加 rwnd 不解除此限制。
3. 零視窗先查接收應用是否停讀及 buffer；遺失 / 逾時查路徑、重排、RTT 及遺失恢復。兩者可能同時存在。
4. 平均值無法描述多流競爭、RTT 優勢、排隊、CPU 與尾端延遲。

L02 至 L08、L10 與 L11

預期輸出（完成預測與紀錄後再核對）：L02 三段 6.36 ms、BDP 500000 bytes、視窗上界 13.1072 Mb/s。L03 網路 .160、廣播 .191、一般主機 30 個、遮罩 255.255.255.224；.20 選 /24、.140 選 /25。L04 id=4660 (0x1234)、flags=0x8180，lesson.test 的 A 為 192.0.2.80、TTL 300；c00c 指回 offset 12。L05 TCP 依序得到 cat、網路與空字串，UDP 得到 cat、網路兩份資料報；recv 每次最多 2 bytes 仍能正確重組。L06 資料 0 與 1 各傳兩次，應用仍只交付 [0,1,2,3,4]。L07 A 到 B、C、D 成本為 2、3、4，D 路徑 A-B-C-D。L08 前兩次入站允許、第三次拒絕，外部對映始終是 203.0.113.5:40000。L10 未計額外 padding 時，outer IPv4 預算 1440、outer IPv6 預算 1420 bytes。L11 A 中位 10.5 ms、p95 50；B 中位 13.5 ms、p95 16。

L02：RTT 加倍使 BDP 加倍，在固定視窗且受 W / RTT 限制時，上界減半；真實 TCP 還受 cwnd 及應用限制。

L03：新增 198.51.100.128/26 後，.140 選 /26，.200 仍選 /25。IPv6 的 2001:db8::80 選 2001:db8::/32，2001:db9::80 選 ::/0；IPv4 路由不匹配 IPv6。更具體但有效的路由被選中；實際下一跳失效是否移除路由、切換備援或仍黑洞，依協定、偵測與平臺，不能保證自動改走預設路由。

L04：QR=1、RD=1、RA=1 是人工回應中的位元，Answer=1。fixture 不能證明 lesson.test 在公共 DNS 存在。NOERROR 且空 Answer 不能推出名稱不存在，可能是該型別無資料、委派或其他情況，需看 Question、authority 及整份訊息；NXDOMAIN 的 RCODE=3 表示查詢名稱不存在。

L05：應用限制 recv 為 2 並不限制 TCP 段大小。4-byte 大端長度定義訊息大小；中途 EOF 應失敗。UDP 用足夠 buffer 觀察兩份資料報。

L06：receiver 先交付 0，但 sender 因 ACK 0 遺失保留未確認；再次收到 0 只 ACK。去掉 ACK 遺失規則後資料 0 只傳一次；--window 1 相當於停等，需 7 回合，預設視窗 3 只需 3 回合。缺少真實時間、序號回繞、TCP byte 序號、cwnd 與核心演算法。

交換表演練：A→B 學 A→1，泛洪 2、3；B→A 學 B→2，只送 1；C→A 學 C→3，只送 1。假設三個埠同 VLAN 且皆可轉送。

L07：原 A-B-C-D 成本 4；改 B-C=10 後 A-B-D 和 A-C-D 皆成本 6；本實作以嚴格小於比較，先處理 B 後保留 A-B-D。等價成本可能有多個正確最短路徑。BGP 還有政策與路由屬性。

L08：EIM 與過濾是獨立欄位；ADF 允許聯絡過的 remote IP 任意 port。改用 --filter APDF 時只有 198.51.100.10:9000 可入站；--elapsed 120 --lifetime 60 時 state 已逾時、對映消失，三次皆拒絕。STUN 回報特定時間及目的下對映，不保證雙方過濾、回程、逾時與其他 NAT 相容。

L10：1500 減 20/40、8、16、16 是預算，仍需檢查 padding、實際路徑及實作選定 MTU。endpoint 需可由 underlay 到達，避免遞迴進入自己的隧道。

L11：A 中位較小、B 這份樣本尾端較小。p95 nearest-rank 以 10 筆取第 10 筆；樣本太少不能穩健估計稀有尾端，也不能比較真實代理。

單元 09 至 16 解答

單元 09 期中題組

1. 網路 192.0.2.64、廣播 .127、一般主機 .65 至 .126。DNS 同網段所以找 .66 MAC，遠端走閘道 .65。完整範圍 10 分、兩次鄰居對象各 5 分。
2. ARP→DNS→路由/閘道鄰居→TCP→HTTP，按本題條件；快取 / IPv6 等會改變。DNS 只提供名稱資料，不證明 TCP、TLS 或 HTTP。依賴 12 分、限制 8 分。
3. BDP 125000 bytes，視窗 65536 小於 BDP；上界 10.48576 Mb/s，內容下界 0.76294 秒。各結果及單位合 20 分；未計啟動與開銷。
4. Content-Length 計 UTF-8 等實際編碼 bytes。中途 EOF 不得當完整內容；使用 HTTP parser 時不足長度應報 IncompleteRead 等錯誤。兩項各 10 分。
5. 正向丟棄、回程不可達、server 未回、state policy 等兩項不同假設各 5 分；提出出口 SYN 和服務端接收/回覆證據 10 分。

單元 10

1. B 經 A-B 成本 2、C 經 A-B-C 成本 3、D 經 A-B-C-D 成本 4。
2. A-B-D 與 A-C-D 皆成本 6，tie-breaking 可選其一或依能力 ECMP。
3. 各節點取得失效與更新資訊的時間不同，舊表可不一致；迴路防護與收斂機制需明列。
4. BGP 考量 AS 政策、授權與屬性，沒有單一全域成本圖決定所有組織願意轉送的路徑。

單元 11

1. 2001:db8::10:1。
2. 通常 RA；DHCPv6 沒有預設路由選項。其他手動設定情境另列。
3. global 位址可路由仍需路徑、服務監聽及允許的防火牆政策。NAT 和存取控制不同。
4. 查 OS 路由、peer 選擇、DNS/AAAA、接管入口、出口與回程，涵蓋 0.0.0.0/0 與 ::/0 的政策及 endpoint 例外。

單元 12

1. EIM 只描述對映；入站可能仍 ADF/APDF。
2. STUN 回報特定目的看到的對映並可做連通性檢查；TURN 提供 relay。
3. ISP 的上游對映仍擋在家用路由外，家庭 port forward 不自動建立 ISP 轉送。
4. NAT 對映可能隨目的、協定、state、時間不同；單次觀察不能覆蓋所有組合。

單元 13

1. 普通 hash 無共享祕密，攻擊者可對修改資料重算；MAC 有 key 並提供對應認證。
2. 舊密文 tag 可仍有效，需要 session、序號視窗或已見材料等狀態防重放。

3. 固定 PSK 洩漏可能解開使用其衍生 key 的舊資料；臨時 DH 在祕密正確銷毀、協定驗證正確條件下提供 PFS。
4. 代理需知道最終目的以建立出口；外層加密保護路徑觀察者，不能隱瞞解密端本來就需處理的請求。

單元 14

1. 信任鏈與名稱是獨立檢查，SAN 須符合預期名稱。
2. 未啟用 ECH 時 SNI 通常可見。成功 ECH 仍有外層 public_name、IP、大小 / 時間，其他 DNS 管道可能暴露目標。
3. 代理可見請求目的、出口 IP 及未被 ECH 保護的協商資訊，未終止內層 TLS 則不直接讀 HTTP 內容。
4. AEAD 驗證完整性不記住已執行操作，0-RTT 有重放風險及不同 PFS 條件，業務需另行處理。

單元 15

1. H2 frames 仍在同一條可靠有序 TCP 中，遺失缺口阻止後續 bytes 交付。
2. stream 按該 stream 可靠有序交付，DATAGRAM 不重傳、可能遺失，仍受壅塞控制。
3. cwnd、連線級流控、路徑、CPU、QPACK 和應用依賴都可產生等待。
4. no-cache 通常要求使用前驗證，不禁止儲存；no-store 禁止儲存該內容的指令語義。

單元 16

1. PHY rate 不等於應用有效速率，媒介競爭、干擾、重傳、標頭、回程及端點能力都會影響。
2. TCP 是否建成、TLS 驗證是否成功、HTTP 對端回應與狀態、內容等依次查；DNS 成功不能代替它們。
3. 固定 route/server/load 比較空間與負載期間 RTT 分布、瓶頸排隊及負載停止後恢復；註明對照與計時。
4. 還缺版本、路徑、工作負載、樣本數、尾端 / 變異、CPU、同時競爭與有效 bytes 定義等。

單元 17 至 24 解答與評量規準

單元 17

1. 否，TCP 可分兩段，內層 TLS 仍由 C 到 S；TLS 終止需另行設計與驗證。
2. 普通 CONNECT 是 TCP 隧道；UDP 需 CONNECT-UDP 等擴充，不是任意 IP 轉送。
3. ATYP 域名可交 P 解析，送 IP 則名稱可能已在 C 解析；實際軟體選項需核對。
4. P 是外層解密 / 代理請求端，需要知道目的，不因外層 TLS 而不知情。

單元 18

1. salt / nonce 是衍生或加密材料，PFS 需長期祕密洩漏不能重建過去會話的 key establishment，單用 PSK 通常不滿足。
2. 格式、key 來源與長度、ciphers、重放狀態、時間檢查及兩端支援，不能只看 AEAD 名稱。
3. VMess 與 SS2022 都可有協定認證的時鐘條件；TLS 憑證則有信任 / 名稱 / 有效期條件；TCP 可達不表示它們成功。
4. 否。外層與內層 key/端點不同，外層 PSK 洩漏可暴露代理目的等，但經正確臨時金鑰協商的內層 TLS 可仍有 PFS。

單元 19

1. VLESS 為代理 protocol，TLS/REALITY 為 transport-security，Vision 為特定 flow，TUN 為 IP 接管介面；WG 為 IP 隧道。
2. 基礎 none 層不加密，新擴充則有特定握手/保護與相容需求，不能把新能力推給全部舊版本。
3. 否，transport/security 相容不等同 flow 相容，需查指定核心與組合。
4. TLS 驗證預期同儕，保密/完整性保護通道；padding 只改部分長度外觀，不保證端點可信或無法辨識。

單元 20

1. TCP 使用可靠 stream，UDP 走不重傳 DATAGRAM；fragment 遺失也可讓整份資料報丟失。
2. 代理段可恢復遺失，卻使舊 UDP 內容延遲到達，需以 deadline 交付率衡量。
3. 否。代理命令並行 / 免等待與 TLS 會話恢復、early-data 是不同層次，需獨立驗證。
4. 過高固定速率 / 補償可使排隊、丟包和競爭加劇，不創造實體頻寬。應設競爭對照。

單元 21

1. 否，OS 還需把封包送到 WG 介面，AllowedIPs 只在 WG 內選 peer 及驗內層來源。
2. peer 解密後可能轉到明文目的，該段需另行保護；peer 知道目的 IP，端點與設定分發也有信任要求。
3. IPv6 使用另一套位址/route，需要 ::/0 等有效策略及出口；IPv4 前綴不匹配 IPv6。
4. 以 TCP 為外層的 IP VPN (如 OpenVPN TCP 模式) 可將原始 TCP 段保留在外層 TCP 中產生雙重恢復；普通 TCP 代理終止原始 TCP 並轉 bytes，是不同模型。WireGuard 外層為 UDP，不形成 TCP-over-TCP。TLS

套 TLS 也不是雙重 TCP 的同義詞。

單元 22

1. 否，TUN 只提供 IP 介面；通道保護、路由、雙協定和 policy 需另行檢查。
2. 系統 proxy 依應用遵守，UDP 支援還依 app 與 relay，未接管資料可走原出口。
3. DoH/DoT 僅改變 DNS 的傳送保護，實際出口仍由路由與接管決定，resolver 仍見查詢。
4. 單次網站測試不能確認所有 apps、UDP、IPv6、DNS、DoH、LAN、P endpoint 和故障 fallback。

單元 23 開放題範例

1. 可反駁假設：「L09 的源站 peer 等於 P 上游 socket 而非 C source」，以端點日誌比對反駁。
2. 設計 A 顯式 SOCKS 入口；B 為 IP VPN 的離線推演，分別列 app 繞過和 OSroute 缺口。
3. L09 證明兩段 TCP 端點，L13 證明 TLS 名稱/信任；它們分開執行，不能證明已部署了一個有 TLS 的 SOCKS 代理。
4. 控制源站與 payload；未控制 OS 背景排程與 CPU 競爭，計時需多次與分布。

單元 24 期末 100 分

1. 15 分：題目只給企業私網路由，普通 IPv4 網站應依其他 IPv4 路由（通常為實體出口的預設路由），不能僅憑私網 route 斷言有外網路由；2001:db8::80 依 OS 的 IPv6 路由，沒有有效 IPv6 路由則不可達，若應用有 IPv4 候選才可能退回 IPv4。兩者都不匹配 10.10.0.0/24。雙協定全隧道還需 OS 路由、WG peer 的 AllowedIPs、endpoint 例外、DNS、出口與回程政策。wg-quick 等工具可能另建路由，要看最終表。路由判斷 5 分，完整條件 10 分。
2. 15 分：VLESS 為代理 protocol，TLS / REALITY 為 transport security，Vision 為 flow，WebSocket 為 transport；TUN 為 IP 接管介面，WireGuard 為 IP VPN（七個名稱分類共 7 分）；說明 TUN / WG 不能與 VLESS 同欄替換（3 分）；此次文件 WebSocket + REALITY 不相容，transport/security 支援也不保證 flow 支援，需指定版本核對（5 分）。
3. 15 分：分別說明 PSK 與臨時協商 / PFS 條件、獨立重放狀態、代理需知目的；每項 5 分。不得以 AEAD 直接推 PFS。
4. 15 分：stream 可靠有序（5 分）；QUIC DATAGRAM 不提供遺失重傳及有序交付保證（5 分）；100 ms 的 deadline 內交付率與最終到達率不同，可靠轉送可能交付已過期內容（5 分）。
5. 10 分：1492-40-8-16-16=1412 bytes（6 分）；外層條件、padding、實際 PMTU 及內層 IPv6 等限制（4 分）。
6. 15 分：對齊 hostname/SAN/服務和 route（7 分），保留鍵/名稱驗證（4 分），再測正負對照（4 分）。不能僅停用驗證。
7. 15 分：IP 網頁僅證明該請求路徑（5 分）；UDP/IPv6/DNS/DoH/直接 IP/LAN/endpoint 逐項預期及證據（10 分）。專題另依 23 單元 100 分規準。開放設計可多解；必要的是明確假設、重現方法與符合證據範圍的推論。

實驗補充解答與報告示例

L09

三種模式的源站都回 HTTP 200；每次的 C source 都等於 P client peer，S 看到的 peer 都等於 P origin source。CONNECT 200 之後轉送客戶端送的 payload，本例為 HTTP 明文，可讀內容；不能由此實驗判斷 HTTPS 不可讀。origin_peer 是 P 出口 socket，因為 P 重新建立到 S 的 TCP；C↔P 與 P↔S 端點分開。增加 HTTPS 需要在隧道上建立經驗證的 TLS 並確認 TLS 終點，不能直接串接兩份獨立輸出。CONNECT 子集不證明 UDP ASSOCIATE、BIND 或 IPv6 能力。

L10 與 L11 補充

outer IPv4 預算 1440、outer IPv6 預算 1420 是 1500 減外層開銷；不同 underlay、padding 與嵌套會改變。IPv6 承載要求合適最小鏈路 MTU。A 樣本中位 10.5、p95=50，B 中位 13.5、p95=16；nearest-rank 定義明示，n=10 的 p95 就是最大，不當真實協定排名。

L12

A 已證明無線關聯，但未拿有效租約/route；先看 DHCP、介面與鏈路，不以改 DNS 替代設定。B 說明預期名稱不符，可為連錯 server 或憑證部署錯；修正匹配、保留驗證。C 的 PMTU / 必要 ICMP 問題和應用大回覆 timeout 都可解釋，需 packet 大小/ICMP/服務端日誌區分。D 表示該網站請求經 P，UDP/IPv6 的實際出口違反全流量意圖；改 DNS 加密不自動改變資料接管。

L13

預期 verified=[true,false,false]：正確案例收到 reply:lesson；錯名稱及未信任都是 SSLCertVerificationError。離線表的判讀：localhost + 明確信任可通過（仍假設有效期與用途符合）；wrong.test 因名稱不符失敗；未信任案例因信任不足失敗。TCP 成功只說明可建傳輸連線；TLS 還驗名稱/chain/key。明確信任和 hostname 獨立，trusted 錯名仍應失敗。關閉 hostname 或驗證把問題隱去並失去端點身分保證。憑證工具與 Python SSL backend 不同，cipher/validation/版本支援可能不同，兩者版本都記。離線路線只能支持條件式推論。

L14

A1：protocol VLESS；encryption none；transport RAW；security TLS；flow Vision；capture SOCKS。A2：此次文件 WebSocket 不配 REALITY。A3：SS2022 PSK/AEAD 在 C-P，內層 HTTPS 在 C-S；長期 PSK 洩漏與內層 TLS 分別分析。A4：TCP 經可靠 QUIC 雙向 stream，UDP 經不可靠 DATAGRAM。A5：TUIC native DATAGRAM 對比 quic 單向 stream 可靠 relay。A6：WG 轉 IP，OS 僅送私網，非預設全隧道。

B：proxy 目的欄位可帶 IP / domain，bootstrap 與目標 DNS 分別寫；PSK、憑證 / peer 設定與會話 key 不混為同一 key。AEAD、重放、PFS 分別評估。C：至少檢查 IPv4/TCP、IPv6/TCP、UDP、DNS/DoH、RA/default-route、直接 IP、LAN 與 endpoint 例外；網頁出口證據不能代替各列。

一份合格的短報告示例

假設：L09 源站見 P 出口。觀察：C source=127.0.0.1:51001，P client peer 同值；P proxy_origin_source=127.0.0.1:51002，S peer 同值（埠為人工示例，非固定預期）。推論：此次模型有兩段 TCP，與代理轉 bytes 一致。限制：未抓握手、未測試外部 DNS、TLS、UDP 與真實核心。下一份證據：若測試 HTTPS，需獨立建立內層 TLS 並驗證名稱/信任與 endpoint。

評分需看事實與解釋相連、結果可重複、資料分類清楚；沒有指定真實核心版本，不得給「協定實測」證據分。

新增工作表解答

L10：MTU 1492 時，outer IPv4 預算 $1492-20-8-16-16=1432$ bytes；outer IPv6 為 1412。普通 TLS/TCP 代理例為 $20+20+5+1+16+20+1000=1082$ bytes，剩 418；若將相同內層應用資料分成兩份 TLS record，增加的內層 header/content-type/tag 等需按實際 cipher、padding 重算。TCP 可跨段 / 合段，以上只在單段人工假設成立。

L11-B：A 期限內成功 $0.95 \times 0.99 = 94.05\%$ ，晚到 $0.95 \times 0.01 = 0.95\%$ ，未到 5%；B 期限內 88%、晚到 12%、未到 0%。A 此分布的期限內成功也較高，不能只用條件百分比 99% 對比 B 的 88%，更不能僅從最終到達率選方案。L11-C 應有四格獨立工作負載及相同控制條件，首次 / 恢復和小 / 大內容分開；恢復不一定啟用 0-RTT，CPU 與 goodput 仍需原始資料。

L12-E：S 可能經 R2 回 C，使 R 的反向轉換狀態未被使用；R2 若無匹配狀態，不能憑空把來源 S:8443 改回 R 的公開端點。還需查 R2 路由、回程擷取及其他政策，不能只由題目斷言唯一原因。修正可讓 S 對 C 的回程經 R，或在 R 做適當 SNAT 使 S 回到 R（代價為 S 不再直接看到 C 原始 IP）；再查兩端四元組與 R 狀態，確認來源反向轉換及回程。

L14-E：H2 後續 bytes 即使含 stream 2 / 3，也需等 TCP 缺口補齊才交付上層；H3 不需等獨立 stream 1 缺口，2 / 3 可先交付。QUIC 共享壅塞控制、CPU 等，且本題排除了 QPACK / 應用依賴，不可推論任何工作負載都不互相影響。

LAN 補充單元與實驗解答

單元 03A

1. 多個三層位址共用 eth0，並未建立 VLAN、埠隔離或 ACL；仍共用二層廣播域。同 VLAN 不同子網能否 IP 互通需另看直連 / 路由及主機設定。
2. 只有 main 時仍走 G1，來源保持 198.51.100.10。G1 與遠端須可回此來源，防火牆 / NAT 狀態也需允許；bind 並不指定閘道。
3. priority 100 查 200 已用 default 成功，所以不繼續查 main 的 /24。修正可在 200 補該直連 /24；或以更早且精確的目的規則查含該 /24 的 main。後者要避免誤將更廣目的含入 main default。
4. src 是未固定來源時的偏好，不是 SNAT。已指定來源 1 保持來源 1；轉送改寫需獨立的 NAT 機制。
5. 保留 priority 0 的 local 後，在 priority 100 之前加目的 /32 例外，例如 `ip rule add priority 50 to 203.0.113.81/32 lookup main`。分別測試無來源、來源 1、來源 2；來源 2 仍在 main 走 G1，還須驗 endpoint 回程。若例外放 150，100 的 default 先成功，目的例外不會執行。
6. 以相同連線 ID 與時間比對 LAN 入口和代理上游來源四元組、OS 查表與實體出口。兩段 socket 屬代理模型；不能由 LAN 客戶端來源規則推論上游匹配。涉及 mark 時要說明設定與恢復時機。

單元 04A

1. 泛洪改變副本出口，目的 MAC 仍是單播；接收端通常不把別人的單播副本交給普通 socket。多埠看見不等於廣播。
2. IPv4 群組的低 23 bits 相同，皆對映到 01:00:5e:40:00:2a；仍是不同 32-bit IP 群組。MAC 過濾不保證精確，IP 與應用層還需匹配。
3. snooping 限制本 VLAN 交換副本；querier 詢問並維持成員資訊；PIM 等多播路由控制在路由器間建立跨鏈路轉送。開 snooping 不代表已開跨 VLAN 多播。
4. 一埠後方可能接 AP 或下游交換器，有多個接收者。應確認成員狀態 / 查詢結果，不能僅依某一主機 leave 刪除整埠。
5. 假設一：mDNS 被 VLAN 邊界 / ACL 限制，查兩端 5353 與 group/interface。假設二：根本未公告所查服務或 cache 過期，查 PTR / SRV / TXT 與 server 狀態。ping 只支持 ICMP 單播可達，不能替探索作證。
6. 不行。服務廣告不提供可信身分；若實際連 HTTPS 仍需獨立驗證名稱 / 信任。一般 IPP 631 可能另有其安全模式，應先確認協定與預期端點。

L15 查表與設定解答

案例	結果	關鍵
no_policy	main , G1	bind 來源 2 未改下一跳
source_unspecified	main , G1 , 偏好來源 1	來源 2 規則未匹配
source_policy	200 , G2	priority 100 命中來源 2
lan_correct	200 , on-link	200 內 /24 勝過 /0
lan_missing_route	200 , G2	default 終止查表，不讀 main
endpoint_exception	main , G1	priority 50 早於 100
local_delivery	local , 本機	priority 0 先成功
throw_fallthrough	main , on-link	200 命中 throw 後繼續
explicit_reject	200 , unreachable	終止，不繼續 main

no_policy 與 source_policy 來源相同；只有表與下一跳改變。設定 src 不會改寫已指定來源。移動 endpoint 例外到 150 後，來源 2 先在 200 選 G2；未指定來源仍可由例外 50 / 150 查 main，需按 case 獨立分析。

Linux 腳本的 203.0.113.80 分別由兩個隔離 namespace 擁有，僅方便觀察出口；不能聲稱測試同一 Internet 主機經兩家 ISP。route get 是核心查表結果，不代表 ARP、回程或應用成功；ping 及 neigh 另提供有限證據。未實際執行的 Linux 路線不列入本機測試通過項目。

L16 交付與服務探索解答

案例	模型出口	原因
unknown_unicast	2、3、4	VLAN 10，排除入口 1 與 VLAN 20 埠 5
known_unicast	2	FDB 命中 B
broadcast	2、3、4	廣播域
multicast_known	2、3、4	成員 2、3 與 router port 4
multicast_after_leave	2、4	假設已確認移除 3
multicast_after_expiry	2、3、4	無有效成員，unknown=flood
multicast_unknown_drop	4	unknown=drop，仍保留 router port
mdns_link_local	2、3、4	模型 link-local 特例
multicast_snooping_off	2、3、4	同 VLAN 泛洪

移除 router port 後，known 只送 2、3；unknown=flood 仍送 2、3、4，unknown=drop 送空集合。收到泛洪副本不證明主機 join，也不證明 socket 交付。埠 3 改 VLAN 後不能再作 VLAN 10 成員，合法成員與出口都需重新推導。

IPv6 延伸需加入 scope、IPv6 群組 / 33:33 對映、MLD 控制、鏈路特殊群組與 router port 政策；不能只把 IPv4 字串換長。模型的 leave 與 expire 是人工狀態變更，未驗 IGMP / MLD 計時器。

工作表：mDNS 是 224.0.0.251 / ff02::fb，UDP 5353；後續 IPP 可往 SRV 指定 printer:631 單播連線，TXT 的 rp 可協助找資源路徑。跨 VLAN 單播可達不會讓 link-local 探索自動穿越；PTR 可見不保證 A/AAAA、port 或服務接受。AAAA 失敗需看解析結果、實際選擇、IPv6 路由、ACL 及服務端日誌，IPv4 成功僅是另一條路徑證據。

反射 gateway 應限制來源 / 目的 VLAN、允許的服務類型與裝置，避免把管理服務廣告意外帶入訪客區；可見性限制與實際服務 ACL / 驗證分開檢查。

LAN 整合評量

新增必讀單元的評量以替換為原則：09 期中第 1 題可改用 03A 題 2 / 3 與 04A 題 1 / 3 的情境；24 期末第 1 題可改用代理上游來源案例，第 7 題可改用跨 VLAN 印表機案例。總分與評量比例不變，題目替換而非無限增加負荷；各替代題的配分見本節最後一段。

專題可選「單介面雙來源政策與 LAN 例外」或「跨 VLAN 探索與單播服務路徑」。離線模型專題需明示 kind=model；Linux 或真實設備專題另附版本、拓樸、原始證據與清除方法。不能以圖表漂亮取代路徑證據。

09 替代題 20 分：依 L15 表預測來源 2 遠端走 200 / G2、LAN 走 200 / 直連，兩案各 6 分含規則 / 表 / 下一跳；未知單播與已知多播各 4 分，須明示 FDB 泛洪與 MDB 成員加 router port，VLAN 邊界不跨越。24 替代第 1 題 15 分：兩段來源 / 查表差異 8 分，LAN 與 endpoint 例外 7 分；替代第 7 題 15 分：探索 3、SRV 與雙協定位址 3、資料路徑 3、可區分的證據與限制 6。