I428034

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I428034 B**

(45)公告日： 中華民國 103 (2014) 年 02 月 21 日

(21)申請案號：099121944 (22)申請日： 中華民國 99 (2010) 年 07 月 02 日

(51)Int. Cl.： *H04W28/02 (2009.01)* *H04W76/04 (2009.01)*

(71)申請人：國立交通大學 (中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)
新竹市大學路 1001 號

(72)發明人：林盈達 LIN, YING DAR (TW) ；鄭宗寰 CHENG, TSUNG HUAN (TW) ；賴源正 LAI, YUAN CHENG (TW) ；陳一瑋 CHEN, I WEI (TW)

(74)代理人：許世正

(56)參考文獻：

US	7376969B1	US	7653006B1
US	2002/0049899A1	US	2004/0090923A1
US	2005/0240656A1	US	2009/0252050A1

審查人員：賴慶仁

申請專利範圍項數：22 項 圖式數：13 共 0 頁

(54)名稱

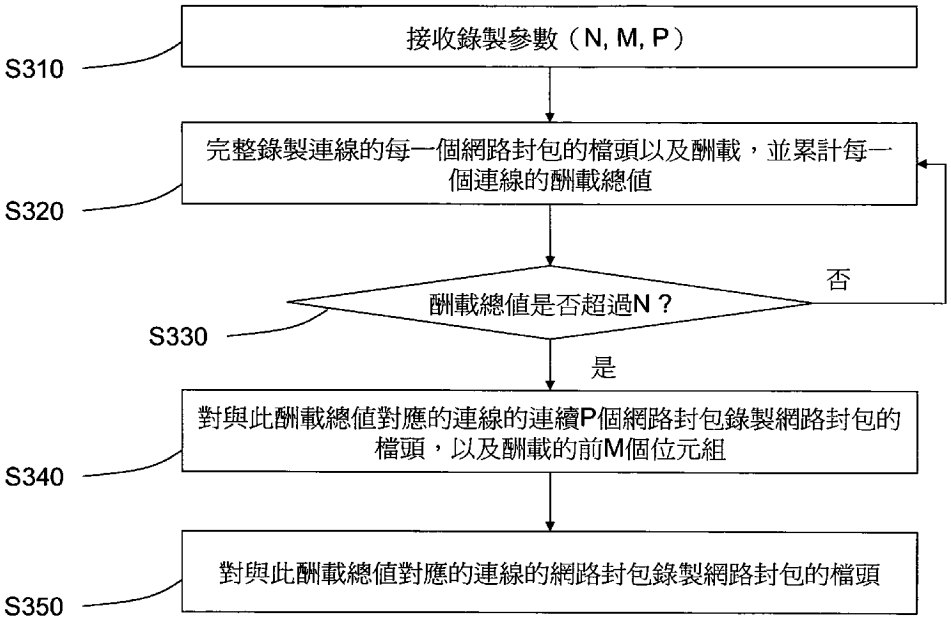
錄製、還原與重播網路流量的方法

RECORDING, RECOVERING, AND REPLAYING REAL TRAFFIC

(57)摘要

一種錄製、還原與重播網路流量的方法係用以處理多個網路連線的多個網路封包。錄製、還原與重播網路流量的方法可包括錄製程序、還原程序或是選擇性重播程序。其中錄製程序包括：接收錄製參數(N,M,P)；完整錄製每一網路封包的檔頭以及酬載，並累計每一網路連線的酬載總值；當酬載總值之一超過 N 時，對與酬載總值對應的網路連線的連續 P 個網路封包錄製每一網路封包的檔頭，以及酬載的前 M 個位元組；以及當酬載總值之一超過 N 並對與酬載總值對應的網路連線連續錄製 P 個網路封包之後，對與酬載總值對應的網路連線錄製每一網路封包的檔頭。

A method for recording, recovering, or replaying real traffic is adapted to process a plurality of packet of a plurality of connection. The method may include a recording process, a recovering process and a replaying process. The recording process includes the steps of receiving a recording parameter (N, M, and P); recording completely a head and a payload of the packets in a connection, and accumulating a payload accumulation value; recording the head and the former M bits of the payload of the continuous P packets in the connection corresponding to the payload accumulation value, when the payload accumulation value is greater than N; and recording the head of the packets in the connection corresponding to the payload accumulation value after recording the continuous P packets.


接收錄製參數（N, M, P）
S310
完整錄製連線的每一個網路封包的檔頭以及酬載，並累計每一個連線的酬載總值
S320
酬載總值是否超過N？
否
S330
是
對與此酬載總值對應的連線的連續P個網路封包錄製網路封包的檔頭，以及酬載的前M個位元組
S340
對與此酬載總值對應的連線的網路封包錄製網路封包的檔頭
S350

第2圖

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：99121944

※申請日：99.7.02　　※IPC 分類：H04W 28/02 (2009.01)
H04W 76/04 (2009.01)

一、發明名稱：（中文/英文）

錄製、還原與重播網路流量的方法

Recording, Recovering, and Replaying Real Traffic

二、中文發明摘要：

一種錄製、還原與重播網路流量的方法係用以處理多個網路連線的多個網路封包。錄製、還原與重播網路流量的方法可包括錄製程序、還原程序或是選擇性重播程序。其中錄製程序包括：接收錄製參數（N, M, P）；完整錄製每一網路封包的檔頭以及酬載，並累計每一網路連線的酬載總值；當酬載總值之一超過 N 時，對與酬載總值對應的網路連線的連續 P 個網路封包錄製每一網路封包的檔頭，以及酬載的前 M 個位元組；以及當酬載總值之一超過 N 並對與酬載總值對應的網路連線連續錄製 P 個網路封包之後，對與酬載總值對應的網路連線錄製每一網路封包的檔頭。

三、英文發明摘要：

A method for recording, recovering, or replaying real traffic is adapted to process a plurality of packet of a plurality of connection.

The method may include a recording process, a recovering process and a replaying process. The recording process includes the steps of receiving a recording parameter (N, M, and P); recording completely a head and a payload of the packets in a connection, and accumulating a payload accumulation value; recording the head and the former M bits of the payload of the continuous P packets in the connection corresponding to the payload accumulation value, when the payload accumulation value is greater than N; and recording the head of the packets in the connection corresponding to the payload accumulation value after recording the continuous P packets.

四、指定代表圖：

(一)本案指定代表圖為：第（2）圖。

(二)本代表圖之元件符號簡單說明：

無。

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無。

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種錄製、還原與重播網路流量的方法，特別是關於可包括錄製程序、還原程序或是選擇性重播程序的方法。

【先前技術】

關於錄製流量的技術，習知做法包括以特殊專屬的硬體設計搭配各種軟體套件來實作，以盡量減少漏錄（capture loss）情況的錄製系統。這種技術的重點常在於討論前置處理器的數目、作業系統、緩衝區大小等等議題。除了提升軟硬體系統效能的技術之外，也有類似時光機器（Time Machine）的技術，以分析網路流量行為的方式來節省儲存空間。這種技術採用10000～20000位元組（bytes）的截斷（cutoff）機制來錄製每條網路連線。由於其發現大流量通常是來自於少數的連線，因此從整體來說，時光機器的技術可以完整錄製到多數小流量的網路連線。而其截斷值係根據對於流量的剖析作動態調整。

然而這些技術卻都不是從「觸發/重製網路事件」的測試用途出發來決定錄製流量的策略、設計錄製流量的方法，而導致目前這些的錄製技術與方法並不十分適合用來作為測試之用。且習知技術需要浪費龐大的儲存空間去儲存沒有價值的網路流量，因而無法完全錄製大量且快速的真實網路流量。更甚者，由於無法應付大量且快速的真實網路流量，而造成漏錄的

情形。

而關於重播網路流量的技術，例如 TCPreplay 係根據時間戳記（timestamp）進行重播；Tomahawk 則會等待上一個封包抵達之後再重播下一個封包。然而這兩種技術在重播網路流量的過程中並沒有維持網路協定的狀態，而產生無狀態重播（stateless replay）的問題。

對此發展出了數種能維持網路協定的狀態（稱為狀態重播，stateful replay）的技術。例如 TCPopera 在重播網路流量時使用 4 種試探法（heuristics）來達到依照傳輸控制/網際網路協定（Transmission Control Protocol/Internet Protocol，TCP/IP）傳送資料的規則。Monkey 則是會自行建立插座（socket）以模擬 TCP/IP 協定並模擬網路情況。Avalanche 則可接受一份追蹤檔案（trace file）樣本，並自行分析追蹤檔案後模擬出同時有多位使用者的大量網路流量。此外還有一些技術不僅可以做到網路層及傳輸層的狀態，還可以做到應用層的狀態。

然而跟錄製流量的技術一樣，目前這些重播流量的技術並沒有完全從「觸發/重製網路事件」的測試用途出發來進行設計與實作，導致目前這些的重播技術與方法並不十分適合用來作為測試之用。習知的重播技術以及工具無法依據不完整的網路封包準確地重播出符合網路協定之網路連線。習知技術亦無法有效率地重製事件（reproduce event），而難以得知網路事件發生的原因。

【發明內容】

由上述分析可以得知，傳統的網路封包（packet）的處理方法中，無論是錄製或是重播網路流量的方法，均具有浪費龐大的儲存空間、浪費龐大的重播時間、無法依據不完整的網路封包播放符合網路協定之網路連線，或是無法精準重現網路事件等問題。

為解決這些的問題，本發明提供一種錄製、還原與重播網路流量的方法，其用以處理網路之多個網路連線的多個網路封包。

本發明提供之錄製、還原與重播網路流量的方法包括一錄製程序，以針對每一個網路連線錄製網路連線的網路封包。錄製程序則包括：接收一錄製參數（N, M, P），其中 N、M 以及 P 係為大於等於零的整數；完整錄製這些網路連線的每一個網路封包的一檔頭以及一酬載（payload），並累計每一個網路連線的一酬載總值；當酬載總值之一超過 N 時，對與酬載總值對應的網路連線的連續 P 個網路封包錄製每一個網路封包的該檔頭，以及酬載的前 M 個位元組；以及當酬載總值之一超過 N 並對與酬載總值對應的網路連線連續錄製 P 個網路封包之後，對與酬載總值對應的網路連線的網路封包錄製每一個網路封包的檔頭。

根據本發明之一實施範例，錄製、還原與重播網路流量的方法另可包括一還原程序，而還原程序可包括以下步驟。逐一

檢查網路封包的檔頭以及酬載是否完整；當得到至少一個不完整的網路封包時，判斷其是否具有完整的檔頭；以及當不完整的網路封包具有完整的檔頭時，執行下述步驟：依據不完整的網路封包的檔頭，得到不完整的網路封包的一酬載長度；以及依據酬載長度，寫入一虛擬值（dummy）作為不完整的網路封包的酬載。

還原程序另可包括以下步驟。當不完整的網路封包具有不完整的檔頭時，執行下述步驟：依據與不完整的網路封包對應的網路連線的其他網路封包，修復不完整的網路封包的檔頭；依據不完整的網路封包的檔頭，得到不完整的網路封包的酬載長度；以及依據酬載長度，寫入虛擬值作為不完整的網路封包的酬載。

還原程序並可包括以下步驟。依據網路連線的網路封包的檔頭的一序號（sequence number）以及一確認號（acknowledgement number），找出被漏錄（capture loss）的至少一漏錄封包；依據與漏錄封包對應的網路連線的其他網路封包，修復漏錄封包的檔頭；依據漏錄封包的檔頭，得到漏錄封包的酬載長度；以及依據酬載長度，寫入虛擬值作為漏錄封包的酬載。

而其中虛擬值係可以為亂數。

根據本發明之一實施範例，錄製、還原與重播網路流量的方法另可包括一選擇性重播程序，而其可包括以下步驟。接收

一事件時間以及一網路連線資訊，其中網路連線資訊包括至少一網路連線位址；以及重播與網路連線位址對應的至少一個網路連線的網路封包。

選擇性重播程序另可包括：依據網路連線資訊的網路連線位址、一網路連線協定以及一網路連線埠，得到這些網路連線中的一特定連線；以及重播特定連線的網路封包。

選擇性重播程序並可包括：重播在事件時間時，正在傳輸的至少一個網路連線的網路封包。

選擇性重播程序又可包括：重播在事件時間之前結束傳輸的至少一個網路連線的網路封包。

其中上述之網路連線位址係可為網際網路協定位址（IP address）。而這些網路連線可為符合傳輸控制協定（Transmission Control Protocol，TCP）或使用者資料協定（User Datagram Protocol，UDP）。

綜上所述，本發明所提供之錄製、還原與重播網路流量的方法能夠解決浪費儲存空間以及無法精準重現網路事件等問題。錄製程序錄製較有價值的網路流量，而節省了絕大的儲存空間。還原程序亦可將錄製程序省略或漏錄的網路封包修復，以得到符合網路通訊協定之完整的網路封包。且選擇性重播程序能找出與網路事件最相關之網路連線的技術，以精準並快速地重現網路事件。

【實施方式】

以下在實施方式中詳細敘述本發明之詳細特徵以及優點，其內容足以使任何熟習相關技藝者了解本發明之技術內容並據以實施，且根據本說明書所揭露之內容、申請專利範圍及圖式，任何熟習相關技藝者可輕易地理解本發明相關之目的及優點。

本發明提供一種錄製、還原與重播網路流量的方法，其用以處理多個網路連線（connection）的多個網路封包（packet）。其中網路連線可以是符合傳輸控制協定檔頭（Transmission Control Protocol，TCP）或是使用者資料協定（User Datagram Protocol，UDP）的網路連線。而網路封包係指網際網路層（Internet Protocol layer，IP layer）的網路封包。

錄製、還原與重播網路流量的方法包括一錄製程序，以針對每一個網路連線錄製這些網路連線的網路封包。對於每一個網路連線，錄製程序僅錄製網路連線中較有價值的封包的部分，而能夠節省大量的儲存空間。

錄製、還原與重播網路流量的方法另可包括一還原程序或是一選擇性重播程序。其中還原程序係用以針對每一個網路連線修復網路連線的網路封包，而選擇性重播程序則由已錄製的網路連線的封包之中，選擇性地重播部分封包以重現一網路事件。其中網路事件例如為網路中的攻擊事件（attack event）、病毒事件（virus event）、點對點應用（peer-to-peer application，P2P application）或是連線中斷事件等。

請參照「第 1 圖」，其係為根據本發明一實施範例之錄製、還原與重播網路流量的方法之流程圖。如「第 1 圖」所示，錄製、還原與重播網路流量的方法可依照執行錄製程序（步驟 S300）、執行還原程序（步驟 S400）以及執行選擇性重播程序（步驟 S500）的步驟。然而本發明提供之錄製程序、還原程序以及選擇性重播程序可個別單獨地執行，亦可以任意順序組合後執行之。舉例而言，選擇性重播程序可直接播放已被完整錄製的網路流量資訊；或是執行錄製程序時可同時執行還原程序，以得到較完整的網路流量資訊。

接下來藉由「第 2 圖」說明錄製程序之步驟，「第 2 圖」係為根據本發明一實施範例之錄製程序之流程圖。

首先接收一錄製參數（N, M, P），其中 N、M 以及 P 係為大於等於零的整數（步驟 S310）。錄製程序可使用相同的錄製參數錄製所有網路連線的網路封包，亦可對於每一個網路連線配置不同的錄製參數以錄製網路封包。錄製程序先完整地錄製這些網路連線的每一個網路封包的一檔頭（header）以及一酬載（payload），並累計每一個網路連線的一酬載總值（步驟 S320）。換句話說，於步驟 S320 中，網路封包的檔頭以及酬載均被完整地錄製。酬載總值係為目前已錄製之網路封包之酬載的總大小，單位可以是位元組（byte）。

錄製程序在錄製網路封包時，同時不斷地判斷酬載總值是否超過錄製參數的 N（步驟 S330）。若酬載總值之一（也就是

任意一個網路連線的酬載總值）尚未超過N，則繼續完整地抓取網路封包的內容。而當酬載總值之一超過N時，對與超過N的此酬載總值對應的網路連線的連續 P 個網路封包錄製每一個網路封包的檔頭，以及酬載的前M個位元組（步驟S340）。換句話說，當發現對一個網路連線所錄製的網路封包的酬載的累積大小超過 N 時，對於此網路連線的接下來的 P 個網路封包便僅錄製其檔頭及酬載的前M個位元組。

而當酬載總值之一超過N並對與超過N的此酬載總值對應的網路連線連續錄製P個網路封包之後，對與酬載總值對應的網路連線的網路封包錄製每一個網路封包的檔頭（步驟S350）。換言之，於步驟S340錄製P個不完整的網路封包後，對於此網路連線的接下來所有的網路封包僅錄製其檔頭，而不在錄製網路封包的酬載。

由於錄製程序依據錄製參數省略了網路連線中後續網路封包的酬載，因此可以大幅減少錄製網路流量時所需的儲存空間。且錄製程序既有錄製所有網路封包的檔頭以及網路連線前期之酬載內容，因此錄製的網路流量的內容是有價值且足以提供給後續程序分析或重播之用的。

錄製參數（N, M, P）係可由實驗法得到，且不同的網路事件可能適合使用不同的值。更詳細地說，對於不同種的網路事件，可逐一測試並調整 N、M 以及 P 的值，以得到最省空間又能精準重現網路事件的錄製參數。

以針對攻擊事件之錄製參數為例，請參照「第 3A 圖」以及「第 3B 圖」，其分別為根據本發明一實施範例之錄製參數驗證圖。其中可見一網路事件-N 值曲線 20、一成功重現網路事件-N 值曲線 21 以及一耗費的儲存空間-N 值曲線 22。

假設在所有錄製到的網路流量中總共發現了 1929 件攻擊事件，其中有 333 件攻擊事件的酬載的長度是超過 2000 bytes。首先以（N, 0, 0）的錄製參數進行實驗。也就是說播放所錄製之網路流量中每個網路連線之酬載的前 N 個 bytes，以實驗這 333 件的攻擊事件是否可以被重現。而實驗的結果如「第 3A 圖」。當 N 為 2000 時即可重現 317 個攻擊事件，而對於剩下未能重現的 16 個攻擊事件須要很大的 N 值才能重現。對此以另一個實驗來看為了要觸發這 16 個攻擊事件所需要耗費的儲存空間大小，而實驗結果如「第 3B 圖」。為了要觸發所有的攻擊事件，則必須以很大的 N 值而耗費相當大的儲存空間才可達成。

接下來針對無法以錄製參數（50000, 0, 0）重現之四個攻擊事件，以錄製參數（0, M, ∞）進行試驗，也就是重播每個網路封包的前 M bytes 的。實驗結果如下表。

攻擊事件之描述訊息	酬載之大小（byte）	M 之最大值
SHELLCODE x86 setgid 0	151611	1300
SQL Injection comment	206085	140

attempt		
Web-CLIENT Windows Media Player zero length bitmap	390745	200
Adobe BMP Image Handler Buffer Overflow	561305	90

由上表可以知悉，當 M 為 200 時，便可以重現其中的三個攻擊事件。此外，再以錄製參數（2000, M, ∞）實驗之前以錄製參數（2000, 0, 0）無法重現的 16 個攻擊事件，結果如「第 3C 圖」。由「第 3C 圖」中的一網路事件-M 值曲線 23 可以知悉，當 M 為 200 bytes 時即可重現其中的 11 的攻擊事件。

接著在實驗中調整 P，找出以錄製參數（2000, 200, ∞）重播時，所需要耗費的儲存空間大小以及網路事件之觸發數量之間的關係。實驗結果如「第 3D 圖」所示。其中可見一成功重現網路事件-P 值曲線 24 以及一耗費的儲存空間-P 值曲線 25。當 P 為 1300 時，11 個攻擊事件皆可被重現。且相較於習知之錄製所有網路封包的做法，當 P 為 1300 時，可節省 87% 的儲存空間。而當 P 為 200 時，則可重現 8 個攻擊事件且節省 90%的儲存空間。

總結來說，對於攻擊事件的網路事件而言，錄製參數（2000, 200, 1300）可以觸發 98.5%的網路事件。且相較於錄製所有封包的習知技術，能夠節省 87%的儲存空間。以類似的方法進行實驗之後，可知對於病毒事件型的網路事件，錄製參數（6000,

0, 0）能夠觸發 93%的網路事件並較習知節省 70%的儲存空間。再例如對於點對點應用，則適合以酬載包含 UDP 資料之網路封包為主進行錄製。

請參照「第 4 圖」，其係為根據本發明一實施範例之錄製裝置之方塊圖。錄製程序可被實作於一錄製裝置 30，其中錄製裝置 30 可包括一連線追蹤模組（connection track module）32、一封包擷取資料庫（process characterization analysis package database，或稱為 packet capture database，PCAP database，PCAP 資料庫）34 以及一網路卡（network interface card，NIC）36。

錄製裝置 30 可與一外部網路以及一內部網路連接，以擷取並錄製在外部網路以及內部網路之間流通之網路連線的網路封包。連線追蹤模組 32 透過網路卡 36 得到這些網路封包，依據上述錄製程序之步驟將網路封包錄製為 PCAP 檔案，並將 PCAP 檔案存進 PCAP 資料庫 34 中。雖本說明書中以 PCAP 檔案以及 PCAP 資料庫 34 為例，然亦可使用其他用以紀錄網路流量之資料庫以及對應的檔案格式。

錄製、還原與重播網路流量的方法並可包括還原程序。請參照「第 5 圖」，其係為根據本發明一實施範例之還原程序之流程圖。

錄製程序可能為節省儲存空間而故意捨去部分的網路封包的資料。因此在依據這些網路封包播放（重現）網路流量前，需要先經由此還原程序經以錄製的網路封包確認其是否完

整。完整的網路封包可直接轉交給選擇性重播程序；而不完正的網路封包則由還原程序處理過後，再提供給選擇性重播程序。

還原程序首先藉由檔頭之封包總長度（total length）欄位等資訊，判斷目前的網路封包的檔頭以及酬載是否完整（步驟S410）。若網路封包本身係為完整，便不需對其進行處理。若網路封包不完整，則進一步藉由檔頭長度（header length，HLEN）欄位等資訊判斷此不完整的網路封包是否具有完整的檔頭（步驟S415）。

當不完整的網路封包具有完整的檔頭時，則依據不完整的網路封包的檔頭，得到不完整的網路封包的一酬載長度（步驟S425）。還原程序再依據酬載長度，寫入一虛擬值（dummy）作為不完整的網路封包的酬載（步驟S430）。更詳細地說，將不完整的網路封包的檔頭中紀錄之封包總長度減去檔頭長度即可獲得酬載長度。而作為網路封包之酬載的虛擬值則可為亂數。

而當不完整的網路封包具有不完整的檔頭時，則需先依據與此不完整的網路封包對應的網路連線的其他網路封包，修復不完整的網路封包的檔頭（步驟S420）。屬於同一個網路連線的網路封包之檔頭的內容大多雷同，例如這些檔頭會具有相同的來源IP位址（Source IP address）、目的IP位址（destination IP address）、通訊協定（Protocol）、存活時間（time to live）或

是旗標值（flags），因此參考同一個網路連線的其他網路封包，可修復不完整的檔頭。對於檔頭中 HLEN 及 total length 這兩個欄位值的修復，可以利用「total length = HLEN + 酬載長度」此關係算出。識別碼（identification）欄位值的算法是對應同一個來源端，每增加一個網路封包 identification 欄位值就加 1；因此可以藉由前後同樣來源端的網路封包的 identification 欄位值來計算得到。最後，便可對修復中的網路封包進行一次校驗和（checksum）的計算，以修復檔頭中 checksum 欄位值。如此一來，便可依據修復好的檔頭執行上述步驟 S425 以及步驟 S430，以得到修復好的整個網路封包。

此之外，還原程序並能檢測出是否有在錄製時漏錄（capture loss）的一漏錄封包並修復之。因為一時網路流量過高等情形，亦可能會產生不完整的網路封包，甚至是完全被漏錄的漏錄封包。對於 TCP，依據拆解酬載後可得到傳輸控制協定檔頭（TCP header）之一序號（sequence number）以及一確認號（acknowledgement number），還原程序能夠發現是否有網路封包被漏錄。至於 UDP，則無法發現網路封包是否發生了漏錄的情形。

請參照「第 6 圖」，其係為根據本發明另一實施範例之還原程序之流程圖。

還原程序可先依據網路連線的網路封包的檔頭的序號以及確認號，判斷是否有漏錄封包（步驟 S435）。若沒發現漏錄

封包，則執行步驟 S410 及後續步驟。

若還原程序找到至少一個漏錄封包，則以下述步驟修復漏錄封包：依據與漏錄網路封包對應的網路連線的其他網路封包，修復漏錄網路封包的檔頭（步驟 S440）；依據漏錄網路封包的檔頭，得到漏錄網路封包的酬載長度（步驟 S445）；以及依據酬載長度，寫入虛擬值作為漏錄網路封包的酬載（步驟 S450）。

更詳細地說，根據 TCP 通訊協定，對於來源 IP 位址與目的 IP 位址固定之同一網路連線中的一個網路封包，其序號會是前一個網路封包的序號加上前一個網路封包的資料長度（data length）。下表為一實施範例之網路連線的網路封包表，依序表示此網路連線內的連續多個網路封包及其具有的序號及確認號等資訊。

網路封包編號	1	2	3	4	5	6
來源→目的	A→B	A→B	B→A	A→B	A→B	B→A
序號	a	a+10	b	a+20	a+40	b
確認號	b	b	a+10	b	b	a+50
資料長度（byte）	10	10	0	20	10	0

如表所示，網路封包 2 的序號會是網路封包 1 的序號加上網路封包 1 的資料長度（10 byte）。

假設網路封包 4 為漏錄封包，則還原程序會得到網路封包 1-3 以及 5-6。其中由同為由 A 到 B 之網路封包 2 以及 5 的序號可以得知，其中應具有一個資料長度為（a+20）-（a+10）的網路封包，也就是網路封包 4。藉由上述邏輯，還原程序可找出漏錄封包，並依據同一網路連線的其他網路封包修復整個漏錄封包。

由此可見，還原程序可透過網路協定之特性找出錄製網路流量時省略或漏錄的網路封包，並提高網路流量其行為的準確性。

得到完整的網路流量之後，選擇性重播程序重播部分的網路流量以精準地重現網路事件。為了避免需重播所有已錄製之網路封包所耗費的時間，選擇性重播程序依據網路事件之相關資訊，逆向操作挑選出部分可能足以重現網路事件之關鍵的網路流量（即網路封包）並重播之。

請參照「第 7 圖」，其係為根據本發明一實施範例之選擇性重播程序之流程圖。

選擇性重播程序首先接收網路事件的一事件時間以及一網路連線資訊（步驟 S510），其中網路連線資訊包括至少一網路連線位址。接著依據網路連線位址，重播與網路連線位址對應的至少一個網路連線的網路封包（步驟 S520）。其中網路連線位址可以是網際網路協定位址（IP address），且其可包括來源 IP 位址以及目標 IP 位址。

更詳細地說，選擇性重播程序在已錄製的網路連線之中尋找具有與接收之網路連線位址相同的來源 IP 位址以及目標 IP 位址的網路連線（網路封包），並重播之。

請再參照「第 8 圖」，其係為根據本發明另一實施範例之選擇性重播程序之流程圖。於本實施範例中，選擇性重播程序逐漸增加播放的網路封包直到成功地重現被指定之網路事件為止。

網路連線資訊除了網路連線位址之外，另可包括一網路連線協定以及一網路連線埠（port）；其中網路連線埠可包括一來源埠以及一目的埠。而依據此 5 維資訊（即來源 IP 位址、目的 IP 位址、通訊協定、來源埠以及目的度埠），便可指定一特定連線。

因此當網路連線資訊包含上述 5 維資訊時，選擇性播放程序可依據網路連線資訊的網路連線位址、網路連線協定以及網路連線程序，得到網路連線中的特定連線（步驟 S512）；並重播此特定連線的網路封包（步驟 S514）。

選擇性播放程序並判斷是否已重現網路事件（步驟 S516）。當僅重播此特定連線之封包不足以重現網路事件，或是當網路連線資訊不足以指定特定連線時，則依據網路連線位址重播與網路連線位址對應的至少一個網路連線的網路封包（步驟 S520）。於步驟 S520 中，可重播所有與網路連線位址對應的所有網路連線，以嘗試重現網路事件。

於步驟 S522 再次重新判斷是否已重現網路事件。若仍未成功，則重播在事件時間時，正在傳輸的至少一個網路連線的網路封包（步驟 S524）。根據事件時間，選擇性重播程序可重播所有其他在網路事件發生時正在傳輸中的網路連線，以嘗試重現網路事件。

類似地，於步驟 S526 再次重新判斷是否已重現網路事件。若仍未成功，則重播在事件時間之前結束傳輸的至少一個網路連線的網路封包（步驟 S528）。

且根據本發明之一實施範例，若於步驟 S528 之後仍未成功地重現網路事件，選擇性播放程序重播所有的網路封包，以重現網路事件。

請對照參考「第 9 圖」，其係為根據本發明一實施範例之選擇性播放之示意圖。根據事件時間 62 以及網路連線資訊，選擇性播放程序由多個網路連線 60 中選擇性地播放，以重現網路事件。假設根據網路連線資訊，可以得到特定連線為網路連線 60e，且網路連線 60e 係為主機 A 與 B 之間的連線。則依據「第 8 圖」的流程，選擇性重播程序將會依照網路連線 60e、網路連線 60a、網路連線 60c、網路連線 60b 以及網路連線 60d 的順序重播這些網路連線 60。

根據本發明之還原程序以及選擇性重播程序可實作為一選擇性播放裝置。請參照「第 10 圖」，其係為根據本發明一實施範例之選擇性重播裝置之方塊圖。一選擇性重播裝置 40 可

包括一選擇性重播介面（selective replay interface）41、一前處理器（preprocessor）42、連線追蹤模組 43、一漏錄修復引擎（loss-recovery engine）44、一重播引擎（replay engine）45、一插座應用程式介面（socket application program interface，socket API）46、一路由模組（routing module）47、一驗證模組（validate source）48、網路卡 49a、網路卡 49b、PCAP 資料庫 422 以及一重播紀錄（replay log）452。且選擇性重播裝置 40 係藉由網路卡 49a 以及 49b 提供重播之網路封包給一待測裝置（device under test）50。

選擇性重播介面 41 係提供給使用者指定事件時間 62 或是網路連線資訊，並將這些資訊傳送給前處理器 42。前處理器 42 並由 PCAP 資料庫 422 中得到已錄製好的網路流量，再將網路流量中完整的 TCP 資料段（TCP segment）或 UDP 資料塊（UDP datagram）提供給連線追蹤模組 43。連線追蹤模組 43 紀錄網路連線 60 的各種狀態，並將由目前之網路封包之酬載得到的 TCP 或 UDP 檔頭的內容提供給漏錄修復引擎 44。漏錄修復引擎 44 則執行還原程序，判斷目前之網路封包是否完整，或是是否有漏錄之封包。有必要時，漏錄修復引擎 44 修復網路封包。且漏錄修復引擎 44 負責確定所以的網路封包的重播順序。

如此一來，重播引擎 45 得到完整的資料流（stream），並透過插座應用程式介面 46 將用以重播的資料傳出去。選擇性

重播裝置40可透過路由模組47以及網路卡49a重播網路流量予待測裝置50；並可透過網路卡49b以及驗證模組48回收由待測裝置50發送之網路封包。經待測裝置50回到選擇性重播裝置40的網路封包可由驗證模組48轉送給插座應用程式介面46，以判斷網路封包是否有被修改過，進而確保網路協定的正確性。

根據本發明之一實施範例，重播引擎45係在確認先前送出之網路封包以被回收後，才重播下一個網路封包給待測裝置50。且重播完網路連線60時，可將此網路連線60之開始連線以及結束連線的時間紀錄於重播紀錄452中。

綜上所述，本發明所提供之錄製、還原與重播網路流量的方法可包括錄製程序、還原程序以及選擇性重播程序。其能夠解決習知技術之浪費龐大儲存空間以及無法精準重現網路事件等問題。藉由錄製參數，錄製程序僅錄製較有價值的網路流量，而節省了絕大的儲存空間。對於錄製程序省略或漏錄的網路封包，還原程序亦可將其修復回符合網路通訊協定之完整的網路封包。而藉由找出與網路事件最相關之網路連線的技術，選擇性重播程序可精準並快速地重現網路事件，進而大幅減少測試測試裝置所需的時間。

雖然本發明以前述之較佳實施例揭露如上，然其並非用以限定本發明，任何熟習相像技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之專利保護範

圍須視本說明書所附之申請專利範圍所界定者為準。

【圖式簡單說明】

第 1 圖係為根據本發明一實施範例之錄製、還原與重播網路流量的方法之流程圖；

第 2 圖係為根據本發明一實施範例之錄製程序之流程圖；

第 3A 圖係為根據本發明一實施範例之錄製參數驗證圖；

第 3B 圖係為根據本發明一實施範例之錄製參數驗證圖；

第 3C 圖係為根據本發明一實施範例之錄製參數驗證圖；

第 3D 圖係為根據本發明一實施範例之錄製參數驗證圖；

第 4 圖係為根據本發明一實施範例之錄製裝置之方塊圖；

第 5 圖係為根據本發明一實施範例之還原程序之流程圖；

第 6 圖係為根據本發明另一實施範例之還原程序之流程圖；

第 7 圖係為根據本發明一實施範例之選擇性重播程序之流程圖；

第 8 圖係為根據本發明另一實施範例之選擇性重播程序之流程圖；

第 9 圖係為根據本發明一實施範例之選擇性播放之示意圖；以及

第 10 圖係為根據本發明一實施範例之選擇性重播裝置之方塊圖。

【主要元件符號說明】

20	網路事件-N 值曲線
21	成功重現網路事件-N 值曲線
22	耗費的儲存空間-N 值曲線
23	網路事件-M 值曲線
24	成功重現網路事件-P 值曲線
25	耗費的儲存空間-P 值曲線
30	錄製裝置
32	連線追蹤模組
34	封包擷取資料庫
36	網路卡
40	選擇性重播裝置
41	選擇性重播介面
42	前處理器
422	封包擷取資料庫
43	連線追蹤模組
44	漏錄修復引擎
45	重播引擎
452	重播紀錄
46	插座應用程式介面
47	路由模組
48	驗證模組
49a, 49b	網路卡

50	待測裝置
60, 60a, 60b, 60c, 60d	網路連線
62	事件時間

七、申請專利範圍：

1. 一種錄製網路流量的方法，用以處理多個網路連線的多個網路封包，該方法包括：

一錄製程序，包括：

接收一錄製參數（N, M, P），其中N、M以及P係為大於等於零的整數；

完整錄製該些網路連線的每一該網路封包的一檔頭以及一酬載，並累計每一該網路連線的一酬載總值；

當該酬載總值之一超過N時，對與該酬載總值對應的該網路連線的連續P個該些網路封包錄製每一該網路封包的該檔頭，以及該酬載的前M個位元組；以及

當該酬載總值之一超過N並對與該酬載總值對應的該網路連線連續錄製P個該些網路封包之後，對與該酬載總值對應的該網路連線的該些網路封包錄製每一該網路封包的該檔頭。

2. 如申請專利範圍第1項所述之錄製網路流量的方法，其中針對攻擊事件的該錄製參數為（2000, 200, 1300）。

3. 如申請專利範圍第1項所述之錄製網路流量的方法，其中針對病毒事件的該錄製參數為（6000, 0, 0）。

4. 如申請專利範圍第1項所述之錄製網路流量的方法，其中該些網路連線係符合傳輸控制協定或使用者資料協定。

5. 一種錄製與還原網路流量的方法，用以處理多個網路連線的

多個網路封包，該方法包括：

一錄製程序，包括：

接收一錄製參數（N, M, P），其中 N、M 以及 P 係為大於等於零的整數；

完整錄製該些網路連線的每一該網路封包的一檔頭以及一酬載，並累計每一該網路連線的一酬載總值；

當該酬載總值之一超過 N 時，對與該酬載總值對應的該網路連線的連續 P 個該些網路封包錄製每一該網路封包的該檔頭，以及該酬載的前 M 個位元組；以及

當該酬載總值之一超過 N 並對與該酬載總值對應的該網路連線連續錄製 P 個該些網路封包之後，對與該酬載總值對應的該網路連線的該些網路封包錄製每一該網路封包的該檔頭；以及

一還原程序，包括：

逐一檢查該些網路封包的該些檔頭以及該些酬載是否完整；

當得到至少一個不完整的該網路封包時，判斷其是否具有完整的該檔頭；以及

當不完整的該網路封包具有完整的該檔頭時，執行下述步驟：

依據不完整的該網路封包的該檔頭，得到不完整的該網路封包的一酬載長度；以及

依據該酬載長度，寫入一虛擬值作為不完整的該網路封包的該酬載。

6. 如申請專利範圍第 5 項所述之錄製與還原網路流量的方法，其中針對攻擊事件的該錄製參數為（2000, 200, 1300）。

7. 如申請專利範圍第 5 項所述之錄製與還原網路流量的方法，其中針對病毒事件的該錄製參數為（6000, 0, 0）。

8. 如申請專利範圍第 5 項所述之錄製與還原網路流量的方法，其中該些網路連線係符合傳輸控制協定或使用者資料協定。

9. 如申請專利範圍第 5 項所述之錄製與還原網路流量的方法，其中該還原程序另包括：

當不完整的該網路封包具有不完整的該檔頭時，執行下述步驟：

依據與不完整的該網路封包對應的該網路連線的其他該些網路封包，修復不完整的該網路封包的該檔頭；

依據不完整的該網路封包的該檔頭，得到不完整的該網路封包的該酬載長度；以及

依據該酬載長度，寫入該虛擬值作為不完整的該網路封包的該酬載。

10. 如申請專利範圍第 5 項所述之錄製與還原網路流量的方法，其中該還原程序另包括：

依據該些網路連線的該些檔頭的一序號以及一確認號，找出被漏錄的至少一漏錄封包；

依據與該漏錄封包對應的該網路連線的其他該些網路封包，修復該漏錄封包的該檔頭；

依據該漏錄封包的該檔頭，得到該漏錄封包的該酬載長度；以及

依據該酬載長度，寫入該虛擬值作為該漏錄封包的該酬載。

11. 如申請專利範圍第 5 項所述之錄製與還原網路流量的方法，其中該虛擬值係為亂數。

12. 一種錄製、還原與重播網路流量的方法，用以處理多個網路連線的多個網路封包，該方法包括：

一錄製程序，包括：

接收一錄製參數（N, M, P），其中 N、M 以及 P 係為大於等於零的整數；

完整錄製該些網路連線的每一該網路封包的一檔頭以及一酬載，並累計每一該網路連線的一酬載總值；

當該酬載總值之一超過 N 時，對與該酬載總值對應的該網路連線的連續 P 個該些網路封包錄製每一該網路封包的該檔頭，以及該酬載的前 M 個位元組；以及

當該酬載總值之一超過 N 並對與該酬載總值對應的該網路連線連續錄製 P 個該些網路封包之後，對與該

酬載總值對應的該網路連線的該些網路封包錄製每一該網路封包的該檔頭；

一還原程序，包括：

逐一檢查該些網路封包的該些檔頭以及該些酬載是否完整；

當得到至少一個不完整的該網路封包時，判斷其是否具有完整的該檔頭；以及

當不完整的該網路封包具有完整的該檔頭時，執行下述步驟：

依據不完整的該網路封包的該檔頭，得到不完整的該網路封包的一酬載長度；以及

依據該酬載長度，寫入一虛擬值作為不完整的該網路封包的該酬載；以及

一重播程序，包括：

接收一事件時間以及一網路連線資訊，其中該網路連線資訊包括至少一網路連線位址；以及

重播與該網路連線位址對應的至少一個該網路連線的該些網路封包。

13. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中針對攻擊事件的該錄製參數為（2000, 200, 1300）。

14. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量

的方法，其中針對病毒事件的該錄製參數為（6000, 0, 0）。

15. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該些網路連線係符合傳輸控制協定或使用者資料協定。

16. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該還原程序另包括：

當不完整的該網路封包具有不完整的該檔頭時，執行下述步驟：

依據與不完整的該網路封包對應的該網路連線的其他該些網路封包，修復不完整的該網路封包的該檔頭；

依據不完整的該網路封包的該檔頭，得到不完整的該網路封包的該酬載長度；以及

依據該酬載長度，寫入該虛擬值作為不完整的該網路封包的該酬載。

17. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該還原程序另包括：

依據該些網路連線的該些檔頭的一序號以及一確認號，找出被漏錄的至少一漏錄封包；

依據與該漏錄封包對應的該網路連線的其他該些網路封包，修復該漏錄封包的該檔頭；

依據該漏錄封包的該檔頭，得到該漏錄封包的該酬載長

度；以及

依據該酬載長度，寫入該虛擬值作為該漏錄封包的該酬載。

18. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該虛擬值係為亂數。

19. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該重播程序另包括：

依據該網路連線資訊的該網路連線位址、一網路連線協定以及一網路連線埠，得到該些網路連線中的一特定連線；以及

重播該特定連線的該些網路封包。

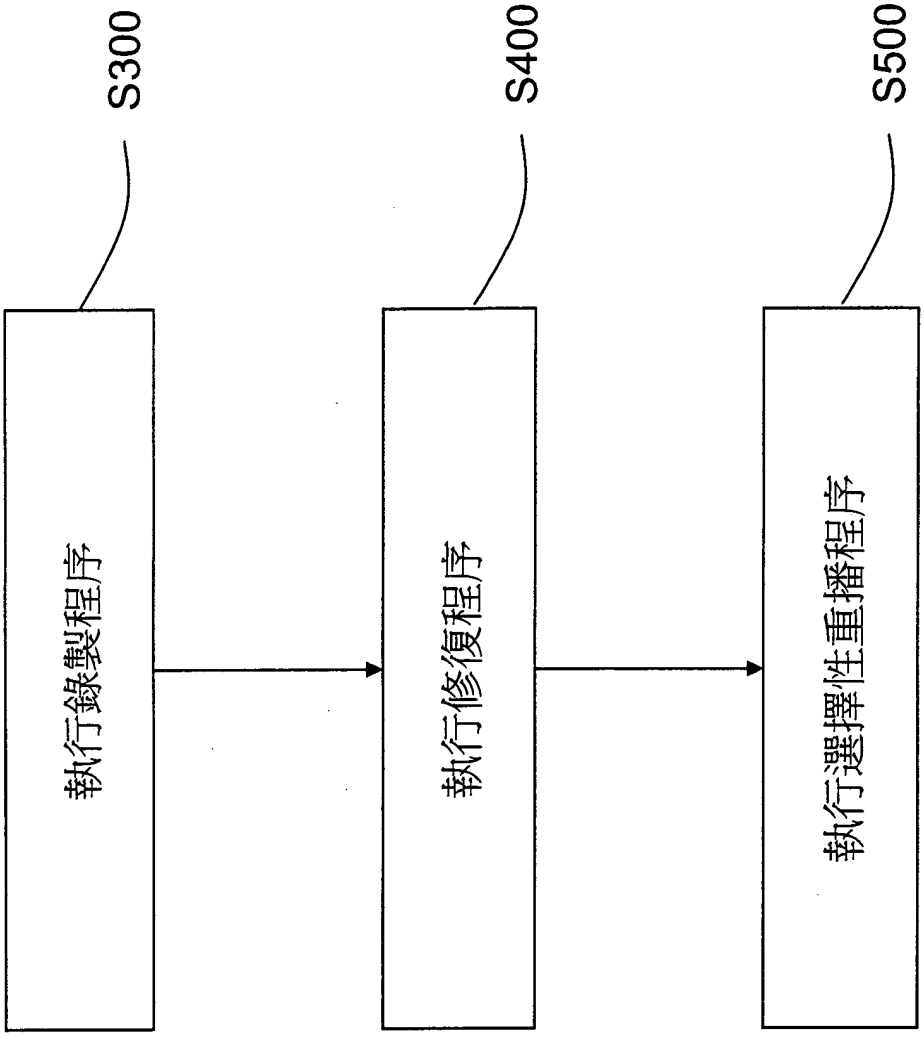
20. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該重播程序另包括：

重播在該事件時間時，正在傳輸的至少一個該網路連線的該些網路封包。

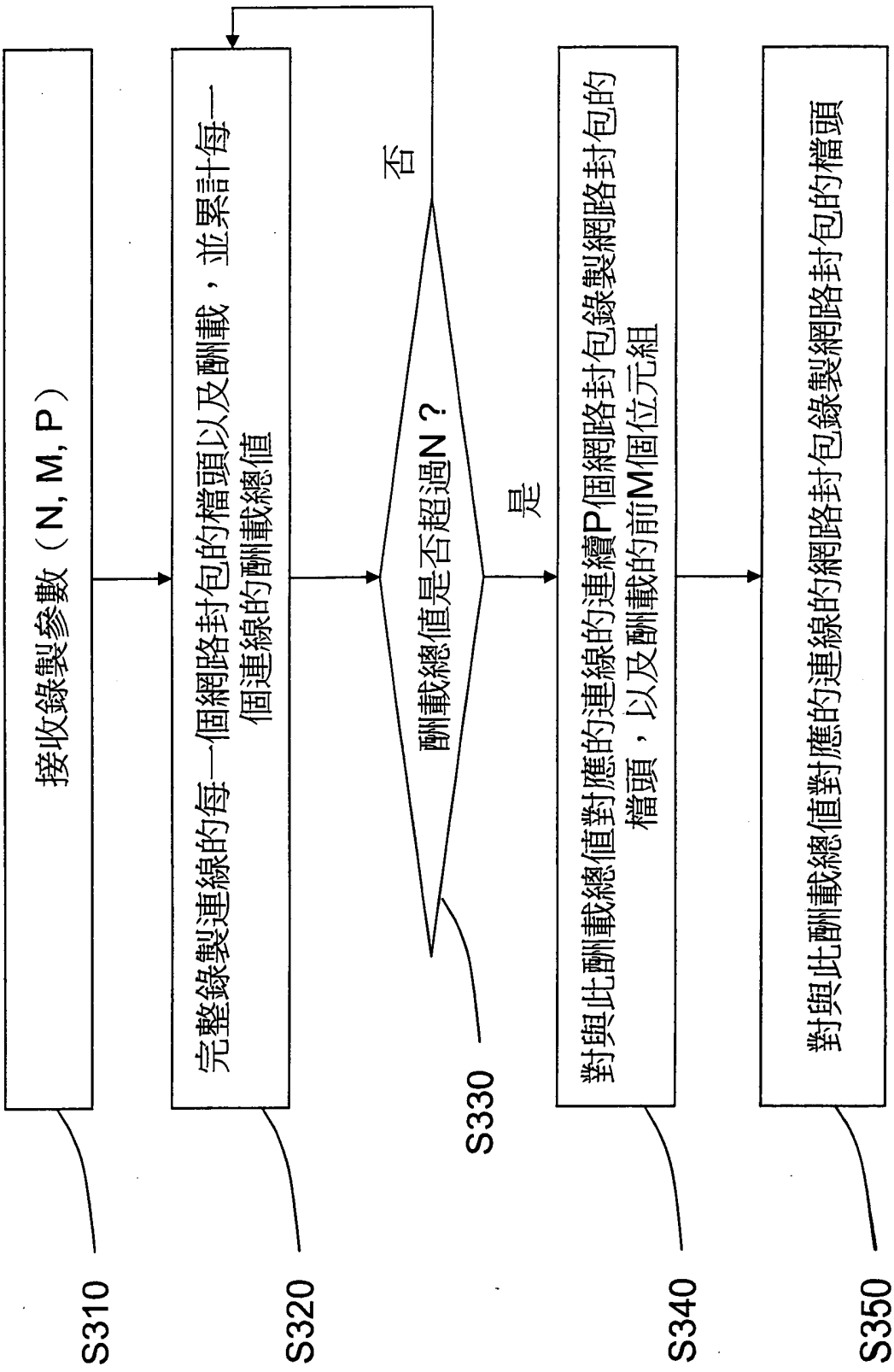
21. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該重播程序另包括：

重播在該事件時間之前結束傳輸的至少一個該網路連線的該些網路封包。

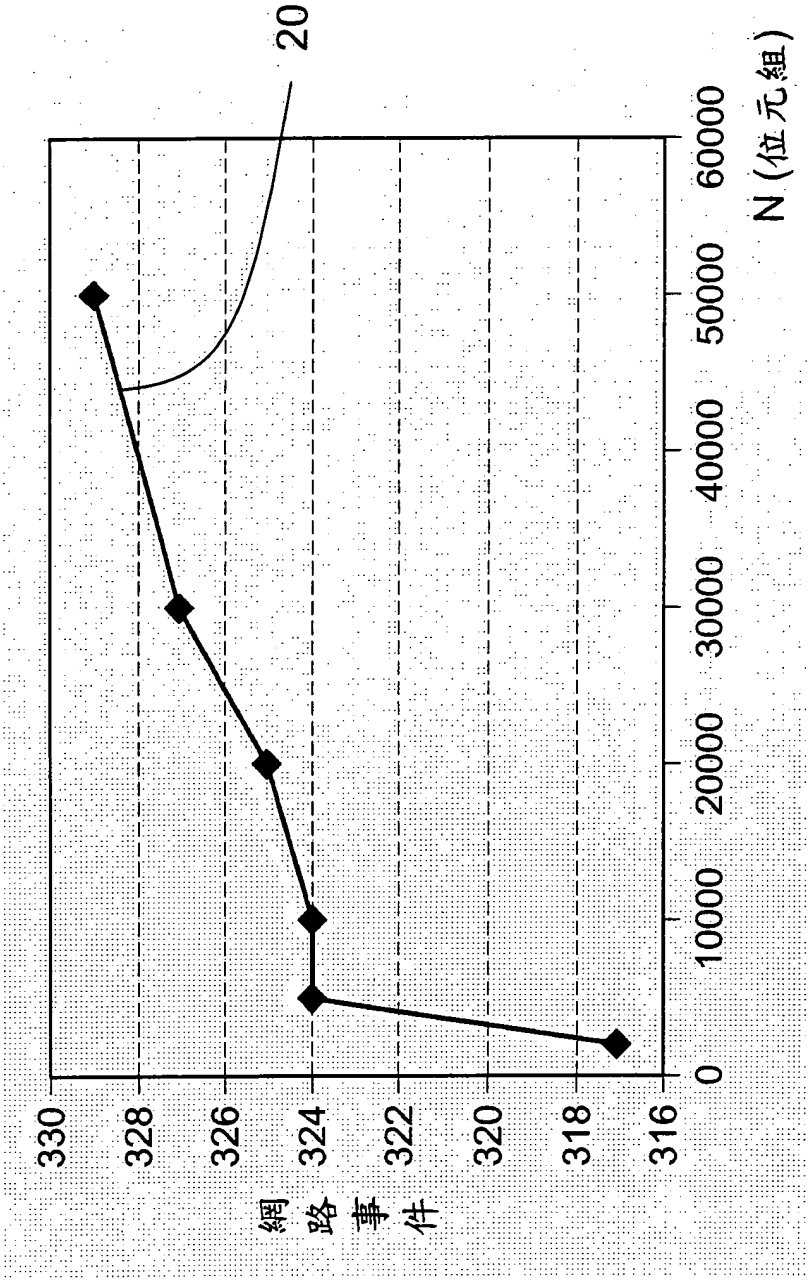
22. 如申請專利範圍第 12 項所述之錄製、還原與重播網路流量的方法，其中該網路連線位址係為網際網路協定位址。



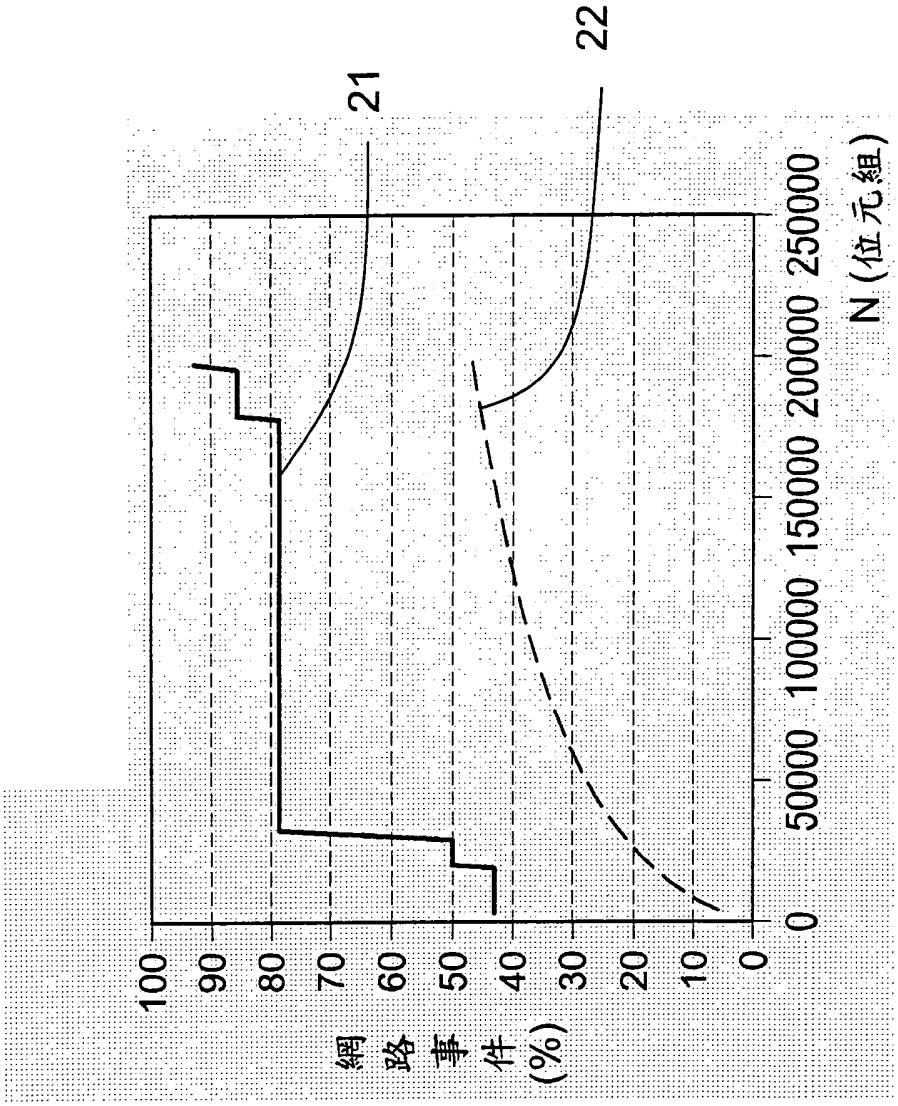
第1圖


接收錄製參數（N, M, P）
S310
完整錄製連線的每一個網路封包的檔頭以及酬載，並累計每一個連線的酬載總值
S320
酬載總值是否超過N？
S330
否
是
對與此酬載總值對應的連線的連續P個網路封包錄製網路封包的檔頭，以及酬載的前M個位元組
S340
對與此酬載總值對應的連線的網路封包錄製網路封包的檔頭
S350

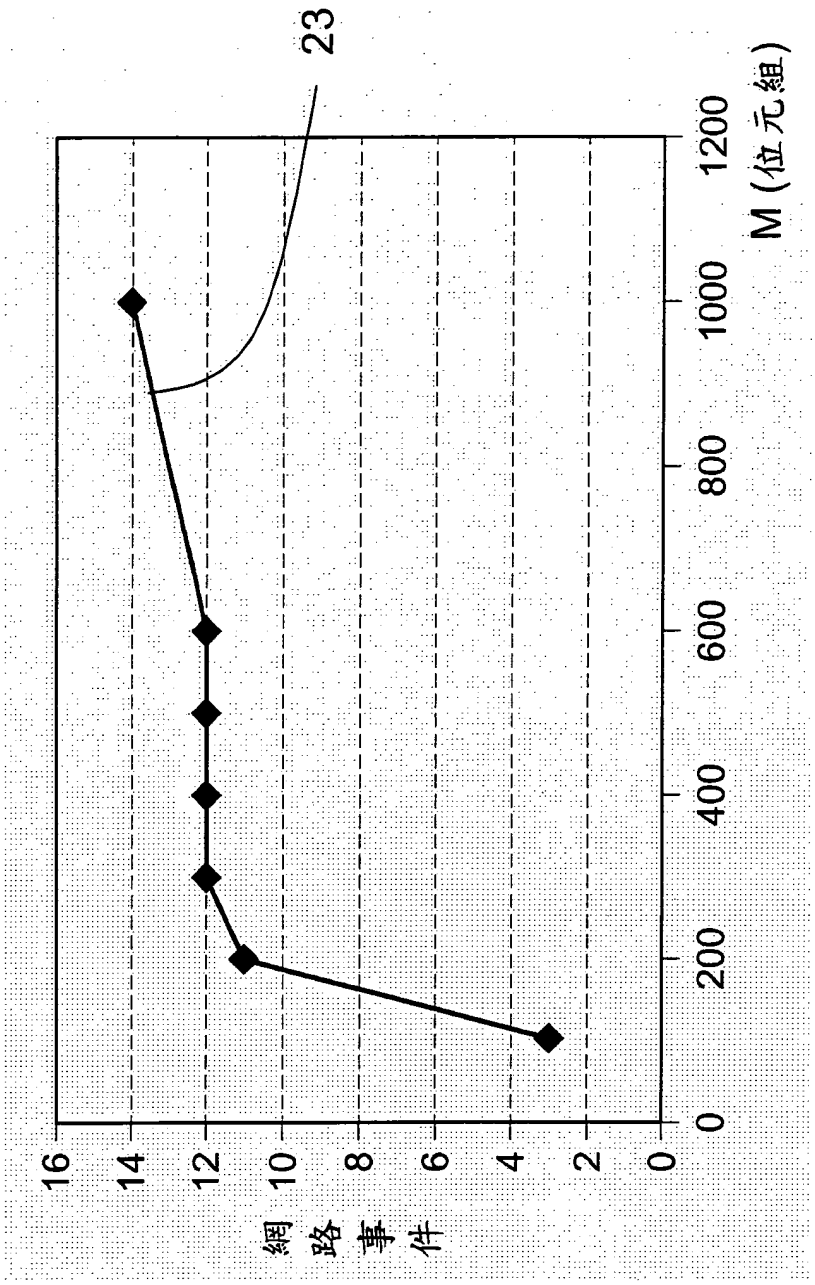
第2圖


20
330
328
326
324
322
320
318
316
網路事件
0
10000
20000
30000
40000
50000
60000
N (位元組)

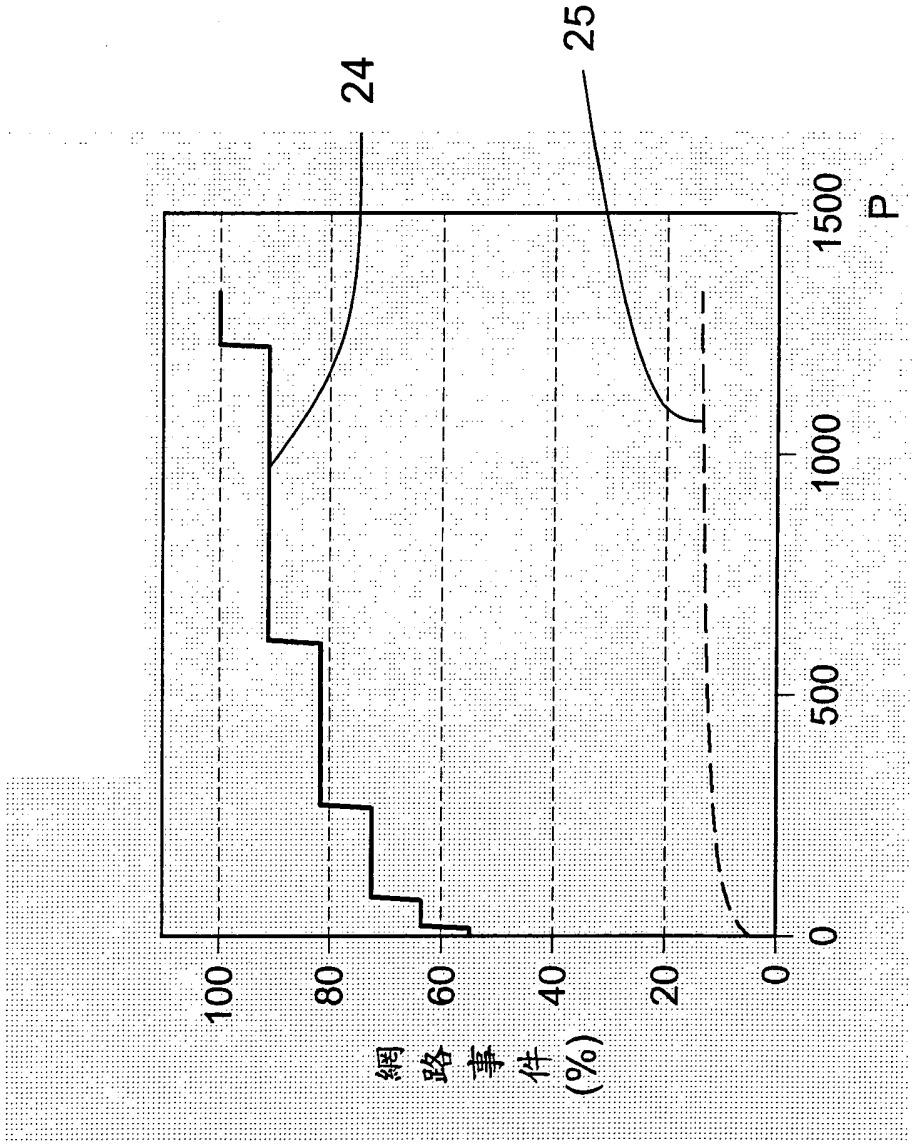
第3A圖


21
22
100
90
80
70
60
50
40
30
20
10
0
網路事件(%)
0
50000
100000
150000
200000
250000
N(位元組)

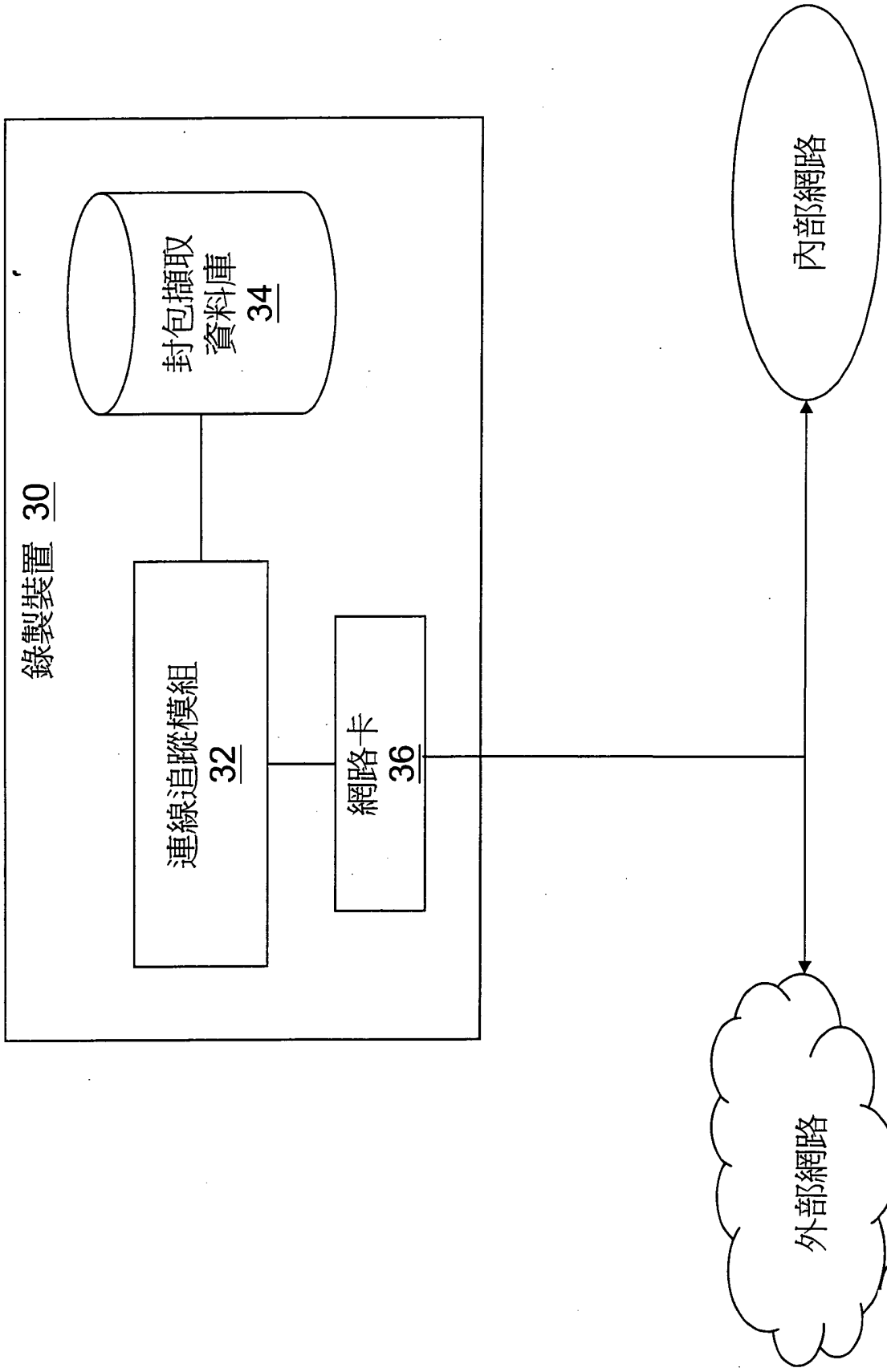
第3B圖



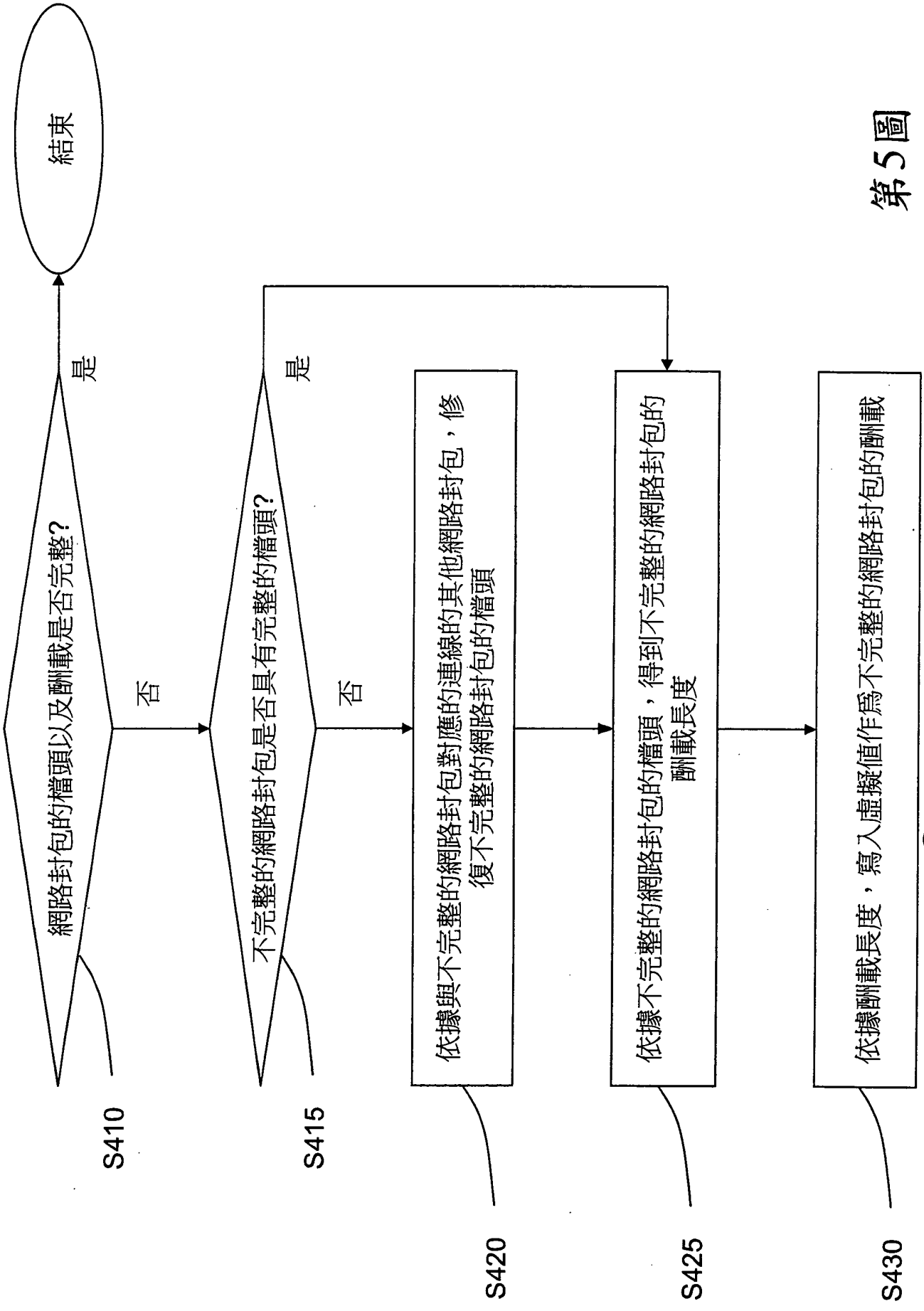
第3C圖



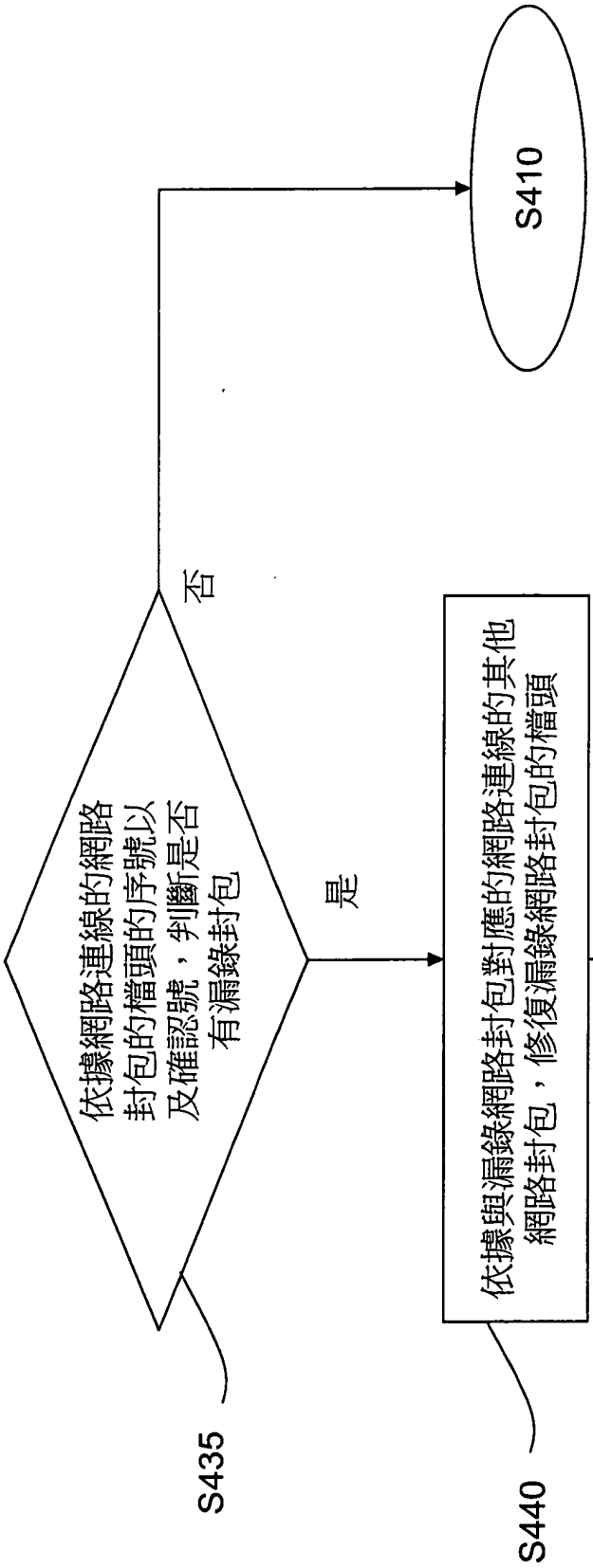
第3D圖



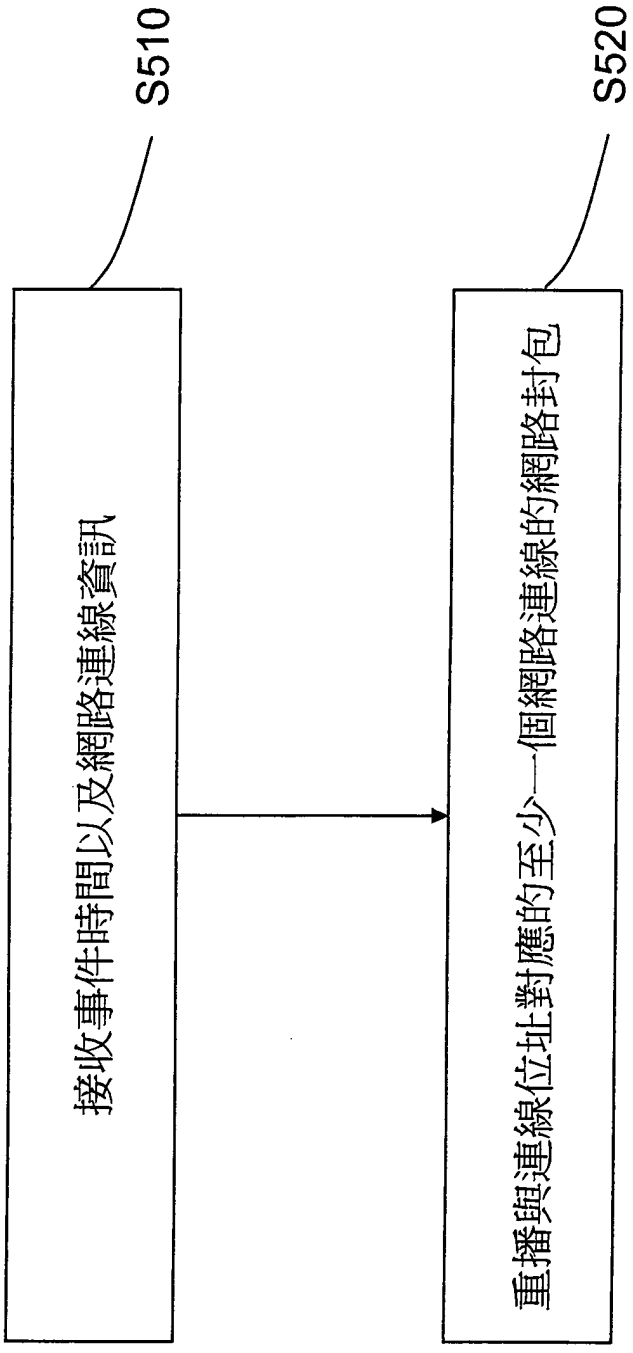
第4圖


結束
網路封包的檔頭以及酬載是否完整?
是
否
不完整的網路封包是否具有完整的檔頭?
是
否
依據與不完整的網路封包對應的連線的其他網路封包，修復不完整的網路封包的檔頭
依據不完整的網路封包的檔頭，得到不完整的網路封包的酬載長度
依據酬載長度，寫入虛擬值作爲不完整的網路封包的酬載
S410
S415
S420
S425
S430

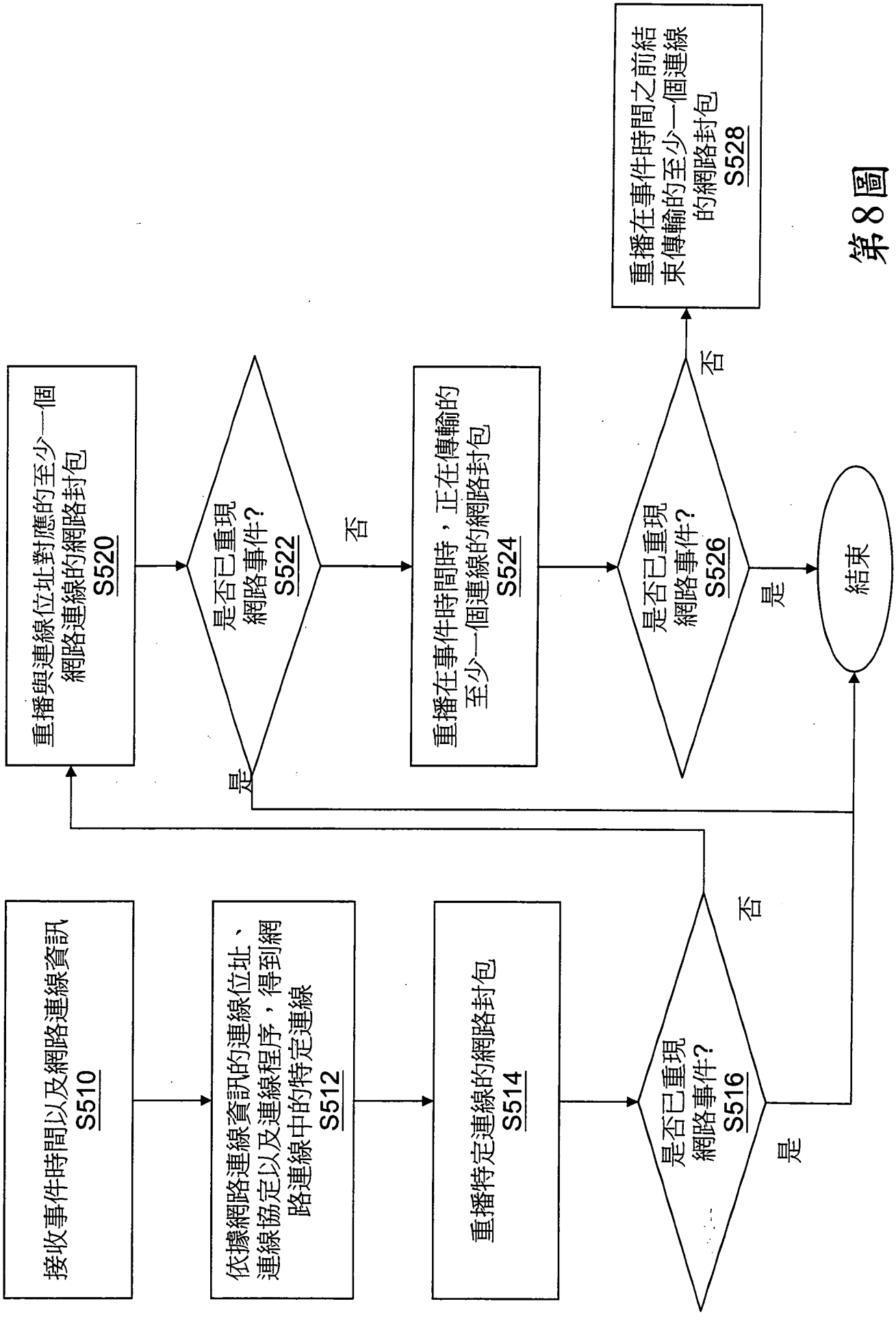
第5圖


依據網路連線的網路封包的檔頭的序號以及確認號，判斷是否有漏錄封包
否
是
S410
S435
依據與漏錄網路封包對應的網路連線的其他網路封包，修復漏錄網路封包的檔頭
S440
依據漏錄網路封包的檔頭，得到漏錄網路封包的酬載長度
S445
依據酬載長度，寫入虛擬值作爲漏錄網路封包的酬載
S450

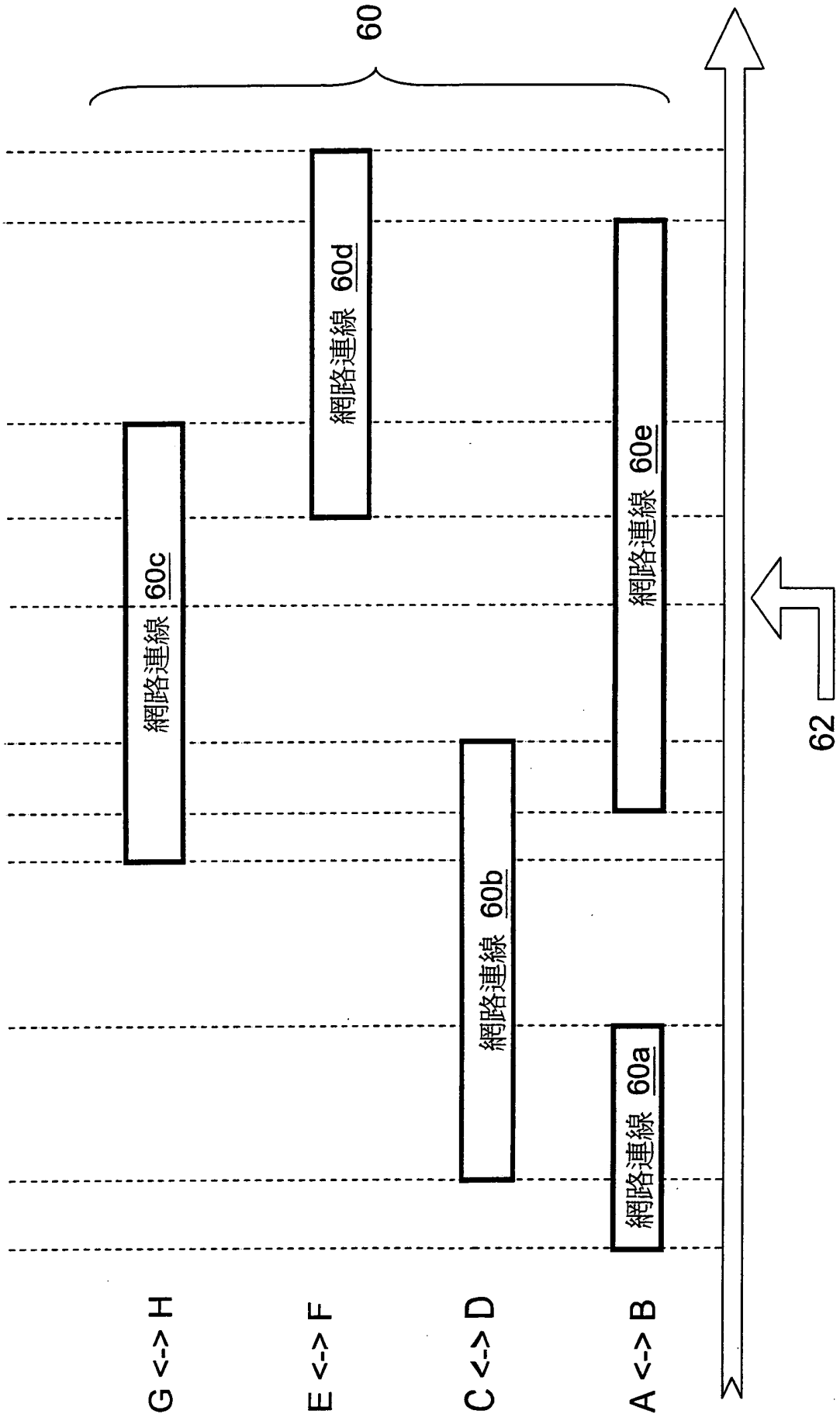
第6圖



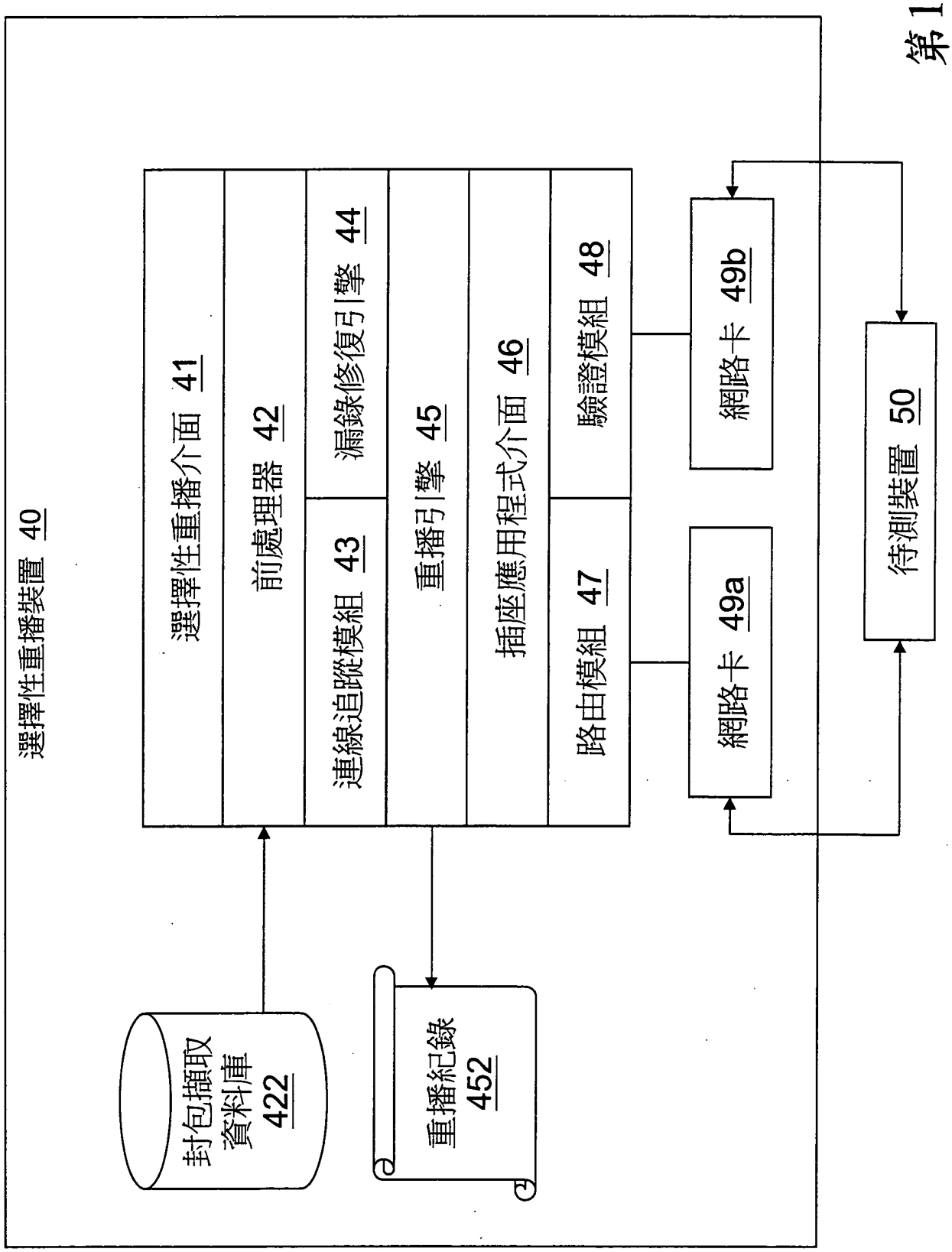
第7圖


接收事件時間以及網路連線資訊
S510
依據網路連線資訊的連線位址、連線協定以及連線程序，得到網路連線中的特定連線
S512
重播特定連線的網路封包
S514
是否已重現網路事件?
S516
否
是
結束
重播與連線位址對應的至少一個網路連線的網路封包
S520
是否已重現網路事件?
S522
否
是
重播在事件時間時，正在傳輸的至少一個連線的網路封包
S524
是否已重現網路事件?
S526
否
是
重播在事件時間之前結束傳輸的至少一個連線的網路封包
S528

第8圖



第9圖


選擇性重播裝置 40
選擇性重播介面 41
前處理器 42
連線追蹤模組 43
漏錄修復引擎 44
重播引擎 45
插座應用程式介面 46
路由模組 47
驗證模組 48
網路卡 49a
網路卡 49b
待測裝置 50
封包擷取資料庫 422
重播紀錄 452

第10圖