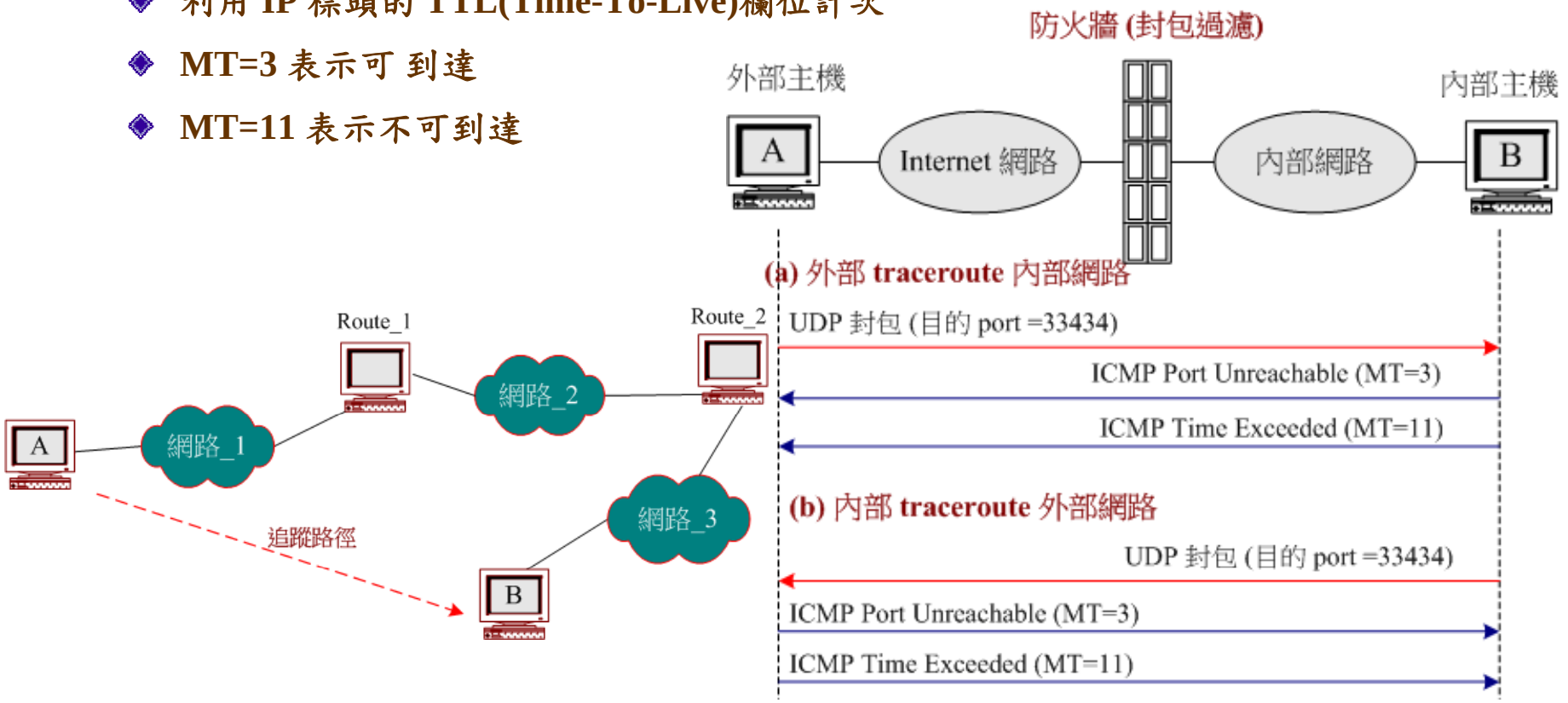
ICMP 範例： traceroute 封包過濾

- **traceroute 命令運作**
  - **UDP 封包發送，33434 ~33523 埠口**
  - **利用 IP 標頭的 TTL(Time-To-Live)欄位計次**
  - **MT=3 表示可 到達**
  - **MT=11 表示不可到達**



traceroute 封包訊息表

Traceroute 封包訊息表

編號	封包方向	址	目的位址	協定型態	來源埠口	目的埠口	訊息型態	封包功能
1	進入	外部	內部	UDP	>1024	33434 ~ 33523		外部進入 traceroute 的UDP 封包。
2	出去	內部	外部	ICMP			3	內部主機回應外部UDP 封包的 ICMP Port Unreachable 封包。
3	出去	內部	外部	ICMP			11	內部主機回應外部UDP 封包的 ICMP Time Exceeded 封包。
4	出去	外部	內部	UDP	>1024	33434 ~33523		內部主機向外部網路 traceroute 所送出的 UDP 封包。
5	進入	內部	外部	ICMP			3	外部主機回應內部 UDP 封包的 ICMP Port Unreachable 封包。
6	進入	外部	內部	ICMP			11	外部主機回應內部UDP 封包的 ICMP Time Exceeded 封包。

traceroute 封包過濾規則表

- 封包過濾規則表
  - 允許內部主機的 traceroute 命令通過防火牆，但不允許外部網路以 traceroute 命令來測試內部網路。

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	訊息型態	措施
A	出去	內部	外部	UDP	>1024	33434 ~33523	Null	允許
B	進入	外部	內部	ICMP	Null	Null	3	允許
C	進入	外部	內部	ICMP	Null	Null	11	允許
D	任意	任意	任意	ICMP	Null	Null	任意	拒絕