(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
H04L 12/66 (2006.01)
H04L 12/56 (2006.01)
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

(11) 공개번호 10-2007-0045282
(43) 공개일자 2007년05월02일

(21) 출원번호 10-2007-7004289
(22) 출원일자 2007년02월23일
심사청구일자 없음
번역문 제출일자 2007년02월23일
(86) 국제출원번호 PCT/US2005/026296
국제출원일자 2005년07월22일
(87) 국제공개번호 WO 2006/012610
국제공개일자 2006년02월02일

(30) 우선권주장
60/590,837 2004년07월23일 미국(US)
60/601,431 2004년08월13일 미국(US)
60/607,420 2004년09월03일 미국(US)
60/608,814 2004년09월10일 미국(US)

(71) 출원인 사이트릭스 시스템스, 인크.
미국 플로리다 33309, 포트 라우더데일, 851 더블류. 사이프레스 크릭 로드

(72) 발명자 라오, 고우담, 피.
미국 캘리포니아 95120, 산 호세, 스탈링 밸리 드라이브 6963
브루그만, 에릭
미국 캘리포니아 95014, 쿠퍼티노, 넘버 606, 스티븐즈 크릭불레바드 5642
로드리게즈, 로버트
미국 캘리포니아 95123, 산 호세, 웰즈 코트 5647

(74) 대리인 신영무

전체 청구항 수 : 총 179 항

(54) 네트워크 노드 간의 통신을 최적화하기 위한 시스템 및방법

(57) 요약

본 발명은 일반적으로 피어투피어 통신과 원격 액세스 연결을 제공하기 위한 원격 액세스 아키텍처에 대한 것이다. 일 실시예에서, 본 발명의 원격 액세스 아키텍처는 게이트웨이와 같은 제3 컴퓨팅 디바이스를 통해 피어 컴퓨팅 디바이스 간의 직접적인 연결을 설정하기 위한 방법을 제공한다. 부가하여, 본 발명은 피어투피어 통신을 최적화하기 위한 다음 기술을 제공한다: 1) 손실 프로토콜을 통한 전송을 위해 구성된 패킷의 무손실 프로토콜을 통한 통신을 가능하게 하는 네트워크 패킷의 수신의 이상 확인, 2) 손실 프로토콜을 통한 전송을 위해 구성된 패킷의 무손실 프로토콜을 통한 통신을 가능하게

하는 네트워크 패킷의 패이로드 시프팅, 3) 암호화로 인한 오버헤드를 고려하여, 최대 전송 단위 (MTU) 파라미터를 조정한 패킷 단편화의 감소, 4) 클라이언트측 네트워크 통신의 어플리케이션 인식 우선 순위, 및 5) 모바일 컴퓨팅에 대한 것과 같이, 신뢰 가능 및 영구적 네트워크 연결성과 액세스를 위한 네트워크 붕괴 차단.

대표도

도 2a

특허청구의 범위

청구항 1.

제1 네트워크 상의 제1 컴퓨팅 디바이스와 제2 네트워크 상의 제2 컴퓨팅 디바이스 간의 피어투피어 통신 세션을 설정하기 위한 방법에 있어서 - 상기 제1 네트워크는 상기 제2 네트워크로부터 분리되어 라우트가능하지 않음 -, 상기 방법은:

(a) 상기 제1 컴퓨팅 디바이스에 의해, 제3 컴퓨팅 디바이스와의 제1 터널링 세션을 설정하고, 상기 제2 컴퓨팅 디바이스에 의해 상기 제3 컴퓨팅 디바이스와의 제2 터널링 세션을 설정하는 단계;

(b) 상기 제1 컴퓨팅 디바이스에 의해, 상기 제3 컴퓨팅 디바이스를 통해 상기 제2 컴퓨팅 디바이스에 대한 통신 세션을 초기화하는 단계;

(c) 서버에 의해 상기 통신 세션을 설정하도록 신호를 수신하는 단계;

(d) 상기 서버에 의해 상기 제2 터널링 세션과 관련된 상기 제2 컴퓨팅 디바이스의 네트워크 주소를 포함하는 제1 네트워크 주소를 상기 제1 컴퓨팅 디바이스에 통신하는 단계;

(e) 상기 제1 컴퓨팅 디바이스에 의해 상기 제1 네트워크 주소를 이용하여 상기 제2 컴퓨팅 디바이스와의 연결을 초기화하는 요청을 통신하는 단계;

(f) 상기 제3 컴퓨팅 디바이스에 의해, 상기 요청을 인터셉트하여 상기 제2 컴퓨팅 디바이스에 대한 제2 네트워크 주소를 상기 제1 컴퓨팅 디바이스에 제공하는 단계 - 상기 제2 네트워크 주소는 상기 제2 컴퓨팅 디바이스와 관련된 공중 네트워크 주소를 포함함 -; 및

(g) 상기 제3 컴퓨팅 디바이스에 의해, 상기 제2 네트워크 주소를 이용하여 상기 제1 컴퓨팅 디바이스로부터의 연결을 허용하는 요청을 상기 제2 컴퓨팅 디바이스에 통신하는 단계

를 포함하는 방법.

청구항 2.

제1항에 있어서, 상기 제1 터널링 세션 또는 상기 제2 터널링 세션 중 하나의 적어도 일부는 보안 소켓 계층이나 가상 사설망 중 하나를 포함하는 방법.

청구항 3.

제1항에 있어서, 상기 제3 컴퓨팅 디바이스는 원격 액세스 게이트웨이를 포함하는 방법.

청구항 4.

제1항에 있어서, 상기 제2 컴퓨팅 디바이스는 상기 제2 네트워크 주소와 관련된 방화벽 뒤에 위치하는 방법.

청구항 5.

제1항에 있어서, 상기 제3 컴퓨팅 디바이스에 의해, 상기 제1 터널링 세션을 통해 상기 제1 컴퓨팅 디바이스에 대역외 신호를 통신함으로써 상기 제1 컴퓨팅 디바이스에 상기 제2 네트워크 주소를 제공하는 단계를 포함하는 방법.

청구항 6.

제1항에 있어서, 상기 제2 컴퓨팅 디바이스에 의해, 상기 제1 컴퓨팅 디바이스가 상기 제2 네트워크 주소를 이용하여 상기 제2 컴퓨팅 디바이스에 통신하도록 방화벽에 포워드 홀을 제공하는 단계를 포함하는 방법.

청구항 7.

제1항에 있어서, 상기 제3 컴퓨팅 디바이스에 의해, 상기 제1 컴퓨팅 디바이스 및 제2 컴퓨팅 디바이스에 키를 통신하는 단계를 포함하는 방법.

청구항 8.

제7항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해, 상기 제2 컴퓨팅 디바이스에 상기 키를 통신하는 단계를 포함하는 방법.

청구항 9.

제8항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해, 상기 제2 컴퓨팅 디바이스로부터 수신된 상기 키가 상기 제2 컴퓨팅 디바이스에 데이터를 전송하기 전에 상기 제1 컴퓨팅 디바이스의 상기 키와 일치하는지를 체크하는 단계를 포함하는 방법.

청구항 10.

제7항에 있어서, 상기 제2 컴퓨팅 디바이스에 의해, 상기 제1 컴퓨팅 디바이스에 상기 키를 통신하는 단계를 포함하는 방법.

청구항 11.

제10항에 있어서, 상기 제2 컴퓨팅 디바이스에 의해, 상기 제1 컴퓨팅 디바이스로부터 수신된 상기 키가 상기 제2 컴퓨팅 디바이스에 데이터를 전송하기 전에 상기 제2 컴퓨팅 디바이스의 상기 키와 일치하는지를 체크하는 단계를 포함하는 방법.

청구항 12.

제1항에 있어서, 상기 제1 컴퓨팅 디바이스와 제1 텔레커뮤니케이션 장치를 관련시키고, 상기 제2 컴퓨팅 디바이스와 제2 텔레커뮤니케이션 장치를 관련시키는 단계를 포함하는 방법.

청구항 13.

제12항에 있어서, 상기 제1 텔레커뮤니케이션 장치나 제2 텔레커뮤니케이션 장치 중 하나는 소프트웨어 컴포넌트나 하드웨어 컴포넌트 중 하나를 포함하는 방법.

청구항 14.

제12항에 있어서, 상기 제1 텔레커뮤니케이션 장치와 상기 제2 텔레커뮤니케이션 장치 간의 텔레커뮤니케이션 세션을 상기 연결을 통해 설정하는 단계를 포함하는 방법.

청구항 15.

제14항에 있어서, 상기 제1 컴퓨팅 디바이스를 관통하지 않고 상기 텔레커뮤니케이션 세션을 통해 상기 제1 텔레커뮤니케이션 장치와 상기 제2 텔레커뮤니케이션 장치 간에 통신하는 단계를 포함하는 방법.

청구항 16.

제1항에 있어서, 상기 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 상기 연결을 통해 원격 디스플레이 프로토콜을 통신하는 단계를 포함하는 방법.

청구항 17.

제16항에 있어서, 상기 원격 데스크톱 프로토콜은 개별적 컴퓨팅 아키텍처 프로토콜 또는 원격 데스크톱 프로토콜 중 하나를 포함하는 방법.

청구항 18.

제1항에 있어서, 상기 제1 컴퓨팅 디바이스의 스크린 뷰를 상기 연결을 통해 상기 제2 컴퓨팅 디바이스와 공유하는 단계를 포함하는 방법.

청구항 19.

게이트웨이에서, 제1 네트워크 상의 제1 컴퓨팅 디바이스와 제2 네트워크 상의 제2 컴퓨팅 디바이스 간의 피어투피어 통신 세션을 설정하기 위한 방법에 있어서 - 상기 제1 네트워크는 상기 제2 네트워크와 분리되어 라우트 가능하지 않음 - 상기 방법은:

(a) 상기 제1 네트워크 상의 상기 제1 컴퓨팅 디바이스와의 제1 터널링 세션을 설정하는 단계;

(b) 상기 제2 네트워크 상의 제2 컴퓨팅 디바이스와의 제2 터널링 세션을 설정하는 단계;

(c) 상기 제2 컴퓨팅 디바이스와의 통신 세션을 초기화하는 상기 제1 컴퓨팅 디바이스에 의한 요청을 수신하는 단계;

(d) 상기 제2 컴퓨팅 디바이스와 접촉하기 위해 상기 제1 컴퓨팅 디바이스에 제1 네트워크 주소를 제공하는 단계 - 상기 제1 네트워크 주소는 상기 제2 터널링 세션과 관련된 상기 제2 컴퓨팅 디바이스의 네트워크 주소를 포함함 - ;

(e) 상기 제1 네트워크 주소를 이용하여 상기 제2 컴퓨팅 디바이스와의 연결을 초기화하는 상기 제1 컴퓨팅 디바이스에 의한 요청을 수신하는 단계;

(f) 상기 연결을 초기화하는 요청을 인터셉트하여, 상기 제2 컴퓨팅 디바이스에 대한 제2 네트워크 주소를 상기 제1 컴퓨팅 디바이스에 제공하는 단계 - 상기 제2 네트워크 주소는 상기 제2 컴퓨팅 디바이스와 관련된 공중 네트워크 주소를 포함함 - ; 및

(g) 상기 제2 네트워크 주소를 이용하여 상기 제1 컴퓨팅 디바이스로부터 상기 제2 컴퓨팅 디바이스로의 연결을 허용하는 요청을 상기 제2 컴퓨팅 디바이스에게 통신하는 단계

를 포함하는 방법.

청구항 20.

제19항에 있어서, 상기 제1 터널링 세션 또는 상기 제2 터널링 세션 중 하나의 적어도 일부는 보안 소켓 계층 또는 가상 사설망 중 하나를 포함하는 방법.

청구항 21.

제19항에 있어서, 상기 제2 컴퓨팅 디바이스는 상기 제2 네트워크 주소와 관련된 방화벽 뒤에 위치되는 방법.

청구항 22.

제19항에 있어서, 상기 제1 터널링 세션을 통해 상기 제1 컴퓨팅 디바이스에 대역외 신호를 통신하여 상기 제1 컴퓨팅 디바이스에 상기 제2 네트워크 주소를 제공하는 단계를 포함하는 방법.

청구항 23.

제19항에 있어서, 상기 제1 컴퓨팅 디바이스에 키를 통신하는 단계를 포함하는 방법.

청구항 24.

제19항에 있어서, 상기 제2 컴퓨팅 디바이스에 키를 통신하는 단계를 포함하는 방법.

청구항 25.

제1 네트워크 상의 제1 컴퓨팅 디바이스와 제2 네트워크 상의 제2 컴퓨팅 디바이스 간의 피어투피어 통신 세션을 제3 컴퓨팅 디바이스를 통해 설정하기 위한 시스템에 있어서 - 상기 제1 네트워크는 상기 제2 네트워크와 분리되어 라우트 가능하지 않음 - 상기 시스템은:

상기 제1 네트워크 상의 제1 컴퓨팅 디바이스;

상기 제2 네트워크 상의 제2 컴퓨팅 디바이스;

상기 제1 컴퓨팅 디바이스와의 제1 터널링 세션과 상기 제2 컴퓨팅 디바이스와의 제2 터널링 세션을 설정하는 제3 컴퓨팅 디바이스;

상기 제3 컴퓨팅 디바이스를 통해 액세스 가능한 서버

를 포함하고, 상기 서버는 상기 제3 컴퓨팅 디바이스를 통해 상기 제1 컴퓨팅 디바이스에 상기 제2 터널링 세션과 관련되는 상기 제2 컴퓨팅 디바이스의 네트워크 주소를 포함하는 제1 네트워크 주소를 통신하고;

상기 제1 컴퓨팅 디바이스는 상기 제1 네트워크 주소를 이용하여 상기 제2 컴퓨팅 디바이스와의 연결을 초기화하려는 제1 요청을 상기 제3 컴퓨팅 디바이스를 통해 통신하고;

상기 제3 컴퓨팅 디바이스는 상기 제1 요청을 인터셉트하고, 상기 제1 컴퓨팅 디바이스에 상기 제2 컴퓨팅 디바이스에 대한 제2 네트워크 주소를 제공하고, 상기 제2 네트워크 주소는 상기 제2 컴퓨팅 디바이스와 관련된 공중 네트워크 주소를 포함하고,

상기 제3 컴퓨팅 디바이스는 상기 제2 네트워크 주소를 이용하여 상기 제1 컴퓨팅 디바이스로부터의 연결을 허용하는 제2 요청을 상기 제2 컴퓨팅 디바이스에 통신하는 시스템.

청구항 26.

제25항에 있어서, 상기 제1 터널링 세션 또는 상기 제2 터널링 세션 중 하나의 적어도 일부는 보안 소켓 계층 또는 가상 사설망 중 하나를 포함하는 시스템.

청구항 27.

제25항에 있어서, 상기 제3 컴퓨팅 디바이스는 원격 액세스 게이트웨이를 포함하는 시스템.

청구항 28.

제25항에 있어서, 상기 제2 컴퓨팅 디바이스는 상기 제2 네트워크 주소와 관련된 방화벽 뒤에 위치되는 시스템.

청구항 29.

제25항에 있어서, 상기 제3 컴퓨팅 디바이스는 상기 제1 터널링 세션을 통해 대역외 신호를 통신하여 상기 제1 컴퓨팅 디바이스에 상기 제2 네트워크 주소를 제공하는 시스템.

청구항 30.

제25항에 있어서, 상기 제2 컴퓨팅 디바이스는 상기 제1 컴퓨팅 디바이스가 상기 제2 네트워크 주소를 이용하여 상기 제2 컴퓨팅 디바이스에 통신하도록 방화벽에 포워드 홀을 제공하는 시스템.

청구항 31.

제25항에 있어서, 상기 제3 컴퓨팅 디바이스는 상기 제1 컴퓨팅 디바이스 및 제2 컴퓨팅 디바이스에 키를 통신하는 시스템.

청구항 32.

제31항에 있어서, 상기 제1 컴퓨팅 디바이스는 상기 제2 컴퓨팅 디바이스에 키를 통신하는 시스템.

청구항 33.

제32항에 있어서, 상기 제1 컴퓨팅 디바이스는 상기 제2 컴퓨팅 디바이스로부터 수신된 상기 키가 상기 제2 컴퓨팅 디바이스에 데이터를 전송하기 전에 상기 제1 컴퓨팅 디바이스의 상기 키와 일치하는지를 체크하는 시스템.

청구항 34.

제31항에 있어서, 상기 제2 컴퓨팅 디바이스는 상기 제1 컴퓨팅 디바이스에 상기 키를 통신하는 시스템.

청구항 35.

제34항에 있어서, 상기 제2 컴퓨팅 디바이스는 상기 제1 컴퓨팅 디바이스로부터 수신된 상기 키가 상기 제2 컴퓨팅 디바이스로 데이터를 전송하기 전에 상기 제2 컴퓨팅 디바이스의 상기 키와 일치하는지를 체크하는 시스템.

청구항 36.

제25항에 있어서, 상기 제1 컴퓨팅 디바이스와 관련되는 제1 텔레커뮤니케이션 장치 및 상기 제2 컴퓨팅 디바이스와 관련되는 제2 텔레커뮤니케이션 장치를 포함하는 시스템.

청구항 37.

제36항에 있어서, 상기 제1 텔레커뮤니케이션 장치나 제2 텔레커뮤니케이션 장치 중 하나는 소프트웨어 컴포넌트나 하드웨어 컴포넌트 중 하나를 포함하는 시스템.

청구항 38.

제37항에 있어서, 상기 제1 텔레커뮤니케이션 장치는 상기 제2 텔레커뮤니케이션 장치와의 텔레커뮤니케이션 세션을 상기 연결을 통해 설정하는 시스템.

청구항 39.

제38항에 있어서, 상기 제1 텔레커뮤니케이션 장치는 상기 제3 컴퓨팅 디바이스를 관통하지 않고 상기 텔레커뮤니케이션 세션을 통해 상기 제2 텔레커뮤니케이션 장치와 통신하는 시스템.

청구항 40.

제25항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스는 상기 연결을 통해 원격 디스플레이 프로토콜을 통신하는 시스템.

청구항 41.

제25항에 있어서, 상기 원격 데스크톱 프로토콜은 개별적 컴퓨팅 아키텍쳐 프로토콜 또는 원격 데스크톱 프로토콜 중 하나를 포함하는 시스템.

청구항 42.

제25항에 있어서, 상기 제1 컴퓨팅 디바이스는 상기 연결을 통해 상기 제2 컴퓨팅 디바이스와 스크린 뷰를 공유하는 시스템.

청구항 43.

제1 네트워크 상의 제1 컴퓨팅 디바이스와 제2 네트워크 상의 제2 컴퓨팅 디바이스 간의 피어투피어 통신 세션을 설정하기 위한 게이트웨이에 있어서 - 상기 제1 네트워크는 상기 제2 네트워크와 분리되어 라우트 가능하지 않음 - 상기 게이트웨이는:

상기 제1 네트워크 상의 상기 제1 컴퓨팅 디바이스와의 제1 터널링 세션을 설정하기 위한 수단;

상기 제2 네트워크 상의 상기 제2 컴퓨팅 디바이스와의 제2 터널링 세션을 설정하기 위한 수단;

상기 제2 컴퓨팅 디바이스와의 통신 세션을 초기화하려는 상기 제1 컴퓨팅 디바이스에 의한 요청을 수신하기 위한 수단;

상기 제2 컴퓨팅 디바이스에 접촉하기 위해 제1 네트워크 주소를 상기 제1 컴퓨팅 디바이스에 제공하기 위한 수단 - 상기 제1 네트워크 주소는 상기 제2 터널링 세션과 관련된 상기 제2 컴퓨팅 디바이스의 네트워크 주소를 포함함 - ;

상기 제1 네트워크 주소를 이용하여 상기 제2 컴퓨팅 디바이스와의 연결을 초기화하려는 상기 제1 컴퓨팅 디바이스에 의한 요청을 수신하기 위한 수단;

상기 연결을 초기화하려는 상기 요청을 인터셉트하고, 상기 제1 컴퓨팅 디바이스에 상기 제2 컴퓨팅 디바이스에 대한 제2 네트워크 주소를 제공하기 위한 수단 - 상기 제2 네트워크 주소는 상기 제2 컴퓨팅 디바이스와 관련된 공중 네트워크 주소를 포함함 - ; 및

상기 제2 네트워크 주소를 이용하여 상기 제1 컴퓨팅 디바이스로부터 상기 제2 컴퓨팅 디바이스로의 연결을 허용하는 요청을 상기 제2 컴퓨팅 디바이스에 통신하기 위한 수단

을 포함하는 게이트웨이.

청구항 44.

제43항에 있어서, 상기 제1 터널링 세션 또는 상기 제2 터널링 세션 중 하나의 적어도 일부는 보안 소켓 계층 또는 가상 사설망 중 하나를 포함하는 게이트웨이.

청구항 45.

제43항에 있어서, 상기 제2 컴퓨팅 디바이스는 상기 제2 네트워크 주소와 관련된 방화벽 뒤에 위치되는 게이트웨이.

청구항 46.

제43항에 있어서, 상기 제1 터널링 세션을 통해 상기 제1 컴퓨팅 디바이스에 대역외 신호를 통신하여 상기 제2 네트워크 주소를 상기 제1 컴퓨팅 디바이스에 제공하기 위한 수단을 포함하는 게이트웨이.

청구항 47.

제43항에 있어서, 상기 제1 컴퓨팅 디바이스에 키를 통신하기 위한 수단을 포함하는 게이트웨이.

청구항 48.

제43항에 있어서, 상기 제2 컴퓨팅 디바이스에 키를 통신하기 위한 수단을 포함하는 게이트웨이.

청구항 49.

손실 프로토콜을 통해 전송하게 구성된 패킷을 무손실 프로토콜을 통해 통신하기 위한 방법에 있어서, 상기 방법은:

(a) 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 연결을 무손실 프로토콜을 통해 설정하는 단계;

(b) 상기 제1 컴퓨팅 디바이스에 의해, 손실 프로토콜에 따라 구성된 하나 이상의 패킷을 갖는 페이로드를 포함하는 무손실 프로토콜 패킷을 검출하는 단계;

(c) 상기 제1 컴퓨팅 디바이스에 의해, 상기 제1 컴퓨팅 디바이스 또는 상기 제2 컴퓨팅 디바이스 중 하나에 상기 무손실 프로토콜 패킷의 수신의 이상 확인을 통신하는 단계;

(d) 상기 제1 컴퓨팅 디바이스에 의해, 상기 무손실 프로토콜 패킷을 상기 제2 컴퓨팅 디바이스에 통신하는 단계

를 포함하는 방법.

청구항 50.

제49항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해, 키를 이용하여 상기 하나 이상의 패킷을 암호화하는 단계를 포함하는 방법.

청구항 51.

제50항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 대역외 전송 보안 계층 세션을 통해 상기 암호화 키를 상기 제1 컴퓨팅 디바이스에 제공하는 단계를 포함하는 방법.

청구항 52.

제49항에 있어서, 상기 하나 이상의 패킷을 패킷 마다에 기초하여 암호화하는 단계를 포함하는 방법.

청구항 53.

제49항에 있어서, 상기 단계 (d) 이전에 상기 단계 (c)를 실행하는 단계를 더 포함하는 방법.

청구항 54.

제49항에 있어서, 상기 제2 컴퓨팅 디바이스는 게이트웨이인 방법.

청구항 55.

제49항에 있어서, 상기 제1 컴퓨팅 디바이스 또는 제2 컴퓨팅 디바이스 중 하나에 의해 상기 무손실 프로토콜 패킷의 수신의 이상 확인을 수신한 것에 응답하여, 상기 제1 컴퓨팅 디바이스 또는 상기 제2 컴퓨팅 디바이스 중 하나의 네트워크 스택이 상기 무손실 프로토콜의 무손실 특성을 제공하는 것과 관련하는 동작을 실행하는 것을 방지하는 단계를 포함하는 방법.

청구항 56.

제49항에 있어서, 상기 무손실 프로토콜은 전송 제어 프로토콜을 포함하는 방법.

청구항 57.

제56항에 있어서, 상기 제1 컴퓨팅 디바이스 또는 상기 제2 컴퓨팅 디바이스 중 하나의 상기 네트워크 스택이 상기 무손실 프로토콜과 관련하여 재전송, 오더링, 흐름 제어 알고리즘, 네이플의 알고리즘 및 슬라이딩 윈도우 알고리즘 중 하나 이상을 실행하는 것을 방지하는 단계를 포함하는 방법.

청구항 58.

제49항에 있어서, 상기 무손실 프로토콜은 유저 데이터그램 프로토콜을 포함하는 방법.

청구항 59.

제49항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해 보안 소켓 계층이나 전송 보안 계층 터널 중 하나를 통해 상기 무손실 프로토콜 패킷을 상기 제2 컴퓨팅 디바이스에 통신하는 단계를 포함하는 방법.

청구항 60.

제49항에 있어서, 상기 하나 이상의 패킷은 실시간 프로토콜을 포함하는 방법.

청구항 61.

제49항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해 상기 하나 이상의 패킷을 통해 실시간 음성, 오디오 또는 데이터 중 하나를 상기 제2 컴퓨팅 디바이스에 통신하는 단계를 포함하는 방법.

청구항 62.

무손실 프로토콜을 통해 전송되게 구성된 패킷을 무손실 프로토콜을 통해 통신하기 위한 시스템에 있어서, 상기 시스템은:

제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 사이의 연결을 무손실 프로토콜을 통해 설정하기 위한 수단;

상기 제1 컴퓨팅 디바이스에 의해, 손실 프로토콜에 따라 구성된 하나 이상의 패킷을 갖는 페이로드를 포함하는 무손실 프로토콜 패킷을 검출하기 위한 수단;

상기 제1 컴퓨팅 디바이스에 의해, 상기 제1 컴퓨팅 디바이스나 상기 제2 컴퓨팅 디바이스 중 하나에 상기 무손실 프로토콜 패킷의 수신의 이상 확인을 통신하기 위한 수단; 및

상기 제1 컴퓨팅 디바이스에 의해, 상기 무손실 프로토콜 패킷을 상기 제2 컴퓨팅 디바이스에 통신하기 위한 수단

을 포함하는 시스템.

청구항 63.

제62항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해 상기 하나 이상의 패킷을 키를 이용하여 암호화하기 위한 수단을 포함하는 시스템.

청구항 64.

제63항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 대역외 전송 보안 계층 세션을 통해 상기 암호화 키를 상기 제1 컴퓨팅 디바이스에 제공하기 위한 수단을 포함하는 시스템.

청구항 65.

제63항에 있어서, 상기 하나 이상의 프로토콜 패킷을 패킷 마다에 기초하여 암호화하기 위한 수단을 포함하는 시스템.

청구항 66.

제62항에 있어서, 상기 무손실 프로토콜 패킷을 통신하기 전에 상기 무손실 프로토콜 패킷의 수신의 이상 확인을 통신하기 위한 수단을 더 포함하는 시스템.

청구항 67.

제62항에 있어서, 상기 제2 컴퓨팅 디바이스는 게이트웨이인 시스템.

청구항 68.

제62항에 있어서, 상기 제1 컴퓨팅 디바이스 또는 제2 컴퓨팅 디바이스 중 하나에 의해 상기 무손실 프로토콜 패킷의 수신의 이상 확인을 수신한 것에 응답하여, 상기 제1 컴퓨팅 디바이스 또는 상기 제2 컴퓨팅 디바이스 중 하나의 네트워크 스택이 상기 무손실 프로토콜의 무손실 특성을 제공하는 것과 관련된 동작을 실행하는 것을 방지하기 위한 수단을 포함하는 시스템,

청구항 69.

제62항에 있어서, 상기 무손실 프로토콜은 전송 제어 프로토콜을 포함하는 시스템.

청구항 70.

제69항에 있어서, 상기 제1 컴퓨팅 디바이스 또는 상기 제2 컴퓨팅 디바이스 중 하나의 상기 네트워크 스택이 상기 무손실 프로토콜과 관련하여 재전송, 오더링, 흐름 제어 알고리즘, 네이플의 알고리즘 및 슬라이딩 윈도우 알고리즘 중 하나 이상을 실행하는 것을 방지하기 위한 수단을 포함하는 시스템.

청구항 71.

제62항에 있어서, 상기 무손실 프로토콜은 유저 데이터그램 프로토콜을 포함하는 시스템.

청구항 72.

제62항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해 보안 소켓 계층이나 전송 보안 계층 터널 중 하나를 통해 상기 무손실 프로토콜 패킷을 상기 제2 컴퓨팅 디바이스에 통신하기 위한 수단을 포함하는 시스템.

청구항 73.

제62항에 있어서, 상기 하나 이상의 패킷은 실시간 프로토콜을 포함하는 시스템.

청구항 74.

제62항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해 상기 하나 이상의 패킷을 통해 실시간 음성, 오디오 또는 데이터 중 하나를 상기 제2 컴퓨팅 디바이스에 통신하기 위한 수단을 포함하는 시스템.

청구항 75.

TCP 연결을 통한 비신뢰성 전송 프로토콜을 이용하여 애플리케이션으로부터 패킷을 전송하기 위한 방법에 있어서:

제1 디바이스에서 비신뢰성 전송 프로토콜을 이용하여 전송되는 제1 패킷을 수신하는 단계;

상기 수신된 제1 패킷의 제1 페이로드 및 상기 제1 디바이스와 제2 디바이스 간에 설정된 TCP 연결과 관련되는 정보의 제1 TCP 헤더를 포함하는 제1 TCP 패킷을 형성하는 단계;

상기 제1 디바이스에 의해, 상기 제1 TCP 패킷을 상기 제2 디바이스에 전송하는 단계;

상기 제1 디바이스에서, 비신뢰성 전송 프로토콜을 이용하여 전송되는 제2 패킷을 수신하는 단계;

상기 수신된 제2 패킷의 제2 페이로드 및 상기 제1 TCP 헤더 정보를 포함하는 제2 TCP 패킷을 형성하는 단계; 및

상기 제1 디바이스에 의해, 상기 제2 디바이스로부터의 상기 제1 페이로드의 수신 확인의 수신 이전에, 상기 제2 TCP 패킷을 상기 제2 디바이스에 전송하는 단계

를 포함하는 방법.

청구항 76.

제75항에 있어서, 상기 비신뢰 전송 프로토콜과 관련되는 포트 번호로 상기 TCP 연결을 설정하는 단계를 포함하는 방법.

청구항 77.

제75항에 있어서, 상기 제1 디바이스에 의해, 상기 제1 TCP 패킷과 상기 제2 TCP 패킷이 비신뢰성 전송 프로토콜을 포함하는지를 동적으로 판정하는 단계를 포함하는 방법.

청구항 78.

제75항에 있어서, 상기 비신뢰성 전송 프로토콜은 UDP인 방법.

청구항 79.

제75항에 있어서, 상기 제1 TCP 패킷과 상기 제2 TCP 패킷을 패킷 캡처링 메커니즘을 이용하여 인터셉트함으로써 상기 제1 디바이스 상의 상기 제1 TCP 패킷과 제2 TCP 패킷을 수신하는 단계를 더 포함하는 방법.

청구항 80.

제75항에 있어서, 상기 제1 디바이스에 의해, VPN 게이트웨이 장치와의 상기 TCP 연결을 설정하는 단계를 포함하는 방법.

청구항 81.

제75항에 있어서, 상기 TCP 연결을 통해 상기 제1 디바이스와 상기 제2 디바이스 간의 피어투피어 통신을 설정하는 단계를 포함하는 방법.

청구항 82.

제75항에 있어서, 상기 제1 디바이스에 의해, 상기 제1 및 제2 TCP 패킷을 암호화하고, 상기 제2 디바이스에 의해 상기 암호화된 제1 및 제2 TCP 패킷을 복호하는 단계를 포함하는 방법.

청구항 83.

TCP 연결을 통해 비신뢰성 전송 프로토콜을 이용하여 애플리케이션으로부터 패킷을 전송하기 위한 방법에 있어서:

제2 디바이스에서, 제1 디바이스에서 형성되어 상기 제2 디바이스에서 수신되는 제1 TCP 패킷을 인터셉트하는 단계 - 상기 제1 TCP 패킷은 비신뢰성 프로토콜을 이용하여 애플리케이션에 의해 형성된 제1 패킷의 제1 페이로드 및 상기 제1 디바이스와 상기 제2 디바이스 간에 설정된 TCP 연결과 관련된 정보의 제1 TCP 헤더를 포함하고, 상기 인터셉트하는 단계는 상기 제1 TCP 패킷이 상기 제2 디바이스에서 TCP 스택에 제공되기 전에 발생함 - ;

상기 TCP 헤더의 정보에 응답하여, 상기 제1 페이로드가 비신뢰 전송 프로토콜을 이용하여 애플리케이션에 의해 형성된 패킷인 것을 식별하는 단계;

상기 제1 TCP 패킷으로부터 상기 TCP 헤더의 정보를 분리하는 단계; 및

상기 비신뢰성 데이터 프로토콜을 이용하여 애플리케이션에 상기 제1 페이로드를 전달하는 단계

를 포함하는 방법.

청구항 84.

제83항에 있어서, 상기 비신뢰성 프로토콜은 UDP인 방법.

청구항 85.

제83항에 있어서, 상기 식별 단계는 상기 TCP 헤더 정보가 상기 비신뢰성 전송 프로토콜과 관련된 포트 번호를 포함하는 것을 식별하는 단계를 포함하는 방법.

청구항 86.

제83항에 있어서, 상기 제2 디바이스에 의해, 패킷 캡쳐 드라이버를 이용하여 상기 제1 TCP 패킷을 인터셉트하는 단계를 더 포함하는 방법.

청구항 87.

제83항에 있어서, 상기 제1 디바이스는 클라이언트 디바이스이고 상기 제2 디바이스는 VPN 게이트웨이인 방법.

청구항 88.

제87항에 있어서, 상기 제1 페이로드를 상기 애플리케이션에 전달하기 전에 상기 제2 디바이스에서 네트워크 주소 변환(NAT)를 실행하는 단계를 더 포함하는 방법.

청구항 89.

TCP 연결을 통해 비신뢰성 전송 프로토콜을 이용하여 애플리케이션으로부터 패킷을 전송하기 위한 시스템에 있어서:

제1 디바이스; 및

상기 제1 디바이스와 통신하는 제2 디바이스

를 포함하고, 상기 제1 디바이스는:

제1 및 제2 패킷을 형성하는 애플리케이션 - 상기 제1 및 제2 패킷은 비신뢰성 전송 프로토콜을 이용하여 전송되는 것임 - ;

상기 제1 및 제2 패킷을 상기 애플리케이션으로부터 인터셉트하여 상기 인터셉트된 패킷을 터널 프로세스로 전달하는 필터 프로세스; 및

상기 제1 디바이스와 제2 디바이스 간의 TCP 연결의 개방을 요청하는 터널 프로세스 - 상기 TCP 연결의 개방 요청은 상기 TCP 연결이 비신뢰성 전송 프로토콜로 전송되려고 하는 패킷을 전송하게 되는 것을 상기 제1 및 제2 디바이스에게 지시하고, 상기 터널 프로세스는 제1 및 제2 TCP 패킷의 페이로드로서 상기 제1 및 제2 패킷을 상기 제2 디바이스에 전달하고, 상기 터널 프로세스는 상기 제1 TCP 패킷을 전송한 후와 상기 제1 TCP 패킷에 대한 확인을 수신하기 전에 상기 제2 TCP 패킷을 전송함 -

를 포함하고, 상기 제2 디바이스는:

상기 제1 디바이스에 의해 요청되는 상기 TCP 연결을 개방하는 제2 터널 프로세스 - 상기 제2 터널 프로세스는 제2 필터 프로세스에 대한 상기 TCP 연결의 소스 주소를 식별하여 전달함 -; 및

상기 제2 디바이스에서 수신된 상기 애플리케이션으로부터의 패킷을 헤더의 상기 TCP 연결 소스 주소로 인터셉트하는 제2 필터 프로세스 - 상기 제2 필터 프로세스는 상기 수신된 패킷으로부터 상기 TCP 헤더를 분리하여 상기 분리된 패킷을 전달하고, 상기 제2 디바이스 상서의 상기 TCP/IP 스택을 의도한 목적지로 보냄 -

를 포함하는 시스템.

청구항 90.

제89항에 있어서, 상기 제1 디바이스 상의 상기 필터 프로세스는 패킷 캡쳐 드라이버를 포함하는 시스템.

청구항 91.

제89항에 있어서, 상기 제2 디바이스 상의 상기 제2 필터 프로세스는 패킷 캡쳐 드라이버를 포함하는 시스템.

청구항 92.

제89항에 있어서, 상기 제1 디바이스는 클라이언트 디바이스이고 상기 제2 디바이스는 VPN 게이트웨이 디바이스인 시스템.

청구항 93.

제89항에 있어서, 상기 분리된 패킷이 전송되는 제3 디바이스를 더 포함하는 시스템.

청구항 94.

제93항에 있어서, 상기 제2 디바이스는 상기 분리된 패킷을 제3 디바이스로 전송하기 전에 네트워크 주소 변환을 실행하는 데에 이용되는 네트워크 주소 변환 (NAT) 테이블을 더 포함하는 시스템.

청구항 95.

제89항에 있어서, 상기 비신뢰성 데이터 프로토콜은 UDP인 시스템.

청구항 96.

네트워크 단편화를 줄이도록 보안 네트워크 통신의 최대 전송 단위를 조정하기 위한 방법에 있어서:

(a) 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 세션을 설정하는 단계 - 상기 제1 컴퓨팅 디바이스는 제1 네트워크 스택을 가짐 - ;

(b) 상기 제1 컴퓨팅 디바이스에 의해 암호화된 페이로드를 갖는 네트워크 패킷을 검출하는 단계;

(c) 상기 제1 컴퓨팅 디바이스에 의해 상기 최대 전송 단위 크기를 상기 페이로드의 상기 암호화된 부분과 관련된 최소한의 크기만큼 줄이도록 상기 제1 네트워크 스택의 최대 전송 단위 파라미터에 대한 세팅을 결정하는 단계; 및

(d) 상기 제1 네트워크 스택의 상기 최대 전송 단위 파라미터를 상기 결정된 세팅으로 변경하는 단계

를 포함하는 방법.

청구항 97.

제96항에 있어서, 상기 네트워크 패킷을 보안 소켓 계층이나 전송 계층 보안 터널 중 하나를 통해 상기 제2 컴퓨팅 디바이스에 통신하는 단계를 포함하는 방법.

청구항 98.

제96항에 있어서, 상기 페이로드는 실시간 프로토콜을 포함하는 방법.

청구항 99.

제96항에 있어서, 상기 제1 네트워크 스택의 네트워크 드라이버 인터페이스 사양 레벨 메커니즘을 통해 상기 최대 전송 단위 파라미터를 변경하는 단계를 더 포함하는 방법.

청구항 100.

제96항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 세션 당 상기 최대 전송 단위 파라미터의 설정치를 동적으로 결정하는 단계를 더 포함하는 방법.

청구항 101.

제96항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 세션을 게이트웨이를 통해 설정하는 단계를 더 포함하는 방법.

청구항 102.

제96항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해 상기 네트워크 패킷의 상기 페이로드를 통해 실시간 음성, 오디오 또는 데이터 중 하나를 상기 제2 컴퓨팅 디바이스에 통신하는 단계를 포함하는 방법.

청구항 103.

제96항에 있어서, 상기 네트워크 패킷을 통신하기 전에 상기 제1 컴퓨팅 디바이스 또는 상기 제2 컴퓨팅 디바이스 중 하나에 상기 네트워크 패킷의 수신의 이상 확인을 통신하는 단계를 포함하는 방법.

청구항 104.

제96항에 있어서, 상기 제1 컴퓨팅 디바이스의 에이전트를 통해 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 세션을 설정하는 단계를 더 포함하는 방법.

청구항 105.

제104항에 있어서, 상기 에이전트에 의해, 상기 최대 전송 단위 파라미터를 상기 결정된 설정치로 변경하기 위해서, IOCTL 애플리케이션 프로그래밍 인터페이스를 통해 상기 제1 네트워크 스택에 통신하는 단계를 포함하는 방법.

청구항 106.

네트워크 단편화를 줄이도록 보안 네트워크 통신의 최대 전송 단위를 조정하기 위한 시스템에 있어서:

(a) 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 세션을 설정하기 위한 수단 - 상기 제1 컴퓨팅 디바이스는 제1 네트워크 스택을 가짐 - ;

(b) 상기 제1 컴퓨팅 디바이스에 의해 암호화된 페이로드를 갖는 네트워크 패킷을 검출하기 위한 수단;

(c) 상기 제1 컴퓨팅 디바이스에 의해 상기 페이로드의 상기 암호화된 부분과 관련된 최소한의 크기만큼 상기 최대 전송 단위 크기를 줄이도록 상기 제1 네트워크 스택의 최대 전송 단위 파라미터에 대한 설정치를 결정하기 위한 수단; 및

(d) 상기 제1 네트워크 스택의 상기 최대 전송 단위 파라미터를 상기 결정된 설정치로 변경하기 위한 수단

를 포함하는 시스템.

청구항 107.

제106항에 있어서, 상기 네트워크 패킷을 제2 소켓 계층이나 전송 계층 보안 터널 중 하나를 통해 상기 제2 컴퓨팅 디바이스에 통신하기 위한 수단을 포함하는 시스템.

청구항 108.

제106항에 있어서, 상기 페이로드는 실시간 프로토콜을 포함하는 시스템.

청구항 109.

제106항에 있어서, 상기 페이로드는 실시간 음성, 오디오 또는 데이터 중 하나의 표현을 포함하는 시스템.

청구항 110.

제106항에 있어서, 상기 제1 네트워크 스택의 네트워크 드라이버 인터페이스 사양 레벨 메커니즘을 통해 상기 제1 컴퓨팅 디바이스의 상기 최대 전송 단위 파라미터를 변경하기 위한 수단을 더 포함하는 시스템.

청구항 111.

제106항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 세션 당 상기 최대 전송 단위 파라미터의 세팅을 동적으로 결정하기 위한 수단을 더 포함하는 시스템.

청구항 112.

제106항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 세션을 게이트웨이를 통해 설정하기 위한 수단을 더 포함하는 시스템.

청구항 113.

제106항에 있어서, 상기 제1 컴퓨팅 디바이스에 의해 상기 네트워크 패킷의 상기 페이로드를 통해 실시간 음성, 오디오 또는 데이터 중 하나를 상기 제2 컴퓨팅 디바이스에 통신하기 위한 수단을 포함하는 시스템.

청구항 114.

제106항에 있어서, 상기 네트워크 패킷을 통신하기 전에 상기 제1 컴퓨팅 디바이스 또는 상기 제2 컴퓨팅 디바이스 중 하나에 상기 네트워크 패킷의 수신의 이상 확인을 통신하기 위한 수단을 포함하는 시스템.

청구항 115.

제106항에 있어서, 상기 네트워크 패킷은 무손실 프로토콜 패킷을 포함하는 시스템.

청구항 116.

제115항에 있어서, 상기 무손실 프로토콜 패킷은 전송 제어 프로토콜을 포함하는 시스템.

청구항 117.

제106항에 있어서, 상기 페이로드는 손실 프로토콜 패킷을 포함하는 시스템.

청구항 118.

제117항에 있어서, 상기 손실 프로토콜 패킷은 유저 데이터그램 프로토콜을 포함하는 시스템.

청구항 119.

제106항에 있어서, 상기 제1 컴퓨팅 디바이스와 상기 제2 컴퓨팅 디바이스 간의 세션을 설정하기 위한 상기 제1 컴퓨팅 디바이스의 에이전트를 포함하는 시스템.

청구항 120.

제119항에 있어서, 상기 에이전트는 상기 최대 전송 단위 파라미터를 상기 결정된 세팅으로 변경하도록 IOCTL 애플리케이션 프로그래밍 인터페이스를 통해 상기 제1 네트워크 스택에 통신하는 시스템.

청구항 121.

클라이언트가 상기 클라이언트의 애플리케이션과 관련된 클라이언트의 네트워크 통신을 우선 순위화하는 방법에 있어서:

(a) 상기 클라이언트에 의해, 상기 클라이언트의 하나 이상의 애플리케이션과 관련된 하나 이상의 네트워크 패킷을 인터셉트하는 단계;

(b) 상기 클라이언트에 의해, 상기 하나 이상의 네트워크 패킷을 큐에 저장하는 단계;

(c) 상기 클라이언트에 의해 상기 큐된 하나 이상의 네트워크 패킷이 상기 클라이언트의 제1 애플리케이션과 관련되지를 판단하는 단계;

(d) 상기 클라이언트에 의해, 상기 클라이언트의 제2 애플리케이션과 관련된 큐에 상기 판단된 하나 이상의 네트워크 패킷을 적어도 하나의 네트워크 패킷 보다 우선하여 위치시키도록 상기 판단된 하나 이상의 네트워크 패킷에 대한 우선 순위를 나타내는 단계; 및

(e) 상기 클라이언트의 네트워크 스택에 의한 통신을 위해 상기 우선 순위된 하나 이상의 네트워크 패킷을 제공하는 단계

를 포함하는 방법.

청구항 122.

제121항에 있어서, 상기 클라이언트에 의해 판단하는 단계는 상기 제1 애플리케이션의 상기 큐된 하나 이상의 네트워크 패킷이 실시간 데이터를 포함한다고 판단하는 단계를 더 포함하는 방법.

청구항 123.

제122항에 있어서, 상기 실시간 데이터는 실시간 프로토콜, 유저 데이터그램 프로토콜, 및 음성이나 오디오 중 하나의 표시중 하나를 포함하는 방법.

청구항 124.

제121항에 있어서, 상기 클라이언트에 의해 상기 제2 애플리케이션의 적어도 하나의 네트워크 패킷이 상기 제1 애플리케이션의 상기 하나 이상의 네트워크 패킷 보다 우선하여 상기 네트워크 스택을 통해 통신되지 않도록 방지하는 단계를 더 포함하는 방법.

청구항 125.

제121항에 있어서, 상기 클라이언트에 의해, 상기 제2 애플리케이션과 관련된 네트워크 패킷을 유지하는 단계; 상기 유지된 네트워크 패킷을 상기 유지된 네트워크 패킷 보다 우선으로 순위된 상기 제1 애플리케이션과 관련된 상기 하나 이상의 네트워크 패킷의 통신시 해제하는 단계를 포함하는 방법.

청구항 126.

제121항에 있어서, 상기 클라이언트에 의해, 상기 하나 이상의 네트워크 패킷을 상기 클라이언트 상의 상기 하나 이상의 애플리케이션에 투명하게 인터셉트하는 단계를 포함하는 방법.

청구항 127.

제121항에 있어서, 상기 제1 애플리케이션을 상기 포그라운드에서, 상기 제2 애플리케이션을 상기 백그라운드에서 실행하는 단계를 포함하는 방법.

청구항 128.

제121항에 있어서, 상기 제1 애플리케이션과 관련된 우선 순위를 상기 제2 애플리케이션과 관련된 우선 순위보다 더 높게 하는 단계를 포함하는 방법.

청구항 129.

제128항에 있어서, 유저에 의해 상기 제1 애플리케이션 또는 상기 제2 애플리케이션 중 하나의 우선 순위을 특정하는 단계를 포함하는 방법.

청구항 130.

제121항에 있어서, 상기 클라이언트에 의해 상기 하나 이상의 네트워크 패킷을 컴퓨팅 디바이스로부터 수신하는 단계를 포함하는 방법.

청구항 131.

제121항에 있어서, 상기 하나 이상의 애플리케이션에 의해, 상기 하나 이상의 네트워크 패킷을 상기 클라이언트로부터 컴퓨팅 디바이스로 통신하기 위해 제공하는 단계를 포함하는 방법.

청구항 132.

클라이언트의 애플리케이션과 관련된 상기 클라이언트의 네트워크 통신을 우선 순위화하기 위한 클라이언트에 있어서:

상기 클라이언트의 하나 이상의 애플리케이션과 관련된 상기 클라이언트의 하나 이상의 네트워크 패킷을 인터셉트하기 위한 메커니즘;

상기 하나 이상의 네트워크 패킷을 큐에 저장하고 상기 하나 이상의 네트워크 패킷을 상기 클라이언트의 네트워크 스택을 거쳐 통신하기 위한 네트워크 드라이버; 및

상기 하나 이상의 네트워크 패킷이 상기 클라이언트의 제1 애플리케이션과 관련되었는지를 판정하여, 상기 판단된 하나 이상의 네트워크 패킷을 적어도 하나의 네트워크 패킷 보다 우선하여 위치시키도록 상기 판단된 하나 이상의 네트워크 패킷에 대한 우선 순위를 상기 네트워크 드라이버에게 나타내기 위한 에이전트

를 포함하는 클라이언트

청구항 133.

제132항에 있어서, 상기 에이전트는 상기 제1 애플리케이션의 상기 하나 이상의 네트워크 패킷이 실시간 데이터를 포함한다고 판정하는 클라이언트.

청구항 134.

제132항에 있어서, 상기 실시간 데이터는 실시간 프로토콜, 유저 데이터그램 프로토콜, 및 음성이나 오디오 중 하나의 표시중 하나를 포함하는 클라이언트.

청구항 135.

제132항에 있어서, 상기 에이전트나 상기 네트워크 드라이버 중 하나는 상기 제2 애플리케이션의 적어도 하나의 네트워크 패킷이 상기 제1 애플리케이션의 상기 하나 이상의 네트워크 패킷 보다 우선하여 상기 네트워크 스택을 통해 통신되지 않도록 방지하는 클라이언트.

청구항 136.

제132항에 있어서, 상기 네트워크 드라이버는 상기 제2 애플리케이션과 관련된 네트워크 패킷을 상기 큐에 유지하는 단계; 상기 유지된 네트워크 패킷을 상기 유지된 네트워크 패킷 보다 우선으로 순위된 상기 제1 애플리케이션과 관련된 상기 하나 이상의 네트워크 패킷의 통신시 해제하는 클라이언트.

청구항 137.

제132항에 있어서, 상기 메커니즘은 상기 하나 이상의 네트워크 패킷을 상기 클라이언트 상의 상기 하나 이상의 애플리케이션에 투명하게 인터셉트하는 클라이언트.

청구항 138.

제132항에 있어서, 상기 제1 애플리케이션을 상기 포그라운드에서, 상기 제2 애플리케이션을 상기 백그라운드에서 실행하는 클라이언트.

청구항 139.

제132항에 있어서, 상기 제1 애플리케이션은 상기 제2 애플리케이션과 관련된 우선 순위보다 더 높은 클라이언트.

청구항 140.

제132항에 있어서, 유저가 상기 우선 순위를 특정하도록 하는 컨피규레이션 메커니즘을 더 포함하는 클라이언트.

청구항 141.

제132항에 있어서, 상기 클라이언트는 상기 하나 이상의 네트워크 패킷을 컴퓨팅 디바이스로부터 수신하는 클라이언트.

청구항 142.

제132항에 있어서, 상기 하나 이상의 애플리케이션은 상기 하나 이상의 네트워크 패킷을 상기 클라이언트로부터 컴퓨팅 디바이스로 통신하기 위해 제공하는 클라이언트.

청구항 143.

제132항에 있어서, 상기 네트워크 드라이버는 네트워크 드라이버 인터페이스 사양 (NDIS) 드라이버를 포함하는 클라이언트.

청구항 144.

제132항에 있어서, 상기 네트워크 드라이버는 상기 클라이언트의 운영 시스템의 커널 모드에서 동작하는 클라이언트.

청구항 145.

제132항에 있어서, 상기 에이전트는 상기 클라이언트의 운영 시스템의 유저 모드에서 동작하는 클라이언트.

청구항 146.

제132항에 있어서, 상기 에이전트나 상기 네트워크 드라이버 중 하나는 상기 클라이언트의 하나 이상의 네트워크 패킷을 인터셉트하기 위한 메커니즘을 포함하는 클라이언트.

청구항 147.

제1 프로토콜을 통해 설정된 세션을 네트워크 붕괴로부터 차단하기 위한 방법에 있어서:

(a) 클라이언트의 에이전트에 의해, 상기 클라이언트와 디바이스 간의 네트워크 연결에 의한 제1 프로토콜을 통한 세션을 설정하는 단계 - 상기 네트워크 연결은 네트워크 스택과 관련되고, 상기 제1 네트워크 스택의 제1 부분은 상기 제1 프로토콜의 상기 층 아래의 상기 네트워크 스택의 하나 이상의 층을 포함하고, 상기 네트워크 스택의 제2 부분은 상기 제1 프로토콜에 대한 층과 상기 제1 프로토콜 위의 상기 네트워크 스택의 하나 이상의 층을 포함함 - ;

(b) 상기 네트워크 스택의 상기 제1 부분이 폐지되게 하는 상기 제1 네트워크 연결의 붕괴를 검출하는 단계;

(c) 상기 에이전트에 의해 상기 붕괴 동안 상기 세션 및 상기 네트워크 스택의 상기 제2 부분을 유지하는 단계; 및

(d) 상기 세션 및 상기 네트워크 스택의 상기 제2 부분을 유지하면서 상기 네트워크 스택의 상기 제2 부분 및 상기 네트워크 연결을 재설정하는 단계

를 포함하는 방법.

청구항 148.

제147항에 있어서,

(e) 상기 네트워크 스택의 상기 유지된 제2 부분과 상기 네트워크 스택의 상기 재설정된 제1 부분으로 상기 세션을 계속하는 단계를 더 포함하는 방법.

청구항 149.

제147항에 있어서,

(e) 상기 네트워크 스택의 상기 제2 부분에 의해 붕괴 동안 네트워크 패킷의 수신을 중단시키는 단계를 더 포함하는 방법.

청구항 150.

제147항에 있어서, 상기 디바이스는 원격 액세스 게이트웨이나 컴퓨팅 디바이스 중 하나를 포함하는 방법.

청구항 151.

제147항에 있어서, 상기 세션을 보안 소켓층 (SSL) 프로토콜, 전송층 보안 (TLS) 프로토콜 및 터널링 프로토콜 중 하나의 제1 프로토콜을 통해 설정하는 단계를 더 포함하는 방법.

청구항 152.

제147항에 있어서, 상기 에이전트에 의해 상기 클라이언트와 상기 디바이스 간의 상기 세션을 통해 실시간 데이터를 통신하는 단계를 포함하는 방법.

청구항 153.

제152항에 있어서, 상기 실시간 데이터는 실시간 프로토콜을 포함하는 방법.

청구항 154.

제152항에 있어서, 상기 실시간 데이터는 음성이나 오디오 중 하나의 표시를 포함하는 방법.

청구항 155.

제147항에 있어서, 상기 에이전트를 상기 클라이언트의 운영 시스템의 유저 모드에서 동작시키는 단계를 포함하는 방법.

청구항 156.

제147항에 있어서, 상기 네트워크의 상기 제1 부분은 전송 제어 프로토콜이나 인터넷 프로토콜 중 하나를 포함하는 방법.

청구항 157.

제147항에 있어서, 상기 네트워크 스택의 상기 제2 부분은 인터넷 프로토콜, 유저 데이터그램 프로토콜 또는 음성 전면 인터넷 프로토콜 중 하나를 포함하는 방법.

청구항 158.

제147항에 있어서, 상기 클라이언트가 원격 디스플레이 프로토콜을 통해 상기 디바이스와 통신하는 단계를 포함하는 방법.

청구항 159.

제158항에 있어서, 상기 원격 디스플레이 프로토콜은 인디펜던트 컴퓨팅 아키텍쳐 프로토콜이나 원격 데스트톱 프로토콜 중 하나를 포함하는 방법.

청구항 160.

제147항에 있어서, 상기 단계(b), (c) 및 (d) 중 하나를 상기 네트워크 연결을 통해 통신하는 상기 클라이언트의 애플리케이션에 투명하게 실행하는 단계를 포함하는 방법.

청구항 161.

제147항에 있어서, 상기 에이전트에 의해 상기 애플리케이션과 관련된 하나 이상의 네트워크 패킷을 상기 클라이언트의 애플리케이션에 대해 투명하게 인터셉트하는 단계를 포함하는 방법.

청구항 162.

제147항에 있어서, 상기 스택의 상기 제2 부분과 관련된 네트워크 드라이버에 의해 상기 애플리케이션과 관련된 하나 이상의 네트워크 패킷을 상기 클라이언트 상의 애플리케이션에 투명하게 인터셉트하는 단계를 포함하는 방법.

청구항 163.

제1 프로토콜을 통해 설정된 세션을 네트워크 붕괴로부터 차단하기 위한 시스템에 있어서:

제1 프로토콜을 통한 네트워크 연결로 상기 클라이언트와 디바이스 간의 연결을 설정하는 클라이언트의 에이전트;

상기 제1 부분과 제2 부분을 갖는 네트워크 스택 - 상기 네트워크 스택의 상기 제1 부분은 상기 제1 프로토콜의 층 아래의 상기 네트워크 스택의 하나 이상의 층을 포함하고, 상기 네트워크 스택의 상기 제2 부분은 상기 제1 프로토콜에 대한 층과 상기 제1 프로토콜 위의 상기 네트워크 층의 하나 이상의 층을 포함함 - ; 및

상기 네트워크 스택의 상기 제2 부분이 폐지되게 하는 상기 네트워크 연결의 붕괴를 검출하기 위한 검출기

를 포함하고, 상기 검출기에 의한 상기 붕괴의 검출시, 상기 에이전트는 상기 붕괴 동안 상기 세션과 상기 네트워크 스택의 상기 제2 부분을 유지하고;

상기 클라이언트는 상기 에이전트가 상기 세션과 상기 네트워크 스택의 상기 제2 부분을 유지하는 동안 상기 네트워크 스택의 상기 제1 부분과 상기 네트워크 연결을 재설정하는 시스템.

청구항 164.

제163항에 있어서, 상기 에이전트는 상기 네트워크 스택의 상기 유지된 제2 부분과 상기 네트워크 스택의 상기 재설정된 제1 부분으로 상기 세션을 계속하는 시스템.

청구항 165.

제163항에 있어서, 상기 네트워크 스택의 상기 제1 부분이나 상기 제2 부분 중 하나는 상기 붕괴 동안 네트워크 패킷의 수신을 중단시키는 시스템.

청구항 166.

제163항에 있어서, 상기 디바이스는 원격 액세스 게이트웨이나 컴퓨팅 디바이스 중 하나를 포함하는 시스템.

청구항 167.

제163항에 있어서, 상기 제1 프로토콜은 보안 소켓층 (SSL) 프로토콜, 전송층 보안 (TLS) 프로토콜 및 터널링 프로토콜 중 하나를 포함하는 시스템.

청구항 168.

제163항에 있어서, 상기 에이전트는 상기 클라이언트와 상기 디바이스 간의 상기 세션을 통해 실시간 데이터를 통신하는 시스템.

청구항 169.

제168항에 있어서, 상기 실시간 데이터는 실시간 프로토콜 중 하나를 포함하는 시스템.

청구항 170.

제168항에 있어서, 상기 실시간 데이터는 음성이나 오디오 중 하나의 표시를 포함하는 시스템.

청구항 171.

제163항에 있어서, 상기 에이전트는 상기 클라이언트의 운영 시스템의 유저 모드에서 동작하는 시스템.

청구항 172.

제163항에 있어서, 상기 네트워크의 상기 제1 부분은 전송 제어 프로토콜이나 인터넷 프로토콜 중 하나를 포함하는 시스템.

청구항 173.

제163항에 있어서, 상기 네트워크 스택의 상기 제2 부분은 인터넷 프로토콜, 유저 데이터그램 프로토콜 또는 음성 전면 인터넷 프로토콜 중 하나를 포함하는 시스템.

청구항 174.

제163항에 있어서, 상기 제1 프로토콜은 원격 디스플레이 프로토콜을 포함하는 시스템.

청구항 175.

제174항에 있어서, 상기 원격 디스플레이 프로토콜은 인디펜던트 컴퓨팅 아키텍쳐 프로토콜이나 원격 데스트톱 프로토콜 중 하나를 포함하는 시스템.

청구항 176.

제163항에 있어서, 상기 에이전트는 상기 클라이언트의 애플리케이션의 하나 이상의 네트워크 패킷을 상기 클라이언트 애플리케이션에 대해 투명하게 인터셉트하는 시스템.

청구항 177.

제163항에 있어서, 상기 네트워크의 상기 제2 부분과 관련된 네트워크 드라이버를 포함하고, 상기 네트워크 드라이버는 상기 클라이언트의 애플리케이션의 하나 이상의 네트워크 패킷을 상기 애플리케이션에 대해 투명하게 인터셉트하고, 상기 하나 이상의 패킷을 상기 세션을 통해 통신하도록 상기 에이전트에 제공하는 시스템.

청구항 178.

제177항에 있어서, 상기 네트워크 드라이버는 네트워크 드라이버 인터페이스 사양 (NDIS) 드라이버를 포함하는 시스템.

청구항 179.

제177항에 있어서, 상기 네트워크 드라이버는 상기 클라이언트의 운영 시스템의 커널 모드에서 동작하는 시스템.

명세서

기술분야

본 발명은 일반적으로 네트워크 상의 노드 간의 네트워크 통신을 최적화하는 것에 관한 것이다.

배경기술

가상 사설망 (VPN)은 터널링과 보안 메커니즘의 이용으로 비밀성을 유지하기 위해, 인터넷 등의 공중 텔레커뮤니케이션 인프라를 이용하는 개인 데이터망이다. 이와 같이, VPN은 공중망을 관통하는 기업의 데이터에 대해 데이터 암호화와 보안성을 제공한다. VPN은 공중망을 통한 기업의 데이터에 대한 보안 액세스를 해결하는 데에 부가하여, 두 개의 분리되거나 아니면 라우트 불가능한 네트워크로부터 네트워크 트래픽을 라우팅하는 것에 관한 것이다. 예를 들어, 10.0.0.0-10.255.255.255 범위의 개인 인터넷 프로토콜 주소를 갖는 제1 사설망은 범위 192.168.0.0-192.168.255.255의 개인 인터넷 프로토콜 주소를 갖는 제2 사설망을 갖는 VPN를 통해 통신할 수 있다. VPN은 제1 사설망에서의 원격 머신이 이 원격 머신으로부터 네트워크 트래픽을 터널링하고 네트워크 트래픽이 제2 사설망에 나타나게 함으로써 제2 사설망의 내부 머신과 통신하게 한다. 이는 원격 컴퓨터가 원격 네트워크 상에 위치된 기업체 서버와 트랜잭션하고 있는 클라이언트-서버 프로토콜에 대해 잘 적용된다.

그러나, 종래의 VPN은 피어투피어 프로토콜에서와 같이, 서로 직접 통신하기 위해 VPN 게이트웨이를 통해 두 원격 컴퓨터가 터널링하는 경우에는 잘 적용되지 않는다. VPN은 두 개의 원격 컴퓨터가 VPN 게이트웨이를 통해 모든 피어투피어 통신을 터널링하는 디스조인트 사설망 주소 공간을 평탄화하여 이 피어투피어 컴퓨팅을 성취한다. 그 결과, 피어들 중 하나로부터의 네트워크 트래픽은 VPN 게이트웨이를 통해 흐르고 인터넷 상에서 다시 피어 컴퓨터로 흐르도록 인트라넷 상의 터널을 전환한다. 피어 컴퓨터들 간의 네트워크 트래픽은 피어 컴퓨터가 이들 사이의 직접적인 경로가 더 짧은 경우에도 더 길거나 짧은 최적의 루트를 이동할 수 있다. 원격 컴퓨터가 더 긴 데이터 경로 루트의 결함을 초래하지 않고 VPN에 의해 가능하게 되는 보안의 이점을 갖게 하는 것이 좋다.

두 컴퓨터 간의 네트워크를 통한 직접적 통신에는 다른 비효율성이 존재한다. 예를 들어, 네트워크 연결은 브레이크다운되기 쉽다. 예를 들어, 클라이언트와 서버 간의 무선 연결은 신뢰 불가능할 때가 있다. 다른 경우, 네트워크 연결은 간헐적이다. 엘레베이터나 터널에 들어갈 때 연결성이 손실되어 다시 나온 이후에만 회복될 수 있다. 다른 예에서, 모바일 컴퓨팅 디바이스가 무선 네트워크 토폴러지에서와 같이 네트워크 액세스 지점에서 네트워크 액세스 지점으로 이동할 때 연결성이 붕괴될 수 있다.

클라이언트와 서버 컴퓨터 간의 통신 세션이 비이상적으로 종료하게 되면, 클라이언트는 새로운 통신 세션을 시작하여 연결성을 재설정해야 한다. 새로운 통신 세션을 시작하기 위해서, 유저는 로긴/패스워드 쌍과 같은 인증 증명서를 서버 컴퓨터에 재전송해야 하므로 서버 컴퓨터는 새로운 통신 세션에 대해 유저를 인증할 수가 있다. 이렇게 다수의 통신 세션을 통한 유저의 인증 증명서의 재전송은 이 유저의 인증 증명서를 잠재적인 침입자에게 반복적으로 노출시키게 되고, 이로 인해 인증 증명서의 보안 수준이 저하되게 된다. 부가하여, 이는 유저의 좌절과 비효율성의 결과를 가져오는 느린 프로세스이다. 더욱, 새로운 통신 세션을 설정할 때, 네트워크는 클라이언트가 인터넷 프로토콜 주소와 같은 새로운 네트워크 식별자를 취득할 필요가 있다. 클라이언트 상의 어플리케이션이나 프로그램은 클라이언트의 네트워크 식별자의 변경으로 인해 재시작될 필요가 있다. 따라서, 컴퓨팅 디바이스를 네트워크 붕괴로부터 차단하는 것이 바람직하다.

피어 컴퓨팅 디바이스 간의 직접적인 통신과 관련된 다른 비효율성은 통신에 이용되는 프로토콜이 원하는 데로 효율적이거나 보안적일 수 없다. 일 예로, 네트워크 통신은 음성 전면 IP (VoIP) 통신과 같이 실시간 데이터 통신을 포함할 수 있다. 실시간 데이터 통신은 전화 호출의 레이턴시를 감소하기 위해서 유저 데이터그램 프로토콜과 같은 신뢰 불가능한 프로토콜을 거쳐 통신된다. 그러나, VoIP 통신은 VoIP 통신에 신뢰가능한 프로토콜을 제공하는 TCP/IP 네트워크나 보안 SSL 게이트웨이를 관통할 수 있다. 이것은 신뢰 불가능한 프로토콜이 감소하려고 하는 전화 호출의 레이턴시를 증가시킬 수 있다. 손실 프로토콜을 이용하여 통신하고자 하는 데이터를 무손실 프로토콜을 통해 전송하기 위한 기술의 필요성이 절실하다.

다른 직접 통신시의 비효율성은 암호화를 이용하게 한다. SSL과 같은 암호화는 보안 네트워크 통신을 제공하는 데에 이용된다. 통신은 보안적이지만, 네트워크 트래픽의 암호화는 네트워크 패킷의 크기를 증가시키고, 이는 패킷 페이로드가 하나의 패킷에 대해 너무 커지게 할 수 있다. 이것은 패킷 단편화의 결과를 가져와, 통신 처리에 대한 오버헤드를 많이 초래한다. 암호화 오버헤드를 고려하기 위한 패킷의 최대 크기를 조정하는 기술이 유용하다.

클라이언트가 통상 네트워크 통신을 유저의 동작과 클라이언트의 어플리케이션에 의해 형성하면서 보내고, 인입 네트워크 통신을 수신하면서 처리한다는 사실로 인해 또 다른 비효율성이 나타난다. 예를 들어, 한 경우에, 어플리케이션이 포그라운드에서 실행중이고 현재 유저에 의해 이용중이어도, 백그라운드에서 실행중인 어플리케이션에 대해 형성되거나 수신된 네트워크 패킷은 포그라운드에서 실행중인 어플리케이션에 대해 형성되거나 수신된 네트워크 패킷 이전에 처리될 수 있다. VoIP의 실시간 데이터 통신에 관련되지 않은 클라이언트 상의 하나 이상의 다른 어플리케이션이 실행중일 수 있다. 이

들 어플리케이션에 대한 네트워크 패킷은 VoIP 전화의 실시간 네트워크 패킷 이전에 처리되고 이로 인해 레이턴시를 증가시키고 음성 통신의 질을 감소시키게 된다. 패킷 트래픽의 어플리케이션 인식, 클라이언트 특정적 우선 순위를 제공하는 것이 바람직하다.

발명의 상세한 설명

본 발명은 일반적으로 피어투피어 통신 및 원격 액세스 연결을 제공하기 위한 원격 액세스 아키텍처에 관한 것이다. 일 실시예에서, 본 발명의 원격 액세스 아키텍처는 게이트웨이와 같은 제3자 컴퓨팅 디바이스를 통해 피어 컴퓨팅 디바이스 간의 직접적 연결을 설정하기 위한 방법을 제공한다. 부가하여, 본 발명은 음성 전면 IP (VoIP) 시그널링과 매체, 비디오 및 그 외 웹 협력, 스크린이나 데스크톱 공유 및 인스턴스 메시징 등의 실시간 데이터 어플리케이션과 같은 실시간 통신을 포함하는 피어투피어 통신을 최적화하기 위한 여러 기술을 제공한다. 본 발명은 다음 피어투피어 최적화 기술을 제공한다: 1) 손실 프로토콜을 통한 전송을 위해 구성된 패킷의 무손실 프로토콜을 통한 통신을 가능하게 하는 네트워크 패킷의 수신의 이상 확인, 2) 손실 프로토콜을 통한 전송을 위해 구성된 패킷의 무손실 프로토콜을 통한 통신을 가능하게 하는 네트워크 패킷의 패이로드 시프팅, 3) 암호화로 인한 오버헤드를 고려하여, 최대 전송 단위 (MTU) 파라미터를 조정한 패킷 단편화의 감소, 4) 클라이언트측 네트워크 통신의 어플리케이션 인식 우선 순위, 및 5) 모바일 컴퓨팅에 대한 것과 같이, 신뢰가능 및 영구적 네트워크 연결성과 액세스를 위한 네트워크 붕괴 차단.

일 형태에서, 본 발명은 제1 네트워크 상의 제1 컴퓨팅 디바이스와 제2 네트어크 상의 제2 컴퓨팅 디바이스 간의 피어투피어 통신 세션을 설정하기 위한 방법에 관한 것이다. 제1 네트워크는 제2 네트워크와 분리되어 이에 라우트 불가능하다. 이 방법은 제1 컴퓨팅 디바이스에 의해, 제3 컴퓨팅 디바이스와의 제1 터널링 세션을 설정하고, 제2 컴퓨팅 디바이스에 의해 제3 컴퓨팅 디바이스와의 제2 터널링 세션을 설정하는 단계를 포함한다. 제3 컴퓨팅 디바이스는 SSL VPN 게이트웨이와 같은 게이트웨이일 수 있다. 제1 컴퓨팅 컴퓨팅 디바이스는 시그널링 프로토콜을 통해서와 같이, 제3 컴퓨팅 디바이스를 통해 제2 컴퓨팅 디바이스에 대한 통신 세션을 초기화한다. 서버는 통신 세션을 설정하도록 신호를 수신하고, 서버는 제2 터널링 세션과 관련된 제2 컴퓨팅 디바이스의 네트워크 주소를 포함하는 제1 네트워크 주소를 제1 컴퓨팅 디바이스에 통신한다. 제1 컴퓨팅 디바이스는 제1 네트워크 주소를 이용하여 제2 컴퓨팅 디바이스와의 연결을 초기화하는 요청을 통신한다. 본 방법은 또한 제3 컴퓨팅 디바이스에 의해, 요청을 인터셉트하여 제2 컴퓨팅 디바이스에 대한 제2 네트워크 주소를 제1 컴퓨팅 디바이스에 제공하는 단계를 포함한다. 제2 네트워크 주소는 제2 컴퓨팅 디바이스와 관련된 공중 네트워크 주소를 식별한다. 제3 컴퓨팅 디바이스는 방화벽을 관통하는 스위머 세션을 통해서와 같이, 제2 네트워크 주소를 이용하여 제1 컴퓨팅 디바이스로부터의 연결을 허용하는 요청을 제2 컴퓨팅 디바이스에 통신한다.

본 발명의 일 실시예에서, 제1 터널링 세션 또는 제2 터널링 세션은 보안 소켓 계층이나 가상 사설망을 이용하여 설정된다. 제3 컴퓨팅 디바이스는 원격 액세스 게이트웨이를 포함한다. 다른 실시예에서, 제2 컴퓨팅 디바이스는 제2 네트워크 주소와 관련된 방화벽 뒤에 위치된다.

다른 실시예에서, 본 발명의 방법은 제3 컴퓨팅 디바이스에 의해, 제1 터널링 세션을 통해 제1 컴퓨팅 디바이스에 대역외 신호를 통신함으로써 제1 컴퓨팅 디바이스에 제2 네트워크 주소를 제공하는 단계를 포함한다. 부가의 실시예에서, 이 방법은 제2 컴퓨팅 디바이스에 의해, 제1 컴퓨팅 디바이스가 제2 네트워크 주소를 이용하여 제2 컴퓨팅 디바이스에 통신하도록 방화벽에 포워드 홀을 제공하는 단계를 포함한다.

본 발명의 다른 실시예에서, 제3 컴퓨팅 디바이스는 제1 컴퓨팅 디바이스 및 제2 컴퓨팅 디바이스에 키를 통신한다. 제1 컴퓨팅 디바이스는 제2 컴퓨팅 디바이스에 키를 통신한다. 부가하여, 제1 및 제2 컴퓨팅 디바이스는 데이터를 다른 컴퓨팅 디바이스에 전송하기 전에 다른 컴퓨팅 디바이스로부터 수신된 키가 일치하는지를 체크한다.

본 발명의 실시예에서, 이 방법은 제1 컴퓨팅 디바이스와 제1 텔레커뮤니케이션 장치를 관련시키고, 제2 컴퓨팅 디바이스와 제2 텔레커뮤니케이션 장치를 관련시킨다. 제1 텔레커뮤니케이션 장치나 제2 텔레커뮤니케이션는 하드 또는 소프트 VoIP 전화와 같은, 소프트웨어 컴포넌트나 하드웨어 컴포넌트를 포함한다. 일 실시예에서, 본 발명의 방법은 제1 텔레커뮤니케이션 장치와 제2 텔레커뮤니케이션 장치 간의 텔레커뮤니케이션 세션을 연결을 통해 설정하는 단계를 포함한다. 제1 텔레커뮤니케이션 장치와 제2 텔레커뮤니케이션 장치는 제3 컴퓨팅 디바이스를 관통하지 않고 텔레커뮤니케이션 세션을 통해 통신한다.

본 발명의 다른 실시예에서, 본 방법은 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 연결을 통해 원격 디스플레이 프로토콜을 통신한다. 원격 데스크톱 프로토콜은 개별적 컴퓨팅 아키텍처 프로토콜 또는 원격 데스크톱 프로토콜 중 하나를 포함한다. 또 다른 실시예에서, 제1 컴퓨팅 디바이스의 스크린 뷰를 연결을 통해 제2 컴퓨팅 디바이스와 공유하는 단계를 포함한다.

일 형태에서, 본 발명은 제1 네트워크 상의 제1 컴퓨팅 디바이스와 제2 네트워크 상의 제2 컴퓨팅 디바이스 간의 피어투피어 통신 세션을 설정하기 위해 게이트웨이에서 실행되는 방법에 관한 것이다. 제1 네트워크는 제2 네트워크와 분리되어 라우트 가능하지 않다. 이 방법은 제1 네트워크 상의 제1 컴퓨팅 디바이스와의 제1 터널링 세션을 설정하는 단계와, 제2 네트워크 상의 제2 컴퓨팅 디바이스와의 제2 터널링 세션을 설정하는 단계를 포함한다. 게이트웨이는 제2 컴퓨팅 디바이스와의 통신 세션을 초기화하는 제1 컴퓨팅 디바이스에 의한 요청을 수신한다. 제2 컴퓨팅 디바이스와 접촉하기 위해 제1 컴퓨팅 디바이스에 제1 네트워크 주소를 제공한다. 제1 네트워크 주소는 제2 터널링 세션과 관련된 제2 컴퓨팅 디바이스의 네트워크 주소를 포함한다. 게이트웨이는 제1 네트워크 주소를 이용하여 제2 컴퓨팅 디바이스와의 연결을 초기화하는 제1 컴퓨팅 디바이스에 의한 요청을 수신하고, 연결을 초기화하는 요청을 인터셉트하여, 제2 컴퓨팅 디바이스에 대한 제2 네트워크 주소를 제1 컴퓨팅 디바이스에 제공한다. 제2 네트워크 주소는 제2 컴퓨팅 디바이스와 관련된 공중 네트워크 주소를 포함한다. 게이트웨이는 방화벽을 관통하는 스위머 세션을 통해서와 같이, 제2 네트워크 주소를 이용하여 제1 컴퓨팅 디바이스로부터 제2 컴퓨팅 디바이스로의 연결을 허용하는 요청을 제2 컴퓨팅 디바이스에게 통신한다.

일 실시예에서, 제1 터널링 세션 또는 제2 터널링 세션은 보안 소켓 계층 또는 가상 사설망을 포함한다. 다른 실시예에서, 제2 컴퓨팅 디바이스는 제2 네트워크 주소와 관련된 방화벽 뒤에 위치된다. 다른 실시예에서, 본 발명의 방법은 제1 터널링 세션을 통해 제1 컴퓨팅 디바이스에 대역외 신호를 통신하여 제1 컴퓨팅 디바이스에 제2 네트워크 주소를 제공하는 단계를 포함한다. 부가하여 게이트웨이는 제1 컴퓨팅 디바이스 및 제2 컴퓨팅 디바이스에 키를 통신한다.

다른 형태에서, 본 발명은 제1 네트워크 상의 제1 컴퓨팅 디바이스와 제2 네트워크 상의 제2 컴퓨팅 디바이스 간의 피어투피어 통신 세션을 제3 컴퓨팅 디바이스를 통해 설정하기 위한 시스템에 관한 것이다. 제1 네트워크는 제2 네트워크와 분리되어 라우트 가능하지 않는다. 시스템은 제1 네트워크 상의 제1 컴퓨팅 디바이스와, 제2 네트워크 상의 제2 컴퓨팅 디바이스를 포함한다. 제3 컴퓨팅 디바이스는 제1 컴퓨팅 디바이스와의 제1 터널링 세션과 제2 컴퓨팅 디바이스와의 제2 터널링 세션을 설정한다. 시스템은 EH한 제3 컴퓨팅 디바이스를 통해 액세스 가능한 서버를 포함한다. 시스템의 동작시, 서버는 제3 컴퓨팅 디바이스를 통해 제1 컴퓨팅 디바이스에 제2 터널링 세션과 관련되는 제2 컴퓨팅 디바이스의 네트워크 주소를 포함하는 제1 네트워크 주소를 통신한다. 제1 컴퓨팅 디바이스는 제1 네트워크 주소를 이용하여 제2 컴퓨팅 디바이스와의 연결을 초기화하려는 제1 요청을 제3 컴퓨팅 디바이스를 통해 통신한다. 제3 컴퓨팅 디바이스는 제1 요청을 인터셉트하고, 제1 컴퓨팅 디바이스에 제2 컴퓨팅 디바이스에 대한 제2 네트워크 주소를 제공하고, 제2 네트워크 주소는 제2 컴퓨팅 디바이스와 관련된 공중 네트워크 주소를 포함한다. 제3 컴퓨팅 디바이스는 제2 네트워크 주소를 이용하여 제1 컴퓨팅 디바이스로부터의 연결을 허용하는 제2 요청을 제2 컴퓨팅 디바이스에 통신한다.

시스템의 일 실시예로, 제1 터널링 세션 또는 제2 터널링 세션은 보안 소켓 계층 또는 가상 사설망을 포함한다. 더욱, 제3 컴퓨팅 디바이스는 SSL VPN 게이트웨이와 같은, 원격 액세스 게이트웨이를 포함한다. 시스템의 다른 실시예로, 제2 컴퓨팅 디바이스는 제2 네트워크 주소와 관련된 방화벽 뒤에 위치된다.

본 발명의 부가의 실시예에서, 제3 컴퓨팅 디바이스는 대역외 TLS 세션을 통해서와 같이, 제1 터널링 세션을 통해 대역외 신호를 통신하여 제1 컴퓨팅 디바이스에 제2 네트워크 주소를 제공한다. 일 실시예에서, 제2 컴퓨팅 디바이스는 제1 컴퓨팅 디바이스가 제2 네트워크 주소를 이용하여 제2 컴퓨팅 디바이스에 통신하도록 방화벽에 포워드 홀을 제공한다.

본 발명의 시스템의 다른 실시예로, 제3 컴퓨팅 디바이스는 제1 컴퓨팅 디바이스 및 제2 컴퓨팅 디바이스에 키를 통신한다. 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스는 제2 컴퓨팅 디바이스에 키를 통신한다. 부가하여, 제1 컴퓨팅 디바이스는 제2 컴퓨팅 디바이스로부터 수신된 키가 제2 컴퓨팅 디바이스에 데이터를 전송하기 전에 제1 컴퓨팅 디바이스의 키와 일치하는지를 체크한다.

본 발명의 몇 실시예에서, 시스템은 제1 컴퓨팅 디바이스와 관련되는 제1 텔레커뮤니케이션 장치 및 제2 컴퓨팅 디바이스와 관련되는 제2 텔레커뮤니케이션 장치를 포함한다. 제1 텔레커뮤니케이션 장치나 제2 텔레커뮤니케이션은 하드 또는 소프트 VoIP 전화와 같은 소프트웨어 컴포넌트나 하드웨어 컴포넌트를 포함한다. 일 실시예에서, 본 발명의 시스템은 제1 텔레커뮤니케이션 장치는 제2 텔레커뮤니케이션 장치와의 텔레커뮤니케이션 세션을 연결을 통해 설정한다. 제1 텔레커뮤니케이션 장치는 제3 컴퓨팅 디바이스를 관통하지 않고 텔레커뮤니케이션 세션을 통해 제2 텔레커뮤니케이션 장치와 통신한다.

본 발명의 다른 실시예에서, 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스는 연결을 통해 원격 디스플레이 프로토콜을 통신한다. 원격 데스크톱 프로토콜은 개별적 컴퓨팅 아키텍쳐 프로토콜 또는 원격 데스크톱 프로토콜을 포함한다. 또 다른 실시예에서, 제1 컴퓨팅 디바이스는 연결을 통해 제2 컴퓨팅 디바이스와 스크린 뷰를 공유한다.

다른 형태로, 본 발명은 손실 프로토콜을 통해 전송하게 구성된 패킷을 무손실 프로토콜을 통해 통신하기 위한 방법에 관한 것이다. 본 방법은 적당한 수단과 메커니즘에 의해 시스템에서와 같이 하나 이상의 전자 장치에서 실행될 수 있다. 이 방법은 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 연결을 무손실 프로토콜을 통해 설정하는 단계를 포함한다. 몇 실시예에서, 제2 컴퓨팅 디바이스는 SSL VPN 게이트웨이와 같은 게이트웨이일 수 있다. 제1 컴퓨팅 디바이스는 손실 프로토콜에 따라 구성된 하나 이상의 패킷을 갖는 페이로드를 포함하는 무손실 프로토콜 패킷을 검출한다. 제1 컴퓨팅 디바이스는 제1 컴퓨팅 디바이스 또는 제2 컴퓨팅 디바이스 중 하나에 무손실 프로토콜 패킷의 수신의 이상 확인을 통신한다. 무손실 프로토콜 패킷의 수신 이상 확인은 무손실 프로토콜의 신뢰성 알고리즘과 메커니즘의 이용을 방지한다. 제1 컴퓨팅 디바이스는 무손실 프로토콜 패킷을 제2 컴퓨팅 디바이스에 통신한다. 몇 실시예에서, 무손실 프로토콜 패킷의 수신의 이상 확인은 무손실 프로토콜 패킷의 통신 이전에 통신된다.

일 실시예에서, 본 방법의 방법은 제1 컴퓨팅 디바이스에 의해, 키를 이용하여 하나 이상의 패킷을 암호화하는 단계를 포함한다. 몇 실시예에서, 암호화키는 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 대역외 전송 보안 계층 세션을 통해 제1 컴퓨팅 디바이스에 제공될 수 있다. 다른 실시예에서, 본 방법은 하나 이상의 패킷을 패킷 마다에 기초하여 암호화한다.

본 발명의 방법의 다른 실시예에서, 제1 컴퓨팅 디바이스 및/또는 제2 컴퓨팅 디바이스는 무손실 프로토콜 패킷의 수신의 이상 확인을 수신한 것에 응답하여, 제1 컴퓨팅 디바이스 또는 제2 컴퓨팅 디바이스 중 하나의 네트워크 스택이 무손실 프로토콜의 무손실 특성을 제공하는 것과 관련하는 동작을 실행하는 것을 방지한다. 일 실시예에서, 무손실 프로토콜은 전송 제어 프로토콜을 포함한다.

다른 실시예에서, 본 발명의 방법은 제1 컴퓨팅 디바이스 또는 제2 컴퓨팅 디바이스 중 하나의 네트워크 스택이 무손실 프로토콜과 관련하여 1) 재전송, 2) 오더링, 3) 흐름 제어 알고리즘, 4) 네이플의 알고리즘 및 5) 슬라이딩 윈도우 알고리즘 중 하나 이상을 실행하는 것을 방지한다.

일 실시예에서, 무손실 프로토콜은 유저 데이터그램 프로토콜을 포함한다. 다른 실시예에서, 본 방법은 제1 컴퓨팅 디바이스에 의해 보안 소켓 계층이나 전송 보안 계층 터널 중 하나를 통해 무손실 프로토콜 패킷을 제2 컴퓨팅 디바이스에 통신하는 단계를 포함한다.

다른 실시예에서, 하나 이상의 패킷은 실시간 프로토콜을 포함한다. 부가의 실시예에서, 이 방법은 제1 컴퓨팅 디바이스에 의해 하나 이상의 패킷을 통해 실시간 음성, 오디오 또는 데이터 중 하나를 제2 컴퓨팅 디바이스에 통신하는 단계를 포함한다.

일 형태에서, 본 발명은 TCP 연결을 통한 비신뢰성 전송 프로토콜을 이용하여 애플리케이션으로부터 패킷을 전송하기 위한 방법에 관한 것이다. 이 방법은 제1 디바이스에서 비신뢰성 전송 프로토콜을 이용하여 전송되는 제1 패킷을 수신하는 단계와, 수신된 제1 패킷의 제1 페이로드 및 제1 디바이스와 제2 디바이스 간에 설정된 TCP 연결과 관련되는 정보의 제1 TCP 헤더를 포함하는 제1 TCP 패킷을 형성하는 단계를 포함한다. 제1 디바이스는 제1 TCP 패킷을 제2 디바이스에 전송한다. 이 방법은 또한 제1 디바이스에서, 비신뢰성 전송 프로토콜을 이용하여 전송되는 제2 패킷을 수신하는 단계와, 수신된 제2 패킷의 제2 페이로드 및 제1 TCP 헤더 정보를 포함하는 제2 TCP 패킷을 형성하는 단계를 포함한다. 제1 디바이스는 제2 디바이스로부터의 제1 페이로드의 수신 확인의 수신 이전에, 제2 TCP 패킷을 제2 디바이스에 전송한다.

일 실시예에서, 본 발명의 방법은 비신뢰 전송 프로토콜과 관련되는 포트 번호로 TCP 연결을 설정하다. 다른 실시예에서, 본 방법은 제1 디바이스에 의해, 제1 TCP 패킷과 제2 TCP 패킷이 비신뢰성 전송 프로토콜을 포함하는지를 동적으로 판정한다.

부가의 실시예에서, 본 방법은 제1 TCP 패킷과 제2 TCP 패킷을 패킷 캡처링 메커니즘을 이용하여 인터셉트함으로써 제1 디바이스 상의 제1 TCP 패킷과 제2 TCP 패킷을 수신하는 단계를 포함한다. 몇 실시예에서, 이 방법은 제1 디바이스에 의해, VPN 게이트웨이 장치와의 TCP 연결을 설정한다. 다른 실시예에서, 이 방법은 TCP 연결을 통해 제1 디바이스와 제2

디바이스 간의 피어투피어 통신을 설정하는 단계를 포함한다. 본 발명의 다른 실시예에서, 이 방법은 제1 디바이스에 의해, 제1 및 제2 TCP 패킷을 암호화하고, 제2 디바이스에 의해 암호화된 제1 및 제2 TCP 패킷을 복호하는 단계를 포함한다.

다른 형태에서, 본 발명은 TCP 연결을 통해 비신뢰성 전송 프로토콜을 이용하여 애플리케이션으로부터 패킷을 전송하기 위한 방법에 관한 것이다. 이 방법은 제2 디바이스에서, 제1 디바이스에서 형성되어 제2 디바이스에서 수신되는 제1 TCP 패킷을 인터셉트하는 단계를 포함한다. 제1 TCP 패킷은 비신뢰성 프로토콜을 이용하여 애플리케이션에 의해 형성된 제1 패킷의 제1 페이로드 및 제1 디바이스와 제2 디바이스 간에 설정된 TCP 연결과 관련된 정보의 제1 TCP 헤더를 포함한다. 본 방법의 인터셉트하는 단계는 제1 TCP 패킷이 제2 디바이스에서 TCP 스택에 제공되기 전에 발생한다. 이 방법은 TCP 헤더의 정보에 응답하여, 제1 페이로드가 비신뢰 전송 프로토콜을 이용하여 애플리케이션에 의해 형성된 패킷인 것을 식별하는 단계와, 제1 TCP 패킷으로부터 TCP 헤더의 정보를 분리하는 단계와, 비신뢰성 데이터 프로토콜을 이용하여 애플리케이션에 제1 페이로드를 전달하는 단계를 포함한다.

일 실시예에서, 비신뢰성 프로토콜은 UDP이다. 다른 실시예에서, 식별 단계는 TCP 헤더 정보가 비신뢰성 전송 프로토콜과 관련된 포트 번호를 포함하는 것을 식별하는 단계를 포함한다. 몇 실시예에서, 이 방법은 제2 디바이스에 의해, 패킷 캡쳐 드라이버를 이용하여 제1 TCP 패킷을 인터셉트하는 단계를 포함한다.

몇 실시예에서, 제1 디바이스는 클라이언트 디바이스이고 제2 디바이스는 VPN 게이트웨이이다. 부가하여, 본 발명의 방법은 제1 페이로드를 애플리케이션에 전달하기 전에 제2 디바이스에서 네트워크 주소 변환 (NAT)를 실행하는 단계를 포함한다.

다른 형태에서, 본 발명은 TCP 연결을 통해 비신뢰성 전송 프로토콜을 이용하여 애플리케이션으로부터 패킷을 전송하기 위한 시스템에 관한 것이다. 시스템은 제1 디바이스와 제2 디바이스를 포함한다. 제1 디바이스는 제1 및 제2 패킷을 형성하는 애플리케이션을 갖는다. 제1 및 제2 패킷은 비신뢰성 전송 프로토콜을 이용하여 전송되는 것이다. 제1 디바이스는 또한 필터 프로세스 및 터널링 프로세스를 갖는다. 필터 프로세스는 제1 및 제2 패킷을 애플리케이션으로부터 인터셉트하여 인터셉트된 패킷을 터널 프로세스로 전달한다. 터널 프로세스는 제1 디바이스와 제2 디바이스 간의 TCP 연결의 개방을 요청한다. TCP 연결의 개방 요청은 TCP 연결이 비신뢰성 전송 프로토콜로 전송되려고 하는 패킷을 전송하게 되는 것을 제1 및 제2 디바이스에게 지시한다. 터널 프로세스는 제1 및 제2 TCP 패킷의 페이로드로서 제1 및 제2 패킷을 제2 디바이스에 전달한다. 터널 프로세스는 제1 TCP 패킷을 전송한 후와 제1 TCP 패킷에 대한 확인을 수신하기 전에 제2 TCP 패킷을 전송한다.

본 발명의 이 시스템의 제2 디바이스는 제1 디바이스와 통신한다. 제2 디바이스는 제2 필터 프로세스와 터널링 프로세스를 갖는다. 제2 터널 프로세스는 제1 디바이스에 의해 요청되는 TCP 연결을 개방하고, 제2 필터 프로세스에 대한 TCP 연결의 소스 주소를 식별하여 전달한다. 제2 필터 프로세스는 제2 디바이스에서 수신된 애플리케이션으로부터의 패킷을 헤더의 TCP 연결 소스 주소로 인터셉트한다. 제2 필터 프로세스는 수신된 패킷으로부터 TCP 헤더를 분리하여 분리된 패킷을 전달하고, 제2 디바이스 상서의 TCP/IP 스택을 의도한 목적지로 보낸다.

본 발명의 시스템의 일 실시예에서, 제1 디바이스 상의 필터 프로세스와 제2 디바이스 상의 제2 필터 프로세스는 패킷 캡쳐 드라이버이다. 몇 실시예에서, 제1 디바이스는 클라이언트 디바이스이고 제2 디바이스는 VPN 게이트웨이 디바이스이다. 일 실시예에서, 비신뢰 데이터 프로토콜은 UDP이다.

다른 실시예에서, 시스템은 분리된 패킷이 전송되는 제3 디바이스를 더 포함한다. 부가하여, 제2 디바이스는 분리된 패킷을 제3 디바이스로 전송하기 전에 네트워크 주소 변환을 실행하는 데에 이용되는 네트워크 주소 변환 (NAT) 테이블을 더 포함한다.

다른 형태에서, 본 발명은 네트워크 단편화를 줄이도록 보안 네트워크 통신의 최대 전송 단위를 조정하기 위한 방법에 관한 것이다. 이 방법은 적당한 수단과 메커니즘에 의해서 시스템에서와 같은 하나 이상의 전자 장치에서 실행될 수 있다. 이 방법은 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 세션을 설정하는 단계를 포함한다. 세션은 제1 컴퓨팅 디바이스의 에이전트에 의해 설정된다. 제1 컴퓨팅 디바이스는 제1 네트워크 스택을 갖는다. 이 방법은 제1 컴퓨팅 디바이스에 의해 암호화된 페이로드를 갖는 네트워크 패킷을 검출하고, 제1 컴퓨팅 디바이스에 의해 최대 전송 단위 크기를 페이로드의 암호화된 부분과 관련된 최소한의 크기만큼 줄이도록 제1 네트워크 스택의 최대 전송 단위 파라미터에 대한 세팅을 결정한다. 이 방법은 제1 네트워크 스택의 최대 전송 단위 파라미터를 결정된 세팅으로 변경한다. 이와 같이, 보고된 MTU 파라미터는 암호화를 고려하여 감소되게 된다.

일 실시예에서, 본 발명의 방법은 네트워크 패킷을 보안 소켓 계층이나 전송 계층 보안 터널 중 하나를 통해 제2 컴퓨팅 디바이스에 통신하는 단계를 포함한다. 제2 컴퓨팅 디바이스는 SSL VPN 게이트웨이와 같은 게이트웨이일 수 있다. 다른 실시예에서, 페이로드는 실시간 프로토콜을 포함한다.

부가하여, 일 실시예에서, 이 방법은 제1 네트워크 스택의 네트워크 드라이버 인터페이스 사양 레벨 메커니즘을 통해 최대 전송 단위 파라미터를 변경하는 단계를 더 포함한다. 다른 실시예에서, 이 방법은 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 세션 당 최대 전송 단위 파라미터의 세팅을 동적으로 결정한다. 일 실시예에서, 제1 컴퓨팅 디바이스의 에이전트는 최대 전송 단위 파라미터를 결정된 설정치로 변경하기 위해서, IOCTL 애플리케이션 프로그래밍 인터페이스를 통해 제1 네트워크 스택에 통신한다.

몇 실시예에서, 본 발명의 방법은 제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간의 세션을 게이트웨이를 통해 설정한다. 다른 실시예에서, 이 방법은 제1 컴퓨팅 디바이스에 의해 네트워크 패킷의 페이로드를 통해 실시간 음성, 오디오 또는 데이터 중 하나를 제2 컴퓨팅 디바이스에 통신한다. 또 다른 실시예에서, 이 방법은 네트워크 패킷을 통신하기 전에 제1 컴퓨팅 디바이스 또는 제2 컴퓨팅 디바이스 중 하나에 네트워크 패킷의 수신의 이상 확인을 통신한다. 일 실시예에서, 네트워크 패킷은 전송 제어 프로토콜과 같은 무손실 프로토콜 패킷을 포함한다. 다른 실시예에서, 페이로드는 유저 데이터그램 프로토콜과 같은 손실 프로토콜 패킷을 포함한다.

부가의 형태로, 본 발명은 클라이언트가 클라이언트의 애플리케이션과 관련된 클라이언트의 네트워크 통신을 우선 순위화하는 방법에 관한 것이다. 이 방법은 클라이언트에 의해, 클라이언트의 하나 이상의 애플리케이션과 관련된 하나 이상의 네트워크 패킷을 인터셉트하는 단계와 하나 이상의 네트워크 패킷을 큐에 저장하는 단계를 포함한다. 클라이언트는 큐된 하나 이상의 네트워크 패킷이 클라이언트의 제1 애플리케이션과 관련되지를 판단한다. 클라이언트는 클라이언트의 제2 애플리케이션과 관련된 큐에 판단된 하나 이상의 네트워크 패킷을 적어도 하나의 네트워크 패킷 보다 우선하여 위치시키도록 판단된 하나 이상의 네트워크 패킷에 대한 우선 순위를 나타낸다. 클라이언트는 클라이언트의 네트워크 스택에 의한 통신을 위해 우선 순위된 하나 이상의 네트워크 패킷을 제공한다.

일 실시예에서, 본 발명의 방법은 클라이언트에 의해 제1 애플리케이션의 큐된 하나 이상의 네트워크 패킷이 실시간 데이터를 포함한다고 판단하는 단계를 더 포함한다. 실시간 데이터는 1) 실시간 프로토콜, 2) 유저 데이터그램 프로토콜, 및 3) 음성이나 오디오 중 하나의 표시중 하나를 포함한다.

다른 실시예에서, 본 발명은 클라이언트에 의해 제2 애플리케이션의 적어도 하나의 네트워크 패킷이 제1 애플리케이션의 하나 이상의 네트워크 패킷 보다 우선하여 네트워크 스택을 통해 통신되지 않도록 방지하는 단계를 포함한다. 다른 실시예에서, 본 발명은 클라이언트에 의해, 제2 애플리케이션과 관련된 네트워크 패킷을 유지하는 단계와 유지된 네트워크 패킷을 유지된 네트워크 패킷 보다 우선으로 순위된 제1 애플리케이션과 관련된 하나 이상의 네트워크 패킷의 통신시 해제하는 단계를 포함한다.

본 발명의 또 다른 실시예에서, 본 발명은 클라이언트에 의해, 하나 이상의 네트워크 패킷을 클라이언트 상의 하나 이상의 애플리케이션에 투명하게 인터셉트하는 단계를 포함한다. 몇 실시예에서, 제1 애플리케이션은 포그라운드에서, 제2 애플리케이션은 백그라운드에서 실행된다.

본 발명의 일 실시예에서, 본 발명은 제1 애플리케이션과 관련된 우선 순위를 제2 애플리케이션과 관련된 우선 순위보다 더 높게 하는 단계를 포함한다. 다른 실시예에서, 유저는 제1 애플리케이션 또는 제2 애플리케이션 중 하나의 우선 순위을 특정한다. 다른 실시예에서, 클라이언트는 하나 이상의 네트워크 패킷을 컴퓨팅 디바이스로부터 수신한다. 또한, 하나 이상의 애플리케이션은 하나 이상의 네트워크 패킷을 클라이언트로부터 컴퓨팅 디바이스로 통신하기 위해 제공한다.

다른 형태로, 본 발명은 클라이언트의 애플리케이션과 관련된 클라이언트의 네트워크 통신을 우선 순위화하기 위한 클라이언트에 관한 것이다. 클라이언트는 클라이언트의 하나 이상의 애플리케이션과 관련된 클라이언트의 하나 이상의 네트워크 패킷을 인터셉트하기 위한 메커니즘을 포함한다. 클라이언트는 또한 하나 이상의 네트워크 패킷을 큐에 저장하고 하나 이상의 네트워크 패킷을 클라이언트의 네트워크 스택을 거쳐 통신하기 위한 네트워크 드라이버를 포함한다. 클라이언트는 또한 하나 이상의 네트워크 패킷이 클라이언트의 제1 애플리케이션과 관련되었는지를 판정하여, 판단된 하나 이상의 네트워크 패킷을 적어도 하나의 네트워크 패킷 보다 우선하여 위치시키도록 판단된 하나 이상의 네트워크 패킷에 대한 우선 순위를 네트워크 드라이버에게 나타내기 위한 에이전트를 포함한다.

일 실시예에서, 본 발명의 에이전트는 제1 애플리케이션의 하나 이상의 네트워크 패킷이 실시간 데이터를 포함한다고 판정한다. 실시간 데이터는 1) 실시간 프로토콜, 2) 유저 데이터그램 프로토콜, 및 3) 음성이나 오디오 중 하나의 표시중 하나를 포함한다.

다른 실시예에서, 본 발명의 에이전트나 네트워크 드라이버는 제2 애플리케이션의 적어도 하나의 네트워크 패킷이 제1 애플리케이션의 하나 이상의 네트워크 패킷 보다 우선하여 네트워크 스택을 통해 통신되지 않도록 방지한다. 일 실시예에서, 네트워크 드라이버는 제2 애플리케이션과 관련된 네트워크 패킷을 큐에 유지하고 유지된 네트워크 패킷을 유지된 네트워크 패킷 보다 우선으로 순위된 제1 애플리케이션과 관련된 하나 이상의 네트워크 패킷의 통신시 해제한다.

다른 실시예에서, 본 발명은 메커니즘에 의해 하나 이상의 네트워크 패킷을 클라이언트 상의 하나 이상의 애플리케이션에 투명하게 인터셉트한다. 몇 실시예에서, 제1 애플리케이션은 포그라운드에서, 제2 애플리케이션은 백그라운드에서 실행된다. 또한, 제1 애플리케이션은 제2 애플리케이션과 관련된 우선 순위보다 더 높다, 더욱, 클라이언트는 유저가 우선 순위를 특정하도록 하는 컨피규레이션 메커니즘을 포함한다. 몇 실시예에서, 클라이언트는 하나 이상의 네트워크 패킷을 컴퓨팅 디바이스로부터 수신한다. 다른 실시예에서, 하나 이상의 애플리케이션은 하나 이상의 네트워크 패킷을 클라이언트로부터 컴퓨팅 디바이스로 통신하기 위해 제공한다.

부가의 실시예에서, 네트워크 드라이버는 네트워크 드라이버 인터페이스 사양 (NDIS) 드라이버를 포함한다. 또한, 네트워크 드라이버는 클라이언트의 운영 시스템의 커널 모드에서 동작한다. 몇 경우, 에이전트는 클라이언트의 운영 시스템의 유저 모드에서 동작한다. 더욱, 에이전트나 네트워크 드라이버는 클라이언트의 하나 이상의 네트워크 패킷을 인터셉트하기 위한 메커니즘을 포함한다.

또 다른 형태에서, 본 발명은 제1 프로토콜을 통해 설정된 세션을 네트워크 붕괴로부터 차단하기 위한 방법에 관한 것이다. 이 방법은 클라이언트의 에이전트에 의해, 클라이언트와 디바이스 간의 네트워크 연결에 의한 제1 프로토콜을 통한 세션을 설정하는 단계를 포함한다. 네트워크 연결은 네트워크 스택과 관련된다. 제1 네트워크 스택의 제1 부분은 제1 프로토콜의 층 아래의 네트워크 스택의 하나 이상의 층을 포함하고, 네트워크 스택의 제2 부분은 제1 프로토콜에 대한 층과 제1 프로토콜 위의 네트워크 스택의 하나 이상의 층을 포함한다. 이 방법은 네트워크 스택의 제1 부분이 폐지되게 하는 제1 네트워크 연결의 붕괴를 검출하는 단계와, 에이전트에 의해 붕괴 동안 세션 및 네트워크 스택의 제2 부분을 유지하는 단계를 포함한다. 이 방법은 또한 세션 및 네트워크 스택의 제2 부분을 유지하면서 상기 네트워크 스택의 제2 부분 및 네트워크 연결을 재설정하는 단계를 포함한다.

일 실시예에서, 이 방법은 네트워크 스택의 유지된 제2 부분과 네트워크 스택의 재설정된 제1 부분으로 세션을 계속하는 단계를 더 포함한다. 몇 실시예에서, 이 방법은 네트워크 스택의 제2 부분에 의해 붕괴 동안 네트워크 패킷의 수신을 중단시키는 단계를 더 포함한다.

다른 실시예에서, 이 디바이스는 원격 액세스 게이트웨이나 컴퓨팅 디바이스 중 하나를 포함한다. 몇 경우, 이 방법은 세션을 1) 보안 소켓층 (SSL) 프로토콜, 2) 전송층 보안 (TLS) 프로토콜 및 3) 터널링 프로토콜 중 하나의 제1 프로토콜을 통해 설정하는 단계를 포함한다. 부가하여, 본 발명의 방법은 에이전트에 의해 클라이언트와 디바이스 간의 세션을 통해 실시간 데이터를 통신하는 단계를 포함한다. 실시간 데이터는 실시간 프로토콜을 포함하거나, 실시간 데이터는 음성이나 오디오를 나타낼 수 있다.

몇 실시예에서, 에이전트는 클라이언트의 운영 시스템의 유저 모드에서 동작한다. 일 실시예에서, 네트워크의 제1 부분은 전송 제어 프로토콜이나 인터넷 프로토콜 중 하나를 포함한다. 다른 실시예에서, 네트워크 스택의 제2 부분은 1) 인터넷 프로토콜, 2) 유저 데이터그램 프로토콜 또는 3) 음성 전면 인터넷 프로토콜 중 하나를 포함한다. 부가하여, 클라이언트는 원격 디스플레이 프로토콜을 통해 디바이스와 통신한다. 원격 디스플레이 프로토콜은 인디펜던트 컴퓨팅 아키텍쳐 프로토콜이나 원격 데스트톱 프로토콜일 수 있다.

다른 실시예에서, 본 발명의 방법은 네트워크 연결을 통해 통신하는 클라이언트의 애플리케이션에 투명하게 실행된다. 일 실시예에서, 이 방법은 에이전트에 의해 애플리케이션과 관련된 하나 이상의 네트워크 패킷을 클라이언트의 애플리케이션에 대해 투명하게 인터셉트하는 단계를 포함한다. 일 실시예에서, 이 방법은 스택의 제2 부분과 관련된 네트워크 드라이버에 의해 애플리케이션과 관련된 하나 이상의 네트워크 패킷을 클라이언트 상의 애플리케이션에 투명하게 인터셉트하는 단계를 포함한다.

부가의 형태로, 본 발명은 제1 프로토콜을 통해 설정된 세션을 네트워크 붕괴로부터 차단하기 위한 시스템에 관한 것이다. 시스템은 제1 프로토콜을 통한 네트워크 연결로 클라이언트와 디바이스 간의 연결을 설정하는 클라이언트의 에이전트를 갖는다. 시스템은 제1 부분과 제2 부분을 갖는 네트워크 스택을 포함한다. 네트워크 스택의 제1 부분은 제1 프로토콜의 층 아래의 네트워크 스택의 하나 이상의 층을 포함하고, 네트워크 스택의 제2 부분은 제1 프로토콜에 대한 층과 제1 프로토콜 위의 네트워크 층의 하나 이상의 층을 포함한다. 시스템은 네트워크 스택의 제2 부분이 폐지되게 하는 네트워크 연결의 붕괴를 검출하기 위한 검출기를 포함한다. 시스템의 동작 및 검출기에 의한 붕괴의 검출시, 에이전트는 붕괴 동안 세션과 네트워크 스택의 제2 부분을 유지한다. 클라이언트는 에이전트가 세션과 네트워크 스택의 제2 부분을 유지하는 동안 네트워크 스택의 제1 부분과 네트워크 연결을 재설정한다.

본 발명의 시스템의 일 실시예에서, 에이전트는 네트워크 스택의 유지된 제2 부분과 네트워크 스택의 재설정된 제1 부분으로 세션을 계속한다. 몇 실시예에서, 네트워크 스택의 제1 부분이나 제2 부분 중 하나는 붕괴 동안 네트워크 패킷의 수신을 중단시킨다.

일 실시예에서, 시스템의 디바이스는 원격 액세스 게이트웨이나 컴퓨팅 디바이스이다. 본 발명의 시스템에 의해 이용되는 제1 프로토콜은 1) 보안 소켓층 (SSL) 프로토콜, 2) 전송층 보안 (TLS) 프로토콜 및 3) 터널링 프로토콜 중 하나를 포함한다. 다른 실시예에서, 에이전트는 클라이언트와 디바이스 간의 세션을 통해 실시간 데이터를 통신한다. 실시간 데이터는 실시간 프로토콜 또는 음성이나 오디오의 표시를 포함한다.

시스템의 몇 실시예에서, 에이전트는 클라이언트의 운영 시스템의 유저 모드에서 동작한다. 일 시스템의 실시예에서, 네트워크의 제1 부분은 전송 제어 프로토콜 및/또는 인터넷 프로토콜이다. 다른 실시예에서, 네트워크 스택의 제2 부분은 1) 인터넷 프로토콜, 2) 유저 데이터그램 프로토콜 또는 3) 음성 전면 인터넷 프로토콜 중 하나를 포함한다. 부가하여, 클라이언트는 인디팬던트 컴퓨팅 아키텍쳐 (ICA) 프로토콜이나 원격 데스크톱 프로토콜 (RDP)일 수 있는 원격 디스플레이 프로토콜을 통해 디바이스와 통신한다.

다른 실시예에서, 본 발명의 시스템은 네트워크 스택의 제2 부분을 유지하고 네트워크 스택의 제1 부분을 네트워크 연결을 통해 통신하는 클라이언트의 애플리케이션에 대해 투명하게 재설정한다. 일 실시예에서, 에이전트는 클라이언트의 애플리케이션의 하나 이상의 네트워크 패킷을 클라이언트 애플리케이션에 대해 투명하게 인터셉트한다. 일 실시예에서, 시스템은 또한 스택의 제2 부분과 관련된 네트워크 드라이버에 의해 클라이언트의 애플리케이션의 하나 이상의 네트워크 패킷을 애플리케이션에 대해 투명하게 인터셉트한다.

본 발명의 여러 실시예의 상세 사항은 첨부한 도면과 이하 설명에 기재된다.

실시예

본 발명의 특정한 설명적 실시예를 이하 기재한다. 그러나, 본 발명은 이들 실시예에만 제한되는 것은 아니고, 여기 기재된 것의 부가와 수정들이 모두 본 발명의 영역 내에 포함되는 것임에 유의해야 한다. 더구나, 여기 기재된 여러 실시예들의 특성은 본 발명의 정신과 영역을 벗어나지 않고 상호 배타적이지 않으며 여러 조합과 교환으로 존재할 수 있지만, 여기에서 명백히 나타내지는 않았다.

본 발명의 설명적 실시예는 피어투피어 통신과 원격 액세스 연결을 제공하기 위한 원격 액세스 아키텍쳐에 관한 것이다. 일 실시예에서, 본 발명의 원격 액세스 아키텍처는 게이트웨이와 같은 제3자 컴퓨팅 디바이스를 통해 피어 컴퓨팅 디바이스간의 직접적인 연결을 설정하기 위한 방법을 제공한다. 피어투피어 통신은 음성 전면 인터넷 프로토콜 (VoIP) 시그널링과 매체, 비디오, 및 그 외 웹 협력, 스크린이나 데스크 공유 및 인스턴스 메시징과 같은 실시간 데이터 어플리케이션과 같은 실시간 통신을 포함한다. 게이트웨이를 통한 피어투피어 연결을 설정하는 것에 부가하여 본 발명은 피어투피어 통신을 최적화하기 위해 다음의 기술을 제공한다: 1) 손실 프로토콜을 통한 전송을 위해 구성된 패킷의 무손실 프로토콜을 통한 통신을 가능하게 하는 네트워크 패킷의 수신시의 이상 확인, 2) 손실 프로토콜을 거친 전송을 위해 구성된 패킷의 무손실 프로토콜을 통한 통신을 가능하게 하는 네트워크 패킷의 패이로드 시프팅, 3) 암호화로 인한 오버헤드를 고려하여, 최대 전송 단위 (MTU) 파라미터를 조정하는 것에 의한 패킷 단편의 감소, 4) 클라이언트측 네트워크 통신의 어플리케이션 인식 우선 순위, 및 5) 모바일 컴퓨팅에 대한 것과 같이, 신뢰 가능 및 영구적 네트워크 연결성과 액세스를 위한 네트워크 붕괴 차단. 이들 기술은 몇 실시예에서 두 클라이언트 간의 피어투피어 통신에서 실시되며, 다른 실시예에서는 본 발명의 설명적 실시예의 SSL VPN 게이트웨이를 통해서와 같이 클라이언트와 게이트웨이 사이 또는 하나의 컴퓨팅 디바이스와 게이트웨이를 거쳐 다른 컴퓨팅 디바이스 간의 통신시 실행될 수 있다.

본 발명의 설명적 실시예에서, 피어투피어 루트 최적화 기술은 클라이언트가 게이트웨이를 거쳐 액세스하려고 하는 리소스에 대한 더욱 최적의 루트를 결정한다. 클라이언트와 서버나 피어 컴퓨터와 같은 클라이언트에 의해 액세스되는 리소스는 게이트웨이를 통하는 것 보다 더욱 직접적인 루트를 갖는다. 예를 들어, 클라이언트와 서버는 서로 근접하지만 게이트웨이와는 멀리 떨어져 위치되므로, 게이트웨이를 거치지 않고 서로 근접하다. 더욱, 게이트웨이를 이용하게 되면 클라이언트와 서버 간의 엔드투엔드 네트워크 통신에 적어도 하나의 부가의 홉 (hop)을 가져온다. 클라이언트와 서버 가상 사설망 (VPN) 할당 인터넷 프로코콜 (IP) 네트워크 주소를 이용하여 게이트웨이를 통해 통신하는 대신에, 본 발명의 게이트웨이와 원격 액세스 아키텍처는 게이트웨이를 이용하지 않고 피어투피어 형식으로 직접적 루트를 거쳐 클라이언트와 서버가 서로 통신하게 한다. 그러나, 어떤 경우, 클라이언트와 서버는 클라이어트 및/또는 서버가 네트워크 어드레스 트랜잭션 (NAT) 방화벽과 같은 방확벽 뒤에 있기 때문에 서로 직접적인 경로를 갖지 않을 수 있다. 본 발명의 피어투피어 루트 최적화 기술과 원격 액세스 아키텍쳐는 클라이언트와 서버가 방화벽의 횡단으로 직접적으로 통신하도록 하는 기술을 제공한다. 이와 같이, 본 발명의 피어투피어 루트 최적화 기술은 게이트웨이를 거치기 보다는 피어 컴퓨터들 간에 더욱 짧은 최적의 루트를 제공한다.

본 발명의 설명적 실시예에서, 본 발명의 실시예의 이상 확인 기술은 무손실 프로토콜을 거쳐 통신되게 구성된 패킷이 손실 프로토콜을 거쳐 통신될 수 있게 한다. 예를 들어, 실시간 프로토콜 (RTP)는 음성 전면 IP (VoIP) 통신용 유저 데이터그램 프로토콜 (UDP)를 통해 구현될 수 있다. UDP와 같은 손실 또는 비신뢰성 프로토콜은 실시간 음성 어플리케이션에서, 네트워크 패킷을 순서데로 얻거나 네트워크 패킷의 전달을 보장하는 것 보다는 수신자에게 네트워크 패킷을 제때에 보내는 것이 중요하기 때문에 음성 통신에 이용될 수 있다. 그러나, 보안 통신 및/또는 보안 소켓 계층 (SSL) 또는 전송 계층 보안 (TLS) 등의 터널링 프로토콜을 이용한 가상 사설망과 원격 액세스 솔루션을 이용하여, UDP와 같은 손실 프로토콜을 거쳐 전송되도록 구성되는 실시간 어플리케이션 데이터가 전송 컨트롤 프로토콜 (TCP)과 같은 무손실이나 신뢰 가능 프로토콜을 거쳐 통신될 수 있다. 본 발명의 기술은 무손실 프로토콜의 무손실 특성 중 하나 이상이 통신에 적용되지 않도록 하면서, RTP와 UDP와 같은 무손실 프로토콜이 TCP와 같은 무손실 프로토콜을 거쳐 통신될 수 있게 한다. 본 발명의 설명적 실시예에서, 이 기술은 무손실 프로토콜이 프로토콜의 신뢰성을 제공하는 알고리즘을 실행하는 것을 방지하기 위해 무손실 프로토콜 네트워크 패킷의 수신 이상 확인을 대응하는 네트워크 스택에 통신한다. 이 기술을 이용하여, 손실 프로토콜은 통신 보안을 위해서, TCP, SSL를 거치거나 또는 게이트웨이의 터널링 프로토콜을 거치는 것과 같이 무손실 프로토콜을 통해 통신되고, 손실 프로토콜 네트워크 패킷이 수신자에게 신뢰되게 가기 보다는 제때에 수신자에게 가게 한다. 일 실시예에서, 이 기술은 피어 간의 SSL 또는 TLS를 통해서나 게이트웨이를 통해서 VoIP와 같은 실시간 데이터 통신을 보안적으로 통신하는 데에 이용될 수 있다.

본 발명의 설명적 실시예는 손실 프로토콜을 통해 패킷이 전송되게 구성된 패킷이 무손실 프로토콜을 거쳐 통신될 수 있게 하는 다른 페이로드 시프팅 기술을 제공한다. 제1 컴퓨팅 디바이스는 비신뢰 전송 프로토콜을 이용하여 전송되는 제1 패킷을 수신하고, 수신된 제1 패킷의 제1 페이로드를 포함하는 제1 TCP 패킷을 형성한다. 제1 TCP 패킷은 제1 및 제2 컴퓨팅 디바이스 간에 설정된 TCP 연결과 관련된 정보를 갖는 TCP 헤더로 형성된다. 제1 TCP 패킷은 제2 컴퓨팅 디바이스에 전송된다. 비신뢰 전송 프로토콜을 이용하여 전송되는 제2 패킷은 제1 컴퓨팅에 의해 수신되고, 다음에 이어서 제1 TCP 패킷의 TCP 헤더 정보를 갖지 않는 수신된 제2 패킷의 페이로드를 포함하는 제2 TCP 패킷을 형성한다. 제2 TCP 패킷은 제2 장치로부터의 제1 TCP 패킷의 수신 확인을 수신하기 전에 제2 컴퓨팅 디바이스에 전송된다. 이와 같이, 페이로드 시프팅 기술은 수신 확인이 수신될 때 까지 TCP 헤더 하에서 다수의 비신뢰 전송 프로토콜 페이로드를 통신한다.

본 발명의 설명적 실시예에서, 최대 전송 단위 조정 기술은 페이로드의 암호화로 인해 네트워크 패킷 크기의 효과를 고려하기 위해 클라이언트의 네트워크 스택의 최대 전송 단위 (MTU) 파라미터의 크기를 감소시킨다. 네트워크 패킷의 페이로드의 암호화는 클라이어트에게 통신되는 네트워크 패킷의 크기를 증가시키고, 네트워크 패킷을 단편화한다. 예를 들어, 서버는 클라이언트에 대한 SSL 게이트웨이를 거쳐 클라이언트에게 네트워크 패킷을 통신할 수 있다. 서버가 클라이언트의 네트워크 스택이 처리할 수 있는 MTU 크기에 맞는 네트워크 패킷을 보내어도, 게이트웨이에 의해 제공되는 암호화는 클라이언트에게 도달하기 전에 네트워크 패킷의 크기를 증가시킨다. 이것은 암호화로 증가된 패킷 크기가 클라이언트의 MTU 크기에는 너무 크기 때문에 게이트웨이를 거쳐 서버로부터 클라이언트에게 통신되는 네트워크 패킷이 단편화되게 한다. 본 발명의 기술은 암호화의 오버헤드를 고려하기 위해 더 적은 크기를 보고하도록 클라이언트의 보고된 MTU 크기를 조정한다. 이 기술은 네트워크 단편을 감소시키거나 아니면 최적이지 않은 단편을 방지한다.

본 발명의 설명적 실시예에서, 우선 순위 기술은 네트워크 통신의 클라이언트측 어플리케이션 인식 우선 순위를 제공한다. 즉, 본 발명의 원격 액세스 클라이언트는 클라이언트측 네트워크 통신 우선 순위를 관리 제어한다. 우선 순위는 클라이언트측의 어플리케이션의 우선 순위에 기초한다. 원격 액세스 클라이언트는 클라이언트에서 실행되는 어플리케이션과 관련되는 네트워크 통신을 투명하게 인터셉트하고, 어플리케이션과 관련되는 네트워크 통신을 검출하고, 어플리케이션에 대한 우선 순위에 기초하여 네트워크 통신에 대한 우선 순위를 결정한다. 예를 들어, 클라이언트측 어플리케이션은 VoIP와 같

은 실시간 데이터 통신을 피어 클라이언트에게 또는 게이트웨이를 거쳐 통신한다. 원격 액세스 클라이언트는 네트워크 패킷을 인터셉트하고, 예를 들어, 네트워크 패킷이 실시간 데이터를 포함하거나 VoIP 어플리케이션으로부터 온 것인지를 검출한다. 원격 액세스 클라이언트는 이 네트워크 패킷에 대한 우선 순위를 나타내므로 네트워크 패킷은 비실시간 데이터 통신 이전에 또는 다른 어플리케이션으로부터의 네트워크 통신 이전에 통신될 수 있다. 이와 같이, 본 발명의 우선 순위 기술은 클라이언트에서 실행되는 어플리케이션에 기초하여 클라이언트 상의 성능, 동작 특성 및 유저 경험을 향상시키거나 증가시킨다.

본 발명의 설명적 실시예에서, 네트워크 붕괴 차단 기술은 피어투피어 통신 세션이나 게이트웨이에 대한 연결과 같이, 클라이언트의 네트워크에 대한 지속적이며 신뢰적인 연결을 제공한다. 예를 들어, 소프트웨어 기반 IP 전화를 갖는 랩톱 등의 모바일 클라이언트는 VoIP 통신용 네트워크에 연결된다. 네트워크 연결의 일시적 붕괴는 모바일 클라이언트가 동일한 네트워크에서 여러 액세스 지점 사이에서 로밍하거나, 클라이언트가 네트워크 간에서 (예를 들어, 유선망에서 무선망으로) 전환할 때 발생할 수 있다. 이는 클라이언트에 대한 네트워크 서비스를 붕괴시키고 VoIP 전화 호출을 끊기게 한다. 부가하여, 모바일 클라이언트가 액세스 지점 사이에서 이동하면, 모바일 클라이언트는 새로운 동적 호스트 컨피규레이션 프로토콜 (DHCP) 대여와 같이, 다른 IP 네트워크 주소를 취득할 수 있다. 이는 네트워크 연결성과 VoIP 전화 통신의 붕괴를 초래할 수 있다. 본 발명의 이 기술은 네트워크의 붕괴를 검출하여 네트워크 스택의 일부를 네트워크 붕괴로부터 차단한다. 이 보호된 네트워크 스택 부분은 다른 네트워크 스택의 부분이 네트워크에 재설정 및 재연결되는 동안 유지된다. 네트워크가 이용 가능하면, 본 발명은 클라이언트의 네트워크 통신이 계속된다. 몇 실시예에서, 네트워크 통신은 네트워크 붕괴 동안 큐잉되어 네트워크가 이용 가능하게 되면 전송된다. 실시간 데이터 통신과 같은 다른 실시예에서는, VoIP 전화 호출과 같은 실시간 통신에서의 레이턴시를 초래할 수 있는 네트워크 패킷의 큐잉을 방지하도록 붕괴 동안 네트워크 패킷이 끊어진다.

본 발명의 설명적 실시예가 일반적으로, 전송 컨트롤 프로토콜 (TCP) 또는 유저 데이터그램 프로토콜 (UDP)와 같은 인터넷 프로토콜 (IP) 기반의 프로토콜과 관련하여 기재되었지만, 본 발명의 기술은 시퀀스 패킷 교환 (SPX) 프로토콜을 이용하여 인터넷워크 패킷 교환 (IPX) 프로콜 기반의 네트워크와 같은 다른 네트워킹 프로토콜을 갖는 다른 유형의 네트워크 환경에서 이용될 수 있다. 또한, UDP 등의 손실이나 비신뢰 프로토콜과 TCP 등의 무손실이나 신뢰 프로토콜이 본 발명의 실시예를 설명하기 위해 이용되고 있지만, 당업자에게 잘 알려진 어느 무손실/신뢰 및 손실/비신뢰 프로토콜이라도 여기 기재된 본 발명의 동작을 실시하는 데에 이용될 수 있다. 더욱, 본 발명의 설명적 실시예가 VoIP와 같은 실시간 데이터 통신과 관련하여 기재되었지만, 본 발명의 기술은 당업자가 또한 이해하는 바와 같이 비실시간 데이터 통신에 적용될 수 있다.

부가하여, 본 발명의 설명적 실시예는 피어투피어 통신과 관련하여 기재되었다. 일 형태에서, 피어투피어 모델은 어느 컴퓨터나 다른 컴퓨터에게 그 리소스에 대한 액세스를 제공하여 서버로서, 또한 다른 컴퓨터로부터 공유 리소스를 액세스하여 클라이언트로서 둘 다 작용할 수 있는 유형의 네트워크를 포함한다. 다른 형태에서, 피어투피어 모델은 클라이언트와 서버의 개념을 포함하지 않지만, 클라이언트와 서버는 피어투피어 통신 뿐만 아니라, 클라이언트에서 클라이언트로, 서버에서 서버로, 또는 클라이언트/서버에서 게이트웨이 등의 컴퓨팅 디바이스로의 통신을 제공할 수 있다. 부가의 형태로, 피어투피어 통신은 컴퓨터들이 제3자 네트워크나 게이트웨이 등의 디바이스의 도움 없이 바로 서로 정보를 교환할 수 있도록 하는 프로세스를 포함한다. 피어투피어 통신이 컴퓨터 간의 직접적인 통신으로 기재되고 있지만, 예를 들어, 네트워크 허브와 같이, 전송 및/또는 통신을 용이하게 하는 컴퓨팅 디바이스들 사이에 다른 네트워크 요소가 있을 수 있다.

더구나, 본 발명의 설명적 실시예가 피어투피어, 포인트투포인트, 클라이언트투서버로 기재되었지만, 당업자라면 본 발명이 어느 네트워크 토폴로지를 통해 어느 방법으로나 컴퓨팅 디바이스 간에서 실행될 수 있으며, 피어투피어, 클라이언/서버의 언급이 본 발명을 어느 식으로든 제한하고자 하는 것이 아님을 이해할 것이다.

일 형태에서, 본 발명은 게이트웨이를 통해 네트워크로 또는 다른 원격 액세스 클라이언트나 다른 컴퓨팅 디바이스로 피어투피어 통신하기 위해 원격 액세스 클라이언트를 갖는 원격 액세스 아키텍처에 관한 것이다. 본 발명의 원격 액세스 아키텍처는 게이트웨이 뒤의 사설망 사이에서 공중망과 같은 외부 네트워크 상의 클라이언트에게 전송되는 네트워크 트래픽을 보안 통신하기 위한 시스템과 방법을 제공한다. 본 발명의 원격 액세스 아키텍처는 게이트웨이 상에 네트워크 주소 변환 (NAT) 기능을 제공하여 클라이언트를 사설망과 분리하는 것을 가능하게 한다. 네트워크 주소 변환 (NAT)를 이용하는 VPN 게이트웨이는 사설망이 클라이언트에 의한 직접적 계층-2 액세스로부터 차단되게 클라이언트의 가장 (masquerading) IP 주소를 제공한다.

이하 도 1A를 참조하면, 환경(180)은 본 발명의 설명적 실시예에서 원격 액세스 아키텍처를 전개하기 위한 시스템을 도시한다. 간단한 개요로, 환경(180)은 하나 이상의 네트워크 연결(341a-341n)를 거쳐 네트워크(104)에 연결되는 컴퓨팅 디바이스(102a-102c) (이하 클라이언트(105a-105c)로 언급)를 포함한다. 하나 이상의 클라이언트(105a-105n)는 게이트웨이(350)를 거쳐 서버(102a), 서버 팜(server farm; 102c) 또는 피어 컴퓨팅 디바이스(102d)에 연결된다.

각 클라이언트(105a-105n)은 도 1C와 관련하여 더욱 상세히 설명되는 원격 액세스 클라이언트(120a-120n) 및 하나 이상의 어플리케이션(338a-338n)을 포함한다. 클라이언트(105a-105n) 각각은 적합한 터널링이나 게이트웨이 프로토콜의 유형을 이용하여 터널링이나 게이트웨이 연결(341a-341n)을 거쳐 네트워크(104)를 통해 게이트웨이(340)에 통신한다. 몇 실시예에서, 게이트웨이 연결부(341a-341n)는 인캡슐화와 암호화에 의해서와 같이, 보안 통신하는 데에 이용되며, 실시간 무손실이나 손실 프로토콜과 같은 다른 프로토콜을 이용할 수도 있다. 다른 실시예에서, 게이트웨이(340)는 하나 이상의 클라이언트(105a-105n) 및 컴퓨팅 디바이스(102d-102n) 사이에 가상 사설망 연결을 제공한다.

클라이언트(105)는 네트워크(104)와 같은 네트워크를 액세스하는 하나 이상의 어플리케이션(338)를 실행할 수 있는 컴퓨팅 디바이스(102)의 형태일 수 있다. 어플리케이션(338)은 웹 브라우저, 웹 기반 클라이언트, 클라이언트-서버 어플리케이션, 씬(thin)-클라이언트 컴퓨팅 클라이언트, ActiveX 컨트롤, 또는 자바 애플릿 및 그 외 클라이언트(105)에서 실행하거나 네트워크(104)를 통해 통신할 수 있는 실행 가능 명령의 형태와 같은 어플리케이션의 형태일 수 있다. 어플리케이션(338)은 프로토콜의 형태를 이용할 수 있으며, 예를 들어, HTTP 클라이언트, FTP 클라이언트, 오스카(Oscar) 클라이언트, 텔넷 클라이언트일 수 있다. 몇 실시예에서, 어플리케이션(338)은 원격 디스플레이 또는 프리젠테이션 레벨 프로토콜을 이용한다. 일 실시예에서, 어플리케이션(338)은 플로리다, 포트 라우더데일 소재의 사이트릭스 시스템즈사에 의해 개발된 ICA 클라이언트이다. 다른 실시예에서, 어플리케이션(338)은 워싱톤 레드몬드 소재의 마이크로소프트사에 의해 개발된 원격 데스크톱 (RDP) 클라이언트를 포함한다. 다른 실시예에서, 어플리케이션(338)은 소프트 IP 텔레폰과 같은 VoIP 통신에 관련된 소프트웨어의 유형을 포함한다. 다른 실시예에서, 어플리케이션(338)는 비디오 및/또는 오디오를 보내기 위한 어플리케이션과 같은, 실시간 데이터 통신에 관한 어플리케이션을 포함한다.

클라이언트(105a-105n)은 동일한 네트워크(104) 상에 있거나, 사설망과 같이 개별의 네트워크에 있을 수 있는 컴퓨팅 디바이스(102d-102n)를 거쳐 제공된 리소스에 액세스할 수 있다. 몇 실시예에서, 컴퓨팅 디바이스(102a-102n)은 클라이언트(105a-105n)의 네트워크(104)로부터 분리되고 라우트 불가능한 네트워크에 있을 수 있다. 일 실시예에서, 클라이언트(105a-105n) 중에는 원격 액세스 클라이언트(102n)와 어플리케이션(338d)를 갖는 피어 컴퓨팅 디바이스(102d)와 통신한다. 예를 들어, 어플리케이션(338d)는 클라이언트(105a-105n) 상의 어플리케이션(338a-338c)에 대응하는 클라이언트/서버나 분산 어플리케이션의 일부를 포함한다. 몇 실시예에서, 원격 액세스 클라이언트(120a-120n) 중에는 게이트웨이(340)를 거쳐 원격 액세스 클라이언트(120n)과 통신할 수 있다.

다른 실시예에서, 클라이언트(105) 중에는 예를 들어, 워싱톤 레드몬드 소재의 마이크로소프트사에 의해 제작된 마이크로소프트 익스체인지와 같은 이메일 서비스를 제공하는 어플리케이션 서버, 웹 또는 인터넷 서버, 또는 데스크톱 공유 서버나 협력 서버일 수 있는, 어플리케이션(338e)를 실행하는 서버(102e)에 게이트웨이(340)를 거쳐 통신한다. 어떤 실시예에서, 어플리케이션(338e)는 플로리다, 포트 라우더데일 소재의 사이트릭스 시스템즈사에 의해 제공되는 GoToMeeting.com, 캘리포니아 산타클라라 소재의 웹엑스사에 의해 제공되는 WebEx.com, 또는 워싱톤 레드몬드 소재의 마이크로소프트사에 의해 제공되는 LiveMeeting.com와 같은 호스트 서비스의 유형을 포함한다.

다른 실시예에서, 클라이언트(105a)는 하나의 엔티티로 관리되는 하나 이상의 서버의 논리 그룹인 서버 팜(102n)이나 서버망에 게이트웨이(340)을 통해 통신할 수 있다. 서버 팜(102n)은 씬 클라이언트 컴퓨팅 또는 원격 디스플레이 프리젠테이션 어플리케이션을 제공하는 어플리케이션(338f) 등의 하나 이상의 어플리케이션(338N)을 실행할 수 있다. 일 실시예에서, 서버(102e) 또는 서버 팜(102n)은 어플리케이션(338e-338n)으로, MetaFrame 또는 Citrix Presentation Server^{TM}과 같이 사이트릭스 시스템즈사에 의한 Citrix Access Suite^{TM}의 일부 및/또는 마이크로소프트사에 의해 제조되는 Microsoft Windows Terminal Services를 실행한다.

도 1A를 참조하면, 게이트웨이(340)는 일 네트워크 상의 하나 이상의 컴퓨팅 디바이스를 다른 네트워크에 연결하는 데에 이용되는 원격 액세스 서버 등의 게이트웨이의 유형을 포함한다. 다른 형태로, 게이트웨이(340)는 사설망에 대한 클라이언트(105a-105n) 액세스를 제공하기 위해 가상 사설망 연결을 제공하는 데에 이용된다. 다른 형태로, 게이트웨이(340)는 두 개의 다른 프로토콜이나 분리된 네트워크가 시스템 사이에서 전환하는 하드웨어나 소프트웨어 셋업일 수 있다. 게이트웨이(340)는 특수 하드웨어나 네트워크 디바이스를 포함하거나, 게이트웨이로서 작용하도록 구성된 컴퓨팅 디바이스일 수 있다. 이와 같이, 게이트웨이(340)는 소프트웨어, 하드웨어 또는 소프트웨어와 하드웨어의 조합을 포함한다. 일 실시예

에서, 클라이언트(105) 및 게이트웨이(340)는 SSL 또는 TLS와 같은 게이트웨이나 터널링 프로토콜(341a-341n) 또는 플로리다 포트 라우더데일 소재의 사이트릭스 시스템즈사에 의해 제조되는 Citrix Gatewary Protocol의 형태를 통해 통신한다.

몇 실시예에서, 게이트웨이(340)는 클라이언트(105a-105c)로부터 수신된 암호화 패킷을 해독하고 클라이언트(105a-105c)에게 통신되는 패킷을 암호화한다. 게이트웨이(340)는 네트워크(104)와 같은 사설망을 보호하는 데에 이용된다. 몇 실시예에서, 게이트웨이(340)는 클라이언트(105a-105c)를 사설 IP 주소나 사설망의 IP 주소와 관련시킨다. 이들 실시예 중 하나에서, 게이트웨이(340)가 클라이언트(105a-105c)로부터 패킷을 수신하면, 게이트웨이(340)는 패킷의 IP 주소를 사설망에 대한 클라이언트(105a-105c)와 관련되는 IP 주소로 변형한다. 몇 실시예에서, 게이트웨이(340)는 클라이언트(105a-105c)로의 및/또는 로부터의 네트워크 트래픽에 액세스 제어 폴리시를 적용한다. 예를 들어, 액세스 제어 폴리시는 최종 목적지로 패킷을 보내기 전에 클라이언트로부터 수신된 패킷에 적용될 수 있다.

게이트웨이(340)의 일 실시예에서, 프레임이 SSL 터널을 통해 게이트웨이(340)에 들어가면, 패킷과 그의 페이로드는 SSL 해독의 기능을 제공하는 유저 모드에서 실행된는 핸들러로 콜백(callback)을 통해 디스패치된다. 다른 실시예에서, openSSL이 이용될 수 있다. 다른 실시예에서, 하드웨어 가속기가 이용된다. 다른 실시예에서, 게이트웨이(340)는 원격 액세스를 제공하기 위해 하나 이상의 블레이드를 포함한다. 패킷이 해독되면, HTTP 네트워크 스택에 주입되고 여기에서 헤더가 조립되어 원격 액세스 블레이드로 전달된다. 원격 액세스 블레이드에서, 패킷은 패킷 내에 포함된 데이터의 유형으로 분류된다. 일 실시예에서, 패킷은 로긴과 등록을 요청하는 HTTP 헤더를 포함한다. 다른 실시예에서, 패킷은 TCP/UDR/RAW/OTHER 연결 설정을 구한다. 또 다른 실시예에서, 패킷은 연결 특정 데이터를 포함한다. 또 다른 실시예에서, 패킷은 다른 유저와의 협력, 유저 디렉토리의 페칭 및 회의와 웹 캐스트 등의 전화 기능의 존재나 요청과 같은 특수 피쳐 요청을 포함한다. 원격 액세스 모듈은 대응하는 서브 핸들러에게 패킷을 적당하게 디스패치한다. 에를 들어, 클라이언트(105)는 연결이 게이트웨이(340) 뒤의 사설망 상의 특정 기기에 셋업되는 것을 요청한다. 원격 액세스 모듈은 액세스 제어 모듈에 협의하여 긍정의 응답이 돌아오면, 원격 액세스 모듈은 요청을 허용하게 된다. 몇 실시예에서, 원격 액세스 모듈(120)은 대응하는 SSL 터널(341a-341n)에 인입하는 프레임을 클라이언트(105a-105c)에 상관시키도록 NAT/PAT를 이용하는 프레임 포워딩 모듈을 이용하여 사설망에서 후속의 프레임을 주입하여 요청을 허용한다.

도 1A에서 나타낸 네트워크(104)는 어느 유형의 네트워크나 가능하다. 네트워크(104)는 회사 인트라넷과 같은 근거리망(LAN), 메트라폴리탄 영역망(MAN), 인터넷이나 월드와이드웹 등의 광영역망(WAN)일 수 있다. 네트워크(104)의 토폴로지는 버스, 스타 또는 링 네트워크 토폴로지일 수 있다. 네트워크(104) 및 네트워크 토폴로지는 여기 기재된 본 발명의 동작을 지원할 수 있는 네트워크나 네트워크 토폴러지일 수 있다. 클라이언트(108) 및 게이트웨이(340)는 표준 전화망, LAN 또는 WAN 링크(예를 들어, T1, T3, 56kb, X.25, SNA, DECNET), 광대역 연결 (ISDN, 프레임 릴레이, ATM, 기가비트 이더넷, 이더넷-오버-SONET) 및 무선 연결이나 이들의 조합을 포함하는 각종 연결을 통해 하나 이상의 네트워크(104)에 연결될 수 있다. 연결은 각종 통신 프로토콜 (예를 들어, TCP/IP, IPX, SPX, NetBIOS, 이더넷, ARCNET, Fiber Distributed Data Interface (FDDI), RS232, IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g 및 직접 비동기적 연결)을 이용하여 설정될 수 있다.

본 발명의 일 실시예에서, 도 1A에 나타낸 게이트웨이(340)는 컴퓨팅 디바이스(102a-102n) 사이의 직접적인 피어투피어 연결을 용이하게 한다. 예를 들어, 클라이언트(105a)는 피어 컴퓨팅 디바이스(102d)에 액세스하기 위해 게이트웨이(340)와의 터널링 세션을 설정한다. 게이트웨이(340)는 클라이언트(105a)의 원격 액세스 클라이언트(120a)과 컴퓨팅 디바이스(102d)의 원격 액세스 클라이언트(120n)을 협상하여 클라이언트(105a)가 게이트웨이(340)를 관통하지 않고 컴퓨팅 디바이스(102d)에 바로 연결되게 한다. 클라이언트(105a)와 컴퓨팅 디바이스(102d) 사이의 네트워크 연결이 설정되면, 클라이언트(105a)는 컴퓨팅 디바이스(102d)와 피어투피어 식으로 통신한다. 본 발명의 게이트웨이(340)는 환경(180)에서 나타낸 컴퓨팅 디바이스(102a-102n) 사이에 직접적인 피어투피어 연결을 용이하게 할 수 있다. 일 실시예에서, 게이트웨이(340)는 어느 클라이언트(105a-105n) 사이에서나, 예를 들어, 클라이언트(105a)와 클라이언트(105b)사이나 클라이언트(105b)와 클라이언트(105c) 간의 피어투피어 연결을 용이하게 한다. 다른 실시예에서, 게이트웨이(340)는 컴퓨팅 디바이스들(102d-102n)사이, 예를 들어, 컴퓨팅 디바이스(102d)와 서버(102e)나 서버 팜(102n) 사이의 피어투피어 연결을 용이하게 한다. 다른 실시예에서, 게이트웨이(340)는 클라이언트(105a-105n) 중 하나와 컴퓨팅 디바이스(102d-102n) 중 하나 간의 피어투피어 연결을 용이하게 한다. 게이트웨이(340)를 통해 피어투피어 연결을 용이하게 하는 기술을 도 2A 및 2B를 참조하여 이하 더욱 상세히 설명한다.

이하 도 1B를 참조하면, 본 발명의 원격 액세스 클라이언트(120)는 게이트웨이(304) 없이 피어투피어 연결의 설명적 실시예에서 이용된다. 예를 들어, 게이트웨이(340)는 도 1에서 나타낸 컴퓨팅 디바이스(102a-102n) 간의 피어투피어 연결을

용이하게 하고 그 후 컴퓨팅 디바이스(102a-102n)는 피어투피어식으로 서로 직접적으로 통신한다. 다른 실시예에서, 컴퓨팅 디바이스(102a)는 연결을 용이하게 하는 게이트웨이(340) 없이 네트워크(104)를 통해 다른 컴퓨팅 디바이스(102b 또는 102c)에 바로 통신할 수 있다.

도 1B의 간단한 개요로, 원격 액세스 클라이언트(120a)는 하나 이상의 어플리케이션(338a)을 실행하는 클라이언트(102a)에서 전개될 수 있다. 컴퓨팅 디바이스(102a)는 컴퓨팅 디바이스(102b) 및/또는 컴퓨팅 디바이스(102c)에 네트워크(104)를 통해 연결된다. 컴퓨팅 디바이스(102b)는 또한 원격 액세스 클라이언트(120b)를 포함하는 피어 또는 클라이언트 컴퓨팅 디바이스일 수 있다. 몇 실시예에서, 원격 액세스 클라이언트(120a 및 120b)는 네트워크(104)를 통해 서로 통신하며, 웹 기반이나 클라이언트/서버 어플리케이션에 대한 것과 같은 어플리케이션(338b)에 통신하기 위해 어플리케이션(338a)에 대해 서로에 관련하여 작용한다. 다른 실시예에서, 원격 액세스 클라이언트(102a)는 원격 액세스 클라이언트(120)를 실행하지 않는 서버일 수 있는 컴퓨팅 디바이스(120c)와 통신한다.

도 1C는 클라이언트(105)로부터 네트워크(104)에 네트워크 패킷을 보내기 위한 원격 액세스 클라이언트(120)를 갖는 시스템을 설명하는 블럭도이다. 간단한 개요로, 시스템은 어플리케이션이나 유저 스페이스로 불리는 유저 모드(332) 및 커널이나 시스템 레벨 스페이스로 불리는 커널 모드(334)를 포함하는 운영 시스템을 갖는 (또한 클라이언트로 언급되는) 컴퓨팅 디바이스(102)를 포함한다. 클라이언트(105)는 일 실시예에서, 유저 모드(332)에서 실행되는 에이전트(326)를 실행한다. 클라이언트(105)는 일 실시예에서, 커널 모드나 커널 스페이스(334)에서 실행하는 필터(322)를 실행한다. 일 실시예에서, 필터(322)와 에이전트(326)은 패킷을 네트워크를 통해 보내기 위해 또는 여기 기재된 본 발명의 동작에 따라 원격 액세스 연결을 제공하기 위해 원격 액세스 클라이언트(120)를 형성한다. 원격 액세스 클라이언트(120) 또는 에이전트(326)이나 필터(322)와 같은 그 일부는 유저 모드(332)나 커널 모드(334)에서 실행된다.

클라이언트(105)는 당업자라면 잘 이해하는 바와 같이, 오픈 시스템 인터커넥션 (OSI) 통신 모델의 네트워크 계층과 같은 하나 이상의 네트워크 계층을 포함하는 네트워크 스택(310)을 갖는다. 네트워크 스택(310)은 당업자라면 잘 아는 바와 같이, 이더넷을 통한 TCP/IP 프로토콜 같은 하나 이상의 프로토콜, 또는 IEEE 802.11와 같은 무선 프로토콜을 포함한다. 더욱, 네트워크 스택(310)은 TCP 드라이버나 네트워크 계층 드라이버와 같은 하나 이상의 계층을 지원하는 하나 이상의 네트워크 드라이버를 포함한다. 네트워크 드라이버는 컴퓨팅 디바이스(102)의 운영 시스템의 일부나 네트워크 인터페이스 카드나 그 외 컴퓨팅 디바이스(102)의 다른 네트워크 액세스 컴포넌트의 일부로 포함될 수 있다. 부가하여, 네트워크 스택(310)의 네트워크 드라이버는 여기 기재된 본 발명의 기술의 지원으로 네트워크 스택(310)의 맞춤 주문되거나 수정된 부분을 제공하도록 맞춤 주문되거나 수정된다. 부가하여, 네트워크 스택(310)의 어플리케이션 계층과 같이, 네트워크 스택(310)의 일부는 커널 모드(334)에서 동작하는 한편, 다른 부분은 유저 모드(332)에서 실행한다.

필터(322)는 패킷 캡쳐링 메커니즘(365)를 포함하고, 필터(322) 및/또는 패킷 캡쳐링 메커니즘(365)은 클라이언트(105)의 네트워크 스택(310)의 계층이나 그 일부에서 동작하는 네트워크 드라이버와 같은 네트워크 드라이버를 포함한다. 필터(322) 및/또는 패킷 캡쳐 메커니즘(365)은 네트워크 드라이버 인터페이스 사양 (NDIS)을 따르는 드라이버 또는 NDIS 드라이버를 포함한다. 다른 실시예에서, 필터(322) 및/또는 패킷 캡쳐 메커니즘(365)은 최소 필터나 미니포트 드라이버를 포함한다. 패킷 캡쳐 메커니즘(365)은 또한 몇 실시예에서 커널 모드(334)에서 동작한다. 패킷 캡쳐 메커니즘(365)는 필터(322)의 일부로 나타내었지만, 패킷 캡쳐 메커니즘(365)은 필터(322)와 분리된다. 부가하여, 필터(322)와 패킷 캡쳐 메커니즘(365)은 클라이언트(105)의 네트워크 스택의 여러 계층이나 그 일부에서 동작한다.

필터(322)는 패킷을 필터링하기 위한 필터 테이블을 이용한다. 필터링 테이블은 패킷 캡쳐 메커니즘(365)에 의해 인터셉트된 패킷과 같은 패킷에 대해 어느 동작이 취해져야 하는지를 결정하기 위한 것이다. 필터(322)는 라우팅 정보와 같은 패킷의 컨텐츠를 검사하여, 필터링 테이블에 기초하여 취할 동작을 결정한다. 몇 실시예에서, 필터(322)는 컨텐츠에 따라 네트워크 패킷을 중단하거나 수용한다. 다른 실시예에서, 필터(322)는 패킷 컨텐트 및/또는 필터링 테이블에 기초하여 에이전트(326)에게 네트워크 패킷을 보낸다. 필터 테이블은 원치 않는 패킷이 폐기되는 것을 확실히 하기 위한 것이다. 필터(322)는 특정 프로토콜에 대한 액세스를 거부하거나 특정 목적지 주소에 대한 패킷을 폐기하여 원격 컴퓨터로부터 비인가 액세스를 방지하는 데에 이용될 수 있다.

몇 실시예에서, 필터링 테이블은 사설망에 대한 정보를 포함한다. 다른 실시예에서, 클라이언트 컴퓨팅 디바이스(102) 상의 필터가 필터링 테이블을 수신한다. 이들 실시예 중 하나에서, 필터(322)는 컴퓨팅 디바이스(102) 상의 어플리케이션(338)이나 에이전트(326)로부터 필터링 테이블을 수신한다. 다른 실시예에서는, 필터(322)가 에이전트(326)로부터 컨피규레이션 세팅을 수신하여 이를 필터링 테이블에 저장한다.

패킷 캡쳐 메커니즘은 어플리케이션(338)와 관련된 네트워크 패킷과 같은, 클라이언트(105)의 네트워크 패킷을 인터셉트한다. 몇 실시예에서, 패킷 캡쳐 메커니즘(365)은 네트워크 트래픽을 어플리케이션(338), 에이전트(326), 게이트웨이

(340) 또는 패킷 캡쳐 메커니즘(365)가 동작하는 계층 위나 아래의 계층에서 동작하는 다른 드라이버나 계층과 같은 클라이언트(105)의 네트워크 스택의 일부에 투명하게 인터셉트한다. 이런 식으로, 본 발명은 여기 기재된 기술로 이용회거나 이의 지원을 받는다. 일 실시예에서, 패킷 캡쳐 메커니즘(365)는 네트워크(104) 및/또는 게이트웨이(340)를 통해 통신되는 네트워크 트래픽과 같은 아웃바운드 패킷 트래픽을 인터셉트한다. 패킷 캡쳐 메커니즘(365)은 에이전트(325) 또는 에이전트(326)의 프레임 모니터 메커니즘(360)에 패킷을 전달한다. 어떤 실시예에서, 필터(322)는 비동기성 I/O 컨트롤 메시지를 통해 에이전트(326)와 통신한다. 이들 실시예 중 하나로, 패킷 캡쳐 메커니즘(365)은 비동기성 I/O 컨트롤 메시지를 통해 게이트웨이(340) 뒤의 사설망으로 어드레스되는 패킷을 전달한다. 다른 실시예에서, 필터(322)는 UDP 패킷을 통해 유저 스페이스(334)에서 실행하는 에이전트(326)과 통신한다. 일 실시예에서, 필터(322)는 비동기성 I/O 컨트롤 메시지를 통해 에이전트(326)의 드라이버로부터 컨피규레이션 세팅을 수신한다. 컨피규레이션 세팅은 어느 네트워크, 프로토콜, 또는 유형의 패킷을 필터링할지에 관한 정보를 포함한다. 일 실시예에서, 필터(322)는 필터링 테이블에 컨피규레이션 세팅을 저장한다. 다른 실시예에서, 필터(322)는 컨피규레이션 세팅을 포함하는 필터링 테이블을 수신한다.

일 실시예에서, 필터(322)는 검사를 위해 클라이언트(105)의 모든 아웃바운드 패킷을 인터셉트한다. 예를 들어, 몇 실시예에서, 필터는 클라이언트(105)에 의한 전송을 위해 유저 모드(322)에서 실행하는 어플리케이션(338)에 의해 형성된 패킷을 인터셉트한다. 패킷이 필터링 테이블에서 목록화된 조건을 만족하면, 필터(322)는 패킷의 원래 목적지가 아닌 에이전트(326)에 패킷을 전송한다. 필터(322)는 패킷을 에이전트(326)에 보내기 위해 비동기성 I/O 컨트롤 메시지를 이용한다. 필터(322)는 라우팅 테이블에 따라서, 또는 이에 응답하여 패킷을 에이전트(326)에 전송한다.

몇 실시예에서, 에이전트(326) 및 필터(322)는 운영 시스템의 마이크로소프트 윈도우에 의해 제공되는 IOCTL 라이브러리와 함수 호출과 같이, IOCTL 어플리케이션 프로그래밍 인터페이스 (API)를 거쳐 통신한다. 다른 실시예에서, 에이전트(326)와 필터(322) 간의 IOCTL 기반의 인터페이스는 클라이언트(105)에서 실행중인 운영 시스템의 일부에 의해 제공된다. I/O 컨트롤 메시지와 IOCTL 인터페이스에 관해서 논의되고 있지만, 에이전트(326)와 필터(322)는 적당한 메커니즘 및/또는 수단을 통해 통신할 수 있다.

클라이언트(105)의 커널(334)는 NDIS 인터페이스를 포함한다. 몇 실시예에서, NDIS 인터페이스는 복수의 중간 필터를 포함한다. 일 실시예에서, 패킷은 복수의 중간 필터를 포함한다. 일 실시예에서, 패킷은 NDIS 인터페이스를 통과하고 복수의 중간 필터에 의해 인터셉트된다. 필터(322)가 NDIS 드라이버로 제공되지만, 필터(322)는 또한 커널(334)에서 실행하는 프로세스나 다른 세트나 유형의 실행 가능 명령일 수 있다.

본 발명의 에이전트(326)는 클라이언트(105) 상의 어플리케이션 스페이스(332)나 유저 모드에서 실행될 수 있다. 다른 실시예에서, 에이전트(326)는 커널 모드(334)에서 동작한다. 몇 실시예에서, 에이전트(326)는 필터(322)로부터 패킷을 수신하기 위한 기능을 제공한다. 다른 실시예에서, 에이전트(326)은 수신된 패킷에 폴리시를 공급하기 위한 기능을 제공한다. 또 다른 실시예에서, 에이전트(326)는 게이트웨이(340)에게 SSL 터널을 관리하기 위한 기능을 제공한다. 또 다른 실시예에서, 에이전트(326)는 패킷을 암호화하여 게이트웨이(340)에게 전송하기 위한 기능을 제공한다. 에이전트(326)는 프레임 모니터 메커니즘(360)을 포함한다. 프레임 모니터(360)는 폴리시 및 수신된 패킷에 폴리시를 적용하기 위한 로직을 포함한다. 에이전트(326)는 프레임 모니터(360)에 의해 행해진 폴리시 기반의 판정에 응답하여 게이트웨이(340)에 패킷을 전송한다.

몇 실시예에서, 프레임 모니터(360)는 폴리시를 적용하여 패킷의 전송시, 클라이언트(105)의 조건이나 엔드포인트를 결정한다. 다른 실시예에서, 프레임 모니터(360)는 패킷을 형성한 어플리케이션(338)을 식별한다. 이들 실시예중에서, 프레임 모니터(360)는 식별된 어플리케이션(338)에 응답하여 게이트웨이(340)에 패킷을 전송하도록 폴리시 기반의 결정을 행한다. 다른 실시예에서, 프레임 모니터(360)는 식별된 어플리케이션이 패킷을 실제 형성한 것을 증명하도록 패킷에 대해 체크섬을 실행한다.

다른 실시예에서, 패킷 캡쳐 메커니즘(365)은 필터(322) 대신이나 이에 부가하여 에이전트(326)에 포함된다. 이와 같이, 에이전트(326)는 네트워크 트래픽을 인터셉트한다. 패킷 캡쳐 메커니즘(365)은 후킹 어플리케이션 프로그래밍 인터페이스 (API)를 이용하여 어플리케이션(338)와 관련된 네트워크 트래픽과 같은, 클라이언트(105)의 인바운드 및/또는 아웃바운드 패킷을 인터셉트, 후킹 (hooking) 또는 취득할 수 있다.

일 실시예에서, TCP 연결은 IP 패킷을 도 1B의 컴퓨팅 디바이스(102c) 또는 도 1A의 게이트웨이(340)와 같은 타겟 컴퓨팅 디바이스에 전송하기 위해 클라이언트(105)에서 실행되는 어플리케이션(338)에 의해 초기화된다. 원격 액세스 클라이언트(120)는 어플리케이션(338)에 의해 형성된 IP 패킷을 인터셉트하거나 캡쳐한다. 원격 액세스 클라이언트(120)는 어플리케이션(338)에 TCP 확인 패킷을 보내고 어플리케이션(338)에 의해 초기화된 TCP 연결을 종료한다. 다음에, 원격 액세스 클라이언트(120)는 제2 컴퓨팅 디바이스(102c)나 게이트웨이(340)에 대한 제2 TCP 연결을 형성하며 제2 TCP 연

결을 통해 캡쳐된 IP 패킷을 전송한다. 몇 실시예에서, 원격 액세스 클라이언트(120)은 버퍼에 캡쳐된 IP 패킷을 저장한다. 이들 실시예에서, 원격 액세스 클라이언트(120)은 버퍼된 IP 패킷을 제2 TCP 연결을 통해 제2 컴퓨팅 디바이스(102c)에 전송한다. 캡쳐된 IP 패킷을 버퍼에 저장하게 되면 네트워크 연결시 붕괴의 경우 패킷의 보존이 가능하게 된다.

일 실시예에서, 캡쳐된 IP 패킷의 수신시, 게이트웨이(340)는 도 1A에서와 같이, 게이트웨이(340)와 타겟 컴퓨팅 디바이스(102d) 사이의 제3 TCP 연결을 형성한다. 게이트웨이(340)는 포트 매핑 네트워크 주소 변환 (NAT) 테이블을 보유하여, 게이트웨이(340)가 타겟 컴퓨팅 디바이스(102d)로부터 클라이언트(105) 상에 IP 패킷을 원래 형성했던 어플리케이션(338)에 의해 모니터된 포트로 응답 패킷을 전송할 수 있게 한다. 클라이언트(105)가 게이트웨이(340)의 공중망 주소로만 통신하기 때문에, 클라이언트(105)는 타겟 컴퓨팅 디바이스(102d)의 네트워크 주소를 모르므로, 타겟 컴퓨팅 디바이스(102d)가 놓인 네트워크의 보안성을 증가시킨다. 유사하게, 게이트웨이(340)가 타겟 컴퓨팅 디바이스(120d)에의 TCP 연결을 시작하기 때문에, 타겟 컴퓨팅 디바이스(102d)는 클라이언트(105)의 주소 정보를 수신하지 않는다. 부가하여, 게이트웨이(340)가 IP 패킷을 수신하기 때문에, 게이트웨이(340)는 타겟 컴퓨팅 디바이스(102d)에 IP 패킷을 전송할지의 여부에 대해 폴리시나 보안 체크에 응답하여 판정하여, 타겟 컴퓨팅 디바이스(102d)가 놓이는 네트워크의 보호성을 더욱 증가시킨다.

일 실시예에서, 본 발명은 게이트웨이(340) 뒤의 사설 보안망으로부터 외부 네트워크(104) 상의 클라이언트(105)에게 전송되는 패킷을 보안하기 위한 방법을 제공한다. 본 발명은 게이트웨이(340) 상의 네트워크 주소 변환 (NAT) 기능을 제공하여 클라이언트(105)을 사설망으로부터 분리하는 것을 가능하게 한다. NAT를 이용하는 VPN 게이트웨이는 사설망을 클라이언트(105)에 의한 직접적 계층-2 액세스로부터 차단하기 위해 가장된 클라이언트(105)의 IP 주소를 제공한다.

일 형태에서, 에이전트(326), 프레임 모니터(360), 필터(322) 및 패킷 캡쳐 메커니즘(365)와 같은 원격 액세스 클라이언트(120)의 임의의 부분은 ASIC 또는 FPGA 등의 소프트웨어, 하드웨어, 또는 이들의 조합을 포함한다. 어떤 실시예에서, 원격 액세스 클라이언트(120)의 일부는 클라이언트(105)에서 하나 이상의 블레이드를 통해 제공된다.

원격 액세스 클라이언트(120)가 에이전트(326)와 필터(322) 등의 다수의 컴포넌트로 설명되지만, 당업자라면 여기 기재된 원격 액세스 클라이언트(120)의 동작과 기능은 하나의 메커니즘이나 하나의 컴포넌트로 실행될 수 있다는 것이 이해될 것이다. 예를 들어, 몇 실시예에서, 원격 액세스 클라이언트(120)의 동작과 기능은 어플리케이션(338) 내에 포함된다. 일 실시예에서, 예를 들어, 원격 액세스 클라이언트(120)의 기능과 동작은 단지 에이전트(326)로, 다른 실시예에서는 필터(322)와 같은 네트워크 드라이버로 제공된다.

몇 실시예에서, 에이전트(326), 프레임 모니터(360), 필터(322) 및 패킷 캡쳐 메커니즘(365)과 같은 원격 액세스 클라이언트(120)나 그 일부는 어플리케이션, 모듈, 서비스, 컴퓨터 프로그램, 소프트웨어 컴포넌트, 웹 서비스, 웹 컴포넌트, 라이브러리, 함수, 프로세스, 태스크, 드레드 또는 그 외 여기 기재된 본 발명의 기능을 실행할 수 있게 설계되며 유저 모드(322) 및/또는 커널 모드(334)의 일부나 조합으로 동작할 수 있는 실행 가능 명령의 형태을 포함한다.

도 1A-1C에서 나타낸 바와 같이, 본 발명의 원격 액세스 클라이언트(120)는 게이트웨이(340)를 거치거나 피어 컴퓨팅 디바이스 간에 직접, 네트워크를 통해 다른 컴퓨팅 디바이스에 원격 액세스 통신하는 여러 가지 방법으로 이용될 수 있다. 이들 여러 환경에서, 원격 액세스 클라이언트(120)는 이하 더욱 상세히 설명되는 바와 같이 본 발명의 최적화 기술 중 하나 이상을 실행하는 데에 이용된다. 예를 들어, 원격 액세스 클라이언트(120)는 도 1A-1C의 설명적 환경에서 VoIP, 데스크톱 공유, 또는 웹 컨퍼런싱과 같은 실시간 데이터 통신을 최적화하는 데에 이용된다.

도 1A-1C의 설명적 실시예에서, 클라이언트(105), 서버, 또는 게이트웨이(340)와 같은 컴퓨팅 디바이스(102a-102n)은 캘리포니아, 팔로 알토 소재의 휴렛팩커드사 또는 텍사스주 라운드 록 소재의 델사에 의해 제조되는 종류의 퍼스널 컴퓨터나 컴퓨터 서버와 같은 컴퓨팅 디바이스의 유형으로 제공된다. 도 1D 및 도 1E는 본 발명의 실시예를 실행하는 데에 유용한 컴퓨팅 디바이스(102)의 블럭도를 나타낸다. 도 1D 및 도 1E에서 나타낸 바와 같이, 각 컴퓨팅 디바이스(102)는 중앙 처리 유닛(102) 및 주요 메모리 유닛(104)를 포함한다. 도 1D에 나타낸 바와 같이, 통상의 컴퓨팅 디바이스(102)는 가상 디스플레이 장치(124), 키보드(126) 및/또는 마우스 등의 포인팅 장치(127)를 포함한다. 각 컴퓨팅 디바이스(102)는 또한 하나 이상의 입/출력 장치(130a-130b; 보통 참조 부호 130으로 언급) 등의 부가의 선택 소자 및 중앙 처리 유닛(102)과 통신하는 캐시 메모리(140)를 포함한다.

중앙 처리 유닛(102)는 주요 메모리 유닛(104)로부터 불러온 명령에 응답하여 이를 처리하는 논리 회로이다. 많은 실시예의 경우, 중앙 처리 유닛은 캘리포니아 마운틴뷰 소재의 인텔사에 의해 제조되는 8088, 80286, 80386, 펜티엄, 펜티엄 프로, 펜티엄 II, 셀레론 또는 제논 프로세서; 일러노이주 슈햄버그 소재의 모토롤라사에 의해 제조되는 68000, 68010, 68020, 68030, 68040, PowerPC601, PowerPC604, PowerPC604e, MPC603e, MPC603ei, MPC603ev, MPC603r,

MPC603p, MPC740, MPC745, MPC750, MPC755, MPC7400, MPC7410, MPC7411, MPC7445, MPC7447, MPC7450, MPC7451, MPC7455, 또는 MPC7457 프로세서; 캘리포니아주 산타클라라 소재의 트란스매터사에 의해 제조되는 Crusoe TM5800, Crusoe TM5600, Crusoe TM5500, Crusoe TM5400, Efficeon TM8600, Efficeon TM8300, 또는 Efficeon TM8620 프로세서; 뉴욕 화이트 플레인 소재의 IBM사에 의해 제조되는 RS/60000 프로세서, RS64, RS64 II, P2SC, POWER3, RS64 II, Power3-II, RS64 IV, POWER4, POWER4+ , POWER5, 또는 POWER6 프로세서; 캘리노피아 서니베일 소재의 어드밴스드 마이크로 디바이스사에 의해 제조되는 AMD Opteron, AMD Athlon 64 FX, AMD Athoon, 또는 AMD Duron 프로세서와 같은 마이크로프로세서 유닛에 의해 제공된다. 컴퓨팅 디바이스(102)는 상술된 프로세서들 중 하나나 여기 기재된 바와 같이 동작하는 다른 프로세서들 기반이 가능하다.

주요 메모리 유닛(104)는 정적 랜덤 액세스 메모리 (SRAM), 버스트 SRAM 또는 싱크버스트 SRAM (BSRAM), 동적 랜덤 액세스 메모리 (DRAM), 패스트 페이지 모드 DRAM (FPM DRAM), 인헨스드 DRAM (EDRAM), 익스탠디드 데이터 아웃풋 RAM (EDORAM), 익스탠디드 데이터 아웃풋 DRAM (EDO DRAM), 버스트 익스탠디드 데이터 아웃풋 DRAM (BEDO DRAM), 인헨스드 DRAM (EDRAM), 동기성 DRAM (SDRAM), JEDEC SRAM, PC100 SDRAM, 더블 데이터 레이트 SDRAM (DDR SDRAM), 인헨스드 SDRAM (ESDRAM), 싱크링크 DRAM (SLDRAM), 디렉트 램버스 DRAM (DRDRAM), 또는 강자성 RAM (FRAM). 메인 메모리(104)는 상술된 메모리 칩이나, 여기 기재된 바와 같이 동작할 수 있는 다른 유용한 메모리 칩에 기초할 수 있다. 도 1E에 나타낸 실시예에서, 프로세서(100)는 시스템 버스(150) (나중에 상세히 설명)를 거쳐 메인 메모리(104)와 통신한다. 도 1E는 프로세서가 메모리 포트(103)에 거쳐 메인 메모리(104)와 바로 통신하는 컴퓨팅 디바이스(102)의 실시예를 도시한다. 예를 들어, 도 1E에서 메인 메모리(104)는 DRDRAM일 수 있다.

도 1D 및 1E는 메인 프로세서(100)가 때로 백사이드 버스로 불리는 이차 버스를 거쳐 캐시 메모리(140)와 직접 통신하는 실시예를 도시한다. 다른 실시예에서, 메인 프로세서(100)는 시스템 버스(150)를 이용하여 캐시 메모리(140)와 통신한다. 캐시 메모리(140)는 메인 메모리(104) 보다 응답 속도가 더 빠르며 통상 SRAM, BSRAM 또는 EDRAM에 의해 제공된다.

도 1D에 나타낸 실시예에서, 프로세서(100)는 로컬 시스템 버스(150)을 거쳐 여러 I/O 장치(130)와 통신한다. 여러 버스는 VESA VL 버스, ISA 버스, EISA 버스, 마이크로채널 아키텍처 (MCA) 버스, PCI 버스, PCI-X 버스, PCI-Express 버스 또는 NuBus를 포함하는 I/O 장치(130)에 중앙 처리 유닛(102)를 연결하는 데에 이용된다. I/O 장치가 비디오 디스플레이(124)인 실시예의 경우, 프로세서(100)는 디스플레이(124)와 통신하도록 어드밴스드 그래픽 포트 (AGP)를 이용한다. 도 1E는 HyperTransport, Rapid I/O, 또는 InfiniBand를 거쳐 I/O 장치(130b)와 직접 통신하는 컴퓨터(102)의 실시예를 도시한다. 도 1E는 또한 로컬 버스와 직접 통신이 혼합된 실시예로: 프로세서(100)는 I/O 장치(130b)와 직접 통신하면서 로컬 인터커넥트 버스를 이용하여 I/O 장치(130a)와 통신한다.

컴퓨팅 디바이스(102)는 3.5인치, 5.25인치 디스크나 ZIP 디스크와 같은 플로피 디스크를 수용하기 위한 플로피 디스크 드라이브, CD-ROM 드라이브, CD-R/RW 드라이브, DVD-ROM 드라이브, 여러 포맷의 테이프 드라이브, USB 장치, 하드 드라이브 또는 그 외 본 발명에 관련한 원격 액세스 클라이언트 소프트웨어(120) 등의 소프트웨어와 프로그램을 설치하는 데에 적합한 장치와 같은, 적합한 설치 장치(116)를 지원한다.

컴퓨팅 디바이스(102)는 운영 시스템과 그 외 관련 소프트웨어를 저장하기 위해 그리고 본 발명의 원격 액세스 클라이언트(120)에 관한 프로그램 등의 어플리케이션 소프트웨어 프로그램을 저장하기 위해, 하나 이상의 하드 디스크 드라이브 또는 리던턴트 어레이의 개별 디스크 등의 저장 장치(128)를 더욱 포함한다. 선택적으로, 설치 장치(118)는 또한 저장 장치(128)에서 이용될 수 있다. 부가하여, 운영 시스템과 프록시 소프트웨어(120)은 부터블 (bootable) 매체, 예를 들어, KNOPPIX®과 같은 부터블 CD, knoppix.net으로부터 분산된 GNU/Lunux로 이용 가능한 GNU/Linux에 대한 부터블 CD로 실행될 수 있다.

더욱, 컴퓨팅 디바이스(102)는 표준 전화선, LAN 또는 WAN 링크 (예를 들어, 802.11, T1, T3, 56kb, X.25), 광대역 연결 (예를 들어, ISDN, 프레임 릴레이, ATM), 무선 연결, 또는 상기의 일부나 모두의 조합을 포함하는 각종 연결을 통해 근거리 영역망(LAN), 원거리 영역망 (WAN), 또는 인터넷에 인터페이스하도록 네트워크 인터페이스(118)를 포함한다. 네트워크 인터페이스(118)는 내장 네트워크 어댑터, 네트워크 인터페이스 카드, PCMCIA 네트워크 카드, 카드 버스 네트워크 어댑터, 무선 네트워크 어댑터, USB 네트워크 어댑터, 모뎀 또는 그 외 여기 기재된 동작을 통신하고 실행할 수 있는 어느 유형의 네트워크에나 컴퓨팅 디바이스(102)를 인터페이스하는 데에 적합한 장치를 포함한다.

각종 I/O 장치(130a-130n)은 컴퓨팅 디바이스(102)에 존재한다. 입력 장치는 키보드, 마우스, 트랙패드, 트랙볼, 마이크로폰, 및 드로잉 태블릿을 포함한다. 출력 장치는 비디오 디스플레이, 스피커, 잉크젯 프린터, 레이저 프린터 및 염료 승화 프린터를 포함한다. I/O 장치는 도 1D에서 나타낸 바와 같이 I/O 컨트롤러(123)에 의해 제어된다. I/O 컨트롤러는 키보드(126)와 마우스나 광학 펜인 포인팅 장치(127)와 같은 하나 이상의 I/O 장치를 제어한다. 더욱, I/O 장치는 저장소(128) 및

/또는 컴퓨팅 디바이스(102)용 설치 매체(118)를 제공한다. 또 다른 실시예에서, 컴퓨팅 디바이스(102)는 캘리포니아 로스알라미토스 소재의 트윈테크 인더스트리사에 의해 제조되는 디바이스의 USB Flash Drive 라인과 같은 핸드헬드형 USB 저장 장치를 수용하기 위한 USB 연결부를 제공한다.

다른 실시예에서, I/O 디바이스(130)는 시스템 버스(150)와 USB 버스, 애플 데스크톱 버스, RS-232 시리얼 연결, SCSI 버스, 파이어와이어 버스, 파이어와이어 800 버스, 이더넷 버스, 애플톡 버스, 기가비트 이더넷 버서, 비동기성 트랜스퍼 모드 버서, HIPPI 버스, 수퍼 HIPPI 버스, 시리얼플러스 버스, SCI/LAMP 버스, 파이버채널 버스, 또는 순차적 부착 소형 컴퓨터 시스템 인터페이스 버스와 같은 외부 통신 버스 간의 브리지(170)일 수 있다.

도 1D 및 1E에 도시된 종류의 컴퓨팅 디바이스는 통상 운영 시스템의 제어하에 동작하며, 이는 태스크의 스케줄링과 시스템 리소스에 대한 액세스를 제어한다. 컴퓨팅 디바이스(102)는 마이크로소프트 윈도우 운영 시스템의 버전, 유닉스와 리눅스 운영 시스템의 여러 배포물, 매킨토시 컴퓨터용 MacOS®의 버전, 매립형 운영 시스템, 실시간 운영 시스템, 오픈 소스 운영 시스템, 독점식 운영 시스템, 모바일 컴퓨팅 디바이스용 운영 시스템, 또는 그 외 컴퓨팅 디바이스에서 실행하며 여기 기재된 동작을 실행할 수 있는 운영 시스템 등의 운영 시스템을 실행할 수 있다. 통상의 운영 시스템은: 모두 워싱톤, 레드몬드 소재의 마이크로소프트사에 의해 제조된 WINDOWS 3.x, WINDOWS 95, WINDOWS 98, WINDOWS 2000, WINDOWS NT 3.51, WINDOWS NT 4.0, WINDOWS CE 및 WINDOWS XP; 캘리포니아, 쿠퍼티노 소재의 애플 컴퓨터에 의해 제조된 MacOS; 뉴욕 아몽크 소재의 IBM사에 의해 제조된 OS/2; 유타 솔트레이크 시티 소재의 칼데라사에 의해 분포된 무료 이용 운영 시스템, 리눅스, 자바나 유닉스를 포함한다.

다른 실시예에서, 컴퓨팅 디바이스(102)는 여러 프로세서, 운영 시스템, 및 디바이스와 호환되는 입력 장치를 갖는다. 예를 들어, 일 실시예에서 컴퓨터(102)는 팜사에 의해 제조되는 Zire 71 퍼스널 디지털 어시스턴트이다. 이 실시예에서, Zire71은 PalmOS 운영 시스템의 제어 하에서 동작되며 스타일러스 입력 장치 뿐만 아니라 5방향 네비게이터 장치를 포함한다.

더구나, 컴퓨팅 디바이스(102)는 워크스테이션, 데스크톱 컴퓨터, 랩톱 또는 노트북 컴퓨터, 서버, 핸드헬드 컴퓨터, 모바일 전화, 그 외 컴퓨터나, 그 외 통신이 가능하며 여기 기재된 동작을 실행할 충분한 프로세서 전력과 메모리 용량을 갖는 컴퓨팅 또는 텔레커뮤니케이션 장치의 형태일 수 있다.

일 형태에서, 본 발명은 설명적 환경 도 1A-1C 중 어느 하나에서 도시된 것과 같이 컴퓨팅 디바이스 간의 통신을 최적화하기 위한 여러 기술을 제공하는 것에 관한 것이다. 본 발명은 다음 기술을 제공하며, 이들은 단독으로 또는 조합하여 실행될 수 있다: 1) 피어투피어 루트 최적화, 2) 손실 프로토콜을 통한 전송을 위해 구성되는 패킷의 무손실 프로토콜을 통한 통신, 3) 암호화를 고려하도록 최대 전송 단위 (MTU)의 조정에 의한 네트워크 단편화 감소, 4) 클라이언트측 어플리케이션 인식 네트워크 통신 우선 순위, 및 5) 디바이스의 네트워크 붕괴 차단. 피어투피어 루트 최적화 기술은 도 2A 및 2B와 관련하여 설명되며, 손실 프로토콜을 통한 전송을 위해 구성된 패킷의 무손실 프로토콜을 통한 통신 기술은 도 3A 및 3B와 관련하여 설명되며, MTU 조정 기술은 도 4와 관련하여, 클라이언트측 어플리케이션 인식 우선 순위 기술은 도 5A 및 5B와 관련하여, 네트워크 붕괴 차단은 도 6A와 6B와 관련하여 설명된다.

일 형태에서, 본 발명은 제2 컴퓨팅 디바이스에 액세스하는 제1 컴퓨팅 디바이스와 도 1A에 나타낸 게이트웨이(340)와 같은 게이트웨이 간의 피어투피어 루트 최적화 기술을 제공한다. 피어투피어 루트 기술은 게이트웨이를 거쳐 통신 세션을 설정하는 컴퓨팅 디바이스들 간의 더욱 최적인 직접 통신을 제공한다. 본 발명의 실시예의 설명적 방법(260)은 도 2A의 설명적 환경(200)에 비추어 설명된다. 간단하게, 이 환경(200)은 IP 주소 범위가 10.10.10.XXX인 네트워크와 같은 사설망에 대한 원격 액세스 연결을 제공하는 게이트웨이(340)을 포함한다. 사설망과 관련하는 게이트웨이(340)는 사설망에서의 통신을 위해 10.10.10.2의 IP 주소가 할당된다. 이 사설망은 서버(102c)를 포함한다. 또한, 사설망은 VoIP 전화의 형태와 같이 텔레커뮤니케이션 장치(210c)를 포함한다. 텔레커뮤니케이션 장치(210c)는 사설망에 IP 주소 10.10.10.100가 할당된다.

일 실시예에서, 서버(102)는 시그널링 서버를 포함하고, 이는 제1 컴퓨팅 다바이스(102a)와 제2 컴퓨팅 디바이스(102b)와 같이, 컴퓨팅 디바이스들 간에 통신 세션을 설정하기 위한 시그널링 서비스의 유형을 제공한다. 일 실시예에서, 서버(102)는 세션 초기화 프로토콜, SIP를 지원하며, 이는 비디오, 음성, 채팅, 게이밍, 및 가상 실현과 같은 멀티미디어 요소를 포함하는 대화형 유저 세션을 초기화하기 위한 인터넷 엔지니어링 태스크 포스 (IEFT) 표준 프로토콜이다. 일 실시예에서, SIP는 오픈 시스템 인터커넥션 (OSI) 통신 모델의 어플리케이션 계층에서 동작한다. 몇 실시예에서, 제1 컴퓨팅 디바이스(102a)는 SIP 프로콜을 통해서와 같이 시그널링으로 세션을, 시그널링 경로(220)을 통해 시그널링 서버(102c)로 초기화한다. 일 실시예에서, 게이트웨이(340)와 관련한 시그널링 서버(102c)는 전화(210a 와 210b) 간의 VoIP 텔레커뮤니케이션 세션에 대해서와 같이, 제1 컴퓨팅 디바이스(102a)와 제2 컴퓨팅 디바이스(102b) 간에 매체 경로(225)를 설정하기 위해 이용된다.

환경(200)의 제1 컴퓨팅 디바이스(102a)는 게이트웨이(340)를 연결(341a)에 의한 네트워크(104)를 통해 액세스하는, 방화벽(205a)를 통과하는 사설 또는 공중망의 일부일 수 있다. 방화벽(205a)는 공중망에 대한 액세스와 통과를 제공하며, 24.24.24.100의 IP 주소가 할당된다. 제1 컴퓨팅 디바이스(102a)는 VoIP 통신 장치와 같은 텔레커뮤니케이션 장치(210a)나 그 외 실시간 데이터 통신 장치와 통신하거나 인터페이스 또는 결합되어 있다. 제2 컴퓨팅 디바이스(102b)는 사설망의 일부로 192.168.20.20의 IP 주소가 할당된다. 부가하여, 제2 컴퓨팅 디바이스(102b)는 소프트웨어 기반의 VoIP 텔레커뮤니케이션 장치나 프로그램과 같은 소프트웨이 기반의 텔레커뮤니케이션 장치(210b)를 포함한다. 제2 컴퓨팅 장치(102b)는 연결(341b)에 의한 네트워크(104)를 통해 게이트웨이(340)에 액세스하여 216.216.10.10의 공중망 IP 주소가 할당된 방화벽을 통과한다. 방화벽(205a 및 205b)는 NAT 방화벽과 같이, 당업자에게는 잘 알려진 방화벽의 유형일 수 있다.

도 2A의 제1 컴퓨팅 디바이스(102a) 및 제2 컴퓨팅 디바이스(102b)는 환경(200)에서 애드혹 피어투피어 가상망 연결을 제공하기 위해 본 발명의 원격 액세스 클라이언트(120)를 포함하여 이용한다. SSL VPN 연결과 같이, 게이트웨이(340)에 대한 터널 및 가상 개인 연결을 유지하는 데에 부가하여, 본 발명의 원격 액세스 클라이언트(120)은 도달하려는 피어에 대한 SSL VPN 연결과 같은, 직접 애드혹 연결을 설정하는 로직, 기능 및 동작을 가지고 있다. 도 2A에 비추어, 도 2B의 설명적 방법(260)은 본 발명의 일 설명적 실시예에서 매체 경로(225)에 대해 피어투피어 보안 통신 세션이 설정되는 방법을 설명하기 위한 것이다. 방법(260)으로 나타낸 본 발명의 피어투피어 라우팅 기술은 VoIP 통신과 그 외 실시간 데이터 통신에 관한 레이턴시를 줄이고 양질의 음성을 제공한다.

설명적 방법(260)의 간단한 개요로, 단계 262에서, 컴퓨팅 디바이스(102a 및 102b)는 게이트웨이(340)와의 터널링 세션을 설정한다. 단계 264에서, 제1 컴퓨팅 디바이스(102a)는 시그널링 서버(102b)에 대한 시그널링 경로(220)를 거쳐 시그널링 프로토콜을 이용하여 게이트웨이(340)를 통해 제2 컴퓨팅 디바이스(102b)에 대한 세션을 초기화한다. 세션은 제1 컴퓨팅 디바이스(102a)와의 통신시 텔레커뮤니케이션 장치(102a)에 의해 초기화된다. 단계 266에서, 시그널링 서버(102c)는 텔레커뮤니케이션 세션을 셋업하고, 단계 268에서, 제1 컴퓨팅 디바이스(102a)에 제2 컴퓨팅 디바이스(102b)의 제1 네트워크 식별자를 제공한다. 제1 네트워크 식별자는 게이트웨이(340)로 터널(341b)를 통해 설정된 IP 주소에 기초하여 제2 컴퓨팅 디바이스(102b)의 호스트 네임이나 IP 주소와 같은 네트워크 주소를 포함한다. 단계 270에서, 제1 컴퓨팅 디바이스(102a)는 연결이나 통신 세션을 설정하도록 제1 네트워크 식별자를 이용하여 제2 컴퓨팅 디바이스(102b)에 통신한다.

다른 개요로, 단계 272에서, 게이트웨이(340)는 제1 컴퓨팅 디바이스(102a)에 의한 통신을 인터셉트하고 제2 컴퓨팅 디바이스(102b)에 대한 제2 네트워크 식별자를 제1 컴퓨팅 디바이스(102a)에 제공한다. 제2 네트워크 식별자는 제2 컴퓨팅 디바이스(102b)의 최근의 공지의 공중 IP 주소와 같이, 제1 컴퓨팅 디바이스(102a)에 의해 직접 또는 공중 액세스 가능한 제2 컴퓨팅 디바이스(102b)의 IP 주소나 호스트 네임을 포함한다. 단계 274에서, 일 실시예에서, 게이트웨이(340)는 제2 컴퓨팅 디바이스(102b)에 통신하여 제2 컴퓨팅 디바이스(102b)에게 제1 컴퓨팅 디바이스(102a)가 방화벽(205b)를 거쳐 제2 컴퓨팅 디바이스(102b)에 연결하도록 스위머 (swimmer) 세션을 설정하라고 요청한다. 몇 실시예에서, 게이트웨이(340)는 단계 276에서 제1 컴퓨팅 디바이스(102a)와 제2 컴퓨팅 디바이스(102b)에 암호화 키를 제공한다. 단계 278에서, 제1 컴퓨팅 디바이스(102a)는 제2 컴퓨팅 디바이스(102b)에 대한 직접 연결, 통신 세션 또는 매체 경로(255)를 설정한다. 다른 실시예에서, 단계280에서, 제1 컴퓨팅 디바이스(102a) 및/또는 제2 컴퓨팅 디바이스(102b)는 통신을 허용하기 전에 다른 컴퓨팅 디바이스에 의해 수신되는 암호화 키에 일치한다.

설명적 단계 262의 실시예에서, 컴퓨팅 디바이스(102a 및 102b)는 터널링이나 게이트웨이 프로토콜의 형태와 같은 적당한 수단 및/또는 메커니즘으로 게이트웨이(304)와의 연결을 설정한다. 몇 실시예에서, 게이트웨이(340)에의 연결(341a 및 341b)은 가상 사설망 연결을 형성하고, 다른 실시예에서는 도 2A에서 IP 범위 10.10.10.XXX로 식별되는 사설망과 같은 사설망에 대한 보안 통신을 제공하도록 SSL 또는 TLS를 이용한다. 일 실시예에서, 컴퓨팅 디바이스(102a 및 102b)는 공중망을 거쳐 방화벽(205a-205b)를 통과하여 게이트웨이(340)에 연결되고, 다른 실시예에서는 컴퓨팅 디바이스(102a 및 102b)는 사설망을 거쳐 게이트웨이(340)에 연결되며 방화벽(205a-205b)을 통과하지 않는다. 당업자라면 컴퓨팅 디바이스(102a-102b)가 게이트웨이(340)에 연결되어 통신하는 다양한 방법을 이해할 것이다.

설명적 단계 264에서, 일 실시예로 하드 IP 폰과 같은 텔레커뮤니케이션 장치(210a)는 소프트 IP 폰과 같은 텔레커뮤니케이션 장치(210b)에 대한 전화 호출과 같은 텔레커뮤니케이션 세션을 초기화한다. 몇 실시예에서, 텔레커뮤니케이션 장치(210a)는 텔레커뮤니케이션 장치(210b)의 연장을 나타내어 전화 호출을 초기화한다. 텔레커뮤니케이션 장치(210a)가 텔레커뮤니케이션 세션을 초기화하면, 텔레커뮤니케이션 세션이나 매체 세션을 설정하는 초기화나 요청이 SIP 프로토콜, 독

점식 시그널링 프로토콜 또는 그 외 시그널링에 적합한 프로토콜을 거쳐 시그널링 서버(102a)에 보내진다. 신호는 게이트웨이(230)에 터널링 세션(341a)를 거쳐 시그널링 경로(220)를 거쳐 통신되며 게이트웨이(340) 뒤의 사설망의 인트라넷 루트를 거쳐 시그널링 서버(102c)에 도달한다.

방법(260)의 설명적 실시예가 VoIP 또는 텔레커뮤니케이션 시그널링 및 세션에 비추어 설명되었지만, 당업자라면 본 발명이 통신 세션, 실시간 또는 비디오, 음성, 채팅, 게이밍 및 가상 실현 등의 멀티미디어 요소를 포함하는 대화형 유저 세션과 같은 것의 형태를 초기화하는 데에 이용된다는 것이 이해될 것이다. 이와 같이, 텔레커뮤니케이션 장치(210a-210b), 시그널링/신호 경로(220) 및 시그널링 서버(120a)는 통신 세션의 유형에 대응하는 장치, 시그널링, 프로토콜 및 통신의 형태를 적당하게 포함할 수 있다.

설명적 단계 266의 실시예로, 신호 서버(102c)는 통신 세션의 형태를 셋업하거나 설정하며, 일 실시예에서 시그널링 서버(102c)는 텔레커뮤니케이션 장치(210a)에 의해 초기화된 VoIP 전화 호출과 같은 텔레커뮤니케이션 세션을 셋업한다. 텔레커뮤니케이션이나 그 외 매체 세션을 셋업할 때, 단계 270에서 시그널링 서버(102c)는 특정 네트워크 주소를 거쳐 피어 텔레커뮤니케이션 장치(210b)에 접촉하고, 신호 보내고, 연결되거나 통신하도록 초기화 텔레커뮤니케이션 장치(210a) 및/또는 제1 컴퓨팅 디바이스(102a)에 명령, 요청하거나 신호 보내거나 통신한다. 몇 실시예에서, 초기화 텔레커뮤니케이션 장치(210a)에 시그널링 서버(102c)에 의해 제공되는 네트워크 주소는 게이트웨이(340) 뒤에 사설망의 컴퓨팅 디바이스(102b)에 대한 네트워크 주소, 즉 10.10.10.XXX를 포함한다. 일 실시예에서, 피어 텔레커뮤니케이션 장치(210b)의 네트워크 주소는 기업체 사설망 주소를 포함한다.

이점에서, VPN 사설 IP 주소를 거쳐 피어 텔레커뮤니케이션 장치(210b)에 접촉하는 대신에, 260의 방법은 원격 액세스 클라이언트(120)를 거쳐 텔레커뮤니케이션 장치(210a) 및/또는 제1 컴퓨팅 디바이스(102a)가 피어 또는 타겟 텔레커뮤니케이션 장치(210b) 또는 제2 컴퓨팅 디바이스(102b)에 직접 접촉하는 것을 용이하게 한다. 본 발명의 기술은 VoIP 프로토콜에 특정적인 것이 아니고, 컴퓨팅 디바이스 간의 피어투피어 프로토콜과 같은 다른 프로토콜에도 적용될 수 있다. 본 발명의 기술은 클라이언트가 연결 시도하고 있는 리소스의 IP 주소를 이용해 결정을 내린다.

단계 270에서, 텔레커뮤니케이션 장치(210a)가 소프트 IP 폰의 VPN 사설 IP 주소와 같이 단계 268에서 시그널링 서버(340)에 의해 제공되는 제1 네트워크 주소로 텔레커뮤니케이션 장치(210b)에 대한 데이터 연결을 초기화한다. 일 실시예에서, 게이트웨이(340)는 동일하게 설정된 VPN 터널(341a)를 통해 대역외 신호를 하드 IP 폰(210a)에 대한 트래픽을 용이하게 하는 제1 컴퓨팅 디바이스(102a)로 보낸다. 당업자라면 게이트웨이(340)는 컴퓨팅 디바이스(102b) 및/또는 텔레커뮤니케이션 장치(210b)를 적합한 수단 및/또는 메커니즘에 의해 직접 접촉하기 위해 텔레커뮤니케이션 장치(210) 및/또는 컴퓨팅 장치(102a)에 통신한다. 예를 들어, 게이트웨이(340)는 제2 터널링 세션을 통해 제1 컴퓨팅 디바이스(102a)에 제2 네트워크 주소를 통신한다.

몇 실시예에서, 게이트웨이는 최근의 공지된 공중 IP 주소의 제1 컴퓨팅 디바이스(102a)에게 제2 컴퓨팅 디바이스(102b)가 게이트웨이(340)에 접촉하는 데에 이용되는 소프트 IP 폰(210b)를 실행하고 있다고 나타낸다. 다른 실시예에서, 이 공중 IP는 제2 컴퓨팅 디바이스의 실제 IP 주소가 아니고 제2 컴퓨팅 디바이스(102b) 뒤에 있는 방화벽(205b)의 IP 주소일 수 있다. 컴퓨팅 디바이스(210a)가 방화벽(205b)의 공중 IP 주소와 직접 접촉하게 되면, 패킷은 방화벽(205b)에 의해 거부된다. 이들 실시예에서, 게이트웨이(340)는 컴퓨팅 디바이스(102b)에게 당업자에게 알려진 것을 제1 컴퓨팅 디바이스(102a)에 대한 스위밍 세션으로 설정하라고 명령한다. 전방 홀이 방화벽(205b)에 뚫리고 이를 통해 제1 컴퓨팅 디바이스(102a) 가 통과하거나 돌아간다. 다른 실시예에서, 적당한 수단 및/또는 메커니즘을 이용하여 제1 컴퓨팅 디바이스(102a)가 제2 컴퓨팅 디바이스(102b)에 연결되어 통신하도록 방화벽(205b)를 관통하게 한다.

설명적 방법 260이 방화벽(205a) 뒤에 제2 컴퓨팅 디바이스(102n)을 갖는 도 2A의 환경(200)과 관련하여 설명되었지만, 당업자가 이해할 수 있는 바와 같이, 이 방법 260은 제2 컴퓨팅 디바이스(102b)가 방화벽(205a)을 통과하지 않고 직접 액세스 가능한 환경에서 이용될 수 있다. 이와 같이, 이 방법 260)은 단계 274에서 제2 컴퓨팅 디바이스(102b)에게 제1 컴퓨팅 디바이스(102a)가 제2 컴퓨팅 디바이스(102b)에게 연결되도록 스위머 세션이나 그 외 메커니즘을 제공하도록 명령할 필요가 없다.

몇 실시예에서, 게이트웨이(340)는 단계 276에서 보안 통신을 위해 컴퓨팅 디바이스(102a-103b) 간의 보안 키를 협상한다. 컴퓨팅 디바이스(102a-102b) 상의 원격 액세스 클라이언트는 이 키를 이용하여 보안 및 암호화 통신하고/하거나 다른 컴퓨팅 디바이스를 인증하거나 인가한다. 다른 실시예에서, 악성 컴퓨팅 디바이스가 이 개방 홀을 이용하지 못하도록, 게이트웨이(340)는 단계 276에서 두 컴퓨팅 디바이스(102a 및 102b) 사이에 보안 키를 협상하고, 각 원격 액세스 클라이언트(120)는 데이터 통신을 허용하기 전에 키가 일치하는 것을 확실히 하게 한다. 예를 들어, 스위머 세션을 설정하는 실시예에서, 이 키는 이 개방 홀에 들어가는 패킷이 스위머 세션이 예정된 컴퓨팅 디바이스로부터 나오는 것을 확실히 한다.

다른 실시예에서, 게이트웨이(340)는 컴퓨팅 디바이스(102a-102b) 사이의 피어투피어 통신 세션의 보안 메커니즘을 제공하도록 단계 276를 실행하지 않는다. 예를 들어, 컴퓨팅 디바이스(102a-102b)는 동일한 사설 기업망에 있으므로, 따라서 신뢰적이다. 다른 실시예에서, 보안 키를 협상하는 게이트웨이(340) 대신에, 컴퓨팅 디바이스(102a-102b)는 피어투피어 통신을 위해 다른 컴퓨팅 디바이스를 인증 및/또는 인가하기 위한 적합한 수단 및/또는 메커니즘을 이용한다. 몇 실시예에서, 컴퓨팅 디바이스(102a-102b)는 경로(341a)를 통해 또는 단계 280에서, 단계 278에서 설정된 매체 경로(225)를 통해서와 같이, 게이트웨이 터널링 세션을 통해 인가 및/또는 인증할 수 있다. 에를 들어, 각 컴퓨팅 디바이스(102-102b)의 원격 액세스 클라이언트(120)는 데이터가 연결(225)을 통해 통신되게 하기 전에 설정된 매체 경로(225)를 통해 키의 일치를 체크한다.

단계 278에서, 통신 유형에 대한 직접 매체 경로(224)는 게이트웨이(340)를 통과하지 않고 컴퓨팅 디바이스(102a-102b) 사이에 설정되고, 어떤 실시예에서는 컴퓨팅 디바이스(102a-102b)의 각 VPN 할당 IP 주소를 이용하지 않고 그 대신에 이들의 상주 네트워크에 의해 할당된 공중 IP 주소나 IP 주소를 이용한다. 본 발명의 기술을 이용하여, 컴퓨팅 디바이스(102a-102b)의 각 원격 액세스 클라이언트(120)는 서로 임시의 피어투피어 SSL 게이트웨이로 작용하여, 게이트웨이(340)를 통해 통신하지 않고 직접 서로의 SSL 세션을 해독한다. 경로(225)를 거친 직접적인 피어투피어 통신 세션은 게이트웨이(340)를 통한 여분의 홉을 방지한다. 이는 게이트웨이(340)를 통하는 더 긴 루트로 인한 레이턴시를 줄여주고, 도 2A에 나타낸 VoIP 통신과 같은 실시간 데이터 통신의 질, 성능 및 경험을 향상시킨다.

몇 실시예에서, 게이트웨이(340)는 컴퓨팅 디바이스(102)가 피어투피어 통신 세션을 설정하거나 게이트웨이(340)를 통해 리소스를 액세스하려고 할 때 마다 방법 260의 기술을 자동으로 실행하도록 구성된다. 다른 실시예에서, 게이트웨이(340)는 발신지 IP 주소, 목적지 IP 주소나 이들의 조합에 대한 특정 IP 주소 범위에 대해서만 이 방법 260의 기술을 자동으로 실행하도록 구성된다. 다른 실시예에서, 게이트웨이(340)는 게이트웨이(340)를 통해 액세스되고 있는 어플리케이션 및/또는 리소스에 기초하여 이 기술을 실행할 수 있다. 예를 들어, 일 실시예에서, 게이트웨이(340)는 게이트웨이(340)를 통해 스크린을 공유하는 데스크톱 또는 스크린 공유 어플리케이션의 형태에 대해 이 기술을 자동으로 실행할 수 있다. 다른 실시예에서, 게이트웨이(340)는 비지니스 규칙, 액세스 제어 폴리시, 또는 그 외 컨피규레이션, 알고리즘 및 통계 자료의 유형에 기초하여 이 기술을 실행하도록 결정할 수 있다. 예를 들어, 게이트웨이(340)는 피어 컴퓨팅 디바이스 사이에 핑 기반 (ping-based)의 타이밍 통계 자료에 기초하여 이 기술을 실행할 수 있다. 피어 컴퓨팅 디바이스는 게이트웨이(340) 보다 서로 근접하는 경우, 게이트웨이는 피어투피어 라우팅 기술을 실행한다. 당업자는 본 발명의 게이트웨이가 본 발명의 피어투피어 라우팅 기술을 실행하도록 구성되는 여러 방법을 이해할 것이다.

일 형태에서, 본 발명은 손실 프로토콜을 거친 전송을 위해 구성된 무손실 프로토콜 패킷을 거친 통신을 가능하게 하는 것과 관련된다. 도 3B에 나타낸 일 기술로, 본 발명은 예를 들어, TCP 또는 SSL/TCP 연결을 통해 UDP에 의해 RTP를 통신하는 것과 같이 무손실이나 신뢰성 프로토콜을 거쳐 손실이나 비신뢰 프로토콜을 통신할 때 이상 확인 기술을 이용한다. 도 3C에 나타낸 다른 기술로, 본 발명은 손실 프로토콜을 거쳐 전송하도록 구성된 무손실 프로토콜 패킷을 거쳐 통신하기 위해 페이로드 시프팅을 이용한다. 몇 실시예에서, 본 발명의 이들 기술은 당업자가 아래 기재에 비추어 이해하는 바와 같이 UDP 레벨에서 전송 계층 보안 (TLS)의 성취를 도와준다.

이상 확인 기술을 실행하기 위한 본 발명의 실시예의 방법 360은 도 3A의 설명적 환경(360)에 관련하여 또한 부가적으로 도 1A-1E에 관련하여 설명된다. 간단한 개요로, 환경(300)은 컴퓨팅 디바이스(102b)의 피어 클라이언트(105b) 또는 다르게는 네트워크(104)를 거친 게이트웨이(34)와 통신하는 컴퓨팅 디바이스(102a)의 클라이언트(105a)를 포함한다. 몇 실시예에서, 클라이언트(105a)는 IP 라우터(305a-305b)를 통과하거나 네트워크(104)는 IP 라우터(305a-305b)를 갖는다. 다른 실시예에서, 컴퓨팅 디바이스(102a-102b)와 게이트웨이(340)는 동일한 네트워크(104)에 있을 수 있다. 부가하여, 텔레커뮤니케이션 장치(210a)는 클라리언트(105a)와 관련되고 제2 텔레커뮤니케이션 장치(210b)는 피어 클라이언트(105b)나 게이트웨이(340)와 관련될 수 있다.

클라이언트(105a)는 제1 네트워크 스택(310a)를 포함하고, 클라이언트(105)나 게이트웨이(340)는 제2 네트워크 스택(310b)를 포함한다. 네트워크 스택(3201a-310a)는 오픈 시스템 인터커넥션 (OSI) 통신 모델의 네트워크 계층과 같은 하나 이상의 네트워크 계층을 포함한다. 예를 들어, 도 3A에서 나타낸 바와 같이, 네트워크 스택(310a-310b)은 TCP/IP 기반의 네트워크(104)에 대해 당업자에게 잘 알려진 바와 같이 적당한 프레임 계층의 상부에 TCP/IP(343a-343) 통신 계층을 포함한다. TCP 계층(343a-343b)는 신뢰 또는 무손실 프로토콜의 설명적 실시예를 포함한다. 예를 들어, 당업자에게 잘 알려진 바와 같이 TCP(343a-343b)에서, 네트워크 스택(310a-310b) 또는 TCP 드라이버와 같은 이들의 드라이버나 메커니즘은 프로토콜의 무손실이나 신뢰 특성 중 하나 이상을 제공하기 위한 알고리즘과 동작을 실행하고, 로직이나 기능

을 포함한다. 예를 들어, TCP(343a-343b)를 지원하기 위해, 네트워크 스택(310a-320b)은 패킷 오더링, 패킷 재전송, 패킷 수신 확인, 흐름 제어 알고리즘, 슬라이딩 윈도우 알고리즘 및/또는 네이글 (nagle)의 알고리즘, 및 그 외 TCP(343a-343b)나 다른 무손실 프로토콜에 비추어 당업자라면 이해하는 바와 같이 신뢰적 동작과 알고리즘을 실행할 수 있다.

부가하여, 네트워크 스택(310a-310b)는 SSL 또는 SSL VPN 통신을 지원하기 위한 SSL(341a-341b) 계층을 포함한다. 예를 들어, SSL 계층(341a-341b)는 원격 액세스 클라이언트들(120) 간이나 원격 액세스 클라이언트(120)와 게이트웨이(340) 간의 게이트웨이나 터널링 세션에 이용된다. 도 3A에 나타낸 바와 같이, 네트워크 스택(310a-310b)는 또한 TCP와 같은 무손실 프로토콜(343a-343b)을 통해 통신되도록, UDP와 같은 손실 프로토콜(342a-342b)에 계층을 제공한다. 몇 실시예에서, 손실이나 비신뢰 프로토콜(342a-342b)은 UDP를 통한 실시간 프로토콜 (RTP)을 포함하고, 음성이나 오디오의 표현과 같은, 실시간 데이터의 형태를 갖는 페이로드를 포함한다. 다른 실시예에서, 손실 프로토콜(342a-342b)은 도 2A 및 2B와 관련하여 상술된 방법 260에 의해 설정된 세션과 같은 VoIP 세션에서 클라이언트(105a)로의 및 로부터의 통신을 통해 VoIP를 전달한다. UDP(342a-342b)와 같은 무손실 프로토콜은 음성과 같은 실시간 어플리케이션에 대해 선택되는데, 이는 무손실 프로토콜을 통해서와 같이, 신뢰적으로 패킷을 얻는 것 보다는 제때에 피어 클라이언트(105b)와 같은 수신자에게 패킷을 얻게 하는 것이 더 중요하기 때문이다.

네트워크 스택(310a-310b)은 본 발명의 원격 액세스 클라이언트(120)의 심(shim; 322-322b)를 포함한다. 심(322a-322b)은 원격 액세스 클라이언트(120)의 일부를 포함하고, 몇 실시예에서는 네트워크 드라이버, 네트워크 드라이버 인터페이스, 또는 그 외 여기 기재된 본 발명의 이상 확인 기술을 제공하기 위한 네트워크 계층 관련 기술을 포함한다. 심(322a-322b)은 소프트웨어, 하드웨어 또는 소프트웨어와 하드웨어의 조합을 포함한다. 일 실시예에서, 심(322a-322b)은 네트워크 패킷이 TCP 층(343a-343b)에 이르기 전에 네트워크 스택의 IP 계층에서 동작한다. 다른 실시예에서, 심(322a-322b)은 TCP 층(343a-343b)에서 동작한다. 당업자라면 심(322a-322b)이 무손실 프로토콜의 계층을 포함하거나 이에 인접하는 네트워크 스택(310a-310b)에서 무손실 프로토콜의 동작 계층과 관련되는 식으로 동작한다.

도 3B의 방법 360으로 나타낸 바와 같이 본 발명의 이상 확인 기술은 UDP(342a-343b) 등의 손실 프로토콜이 TCP(343a-343b) 등의 무손실 프로콜을 거쳐 통신되게 한다. 심(322a-322b)이 TCP 패킷의 수신의 이상 확인을 발함으로서, 본 발명의 기술은 TCP(343a-343b)의 예에서, 패킷 오더링, 패킷 재전송, 흐름 제어 알고리즘, 슬라이딩 윈도우 알고리즘 및/또는 네이글의 알고리즘과 같은, 무손실 프로토콜의 신뢰성 메커니즘, 동작 및 알고리즘을 방지한다. 이와 같이, 손실 프로토콜(342a-342b)는 무손실 프로토콜(343a-343b)를 통해 통신되지만 실시간 데이터 통신시와 같이 원하는 손실이나 비신뢰 특성을 유지할 수 있다. 이 기술은 손실 프로토콜이 보안 통신되게 하거나 터널링 프로토콜을 통해서나, 무손실 프로토콜의 무손실 특성을 손실 프로토콜 통신에 적용하지 않으면서 간단히 TCP/IP를 통해 게이트웨이를 통과하게 한다.

방법 360의 간단한 개요로, 단계 365에서, 컴퓨팅 디바이스(102a 및 102b) 또는 게이트웨이(340)는 TCP 연결과 같은 무손실 프로토콜 기반의 연결을 설정하고, 이로 인해 무손실 프로토콜 패킷이 통신되게 된다. 단계 370에서, 본 발명의 원격 액세스 클라이언트(120)는 무손실 프로토콜 패킷의 페이로드가 RTP 또는 UDP 등의 손실 프로토콜을 포함하거나, 실시간 데이터를 포함한다고 검출할 수 있다. 일 실시예에서, 단계 375에서, 방법 360은 단계 367의 대역외 TLS 또는 SSL 세션을 통해 제공되는 키와 같은 키로 페이로드를 암호화한다. 단계 380에서, 무손실 프로토콜 패킷의 수신 이상 확인은 심(322a-322b)에 의해서와 같이, 네트워크 스택(310a-310b)에 통신되거나 제공된다. 무손실 프로토콜 패킷의 수신 이상 확인에 응답하여, 단계 385에서, 각 네트워크 스택(310a-310b)은 무손실 프로토콜의 신뢰 또는 무손실 특성을 제공하는 알고리즘과 동작 중 하나 이상이나 모두를 실행하지 못한다. 단계 390에서, 손실 프로토콜 페이로드를 갖는 무손실 프로토콜 패킷은 네트워크 스택(310a-310b) 사이에서 통신된다.

방법 360의 단계 365에서, 무손실 프로토콜 연결은 무손실 프로토콜의 유형을 이용하여 적당한 수단 및/또는 메커니즘을 통해 설정된다. 일 실시예에서, 클라이언트(105a)의 네트워크 스택(310a)은 네트워크 스택(310b)을 갖는 피어 클라이언트(105a)에게 TCP와 같은 무손실 프로토콜 연결을 설정한다. 다른 실시예에서, 클라이언트(105a)의 네트워크 스택(310a)는 네트워크 스택(310b)를 갖는 게이트웨이(340)에 대한 무손실 프로토콜 연결을 설정한다. 부가하여, 단계 365의 무손실 프로토콜 연결은 SSL와 같이 보안식으로 또는 가상 개인 연결로 설정된다. 네트워크 스택(310a-310b)이 동일한 네트워크 계층을 갖는 것으로 도시되었지만, 당업자라면 네트워크 스택이 다른 버전으로 되어 있거나 다른 운영 시스템 및/또는 드라이버와 관련되는 대응하는 계층을 가지며, 각 네트워크 계층(310a-310b)은 부가의 층, 적은 층 또는 다른 층을 가질 수 있다는 것이 이해될 것이다.

일 실시예에서 단계 360에서, 원격 액세스 클라이언트(120)는 패킷 캡쳐 메커니즘(365)를 통하는 것과 같이 네트워크 패킷을 인터셉트하여, 네트워크 패킷의 페이로드에서 이용되는 프로토콜의 유형이나 네트워크 패킷의 페이로드의 컨텐트의 유형을 결정하는 데에 적합한 수단 및/또는 메커니즘에 의해 네트워크 패킷을 조사한다. 몇 실시예에서, 원격 액세스 클라이언트(120)의 심(322a-322b)은 네트워크 패킷을 인터셉트하여 검사하는 데에 이용된다. 일 실시예에서, 원격 액세스 클

라이언트(120)는 네트워크 패킷을 차단하여 네트워크 패킷이 무손실 프로토콜이나 TCP와 같은 특정 무손실 프로토콜을 포함하는지를 판정한다. 네트워크 패킷이 무손실 프로토콜인 경우, 원격 액세스 클라이언트(120)는 프로토콜의 유형 및/또는 데이터의 유형을 판정하도록 페이로드를 체크한다. 일 실시예에서, 원격 액세스 클라이언트(120)는 페이로드를 나타내는 손실 프로토콜의 헤더의 일부와 같은 네트워크 패킷의 페이로드의 적합한 필드에 의해, 페이로드가 손실 프로토콜 컨텐트를 갖는지를 판정한다. 다른 실시예에서, 원격 액세스 클라이언트(120)는 페이로드의 데이터에 의해, 페이로드가 손실 프로토콜을 포함하거나 실시간 데이터를 포함하는지를 판정한다.

일 실시예에서, 원격 액세스 클라이언트(120)는 TCP 패킷이 RTP나 UDP의 페이로드를 포함한다고 판단하여, 페이로드의 암호화를 적용한다. 원격 액세스 클라이언트(120)는 적합한 방법으로 제공되는 키로 암호화의 유형을 이용하여 네트워크 패킷의 페이로드를 암호화한다. 몇 실시예에서, 키나 사이퍼(cipher)는 다른 실시예에서 세션이 먼저 협상된 후 동일한 소켓이 데이터 통신에 이용되는 종래의 TLS 세션과 대비하여, 도 3A에서 나타낸 바와 같이 클라이언트(105a-105b) 간이나 클라이언트(105a)와 게이트웨이 간의 대역외 TLS 세션을 통해 협상된다. 몇 실시예에서, 단계 375에서의 암호화는 패킷마다 실행된다. 다른 실시예에서, 암호화는 한번에 다수의 패킷에 대해 실행된다.

본 발명의 방법 360의 단계 380에서, 네트워크 패킷, 예를 들어 무손실 프로토콜 패킷의 수신 이상 확인이 각 전송 및 수신 컴퓨팅 디바이스(102a-102b) 또는 게이트웨이(340)을 포함하는 네트워크 스택(310a-310b)에 발해지고, 통신되어, 제공된다. 심(322a-322b), 원격 액세스 클라이언트(120)의 일부, 네트워크 스택(310a-310b)의 일부는 네트워크 패킷의 수신 이상 확인을 발한다. 일 형태에서, 네트워크 패킷의 수신 이상 확인은 네트워크 패킷의 실제 수신을 확인하기 위한 것이 아니고 네트워크 스택(310a-310b)과 관련된 무손실 프로토콜의 무손실 및 신뢰 메커니즘을 방지하기 위해서 통신된다는 점에서 실패이다. 이와 같이, 네트워크 패킷의 수신 이상 확인은 네트워크 패킷의 수신의 실제 확인과 동일한 형태로 이루어진다.

몇 실시예에서, 수신의 이상 확인은 네트워크 패킷이나 패킷들을 통신하기 전에 네트워크 스택(310a-310b)에 발해진다. 다른 실시예에서, 수신의 이상 확인은 네트워크 패킷을 통신한 후지만 한번에 또는 수신 네트워크 스택(310a-310b)의 무손실 프로토콜 메커니즘이 전송된 네트워크 패킷에 인가되지 않도록 하는 식으로 발해진다. 일 실시예에서, 네트워크 패킷의 수신의 이상 확인은 각 네트워크 패킷에 발해지고, 다른 실시예에서는 통신 세션이나 무손실 프로토콜 연결에 대해 한번씩 발해진다. 더욱, 당업자가 이해할 수 있는 바와 같이 수신의 이상 확인은 여러 운영 시스템에 대해 네트워크 스택(310a-310b)의 여러 위치에서 실행될 수 있다. 예를 들어, 일 실시예에서, 수신 확인은 마이크로소프트의 윈도우 운영 시스템에서 네트워크 드라이버 인터페이스 사양 (NDIS) 드라이버 레벨에서 발해질 수 있다.

방법 360의 단계 385에서, 단계 380로부터 네트워크 패킷의 수신의 이상 확인을 수신한 네트워크 스택(310a-310b)는 이런 수신에 응답하여, 무손실 프로토콜의 하나 이상의 무손실 특성을 제공하는 하나 이상의 알고리즘과 동작을 실행하지 않거나 실행 중단하거나, 실행 방지할 수 있다. 예를 들어, 무손실 프로토콜로서의 TCP의 실시예에서, 네트워크 스택(310a-310b)은 네트워크 패킷에 관련하여 다음 중 하나 이상을 실행하지 않는다: 패킷 오더링, 패킷 재전송, 흐름 제어 알고리즘, 슬라이딩 윈도우 알고리즘, 및/또는 네이글의 알고리즘. 몇 실시예에서, 수신의 이상 확인은 네트워크 스택(310a-310b)의 무손실 계층이 신뢰 알고리즘을 이용하지 않게 하기 위해 패킷 마다 수신되어야 한다. 이와 같이, 수신 네트워크 스택(310a-310b)은 패킷 마다 본 발명의 이상 확인 신호를 어느 패킷에 적용할지를 결정할 수 있다. 무손실 프로토콜의 신뢰 알고리즘이 적용되어야 하는 손실 프로토콜을 포함하는 무손실 프로토콜 네트워크 패킷이 있을 수 있다. 다른 실시예에서, 네트워크 패킷의 수신의 이상 확인은 무손실 프로토콜 세션이나 연결 동안 수신된 후속 패킷에 대해 신뢰 알고리즘을 이용하지 못하게 하기 위해 무손실 프로토콜 연결에 대해 한번 수신될 수 있다.

단계 390에서, 설명적 방법 360은 네트워크 스택(310a-310b)을 거쳐 무손실 프로토콜 페이로드를 갖는 무손실 프로토콜 패킷을 통신한다. 일 실시예에서, 무손실 프로토콜 패킷은 단계 385 후에, 다른 실시예에서는 단계 385 이전에 통신된다. 그런데, 무손실 프로토콜 패킷이 네트워크에서 손실되어도, 손실 프로토콜 패킷에 대해 예상하는 바와 같이 패킷을 재청구하려는 시도가 이루어지지 않는다.

방법 360의 설명적 실시예가 TCP에서와 같이 네트워크 패킷의 수신 이상 확인을 이용하여 설명되지만, 임의 유형의 표시, 요청 또는 명령들이 무손실 프로토콜의 신뢰 또는 무손실 알고리즘의 이용을 방지하도록 네트워크 스택(310a-310b)에 통신될 수 있다. 몇 실시예에서, 네트워크 스택(310a-310b)의 무손실 프로토콜 계층은 패킷 마다, 또는 세션이나 연결에 기초하여, 신뢰 알고리즘을 이용하지 않는 컨피규레이션, 플랙, 또는 명령을 갖도록 구성될 수 있다. 예를 들어, 무손실 프로토콜은 무손실 프로토콜 패킷의 헤더에 필드를 가지며, 이는 신뢰성이 패킷에 대해 폐기되거나 금지되어야 하는지의 여부를 나타낸다.

이하 도 3C를 참조하여, 무손실 프로토콜을 통해 손실 프로토콜에 따라 구성된 패킷을 전송하기 위해 행해지는 다른 실시예의 단계들을 페이로드 시프팅 기술로 언급되는 방법 345으로 나타낸다. 방법 345의 간단한 개요로, 단계 348에서, 비신뢰 전송 프로토콜을 이용하여 전송되는 제1 패킷은 클라이언트(105)와 같은 제1 디바이스에 의해 수신된다. 단계 350에서, 제1 디바이스(105)는 수신된 제1 패킷의 제1 페이로드와 제1 디바이스(105)와 제2 디바이스 사이에 설정된 TCP 연결과 관련되는 정보의 제1 TCP 헤더를 포함하는 제1 TCP 패킷을 형성한다. 제1 디바이스(105)는 단계 352에서 제1 TCP 패킷을 제2 디바이스에 전송한다. 단계 354에서, 제1 디바이스(105)는 비신뢰 전송 프로토콜을 이용하여 전송되는 제2 패킷을 수신하고, 단계 356에서 수신된 제2 패킷의 제2 페이로드와 제1 TCP 헤더 정보를 포함하는 제2 TCP 패킷을 형성한다. 단계 358에서, 제1 디바이스는 제2 디바이스로부터의 제1 페이로드의 수신의 확인을 수신하기 전에, 제2 디바이스에 제2 TCP 패킷을 전송한다.

도 3C를 이하 더욱 상세히 참조하면, 단계 348에서 비신뢰 전송 프로토콜을 이용하여 전송되는 제1 패킷이 제1 디바이스(105)에 의해 수신된다. 몇 실시예에서, 패킷은 UDP의 손실 프로토콜을 이용하여 전송되게 된다. 다른 실시예에서, 패킷은 UDP을 통한 RDP를 포함한다. 다른 실시예에서, 제1 패킷은 재전송을 위해 제1 디바이스(105)에 의해 수신된다. 또 다른 실시예에서, 제1 패킷은 네트워크 패킷(310a-310b)에 이르기 전에 필터 프로세스(322)에 의해 인터셉트된다. 필터 프로세스(322)는 유저 모드(332) 또는 커널 모드(334)에서 실행된다. 몇 실시예에서, 필터(322)는 미니 드라이버이다. 다른 실시예에서, 필터(322)는 NDIS 드라이버이다. 다른 실시예에서, 필터(322)는 제1 패킷을 인터셉트하도록 어플리케이션 후킹을 이용한다. 다른 실시예에서, 어플리케이션 후킹은 어플리케이션 프로그래밍 인터페이스 (API)를 통해 구현된다. 일 실시예에서, 네트워크 패킷의 후킹은 네트워크 스택(310a-310n)의 네트워크 계층에서 발생한다.

단계 350에서, 제1 디바이스(105)는 수신된 제1 패킷의 제1 페이로드와 제1 디바이스(105)와 제2 디바이스 간에 설정된 TCP 연결과 관련되는 정보의 제1 TCP 헤더를 포함하는 제1 TCP 패킷을 형성한다. 예를 들어, TCP 연결은 일 실시예에서 클라이언트(105)와 피처 컴퓨팅 디바이스(102b) 사이에, 그리고 다른 실시예에서는 클라이언트(105)와 게이트웨이(340) 사이에 설정된다. 몇 실시예에서, 제1 디바이스(105)는 TCP 패킷이 특정 TCP 포트를 개방하여 손실 프로토콜을 통해 전송되도록 구성된 패킷의 페이로드를 포함하는 것을 지시한다. 다른 실시예에서, 제1 디바이스(105)는 TCP 패킷이 TCP 헤더에 플랙을 설정하여 손실 프로토콜을 거쳐 전송되도록 구성된 패킷의 페이로드를 포함하는 것을 지시한다. TCP 헤더는 소스 노드에 관한 정보, 목적지 노드에 관한 정보, 또는 TCP 패킷을 특별히 식별하는 순서 번호를 포함한다.

단계 352에서, 제1 디바이스(105)는 제2 디바이스에 제1 TCP 패킷을 전송한다. 몇 실시예에서, 제2 디바이스는 게이트웨이(340)일 수 있다. 다른 실시예에서, 제2 디바이스는 "피어" 컴퓨팅 디바이스(102b)이다. 제1 TCP 패킷은 예를 들어, SSL 또는 TLS를 이용하여 제2 디바이스에 전송되기 전에 암호화된다.

단계 354에서, 제1 디바이스는 UDP와 같은 비신뢰 전송 프로토콜을 이용하여 전송되는 제2 패킷을 수신한다. 제2 패킷은 제1 패킷을 형성한 동일한 어플리케이션(338)으로부터 수신된다. 단계 356에서, 제1 디바이스(105)는 상술된 바와 같이, 수신된 제2 패킷의 제2 페이로드와 제1 TCP 헤더 정보를 포함하는 제2 TCP 패킷을 형성한다. 단계 358에서, 제1 디바이스(105)는 제2 디바이스로부터의 제1 페이로드의 수신 확인의 수신 전에, 제2 디바이스에 제2 TCP 패킷을 전송한다. 몇 실시예에서, 확인이 제2 디바이스로부터 수신되면, 제1 디바이스(105)는 패킷을 전송하기 전에 TCP 헤더 정보를 갱신한다. 다른 실시예에서, 제1 디바이스(105)는 갱신된 TCP 헤더 정보를 가지며 제2 페이로드를 갖는 제3 TCP 패킷을 형성한다. 제1 디바이스는 제3 TCP 패킷을 전송한다.

TCP 패킷의 수신시, 제2 디바이스는 필요하다면 이를 해독하여 페이로드가 손실 프로토콜을 이용하여 전송되게 구성된 하나 이상의 패킷이라고 결정한다. 제2 디바이스는 패킷이 수신되는 포트에 기초하여 또는 TCP 헤더 정보의 플랙에 의해 이를 결정한다. 한번 결정되면, 제2 디바이스는 페이로드로부터 TCP 헤더를 분리하여 페이로드를 전달한다.

다른 형태에서, 본 발명은 암호화된 네트워크 패킷에 대한 패킷 단편화를 줄임으로써 네트워크 통신을 최적화하기 위해 보고된 최대 전송 단위 (MTU) 파라미터를 조정하는 것과 관련된다. 이 기술은 도 3A의 환경(300)의 하나나 두 네트워크 스택(310a-310b)에 적용된다. 상술된 방법 360에 따라 처리된 네트워크 패킷과 같은 네트워크 패킷의 페이로드를 암호화하는 것은 페이로드의 크기를 증가시킨다. 즉, 네트워크 패킷의 크기는 암호화되지 않은 원래의 페이로드의 크기의 암호화된 페이로드로의 변경을 고려하여 증가한다.

도 3A를 참조하여, 네트워크 스택(310a-310b)는 이더넷 기반의 네트워크와 같은 네트워크에서 물리적 매체의 유형을 통해 전송될 수 있는 최대 단위의 데이터의 크기를 나타내기 위해 최대 전송 단위(402a-402b) (MTU) 파라미터를 포함한다. TCP/IP의 실시예에서, MTU(402a-402b)는 인터페이스가 데이터그램을 더 적은 유닛으로 파손하거나 단편화할 필요없이 인터넷 프로토콜 (IP) 계층 인터페이스에 의해 전송될 수 있는 최대 크기의 데이터그램이나 패킷을 나타낸다. MTU

파라미터(402a-402b)는 네트워크 인터페이스 카드와 같은 통신 인터페이스와 관련된다. 이더넷에 대한 디폴트 MTU 크기는 1,500바이트이고, IEEE 802.3은 1,492바이트이다. 당업자가 이해하는 바와 같이, 디폴트 MTU 크기는 토큰 링, FDDI, X.25 등과 같은 네트워킹 기술에 근거하게 된다.

도 4를 이하 참조하면, 흐름도는 본 발명의 MTU 조정 방법(400)의 실시예를 설명한다. 간단한 개요로, 단계 405에서, 컴퓨팅 디바이스 간의 세션은 제1 컴퓨팅 디바이스(102a)와 제2 컴퓨팅 디바이스(102b) 사이에 설정된다. 단계 410에서, 제1 컴퓨팅 디바이스(102a)와 같은 컴퓨팅 디바이스(102) 중 하나는 암호화된 페이로드를 갖는 네트워크 패킷을 검출한다. 단계 415에서, 컴퓨팅 디바이스(102a-102b)는 페이로드의 암호화 부분의 크기를 고려하도록 네트워크 스택(310a-310b)의 MTU(402a-402b)에 대한 세팅을 결정한다. 단계 420에서, MTU(402a-402b) 파라미터는 암호화 부분을 고려하여 감소된다. MUT(402a-402b)가 요청되거나 보고되면, MTU(402a-402b)는 이더넷에 대해 1,500와 같이, 물리적 계층과 관련된 MTU 크기 보다 더 작은 크기를 나타나게 된다.

이 기술을 이용하면, 네트워크(104)에서의 디바이스는 단편화되지 않고 네트워크 스택(310a-310b)에 대한 루트를 따라 암호화될 수 있는 감소된 MTU 크기에 따라 네트워크 스택(310a-310b)에 네트워크 패킷을 통신한다. 네트워크 패킷은 암호화되면 이더넷과 같은 물리적 네트워크 계층의 실제 MTU 크기에 맞추어야 한다. 예를 들어, MTU 파라미터(402a-402b)는 이더넷에 대해 디폴트 MTU 크기 1,500으로 설정되며, 방법 400에 따르면 암호화 오버헤드를 고려하기 위해 결정된 바이트 수, 예를 들어 100만큼 감소된다. 네트워크 패킷이 서버 리소스로부터 보고된 MTU(402a-402b) 크기 1,400와 동일한 크기를 포함하는 클라이언트에 전송된다. 네트워크 패킷이 게이트웨이(340)를 통과하여 SSL 터널을 거쳐 암호화되고, 이는 이어서 네트워크 패킷 크기를 1,475로 증가시킨다. 이 크기가 이더넷 물리적 매체의 MTU 크기에 맞기 때문에, 네트워크 패킷은 단편화되지 않게 된다.

방법 400의 단계 405에서, 도 2A의 클라이언트(105b) 또는 게이트웨이(340)와 같은, 제1 컴퓨팅 디바이스(102a)와 제2 컴퓨팅 디바이스(102b) 간에 통신 세션의 형태가 설정될 수 있다. 몇 실시예에서, 세션은 제1 컴퓨팅 디바이스 상의 원격 액세스 클라이언트(120)를 이용하여 설정된다. 일 실시예에서, 원격 액세스 클라이언트(120)는 SSL VPN 세션과 같은 게이트웨이(340)와의 세션이나, 피어 컴퓨팅 디바이스(102b) 상의 다른 원격 액세스 클라이언트(120)에 대한 세션을 설정한다.

단계 410의 실시예에서, 원격 액세스 클라이언트(120)는 암호화된 페이로드를 갖는 네트워크 패킷을 검출한다. 일 실시예에서, 패킷 캡쳐 메커니즘(365)은 네트워크 패킷을 인터셉트하고 에이전트(326)는 패킷이 암호화되었는지를 결정한다. 그러나, 필터(322) 또는 프레임 모니터(360)와 같은 원격 액세스 클라이언트(120)의 다른 부분이 패킷이 암호화되었는지를 결정할 수 있다. 일 실시예에서, 네트워크 패킷의 전체 페이로드가 암호화되는 한편, 다른 실시예에서는 페이로드의 일부가 암호화된다. 본 발명은 패킷이 암호를 갖는지를 결정하기 위한 수단이나 메커니즘의 형태를 이용한다. 예를 들어, 몇 경우, 원격 액세스 클라이언트(120)는 페이로드가 암호화된 것을 나타내는 네트워크 패킷의 플랙이나 필드를 체크한다. 다른 실시예에서, 원격 액세스 클라이언트(120)는 페이로드의 어느 부분이 비지능적인지를 체크하는데, 이것이 암호화로 인한 랜덤 데이터나 노이즈를 포함하기 때문이다. 부가하여, 암호화된 페이로드는 계층 2, 3, 6 또는 7의 암호화와 같이, 네트워크 스택(310a-310b)의 층과 관련하여 암호화될 수 있다.

단계 415의 실시예에서, 본 발명의 방법 400은 패킷마다에 기초하여, 또는 다른 실시예에서는 연결이나 세션에 기초하여 보고된 MTU(402a-402b) 크기의 조정을 결정하고, 단계 420에서 이에 따라 MTU(402a-402b)를 조정한다. 일 실시예에서, MTU(402a-402b)는 네트워크 패킷의 암호화 오버헤드의 양만큼 정확히 감소된다. 어떤 경우, 이 방법 400은 전체 세션이나 연결에 대해 MTU(402a-402b) 크기 조정을 결정하여 전체 세션에 대한 암호화 오버헤드를 고려하는 값으로 MTU(402a-402b)의 크기를 감소한다. 예를 들어, 네트워크 패킷이 가변 암호화 오버헤드를 갖지만, 조정은 최대 암호화 오버헤드를 고려하게 된다. 다른 실시예에서, MTU(402a-402b)는 네트워크 패킷의 엔드투엔드 네트워크 이동시 발생하는 게이트웨이에 의한 암호화와 같이, 네트워크 패킷이 네트워크 스택(310a-310b)를 떠날 때 발생할 수 있는 암호화를 고려하도록 조정될 수 있다.

부가하여, MTU(402a-402b) 크기는 암호화 오버헤드에 부가하여 다른 네트워크 성능 인자에 대해 조정된다. 몇 실시예에서, MTU(402a-402b)는 암호화 오버헤드로 인해 감소되지만, 또한 네트워크 통신에 관한 다른 오버헤드와 인자를 고려하도록 더욱 감소될 뿐만 아니라, 다른 경우에는 증가될 수도 있다. 예를 들어, MTU(402a-402b)는 암호화에 관련되지 않은 인자에 대해 이미 조정되었으며 본 발명의 이 기술을 이용한 후에 MTU(402a-402b)는 암호화 오버헤드를 고려하도록 감소된다. 당업자라면 본 발명의 기술에 따라서 암호화 오버헤드를 조정하는 것에 부가하여 MTU를 조정하기 위한 다른 요인이나 고려 사항이 있을 수 있다는 것이 이해될 것이다.

이하 도 5A 및 도 5B를 참조하면, 부가의 형태의 본 발명은 클라이언트측 어플리케이션 인식 네트워크 통신 우선 순위 기술에 관련된다. 본 발명의 원격 액세스 클라이언트(120)는 어플리케이션의 유형이나 우선 순위에 기초하여 클라이언트 상의 어플리케이션 네트워크 통신의 지능적 및 클라이언트 중심 우선 순위를 제공한다. 도 5A의 시스템(500)에서 도시된 바와 같이, 컴퓨팅 디바이스(102)의 원격 액세스 클라이언트(105)는 네트워크(104)에 연결된다. 클라이언트(105)는 하나 이상의 어플리케이션(338a-338n)을 실행하며, 이는 원격 액세스 클라이언트(102)의 에이전트(326)와 필터(322)를 거쳐 네트워크(104)에 액세스한다. 몇 실시예에서, 어플리케이션(338a-338n)은 VoIP와 같은 하나 이상의 실시간 데이터 통신을 제공한다. 다른 실시예에서, 어플리케이션(338a-338n) 중 하나 이상은 이메일, 협력, 온라인 미팅, 및/또는 데스크톱 공유 관련 서비스나 기능을 제공한다.

도 5A에 도시된 바와 같이, 패킷 캡쳐 메커니즘(365, 365')은 클라이언트(105)의 어플리케이션(338a-338n)중 임의의 것의 네트워크 트래픽을 차단하기 위해, 원격 액세스 클라이언트(102)의 필터(322)나 에이전트(326)에 포함될 수 있다. 원격 액세스 클라이언트(120)는 클라이언트(105)의 네트워크 통신을 큐잉하고 우선 순위화하기 위해 큐(540a-540n)를 포함한다. 일 실시예에서, 큐(540a-540b)는 필터(322)에 대한 NDIS 드라이버와 같은 네트워크 드라이버에 포함되며, 다른 실시예에서는 에이전트(326)에 포함되거나 이에 의해 액세스될 수 있다. 큐(540a-540b)는 패킷 캡쳐 메커니즘(365)에 의해 차단된 네트워크 패킷과 같은 네트워크 패킷을 저장 및/또는 배열하는 데에 적합한 수단 및/또는 메커니즘의 형태를 포함한다. 몇 실시예에서, 큐(540a-540b)는 클라이언트(105)의 어플리케이션(338a-338n)에 관한 네트워크 패킷과 관련되거나 이에 할당된다. 다른 실시예에서, 큐(540a-540n)는 고, 중, 저와 같은 순위 레벨로 또는 우선 순위 1,.., 10와 같이 수치적으로 체계화된다. 당업자라면 큐(540a-540b)의 수는 3, 5, 또는 10 레벨의 우선 수위와 같이, 원하는 우선 순위에 기초할 수 있다는 것이 이해될 것이다. 부가하여, 큐(540a-540b) 중에서 약간은 우선 순위에 기초한 큐(540a-540b)에 놓이거나 여기에서 벗어나기 전에 네트워크 패킷을 수신 및/또는 전송하는 데에 이용될 수 있다.

원격 액세스 클라이언트(120)는 게이트웨이(340)를 통해 네트워크(104) 상에서와 같이, 에이전트(326)를 거쳐 클라이언트의 네트워크 패킷을 보내는 방법을 결정하기 위해 라우팅 테이블(538)를 갖고, 액세스하거나 이용할 수 있다. 일 실시예에서, 에이전트(326)는 예를 들어, 도 1A에서 나타낸 바와 같이 게이트웨이(340)에 SSL VPN 연결을 설정 및 유지한다. 일 실시예에서, 라우팅 테이블(538)은 발신지와 목적지 통신 지점 간의 통신 경로나 연결을 식별하기 위해 발신지 컴퓨팅 디바이스와 목적지 컴퓨팅 디바이스에 대한 정보를 포함한다. 라우팅 테이블(538)은 네트워크(104) 상의 통신 경로를 식별하기 위해 발신지 IP 주소와 발신지 포트, 및 목적지 IP 주소와 목적지 포트를 포함한다. 예를 들어, 발신지 IP 주소와 발신지 포트는 클라이언트 상의 어플리케이션(338a-338b)이 네트워크(105) 상에서 통신하게 하는 클라이언트(105)의 IP 주소와 포트를 나타낸다. 목적지 IP 주소는 어플리케이션(338a-338b)이 피어 장치에 의해 이용되는 목적지 포트를 거쳐 통신하게 되는 피어 컴퓨팅 디바이스의 IP 주소를 나타낸다.

부가하여, 원격 액세스 클라이언트(120)는 어플리케이션에서 실행하는 어플리케이션(38a-338n)에 관한 네트워크 통신의 클라이언트측 우선 순위를 특정하기 위한 하나 이상의 폴리시(520)를 갖는다. 이들 폴리시(520)는 적합한 수단 및/또는 메커니즘에 의해 특정될 수 있다. 몇 실시예에서, 폴리시(520)는 어플리케이션(338a-338n)의 이름 및/또는 어플리케이션(338a-338n)의 유형으로 특정된다. 다른 실시예에서, 폴리시(520)는 어플리케이션(338a-338n)에 의해 이용되는 하나 이상의 프로토콜의 유형 및/또는 네트워크 패킷의 페이로드의 크기에 따라 특정된다. 다른 실시예에서, 폴리시(520)는 어플리케이션이 클라이언트(105)의 포그라운드 또는 백그라운드에서 실행중인지에 대해 기초하여 우선 순위를 정의한다. 또 다른 실시예에서, 폴리시(520)는 호스트 이름이나 IP 주소와 같은 목적지 네트워크 주소 및/또는 목적지 포트 번호에 기초하여 우선 순위를 나타낸다. 부가하여, 폴리시(520)는 어느 지점에서나 클라이언트(105) 상에서 실행될 수 있는 다수의 어플리케이션(338a-338n) 및/또는 다수의 프로토콜을 고려하도록 계층적으로 지정된다. 더욱, 폴리시(520)는 하나의 어플리케이션(338a)이 실행중인 경우, 제2 어플리케이션(338b)이 더 높거나 낮은 우선 순위를 갖는 것과 같이 조건부로 지정된다. 당업자라면 클라이언측 어플리케이션 우선 순위를 정의하는 여러 방법을 이해할 것이다.

폴리시(520)는 에이전트(326)에 의해 액세스되며, 에이전트(326)에 구성되거나 에이전트(326)에 의해 로딩된다. 예를 들어, 폴리시(520)는 게이트웨이(340)에 의해 제공되거나 이를 통해 다운로드된다. 폴리시(520)는 폴리시를 특정하기 위한 문장 및/또는 언어의 유형과 포맷을 포함하며, 전자적으로 하나 이상의 네트워크 패킷에 의해 또는 XML 파일과 같은 파일을 통해서와 같이 매체의 유형 및/또는 형태를 통해 제공된다. 폴리시(520)는 적합한 수단 및/또는 메커니즘에 의해 유저에 의해 구성 가능하다. 예를 들어, 에이전트(326)는 폴리시(520)를 구성하거나 지정하기 위해 구성된 유저 인터페이스, 그래픽, 또는 디자인과 같은 구성 메커니즘을 제공한다.

도 5A 및 도 1A-1C의 시스템(500)에 비추어, 도 5B의 방법 550으로 설명되는 본 발명의 우선 순위 기술을 설명한다. 간단한 개요로, 이 방법 550의 단계 555에서, 클라이언트(105)는 클라이언트(105) 상의 어플리케이션(338a-338n)과 관련된 하나 이상의 네트워크 패킷을 인터셉트하고, 단계 560에서 네트워크 패킷은 큐(540a-540n)에 저장된다. 단계 565에

서, 인터셉트되어 큐된 네트워크 패킷의 우선 순위는 어플리케이션(338a-338n)의 유형 및/또는 우선 순위에 기초하여 결정된다. 단계 570에서, 결정된 우선 순위를 네트워크 패킷에 대해 나타내며, 단계 575에서 네트워크 패킷은 결정된 우선 순위에 따라 통신된다. 이와 같이, 클라이언트(105) 상의 어플리케이션(338a-338b)에 의해 형성된 아웃바운드 네트워크 패킷은 어플리케이션(338a-338b)의 유형 및/또는 우선 순위에 기초하여 전송하기 전에 클라이언트(105)에 의해 우선 순위화된다. 예를 들어, 어플리케이션(338a)은 게이트웨이(340)에의 SSL 연결의 TCP/IP 세션을 통해 UPD에 의한 RTP와 같이, VoIP 통신의 실시간 데이터를 형성한다. 본 발명의 기술을 이용하여 클라이언트(105)는 비실시간 데이터 통신 어플리케이션과 같이, 다른 어플리케이션 이전에 어플리케이션(338a)의 실시간 데이터 통신을 우선 순위화한다. 이 기술은 네트워크 트래픽 우선 순위가 스위치와 라우터와 같은 중간 네트워크 장치에서 발생하는 퀄러티 오브 서비스 (QOS) 네트워크에 이점이 있다.

이 방법 500의 단계 555는 어플리케이션(338a-338n), 게이트웨이(340), 피어 컴퓨팅 장치 및 그 외 네트워크 스택의 네트워크 계층에 투명하게 하나 이상의 어플리케이션(338a-338n)의 네트워크 패킷을 인터셉트한다. 이런 식으로, 본 발명의 기술은 클라이언트(105) 상의 어느 유형의 어플리케이션(338a-338n)이라도 지원하게 된다. 몇 실시예에서, 네트워크 패킷은 에이전트(326) 또는 필터(322)를 거쳐 패킷 캡쳐 메커니즘(360)에 의해 인터셉트된다. 어플리케이션(338a-338n)의 인바운드 및/또는 아웃바운드 네트워크 패킷은 본 발명의 원격 액세스 클라이언트(120)에 의해 차단된다.

단계 560에서, 단계 555에서 차단된 네트워크 패킷이 큐(540a-540n)에 저장된다. 일 실시예에서, 네트워크 패킷은 단계 565와 570에서 네트워크 패킷을 우선 순위화하기 전에 임시 큐(540a-540n)에 저장된다. 다른 실시예에서, 네트워크 패킷은 네트워크 패킷이 단계 565 및/또는 단계 570에서 우선 순위화된 후에 결정된 우선 순위 큐(540a-540n)와 어플리케이션(338a-338n)과 관련된 큐(540a-540n)에 저장된다.

단계 565에서, 본 발명의 원격 액세스 클라이언트(120)는 우선 순위를 결정하여 우선 순위에 근거한 폴리시(520)를 결정하기 위해서 어플리케이션(338a-338n)과 네트워크 패킷의 관련을 결정한다. 에이전트(326)와 같은 클라이언트(105)는 적합한 수단 및/또는 메커니즘에 의해 어플리케이션(338a-338n)과 네트워크 트래픽을 관련시킨다. 몇 실시예에서, 에이전트(326)는 네트워크 패킷의 페이로드의 헤더, 필드 또는 데이터의 유형과 컨텐트와 같은, 네트워크 패킷의 컨텐트에 의해 어플리케이션(338a-338n)으로부터 발생되어지는 네트워크 패킷을 식별한다. 다른 실시예에서, 네트워크 패킷은 발신지 및 목적지 IP 주소와 포트 번호와 같은 라우팅 테이블(538)로부터의 정보를 네트워크 패킷의 IP 주소 및 포트 번호와 일치시킴으로써 어플리케이션(338a-338n)과 관련되게 된다. 몇 실시예에서, 프레임 모니터(360)와 같은 에이전트(326)는 식별된 애플리케이션이 실제로 패킷을 형성한 것을 증명하기 위해 패킷 상에서 체크섬을 실행한다.

부가하여, 원격 액세스 클라이언트(120)는 네트워크 패킷과 관련되는 어플리케이션(338a-338n)이 클라이언트(105)의 포그라운드와 백그라운드에서 실행중인지를 결정한다. 더욱, 원격 액세스 클라이언트(120)는 클라이언트(105)의 운영 시스템에 의해 어플리케이션(338a-338n)에 할당된 프로세스 태스크 우선 순위 등의 우선 순위를 결정한다. 다른 실시예에서, 원격 액세스 클라이언트(120)는 크기, 메모리 이용량, 총 실행 시간, 및/또는 이용 회수와 같이, 어플리케이션(338a-338n)의 특성이나 통계치를 결정할 수 있다. 당업자라면 본 발명이 클라이언트측 어플리케이션 인식 네트워크 통신 우선 순위를 제공하기 위해 이용할 수 있는 어플리케이션의 여러 특성을 이해할 것이다.

단계 570에서, 본 발명의 원격 액세스 클라이언트(120)는 단계 565에서 패킷과 관련되는 어플리케이션(338a-338n)에 기초하여 인터셉트되어 큐된 네트워크 패킷에 대한 우선 순위를 나타낸다. 일 실시예에서, 에이전트(326)는 폴리시(520)를 이용하여 폴리시(520)에 의해 특정되거나 나타내지는 우선 순위 규칙에 따라 어플리케이션(338a-338n)의 네트워크 패킷에 우선 순위를 적용한다. 몇 실시예에서, 에이전트(326)는 어플리케이션(338a-338n)의 네트워크 패킷의 우선 순위를 나타내기 위해, 포그라운드 또는 백그라운드에서 실행하는 것과 같은 어플리케이션(338a-338n)의 특성을 이용한다. 다른 실시예에서, 에이전트(326)는 어플리케이션(338a-338n)의 네트워크 패킷에 대한 우선 순위를 나타내기 위해 폴리시(520)와 어플리케이션(338a-338n)의 특성의 조합을 이용한다.

몇 실시예에서, 에이전트(326)는 네트워크 패킷 큐(540a-540n)의 관리를 위해 필터(322)에 우선 순위를 나타내어, 이 나타낸 우선 순위를 적용한다. 에이전트(326)는 IOCTL 인터페이스와 같은 어플리케이션 프로그래밍 인터페이스(API) 또는 당업자에게 잘 알려진 인터페이스의 유형을 통해서와 같이 적합한 수단 및/또는 메커니즘에 의해 필터(322)에 네트워크 패킷의 우선 순위를 통신할 수 있다. 일 실시예에서, 필터(322)는 이름으로 어플리케이션(338a-338n)을 아는 것이 아니라 라우팅 테이블(538)에 의해 어플리케이션(338a-338n)의 네트워크 패킷에 우선 순위를 관련시킨다. 네트워크 패킷에 대응하는 어플리케이션(338a-338n)은 IP 주소와 포트 번호와 같은 발신지와 목적지 식별자의 조합으로 식별될 수 있다. 이와 같이, 어떤 실시예에서는, 에이전트(326)는 어플리케이션 이름 대신에 라우팅 정보로 필터(322)에 우선 순위를 나타낸다. 다른 실시예에서, 에이전트(326)는 라우팅 테이블(538)에서의 라우팅 정보에 대해, 어플리케이션 이름이나 프로세스 id에 의해서와 같이, 어플리케이션(338a-338n)간의 매핑을 필터(322)에 제공한다.

어플리케이션(338a-338n)에 대해 나타낸 우선 순위에 기초하여, 몇 실시예에서는, 필터(322)가 우선 순위를 지원하여 큐(540a-540n) 내로 네트워크 패킷을 위치, 배열하거나 조정한다. 일 실시예에서, 필터(322)는 임시 큐(540a-540n)로부터 또는 메모리나 그 외 저장소로부터 어플리케이션(338a-338n)과 관련된 큐(540a-540n), 우선 순위와 관련되는 큐(540a-540n), 또는 어플리케이션와 우선 순위 둘다와 관련되는 큐(540a-540n)로 네트워크 패킷을 이동시킨다. 예를 들어, 일 실시예에서, 모든 고 우선 순위 네트워크 트래픽은 고 우선 순위 큐(540a)에 위치되며 다른 어플리케이션(338a-338n) 이전에 실시간 데이터 어플리케이션(338a-338n)과 같이, 어플리케이션(338a-338n)의 우선 순서에 기초하여 순서데로 배열된다. 몇 실시예에서, 네트워크 패킷은 FIFO 식으로와 같이, 네트워크 패킷이 패킷 캡쳐 메커니즘(365)에 의해 인터셉트될 때에 기초하여 우선 순위 큐(540a-540n)에 순서데로 배열된다. 또 다른 실시예에서, 하나의 큐(540a-540n)는 필터(322)에 의한 우선 순위에 이용된다. 각 네트워크 패킷은 모든 어플리케이션(338a-338n)에 걸친 패킷 우선 순위에 의한 패킷과 차단된 네트워크 패킷을 제공하기 위해 모든 다른 차단된 네트워크 패킷에 대해 우선 순서데로 위치 배열된다. 당업자라면 네트워크 패킷이 고, 중, 저와 같은 여러 우선 순위 큐(540a-540n)으로 배열되고 상술된 본 발명의 동작을 실행할 때 적합한 방법으로 큐에 위치 배열될 수 있다.

일 실시예에서, 어플리케이션(338a-338n)의 모든 네트워크 패킷은 어플리케이션(338a-338n)과 관련되는 큐(540a-540n)에 위치된다. 예를 들어, 제1 목적지 IP 주소에 통신하는 어플리케이션에 대해 인터셉트된 네트워크 패킷과 제1 목적지 포트가 제1 큐(540a)에 놓인다. 다른 실시예에서, 이메일이나 음성 어플리케이션과 같은 유형의 어플리케이션(338a-338n)에 대한 모든 네트워크 패킷 또는 RTP 또는 UDP와 같은 어플리케이션(338a-338n)에 의해 이용되는 유형의 프로토콜에 대한 모든 네트워크 패킷이 하나 이상의 어플리케이션에 대해 네트워크 패킷을 우선 순위화하기 위해 큐(540a-540n)에 놓인다. 예를 들어, 온라인 협력 관련 어플리케이션(338a-338n)은 협력 관련 어플리케이션에 대한 제1 큐(540a)에 놓여 우선 순위화된다. 제2 큐(540b)는 이메일 관련 어플리케이션(338a-338n)에 이용된다. 다른 예에서, 큐(540a)는 실시간 데이터를 통신하거나 RTP 및/또는 UDP 프로토콜을 이용하여 통신하는 어플리케이션(338a-338n)에 대해 이용된다. 다른 예에서, 큐(540a)는 ICA 또는 RDP와 같이, 원격 디스플레이 프로토콜을 이용하여 통신하는 어플리케이션(338a-338n)에 대해 이용된다.

특정 어플리케이션(338a-338n)에 의해 체계화되는 각 어플리케이션 관련 큐(540a-540n) 내에는, 어플리케이션(338a-338n)의 유형이나 카테고리나, 네트워크 패킷이 이들을 형성하는 어플리케이션(338a-338n)의 특성, 예를 들어, 포그라운드 어플리케이션, 네트워크 패킷의 크기 또는 네트워크 패킷이 차단되는 시간에 의해 우선 순위화된다. 몇 실시예에서, 하나 이상의 큐(540a-540n)는 폴리시(520)가 네트워크 패킷에 적용되지 않거나, 폴리시(520)가 우선 순위를 위해 네트워크 패킷을 무시하거나 처리하지 않는 것을 나타내기 때문에 인터셉트되지만 우선 순위화되지 않은 네트워크 패킷에 이용된다. 당업자라면 네트워크 패킷이 어플리케이션(338a-338n), 어플리케이션(338a-338n)의 유형이나 어플리케이션(338a-338n)에 의해 이용되는 프로토콜과 관련되는 큐(540a-540n)에서 우선 순위에 근거하여 위치 배열되고, 우선 순위가 클라이언트(105)에 대해 특정된 폴리시(520)에 대해 기초할 수 있다는 것을 이해할 것이다.

방법 550의 단계 575에서, 네트워크 패킷은 네트워크 패킷에 대해 결정된 우선 순위에 따라 큐(540a-540n)로부터 통신된다. 몇 실시예에서, 네트워크 패킷은 우선 순위 큐(540a-540b)로 체계화되어 최고 순위 큐(540a-540n)의 네트워크 패킷이 먼저 통신되고 다음 최고 순위 큐(540a-540n)가 두번째로 통신되게 된다. 다른 실시예에서, 큐(540a-540n)는 어플리케이션(338a-338n)에 의해 체계화되고, 따라서 단계 575에서 본 발명은 어플리케이션(338a-338n)의 각 우선 순위에 기초하여 큐(540a-540n)으로부터 네트워크 패킷을 통신한다. 큐(540a-540n)의 체계와 관리에 상관 없이, 당업자라면 본 발명의 원격 액세스 클라이언트가 결정된 순위에 따라서 큐로부터 네트워크 패킷을 통신하게 되고, 다음에 클라이어트의 폴리시(520)에 기초하거나 이로부터 유도된다는 것을 이해할 것이다.

몇 실시예에서, 본 발명의 원격 액세스 클라이언트(120)는 어느 네트워크 패킷이 어느 큐로부터 통신하는지를 결정할 때 다른 네트워크 요인을 고려한다. 예를 들어, 원격 액세스 클라이언트(120)는 어플리케이션(338a-338n)에 관한 TCP 연결에 대해 제로의 윈도우 크기를 수신하는 것과 같이, 네트워크 밀집의 표시를 수신한다. 다른 예에서, 원격 액세스 클라이언트(120)는 특정 목적지에 대한 다수의 재전송을 인식한다. 이와 같이, 어떤 실시예에서, 원격 액세스 클라이언트(120)는 네트워크 패킷이 큐(540a-540n)에 다른 네트워크 패킷 보다 높은 순위를 갖고 있어도, 밀집과 같은 다른 네트워크 요인에 관련된 네트워크 패킷을 억압하거나 통신하지 않는다. 따라서, 클라이언트(105)는 어플리케이션(338a-338n) 마다 클라이언트(105)에 대한 폴리시(520)에 따르고 네트워크에서 발생하는 네트워크 통계치와 그 외 요인들에 비추어서 클라이언트(105)의 네트워크 통신의 우선 순위를 제어 및 관리한다.

또 다른 형태로 이하 도 6A 및 도 6B를 참조하면, 본 발명은 지속적 및 신뢰적 연결을 위해 네트워크 붕괴 차단 기술을 제공하는 것과 관련된다. 도 6A는 도 3A와 관련하여 설명된 환경(300)을 나타낸다. 환경(300)은 네트워크 스택(310a 및 310b)를 나타내며, 이는 도 1A-1C, 2A 또는 5C에서 나타낸 컴퓨팅 디바이스(102) 및 게이트웨이(340)와 같이, 컴퓨팅

디바이스(120a-120b) 또는 게이트웨이(340)의 네트워크 스택을 나타낸다. 각 네트워크 스택(310a-310b)은 당업자가 잘 이해하는 바와 같이 프레임 네트워크 계층의 상부 상의 TCP/IP 네트워크 계층과 같은 하나 이상의 네트워크 계층을 포함한다. 네트워크 스택(310a-310b)을 특정 세트의 네트워크 계층을 갖는 도 6A의 환경(300)에 나타내었지만, 당업자라면 네트워크 스택(310a-310b)이 네트워크 계층의 유형을 가지며, 네트워크 스택(310a-310b) 각각이 다른 네트워크 스택에 관련하여 다른 유형의 각 계층을 갖는다는 것을 이해할 것이다.

네트워크 스택(310a-310b)이 네트워크 스택의 제1 부분(605a-605b) 및 네트워크 스택의 제2 부분(610a-610b)을 갖는 것으로 한다. 도 6A의 예시의 네트워크 스택(310a-310b)에 도시된 바와 같이, 네트워크 스택의 제1 부분(605a-605b)는 TCP 네트워크 계층과 그 아래에 네트워크 계층을 포함한다. 제2 부분(610a-610b)은 SSL 프로토콜 계층을 통한 UDP와 같이, TCP 네트워크 계층 위에 이들 네트워크 계층을 포함한다. 제1 부분(605a-605b) 및 제2 부분(610a-610b)는 TCP 계층에서 할당, 단편화 또는 분할된 것으로 나타나 있지만, 제1 부분과 제2 부분은 당업자가 이해하는 바와 같이 본 발명의 네트워크 붕괴 차단 기술을 실행할 때 더 높거나 낮은 분할 계층에 형성될 수 있다.

도 6A에 나타낸 네트워크 스택(310a-310b)은 도 5A에서 도시된 클라이언트와 같이, 클라이언트(105) 상의 어플리케이션(338a-338n)을 나타내며, 제2 컴퓨팅 디바이스(102b) 또는 다르게 게이트웨이(340)에 대한 피어투피어 SSL VPN 연결을 설정한다. 클라이언트(105)는 노트북, 퍼스널 디지털 어시스턴트 (PDA), 스마트폰, 또는 그 외 유형의 모바일 컴퓨팅 또는 텔레커뮤니케이션 장치와 같은 모바일 클라이언트일 수 있다. 클라이언트(105)는 UDP 프로토콜을 통한 VoIP 통신 또는 피어 장치(102b)나 게이트웨이(340)에 설정된 SSL 세션을 통한 UDP에 의한 RTP 등의 실시간 데이터를 통신할 수 있다. 일 실시예에서, 원격 액세스 클라이언트(120)의 에이전트(326)는 게이트웨이(340)이나 피어 컴퓨팅 디바이스(102b)에 대한 SSL 또는 SSL VPN 세션을 설정 유지한다. 에이전트(326)는 유저 모드(332)에서 동작하며, 어플리케이션 계층 프로토콜과 함께 네트워크 스택(310a-310b)의 제2 부분(610a-610b)에 관한 네트워크 계층과 프로토콜 처리를 처리할 수 있다. TCP/IP 기반의 네트워크(104)로서, 네트워크 스택(310a-310b)의 제2 부분(610a-610b)의 SSL 세션에 대한 UDP는 네트워크 스택(310a-310b)의 제1 부분(605a-605b)을 형성하는 TCP/IP 스택에 대해 통신될 수 있다. 도 1A 또는 5A에서 나타낸 것과 같은, 본 발명의 원격 액세스 클라이언트(120)에 비추어, 필터(322)는 네트워크 스택(310a-310b)의 제1 부분(605a-605b) 내의 커널 모드(332)에서 동작하는 네트워크 드라이버일 수 있다.

본 발명은 네트워크 스택(310a-310b)의 제1 부분(605a-605b)에 네트워크 붕괴의 유형과 같이, 네트워크 레벨 연결 중단으로 네트워크 스택(310a-310b)의 제2 부분(610a-610b)를 유지하도록 도 6B의 방법 650에서 의해 나타낸 바와 같은 네트워크 붕괴 차단 기술을 이용한다. 본 발명의 네트워크 붕괴 차단 기술은 클라이언트(105)의 어플리케이션(338a-338n), 클라이언트(105)의 유저, 제1 부분(605a-605b) 위의 하나 이상의 네트워크 계층, 및 게이트웨이(340)이나 피어 컴퓨팅 디바이스(102b), 및 각 네트워크 스택(310a-310b)의 일부에 대해 투명하게 실행된다. 일 실시예에서, 네트워크 붕괴는 네트워크가 붕괴되거나 세션이 인터셉트된 것을 클라이언트의 유저에게 통지하지 않고 차단된다.

방법 650의 간단한 개요로, 단계 655에서, 클라이언트(105)는 피어 컴퓨팅 디바이스나 게이트웨이와 같이, 클라이언트와 다른 장치 간의 네트워크 연결에 의해 적어도 제1 프로토콜을 통해 세션을 설정한다. 이와 같이, 네트워크 스택(310a-310b)은 클라이언트(105) 상에서 설정되거나 이용된다. 네트워크 스택(310a-310b)은 제1 부분(605a-605b) 및 제2 부분(610a-610b)을 갖는다. 단계 660에서, 네트워크 연결의 붕괴가 검출되어 네트워크 스택(310a-310b)의 제1 부분(605a-605b)이 폐지되게 하거나, 아니면 이용되지 않거나 계속 이용되지 않게 붕되게 한다. 단계 665에서, 본 발명은 이 붕괴 동안 네트워크 스택(310a-310b)의 제2 부분(610a-610b)을 보유하여, 제2 부분(610a-610b)의 네트워크 계층과 관련되는 세션을 보유하게 된다.

붕괴 동안, 단계 670에서, 네트워크 스택(310a-310b)의 제2 부분(610a-610b)에 관한 네트워크 패킷이 큐잉된다. 단계 675에서, 네트워크 스택(310a-310b)의 제1 부분(605a-605b)이 재설정되는 반면, 본 발명은 제2 부분(610a-610b) 및 그 세션을 보유하고, 단계 680에서 네트워크 스택(310a-310b)의 제1 부분(605a-605b)과 제2 부분(610a-610b)를 결합하거나 재관련시킴으로써 세션을 계속한다. 네트워크 연결 및/또는 세션은 단계 680에서 자동으로 재인증될 수 있다. 단계 685에서, 이 방법은 큐잉된 네트워크 패킷을 통신하며 네트워크 붕괴가 발생하지 않은 것같이 세션을 계속한다.

단계 655의 실시예에서, 제1 컴퓨팅 디바이스(102a)는 적합한 수단 및/또는 메커니즘에 의해 연결 기반의 프로토콜의 유형을 이용하여, 피어 컴퓨팅 디바이스(102b) 또는 게이트웨이(340)와 같은 제2 디바이스와의 네트워크 연결을 설정할 수 있다. 예를 들어, 네트워크 연결은 TCP/IP 네트워크 상에서의 TCP 연결을 통해서나 IPX/SPX 네트워크 상에서 SPX 연결에 의해 설정된다. 몇 실시예에서, 네트워크 연결은 도 5A에서 나타낸 어플리케이션과 같이 클라이언트 상에서의 어플리케이션(338a-338n)에 의해 초기화된다. 예를 들어, 사이트릭스 시스템사의 ICA 클라이언트와 같은 원격 디스플레이 클라이언트나 마이크로소프트사의 원격 디스플레이 클라이언트는 네트워크 연결을 초기화하거나 설정한다. 다른 실시예에서, 단계 665의 네트워크 연결은 에이전트(326), 필터(322), 또는 그 외 원격 액세스 클라이언트(120)의 부분을 통해 초기화

및/또는 설정된다. 일 실시예에서, 네트워크 연결의 설정은 네트워크 스택(310a-310b)의 제1 부분(605a-605b)을 형성한다. 다른 실시예에서, 네트워크 스택(310a-310b)의 제1 부분(605a-605b) 또는 그 일부는 클라이언트(105)의 기동시 네트워크(104)에 대한 연결로 설정된다.

몇 실시예에서, 네트워크 스택(310a-310b)의 제2 부분(601a-601b)는 ICA 또는 RDP의 원격 디스플레이 프로토콜을 통해, SSL 세션과 같은 하나 이상의 세션을 설정하여 형성된다. 세션은 어플리케이션(338a-338n) 또는 클라이언트의 원격 액세스 클라이언트(120)을 통해 설정된다. 일 실시예에서, 세션은 피어 컴퓨팅 디바이스(102b) 또는 게이트웨이(340)를 갖는 터널링 또는 게이트웨이 세션에 대응한다. 다른 실시예에서, 세션은 시그널링 프로토콜, 예를 들어 SIP를 통해 설정된 매체 세션과 같은 대화형 세션의 형태일 수 있다. 예를 들어, 네트워크 스택(310a-310b)의 제2 부분(610a-610b)의 세션은 도 2B의 방법 260에 의해 설정된 것과 같은 VoIP 통신 세션을 포함한다. 부가하여, 네트워크 스택(310a-310b)의 제2 부분(610a-610b)과 관련된 다수의 세션이 있다. 예를 들어, SSl 또는 SSL VPN 세션은 하나의 세션을 형성하는 반면, UDP에 의한 RTP를 통한 매체 세션과 같은 제2 세션이 다른 세션을 형성한다. 부가하여, 네트워크 스택(310a-310b)의 어플리케이션 계층에서, 클라이언트(105) 측 하나 이상의 어플리케이션(338a-338n)은 피어 컴퓨팅 디바이스(102b)를 갖는 어플리케이션 레벨 세션을 설정한다. 일 실시예에서, 원격 액세스 클라이언트(120)의 에이전트(326)는 네트워크 스택(310a-310b)의 제2 부분(610a-610b) 및 관련 세션 중 하나 이상을 설정 유지한다.

본 발명의 방법 650의 단계 660에서, 네트워크 연결의 붕괴가 검출된다. 일 실시예에서, 네트워크 붕괴는 네트워크와 네트워크 세그먼트 간의 모바일 클라이언트(105) 로밍으로 인한 것이며, 이로 인해 어떤 실시예에서 클라이언트(105)가 새로운 네트워크 IP 주소 및/또는 호스트 이름을 갖게 된다. 몇 실시예에서, 이 붕괴는 네트워크 스택(310a-310b)의 제1 부분(605a-605b)를 붕괴시켜, 예를 들어, TCP 또는 SPX 연결이 분리되게 한다. 일 형태에서, 이 붕괴는 네트워크 스택(310a-310b)의 제1 부분(605a-605b)나 그 부분이 붕괴되게 하거나, 재설정, 재연결, 재구성 또는 재구축될 필요가 있게 한다. 예를 들어, 몇 실시예에서, 네트워크 스택의 IP 계층은 변하지 않고 유지되지만 TCP 계층은 붕괴된다. 일 실시예에서 TCP 관련 드라이버는 재기동될 필요가 있다. 다른 실시예에서, 네트워크 연결이 붕괴되어도 TCP/IP 층은 그대로이어야 하고, 새로운 TCP 연결만이 설정될 필요가 있다. 다른 실시예에서, TCP/IP 계층은 그대로이지만 클라이언트(105)의 IP 주소를 변경하는 것과 같이, 새로운 네트워크나 네트워크 세그먼트에 대해서 재구성할 필요가 있다. 당업자라면 네트워크 연결이 붕괴되어 네트워크 스택의 제1 부분에 영향을 미칠 수 있다는 것이 이해될 것이다.

몇 실시예에서, 에이전트(326) 또는 그 외 원격 액세스 클라이언트(120)의 다른 부분은 적합한 수단 및/또는 메커니즘에 의해 네트워크 붕괴를 검출한다. 일 실시예에서, 에이전트(326)는 네트워크 스택(310a-310b)의 제1 부분(605a-605b)에 API 호출을 실행할 때 에러 메시지나 이상을 수신하여 네트워크 붕괴를 결정하게 된다. 예를 들어, 제2 부분(610a-610b)의 에이전트(326)에 의해 유지되는 SSL 세션은 네트워크 스택(310a-310b)의 제1 부분(605a-605b)의 TCP 연결에 좌우된다. 에이전트(326)가 SSL 세션을 통해 처리하므로, 에이전트(326)는 TCP 연결의 문제를 나타내는 에러나 이상 메시지를 수신한다. 다른 실시예에서, 에이전트(326)는 네트워크 붕괴를 나타내는 네트워크 스택(310a-310b)의 제1 부분(605a-605b)의 네트워크 계층으로부터 이벤트나 메시지를 수신한다. 당업자라면 네트워크 붕괴가 검출되는 여러 방법을 이해할 것이다.

단계 665에서, 네트워크 붕괴의 검출시, 본 발명의 에이전트(326)나 그 외 원격 액세스 클라이언트(120)의 부분은 붕괴 동안 네트워크 스택(310a-310b)의 제2 부분(610a-610b)를 유지한다. 예를 들어, 에이전트(326)에 의해 유지되는 SSL 기반의 세션이 기본 TCP 연결에 좌우되지만, 에이전트(326)는 TCP 연결의 붕괴로 SSL 세션을 개방 또는 활성으로 유지한다. 네트워크 스택의 제2 부분(610a-610b)의 하나 이상의 계층과 관련하여 다수의 세션이 있을 수 있기 때문에, 에이전트(326)는 몇 실시예에서, 네트워크 스택(310a-310b)의 제1 부분(605a-605b)이 붕괴되었지만 다수의 세션 중 하나 이상이나 모두를 개방 또는 활성으로 유지한다.

방법 650의 단계 670에서, 본 발명의 원격 액세스 클라이언트(120)은 몇 실시예에서, 네트워크 붕괴 동안 네트워크 스택(310a-310b)의 제2 부분(610a-610b)에 관한 프로토콜의 하나 이상의 네트워크 패킷을 큐잉한다. 원격 액세스 클라이언트(120)는 도 5A에 나타낸 큐(540a-540n)와 같은 큐잉 메커니즘의 유형을 이용한다. 다른 실시예에서, 원격 액세스 클라이언트(120)는 음성 통신을 위한 UDP를 통한 RTP와 같은 손실 프로토콜에 관한 패킷과 같이, 붕괴 동안 네트워크 패킷을 폐기한다. 어떤 경우에는, 음성 통신시와 같이, 레이턴시와 품질의 문제를 줄이기 위해서, UDP 패킷과 같은 패킷을 폐기하는 것이 바람직할 수 있다. 다른 실시예에서, 원격 액세스 클라이언트(120)는 네트워크 패킷을 큐잉하고 다른 네트워크 패킷을 폐기할 수 있다. 부가의 실시예에서, 원격 액세스 클라이언트(120)는 네트워크 패킷을 큐잉하고, 소정의 시간 이후 네트워크 패킷의 일부나 모두를 폐기한다. 원격 액세스 클라이언트(120)는 어느 네트워크 패킷을 큐잉 및/또는 폐기할지를 결정하도록 폴리시(520)를 이용한다. 예를 들어, 제1 애플리케이션(338a)의 네트워크 패킷이 큐잉되는 반면 제2 애플리

케이션의 네트워크 패킷은 폐기된다. 다른 실시예에서, 원격 액세스 클라이언트(120)는 붕괴 동안 네트워크 패킷을 큐잉할지 폐기할지를 결정하기 위해 당업자에게 잘 알려진 바와 같이, 네트워크 통계 자료나 네트워크 트래픽 검사 기술, 예를 들어 상태 기반 검사를 이용할 수 있다.

방법 650의 단계 675에서, 네트워크 스택(310a-310b)의 제1 부분(605a-605b)은 재설정되는 반면 네트워크 스택(310a-310b)의 제2 부분(610a-610b)은 네트워크 스택(310a-310b)의 제2 부분(610a-610b)의 원하는 세션을 유지하면서 유지되게 된다. 네트워크 스택(310a-310b)의 제1 부분(605a-605b)은 적당한 수단 및/또는 메커니즘에 의해 재설정된다. 예를 들어, 클라이언트(105)는 로밍 모바일 클라이언트(105)에 대해 새로운 네트워크에 로깅함으로써, 네트워크(104)에 대한 TCP/IP 연결을 재설정한다. 다른 실시예에서, 에이전트(326)나 필터(322)를 통해서와 같이, 원격 액세스 클라이언트(120)는 네트워크 스택(310a-310b)의 제1 부분(605a-605b)를 재설정한다. 예를 들어, 에이전트(326)는 새로운 TCP 연결을 초기화 설정한다. 제1 부분(605a-605b)을 재설정할 때, 네트워크 스택(310a-310b)의 제2 부분(610a-610b)은 네트워크 스택(310a-310b)을 재설정하도록 제1 부분(605a-605b)과 결합되거나 재설정되거나, 이를 이용하거나 계속 이용하기 시작하게 된다. 몇 실시예에서, 에이전트(326)는 제1 부분(605a-605b)이 재설정된 것을 네트워크 계층에 의해 통지받거나 다른 실시예의 경우에는 제1 부분(605a-605b)이 재설정된 것을 결정하기 위해 미리 결정된 회수 폴(poll)한다. 예를 들어, 에이전트(326)는 TCP 연결이 활성인지 재연결될 수 있는지를 검사한다.

몇 실시예에서, 단계 680에서 에이전트(326)와 같은 원격 액세스 클라이언트(120)는 네트워크 스택(310a-310b)의 제1 부분(605a-605b)의 TCP 연결과 같은 네트워크 연결을 위해 클라이언트(105)나 클라이언트(105)의 유저를 자동으로 재인증할 수 있다. 예를 들어, 원격 액세스 클라이언트(120)는 클라이언트(105)의 유저의 네트워크 관련 증명서를 이용하여 네트워크(104)에 클라이언트(105)를 자동으로 재인증한다. 부가하여, 원격 액세스 클라이언트(120)는 네트워크 스택(310a-310b)의 제2 부분(610a-610b)과 관련된 세션에 대해 클라이언트(105)나 클라이언트(105)의 유저를 자동으로 재인증한다. 예를 들어, 에이전트(326)와 게이트웨이(340) 또는 피어 컴퓨팅 디바이스(102c) 간의 SSL 세션이 재인증된다.

다른 예에서, 애플리케이션(338a)은 액세스를 위한 인증 증명서를 이용하는 호스트 서비스, 웹 서버, 또는 애플리케이션 서버를 액세스할 수 있다. 에이전트(326)는 애플리케이션 관련 인증 증명서를 이용하여 대응하는 서비스나 서버에 애플리케이션(338a)를 자동으로 재인증한다. 몇 실시예에서, 원격 액세스 클라이언트(120)는 네트워크 액세스 및/또는 TCP 연결, SSL 또는 SSL VPN 세션과 같은 다중 레벨 및/또는 매체 상호 작용 유저 세션, 예를 들어, VoIP 전화 세션과 같은 애플리케이션 레벨 세션에서 클라이언트 및/또는 클라이언트(105)의 유저를 재인증한다. 더구나, 원격 액세스 클라이언트(120)는 단계 685 이전, 예를 들어, 큐잉 네트워크 패킷을 통신한 후지만 다른 통신에 이어지기 전인 단계 685 동안, 또는 서버나 게이트웨이(340)와 같은 피처 컴퓨팅 디바이스로부터의 인증 요청에 응답하여 단계 865 후, 어느 때나 재인증할 수 있다.

방법 650의 단계 685에서, 본 발명의 원격 액세스 클라이언트(120)는 네트워크 스택의 제2 부분(610a-610b)의 세션을 계속 이용하게 된다. 네트워크 패킷이 단계 670에서 큐잉되거나 계속 큐잉되면, 원격 액세스 클라이언트(120)는 큐잉 네트워크 패킷을 통신하고 클라이언트(105)의 하나 이상의 애플리케이션(338a-338n)에 의해 형성되거나 여기에 보내진 네트워크 패킷과 같이, 클라이언트(105)의 네트워크 패킷을 통신하거나 계속 통신하게 된다. 이와 같이, 본 발명의 네트워크 붕괴 차단 기술은 이동 모바일 컴퓨팅 솔루션에 있어서 신뢰적이며 지속적인 네트워크 연결 및 액세스를 일반적으로 제공하기 위한 투명한 솔루션을 제공한다.

VoIP 통신의 예로, 본 발명의 방법(650)은 네트워크 붕괴로 인한 전화 호출 끊어짐의 회수를 줄이고 VoIP의 이용과 체험을 향상시키게 된다. VoIP 유저는 본 발명의 원격 액세스 클라이언트(120)가 자동으로 세션을 유지하고 네트워크에 재연결되게 되면서 네트워크 이용 가능성의 임시적인 네트워크 붕괴로 인해 전화 호출을 재연결할 필요가 없게 된다. 부가하여, 본 발명의 원격 액세스 클라이언트(120)는 네트워크 붕괴 이후 보안을 제공하기 위해 연결 및 세션을 자동으로 재인증하게 된다. 더구나, 본 발명의 네트워크 차단 기술은 1) 네트워크 붕괴 동안 트랜잭션, 커맨드, 또는 동작을 자동으로 이어주고, 2) 네트워크 붕괴 동안 세션 관련 컨텍스트 및 캐시를 유지하고, 3) 네트워크의 변화로 인해 클라이언트의 네트워크 주소의 변경을 자동으로 취급하는 데에 유용하다.

신뢰성 및 지속적인 연결을 제공함으로써, 본 발명은 또한 도 1C에서의 클라이언트(105a 및 105b)와 같이 제1 컴퓨팅 디바이스(102a) 및 제2 컴퓨팅 디바이스(102b) 사이에서 실행되는 기능의 일부로서 트랜잭션, 명령 또는 동작의 차단을 방지하게 된다. 예를 들어, 윈도우 익스플로러를 이용한 파일 카피 동작은 네트워크 연결시의 붕괴가 있은 후에 계속 작동하고 있도록 설계되어 있지 않다. 클라이언트(105) 상의 유저는 클라이언트(150)로부터 서버(102c)로 파일을 카피하도록 윈도우 익스플로어의 파일 카피 피쳐를 이용한다. 파일의 크기로 인해, 이 동작은 완료하는 데에 비교적 긴 시간이 소요된다. 서버에의 파일 카피 동작의 중간에, 클라이언트(105)와 서버 간에 네트워크 연결의 중단이 있게 되면, 파일 카피는 실패하게 된다. 네트워크 연결이 재설정되면, 유저는 클라이언트(105)로부터 서버로 파일을 카피하기 위해 윈도우 익스플로

어로부터 다른 파일 카피 동작을 시작해야 한다. 본 발명에서는, 유저가 다른 파일 카피 동작을 시작할 필요가 없다. 네트워크 연결은 도 6B에서 나타낸 바와 같이 본 발명의 네트워크 붕괴 차단 기술에 따라 재설정된다. 이와 같이, 윈도우 익스플로어의 파일 카피는 네트워크 연결의 중단을 통지받지 않으므로, 실패하지 않는다. 원격 액세스 클라이언트(120)는 연결을 재설정하여 큐잉 데이터를 전송하므로 동작은 실패 없이 계속될 수 있다. 원격 액세스 클라이언트(120)는 네트워크 연결시의 차단 때문에 서버에 전달되지 않는 파일 카피 동작에 관한 데이터의 큐를 유지한다. 네트워크 연결이 재설정되면, 원격 액세스 클라이언트(120)는 큐잉 데이터를 전송한 다음에 파일 카피 동작에 관한 데이터를 계속 전달할 수 있다.

본 발명의 이러한 형태가 파일 카피 동작 예에 관련하여 설명되었지만, 당업자라면 제1 컴퓨팅 디바이스(102a)와 제2 컴퓨팅 디바이스(102b) 간에서 트랜잭트되는 동작, 트랜잭션, 명령, 기능 호출이 네트워크 연결 붕괴의 이상 없이 또한 클라이언트(105)나 클라이언트(105)의 유저가 붕괴가 있음을 인식하거나 붕괴의 통지를 받지 않고 유지될 수 있다. 부가하여, 트랜잭션 또는 동작은 애플리케이션(338), 게이트웨이(340), 제2 컴퓨팅 디바이스(102c), 및 네트워크 스택(310a-310b)의 제2 부분(610a-610b)의 일부에 투명하게 유지될 수 있다.

클라이언트(105)에게 피어 컴퓨팅 디바이스(102b)나 게이트웨이(340)에의 신뢰성 및 지속성 연결을 제공함으로써, 본 발명은 네트워크 연결 중단 동안 유저 세션을 유지하여 서버상의 호스트 서비스와 같은, 피어상의 애플리케이션(338)과의 새로운 유저 세션을 개방하는 프로세스를 방지하게 된다. 피어 컴퓨팅 디바이스 간의 각 유저 세션에 대해, 각 컴퓨팅 디바이스는 세션 특정 컨텍스트와 캐시 및, 그 외 유저 세션의 인스턴스에 관한 애플리케이션 특정 메커니즘을 유지한다. 설정된 각각의 새로운 유저 세션에 대해, 이들 세션에 특정적인 컨텍스트 및 캐시는 새로운 유저 세션을 반영하도록 재설정될 필요가 있다. 예를 들어, 클라이언트(105)상의 유저는 웹 서버나 웹 애플리케이션을 갖는 서버(102c)와의 http 세션을 가질 수 있다. 컨텍스트는 서버의 메모리, 서버의 파일, 데이터베이스 또는 그 외 서버(102c)의 기능을 제공하는 것과 관련된 컴포넌트에 저장될 수 있다. 또한, 클라이언트(105)는 웹 서버에 대한 중요한 요청을 추적하기 위한 메커니즘과 같은, http 세션의 인스턴스에 특정적인 국부적 컨텍스트를 가질 수 있다. 이 컨텍스트는 클라이언트(105)의 메모리, 클라이언트(105) 상의 파일, 또는 클라이언트(105)와 인터페이스하는 소프트웨어 컴포넌트에 저장될 수 있다. 클라이언트(105)와 서버(102c) 간의 연결이 지속적이지 않으면, 새로운 유저 세션은 서버(102c)와 클라이언트(105) 상의 새로운 세션 특정 컨텍스트로 설정될 필요가 있다. 본 발명은 세션을 유지하여 새로운 세션, 이에 따라 새로운 특정 세션 컨텍스트가 재설정될 필요가 없게 한다.

본 발명은 네트워크 레벨 연결 중단 동안 세션이 중단된 것을 클라이언트의 유저에게 통지하지 하지 않고 유저 세션을 유지한다. 본 발명의 이 형태의 동작시, 클라이언트(105)는 피어 컴퓨팅 디바이스에의 연결을 설정한다. 연결을 통해, 클라이언트(105)와 서버 간의 세션이 설정된다. 원격 액세스 클라이언트(120)는 인증 증명서, 설정된 세션에 대한 클라이언트(105)와 호스트 서버(102c) 컨텍스트와 같은 세션 관련 정보를 저정하여 보유한다. 네트워크 연결의 붕괴 검출시, 원격 액세스 클라이언트(120)는 네트워크 스택의 제2 부분(610a-610b)을 유지하면서 네트워크 스택(310a-310b)의 제1 부분(605a-605b)을 재설정할 수 있다. 네트워크 연결 붕괴는 클라이언트(105)와 서버(102c) 간의 세션에 의해 이용되는 기초 TCP/IP 연결의 중단을 초래할 수 있다. 그러나, 네트워크 스택(310a-310b)의 제2 부분(610a-610b)이 유지되기 때문에, 클라이언트(105) 상의 유저에게 세션이 중단된 것을 통지하지 않고 네트워크 연결이 재설정된 후에 세션이 재설정 및/또는 계속될 수 있다. 따라서, 네트워크 연결 붕괴로 인한 세션의 중단은 본 발명의 네트워크 붕괴 차단 기술을 이용하여 유저로부터 효율적으로 숨겨지게 된다.

더욱이, 본 발명은 신뢰적이며 지속적인 연결을 제공함으로써, 클라이언트(105)에서 세션이나 애플리케이션(338)을 다시 시작하지 않고 클라이언트(105)가 여러 네트워크 토폴러지를 관통할 수 있게 한다. 예를 들어, 클라이언트(105)는 무선 네트워크 연결을 갖는 컴퓨터 노트북일 수 있다. 클라이언트(105)가 제1 무선 네트워크로부터 제2 무선 네트워크로 이동하면, 클라이언트의 네트워크 연결은 네트워크 연결이 제2 무선 네트워크로 설정되기 때문에 제1 무선 네트워크로부터 임시로 붕괴될 수 있다. 제2 무선 네트워크는 호스트 이름이나 인터넷 프로토콜 주소와 같은 새로운 네트워크 식별자를 클라이언트(105)에게 할당한다. 이 새로운 네트워크 식별자는 제1 무선 네트워크에 의해 클라이언트(105)에게 할당된 네트워크 식별자와는 다르다. 다른 예에서, 클라이언트(105)는 네트워크 상의 포트에 이더넷 케이블을 통해 물리적으로 연결된다. 물리적 연결은 언플러그될 수 있으며 클라이언트(105)는 다른 위치로 이동하여 네트워크 상의 여러 포트에 플러그하게 된다. 이는 네트워크 연결의 붕괴 및 가능하게는 할당된 네트워크 식별자의 변경을 초래한다. 본 발명이 아니면, 피어 컴퓨팅 디바이스 간의 세션은 네트워크 토폴러지의 변경, 네트워크 연결의 붕괴 및/또는 할당된 네트워크 식별자의 변경으로 인해 재시작되어야 한다. 여기 기재된 방법과 시스템에 의해, 본 발명의 원격 액세스 클라이언트(120)는 네트워크 토폴러지와 네트워크 식별자의 변경을 취급하는 것을 포함하여 클라이언트에 대한 네트워크 연결을 유지하고 클라이언트(105)의 네트워크 연결을 자동으로 재설정한다. 클라이언트(105) 및 클라이언트(105)의 애플리케이션이나 세션은 네트워크 연결 붕괴 또는 네트워크 식별자의 붕괴가 없었던 것처럼 계속 동작할 수 있다. 더욱, 클라이언트(105)의 유저는 중단이나 변경이 있었던 것을 인식하지 못하고, 클라이언트(105)는 이런 중단의 보고를 수신하지 않는다.

부가의 형태에서, 도 2B, 3B, 3C, 4, 5B 및 6B의 방법과 같이, 본 발명의 기술은 서로 하나 이상의 조합으로 실행될 수 있다. 일 실시예에서, 피어투피어 라우팅 기술은 이상 확인 및/또는 MTU 조정 기술로 실행될 수 있다. 이것은 암호화 오버헤드로 인한 단편화를 줄이고 TCP의 신뢰적 메커니즘으로 인한 레이턴시를 방지하면서, 더욱 최적이며 직접적인 루트를 통해 피어에 연결되어 보안적인 SSL/TCP/IP 연결로 UDP를 통해 실시간 데이터를 통신하기 위해서, IP와 같은 클라이언트 통신 실시간 데이터를 제공한다. 부가하여, 이 실시예는 클라이언트측 애플리케이션 인식 우선 순위 기술과 더욱 결합될 수 있다. 이와 같이, 보안 실시간 데이터 통신은 VoIP와 같은 실시간 경험의 품질을 개선하기 위해 클라이언트의 다른 애플리케이션 보다 더욱 우선 순위가 높은 클라이언트로부터 통신될 수 있다. 네트워크 붕괴 기술은 네트워크의 소프트폰과 같은 모바일 VoIP 폰이 네트워크 액세스 지점 간에서 로밍하여 자동으로 세션을 유지할 수 있게 한다.

본 발명의 기술들은 SSL VPN 게이트웨이를 통한 VoIP 통신에서와 같이, 네트워크 통신 최적화를 위해 서로 상보적인 것이다. 이와 같이, 본 발명의 1) 피어투피어 라우팅 기술, 2) 이상 확인 기술, 3) 페이로드 시프팅 기술, 4) MTU 조정 기술, 5) 클라이언트측 애플리케이션 인식 기술, 및 6) 네트워크 붕괴 차단 기술 각각은 본 발명의 다음 기술 중 하나 이상으로 실행될 수 있다: 1) 피어투피어 라우팅 기술, 2) 이상 확인 기술, 3) 페이로드 시프팅 기술, 4) MTU 조정 기술, 5) 클라이언트측 애플리케이션 인식 기술, 및 6) 네트워크 붕괴 차단 기술.

본 발명의 다른 예시로, GoToMeeting.com, WebEx.com, 또는 LiveMeeting.com의 호스트 서비스와 같은 온라인 미팅, 협력 및/또는 데스크톱 공유 서비스는 하나 이상의 조합으로 본 발명의 기술을 이용한다. 호스트 서비스는 미팅 프리젠터의 제1 컴퓨팅 디바이스와 미팅 출석자의 제2 컴퓨팅 디바이스 간의 피어투피어 연결을 용이하게 하도록 게이트웨이(340) 및 방법 260의 기술을 이용한다. 미팅 프리젠터와 출석자의 컴퓨팅 디바이스는 원격 액세스 클라이언트(120)를 통해 다운로드된다. 미팅 프리젠터와 미팅 출석자가 피어투피어 연결을 설정하면, 피어 컴퓨팅 디바이스는 MTU 조정 기술, 클라이언트측 애플리케이션 인식 기술 또는 네트워크 붕괴 차단 기술과 같은 통신을 최적화하는 본 발명의 최적화 기술을 이용한다. 피어투피어 라우팅과 함께, 본 발명의 최적화 기술은 온라인 미팅, 협력 또는 데스크톱 공유의 성능, 효율 및 유저 경험을 개선하게 된다.

도 2A의 또 다른 형태에서, 예를 들어, 본 발명의 원격 액세스 클라이언트(120)는 하드웨어나 소프트웨어 기반의 VoIP 전화와 같은 텔레커뮤니케이션 장치(210a-210b)에 클라이언트(105)의 동적 호스트 컨피규레이션 프로토콜 (DHCP) IP 주소나 공중 가시 IP 주소를 분배할 수 있다. 본 발명의 게이트웨이(340)는 도 2A에서 나타낸 클라이언트(105b)와 같이 클라이언트의 공중 IP 주소의 발견을 용이하게 한다. 이와 같이, 본 발명의 기술은 프로토콜을 통해 IP 주소를 통신하는 프로토콜이 계속 기능할 수 있도록 한다.

본 발명의 정신와 영역에서 벗어나지 않고 당업자라면 많은 변형들을 행할 수 있을 것이다. 따라서, 설명된 실시예들은 예시의 목적으로만 나타낸 것이며 다음 청구범위에서 정의된 본 발명을 제한하고자 하는 것이 아님을 명백히 이해해야 한다. 이들 청구범위는 상기 설명에서 나타내고 기재하고 있는 것과 관련하여 동일하지 않더라도, 이들의 설명하고 있는 것을 포함하여 비실질적으로 다른 등가의 요소를 포함하는 것으로 판독되어야 한다.

도면의 간단한 설명

본 발명의 상기 및 그 외 목적, 형태, 특성 및 장점은 첨부한 도면과 관련한 다음 설명을 참조하여 더욱 명확하게 될 것이며 잘 이해될 것이다.

도 1A는 네트워크 환경에서 게이트웨이를 거쳐 본 발명의 동작을 실행하기 위한 실시예를 도시하는 블럭도.

도 1B는 피어투피어 네트워크 환경에서 본 발명의 동작을 실행하기 위한 다른 실시예의 블럭도.

도 1C는 네트워크 통신을 위해 본 발명의 원격 액세스 클라이언트의 실시예를 도시한 블럭도.

도 1D 및 1E는 본 발명의 실시예를 실행하는 데에 유용한 컴퓨팅 디바이스의 실시예를 도시하는 블럭도.

도 2A는 피어투피어 통신 루트를 설정하기 위해 본 발명의 기술의 실시예를 실행하기 위한 피어투피어 네트워크 환경의 실시예를 도시하는 블럭도.

도 2B는 본 발명의 피어투피어 루트 최적화 기술을 최적화하기 위해 실행되는 일 실시예의 단계를 도시하는 흐름도.

도 3A는 도 1A-1C에 도시된 설명적 환경의 컴퓨팅 디바이스의 네트워크 스택의 실시예를 도시하는 블럭도.

도 3B는 손실 프로토콜을 통한 전송을 위해 구성된 무손실 프로토콜 패킷을 통해 통신하도록 네트워크 패킷의 수신의 이상 확인을 이용하기 위해 실행되는 일 실시예의 단계를 도시한 흐름도.

도 3C는 손실 프로토콜을 통한 전송을 위해 구성된 무손실 프로토콜 패킷을 통해 통신하기 위해 실행되는 일 실시예의 단계를 도시하는 흐름도.

도 4는 최대 전송 단위 파라미터를 조정하기 위해 실행되는 일 실시예의 단계를 도시하는 흐름도.

도 5A는 클라이언트측 어플리케이션 인식 우선 순위 기술을 제공하기 위한 클라이언트의 환경을 도시한 블럭도.

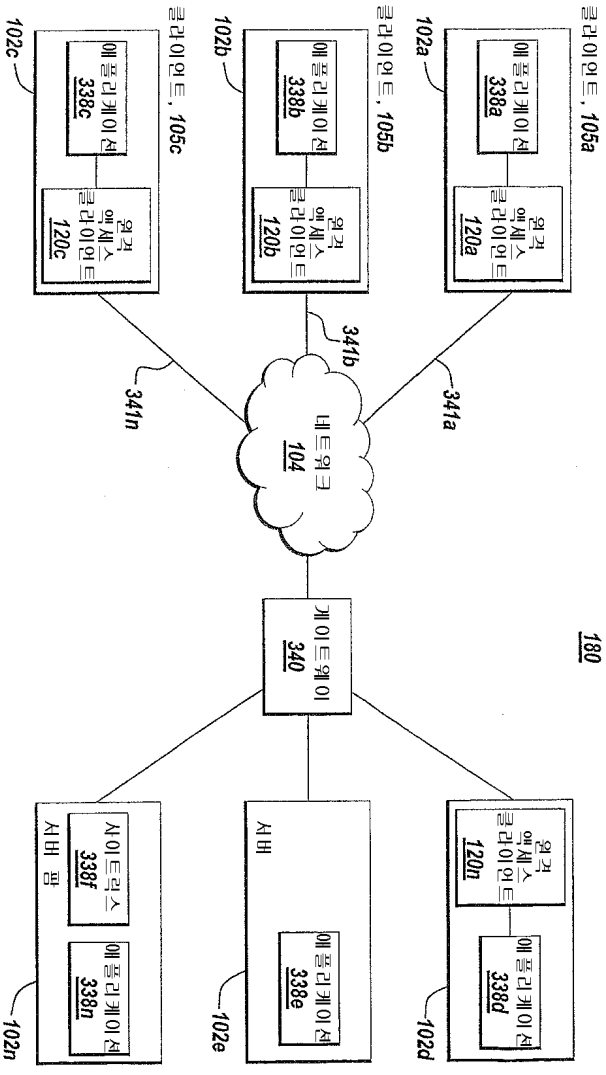
도 5B는 클라이언트측 어플리케이션 인식 우선 순위를 제공하기 위해 실행되는 단계의 일 실시예를 도시하는 흐름도.

도 6A는 디바이스의 네트워크 붕괴를 차단하기 위한 장치의 환경을 설명하는 블럭도.

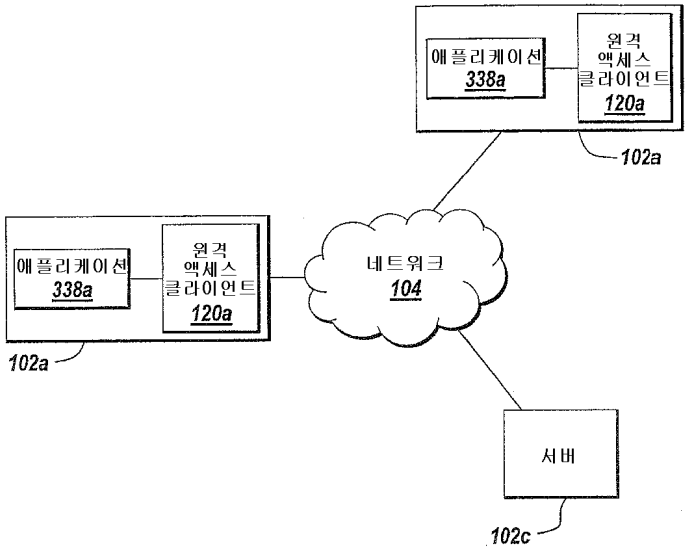
도 6B는 다바이스의 네트워크 붕괴를 차단하기 위해 실행되는 일 실시예의 단계를 설명하는 흐름도.

도면

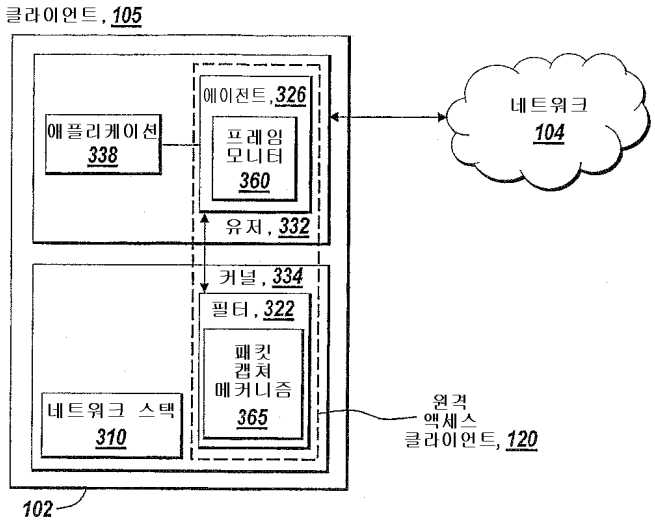
도면1a



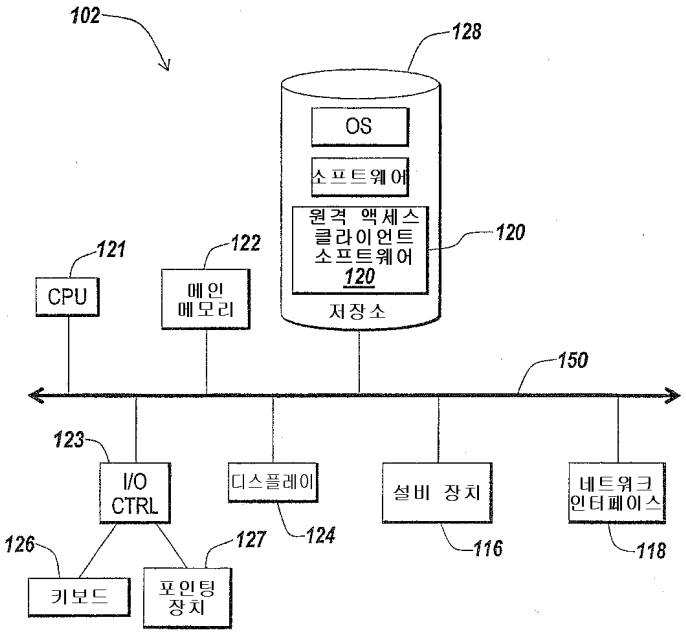
도면1b


애플리케이션
338a
원격
액세스
클라이언트
120a
102a
네트워크
104
서버
102c

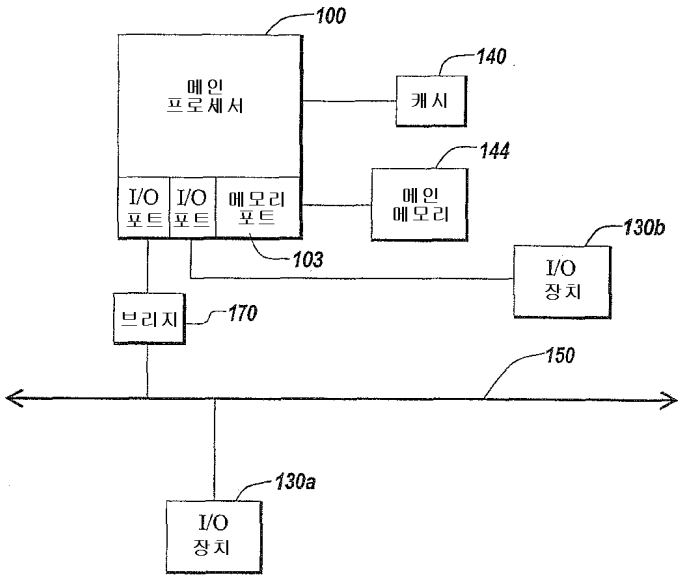
도면1c


클라이언트, 105
애플리케이션
338
에이전트, 326
프레임
모니터
360
유저, 332
네트워크
104
커널, 334
필터, 322
패킷
캡쳐
메커니즘
365
네트워크 스택
310
원격
액세스
클라이언트, 120
102

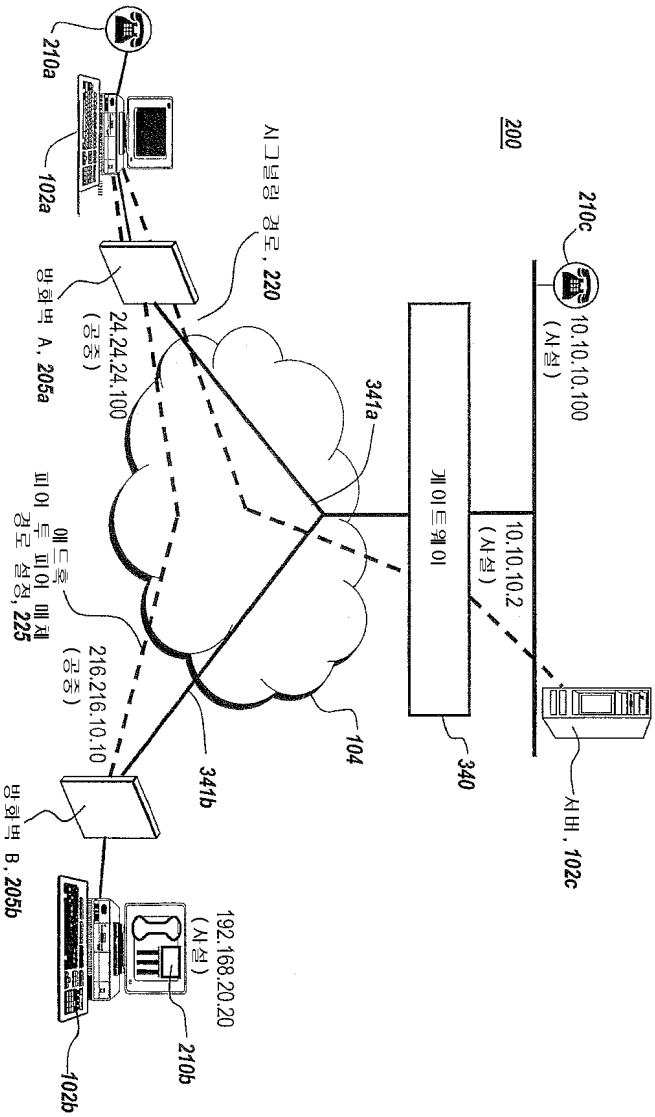
도면1d


102
128
OS
소프트웨어
원격 액세스 클라이언트 소프트웨어 120
120
저장소
121
CPU
122
메인 메모리
150
123
I/O CTRL
디스플레이
124
설비 장치
116
네트워크 인터페이스
118
126
키보드
127
포인팅 장치

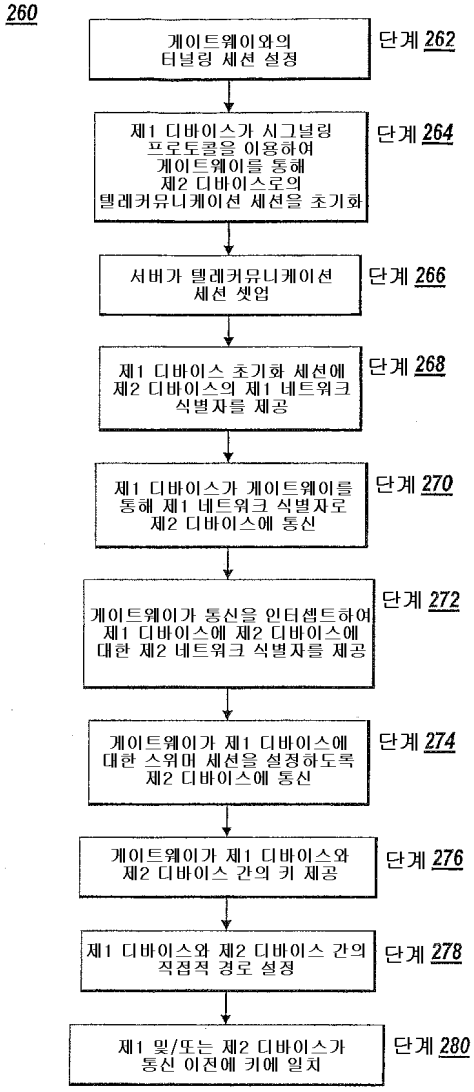
도면1e


100
메인 프로세서
140
캐시
144
I/O 포트
I/O 포트
메모리 포트
메인 메모리
130b
103
I/O 장치
브리지
170
150
130a
I/O 장치

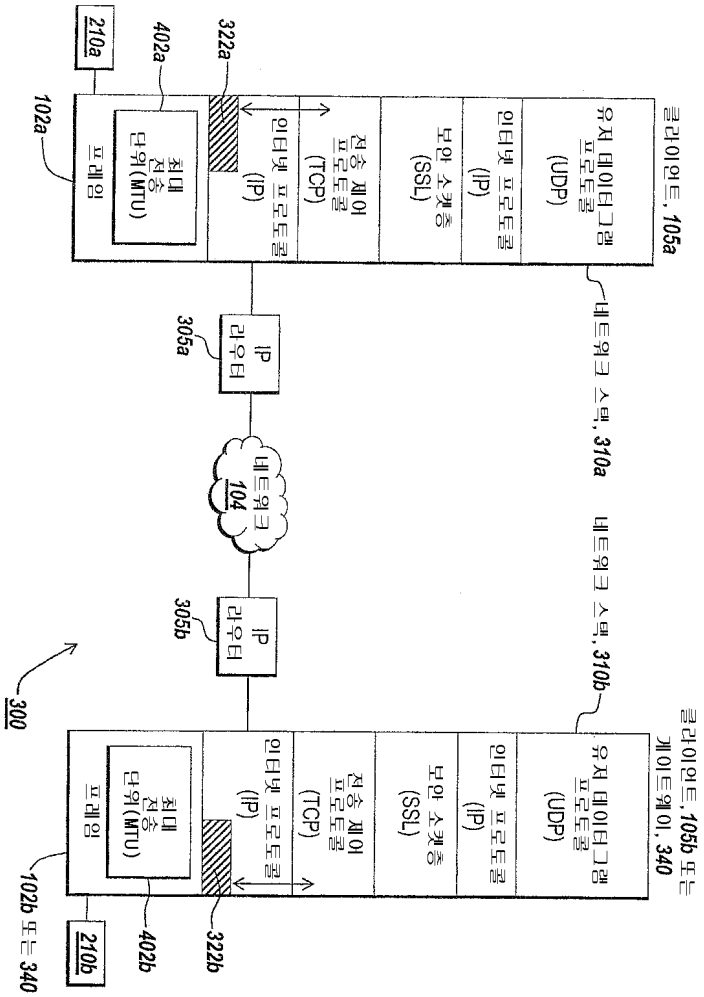
도면2a


200
210c
10.10.10.100
(사설)
시그널링 경로, 220
210a
102a
방화벽 A, 205a
24.24.24.100
(공중)
341a
게이트웨이
10.10.10.2
(사설)
에드홈 피어 투 피어 매체 경로 설정, 225
216.216.10.10
(공중)
104
340
서버, 102c
341b
방화벽 B, 205b
192.168.20.20
(사설)
210b
102b

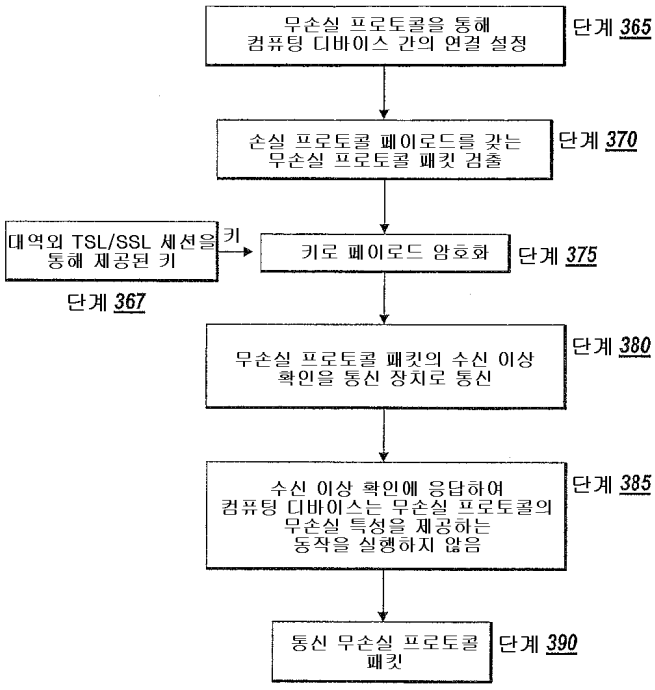
도면2b


260
게이트웨이와의 터널링 세션 설정
단계 262
제1 디바이스가 시그널링 프로토콜을 이용하여 게이트웨이를 통해 제2 디바이스로의 텔레커뮤니케이션 세션을 초기화
단계 264
서버가 텔레커뮤니케이션 세션 셋업
단계 266
제1 디바이스 초기화 세션에 제2 디바이스의 제1 네트워크 식별자를 제공
단계 268
제1 디바이스가 게이트웨이를 통해 제1 네트워크 식별자로 제2 디바이스에 통신
단계 270
게이트웨이가 통신을 인터셉트하여 제1 디바이스에 제2 디바이스에 대한 제2 네트워크 식별자를 제공
단계 272
게이트웨이가 제1 디바이스에 대한 스위머 세션을 설정하도록 제2 디바이스에 통신
단계 274
게이트웨이가 제1 디바이스와 제2 디바이스 간의 키 제공
단계 276
제1 디바이스와 제2 디바이스 간의 직접적 경로 설정
단계 278
제1 및/또는 제2 디바이스가 통신 이전에 키에 일치
단계 280

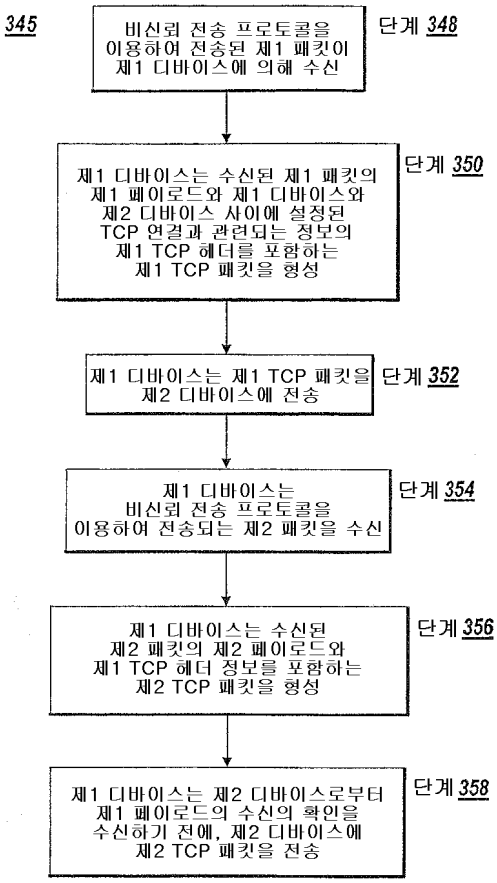
도면3a


클라이언트, 105a
유저 데이터그램 프로토콜 (UDP)
인터넷 프로토콜 (IP)
보안 소켓층 (SSL)
전송 제어 프로토콜 (TCP)
인터넷 프로토콜 (IP)
최대 전송 단위(MTU)
프레임
210a
402a
322a
102a
네트워크 스택, 310a
IP 라우터
305a
네트워크 104
IP 라우터
305b
네트워크 스택, 310b
300
클라이언트, 105b 또는 게이트웨이, 340
유저 데이터그램 프로토콜 (UDP)
인터넷 프로토콜 (IP)
보안 소켓층 (SSL)
전송 제어 프로토콜 (TCP)
인터넷 프로토콜 (IP)
최대 전송 단위(MTU)
프레임
102b 또는 340
210b
402b
322b

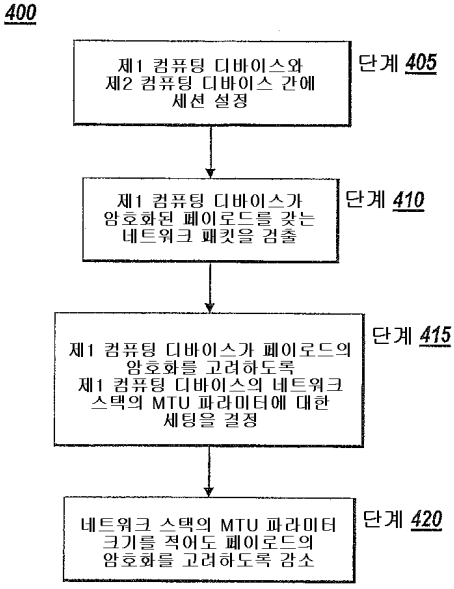
도면3b


무손실 프로토콜을 통해 컴퓨팅 디바이스 간의 연결 설정
단계 365
손실 프로토콜 페이로드를 갖는 무손실 프로토콜 패킷 검출
단계 370
대역외 TSL/SSL 세션을 통해 제공된 키
키
단계 367
키로 페이로드 암호화
단계 375
무손실 프로토콜 패킷의 수신 이상 확인을 통신 장치로 통신
단계 380
수신 이상 확인에 응답하여 컴퓨팅 디바이스는 무손실 프로토콜의 무손실 특성을 제공하는 동작을 실행하지 않음
단계 385
통신 무손실 프로토콜 패킷
단계 390

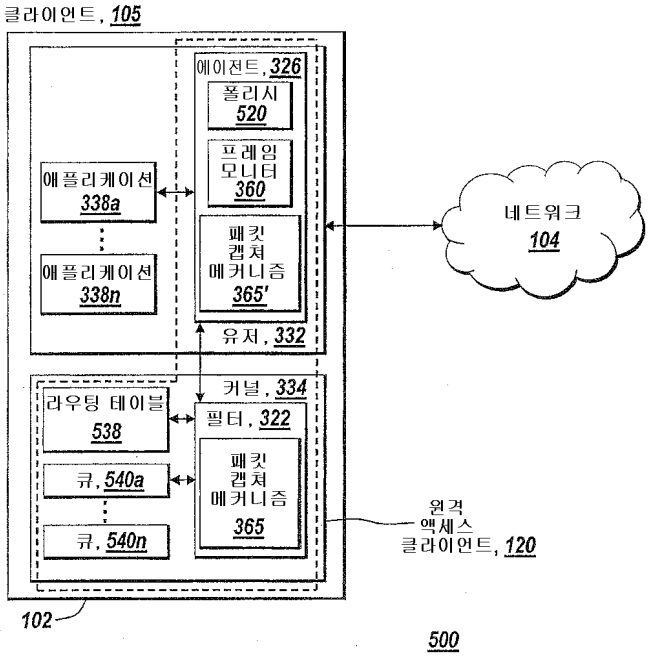
도면3c


345
비신뢰 전송 프로토콜을 이용하여 전송된 제1 패킷이 제1 디바이스에 의해 수신
단계 348
제1 디바이스는 수신된 제1 패킷의 제1 페이로드와 제1 디바이스와 제2 디바이스 사이에 설정된 TCP 연결과 관련되는 정보의 제1 TCP 헤더를 포함하는 제1 TCP 패킷을 형성
단계 350
제1 디바이스는 제1 TCP 패킷을 제2 디바이스에 전송
단계 352
제1 디바이스는 비신뢰 전송 프로토콜을 이용하여 전송되는 제2 패킷을 수신
단계 354
제1 디바이스는 수신된 제2 패킷의 제2 페이로드와 제1 TCP 헤더 정보를 포함하는 제2 TCP 패킷을 형성
단계 356
제1 디바이스는 제2 디바이스로부터 제1 페이로드의 수신의 확인을 수신하기 전에, 제2 디바이스에 제2 TCP 패킷을 전송
단계 358

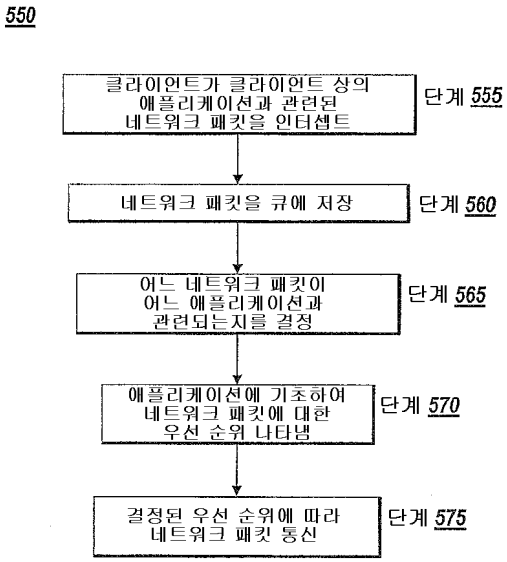
도면4


400
제1 컴퓨팅 디바이스와 제2 컴퓨팅 디바이스 간에 세션 설정
단계 405
제1 컴퓨팅 디바이스가 암호화된 페이로드를 갖는 네트워크 패킷을 검출
단계 410
제1 컴퓨팅 디바이스가 페이로드의 암호화를 고려하도록 제1 컴퓨팅 디바이스의 네트워크 스택의 MTU 파라미터에 대한 세팅을 결정
단계 415
네트워크 스택의 MTU 파라미터 크기를 적어도 페이로드의 암호화를 고려하도록 감소
단계 420

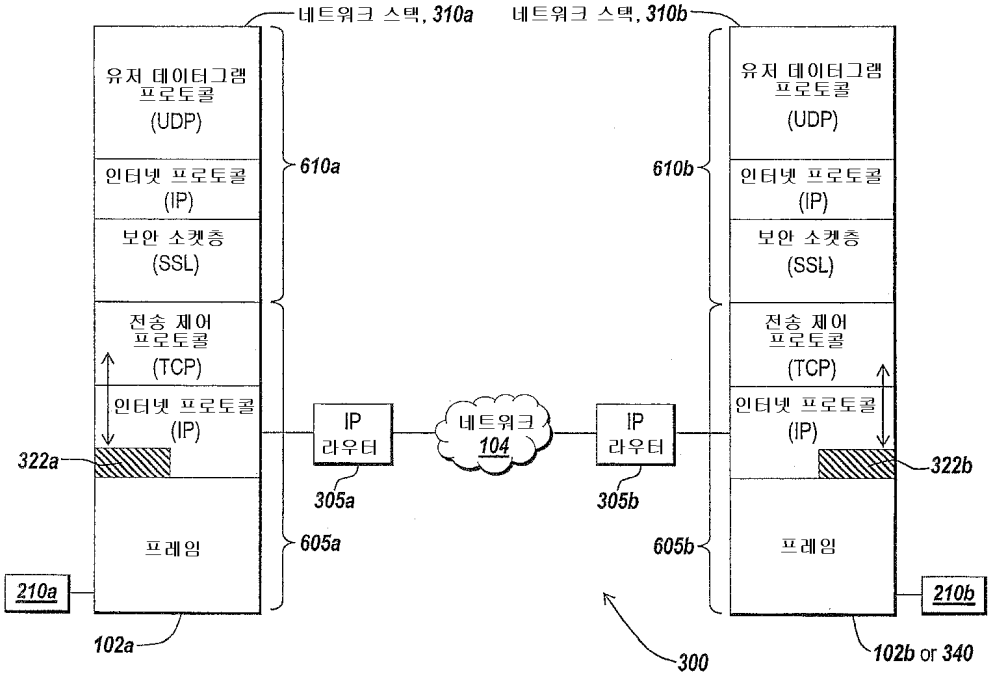
도면5a


클라이언트, 105
에이전트, 326
폴리시 520
프레임 모니터 360
애플리케이션 338a
애플리케이션 338n
패킷 캡쳐 메커니즘 365'
네트워크 104
유저, 332
커널, 334
라우팅 테이블 538
필터, 322
큐, 540a
큐, 540n
패킷 캡쳐 메커니즘 365
원격 액세스 클라이언트, 120
102
500

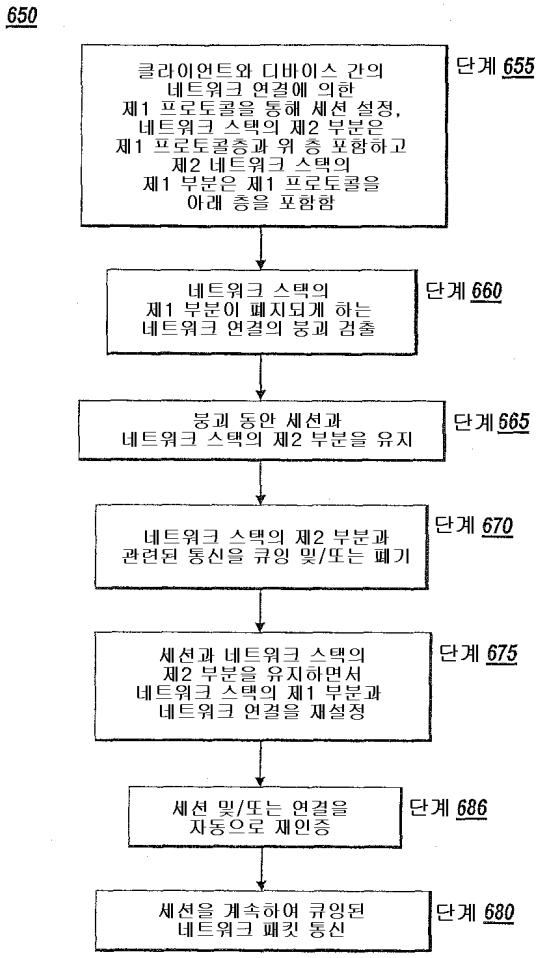
도면5b


550
클라이언트가 클라이언트 상의 애플리케이션과 관련된 네트워크 패킷을 인터셉트
단계 555
네트워크 패킷을 큐에 저장
단계 560
어느 네트워크 패킷이 어느 애플리케이션과 관련되는지를 결정
단계 565
애플리케이션에 기초하여 네트워크 패킷에 대한 우선 순위 나타냄
단계 570
결정된 우선 순위에 따라 네트워크 패킷 통신
단계 575

도면6a


네트워크 스택, 310a
네트워크 스택, 310b
유저 데이터그램 프로토콜 (UDP)
인터넷 프로토콜 (IP)
보안 소켓층 (SSL)
전송 제어 프로토콜 (TCP)
인터넷 프로토콜 (IP)
프레임
610a
605a
610b
605b
322a
322b
IP 라우터
305a
네트워크 104
IP 라우터
305b
210a
210b
102a
300
102b or 340

도면6b


650
클라이언트와 디바이스 간의 네트워크 연결에 의한 제1 프로토콜을 통해 세션 설정, 네트워크 스택의 제2 부분은 제1 프로토콜층과 위 층 포함하고 제2 네트워크 스택의 제1 부분은 제1 프로토콜을 아래 층을 포함함
단계 655
네트워크 스택의 제1 부분이 폐지되게 하는 네트워크 연결의 붕괴 검출
단계 660
붕괴 동안 세션과 네트워크 스택의 제2 부분을 유지
단계 665
네트워크 스택의 제2 부분과 관련된 통신을 큐잉 및/또는 폐기
단계 670
세션과 네트워크 스택의 제2 부분을 유지하면서 네트워크 스택의 제1 부분과 네트워크 연결을 재설정
단계 675
세션 및/또는 연결을 자동으로 재인증
단계 686
세션을 계속하여 큐잉된 네트워크 패킷 통신
단계 680