(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103814551 B
(45)授权公告日 2017.05.17

(21)申请号 201180073001.3

(22)申请日 2011.11.10

(65)同一申请的已公布的文献号
申请公布号 CN 103814551 A

(43)申请公布日 2014.05.21

(30)优先权数据
2011-180215 2011.08.22 JP

(85)PCT国际申请进入国家阶段日
2014.02.21

(86)PCT国际申请的申请数据
PCT/JP2011/075963 2011.11.10

(87)PCT国际申请的公布数据
WO2013/027302 JA 2013.02.28

(73)专利权人 英托株式会社
地址 日本东京都

(72)发明人 小川惠子

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 何欣亭 王忠忠

(51)Int.Cl.
H04L 12/46(2006.01)
H04L 9/14(2006.01)

(56)对比文件
CN 1604540 A,2005.04.06,
US 2011040897 A1,2011.02.17,

审查员 陈希元

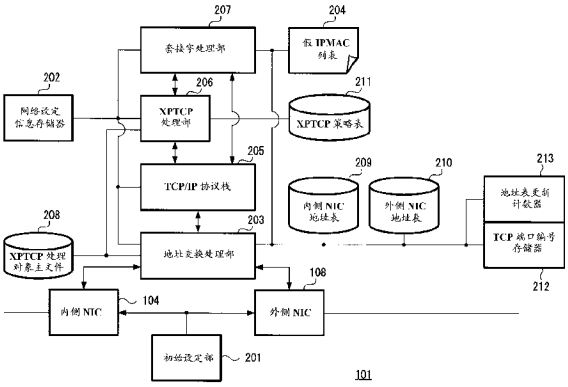
权利要求书2页 说明书28页 附图28页

(54)发明名称

网关装置

(57)摘要

为了能使TCP/IP协议栈(205)处理应该与分配给XPTCP网关装置(101)的IP地址无关的分组，预先在改写表中记录附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号。而且，附加在所接收的分组的发送源MAC地址及发送源IP地址被改写为伪MAC地址及伪IP地址，目的地MAC地址及目的地IP地址被改写为分配给XPTCP网关装置(101)的IP地址及MAC地址，然后提供给TCP/IP协议栈(205)。



CN 103814551 B

1.一种网关装置,包括:

第一NIC;

第二NIC;

初始设定部,对所述第一NIC及所述第二NIC设定混杂模式;

TCP/IP协议栈,在所述第一NIC及所述第二NIC之间进行TCP/IP通信处理;以及

地址变换处理部,将附加在从所述第一NIC接收的接收分组的发送源MAC地址变换为第一假MAC地址,将发送源IP地址变换为第一假IP地址,将目的地MAC地址变换为附加在所述第一NIC的第一NICMAC地址,将目的地IP地址变换为附加在所述第一NIC的第一NICIP地址,向所述TCP/IP协议栈发送所述接收分组,并且将附加在从所述TCP/IP协议栈接收的发送分组的发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址回写为附加在所述接收分组的所述发送源MAC地址、所述发送源IP地址、所述目的地MAC地址及所述目的地IP地址而向所述第二NIC发送。

2.根据权利要求1所述的网关装置,还包括:

地址变换表,具备存放附加在所述接收分组的所述发送源MAC地址的发送源MAC地址字段、存放附加在所述接收分组的所述发送源IP地址的发送源IP地址字段、存放附加在所述接收分组的所述目的地MAC地址的目的地MAC地址字段、记录附加在所述接收分组的所述目的地IP地址的目的地IP地址字段、和记录具有唯一性的用于索引的索引用端口编号的索引用端口编号字段,

所述地址变换处理部将附加在所述接收分组的发送源端口编号变换为记录在所述索引用端口编号字段的所述索引用端口编号,并且以附加在所述发送分组的目的地端口编号来检索所述地址变换表的所述索引用端口编号字段,确定应该回写的记录。

3.根据权利要求2所述的网关装置,还包括:

扩展TCP处理部,对从所述TCP/IP协议栈接收的接收分组的有效载荷部分施行既定加密处理,再次送回所述TCP/IP协议栈。

4.根据权利要求3所述的网关装置,还包括:

套接字处理部,具备用于对所述第一NIC形成第一TCP连接的服务器功能、和用于对所述第二NIC形成第二TCP连接的客户端功能,并且在TCP FIN分组从所述第一NIC过来时,检测TCP FIN分组从所述第二NIC过来的情况,将断开所述第一TCP连接的指示发送给所述TCP/IP协议栈。

5.根据权利要求4所述的网关装置,其中,

所述地址变换处理部在TCP SYN分组从所述第一NIC过来时,向所述地址变换表追加记录。

6.根据权利要求5所述的网关装置,其中,

所述扩展TCP处理部对从所述第一TCP连接中产生并且要到达所述套接字处理部的流数据施行所述加密处理之后,向所述第二TCP连接传输。

7.根据权利要求4所述的网关装置,其中,

所述地址变换处理部在与TCP SYN分组从所述第一NIC过来的情况呼应而形成所述第二TCP连接时,若接收从所述TCP/IP协议栈发来的ARP请求分组,则对所述TCP/IP协议栈回复包含伪MAC地址的模拟ARP应答分组。

8.根据权利要求4所述的网关装置，其中，

所述地址变换处理部在TCP SYN分组从所述第一NIC过来时，向所述地址变换表追加记录。

9.根据权利要求8所述的网关装置，还包括：

扩展TCP处理部，对从所述TCP/IP协议栈接收的接收分组的有效载荷部分施行既定加密处理，再次回送所述TCP/IP协议栈。

10. 根据权利要求1所述的网关装置，还包括：

第一NIC地址变换表，具备存放附加在所述接收分组的所述发送源MAC地址的第一发送源MAC地址字段、存放附加在所述接收分组的所述发送源IP地址的第一发送源IP地址字段、存放附加在所述接收分组的所述目的地MAC地址的第一目的地MAC地址字段、记录附加在所述接收分组的所述目的地IP地址的第一目的地IP地址字段、和记录具有唯一性的用于索引的索引用端口编号的第一索引用端口编号字段；以及

第二NIC地址变换表，具备第二发送源MAC地址字段、第二发送源IP地址字段、第二目的地MAC地址字段、第二目的地IP地址字段、记录所述索引用端口编号的第二索引用端口编号字段、和记录所述TCP/IP协议栈生成的动态端口编号的动态端口编号字段，

所述地址变换处理部将附加在所述接收分组的发送源端口编号变换为记录在所述第一NIC地址变换表的所述第一索引用端口编号字段的所述索引用端口编号，并且以附加在所述发送分组的目的地端口编号来检索所述第二NIC地址变换表的所述第二索引用端口编号字段，确定应该回写的记录。

11.根据权利要求1所述的网关装置，还包括：

扩展TCP处理对象主文件，其具有发送源IP地址字段、发送源端口编号字段、目的地IP地址字段、和目的地端口编号字段，

所述地址变换处理部，在从所述第一NIC接收的TCP分组的发送源及目的地的IP地址及端口编号的组合登记在所述扩展TCP处理对象主文件时，变换附加在从所述第一NIC接收的接收分组的所述发送源MAC地址、所述发送源IP地址、所述目的地MAC地址及所述目的地IP地址，若从所述第一NIC接收的分组未登记在所述扩展TCP处理对象主文件，则将从所述第一NIC接收的接收分组从所述第一NIC传输到第二NIC。

12.根据权利要求11所述的网关装置，其中，

所述地址变换处理部，

在从所述第一NIC接收的TCP分组的发送源及目的地的IP地址及端口编号的组合登记在所述扩展TCP处理对象主文件时，变换附加在从所述第一NIC接收的接收分组的所述发送源MAC地址、所述发送源IP地址、所述目的地MAC地址及所述目的地IP地址，

在从所述第一NIC接收的TCP分组未登记在所述扩展TCP处理对象主文件，且所述TCP分组的目的地IP地址为本来附加在所述第一NIC的IP地址的情况下，将所述TCP分组原样传输到所述TCP/IP协议栈。

网关装置

技术领域

[0001] 本发明涉及网关(network gateway)装置。

[0002] 更具体涉及对已有的网络环境不强加任何设定变更而能够容易追加提高安全性的加密通信功能的网关装置。

背景技术

[0003] 发明人从互联网爆炸性地在普通层面普及的早期阶段，认识到TCP/IP网络的可能性和技术极限以及问题点。例如，互联网邮件基本上等同于明信片，如果在通信路径上进行窃听(tapping:窃听)就能够容易取得邮件报头及正文。再者，互联网邮件、web等的通信应用中要进行提高安全性的加密时，全部由应用程序来对应。因此，对应于加密通信的应用无法进行与未对应加密通信的应用的加密通信，陷入了不管经过多久都不会普及加密通信对应应用的困境。

[0004] 此外，加密通信环境很难普及这样的问题点，对网络层中实现加密通信的IPSec而言也是同样的。不是应用层的途径，而是在网络层中将所有的通信整个加密这样的IPSec的基本技术思想是很好的着眼点。但是，指出了难以联系到现实、联系到现实为止的设定太困难、通信易断或者必须另外考虑用户认证等的问题点，直至现在也未能根本解决问题而普及更是没有头绪。

[0005] 鉴于这样的TCP/IP网络的可能性和技术极限以及问题点，发明人发明了在传输层实现认证及加密通信的技术，直至今日致力于该技术的实际安装和改良。此外，在本说明书中将这以后基于专利文献1所公开的技术的、传输层中的认证及加密的技术，加进TCP的扩展(eXPand)的意思而称为“XPTCP”。

[0006] 专利文献1是发明人做出的传输层的加密协议相关的现有技术文献。

[0007] 专利文献1:日本特许3783142号公报。

发明内容

[0008] 在将专利文献1中公开的XPTCP引入已有的网络环境时，最好尽量降低其引入壁垒。理想的是，网络上的所有终端为“零配置(Zero Configuration)”，即完全没有变更设定等或者引入新的软件，最好能利用XPTCP提供的新的功能。

[0009] 作为不向终端引入软件而实现新功能的方法，可考虑使网关装置介入网络的路径上的方法。但是，该网关装置对迄今所知道的装置、应用的形态来说，无论如何都需要终端的设定变更。

[0010] 例如，在网关装置为代理服务器的情况下，终端利用代理服务器对应应用程序，应用程序中必须设定代理服务器的IP地址和端口编号。即，如果应用程序不与代理服务器对应，则经由代理服务器的通信本身将无法实现。

[0011] 此外例如，在网关装置为路由器的情况下，终端必须重新设定默认网关的IP地址。

[0012] 而且，如果考虑网关装置被引入到已有的网络环境的情况，除了必须确定用于网

关装置的空着的IP地址以外，对已有的成为默认网关的路由器等的其他的网络装置也需要进行设定变更。

[0013] 本发明目的在于提供一种网关装置以解决涉及的课题，对已有的网络环境不强加任何设定变更而能够容易追加提高安全性的加密通信功能。

[0014] 为了解决上述课题，本发明的网关装置包括：内侧NIC；外侧NIC；初始设定部，对内侧NIC及外侧NIC设定混杂模式(promiscuous mode)；TCP/IP协议栈，在内侧NIC及外侧NIC之间进行TCP/IP通信处理；以及地址变换处理部，将附加在从内侧NIC接收的接收分组的发送源MAC地址变换为第一伪装MAC地址，将发送源IP地址变换为第一伪装IP地址，将目的地MAC地址变换为附加在内侧NIC的内侧NICMAC地址，将目的地IP地址变换为附加在内侧NIC的内侧NICIP地址，向TCP/IP协议栈发送收发分组，并且将附加在从TCP/IP协议栈接收的发送分组的发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址回写为附加在接收分组的发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址而向外侧NIC发送。

[0015] 为了使TCP/IP协议栈能够处理应该与分配到内侧NIC及外侧NIC的IP地址无关的分组，将附加到接收分组的发送源MAC地址及发送源IP地址改写为伪MAC地址及伪IP地址，将目的地MAC地址及目的地IP地址改写为分配给内侧NIC的IP地址及MAC地址后，提供给TCP/IP协议栈。

[0016] 通过本发明，能够提供对已有的网络环境不强加任何设定变更而能够容易追加提高安全性的加密通信功能的网关装置。

附图说明

[0017] 图1是包含本发明的实施方式的网关装置的网络的简略图；

[0018] 图2是XPTCP网关装置的功能块图；

[0019] 图3是示出XPTCP网关装置所具备的各种表格及列表的字段构成的图；

[0020] 图4是示出分组的结构的简略图；

[0021] 图5是地址变换处理部的功能块图；

[0022] 图6是内侧NIC接收处理部的功能块图；

[0023] 图7是外侧NIC接收处理部的功能块图；

[0024] 图8是外侧NIC发送处理部的功能块图；

[0025] 图9是内侧NIC发送处理部的功能块图；

[0026] 图10是XPTCP处理部的功能块图；

[0027] 图11是示出地址变换处理部的、内侧NIC中的分组接收处理动作的流程的流程图；

[0028] 图12是示出地址变换处理部的、外侧NIC中的分组接收处理动作的流程的流程图；

[0029] 图13是示出地址变换处理部的、外侧NIC中的分组发送处理动作的流程的流程图；

[0030] 图14是示出地址变换处理部的、内侧NIC中的分组发送处理动作的流程的流程图；

[0031] 图15是示出XPTCP处理部的XPTCP处理的流程的流程图；

[0032] 图16是示出套接字(socket)处理部的初始动作的流程的流程图；

[0033] 图17是示出套接字处理部的连接请求传输处理的流程的流程图；

[0034] 图18是示出通过XPTCP网关装置的分组的变化的简略图；

[0035] 图19是示出通过XPTCP网关装置的分组的变化的简略图；

[0036] 图20是示出通过XPTCP网关装置的分组的变化的简略图；

[0037] 图21是示出XPTCP网关装置中的、表示TCP连接确立序列的时序图整体的俯视图；

[0038] 图22是示出XPTCP网关装置中的、表示TCP连接确立序列的时序图之中前半处理内容的详细图；

[0039] 图23是示出XPTCP网关装置中的、表示TCP连接确立序列的时序图之中后半处理内容的详细图；

[0040] 图24是XPTCP网关装置中的、TCP数据传输序列的时序图；

[0041] 图25是示出XPTCP网关装置中的、表示TCP断开序列的时序图整体的俯视图；

[0042] 图26是示出XPTCP网关装置中的、表示TCP断开序列的时序图之中前半处理内容的详细图；

[0043] 图27是示出XPTCP网关装置中的、表示TCP断开序列的时序图之中后半处理内容的详细图；

[0044] 图28是说明XPTCP网关装置中改写所发送的分组的目的地IP地址的应用方式的简略图；

[0045] 图29是说明XPTCP网关装置中改写所发送的分组的发送源IP地址的应用方式的简略图。

具体实施方式

[0046] [网络的概要]

[0047] 图1是包含本发明的实施方式的网关装置的网络的简略图。

[0048] 本实施方式的网关装置提供XPTCP功能，因此下面将网关装置称为XPTCP网关装置101。

[0049] 图1中示出包含XPTCP网关装置101的网络。

[0050] 隔着XPTCP网关装置101而在左侧，非对应于XPTCP的两台终端即XPTCP非对应PC102及XPTCP非对应PC103，与XPTCP网关装置101的内侧NIC104连接。

[0051] 隔着XPTCP网关装置101而在右侧，非对应于XPTCP的终端即XPTCP非对应PC105和对应于XPTCP的终端即XPTCP对应PC106以及对应于XPTCP的服务器即XPTCP对应服务器107，与XPTCP网关装置101的外侧NIC108连接。

[0052] 下面，将隔着XPTCP网关装置101的左侧的网络称为XPTCP非对应网络109，将隔着XPTCP网关装置101的右侧的网络称为XPTCP对应网络110。

[0053] 即，XPTCP网关装置101中，也称为第一NIC的内侧NIC104与XPTCP非对应网络109连接，也称为第二NIC的外侧NIC108与XPTCP对应网络110连接。

[0054] XPTCP网关装置101加工分组，以能够用XPTCP的功能来将存在于XPTCP非对应网络109的XPTCP非对应PC102及XPTCP非对应PC103这样的XPTCP非对应的网络设备连接到存在于XPTCP对应网络110的XPTCP对应PC106及XPTCP对应服务器107这样的XPTCP对应的网络设备。

[0055] XPTCP网关装置101对与内侧NIC104连接的XPTCP非对应PC102提供XPTCP的功能。具体而言，在XPTCP非对应网络109上的XPTCP非对应PC102要与XPTCP对应网络110上的

XPTCP非对应PC105连接时，XPTCP网关装置101使分组原样流过，进行与现有的同样的一般的TCP/IP网络中的通信。但是，在XPTCP非对应网络109上的XPTCP非对应PC102要与XPTCP对应网络110上的XPTCP对应PC106或XPTCP对应服务器107连接时，XPTCP网关装置101将从XPTCP非对应PC102发送的分组改写为对应于XPTCP的分组，向XPTCP对应PC106或XPTCP对应服务器107发送。

[0056] [XPTCP网关装置101的内部构成]

[0057] 图2是XPTCP网关装置101的功能块图。

[0058] XPTCP网关装置101能够通过向运行有网络OS的计算机引入用于作为XPTCP网关装置101运行的程序来实现。网络OS例如能够利用周知的Windows(注册商标)或Linux(注册商标)等的OS。但是，XPTCP网关装置101需要设置在网络的路径上，因此计算机需要具备两个NIC(网络接口卡:Network Interface Card)。这就是内侧NIC104和外侧NIC108。

[0059] 内侧NIC104和外侧NIC108分别为周知的用于连接到TCP/IP网络的一般的接口卡。因而，内侧NIC104和外侧NIC108分别具有周知且固有的48比特的MAC地址(介质存取控制地址:Media Access Control address)。再者，图2中以功能块示出的内侧NIC104和外侧NIC108，除了作为硬件的NIC本身之外，还包含装置驱动器的功能。

[0060] 初始设定部201除了起动网络OS时设定的网络的基本设定操作之外，还对内侧NIC104和外侧NIC108设定“混杂模式(promiscuous mode)”。也称为“无差别模式”的该模式，能够接收并读取流过网络上的所有分组。对本实施方式的XPTCP网关装置101而言是必要的设定。

[0061] 未图示的网络OS在起动时进行网络的基本设定。此时的内侧NIC104及外侧NIC108的MAC地址及IP地址被存储在网络设定信息存储器202。

[0062] 针对从内侧NIC104接收的分组，地址变换处理部203从网络设定信息存储器202、假IPMAC列表204及内侧NIC地址表209分别读入信息，将附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址及目的地IP地址，变换为第一假NICMAC地址、第一假NICIP地址、索引用端口编号、内侧NICMAC地址及内侧NICIP地址，交给OS所具备的TCP/IP协议栈205。

[0063] 此外，目的地端口编号保持原样不变。

[0064] 同样地，针对从外侧NIC108接收的分组，地址变换处理部203从网络设定信息存储器202、假IPMAC列表204及外侧NIC地址表210分别读入信息，将附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，变换为第二假NICMAC地址、第二假NICIP地址、索引用端口编号、外侧NICMAC地址、外侧NICIP地址及动态端口编号，交给OS所具备的TCP/IP协议栈205。

[0065] 此外，针对从TCP/IP协议栈205发送到外侧NIC108的分组，地址变换处理部203以索引用端口编号为线索并参照外侧NIC地址表210，将附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号回写为先前改写以前的状态后，从外侧NIC108进行发送。

[0066] 同样地，针对从TCP/IP协议栈205发送到内侧NIC104的分组，地址变换处理部203以索引用端口编号为线索并参照内侧NIC地址表209，将附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号回写为先前

改写以前的状态后，从内侧NIC104进行发送。

[0067] 进而，针对从TCP/IP协议栈205发送到外侧NIC108的ARP(地址解析协议：Address Resolution Protocol)请求分组，地址变换处理部203通过以在假IPMAC列表204中记载的伪MAC地址进行应答，犹如从物理介质有应答的那样欺骗TCP/IP协议栈205而使之正常动作。

[0068] 也称为第一NIC地址变换表的内侧NIC地址表209，是用于地址变换处理部203在内侧NIC104与TCP/IP协议栈205之间，改写或回写附加在分组的MAC地址、IP地址及端口编号的表格。

[0069] 也称为第二NIC地址变换表的外侧NIC地址表210，是用于地址变换处理部203在外侧NIC108与TCP/IP协议栈205之间，改写或回写附加在分组的MAC地址、IP地址及端口编号的表格。

[0070] 这些内侧NIC地址表209及外侧NIC地址表210也称为地址变换表。

[0071] 再者，说明的方便起见，下面，将存在于XPTCP非对应网络109的XPTCP非对应PC102、103等的非对应于XPTCP的网络设备称为“终端”，将存在于XPTCP对应网络110的XPTCP对应服务器107、XPTCP对应PC106等的对应于XPTCP的网络设备称为“服务器”。关于XPTCP非对应PC105，由于是在采用XPTCP的通信的对象之外，所以在“终端”“服务器”的定义中除外。

[0072] TCP/IP协议栈205是网络OS所具备的网络驱动器程序。该TCP/IP协议栈205经由地址变换处理部203，在NIC之间进行分组的收发，在应用程序之间进行数据的收发。

[0073] TCP/IP协议栈205对应用程序提供周知的称为套接字(以称为“BSD套接字”的名称而周知。)的应用程序接口(API)。

[0074] TCP/IP协议栈205将从NIC接收的分组按照ARP报头、IP报头、TCP或UDP报头的顺序除去，连结分组的有效载荷后返回给流数据，交给既定的应用。

[0075] 相反，TCP/IP协议栈205通过TCP/IP协议栈205事先形成并从应用指定的套接字，将从应用接受的流数据分割为既定数据大小的有效载荷之后，按照TCP或UDP报头、IP报头、ARP报头的顺序附加报头，通过NIC发送到发送目的地。

[0076] 特别是，在处理TCP协议的分组的情况下，TCP/IP协议栈205通过称为SYN－ACK＆SYN－ACK的周知的三次握手(3way- handshake)在TCP/IP协议栈205的内部形成周知的称为连接的虚拟的通信路。

[0077] 本实施方式的XPTCP网关装置101在内侧NIC104和外侧NIC108两者形成连接，在该连接彼此间进行数据的传输。

[0078] 内侧NIC地址表209及外侧NIC地址表210通过设置索引用端口编号来实现TCP/IP协议栈205作成的连接与实际附加在分组的本来的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号之间的关联建立。

[0079] 内侧NIC地址表209及外侧NIC地址表210也称为TCP/IP协议栈205作成的管理连接的表格。

[0080] 也称为扩展TCP处理部的XPTCP处理部206，从TCP/IP协议栈205形成的套接字即“一个连接的出入口”接收数据，将接收的数据向TCP/IP协议栈205形成的其他的套接字即“另一个连接的出入口”传输。

[0081] 此外，XPTCP处理部206响应存储在XPTCP处理对象主文件(master)208的指示内容，进行认证处理及加密通信处理。特别是XPTCP处理部206在将从TCP/IP协议栈205接收的数据再回送给TCP/IP协议栈205时，改写附加在套接字的发送源IP地址、发送源端口编号、目的地IP地址、目的地端口编号。

[0082] 套接字处理部207是网络OS起动后自动执行的较小的模拟服务器程序，并且因为从内侧NIC104接收的分组，而从TCP/IP协议栈205接受connect事件时，从附加在接受connect事件的套接字的发送源IP地址、发送源端口编号、目的地IP地址、目的地端口编号，向TCP/IP协议栈205产生用于面向外侧NIC108作成新的套接字的connect request事件即连接请求。

[0083] 套接字处理部207对于TCP/IP协议栈205仅进行套接字打开/关闭处理，与TCP/IP协议栈205的实际的数据收发是由XPTCP处理部206进行的。

[0084] 图2所示的XPTCP网关装置101的块图中，内侧NIC104、外侧NIC108、地址变换处理部203、TCP/IP协议栈205、XPTCP处理部206及套接字处理部207依照周知的遵循7层的OSI参考模型的TCP/IP的分层模型。

[0085] 内侧NIC104和外侧NIC108包括NIC驱动器在内相当于物理层和数据链接层。

[0086] TCP/IP协议栈205相当于网络层(IP、ICMP(网络控制消息协议:Internet Control Message Protocol)、ARP)和传输层(TCP、UDP)。

[0087] 套接字处理部207相当于应用层。

[0088] 地址变换处理部203潜伏在数据链接层与网络层之间，以使TCP/IP协议栈205能够处理本来应该无关的分组的方式改写附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号。因此，地址变换处理部203相当于网络层。

[0089] XPTCP处理部206介于传输层和应用层之间，进行套接字打开/关闭处理以外的、网络流数据的传输和认证及加密或解码。因此，XPTCP处理部206相当于实现应用层不能介入的认证及加密通信的传输层，并且在传输数据这样的功能中也相当于应用层。

[0090] 标准搭载于网络OS的TCP/IP协议栈205，本来只能处理针对存储在网络设定信息存储器202的IP地址即附加在自己的NIC的IP地址的通信。另一方面，XPTCP网关装置101有必要处理所有的分组。此外，XPTCP利用通信步骤复杂的TCP/IP的功能，并且实现传输层中的认证和加密处理。

[0091] 因此，为了在最大限度地有效活用TCP/IP协议栈205的功能的同时，追加必要的最小限度的程序从而实现XPTCP网关装置101，本实施方式的XPTCP网关装置101施行“欺骗”TCP/IP协议栈205的处理。

[0092] 即，为了使TCP/IP协议栈205能够处理应该与被分配给XPTCP网关装置101的IP地址无关的分组，将附加在从内侧NIC104或外侧NIC108接收的分组的发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址，暂时改写为分配给XPTCP网关装置101的IP地址、MAC地址等。然后，将改写了发送源及目的地的MAC地址、IP地址及端口编号的有关分组交给TCP/IP协议栈205。

[0093] 在地址变换处理部203及XPTCP处理部206中进行的改写处理、即附加在分组的发送源及目的地的MAC地址、IP地址以及端口编号的改写处理的详细，后面将通过图18、图19

及图20进行叙述。

[0094] [表格及列表的构成]

[0095] 图3是示出XPTCP网关装置101所具备的各种表格及列表的字段构成的图。

[0096] 图2所示的XPTCP网关装置101所拥有的内侧NIC地址表209、外侧NIC地址表210、XPTCP策略表(policy table)211、假IPMAC列表204设在未图示的RAM内。此外，XPTCP处理对象主文件208设在硬盘装置等的未图示的非易失存储体中，在地址变换处理部203起动时，复制到未图示的RAM内。网络设定信息存储器202通过网络OS设在未图示的RAM内。

[0097] 图4是示出分组的结构的简略图。参照图3的字段构成图和图4的简略图说明内侧NIC地址表209及外侧NIC地址表210的字段。

[0098] 内侧NIC地址表209具有协议种类字段、发送源MAC地址字段、发送源IP地址字段、发送源端口编号字段、目的地MAC地址字段、目的地IP地址字段、目的地端口编号字段、索引用端口编号字段、和定时器用计数值字段。

[0099] 外侧NIC地址表210具有协议种类字段、发送源MAC地址字段、发送源IP地址字段、发送源端口编号字段、目的地MAC地址字段、目的地IP地址字段、目的地端口编号字段、索引用端口编号字段、动态端口编号字段、和定时器用计数值字段。

[0100] 在协议种类字段中存放有表示TCP或UDP的标志(flag)，作为从内侧NIC104或外侧NIC108进入的分组的种类。它是从IP报头401的协议编号读取的。此外，本实施方式的XPTCP网关装置101在现阶段只处理TCP分组，但是为了在不久的将来能够处理UDP分组，而准备了该协议种类字段。

[0101] 在发送源MAC地址字段中存放有附加在从内侧NIC104或外侧NIC108进入的分组的发送源MAC地址。它是从MAC报头402的发送源MAC地址读取的。

[0102] 在发送源IP地址字段中存放有附加在从内侧NIC104或外侧NIC108进入的分组的发送源IP地址。它是从IP报头401的发送源IP地址读取的。

[0103] 在发送源端口编号字段中存放有附加在从内侧NIC104或外侧NIC108进入的分组的发送源端口编号。它是从TCP报头403或UDP报头404的发送源端口编号读取的。

[0104] 在目的地MAC地址字段中存放有附加在从内侧NIC104或外侧NIC108进入的分组的目的地MAC地址。它是从MAC报头402的目的地MAC地址读取的。

[0105] 在目的地IP地址字段中存放有附加在从内侧NIC104或外侧NIC108进入的分组的目的地IP地址。它是从IP报头401的目的地IP地址读取的。

[0106] 在目的地端口编号字段中存放有附加在从内侧NIC104或外侧NIC108进入的分组的目的地端口编号。它是从TCP报头403或UDP报头404的目的地端口编号读取的。

[0107] 在索引用端口编号字段存放有在地址变换处理部203即将从内侧NIC104或外侧NIC108发送分组之前，回写附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号时，用于确定在内侧NIC地址表209或外侧NIC地址表210的哪个记录中被记述的索引信息。

[0108] 当从内侧NIC104发来作为处理对象与XPTCP处理对象主文件208的记录一致的TCP SYN分组时，地址变换处理部203向内侧NIC地址表209追加记录新记录之际，该索引用端口编号采用图2的TCP端口编号存储器212的值。索引用端口编号将端口编号用作索引信息，因此希望具有唯一性(独特的、不重复)。因此，要利用TCP端口编号存储器212的值时，已经使

用了该编号的情况下，增加TCP端口编号存储器212的值，确认该端口编号是否空着。

[0109] TCP SYN分组是周知的表示TCP通信开始(连接的确立请求)的分组，是存在于TCP报头403中的6比特的代码比特的第5比特为“1”的分组。

[0110] TCP ACK分组是周知的表示TCP通信中的确认应答的分组，是存在于TCP报头403中的6比特的代码比特的第2比特为“1”的分组。

[0111] TCP FIN分组是周知的表示TCP通信结束(连接的断开请求)的分组，是存在于TCP报头403中的6比特的代码比特的第6比特为“1”的分组。

[0112] TCP ACK/SYN分组是存在于TCP报头403中的6比特的代码比特的第2比特和第5比特为“1”的分组，同时具备TCP SYN分组和TCP ACK分组的两个意思。

[0113] 仅设在外侧NIC地址表210的动态端口编号存放于动态端口编号字段中。该动态端口编号是在TCP/IP协议栈205通过外侧NIC108而形成与存在于XPTCP对应网络110的XPTCP对应服务器107、XPTCP对应PC106等的对应于XPTCP的网络设备、即服务器的连接时，作为该连接的发送源端口编号，TCP/IP协议栈205自动生成的端口编号。多数情况下，动态端口编号是也被称为“短命端口”的周知的短暂端口的编号即由TCP/IP协议栈205赋予的端口编号49152到65535的编号。

[0114] 在定时器用计数值字段中存放有判断出内侧NIC地址表209或外侧NIC地址表210的有关记录没有被利用而废弃时的、用于测量经过时间的地址表更新计数器213的值。

[0115] 在图3所示的网络设定信息存储器202中存储有网络OS起动时进行了网络的基本设定的结果的、内侧NIC104及外侧NIC108的MAC地址及IP地址。即，网络设定信息存储器202由网络OS设置。

[0116] 内侧NICMAC地址表示内侧NIC104的本来的MAC地址。

[0117] 内侧NICIP地址表示内侧NIC104的本来的IP地址。

[0118] 外侧NICMAC地址表示外侧NIC108的本来的MAC地址。

[0119] 外侧NICIP地址表示外侧NIC108的本来的IP地址。

[0120] 同样地图3所示的假IPMAC列表204具有内侧NICIP地址字段、第一假MAC地址字段、第一假IP地址字段、外侧NICIP地址字段、第二假MAC地址字段、和第二假IP地址字段。

[0121] 在内侧NICIP地址字段中存放有内侧NIC104的IP地址。它是从网络设定信息存储器202取得的。

[0122] 在第一假MAC地址字段中存放有第一假MAC地址。

[0123] 在第一假IP地址字段中存放有第一假IP地址。

[0124] 在外侧NICIP地址字段中存放有外侧NIC108的IP地址。它是从网络设定信息存储器202取得的。

[0125] 在第二假MAC地址字段中存放有第二假MAC地址。

[0126] 在第二假IP地址字段中存放有第二假IP地址。

[0127] 第一假MAC地址、第一假IP地址、第二假MAC地址及第二假IP地址是地址变换处理部203及XPTCP处理部206使用的伪MAC地址及IP地址。

[0128] 同样地也称为扩展TCP处理对象主文件的图3所示的XPTCP处理对象主文件208具有记录编号字段、协议种类字段、发送源IP地址字段、发送源端口编号字段、目的地IP地址字段、目的地端口编号字段、和密码种类其他字段。

[0129] 记录编号字段是XPTCP处理对象主文件208的记录编号本身。是唯一地识别XPTCP处理对象主文件208的记录的连号的编号。此外，存放在记录编号字段的信息是用在后述的XPTCP策略表211的、用于唯一地识别记录的信息。因而，只要能唯一地进行识别，也可以不一定是记录编号。

[0130] 在协议种类字段中，作为从内侧NIC104进入的分组的种类，存放有表示TCP或UDP的标志。它是从IP报头401的协议编号读取的。

[0131] 在发送源IP地址字段中存放有附加在从内侧NIC104进入的分组的发送源IP地址。它是从IP报头401的发送源IP地址读取的。

[0132] 在发送源端口编号字段中存放有附加在从内侧NIC104进入的分组的发送源端口编号。它是从TCP报头403或UDP报头404的发送源端口编号读取的。

[0133] 在目的地IP地址字段中存放有附加在从内侧NIC104进入的分组的目的地IP地址。它是从IP报头401的目的地IP地址读取的。

[0134] 在目的地端口编号字段中存放有附加在从内侧NIC104进入的分组的目的地端口编号。它是从TCP报头403或UDP报头404的目的地端口编号读取的。

[0135] 在密码种类其他字段中存放有用于该XPTCP会话(session)的认证、密码的种类等的信息。

[0136] 即，在XPTCP处理对象主文件208中存储有从终端向服务器发送的分组的IP地址及端口编号的组合、和根据具有该IP地址及端口编号的组合的分组，适用于通过在内侧NIC104及外侧NIC108分别形成的连接的数据流的、与加密等相关的信息。

[0137] 同样地图3所示的XPTCP策略表211具有协议种类字段、索引用端口编号字段、和记录编号字段。

[0138] 在协议种类字段中，与XPTCP处理对象主文件208同样地，作为从内侧NIC104进入的分组的种类，存放有表示TCP或UDP的标志。它是从IP报头401的协议编号读取的。

[0139] 在索引用端口编号字段中，存放有通过地址变换处理部203对该会话的分组附加的索引用端口编号。

[0140] 记录编号字段是XPTCP处理对象主文件208的记录编号本身。因而，以记在该字段的记录编号指定XPTCP处理对象主文件208的记录，并参考有关记录的密码种类其他字段。

[0141] XPTCP策略表211通过将索引用端口编号和密码种类其他的信息相关联，来确定适用于通过索引用端口编号所涉及的TCP连接的数据流的密码种类等。

[0142] 再次返回图2，继续说明各部分。

[0143] 地址表更新计数器213是在删除内侧NIC地址表209及外侧NIC地址表210的成为不使用的记录时，用于查看经过时间的计数器。作为一例，地址表更新计数器213是计数从0到119的数的循环计数器。从0开始，每过1秒计数值增1，计数到119时，再次从0开始计数。

[0144] 地址变换处理部203在后述的TCP断开序列中，与从内侧NIC104及外侧NIC108的两者发来TCP FIN分组的情况呼应，将地址表更新计数器213的值写入内侧NIC地址表209及外侧NIC地址表210的有关的记录的定时器用计数值字段。然后，比较定时器用计数值字段的值与当前的地址表更新计数器213的值，如果判断为经过了60秒以上，就判断为该记录中所示的通信会话已经结束，并删除有关记录。

[0145] TCP端口编号存储器212是存放用于将值记入于内侧NIC地址表209及外侧NIC地址

表210的索引用端口编号字段的端口编号的存储器。

[0146] 当从内侧NIC104发来TCP SYN分组时，需要作成新的连接。为了在TCP/IP协议栈205作成连接，地址变换处理部203进行地址变换处理。通过地址变换处理，TCP/IP协议栈205对于附加了与本来的发送源IP地址及目的地IP地址等不同的、伪发送源IP地址及目的地IP地址等的分组形成连接。

[0147] 地址变换处理部203在对分组附加伪发送源IP地址及目的地IP地址等之际，必须进行TCP/IP协议栈205作成的连接与其伪发送源IP地址及目的地IP地址等的关联建立。为了识别该连接并且最终回到本来的发送源IP地址及目的地IP地址等，需要对分组附加识别信息。这就是索引用端口编号。

[0148] 在对内侧NIC地址表209作成了新的记录时，将TCP端口编号存储器212的值增1，将该值写入索引用端口编号字段。

[0149] 索引用端口编号必须为TCP/IP协议栈205能够辨别的编号，因此记入TCP端口编号存储器212的最大值为65535。

[0150] TCP端口编号存储器212被写入也称为“短命端口”的周知的短暂端口的编号即从端口编号49152逐一增加到65535的值。再者，TCP端口编号存储器212也可以由循环计数器构成。

[0151] [地址变换处理部203的内部构成]

[0152] 图5是地址变换处理部203的功能块图。

[0153] 地址变换处理部203分为内侧NIC接收处理部501、外侧NIC接收处理部502、外侧NIC发送处理部503、内侧NIC发送处理部504、表更新处理部505、及策略回答部506这五个功能块。

[0154] 首先，说明内侧NIC接收处理部501的详细。图6是内侧NIC接收处理部501的功能块图。

[0155] 关于内侧NIC104接收的分组，最先接收分组判定部601参考XPTCP处理对象主文件208，判定该分组是否成为XPTCP处理的对象等。

[0156] 如果内侧NIC104接收的分组例如为ICMP分组或不符合XPTCP处理对象主文件208的处理对象外分组的情况下，接收分组判定部601将该分组原样传输到外侧NIC108。

[0157] 如果内侧NIC104接收的分组为对XPTCP网关装置101发送的XPTCP处理对象外分组的情况下，接收分组判定部601将该分组原样传输到TCP/IP协议栈205。

[0158] 如果从内侧NIC104输入的分组为符合XPTCP处理对象主文件208的处理对象分组的情况下，接收分组判定部601接着查看该分组的详细。

[0159] 接收分组判定部601在该分组为TCP数据分组时，将该TCP数据分组交给地址置换部602。

[0160] 地址置换部602以发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号来检索内侧NIC地址表209，并确定记录，改写分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址及目的地IP地址，向TCP/IP协议栈205传输。

[0161] 若在接收分组判定部601处理的分组为TCP SYN分组，则为未登记在内侧NIC地址表209的分组。因此，接收分组判定部601将TCP SYN分组交给连接登记处理部603。连接登记

处理部603以附加在TCP SYN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，向内侧NIC地址表209追加记录新的记录。然后，将TCP端口编号存储器212的值增1并进行参考，将该值作为索引用端口编号记录于内侧NIC地址表209的索引用端口编号字段。进而，向外侧NIC地址表210也追加记录相同内容的记录。其后，连接登记处理部603将TCP SYN分组交给地址置换部602。地址置换部602与前述的TCP数据分组同样地，改写TCP SYN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址及目的地IP地址，向TCP/IP协议栈205传输。

[0162] 如果在接收分组判定部601处理的分组为TCP FIN分组，不仅意味着形成在TCP/IP协议栈205的连接结束，而且产生删除内侧NIC地址表209及外侧NIC地址表210的该记录的必要。但是，删除记录的时期，需要从面向内侧NIC104形成的连接和面向外侧NIC108形成的连接这两个的连接结束起经过既定时间。

[0163] 因此，接收分组判定部601将TCP FIN分组交给记录删除准备处理部604。

[0164] 记录删除准备处理部604以附加在TCP FIN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号来检索内侧NIC地址表并确定记录，将有关记录的索引端口编号写在删除预定列表605。删除预定列表605是设在未图示的RAM内的、记录了预定删除的记录的索引端口编号的列表。其后，记录删除准备处理部604将TCP FIN分组交给地址置换部602。地址置换部602与前述的TCP数据分组及TCP SYN分组同样地，改写TCP FIN分组的发送源MAC地址、发送源IP地址，发送源端口编号、目的地MAC地址及目的地IP地址，向TCP/IP协议栈205传输。

[0165] 此外，地址置换部602在TCP数据分组、TCP SYN分组及TCP FIN分组的任何情况下都不改写目的地端口编号。

[0166] 地址置换部602在改写附加在分组的MAC地址、IP地址及端口编号时，参考假IPMAC列表204。

[0167] 接着，说明外侧NIC接收处理部502的详细。

[0168] 图7是外侧NIC接收处理部502的功能块图。

[0169] 关于外侧NIC108接收的分组，最先接收分组判定部701参考XPTCP处理对象主文件208，判定该分组是否成为XPTCP处理的对象等。

[0170] 如果外侧NIC108接收的分组例如为不符合ICMP分组、XPTCP处理对象主文件208的处理对象外分组的情况下，外侧NIC接收处理部502将该分组原样传输到内侧NIC104。

[0171] 如果外侧NIC108接收的分组为对XPTCP网关装置101发送的XPTCP处理对象外分组的情况下，外侧NIC接收处理部502将该分组原样传输到TCP/IP协议栈205。

[0172] 如果从外侧NIC108输入的分组为符合XPTCP处理对象主文件208的处理对象分组的情况下，接收分组判定部701接着查看该分组的详细。

[0173] 如果该分组为TCP数据分组，则接收分组判定部701将该TCP数据分组交给地址置换部702。

[0174] 地址置换部702以发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号来检索外侧NIC地址表210并确定记录，改写分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，向TCP/IP协议栈205传输。

[0175] 接收分组判定部701中，如果该分组为TCP FIN分组，就意味在TCP/IP协议栈205形成的连接结束，并且产生删除内侧NIC地址表209及外侧NIC地址表210的有关记录的必要。如上所述，删除记录的时期需要从面向外侧NIC108形成的连接和面向外侧NIC108形成的连接这两个的连接结束起经过既定时间。

[0176] 因此，接收分组判定部701将TCP FIN分组交给记录删除处理部703。

[0177] 记录删除处理部703以附加在TCP FIN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号来检索内侧NIC地址表并确定记录，取得有关记录的索引端口编号。

[0178] 接着，确认取得的索引端口编号是否在删除预定列表605。如果在删除预定列表605中有该索引端口编号，将当前时间点的地址表更新计数器213的值写入该索引端口编号涉及的外侧NIC地址表210及内侧NIC地址表209的记录的定时器用计数值字段。其后，记录删除处理部703将TCP FIN分组交给地址置换部702。

[0179] 地址置换部702与上述的TCP数据分组同样地，改写TCP FIN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址目的地IP地址及目的地端口编号，向TCP/IP协议栈205传输。

[0180] 地址置换部702在改写附加在分组的MAC地址、IP地址及端口编号时，参考假IPMAC列表204。

[0181] 接着，说明外侧NIC发送处理部503的详细。

[0182] 图8是外侧NIC发送处理部503的功能块图。

[0183] 关于发送分组判定部801，若接收从TCP/IP协议栈205送出的分组，最先判定分组为地址改写对象外分组还是地址改写对象TCP分组、或者是ARP请求分组。

[0184] 如果分组为地址改写对象外的分组，不做任何变动而保持原样向外侧NIC108发送。

[0185] 如果分组为ARP请求分组，且附加在ARP请求分组的查询IP地址为第二假IP地址的情况下，为了确定附加在分组的MAC地址，该分组为TCP/IP协议栈205形成连接时发送的分组。因此，发送分组判定部801将ARP请求分组交给ARP应答处理部802。

[0186] ARP应答处理部802参考假IPMAC列表204，向TCP/IP协议栈205回答第二假MAC地址。

[0187] 如果分组为TCP分组，附加在分组的目的地IP地址为第二假IP地址的情况下，发送分组判定部801接着确认该分组是否为TCP SYN分组。如果为TCP SYN分组，其表示TCP/IP协议栈205重新作成了连接。因而，需要将TCP/IP协议栈205重新作成的连接的发送源端口编号即动态端口编号存储在外侧NIC地址表210。因此，发送分组判定部801将TCP SYN分组交给动态端口记录处理部803。

[0188] 动态端口记录处理部803取得附加在TCP SYN分组的发送源端口编号即动态端口编号和作为目的地端口编号附加的索引端口编号。然后，如果以索引端口编号确定了外侧NIC地址表210的有关记录，则向该记录的动态端口编号字段记录动态端口编号。然后，动态端口记录处理部803将该TCP SYN分组交给地址复原部804。

[0189] 地址复原部804取得外侧NIC地址表210的之前以目的地端口编号确定的记录的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端

口编号，并回写分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，向外侧NIC108发送。

[0190] 如果分组为TCP分组，附加在分组的目的地IP地址为第二假IP地址的情况下，发送分组判定部801接着确认该分组是否为TCP SYN分组。如果不是TCP SYN分组，则发送分组判定部801将该TCP分组交给地址复原部804。

[0191] 地址复原部804取得外侧NIC地址表210的之前以索引端口编号确定的记录的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，并回写分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，向外侧NIC108发送。

[0192] 接着，说明内侧NIC发送处理部504的详细。

[0193] 图9是内侧NIC发送处理部504的功能块图。

[0194] 若接收从TCP/IP协议栈205送出的分组，则发送分组判定部901最先判定分组是否为地址改写对象外分组，或者是否为地址改写对象TCP分组。

[0195] 如果分组为地址改写对象外的分组，则不做任何变动而保持原样发送到内侧NIC104。

[0196] 如果分组为TCP分组，附加在分组的目的地IP地址为第一假IP地址的情况下，发送分组判定部901将该TCP分组交给地址复原部902。

[0197] 地址复原部902取得内侧NIC地址表209的以索引端口编号确定的记录的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，并回写分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号，向内侧NIC104发送。

[0198] 接着，说明表更新处理部505的详细。

[0199] 表更新处理部505每过1秒起动，将地址表更新计数器213的值增1，检查内侧NIC地址表209及外侧NIC地址表210的所有的记录的定时器用计数值字段，确认是否有TCP FIN分组过来而关闭的连接经过了60秒以上的记录。然后，如果有这样的记录就删除有关记录。

[0200] 接着，说明策略回答部506的详细。

[0201] 策略回答部506对于从XPTCP处理部206送出的、伴随索引端口编号的策略查询，参考XPTCP处理对象主文件208及内侧NIC地址表209，回答用于指定对于以该索引端口编号确定的连接的密码种类等的、XPTCP处理对象主文件208的记录编号。

[0202] [XPTCP处理部206的内部构成]

[0203] 图10是XPTCP处理部206的功能块图。

[0204] 事件检测部1001检测从TCP/IP协议栈205取得的accept事件、connect request事件及close事件，控制套接字操作部1002及策略设定部1003。

[0205] 套接字操作部1002对于通过TCP/IP协议栈205在未图示的RAM上形成的套接字存储器区域1004，将从套接字取得的流数据交给加密处理部1005或解码处理部1006，将处理后的流数据交给套接字存储器区域1004上的既定套接字。

[0206] 策略设定部1003以从套接字操作部1002通过事件检测部1001而获得的索引端口编号为自变量，对地址变换处理部查询策略。对于该查询，地址变换处理部的策略回答部506回答XPTCP处理对象主文件208的记录编号。于是，策略设定部1003向XPTCP策略表211记

录索引端口编号和XPTCP处理对象主文件208的记录编号并进行关联。

[0207] 加密处理部1005参考XPTCP策略表211及XPTCP处理对象主文件208，对于从套接字操作部1002接受的流数据，执行所指定的加密处理。

[0208] 解码处理部1006参考XPTCP策略表211及XPTCP处理对象主文件208，对于从套接字操作部1002接受的流数据，执行所指定的解码处理。

[0209] 此外，本来在XPTCP处理部206中还存在与认证相关的功能，但是在本实施方式的XPTCP网关装置101中，与认证相关的动作脱离发明的范畴，因此硬省略了与认证相关的记述。因此，在图10所示的XPTCP处理部206的功能块图中，省略了与认证相关的功能块。

[0210] [XPTCP网关装置101的动作/地址变换处理部203的动作]

[0211] 由此，基于图11到图17的流程图，说明XPTCP网关装置101的动作的流程。

[0212] 图11是示出地址变换处理部203的、内侧NIC104中的分组接收处理的动作的流程的流程图。这相当于内侧NIC接收处理部501的动作的流程。

[0213] 若开始处理(S1101)，则接收分组判定部601最先判定内侧NIC104接收的分组是否为例如ARP分组、ICMP分组等的、明显成为传输对象的处理对象外分组(S1102)。

[0214] 判定的结果，在接收的分组为ARP分组、ICMP分组等的、明显成为传输对象的处理对象外分组的情况下(S1102的“是(YES)”)，接收分组判定部601将该分组原样传输到外侧NIC108(S1103)，结束一连串的处理(S1104)。

[0215] 步骤S1102中，在接收的分组不是明显成为传输对象的处理对象外分组的情况下(S1102的“否(ON)”)，接收分组判定部601接着判定该分组是否为对XPTCP网关装置101发送的XPTCP处理对象外分组(S1105)。

[0216] 判定的结果，在接收的分组为对XPTCP网关装置101发送的XPTCP处理对象外分组的情况下(S1105的“是”)，接收分组判定部601将该分组原样传输给TCP/IP协议栈205(S1106)，结束一连串的处理(S1104)。

[0217] 步骤S1105中，在接收的分组不是对XPTCP网关装置101发送的XPTCP处理对象外分组的情况下(S1105的“否”)，接收分组判定部601接着以该分组的发送源IP地址、发送源端口编号、目的地IP地址及目的地端口编号来检索XPTCP处理对象主文件208(S1107)。

[0218] 检索的结果，如果XPTCP处理对象主文件208中没有接收的分组的发送源IP地址、发送源端口编号、目的地IP地址及目的地端口编号的组合(S1108的“否”)，则该分组为XPTCP网关装置101的处理对象之外，因此接收分组判定部601将该分组原样传输给外侧NIC108(S1103)，结束一连串的处理(S1104)。

[0219] 步骤S1108中，如果在XPTCP处理对象主文件208中有接收的分组的发送源IP地址、发送源端口编号、目的地IP地址及目的地端口编号的组合(S1108的“是”)，则该分组为XPTCP网关装置101的处理对象，需要改写附加在分组的MAC地址、IP地址及端口编号。因此，接收分组判定部601进一步查看接收的分组的详细。

[0220] 接收分组判定部601判定接收的分组是否为TCP SYN分组(S1109)。

[0221] 判定的结果，如果接收的分组为TCP SYN分组(S1109的“是”)，则接收分组判定部601将该TCP SYN分组交给连接登记处理部603。

[0222] 连接登记处理部603若接受TCP SYN分组，则参考TCP端口编号存储器，在取得当前时间点未被使用的(不重复的)新的索引端口编号后，与所接收的分组的发送源IP地址、发

送源端口编号、目的地IP地址及目的地端口编号一起，向内侧NIC地址表209作为新的记录进行追加记录(S1110)。进而，以相同的内容对外侧NIC地址表210也同样地追加记录新的记录(S1111)。

[0223] 连接登记处理部603在向内侧NIC地址表209和外侧NIC地址表210追加记录新的记录后，将从接收分组判定部601交给的TCP SYN分组交给地址置换部602。

[0224] 地址置换部602参考从连接登记处理部603交给的索引端口编号和假IPMAC列表204，改写TCP SYN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址及目的地IP地址(S1112)。具体而言，

[0225] ·将附加在分组的发送源MAC地址改写为第一假MAC地址；

[0226] ·将附加在分组的发送源IP地址改写为第一假IP地址；

[0227] ·将附加在分组的发送源端口编号改写为索引端口编号；

[0228] ·将附加在分组的目的地MAC地址改写为内侧NICMAC地址；

[0229] ·将附加在分组的目的地IP地址改写为内侧NICIP地址。

[0230] 然后，目的地端口编号不变更。

[0231] 地址置换部602在进行IP地址等的置换处理后，将该TCP SYN分组向TCP/IP协议栈205发送(S1106)，结束一连串的处理(S1104)。

[0232] 步骤S1109中，如果接收的分组不是TCP SYN分组(S1109的“否”)，接收分组判定部601判定接着接收的分组是否为TCP FIN分组(S1113)。

[0233] 判定的结果，如果接收的分组为TCP FIN分组(S1109的“是”)，接收分组判定部601将该TCP FIN分组与索引端口编号一起交给记录删除准备处理部604。

[0234] 记录删除准备处理部604向删除预定列表605写入该TCP FIN分组的索引端口编号(S1104)。其后，记录删除准备处理部604将TCP FIN分组和索引端口编号交给地址置换部602。

[0235] 地址置换部602参考从接收分组判定部601通过记录删除准备处理部604而交给的索引端口编号和假IPMAC列表204，改写TCP FIN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址及目的地IP地址(S1112)。具体而言，将附加在分组的发送源MAC地址改写为第一假MAC地址，将附加在分组的发送源IP地址改写为第一假IP地址，将附加在分组的发送源端口编号改写为索引端口编号，将附加在分组的目的地MAC地址改写为内侧NICMAC地址，将附加在分组的目的地IP地址改写为内侧NICIP地址。然后，目的地端口编号不变更。

[0236] 地址置换部602在进行IP地址等的置换处理后，将该TCP FIN分组发送给TCP/IP协议栈205(S1106)，结束一连串的处理(S1104)。

[0237] 步骤S1113中，如果接收的分组不是TCP FIN分组(S1113的“否”)，则该分组为TCP数据分组。因此，接收分组判定部601将该TCP数据分组与索引端口编号一起交给地址置换部602。

[0238] 地址置换部602参考从接收分组判定部601交给的索引端口编号和假IPMAC列表204，改写TCP数据分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址及目的地IP地址(S1112)。具体而言，将附加在分组的发送源MAC地址改写为第一假MAC地址，将附加在分组的发送源IP地址改写为第一假IP地址，将附加在分组的发送源端口编号

改写为索引端口编号，将附加在分组的目的地MAC地址改写为内侧NICMAC地址，将附加在分组的目的地IP地址改写为内侧NICIP地址。然后，目的地端口编号不变更。

[0239] 地址置换部602在进行IP地址等的置换处理后，将该TCP数据分组发送给TCP/IP协议栈205(S1106)，结束一连串的处理(S1104)。

[0240] 图12是示出地址变换处理部203的、外侧NIC108中的分组接收处理的动作的流程的流程图。这相当于外侧NIC接收处理部502的动作流程。

[0241] 若开始处理(S1201)，则接收分组判定部701最先判定外侧NIC108接收的分组是否为例如ARP分组、ICMP分组等的、明显成为传输对象的处理对象外分组(S1202)。

[0242] 判定的结果，在接收的分组为ARP分组、ICMP分组等的、明显成为传输对象的处理对象外分组的情况下(S1202的“是”)，接收分组判定部701将该分组原样传输给内侧NIC104(S1203)，结束一连串的处理(S1204)。

[0243] 步骤S1202中，在接收的分组不是明显成为传输对象的处理对象外分组的情况下(S1202的“否”)，接收分组判定部701接着判定该分组是否为对XPTCP网关装置101发送的XPTCP处理对象外分组(S1205)。

[0244] 判定的结果，在接收的分组为对XPTCP网关装置101发送的XPTCP处理对象外分组的情况下(S1205的“是”)，接收分组判定部701将该分组原样传输给TCP/IP协议栈205(S1206)，结束一连串的处理(S1204)。

[0245] 步骤S1205中，在接收的分组不是对XPTCP网关装置101发送的XPTCP处理对象外分组的情况下(S1205的“否”)，接收分组判定部701接着以该分组的发送源IP地址、发送源端口编号、目的地IP地址及目的地端口编号来检索XPTCP处理对象主文件208(S1207)。

[0246] 检索的结果，如果在XPTCP处理对象主文件208中没有所接收的分组的发送源IP地址、发送源端口编号、目的地IP地址及目的地端口编号的组合(S1208的“否”)，则该分组为XPTCP网关装置101的处理对象之外，因此接收分组判定部701将该分组原样传输给内侧NIC104(S1203)，结束一连串的处理(S1204)。

[0247] 步骤S1208中，如果在XPTCP处理对象主文件208中有接收的分组的发送源IP地址、发送源端口编号、目的地IP地址及目的地端口编号的组合(S1208的“是”)，则该分组为XPTCP网关装置101的处理对象，需要改写附加在分组的MAC地址、IP地址及端口编号。因此，接收分组判定部701进一步查看接收的分组的详细。

[0248] 接收分组判定部701判定接收的分组是否为TCP FIN分组(S1209)。

[0249] 判定的结果，如果接收的分组为TCP FIN分组(S1209的“是”)，接收分组判定部701将该TCP FIN分组与索引端口编号一起交给记录删除处理部703。

[0250] 记录删除处理部703如果确认了删除预定列表605中有该TCP FIN分组的索引端口编号，则向内侧NIC地址表209的、该索引端口编号涉及的记录的定时器用计数值字段写入地址表更新计数器213的值(S1210)。

[0251] 其后，记录删除处理部703将TCP FIN分组和索引端口编号交给地址置换部702。

[0252] 地址置换部702参考从接收分组判定部701通过记录删除处理部703交给的索引端口编号和假IPMAC列表204，改写TCP FIN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号(S1211)。具体而言，

[0253] ·将附加在分组的发送源MAC地址改写为第二假MAC地址；

[0254] ·将附加在分组的发送源IP地址改写为第二假IP地址；

[0255] ·将附加在分组的发送源端口编号改写为索引端口编号；

[0256] ·将附加在分组的目的地MAC地址改写为外侧NICMAC地址；

[0257] ·将附加在分组的目的地IP地址改写为外侧NICIP地址；

[0258] ·将附加在分组的目的地端口编号改写为动态端口编号。

[0259] 地址置换部702在进行IP地址等的置换处理后，将该TCP FIN分组发送给TCP/IP协议栈205(S1206)，结束一连串的处理(S1204)。

[0260] 步骤S1209中，如果接收的分组不是TCP FIN分组(S1209的“否”)，则该分组为TCP数据分组。因此，接收分组判定部701将该TCP数据分组与索引端口编号一起交给地址置换部702。

[0261] 地址置换部702参考从接收分组判定部701交给的索引端口编号和假IPMAC列表204，改写TCP数据分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号(S1212)。具体而言，将附加在分组的发送源MAC地址改写为第二假MAC地址，将附加在分组的发送源IP地址改写为第二假IP地址，将附加在分组的发送源端口编号改写为索引端口编号，将附加在分组的目的地MAC地址改写为外侧NICMAC地址，将附加在分组的目的地IP地址改写为外侧NICIP地址，将附加在分组的目的地端口编号改写为动态端口编号。

[0262] 地址置换部702在进行IP地址等的置换处理后，将该TCP数据分组发送给TCP/IP协议栈205(S1206)，结束一连串的处理(S1204)。

[0263] 图13是示出地址变换处理部203的、外侧NIC108中的分组发送处理的动作的流程的流程图。这相当于外侧NIC发送处理部503的动作的流程。

[0264] 若开始处理(S1301)，发送分组判定部最先查看从TCP/IP协议栈205接受的分组的种类和目的地IP地址。

[0265] 在分组的种类为ICMP分组或UDP分组的情况下；在分组的种类为ARP请求分组且探索IP地址不是记在假IPMAC列表204的第二假IP地址的情况下；在分组的种类为TCP分组且目的地IP地址不是记在假IPMAC列表204的第二假IP地址的情况下(S1302的“否”)，这些分组为XPTCP网关装置101未处理的分组。因此，发送分组判定部对该分组不做任何加工，保持原样而通过外侧NIC108进行发送(S1303)，结束一连串的处理(S1304)。

[0266] 步骤S1302中，在从TCP/IP协议栈205接受的分组的种类为TCP分组且目的地IP地址为记在假IPMAC列表204的第二假IP地址的情况下，或者为ARP请求分组且探索IP地址为记在假IPMAC列表204的第二假IP地址的情况下(S1302的“是”)，进一步判定该分组是否为ARP请求分组(S1305)。

[0267] 在是ARP请求分组且探索IP地址为记在假IPMAC列表204的第二假IP地址的情况下(S1305的“是”)，该ARP请求分组是TCP/IP协议栈205要对实际不存在的第二假IP地址发送分组的结果生成的分组。该ARP请求分组并不由外侧NIC108发送，而与第二假IP地址同样地必须以实际不存在的MAC地址即第二假MAC地址生成ARP应答分组并进行回答。因此，发送分组判定部将该ARP请求分组交给ARP应答处理部802。

[0268] ARP应答处理部802若从发送分组判定部接受ARP请求分组，则参考假IPMAC列表，以第二假MAC地址生成ARP应答分组，回送给TCP/IP协议栈205(S1306)，结束一连串的处理

(S1304)。

[0269] 步骤S1305中,在从TCP/IP协议栈205接受的分组为TCP分组且目的地IP地址为记在假IPMAC列表204的第二假IP地址的情况下(S1305的“否”),该分组为XPTCP网关装置101处理的分组,有必要将附加在分组的MAC地址、IP地址及端口编号回写为内侧NIC接收处理部501改写以前的状态。因此,发送分组判定部进一步查看接收的分组的详细。

[0270] 发送分组判定部判定从TCP/IP协议栈205接受的分组是否为TCP SYN分组(S1307)。

[0271] 判定的结果,如果从TCP/IP协议栈205接受的分组为TCP SYN分组(S1307的“是”),则该TCP SYN分组是表示重新生成连接的分组。此时,在TCP/IP协议栈205生成连接之际,作为发送源端口编号自动赋予动态端口编号。有必要将该动态端口编号先存储在外侧NIC地址表210。因此,发送分组判定部将该TCP SYN分组交给动态端口记录处理部803。

[0272] 动态端口记录处理部803在接受了TCP SYN分组时,首先取得TCP SYN分组的发送源端口编号。接着,以记在目的地端口编号的索引端口编号来检索外侧NIC地址表210,向确定的记录的动态端口编号字段写入在之前先取得的TCP SYN分组的发送源端口编号(S1308)。

[0273] 这样,通过先存储附加在表示连接的开始的TCP SYN分组的动态端口编号,能够正确地置换或复原以后经由该连接的分组的IP地址等。

[0274] 动态端口记录处理部803在进行动态端口编号的记录之后,将TCP SYN分组交给地址复原部902。

[0275] 地址复原部902参考在之前动态端口记录处理部803确定的外侧NIC地址表210的记录,复原TCP SYN分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号(S1309)。然后,通过外侧NIC108发送该TCP SYN分组(S1303),结束一连串的处理(S1304)。

[0276] 步骤S1307中,如果从TCP/IP协议栈205接受的分组不是TCP SYN分组(S1307的“否”),则发送分组判定部将该TCP分组交给地址复原部902。

[0277] 地址复原部902以附加在TCP分组的目的地端口编号的索引端口编号来检索外侧NIC地址表210的记录并确定记录,复原TCP分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号(S1309)。然后,通过外侧NIC108发送该TCP SYN分组(S1303),结束一连串的处理(S1304)。

[0278] 图14是示出地址变换处理部203的、内侧NIC104中的分组发送处理的动作的流程的流程图。这相当于内侧NIC发送处理部504的动作的流程。

[0279] 若开始处理(S1401),则发送分组判定部最先查看从TCP/IP协议栈205接受的分组的种类和目的地IP地址。

[0280] 在分组的种类为ICMP分组、ARP分组或UDP分组的情况下;在分组的种类为TCP分组且目的地IP地址不是记在假IPMAC列表204的第一假IP地址的情况下(S1402的“否”),这些分组是XPTCP网关装置101未处理的分组。因此,发送分组判定部对该分组不做任何加工,保持原样而通过内侧NIC104进行发送(S1403),结束一连串的处理(S1404)。

[0281] 步骤S1402中,在从TCP/IP协议栈205接受的分组的种类为TCP分组且目的地IP地址为记在假IPMAC列表204的第一假IP地址的情况下(S1402的“是”),该分组是XPTCP网关装

置101处理的分组，有必要将附加在分组的MAC地址、IP地址及端口编号回写为内侧NIC接收处理部501改写以前的状态。因此，发送分组判定部将该TCP分组交给地址复原部902。

[0282] 地址复原部902以附加在TCP分组的目的地端口编号的索引端口编号来检索内侧NIC地址表209的记录并确定记录，复原TCP分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号(S1405)。然后，通过内侧NIC104发送该TCP SYN分组(S1403)，结束一连串的处理(S1404)。

[0283] [XPTCP网关装置101的动作/XPTCP处理部206的动作]

[0284] 图15是示出XPTCP处理部206的XPTCP处理的流程的流程图。

[0285] XPTCP处理是指对TCP或UDP分组施行传输层中既定认证及加密处理的处理。XPTCP处理的基本技术内容已公开于专利文献1，因此在本实施方式中不做详细说明。取而代之，说明在前述的地址变换处理部203及后述的套接字处理部207中进行的、与套接字的处理相关的内容。

[0286] 若开始处理(S1501)，则事件检测部1001确认是否从套接字处理部207检测到对于内侧NIC104的连接所涉及的accept事件(S1502)。如果检测到accept事件(S1502的“是”)，则事件检测部1001控制套接字操作部1002，取得该accept事件所涉及的、生成的套接字的、套接字存储器区域1004内的地址(S1503)。然后，事件检测部1001起动策略设定部1003。

[0287] 关于该accept事件涉及的套接字，策略设定部1003利用索引端口编号对地址变换处理部203进行策略的查询。地址变换处理部203的策略回答部506以索引端口编号来检索内侧NIC地址表209并确定记录。然后，利用确定的记录的发送源IP地址及端口编号、目的地IP地址及端口编号来检索XPTCP处理对象主文件208，并确定记录，如果取得有关记录的记录编号，向策略设定部1003回答该记录编号。策略设定部1003将得到的记录编号和索引端口编号记录在XPTCP策略表211并进行关联。在该时间点，加密处理部1005以索引端口编号为线索，确定XPTCP处理对象主文件208的记录，从而能够设定加密的策略(S1504)。然后，结束一连串的处理(S1505)。

[0288] 步骤S1502中，如果未能检测到accept事件(S1502的“否”)，则事件检测部1001接着确认是否从TCP/IP协议栈205检测到对于外侧NIC108的连接所涉及的connect应答事件(S1506)。如果检测到connect应答事件(S1506的“是”)，则事件检测部1001控制套接字操作部1002，取得该connect应答事件所涉及的、生成的套接字的、套接字存储器区域1004内的地址(S1507)。

[0289] 接着，事件检测部1001进行共有索引端口编号的、对于内侧NIC104的连接所涉及的套接字与对于外侧NIC108的连接所涉及的套接字之间的关联建立(S1508)。在该时间点，解码处理部1006以索引端口编号为线索，确定XPTCP处理对象主文件208的记录，从而能够设定解码的策略(S1509)。然后，结束一连串的处理(S1505)。

[0290] 由此，从对于内侧NIC104的连接所涉及的套接字取得的流数据，通过加密处理部1005进行加密，加密后的流数据输出到对于外侧NIC108的连接所涉及的套接字。此外相反，从对于外侧NIC108的连接所涉及的套接字取得的流数据，通过解码处理部1006进行解码，解码后的流数据输出到对于内侧NIC104的连接所涉及的套接字。

[0291] 步骤S1506中，如果未能检测到connect应答事件(S1506的“否”)，则事件检测部1001接着确认是否从TCP/IP协议栈205检测到对于外侧NIC108的连接所涉及的close事件

(S1510)。如果检测到close事件(S1510的“是”),则事件检测部1001控制套接字操作部1002,放开该close事件所涉及的、生成的套接字彼此的关联,并且删除XPTCP策略表211的有关记录(S1511)。然后,结束一连串的处理(S1505)。

[0292] 步骤S1510中,如果未能检测到close事件(S1510的“否”),则事件检测部1001不做任何特别地动作。取而代之,加密处理部1005及解码处理部1006从套接字操作部1002接受流数据,基于在XPTCP策略表211确定的加密或解码策略执行加密或解码处理(S1512),套接字操作部1002传输这些处理后的流数据(S1513)。然后,结束一连串的处理(S1505)。

[0293] [XPTCP网关装置101的动作/套接字处理部207的动作]

[0294] 图16是示出套接字处理部207的初始动作的流程的流程图。

[0295] 若开始处理(S1601),则套接字处理部207起动针对预先确定的端口编号的TCP服务器功能(S1602)。此时,面向内侧NIC104作成用于接受要求(request)的套接字(socket函数),在该套接字中定义有接受要求时的端口编号(bind函数)。然后,结束一连串的处理(S1603)。

[0296] 图17是示出套接字处理部207的连接请求传输处理的流程的流程图。

[0297] 套接字处理部207当从TCP/IP协议栈205接受了connect事件时(S1301),通过套接字对内侧NIC104发行表示允许连接的accept事件(S1702)。这是作为服务器的动作。接着套接字处理部207向外侧NIC108发行请求连接的connect request事件(S1703)。这是作为客户端的动作。然后,结束一连串的处理(S1704)。

[0298] [XPTCP网关装置101的动作/地址变换处理部203进行的分组的变化]

[0299] 图18、图19及图20是示出通过XPTCP网关装置101的分组的变化的简略图。

[0300] XPTCP非对应PC103中被赋予第一MAC地址和第一IP地址。

[0301] XPTCP对应服务器107中被赋予第二MAC地址和第二IP地址。

[0302] 若从XPTCP非对应PC103向XPTCP对应服务器107发送分组,则发送分组通过内侧NIC104,到达地址变换处理部203。地址变换处理部203参考内侧NIC地址表209,施行地址变换处理。这样,发送分组变化为地址变换处理完成发送分组。

[0303] 地址变换处理完成发送分组中,目的地IP地址为内侧NIC104的IP地址。因而,TCP/IP协议栈205接受地址变换处理完成发送分组,从分组中按照MAC报头、IP报头、TCP报头的顺序除去报头,连结有效载荷并复原流数据。复原后的流数据通过套接字到达XPTCP处理部。XPTCP处理部对流数据施行既定加密处理。然后,加密后的流数据被供给至面向外侧NIC108作成的套接字。

[0304] TCP/IP协议栈205将加密后的流数据划成既定字节长度,附加TCP报头、IP报头及MAC报头,作成加密及地址变换处理完成发送分组。即,在该时间点作成的分组的目的地IP地址为第二假IP地址,并不是本来的发送目的地即XPTCP对应服务器107的IP地址(第二IP地址)。因此,地址变换处理部参考外侧NIC地址表210,施行地址复原处理。这样,加密及地址变换处理完成发送分组成为加密处理完成发送分组,到达XPTCP对应服务器107。

[0305] 若从XPTCP对应服务器107向XPTCP非对应PC103回送加密处理完成接收分组,则加密处理完成接收分组通过外侧NIC108,到达地址变换处理部203。地址变换处理部203参考外侧NIC地址表210,施行地址变换处理。这样,加密处理完成接收分组变化为加密及地址变换处理完成接收分组。

[0306] 加密及地址变换处理完成接收分组中，目的地IP地址为外侧NIC108的IP地址。因而，TCP/IP协议栈205接受加密及地址变换处理完成接收分组，从分组中按照MAC报头、IP报头、TCP报头的顺序除去报头，连结有效载荷并复原加密流数据。复原后的加密流数据通过套接字后到达XPTCP处理部。XPTCP处理部对流数据施行既定解码处理。然后，解码后的流数据被供给到面向外侧NIC108作成的套接字。

[0307] TCP/IP协议栈205将解码后的流数据划成既定字节长度，附加TCP报头、IP报头及MAC报头，作成地址变换处理完成接收分组。即，在该时间点作成的分组的目的地IP地址为第一假IP地址，并不是本来的发送目的地即XPTCP非对应PC103的IP地址（第一IP地址）。因此，地址变换处理部参考内侧NIC地址表209，施行地址复原处理。这样，地址变换处理完成接收分组成为接收分组，到达XPTCP非对应PC103。

[0308] [XPTCP网关装置101的动作/TCP连接确立序列]

[0309] 图21、图22及图23是XPTCP网关装置101中的TCP连接确立序列的时序图。图21是示出整个时序图的俯视图，图22是示出时序图中前半处理内容的详细图，图23是示出时序图中后半处理内容的详细图。

[0310] 示出与从终端发送TCP SYN分组的情况呼应而在终端与XPTCP网关装置101之间，以及在服务器与XPTCP网关装置101之间各自形成TCP连接为止的、XPTCP网关装置101在时序列上的动作演进。

[0311] XPTCP非对应PC103使web浏览器等的应用程序动作，要与XPTCP对应服务器107连接时，因为应用程序而XPTCP非对应PC103发送TCP SYN分组(S2101)。

[0312] TCP SYN分组通过内侧NIC104到达地址变换处理部203。地址变换处理部203的内侧NIC接收处理部501变换TCP SYN分组的发送源及目的地MAC地址、IP地址及端口编号(S2102)。再者，在该时间点对内侧NIC地址表209追加记录新的记录，能够以索引端口编号确定有关记录。

[0313] 被施行地址变换处理的TCP SYN分组，到达TCP/IP协议栈205。TCP/IP协议栈205辨识套接字处理部207预先作成的对端口编号发送的TCP SYN分组，为了开始连接的作成，对套接字处理部207发行connect事件(S2103)。

[0314] 套接字处理部207通过自身的服务器功能，对TCP/IP协议栈205发行针对connect事件(连接请求)的accept事件(允许连接)(S2104)。

[0315] XPTCP处理部206挂上(hook)该accept事件，辨识面向内侧NIC104的连接的形成开始的情况(S2105)。这样，XPTCP处理部206对于地址变换处理部203，查询伴随索引端口编号而适用于该连接的策略(S2106)。对于该查询地址变换处理部203参考XPTCP处理对象主文件208和内侧NIC地址表209，回答XPTCP处理对象主文件208的记录编号(S2107)。XPTCP处理部206向XPTCP策略表211登记记录编号和索引端口编号并加以关联，设定解码处理部1006的策略(S2108)。

[0316] 在步骤S2104中发行的accept事件到达TCP/IP协议栈205。TCP/IP协议栈205接受accept事件，生成TCP ACK/SYN分组(S2109)。TCP ACK/SYN分组到达地址变换处理部203。地址变换处理部203的内侧NIC发送处理部504复原TCP ACK/SYN分组的发送源及目的地MAC地址、IP地址及端口编号(S2110)。

[0317] TCP ACK/SYN分组通过内侧NIC104到达XPTCP非对应PC103。XPTCP非对应PC103接

受TCP ACK/SYN分组，并以TCP ACK分组进行应答(S2111)。

[0318] TCP ACK分组通过内侧NIC104到达地址变换处理部203。地址变换处理部203的内侧NIC接收处理部501变换TCP ACK分组的发送源及目的地MAC地址、IP地址及端口编号(S2112)。

[0319] 施行地址变换处理的TCP ACK分组到达TCP/IP协议栈205。TCP/IP协议栈205根据TCP ACK分组的到达，辨识确立连接的情况(S2113)。之后，在该连接中进行TCP数据分组的收发。

[0320] 套接字处理部207在步骤S2104中向内侧NIC104发行作为服务器功能的accept事件后，向外侧NIC108发行作为客户端功能表示连接请求的connect request事件(S2114)。

[0321] connect request事件到达TCP/IP协议栈205。TCP/IP协议栈205接受connect request事件，生成ARP请求分组(S2115)。

[0322] ARP请求分组到达地址变换处理部203。地址变换处理部203的外侧NIC发送处理部503生成针对ARP请求分组的ARP应答分组，回送给TCP/IP协议栈205(S2116)。

[0323] TCP/IP协议栈205在接受到ARP应答分组时，由于完成了生成与步骤S2114中的connect request事件对应的TCP SYN分组的准备，所以生成TCP SYN分组(S2117)。

[0324] 在步骤S2117中生成的TCP SYN分组到达地址变换处理部203。地址变换处理部203的外侧NIC发送处理部503变换TCP SYN分组的发送源及目的地MAC地址、IP地址及端口编号(S2118)。此外，在该时间点对于外侧NIC地址表210的有关记录，作为TCP SYN分组的发送源端口编号，记录通过TCP/IP协议栈205自动附加的动态端口编号。

[0325] TCP SYN分组通过外侧NIC108到达XPTCP对应服务器107。XPTCP对应服务器107接受TCP SYN分组，以TCP ACK/SYN分组进行应答(S2119)。

[0326] TCP ACK/SYN分组通过外侧NIC108到达地址变换处理部203。地址变换处理部203的外侧NIC接收处理部502变换TCP ACK/SYN分组的发送源及目的地MAC地址、IP地址及端口编号(S2120)。

[0327] 已施行地址变换处理的TCP ACK/SYN分组到达TCP/IP协议栈205。TCP/IP协议栈205接受TCP ACK/SYN分组，以TCP ACK分组进行应答(S2121)。此时，TCP/IP协议栈205将connect应答事件通知到作为客户端程序的套接字处理部207。

[0328] XPTCP处理部206挂上该connect应答事件，辨识面向外侧NIC108的连接的形成开始的情况(S2122)。这样，XPTCP处理部206对于地址变换处理部203查询伴随索引端口编号而适用于该连接的策略(S2123)。对于该查询，地址变换处理部203参考XPTCP处理对象主文件208和内侧NIC地址表209，回答XPTCP处理对象主文件208的记录编号(S2124)。XPTCP处理部206向XPTCP策略表211登记记录编号和索引端口编号并加以关联，设定加密处理部1005的策略(S2125)。

[0329] 在步骤S2121中从TCP/IP协议栈205发行的TCP ACK分组到达地址变换处理部203。地址变换处理部203的外侧NIC发送处理部503复原TCP ACK分组的发送源及目的地MAC地址、IP地址及端口编号(S2126)。

[0330] TCP ACK分组通过外侧NIC108到达XPTCP对应服务器107。XPTCP对应服务器107根据TCP ACK分组的到达，辨识确立连接的情况(S2127)。之后，在该连接中进行TCP数据分组的收发。

[0331] [XPTCP网关装置101的动作/TCP数据传输序列]

[0332] 图24是XPTCP网关装置101中的、TCP数据传输序列的时序图。示出与从终端发送TCP数据分组的情况呼应而在终端与XPTCP网关装置101之间，以及在服务器与XPTCP网关装置101之间各自形成的TCP连接中通过TCP数据分组时的、XPTCP网关装置101在时序列上的动作演进。

[0333] XPTCP非对应PC103使web浏览器等的应用程序动作，要向XPTCP对应服务器107发送数据时，因为应用程序而XPTCP非对应PC103发送TCP数据分组(S2401)。

[0334] TCP数据分组通过内侧NIC104到达地址变换处理部203。地址变换处理部203的内侧NIC接收处理部501变换TCP数据分组的发送源及目的地MAC地址、IP地址及端口编号(S2402)。

[0335] 已施行地址变换处理的TCP数据分组，到达TCP/IP协议栈205。TCP/IP协议栈205除去TCP数据分组的报头，连结TCP数据分组有效载荷，复原为流数据(S2403)。

[0336] 流数据被XPTCP处理部206施行加密处理，传输到外侧NIC108的套接字(S2404)。

[0337] 已施行加密处理的流数据，到达TCP/IP协议栈205。TCP/IP协议栈205按每个既定字节长度分割流数据后，附加报头，变换为TCP数据分组(S2405)。

[0338] TCP数据分组到达地址变换处理部203。地址变换处理部203的外侧NIC发送处理部503变换TCP数据分组的发送源及目的地MAC地址、IP地址及端口编号(S2406)。

[0339] 已施行地址复原处理的TCP数据分组，通过外侧NIC108而到达XPTCP对应服务器107(S2407)。XPTCP对应服务器107接受TCP数据分组，进行既定处理后，向XPTCP非对应PC103发送作为回复数据的TCP数据分组(S2408)。

[0340] TCP数据分组通过外侧NIC108到达地址变换处理部203。地址变换处理部203的外侧NIC接收处理部502变换TCP数据分组的发送源及目的地MAC地址、IP地址及端口编号(S2409)。

[0341] 已施行地址变换处理的TCP数据分组，到达TCP/IP协议栈205。TCP/IP协议栈205除去TCP数据分组的报头，连结TCP数据分组有效载荷，复原为流数据(S2410)。

[0342] 流数据被XPTCP处理部206施行解码处理，传输到内侧NIC104的套接字(S2411)。

[0343] 已施行解码处理的流数据，到达TCP/IP协议栈205。TCP/IP协议栈205按每个既定字节长度分割流数据后，附加报头，变换为TCP数据分组(S2412)。

[0344] TCP数据分组到达地址变换处理部203。地址变换处理部203的内侧NIC发送处理部504变换TCP数据分组的发送源及目的地MAC地址、IP地址及端口编号(S2413)。

[0345] 已施行地址复原处理的TCP数据分组，通过内侧NIC104到达XPTCP非对应PC103(S2414)。

[0346] [XPTCP网关装置101的动作/TCP断开序列]

[0347] 图25、图26及图27是XPTCP网关装置101中的、TCP断开序列的时序图。图25是示出整个时序图的俯视图，图26是示出时序图中前半处理内容的详细图，图27是示出时序图中后半处理内容的详细图。

[0348] 示出与从终端发送TCP FIN分组的情况呼应而在终端与XPTCP网关装置101之间，以及在服务器与XPTCP网关装置101之间各自形成的TCP连接结束(close:关闭)为止的、XPTCP网关装置101在时序列上的动作演进。

[0349] XPTCP非对应PC103使web浏览器等的应用程序动作，对XPTCP对应服务器107请求既定数据，如果得到该请求的数据，则因为应用程序而XPTCP非对应PC103发送TCP FIN分组(S2501)。

[0350] TCP FIN分组通过内侧NIC104到达地址变换处理部203。地址变换处理部203的内侧NIC接收处理部501变换TCP FIN分组的发送源及目的地MAC地址、IP地址及端口编号(S2102)。此外，在该时间点向删除预定列表605追加记录索引端口编号。

[0351] 已施行地址变换处理的TCP FIN分组到达TCP/IP协议栈205。TCP/IP协议栈205辨识套接字处理部207预先作成的对端口编号发送的TCP FIN分组，为了向作为服务器程序的套接字处理部207通知连接结束，对套接字处理部207发行close事件(S2503)。

[0352] 套接字处理部207在步骤S2503中接受对于内侧NIC104为服务器功能的close事件后，向外侧NIC108发行作为表示断开请求的close request事件作为客户端功能(S2504)。

[0353] close request事件到达TCP/IP协议栈205。TCP/IP协议栈205接受close request事件，生成TCP FIN分组(S2505)。

[0354] 在步骤S2505生成的TCP FIN分组到达地址变换处理部203。地址变换处理部203的外侧NIC发送处理部503变换TCP FIN分组的发送源及目的地MAC地址、IP地址及端口编号(S2506)。

[0355] TCP FIN分组通过外侧NIC108到达XPTCP对应服务器107(S2507)。XPTCP对应服务器107接受TCP FIN分组，如果判断为发送了全部应该对XPTCP非对应PC103发送的数据，则发送TCP ACK/FIN分组(S2508)。

[0356] TCP ACK/FIN分组通过外侧NIC108到达地址变换处理部203。地址变换处理部203的外侧NIC接收处理部502变换TCP ACK/FIN分组的发送源及目的地MAC地址、IP地址及端口编号(S2509)。

[0357] 已施行地址变换处理的TCP ACK/FIN分组到达TCP/IP协议栈205。TCP/IP协议栈205接受TCP ACK/FIN分组，以TCP ACK分组进行应答(S2510)。此时，TCP/IP协议栈205将close应答事件通知给作为客户端程序的套接字处理部207。

[0358] XPTCP处理部206挂上该close应答事件，解除面向外侧NIC108的连接和面向内侧NIC104的连接之间的关联(S2511)。

[0359] 在步骤S2510中通过TCP/IP协议栈205生成的TCP ACK分组，到达地址变换处理部203。地址变换处理部203的外侧NIC发送处理部503变换TCP ACK分组的发送源及目的地MAC地址、IP地址及端口编号(S2512)。

[0360] TCP ACK分组通过外侧NIC108到达XPTCP对应服务器107。XPTCP对应服务器107接受TCP ACK分组，辨识该分组所涉及的连接完成断开的(关闭的)情况(S2513)。

[0361] 另一方面，在步骤S2510中通过TCP/IP协议栈205生成的close应答事件到达套接字处理部207。套接字处理部207在检测到close应答事件时，辨识对于面向外侧NIC108的连接的TCP FIN分组过来的情况。在该时间点，也能执行面向对应的内侧NIC104的连接的断开处理。因此，在步骤S2503中作为对于TCP/IP协议栈205送出的close事件的应答，向TCP/IP协议栈205送出意味着允许的accept事件(S2514)。

[0362] 在步骤S2514中套接字处理部207送出的accept事件到达TCP/IP协议栈205。TCP/IP协议栈205接受accept事件，生成TCP ACK/FIN分组(S2515)。TCP ACK/FIN分组到达地址

变换处理部203。地址变换处理部203的内侧NIC发送处理部504复原TCP ACK/FIN分组的发送源及目的地MAC地址、IP地址及端口编号(S2516)。

[0363] TCP ACK/FIN分组通过内侧NIC104到达XPTCP非对应PC103。XPTCP非对应PC103接受TCP ACK/FIN分组,以TCP ACK分组进行应答(S2517)。

[0364] TCP ACK分组通过内侧NIC104到达地址变换处理部203。地址变换处理部203的内侧NIC接收处理部501变换TCP ACK分组的发送源及目的地MAC地址、IP地址及端口编号(S2518)。

[0365] 已施行地址变换处理的TCP ACK分组到达TCP/IP协议栈205。TCP/IP协议栈205根据TCP ACK分组的到达,辨识连接完成断开的情况(S2519)。

[0366] 另一方面,在步骤S2509进行地址变换后,地址变换处理部将地址表更新计数器的值写入内侧NIC地址表209及外侧NIC地址表210的定时器用计数值字段(S2520)。表更新处理部505定期地监视内侧NIC地址表209及外侧NIC地址表210的计数值字段,如果经过了既定时间,则删除内侧NIC地址表209及外侧NIC地址表210的有关记录(S2521、S2522)。

[0367] 此外,断开TCP连接的单元并不只是TCP FIN分组。为了在陷入应用程序的冻结(freeze)等、异常状态时强制断开TCP连接,存在TCP RST分组。在产生TCP RST分组时的断开序列,在图25、图26及图27的由虚线包围的范围的处理会发生变化,但详细从略。

[0368] [总结]

[0369] 从XPTCP非对应PC102接收的分组P1402,与内侧NIC104及外侧NIC108的IP地址无关。因此,以分组P1402的状态,TCP/IP协议栈205无法进行既定分组的处理。因此,先暂时在内侧NIC地址表209的记录中,记录附加在分组P1402的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号。进而,为了在后面进行回写而以连号的方式赋予成为索引的端口编号。然后,为使TCP/IP协议栈205能够进行分组的接收处理,将分组P1402改写为设为"从具有第一假IP地址的架空的主机(host),向内侧NIC的IP地址发送的分组"的分组P1405。

[0370] 再者,此时,对发送源端口编号赋予索引PORT,目的地端口编号并不变更。大部分情况下,目的地端口编号是周知的被称为公认端口(well known port)的特定的端口编号。此外,XPTCP也向特定的服务而安装。XPTCP有必要施行按每个服务不同的加密处理,必须以目的地端口编号区别服务,因此内侧NIC接收处理部501在改写附加在分组的发送源及目的地MAC地址、IP地址及端口编号时,仅有目的地端口编号不变更。

[0371] 如以上说明地,XPTCP网关装置101以内部的TCP/IP协议栈205暂时处理所接收的分组的方式,改写所接收的附加在分组的发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址。然后,在即将发送之前再次回写发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址。因此,XPTCP网关装置101完全不需要对已有网络环境的设定变更,只是以夹着XPTCP网关装置101的方式连接到通信路径上,就能容易地提供XPTCP功能。

[0372] 而且作为附加效果,从连接在XPTCP网关装置101的所有终端、服务器是不能辨识XPTCP网关装置101。连PING等的ICMP分组也都会原样传输,因此XPTCP网关装置101作为网络上完全看不到的装置起作用。

[0373] 而且更进一步的附加效果,XPTCP网关装置101的在内侧NIC104及外侧NIC108设定的IP地址,不干涉与XPTCP网关装置101连接的所有主机。即,在内侧NIC104及外侧NIC108设

定的IP地址，即便设定与XPTCP网关装置101连接的子网毫无关系的IP地址，或者为与连接的主机重复的IP地址，也完全没有问题。全部的分组在XPTCP网关装置101内部被施行地址变换，发送时地址被回写，因此在内侧NIC104及外侧NIC108设定的IP地址不会出现在网络之外。在内侧NIC104及外侧NIC108设定的IP地址，除了回送地址、组播地址等的特殊地址以外，设定为任何地址都可以。

[0374] ［应用例］

[0375] 本实施方式所涉及的XPTCP网关装置101可考虑如下的应用例。

[0376] (1)XPTCP网关装置101能够容易安装服务器功能。例如，为了提供用于编辑XPTCP处理对象主文件的用户接口而使web服务器程序运行，预先对应特定的端口编号。作为一例，设为使用称为10030的端口编号。

[0377] XPTCP处理部206在目的地端口编号为该10030的情况下，不施行加密处理，原样交给web服务器程序。通过这样构成XPTCP处理部206，XPTCP网关装置101能够容易安装服务器功能。

[0378] (2)地址变换处理部203采用以内侧NIC地址表209和外侧NIC地址表210这两个表格来改写发送源及目的地MAC地址、IP地址及端口编号的安装方式是有理由的。

[0379] 若改写外侧NIC地址表210的目的地IP地址字段，则终端能够与意图的IP地址不同的IP地址的服务器进行通信。

[0380] 图28是说明XPTCP网关装置101中改写发送的分组的目的地IP地址的应用方式的简略图。

[0381] 对于终端2801赋予称为“A”的IP地址。现在，当终端2801想要与被赋予称为“B”的IP地址的服务器2802连接时，设为发送分组P2803。分组P2803的发送源IP地址为“A”，目的地IP地址为“B”。

[0382] XPTCP网关装置101的内侧NIC地址表209有必要能够忠实地再现“A”和“B”这样的对应关系，因此记录保持原样的IP地址。

[0383] 但是，外侧NIC地址表210也可以不一定能够忠实地再现“A”和“B”这一对应关系。现在，若将目的地IP地址改写为“C”，则从XPTCP网关装置101送出的分组P2804中，发送源IP地址为“A”，目的地IP地址成为“C”。这样，分组P2804到达IP地址为“C”的服务器2805。

[0384] 如此，XPTCP网关装置101通过改写登记在外侧NIC地址表210的目的地IP地址，能够将目的地IP地址变换为终端2801没有掌握的目的地。应用该动作，通过将XPTCP网关装置101以两台以上连成一串构成，能够容易构筑VPN(虚拟专用网：Virtual Private Network)。

[0385] (3)地址变换处理部203采用以内侧NIC地址表209和外侧NIC地址表210这两个表改写发送源及目的地MAC地址、IP地址及端口编号的安装方式是有理由的。

[0386] 若改写外侧NIC地址表210的发送源IP地址字段，则能够对存在服务器一侧的存有恶意的第三者隐蔽终端2801的真正的IP地址。

[0387] 图29是说明XPTCP网关装置101中、改写发送的分组的发送源IP地址的应用方式的简略图。

[0388] 对终端2901赋予称为“A”的IP地址。现在，当终端2901想要与赋予称为“B”的IP地址的服务器2902连接时，设为发送分组P2903。分组P2903的发送源IP地址为“A”，目的地IP

地址为“B”。

[0389] XPTCP网关装置101的内侧NIC地址表209有必要能够忠实地再现“A”和“B”的对应关系，因此记录有保持原样的IP地址。

[0390] 但是，外侧NIC地址表210也可以不一定能够忠实地再现“A”和“B”的对应关系。现在，若将发送源IP地址改写为“D”，则从XPTCP网关装置101送出的分组P2904中，发送源IP地址为“D”，目的地IP地址成为“B”。这样，从服务器2902来看犹如从发送源IP地址为“D”的虚拟终端2905发送，因此能够隐蔽IP地址“A”的终端2901的存在。

[0391] 如此，XPTCP网关装置10通过改写登记在外侧NIC地址表210的发送源IP地址，能够对存有恶意的第三者隐蔽发送源IP地址。

[0392] (4)加密处理部1005对于TCP/IP协议栈205从TCP数据分组抽取有效载荷部分并复原后的流数据，施行加密处理。该加密处理不一定限于加密流数据整体。

[0393] 例如，在周知的TELNET(TCP端口23号)的情况下，需要全部加密流数据。

[0394] 但是，例如在周知的SMTP(简单邮件传送协议(Simple Mail Transfer Protocol):TCP端口25号)的情况下，有可能发送的邮件在SMTP服务器来回传输。此时，全部的SMTP服务器对应于XPTCP的认证及加密处理是很困难的。因此，使发送源的终端仅与最终接收一侧的主机的认证及加密处理对应，加密的对象仅设为SMTP消息的正文。如众所周知地，SMTP消息将一行的空换行作为分隔符分为报头和正文，对报头追加记录邮件经由SMTP服务器等的主机时记录的信息(Received:报头)。

[0395] 本实施方式的加密处理部1005也优选包含：在SMTP、HTTP等、能将流数据分离为报头和正文的协议的情况下等，按照协议只对加密的对象正文而不是对全部流数据进行的处理。

[0396] 在本实施方式公开了网关装置。

[0397] 为了最大限度地有效活用标准搭载于已有的网络OS的TCP/IP协议栈205的功能，并且通过追加必要的最小限度的程序来实现XPTCP网关装置101，施行“欺骗”TCP/IP协议栈205的处理。为使TCP/IP协议栈205能够处理应该与分配给XPTCP网关装置101的IP地址无关的分组，预先在内侧NIC地址表209及外侧NIC地址表210记录附加在分组的发送源MAC地址、发送源IP地址、发送源端口编号、目的地MAC地址、目的地IP地址及目的地端口编号。进而，将接收的附加在分组的发送源MAC地址及发送源IP地址改写为伪MAC地址及伪IP地址，将目的地MAC地址及目的地IP地址改写为分配给XPTCP网关装置101的IP地址及MAC地址后，提供给TCP/IP协议栈205。

[0398] 而且，要在向本来的发送目的地发送分组时，以从分配给XPTCP网关装置101的IP地址及MAC地址回送到伪MAC地址及伪IP地址的方式，欺骗TCP/IP协议栈205，将从TCP/IP协议栈205发送的分组的发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址回写为记录在之前改写的表格的本来的地址，向本来的发送目的地发送。

[0399] 这样XPTCP网关装置101中，改写已接收的附加在分组的发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址，以使内部的TCP/IP协议栈205暂时处理接收的分组。然后，即将发送之前再次回写发送源MAC地址、发送源IP地址、目的地MAC地址及目的地IP地址。因此，XPTCP网关装置101完全不需要变更已有的网络环境的设定，仅仅在通信路径上以夹着XPTCP网关装置101的方式进行连接，就能够容易提供XPTCP功能。

[0400] 以上，说明了本发明的实施方式例，但本发明并不限定于上述实施方式例，只要不超出权利要求书记载的本发明的要旨，将涵盖其他的变形例、应用例。

[0401] 引用符号的说明

[0402] 101…XPTCP网关装置，102…XPTCP非对应PC，103…XPTCP非对应PC，104…内侧NIC，105…XPTCP非对应PC，106…XPTCP对应PC，107…XPTCP对应服务器，108…外侧NIC，109…XPTCP非对应网络，110…XPTCP对应网络，201…初始设定部，202…网络设定信息存储器，203…地址变换处理部，204…假IPMAC列表，205…TCP/IP协议栈，206…XPTCP处理部，207…套接字处理部，208…XPTCP处理对象主文件，209…内侧NIC地址表，210…外侧NIC地址表，211…XPTCP策略表，212…TCP端口编号存储器，213…地址表更新计数器，401…IP报头，402…MAC报头，403…TCP报头，404…UDP报头，501…内侧NIC接收处理部，502…外侧NIC接收处理部，503…外侧NIC发送处理部，504…内侧NIC发送处理部，505…表更新处理部，506…策略回答部，601…接收分组判定部，602…地址置换部，603…连接登记处理部，604…记录删除准备处理部，605…删除预定列表，701…接收分组判定部，702…地址置换部，703…记录删除处理部，801…发送分组判定部，802…ARP应答处理部，803…动态端口记录处理部，804…地址复原部，901…发送分组判定部，902…地址复原部，1001…事件检测部，1002…套接字操作部，1003…策略设定部，1004…套接字存储器区域，1005…加密处理部，1006…解码处理部，2801…终端，2802…服务器，2805…服务器，2901…终端，2902…服务器，2905…虚拟终端。

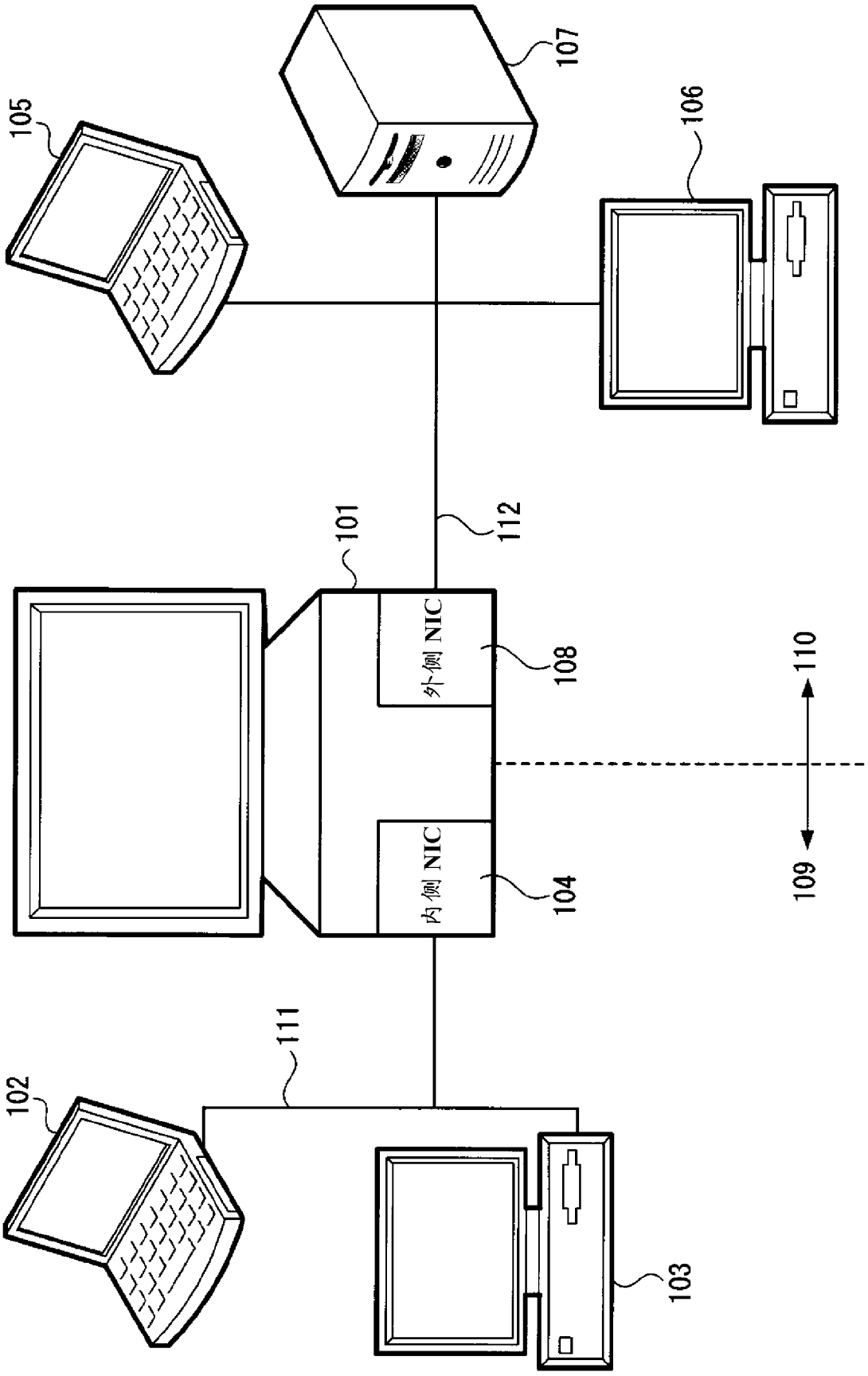


图 1

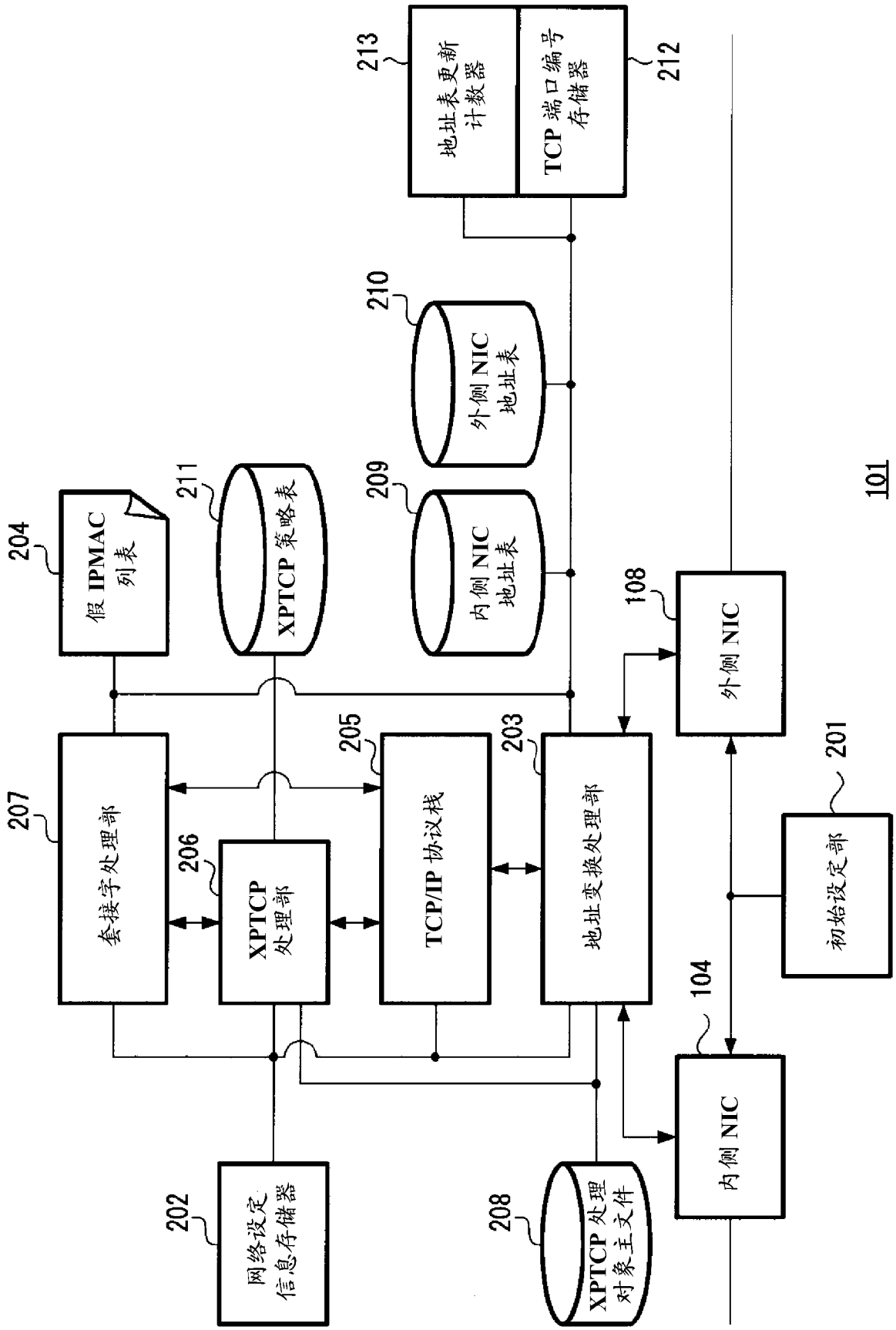

213
地址表更新计数器
212
TCP 端口编号存储器
210
外侧 NIC 地址表
211
XPTCP 策略表
209
内侧 NIC 地址表
204
假 IPMAC 列表
101
108
外侧 NIC
207
套接字处理部
205
TCP/IP 协议栈
203
地址变换处理部
206
XPTCP 处理部
201
初始设定部
104
内侧 NIC
202
网络设定信息存储器
208
XPTCP 处理对象主文件

图 2

209

协议种类（TCP/UDP）
发送源 MAC 地址
发送源 IP 地址
发送源端口编号
目的地 MAC 地址
目的地 IP 地址
目的地端口编号
索引用端口编号
定时器用计数值

210

协议种类（TCP/UDP）
发送源 MAC 地址
发送源 IP 地址
发送源端口编号
目的地 MAC 地址
目的地 IP 地址
目的地端口编号
索引用端口编号
动态端口编号
定时器用计数值

211

协议种类（TCP/UDP）
索引用端口编号
记录编号

202

内侧 NICMAC 地址
内侧 NICIP 地址
外侧 NICMAC 地址
外侧 NICIP 地址

204

内侧 NICIP 地址
第一假 MAC 地址
第一假 IP 地址
外侧 NICIP 地址
第二假 MAC 地址
第二假 IP 地址

208

记录编号
协议种类（TCP/UDP）
发送源 IP 地址
发送源端口编号
目的地 IP 地址
目的地端口编号
密码种类其他

图 3

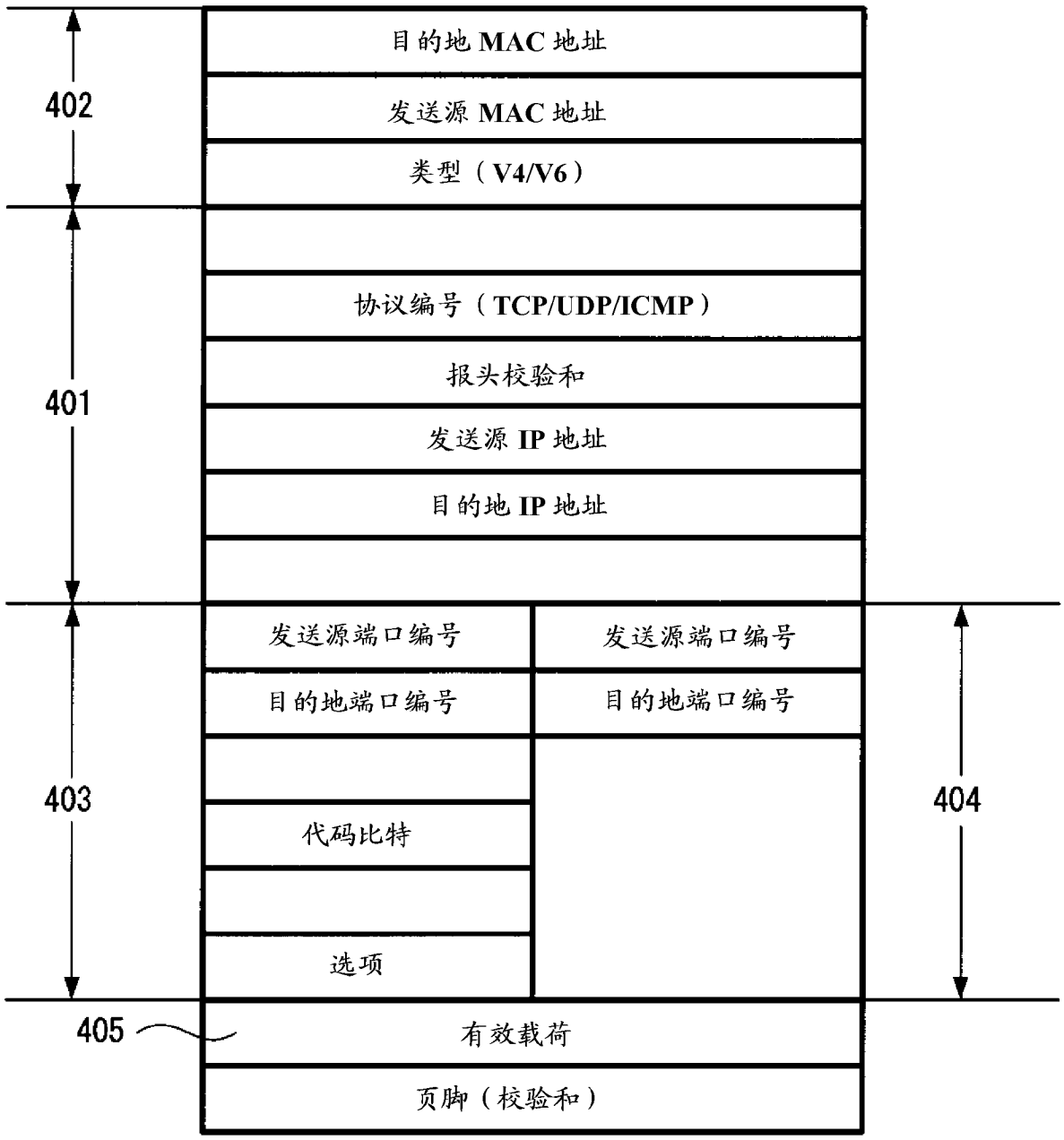

402
401
403
404
405
目的地 MAC 地址
发送源 MAC 地址
类型（V4/V6）
协议编号（TCP/UDP/ICMP）
报头校验和
发送源 IP 地址
目的地 IP 地址
发送源端口编号
发送源端口编号
目的地端口编号
目的地端口编号
代码比特
选项
有效载荷
页脚（校验和）

图 4

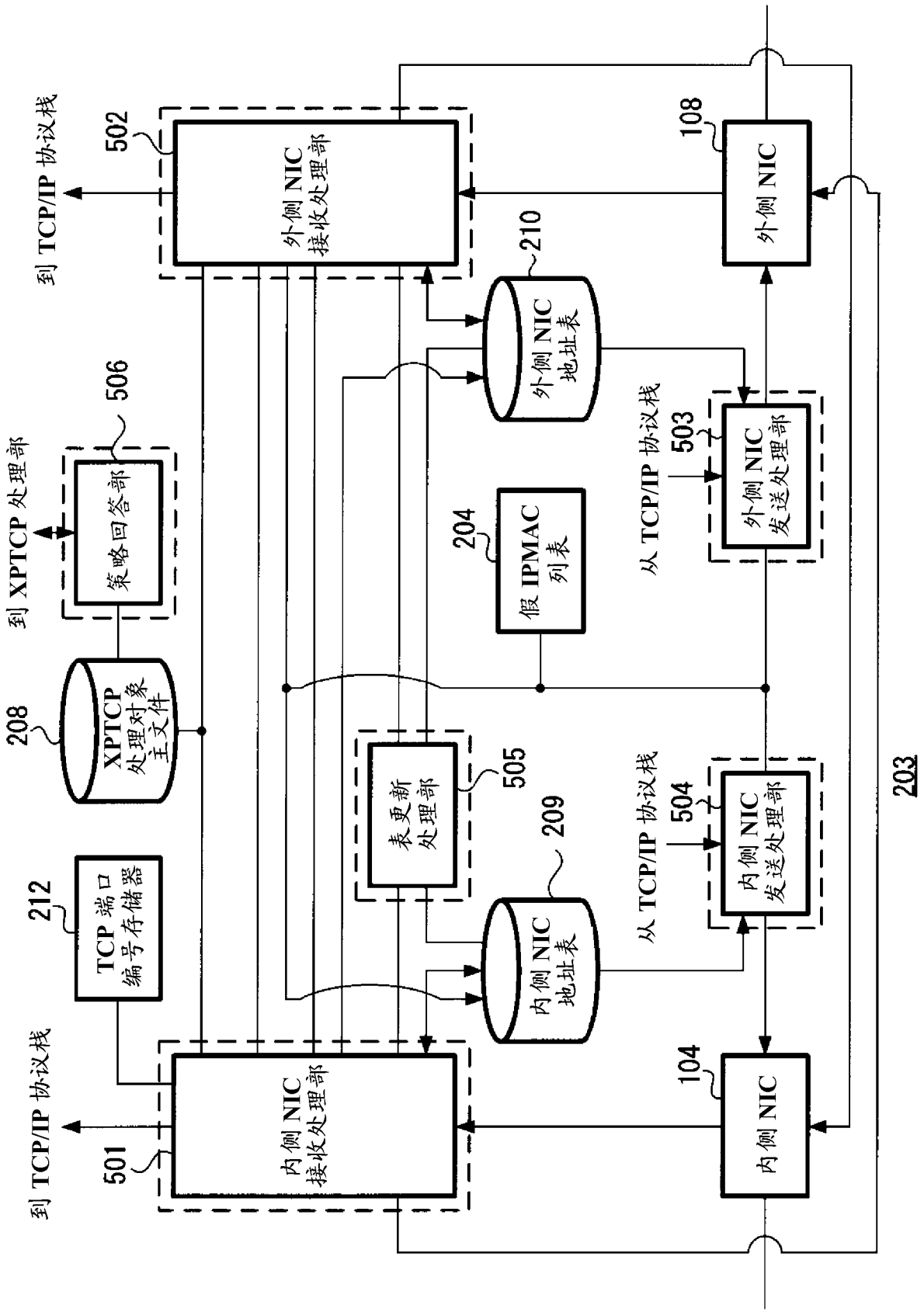

到 TCP/IP 协议栈
502
外侧 NIC
接收处理部
108
外侧 NIC
210
外侧 NIC
地址表
到 XPTCP 处理部
506
策略回答部
从 TCP/IP 协议栈
503
外侧 NIC
发送处理部
204
假 IPMAC
列表
208
XPTCP
处理对象
主文件
505
表更新
处理部
209
212
TCP 端口
编号存储器
内侧 NIC
地址表
从 TCP/IP 协议栈
504
内侧 NIC
发送处理部
203
到 TCP/IP 协议栈
501
内侧 NIC
接收处理部
104
内侧 NIC

图 5

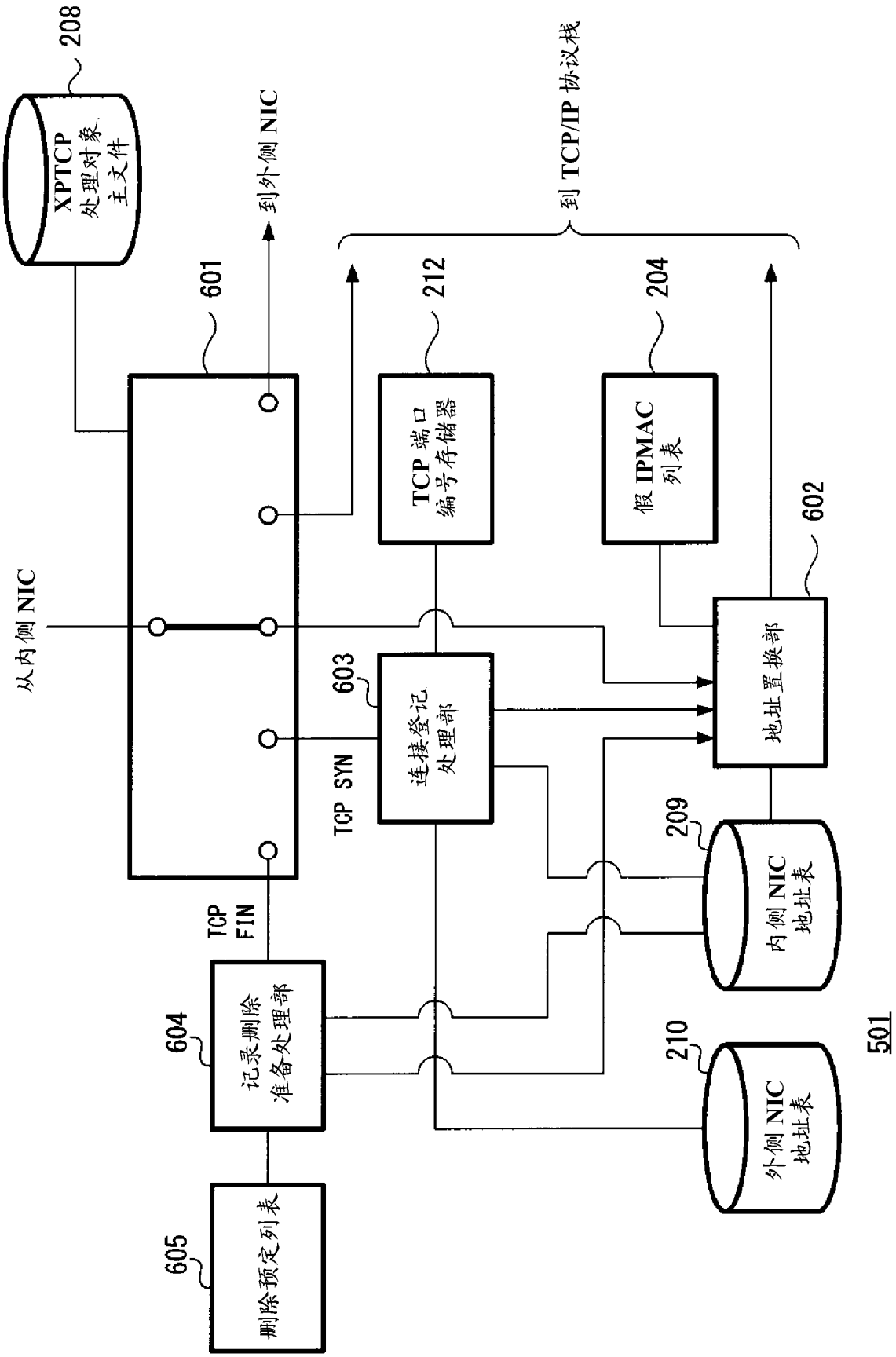

208
XPTCP
处理对象
主文件
到外侧 NIC
到 TCP/IP 协议栈
601
212
204
602
从内侧 NIC
TCP 端口
编号存储器
假 IPMAC
列表
603
连接登记
处理部
地址置换部
TCP SYN
209
内侧 NIC
地址表
TCP
FIN
604
记录删除
准备处理部
210
外侧 NIC
地址表
501
605
删除预定列表

图 6

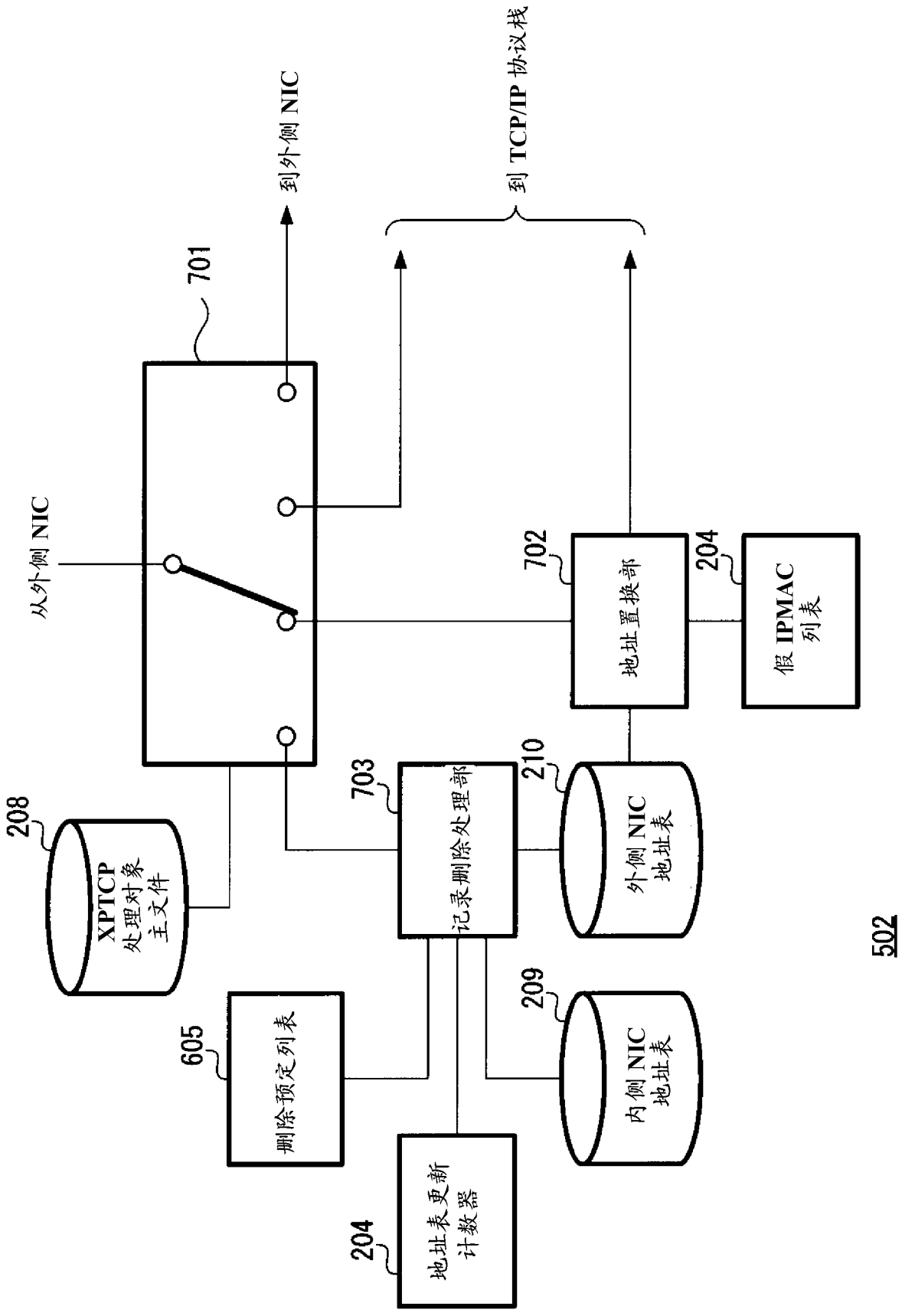

到外侧 NIC
到 TCP/IP 协议栈
701
从外侧 NIC
702
地址置换部
204
假 IPMAC 列表
208
XPTCP 处理对象主文件
703
记录删除处理部
210
外侧 NIC 地址表
605
删除预定列表
209
内侧 NIC 地址表
204
地址表更新计数器
502

图 7

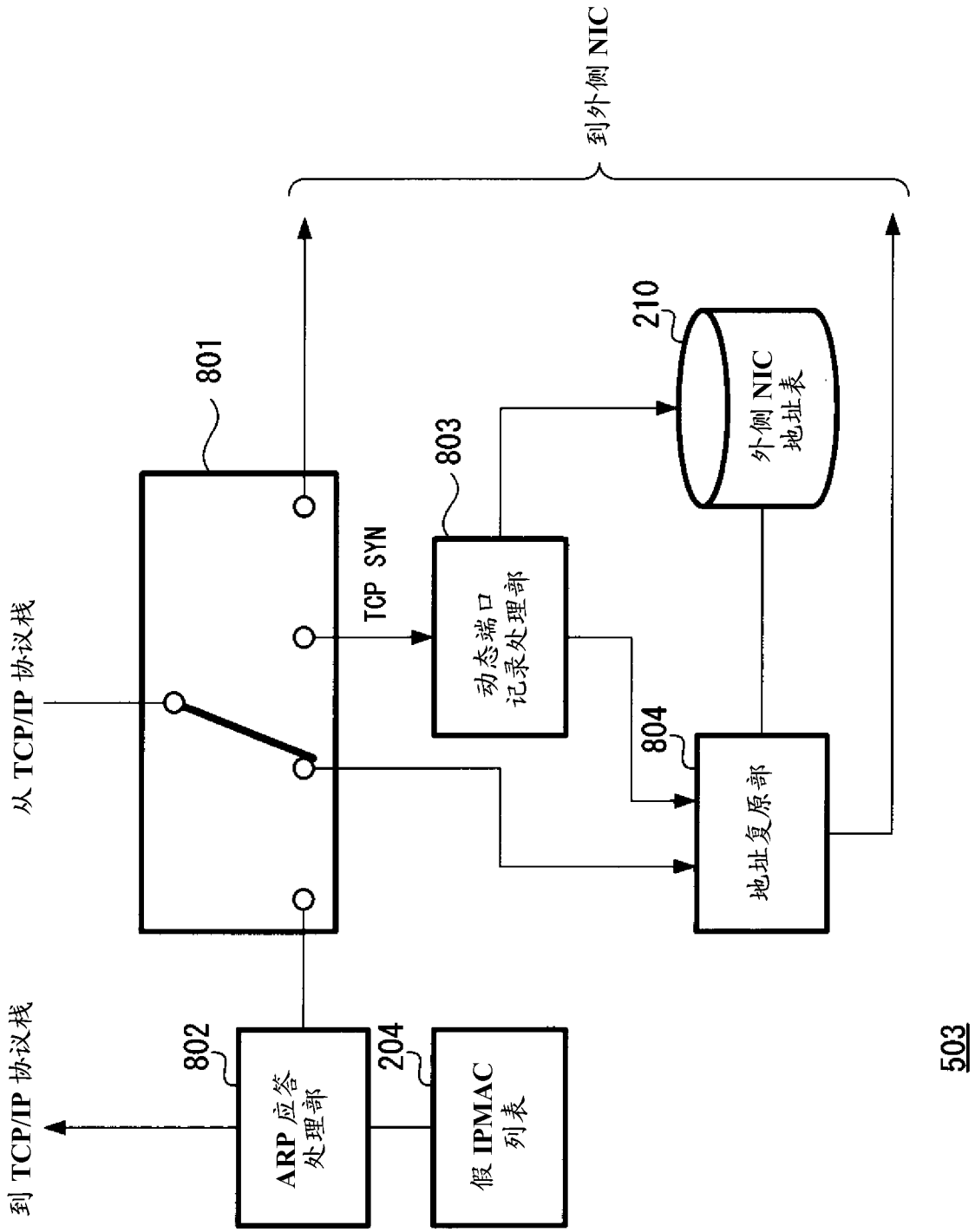

到外侧 NIC
210
外侧 NIC
地址表
801
803
TCP SYN
动态端口
记录处理部
804
地址复原部
从 TCP/IP 协议栈
到 TCP/IP 协议栈
802
ARP 应答
处理部
204
假 IPMAC
列表
503

图 8

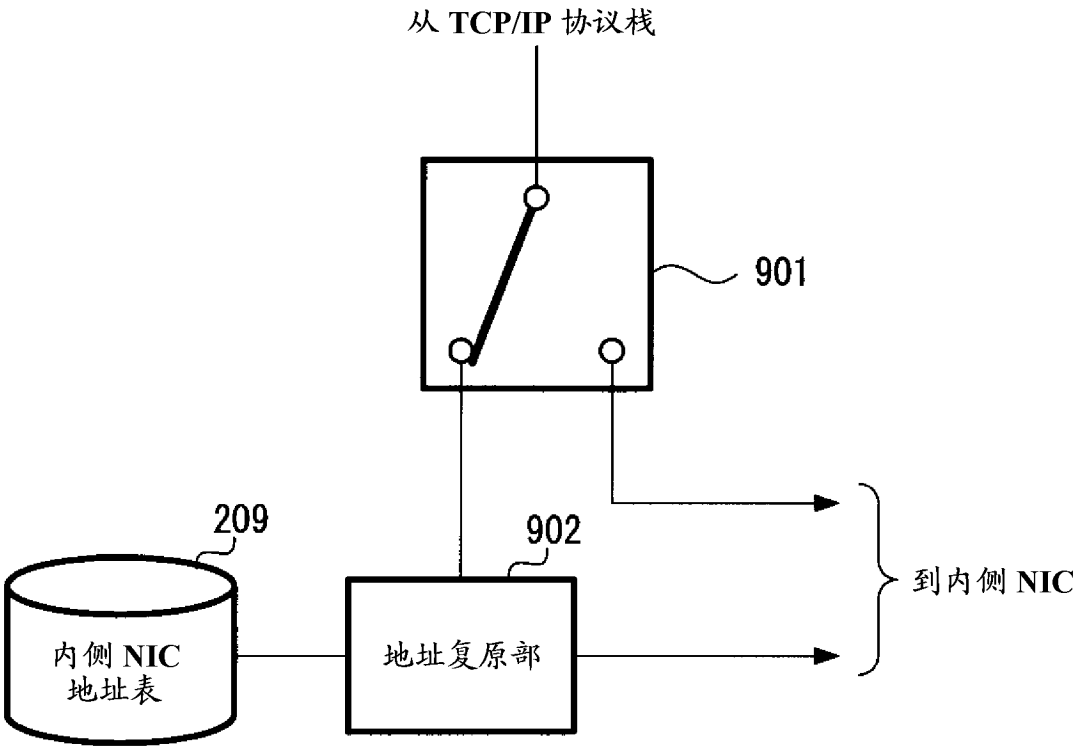


图 9

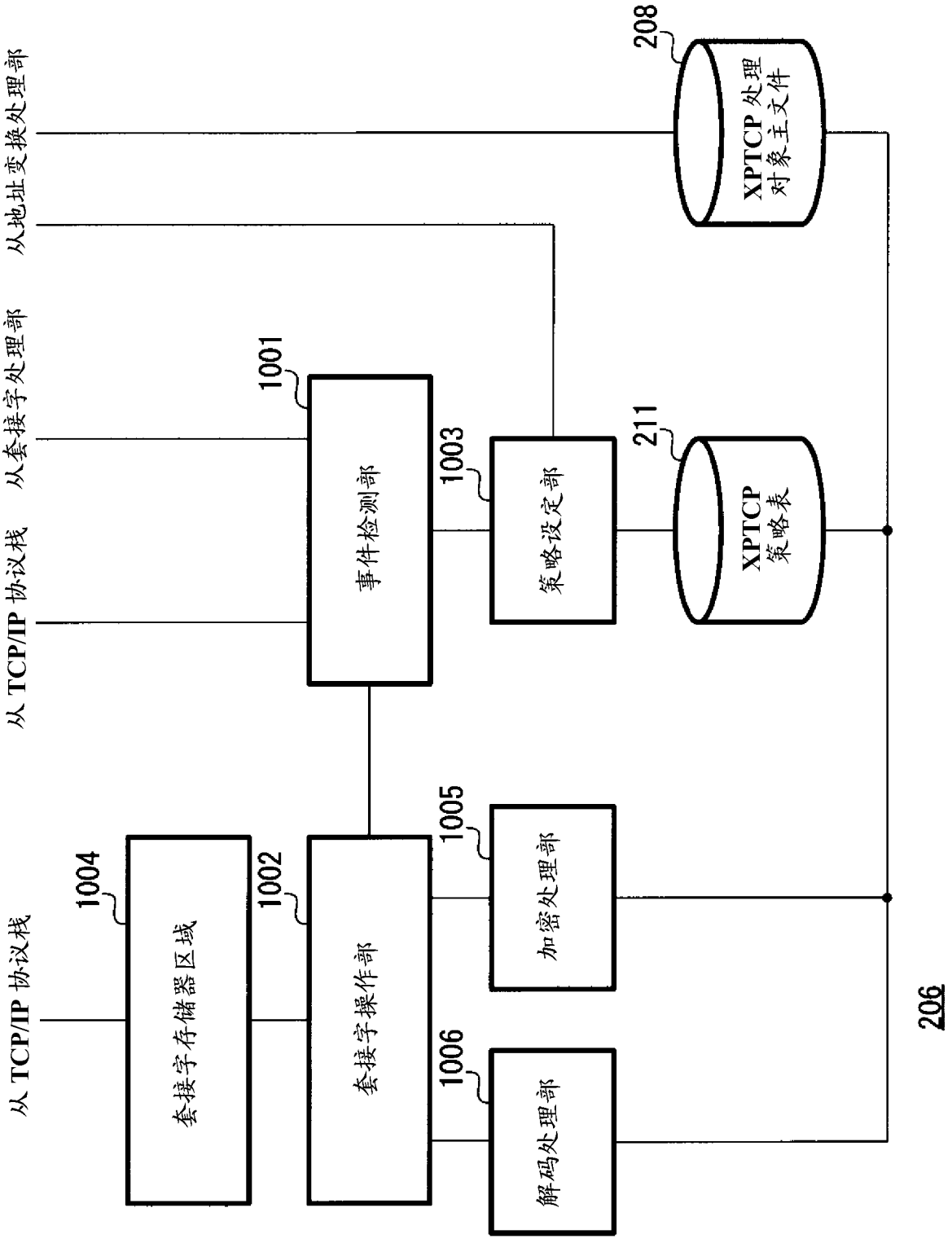

从地址变换处理部
从套接字处理部
从 TCP/IP 协议栈
从 TCP/IP 协议栈
208
XPTCP 处理对象主文件
1001
事件检测部
1003
策略设定部
211
XPTCP 策略表
1004
套接字存储器区域
1002
套接字操作部
1005
加密处理部
1006
解码处理部
206

图 10

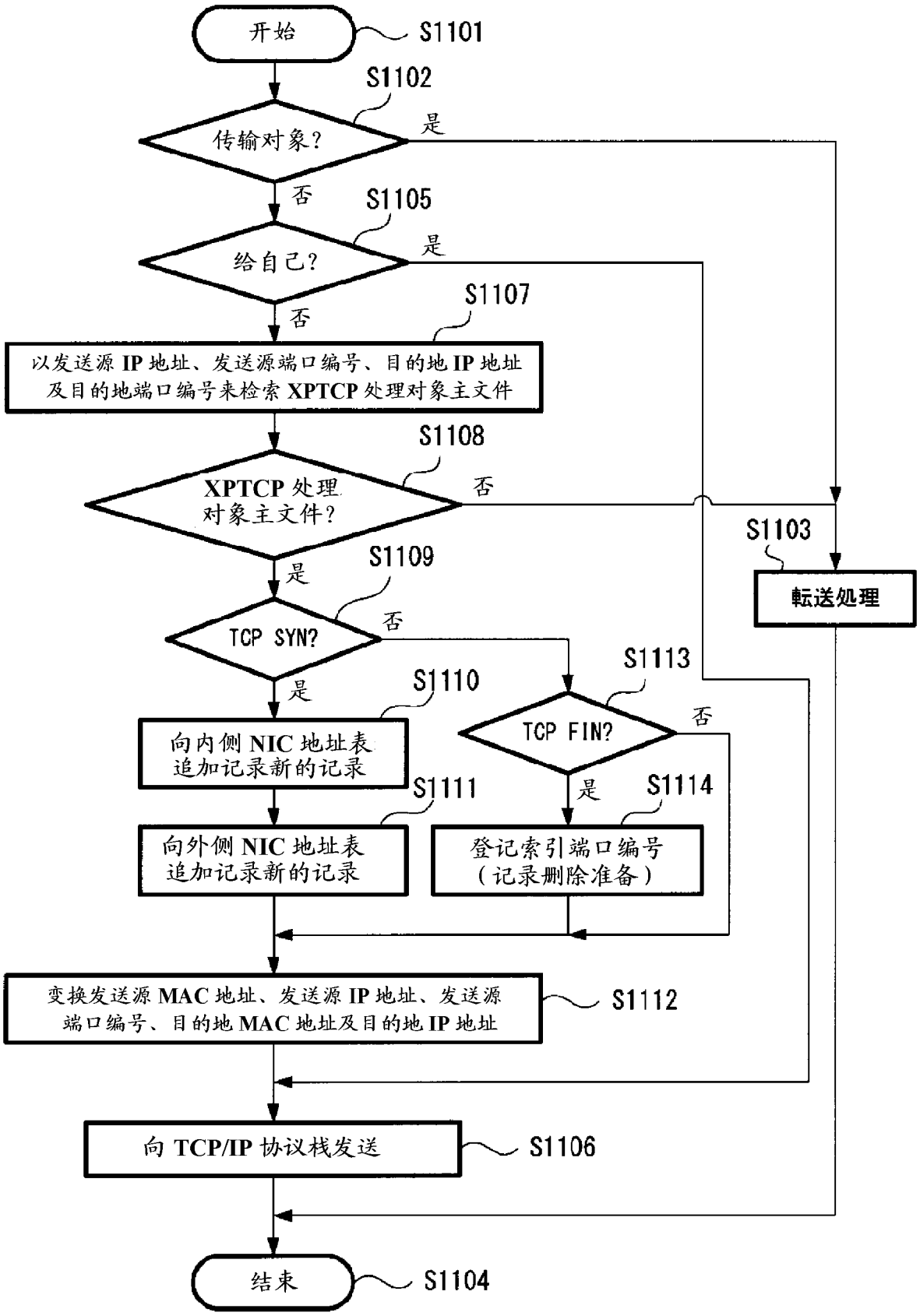

开始
S1101
S1102
传输对象?
是
否
S1105
给自己?
是
否
S1107
以发送源 IP 地址、发送源端口编号、目的地 IP 地址及目的地端口编号来检索 XPTCP 处理对象主文件
S1108
XPTCP 处理对象主文件?
否
是
S1103
转送处理
S1109
TCP SYN?
否
是
S1110
向内侧 NIC 地址表追加记录新的记录
S1111
向外侧 NIC 地址表追加记录新的记录
S1113
TCP FIN?
否
是
S1114
登记索引端口编号（记录删除准备）
变换发送源 MAC 地址、发送源 IP 地址、发送源端口编号、目的地 MAC 地址及目的地 IP 地址
S1112
向 TCP/IP 协议栈发送
S1106
结束
S1104

图 11

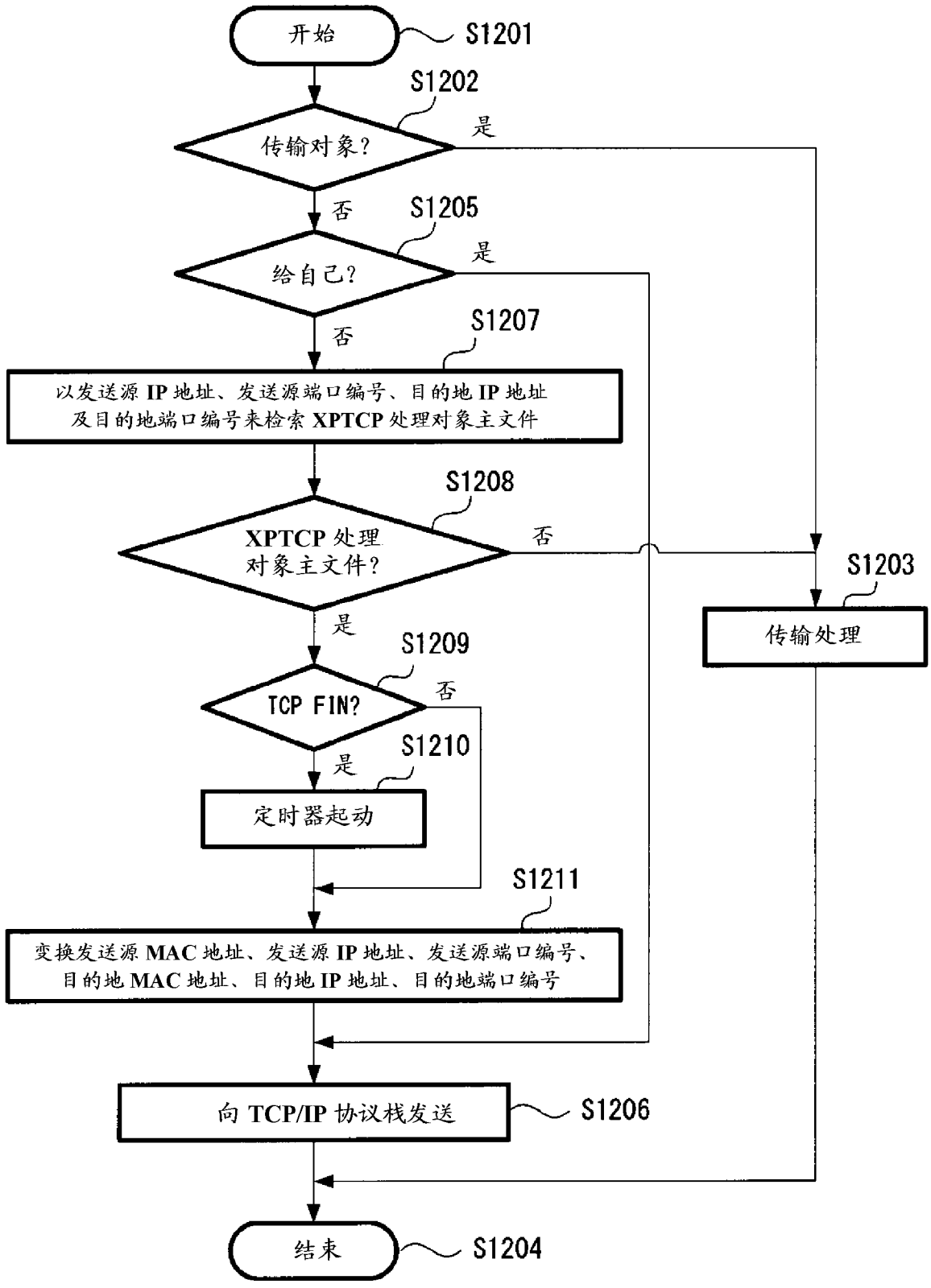

开始
S1201
S1202
传输对象?
是
否
S1205
给自己?
是
否
S1207
以发送源 IP 地址、发送源端口编号、目的地 IP 地址
及目的地端口编号来检索 XPTCP 处理对象主文件
S1208
XPTCP 处理
对象主文件?
否
是
S1203
传输处理
S1209
TCP FIN?
否
是
S1210
定时器起动
S1211
变换发送源 MAC 地址、发送源 IP 地址、发送源端口编号、
目的地 MAC 地址、目的地 IP 地址、目的地端口编号
向 TCP/IP 协议栈发送
S1206
结束
S1204

图 12

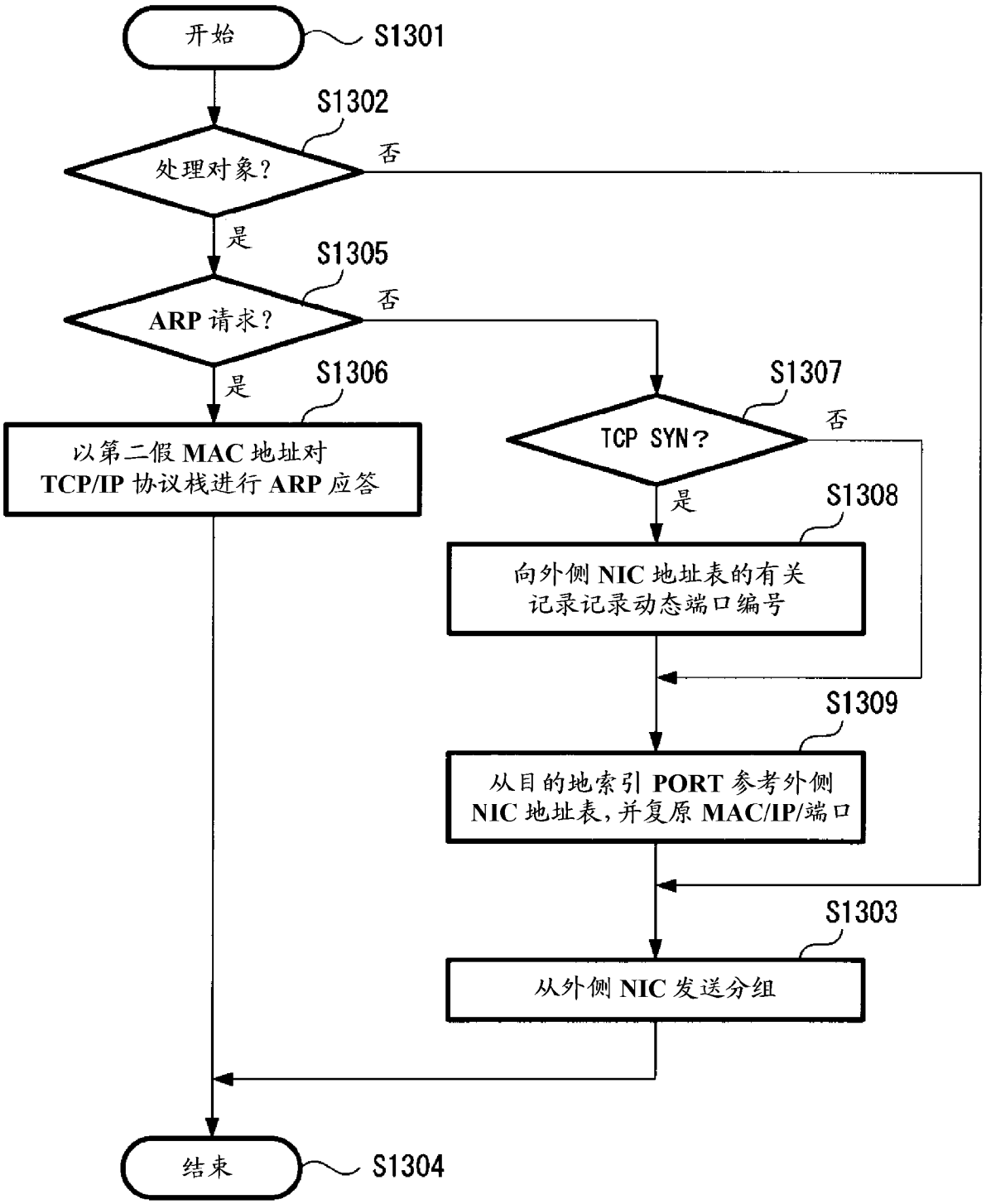

开始
S1301
S1302
处理对象?
否
是
S1305
ARP 请求?
否
是
S1306
以第二假 MAC 地址对
TCP/IP 协议栈进行 ARP 应答
S1307
TCP SYN?
否
是
S1308
向外侧 NIC 地址表的有关
记录记录动态端口编号
S1309
从目的地索引 PORT 参考外侧
NIC 地址表，并复原 MAC/IP/端口
S1303
从外侧 NIC 发送分组
结束
S1304

图 13

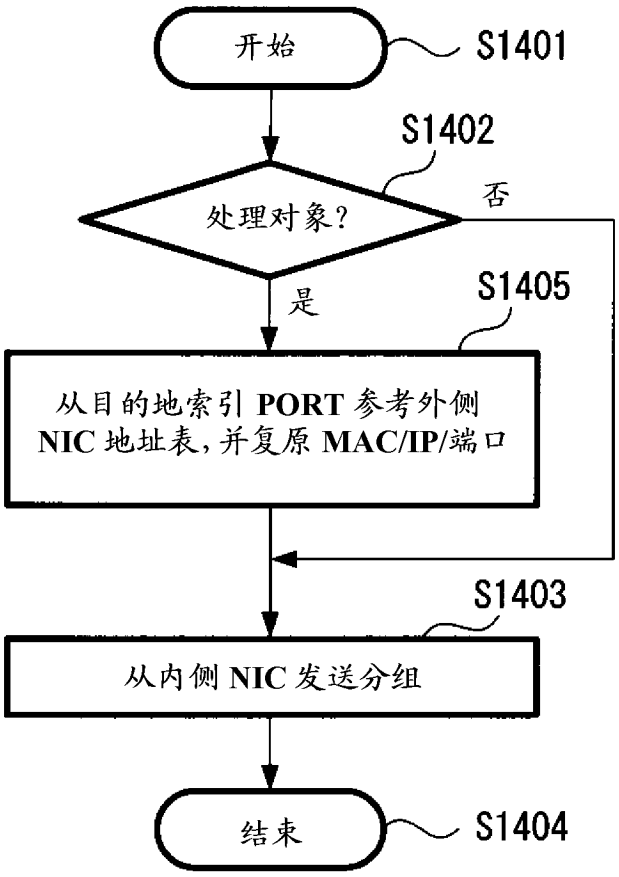

开始
S1401
S1402
处理对象?
否
是
S1405
从目的地索引 PORT 参考外侧
NIC 地址表，并复原 MAC/IP/端口
S1403
从内侧 NIC 发送分组
结束
S1404

图 14

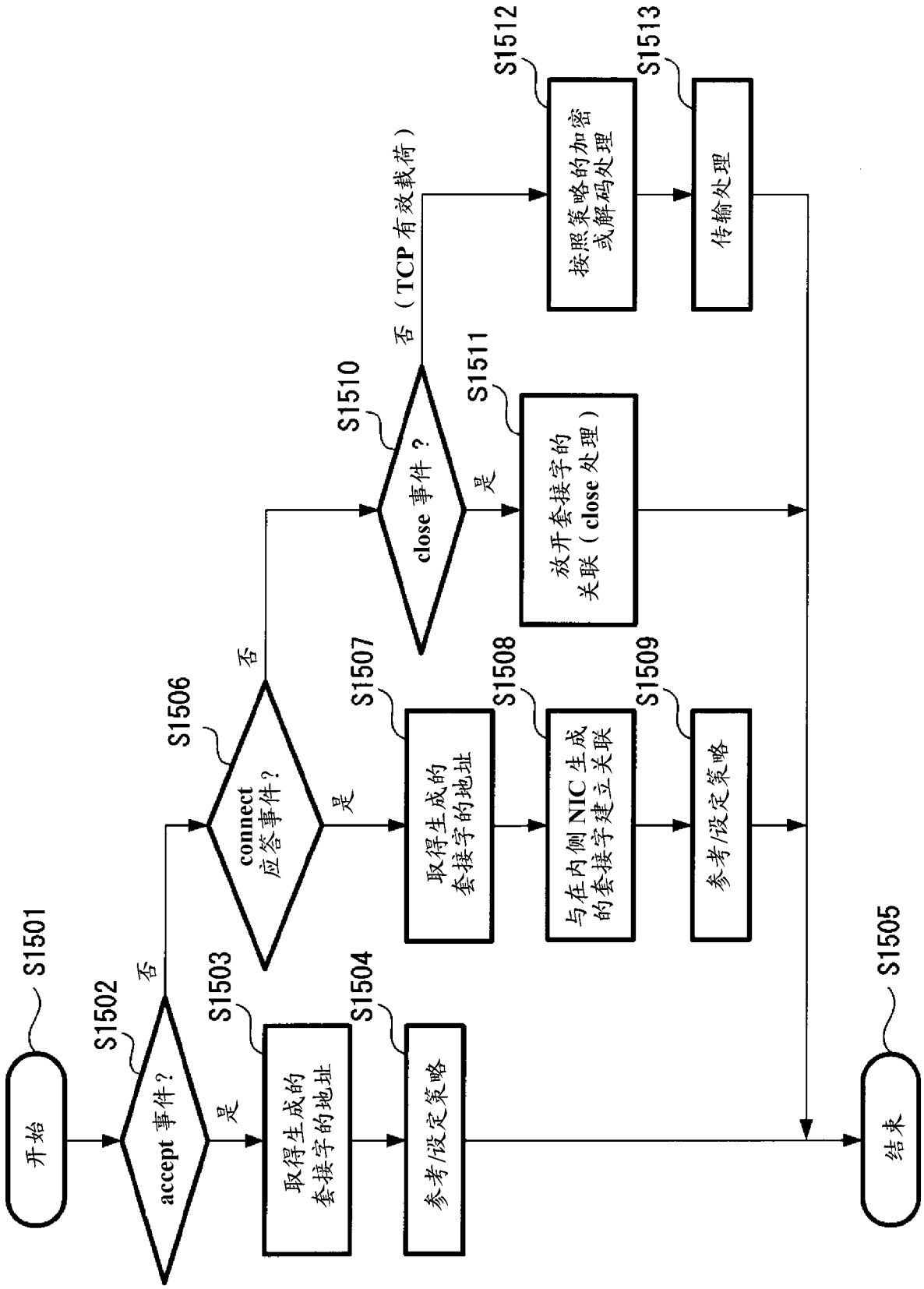

开始
S1501
accept 事件？
S1502
是
否
取得生成的套接字的地址
S1503
参考/设定策略
S1504
connect 应答事件？
S1506
是
否
取得生成的套接字的地址
S1507
与在内侧 NIC 生成的套接字建立关联
S1508
参考/设定策略
S1509
close 事件？
S1510
是
否（TCP 有效载荷）
放开套接字的关联（close 处理）
S1511
按照策略的加密或解码处理
S1512
传输处理
S1513
结束
S1505

图 15

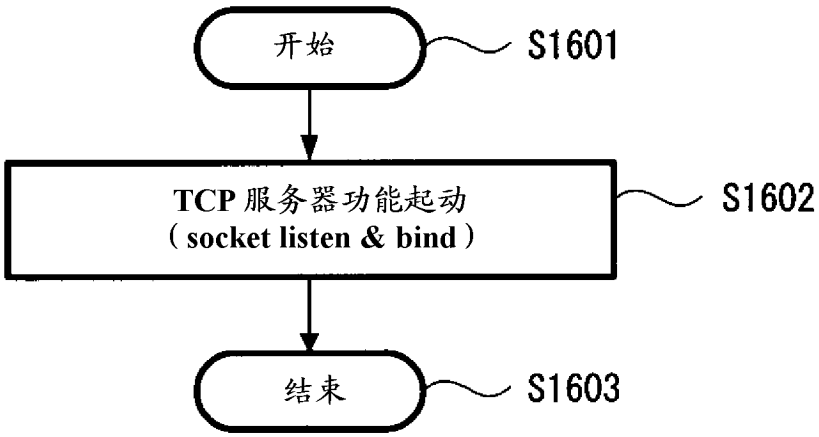

开始
S1601
TCP 服务器功能起动
（socket listen & bind）
S1602
结束
S1603

图 16

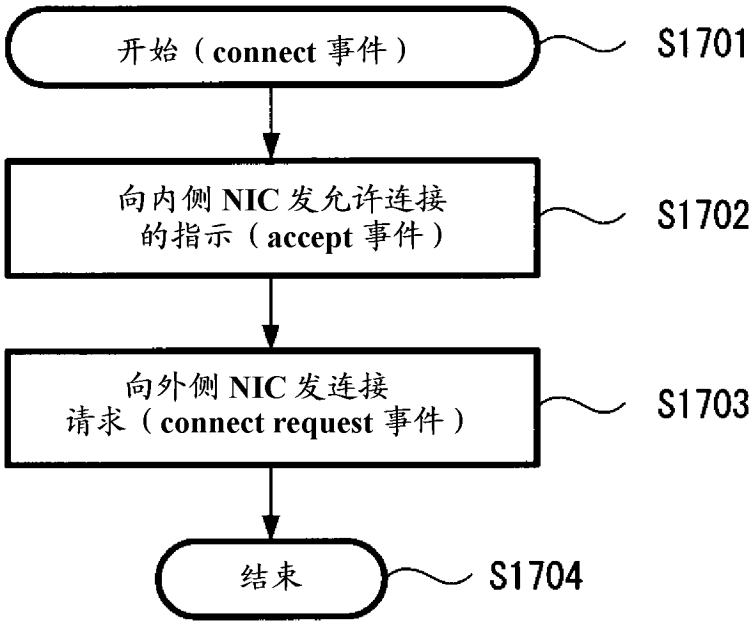

开始（connect 事件）
S1701
向内侧 NIC 发允许连接
的指示（accept 事件）
S1702
向外侧 NIC 发连接
请求（connect request 事件）
S1703
结束
S1704

图 17

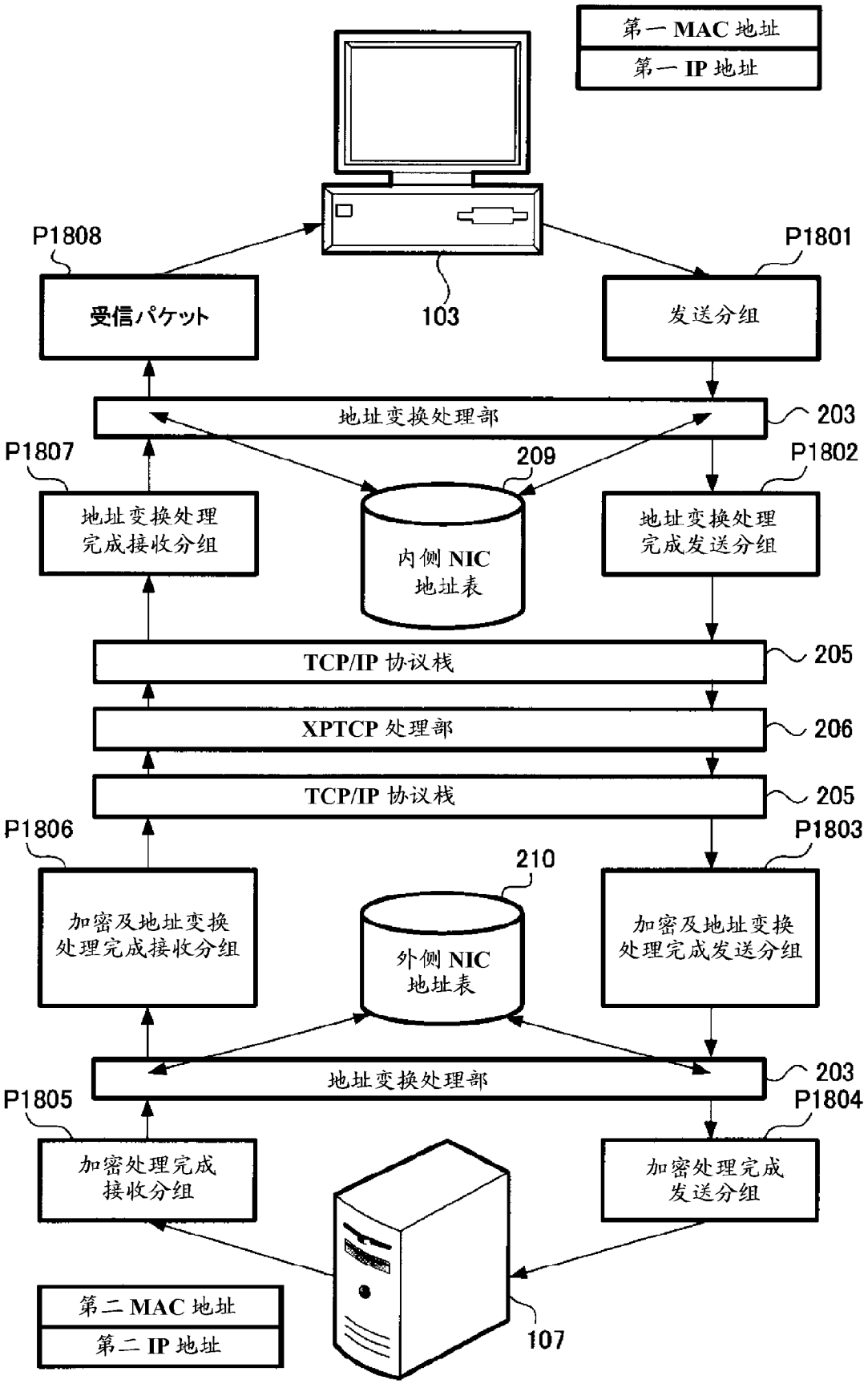

第一 MAC 地址
第一 IP 地址
P1808
受信パケット
103
P1801
发送分组
地址变换处理部
203
P1807
209
P1802
地址变换处理
完成接收分组
内侧 NIC
地址表
地址变换处理
完成发送分组
TCP/IP 协议栈
205
XPTCP 处理部
206
TCP/IP 协议栈
205
P1806
P1803
210
加密及地址变换
处理完成接收分组
外侧 NIC
地址表
加密及地址变换
处理完成发送分组
地址变换处理部
203
P1805
P1804
加密处理完成
接收分组
加密处理完成
发送分组
第二 MAC 地址
第二 IP 地址
107

图 18

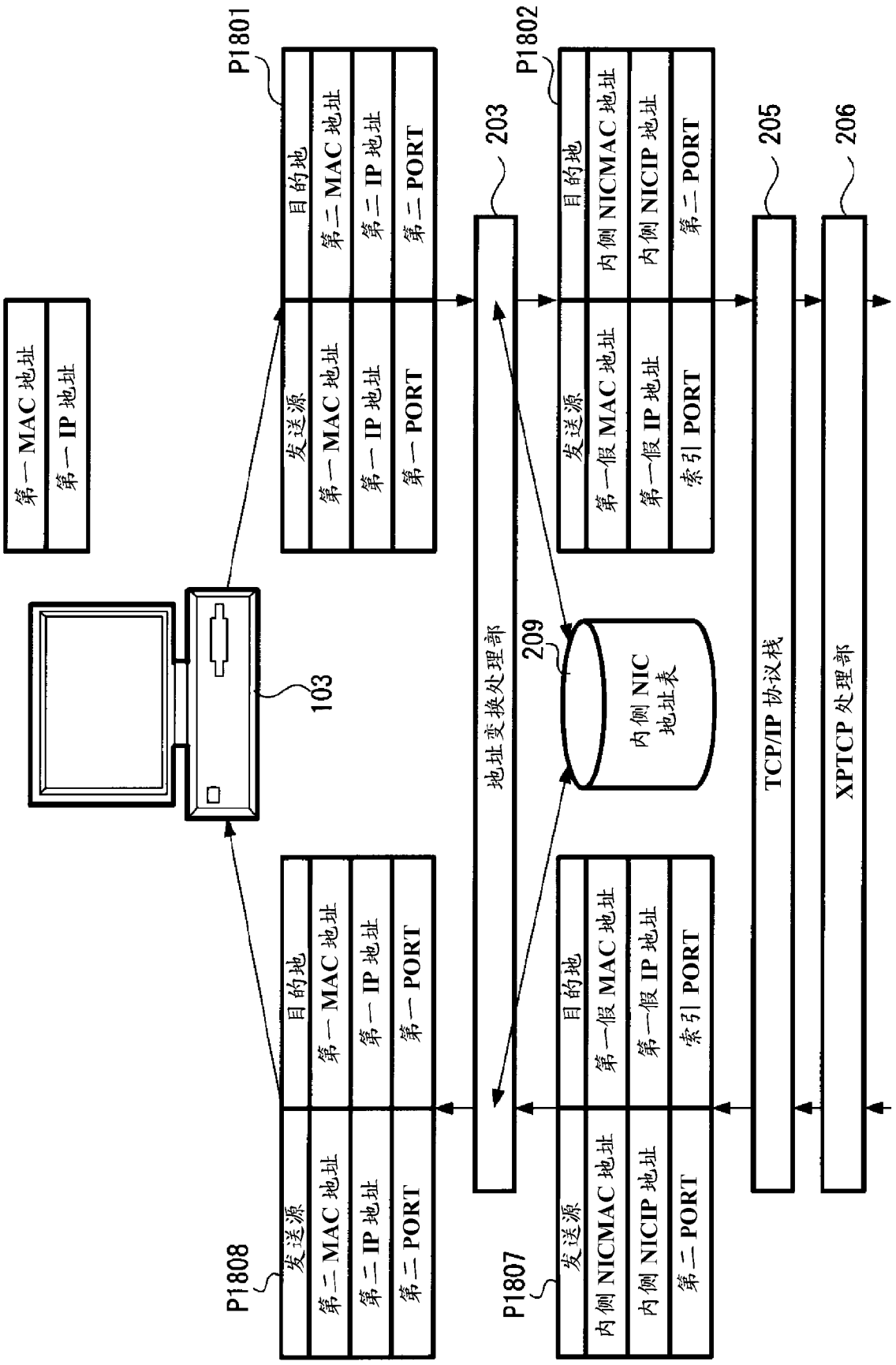

第一 MAC 地址
第一 IP 地址
P1801
目的地
第二 MAC 地址
第二 IP 地址
第二 PORT
发送源
第一 MAC 地址
第一 IP 地址
第一 PORT
203
P1802
目的地
内侧 NICMAC 地址
内侧 NICIP 地址
第二 PORT
发送源
第一假 MAC 地址
第一假 IP 地址
索引 PORT
205
206
103
209
内侧 NIC
地址表
地址变换处理部
TCP/IP 协议栈
XPTCP 处理部
P1808
目的地
第一 MAC 地址
第一 IP 地址
第一 PORT
发送源
第二 MAC 地址
第二 IP 地址
第二 PORT
P1807
目的地
第一假 MAC 地址
第一假 IP 地址
索引 PORT
发送源
内侧 NICMAC 地址
内侧 NICIP 地址
第二 PORT

图 19

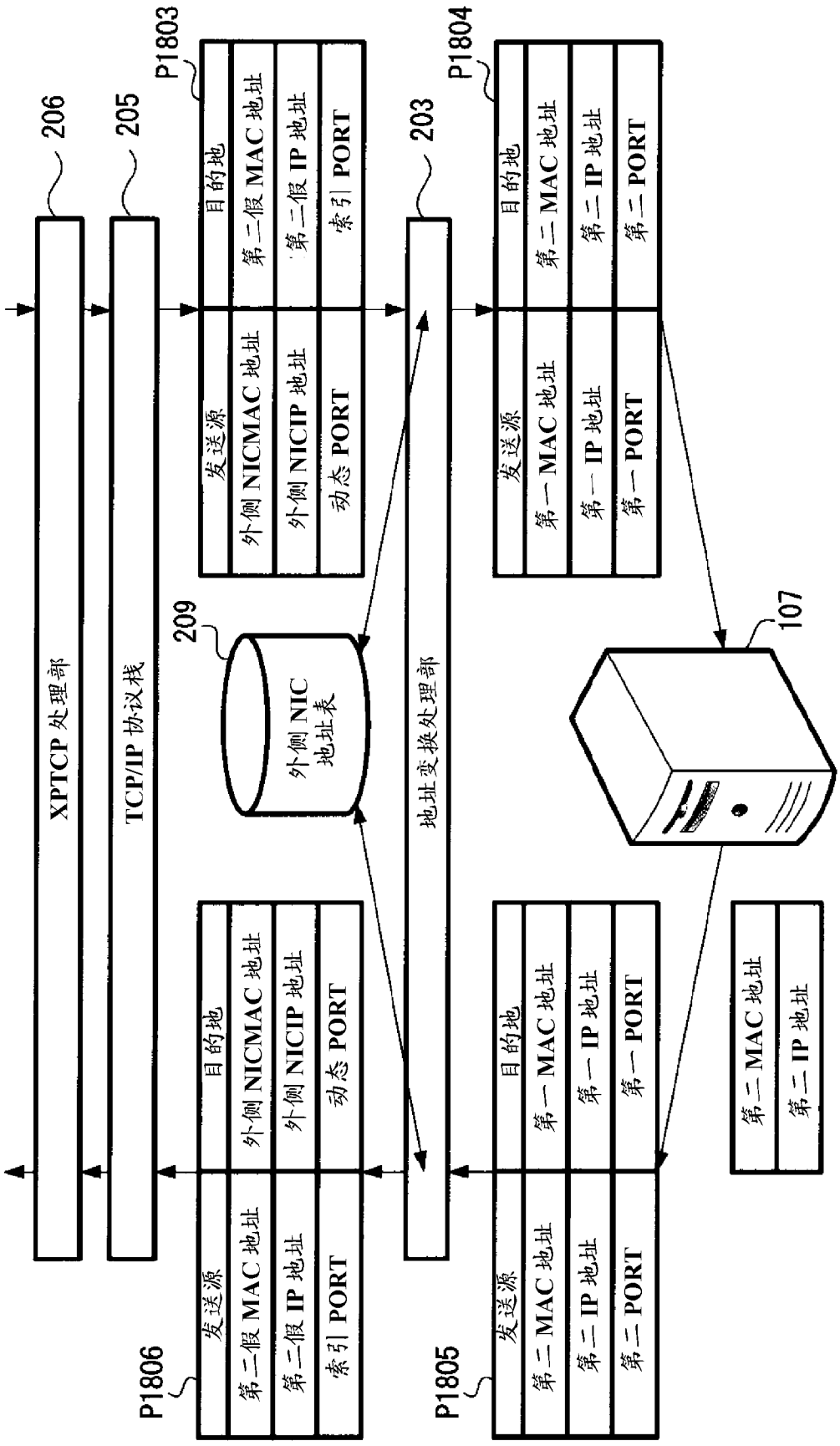

206
205
203
P1803
P1804
XPTCP 处理部
TCP/IP 协议栈
地址变换处理部
目的地
第二假 MAC 地址
第二假 IP 地址
索引 PORT
发送源
外侧 NICMAC 地址
外侧 NICIP 地址
动态 PORT
第一 MAC 地址
第一 IP 地址
第一 PORT
第二 MAC 地址
第二 IP 地址
第二 PORT
209
外侧 NIC
地址表
107
P1806
P1805

图 20

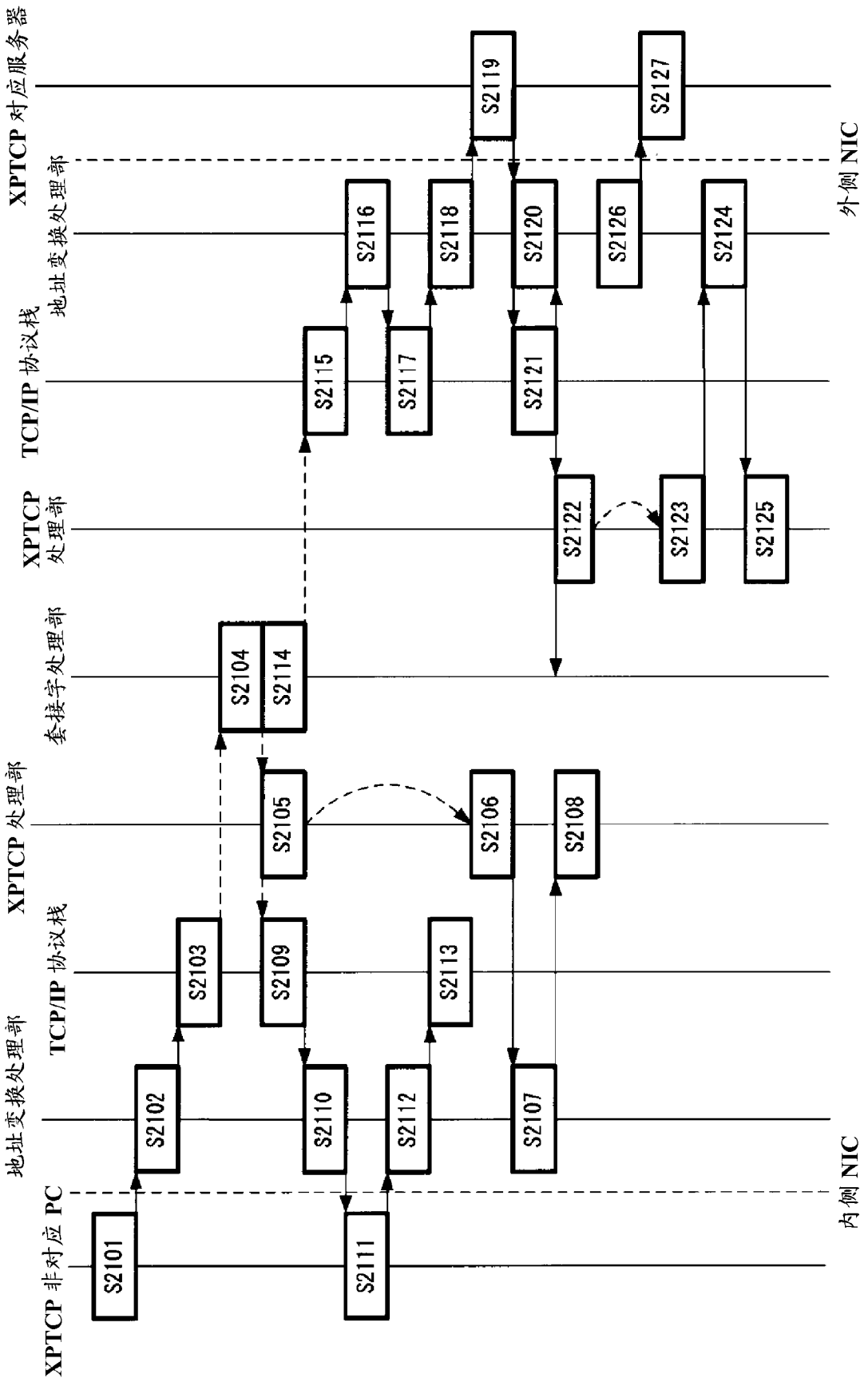

XPTCP 对应服务器
地址变换处理部
TCP/IP 协议栈
XPTCP 处理部
套接字处理部
XPTCP 处理部
TCP/IP 协议栈
地址变换处理部
XPTCP 非对应 PC
外侧 NIC
内侧 NIC
S2101
S2102
S2103
S2104
S2105
S2106
S2107
S2108
S2109
S2110
S2111
S2112
S2113
S2114
S2115
S2116
S2117
S2118
S2119
S2120
S2121
S2122
S2123
S2124
S2125
S2126
S2127

图 21

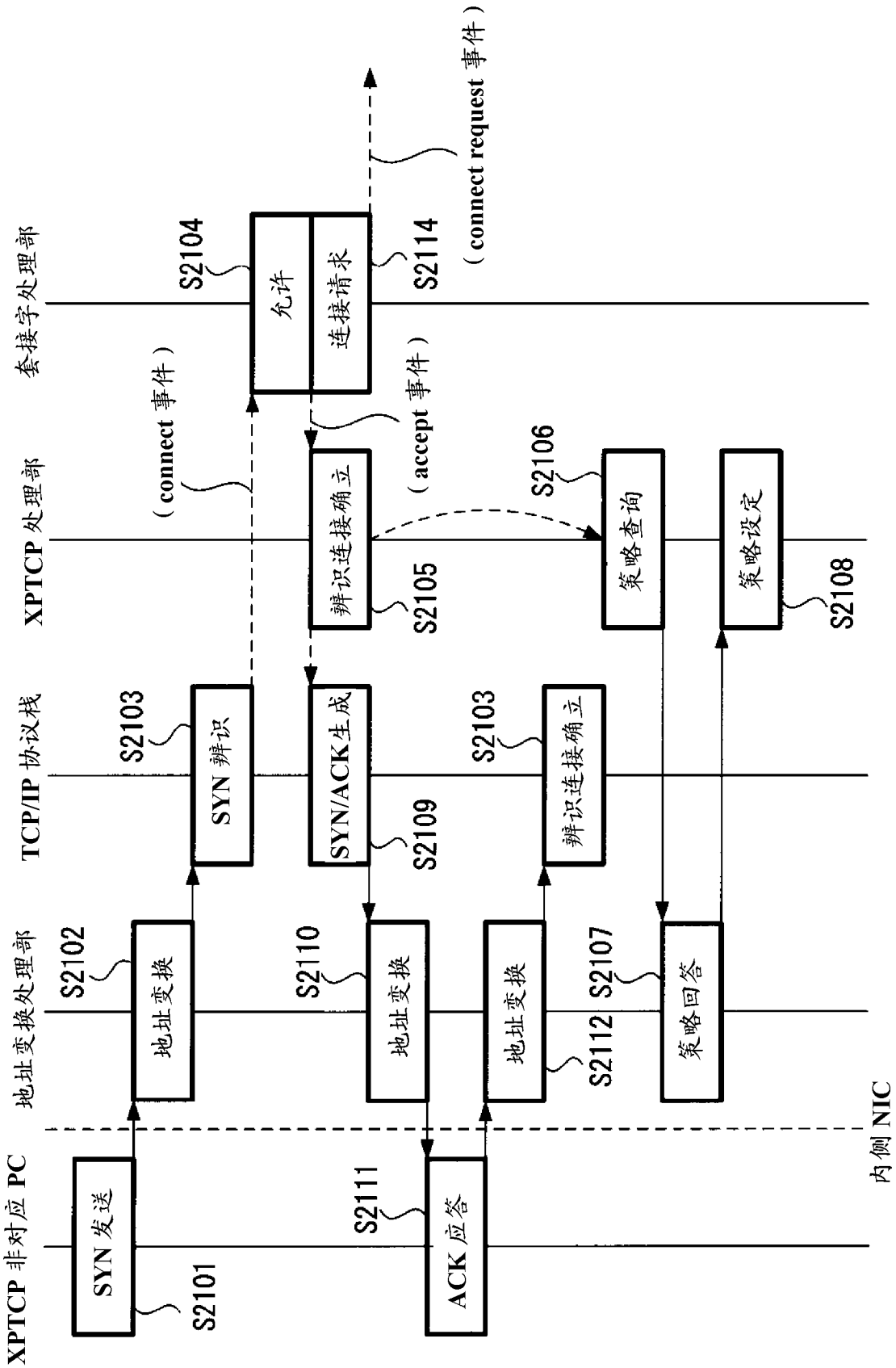

XPTCP 非对应 PC
地址变换处理部
TCP/IP 协议栈
XPTCP 处理部
套接字处理部
内侧 NIC
SYN 发送
地址变换
SYN 辨识
SYN/ACK生成
辨识连接确立
允许
连接请求
S2101
S2102
S2103
S2104
S2105
S2106
S2107
S2108
S2109
S2110
S2111
S2112
S2114
（connect 事件）
（accept 事件）
（connect request 事件）
ACK 应答
地址变换
辨识连接确立
策略查询
策略回答
策略设定

图 22

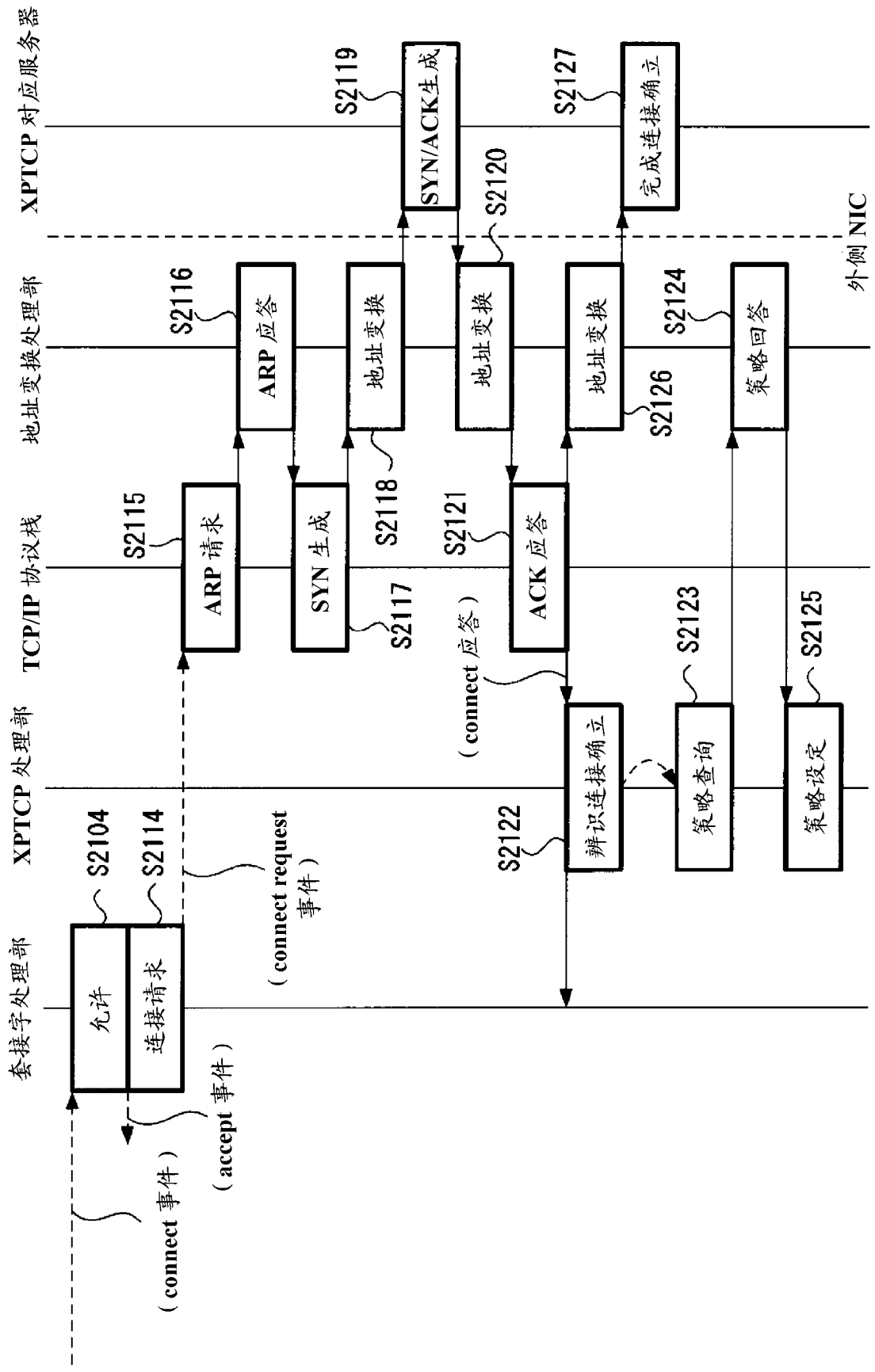

套接字处理部
XPTCP 处理部
TCP/IP 协议栈
地址变换处理部
XPTCP 对应服务器
外侧 NIC
允许
连接请求
S2104
S2114
(connect 事件)
(accept 事件)
(connect request 事件)
S2115
ARP 请求
S2116
ARP 应答
SYN 生成
S2117
地址变换
S2118
S2119
SYN/ACK生成
S2120
地址变换
S2121
(connect 应答)
ACK 应答
S2122
辨识连接确立
地址变换
S2123
策略查询
S2124
策略回答
S2125
策略设定
S2126
S2127
完成连接确立

图 23

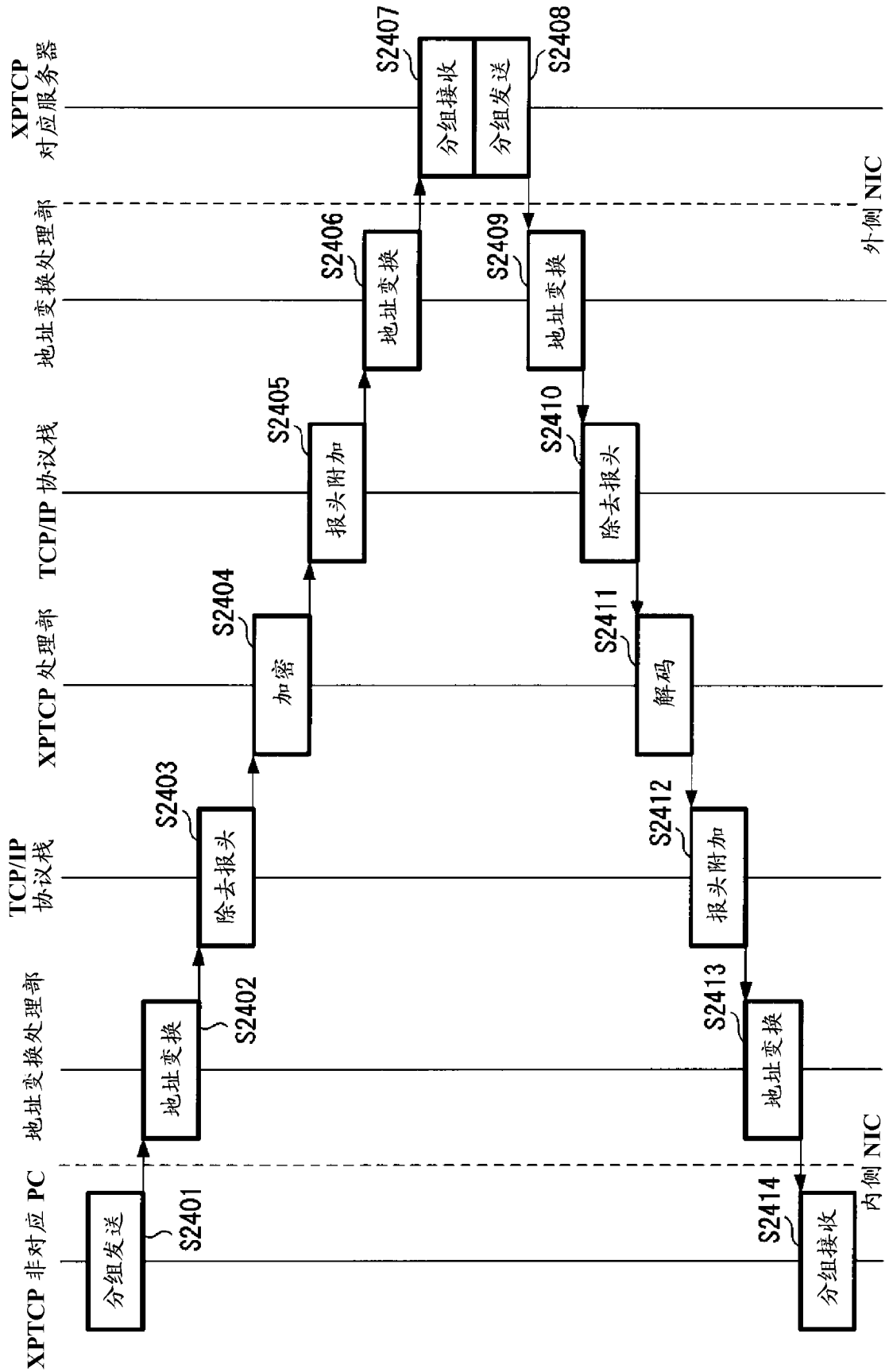

XPTCP 非对应 PC
地址变换处理部
TCP/IP 协议栈
XPTCP 处理部
TCP/IP 协议栈
地址变换处理部
XPTCP 对应服务器
内侧 NIC
外侧 NIC
分组发送
地址变换
除去报头
加密
报头附加
地址变换
分组接收
分组发送
地址变换
除去报头
解码
报头附加
地址变换
分组接收
S2401
S2402
S2403
S2404
S2405
S2406
S2407
S2408
S2409
S2410
S2411
S2412
S2413
S2414

图 24

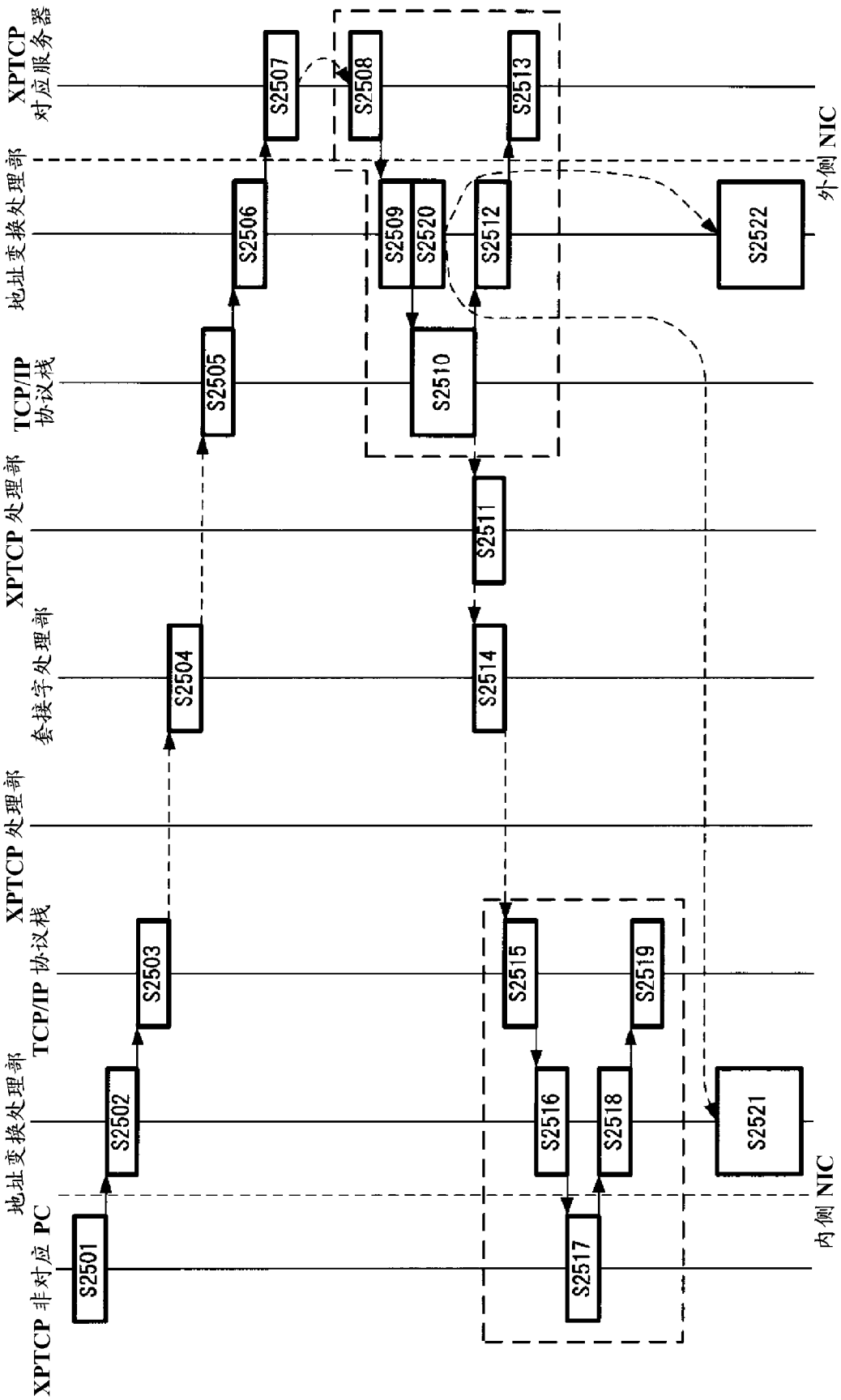

XPTCP 非对应 PC
地址变换处理部
TCP/IP 协议栈
XPTCP 处理部
套接字处理部
XPTCP 处理部
TCP/IP 协议栈
地址变换处理部
XPTCP 对应服务器
内侧 NIC
外侧 NIC
S2501
S2502
S2503
S2504
S2505
S2506
S2507
S2508
S2509
S2510
S2511
S2512
S2513
S2514
S2515
S2516
S2517
S2518
S2519
S2520
S2521
S2522

图 25

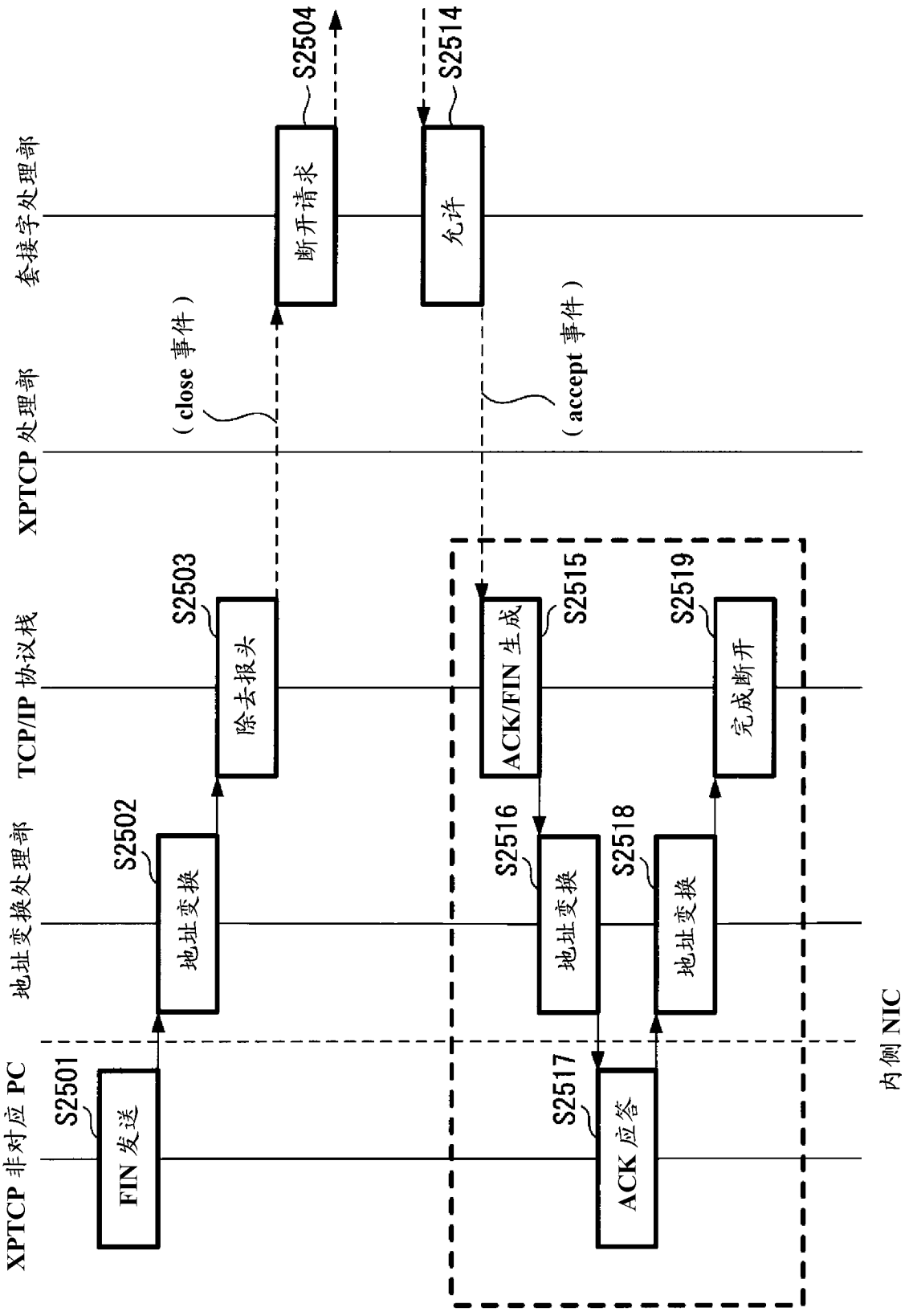

XPTCP 非对应 PC
地址变换处理部
TCP/IP 协议栈
XPTCP 处理部
套接字处理部
内侧 NIC
S2501
FIN 发送
S2502
地址变换
S2503
除去报头
S2504
断开请求
(close 事件)
S2514
允许
(accept 事件)
S2515
ACK/FIN 生成
S2516
地址变换
S2517
ACK 应答
S2518
地址变换
S2519
完成断开

图 26

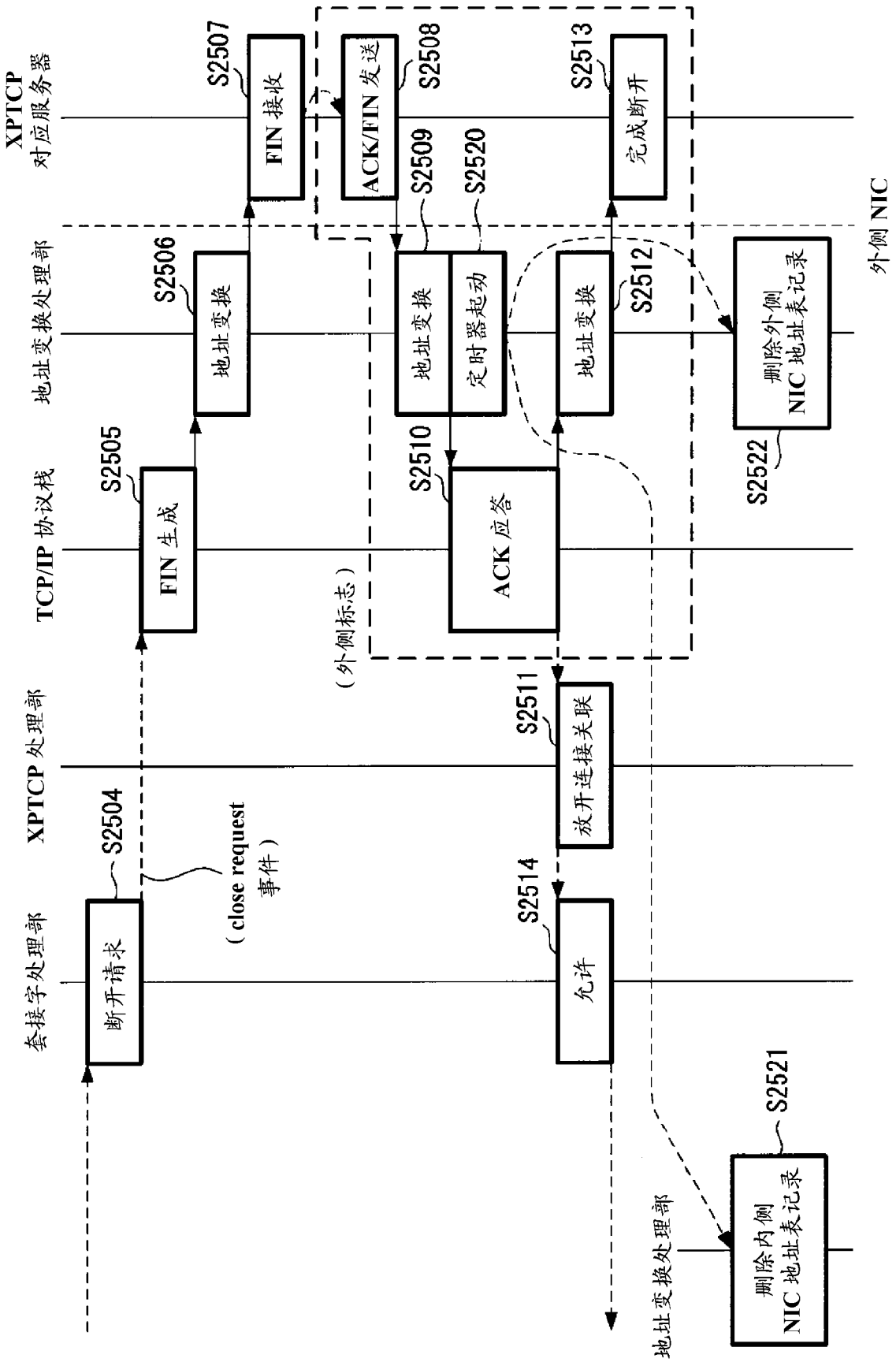

XPTCP 对应服务器
地址变换处理部
TCP/IP 协议栈
XPTCP 处理部
套接字处理部
外侧 NIC
S2507
FIN 接收
S2508
ACK/FIN 发送
S2513
完成断开
S2506
地址变换
S2509
地址变换
S2520
定时器起动
S2512
地址变换
删除外侧 NIC 地址表记录
S2522
S2505
FIN 生成
S2510
ACK 应答
（外侧标志）
S2511
放开连接关联
S2504
断开请求
（close request 事件）
S2514
允许
S2521
删除内侧 NIC 地址表记录
地址变换处理部

图 27

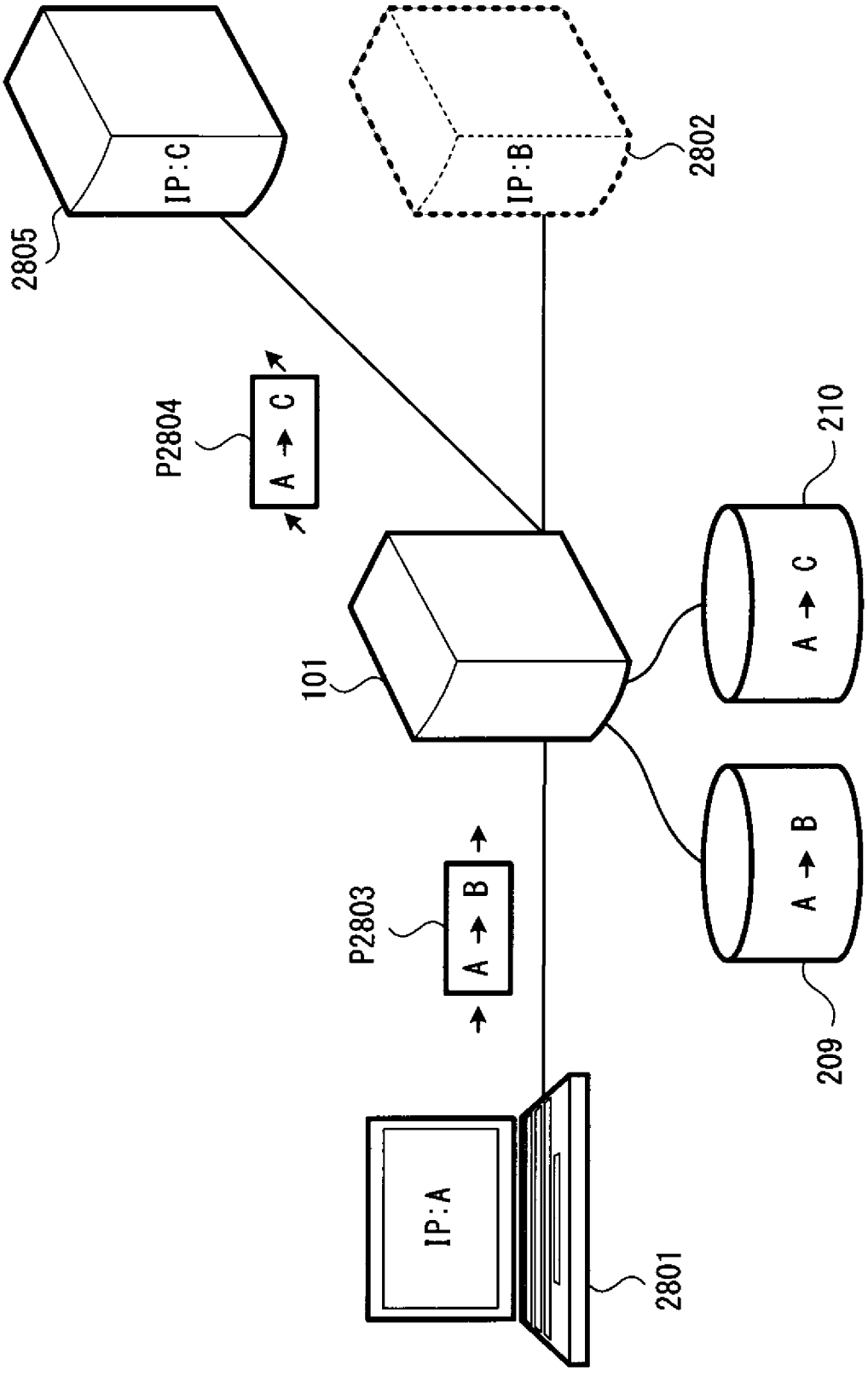


图 28

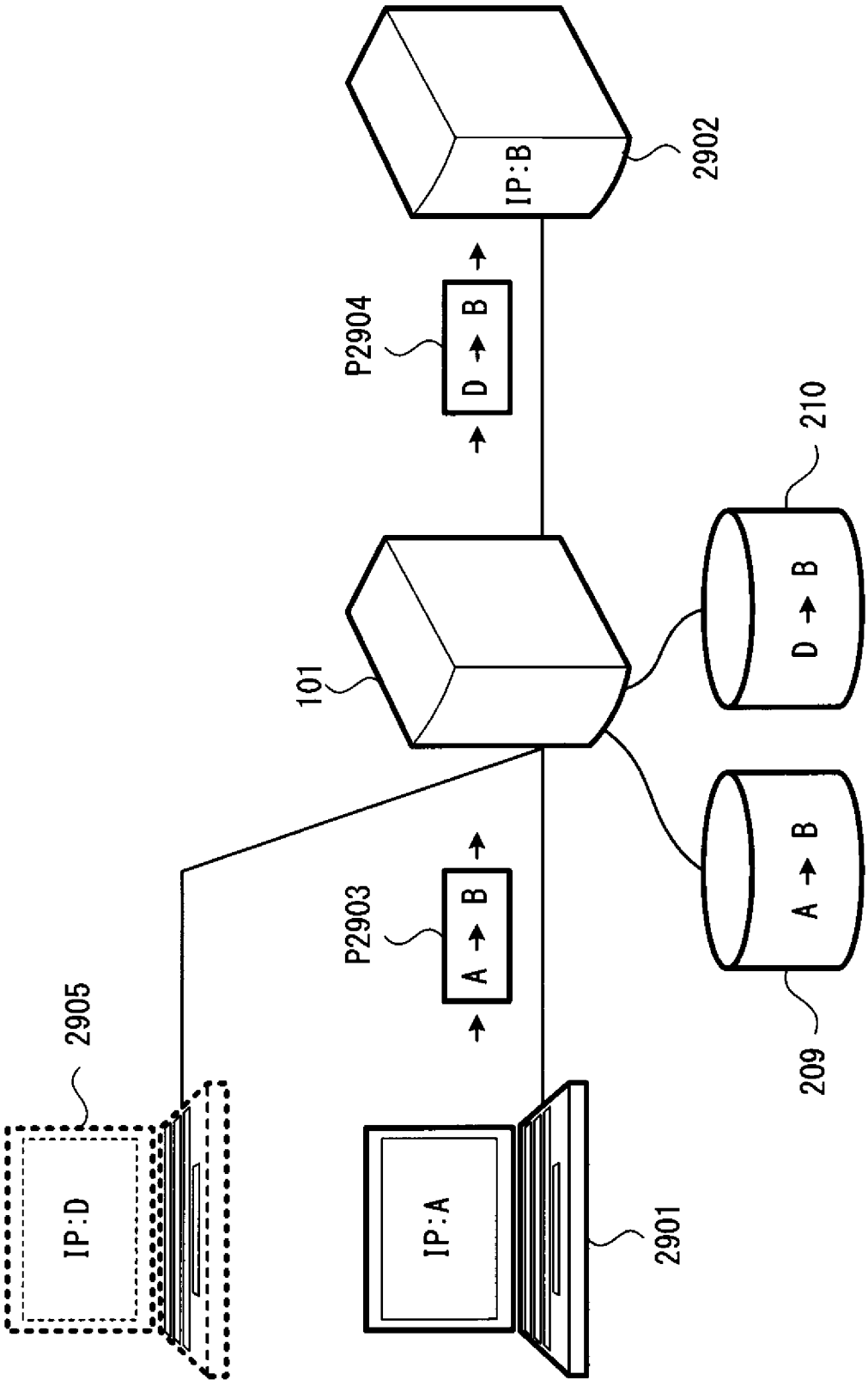


图 29