I478564

(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 I478564 B**

(45)公告日： 中華民國 104 (2015) 年 03 月 21 日

(21)申請案號：098126576 (22)申請日： 中華民國 98 (2009) 年 08 月 06 日

(51)Int. Cl.： ***H04L29/12 (2006.01)***

(30)優先權：2008/08/08 美國 12/189,034

(71)申請人：微軟公司 (美國) MICROSOFT CORPORATION (US)
美國

(72)發明人：崔斯羅伯M TRACE, ROB M. (US) ；莫倫利比 MEREN, LIBBY (US)

(74)代理人：蔡坤財；李世章

(56)參考文獻：

US	6338082B1	US	6560634B1
US	6678717B1	US	6760746B1

審查人員：黃偉倫

申請專利範圍項數：19 項 圖式數：10 共 68 頁

(54)名稱

用於安全資源名稱解析的方法、電腦可讀取儲存媒體及設備

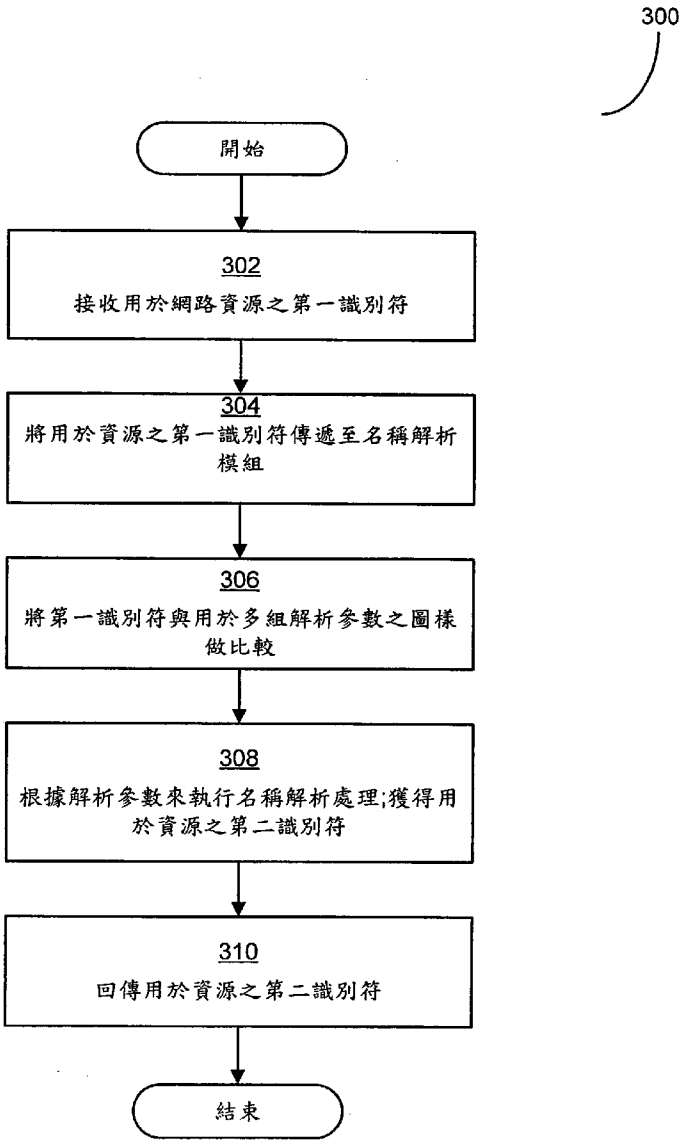
METHOD, COMPUTER-READABLE STORAGE MEDIUM, AND APPARATUS FOR SECURE RESOURCE NAME RESOLUTION

(57)摘要

茲揭示用於安全名稱解析科技以及確保名稱解析科技能夠在現代網路中發揮作用的技術，現代網路具有複數個可經由單一網路介面來進行存取的疊蓋網路。根據在此所述之某些原理，一組解析參數可由一使用者(像是一末端使用者或是一管理者)所實現以在一名稱解析過程期間使用，以在一疊蓋網路中用於保全該處理及/或用於導入該處理。在某些實作中，可將該組解析參數維持成一規則表，並將其用於支配名稱解析處理。例如，可產生能支配一 DNSSEC 會話的解析參數，或是支配如何用微軟直接存取之疊蓋科技來與網路通訊之方式，或是支配使用任何其他網路科技的通訊。

Techniques for securing name resolution technologies and for ensuring that name resolution technologies can function in modern networks that have a plurality of overlay networks accessible via a single network interface. In accordance with some of the principles described herein, a set of resolution parameters may be implemented by a user, such as an end user or an administrator, to be used during a name resolution process for securing the process and/or for conducting the process in an overlay network. In some implementations, the set of resolution parameters may be maintained as a table of rules, and used to govern name resolution processes. For example, resolution parameters may be created that govern a DNSSEC session, or that govern how to communicate with networks implemented with Microsoft's Direct Access overlay technologies, or that govern communications using any other networking technology.

302-310・・・方法步驟



第3圖

第 98126576 號專利申請案 103 年 10 月 29 日修正

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；惟已有申請案號者請填寫）

※ 申請案號：98126576

※ 申請日期：2009 年 8 月 6 日　　※IPC 分類：H04L 29/12 (2006.01)

一、發明名稱：（中文/英文）

用於安全資源名稱解析的方法、電腦可讀取儲存媒體及設備

METHOD, COMPUTER-READABLE STORAGE MEDIUM, AND APPARATUS FOR SECURE RESOURCE NAME RESOLUTION

二、中文發明摘要：

茲揭示用於安全名稱解析科技以及確保名稱解析科技能夠在現代網路中發揮作用的技術，現代網路具有複數個可經由單一網路介面來進行存取的疊蓋網路。根據在此所述之某些原理，一組解析參數可由一使用者(像是一末端使用者或是一管理者)所實現以在一名稱解析過程期間使用，以在一疊蓋網路中用於保全該處理及/或用於導入該處理。在某些實作中，可將該組解析參數維持成一規則表，並將其用於支配名稱解析處理。例如，可產生能支配一 DNSSEC 會話的解析參數，或是支配如何用微軟直接存取之疊蓋科技來與網路通訊之方式，或是支配使用任何其他網路科技的通訊。

三、英文發明摘要：

Techniques for securing name resolution technologies and for ensuring that name resolution technologies can function in modern networks that have a plurality of overlay networks accessible via a single network interface. In accordance with some of the principles described herein, a set of resolution

parameters may be implemented by a user, such as an end user or an administrator, to be used during a name resolution process for securing the process and/or for conducting the process in an overlay network. In some implementations, the set of resolution parameters may be maintained as a table of rules, and used to govern name resolution processes. For example, resolution parameters may be created that govern a DNSSEC session, or that govern how to communicate with networks implemented with Microsoft's Direct Access overlay technologies, or that govern communications using any other networking technology.

四、指定代表圖：

(一)本案指定代表圖為：第（3）圖。

(二)本代表圖之元件符號簡單說明:

302-310 方法步驟

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】

本發明係有關於名稱解析科技。

【先前技術】

在電腦通訊網路中，可使用若干不同的科技以識別可經由網路進行存取的資源。該等資源可包括附接到網路的主機(Host)，像是客戶端以及伺服器計算裝置，以及像是路由器、閘道器、防火牆等等的網路資源。在一技術中，可由一或更多的識別號碼來識別資源，像是媒體存取控制(MAC)位址或是網際網路協定(IP)位址。然而，可以理解的是，在這些位址在電腦對電腦的通訊上很實用的同時，使用者通常會發現到要記住這些識別號碼是很困難的，而這困難很可能會讓使用者因此放棄對網路資源的存取。因此，亦可額外或替代地由更容易為使用者所記住的文字識別符(textual identifier)來識別資源。實現能用來識別資源之文字識別符的科技包括了NetBIOS 、區域鏈結多播名稱解析(LLMNR)以及網域名稱系統(DNS)。

提供此類文字識別符之科技亦可提供翻譯服務以將一能輕易讓使用者記憶住之文字識別符，與一能讓計算裝置更容易處理的數字識別符相匹配(反之亦然)。舉例而言，在 DNS 中，當一使用者輸入一計算裝置到一文字識

別符(在 DNS 中的「網域名稱」)以初始與一由網域名稱所識別之資源間的通訊，在計算裝置上之一 DNS 客戶端將會查詢一 DNS 伺服器以將該網域名稱「解析」成一 IP 位址。在接收了一查詢之後，該 DNS 伺服器將通過本地對該 IP 位址可用之資訊亦或是透過查詢其他 DNS 伺服器，來找尋一對應到一網域名稱之 IP 位址，然後將該 IP 位址回傳給該 DNS 客戶端。該計算裝置則可初始與使用該 IP 位址之資源間的通訊。

吾人已了解到某些此類的名稱解析技術會被濫用。例如在 DNS 中，一攻擊者可以藉由在該 DNS 伺服器對該正確 IP 位址做出回應之前先以該攻擊者資源之 IP 位址對一 DNS 查詢作出回應的方式，來將一計算裝置誤導到該攻擊者自身的資源上(例如 該攻擊者的伺服器)。該計算裝置則可被誤導且將會連接到該攻擊者的資源，而不是正確的資源。然後，當連接到該攻擊者之資源時，該計算裝置可將資料透露給攻擊者或是從該攻擊者處接收偽造資料或是蠕蟲軟體(malware)。

某些安全技術已被實現已減少此種情形發生的可能性，例如，藉由將隨機識別符含括在 DNS 查詢各者內以及要求他們須被含括在對該查詢的回應內的方式，以制止攻擊者對該虛假位址進行回應的行為，除非該攻擊者能夠猜測或偵測到該查詢的隨機識別符。其中一種建議用來解決這些安全考量的安全技術，就是用 DNS 實作而成的網域名稱系統安全延伸(DNSSEC)協定。DNSSEC 透

[S]

過憑證管理的方式(CA)提供了 DNS 結果的數位發訊，從而該等結果可被精確地驗證。此外，依網際網路協定安全(IPsec)來使用 DNS 或 DNSSEC 的方式已被提出，以考量到在 DNS 客戶端及 DNS 伺服器端之間通訊的加密及/或鑑定。

【發明內容】

申請人已體認並了解到習知的名稱解析科技(包括DNS)的安全性可再加以增進。進一步而言，習知的名稱解析科技並未設計成能按照經由單一網路介面及單組網路硬體連接到多個網路的方式來運作，而因此疊蓋網路的成長被阻礙了。

在此所述是用於保全名稱解析科技之原理，以及用於確保名稱解析科技能在現代網路中發揮作用的原理。某些所述方式能與具有一疊蓋網路之網路組態相容，該疊蓋網路可如同一承載網路般經由相同介面進行存取。根據某些在此所述之原理，一組解析參數可由一使用者(像是一末端使用者或是一管理者)所實現以在一名稱解析過程期間使用，以在一疊蓋網路中用於保全該處理及/或用於導入該處理。在某些實作中，可將該組解析參數維持成一規則表，並將其用於支配名稱解析處理。例如，可產生能支配一 DNSSEC 會話的解析參數，或是支配如何用微軟直接存取之疊蓋科技來與網路通訊之方式，或

是支配使用任何其他網路科技的通訊。

在某些具體實施例中，茲提供了一種方法，其包含以下步驟：將用於一網路資源之一第一識別符當做輸入來接受；諮詢多組解析參數之一集合以判斷能應用到該第一識別符的一組可應用解析參數；以及獲得用於該網路資源之一第二識別符。該獲得步驟包含導入一名稱解析處理，以基於該第一識別符來判斷用於該網路資源之該第二識別符。該名稱解析處理是由該組可應用解析參數所支配。

在其他具體實施例中，茲提供至少一種用電腦可運行指令來編碼的電腦可讀取儲存媒體，當其執行時，會使得一電腦能執行一種方法。該方法包含以下步驟：依據一應用程式而將一用於一網路資源之網域名稱當做輸入來接受；判斷來自多組解析參數之集合中的一組可應用解析參數；根據該組可應用解析參數而在該網路上建立對一網域名稱服務(DNS)伺服器之連結。該 DNS 伺服器可由該組可應用解析參數來識別。該方法更包含根據該組可應用解析參數而對該 DNS 伺服器發送一 DNS 查詢；從該 DNS 伺服器處接收一回應，其包含一用於該網路資源之數字識別符；以及對該應用程式提供該數字識別符。

在更進一步之具體實施例中，茲提供一種設備，其至少包含：至少一處理器；以及至少一編碼一資料結構之

[S]

有形電腦可讀取儲存媒體。該資料結構包含相關於一組解析參數之資訊，該資料結構能按照由一名稱解析軟體組件所可使用的方法來儲存，以支配一名稱解析處理，該資料結構包含：一資訊正準備記錄於其中之第一位置，其定義一組用於網路資源之一或更多之識別符，其中該等解析參數能應用於該組識別符；一資訊正準備記錄於其中之第二位置，其定義一被時現在一通訊通道上之安全類型，其中該名稱解析處理係透過該通道來交換資訊；一資訊正準備記錄於其中之第三位置，其定義至少一受信任之憑證管理；以及一資訊正準備記錄於其中之第四位置，其定義至少一網路資源，其中正準備與該網路資源建立該通訊通道。該至少一有形電腦可讀取儲存媒體包含該資料結構之複數個實例，該資料結構之各個實例係與特定一組解析參數相關連。該至少一處理器適用於運行該名稱解析軟體組件，而該名稱解析軟體組件係適用於根據至少一組應用解析參數來執行該名稱解析處理。該名稱解析軟體組件能讀取至少某些的複數個資料結構實例，該等資料結構實例係編碼在至少一有形電腦可讀取儲存媒體上，以判斷一或更多組應用解析參數。

前述內容是作為本發明之非限制性概括摘要，而本發明係由隨附的申請專利範圍所定義。

【實施方式】

[S]

申請人已體認並了解到習知的名稱解析科技(包括DNS)的安全性，可再加以增進。進一步而言，習知的名稱解析技術並未被設計成能以通過單一網路介面及單組網路硬體而連接到若干網路的方式來運作，因此阻礙了疊蓋網路的成長。

例如，當 DNSSEC 被提出用來確保 DNS 查詢的結果是正確的同時，其卻需依賴兩個許多人認為無法接受的條件。第一，各個用於回應一 DNS 查詢(其可為不同位置且由不同方所管理)之 DNS 伺服器必須實作成負責處理 DNSSEC，而這會讓整體網路變得更難轉出(rollout)。第二，DNS 客戶端基本上將必須扮演一完整解析器的角色，而不是一種如正常 DNS 般會將大多數用於解析查詢之回應傳遞給一完整解析器(DNS 伺服器)的「柱形解析器」(stub resolver)。這會增加該客戶端的處理，因為 DNS 客戶端將會變成要負責確保回傳到 DNS 客戶端的各結果是合法且正確的，藉由審視該結果之數位簽名以判斷用來發出在該結果上簽名之憑證的憑證管理(CA)是否值得信任。將此責任交給執行該 DNS 客戶端之客戶端計算裝置，會有使該計算裝置負載過重的風險，特別是在考量到較不具運算能力的計算裝置像是個人數位助理(PDA)及行動手機的情況下。為了能從客戶端卸去此重擔，可將此工作交給伺服器或其他網路資源。

進一步而言，習知的名稱解析技術並不適用於工作在疊蓋網路可能存在的情境下。在過去，一計算裝置可藉

[S]

由一專屬網路介面而連接到各網路，而該網路介面將由使用者及／或由裝置來在各網路上進行設置以與該等網路互動，包括設置該介面以支援由網路所實現之名稱解析技術。例如，當一計算裝置(像是一膝上型電腦)連接到無線網路時，在網路上之動態主機組態協定(DHCP)伺服器可提供在其他參數中之一 IP 位址、一用於閘道器之識別符以及一用於 DNS 伺服器之識別符給該計算裝置。然後，任何通過使用一文字識別符之介面的通訊，將通過 DNS 伺服器來解析。若一計算裝置要連接到不同網路或是使用不同名稱解析技術，則將必須設置另一個界面。舉例而言，可使用第二有線介面，或是使用無線介面。

申請人已經體認並了解到，在現代網路中，「疊蓋」(Overlay)網路已經變得越來越普遍。這些疊蓋網路被設置成能與現存網路共同存在於相同硬體上，且係位於現存硬體網路之上的邏輯疊蓋。連接到疊蓋網路之各網路裝置亦可連接到一或更多現存硬體，像是現存的區域網路及／或現存的廣域網路。此類疊蓋網路可以各種方式來實現，例如，使用微軟直接存取(Microsoft Direct Access)。該疊蓋網路可因此被視為一或更多其他網路的受限子群組。

使用這些科技，一連接到給定硬體網路之計算裝置，可因此能經由單一介面而同時地連接到多個網路，包括承載(underlying)網路以及一或更多疊蓋網路。習知的名

[S]

稱解析技術是無法支援此類網路(像是名稱解析協定的類型)的，或者計算裝置應與其通訊之用於名稱解析的網路資源（例如 DNS 伺服器），與承載網路之名稱解析科技相比下，會與用於疊蓋網路之網路資源不同。

進一步而言，因為某些網路能將某些關於如何存取在網路上之某些資源的資訊保持隱密－例如，該一特定安全伺服器之位置／身分或是其他網路資源－而讓這些資訊能避免被給予至潛在的攻擊者，一特定伺服器或其他資源可為一名稱解析查詢之所欲結果的唯一可能來源。替代地，一特定網路資源可具有一在疊蓋網路之外都不為人知的識別符，或著那是該疊蓋網路外部之另一資源的文字識別符的複製品，而一特定伺服器或其他資源可為用於該特定網路資源之一名稱解析查詢之所欲結果的該唯一可能來源。據此，對於計算裝置而言，即使該等疊蓋網路使用相同的名稱解析技術，在名稱解析處理期間與一特定伺服器或其他資源接觸仍是有必要的，該名稱解析處理對於在該(等)疊蓋網路上的通訊而言可相異於承載硬體網路。有鑑於此，對於一計算裝置的網路介面而言，要針對多個疊蓋網路各者維持 DNS 伺服器之多個位址是有必要的，使得該計算裝置可與各疊蓋網路通訊。若採用習知的計算裝置、網路技術以及名稱解析科技，則這是不可能達成的。

在此所述為用於安全名稱解析科技以及用於確保名稱解析科技可在現代網路(其具有複數個可經由單一網路

[S]

介面來進行存取的疊蓋網路)中發揮作用的原理。在某些實作中，一使用者，像是一末端使用者及／或一管理者，可編譯一組解析參數，該組解析參數可應用到一計算裝置上以由該計算裝置之一個、多個或全部的網路介面來使用，以藉由使用介面可存取之網路的名稱解析科技來解析名稱。然後，該等解析參數可支配由介面所執行的名稱解析處理。例如，在某些實作中，解析參數可指定DNSSEC 參數及／或關於直接存取的參數，吾人應了解到亦可使用其他的名稱解析科技及其他類型的網路及安全技術。該等解析參數可按任何方式來儲存，例如，在一規則表中可由一名稱解析模組來審視並且用來裝配(assemble)一名稱解析查詢。

該等解析參數可包含任何關於如何實行一名稱解析處理的適合資訊。更甚者，所用之特定資訊可視名稱解析所尋找之網路類型而定。例如，對於 DNSSEC 用作為名稱解析科技的網路而言，該等參數可包括安全參數，像是該等解析參數能應用於哪些網域、確認該伺服器是否曾經驗證一回應、加密是否應該被用於與該伺服器之通訊中、應該使用什麼類型的加密、是否應該信任憑證管理(CA)或是認證以簽名結果、以及應該針對結果查詢哪個 DNS 伺服器。如另一範例般，對於一疊蓋網路而言，像是使用直接存取之疊蓋網路、或是諸如以下之解析參數，像是：該等解析參數能應用於哪個網路／網域、應該針對結果查詢哪個 DNS 伺服器、是否應該使用加密、

[S]

應該使用什麼類型的加密、是否應該信任憑證管理以簽名結果、以及當與一疊蓋網路進行通訊時應該使用什麼代理伺服器等，皆可被實現。可依據網路以及其所實作之名稱解析技術來使用任何適合的解析參數。

如在此所用般，根據任何適合的名稱解析協定，一名稱解析處理可為任何用於判斷一對映到一文字識別符之數字識別符之適合技術，反之亦然。在如下所概述之範例中，網域名稱伺服器(DNS)協定可被當作一名稱解析協定之範例來使用，而名稱解析處理可被描述為確認該DNS協定。然而，吾人應了解到，DNS僅是一名稱解析協定之範例，其中根據在此所述原理所運作之技術可與該名稱解析協定共同運作，且可實現任何適合的名稱解析協定，本發明之具體實施例並不僅限於此。

吾人應了解到，許多範例在此是按判斷一數字識別符對應到一輸入文字識別符的背景來描述之同時，在某些具體實施例中可實現名稱解析處理，以額外或替代地將其用作為輸入一數字識別符以及判斷一對應之文字識別符。進一步而言，吾人應了解到在以下概述範例描述能運作於文字識別符及數字識別符間之一對一對應的技術－判斷對應於單一文字識別符的單一數字識別符－同時，這是唯一的示範性具體實施例，且在某些實作中一文字識別符可具有複數個對應之數字識別符，且數字識別符可具有複數個相對應之文字識別符。

在此所述之技術可實現於各種計算系統中，其範例會

[S]

在以下作更詳細的描述。此系統通常牽涉到實作一些功能性模組之適當設置(suitably-configured)計算裝置的使用，該等模組各者提供完成此技術之所需執行的一或更多運作。各功能模組可按其本身方式來實作；所有模組並不需以相同方式來實作。如在此所使用般，一功能性模組是一系統之結構性組件，該系統是執行一運作性角色(operational role)。該運作性角色可為軟體元件之一部分或是全部。例如，一功能性模組可執行一處理功能、一分離式處理、或任何其他合適的處理單元。一功能性模組可包含電腦可執行元件，且可在一電腦儲存媒體上編碼。額外地，此電腦可運行指令可使用任何適當的程式語言及／或程式或腳本(scripting)工具，且亦可被編譯成能在一框架或虛擬機器上執行的機械語言碼或中間碼。功能性模組可以視情況依並列或是串列方式來執行，且可在彼此間使用在他們所運行之電腦上之共享記憶體、使用一訊息傳遞協定或任何其他適當方式來傳遞資訊。以下描述之示例功能性模組能實行一或更多任務，因此其應了解到該等功能性模組及任務部分是僅用來描述可實現在此所述之示範性技術的功能性模組的類型，且本發明並未被限制只能用功能性模組之任何特定方式、部分、或類型來實現。在某些實作中，所有功能可被實現成一單一功能性模組。再者，為了清楚起見，以下討論之功能性模組，全部都是在一或兩個計算裝置上執行，然吾人應了解到，在某些實作中，該等功能性

[S]

模組可實作在許多適用於與彼此通訊之個別計算裝置上。例如，一計算裝置可適用於運行一輸入模組以接收一第一識別符，像是一文字識別符，並與一在一第二計算裝置上之名稱解析模組通訊，以執行一名稱解析處理來判斷一對應到文字識別符之數字識別符。

在此所述原理的一示範性實作中，一在一計算裝置上運行之軟體應用程式可接受一所欲網路資源之文字識別符之使用者輸入，其中該軟體應用程式要與該所欲網路資源建立一連接。舉例而言，該軟體應用程式可為一網頁瀏覽器，該文字識別符可為一網站的網域名稱，而該網路資源可為一管理該網站之網頁伺服器。為了開啟對所欲網路資源之連結，該軟體應用程式或一連結模組將使用一針對該網路資源之數字識別符，所以一名稱解析模組(在此亦稱為「解析模組」)可將該文字識別符轉換成一扮演網路位址角色之數字識別符，像是 IPv4 或 IPv6 之 IP 位址。

用於網路資源之文字識別符將因此能傳遞至一名稱解析模組，該名稱解析模組適用於執行一名稱解析處理以獲得該數字識別符，其中該名稱解析模組則可回傳至該軟體應用程式。然而，在執行該名稱解析處理之前，該解析模組可重新檢視多組解析參數的集合以判斷，如果有的話，是哪組解析參數應用到該正待執行之名稱解析處理。此集合可按任何適合方式以任何適當形式來儲存，包括儲存在一電腦儲存媒體，像是記憶體中。為了

[S]

重新檢視該集合以判斷哪組參數能應用‘該解析模組可從記憶體中擷取某些或全部的集合並執行各種形式的比對處理，像是將一輸入識別符與某些或全部集合中之一參數進行比對，以表示一組特定解析參數是應用到哪個網路資源。

在該集合中之各組解析參數可應用到一或更多之網路資源‘且可管理一名稱解析處理在判斷用於其所應用之網路資源之識別符的方式。這些解析參數可含有任何適當的參數，其可影響該名稱解析處理如何實行的方式，包括任何以上曾討論之範例參數。例如，各組名稱解析參數可依據哪個解析模組應該與之通訊來指定一特定解析資源，以判斷該數字識別符，像是一特定 DNS 伺服器。

由解析模組對該集合重新檢視之過程可用任何適當方式來完成。在一實作中，重新檢視可包含將該文字識別符與用於多組解析參數各者之識別符相比對，以判斷該等識別符之間是否匹配。舉例而言，用於一組解析參數之識別符可為一 DNS 尾綴碼 (suffix)，像是「*.corp.contoso.com」，從而任何與該識別符後面部分相匹配之文字識別符會成為該等解析參數所應用之識別符。因此，若輸入文字識別符是「webserver.corp.contoso.com」，則該組參數將會成為一組與識別符相關之參數，且可被視為一組可應用解析參數。一旦能判斷一或更多組可應用解析參數，則一名稱解析處理可根據該等可應用解析參數而被實行。舉例而

[S]

言，若該等參數指定一特定解析資源，像是一 DNS 伺服器，則將能建立對解析資源的一連結，若該等參數指定了正待使用之加密層級，則與一名稱解析資源之通訊將會使用該加密層級。

一旦該解析模組已使用可應用參數而建立了與該解析資源之連結，則通過該連結而發佈一解析請求到該解析資源，該解析請求包括該文字識別符及請求該對應數字識別符。該解析資源可執行任何適合的處理，包括在該領域中已知的任何各種處理，以用於判斷該對應數字識別符，像是藉由諮詢其於本地端維護之資訊，或根據可應用解析參數而發送該請求到另一解析資源。一旦該解析資源已判斷該數字識別符，則該解析資源可在該數字識別符上執行任何適合的驗證處理。例如，若可應用解析參數指定 DNSSEC 應被用於判斷該數字識別符，並指定一或更多受到信任而提供一有效憑證（其可用於鑑定結果）之特定憑證管理，則該解析資源可在該驗證處理期間，判斷該結果是否使用由一或更多特定憑證管理中所發出之任一憑證來簽名。若是，則該解析資源可提供該數字識別符給在該計算裝置上之解析模組，來做為該解析請求之結果。該解析模組則可確認該結果是否曾根據可應用解析參數而產生，以及將該結果呈現給軟體應用程式以用於建立對該所欲網路資源之連結。在另一方面，若該結果未使用一指定憑證來簽名，則該結果可被忽略，或是提供給該解析模組一指示符，該指示符是指

[S]

示該結果未根據解析參數來簽名。

這些明顯的優勢，可根據在此所述原理透過執行一名稱解析處理的方式來加以提供。首先，藉由維持一組解析參數之集合，一名稱解析處理可使用該等解析參數而被參數化，以確保該解析處理是安全的以及其結果是可信任的。例如，在傳統的名稱解析科技中，一計算裝置必須信任來自一曾是一正確特定結果的結果，來自該集合之解析參數允許在一計算裝置內之解析模組能查詢一特定、受信任的解析資源以在對回應是正確具有高度信心的狀況下而獲得一所欲網路資源之識別符（數字或文字）。進一步而言，該解析模組可更確信該目標解析資源將會有該模組正在尋找之對應識別符。此外，藉由使用解析參數之集合，一解析處理可，藉由例如具體指明是否使用加密、應該使用哪個類型的加密、以及應該如何驗證加密的方式，而更安全地完成。進一步而言，藉由具體指明是要與哪個特定解析資源進行通訊，該集合可使得在計算裝置上之解析模組能執行較少功能，且在計算裝置上會較不顯累贅，而當某些功能可被推動至網路資源（像是解析資源）時，該等集合指示符能適於處理。例如，在一示範性 DNSSEC 實作中，某些驗證處理可在該網路中之解析資源上執行，像是一 DNS 伺服器。具有該集合之解析模組將會知道要去接觸該能夠執行 DNSSEC 任務的特定解析資源。額外地，使用該集合，一解析模組能夠執行用於不同輸入識別符之不同解析參

[S]

數，像是接觸一用於在一疊蓋網路中之網路資源之一文字識別符的特定解析資源，或是使用一安全通訊通道以用於交換相關於特定安全網路資源之識別符。

根據在此所述原理所運作之該等技術之額外功能及優勢，將能依據以下所述之範例而更完全地了解。以下範例意圖促進對本發明之了解並詳細說明在此所述原理的益處，但是並未將本發明之具體實施例的全部範疇作為例示。

根據在此所述原理而運作的技術可採用任何適當的電腦系統來實作，該等電腦系統包含任何適當數目或類型的計算裝置，亦包括任何適當數目及類型的網路資源。地 1 圖顯示一繪例性電腦系統，其中在此所述原理之某些示範性實作可於其中動作。然而，吾人應了解到，其他的實作亦可運作於任何其他適當的電腦系統中。

第 1 圖顯示一包含通訊網路 100 的電腦系統，該通訊網路 100 係一使用者裝置（亦即電腦裝置 102）可相連接的。通訊網路 100 可為任何適合的有線及/或無線網路，包括較大有線及/或無線網路的一部分，像是一歸屬（home）網路、企業網路的一子網路(subnet)、網際網路等等。計算裝置 102 可顯示為一桌上型個人電腦，但亦可為任何適合的計算裝置，像是膝上型個人電腦、PDA、智慧型手機、伺服器、機架式電腦、網路裝置(像是路由器或交換器)或其他計算裝置。

計算裝置 102 係耦接到資料儲庫(data store)104，其儲

[S]

存多組解析參數之集合。該資料儲庫 104 可被編碼在任何適合的電腦儲存媒體或媒介上，並可按任何適合格式來儲存資訊。在資料儲庫 104 中所儲存的資料是可被用來支配解析參數處理以用於判斷對應到一輸入第一識別符之第二識別符，像是判斷一用於網路資源之數字識別符，該網路資源係對應於一輸入文字識別符。如上所討論般，該等解析參數可包含可於名稱解析處理期間所使用的任何適合資訊。該計算裝置 102 可適用於運行一或更多實作此一名稱解析處理的功能性模組，其中該等解析參數被用來形成一連到網路資源之連結，而網路資源是與通訊網路 100 相連接。

儲存於資料儲庫 104 中之多組解析參數之集合可按任何各種方式來儲備，包括由在計算裝置 102 本地端之使用者使用任何適合之使用者介面來輸入及/或藉由使用計算裝置 106 之管理者來遠端地儲備。在一範例中，一管理者可在計算裝置 106 處指定該等解析參數並通過任何適合之網路管理技術將他們往下推至計算裝置 102。例如，若該通訊網路 100 包含來自位於 Redmond, Washington 之微軟股份有限公司的微軟視窗網路，則該管理者可使用一網域控制器以通過目錄服務協定（Active Directory protocol）來使用群組政策的方式將該等解析參數向外推出。然而，吾人應了解到，這僅僅是可用來實作之網路管理技術的一個範例，且可根據在網路上可用之資源來使用任何適合的技術。

[S]

該計算裝置 102 可使用多組解析參數之集合以執行名稱解析處理以用於判斷一用於網路資源（像是網路資源 108）之識別符（文字或數字），其可為任何能經由網路來存取之計算裝置，像是任何種類的伺服器。為了達成此目的，該計算裝置 102，在接受用於網路資源 108 之第一識別符的輸入後，可在考量到儲存於資料儲庫 104 中之多組解析參數之集合後來判斷一組可應用之解析參數，然後執行由該組可應用解析參數所支配之名稱解析處理。在名稱解析處理期間，一在該計算裝置 102 上運行之解析模組可與一名稱解析資源 110 進行通訊以判斷一或更多用於網路資源 108 之識別符。可根據在此所述原理來運行任何適合的名稱解析處理，包括任何以下描述之示範性名稱解析處理。此一處理可包括按任何方式使用任何適合網路裝置（如解析資源 110）來進行之資訊交換。當解析資源 110 如第 1 圖般繪示為一伺服器的同時，吾人應了解到任何適合的計算裝置可被當做一解析資源來使用，包括多用途裝置(像是個人電腦)以及單用途裝置（像是硬體名稱解析裝置）。

在某些實施例中，該通訊網路 100 可非為單一網路，但可為具有一或更多疊蓋網路 100A 於其上例示的硬體網路。該（等）疊蓋網路 100A 可完整地例示於硬體實作通訊網路 100 上，或是可在用於通訊網路 100 上之硬體上運作。該（等）疊蓋網路 100A 可與該通訊網路 100 共享網路硬體，像是路由器或是交換器，但是可以有某

[S]

些資源，像是客戶端及伺服器端計算裝置，能經由硬體與通訊網路100連接但是不可以被非疊蓋網路100A成員的裝置所存取。

如上所討論，為了與在疊蓋網路上之網路資源通訊，計算裝置102必須與具有在疊蓋網路100A上之可用網路資源上之資訊的特定解析資源進行通訊，因為只有這些特定解析資源具有在疊蓋網路 100A 上之可用網路資源上之的知識。在此類實作中，多組解析參數之集合可具體指明一或更多可在一名稱解析處理中與該計算裝置102通訊之特定解析資源110A，以獲得用於網路資源（像是網路資源 108）識別符。在該集合中某些或所有組的解析參數可具有與疊蓋網路 100A 之網路資源相匹配的識別符。當計算裝置 102 的解析模組重新檢視該集合以判斷該組可應用解析參數時，該等可應用解析參數可指示那些用於所欲網路資源之識別符可從該特定解析資源110A處擷取。因此，當由計算裝置 102 所運行的名稱解析處理被該組可應用解析參數予以參數化時，可與該指定解析資源110A進行通訊以擷取用於所欲網路資源108之識別符。吾人應了解到此重新檢視以及名稱解析處理可按任何適合方式來實行，包括以下所述之任何示範性技術。

額外地，在某些實作中，該等可應用解析參數亦可具體指明了對網路資源 108 之通訊應經由代理伺服器 112 來完成。然後，在回傳用於網路資源之第二識別符途中，

[S]

該解析模組可額外或替代地回傳一識別符，像是用於代理伺服器 112 的數字或文字識別符。

如上所討論，一組解析參數可包括能用於實行名稱解析處理之任何資訊。第 2A 及 2B 圖繪示了儲存多組解析參數之集合的示範性資料結構，該等解析參數係根據在此所述之採用兩個示範性網路技術的原理而用於某些實作中。額外地，在第 2A 及 2B 圖顯示包含相關於兩種不同技術之參數的兩種不同集合的同時，吾人應了解到，在某些實作中，這些科技可被實現於同一組的解析參數中。進一步而言，一集合可被實現成任何適合的資料結構，且在某些實作中，可包含其他資料結構，各個資料結構能儲存相關於一或更多組解析參數的資訊。這些資料結構可被儲存在關連於客戶端計算裝置的電腦可讀取儲存媒體中，該客戶端計算裝置可請求名稱解析。吾人應了解到在第 2A 及 2B 圖中所示之資料結構以及其所儲存之參數是僅作為說明可以使用之資料結構及參數的類型，像是可使用任何類型的網路科技。

第 2A 圖顯示儲存解析參數之集合 200A 的第一資料結構，其具有兩組示範性之解析參數在該集合中。如第 2A 圖所示，在某些實作中，解析參數之集合可被組織成一表格，其包含複數個欄位及列，各欄位具體指明一類型之解析參數，而各列具體指明一組解析參數，而弱使用任何適當格式的話則其他的實作方亦是有可能的。在集合 200A 中之說明性解析參數包括相關於一 DNS 解析處

[S]

理的參數，像是是否使用一 DNSSEC 協定以及是否或是如何實現其他的 DNS 安全參數。然而，如上所述般，吾人應了解到 DNS 僅是解析參數科技的示範類型，而在此所述原理可運作之協定，則可如同任何適合的名稱解析協定般使用。

第 2A 圖中所示之第一說明性解析參數是「名稱」(Name)參數 202。此參數 202 指示一組解析參數能應用於哪個識別符，以及該組解析參數能應用於哪個網路資源。該名稱參數 202 可由一解析模組所使用，以判斷在一集合中的哪組解析參數能應用於一用於輸入識別符的給定解析處理。該名稱參數 202 可儲存任何用於一網路資源之識別符，包括任何數字或文字的識別符。例如，一數字識別符可為一用於指定網路資源的識別符，像是 IP 位址“1.2.3.4”或可為能用於一網路資源範圍的識別符，像是 IP 網址子網路“157.0.0/8”。相似地，一可用於名稱參數之文字識別符可為一用於特定網路資源之識別符，像是完整網域名稱（FQDN），例如 “itweb.contoso.com”，或是用於網路資源範圍的識別符，像是 DNS 尾綴碼，像是“*.contoso.com”或是 DNS 前綴碼，像是“itweb.*”。

在第 2A 圖中所示的次個解析參數是 DNSSEC 參數 204。更具體而言，該範例“DNSSEC”參數儲存一個二進位值(開啟或關閉)，其指示在一用於網路資源的解析處理（其與名稱參數相匹配）中是需要 DNSSEC 驗證的。當一組解析參數中之 DNSSEC 參數 204 被設定為開啟/

[S]

真（on/true），一解析參數可根據該 DNSSEC 協定來執行一解析處理，且可確保任何結果是根據解析參數而驗證的。一運行該解析參數之解析模組亦可確保 DNS 查詢之任何結果已經根據 DNSSC 標準而驗證，且可在一經傳輸 DNS 請求中指示已經請求了 DNSSEC 驗證，例如藉由在該請求之標頭中設定一“DNSSEC OK”(DO)旗標的方式。

次個參數係相關於在計算裝置之間的 DNS 交換的安全性，例如在 DNS 客戶端及 DNS 伺服器端之間或是在任何其他組的裝置之間。該第一參數 “DNS over IPsec”參數 206，可儲存一個二進位(開啟/關閉或真/偽)值，旗指示是否在用於名稱解析處理之通訊通道上實現 IPsec。例如，若 IPsec 參數被設定為真，則當建立一對名稱解析資源的連結時，一解析模組可執行加密及/或鑑定（authentication）處理。若用於一組解析參數之“DNS over IPsec”被設定為開啟/真，則該解析模組可審視該組中之其他參數以判斷該 IPsec 協定的設定。次兩個參數“IPsec Encryption Level”208 及“IPsec CA”210 為此類參數之範例。“IPsec Encryption Level”可儲存任何能具體體指明是否應使用加密的數值，及/或應該使用什麼類型的加密。“IPsec Encryption Level”參數 208 可儲存一無/低/中/高的數值，其用於指示特定類型的加密，例如，「低」可指示任何大小的三重資料加密標準（3DES）或進階加密標準(AES)之加密，而「高」可指示 192 或 256 位元的 AES 加密。替代地，該 IPsec 加密層級可儲存對於一特

[S]

定加密標準的參考值，像是 AES(256)。“IPsec CA”210 可儲存用於一或更多憑證管理的識別符，該等憑證管理受信任以發出對於解析資源之鑑定憑證。當設定好時，在 IPsec 的鑑定處理期間，該解析模組可確認一解析結果是按一鑑定憑證所鑑定，該鑑定認證是由受信任 CA 其中之一對一受信任解析資源所發出。額外地，若 DNSSEC 被開啟，則檢查來自 DNS 伺服器之回應並判斷在該回應中之延伸金鑰用途(EKU)簽名是否來自於受信任 CA 的其中之一，且因此產生該結果的 DNS 伺服器由解析參數所授權，以代表計算裝置來執行 DNSSEC 認證。

在第 2A 圖中所示的最後參數，“DNS server”212，可儲存一或更多伺服器的列表，其中在解析處理期間一解析模組應與該等一或更多伺服器進行通訊。當輸入到一解析模組之識別符與用於一組解析參數之名稱參數相匹配時，則該解析模組將查詢列於用於識別符之“DNS server”參數中的任何 DNS 伺服器，該“DNS server”參數係對應到輸入識別符。“DNS server”參數可儲存用於一或更多 DNS 伺服器之任何適合識別符，其可被用來建立對該（等）DNS 伺服器的連結，包括任何適合的數字及/或文字識別符。

第 2A 圖顯示兩個儲存多組解析參數之說明性資料結構，該等多組解析參數能形成該集合 200A，各組參數包含可被當做該集合之參數來儲存的說明性數值。吾人應了解到這些多組參數是多組參數之可使用類型的範例，

[S]

且可使用任何數值來做為參數，且可使用任何數量的多組參數。

第 2B 圖顯示儲存解析參數之集合 200B 的第二示範性資料結構。如第 2A 圖中所示，該集合 200B 被組織成一表格，其具有複數個識別參數之欄位以及複數個識別多組解析參數之列，但是吾人應了解到任何格式皆可被使用。進一步而言，在第 2B 圖的範例中，該等解析參數包括可被用來與用於疊蓋網路之微軟直接存取(Microsoft Direct Access)功能建立連結。然而，吾人應了解到，直接存取僅為網路科技類型及協定的範例，其中在此所述之原理可與該等網路科技類型及協定一起運作，同時，可使用任何適合的網路科技，包括任何適合的疊蓋網路科技。

第 2B 圖中所是的第一參數是“Name”參數 220。近似於集合 200A 中的名稱參數 202，此參數識別一組解析參數可應用到之該（等）網路資源，且可由一解析模組來使用以判斷在一集合中的哪組解析參數能應用到用於一輸入識別符的給定解析處理。該名稱參數 220 可儲存用於網路資源之任何識別符，包括任何數字或文字識別符，包括任何上述關連於集合 200A 之示範性識別符。

在第 2B 圖中之次個參數係相關於直接存取技術。該“Zone-Specific DNS server(s)”參數 222 可儲存用於一或更多 DNS 伺服器之任何識別符，其可被當做在疊蓋網路上可用網路資源的名稱解析處理中的一部分來查詢。如

[S]

上所討論，在某些疊蓋網路中，某些網路資源不允許由在硬體網路上之全部計算裝置進行一般存取，其中疊蓋網路上存在於該硬體網路上，而可藉由不去廣泛散布用於網路資源之識別符的方式來多少強迫實施此限制。然後，為了獲得在疊蓋網路上用於一網路資源之識別符，一解析模組可接觸一組或較小組的解析資源。據此，若輸入到一解析模組的識別符與用於一組解析參數之該名稱參數 220 相匹配，則該解析模組可接觸一在“Zone-Specific DNS server(s)”參數 222 中具體指明之 DNS 伺服器，以獲得用於網路資源之對應識別符。

“Zone-Specific Proxy”參數 224 是次個顯示的參數。此參數 224 可由解析模組來使用以對軟體應用程式指示該軟體應用程式正與在疊蓋網路上之網路資源接觸，並設置該軟體應用程式以使用一代理伺服器以執行其連結，或使用一經識別之代理伺服器以執行其連結。例如，若該軟體應用程式想要對一特定網路資源進行連接，而該組可硬備解析參數對該解析模組指示應使用一代理伺服器，則該解析模組可指示該軟體應用程式其應經由該代理伺服器與該網路資源進行連接。該集合 200B 之代理伺服器參數 224 可儲存任何可接受數值，包括用於資源之數字及/或文字識別符，一零值或其他指示不需要代理伺服器的指示符，或指示該預設代理伺服器之設定應由該軟體應用程式來使用的數值。

次個參數“Remote DNS over IPsec”226 被用來指示在

[S]

疊蓋網路上對網路資源之連結是否應根據該 IPsec 協定來加以保全，像是予以加密及/或鑑定。如同集合 200A 之“DNS over IPsec”參數 206 般，集合 200B 之“DNS over IPsec”參數 226 可採用二進位數值，像是開啟/關閉或真/偽，用來指示是否使用 IPsec。亦與集合 200A 相似的是，“Remote Encryption Level”228 可儲存任何適合的數值，其指示是否應使用加密以及使用哪種類型的加密，以保全對解析資源的連結，而 “IPsec CA”230 可儲存用於一或更多憑證管理之任何適合識別符，該等憑證管理被信任以發出用於解析資源之鑑定憑證。

如第 2A 圖般，第 2B 圖亦顯示兩個儲存多組解析參數之說明性資料結構，該等多組解析參數能形成該集合 200B，各組參數包含可被當做該集合之參數來儲存的說明性數值。吾人應了解到這些多組參數是多組參數之可使用類型的範例，且可使用任何數值來做為參數，且可使用任何數量的多組參數。

更進一步，吾人應了解到當兩個集合 200A 及 200B 係分別顯示並著墨於兩個不同科技－DNS 安全/DNSSEC 及直接存取－吾人應了解到在某些實作中，一組解析參數可包括關於該等科技及/或任何其他類型之網路科技兩者的參數。例如，針對一給定疊蓋網路，該組解析參數可對一解析模組發出指令以使用 DNSSEC 及其他 DNS 保全以執行用於該疊蓋網路之名稱解析。

在根據在此所述原理所運作之某些技術中，額外的解

[S]

析參數可被含括在解析參數之集合內，但其不屬於任何特定一組解析參數的一部分。這些全域(global)參數亦可被用於支配一解析處理，但可指示何時或是否使用任何一組解析參數、可只是如何處理在名稱解析中的錯誤、或可為能應用到所有組的參數。例如，若一計算裝置支援網路區域察知(NLA)，該網路區域察知可通知其所連接之硬體網路之計算裝置，該集合可包括一全域設定，其指示是否基於該裝置所連接之網路的身分或類型，而放棄對全部或部分表格的重新檢視。例如，若 NLD 指示該計算裝置未連接到一存在著疊蓋網路之特定硬體網路，則「NLA 旁通」(NLA Bypass)參數可對該解析模組指示，其應放棄對關於疊蓋網路之所有組參數的重新檢視，或是可指示其應放棄對用於一特定疊蓋網路之所有組解析參數的重新檢視。

額外或替代地，一全域參數可指示若處於一特定網路之外的話應如何發出一解析請求。例如，若該計算裝置是位於一特定硬體網路之外，則一"Query Behavior"參數可指示該解析參數應針對特定類型的識別符進行查詢，像是在 IPv4 數字識別符之前的 IPv6 數字識別符，或是只有 IPv6 數字識別符。另一全域參數可相關於若是名稱解析處理失敗時該如何反應，因為第二識別符並未根據該組可應用解析參數來定位。此"Fallback Behavior"可指示該解析模組應該嘗試使用替代之名稱解析科技，或是可指示不允許後降(fallback)。例如，該參數可指示，若

[S]

一 NDS 處理失敗，則可嘗試 LLMNR 或 NetBIOS 處理。

這些示範性集合及解析參數，以及在任何適合集合中之任何其他適合之解析參數，可由一解析模組所使用以根據任何類型之名稱解析科技來運行一名稱解析處理。任何適合的名稱解析處理可由該組可應用解析參數來實作並支配。第 3 圖顯示一可實行名稱解析的處理 300。然而，吾人應了解到，該處理 300 僅為可實作科技之類型的範例，同時可使用任何適合的技術。

處理 300 開始於方塊 302，其中用於一網路資源之第一識別符是由一計算裝置之功能性模組所接收。第一識別符可被任何適合來源所接收或自任何適合來源處接收，該來源包括來自一經由適合使用者介面的使用者，該適合使用者介面包括一軟體應用程式之使用者介面。該第一識別符可為用於一網路資源之任何適合識別符，包括根據一名稱解析協定之任何適合文字識別符，像是 DNS 協定之網域名稱。在方塊 304，第一識別符則可被傳遞到一名稱解析模組以判斷用於該網路資源之第二識別符。這可用任何理由來完成。例如，若該第一識別符曾為由一軟體應用程式所接收之文字識別符，則該軟體應用程式可判斷其如第二識別符般需要一用於網路資源之數字識別符以建立對該網路資源之連結。此使用案例僅僅為示範性，然而，在此所述之原理是能與以任何適合動機來運行的名稱解析處理相容。

在方塊 306，該解析模組判斷該集合是否具有能應用

[S]

到該識別符的任何一組解析參數，其中該識別符係為名稱解析所正尋找之識別符。此可按任何適合方式來完成。例如，該解析模組可從一資料儲庫擷取多組解析參數之集合，並將該第一識別符與該集合做比較，以判斷若有可能的話，是哪組解析參數能應用到第一識別符。可用任何方式來完成此比較，像是藉由將該第一識別符與在第 2A 及 2B 圖中所述之「名稱」參數進行比較。該解析模組則可判斷一或多組之解析參數能應用到一正待由該模組運行的名稱解析處理，且還可使用該組可應用解析參數以支配該處理，或按任何適合方式透過合併多組解析參數來判斷一組可應用解析參數。

對一組可應用解析參數之判斷步驟 306 可按任何適合方式來實行。所實行的確切方式可視該集合的格式而定，以及視被選中含闊在該集合中的解析參數而定。第 4 圖顯示一判斷處理之範例，但是吾人應了解到該處理 400 僅為說明可當做處理 300 之方塊 306 部分來執行之動作，而其他處理也是可能的。

處理 400 開始於方塊 402，其中該解析模組對來自一資料儲庫之多組解析參數的集合進行存取。此資料儲庫對於該計算裝置而言為本地端，其中該解析模組係執行於該計算裝置上，如同第 1 圖的範例般，或其可經由任何適合的通訊媒體或媒介（像是電腦通訊網路）而為可用。在方塊 404，針對在該集合中之各組解析參數，該解析模組可擷取用於與識別符相匹配的圖樣(pattern)，其

[S]

指示各組參數是應用於哪個用於網路之識別符。該圖樣可為網路資源之任何適合指示符，包括上述關連於第 2A 及 2B 圖之名稱參數或任何其他的數字及文字指示符。在方塊 406，第一識別符係與各圖樣相比較以判斷該組解析參數是否對應到一應用到該第一識別符之圖樣。例如，若第一識別符為“webserver.corp.contoso.com”而圖樣為“*.corp.contoso.com”（其中是*萬用字元），則在方塊 406 中可判斷該組解析參數能應用到第一識別符。

在方塊 408，一旦判斷了該組可應用解析參數，則擷取該組中的參數並將其用於支配一名稱解析處理。在某些實作中，只有單組解析參數會被當做一組可應用解析參數來擷取，同時可擷取在其他多組中的解析參數。若獲得了多組，則可使用任何適合處理來判斷來自多組解析參數中之該組可應用解析參數。例如，可將該等參數合併以判斷一組具有最高安全層級、或是最低安全層級、或是任何其他適合標準的可應用解析參數。如另一範例般，若多組解析參數相匹配，則該解析模組可選擇具有能最接近地匹配之圖樣的該組參數。例如，若第一識別符為“a.corp.ms.com”而在該集合中之某一組為“corp.ms.com”而某一組為“ms.com”，則可選擇用於“corp.ms.com”的該組解析參數，因為其更加地具體指明了。

回到第 3 圖的處理 300，在方塊 308 中，一旦已經判斷了該組可應用解析參數，則該解析模組可執行一用該

[S]

組可應用解析參數來加以參數化的名稱解析處理。然後，該解析模組可如同該解析處理之輸出般，獲得用於該網路資源之第二識別符。例如，若第一識別符為一文字識別符，則第二識別符為一數字識別符，像是IP位址，反之亦然。在方塊310中，該解析模組則可將第二識別符回傳到該功能性模組，其在方塊302中曾將第一識別符傳遞給該解析模組，然後該處理結束。

方塊308及310可按任何適合的方式來實行。第5圖顯示一示範性處理500，其中可執行一用一組可應用解析參數來加以參數化的名稱解析處理。然而，吾人應了解到，該處理僅為說明可實現之名稱解析處理之類型，同時任何適合處理可根據任何適合的名稱解析科技及協定來實現。吾人亦應了解到在處理500以特定解析參數之角度來描述的同時，這些參數亦只為示範性，同時任何適合參數可根據在此所述之原理來使用。

第5圖之處理500，開始於方塊502，其中該解析模組可建立對一名稱解析資源的連結，該名稱解析資源係由該組可應用解析參數來識別，像是由“DNS server(s)”參數。視名稱解析科技及協定所實作的類型而定，可隨之改變解析資源的本質。然而，在某些實作中，該名稱解析科技可為一網路資源，像是一DNS伺服器。在方塊504中，根據被設定為開啟/真的“DNS over IPsec”參數，可保全對該解析資源之連結。該連結之安全性可視其他參數而定，像是識別加密類型來使用之“Encryption Level”

[S]

參數，及/或識別一或更多可發出能鑑定出該解析資源之身分之憑證的憑證管理的“IPsec CA”參數。使用 IPsec 協定來保全通訊連結的技術在該領域中是已知的，而如此一來將不會在此做進一步的討論。

在方塊 506 中，一旦對解析資源之連結被保全，則該解析模組可透過該通道而與一名稱解析請求進行通訊。該解析請求可包括能用於執行一名稱解析之任何適合資料，包括第一識別符以及能指示一處理之任何參數，該指示係關於要該處理需要去注意該解析資源。例如，根據該組可應用解析參數中的一參數，該解析請求可指示，DNSSEC 已為了該解析請求而被啟用，且該解析資源應根據 DNSSEC 而在回傳該第二識別符之前在第二識別符上執行一認證處理。例如，該解析請求可包括用於一或更多憑證管理之一或更多指示符，其中該組解析參數指示是受信任的以用於回傳授信任結果，而該解析資源可確認其中之一已經被使用。

根據由解析參數所選及所指示的特定名稱解析科技，任何適合技術可由該解析資源來實行，以獲得用於一網路資源之第二識別符。例如，若該解析資源為 DNS 伺服器，則該解析資源可審視識別符的本地快取，以判斷其是否「知道」在該解析請求中接收並對應到第一識別符的第二識別符。若第二識別符並不在其快取上，則其可沿著另一 DNS 伺服器來傳遞該解析請求，該另一伺服器則接著可實行相同處理。這將會持續直到原本的解析資

[S]

源接收到包括第二識別符的回應為止。若 DNSSEC 是被該組可應用解析參數指示成為「開啟」，則當解析參數獲得一結果時－不是來自其本身快取就是來自另一 DNS 伺服器－則該解析資源可審視該結果，以判斷其是否已經被一值得信任的來源所「簽名」，該值得信任的來源可擔保該結果的正確性。若判斷該結果是可靠的，則可姜琦回傳到發出該解析請求之解析模組。

在方塊 508 中，該解析模組透過安全通道而自該解析資源處接收回應，以及在方塊 510 中，確認第二識別符曾由該解析資源所認證並由一受信任憑證管理所簽名。在方塊 512 中，根據方塊 510 的判斷，該解析模組判斷該識別符是否曾根據該組可應用解析參數來認證。若曾認證該第二識別符，則在方塊 514 中會將該第二識別符回傳到該功能性模組然後該處理結束，其中該功能性模組原本是藉由提供該第一識別符(如第 3 圖之方塊 302)而發出該請求。在另一方面，如果不曾根據該組可應用解析參數來認證該回應，則在方塊 516 中該解析模組會將結果暴露出來並將一表示沒有找到結果之錯誤訊息回傳到該功能性模組，然後該處理結束。

在某些實作中，一解析模組亦可維持用於網路資源之識別符之本地快取。該解析模組在接收含有第二識別符之解析請求的回應之後，可將該第一識別符、該第二識別符、以及用於獲得該第二識別符之解析參數儲存於一快取中。然後，當該解析模組接收用於第二識別符的新

[S]

請求時，該解析模組可審視該快取，以判斷其是否已經儲存該第二識別符，而若是如此，則可從該快取處回傳第二識別符而無需發出對一解析資源的解析請求。第 6 圖顯示一示範性處理 600，其使用快取來執行此一解析處理。然而，吾人應了解到，該處理 600 僅做為說明，且可根據在此所述原理來實現任何適合的技術。

該處理 600 開始於方塊 602，其中該解析模組接收第一識別符並判斷一組可應用解析參數。此可按任何適合方式來完成，包括任何上述的示範性技術。在方塊 604，該解析模組可審視快取以判斷該第一識別符是否列於該快取中。依據方塊 606 的抉擇，若該第一識別符不在快取中，則在方塊 608 中該名稱解析處理會如上討論般的繼續進行。當第二識別符由該名稱解析處理所獲得時，在方塊 610 中，於獲得步驟中所描述之資訊可儲存在快取中。此資訊可包含在獲得處理上之各種類型的資料及指令中的任一者。例如，該資訊可包含第一識別符、第二識別符、及/或用於獲得步驟中之該組可應用解析參數。一旦將資訊儲存於快取中，則該處理 600 結束。

在另一方面，若在方塊 606 中判斷第一識別符是在該快取中，則在方塊 612 中與第一識別符一起儲存於快取中之解析參數會被擷取並與該組在方塊 602 中所擷取的可應用解析參數相比較。可靠著執行該比較過程來確保從快取處回傳之任何第二識別符是一曾根據該組可應用解析參數來獲得的識別符。例如，方塊 612 之比較過程

[S]

可判斷該參數是相等的，或是用於獲得儲存在快取中之識別符是至少與在方塊 602 中所擷取的參數一樣地安全。替代地，方塊 612 之比較過程可判斷在快取中第二識別符之來源－曾從該第二識別符處獲得之解析資源－是與該組可應用解析參數所獲得之來源相同。如另一範例般，該快取反而可儲存該第二識別符曾經擷取的時間，而該解析模組可將該時間與該解析參數曾編輯的最後時間做比較，以判斷在運行時之解析參數是否與擷取了快取中之識別符時的解析參數相同。任何適合的比較處理可在方塊 612 中實行。

在方塊 614 中，若該等參數並未匹配，則如上討論搬根據該組可應用解析參數來實行一名稱解析處理，以確保能夠適當地獲得任何該獲得的識別符。然而，若在方塊 614 中，確定了該參數是相匹配的，則在方塊 616 中將第二識別符從快取處回傳到提供該第一識別符的功能性模組，然後處理 600 結束。

上述內容為用於根據由一功能性模組輸入到一解析模組之第一識別符來判斷第二識別符的若干不同技術。然而，吾人應了解到，這些技術各者僅為說明可根據在此所述原理來實現之技術的類型。可實現任何類型的方法來實行一名稱解析處理，以依據名稱解析科技（無論其是實作成硬體網路或是實作成疊蓋網路），或是依據已經為解析模組做準備的解析參數，來判斷用於網路資源的識別符。

[S]

針對解析模組做準備的解析參數可按任何適合的方式來做準備。例如，在一實作中，可於本地端由一計算裝置之使用者來輸入解析參數，並將其儲存到與該計算裝置相關連的資料儲庫中。在另一實作中，當該計算裝置與網路連接時，可透過網路來提供該等解析參數。第 7 圖顯示此一較後面處理之範例，其用於將解析參數經優網路提供給一計算裝置。然而，吾人應了解到，第 7 圖之處理 700 僅為說明性，而其他處理方式亦是有可能的。進一步而言，吾人應了解到第 7 圖之範例是按微軟視窗電腦網路的觀點來描述，而在計算裝置連接到網路之時透過網路來設置這些計算裝置的其他種網路亦是有可能的。

該處理 700 開始於方塊 702，其中一管理者將解析參數之集合輸入到該網路之網域控制器。此解析參數之集合可按任何方式來輸入，包括作為用於網路之微軟目錄服務群組政策(Microsoft Active Directory Group Policy)的一部分。該群組政策可應用到網路的任何部分，包括連接到網路之計算裝置之群組及/或網路使用者之群組。在方塊 704 中，該網域控制器接收該等解析參數並姜琦儲存成一群組政策，然後將該群組政策傳輸到該群組中之所有成員。方塊 704 的傳輸可在一設定時間週期之後來實行，像是每隔 15 分鐘，或是當該群組成員（電腦亦或是使用者）加入或簽名至該網路。在方塊 706，如此處所述般運行一解析模組之計算裝置能按任何適合

[S]

當是來接收該群組政策，並將其儲存在一關連於該計算裝置的資料儲庫中。然後，在方塊 708 中，當運行一名稱解析處理時，該解析模組會按任何適合當是將解析模組之集合應用到該名稱解析處理，包括上述之任何示範性技術。

任何適合的使用者介面可被用來輸入解析參數。舉例而言，在某些實作中，一文字式命令行工具可被用來輸入解析參數。在某些實作中，一圖形式使用者介面可被用來輸入解析參數。第 8 圖顯示此一圖像是使用者介面的範例，其可根據在此所述之某些原理來使用。然而，吾人應了解到，某些實作可使用替代的使用者介面，同時並未將本發明之具體實施例限制在只能使用任何用於解析參數之特定輸入技術。

圖像式使用者介面 800 包含一定數目的控制碼，其可被用來輸入解析參數。一文字方塊 802 可被用來輸入一網路資源之名稱，包括用來與網路資源名稱相匹配之圖樣，像是上述關於第 2A 及 2B 圖之「名稱」參數。該圖像式使用者介面亦可包含一文字方塊 804，以輸入相關於一憑證管理的資訊，其中可根據安全名稱解析科技（像是 DNSSEC）而針對一 IPsec 安全性處理及/或針對簽名識別符來使用該憑證管理。亦可實作相關於 DNS 安全的一系列控制碼 806，其中控制碼指示以下參數，像是：是否需要 DNSSEC 認證、是否使用 IPsec、以及若正準備使用 IPsec 應使用哪種類型的加密。另一系列的控制碼

[S]

808 亦可被實作以用在疊蓋網路上，像是直接存取，其能接收以下參數，像是用於可接收解析資源(像是 DNS 伺服器)之識別符的、用於一代理伺服器之識別符、是否使用 IPsec、以及若正準備實現 IPsec 則應使用哪種類型的加密。該圖像式使用者介面 800 亦包含用於建立及更新一組解析參數的按鈕 810，該組解析參數包括在各個控制碼 802-805 中所輸入的參數。其他方面，全域解析參數亦可經由一訊框 812 而被輸入至圖像介面。一旦已經建立起一組解析參數，則可在一訊框 814 中於該圖像式使用者介面 800 之底部顯示該組解析參數，該圖像式使用者介面 800 具有複數個與參數類型對準的欄，其可使用介面 800 來輸入。

當使用該圖像式使用者介面 800 來建立或更新一組參數時，該組參數可按任何適合的格式被儲存在任何適合的資料結構中。該資料結構可被儲存在一儲存多組解析參數之集合(像是。第 2A 及 2B 圖之集合 200A 及 200B)的資料結構中。如上所討論之這些資料結構，可在任何適合的電腦儲存媒體上編碼。據此，當一使用者使用該圖像式使用者介面 800 來輸入參數時，該圖像式使用者介面 800 可起始一記錄處理，以用任何適合方式將輸入參數記錄到一電腦可讀取媒體上。

根據在此所述之某些或全部原理所運作的技術可用任何適合方式來實現。例如，在某些具體實施例中，可將該等技術實現成在一或更多電腦可讀取儲存媒介上所編

[S]

碼之電腦可運行指令，像是磁性媒介(例如，硬碟)、一壓縮光碟(CD)、一數位多功能光碟(DVD)、一持續性或非持續性之固態記憶體(例如，快閃記憶體、磁性 RAM 等等)、或是任何其他適合的儲存媒介。該電腦儲存媒介可被實作成第 9 圖之電腦可讀取儲存媒介 906（亦即，作為計算裝置 900 的一部分），或是作為個別的電腦儲存媒體。如此處所使用般，吾人應了解到「電腦可讀取媒體」，包括「電腦可讀取儲存媒體」，可視為具有至少一實體結構的有形儲存媒體，其可在於其上進行記錄資料處理期間以某些方式來加以變更。例如，電腦可讀取媒體之實體結構中一部分的磁性狀態可在一記錄處理過程期間變更。

在某些此類的具體實施例中，能將根據在此所述原理所運作之技術加以實現的電腦可運行指令，可實現成一或更多的獨立功能性模組（例如，上述之解析模組）。如上所述，「功能性模組」是能扮演一特定運作角色的系統之結構性組件，然而作為示例，其可為軟體元件的一部分或整體（例如 一函數或一分散處理）。通常而言，功能性模組包括常式、程式、物件、組件、資料結構等，其執行特定任務或實現特定的抽象資料類型。典型地，該功能性模組的功能性可按不同具體實施例的需求而結合或分散。在某些具體實施例中，這些功能性模組可適用於與其他未相關之功能性模組及/或處理互動，像是實現軟體應用程式或實現用於計算裝置之作業系統的功能

[S]

性模組，或是在其他實作中，該等模組可適用於與其他功能性模組互動，其連同該等模組一起形成一整體系統，像是一作業系統，例如來自 Redmond, Washington 之微軟股份有限公司的微軟作業系統(亦即 可將功能性模組實作成作業系統的一部分或是實作於作業系統之外）。吾人亦應了解到，在某些實作中，可分別地從其他模組處來實現某些功能性模組，或者可不實現某些功能模組。

在某些但非全部的的實作中，可將該等技術具體實施成電腦可運行指令，其可在任何適合計算裝置上運行，該等計算裝置運行於任何適合的電腦系統中，包括第 1 圖中所示之示範性電腦系統。舉例而言，根據在此所述之某些或全部原理所運作的技術，可在以下系統上運作：單個多用途可程式數位電腦設備、在二或更多個多用途電腦設備（其共享處理功率並共同實行在此所述之技術）中的座標系統、專用於運行在此所述技術之單個電腦設備或電腦設備的座標系統（共同定位地或是在地理上分散地）、用於實現在此所述技術之一或更多的特殊應用積體電路（ASIC）、用於實現在此所述技術之一或更多的場效可程式閘陣列(FPGA)，或其他適合的系統。

第 9 圖說明一計算裝置之示範性實作，該計算裝置是以可在實現此處所述技術之系統中使用的計算裝置 900 的形式表現，而其他形式也是可能的。進一步而言，吾人應了解到第 9 圖沒有意圖描述根據在此所述原理而運

[S]

作之計算裝置的必要組件，亦無意圖做廣泛性的描述。

計算裝置 900 可包含一處理器 902、一網路配接器 904、及電腦可讀取儲存媒介 906。例如，計算裝置 900 可為桌上型或膝上型個人電腦、工作站、伺服器、大型電腦、智慧型手機、或任何其他適合的計算裝置。網路配接器 904 可為任何適合的硬體及/或軟體，以讓計算裝置 900 能夠與任何其他適合的計算裝置透過任何適合的計算網路進行通訊。該計算網路可為任何適合的有線/無線通訊媒體或媒介，以用於在二或更多的電腦之間交換資料，包括網際網路。在某些實作中，網路配接器 904 可實作成二或更多之個別網路配接器，經由二或更多之網路介面類型來提供連接性（例如，一有線網路配接器，像是一 Ethernet 配接器以及一無線網路配接器，像是 IEEE802.11g 配接器）。電腦可讀取儲存媒介 906 可為任何適合的有形儲存媒體，其適於儲存準備被處理之資料及/或準備由處理器 902 所運行之指令。處理器 902 能啟動資料的處理及指令的運行。可將資料及指令儲存在電腦可讀取儲存媒介 906 上，且可，例如，啟動在計算裝置 900 間組件的通訊。

儲存在電腦可讀取儲存媒介 906 上的資料及指令，可包含電腦可運行指令，該等指令能實現根據在此所述原理來運作之技術。在第 9 圖之範例中，電腦可讀取儲存媒介 906 儲存了如上所述般實現各種模組並儲存各種資訊之電腦可運行指令。電腦可讀取儲存媒介 906 儲存了

[S]

相關於一或更多應用程式 908 的資料及指令，該應用程式 908 可在計算裝置上運行。這些應用程式可包括那些能接受網路資源之第一識別符的應用程式，並尋找以獲得用於網路資源之第二識別符。該電腦可讀取儲存媒介 906 亦包括名稱解析模組 910，其係根據任何適合技術而基於第一識別符，來判斷用於網路資源之第二識別符，任何適合技術包括任何上述之示範性技術。電腦可讀取儲存媒介 906 亦包含多組解析參數之集合 912。如上所討論，此集合可按任何適合的方式而被組織並格式化，且該等解析參數可包括能用於支配名稱解析模組 910 之名稱解析處理之執行的任何適合參數。舉例而言，在一實作中，該集合 912 可被實作在電腦可讀取儲存媒介 906 上，以作為微軟視窗作業系統之註冊機(Registry)的一部分。電腦可讀取儲存媒介 906 可額外地包含識別符之快取 914，其已由名稱解析模組 910 所擷取。該快取可按任何適合的方式來組織且可獲得任何適合類型的資訊，包括多組用於網路資源之第一及第二識別符、多組用於獲得識別符之解析參數、曾獲得識別符之次數、及/或任何其他類型的資訊。

最後，在第 9 圖之範例中，電腦可讀取儲存媒介 906 可包含一組應用可程式介面(API)函數以影響多組解析參數之集合，並判斷該集合之內容。舉例而言，該 API 可實現一 GetProxyInfo 函數來判斷一可被用來接觸特定網路資源的代理伺服器，並將用於網路資源之一識別

[S]

符作為輸入。該 GetProxyInfo 函數可使用該用於資源之輸入識別符，以定位在集合中一組或多組能應用至網路資源之解析參數，然後若任何一組解析參數指示了一代理伺服器正待被使用，則可回傳用於代理伺服器之識別符。一 GetPolicyTableInfo API 函數亦可被實現以回傳一集合（亦即 該組解析參數）之內容。另外，一 GetEffectivePolicy API 函數可回傳在該集合中之某些（或全部）的多組解析參數，其取決於不能應用於該給定環境之參數而定。例如，若某些組解析參數應用到特定網路，且該計算裝置 900 未連接到該網路，則那些組參數不可被當做 GetEffectivePolicy 函數之輸出的一部分來回傳。額外地，可實現能將第一識別符當做輸入並運行由多組解析參數之集合所支配的名稱解析處理的 GetAddrInfo 或 DnsQuery 函數以判斷一第二識別符，並回傳該第二識別符。吾人應了解到這些 API 函數僅是示範可實現之 API 函數的類型，同時本發明之具體實施例並未受限於此。

能實現根據在此所述原理所運作之技術的模組可用任何適合方式來互動。

在第 10 圖之範例中，一應用程式 1000 能與一連結模組 1002 及一名稱解析模組 1004 其中之一者或兩者互動，以判斷對應到第一識別符之第二識別符。例如，該應用程式 1000 可直接地查詢名稱解析模組 1004，或者該應用程式 1000 可使用該連接模組 1002 來嘗試開啟一

[S]

對網路資源之連結，而該連結模組可請求一來自名稱解析模組之第二識別符，以用來開啟該連結。該名稱解析模組 1004，在嘗試獲得第二識別符時，可使用如上所討論之多組解析參數之集合 1006，且可進一步使用如上所討論之識別符之快取 1008。最後，在使用解析參數之集合 1006 以獲得第二識別符時，名稱解析模組 1004 亦可使用各式的連結科技 1010，包括一連結模組 1012，其用來開啟對解析資源之連結，並包括鑑定及/或加密模組 1014 及 1016，其用來執行可由在集合中之解析參數所指定的任何安全處理。

茲已描述了此發明之至少一具體實施例之若干態樣，吾人應了解到各種變更、修改、及增進將會很快地由在該領域中熟悉技術人士來實現。

此類的變更、修改、及增進意圖作為此揭示的一部分，且意圖含括在本發明之精神與範疇內。因此，先前的描述及圖式僅僅作為範例使用。

本發明之各種態樣可被單獨使用、合併使用、或用各種未在先前具體實施例中具體討論的配置方式來使用，且因此不限於其詳細應用方式，以及在先前描述中所述或是在圖式中所繪示之組件配置。例如，在一具體實施例中所述之態樣可用其他具體實施例中所描述之態樣以任何方式來結合。

同樣地，本發明可被具體實施成一種提供了範例的方法。作為方法中之一部分所執行的步驟可按任何適合的

[S]

方式來排序。因此，可用不同於發明中所述之順序來執行步驟進而構成具體實施例，而這順序包括同時地執行某些步驟，即使在具體實施例中其顯示為循序執行的步驟。

在申請專利範圍中使用順序詞彙，像是「第一」、「第二」、「第三」等等，來修改一請求項元件，其本身並未暗示著一請求項元件的優先順序高於另一者，或是暗示其為執行方法步驟之時間順序，而是僅用作為標記以將一具有特定名稱的請求項元件與另一具有相同名稱之元件加以區別(但是作為順序詞彙來使用)，以分辨該等請求項元件。

同樣地，在此所用之片語及詞彙方式是作為描述性使用而不應被視為限制。「包括」、「包含」、「具有」、「含有」「涉及」以及在此提及之其他變化型的使用，是意味著含括了之後所列之項目以及其均等物還有額外的項目。

【圖式簡單說明】

隨附的圖式並未意圖按等比例繪製。在圖式中，被繪示在許多圖式中之各個相同或近乎相同的組件係以一相似編號來表示。為了清楚起見，並非每個組件會在每個圖式中加以標示。在以下圖式中；

第 1 圖說明一示範性電腦系統，根據某些在此所述原理所運作之技術可運作於其中；

第 2A 及 2B 圖說明一示範性解析參數之表格，其可根據某些在此所述原理來實現；

第 3 圖是用於執行一名稱解析之示範性處理之流程圖，其可根據某些在此所述原理來實現；

第 4 圖是用於識別一組可應用解析參數之示範性處理之流程圖，其可根據某些在此所述原理來實現；

第 5 圖是用於將一文字識別符解析成一數字識別符之示範性處理之流程圖，其可根據某些在此所述原理來實現；

第 6 圖是用於判斷一儲存在快取中之識別符是否可當成一名稱解析處理的結果來回傳之示範性處理之流程圖，其可根據某些在此所述原理來實現；

第 7 圖是用於建立一組解析參數之示範性處理之流程圖，其可根據某些在此所述原理來實現；

第 8 圖說明一示範性使用者介面，可將解析參數輸入於其中；

第 9 圖是一示範性計算裝置之組件的方塊圖，其可實現根據某些在此所述原理所運作之技術；

第 10 圖是模組間相互可運作性之示範性方法的方塊圖，其可根據一或更多之技術來實現，而該等技術係根據在此所述原理來運作。

【主要元件符號說明】

100 通訊網路

100A 疊蓋網路

102 使用者之裝置

104 解析參數

106 管理者之裝置

108 網路資源

110 名稱解析資源

110A 名稱解析資源

112 代理伺服器

900 計算裝置

902 處理器

904 網路配接器

906 電腦可讀取儲存媒介

908 應用程式

910 名稱解析客戶端

912 多組解析參數之集合

914 識別符之快取

916 API

1000 應用程式

1002 連結模組

1004 名稱解析模組

1006 資源參數之集合

1008 識別符快取

1010 連結科技

[S]

1012 連結模組

1014 鑑定模組

1016 加密模組

七、申請專利範圍：

1. 一種用於實施名稱解析之方法，其包含以下步驟：

(A)將用於一網路資源之一第一識別符接受做為一輸入；

(B)諮詢多組解析參數之一集合以判斷應用到該第一識別符的一組可應用解析參數，該組可應用解析參數支配與一遠端計算裝置的通訊；及

(C)獲得來自該遠端計算裝置的用於該網路資源之一第二識別符，該獲得步驟包含導入一名稱解析處理，以基於該第一識別符來判斷用於該網路資源之該第二識別符，其中該名稱解析處理是由該組可應用解析參數所支配。

2. 如申請專利範圍第 1 項所述之方法，其中該獲得步驟進一步包含：

(C1) 根據該組可應用解析參數將一名稱解析請求傳輸到該遠端計算裝置。

3. 如申請專利範圍第 1 項所述之方法，其中諮詢多組解析參數之該集合的步驟包含：

(B1) 將該網路資源之該第一識別符與關連於該等多組解析參數之每一者的圖樣進行比較，以判斷是否各組解析參數應用到該第一識別符。

4. 如申請專利範圍第1項所述之方法，其中該第一識別符是用於該網路資源之一文字識別符，而該第二識別符是用於該網路資源之一數字識別符。

5. 如申請專利範圍第1項所述之方法，其中該等解析參數包含在要使用的一或更多個加密類型上的資訊。

6. 如申請專利範圍第1項所述之方法，其中該等解析參數包含用於在該名稱解析處理期間要交換資訊之一或更多個網路資源之識別符。

7. 如申請專利範圍第1項所述之方法，其中該名稱解析處理是根據網域名稱系統(DNS)協定之一處理。

8. 如申請專利範圍第7項所述之方法，其中該名稱解析處理是根據DNS安全延伸(DNSSEC)之一處理。

9. 如申請專利範圍第7項所述之方法，其中該名稱解析處理係適用於與使用直接存取來實現之一疊蓋網路共同作用。

10. 一種用電腦可執行指令來編碼的電腦可讀取儲存媒體，當其執行時，會使得一電腦能執行一方法，該方法

包含以下步驟：

(A)將用於通過一網路可存取的一網路資源之一網域名稱接受做為來自一應用程式的輸入；

(B) 判斷來自多組解析參數之一集合的一組可應用解析參數；

(C) 根據該組可應用解析參數而在該網路上建立對一網域名稱服務(DNS)伺服器之一連結；

(D) 根據該組可應用解析參數來對該DNS伺服器通訊一DNS查詢；

(E) 從該DNS伺服器處接收一回應，該回應包含用於該網路資源之一數字識別符；及

(F) 對該應用程式提供該數字識別符。

11. 如申請專利範圍第 10 項所述之電腦可讀取儲存媒體，其中該建立對一DNS伺服器之一連結的步驟包含：建立對由該組可應用解析參數所識別之一DNS伺服器之一連結。

12. 如申請專利範圍第 10 項所述之電腦可讀取儲存媒體，其中該方法進一步包含：

確認出曾根據該等解析參數來產生該回應；以及

若未曾根據該等解析參數來產生該回應，則不對該應用程式提供該數字識別符。

13. 如申請專利範圍第 12 項所述之電腦可讀取儲存媒體，其中確認出曾根據該等解析參數來產生該回應之步驟包含：判斷是否曾根據該 DNS 安全延伸(DNSSEC)協定來認證該回應。

14. 如申請專利範圍第 13 項所述之電腦可讀取儲存媒體，其中根據該組可應用解析參數來對該 DNS 伺服器通訊一 DNS 查詢之步驟包含：根據由該組可應用解析參數所識別之加密技術，來對通訊進行加密。

15. 如申請專利範圍第 10 項所述之電腦可讀取儲存媒體，其中該方法進一步包含：

儲存該回應以及用於在一快取中擷取該回應之該組可應用解析參數；及

就在接收該網域名稱當做作為針對該數字識別符之一第二請求的一部分的一第二輸入後，便判斷是否用於擷取該回應之該組可應用解析參數足以對該第二請求提供該回應，且若是，則從該快取提供該回應。

16. 如申請專利範圍第 10 項所述之電腦可讀取儲存媒體，其中判斷來自多組解析參數之該集合之該組可應用解析參數的步驟包含：將該網路資源之該網域名稱與關連於該等多組解析參數之每一者之圖樣做比較，以判斷是否該組解析參數應用於該網域名稱。

17. 如申請專利範圍第 10 項所述之電腦可讀取儲存媒體，其中該步驟(F)進一步包含：

(F1)對該應用程式提供用於該網路資源之一代理伺服器之一識別符。

18. 一種用於實施名稱解析之設備，其包含：

至少一個處理器；以及

至少一個有形電腦可讀取儲存媒體，於其上編碼一資料結構，該資料結構包含相關於一組解析參數之資訊，該資料結構能按照由一名稱解析軟體組件所可使用的方法來儲存，以支配一名稱解析處理，該資料結構包含：

要記錄資訊於其中之一第一位置，其定義用於網路資源之一組一或更多個識別符，其中該等解析參數應用於該組識別符；

要記錄資訊於其中之一第二位置，其定義被實現在一通訊通道上之一安全類型，其中該名稱解析處理係透過該通道要來交換資訊；

要記錄資訊於其中之一第三位置，其定義至少一個受信任之憑證管理(certifying authority)；以及

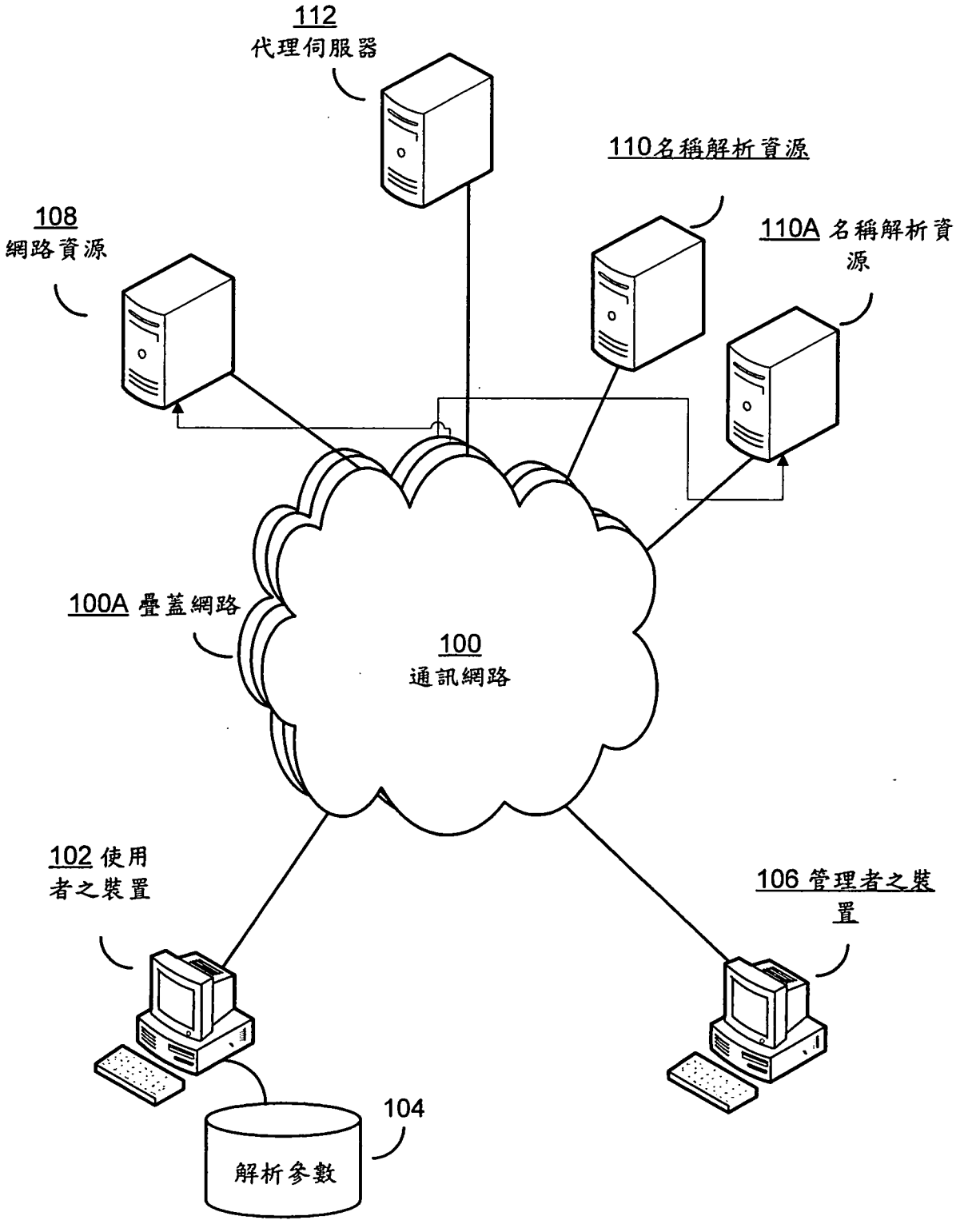
要記錄資訊於其中之一第四位置，其定義至少一個網路資源，其中要與該網路資源建立該通訊通道，

其中該至少一個有形電腦可讀取儲存媒體包含該資料結構的複數個實例(instances)，該資料結構的每一實例

係關聯於一特定組解析參數，及

其中該至少一個處理器係適用於執行該名稱解析軟體組件，該名稱解析軟體組件係適用於根據至少一組可應用解析參數來執行該名稱解析處理，該名稱解析軟體組件讀取編碼在至少一個有形電腦可讀取儲存媒體上的至少某些的複數個資料結構實例，以判斷一或更多組可應用解析參數。

19. 如申請專利範圍第 18 項所述之設備，其中該處理器係進一步適用於根據該至少一組可應用解析參數來與至少一個遠端網路資源交換資訊。


112
代理伺服器
110名稱解析資源
108
網路資源
110A 名稱解析資源
100A 疊蓋網路
100
通訊網路
102 使用者之裝置
106 管理者之裝置
104
解析參數

第1圖[S]

200A

DNSSEC

DNS協定安全

202	204	206	208	210	212
Name 文字識別符 (完整網域名稱, DNS前綴碼, DNS後綴碼, IP位址子網路)	DNSSEC 二進位－開啟或關閉	DNS over IPsec 二進位－開啟或關閉	IPsec Encryption Level 無/低/中/高，或 特定的加密協定	IPsec CA 一或更多用於加密之受信任憑證授權之文字識別符	DNS server(s) 用於一或更多可接受之DNS伺服器的識別符（數字及/或文字）
*.microsoft.com	On	On	Medium	VeriSign	ns1.microsoft.com
*.corp.contoso.com	Off	Off	-	-	ns1.corp.contoso.com

[S]

第2A圖

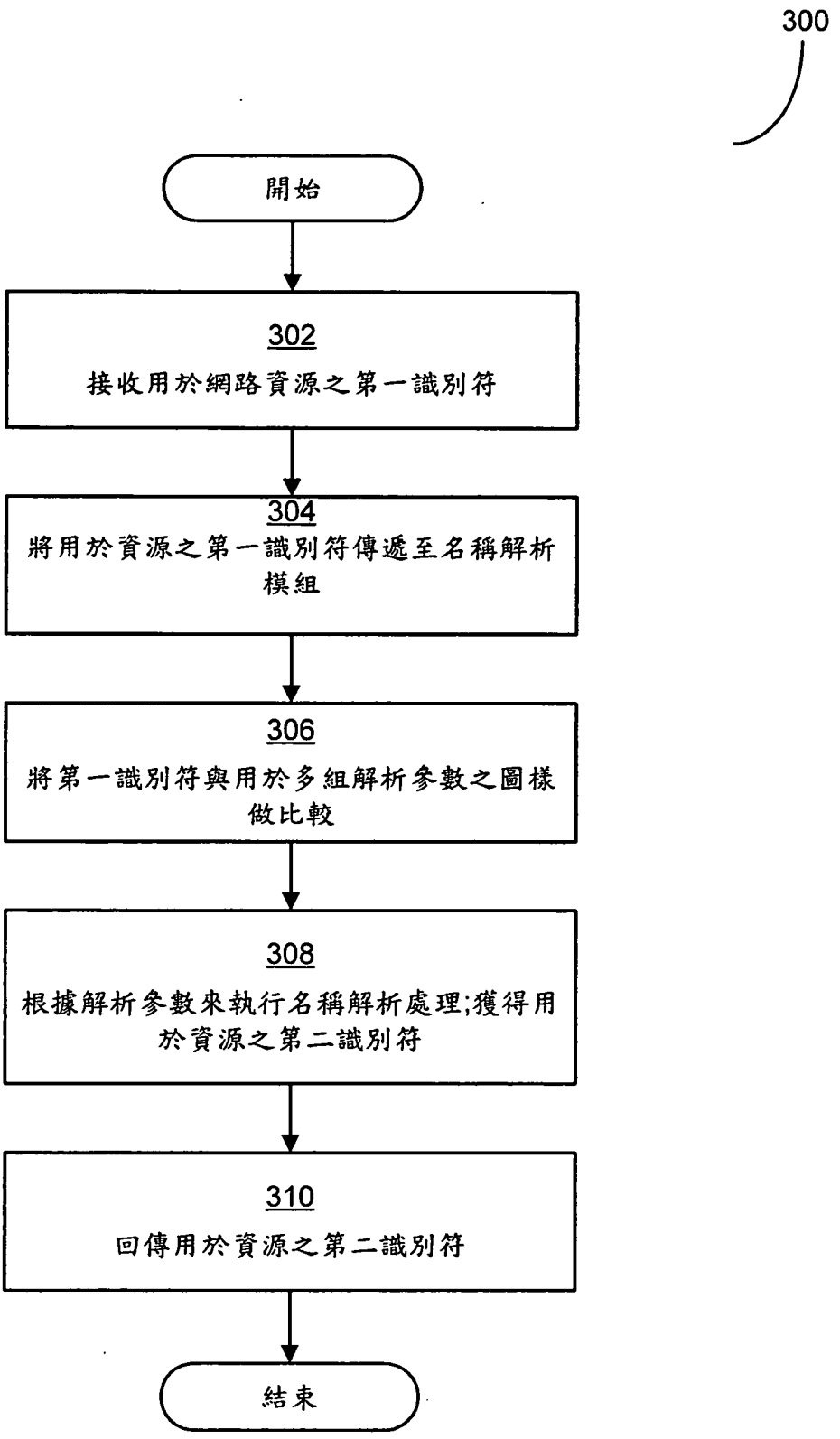
200B

直接存取

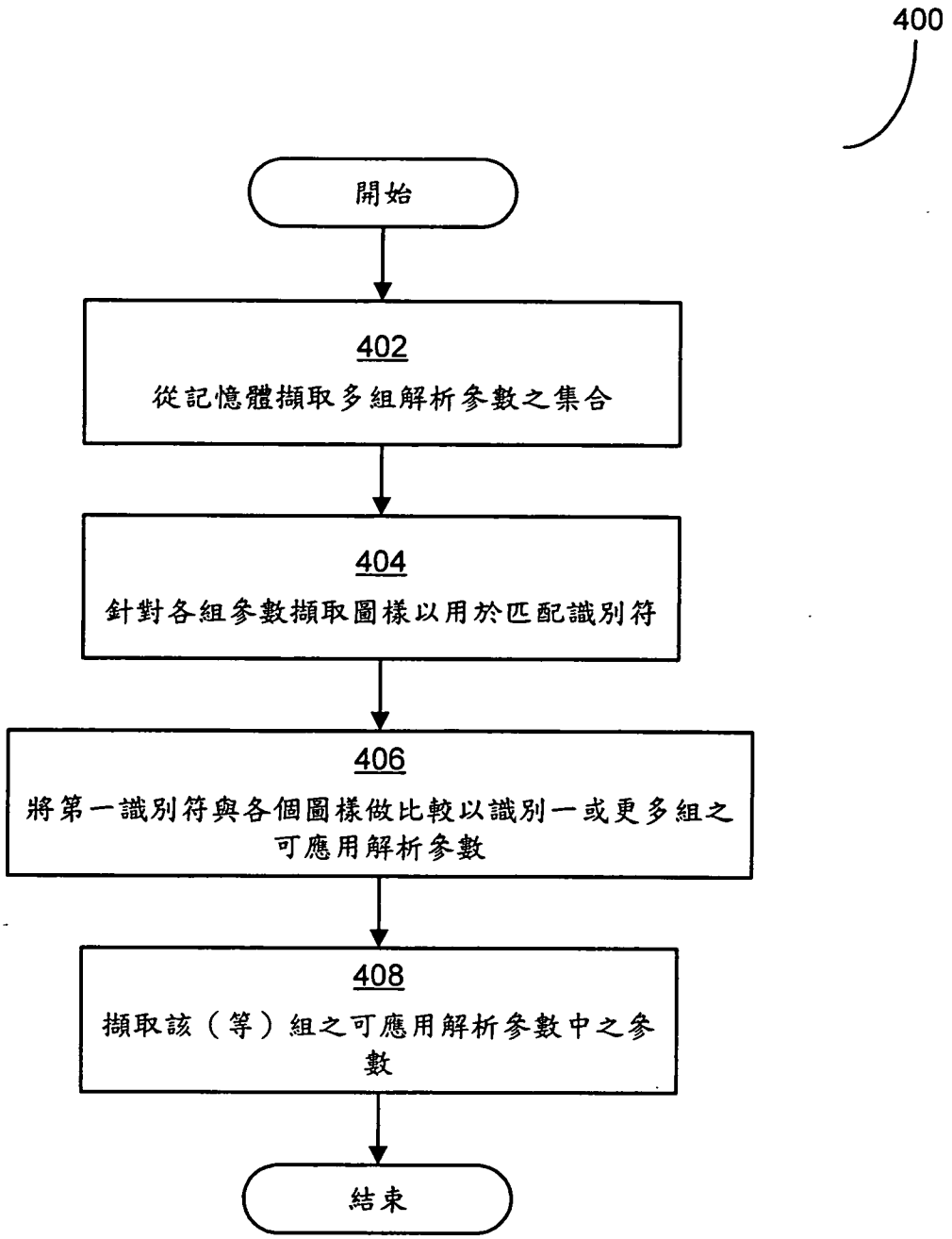
220	222	224	226	228	230
Name 文字識別符(完整網域名稱, DNS 前綴碼, DNS 後綴碼, IP位址子網路)	Zone-Specific DNS server(s) 用於一或更多可接受之 DNS伺服器的識別符（數字及/或文字）	Zone-Specific Proxy 以下其中之一: 用於代理伺服器;之識別符（數字/文字); 使用預設值; 或無	Remote DNS over IPsec 二進位－開啟或關閉	Remote DNS Encryption Level 無/低/中/高，或特定的加密協定	IPsec CA 一或更多用於加密之受信任憑證授權之文字識別符
*.microsoft.com	ns1.microsoft.com	None	On	High	VeriSign
*.corp.contoso.com	a.corp.contoso.com	prx.corp.contoso.com	Off	-	-

⋮

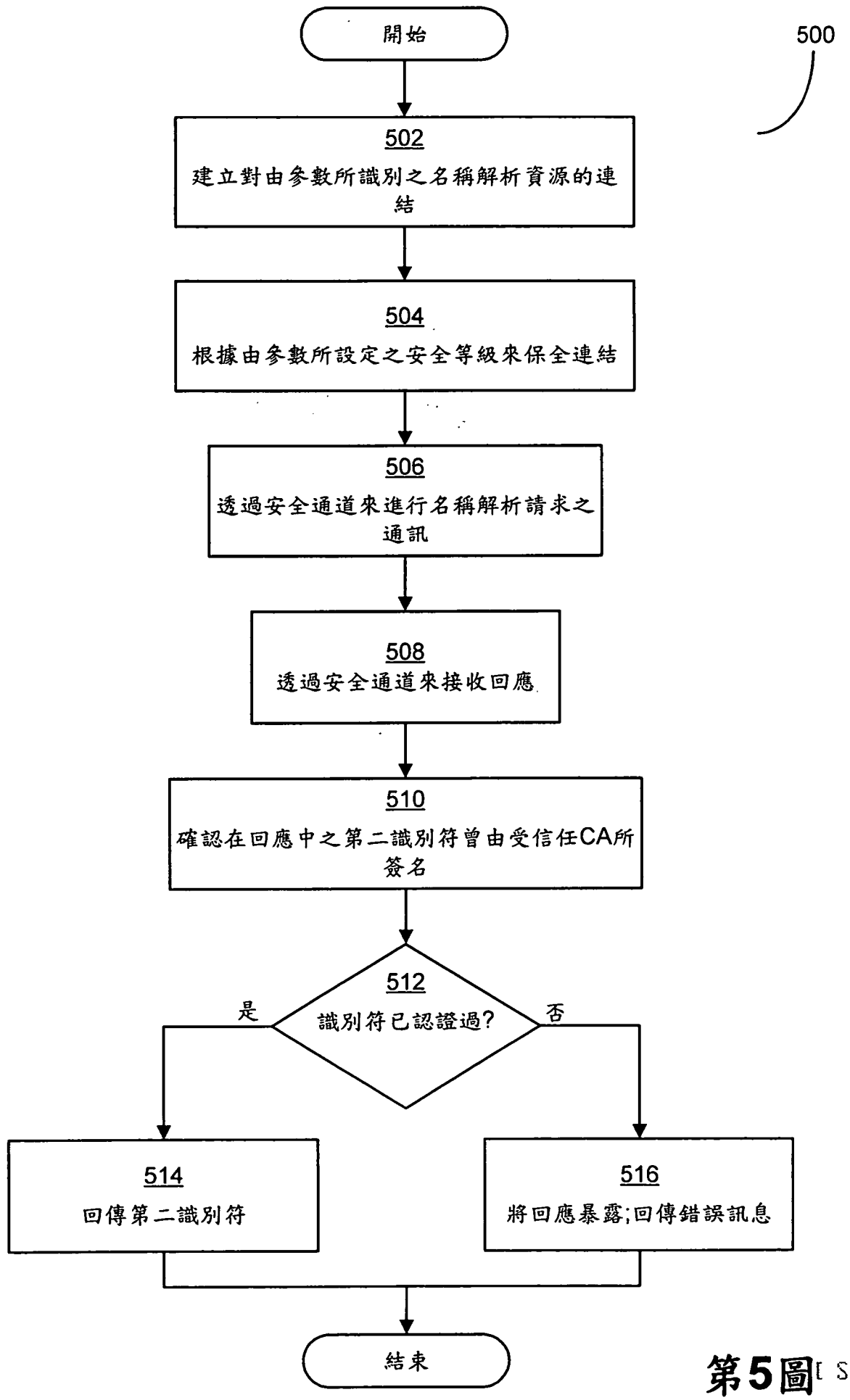
第2B圖


300
開始
302
接收用於網路資源之第一識別符
304
將用於資源之第一識別符傳遞至名稱解析模組
306
將第一識別符與用於多組解析參數之圖樣做比較
308
根據解析參數來執行名稱解析處理;獲得用於資源之第二識別符
310
回傳用於資源之第二識別符
結束

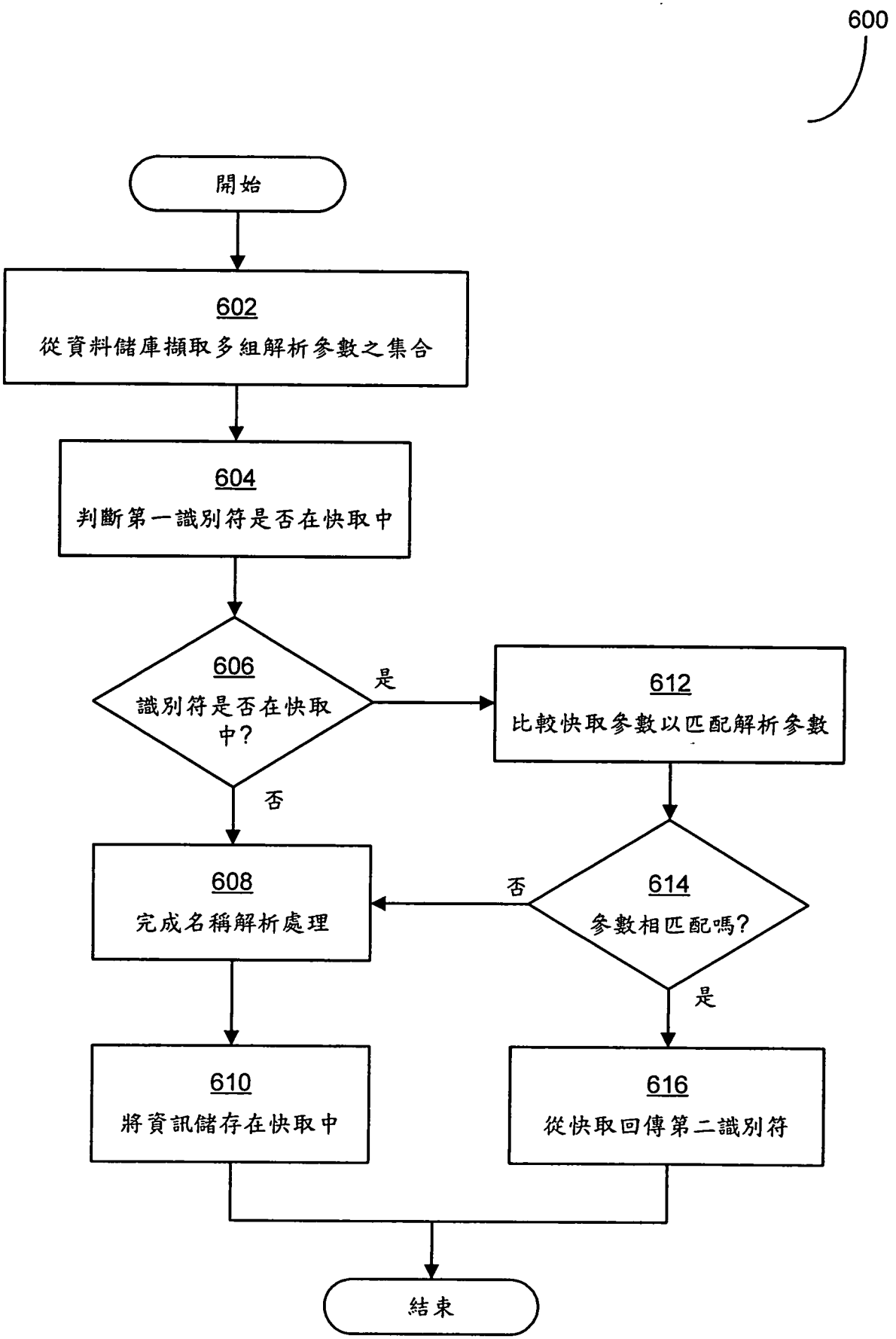
第3圖[S]


400
開始
402
從記憶體擷取多組解析參數之集合
404
針對各組參數擷取圖樣以用於匹配識別符
406
將第一識別符與各個圖樣做比較以識別一或更多組之可應用解析參數
408
擷取該（等）組之可應用解析參數中之參數
結束

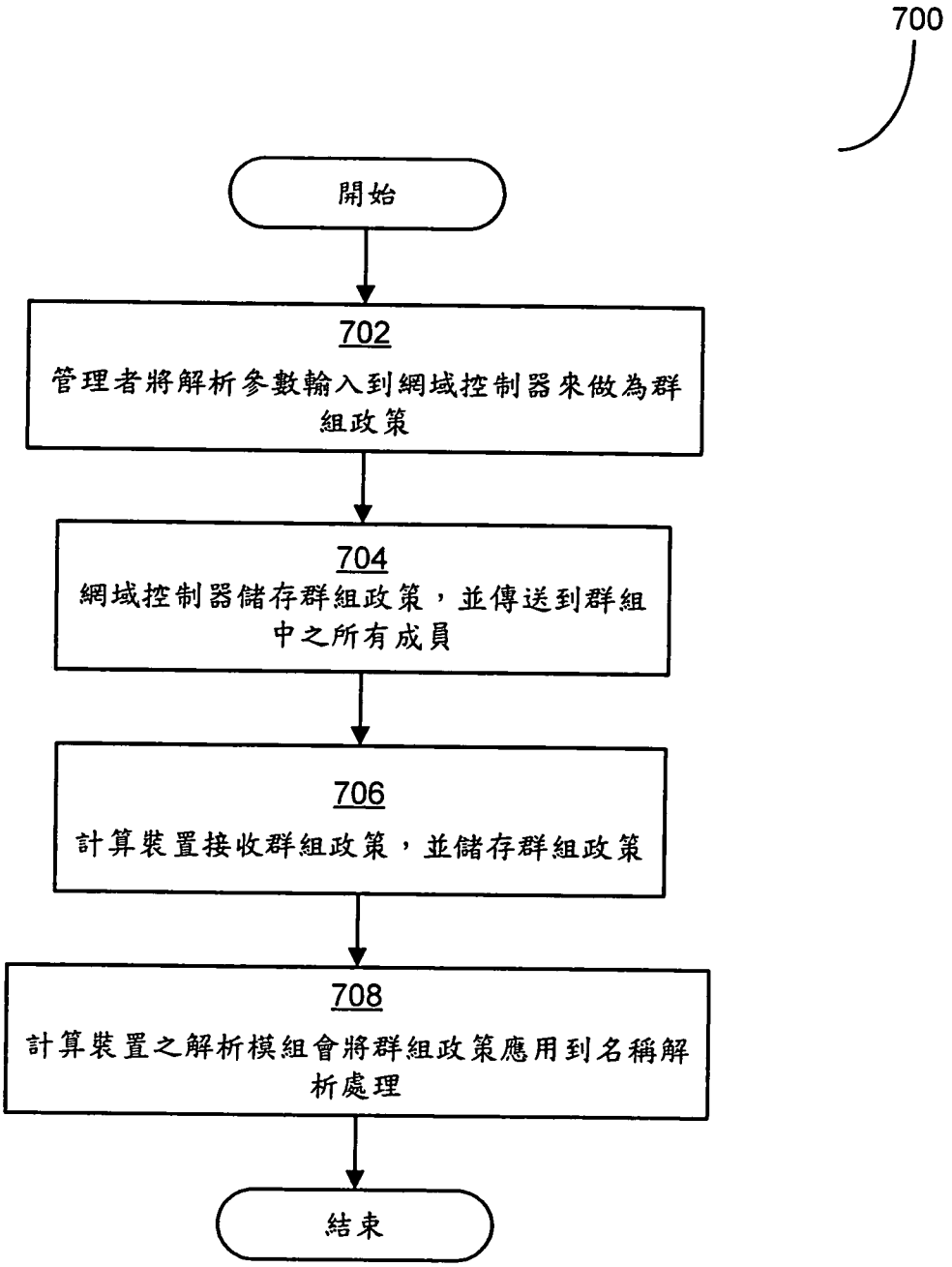
第4圖[S]


500
開始
502
建立對由參數所識別之名稱解析資源的連結
504
根據由參數所設定之安全等級來保全連結
506
透過安全通道來進行名稱解析請求之通訊
508
透過安全通道來接收回應
510
確認在回應中之第二識別符曾由受信任CA所簽名
512
識別符已認證過?
是
否
514
回傳第二識別符
516
將回應暴露;回傳錯誤訊息
結束

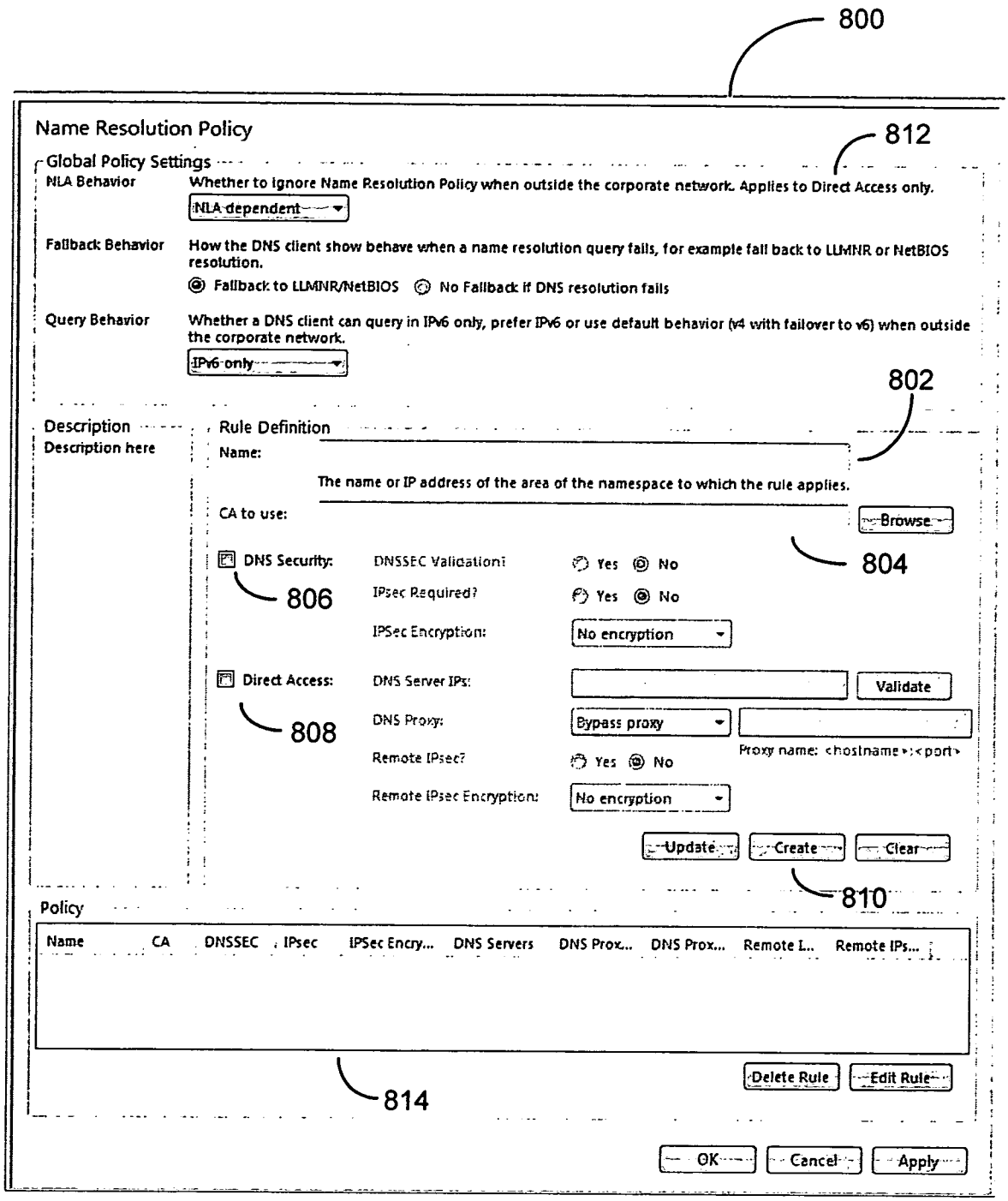
第5圖[S]


600
開始
602
從資料儲庫擷取多組解析參數之集合
604
判斷第一識別符是否在快取中
606
識別符是否在快取中?
是
否
612
比較快取參數以匹配解析參數
614
參數相匹配嗎?
否
是
608
完成名稱解析處理
610
將資訊儲存在快取中
616
從快取回傳第二識別符
結束

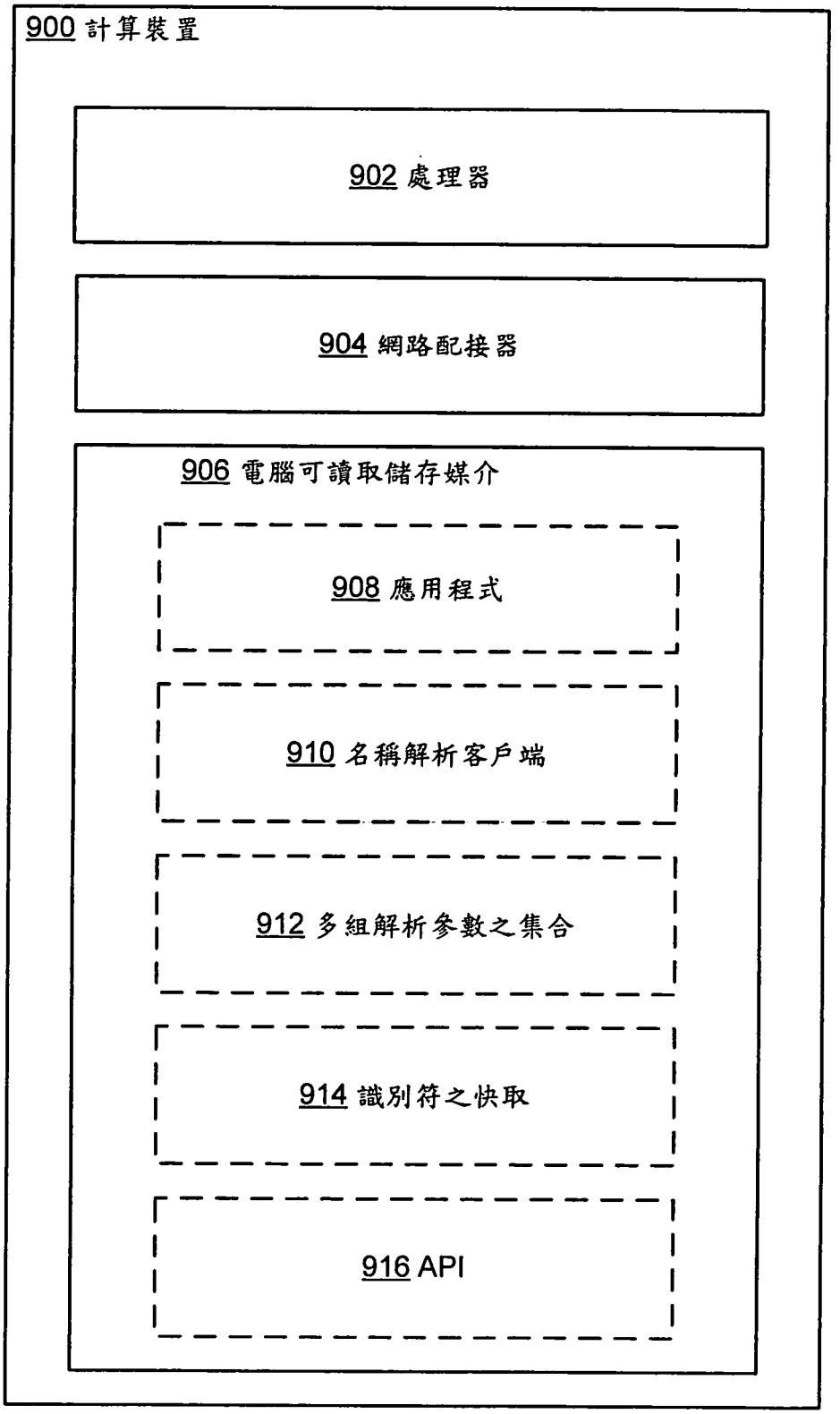
第6圖 [S]


700
開始
702
管理者將解析參數輸入到網域控制器來做為群組政策
704
網域控制器儲存群組政策，並傳送到群組中之所有成員
706
計算裝置接收群組政策，並儲存群組政策
708
計算裝置之解析模組會將群組政策應用到名稱解析處理
結束

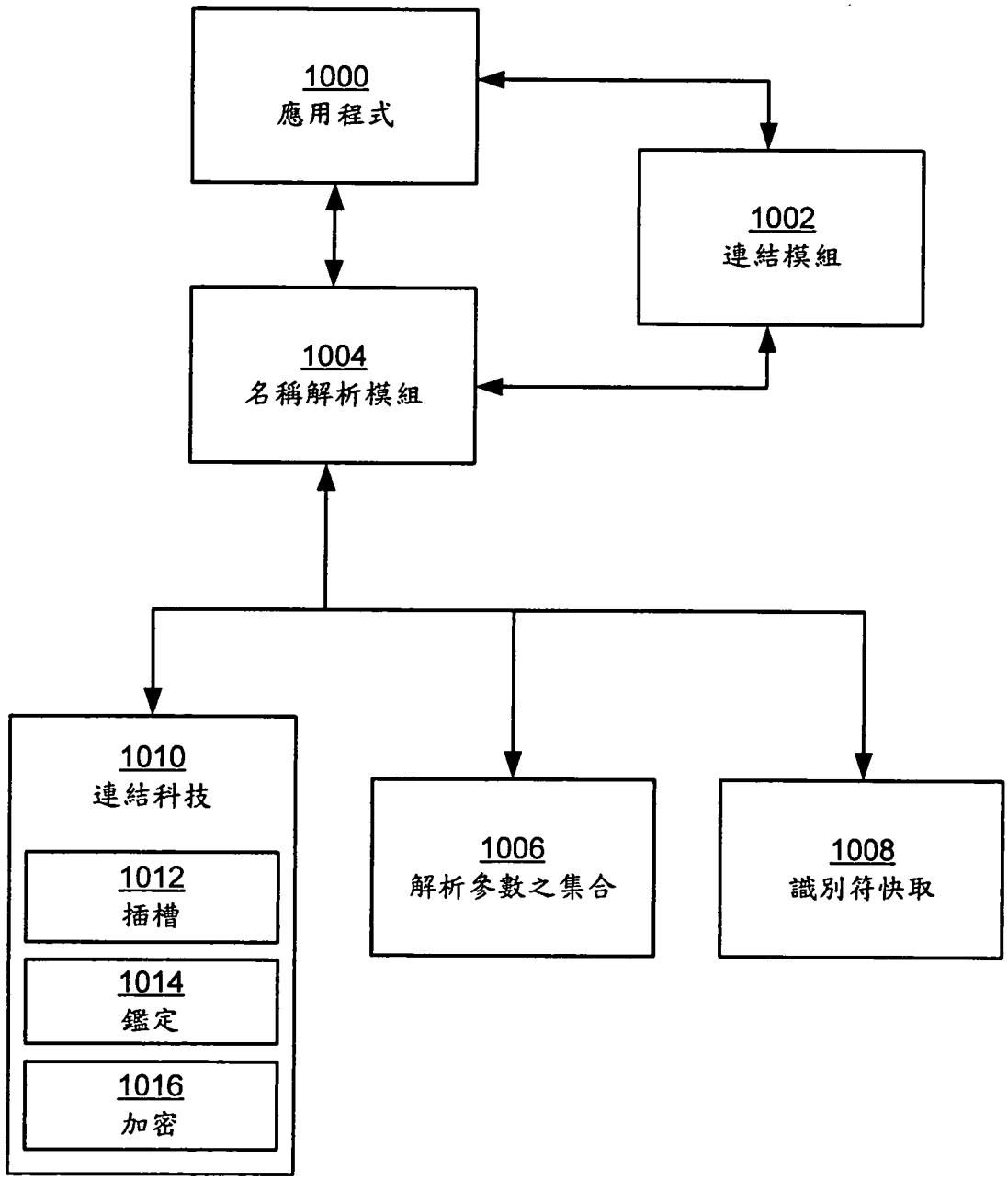
第7圖 [S]


800
Name Resolution Policy
812
Global Policy Settings
NLA Behavior
Whether to ignore Name Resolution Policy when outside the corporate network. Applies to Direct Access only.
NLA dependent
Fallback Behavior
How the DNS client show behave when a name resolution query fails, for example fall back to LLMNR or NetBIOS resolution.
Fallback to LLMNR/NetBIOS
No Fallback if DNS resolution fails
Query Behavior
Whether a DNS client can query in IPv6 only, prefer IPv6 or use default behavior (v4 with failover to v6) when outside the corporate network.
IPv6 only
802
Description
Description here
Rule Definition
Name:
The name or IP address of the area of the namespace to which the rule applies.
CA to use:
Browse
804
DNS Security:
806
DNSSEC Validation?
Yes
No
IPsec Required?
Yes
No
IPSec Encryption:
No encryption
Direct Access:
808
DNS Server IPs:
Validate
DNS Proxy:
Bypass proxy
Proxy name: <hostname>:<port>
Remote IPsec?
Yes
No
Remote IPsec Encryption:
No encryption
Update
Create
Clear
810
Policy
Name
CA
DNSSEC
IPsec
IPSec Encry...
DNS Servers
DNS Prox...
DNS Prox...
Remote I...
Remote IPs...
814
Delete Rule
Edit Rule
OK
Cancel
Apply

第8圖 [S]


900 計算裝置
902 處理器
904 網路配接器
906 電腦可讀取儲存媒介
908 應用程式
910 名稱解析客戶端
912 多組解析參數之集合
914 識別符之快取
916 API

第9圖 [S]


1000
應用程式
1002
連結模組
1004
名稱解析模組
1010
連結科技
1012
插槽
1014
鑑定
1016
加密
1006
解析參數之集合
1008
識別符快取

第10圖[S]