(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년04월26일
(11) 등록번호 10-1851826
(24) 등록일자 2018년04월18일

(51) 국제특허분류(Int. Cl.)
H04L 12/66 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2014-7006671
(22) 출원일자(국제) 2011년11월10일
심사청구일자 2016년09월23일
(85) 번역문제출일자 2014년03월12일
(65) 공개번호 10-2014-0050725
(43) 공개일자 2014년04월29일
(86) 국제출원번호 PCT/JP2011/075963
(87) 국제공개번호 WO 2013/027302
국제공개일자 2013년02월28일
(30) 우선권주장
JP-P-2011-180215 2011년08월22일 일본(JP)
(56) 선행기술조사문헌
US20040098506 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인토 씨오 엘티디
일본국 도쿄토 도시마쿠 미나미오오츠카 2쵸메 37반 5고
(72) 발명자
오가와, 케이코
일본국 1700005 도쿄토 도시마쿠 미나미오오츠카 2쵸메 37반 5고 인토 씨오 엘티디 내
(74) 대리인
특허법인 무한

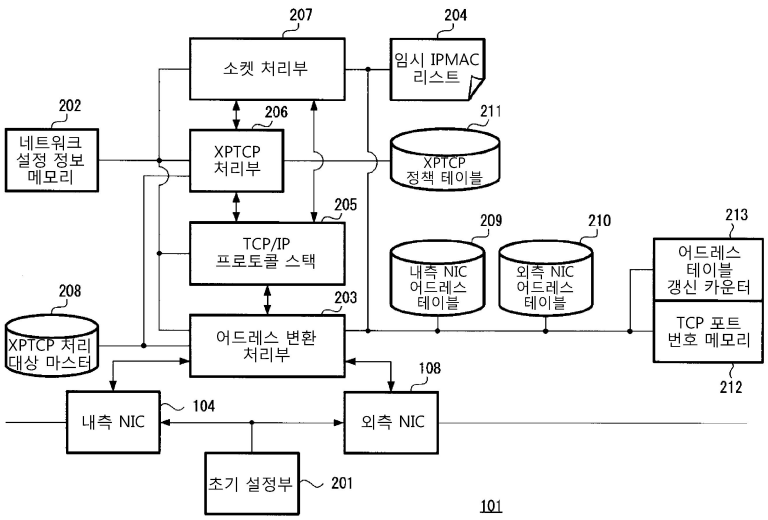
전체 청구항 수 : 총 9 항 심사관 : 김대성

(54) 발명의 명칭 **네트워크 게이트웨이 장치**

(57) 요 약

XPTCP 게이트웨이 장치(101)에 할당되고 있는 IP 어드레스와는 무관계여야 할 패킷을 TCP/IP 프로토콜 스택(205)이 처리할 수 있도록 하기 위해, 미리 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 개서 테이블에 메모해 둔다. 그 다음에, 수신한 패킷에 첨부되고 있는 송신원 MAC 어드레스 및 송신원 IP 어드레스는 가짜의 MAC 어드레스 및 가짜의 IP 어드레스로, 목적지 MAC 어드레스 및 목적지 IP 어드레스는 XPTCP 게이트웨이 장치(101)에 할당되고 있는 IP 어드레스 및 MAC 어드레스로 개서하고 나서, TCP/IP 프로토콜 스택(205)에게 준다.

대 표 도



명 세 서

청구범위

청구항 1

제1 NIC와,

제2 NIC와,

상기 제1 NIC 및 상기 제2 NIC에 프로미스큐어스 모드(promiscuous mode)를 설정하는 초기 설정부와,

상기 제1 NIC 및 상기 제2 NIC 사이에서 TCP/IP 통신 처리를 수행하는 TCP/IP 프로토콜 스택과,

상기 제1 NIC로부터 수신한 수신 패킷에 첨부되고 있는 송신원 MAC 어드레스를 제1 임시 MAC 어드레스로 변환하고, 송신원 IP 어드레스를 제1 임시 IP 어드레스로 변환하고, 목적지 MAC 어드레스를 상기 제1 NIC에 첨부되고 있는 제1 NICMAC 어드레스로 변환하고, 목적지 IP 어드레스를 상기 제1 NIC에 첨부되고 있는 제1 NICIP 어드레스로 변환하여, 상기 TCP/IP 프로토콜 스택에 상기 수신 패킷을 송신함과 동시에, 상기 TCP/IP 프로토콜 스택으로부터 수신한 송신 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 상기 수신 패킷에 첨부되고 있던 상기 송신원 MAC 어드레스, 상기 송신원 IP 어드레스, 상기 목적지 MAC 어드레스 및 상기 목적지 IP 어드레스로 복원(restore)하여, 상기 제2 NIC에 송신하는 어드레스 변환 처리부와,

상기 제1 NIC에 대해 제1 TCP 커넥션을 형성하기 위한 서버 기능과, 상기 제2 NIC에 대해 제2 TCP 커넥션을 형성하기 위한 클라이언트 기능을 갖춤과 동시에, 상기 제1 NIC로부터 TCP FIN 패킷이 오면, 상기 제2 NIC로부터 TCP FIN 패킷이 온 것을 검출하여, 상기 제1 TCP 커넥션을 절단하는 지시를 상기 TCP/IP 프로토콜 스택으로 보내는 소켓 처리부

를 구비하는 네트워크 게이트웨이 장치.

청구항 2

제1항에 있어서,

상기 수신 패킷에 첨부되고 있는 상기 송신원 MAC 어드레스를 격납하는 송신원 MAC 어드레스 필드와, 상기 수신 패킷에 첨부되고 있는 상기 송신원 IP 어드레스를 격납하는 송신원 IP 어드레스 필드와, 상기 수신 패킷에 첨부되고 있는 상기 목적지 MAC 어드레스를 격납하는 목적지 MAC 어드레스 필드와, 상기 수신 패킷에 첨부되고 있는 상기 목적지 IP 어드레스를 기록하는 목적지 IP 어드레스 필드와, 일의성을 가지는 색인용의 색인용 포트 번호를 기록하는 색인용 포트 번호 필드를 갖추는 어드레스 변환 테이블

을 더 갖추고,

상기 어드레스 변환 처리부는 상기 수신 패킷에 첨부되고 있는 송신원 포트 번호를 상기 색인용 포트 번호 필드에 기록한 상기 색인용 포트 번호로 변환함과 동시에, 상기 송신 패킷에 첨부되고 있는 목적지 포트 번호로 상기 어드레스 변환 테이블의 상기 색인용 포트 번호 필드를 검색하여, 복원해야 할 레코드를 특정하는, 네트워크 게이트웨이 장치.

청구항 3

제2항에 있어서,

상기 TCP/IP 프로토콜 스택으로부터 수신한 수신 패킷의 페이로드(payload) 부분에 소정의 암호화 처리를 행하여 다시 상기 TCP/IP 프로토콜 스택으로 반송하는 확장 TCP 처리부

를 더 갖추는 네트워크 게이트웨이 장치.

청구항 4

삭제

청구항 5

제2항에 있어서,

상기 어드레스 변환 처리부는, 상기 제1 NIC로부터 TCP SYN 패킷이 오면, 상기 어드레스 변환 테이블에 레코드를 추가하는,

네트워크 게이트웨이 장치.

청구항 6

제3항에 있어서,

상기 확장 TCP 처리부는, 상기 제1 TCP 커넥션에서 발생하여 상기 소켓 처리부에 도달하려는 스트림 데이터에 상기 암호화 처리를 행한 후, 상기 제2 TCP 커넥션으로 전송하는, 네트워크 게이트웨이 장치.

청구항 7

제1항에 있어서,

상기 어드레스 변환 처리부는, 상기 제1 NIC로부터 TCP SYN 패킷이 온 것에 호응하여 상기 제2 TCP 커넥션이 형성될 때, 상기 TCP/IP 프로토콜 스택으로부터 발생되는 ARP 요구 패킷을 수신하면, 상기 TCP/IP 프로토콜 스택에 대해 가짜의 MAC 어드레스를 포함한 의사 ARP 응답 패킷을 회신하는, 네트워크 게이트웨이 장치.

청구항 8

삭제

청구항 9

삭제

청구항 10

제1항에 있어서,

상기 수신 패킷에 첨부되고 있는 상기 송신원 MAC 어드레스를 격납하는 제1 송신원 MAC 어드레스 필드와, 상기 수신 패킷에 첨부되고 있는 상기 송신원 IP 어드레스를 격납하는 제1 송신원 IP 어드레스 필드와, 상기 수신 패킷에 첨부되고 있는 상기 목적지 MAC 어드레스를 격납하는 제1 목적지 MAC 어드레스 필드와, 상기 수신 패킷에 첨부되고 있는 상기 목적지 IP 어드레스를 기록하는 제1 목적지 IP 어드레스 필드와, 일의성을 가지는 색인용의 색인용 포트 번호를 기록하는 제1 색인용 포트 번호 필드를 갖추는 제1 NIC 어드레스 변환 테이블과,

제2 송신원 MAC 어드레스 필드와, 제2 송신원 IP 어드레스 필드와, 제2 목적지 MAC 어드레스 필드와, 제2 목적지 IP 어드레스 필드와, 상기 색인용 포트 번호를 기록하는 제2 색인용 포트 번호 필드와, 상기 TCP/IP 프로토콜 스택이 생성하는 동적 포트 번호를 기록하는 동적 포트 번호 필드를 갖추는 제2 NIC 어드레스 변환 테이블

을 더 갖추고,

상기 어드레스 변환 처리부는 상기 수신 패킷에 첨부되고 있는 송신원 포트 번호를 상기 제1 NIC 어드레스 변환 테이블의 상기 제1 색인용 포트 번호 필드에 기록한 상기 색인용 포트 번호로 변환함과 동시에, 상기 송신 패킷에 첨부되고 있는 목적지 포트 번호로 상기 제2 NIC 어드레스 변환 테이블의 상기 제2 색인용 포트 번호 필드를 검색하여, 복원해야 할 레코드를 특정하는,

네트워크 게이트웨이 장치.

청구항 11

제1항에 있어서,

송신원 IP 어드레스 필드와, 송신원 포트 번호 필드와, 목적지 IP 어드레스 필드와, 목적지 포트 번호 필드를 가지는 확장 TCP 처리 대상 마스터

를 더 갖추고,

상기 어드레스 변환 처리부는, 상기 제1 NIC로부터 수신한 TCP 패킷의 송신원 및 목적지의 IP 어드레스 및 포트 번호의 조합이 상기 확장 TCP 처리 대상 마스터에 등록되어 있으면, 상기 제1 NIC로부터 수신한 수신 패킷에 첨부되고 있는 상기 송신원 MAC 어드레스, 상기 송신원 IP 어드레스, 상기 목적지 MAC 어드레스 및 상기 목적지 IP 어드레스를 변환하고, 상기 제1 NIC로부터 수신한 패킷이 상기 확장 TCP 처리 대상 마스터에 등록되어 있지 않으면, 상기 제1 NIC로부터 수신한 수신 패킷을 상기 제1 NIC로부터 제2 NIC로 전송하는, 네트워크 게이트웨이 장치.

청구항 12

제11항에 있어서,

상기 어드레스 변환 처리부는,

상기 제1 NIC로부터 수신한 TCP 패킷의 송신원 및 목적지의 IP 어드레스 및 포트 번호의 조합이 상기 확장 TCP 처리 대상 마스터에 등록되어 있으면, 상기 제1 NIC로부터 수신한 수신 패킷에 첨부되고 있는 상기 송신원 MAC 어드레스, 상기 송신원 IP 어드레스, 상기 목적지 MAC 어드레스 및 상기 목적지 IP 어드레스를 변환하고,

상기 제1 NIC로부터 수신한 TCP 패킷이 상기 확장 TCP 처리 대상 마스터에 등록되어 있지 않고, 또한 상기 TCP 패킷의 목적지 IP 어드레스가 상기 제1 NIC에 본래 첨부되고 있는 IP 어드레스일 경우에는, 상기 TCP 패킷을 그대로 상기 TCP/IP 프로토콜 스택으로 전송하는,

네트워크 게이트웨이 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은, 네트워크 게이트웨이 장치에 관한 것이다.

[0002] 보다 상세하게는, 기존의 네트워크 환경에 대해 아무런 설정 변경을 강요하지 않고, 용이하게 시큐리티를 높인 암호화 통신기능을 추가할 수 있는 네트워크 게이트웨이 장치에 관한 것이다.

배 경 기 술

[0003] 발명자는, 인터넷이 폭발적으로 일반층에 보급되는 조기 단계부터, TCP/IP 네트워크의 가능성과 기술적 한계, 그리고 문제점을 인식하고 있었다. 예를 들면, 인터넷 메일은 기본적으로 엽서와 동등하며, 통신 경로 상에서 탭핑(tapping: 도청)을 수행하면 용이하게 메일 헤더 및 본문을 취득할 수 있다. 그리고, 인터넷 메일이나 web 등의 통신 어플리케이션에, 시큐리티를 향상시키기 위한 암호화를 수행 시에는, 모든 어플리케이션 프로그램이 대응하고 있었다. 이 때문에, 암호화 통신에 대응하는 어플리케이션은 암호화 통신에 대응하지 않는 어플리케이션과 암호화 통신을 행하지 못하고, 언제까지 지나도 암호화 통신 대응 어플리케이션이 보급되지 않는다, 라는 딜레마에 빠져 있었다.

[0004] 또한, 암호화 통신 환경이 좀처럼 보급되지 않는다, 라는 같은 문제점은, 네트워크층(network layer)에서 암호화 통신을 실현하는 IPSec에도 말할 수 있다. 어플리케이션층(applcation Layer)의 어프로치가 아닌, 네트워크층에서 모든 통신을 통째로 암호화한다, 라는 IPSec의 기본적 기술 사상은 좋은 착안점일 것이다. 그러나, 현실적으로는 연결되기 어렵다, 연결될 때까지의 설정이 힘들다, 통신이 끊어지지 쉽다, 혹은 유저 인증을 별도로 고려하지 않으면 안 된다 등의 문제점이 지적되어, 근본적인 해결이 이루어지지 않고 보급의 목표도 세워지지 않은 채 현재에 이르고 있다.

[0005] 이러한 TCP/IP 네트워크의 가능성과 기술적 한계, 그리고 문제점을 감안하여, 발명자는 트랜스포트층(transport layer)에서 인증 및 암호화 통신을 실현하는 기술을 발명하고, 오늘에 이르기까지 그 기술의 실장과 개량에 노력하고 있다. 또한, 본 명세서에서는 이후, 특허문헌 1에 개시한 기술에 근거하는, 트랜스포트층에서의 인증 및 암호화의 기술을, TCP의 확장(eXPand)이라는 의미를 담아 「XPTCP」로 칭한다.

[0006] 특허문헌 1은, 발명자에 의한 트랜스포트층의 암호화 프로토콜에 관한 선행기술문헌이다.

[0007] 특허문헌 1: 일본 특허 3783142호 공보

발명의 내용

[0008] 특허문헌 1에 개시한 XPTCP를 기존의 네트워크 환경에 도입할 때, 그 도입 장벽은 가능한 낮은 것이 바람직하다. 이상적으로는, 네트워크 상의 모든 단말이 「제로 컨피그레이션(Zero Configuration)」, 즉 전혀 설정 등을 변경하거나 신규의 소프트웨어를 도입하지 않고, XPTCP가 제공하는 새로운 기능을 이용할 수 있게 되는 것이 바람직하다.

[0009] 단말에 소프트웨어를 도입하지 않고 신기능을 실현하는 방법으로서, 네트워크의 경로 상에 게이트웨이 장치를 개입시키는 방법을 생각할 수 있다. 그러나, 이 게이트웨이 장치는, 지금까지 알려져 있는 장치나 어플리케이션의 양태에서는, 무슨 일이 있어도 단말의 설정 변경이 필요하게 된다.

[0010] 예를 들면, 게이트웨이 장치가 프록시 서버일 경우, 단말은 프록시 서버 대응 어플리케이션 프로그램을 이용해, 어플리케이션 프로그램에는 프록시 서버의 IP 어드레스와 포트 번호를 설정해야 한다. 즉, 어플리케이션 프로그램이 프록시 서버에 대응하지 않으면, 프록시 서버를 통한 통신 그 자체를 실현할 수 없다.

[0011] 또한 예를 들면, 게이트웨이 장치가 라우터일 경우, 단말은 디폴트 게이트웨이의 IP 어드레스를 다시 설정하지 않으면 안 된다.

[0012] 게다가, 게이트웨이 장치가 기존의 네트워크 환경에 도입되는 것을 생각하면, 게이트웨이 장치를 위한 비어 있는 IP 어드레스를 확보해야 하는 것 외에, 이미 디폴트 게이트웨이가 되고 있는 라우터 등, 다른 네트워크 장치에도 설정 변경이 필요하게 될 수도 있다.

[0013] 본 발명은 이러한 과제를 해결하고, 기존의 네트워크 환경에 대해 설정 변경을 조금도 강요하지 않고, 용이하게 시큐리티를 높인 암호화 통신기능을 추가할 수 있는 네트워크 게이트웨이 장치를 제공하는 것을 목적으로 한다.

[0014] 상기 과제를 해결하기 위해, 본 발명의 네트워크 게이트웨이 장치는, 내측 NIC와, 외측 NIC와, 내측 NIC 및 외측 NIC에 프로미스큐어스 모드(promiscuous mode)를 설정하는 초기 설정부와, 내측 NIC 및 외측 NIC 사이에서 TCP/IP 통신 처리를 수행하는 TCP/IP 프로토콜 스택과, 내측 NIC로부터 수신한 수신 패킷에 첨부되고 있는 송신원 MAC 어드레스를 제1 위장 MAC 어드레스로 변환하고, 송신원 IP 어드레스를 제1 위장 IP 어드레스로 변환하고, 목적지 MAC 어드레스를 내측 NIC에 첨부되고 있는 내측 NICMAC 어드레스로 변환하고, 목적지 IP 어드레스를 내측 NIC에 첨부되고 있는 내측 NICIP 어드레스로 변환하여, TCP/IP 프로토콜 스택에 수신 패킷을 송신함과 동시에, TCP/IP 프로토콜 스택으로부터 수신한 송신 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 수신 패킷에 첨부되고 있던 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스로 복원(restore)하여, 외측 NIC에 송신하는 어드레스 변환 처리부를 구비한다.

[0015] 내측 NIC 및 외측 NIC에 할당되고 있는 IP 어드레스와는 무관계여야 할 패킷을 TCP/IP 프로토콜 스택이 처리할 수 있도록 하기 위해, 수신 패킷에 첨부되고 있는 송신원 MAC 어드레스 및 송신원 IP 어드레스는 가짜의 MAC 어드레스 및 가짜의 IP 어드레스로, 목적지 MAC 어드레스 및 목적지 IP 어드레스는 내측 NIC에 할당되고 있는 IP 어드레스 및 MAC 어드레스로 개서(改書)하고 나서, TCP/IP 프로토콜 스택에게 준다.

[0016] 본 발명에 의해, 기존의 네트워크 환경에 대해 설정 변경을 어떤 강요하지 않고, 용이하게 시큐리티를 높인 암호화 통신기능을 추가할 수 있는 네트워크 게이트웨이 장치를 제공할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시 형태에 따른 네트워크 게이트웨이 장치를 포함한 네트워크의 개략도이다.

도 2는 XPTCP 게이트웨이 장치의 기능 블록도이다.

도 3은 XPTCP 게이트웨이 장치에 갖춰지고 있는 각종 테이블 및 리스트의 필드 구성을 나타내는 도면이다.

도 4는 패킷의 구조를 나타내는 개략도이다.

도 5는 어드레스 변환 처리부의 기능 블록도이다.

도 6은 내측 NIC 수신 처리부의 기능 블록도이다.

도 7은 외측 NIC 수신 처리부의 기능 블록도이다.

도 8은 외측 NIC 송신 처리부의 기능 블록도이다.

도 9는 내측 NIC 송신 처리부의 기능 블록도이다.

도 10은 XPTCP 처리부의 기능 블록도이다.

도 11은 어드레스 변환 처리부의, 내측 NIC에서의 패킷 수신 처리 동작의 흐름을 나타내는 플로우 차트이다.

도 12는 어드레스 변환 처리부의, 외측 NIC에서의 패킷 수신 처리 동작의 흐름을 나타내는 플로우 차트이다.

도 13은 어드레스 변환 처리부의, 외측 NIC에서의 패킷 송신 처리 동작의 흐름을 나타내는 플로우 차트이다.

도 14는 어드레스 변환 처리부의, 내측 NIC에서의 패킷 송신 처리 동작의 흐름을 나타내는 플로우 차트이다.

도 15는 XPTCP 처리부의 XPTCP 처리의 흐름을 나타내는 플로우 차트이다.

도 16은 소켓 처리부의 초기 동작의 흐름을 나타내는 플로우 차트이다.

도 17은 소켓 처리부의 접속 요구 전송 처리의 흐름을 나타내는 플로우 차트이다.

도 18은 XPTCP 게이트웨이 장치를 통과하는 패킷의 변화를 나타내는 개략도이다.

도 19는 XPTCP 게이트웨이 장치를 통과하는 패킷의 변화를 나타내는 개략도이다.

도 20은 XPTCP 게이트웨이 장치를 통과하는 패킷의 변화를 나타내는 개략도이다.

도 21은 XPTCP 게이트웨이 장치에서의, TCP 접속 확립 시퀀스를 나타내는 타임 차트의, 전체를 나타내는 조감도이다.

도 22는 XPTCP 게이트웨이 장치에서의, TCP 접속 확립 시퀀스를 나타내는 타임 차트 중, 전반의 처리 내용을 나타내는 상세도이다.

도 23은 XPTCP 게이트웨이 장치에서의, TCP 접속 확립 시퀀스를 나타내는 타임 차트 중, 후반의 처리 내용을 나타내는 상세도이다.

도 24는 XPTCP 게이트웨이 장치에서의, TCP 데이터 전송 시퀀스의 타임 차트이다.

도 25는 XPTCP 게이트웨이 장치에서의, TCP 절단 시퀀스를 나타내는 타임 차트의, 전체를 나타내는 조감도이다.

도 26은 XPTCP 게이트웨이 장치에서의, TCP 절단 시퀀스를 나타내는 타임 차트 중, 전반의 처리 내용을 나타내는 상세도이다.

도 27은 XPTCP 게이트웨이 장치에서의, TCP 절단 시퀀스를 나타내는 타임 차트 중, 후반의 처리 내용을 나타내는 상세도이다.

도 28은 XPTCP 게이트웨이 장치에서, 송신하는 패킷의 목적지 IP 어드레스를 개서하는 응용 형태를 설명하는 개략도이다.

도 29는 XPTCP 게이트웨이 장치에서, 송신하는 패킷의 송신원 IP 어드레스를 개서하는 응용 형태를 설명하는 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0018] [네트워크의 개략]

[0019] 도 1은, 본 발명의 실시 형태에 따른 네트워크 게이트웨이 장치를 포함한 네트워크의 개략도이다.

[0020] 본 실시 형태의 네트워크 게이트웨이 장치는 XPTCP 기능을 제공하므로, 이후, 네트워크 게이트웨이 장치를 XPTCP 게이트웨이 장치(101)로 칭한다.

[0021] 도 1에는, XPTCP 게이트웨이 장치(101)를 포함한 네트워크가 나타나고 있다.

[0022] XPTCP 게이트웨이 장치(101)를 통해 좌측에는, XPTCP에 비대응인 2대의 단말, XPTCP 비대응 PC(102) 및 XPTCP 비대응 PC(103)가, XPTCP 게이트웨이 장치(101)의 내측 NIC(104)에 접속되고 있다.

[0023] XPTCP 게이트웨이 장치(101)를 통해 우측에는, XPTCP에 비대응인 단말인 XPTCP 비대응 PC(105)와, XPTCP에 대

응하고 있는 단말인 XPTCP 대응 PC(106), 및 XPTCP에 대응하고 있는 서버인 XPTCP 대응 서버(107)가, XPTCP 게이트웨이 장치(101)의 외측 NIC(108)에 접속되고 있다.

[0024] 이후, XPTCP 게이트웨이 장치(101)를 통해 좌측의 네트워크를 XPTCP 비대응 네트워크(109)로, XPTCP 게이트웨이 장치(101)를 통해 우측의 네트워크를 XPTCP 대응 네트워크(110)로 각각 칭한다.

[0025] 즉, XPTCP 게이트웨이 장치(101)는, 제1 NIC라고도 할 수 있는 내측 NIC(104)가 XPTCP 비대응 네트워크(109)에 접속되고, 제2 NIC라고도 할 수 있는 외측 NIC(108)가 XPTCP 대응 네트워크(110)에 접속된다.

[0026] XPTCP 게이트웨이 장치(101)는, XPTCP 비대응 네트워크(109)에 존재하는 XPTCP 비대응 PC(102) 및 XPTCP 비대응 PC(103)와 같은, XPTCP 비대응인 네트워크 기기를, XPTCP 대응 네트워크(110)에 존재하는 XPTCP 대응 PC(106) 및 XPTCP 대응 서버(107)와 같은, XPTCP 대응인 네트워크 기기에, XPTCP의 기능으로 접속할 수 있도록, 패킷을 가공한다.

[0027] XPTCP 게이트웨이 장치(101)는, 내측 NIC(104)에 접속되고 있는 XPTCP 비대응 PC(102)에 대해, XPTCP의 기능을 제공한다. 구체적으로는, XPTCP 비대응 네트워크(109) 상의 XPTCP 비대응 PC(102)가 XPTCP 대응 네트워크(110) 상의 XPTCP 비대응 PC(105)에 접속하려고 하는 경우에는, XPTCP 게이트웨이 장치(101)는 패킷을 그대로 흐르게 해서, 종래와 같은 일반적인 TCP/IP 네트워크에서의 통신을 수행한다. 그러나, XPTCP 비대응 네트워크(109) 상의 XPTCP 비대응 PC(102)가 XPTCP 대응 네트워크(110) 상의 XPTCP 대응 PC(106) 혹은 XPTCP 대응 서버(107)에 접속하려고 하는 경우에는, XPTCP 게이트웨이 장치(101)는 XPTCP 비대응 PC(102)로부터 송신되는 패킷을 XPTCP에 대응한 패킷으로 개서하여, XPTCP 대응 PC(106) 혹은 XPTCP 대응 서버(107)에 송신한다.

[0028] [XPTCP 게이트웨이 장치(101)의 내부 구성]

[0029] 도 2는 XPTCP 게이트웨이 장치(101)의 기능 블록도이다.

[0030] XPTCP 게이트웨이 장치(101)는, 네트워크 OS가 가동하는 컴퓨터에 XPTCP 게이트웨이 장치(101)로서 가동하기 위한 프로그램을 도입 함으로써 실현될 수 있다. 네트워크 OS는, 예를 들면 주지의 Windows(등록상표) 혹은 Linux(등록상표) 등의 OS가 이용 가능하다. 단, XPTCP 게이트웨이 장치(101)는 네트워크의 경로 상에 설치될 필요가 있으므로, 컴퓨터에는 2개의 NIC(Network Interface Card)가 갖춰질 필요가 있다. 이것이 내측 NIC(104)와 외측 NIC(108)이다.

[0031] 내측 NIC(104)와 외측 NIC(108)는, 각각 주지의 TCP/IP 네트워크에 접속하기 위한, 일반적인 인터페이스 카드이다. 따라서, 내측 NIC(104)와 외측 NIC(108)에는 각각 주지의 또한 고유의, 48 비트의 MAC 어드레스(Media Access Control address)를 가진다. 또한, 도 2에 기능 블록으로서 나타내는 내측 NIC(104)와 외측 NIC(108)는, 하드웨어로서의 NIC 그 자체뿐 아니라, 디바이스 드라이버의 기능도 포함하고 있다.

[0032] 초기 설정부(201)는, 네트워크 OS가 기동했을 때에 설정되는 네트워크의 기본 설정 작업에 더해, 내측 NIC(104)와 외측 NIC(108)에 「프로미스큐어스 모드(promiscuous mode)」를 설정한다. 「무차별 모드」라고도 하는 이 모드는, 네트워크 상을 흐르는 모든 패킷을 수신해 읽어 들일 수 있다. 본 실시 형태의 XPTCP 게이트웨이 장치(101)에는 필요한 설정이다.

[0033] 도시하지 않은 네트워크 OS는, 기동 시에 네트워크의 기본 설정을 수행한다. 그 때의, 내측 NIC(104) 및 외측 NIC(108)의 MAC 어드레스 및 IP 어드레스는, 네트워크 설정 정보 메모리(202)에 기억된다.

[0034] 어드레스 변환 처리부(203)는, 내측 NIC(104)로부터 수신한 패킷에 대해, 네트워크 설정 정보 메모리(202), 임시 IPMAC 리스트(204) 및 내측 NIC 어드레스 테이블(209)로부터 각각 정보를 읽어 들여, 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스 및 목적지 IP 어드레스를, 제1 임시 NICMAC 어드레스, 제1 임시 NICIP 어드레스, 색인용 포트 번호, 내측 NICMAC 어드레스 및 내측 NICIP 어드레스로 변환하고, OS에 갖춰지는 TCP/IP 프로토콜 스택(205)에 인도(引渡)한다. 또한, 목적지 포트 번호는 그대로 변경하지 않는다.

[0035] 마찬가지로, 어드레스 변환 처리부(203)는, 외측 NIC(108)로부터 수신한 패킷에 대해, 네트워크 설정 정보 메모리(202), 임시 IPMAC 리스트(204) 및 외측 NIC 어드레스 테이블(210)로부터 각각 정보를 읽어 들여, 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를, 제2 임시 NICMAC 어드레스, 제2 임시 NICIP 어드레스, 색인용 포트 번호, 외측 NICMAC 어드레스, 외측 NICIP 어드레스 및 동적 포트 번호로 변환하고, OS에 갖춰지는 TCP/IP 프로토콜 스택

(205)에 인도한다.

[0036] 또한, 어드레스 변환 처리부(203)는, TCP/IP 프로토콜 스택(205)에서 외측 NIC(108)로 송신되는 패킷에 대해, 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를, 색인용 포트 번호를 단서로 외측 NIC 어드레스 테이블(210)을 참조하여, 앞서 개서하기 이전으로 복원한 후, 외측 NIC(108)로부터 송신한다.

[0037] 마찬가지로, 어드레스 변환 처리부(203)는, TCP/IP 프로토콜 스택(205)에서 내측 NIC(104)로 송신되는 패킷에 대해, 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를, 색인용 포트 번호를 단서로 내측 NIC 어드레스 테이블(209)을 참조하여, 앞서 개서하기 이전으로 복원한 후, 내측 NIC(104)로부터 송신한다.

[0038] 게다가, 어드레스 변환 처리부(203)는, TCP/IP 프로토콜 스택(205)에서 외측 NIC(108)로 송신되는 ARP(Address Resolution Protocol) 요구 패킷에 대해, 임시 IPMAC 리스트(204)에 기재되어 있는 가짜의 MAC 어드레스로 응답 함으로써, 마치 물리 매체에서 응답이 있던 것처럼 TCP/IP 프로토콜 스택(205)을 속여 정상으로 동작시킨다.

[0039] 제1 NIC 어드레스 변환 테이블이라고도 할 수 있는 내측 NIC 어드레스 테이블(209)은, 어드레스 변환 처리부(203)가 내측 NIC(104)와 TCP/IP 프로토콜 스택(205)과의 사이에서, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를 개서하거나 또는 복원하기 위한 테이블이다.

[0040] 제2 NIC 어드레스 변환 테이블이라고도 할 수 있는 외측 NIC 어드레스 테이블(210)은, 어드레스 변환 처리부(203)가 외측 NIC(108)와 TCP/IP 프로토콜 스택(205) 사이에서, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를 개서하거나 또는 복원하기 위한 테이블이다.

[0041] 이들 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)은, 어드레스 변환 테이블이라고도 할 수 있다.

[0042] 또한, 설명의 편의를 위해, 이하에서는, XPTCP 비대응 네트워크(109)에 존재하는 XPTCP 비대응 PC(102, 103) 등의 XPTCP에 비대응인 네트워크 기기를 「단말」로 칭하고, XPTCP 대응 네트워크(110)에 존재하는 XPTCP 대응 서버(107)나 XPTCP 대응 PC(106) 등의 XPTCP에 대응하고 있는 네트워크 기기를 「서버」로 칭한다. XPTCP 비대응 PC(105)에 대해서는, XPTCP를 이용한 통신의 대상 외이므로, 「단말」「서버」의 정의에서는 제외한다.

[0043] TCP/IP 프로토콜 스택(205)은, 네트워크 OS에 갖춰지는 네트워크 드라이버 프로그램이다. 이 TCP/IP 프로토콜 스택(205)은, 어드레스 변환 처리부(203)를 경유하여, NIC와의 사이에서 패킷의 송수신을 수행하고, 어플리케이션 프로그램과의 사이에서 데이터의 송수신을 수행한다.

[0044] TCP/IP 프로토콜 스택(205)은 어플리케이션 프로그램에 대해, 주지의 소켓(「BSD 소켓」이라는 명칭으로 주지이다.)이라고 하는 어플리케이션 프로그램 인터페이스(API)를 제공한다.

[0045] TCP/IP 프로토콜 스택(205)은, NIC로부터 수신한 패킷을, ARP 헤더, IP 헤더, TCP 또는 UDP 헤더의 순서로 제거하고, 패킷의 페이로드(payload)를 연결해 스트림 데이터로 되돌려, 소정의 어플리케이션에 인도한다.

[0046] 반대로, TCP/IP 프로토콜 스택(205)은, 어플리케이션으로부터 받은 스트림 데이터를, TCP/IP 프로토콜 스택(205)이 사전에 형성해 어플리케이션으로부터 지정된 소켓을 통해, 소정의 데이터 사이즈의 페이로드로 분할한 후, TCP 또는 UDP 헤더, IP 헤더, ARP 헤더의 순서로 헤더를 부가해, NIC를 통해 송신지로 송신한다.

[0047] 특히, TCP 프로토콜의 패킷을 취급하는 경우에는, TCP/IP 프로토콜 스택(205)은, 주지의 커넥션이라는 가상적인 통신로를, SYN-ACK&SYN-ACK라는 주지의 3-웨이 핸드쉐이킹(three-way handshaking)으로 TCP/IP 프로토콜 스택(205)의 내부에 형성한다.

[0048] 본 실시 형태의 XPTCP 게이트웨이 장치(101)는, 내측 NIC(104)와 외측 NIC(108) 쌍방으로 커넥션을 형성하고, 그 커넥션끼리 데이터의 전송을 수행한다.

[0049] 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)은, TCP/IP 프로토콜 스택(205)이 작성하는 커넥션과, 실제 패킷에 첨부되고 있는 본래의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호와의 연관지음을, 색인용 포트 번호를 마련 함으로써 실현하고 있다.

[0050] 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)은, TCP/IP 프로토콜 스택(205)이 작성하는

커넥션을 관리하는 테이블이다, 라고도 할 수 있다.

[0051] 확장 TCP 처리부라고도 할 수 있는 XPTCP 처리부(206)는, TCP/IP 프로토콜 스택(205)이 형성한 소켓, 즉 「한쪽의 커넥션의 출입구」로부터 데이터를 수신해, 수신한 데이터를 TCP/IP 프로토콜 스택(205)이 형성한 다른 소켓, 즉 「다른 쪽의 커넥션의 출입구」로 전송한다.

[0052] 또한, XPTCP 처리부(206)는 XPTCP 처리 대상 마스터(208)에 기억되고 있는 지시 내용에 따라, 인증 처리 및 암호화 통신 처리를 수행한다. 특히 XPTCP 처리부(206)는, TCP/IP 프로토콜 스택(205)으로부터 수신한 데이터를 다시 TCP/IP 프로토콜 스택(205)으로 반송할 때에, 소켓에 첨부되고 있는 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스, 목적지 포트 번호를 개서한다.

[0053] 소켓 처리부(207)는, 네트워크 OS 기동 후에 자동 실행되는 작은 의사 서버 프로그램임과 동시에, 내측 NIC(104)로부터 수신한 패킷에 기인 하여, TCP/IP 프로토콜 스택(205)으로부터 connect 이벤트를 받으면, connect 이벤트를 받은 소켓에 첨부되고 있는 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스, 목적지 포트 번호로부터, 외측 NIC(108)를 향해 새로운 소켓을 작성하기 위한 connect request 이벤트, 즉 접속 요구를 TCP/IP 프로토콜 스택(205)을 향해 발생한다.

[0054] 소켓 처리부(207)는 TCP/IP 프로토콜 스택(205)에 대해 소켓 오픈/클로즈 처리만 수행하고, TCP/IP 프로토콜 스택(205)과의 실제의 데이터 송수신은 XPTCP 처리부(206)가 수행한다.

[0055] 도 2에 나타내는 XPTCP 게이트웨이 장치(101)의 블록도 가운데, 내측 NIC(104), 외측 NIC(108), 어드레스 변환 처리부(203), TCP/IP 프로토콜 스택(205), XPTCP 처리부(206) 및 소켓 처리부(207)는, 주지의 7 계층 OSI 참조 모델에 준거하는, TCP/IP의 계층 모델을 따르고 있다.

[0056] 내측 NIC(104)와 외측 NIC(108)는, NIC 드라이버를 포함해 물리층(physical layer)과 데이터 링크층(data link layer)에 해당한다.

[0057] TCP/IP 프로토콜 스택(205)은, 네트워크층(IP, ICMP(Internet Control Message Protocol), ARP)와 트랜스포트층(TCP, UDP)에 해당한다.

[0058] 소켓 처리부(207)는 어플리케이션층에 해당한다.

[0059] 어드레스 변환 처리부(203)는 데이터 링크층과 네트워크층의 사이에 들어가서, TCP/IP 프로토콜 스택(205)이 본래라면 무관계여야 할 패킷을 처리할 수 있도록, 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 개서한다. 이 때문에, 어드레스 변환 처리부(203)는 네트워크층에 해당한다.

[0060] XPTCP 처리부(206)는 트랜스포트층과 어플리케이션층 사이에 개재하여, 소켓 오픈/클로즈 처리 이외의, 네트워크 스트림 데이터의 전송과, 인증 및 암호화 혹은 복호를 수행한다. 이 때문에, XPTCP 처리부(206)는 어플리케이션층이 개재할 수 없는 인증 및 암호화 통신을 실현하는 트랜스포트층에 해당함과 동시에, 데이터를 전송한다라는 기능에 있어서 어플리케이션층에도 해당한다.

[0061] 네트워크 OS에 표준 탑재되고 있는 TCP/IP 프로토콜 스택(205)은, 본래라면 네트워크 설정 정보 메모리(202)에 기억되고 있는 IP 어드레스, 즉 자신의 NIC에 첨부되고 있는 IP 어드레스에 대한 통신밖에 취급하지 않는다. 한편, XPTCP 게이트웨이 장치(101)는 모든 패킷을 취급할 필요가 있다. 또한, XPTCP는 통신 순서가 복잡한 TCP/IP의 기능을 이용하면서, 트랜스포트층에서의 인증과 암호화 처리를 실현한다.

[0062] 그래서, TCP/IP 프로토콜 스택(205)의 기능을 최대한 유효하게 활용하면서, 필요 최소한의 프로그램을 추가 함으로써 XPTCP 게이트웨이 장치(101)를 실현하기 위해, 본 실시 형태의 XPTCP 게이트웨이 장치(101)는, TCP/IP 프로토콜 스택(205)을 「속이는」 처리를 행한다.

[0063] 즉, XPTCP 게이트웨이 장치(101)에 할당되고 있는 IP 어드레스와는 무관계여야 할 패킷을 TCP/IP 프로토콜 스택(205)이 처리할 수 있도록 하기 위해서, 내측 NIC(104) 또는 외측 NIC(108)로부터 수신한 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를, 일단, XPTCP 게이트웨이 장치(101)에 할당되고 있는 IP 어드레스, MAC 어드레스 등에 개서한다. 그리고, 송신원 및 목적지의 MAC 어드레스, IP 어드레스 및 포트 번호를 개서한 해당 패킷을 TCP/IP 프로토콜 스택(205)에 인도한다.

[0064] 어드레스 변환 처리부(203) 및 XPTCP 처리부(206)에서 수행하는 개서 처리, 즉 패킷에 첨부되고 있는 송신원 및 목적지의 MAC 어드레스, IP 어드레스 그리고 포트 번호의 개서 처리의 상세는, 도 18, 도 19 및 도 20에서 후술

한다.

[0065] [테이블 및 리스트의 구성]

[0066] 도 3은, XPTCP 게이트웨이 장치(101)에 갖춰지고 있는 각종 테이블 및 리스트의 필드 구성을 나타내는 도면이다.

[0067] 도 2에 나타내는 XPTCP 게이트웨이 장치(101)가 보유하는, 내측 NIC 어드레스 테이블(209), 외측 NIC 어드레스 테이블(210), XPTCP 폴리시 테이블(211), 임시 IPMAC 리스트(204)는, 도시하지 않은 RAM 내에 설치된다. 또한, XPTCP 처리 대상 마스터(208)는 하드 디스크 장치 등의 도시하지 않은 불휘발성 스토리지에 설치되어, 어드레스 변환 처리부(203)가 기동할 때, 도시하지 않은 RAM 내에 복사된다. 네트워크 설정 정보 메모리(202)는 네트워크 OS에 의해 도시하지 않은 RAM 내에 설치된다.

[0068] 도 4는 패킷의 구조를 나타내는 개략도이다. 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 필드를, 도 3의 필드 구성도와 도 4의 개략도를 참조해 설명한다.

[0069] 내측 NIC 어드레스 테이블(209)은, 프로토콜 종별 필드와, 송신원 MAC 어드레스 필드와, 송신원 IP 어드레스 필드와, 송신원 포트 번호 필드와, 목적지 MAC 어드레스 필드와, 목적지 IP 어드레스 필드와, 목적지 포트 번호 필드와, 색인용 포트 번호 필드와, 타이머용 카운터 값 필드를 가진다.

[0070] 외측 NIC 어드레스 테이블(210)은, 프로토콜 종별 필드와, 송신원 MAC 어드레스 필드와, 송신원 IP 어드레스 필드와, 송신원 포트 번호 필드와, 목적지 MAC 어드레스 필드와, 목적지 IP 어드레스 필드와, 목적지 포트 번호 필드와, 색인용 포트 번호 필드와, 동적 포트 번호 필드와, 타이머용 카운터 값 필드를 가진다.

[0071] 프로토콜 종별 필드에는, 내측 NIC(104) 또는 외측 NIC(108)로부터 들어오는 패킷의 종별로서, TCP 또는 UDP를 나타내는 플래그가 격납된다. 이는 IP 헤더(401)의 프로토콜 번호로부터 읽어낸다. 또한, 본 실시 형태의 XPTCP 게이트웨이 장치(101)는, 현 단계에서는 TCP 패킷만을 취급하지만, 가까운 장래에 UDP 패킷을 처리 가능하게 하기 위해, 이 프로토콜 종별 필드가 준비되어 있다.

[0072] 송신원 MAC 어드레스 필드에는, 내측 NIC(104) 또는 외측 NIC(108)로부터 들어오는 패킷에 첨부되고 있는 송신원 MAC 어드레스가 격납된다. 이는 MAC 헤더(402)의 송신원 MAC 어드레스로부터 읽어낸다.

[0073] 송신원 IP 어드레스 필드에는, 내측 NIC(104) 또는 외측 NIC(108)로부터 들어오는 패킷에 첨부되고 있는 송신원 IP 어드레스가 격납된다. 이는 IP 헤더(401)의 송신원 IP 어드레스로부터 읽어낸다.

[0074] 송신원 포트 번호 필드에는, 내측 NIC(104) 또는 외측 NIC(108)로부터 들어오는 패킷에 첨부되고 있는 송신원 포트 번호가 격납된다. 이는 TCP 헤더(403) 또는 UDP 헤더(404)의 송신원 포트 번호로부터 읽어낸다.

[0075] 목적지 MAC 어드레스 필드에는, 내측 NIC(104) 또는 외측 NIC(108)로부터 들어오는 패킷에 첨부되고 있는 목적지 MAC 어드레스가 격납된다. 이는 MAC 헤더(402)의 목적지 MAC 어드레스로부터 읽어낸다.

[0076] 목적지 IP 어드레스 필드에는, 내측 NIC(104) 또는 외측 NIC(108)로부터 들어오는 패킷에 첨부되고 있는 목적지 IP 어드레스가 격납된다. 이는 IP 헤더(401)의 목적지 IP 어드레스로부터 읽어낸다.

[0077] 목적지 포트 번호 필드에는, 내측 NIC(104) 또는 외측 NIC(108)로부터 들어오는 패킷에 첨부되고 있는 목적지 포트 번호가 격납된다. 이는 TCP 헤더(403) 또는 UDP 헤더(404)의 목적지 포트 번호로부터 읽어낸다.

[0078] 색인용 포트 번호 필드에는, 어드레스 변환 처리부(203)가 패킷을 내측 NIC(104) 또는 외측 NIC(108)로부터 송신하는 직전에, 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 개서할 때에, 내측 NIC 어드레스 테이블(209) 또는 외측 NIC 어드레스 테이블(210) 중 어느 레코드에 기술되고 있는지를 특정하기 위한 색인 정보가 격납된다.

[0079] 이 색인용 포트 번호는, XPTCP 처리 대상 마스터(208)의 레코드에 처리 대상으로서 합치하는 TCP SYN 패킷이 내측 NIC(104)로부터 왔을 때에, 어드레스 변환 처리부(203)가 내측 NIC 어드레스 테이블(209)에 신규 레코드를 추가로 기록할 때, 도 2의 TCP 포트 번호 메모리(212)의 값이 이용된다. 색인용 포트 번호는, 포트 번호를 색인 정보로서 이용하므로, 일의성(독특하고, 중복 하지 않는다)을 가지는 것이 요구된다. 이 때문에, TCP 포트 번호 메모리(212)의 값을 이용했을 때에, 이미 해당 번호가 사용되고 있는 경우에는, TCP 포트 번호 메모리(212)의 값을 인크리먼트(increment)해서, 해당 포트 번호가 비어 있는지 확인한다.

[0080] TCP SYN 패킷은, 주지의 TCP 통신의 개시(커넥션의 확립 요구)를 나타내는 패킷이며, TCP 헤더(403)에 존재하는

6비트의 코드비트 중 5번째 비트가 「1」인 패킷이다.

[0081] TCP ACK 패킷은, 주지의 TCP 통신에서의 확인 응답을 나타내는 패킷이며, TCP 헤더(403)에 존재하는 6비트의 코드비트 중 2번째 비트가 「1」인 패킷이다.

[0082] TCP FIN 패킷은, 주지의 TCP 통신의 종료(커넥션의 절단 요구)를 나타내는 패킷이며, TCP 헤더(403)에 존재하는 6비트의 코드비트 중 6번째 비트가 「1」인 패킷이다.

[0083] TCP ACK/SYN 패킷은, TCP 헤더(403)에 존재하는 6비트의 코드비트 중 2번째 비트와 5번째 비트가 「1」인 패킷이며, TCP SYN 패킷과 TCP ACK 패킷의, 2개의 의미를 동시에 갖추고 있다.

[0084] 외측 NIC 어드레스 테이블(210)에만 설치되고 있는 동적 포트 번호는, 동적 포트 번호 필드에 격납된다. 이 동적 포트 번호는, TCP/IP 프로토콜 스택(205)이 외측 NIC(108)를 통해, XPTCP 대응 네트워크(110)에 존재하는 XPTCP 대응 서버(107)나 XPTCP 대응 PC(106) 등의, XPTCP에 대응하고 있는 네트워크 기기, 즉 서버와의 커넥션을 형성할 때, 해당 커넥션의 송신원 포트 번호로서, TCP/IP 프로토콜 스택(205)이 자동적으로 생성하는 포트 번호이다. 많은 경우, 동적 포트 번호는 「수명이 짧은 포트」라고도 불리는 주지의 임시 포트 번호(ephemeral port number)인, 포트 번호 49152에서 65535까지의 번호가, TCP/IP 프로토콜 스택(205)에 의해 부여된다.

[0085] 타이머용 카운터 값 필드에는, 내측 NIC 어드레스 테이블(209) 또는 외측 NIC 어드레스 테이블(210)의 해당 레코드가 이용되지 않게 된 것을 판단하여 파기할 때의, 경과시간을 계측하기 위한 어드레스 테이블 갱신 카운터(213)의 값이 격납된다.

[0086] 도 3에 나타내는 네트워크 설정 정보 메모리(202)에는, 네트워크 OS가 기동할 때에 네트워크의 기본 설정을 수행한 결과인, 내측 NIC(104) 및 외측 NIC(108)의 MAC 어드레스 및 IP 어드레스가 기억된다. 즉, 네트워크 설정 정보 메모리(202)는 네트워크 OS에 의해 설치된다.

[0087] 내측 NICMAC 어드레스는, 내측 NIC(104)의, 본래의 MAC 어드레스를 나타낸다.

[0088] 내측 NICIP 어드레스는, 내측 NIC(104)의, 본래의 IP 어드레스를 나타낸다.

[0089] 외측 NICMAC 어드레스는, 외측 NIC(108)의, 본래의 MAC 어드레스를 나타낸다.

[0090] 외측 NICIP 어드레스는, 외측 NIC(108)의, 본래의 IP 어드레스를 나타낸다.

[0091] 마찬가지로 도 3에 나타내는 임시 IPMAC 리스트(204)는, 내측 NICIP 어드레스 필드와, 제1 임시 MAC 어드레스 필드와, 제1 임시 IP 어드레스 필드와, 외측 NICIP 어드레스 필드와, 제2 임시 MAC 어드레스 필드와, 제2 임시 IP 어드레스 필드를 가진다.

[0092] 내측 NICIP 어드레스 필드에는, 내측 NIC(104)의 IP 어드레스가 격납된다. 이는 네트워크 설정 정보 메모리(202)로부터 얻을 수 있다.

[0093] 제1 임시 MAC 어드레스 필드에는, 제1 임시 MAC 어드레스가 격납된다.

[0094] 제1 임시 IP 어드레스 필드에는, 제1 임시 IP 어드레스가 격납된다.

[0095] 외측 NICIP 어드레스 필드에는, 외측 NIC(108)의 IP 어드레스가 격납된다. 이는 네트워크 설정 정보 메모리(202)로부터 얻을 수 있다.

[0096] 제2 임시 MAC 어드레스 필드에는, 제2 임시 MAC 어드레스가 격납된다.

[0097] 제2 임시 IP 어드레스 필드에는, 제2 임시 IP 어드레스가 격납된다.

[0098] 제1 임시 MAC 어드레스, 제1 임시 IP 어드레스, 제2 임시 MAC 어드레스 및 제2 임시 IP 어드레스는, 어드레스 변환 처리부(203) 및 XPTCP 처리부(206)에서 이용하는, 가짜의 MAC 어드레스 및 IP 어드레스이다.

[0099] 마찬가지로 확장 TCP 처리 대상 마스터라고도 할 수 있는, 도 3에 나타내는 XPTCP 처리 대상 마스터(208)는, 레코드 번호 필드와, 프로토콜 종별 필드와, 송신원 IP 어드레스 필드와, 송신원 포트 번호 필드와, 목적지 IP 어드레스 필드와, 목적지 포트 번호 필드와, 암호 종별 타 필드를 가진다.

[0100] 레코드 번호 필드는, XPTCP 처리 대상 마스터(208)의 레코드 번호 그 자체이다. XPTCP 처리 대상 마스터(208)의 레코드를 일의에 식별하는 연번의 번호이다. 또한, 레코드 번호 필드에 격납하는 정보는, 후술하는 XPTCP 폴리시 테이블(211)에서 이용하는, 레코드를 일의에 식별하기 위한 정보이다. 따라서, 일의에 식별이

가능하면, 반드시 레코드 번호가 아니어도 무방하다.

[0101] 프로토콜 종별 필드에는, 내측 NIC(104)로부터 들어오는 패킷의 종별로서 TCP 또는 UDP를 나타내는 플래그가 격납된다. 이는 IP 헤더(401)의 프로토콜 번호로부터 읽어낸다.

[0102] 송신원 IP 어드레스 필드에는, 내측 NIC(104)로부터 들어오는 패킷에 첨부되고 있는 송신원 IP 어드레스가 격납된다. 이는 IP 헤더(401)의 송신원 IP 어드레스로부터 읽어낸다.

[0103] 송신원 포트 번호 필드에는, 내측 NIC(104)로부터 들어오는 패킷에 첨부되고 있는 송신원 포트 번호가 격납된다. 이는 TCP 헤더(403) 또는 UDP 헤더(404)의 송신원 포트 번호로부터 읽어낸다.

[0104] 목적지 IP 어드레스 필드에는, 내측 NIC(104)로부터 들어오는 패킷에 첨부되고 있는 목적지 IP 어드레스가 격납된다. 이는 IP 헤더(401)의 목적지 IP 어드레스로부터 읽어낸다.

[0105] 목적지 포트 번호 필드에는, 내측 NIC(104)로부터 들어오는 패킷에 첨부되고 있는 목적지 포트 번호가 격납된다. 이는 TCP 헤더(403) 또는 UDP 헤더(404)의 목적지 포트 번호로부터 읽어낸다.

[0106] 암호 종별 타 필드에는, 해당 XPTCP 세션에 이용하는 인증이나 암호의 종류 등의 정보가 격납된다.

[0107] 즉, XPTCP 처리 대상 마스터(208)에는, 단말에서 서버를 향해 송신되는 패킷의 IP 어드레스 및 포트 번호의 조합과, 그 IP 어드레스 및 포트 번호의 조합을 가지는 패킷에 의해, 내측 NIC(104) 및 외측 NIC(108)의 각각에 형성되는 커넥션을 통과하는 데이터 스트림에 적용하는, 암호화 등에 관한 정보가 기억된다.

[0108] 마찬가지로 도 3에 나타내는 XPTCP 폴리시 테이블(211)은, 프로토콜 종별 필드와, 색인용 포트 번호 필드와, 레코드 번호 필드를 가진다.

[0109] 프로토콜 종별 필드에는, XPTCP 처리 대상 마스터(208)와 같이, 내측 NIC(104)로부터 들어오는 패킷의 종별로서, TCP 또는 UDP를 나타내는 플래그가 격납된다. 이는 IP 헤더(401)의 프로토콜 번호로부터 읽어낸다.

[0110] 색인용 포트 번호 필드에는, 해당 세션의 패킷에 대해 어드레스 변환 처리부(203)에 의해 첨부되고 있는, 색인용 포트 번호가 격납된다.

[0111] 레코드 번호 필드는, XPTCP 처리 대상 마스터(208)의 레코드 번호 그 자체이다. 따라서, 이 필드에 기록되고 있는 레코드 번호로, XPTCP 처리 대상 마스터(208)의 레코드를 지정해, 해당 레코드의 암호 종별 타 필드를 참조한다.

[0112] XPTCP 폴리시 테이블(211)은, 색인용 포트 번호와 암호 종별 타 정보를 연관시킴으로써, 색인용 포트 번호에 따른 TCP 커넥션을 통과하는 데이터 스트림에 적용하는, 암호 종별 등을 특정한다.

[0113] 다시 도 2로 돌아와서, 각 부의 설명을 계속한다.

[0114] 어드레스 테이블 갱신 카운터(213)는, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의, 사용되지 않게 된 레코드를 삭제할 때에, 경과시간을 보기 위한 카운터이다. 어드레스 테이블 갱신 카운터(213)는, 일례로서는 0에서 119까지의 수를 계수하는 루프 카운터이다. 0부터 시작되어, 1초 마다 계수치가 1 인크리먼트하여, 119까지 계수하면, 다시 0부터 계수를 개시한다.

[0115] 어드레스 변환 처리부(203)는, 후술하는 TCP 절단 시퀀스에서, TCP FIN 패킷이 내측 NIC(104) 및 외측 NIC(108) 양쪽 모두로부터 온 것에 호응하여, 어드레스 테이블 갱신 카운터(213)의 값을, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 해당하는 레코드의, 타이머용 카운트 값 필드에 기입한다. 그리고, 타이머용 카운트 값 필드의 값과 현재의 어드레스 테이블 갱신 카운터(213)의 값을 비교해서, 60초 이상을 경과했다고 판단하면, 이미 그 레코드에 나타나는 통신 세션은 종료했다고 판단해, 해당 레코드를 삭제한다.

[0116] TCP 포트 번호 메모리(212)는, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 색인용 포트 번호 필드에 값을 기입하기 위한 포트 번호가 격납되는 메모리이다.

[0117] 내측 NIC(104)로부터 TCP SYN 패킷이 오면, 새로운 커넥션을 작성할 필요가 있다. 어드레스 변환 처리부(203)는 TCP/IP 프로토콜 스택(205)에 커넥션을 작성시키기 위해, 어드레스 변환 처리를 수행한다. 어드레스 변환 처리에 의해, TCP/IP 프로토콜 스택(205)은 본래의 송신원 IP 어드레스 및 목적지 IP 어드레스 등과는 다른, 가짜의 송신원 IP 어드레스 및 목적지 IP 어드레스 등이 첨부된 패킷에 대해, 커넥션을 형성한다.

[0118] 어드레스 변환 처리부(203)는, 가짜의 송신원 IP 어드레스 및 목적지 IP 어드레스 등을 패킷에 첨부할 때,

TCP/IP 프로토콜 스택(205)이 작성하는 커넥션과, 그 가짜의 송신원 IP 어드레스 및 목적지 IP 어드레스 등과의 관련지음을 수행하지 않으면 안 된다. 이 커넥션을 식별해서, 최종적으로 본래의 송신원 IP 어드레스 및 목적지 IP 어드레스 등으로 되돌리기 위해, 패킷에 식별 정보를 첨부할 필요가 있다. 이것이, 색인용 포트 번호이다.

[0119] 내측 NIC 어드레스 테이블(209)에 새로운 레코드가 작성되었을 때, TCP 포트 번호 메모리(212)의 값을 1 인크리먼트해서, 그 값을 색인용 포트 번호 필드에 기입한다.

[0120] 색인용 포트 번호는 TCP/IP 프로토콜 스택(205)이 인식 가능한 번호가 아니면 안되기 때문에, TCP 포트 번호 메모리(212)에 기입되는 최대치는 65535이다.

[0121] TCP 포트 번호 메모리(212)는, 「수명이 짧은 포트」라고도 불리는 주지의 임시(ephemeral) 포트 번호인, 포트 번호 49152에서 65535까지를 1씩 인크리먼트하는 값이 기입된다. 또한, TCP 포트 번호 메모리(212)는 루프 카운터로 구성해도 무방하다.

[0122] [어드레스 변환 처리부(203)의 내부 구성]

[0123] 도 5는, 어드레스 변환 처리부(203)의 기능 블록도이다.

[0124] 어드레스 변환 처리부(203)는, 내측 NIC 수신 처리부(501), 외측 NIC 수신 처리부(502), 외측 NIC 송신 처리부(503), 내측 NIC 송신 처리부(504), 테이블 갱신 처리부(505), 및 폴리시 회답부(506)의, 5개의 기능 블록으로 나뉘어진다.

[0125] 우선, 내측 NIC 수신 처리부(501)의 상세를 설명한다. 도 6은, 내측 NIC 수신 처리부(501)의 기능 블록도이다.

[0126] 내측 NIC(104)가 수신한 패킷은, 처음에 수신 패킷 판정부(601)가 XPTCP 처리 대상 마스터(208)를 참조하여, 해당 패킷이 XPTCP 처리의 대상이 되는지 여부 등을 판정한다.

[0127] 만약, 내측 NIC(104)가 수신한 패킷이, 예를 들면 ICMP 패킷이나 XPTCP 처리 대상 마스터(208)에 합치하지 않는 처리 대상 외 패킷일 경우에는, 수신 패킷 판정부(601)는 그 패킷을 그대로 외측 NIC(108)로 전송한다.

[0128] 만약, 내측 NIC(104)가 수신한 패킷이, XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷일 경우에는, 수신 패킷 판정부(601)는 그 패킷을 그대로 TCP/IP 프로토콜 스택(205)으로 전송한다.

[0129] 만약, 내측 NIC(104)로부터 입력된 패킷이 XPTCP 처리 대상 마스터(208)에 합치하는 처리 대상 패킷일 경우에는, 수신 패킷 판정부(601)는 다음으로 그 패킷의 상세를 본다.

[0130] 수신 패킷 판정부(601)는, 그 패킷이 TCP 데이터 패킷이면, 해당 TCP 데이터 패킷을 어드레스 치환부(602)에 인도한다.

[0131] 어드레스 치환부(602)는 내측 NIC 어드레스 테이블(209)을 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호로 검색하여, 레코드를 특정하고, 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서하여, TCP/IP 프로토콜 스택(205)으로 전송한다.

[0132] 수신 패킷 판정부(601)에서 처리하는 패킷이 TCP SYN 패킷이면, 그것은 내측 NIC 어드레스 테이블(209)에 미등록된 패킷이다. 그러므로, 수신 패킷 판정부(601)는 TCP SYN 패킷을 커넥션 등록 처리부(603)에 인도한다. 커넥션 등록 처리부(603)는, TCP SYN 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호로, 내측 NIC 어드레스 테이블(209)에 신규의 레코드를 추가로 기록한다. 그리고, TCP 포트 번호 메모리(212)의 값을 1 인크리먼트하여 참조하고, 그 값을 색인용 포트 번호로서 내측 NIC 어드레스 테이블(209)의 색인용 포트 번호 필드에 기록한다. 게다가, 같은 내용의 레코드를 외측 NIC 어드레스 테이블(210)에도 추가로 기록한다. 그 후, 커넥션 등록 처리부(603)는 TCP SYN 패킷을 어드레스 치환부(602)에 인도한다. 어드레스 치환부(602)는 전술한 TCP 데이터 패킷과 같이, TCP SYN 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서하여, TCP/IP 프로토콜 스택(205)으로 전송한다.

[0133] 수신 패킷 판정부(601)에서 처리하는 패킷이 TCP FIN 패킷이면, 그것은 TCP/IP 프로토콜 스택(205)에 형성된 커넥션의 종료를 의미함과 동시에, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 해당 레코드를 삭제할 필요가 생긴다. 단, 레코드를 삭제하는 시기는, 내측 NIC(104)를 향해 형성되는 커넥션과, 외측

NIC(108)를 향해 형성되는 커넥션의, 양쪽 커넥션의 종료로부터 소정의 시간을 경과시킬 필요가 있다.

[0134] 그러므로, 수신 패킷 판정부(601)는 TCP FIN 패킷을 레코드 삭제 준비 처리부(604)에 인도한다.

[0135] 레코드 삭제 준비 처리부(604)는, TCP FIN 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호로 내측 NIC 어드레스 테이블을 검색해 레코드를 특정하고, 해당 레코드의 색인 포트 번호를 삭제 예정 리스트(605)에 써낸다. 삭제 예정 리스트(605)는, 도시하지 않은 RAM 내에 설치된, 삭제를 예정하고 있는 레코드의 색인 포트 번호가 기록되는 리스트이다. 그 후, 레코드 삭제 준비 처리부(604)는 TCP FIN 패킷을 어드레스 치환부(602)에 인도한다. 어드레스 치환부(602)는 전술한 TCP 데이터 패킷 및 TCP SYN 패킷과 같이, TCP FIN 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서하여, TCP/IP 프로토콜 스택(205)으로 전송한다.

[0136] 또한, 어드레스 치환부(602)는, TCP 데이터 패킷, TCP SYN 패킷 및 TCP FIN 패킷 중 어느 경우에 있어서도 목적지 포트 번호는 개서하지 않는다.

[0137] 어드레스 치환부(602)는, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를 개서할 때, 임시 IPMAC 리스트(204)를 참조한다.

[0138] 다음으로, 외측 NIC 수신 처리부(502)의 상세를 설명한다.

[0139] 도 7은, 외측 NIC 수신 처리부(502)의 기능 블록도이다.

[0140] 외측 NIC(108)가 수신한 패킷은, 처음에 수신 패킷 판정부(701)가 XPTCP 처리 대상 마스터(208)를 참조하여, 해당 패킷이 XPTCP 처리의 대상이 되는지 여부 등을 판정한다.

[0141] 만약, 외측 NIC(108)가 수신한 패킷이, 예를 들면 ICMP 패킷이나 XPTCP 처리 대상 마스터(208)에 합치하지 않는 처리 대상 외 패킷일 경우에는, 외측 NIC 수신 처리부(502)는 그 패킷을 그대로 내측 NIC(104)로 전송한다.

[0142] 만약, 외측 NIC(108)가 수신한 패킷이, XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷일 경우에는, 외측 NIC 수신 처리부(502)는 그 패킷을 그대로 TCP/IP 프로토콜 스택(205)으로 전송한다.

[0143] 만약, 외측 NIC(108)로부터 입력된 패킷이 XPTCP 처리 대상 마스터(208)에 합치하는 처리 대상 패킷일 경우에는, 수신 패킷 판정부(701)는 다음으로 그 패킷의 상세를 본다.

[0144] 수신 패킷 판정부(701)는, 그 패킷이 TCP 데이터 패킷이면, 해당 TCP 데이터 패킷을 어드레스 치환부(702)에 인도한다.

[0145] 어드레스 치환부(702)는 외측 NIC 어드레스 테이블(210)을 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호로 검색하여 레코드를 특정하고, 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 개서하여, TCP/IP 프로토콜 스택(205)으로 전송한다.

[0146] 수신 패킷 판정부(701)는, 만약, 그 패킷이 TCP FIN 패킷이면, 그것은 TCP/IP 프로토콜 스택(205)에 형성된 커넥션의 종료를 의미함과 동시에, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 해당 레코드를 삭제할 필요가 생긴다. 전술과 같이, 레코드를 삭제할 시기는, 외측 NIC(108)를 향해 형성되는 커넥션과, 외측 NIC(108)를 향해 형성되고 있는 커넥션의, 양쪽 커넥션의 종료로부터 소정의 시간을 경과시킬 필요가 있다.

[0147] 그러므로, 수신 패킷 판정부(701)는 TCP FIN 패킷을 레코드 삭제 처리부(703)에 인도한다.

[0148] 레코드 삭제 처리부(703)는, TCP FIN 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호로 내측 NIC 어드레스 테이블을 검색하여 레코드를 특정하고, 해당 레코드의 색인 포트 번호를 취득한다.

[0149] 다음으로, 취득한 색인 포트 번호가 삭제 예정 리스트(605)에 있는지 여부를 확인한다. 삭제 예정 리스트(605)에 해당 색인 포트 번호가 있다면, 현시점의 어드레스 테이블 갱신 카운터(213)의 값을, 해당 색인 포트 번호에 따른 외측 NIC 어드레스 테이블(210) 및 내측 NIC 어드레스 테이블(209)의 레코드의, 타이머용 카운터 값 필드에 기입한다. 그 후, 레코드 삭제 처리부(703)는 TCP FIN 패킷을 어드레스 치환부(702)에 인도한다.

[0150] 어드레스 치환부(702)는 전술한 TCP 데이터 패킷과 같이, TCP FIN 패킷의 송신원 MAC 어드레스, 송신원 IP 어드

레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 개서하여, TCP/IP 프로토콜 스택(205)으로 전송한다.

[0151] 어드레스 치환부(702)는, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를 개서할 때, 임시 IPMAC 리스트(204)를 참조한다.

[0152] 다음으로, 외측 NIC 송신 처리부(503)의 상세를 설명한다.

[0153] 도 8은, 외측 NIC 송신 처리부(503)의 기능 블록도이다.

[0154] 송신 패킷 판정부(801)는, TCP/IP 프로토콜 스택(205)에서 송출된 패킷을 수신하면, 처음에 패킷이 어드레스 개서 대상 외 패킷인지, 어드레스 개서 대상 TCP 패킷인지, 혹은 ARP 요구 패킷인지를 판정한다.

[0155] 만약, 패킷이 어드레스 개서 대상 외의 패킷이면, 그대로 아무것도 하지 않고 외측 NIC(108)에 송신한다.

[0156] 만약, 패킷이 ARP 요구 패킷이며, 또한 ARP 요구 패킷에 첨부되고 있는 문의 IP 어드레스가 제2 임시 IP 어드레스일 경우에는, 해당 패킷은, 패킷에 첨부하는 MAC 어드레스를 특정하기 위해서, TCP/IP 프로토콜 스택(205)이 커넥션을 형성할 때에 송신하는 패킷이다. 그러므로, 송신 패킷 판정부(801)는 ARP 요구 패킷을 ARP 응답 처리부(802)에 인도한다.

[0157] ARP 응답 처리부(802)는 임시 IPMAC 리스트(204)를 참조하여, TCP/IP 프로토콜 스택(205)에 제2 임시 MAC 어드레스를 회신한다.

[0158] 만약, 패킷이 TCP 패킷이며, 패킷에 첨부되고 있는 목적지 IP 어드레스가 제2 임시 IP 어드레스일 경우에는, 송신 패킷 판정부(801)는 다음으로 해당 패킷이 TCP SYN 패킷인지 여부를 확인한다. TCP SYN 패킷이면, 그것은 TCP/IP 프로토콜 스택(205)이 커넥션을 신규로 작성한 것을 나타낸다. 따라서, TCP/IP 프로토콜 스택(205)이 신규로 작성한 커넥션의 송신원 포트 번호, 즉 동적 포트 번호를, 외측 NIC 어드레스 테이블(210)에 기억해 둘 필요가 있다. 그러므로, 송신 패킷 판정부(801)는 TCP SYN 패킷을 동적 포트 기록 처리부(803)에 인도한다.

[0159] 동적 포트 기록 처리부(803)는, TCP SYN 패킷에 첨부되고 있는 송신원 포트 번호, 즉 동적 포트 번호와, 목적지 포트 번호로서 첨부되고 있는 색인 포트 번호를 취득한다. 그리고, 색인 포트 번호로 외측 NIC 어드레스 테이블(210)의 해당 레코드를 특정하면, 해당 레코드의 동적 포트 번호 필드에, 동적 포트 번호를 기록한다. 그리고, 동적 포트 기록 처리부(803)는 해당 TCP SYN 패킷을 어드레스 복원부(804)에 인도한다.

[0160] 어드레스 복원부(804)는 외측 NIC 어드레스 테이블(210)의, 앞서 목적지 포트 번호로 특정한 레코드의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 취득하고, 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 복원하여, 외측 NIC(108)에 송신한다.

[0161] 만약, 패킷이 TCP 패킷이며, 패킷에 첨부되고 있는 목적지 IP 어드레스가 제2 임시 IP 어드레스일 경우에는, 송신 패킷 판정부(801)는 다음으로 해당 패킷이 TCP SYN 패킷인지 여부를 확인한다. TCP SYN 패킷이 아니면,

[0162] 송신 패킷 판정부(801)는 해당 TCP 패킷을 어드레스 복원부(804)에 인도한다.

[0163] 어드레스 복원부(804)는 외측 NIC 어드레스 테이블(210)의, 앞서 색인 포트 번호로 특정한 레코드의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 취득하고, 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 복원하여, 외측 NIC(108)에 송신한다.

[0164] 다음으로, 내측 NIC 송신 처리부(504)의 상세를 설명한다.

[0165] 도 9는, 내측 NIC 송신 처리부(504)의 기능 블록도이다.

[0166] 송신 패킷 판정부(901)는, TCP/IP 프로토콜 스택(205)으로부터 송출된 패킷을 수신하면, 처음에 패킷이 어드레스 개서 대상 외 패킷인지, 혹은 어드레스 개서 대상 TCP 패킷인지를 판정한다.

[0167] 만약, 패킷이 어드레스 개서 대상 외의 패킷이면, 그대로 아무것도 하지 않고 내측 NIC(104)에 송신한다.

[0168] 만약, 패킷이 TCP 패킷이며, 패킷에 첨부되고 있는 목적지 IP 어드레스가 제1 임시 IP 어드레스일 경우에는, 송신 패킷 판정부(901)는 해당 TCP 패킷을 어드레스 복원부(902)에 인도한다.

[0169] 어드레스 복원부(902)는 내측 NIC 어드레스 테이블(209)의, 색인 포트 번호로 특정한 레코드의 송신원 MAC 어드

레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 취득하고, 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 복원하여, 내측 NIC(104)에 송신한다.

[0170] 다음으로, 테이블 갱신 처리부(505)의 상세를 설명한다.

[0171] 테이블 갱신 처리부(505)는 1초 마다 기동해, 어드레스 테이블 갱신 카운터(213)의 값을 1 인크리먼트해서, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 모든 레코드의 타이머용 카운트 값 필드를 검사하고, TCP FIN 패킷이 와서 클로즈된 커넥션이 60초 이상 경과한 레코드가 있는지 여부를 확인한다. 그리고, 그러한 레코드가 있으면 해당 레코드를 삭제한다.

[0172] 다음으로, 폴리시 회답부(506)의 상세를 설명한다.

[0173] 폴리시 회답부(506)는, XPTCP 처리부(206)로부터 송출되는, 색인 포트 번호를 수반하는 폴리시 문의에 대해, XPTCP 처리 대상 마스터(208) 및 내측 NIC 어드레스 테이블(209)을 참조하여, 해당 색인 포트 번호로 특정되는 커넥션에 대한 암호 종별 등을 지정하기 위한, XPTCP 처리 대상 마스터(208)의 레코드 번호를 회신한다.

[0174] [XPTCP 처리부(206)의 내부 구성]

[0175] 도 10은, XPTCP 처리부(206)의 기능 블록도이다.

[0176] 이벤트 검출부(1001)는, TCP/IP 프로토콜 스택(205)으로부터 얻어지는, accept 이벤트, connect request 이벤트 및 close 이벤트를 검출하여, 소켓 조작부(1002) 및 폴리시 설정부(1003)를 제어한다.

[0177] 소켓 조작부(1002)는, TCP/IP 프로토콜 스택(205)에 의해 도시하지 않은 RAM 상에 형성된 소켓 메모리 영역(1004)에 대해, 소켓으로부터 얻어진 스트림 데이터를, 암호화 처리부(1005) 또는 복호 처리부(1006)에 인도하고, 처리된 스트림 데이터를 소켓 메모리 영역(1004) 상의 소정의 소켓에 인도한다.

[0178] 폴리시 설정부(1003)는, 소켓 조작부(1002)로부터 이벤트 검출부(1001)를 통해 얻어진 색인 포트 번호를 인수로서, 어드레스 변환 처리부에 대해 폴리시(policy)를 문의한다. 이 문의에 대해서는, 어드레스 변환 처리부의 폴리시 회답부(506)가 XPTCP 처리 대상 마스터(208)의 레코드 번호를 회신한다. 그러면, 폴리시 설정부(1003)는 XPTCP 폴리시 테이블(211)에, 색인 포트 번호와 XPTCP 처리 대상 마스터(208)의 레코드 번호를 기록하여, 연관시킨다.

[0179] 암호화 처리부(1005)는, XPTCP 폴리시 테이블(211) 및 XPTCP 처리 대상 마스터(208)를 참조하여, 소켓 조작부(1002)로부터 받은 스트림 데이터에 대해, 지정된 암호화 처리를 수행한다.

[0180] 복호 처리부(1006)는, XPTCP 폴리시 테이블(211) 및 XPTCP 처리 대상 마스터(208)를 참조하여, 소켓 조작부(1002)로부터 받은 스트림 데이터에 대해, 지정된 복호 처리를 수행한다.

[0181] 또한, 본래라면 XPTCP 처리부(206)에는, 인증에 관한 기능도 존재하지만, 본 실시 형태의 XPTCP 게이트웨이 장치(101)에서는, 인증에 관한 동작은 발명의 범주에서 벗어나므로, 인증에 관한 기술은 생략하고 있다. 이 때문에, 도 10에 나타내는 XPTCP 처리부(206)의 기능 블록도에는, 인증에 관한 기능 블록은 기술을 생략하고 있다.

[0182] [XPTCP 게이트웨이 장치(101)의 동작·어드레스 변환 처리부(203)의 동작]

[0183] 이제부터, 도 11에서 도 17의 플로우 차트에 근거해, XPTCP 게이트웨이 장치(101)의 동작의 흐름을 설명한다.

[0184] 도 11은, 어드레스 변환 처리부(203)의, 내측 NIC(104)에서의 패킷 수신 처리 동작의 흐름을 나타내는 플로우 차트이다. 이는 내측 NIC 수신 처리부(501)의 동작의 흐름에 해당한다.

[0185] 처리를 개시하면(S1101), 수신 패킷 판정부(601)는, 처음에 내측 NIC(104)가 수신한 패킷이, 예를 들면 ARP 패킷이나 ICMP 패킷 등의, 분명히 전송 대상이 되는 처리 대상 외 패킷인지 여부를 판정한다(S1102).

[0186] 판정 결과, 수신한 패킷이, ARP 패킷이나 ICMP 패킷 등의, 분명히 전송 대상이 되는 처리 대상 외 패킷일 경우에는(S1102의 YES), 수신 패킷 판정부(601)는 그 패킷을 그대로 외측 NIC(108)로 전송해(S1103), 일련의 처리를 종료한다(S1104).

[0187] 단계 S1102에서, 수신한 패킷이, 분명히 전송 대상이 되는 처리 대상 외 패킷이 아닐 경우(S1102의 NO)에는, 수신 패킷 판정부(601)는 다음으로 그 패킷이 XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷인지 여부를 판정한다(S1105).

[0188] 판정 결과, 수신한 패킷이, XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷일 경우에는(S1105의 YES), 수신 패킷 판정부(601)는 그 패킷을 그대로 TCP/IP 프로토콜 스택(205)으로 전송해(S1106), 일련의 처리를 종료한다(S1104).

[0189] 단계 S1105에서, 수신한 패킷이, XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷이 아닐 경우에는(S1105의 NO), 수신 패킷 판정부(601)는 다음으로 해당 패킷의 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스 및 목적지 포트 번호로 XPTCP 처리 대상 마스터(208)를 검색한다(S1107).

[0190] 검색 결과, 수신한 패킷의 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스 및 목적지 포트 번호의 조합이, XPTCP 처리 대상 마스터(208)에 없으면(S1108의 NO), 해당 패킷은 XPTCP 게이트웨이 장치(101)의 처리 대상 외이므로, 수신 패킷 판정부(601)는 그 패킷을 그대로 외측 NIC(108)로 전송해(S1103), 일련의 처리를 종료한다(S1104).

[0191] 단계 S1108에서, 수신한 패킷의 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스 및 목적지 포트 번호의 조합이, XPTCP 처리 대상 마스터(208)에 있으면(S1108의 YES), 해당 패킷은 XPTCP 게이트웨이 장치(101)의 처리 대상이며, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를 개서할 필요가 있다. 그러므로, 수신 패킷 판정부(601)는 더 한층 수신한 패킷의 상세를 본다.

[0192] 수신 패킷 판정부(601)는, 수신한 패킷이 TCP SYN 패킷인지 여부를 판정한다(S1109).

[0193] 판정 결과, 수신한 패킷이 TCP SYN 패킷이면(S1109의 YES), 수신 패킷 판정부(601)는 해당 TCP SYN 패킷을 커넥션 등록 처리부(603)에 인도한다.

[0194] 커넥션 등록 처리부(603)는, TCP SYN 패킷을 받으면, TCP 포트 번호 메모리를 참조하여, 현시점에서 사용되지 않는(중복하지 않는) 새로운 색인 포트 번호를 얻은 후, 수신한 패킷의 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스 및 목적지 포트 번호와 함께, 내측 NIC 어드레스 테이블(209)에 신규의 레코드로서 추가로 기록한다(S1110). 게다가, 같은 내용으로 외측 NIC 어드레스 테이블(210)에도 마찬가지로 신규 레코드를 추가로 기록한다(S1111).

[0195] 커넥션 등록 처리부(603)는, 내측 NIC 어드레스 테이블(209)과 외측 NIC 어드레스 테이블(210)에 신규 레코드를 추가로 기록한 후, 수신 패킷 판정부(601)로부터 인도된 TCP SYN 패킷을 어드레스 치환부(602)에 인도한다.

[0196] 어드레스 치환부(602)는, 커넥션 등록 처리부(603)로부터 인도된 색인 포트 번호와 임시 IPMAC 리스트(204)를 참조하여, TCP SYN 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서한다(S1112). 구체적으로는,

[0197] ・패킷에 첨부되고 있는 송신원 MAC 어드레스를 제1 임시 MAC 어드레스로,

[0198] ・패킷에 첨부되고 있는 송신원 IP 어드레스를 제1 임시 IP 어드레스로,

[0199] ・패킷에 첨부되고 있는 송신원 포트 번호를 색인 포트 번호로,

[0200] ・패킷에 첨부되고 있는 목적지 MAC 어드레스를 내측 NICMAC 어드레스로,

[0201] ・패킷에 첨부되고 있는 목적지 IP 어드레스를 내측 NICIP 어드레스로 개서한다.

[0202] 그리고, 목적지 포트 번호는 변경하지 않는다.

[0203] 어드레스 치환부(602)는 IP 어드레스 등의 치환 처리를 수행한 후, 해당 TCP SYN 패킷을 TCP/IP 프로토콜 스택(205)으로 송신해(S1106), 일련의 처리를 종료한다(S1104).

[0204] 단계 S1109에서, 수신한 패킷이 TCP SYN 패킷이 아니면(S1109의 NO), 수신 패킷 판정부(601)는 다음으로 수신한 패킷이 TCP FIN 패킷인지 여부를 판정한다(S1113).

[0205] 판정 결과, 수신한 패킷이 TCP FIN 패킷이면(S1109의 YES), 수신 패킷 판정부(601)는 해당 TCP FIN 패킷을 색인 포트 번호와 함께 레코드 삭제 준비 처리부(604)에 인도한다.

[0206] 레코드 삭제 준비 처리부(604)는, 해당 TCP FIN 패킷의 색인 포트 번호를 삭제 예정 리스트(605)에 기입한다(S1104). 그 후, 레코드 삭제 준비 처리부(604)는 TCP FIN 패킷과 색인 포트 번호를 어드레스 치환부(602)에 인도한다.

[0207] 어드레스 치환부(602)는, 수신 패킷 판정부(601)로부터 레코드 삭제 준비 처리부(604)를 통해 인도된 색인 포트

번호와 임시 IPMAC 리스트(204)를 참조하여, TCP FIN 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서한다(S1112). 구체적으로는, 패킷에 첨부되고 있는 송신원 MAC 어드레스를 제1 임시 MAC 어드레스로, 패킷에 첨부되고 있는 송신원 IP 어드레스를 제1 임시 IP 어드레스로, 패킷에 첨부되고 있는 송신원 포트 번호를 색인 포트 번호로, 패킷에 첨부되고 있는 목적지 MAC 어드레스를 내측 NICMAC 어드레스로, 패킷에 첨부되고 있는 목적지 IP 어드레스를 내측 NICIP 어드레스로 개서한다. 그리고, 목적지 포트 번호는 변경하지 않는다.

[0208] 어드레스 치환부(602)는 IP 어드레스 등의 치환 처리를 수행한 후, 해당 TCP FIN 패킷을 TCP/IP 프로토콜 스택(205)으로 송신해(S1106), 일련의 처리를 종료한다(S1104).

[0209] 단계 S1113에서, 수신한 패킷이 TCP FIN 패킷이 아니면(S1113의 NO), 해당 패킷은 TCP 데이터 패킷이다. 그러므로, 수신 패킷 판정부(601)는 해당 TCP 데이터 패킷을 색인 포트 번호와 함께 어드레스 치환부(602)에 인도한다.

[0210] 어드레스 치환부(602)는, 수신 패킷 판정부(601)로부터 인도된 색인 포트 번호와 임시 IPMAC 리스트(204)를 참조하여, TCP 데이터 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서한다(S1112). 구체적으로는, 패킷에 첨부되고 있는 송신원 MAC 어드레스를 제1 임시 MAC 어드레스로, 패킷에 첨부되고 있는 송신원 IP 어드레스를 제1 임시 IP 어드레스로, 패킷에 첨부되고 있는 송신원 포트 번호를 색인 포트 번호로, 패킷에 첨부되고 있는 목적지 MAC 어드레스를 내측 NICMAC 어드레스로, 패킷에 첨부되고 있는 목적지 IP 어드레스를 내측 NICIP 어드레스로 개서한다. 그리고, 목적지 포트 번호는 변경하지 않는다.

[0211] 어드레스 치환부(602)는 IP 어드레스 등의 치환 처리를 수행한 후, 해당 TCP 데이터 패킷을 TCP/IP 프로토콜 스택(205)으로 송신해(S1106), 일련의 처리를 종료한다(S1104).

[0212] 도 12는, 어드레스 변환 처리부(203)의, 외측 NIC(108)에서의 패킷 수신 처리 동작의 흐름을 나타내는 플로우 차트이다. 이는 외측 NIC 수신 처리부(502)의 동작의 흐름에 해당한다.

[0213] 처리를 개시하면(S1201), 수신 패킷 판정부(701)는, 처음에 외측 NIC(108)가 수신한 패킷이, 예를 들면 ARP 패킷이나 ICMP 패킷 등의, 분명히 전송 대상이 되는 처리 대상 외 패킷인지 여부를 판정한다(S1202).

[0214] 판정 결과, 수신한 패킷이, ARP 패킷이나 ICMP 패킷 등의, 분명히 전송 대상이 되는 처리 대상 외 패킷일 경우에는(S1202의 YES), 수신 패킷 판정부(701)는 그 패킷을 그대로 내측 NIC(104)로 전송해(S1203), 일련의 처리를 종료한다(S1204).

[0215] 단계 S1202에서, 수신한 패킷이, 분명히 전송 대상이 되는 처리 대상 외 패킷이 아닐 경우(S1202의 NO)에는, 수신 패킷 판정부(701)는 다음으로 그 패킷이 XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷인지 여부를 판정한다(S1205).

[0216] 판정 결과, 수신한 패킷이, XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷일 경우에는(S1205의 YES), 수신 패킷 판정부(701)는 그 패킷을 그대로 TCP/IP 프로토콜 스택(205)으로 전송해(S1206), 일련의 처리를 종료한다(S1204).

[0217] 단계 S1205에서, 수신한 패킷이, XPTCP 게이트웨이 장치(101)에 대해 송신된, XPTCP 처리 대상 외 패킷이 아닐 경우에는(S1205의 NO), 수신 패킷 판정부(701)는 다음으로 해당 패킷의 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스 및 목적지 포트 번호로 XPTCP 처리 대상 마스터(208)를 검색한다(S1207).

[0218] 검색 결과, 수신한 패킷의 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스 및 목적지 포트 번호의 조합이, XPTCP 처리 대상 마스터(208)에 없으면(S1208의 NO), 해당 패킷은 XPTCP 게이트웨이 장치(101)의 처리 대상 외이므로, 수신 패킷 판정부(701)는 그 패킷을 그대로 내측 NIC(104)로 전송해(S1203), 일련의 처리를 종료한다(S1204).

[0219] 단계 S1208에서, 수신한 패킷의 송신원 IP 어드레스, 송신원 포트 번호, 목적지 IP 어드레스 및 목적지 포트 번호의 조합이, XPTCP 처리 대상 마스터(208)에 있으면(S1208의 YES), 해당 패킷은 XPTCP 게이트웨이 장치(101)의 처리 대상이며, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를 개서할 필요가 있다. 그러므로, 수신 패킷 판정부(701)는 더 한층 수신한 패킷의 상세를 본다.

[0220] 수신 패킷 판정부(701)는, 수신한 패킷이 TCP FIN 패킷인지 여부를 판정한다(S1209).

[0221] 판정 결과, 수신한 패킷이 TCP FIN 패킷이면(S1209의 YES), 수신 패킷 판정부(701)는 해당 TCP FIN 패킷을 색인 포트 번호와 함께 레코드 삭제 처리부(703)에 인도한다.

[0222] 레코드 삭제 처리부(703)는, 해당 TCP FIN 패킷의 색인 포트 번호가 삭제 예정 리스트(605)에 있음을 확인하면, 내측 NIC 어드레스 테이블(209)의, 해당 색인 포트 번호에 따른 레코드의 타이머용 카운터 값 필드에, 어드레스 테이블 갱신 카운터(213)의 값을 기입한다(S1210).

[0223] 그 후, 레코드 삭제 처리부(703)는 TCP FIN 패킷과 색인 포트 번호를 어드레스 치환부(702)에 인도한다.

[0224] 어드레스 치환부(702)는, 수신 패킷 판정부(701)로부터 레코드 삭제 처리부(703)를 통해 인도된 색인 포트 번호와 임시 IPMAC 리스트(204)를 참조하여, TCP FIN 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 개서한다(S1211). 구체적으로는,

[0225] ·패킷에 첨부되고 있는 송신원 MAC 어드레스를 제2 임시 MAC 어드레스로,

[0226] ·패킷에 첨부되고 있는 송신원 IP 어드레스를 제2 임시 IP 어드레스로,

[0227] ·패킷에 첨부되고 있는 송신원 포트 번호를 색인 포트 번호로,

[0228] ·패킷에 첨부되고 있는 목적지 MAC 어드레스를 외측 NICMAC 어드레스로,

[0229] ·패킷에 첨부되고 있는 목적지 IP 어드레스를 외측 NICIP 어드레스로,

[0230] ·패킷에 첨부되고 있는 목적지 포트 번호를 동적 포트 번호로 개서한다.

[0231] 어드레스 치환부(702)는 IP 어드레스 등의 치환 처리를 수행한 후, 해당 TCP FIN 패킷을 TCP/IP 프로토콜 스택(205)으로 송신해(S1206), 일련의 처리를 종료한다(S1204).

[0232] 단계 S1209에서, 수신한 패킷이 TCP FIN 패킷이 아니면(S1209의 NO), 해당 패킷은 TCP 데이터 패킷이다. 그러므로, 수신 패킷 판정부(701)는 해당 TCP 데이터 패킷을 색인 포트 번호와 함께 어드레스 치환부(702)에 인도한다.

[0233] 어드레스 치환부(702)는, 수신 패킷 판정부(701)로부터 인도된 색인 포트 번호와 임시 IPMAC 리스트(204)를 참조하여, TCP 데이터 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 개서한다(S1212). 구체적으로는, 패킷에 첨부되고 있는 송신원 MAC 어드레스를 제2 임시 MAC 어드레스로, 패킷에 첨부되고 있는 송신원 IP 어드레스를 제2 임시 IP 어드레스로, 패킷에 첨부되고 있는 송신원 포트 번호를 색인 포트 번호로, 패킷에 첨부되고 있는 목적지 MAC 어드레스를 외측 NICMAC 어드레스로, 패킷에 첨부되고 있는 목적지 IP 어드레스를 외측 NICIP 어드레스로, 패킷에 첨부되고 있는 목적지 포트 번호를 동적 포트 번호로 개서한다.

[0234] 어드레스 치환부(702)는 IP 어드레스 등의 치환 처리를 수행한 후, 해당 TCP 데이터 패킷을 TCP/IP 프로토콜 스택(205)으로 송신해(S1206), 일련의 처리를 종료한다(S1204).

[0235] 도 13은, 어드레스 변환 처리부(203)의, 외측 NIC(108)에서의 패킷 송신 처리 동작의 흐름을 나타내는 플로우 차트이다. 이는 외측 NIC 송신 처리부(503)의 동작의 흐름에 해당한다.

[0236] 처리를 개시하면(S1301), 송신 패킷 판정부는, 처음에 TCP/IP 프로토콜 스택(205)으로부터 받은 패킷의 종별과 목적지 IP 어드레스를 본다.

[0237] 패킷의 종별이 ICMP 패킷이나 UDP 패킷일 경우, 패킷의 종별이 ARP 요구 패킷이고 또한 탐색 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제2 임시 IP 어드레스가 아닐 경우, 패킷의 종별이 TCP 패킷이며 또한 목적지 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제2 임시 IP 어드레스가 아닐 경우에는(S1302의 NO), 이들 패킷은 XPTCP 게이트웨이 장치(101)가 처리하고 있지 않는 패킷이다. 그러므로, 송신 패킷 판정부는 그 패킷에 대해 아무런 가공을 하지 않고, 그대로 외측 NIC(108)를 통해 송신해(S1303), 일련의 처리를 종료한다(S1304).

[0238] 단계 S1302에서, TCP/IP 프로토콜 스택(205)으로부터 받은 패킷의 종별이 TCP 패킷이며 또한 목적지 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제2 임시 IP 어드레스일 경우, 또는 ARP 요구 패킷이며 또한 탐색 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제2 임시 IP 어드레스일 경우(S1302의 YES)에는, 더욱 해당 패킷이 ARP 요구 패킷인지 여부를 판정한다(S1305).

[0239] ARP 요구 패킷이며 또한 탐색 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제2 임시 IP 어드레스일 경우(S1305의 YES)에는, 이 ARP 요구 패킷은 TCP/IP 프로토콜 스택(205)이 실재하지 않는 제2 임시 IP 어드레스에 대해 패킷을 송신하려고 한 결과, 생성된 패킷이다. 이 ARP 요구 패킷은 외측 NIC(108)로부터 송신시키는 것이 아니라, 제2 임시 IP 어드레스와 같이 실재하지 않는 MAC 어드레스인 제2 임시 MAC 어드레스로, ARP 응답 패킷을 생성해 회신해야 한다. 그러므로, 송신 패킷 판정부는 해당 ARP 요구 패킷을 ARP 응답 처리부(802)에 인도한다.

[0240] ARP 응답 처리부(802)는, 송신 패킷 판정부로부터 ARP 요구 패킷을 받으면, 임시 IPMAC 리스트를 참조하여, 제2 임시 MAC 어드레스로 ARP 응답 패킷을 생성해서, TCP/IP 프로토콜 스택(205)으로 반송해(S1306), 일련의 처리를 종료한다(S1304).

[0241] 단계 S1305에서, TCP/IP 프로토콜 스택(205)으로부터 받은 패킷이 TCP 패킷이며 또한 목적지 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제2 임시 IP 어드레스일 경우에는(S1305의 NO), 해당 패킷은 XPTCP 게이트웨이 장치(101)가 처리한 패킷이며, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를, 내측 NIC 수신 처리부(501)가 개서하기 이전 상태로 복원할 필요가 있다. 그러므로, 송신 패킷 판정부는 더욱이 수신한 패킷의 상세를 본다.

[0242] 송신 패킷 판정부는, TCP/IP 프로토콜 스택(205)으로부터 받은 패킷이 TCP SYN 패킷인지 여부를 판정한다(S1307).

[0243] 판정 결과, TCP/IP 프로토콜 스택(205)으로부터 받은 패킷이 TCP SYN 패킷이면(S1307의 YES), 해당 TCP SYN 패킷은 커넥션이 새롭게 생성된 것을 나타내는 패킷이다. 그 때, TCP/IP 프로토콜 스택(205)이 커넥션을 생성할 때에, 송신원 포트 번호로서 동적 포트 번호를 자동적으로 부여하고 있다. 이 동적 포트 번호를, 외측 NIC 어드레스 테이블(210)에 기억해 둘 필요가 있다. 그러므로, 송신 패킷 판정부는 해당 TCP SYN 패킷을 동적 포트 기록 처리부(803)에 인도한다.

[0244] 동적 포트 기록 처리부(803)는, TCP SYN 패킷을 받으면, 먼저 TCP SYN 패킷의 송신원 포트 번호를 취득한다. 다음으로, 목적지 포트 번호에 기록되고 있는 색인 포트 번호로 외측 NIC 어드레스 테이블(210)을 검색하여, 특정한 레코드의 동적 포트 번호 필드에, 앞서 취득한 TCP SYN 패킷의 송신원 포트 번호를 기입한다(S1308).

[0245] 이렇게 해서, 커넥션의 개시를 나타내는 TCP SYN 패킷에 첨부되고 있는 동적 포트 번호를 기억해 둠으로써, 이후에 해당 커넥션을 경유하는 패킷의 IP 어드레스 등을 올바르게 치환 또는 복원할 수 있다.

[0246] 동적 포트 기록 처리부(803)는, 동적 포트 번호의 기록을 수행한 후, TCP SYN 패킷을 어드레스 복원부(902)에 인도한다.

[0247] 어드레스 복원부(902)는, 앞서 동적 포트 기록 처리부(803)가 특정한 외측 NIC 어드레스 테이블(210)의 레코드를 참조하여, TCP SYN 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 복원한다(S1309). 그리고, 해당 TCP SYN 패킷을 외측 NIC(108)를 통해 송신하여(S1303), 일련의 처리를 종료한다(S1304).

[0248] 단계 S1307에서, TCP/IP 프로토콜 스택(205)으로부터 받은 패킷이 TCP SYN 패킷이 아니면(S1307의 NO), 송신 패킷 판정부는 해당 TCP 패킷을 어드레스 복원부(902)에 인도한다.

[0249] 어드레스 복원부(902)는, TCP 패킷의 목적지 포트 번호에 첨부되고 있는 색인 포트 번호로 외측 NIC 어드레스 테이블(210)의 레코드를 검색해 레코드를 특정하고, TCP 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 복원한다(S1309). 그리고, 해당 TCP SYN 패킷을 외측 NIC(108)를 통해 송신하여(S1303), 일련의 처리를 종료한다(S1304).

[0250] 도 14는, 어드레스 변환 처리부(203)의, 내측 NIC(104)에서의 패킷 송신 처리 동작의 흐름을 나타내는 플로우차트이다. 이는 내측 NIC 송신 처리부(504)의 동작의 흐름에 해당한다.

[0251] 처리를 개시하면(S1401), 송신 패킷 판정부는, 처음에 TCP/IP 프로토콜 스택(205)으로부터 받은 패킷의 종별과 목적지 IP 어드레스를 본다.

[0252] 패킷의 종별이 ICMP 패킷이나 ARP 패킷이나 UDP 패킷일 경우, 패킷의 종별이 TCP 패킷이며 또한 목적지 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제1 임시 IP 어드레스가 아닐 경우에는(S1402의 NO), 이들 패킷은 XPTCP 게이트웨이 장치(101)가 처리하고 있지 않는 패킷이다. 그러므로, 송신 패킷 판정부는 그 패킷에

대해 아무런 가공을 하지 않고, 그대로 내측 NIC(104)를 통해 송신해(S1403), 일련의 처리를 종료한다(S1404).

[0253] 단계 S1402에서, TCP/IP 프로토콜 스택(205)으로부터 받은 패킷의 종별이 TCP 패킷이며 또한 목적지 IP 어드레스가 임시 IPMAC 리스트(204)에 기록되고 있는 제1 임시 IP 어드레스일 경우(S1402의 YES)에는, 해당 패킷은 XPTCP 게이트웨이 장치(101)가 처리한 패킷이며, 패킷에 첨부되고 있는 MAC 어드레스, IP 어드레스 및 포트 번호를, 내측 NIC 수신 처리부(501)가 개서하기 이전 상태로 복원할 필요가 있다. 그러므로, 송신 패킷 판정부는 해당 TCP 패킷을 어드레스 복원부(902)에 인도한다.

[0254] 어드레스 복원부(902)는, TCP 패킷의 목적지 포트 번호에 첨부되고 있는 색인 포트 번호로 내측 NIC 어드레스 테이블(209)의 레코드를 검색해 레코드를 특정하고, TCP 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 복원한다(S1405). 그리고, 해당 TCP SYN 패킷을 내측 NIC(104)를 통해 송신하여(S1403), 일련의 처리를 종료한다(S1404).

[0255] [XPTCP 게이트웨이 장치(101)의 동작·XPTCP 처리부(206)의 동작]

[0256] 도 15는, XPTCP 처리부(206)의 XPTCP 처리의 흐름을 나타내는 플로우 차트이다.

[0257] XPTCP 처리는, TCP 또는 UDP 패킷에 대해, 트랜스포트층에서 소정의 인증 및 암호화 처리를 가하는 처리이다. XPTCP 처리의 기본적인 기술 내용은 특허문헌 1에 개시되고 있으므로, 본 실시 형태에서는 상세하게는 설명하지 않는다. 그 대신해, 전술한 어드레스 변환 처리부(203) 및 후술하는 소켓 처리부(207)에서 행하고 있는, 소켓의 처리에 관계되는 내용을 설명한다.

[0258] 처리를 개시하면(S1501), 이벤트 검출부(1001)는 소켓 처리부(207)로부터 내측 NIC(104)에 대한 커넥션에 따른 accept 이벤트를 검출했는지 여부를 확인한다(S1502). accept 이벤트를 검출 했다면(S1502의 YES), 이벤트 검출부(1001)는 소켓 조작부(1002)를 제어해서, 해당 accept 이벤트에 따른, 생성된 소켓의, 소켓 메모리 영역(1004) 내에서의 어드레스를 취득한다(S1503). 그리고, 이벤트 검출부(1001)는 폴리시 설정부(1003)를 기동한다.

[0259] 폴리시 설정부(1003)는 해당 accept 이벤트에 따른 소켓과 관련하여, 색인 포트 번호로 어드레스 변환 처리부(203)에 대해 폴리시 문의를 행한다. 어드레스 변환 처리부(203)의 폴리시 회답부(506)는, 내측 NIC 어드레스 테이블(209)을 색인 포트 번호로 검색해 레코드를 특정한다. 그리고, 특정한 레코드의 송신원 IP 어드레스 및 포트 번호, 목적지 IP 어드레스 및 포트 번호를 이용해 XPTCP 처리 대상 마스터(208)를 검색하여, 레코드를 특정하고, 해당 레코드의 레코드 번호를 취득하면, 그 레코드 번호를 폴리시 설정부(1003)에 회답한다. 폴리시 설정부(1003)는, 얻어진 레코드 번호와 색인 포트 번호를, XPTCP 폴리시 테이블(211)에 기록하여, 연관시킨다. 이 시점에서, 암호화 처리부(1005)는 색인 포트 번호를 단서로, XPTCP 처리 대상 마스터(208)의 레코드를 특정해서, 암호화의 폴리시를 설정할 수 있다(S1504). 그리고, 일련의 처리를 종료한다(S1505).

[0260] 단계 S1502에서, accept 이벤트를 검출할 수 없었다면(S1502의 NO), 이벤트 검출부(1001)는 다음으로 TCP/IP 프로토콜 스택(205)으로부터 외측 NIC(108)에 대한 커넥션에 따른 connect 응답 이벤트를 검출했는지 여부를 확인한다(S1506). connect 응답 이벤트를 검출했다면(S1506의 YES), 이벤트 검출부(1001)는 소켓 조작부(1002)를 제어해서, 해당 connect 응답 이벤트에 따른, 생성된 소켓의, 소켓 메모리 영역(1004) 내에서의 어드레스를 취득한다(S1507).

[0261] 다음으로, 이벤트 검출부(1001)는 색인 포트 번호를 공유하는, 내측 NIC(104)에 대한 커넥션에 따른 소켓과, 외측 NIC(108)에 대한 커넥션에 따른 소켓의 관련지음을 수행한다(S1508). 이 시점에서, 복호 처리부(1006)는 색인 포트 번호를 단서로, XPTCP 처리 대상 마스터(208)의 레코드를 특정해서, 복호의 폴리시를 설정할 수 있다(S1509). 그리고, 일련의 처리를 종료한다(S1505).

[0262] 이렇게 하는 것으로, 내측 NIC(104)에 대한 커넥션에 따른 소켓으로부터 얻어진 스트림 데이터는, 암호화 처리부(1005)를 통해 암호화되고, 암호화된 스트림 데이터는 외측 NIC(108)에 대한 커넥션에 따른 소켓에 출력된다. 또한 반대로, 외측 NIC(108)에 대한 커넥션에 따른 소켓으로부터 얻어진 스트림 데이터는, 복호 처리부(1006)를 통해 복호되고, 복호된 스트림 데이터는 내측 NIC(104)에 대한 커넥션에 따른 소켓에 출력된다.

[0263] 단계 S1506에서, connect 응답 이벤트를 검출할 수 없었다면(S1506의 NO), 이벤트 검출부(1001)는 다음으로 TCP/IP 프로토콜 스택(205)으로부터 외측 NIC(108)에 대한 커넥션에 따른 close 이벤트를 검출했는지 여부를 확인한다(S1510). close 이벤트를 검출 했다면(S1510의 YES), 이벤트 검출부(1001)는 소켓 조작부(1002)를 제어해서, 해당 close 이벤트에 따른, 생성된 소켓 간 관련지음을 개방함과 동시에, XPTCP 폴리시 테이블(211)의 해

당 레코드를 삭제한다(S1511). 그리고, 일련의 처리를 종료한다(S1505).

[0264] 단계 S1510에서, close 이벤트를 검출할 수 없었다면(S1510의 NO), 이벤트 검출부(1001)는 특별히 아무것도 하지 않는다. 그 대신에, 암호화 처리부(1005) 및 복호 처리부(1006)는, 소켓 조작부(1002)로부터 스트림 데이터를 받고, XPTCP 폴리시 테이블(211)에서 특정한 암호화 또는 복호 폴리시에 근거해 암호화 또는 복호 처리를 실행하고(S1512), 소켓 조작부(1002)는 그것들 처리된 스트림 데이터를 전송한다(S1513). 그리고, 일련의 처리를 종료한다(S1505).

[0265] [XPTCP 게이트웨이 장치(101)의 동작·소켓 처리부(207)의 동작]

[0266] 도 16은, 소켓 처리부(207)의 초기 동작의 흐름을 나타내는 플로우 차트이다.

[0267] 처리를 개시하면(S1601), 소켓 처리부(207)는 미리 정해진 포트 번호에 대한, TCP 서버 기능을 기동한다(S1602). 이때, 내측 NIC(104)를 향해 리퀘스트(request)를 받아들이기 위한 소켓이 작성되고(socket 함수), 해당 소켓에는 리퀘스트를 받아들일 때의 포트 번호가 정의된다(bind 함수). 그리고, 일련의 처리를 종료한다(S1603).

[0268] 도 17은, 소켓 처리부(207)의 접속 요구 전송 처리의 흐름을 나타내는 플로우 차트이다.

[0269] 소켓 처리부(207)는, TCP/IP 프로토콜 스택(205)으로부터 connect 이벤트를 받으면(S1301), 소켓을 통해 내측 NIC(104)에 대해 접속 허가를 나타내는 accept 이벤트를 발행한다(S1702). 이는 서버로서의 행위이다. 다음으로 소켓 처리부(207)는, 외측 NIC(108)를 향해, 접속을 요구하는 connect request 이벤트를 발행한다(S1703). 이는 클라이언트로서의 행위이다. 그리고, 일련의 처리를 종료한다(S1704).

[0270] [XPTCP 게이트웨이 장치(101)의 동작·어드레스 변환 처리부(203)에 의한 패킷의 변화]

[0271] 도 18, 도 19 및 도 20은, XPTCP 게이트웨이 장치(101)를 통과하는 패킷의 변화를 나타내는 개략도이다.

[0272] XPTCP 비대응 PC(103)에는, 제1 MAC 어드레스와 제1 IP 어드레스가 부여되고 있다.

[0273] XPTCP 대응 서버(107)에는, 제2 MAC 어드레스와 제2 IP 어드레스가 부여되고 있다.

[0274] XPTCP 비대응 PC(103)로부터 XPTCP 대응 서버(107)를 향해 패킷이 송신되면, 송신 패킷은 내측 NIC(104)를 통해, 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)는 내측 NIC 어드레스 테이블(209)을 참조하여, 어드레스 변환 처리를 행한다. 그러면, 송신 패킷은 어드레스 변환 처리종료 송신 패킷으로 변화한다.

[0275] 어드레스 변환 처리종료 송신 패킷은, 목적지 IP 어드레스가 내측 NIC(104)의 IP 어드레스이다. 따라서, TCP/IP 프로토콜 스택(205)은 어드레스 변환 처리종료 송신 패킷을 받아들여, 패킷으로부터 MAC 헤더, IP 헤더, TCP 헤더의 순서로 헤더를 제거하고, 페이로드를 연결하여 스트림 데이터를 복원한다. 복원된 스트림 데이터는 소켓을 통해 XPTCP 처리부에 도달한다. XPTCP 처리부는 스트림 데이터에 소정의 암호화 처리를 행한다. 그리고, 암호화된 스트림 데이터는 외측 NIC(108)를 향해 작성된 소켓에 공급된다.

[0276] TCP/IP 프로토콜 스택(205)은 암호화된 스트림 데이터를 소정의 바이트(Byte) 길이로 구분하고, TCP 헤더, IP 헤더 및 MAC 헤더를 부가하여, 암호화 및 어드레스 변환 처리종료 송신 패킷을 작성한다. 즉, 이 시점에서 작성된 패킷의 목적지 IP 어드레스는, 제2 임시 IP 어드레스이며, 본래의 송신지인 XPTCP 대응 서버(107)의 IP 어드레스(제2 IP 어드레스)는 아니다. 그러므로, 어드레스 변환 처리부는 외측 NIC 어드레스 테이블(210)을 참조하여, 어드레스 복원 처리를 행한다. 그러면, 암호화 및 어드레스 변환 처리종료 송신 패킷은, 암호화 처리종료 송신 패킷이 되어, XPTCP 대응 서버(107)에 도달한다.

[0277] XPTCP 대응 서버(107)로부터 XPTCP 비대응 PC(103)를 향해 암호화 처리종료 수신 패킷이 반송되면, 암호화 처리종료 수신 패킷은 외측 NIC(108)를 통해, 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)는 외측 NIC 어드레스 테이블(210)을 참조하여, 어드레스 변환 처리를 행한다. 그러면, 암호화 처리종료 수신 패킷은 암호화 및 어드레스 변환 처리종료 수신 패킷으로 변화한다.

[0278] 암호화 및 어드레스 변환 처리종료 수신 패킷은, 목적지 IP 어드레스가 외측 NIC(108)의 IP 어드레스이다. 따라서, TCP/IP 프로토콜 스택(205)은 암호화 및 어드레스 변환 처리종료 수신 패킷을 받아들여, 패킷으로부터 MAC 헤더, IP 헤더, TCP 헤더의 순서로 헤더를 제거하고, 페이로드를 연결하여 암호화 스트림 데이터를 복원한다. 복원된 암호화 스트림 데이터는 소켓을 통해 XPTCP 처리부에 도달한다. XPTCP 처리부는 스트림 데이터에

소정의 복호 처리를 행한다. 그리고, 복호된 스트림 데이터는 외측 NIC(108)를 향해 작성된 소켓에 공급된다.

[0279] TCP/IP 프로토콜 스택(205)은 복호된 스트림 데이터를 소정의 바이트 길이로 구분하고, TCP 헤더, IP 헤더 및 MAC 헤더를 부가하여, 어드레스 변환 처리종료 수신 패킷을 작성한다. 즉, 이 시점에서 작성된 패킷의 목적지 IP 어드레스는, 제1 임시 IP 어드레스이며, 본래의 송신지인 XPTCP 비대응 PC(103)의 IP 어드레스(제1 IP 어드레스)는 아니다. 그러므로, 어드레스 변환 처리부는 내측 NIC 어드레스 테이블(209)을 참조하여, 어드레스 복원 처리를 행한다. 그러면, 어드레스 변환 처리종료 수신 패킷은, 수신 패킷이 되어, XPTCP 비대응 PC(103)에 도달한다.

[0280] [XPTCP 게이트웨이 장치(101)의 동작·TCP 접속 확립 시퀀스]

[0281] 도 21, 도 22 및 도 23은, XPTCP 게이트웨이 장치(101)에서의, TCP 접속 확립 시퀀스의 타임 차트이다. 도 21은 타임 차트 전체를 나타내는 조감도이며, 도 22는 타임 차트 중, 전반의 처리 내용을 나타내는 상세도이며, 도 23은 타임 차트 중, 후반의 처리 내용을 나타내는 상세도이다.

[0282] 단말로부터 TCP SYN 패킷이 송신된 것에 호응하여, 단말과 XPTCP 게이트웨이 장치(101)의 사이와, 서버와 XPTCP 게이트웨이 장치(101)의 사이 각각에, TCP 커넥션이 형성될 때까지의, XPTCP 게이트웨이 장치(101)의 시계열 상의 동작의 추이를 나타낸다.

[0283] XPTCP 비대응 PC(103)가 web 브라우저 등의 어플리케이션 프로그램을 동작시켜, XPTCP 대응 서버(107)에 접속하려고 하면, XPTCP 비대응 PC(103)는 어플리케이션 프로그램에 기인하여 TCP SYN 패킷을 송신한다(S2101).

[0284] TCP SYN 패킷은, 내측 NIC(104)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 수신 처리부(501)는, TCP SYN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2102). 또한, 이 시점에서 내측 NIC 어드레스 테이블(209)에 신규 레코드가 추가로 기록되며, 해당 레코드는 색인 포트 번호로 특정 가능하게 된다.

[0285] 어드레스 변환 처리가 행해진 TCP SYN 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, 소켓 처리부(207)가 미리 작성한 포트 번호에 대해 송신된 TCP SYN 패킷을 인식하여, 커넥션의 작성을 개시하기 위해, 소켓 처리부(207)에 대해 connect 이벤트를 발행한다(S2103).

[0286] 소켓 처리부(207)는, 자신의 서버 기능에 의해, connect 이벤트(접속 요구)에 대한 accept 이벤트(접속 허가)를, TCP/IP 프로토콜 스택(205)에 대해 발행한다(S2104).

[0287] XPTCP 처리부(206)는, 이 accept 이벤트를 후크(hook) 해서, 내측 NIC(104)를 향한 커넥션의 형성이 시작된 것을 인식한다(S2105). 그러면, XPTCP 처리부(206)는 어드레스 변환 처리부(203)에 대해, 색인 포트 번호를 수반하여 해당 커넥션에 적용하는 폴리시를 문의한다(S2106). 어드레스 변환 처리부(203)는 이 문의에 대해 XPTCP 처리 대상 마스터(208)와 내측 NIC 어드레스 테이블(209)을 참조하여, XPTCP 처리 대상 마스터(208)의 레코드 번호를 회답한다(S2107). XPTCP 처리부(206)는 XPTCP 폴리시 테이블(211)에 레코드 번호와 색인 포트 번호를 등록하여 연관시키고, 복호 처리부(1006)의 폴리시를 설정한다(S2108).

[0288] 단계 S2104에서 발행된 accept 이벤트는 TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은 accept 이벤트를 받고, TCP ACK/SYN 패킷을 생성한다(S2109). TCP ACK/SYN 패킷은 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 송신 처리부(504)는, TCP ACK/SYN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 복원한다(S2110).

[0289] TCP ACK/SYN 패킷은, 내측 NIC(104)를 통해 XPTCP 비대응 PC(103)에 도달한다. XPTCP 비대응 PC(103)는, TCP ACK/SYN 패킷을 받고, TCP ACK 패킷으로 응답한다(S2111).

[0290] TCP ACK 패킷은, 내측 NIC(104)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 수신 처리부(501)는, TCP ACK 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2112).

[0291] 어드레스 변환 처리가 행해진 TCP ACK 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, TCP ACK 패킷의 도착으로, 커넥션이 확립한 것을 인식한다(S2113). 이후, 해당 커넥션에는 TCP 데이터 패킷이 송수신된다.

[0292] 소켓 처리부(207)는, 단계 S2104에서 내측 NIC(104)를 향해 서버 기능으로서의 accept 이벤트를 발행한 후, 외측 NIC(108)를 향해 클라이언트 기능으로서 접속 요구를 나타내는 connect request 이벤트를 발행한다(S2114).

[0293] connect request 이벤트는 TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은 connect request 이벤트를 받고, ARP 요구 패킷을 생성한다(S2115).

[0294] ARP 요구 패킷은 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 송신 처리부(503)는, ARP 요구 패킷에 대한 ARP 응답 패킷을 생성하여, TCP/IP 프로토콜 스택(205)으로 반송한다(S2116).

[0295] TCP/IP 프로토콜 스택(205)은, ARP 응답 패킷을 받으면, 단계 S2114에서의 connect request 이벤트에 대응하는 TCP SYN 패킷을 생성할 준비가 갖추어졌으므로, TCP SYN 패킷을 생성한다(S2117).

[0296] 단계 S2117에서 생성되는 TCP SYN 패킷은 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 송신 처리부(503)는, TCP SYN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2118). 또한, 이 시점에서 외측 NIC 어드레스 테이블(210)의 해당 레코드에, TCP SYN 패킷의 송신원 포트 번호로서, TCP/IP 프로토콜 스택(205)에 의해 자동적으로 첨부되고 있는 동적 포트 번호가 기록된다.

[0297] TCP SYN 패킷은, 외측 NIC(108)를 통해 XPTCP 대응 서버(107)에 도달한다. XPTCP 대응 서버(107)는, TCP SYN 패킷을 받고, TCP ACK/SYN 패킷으로 응답한다(S2119).

[0298] TCP ACK/SYN 패킷은, 외측 NIC(108)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 수신 처리부(502)는, TCP ACK/SYN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2120).

[0299] 어드레스 변환 처리가 행해진 TCP ACK/SYN 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, TCP ACK/SYN 패킷을 받고, TCP ACK 패킷으로 응답한다(S2121). 이때, TCP/IP 프로토콜 스택(205)은 connect 응답 이벤트를 클라이언트 프로그램인 소켓 처리부(207)에 통지한다.

[0300] XPTCP 처리부(206)는, 이 connect 응답 이벤트를 후크 해서, 외측 NIC(108)를 향한 커넥션의 형성이 시작된 것을 인식한다(S2122). 그러면, XPTCP 처리부(206)는 어드레스 변환 처리부(203)에 대해, 색인 포트 번호를 수반하여 해당 커넥션에 적용하는 폴리시를 문의한다(S2123). 어드레스 변환 처리부(203)는 이 문의에 대해 XPTCP 처리 대상 마스터(208)와 내측 NIC 어드레스 테이블(209)을 참조하여, XPTCP 처리 대상 마스터(208)의 레코드 번호를 회답한다(S2124). XPTCP 처리부(206)는 XPTCP 폴리시 테이블(211)에 레코드 번호와 색인 포트 번호를 등록해 연관시키고, 암호화 처리부(1005)의 폴리시를 설정한다(S2125).

[0301] 단계 S2121에서 TCP/IP 프로토콜 스택(205)으로부터 발행된 TCP ACK 패킷은, 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 송신 처리부(503)는, TCP ACK 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 복원한다(S2126).

[0302] TCP ACK 패킷은, 외측 NIC(108)를 통해 XPTCP 대응 서버(107)에 도달한다. XPTCP 대응 서버(107)는, TCP ACK 패킷의 도착으로, 커넥션이 확립한 것을 인식한다(S2127). 이후, 해당 커넥션에는 TCP 데이터 패킷이 송수신된다.

[0303] [XPTCP 게이트웨이 장치(101)의 동작 · TCP 데이터 전송 시퀀스]

[0304] 도 24는, XPTCP 게이트웨이 장치(101)에서의, TCP 데이터 전송 시퀀스의 타임 차트이다. 단말로부터 TCP 데이터 패킷이 송신된 것에 호응하여, 단말과 XPTCP 게이트웨이 장치(101)의 사이와, 서버와 XPTCP 게이트웨이 장치(101)의 사이 각각에 형성된 TCP 커넥션에 TCP 데이터 패킷이 통과할 때의, XPTCP 게이트웨이 장치(101)의 시계열 상의 동작의 추이를 나타낸다.

[0305] XPTCP 비대응 PC(103)가 web 브라우저 등의 어플리케이션 프로그램을 동작시켜, XPTCP 대응 서버(107)에 데이터를 송신하려고 하면, XPTCP 비대응 PC(103)는 어플리케이션 프로그램에 기인하여 TCP 데이터 패킷을 송신한다(S2401).

[0306] TCP 데이터 패킷은, 내측 NIC(104)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 수신 처리부(501)는, TCP 데이터 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2402).

[0307] 어드레스 변환 처리가 행해진 TCP 데이터 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, TCP 데이터 패킷의 헤더를 제거하고, TCP 데이터 패킷 페이로드를 연결하여, 스트림 데이터로 복원한다(S2403).

[0308] 스트림 데이터는 XPTCP 처리부(206)에 의해 암호화 처리가 행해져 외측 NIC(108)의 소켓으로 전송된다(S2404).

[0309] 암호화 처리가 행해진 스트림 데이터는, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, 스트림 데이터를 소정의 바이트 길이 단위로 분할한 후, 헤더를 부가해서, TCP 데이터 패킷으로 변환한다(S2405).

[0310] TCP 데이터 패킷은 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 송신 처리부(503)는, TCP 데이터 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2406).

[0311] 어드레스 복원 처리가 행해진 TCP 데이터 패킷은, 외측 NIC(108)를 통해 XPTCP 대응 서버(107)에 도달한다(S2407). XPTCP 대응 서버(107)는, TCP 데이터 패킷을 받고, 소정의 처리를 수행한 후, 회신 데이터로서의 TCP 데이터 패킷을, XPTCP 비대응 PC(103)를 향해 송신한다(S2408).

[0312] TCP 데이터 패킷은, 외측 NIC(108)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 수신 처리부(502)는, TCP 데이터 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2409).

[0313] 어드레스 변환 처리가 행해진 TCP 데이터 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, TCP 데이터 패킷의 헤더를 제거하고, TCP 데이터 패킷 페이로드를 연결하여, 스트림 데이터로 복원한다(S2410).

[0314] 스트림 데이터는 XPTCP 처리부(206)에 의해 복호 처리가 행해져 내측 NIC(104)의 소켓으로 전송된다(S2411).

[0315] 복호 처리가 행해진 스트림 데이터는, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, 스트림 데이터를 소정의 바이트 길이 단위로 분할한 후, 헤더를 부가해서, TCP 데이터 패킷으로 변환한다(S2412).

[0316] TCP 데이터 패킷은 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 송신 처리부(504)는, TCP 데이터 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2413).

[0317] 어드레스 복원 처리가 행해진 TCP 데이터 패킷은, 내측 NIC(104)를 통해 XPTCP 비대응 PC(103)에 도달한다(S2414).

[0318] [XPTCP 게이트웨이 장치(101)의 동작 · TCP 절단 시퀀스]

[0319] 도 25, 도 26 및 도 27은, XPTCP 게이트웨이 장치(101)에서의, TCP 절단 시퀀스의 타임 차트이다. 도 25는 타임 차트 전체를 나타내는 조감도이며, 도 26은 타임 차트 중, 전반의 처리 내용을 나타내는 상세도이며, 도 27은 타임 차트 중, 후반의 처리 내용을 나타내는 상세도이다.

[0320] 단말로부터 TCP FIN 패킷이 송신된 것에 호응하여, 단말과 XPTCP 게이트웨이 장치(101)의 사이와, 서버와 XPTCP 게이트웨이 장치(101)의 사이 각각에 형성되어 있던 TCP 커넥션이 종료(close : 클로즈)될 때까지의, XPTCP 게이트웨이 장치(101)의 시계열 상의 동작의 추이를 나타낸다.

[0321] XPTCP 비대응 PC(103)가 web 브라우저 등의 어플리케이션 프로그램을 동작시켜, XPTCP 대응 서버(107)에 대해 소정의 데이터를 요구하고, 그 요구한 데이터가 얻어진다면, XPTCP 비대응 PC(103)는 어플리케이션 프로그램에 기인해 TCP FIN 패킷을 송신한다(S2501).

[0322] TCP FIN 패킷은, 내측 NIC(104)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 수신 처리부(501)는, TCP FIN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2102). 또한, 이 시점에서 삭제 예정 리스트(605)에 색인 포트 번호가 추가로 기록된다.

[0323] 어드레스 변환 처리가 행해진 TCP FIN 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, 소켓 처리부(207)가 미리 작성한 포트 번호에 대해 송신된 TCP FIN 패킷을 인식하고, 서버 프로그램인 소켓 처리부(207)에 커넥션의 종료를 통지하기 위해, 소켓 처리부(207)에 대해 close 이벤트를 발행한다(S2503).

[0324] 소켓 처리부(207)는, 단계 S2503에서 내측 NIC(104)를 향해 서버 기능으로서의 close 이벤트를 받은 후, 외측 NIC(108)를 향해 클라이언트 기능으로서 절단 요구를 나타내는 close request 이벤트를 발행한다(S2504).

[0325] close request 이벤트는 TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은 close

request 이벤트를 받고, TCP FIN 패킷을 생성한다(S2505).

[0326] 단계 S2505에서 생성되는 TCP FIN 패킷은 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 송신 처리부(503)는, TCP FIN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2506).

[0327] TCP FIN 패킷은, 외측 NIC(108)를 통해 XPTCP 대응 서버(107)에 도달한다(S2507). XPTCP 대응 서버(107)는 TCP FIN 패킷을 받고, XPTCP 비대응 PC(103)에 대해 송신해야 할 데이터를 모두 송신했다고 판단하면, TCP ACK/FIN 패킷을 송신한다(S2508).

[0328] TCP ACK/FIN 패킷은, 외측 NIC(108)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 수신 처리부(502)는, TCP ACK/FIN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2509).

[0329] 어드레스 변환 처리가 행해진 TCP ACK/FIN 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, TCP ACK/FIN 패킷을 받고, TCP ACK 패킷으로 응답한다(S2510). 이때, TCP/IP 프로토콜 스택(205)은 close 응답 이벤트를 클라이언트 프로그램인 소켓 처리부(207)에 통지한다.

[0330] XPTCP 처리부(206)는, 이 close 응답 이벤트를 후크 해서, 외측 NIC(108)를 향한 커넥션과 내측 NIC(104)를 향한 커넥션과의 관련지음을 해방한다(S2511).

[0331] 단계 S2510에서 TCP/IP 프로토콜 스택(205)에 의해 생성되는 TCP ACK 패킷은, 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 외측 NIC 송신 처리부(503)는, TCP ACK 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2512).

[0332] TCP ACK 패킷은, 외측 NIC(108)를 통해 XPTCP 대응 서버(107)에 도달한다. XPTCP 대응 서버(107)는, TCP ACK 패킷을 받고, 해당 패킷에 따른 커넥션의 절단이 완료한(클로즈된) 것을 인식한다(S2513).

[0333] 한편, 단계 S2510에서 TCP/IP 프로토콜 스택(205)에 의해 생성되는 close 응답 이벤트는, 소켓 처리부(207)에 도달한다. 소켓 처리부(207)는, close 응답 이벤트를 검출하면, 외측 NIC(108)를 향한 커넥션에 대한 TCP FIN 패킷이 온 것을 인식한다. 이 시점에서, 대응하는 내측 NIC(104)를 향한 커넥션의 절단 처리도 수행할 수 있게 된다. 그러므로, 단계 S2503에서 TCP/IP 프로토콜 스택(205)이 송출한 close 이벤트에 대한 응답으로서, 허가를 의미하는 accept 이벤트를, TCP/IP 프로토콜 스택(205)에 송출한다(S2514).

[0334] 단계 S2514에서 소켓 처리부(207)가 송출한 accept 이벤트는, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은 accept 이벤트를 받고, TCP ACK/FIN 패킷을 생성한다(S2515). TCP ACK/FIN 패킷은 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 송신 처리부(504)는, TCP ACK/FIN 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 복원한다(S2516).

[0335] TCP ACK/FIN 패킷은, 내측 NIC(104)를 통해 XPTCP 비대응 PC(103)에 도달한다. XPTCP 비대응 PC(103)는, TCP ACK/FIN 패킷을 받고, TCP ACK 패킷으로 응답한다(S2517).

[0336] TCP ACK 패킷은, 내측 NIC(104)를 통해 어드레스 변환 처리부(203)에 도달한다. 어드레스 변환 처리부(203)의 내측 NIC 수신 처리부(501)는, TCP ACK 패킷의 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 변환한다(S2518).

[0337] 어드레스 변환 처리가 행해진 TCP ACK 패킷은, TCP/IP 프로토콜 스택(205)에 도달한다. TCP/IP 프로토콜 스택(205)은, TCP ACK 패킷의 도착으로, 커넥션의 절단이 완료한 것을 인식한다(S2519).

[0338] 한편, 단계 S2509에서 어드레스 변환을 수행한 후, 어드레스 변환 처리부는 어드레스 테이블 갱신 카운터의 값을, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 타이머용 카운터 값 필드에 기입한다(S2520). 테이블 갱신 처리부(505)는 정기적으로 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 카운터 값 필드를 감시하고, 소정 시간이 경과하면, 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)의 해당 레코드를 삭제한다(S2521, S2522).

[0339] 또한, TCP 커넥션을 절단하는 수단은, TCP FIN 패킷 만이 아니다. 어플리케이션 프로그램의 프리즈(freeze) 등, 이상한 상태에 빠졌을 때에 TCP 커넥션을 강제적으로 절단하기 위해, TCP RST 패킷이 존재한다. TCP RST 패킷이 발생했을 때의 절단 시퀀스는, 도 25, 도 26 및 도 27의 점선으로 둘러싼 범위의 처리가 바뀌게 되지만, 자세한 것은 생략한다.

[0340] [정리]

[0341] XPTCP 비대응 PC(102)로부터 수신한 패킷 P(1402)는, 내측 NIC(104) 및 외측 NIC(108)의 IP 어드레스와는 무관계하다. 이 때문에, 패킷 P(1402)의 상태로는, TCP/IP 프로토콜 스택(205)이 소정의 패킷의 처리를 수행할 수 없다. 그러므로, 일단 내측 NIC 어드레스 테이블(209)의 레코드에, 패킷 P(1402)에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 메모해 둔다. 게다가, 나중에 복원하기 위해 색인이 되는 포트 번호를 연번으로 부여한다. 그리고, TCP/IP 프로토콜 스택(205)이 패킷의 수신 처리를 할 수 있도록 하기 위해, 패킷 P(1402)를 「제1 임시 IP 어드레스를 가지는 가공의 호스트로부터, 내측 NIC의 IP 어드레스를 향해 송신된 패킷」으로 하는, 패킷 P(1405)로 개서한다.

[0342] 또한, 이때, 송신원 포트 번호에는 색인 PORT를 부여하고, 목적지 포트 번호는 굳이 변경하지 않는다. 대부분의 경우, 목적지 포트 번호는 주지의 잘 알려진 포트(well known port)로 불리는 특정 포트 번호이다. 또한, XPTCP도 특정 서비스를 위해 실장하고 있다. XPTCP는 서비스마다 다른 암호화 처리를 행할 필요가 있으며, 목적지 포트 번호로 서비스를 구별해야 하므로, 내측 NIC 수신 처리부(501)는 패킷에 첨부되고 있는 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 개서할 때, 목적지 포트 번호만은 변경하지 않는다.

[0343] 이상 설명한 것처럼, XPTCP 게이트웨이 장치(101)는, 수신한 패킷을 일단 내부의 TCP/IP 프로토콜 스택(205)이 취급할 수 있도록, 수신한 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서한다. 그리고, 송신하기 직전에 다시 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 복원한다. 이 때문에, XPTCP 게이트웨이 장치(101)는 기존의 네트워크 환경에 전혀 설정의 변경을 필요로 하지 않고, 단지 통신 경로 상에 XPTCP 게이트웨이 장치(101)를 끼워 넣도록 접속하는 것 만으로, 용이하게 XPTCP 기능을 제공할 수 있다.

[0344] 게다가 부차적 효과로서, XPTCP 게이트웨이 장치(101)에 접속되는 모든 단말이나 서버로부터는, XPTCP 게이트웨이 장치(101)를 인식할 수 없다. PING 등의 ICMP 패킷조차 그대로 전송되어 버리므로, XPTCP 게이트웨이 장치(101)는 네트워크적으로 전혀 보이지 않는 장치로서 작용한다.

[0345] 그리고 더욱 부차적 효과로서 XPTCP 게이트웨이 장치(101)의 내측 NIC(104) 및 외측 NIC(108)로 설정하는 IP 어드레스는, XPTCP 게이트웨이 장치(101)에 접속되는 모든 호스트와 간섭하지 않는다. 즉, 내측 NIC(104) 및 외측 NIC(108)에 설정하는 IP 어드레스는, XPTCP 게이트웨이 장치(101)가 접속되는 서브넷(subnet)과는 일절 관계없는 IP 어드레스를 설정해도, 혹은 접속되는 호스트와 중복하는 IP 어드레스여도 전혀 문제가 없다. 모든 패킷은 XPTCP 게이트웨이 장치(101) 내부에서 어드레스 변환이 행해져, 송신될 때에는 어드레스가 복원되므로, 내측 NIC(104) 및 외측 NIC(108)에 설정하는 IP 어드레스는 네트워크 밖으로 나타나지 않는다. 내측 NIC(104) 및 외측 NIC(108)에 설정하는 IP 어드레스는, 루프백 어드레스(loop-back address)나 멀티캐스트 어드레스 등의 특수한 것을 제외하고, 무엇을 설정해도 무방하다.

[0346] [응용예]

[0347] 본 실시 형태에 따른 XPTCP 게이트웨이 장치(101)는, 이하와 같은 응용예를 생각할 수 있다.

[0348] (1) XPTCP 게이트웨이 장치(101)는, 용이하게 서버 기능을 실장할 수 있다. 예를 들면, XPTCP 처리 대상 마스터를 편집하기 위한 유저 인터페이스를 제공하기 위해 web 서버 프로그램을 가동시켜, 미리 특정의 포트 번호에 대응해 둔다. 일례로서, 10030이라는 포트 번호를 이용한다고 한다.

[0349] XPTCP 처리부(206)는, 목적지 포트 번호가 이 10030인 경우, 암호화 처리를 행하지 않고, 그대로 web 서버 프로그램에 인도한다. 이와 같이 XPTCP 처리부(206)를 구성 함으로써, XPTCP 게이트웨이 장치(101)는 용이하게 서버 기능을 실장할 수 있다.

[0350] (2) 어드레스 변환 처리부(203)가, 내측 NIC 어드레스 테이블(209)과 외측 NIC 어드레스 테이블(210)의, 2개의 테이블에서 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 개서하는 실장 형태인 것에는 이유가 있다.

[0351] 외측 NIC 어드레스 테이블(210)의, 목적지 IP 어드레스 필드를 개서하면, 단말이 의도하고 있는 IP 어드레스와는 다른 IP 어드레스의 서버와 통신할 수 있다.

[0352] 도 28은, XPTCP 게이트웨이 장치(101)에서, 송신하는 패킷의 목적지 IP 어드레스를 개서하는 응용 형태를 설명

하는 개략도이다.

[0353] 단말(2801)에는 「A」라는 IP 어드레스가 부여되고 있다. 지금, 단말(2801)은 「B」라는 IP 어드레스가 부여되고 있는 서버(2802)에 접속하려고, 패킷 P(2803)를 송신했다고 한다. 패킷 P(2803)의 송신원 IP 어드레스는 「A」이며, 목적지 IP 어드레스는 「B」이다.

[0354] XPTCP 게이트웨이 장치(101)의 내측 NIC 어드레스 테이블(209)은, 「A」와 「B」라는 대응 관계를 충실히 재현할 수 있을 필요가 있으므로, 그대로의 IP 어드레스가 기록된다.

[0355] 그러나, 외측 NIC 어드레스 테이블(210)은, 「A」와 「B」라는 대응 관계를 반드시 충실히 재현할 수 없어도 무방하다. 지금, 목적지 IP 어드레스를 「C」로 개서하면, XPTCP 게이트웨이 장치(101)로부터 송출되는 패킷 P(2804)는, 송신원 IP 어드레스가 「A」이며, 목적지 IP 어드레스가 「C」가 된다. 그러면, 패킷 P(2804)는 IP 어드레스가 「C」인 서버(2805)에 도달한다.

[0356] 이와 같이, XPTCP 게이트웨이 장치(101)는, 외측 NIC 어드레스 테이블(210)에 등록되어 있는 목적지 IP 어드레스를 개서 함으로써, 목적지 IP 어드레스를 단말(2801)이 파악하고 있지 않는 곳에서 변환할 수 있다. 이 동작을 응용하면, XPTCP 게이트웨이 장치(101)를 2대 이상 연결하여 구성하는 것으로, 용이하게 VPN(Virtual Private Network)을 구축할 수 있다.

[0357] (3) 어드레스 변환 처리부(203)가, 내측 NIC 어드레스 테이블(209)과 외측 NIC 어드레스 테이블(210)의, 2개의 테이블로 송신원 및 목적지 MAC 어드레스, IP 어드레스 및 포트 번호를 개서하는 실장 형태인 것에는 이유가 있다.

[0358] 외측 NIC 어드레스 테이블(210)의, 송신원 IP 어드레스 필드를 개서하면, 서버 측에 존재하는 악의를 가진 제3자로부터, 단말(2801)의 진정한 IP 어드레스를 은폐할 수 있다.

[0359] 도 29는, XPTCP 게이트웨이 장치(101)에서, 송신하는 패킷의 송신원 IP 어드레스를 개서하는 응용 형태를 설명하는 개략도이다.

[0360] 단말(2901)에는 「A」라는 IP 어드레스가 부여되고 있다. 지금, 단말(2901)은 「B」라는 IP 어드레스가 부여되고 있는 서버(2902)에 접속하려고, 패킷 P(2903)를 송신했다고 한다. 패킷 P(2903)의 송신원 IP 어드레스는 「A」이며, 목적지 IP 어드레스는 「B」이다.

[0361] XPTCP 게이트웨이 장치(101)의 내측 NIC 어드레스 테이블(209)은, 「A」와 「B」라는 대응 관계를 충실히 재현할 수 있을 필요가 있으므로, 그대로의 IP 어드레스가 기록된다.

[0362] 그러나, 외측 NIC 어드레스 테이블(210)은, 「A」와 「B」라는 대응 관계를 반드시 충실히 재현할 수 없어도 무방하다. 지금, 송신원 IP 어드레스를 「D」로 개서하면, XPTCP 게이트웨이 장치(101)로부터 송출되는 패킷 P(2904)는, 송신원 IP 어드레스가 「D」이며, 목적지 IP 어드레스가 「B」가 된다. 그러면, 서버(2902)에서 보면 마치 송신원 IP 어드레스가 「D」인 가상 단말(2905)로부터 송신된 것처럼 보이므로, IP 어드레스 「A」인 단말(2901)의 존재를 은폐할 수 있다.

[0363] 이와 같이, XPTCP 게이트웨이 장치(101)는, 외측 NIC 어드레스 테이블(210)에 등록되어 있는 송신원 IP 어드레스를 개서 함으로써, 송신원 IP 어드레스를 악의를 가진 제3자로부터 은폐할 수 있다.

[0364] (4) 암호화 처리부(1005)는, TCP/IP 프로토콜 스택(205)이 TCP 데이터 패킷으로부터 페이로드 부분을 꺼내 복원한 스트림 데이터에 대해, 암호화 처리를 행한다. 이 암호화 처리는, 반드시 스트림 데이터 전체를 암호화한다고는 할 수 없다.

[0365] 예를 들면, 주지의 TELNET(TCP 포트 23번)의 경우에는, 스트림 데이터를 모두 암호화할 필요가 있다.

[0366] 그러나, 예를 들면 주지의 SMTP(Simple Mail Transfer Protocol : TCP 포트 25번)의 경우에는, 송신한 메일이 SMTP 서버를 전전하며 전송될 가능성이 있다. 그 때, 모든 SMTP 서버가 XPTCP의 인증 및 암호화 처리에 대응하는 것은 곤란하다. 그러므로, 송신원인 단말과, 최종적으로 수신하는 측의 호스트만 인증 및 암호화 처리에 대응시켜, 암호화의 대상은 SMTP 메시지의 본문만으로 한다. 주지하는 바와 같이, SMTP 메시지는 한 줄의 빈 개행을 세퍼레이터(separator)로 하여 헤더와 본문으로 나눠지며, 헤더에는 메일이 SMTP 서버 등의 호스트를 경유할 때에 기록되는 정보(Received: 헤더)가 추기된다.

[0367] 본 실시 형태의 암호화 처리부(1005)도, SMTP나 HTTP 등, 스트림 데이터가 헤더와 본문으로 분리할 수 있는 프

로토콜인 경우 등, 프로토콜에 따라 암호화의 대상을 스트림 데이터 전부가 아니라 본문만으로 한다,와 같은 처리가 포함되는 것이 바람직하다.

[0368] 본 실시 형태에서는, 네트워크 게이트웨이 장치를 개시했다.

[0369] 기존의 네트워크 OS에 표준 탑재되고 있는 TCP/IP 프로토콜 스택(205)의 기능을 최대한 유효하게 활용하면서, 필요 최소한의 프로그램을 추가 함으로써 XPTCP 게이트웨이 장치(101)를 실현하기 위해, TCP/IP 프로토콜 스택(205)을 「속이는」 처리를 행한다. XPTCP 게이트웨이 장치(101)에 할당되고 있는 IP 어드레스와는 무관계여야 할 패킷을 TCP/IP 프로토콜 스택(205)이 처리할 수 있도록 하기 위해, 미리 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 송신원 포트 번호, 목적지 MAC 어드레스, 목적지 IP 어드레스 및 목적지 포트 번호를 내측 NIC 어드레스 테이블(209) 및 외측 NIC 어드레스 테이블(210)에 메모해 둔다. 그 다음에, 수신한 패킷에 첨부되고 있는 송신원 MAC 어드레스 및 송신원 IP 어드레스는 가짜의 MAC 어드레스 및 가짜의 IP 어드레스로, 목적지 MAC 어드레스 및 목적지 IP 어드레스는 XPTCP 게이트웨이 장치(101)에 할당되고 있는 IP 어드레스 및 MAC 어드레스로 개서하고 나서, TCP/IP 프로토콜 스택(205)에게 준다.

[0370] 게다가, 패킷을 본래의 송신지에 송신할 때에는, XPTCP 게이트웨이 장치(101)에 할당되고 있는 IP 어드레스 및 MAC 어드레스에서 가짜의 MAC 어드레스 및 가짜의 IP 어드레스로 반송하도록, TCP/IP 프로토콜 스택(205)을 속여, TCP/IP 프로토콜 스택(205)으로부터 송신되는 패킷의 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 앞서 개서 테이블에 메모한 본래의 어드레스로 복원하여, 본래의 송신지에 송신한다.

[0371] 이와 같이 XPTCP 게이트웨이 장치(101)는, 수신한 패킷을 일단 내부의 TCP/IP 프로토콜 스택(205)이 취급할 수 있도록, 수신한 패킷에 첨부되고 있는 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 개서한다. 그리고, 송신하기 직전에 다시 송신원 MAC 어드레스, 송신원 IP 어드레스, 목적지 MAC 어드레스 및 목적지 IP 어드레스를 복원한다. 이 때문에, XPTCP 게이트웨이 장치(101)는 기존의 네트워크 환경에 전혀 설정의 변경을 필요로 하지 않고, 단지 통신 경로 상에 XPTCP 게이트웨이 장치(101)를 끼워 넣도록 접속하는 것만으로, 용이하게 XPTCP 기능을 제공할 수 있다.

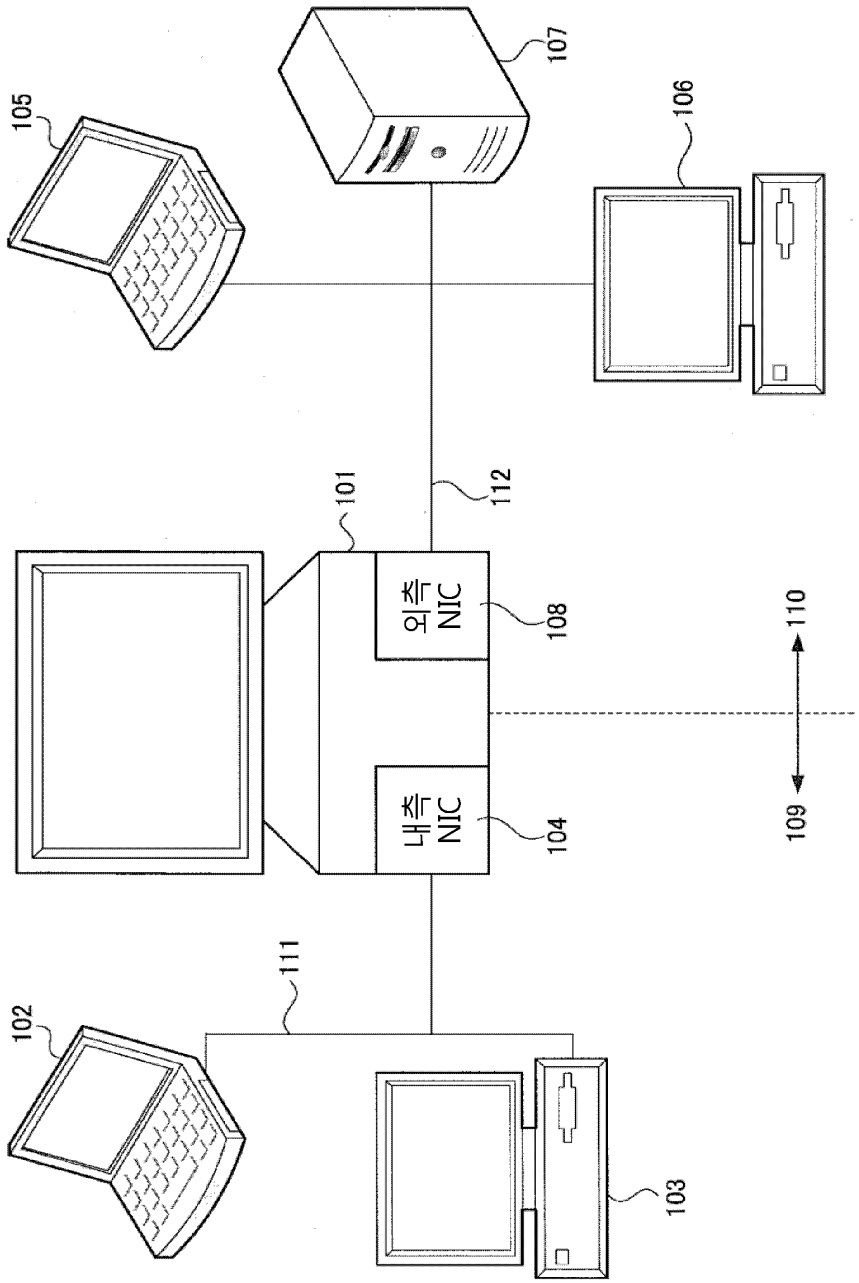
[0372] 이상, 본 발명의 실시 형태예에 대해 설명했지만, 본 발명은 상기 실시 형태예로 한정되는 것은 아니고, 특허청구범위에 기재한 본 발명의 요지를 벗어나지 않는 범위에서, 다른 변형예, 응용예를 포함한다.

부호의 설명

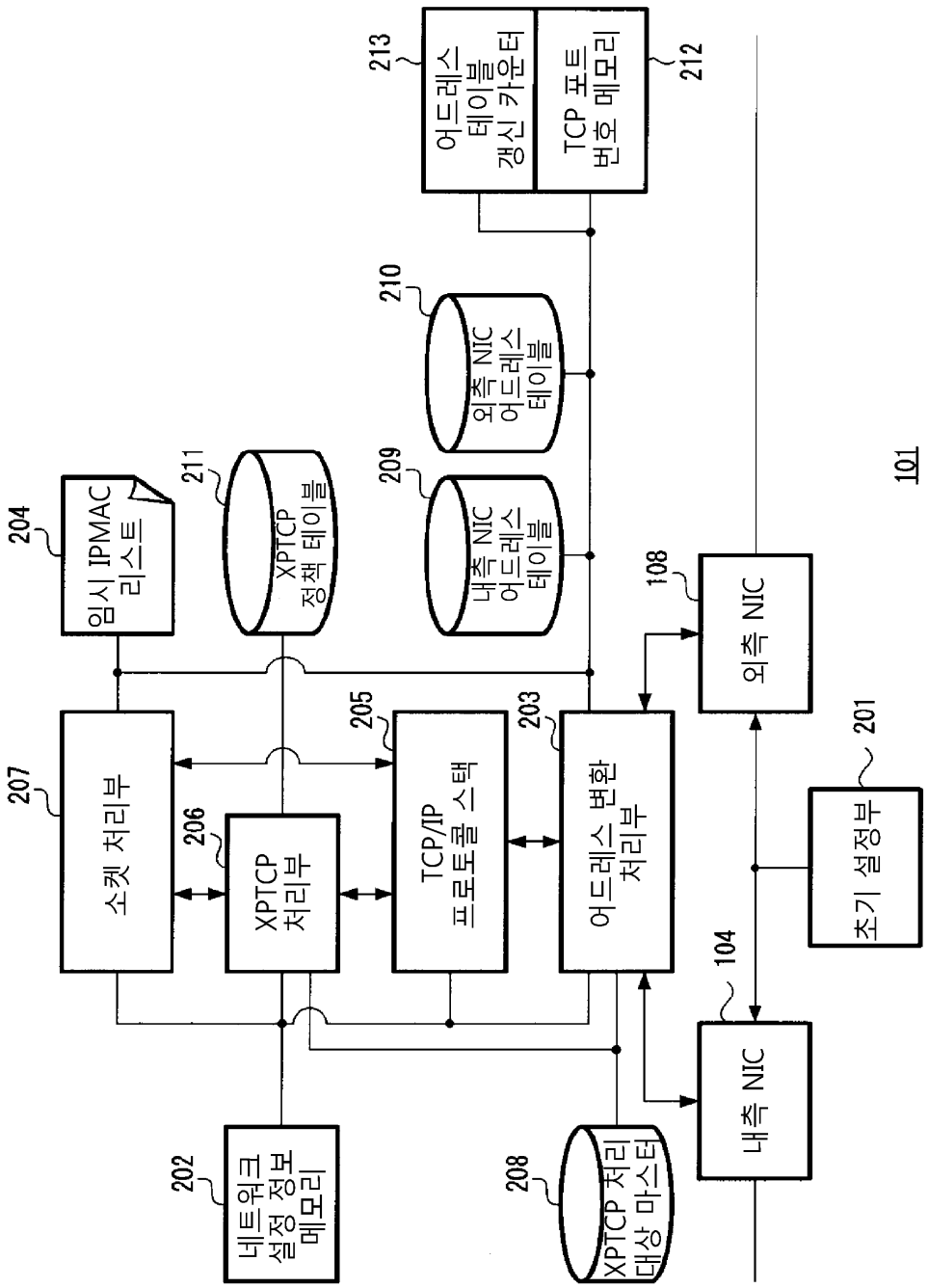
[0373] 101: XPTCP 게이트웨이 장치, 102: XPTCP 비대응 PC, 103: XPTCP 비대응 PC, 104: 내측 NIC, 105: XPTCP 비대응 PC, 106: XPTCP 대응 PC, 107: XPTCP 대응 서버, 108: 외측 NIC, 109: XPTCP 비대응 네트워크, 110: XPTCP 대응 네트워크, 201: 초기 설정부, 202: 네트워크 설정 정보 메모리, 203: 어드레스 변환 처리부, 204: 임시 IPMAC 리스트, 205: TCP/IP 프로토콜 스택, 206: XPTCP 처리부, 207: 소켓 처리부, 208: XPTCP 처리 대상 마스터, 209: 내측 NIC 어드레스 테이블, 210: 외측 NIC 어드레스 테이블, 211: XPTCP 폴리시 테이블, 212: TCP 포트 번호 메모리, 213: 어드레스 테이블 갱신 카운터, 401: IP 헤더, 402: MAC 헤더, 403: TCP 헤더, 404: UDP 헤더, 501: 내측 NIC 수신 처리부, 502: 외측 NIC 수신 처리부, 503: 외측 NIC 송신 처리부, 504: 내측 NIC 송신 처리부, 505: 테이블 갱신 처리부, 506: 폴리시 회답부, 601: 수신 패킷 판정부, 602: 어드레스 치환부, 603: 커넥션 등록 처리부, 604: 레코드 삭제 준비 처리부, 605: 삭제 예정 리스트, 701: 수신 패킷 판정부, 702: 어드레스 치환부, 703: 레코드 삭제 처리부, 801: 송신 패킷 판정부, 802: ARP 응답 처리부, 803: 동적 포트 기록 처리부, 804: 어드레스 복원부, 901: 송신 패킷 판정부, 902: 어드레스 복원부, 1001: 이벤트 검출부, 1002: 소켓 조작부, 1003: 폴리시 설정부, 1004: 소켓 메모리 영역, 1005: 암호화 처리부, 1006: 복호 처리부, 2801: 단말, 2802: 서버, 2805: 서버, 2901: 단말, 2902: 서버, 2905: 가상 단말

도면

도면1



도면2


213
어드레스 테이블 갱신 카운터
TCP 포트 번호 메모리
212
210
외측 NIC 어드레스 테이블
209
내측 NIC 어드레스 테이블
211
XPTCP 정책 테이블
204
임시 IPMAC 리스트
101
108
외측 NIC
207
소켓 처리부
206
XPTCP 처리부
205
TCP/IP 프로토콜 스택
203
어드레스 변환 처리부
201
초기 설정부
104
내측 NIC
202
네트워크 설정 정보 메모리
208
XPTCP 처리 대상 마스터

도면3

209

프로토콜 종별(TCP/UDP)
송신원 MAC 어드레스
송신원 IP 어드레스
송신원 포트 번호
목적지 MAC 어드레스
목적지 IP 어드레스
목적지 포트 번호
색인용 포트 번호
타이머용 카운터 값

210

프로토콜 종별(TCP/UDP)
송신원 MAC 어드레스
송신원 IP 어드레스
송신원 포트 번호
목적지 MAC 어드레스
목적지 IP 어드레스
목적지 포트 번호
색인용 포트 번호
동적 포트 번호
타이머용 카운터 값

211

프로토콜 종별(TCP/UDP)
색인용 포트 번호
레코드 번호

202

내측 NICMAC 어드레스
내측 NICIP 어드레스
외측 NICMAC 어드레스
외측 NICIP 어드레스

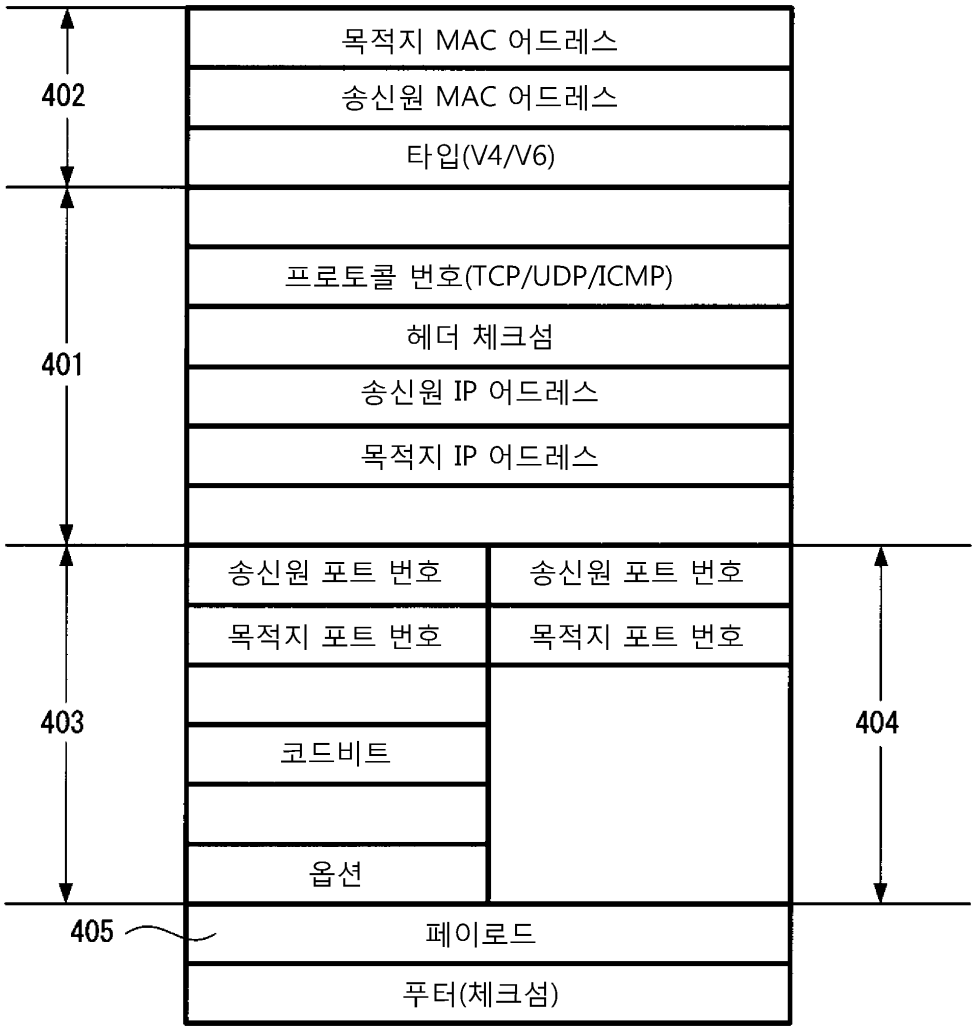
204

내측 NICIP 어드레스
제1 임시 MAC 어드레스
제1 임시 IP 어드레스
외측 NICIP 어드레스
제2 임시 MAC 어드레스
제2 임시 IP 어드레스

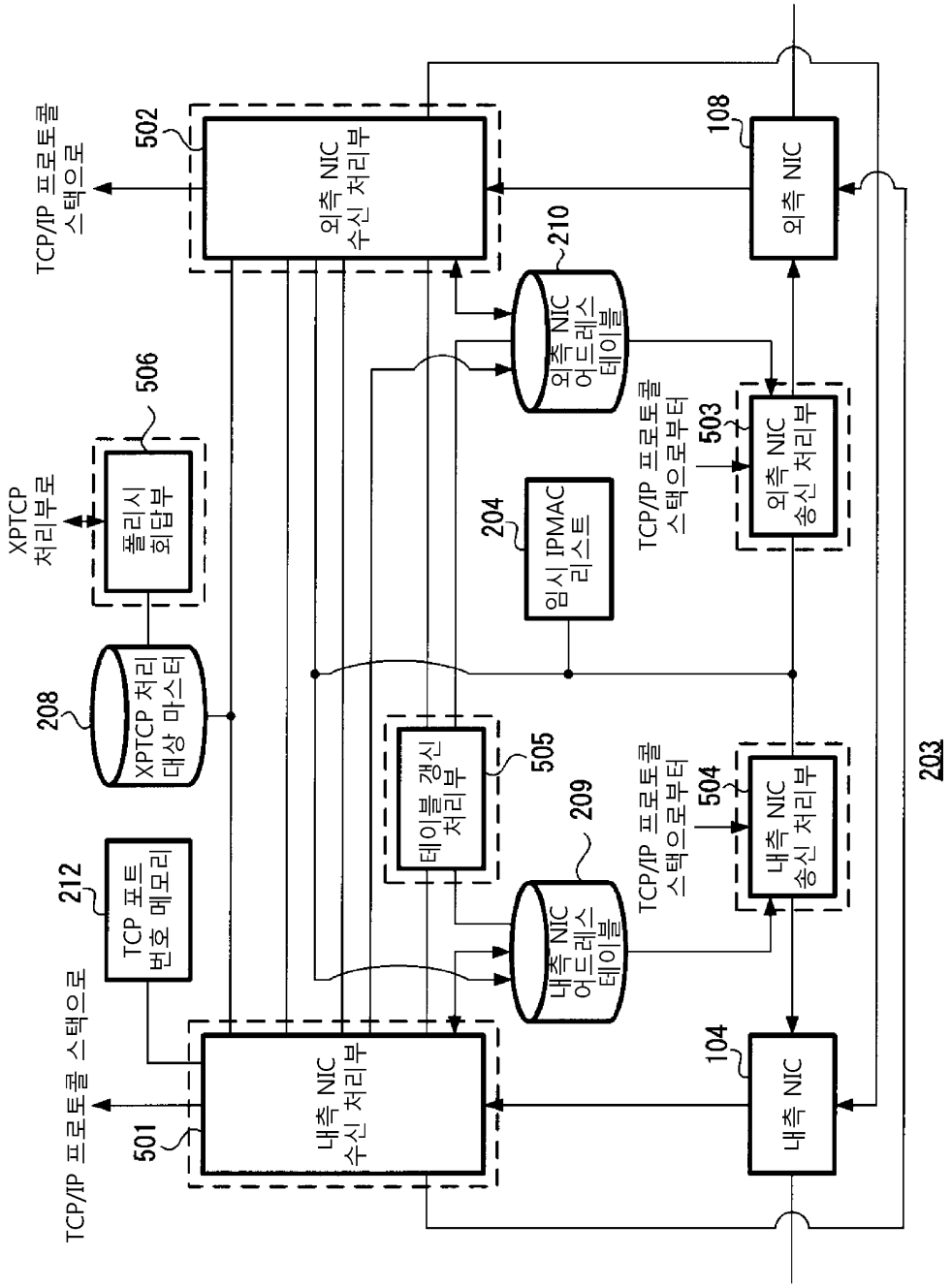
208

레코드 번호
프로토콜 종별(TCP/UDP)
송신원 IP 어드레스
송신원 포트 번호
목적지 IP 어드레스
목적지 포트 번호
암호 종별 타

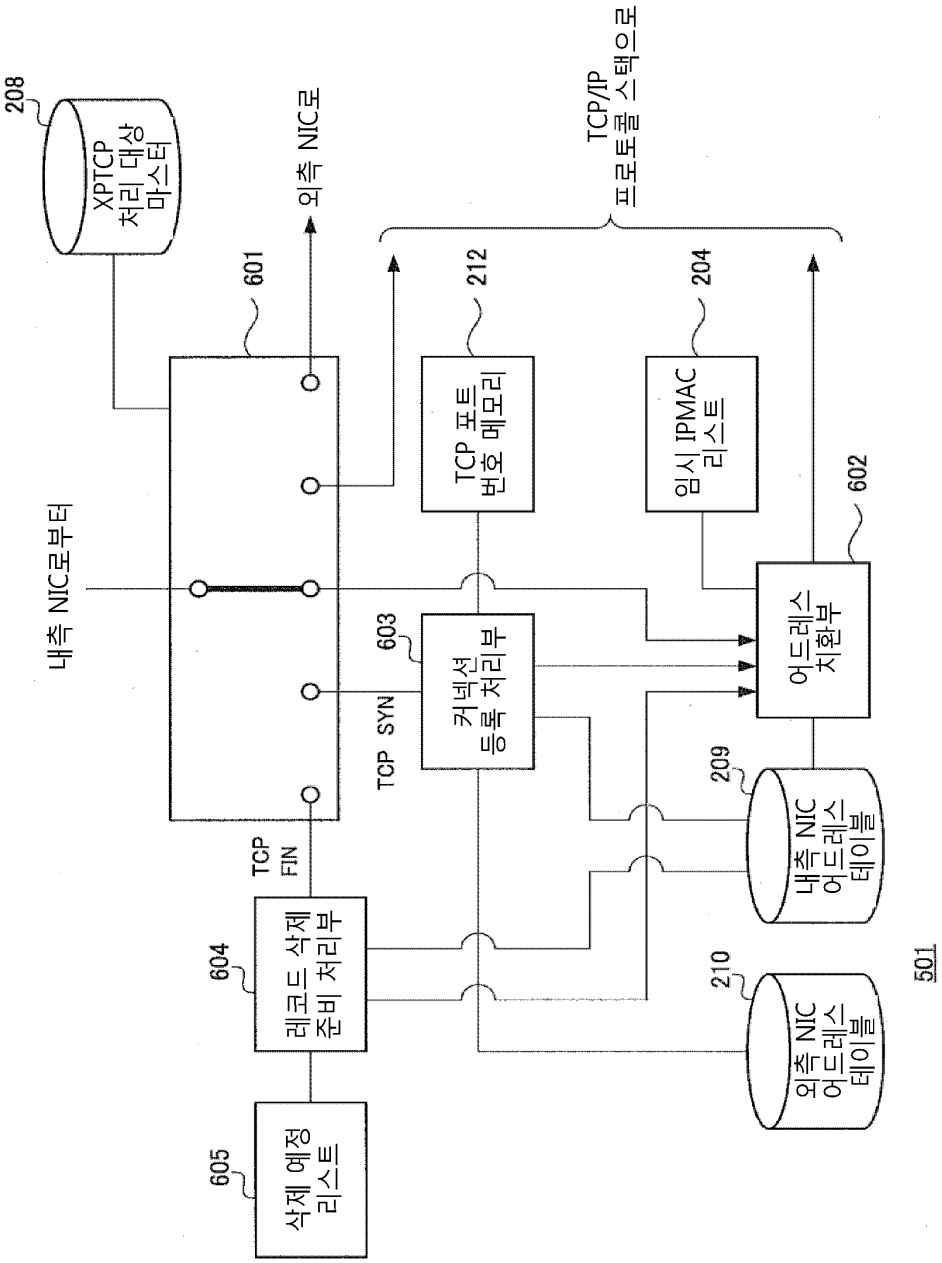
도면4


402
401
403
404
405
목적지 MAC 어드레스
송신원 MAC 어드레스
타입(V4/V6)
프로토콜 번호(TCP/UDP/ICMP)
헤더 체크섬
송신원 IP 어드레스
목적지 IP 어드레스
송신원 포트 번호
송신원 포트 번호
목적지 포트 번호
목적지 포트 번호
코드비트
옵션
페이로드
푸터(체크섬)

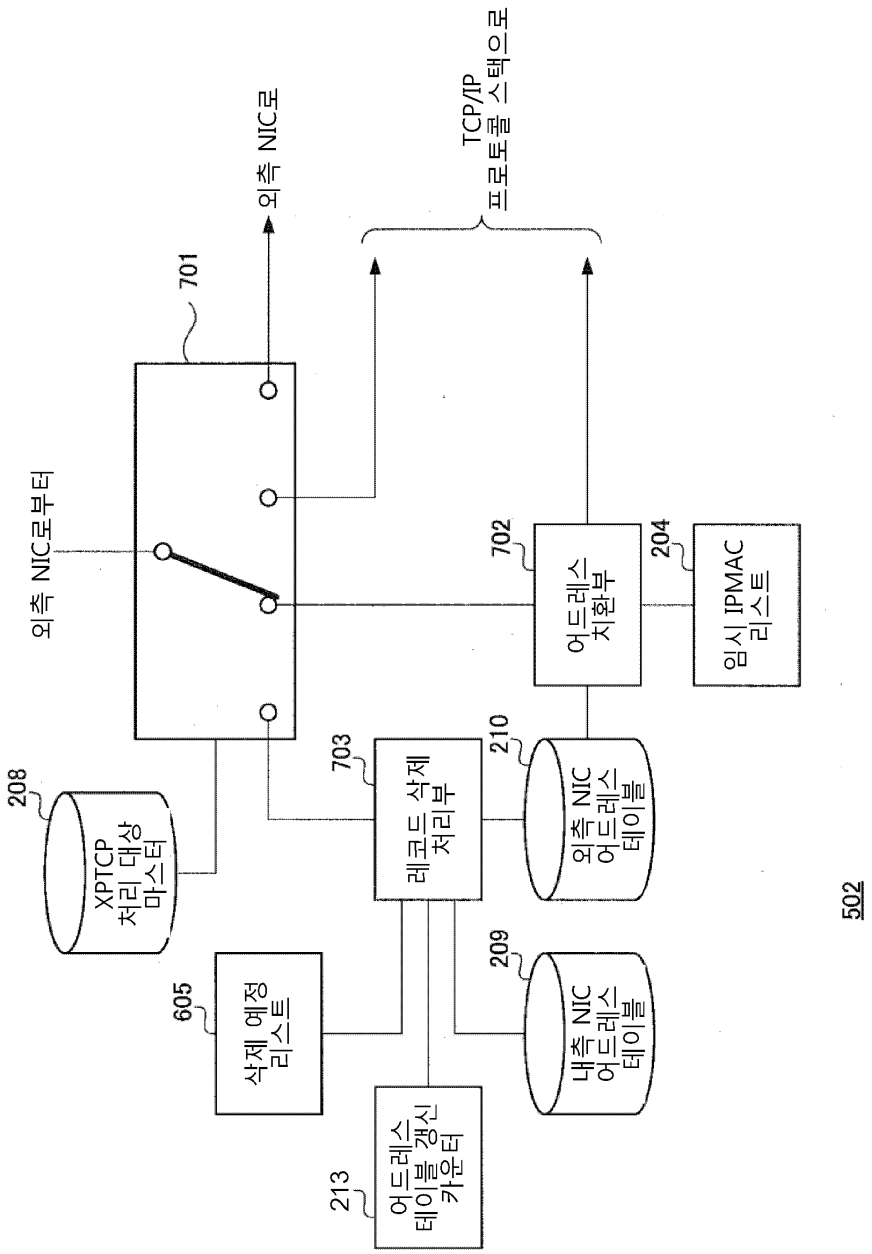
도면5


TCP/IP 프로토콜 스택으로
502
외측 NIC 수신 처리부
108
외측 NIC
210
외측 NIC 어드레스 테이블
506
폴리시 회답부
XPTCP 처리부로
204
임시 IPMAC 리스트
TCP/IP 프로토콜 스택으로부터
503
외측 NIC 송신 처리부
208
XPTCP 처리 대상 마스터
505
테이블 갱신 처리부
209
내측 NIC 어드레스 테이블
504
내측 NIC 송신 처리부
203
212
TCP 포트 번호 메모리
104
내측 NIC
TCP/IP 프로토콜 스택으로
501
내측 NIC 수신 처리부

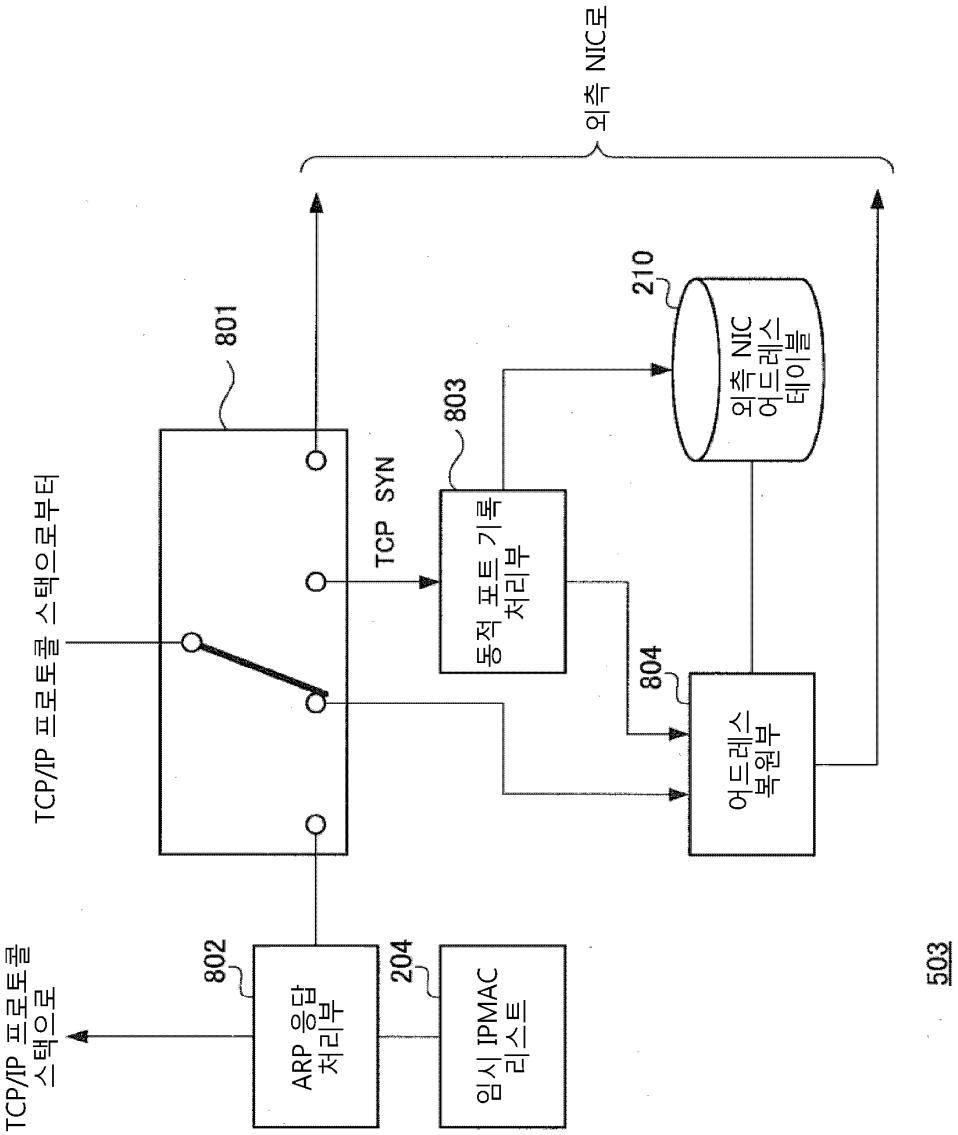
도면6


208
XPTCP 처리 대상 마스터
외측 NIC로
TCP/IP 프로토콜 스택으로
601
212
204
602
내측 NIC로부터
TCP 포트 번호 메모리
임시 IPMAC 리스트
603
TCP SYN
커넥션 등록 처리부
어드레스 치환부
209
내측 NIC 어드레스 테이블
TCP FIN
604
레코드 삭제 준비 처리부
210
외측 NIC 어드레스 테이블
501
605
삭제 예정 리스트

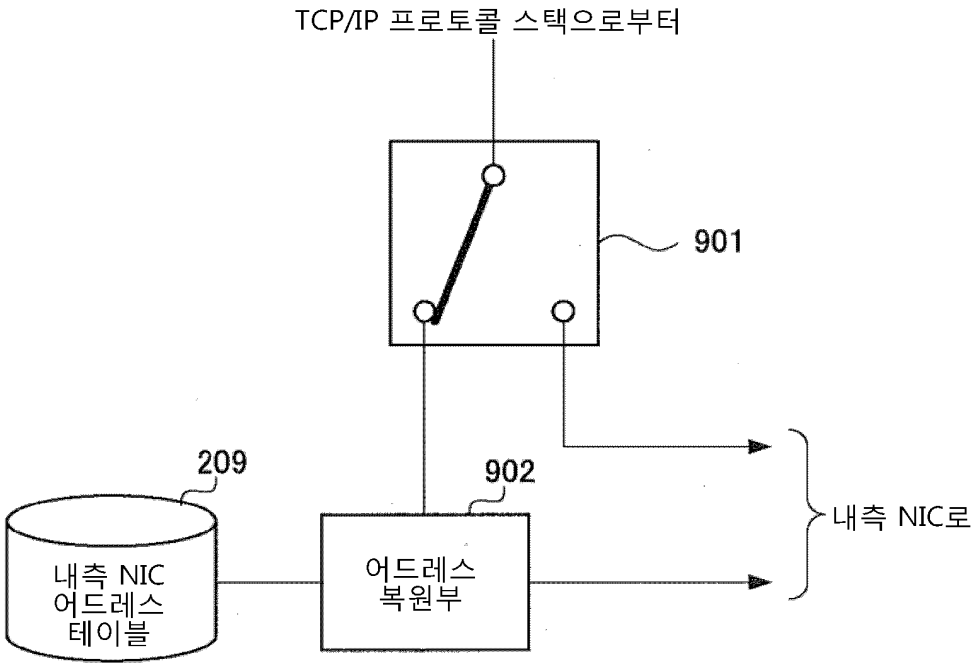
도면7


외측 NIC로부터
701
외측 NIC로
TCP/IP
프로토콜 스택으로
702
어드레스
처환부
204
임시 IPMAC
리스트
208
XPTCP
처리 대상
마스터
703
레코드 삭제
처리부
210
외측 NIC
어드레스
테이블
605
삭제 예정
리스트
209
내측 NIC
어드레스
테이블
213
어드레스
테이블갱신
카운터
502

도면8

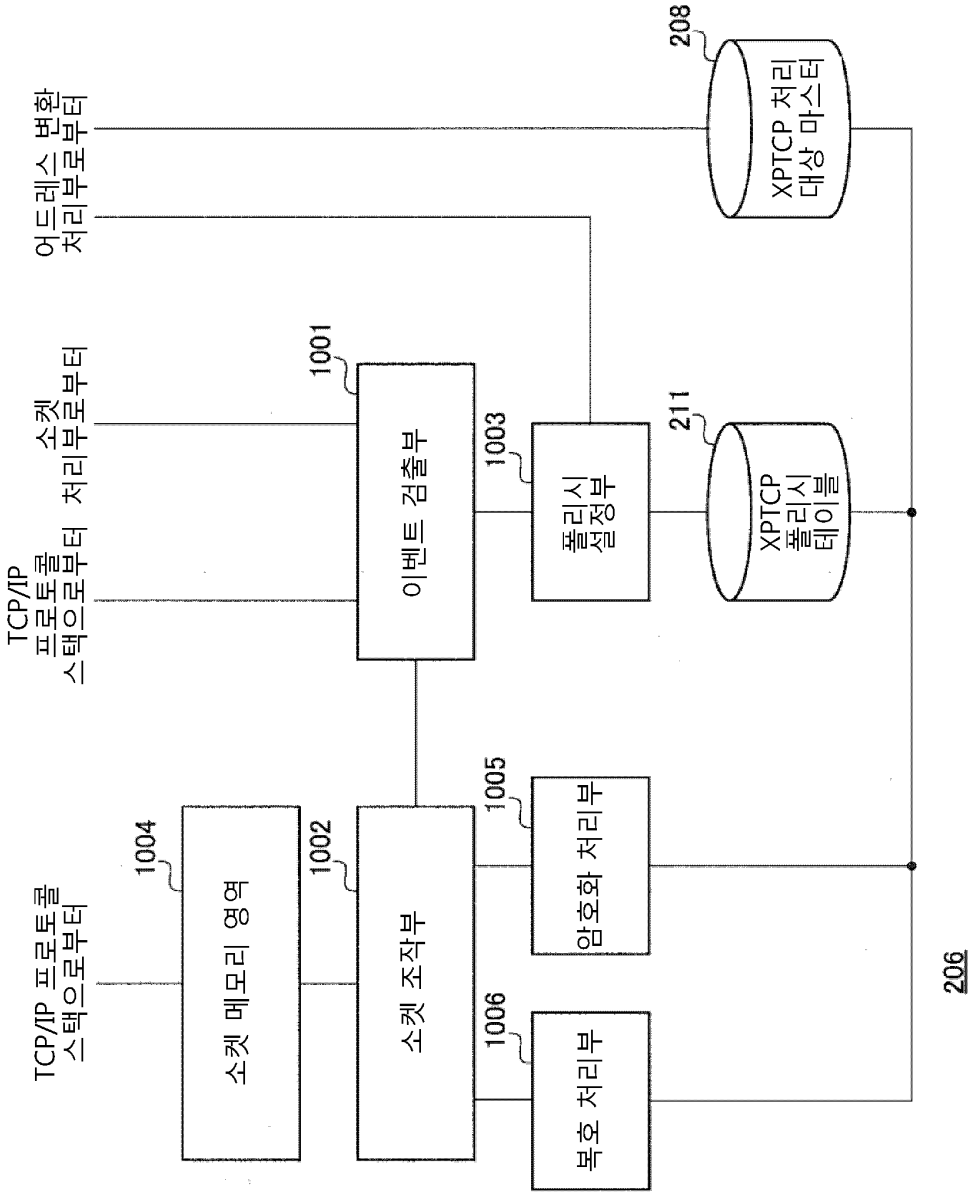

외측 NIC로
210
외측 NIC
어드레스
테이블
801
803
TCP SYN
동적 포트 기록
처리부
804
어드레스
복원부
TCP/IP 프로토콜 스택으로부터
802
ARP 응답
처리부
204
임시 IPMAC
리스트
TCP/IP 프로토콜
스택으로
503

도면9

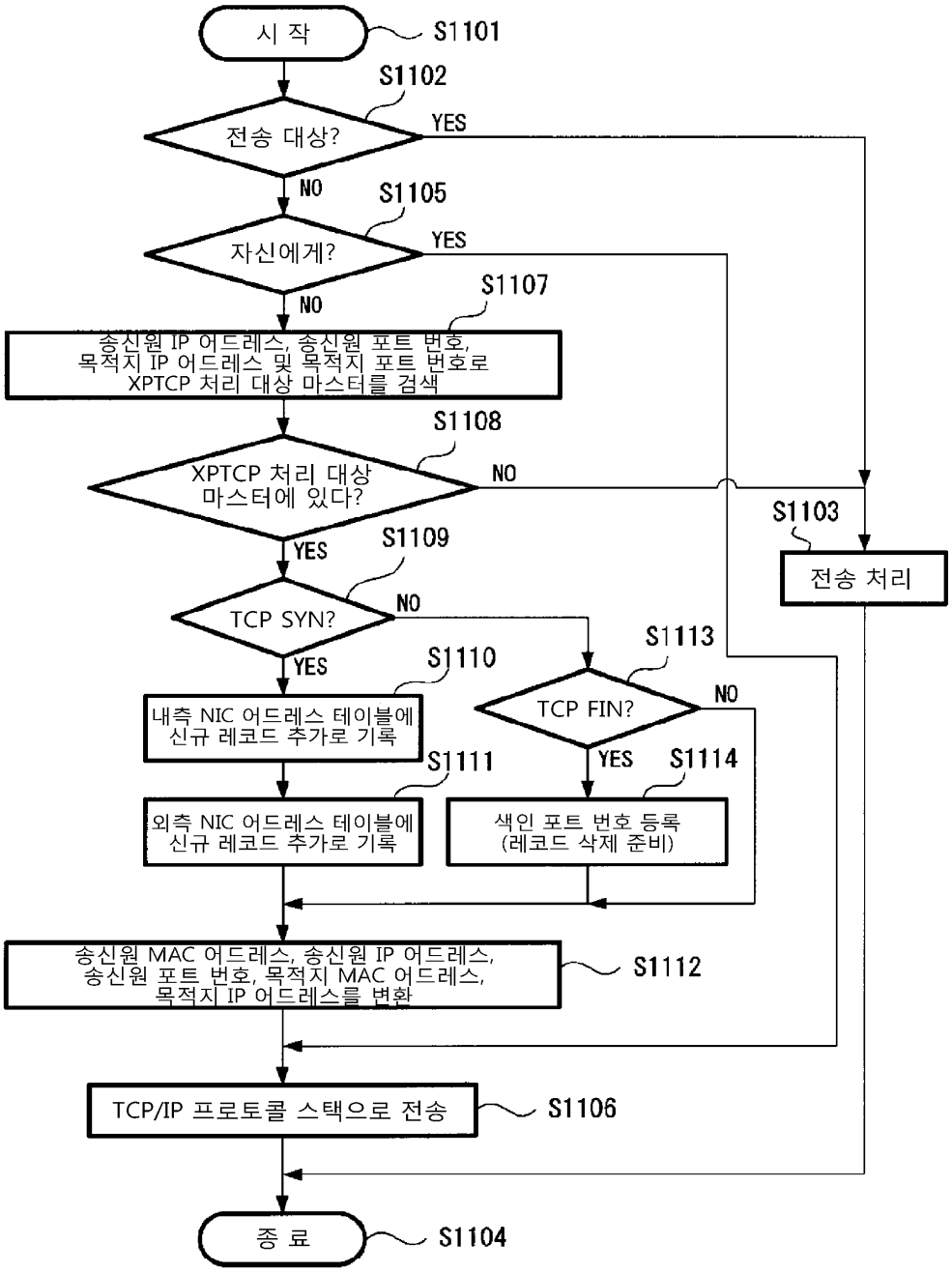


504

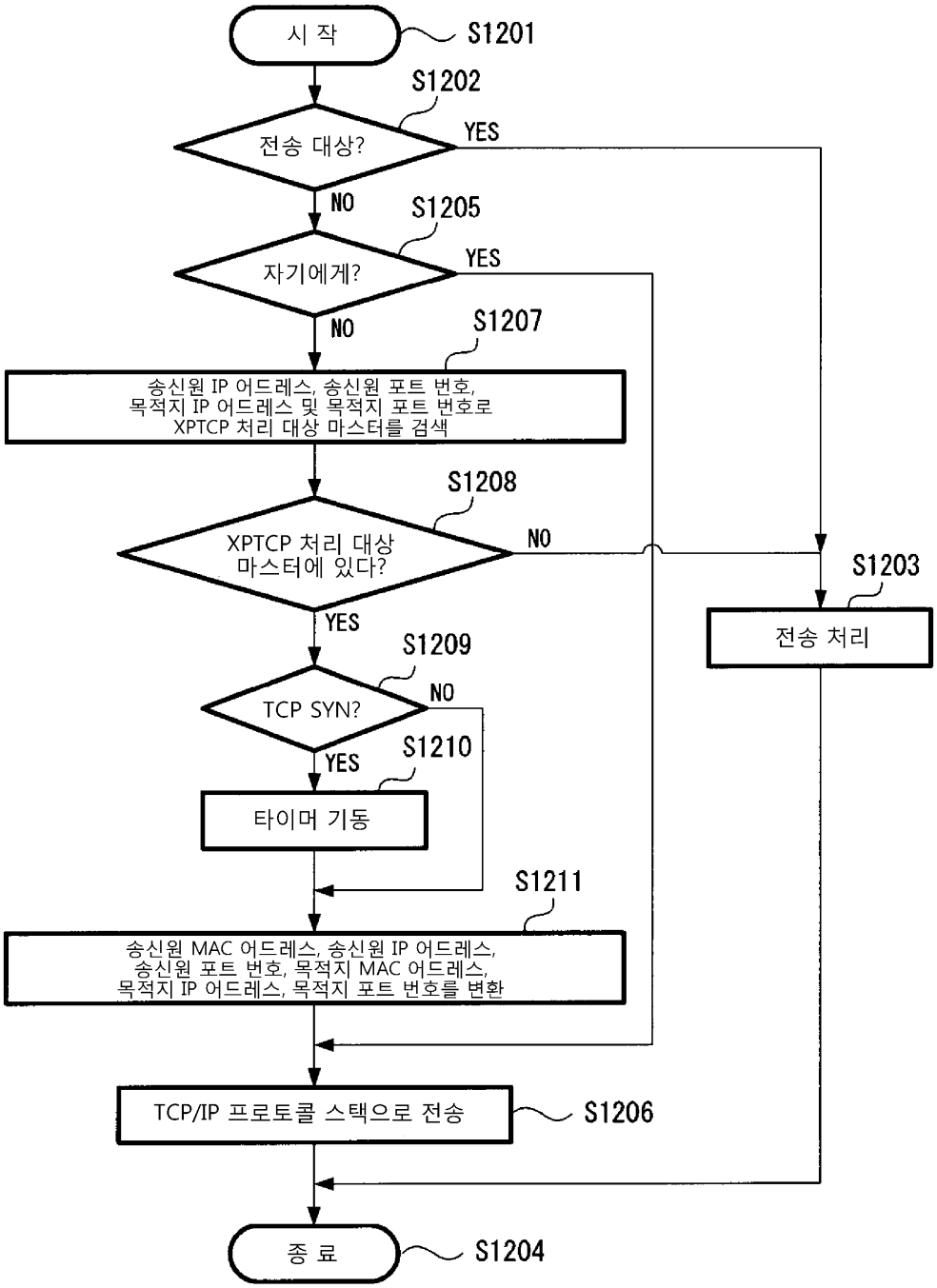
도면10


208
XPTCP 처리 대상 마스터
어드레스 변환 처리부로부터
1001
소켓 처리부로부터
이벤트 검출부
1003
폴리시 설정부
211
XPTCP 폴리시 테이블
TCP/IP 프로토콜 스택으로부터
1004
소켓 메모리 영역
1002
소켓 조작부
1005
암호화 처리부
1006
복호 처리부
TCP/IP 프로토콜 스택으로부터
206

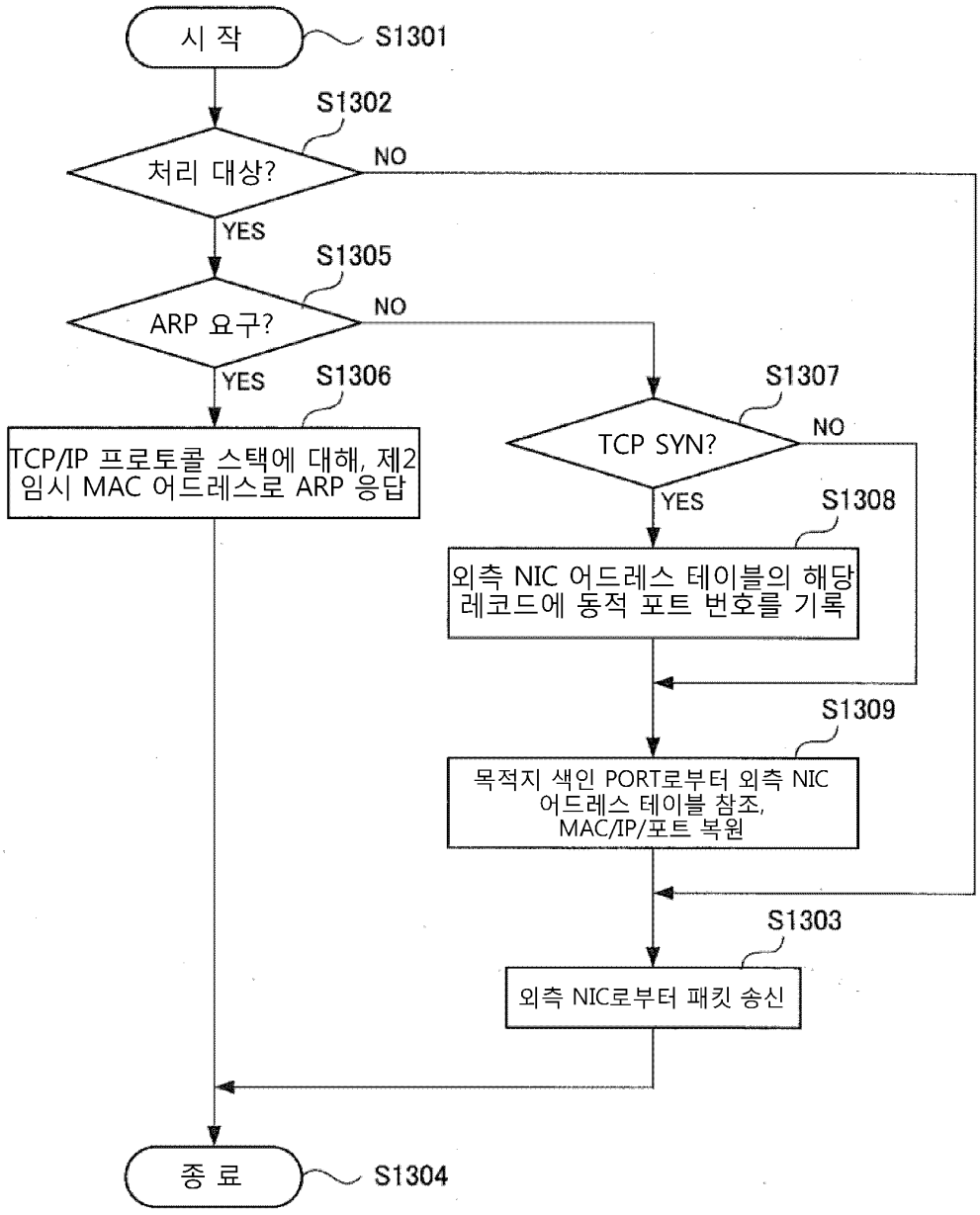
도면11


시 작
S1101
S1102
전송 대상?
YES
NO
S1105
자신에게?
YES
NO
S1107
송신원 IP 어드레스, 송신원 포트 번호,
목적지 IP 어드레스 및 목적지 포트 번호로
XPTCP 처리 대상 마스터를 검색
S1108
XPTCP 처리 대상
마스터에 있다?
NO
YES
S1109
TCP SYN?
NO
YES
S1110
내측 NIC 어드레스 테이블에
신규 레코드 추가로 기록
S1111
외측 NIC 어드레스 테이블에
신규 레코드 추가로 기록
S1113
TCP FIN?
NO
YES
S1114
색인 포트 번호 등록
(레코드 삭제 준비)
S1103
전송 처리
송신원 MAC 어드레스, 송신원 IP 어드레스,
송신원 포트 번호, 목적지 MAC 어드레스,
목적지 IP 어드레스를 변환
S1112
TCP/IP 프로토콜 스택으로 전송
S1106
종 료
S1104

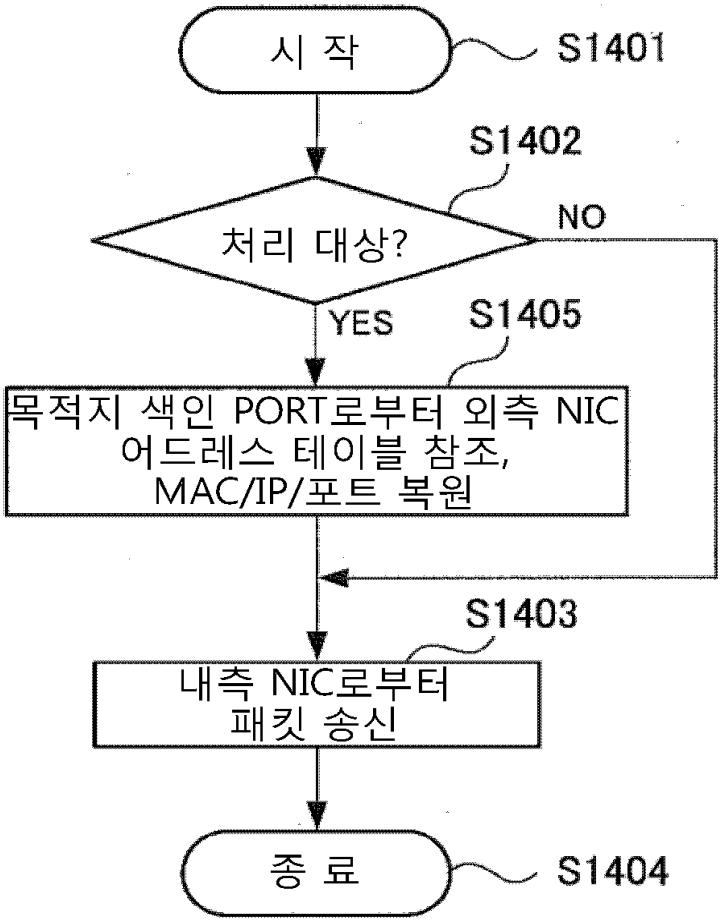
도면12


시 작
S1201
S1202
전송 대상?
YES
NO
S1205
자기에게?
YES
NO
S1207
송신원 IP 어드레스, 송신원 포트 번호,
목적지 IP 어드레스 및 목적지 포트 번호로
XPTCP 처리 대상 마스터를 검색
S1208
XPTCP 처리 대상
마스터에 있다?
NO
YES
S1203
전송 처리
S1209
TCP SYN?
NO
YES
S1210
타이머 기동
S1211
송신원 MAC 어드레스, 송신원 IP 어드레스,
송신원 포트 번호, 목적지 MAC 어드레스,
목적지 IP 어드레스, 목적지 포트 번호를 변환
TCP/IP 프로토콜 스택으로 전송
S1206
종 료
S1204

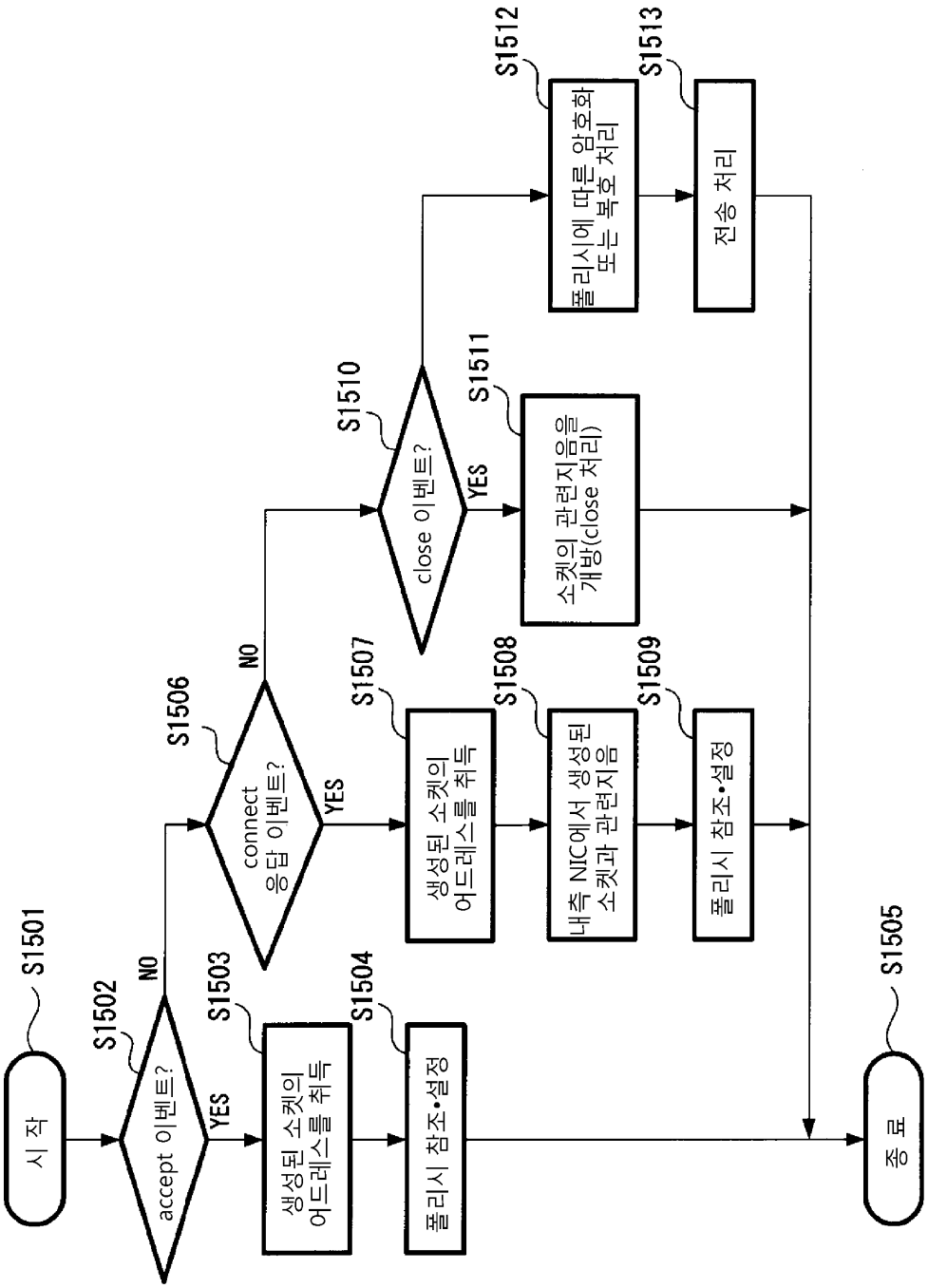
도면13


시 작
S1301
S1302
처리 대상?
NO
YES
S1305
ARP 요구?
NO
YES
S1306
TCP/IP 프로토콜 스택에 대해, 제2 임시 MAC 어드레스로 ARP 응답
S1307
TCP SYN?
NO
YES
S1308
외측 NIC 어드레스 테이블의 해당 레코드에 동적 포트 번호를 기록
S1309
목적지 색인 PORT로부터 외측 NIC 어드레스 테이블 참조, MAC/IP/포트 복원
S1303
외측 NIC로부터 패킷 송신
종 료
S1304

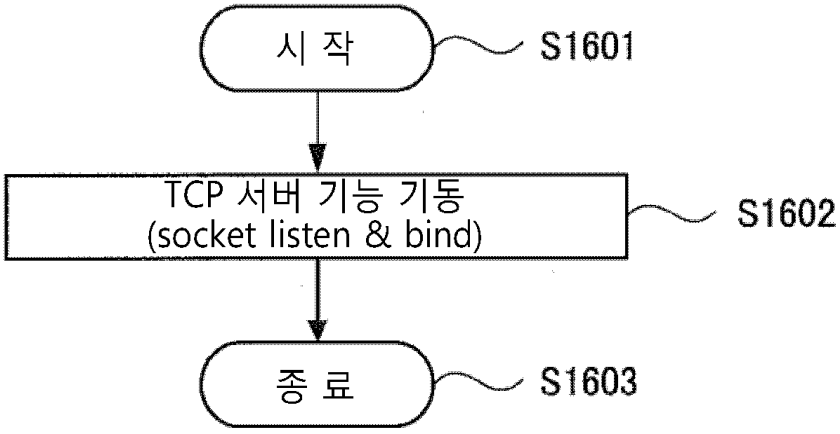
도면14


시 작
S1401
S1402
처리 대상?
NO
YES
S1405
목적지 색인 PORT로부터 외측 NIC 어드레스 테이블 참조, MAC/IP/포트 복원
S1403
내측 NIC로부터 패킷 송신
종 료
S1404

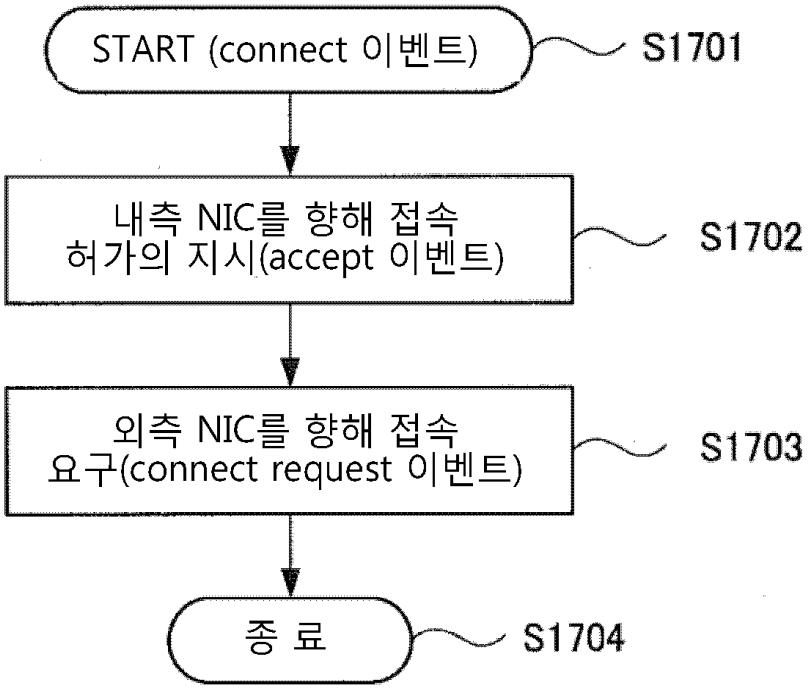
도면15


S1501
시 작
S1502
accept 이벤트?
NO
YES
S1503
생성된 소켓의 어드레스를 취득
S1504
폴리시 참조•설정
S1505
종 료
S1506
connect 응답 이벤트?
NO
YES
S1507
생성된 소켓의 어드레스를 취득
S1508
내측 NIC에서 생성된 소켓과 관련지음
S1509
폴리시 참조•설정
S1510
close 이벤트?
YES
S1511
소켓의 관련지음을 개방(close 처리)
S1512
폴리시에 따른 암호화 또는 복호 처리
S1513
전송 처리

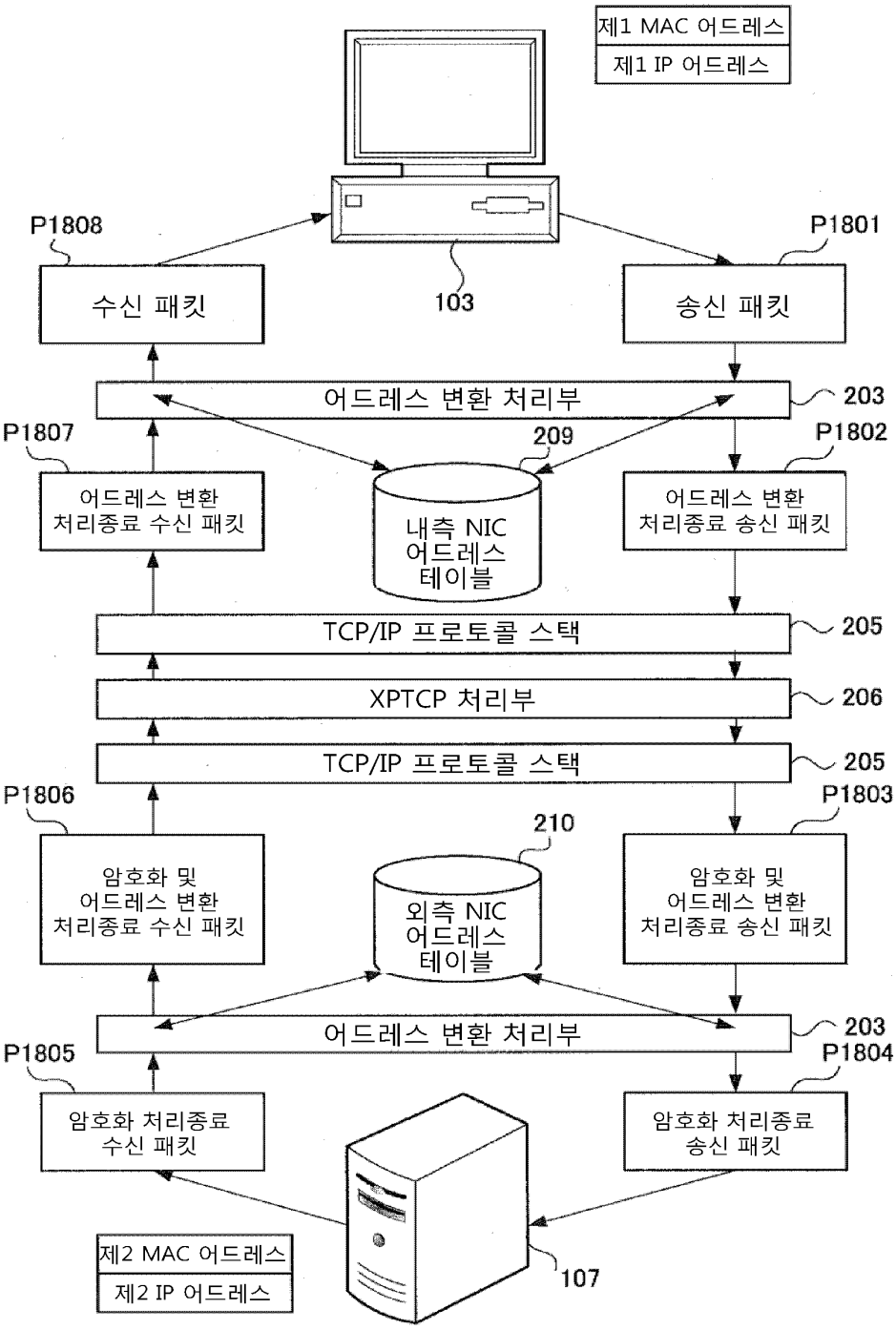
도면16


시 작
S1601
TCP 서버 기능 기동
(socket listen & bind)
S1602
종 료
S1603

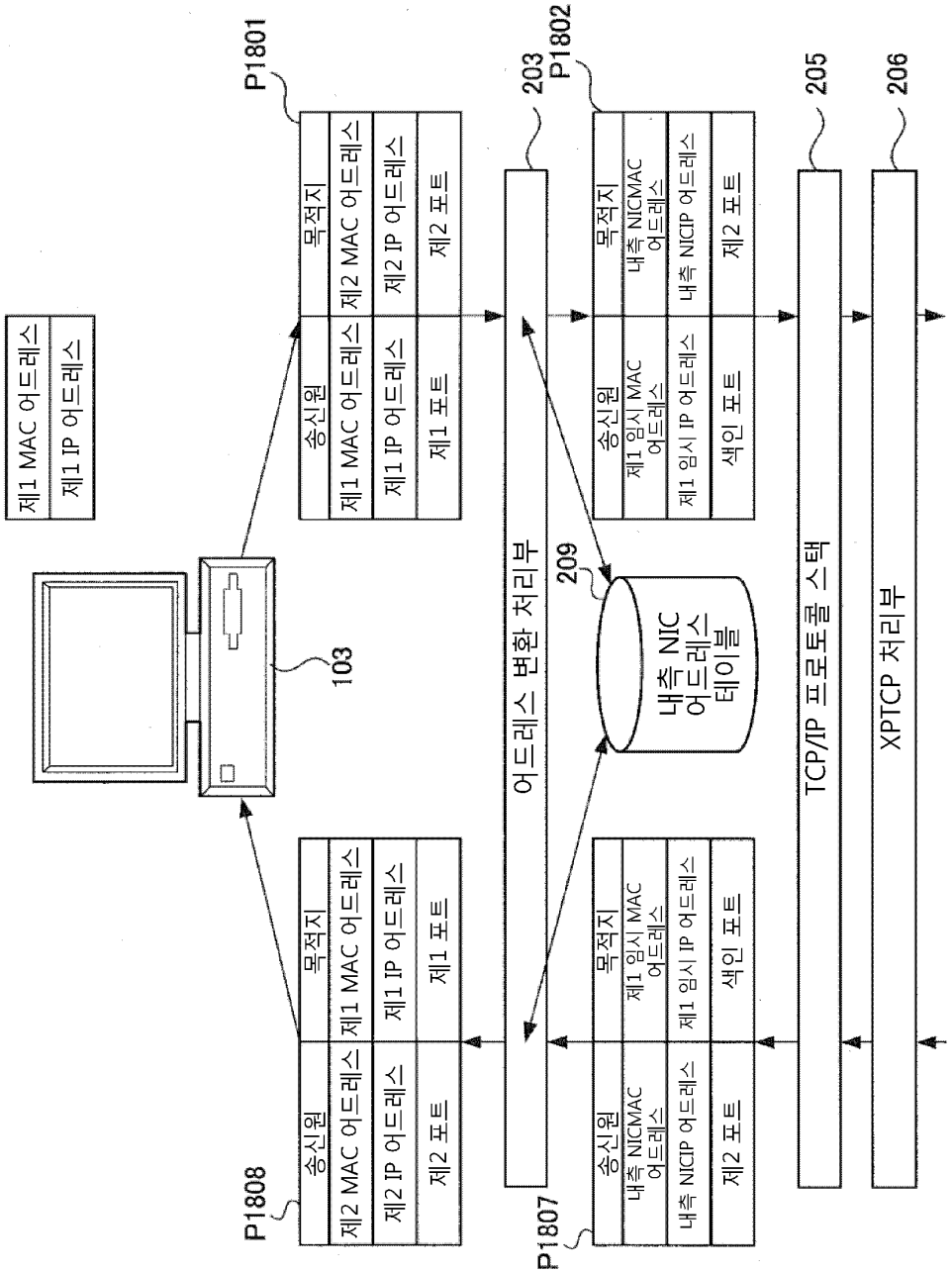
도면17


START (connect 이벤트)
S1701
내측 NIC를 향해 접속
허가의 지시(accept 이벤트)
S1702
외측 NIC를 향해 접속
요구(connect request 이벤트)
S1703
종 료
S1704

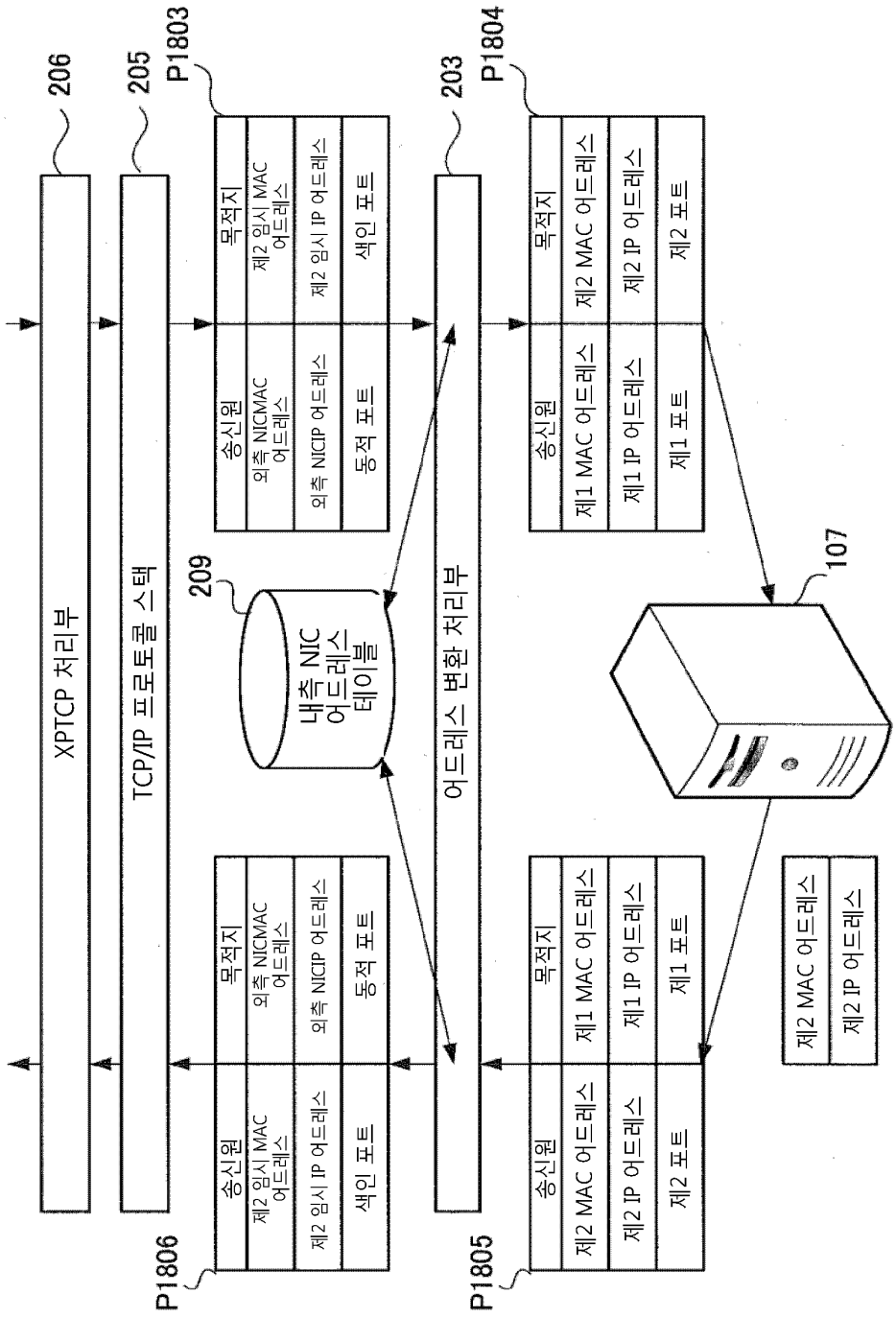
도면18


제1 MAC 어드레스
제1 IP 어드레스
103
P1808
수신 패킷
P1801
송신 패킷
어드레스 변환 처리부
203
P1807
어드레스 변환
처리종료 수신 패킷
209
내측 NIC
어드레스
테이블
P1802
어드레스 변환
처리종료 송신 패킷
TCP/IP 프로토콜 스택
205
XPTCP 처리부
206
TCP/IP 프로토콜 스택
205
P1806
암호화 및
어드레스 변환
처리종료 수신 패킷
210
외측 NIC
어드레스
테이블
P1803
암호화 및
어드레스 변환
처리종료 송신 패킷
어드레스 변환 처리부
203
P1805
암호화 처리종료
수신 패킷
P1804
암호화 처리종료
송신 패킷
제2 MAC 어드레스
제2 IP 어드레스
107

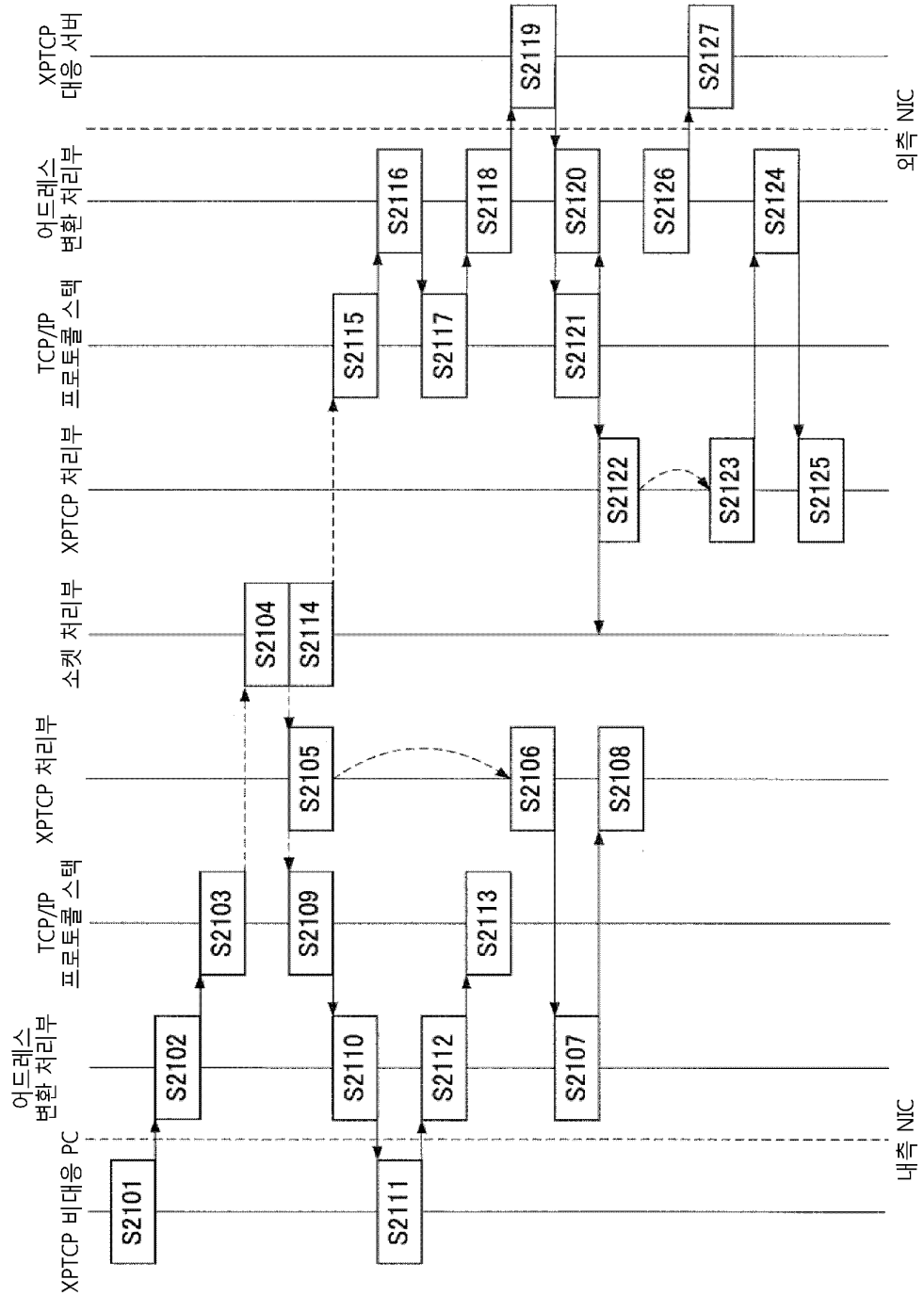
도면19


제1 MAC 어드레스
제1 IP 어드레스
103
P1801
송신원
목적지
제1 MAC 어드레스
제2 MAC 어드레스
제1 IP 어드레스
제2 IP 어드레스
제1 포트
제2 포트
P1808
송신원
목적지
제2 MAC 어드레스
제1 MAC 어드레스
제2 IP 어드레스
제1 IP 어드레스
제2 포트
제1 포트
203
어드레스 변환 처리부
P1807
송신원
목적지
내측 NICMAC 어드레스
제1 임시 MAC 어드레스
내측 NICIP 어드레스
제1 임시 IP 어드레스
제2 포트
색인 포트
209
내측 NIC 어드레스 테이블
P1802
송신원
목적지
제1 임시 MAC 어드레스
내측 NICMAC 어드레스
제1 임시 IP 어드레스
내측 NICIP 어드레스
색인 포트
제2 포트
205
TCP/IP 프로토콜 스택
206
XPTCP 처리부

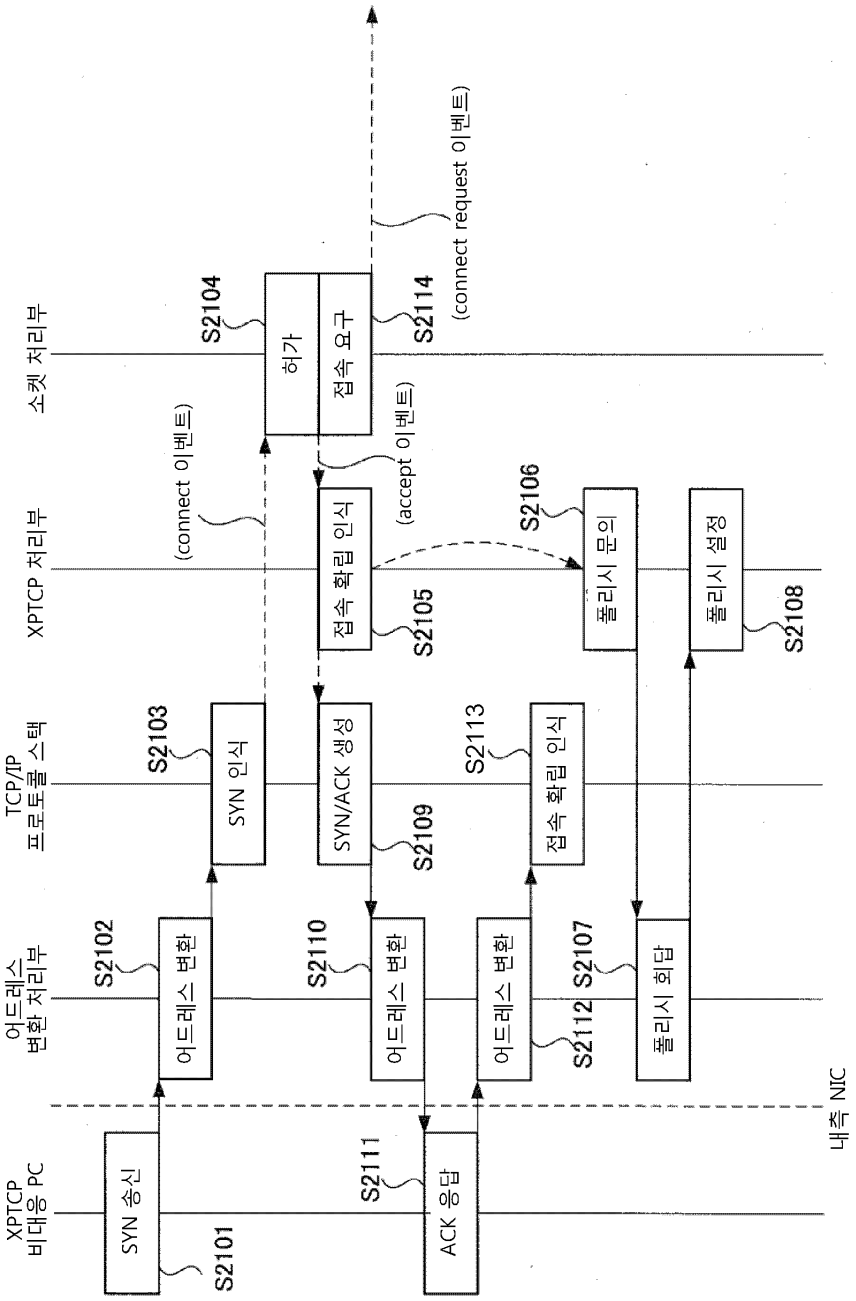
도면20


206
205
P1803
203
P1804
XPTCP 처리부
TCP/IP 프로토콜 스택
어드레스 변환 처리부
209
내측 NIC 어드레스 테이블
107
송신원
목적지
제2 임시 MAC 어드레스
외측 NICMAC 어드레스
제2 임시 IP 어드레스
외측 NICIP 어드레스
색인 포트
동적 포트
제1 MAC 어드레스
제2 MAC 어드레스
제1 IP 어드레스
제2 IP 어드레스
제1 포트
제2 포트
P1806
P1805

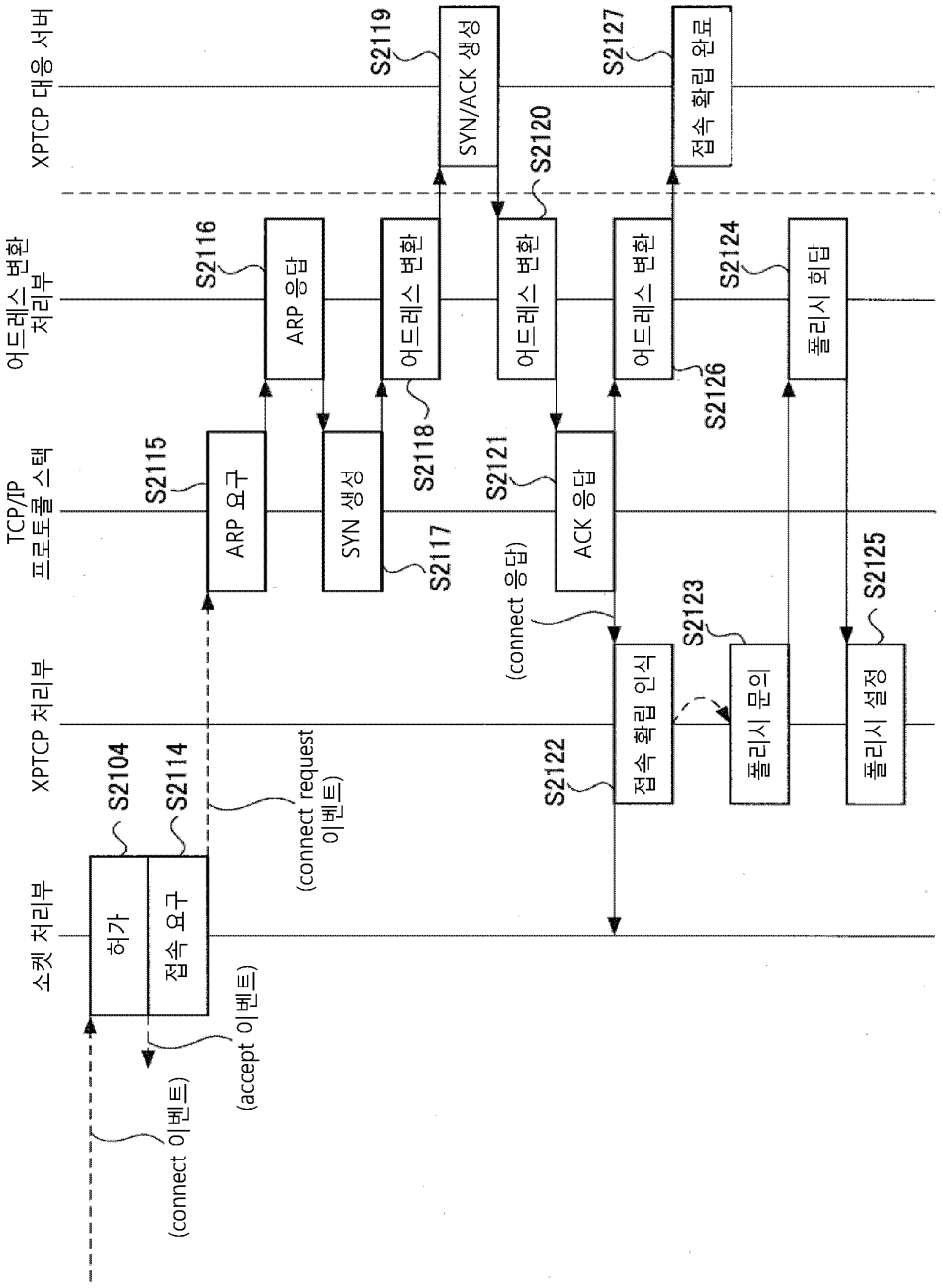
도면21


XPTCP 대응 서버
어드레스 변환 처리부
TCP/IP 프로토콜 스택
XPTCP 처리부
소켓 처리부
XPTCP 처리부
TCP/IP 프로토콜 스택
어드레스 변환 처리부
XPTCP 비대응 PC
외측 NIC
내측 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

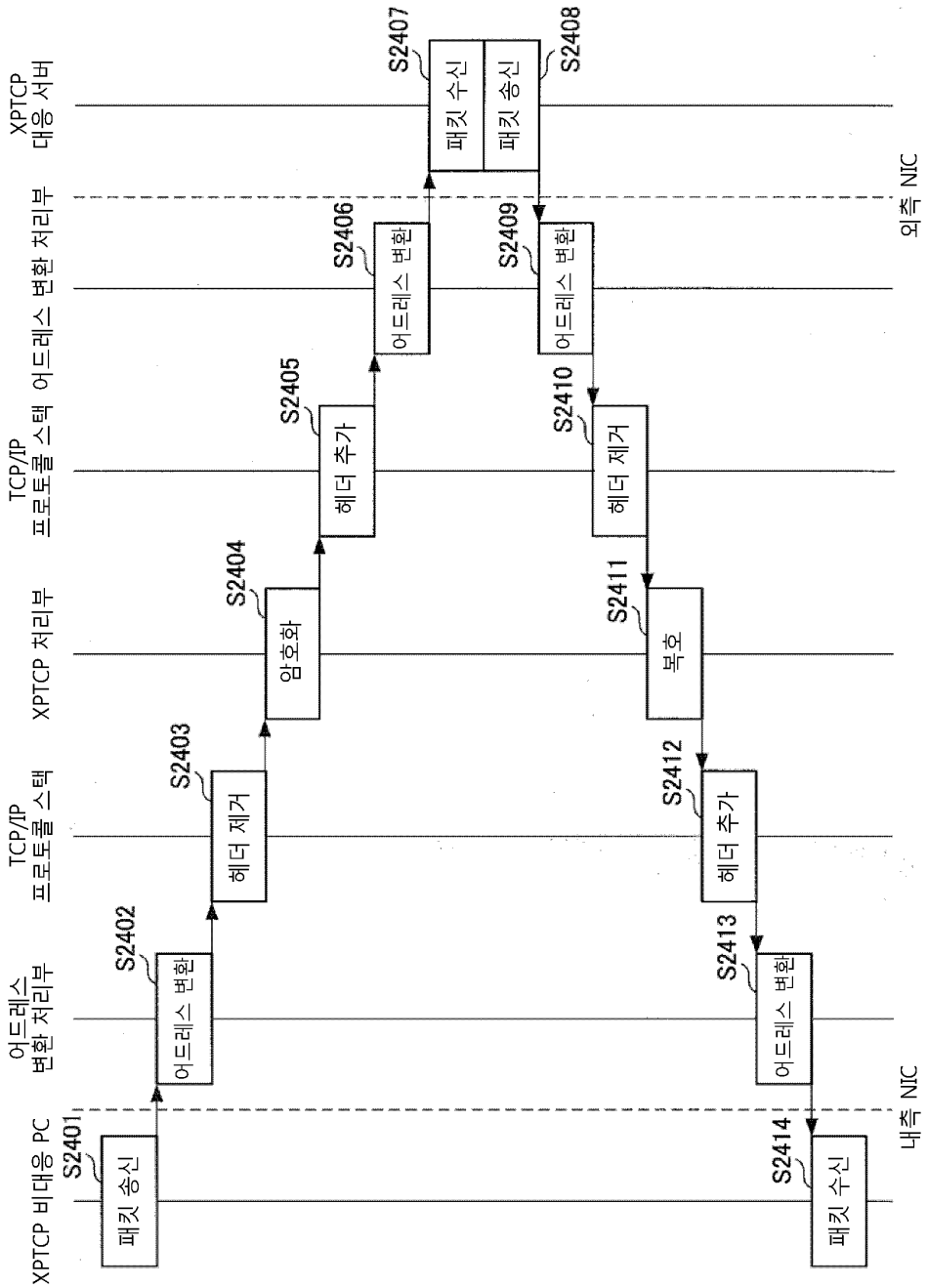
도면22


XPTCP 비대응 PC
어드레스 변환 처리부
TCP/IP 프로토콜 스택
XPTCP 처리부
소켓 처리부
내측 NIC
SYN 송신
어드레스 변환
SYN 인식
SYN/ACK 생성
접속 확립 인식
폴리시 문의
폴리시 설정
폴리시 회답
ACK 응답
허가
접속 요구
(connect request 이벤트)
(connect 이벤트)
(accept 이벤트)
S2101
S2102
S2103
S2104
S2105
S2106
S2107
S2108
S2109
S2110
S2111
S2112
S2113
S2114

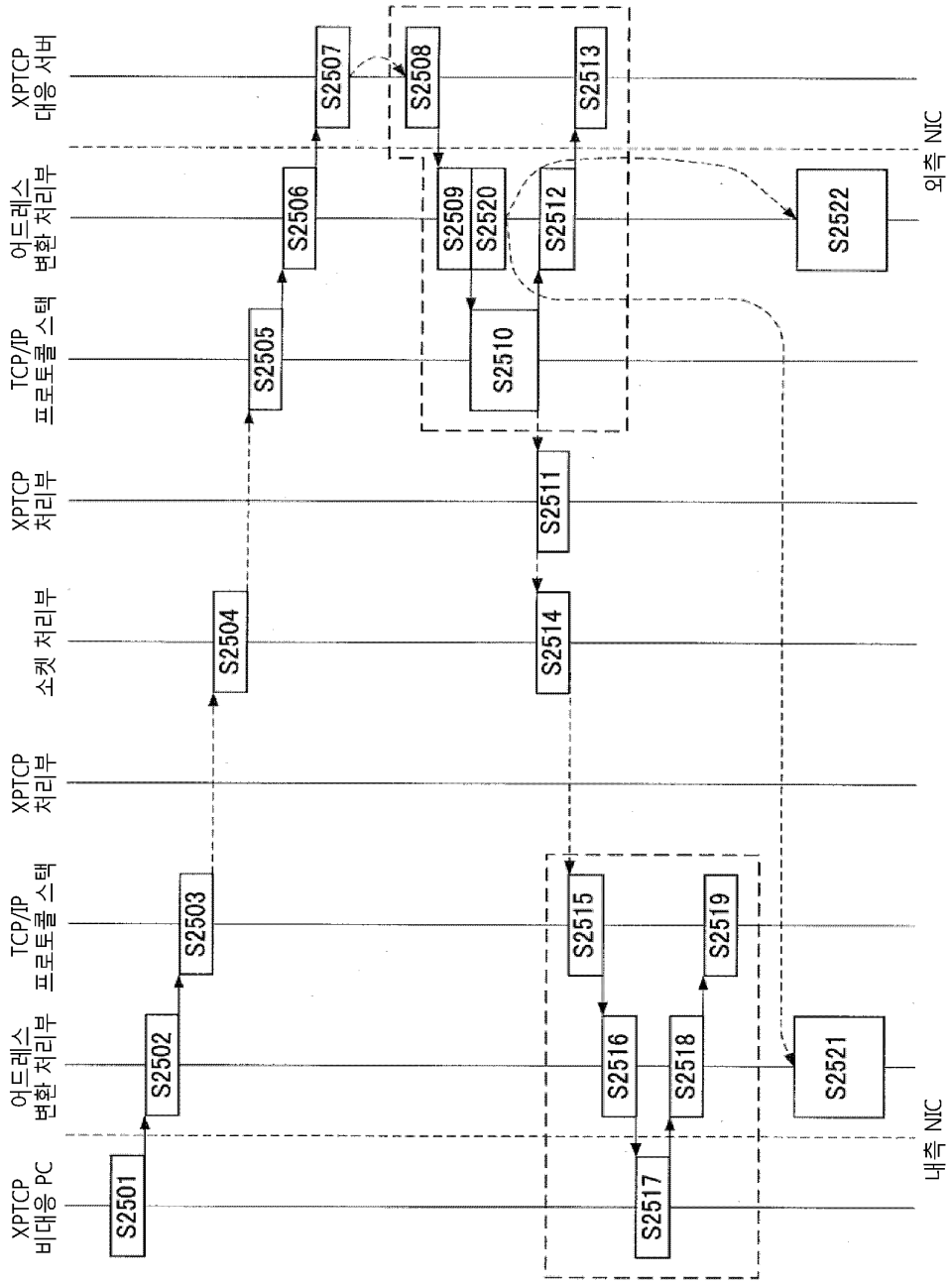
도면23


소켓 처리부
XPTCP 처리부
TCP/IP 프로토콜 스택
어드레스 변환 처리부
XPTCP 대응 서버
허가
S2104
접속 요구
S2114
(connect 이벤트)
(accept 이벤트)
(connect request 이벤트)
ARP 요구
S2115
ARP 응답
S2116
어드레스 변환
SYN 생성
S2117
어드레스 변환
S2118
SYN/ACK 생성
S2119
어드레스 변환
S2120
ACK 응답
S2121
(connect 응답)
어드레스 변환
S2126
접속 확립 완료
S2127
접속 확립 인식
S2122
폴리시 문의
S2123
폴리시 회답
S2124
폴리시 설정
S2125

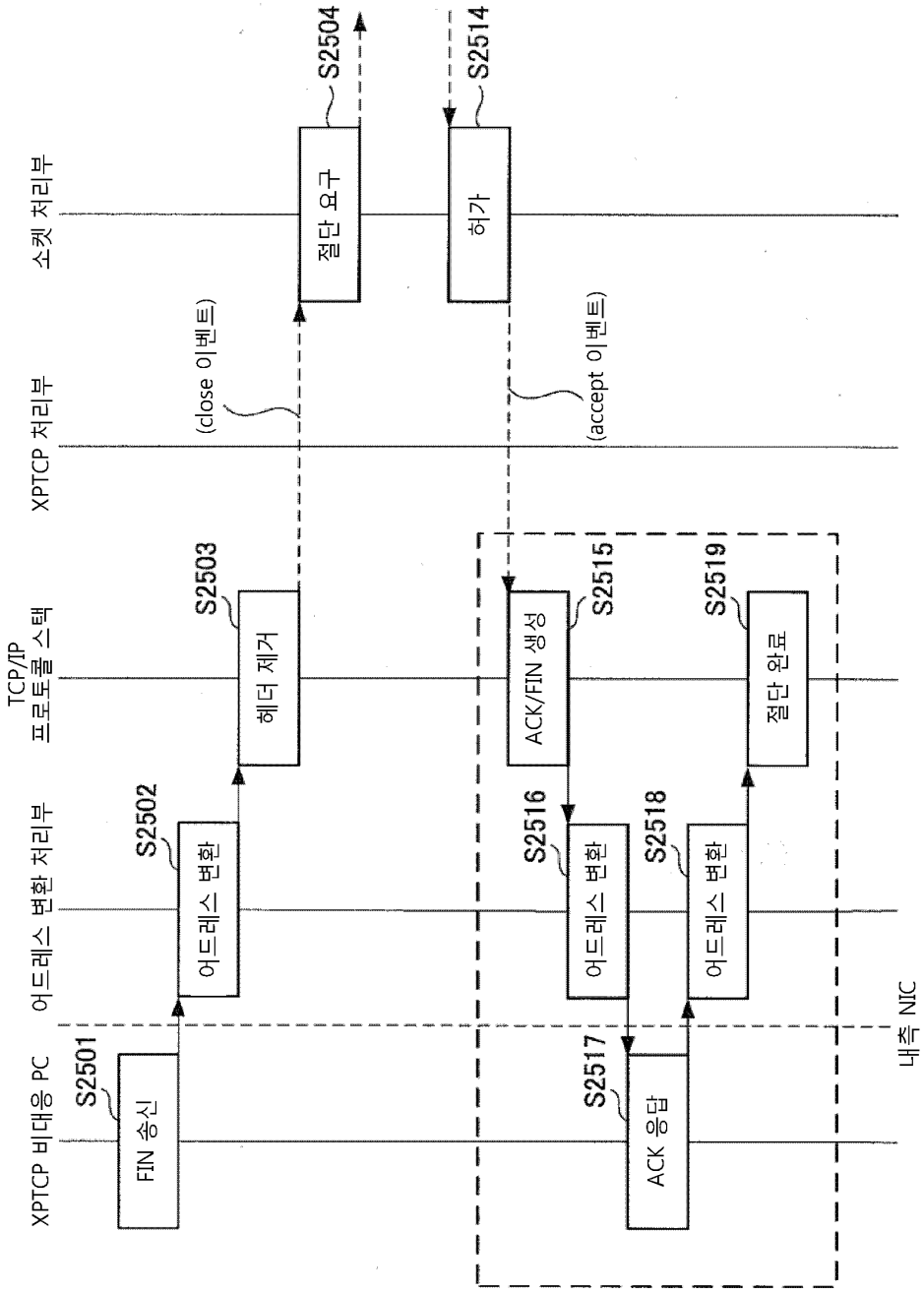
도면24


XPTCP 비대응 PC
어드레스 변환 처리부
TCP/IP 프로토콜 스택
XPTCP 처리부
TCP/IP 프로토콜 스택
어드레스 변환 처리부
XPTCP 대응 서버
내측 NIC
외측 NIC
S2401
패킷 송신
S2402
어드레스 변환
S2403
헤더 제거
S2404
암호화
S2405
헤더 추가
S2406
어드레스 변환
S2407
패킷 수신
S2408
패킷 송신
S2409
어드레스 변환
S2410
헤더 제거
S2411
복호
S2412
헤더 추가
S2413
어드레스 변환
S2414
패킷 수신

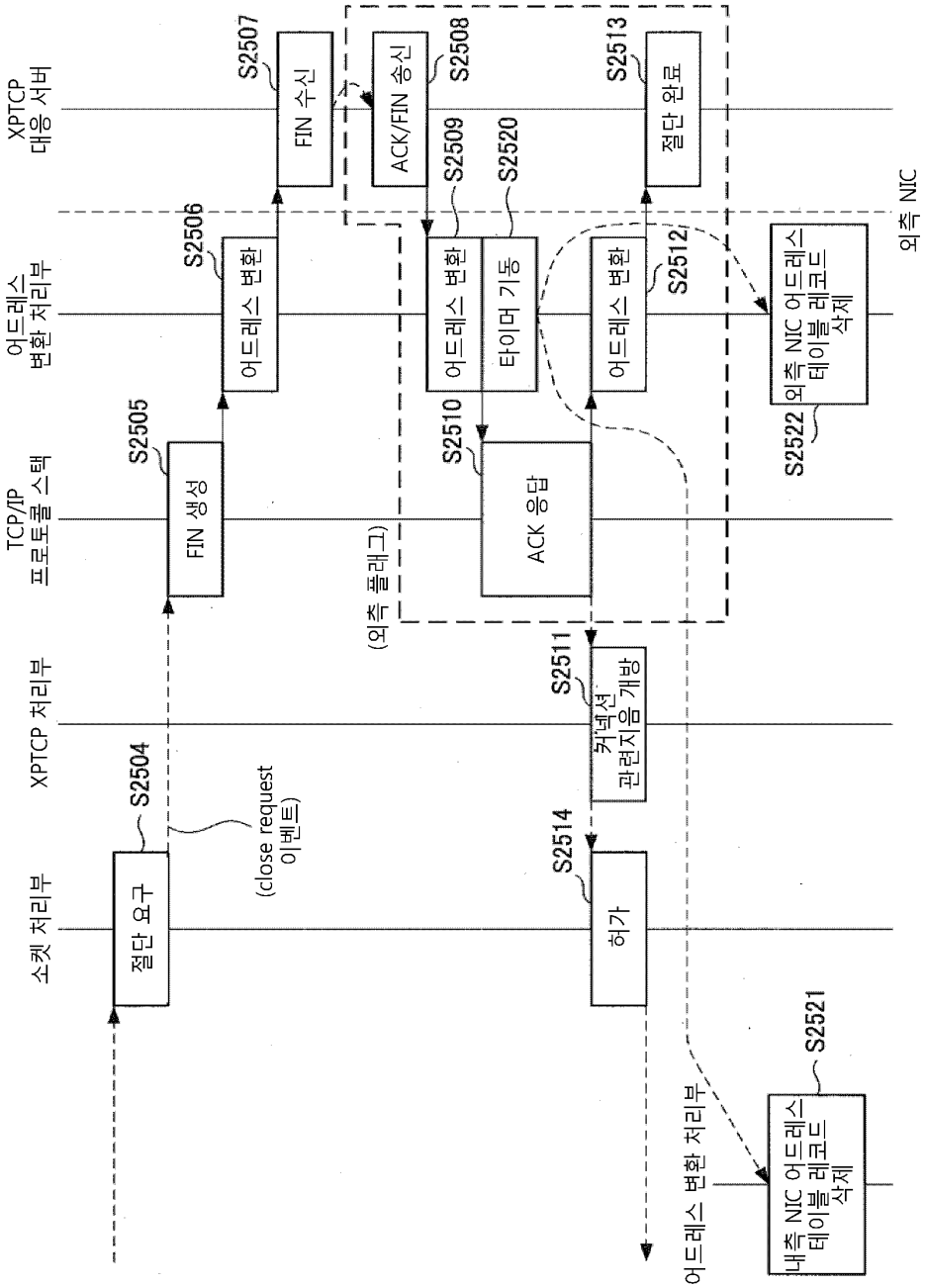
도면25


XPTCP 대응 서버
어드레스 변환 처리부
TCP/IP 프로토콜 스택
XPTCP 처리부
소켓 처리부
XPTCP 처리부
TCP/IP 프로토콜 스택
어드레스 변환 처리부
XPTCP 비대응 PC
외측 NIC
내측 NIC
S2501
S2502
S2503
S2504
S2505
S2506
S2507
S2508
S2509
S2510
S2511
S2512
S2513
S2514
S2515
S2516
S2517
S2518
S2519
S2520
S2521
S2522

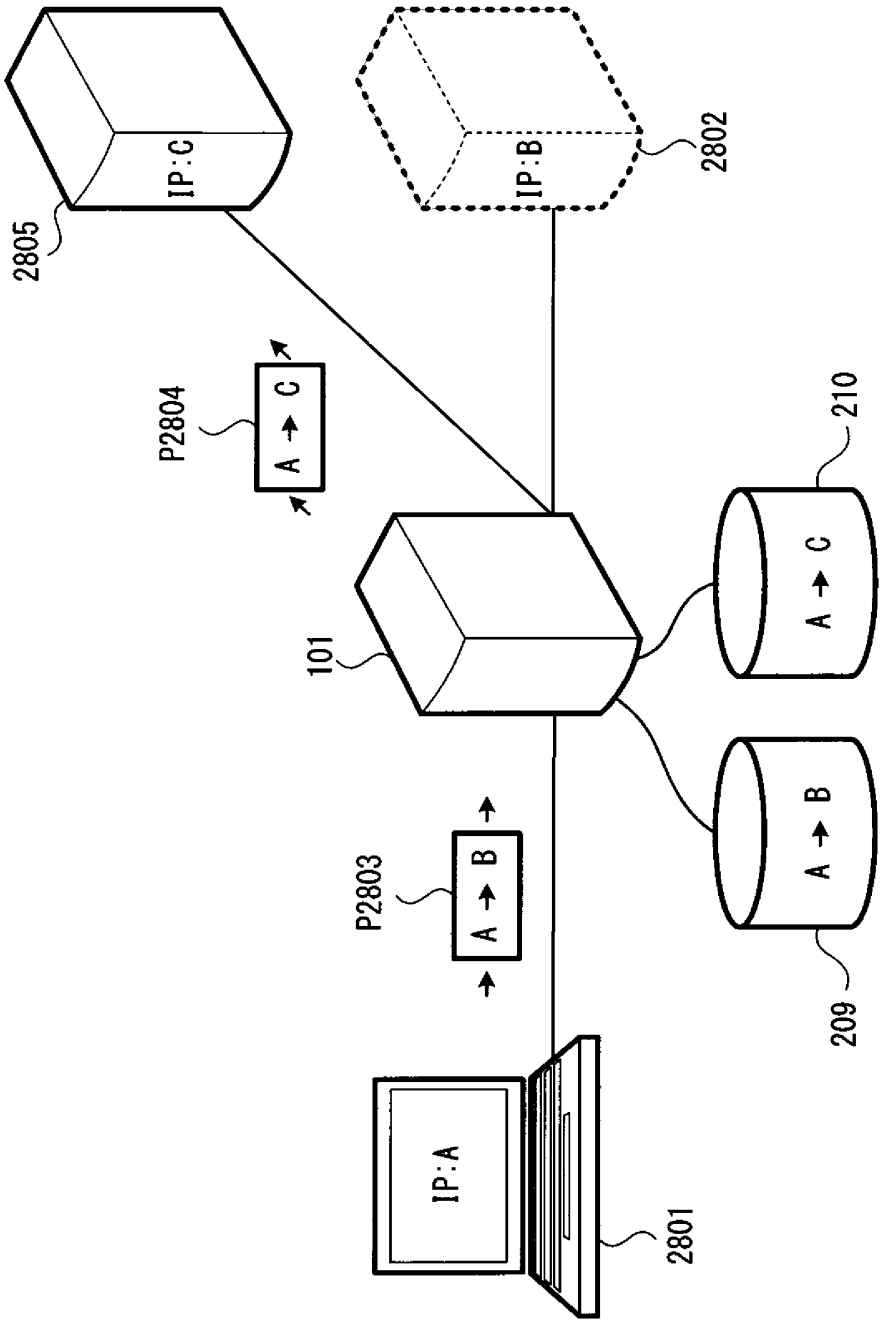
도면26


XPTCP 비대응 PC
어드레스 변환 처리부
TCP/IP 프로토콜 스택
XPTCP 처리부
소켓 처리부
내측 NIC
S2501
FIN 송신
S2502
어드레스 변환
S2503
헤더 제거
S2504
절단 요구
(close 이벤트)
S2514
허가
(accept 이벤트)
S2515
ACK/FIN 생성
S2516
어드레스 변환
S2517
ACK 응답
S2518
어드레스 변환
S2519
절단 완료

도면27


XPTCP 대응 서버
어드레스 변환 처리부
TCP/IP 프로토콜 스택
XPTCP 처리부
소켓 처리부
어드레스 변환 처리부
외측 NIC
S2507
FIN 수신
S2508
ACK/FIN 송신
S2513
절단 완료
S2506
어드레스 변환
S2509
어드레스 변환
S2520
타이머 기동
S2512
어드레스 변환
S2522
외측 NIC 어드레스 테이블 레코드 삭제
S2505
FIN 생성
S2510
ACK 응답
(외측 플래그)
S2511
커넥션 관련지음 개방
S2504
절단 요구
(close request 이벤트)
S2514
허가
S2521
내측 NIC 어드레스 테이블 레코드 삭제

도면28



도면29

