



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년03월17일
(11) 등록번호 10-0814546
(24) 등록일자 2008년03월11일

- (51) Int. Cl.
H04L 12/26 (2006.01)
- (21) 출원번호 10-2001-7006533
- (22) 출원일자 2001년05월24일
심사청구일자 2004년11월23일
번역문제출일자 2001년05월24일
- (65) 공개번호 10-2001-0101075
- (43) 공개일자 2001년11월14일
- (86) 국제출원번호 PCT/US1999/027969
국제출원일자 1999년11월23일
- (87) 국제공개번호 WO 2000/31963
국제공개일자 2000년06월02일
- (30) 우선권주장
60/109,718 1998년11월24일 미국(US)
- (56) 선행기술조사문헌
US05787253 A1
KR1020020077460 A
KR1019990087162 A
KR1019960027840 A
- (73) 특허권자
닉션, 인크.
미국 뉴저지주 08852 몬머스 정선 콘월 로드 1100
- (72) 발명자
프루티 파라그
미국 뉴저지주 08816 이스트 브룬스윅 말로우 로드 18
헤이베이 앤드류
미국 펜실베이니아주 17402 요크 로빈우드 로드 4074
쿠리엔 텍탈락칼 바루기스
미국 뉴욕주 08536 플랜스보로 폭스 런 드라이브 901
- (74) 대리인
김진희, 김태홍

전체 청구항 수 : 총 66 항

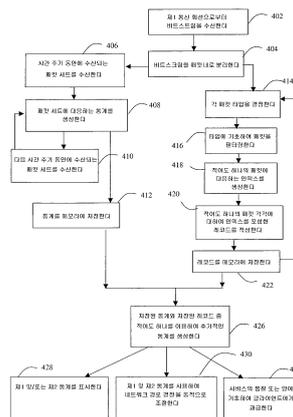
심사관 : 퇴-신성길

(54) 통신 데이터를 수집하여 분석하는 장치 및 방법

(57) 요약

본 발명은 제1 통신 회선상의 데이터를 모니터링하는 방법에 관한 것이다. 데이터는 상기 제1 통신 회선(402)으로부터 수신되고, 복수의 패킷들(406)은 그 데이터로부터 추출된다(416). 그후 복수의 패킷들에 대응하는 통계는 반복적으로 생성된다(408).

대표도 - 도4



(81) 지정국

국내특허 : 알바니아, 아르메니아, 오스트리아(실용신안포함), 오스트레일리아(소특허), 아제르바이잔, 보스니아 헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코(실용신안포함), 독일(실용신안포함), 덴마크(실용신안포함), 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르기스스탄, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아(실용신안포함), 타지키스탄, 투르크멘, 터키, 트리니다드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투갈, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 아랍에미리트, 남아프리카, 그라나다, 가나, 감비아, 크로아티아, 인도네시아, 인도, 시에라리온, 세르비아 앤 몬테네그로, 짐바브웨

AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 시에라리온, 가나, 감비아, 짐바브웨, 탄자니아

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르기스스탄, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크멘

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투갈, 스웨덴, 핀란드, 사이프러스

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디부아르, 카메룬, 가봉, 기니, 말리, 모리타니, 기니 비사우

특허청구의 범위

청구항 1

제1 통신 회선상의 제1 데이터를 수집 및 분석하는 방법으로서,

- (a) 상기 제1 통신 회선으로부터 상기 제1 데이터를 수신하는 단계와;
 - (b) 상기 제1 데이터를 패킷들로 분리(seggregate)하는 단계와;
 - (c) 각 패킷의 개별적인 제1 특성에 기초하여 패킷들을 선택하는 단계와;
 - (d) 개별적인 인덱스를 상기 선택된 패킷들 각각과 연관시키는 단계와;
 - (e) 상기 선택된 패킷들 각각을 상기 패킷의 개별적인 인덱스를 포함하는 개별적인 레코드로 변환하는 단계와;
 - (f) 상기 레코드들을 저장하는 단계와;
 - (g) 복수의 연속적인 주기들의 각각의 주기 동안 수신된 상기 선택된 패킷들 각각의 개별적인 제2 특성에 기초하여 카운트를 저장하는 단계;
- 를 포함하는 데이터 수집 및 분석 방법.

청구항 2

제1 통신 회선상의 데이터를 모니터링하는 방법으로서,

- (a) 상기 제1 통신 회선으로부터 제1 데이터를 수신하는 단계와;
 - (b) 상기 제1 데이터를 패킷들로 분리하는 단계와;
 - (c) 복수의 연속적인 제1 시간 주기들의 각각의 주기 동안 수신된 패킷들에 대응하여 통계를 생성하는 단계로서, 상기 제1 시간 주기들은 제1 지속시간 값을 구비하는 것인, 상기 통계 생성 단계와;
 - (d) 상기 복수의 연속적인 제1 시간 주기들의 각각의 주기 동안 상기 생성된 통계들을 분리하여 저장하는 단계와;
 - (e) 상기 복수의 저장된 통계들을 모음(aggregate)함으로써 추가적인 통계를 생성하는 단계;
- 를 포함하는 데이터 모니터링 방법.

청구항 3

제2항에 있어서,

- 각 패킷들의 개별적인 종류에 기초하여 패킷들을 선택하는 단계로서, 상기 단계 (c)에서 생성된 상기 통계들은 상기 선택된 패킷들에 대응하는 것인, 상기 패킷 선택 단계와;
- 개별적인 인덱스를 각 패킷과 연관시키는 단계와;
- 각 패킷을, 각 패킷의 개별적인 인덱스를 포함하는 개별적인 레코드로 변환하는 단계와;
- 상기 레코드들을 저장하는 단계;
- 를 포함하는 데이터 모니터링 방법.

청구항 4

제2항에 있어서,

- 상기 제1 시간 주기보다 더 긴 제2 시간 주기에 대응하는 제2 지속시간 값을 수신하는 단계를 포함하고,
- 상기 추가적인 통계는 상기 제2 시간 주기 동안 수신된 패킷들에 대응하는 것인 데이터 모니터링 방법.

청구항 5

제3항에 있어서,

상기 제1 시간 주기보다 더 긴 제2 시간 주기에 대응하는 제2 지속시간 값을 수신하는 단계를 포함하고;

적어도 하나의 제1 시간 주기를 포함하는 상기 제2 시간 주기 동안 수신된 패킷들에 대응하는 상기 추가적인 통계는 상기 저장된 레코드들 및 상기 저장된 통계들 중 적어도 어느 하나를 이용하여 생성되는 것인 데이터 모니터링 방법.

청구항 6

제2항에 있어서, 상기 복수의 연속적인 제1 시간 주기들의 각각 동안 수신된 패킷에 대응하는 상기 통계는, 비트들의 개수, 바이트들의 개수, 패킷들의 개수, 사전결정된 프로토콜의 패킷들의 개수, 사전결정된 프로토콜 계층의 패킷들의 개수, 사전결정된 소스 어드레스를 구비한 패킷들의 개수 및 개별적인 패킷의 사전결정된 목적지 어드레스를 구비한 패킷들의 개수 중 적어도 하나를 포함하는 것인 데이터 모니터링 방법.

청구항 7

제3항에 있어서, 하나의 레코드는 상기 레코드의 개별적인 패킷의 일부와 상기 패킷의 개별적인 인덱스의 일부를 포함하는 것인 데이터 모니터링 방법.

청구항 8

제3항에 있어서, 패킷의 상기 개별적인 인덱스는 상기 패킷이 수신된 시간에 대응하는 것인 데이터 모니터링 방법.

청구항 9

제8항에 있어서, 절대 시간을 나타내는 글로벌 위치 지정 위성으로부터 시간 신호를 수신하는 단계와; 상기 패킷이 상기 절대 시간에 기초하여 수신된 상기 시간을 생성하는 단계를 더 포함하는 것인 데이터 모니터링 방법.

청구항 10

제3항에 있어서,

제2 통신 회선으로부터 발신된 상기 수신 패킷들 각각은 상기 제2 통신 회선 상의 상기 패킷의 전송에 대응하는 개별적인 제1 시간의 표시를 포함하는 것이고,

각 패킷이 상기 제1 통신 회선으로부터 수신되는 경우 개별적인 제2 시간을 결정하는 단계와;

상기 패킷의 개별적인 제1 시간으로부터 상기 패킷의 개별적인 제2 시간을 감산함으로써 각 패킷에 대응하는 전송 지연을 계산하는 단계;

를 더 포함하는 데이터 모니터링 방법.

청구항 11

제10항에 있어서, 각 패킷에 대응하는 상기 전송 지연은, 상기 패킷이 제1 통신 회선 상에서 검출되는 시간과, 상기 패킷이 제2 통신 회선 상에서 검출되는 시간과, 상기 제1 통신 회선 상의 데이터 전송 속도와, 상기 제1 통신 회선 상의 상기 패킷의 길이에 기초하여 계산되는 것인 데이터 모니터링 방법.

청구항 12

제3항에 있어서, 상기 단계 (a)는 상기 제1 통신 회선으로의 비-개입 접속(non-intrusive coupling)을 이용하여 상기 제1 통신 회선으로부터 상기 제1 데이터를 수신하는 단계를 포함하는 것인 데이터 모니터링 방법.

청구항 13

제3항에 있어서,

선택될 패킷들의 종류, 상기 제1 지속시간 값, 단계 (c)에서 생성된 상기 통계의 식별 중 적어도 하나를 나타내는 정보를 수신하는 단계를 더 포함하는 데이터 모니터링 방법.

청구항 14

제13항에 있어서, 상기 정보는 상기 제1 통신 회선을 통해 수신되는 것인 데이터 모니터링 방법.

청구항 15

삭제

청구항 16

제10항에 있어서, 상기 제2 시간을 결정하기 위하여 글로벌 위치 지정 위성으로부터 시간 신호를 수신하는 단계를 포함하는 데이터 모니터링 방법.

청구항 17

제3항에 있어서, 상기 단계 (c)는 각 개별적인 연속 시간 주기 동안 수신된 사전결정된 패킷 종류의 패킷들에 대응하는 각 연속 시간 주기에 대한 적어도 하나의 서비스 품질 값을 생성하는 단계를 포함하는 것인 데이터 모니터링 방법.

청구항 18

제17항에 있어서, 상기 적어도 하나의 서비스 품질 값은 상기 개별적인 연속 시간 주기 동안에 수신된 사전결정된 패킷 종류의 상기 패킷들에 대응하는 재전송률 및 라운드 트립 지연(round trip delay) 중 적어도 하나를 나타내는 것인 데이터 모니터링 방법.

청구항 19

제3항에 있어서,

상기 개별적인 종류에 기초하여 패킷들을 선택하기 위하여 대응하는 어플리케이션 종류, 대응하는 패킷 콘텐츠, 패킷 소스 및, 패킷 목적지 중 적어도 하나에 기초하여 각 패킷의 개별적인 종류를 결정하는 단계를 포함하는 데이터 모니터링 방법.

청구항 20

제3항에 있어서, 상기 제1 통신 회선은 사용자를 포함하는 네트워크 내에 있고, 상기 단계 (c)는 개별적인 연속 시간 주기 동안에 수신되는 사용자로부터의 패킷들 또는 사용자에게 보내지는 패킷들에 대응하는 각 연속 시간 주기에 대한 적어도 하나의 사용자 프로필 통계를 생성하는 단계를 포함하는 것인 데이터 모니터링 방법.

청구항 21

제20항에 있어서, 상기 적어도 하나의 사용자 프로필 통계는 상기 저장된 레코드들을 사용하여 생성되는 것인 데이터 모니터링 방법.

청구항 22

제2항에 있어서, 상기 데이터 모니터링 방법은, 사용자 통계를 식별하는 사용자로부터의 입력을 수신하는 단계를 더 포함하고, 단계 (c)는 상기 사용자 통계를 생성하는 단계를 포함하는 것인 데이터 모니터링 방법.

청구항 23

제3항에 있어서,

사용자 통계를 식별하는 사용자로부터의 입력을 수신하는 단계와;

상기 저장된 통계들 및 상기 저장된 상기 레코드들 중 적어도 하나를 이용하여 상기 식별된 사용자 통계를 생성하는 단계;

를 더 포함하는 데이터 모니터링 방법.

청구항 24

제2항에 있어서, 상기 제1 데이터는 제1 프로토콜에 따라 상기 제1 통신 회선 상에 전송되는 것이고,

상기 데이터 모니터링 방법은, 상기 제1 프로토콜에 대응하는 복호화 파라미터들을 수신하는 단계를 더 포함하고,

상기 단계 (a)는 상기 복호화 파라미터에 따라 상기 제1 데이터를 수신하는 단계를 포함하며, 상기 단계 (b)는 상기 수신된 제1 데이터를 상기 복호화 파라미터들에 따라 패킷들로 분리하는 단계를 포함하는 것인 데이터 모니터링 방법.

청구항 25

제2항에 있어서,

상기 연속적인 제1 시간 주기들의 각각 동안 수신된 복수의 패킷 종류들 각각의 패킷들을 카운트하는 단계와; 표시 장치의 표시 영역의 제1 부분에서 상기 제1 시간 주기보다 더 큰 제2 시간 주기 동안 축적된 상기 복수의 패킷 종류들 및 그 대응하는 카운트들을 표시하는 단계를 포함하는 데이터 모니터링 방법.

청구항 26

제25항에 있어서, 상기 복수의 패킷 종류들은 사용자에게 의해 선택 가능한 것이고,

상기 데이터 모니터링 방법은, 사용자에게 의해 상기 패킷 종류들 중 하나의 사용자 선택을 수신하는 단계와; 상기 제2 시간 주기 동안에 수신된 상기 선택된 패킷 종류의 패킷들에 대응하는 통계들을 표시하는 단계를 더 포함하는 데이터 모니터링 방법.

청구항 27

제25항에 있어서, 상기 표시 영역의 제2 부분에 상기 제2 시간 주기에 걸쳐 플롯(plot)으로 상기 복수의 패킷 종류들에 대응하는 상기 통계들을 그래픽으로 표시하는 단계를 더 포함하는 데이터 모니터링 방법.

청구항 28

제25항에 있어서,

상기 표시 영역의 제2 부분에 상기 제2 시간 주기에 걸친 범위 동안 플롯으로 상기 복수의 패킷 종류들에 대응하는 상기 통계들의 그래픽 표시를 생성하는 단계로서, 상기 플롯은 복수의 이산 선택 가능 시간 주기들을 포함하는 것인, 상기 그래픽 표시 생성 단계와;

복수의 이산 선택 가능 시간 주기들의 범위의 사용자 선택을 수신하는 단계와;

상기 선택된 시간 주기들에 대응하는 통계들을 표시하기 위해 상기 그래픽 표시를 갱신하는 단계를 더 포함하는 데이터 모니터링 방법.

청구항 29

제3항에 있어서,

데이터 스트림에 속하는 패킷들을 식별하는 단계와;

상기 식별된 패킷들에 대응하는 상기 레코드들에 별도의 레코드 및 별도의 필드 중 하나로서 스트림 식별 정보를 저장하는 단계;

를 더 포함하는 데이터 모니터링 방법.

청구항 30

제29항에 있어서, 상기 저장된 레코드들 및 상기 저장된 스트림 식별 정보를 이용하여 상기 데이터 스트림을 재생성하는 단계를 더 포함하는 데이터 모니터링 방법.

청구항 31

제3항에 있어서,

상기 제1 통신 회선은 제2 통신 회선을 포함하는 네트워크 내에 있고, 각 선택된 패킷과 연관된 상기 개별적인

인덱스는 상기 패킷의 개별적인 시간 값을 포함하고, 각 레코드는 상기 선택된 개별적인 패킷의 고유하게 식별 가능한 부분을 포함하는 것이고,

상기 데이터 모니터링 방법은,

상기 제2 통신 회선으로부터 제2 데이터를 수신하는 단계와;

상기 제2 데이터를 패킷들로 분리하는 단계와;

각 패킷의 개별적인 종류에 기초하여 상기 제2 통신 회선으로부터 수신된 패킷들을 선택하는 단계와;

상기 제2 통신 회선으로부터 수신된 상기 선택된 패킷들 각각이 수신된 시간에 대응하는 개별적인 시간값을 결정하는 단계와;

개별적인 인덱스를 상기 제2 통신 회선으로부터 수신된 상기 선택된 패킷들의 각각과 연관시키는 단계로서, 상기 개별적인 인덱스는 상기 개별적인 시간값을 포함하는 것인, 상기 연관 단계와;

상기 제2 통신 회선으로부터 수신된 선택된 패킷들 각각을, 상기 제2 통신 회선으로부터 선택된 패킷의 고유 식별 가능 부분을 포함하고 상기 패킷의 개별적인 인덱스를 포함하는 개별적인 레코드로 변환하는 단계와;

상기 제2 통신 회선으로부터 수신된 상기 선택된 패킷들에 대응하는 상기 레코드들을 저장하는 단계와;

상기 제1 통신 회선으로부터 수신된 선택된 패킷들 중 어느 패킷들이 패킷들의 정합된 쌍들을 생성하기 위하여 상기 제2 통신 회선으로부터 수신된 패킷들에 대응하는지 결정하기 위하여, 상기 제1 통신 회선으로부터 수신된 레코드들 내의 패킷들의 상기 고유 식별 가능 부분들을 상기 제2 통신 회선으로부터 수신된 패킷들의 상기 고유 식별 가능 부분들과 비교하는 단계와;

그 개별적인 인덱스들을 사용하여 패킷들의 정합된 쌍들에 대응하는 전송 지연을 생성하는 단계;

를 포함하는 데이터 모니터링 방법.

청구항 32

제31항에 있어서,

특정의 정합된 패킷에 대한 상기 전송 지연은,

상기 제1 전송 회선 상의 상기 정합된 패킷의 수신 시간과, 상기 제2 전송 회선 상의 상기 정합 패킷의 수신 시간과, 상기 제1 전송 회선 상의 데이터 전송 속도와, 상기 제1 전송 회선 상의 상기 정합 패킷의 길이에 기초하여 계산되는 것인 데이터 모니터링 방법.

청구항 33

제32항에 있어서, 상기 제1 통신 회선은 제1 프로토콜을 이용하여 데이터를 전송하고, 상기 제2 통신 회선은 상기 제1 프로토콜과는 상이한 제2 프로토콜을 이용하여 데이터를 전송하는 것인 데이터 모니터링 방법.

청구항 34

제31항에 있어서, 상기 전송 지연은 10 마이크로초 이하의 정확도 레벨에서 생성되는 것인 데이터 모니터링 방법.

청구항 35

제1 지점과 제2 지점 사이의 복수의 경로들을 포함하는 통신 네트워크에서 상기 제1 지점으로부터 상기 제2 지점으로 제1 데이터를 라우팅하는 방법으로서,

상기 제1 지점과 상기 제2 지점 사이의 상기 복수의 경로들 상의, 상기 제1 데이터와는 분리된 제2 데이터의 흐름에 기초하여 흐름 통계들을 생성하는 단계와;

상기 생성된 흐름 통계들에 기초하여 상기 제1 및 제2 지점 사이의 상기 제1 데이터를 라우팅하는 단계;

를 포함하는 데이터 라우팅 방법.

청구항 36

표시 영역을 구비한 표시 장치 상에 시간 구간 동안 제1 통신 회선으로부터 수신된 패킷들에 대응하는 하나 이상의 패킷 특성들 또는 통계들을 표시하는 방법으로서,

(a) 상기 표시 영역의 제1 부분에 상기 하나 이상의 패킷 특성들 또는 통계들을 목록화한 테이블을 표시하는 단계와;

(b) 상기 표시 영역의 제2 부분에 상기 시간 구간에 걸쳐 하나 이상의 상기 패킷 특성들 또는 통계들의 플롯을 표시하는 단계로서, 상기 플롯은 두 개의 축들을 갖고, 상기 패킷 특성들 또는 통계들은 상기 플롯의 일축에 도시되며, 상기 시간은 상기 플롯의 타축에 도시되는 것인, 상기 플롯 표시 단계를

를 포함하는 표시 방법.

청구항 37

제36항에 있어서, 상기 패킷들은 프로토콜 계층에서 복수의 프로토콜에 대응하는 것이고, 상기 단계 (a)는 상기 복수의 프로토콜 각각 및 그 대응하는 패킷들의 수를 목록화하는 테이블을 표시하는 단계를 포함하는 것인 표시 방법.

청구항 38

제37항에 있어서, 상기 복수의 프로토콜들 중 하나의 선택을 검출하는 단계와; 상기 선택된 프로토콜의 패킷들에 대응하는 패킷의 특성들을 표시하기 위한 테이블과, 상기 선택된 프로토콜의 상기 패킷의 특성들을 표시하기 위한 상기 플롯 중 적어도 하나를 갱신하는 단계를 더 포함하는 표시 방법.

청구항 39

제36항에 있어서, 텍스트 필드의 시간들의 엔트리 중 하나에 의한 시간 구간 보다 작은 시간 서브구간의 선택과, 상기 플롯의 시간 축에 따른 시간 구간의 선택을 수신하는 단계와; 상기 선택한 시간 서브 구간에 응답하여 상기 테이블들 및 상기 플롯들 중 적어도 하나를 갱신하는 단계를 더 포함하는 표시 방법.

청구항 40

제37항에 있어서, 상기 복수의 프로토콜들 중 하나의 선택을 검출하고, 상기 선택된 프로토콜의 상기 패킷 특성들과 모든 프로토콜들의 상기 패킷 특성들 양쪽 모두를 동시에 표시하기 위해 상기 플롯을 갱신하는 단계를 더 포함하는 표시 방법.

청구항 41

제36항에 있어서, 개시 시간 및 상기 시간 구간 보다 더 긴 지속시간에 걸쳐 있는 종료 시간을 수신하는 단계와; 상기 지속시간에 대응하도록 상기 테이블들 및 상기 플롯들 중 적어도 하나를 갱신하는 단계를 더 포함하는 표시 방법.

청구항 42

제36항에 있어서, 상기 패킷들의 서브세트는 호스트에 대응하는 것이고,

상기 표시 방법은 상기 호스트의 선택을 검출하고, 상기 패킷들의 서브세트에 대응하는 통계들을 표시하는 단계를 더 포함하는 표시 방법.

청구항 43

제36항에 있어서, 상기 패킷들은 복수의 프로토콜들에 대응하고, 상기 패킷들의 서브세트는 상기 복수의 프로토콜들 중 하나에 대응하는 것이고,

상기 표시 방법은, 상기 복수의 프로토콜들 중 하나의 선택을 검출하고, 상기 복수의 프로토콜들 중 상기 선택된 하나에 대응하는 통계들을 표시하는 단계를 더 포함하는 표시 방법.

청구항 44

호스트 컴퓨터상의 호스트 클럭을 네트워크 인터페이스 카드상의 인터페이스 클럭과 동기시키는 방법으로서,

상기 네트워크 인터페이스 카드로부터 인터페이스 클럭 값을 수신하는 단계와;
 상기 인터페이스 클럭 값에서 사전결정된 서비스 시간을 감산함으로써 조정된 인터페이스 클럭 값을 생성하는 단계와;
 상기 조정된 인터페이스 클럭 값을 상기 호스트 컴퓨터에 제공하는 단계와;
 상기 호스트 클럭 값을 수신하는 단계와;
 상기 조정된 인터페이스 클럭 값을 상기 호스트 클럭 값과 상관시키는 단계;
 를 포함하는 동기 방법.

청구항 45

제1 통신 회선 및 상기 제1 통신 회선과는 상이한 제2 통신 회선을 구비한 네트워크 상의 통신을 모니터링하는 방법으로서,

- (a) 상기 제1 통신 회선으로부터 제1 복수의 패킷들을 수신하는 단계와;
- (b) 상기 제2 통신 회선으로부터 제2 복수의 패킷들을 수신하는 단계와;
- (c) 상기 제1 복수의 패킷들과 상기 제2 복수의 패킷들을 상관시키는 단계;

를 포함하는 모니터링 방법.

청구항 46

제45항에 있어서, 상기 단계 (c)는 상기 제1 복수의 각 패킷들과 상기 제2 복수의 각 패킷들 각각의 고유의 식별 부분을 추출하는 단계와; 일치된 패킷 쌍들을 생성하기 위하여, 상기 제1 복수의 패킷들의 상기 고유의 식별 부분들을, 상기 제2 복수의 패킷들의 상기 고유의 식별 부분들과 비교하는 단계를 포함하는 것인 모니터링 방법.

청구항 47

제45항에 있어서, 상기 제1 복수의 패킷들은 제1 네트워크 모니터에 의해 수신되고 상기 제2 복수의 패킷들은 제2 네트워크 모니터에 의해 수신되는 것이고,

상기 단계 (a)는 상기 제1 복수의 패킷들을 시간 스탬핑하는 단계를 포함하고, 상기 단계 (b)는 상기 제2 복수의 패킷들을 시간 스탬핑하는 단계를 포함하는 것이고,

상기 모니터링 방법은, 상기 제1 및 제2 네트워크 모니터들을 절대 클럭 기준과 동기시키는 단계를 더 포함하는 모니터링 방법.

청구항 48

제47항에 있어서, 상기 네트워크 모니터들은 글로벌 위치 지정 위성으로부터 시간 신호를 수신함으로써 동기되는 것인 모니터링 방법.

청구항 49

제1 통신 회선 및 제2 통신 회선을 포함하는 네트워크 상의 통신을 모니터링하는 시스템으로서,

제1 클럭을 갖고, 상기 제1 통신 회선에 결합되어, 상기 제1 통신 회선으로부터 제1 데이터를 수신하는 제1 네트워크 모니터와;

제2 클럭을 갖고, 상기 제2 통신 회선에 결합되어, 상기 제2 통신 회선으로부터 제2 데이터를 수신하는 제2 네트워크 모니터와;

상기 제1 클럭을 상기 제2 클럭과 동기시키는 동기 수단;

을 포함하는 모니터링 시스템.

청구항 50

제49항에 있어서, 상기 제1 클럭 및 상기 제2 클럭은 서로 1 마이크로초 내로 동기되는 것인 모니터링 시스템.

청구항 51

제49항에 있어서, 상기 동기 수단은, 상기 제1 네트워크 모니터에 연관되어 공통 클럭 기준으로부터 시간 신호를 수신하는 수신기와; 상기 제2 네트워크 모니터에 연관되어 상기 공통 클럭 기준으로부터 시간 신호를 수신하는 수신기를 포함하는 것인 모니터링 시스템.

청구항 52

제51항에 있어서, 상기 공통 클럭 기준은 글로벌 위치 지정 위성 시스템인 것인 모니터링 시스템.

청구항 53

통신 네트워크의 사용자에게 과금하는 방법으로서,
 사용자가 상기 통신 네트워크를 사용한 것에 상응하는 서비스 품질 매트릭스를 결정하는 단계와;
 상기 결정된 서비스 품질에 기초하여 상기 사용자에게 과금하는 단계;
 를 포함하는 과금 방법.

청구항 54

통신 회선상으로 데이터를 전송하는 방법으로서,
 시간을 상기 데이터와 연관시키는 단계와;
 복수의 필드들을 포함하는 패킷을 생성하는 단계로서, 적어도 하나의 필드는 상기 관련 시간에 대응하고, 적어도 하나의 필드는 상기 데이터에 대응하는 것인, 상기 패킷 생성 단계와;
 상기 통신 회선 상으로 상기 패킷을 전송하는 단계;
 를 포함하는 데이터 전송 방법.

청구항 55

통신 회선 상으로 데이터를 전송하는 장치로서,
 상기 데이터에 대응하는 시간 값을 제공하는 클럭과;
 복수의 필드들을 포함하는 패킷을 암호화하는 인코더와;
 상기 통신 회선에 상기 패킷을 제공하는 송신기를 포함하고,
 적어도 하나의 필드는 상기 시간 값에 대응하고, 적어도 하나의 필드는 상기 데이터에 대응하는 것인 데이터 전송 장치.

청구항 56

삭제

청구항 57

삭제

청구항 58

삭제

청구항 59

삭제

청구항 60

삭제

청구항 61

삭제

청구항 62

삭제

청구항 63

삭제

청구항 64

제1 통신 회선상의 데이터를 모니터링하는 시스템으로서,

상기 제1 통신 회선으로부터 제1 데이터를 수신하는 수단과;

상기 제1 데이터를 패킷들로 분리하는 수단과;

복수의 연속적인 제1 시간 주기들의 각각의 주기 동안 수신된 패킷들에 대응하는 통계를 생성하는 수단으로서, 상기 제1 시간 주기들은 제1 지속시간 값을 구비하는 것인, 상기 통계 생성 수단과;

상기 복수의 연속적인 제1 시간 주기들의 각각의 주기 동안 상기 통계를 분리하여 저장하는 수단과;

상기 복수의 저장된 통계들을 모음으로써 추가적인 통계를 생성하는 수단;

을 포함하는 데이터 모니터링 시스템.

청구항 65

제64항에 있어서,

각 패킷의 개별적인 종류에 기초하여 패킷들을 선택하고, 상기 선택된 패킷들을 상기 통계 생성 수단에 제공하는 수단과;

개별적인 인덱스를 각 패킷과 연관시키는 수단과;

각 패킷을 각 패킷의 개별적인 인덱스를 포함하는 개별적인 레코드로 변환하는 수단과;

상기 레코드들을 저장하는 메모리;

를 포함하는 데이터 모니터링 시스템.

청구항 66

제64항에 있어서, 상기 생성된 통계들을 표시하는 표시 장치를 더 포함하는 데이터 모니터링 시스템.

청구항 67

제65항에 있어서, 상기 통계와, 상기 제1 시간 주기 중 적어도 하나를 정의하는 사용자 인터페이스를 더 포함하는 모니터링 시스템.

청구항 68

제65항에 있어서, 절대 시간 소스에 동기되는 시간 소스와; 상기 복수의 패킷들 중 각 개별적인 패킷이 상기 제1 통신 회선으로부터 수신된 시간을 결정하는 수단을 포함하는 모니터링 시스템.

청구항 69

제68항에 있어서, 상기 시간 소스는 글로벌 위치 지정 위성으로부터 시간 신호를 수신하는 수신기인 것인 모니터링 시스템.

청구항 70

삭제

청구항 71

삭제

청구항 72

제1항, 제2항, 제35항, 제36항, 제44항, 제45항, 제53항, 또는 제54항 중 어느 한 항에 있어서의 방법을 실행하기 위하여 기계에 의하여 실행 가능한 명령어들의 프로그램을 갖는 컴퓨터 판독가능한 기록 매체.

청구항 73

삭제

청구항 74

삭제

청구항 75

삭제

청구항 76

삭제

청구항 77

삭제

청구항 78

삭제

청구항 79

통신 회선 상에서 데이터를 처리하는 방법으로서,

- (a) 상기 통신 회선으로부터 상기 데이터를 수신하는 단계와;
 - (b) 상기 데이터를 패킷들로 분리하는 단계와;
 - (c) 통신 세션들에 대응하는 패킷들을 선택하는 단계와;
 - (d) 상기 선택된 패킷들 중 어느 패킷들이 실패한 통신 세션들에 대응하는지 식별하는 단계;
- 를 포함하는 데이터 처리 방법.

청구항 80

제79항에 있어서,

상기 단계 (c)는 TCP 세션들에 대응하는 패킷들을 선택하는 단계를 포함하는 것이고, 상기 단계 (d)는 실패한 TCP 세션들에 대응하는 패킷들을 식별하는 단계를 포함하는 것이고,

상기 데이터 처리 방법은,

- (e) 시간 주기 동안 전체 TCP 세션들의 양과 실패한 TCP 세션들의 양의 비를 생성하는 단계를 더 포함하는 데이터 처리 방법.

청구항 81

제80항에 있어서, 상기 단계 (d)에서 상기 실패한 TCP 세션들은 대응하는 서버를 제외한 서버에 의하여 폐쇄되었던 TCP 세션들로 식별되는 것인 데이터 처리 방법.

청구항 82

제79항의 방법을 실행하기 위하여 기계에 의하여 실행 가능한 명령어들의 프로그램을 갖는 컴퓨터 판독가능한 기록 매체.

청구항 83

제 2 항에 있어서, 상기 복수의 연속적인 제1 시간 주기들은 각 제1 시간 주기보다 긴 지속시간을 갖는 제2 시간 주기 내이며,

복수의 연속적인 제2 시간 주기들 각각의 주기 동안 복수의 연속적인 제1 시간 주기들 각각 동안에 수신된 패킷들에 대응하는 각 통계를 생성하는 단계;

상기 복수의 연속적인 제1 시간 주기들 각각의 주기에 대하여 상기 생성된 통계들을 개별적으로 기억하는 단계; 및

대응하는 제2 시간 주기 동안 수신된 패킷들에 대응하는 상기 복수의 기억된 통계들을 모음으로써 복수의 또다른 통계들 각각을 생성하는 단계

를 포함하는 데이터 모니터링 방법.

명세서

기술분야

<1> 본 발명은 일반적으로 데이터 통신에 관한 것으로, 특히 데이터 통신을 수집, 분석 및 모니터링하는 시스템 및 그와 관련된 방법에 관한 것이다.

배경기술

<2> 본 명세서는 참조를 위해 첨부되고, 1998년 11월 24일에 출원된 미국 특허 가출원 번호 제60/109,718호를 35 U.S.C. § 119하에서 우선권을 주장한다.

<3> 현재, 데이터 및 다른 정보는 통신 또는 데이터 네트워크를 통해 상이한 지점과 통신하도록 경로가 결정된다. 이러한 데이터 네트워크들의 일례는 이러한 네트워크들을 구성하는 여러 경로들을 따라 서로 통신하는 복수의 최종 사용자 컴퓨터(end-user computer)들을 포함한다. 이러한 컴퓨터 네트워크들의 복잡성은 비교적 소수의 기계 중에서의 간단한 피어 투 피어(peer-to-peer) 접속으로부터 LAN, WAN 및 인터넷으로 알려진 글로벌 컴퓨터 네트워크에까지 이를 수 있다. 이러한 네트워크들의 아키텍처는 특정 어플리케이션에 따라 광범위하게 변화하지만, 대부분의 정교한 네트워크들은 이러한 백본, 노드 및 네트워크들 상에서 데이터 및 정보의 전송을 지원하는 컴퓨터 서버들을 이용한다.

<4> 컴퍼니 및 개인은 정보의 송수신뿐만 아니라 상거래 및 정보의 송수신 또는 뷰잉(viewing)을 포함하는 소정의 상상할 수 있는 수의 다른 활동을 위한 이러한 데이터 네트워크들에 더욱 더 의존하고 있다. 인터넷의 출현 및 인터넷의 계속되는 개발은 컴퍼니, 개인 및 이러한 네트워크들의 다른 사용자들 사이에서의 효과적인 통신을 위한 요구를 증가시킬 뿐이다.

<5> 이러한 네트워크들 상에서 데이터를 송수신하기 위한 요구는 소위 "트래픽(traffic)", 즉 볼륨(volume) 또는 네트워크 상에서 적절한 경로를 통과하는 디지털적으로 부호화된 "페이로드(payload)"를 생성시킨다. 불행하게도, 네트워크를 통과하는 트래픽은 흔히 혼잡(congestion) 또는 소정의 지점 또는 네트워크의 소정의 경로들을 따라 "장애 개소(trouble spot)"를 야기한다. 이러한 혼잡은 데이터를 대단히 느리게 전송하는 형태 또는 최악의 경우 이러한 네트워크 상에서 필요한 정보의 송수신을 완전히 무능력하게 하는 형태일 수 있다. 이 문제는 소정의 네트워크 아키텍처하에서 트래픽이 일반적으로 트래픽의 가능 느린 링크 또는 허용되는 경로의 속도만큼만 진행 시킴으로써 타협점에 이른다.

<6> 이러한 트래픽 혼잡이 소정수의 이유로 바람직하지 않다는 것이 명백하다. 이러한 트래픽에서의 사용자들의 "스턱(stuck)"은 그 혼잡을 사용자들의 네트워크 서비스 제공자 탓으로 돌려, 이러한 제공자가 잠재적으로 사업을

상실하게 할 수 있다. 또한, 이러한 네트워크 지연은 네트워크들의 사용자들의 생산성에 간접 및 비간접적으로 부정적인 영향을 미친다.

- <7> 이러한 네트워크 혼잡 또는 다른 네트워크 "장애 해소"를 경감시키기 위한 하나의 해결 방법은 혼잡 또는 장애 해소에 관한 시기 적절하고 정확한 정보를 얻는 것이다. 불행하게도, 컴퓨터 네트워크의 복잡한 사항을 해결하고 혼잡을 경감하기 위한 현행 기술의 시도에는 여러 가지 결점 및 단점이 있다. 예를 들면, 현행 기술의 네트워크 모니터링 툴은 맞춤(customize)에 어려움이 때문에, 네트워크 혼잡 또는 장애 해소를 분석하기 위해 필요한 툴이 부족할 수 있다. 이러한 네트워크 "스니퍼(sniffer)"는 흔히 소정의 특정 프로토콜의 트래픽 덤프(traffic dump)를 실행하기 위해 한정되고, 다시 네트워크 혼잡의 소스를 정확히 설명하거나 또는 정확히 지적하지 못할 수 있다. 바꿔 말하면, 대부분의 네트워크 모니터들 및 현행 기기들의 "스니퍼들"은 실시간 데이터를 도표 작성하거나, 또는 연장된 시간 주기에 걸쳐 데이터를 기록하는 그들의 능력에 한정된다.
- <8> 현행 기술의 네트워크 모니터는 일반적으로 네트워크내로 억지로 개입하여 네트워크 성능을 평가(evaluate) 또는 추정(estimate)하고 있다. 이러한 기술 중 하나가 1994년, 에디슨-웨슬리 출판사(Addison-Wesley Publishing Co.)에서 시판된 참조 문헌인 "TCP/IP illustrated, Volumn I-The Protocols, "7장 및 8장"에 개시되어 있다. 인터넷에 있어서, 정보의 "패킷"에 대한 라운드 트립(Round-trip) 시간을 추정하기 위해서는, 네트워크 모니터는 추가 패킷들을 네트워크내로 삽입하고 이러한 추가 패킷의 이동(travel)을 뒤따른다. 따라서, 네트워크 성능 자체를 결정하는 바로 그 처리는 추가적인 정보의 패킷을 트래픽에 부가함으로써 성능을 더욱 저하시킨다.
- <9> 상기한 방법은 주제넘는 참견일 뿐만 아니라 상기 방법은 일반적으로 부정확하다. 특히, 일방향의 시간은 일반적으로 테스트 패킷의 라운드 트립 지연을 2로 나눔으로써 평가되지만, 라운드 트립 시간의 절반은 일반적으로 네트워크에서의 비대칭(이하에 기술됨)에 일부 기초하여 일방향 지연과 동등하지 않다. 이 부정확성을 보상하기 위해서는 현행 기술의 특정 교시는 테스트 패킷을 네트워크내로 더욱 빈번히 삽입하는데, 이 해결책은 테스트 또는 모니터링되는 네트워크의 성능을 더욱 저하시킬 수 있다.
- <10> 네트워크 성능은 네트워크 트래픽 흐름 또는 네트워크 대역폭 치수가 보다 정확하게 모델링될 수 있으면 더욱 향상될 수 있다. 특히, 트래픽이 소정의 네트워크 경로를 대칭적으로 통과할 필요는 없다. 이것은 특히 경로가 인터넷 접속 상에서 최종 사용자에서 종료하는 경우 틀림없다. 이러한 경로는 최종 사용자가 정상적으로 업로드할 때보다도 페이로드 또는 트래픽을 다운로드할 때 비대칭적이다. 현행 기술의 네트워크 모니터는 일반적으로 이러한 비대칭을 검출 또는 모델링하지 못하며, 그 결과 다른 방법에서 필요로 하는 것 보다 더 많은 네트워크 자원이 특정 루트로 가해진다. 이것은 추가 비용을 들게 하고 컴퓨터 자원을 낭비하게 된다.
- <11> 따라서, 네트워크 성능을 개선하여 네트워크 트래픽 혼잡을 경감시킬 필요가 있다. 트래픽 흐름 상에 억지로 개입하지 않고, 상이한 트래픽 파라미터 또는 "패킷"의 타입을 분석할 수 있으며, 신속하고 정확하게 요구되는 통계를 수집하여 도표 작성하는 툴이 추가로 필요하다.
- <12> 컴퓨터 데이터 네트워크의 사용이 증가함에 따라, 컴퍼니 및 개인은 이러한 네트워크들 상에서 사용자들 또는 사용자들의 트래픽에 관한 데이터의 수집, 필터링 또는 프로파일 작성(profiling)에 점차 흥미를 갖게 되었다. 마케팅 기업 또는 다른 판매 기기들은 특히 인구 통계학 또는 네트워크 트래픽의 정확한 기록 및 분석에 의해 수집될 수 있는 다른 데이터에 매혹될 수 있다. 불행하게도, 많은 인터넷 광고주는 사용자로 하여금 양식(form) 및 앙케이트(questionnaire)에 기입하도록 요구함으로써 고객의 프로필을 얻는다. 광고주는 고객들이 흔히 이러한 질문에 답하는 것에 의해 귀찮아지는 것을 원치 않기 때문에 대부분의 이러한 고객 정보를 얻지 못한다. 따라서, 보다 덜 억지로 개입하는 방법으로 고객의 "프로필"을 얻을 필요가 있다.
- <13> 마찬가지로, 네트워크의 사용을 확장하면, "해커(hacker)" 또는 "특허(propriety) 또는 보호 네트워크에서 해악 또는 심지어 범죄적인 활동을 행하는 다른 해로운 침입자의 가능성도 확장된다. 그렇기 때문에, 보안 위반의 출처를 결정할 수 있는 시스템은 컴퓨터 관련 범죄 및 경범죄의 풍조를 저지하는 FBI와 같은 집행 기관에 매우 유용하다. 다시, 일반적으로, 현행 기술은 보안 활동을 용이하게 하기 위해 최적의 방법으로 네트워크상의 데이터의 흐름을 분석, 도표 작성, 모니터링 또는 기록하는데 부족하다.
- <14> 네트워크를 모니터링해야 할 의무가 있는 컴퍼니 또는 개인은 적시의 방법으로 막대한 양의 정보 및 통계를 얻을 필요가 있을 뿐만 아니라, 또한 이러한 데이터를 신속하고, 용이하게, 이해할 수 있는 포맷으로 뷰잉할 필요가 있다. 다시, 현행 기술의 해결책은 흔히 이러한 데이터의 부정확한 통계학적 컴파일 또는 그래픽 표시로 흔히 연대순으로 "덤프(dump)"를 제공하기 위해 한정된다. 따라서, 네트워크 트래픽 정보를 컴파일할 뿐만 아니라

소정의 통상적으로 요구되는 계산을 실행하고, 사용자에게 친숙하고 다루기 쉬운 포맷으로 이러한 계산을 그래픽으로 나타내는 것이 바람직하다.

<15> 종래의 데이터 통신 모니터링 방법 및 시스템의 단점을 극복하기 위해서는 새로운 통신 회선을 모니터링하는 방법이 제공된다. 본 발명의 목적은 통신 데이터를 수집 및 분석하는 네트워크 모니터를 제공하는 것이다. 본 발명의 또 다른 목적은 통신 데이터를 수집 및 분석하는 방법을 제공하는 것이다.

발명의 상세한 설명

<16> 이들 목적 및 다른 목적들을 달성하기 위해서는, 본 발명의 목적들의 견지에서 본 발명은 제1 통신 회선상의 데이터를 모니터링하는 방법을 제공한다. 데이터는 제1 통신 회선으로부터 수신되고, 복수의 패킷이 그 데이터로부터 추출된다. 그 후, 그 복수의 패킷에 대응하는 통계가 반복적으로 생성된다.

<17> 상기한 일반적인 설명 및 이하의 상세한 설명 양쪽 모두는 예시적인 것이지만 본 발명을 한정하는 것이 아니라는 것이 이해될 것이다.

실시 예

<29> 본 발명은 첨부되는 도면을 참조하여 읽을 때 이하의 상세한 설명이 가장 잘 이해된다. 통상적인 실시예에 따르면, 도면의 여러 특징부가 비율에 따라 그려지지 않았다는 것이 강조된다. 그와 반대로, 여러 특징부의 치수는 명백하게 하기 위해 임의적으로 확대되거나 또는 감소되었다.

<30> 도면을 참조하면, 동일 참조 번호는 도면 전체에서 동일 소자를 칭한다. 도 1은 본 발명에 따른 예시적인 네트워크 모니터(102)를 도시하고 있으며, 이 모니터는 제1 통신 회선(104)을 경유해서 예시적인 네트워크 N1(106)에 결합된다. 네트워크 모니터(102)는 통신 회선(104)상의 데이터 통신(트래픽)을 수신(모니터링)하여 통신 회선(104)상의 실시간 매트릭스(metrics) 또는 통계를 제공한다.

<31> 통신 회선(104)은 복수의 상이한 상위 계층적 프로토콜 계층 프로토콜인 전송 트래픽에 단일 데이터 링크 계층 프로토콜을 사용한다. 도 2에는 이러한 계층적 프로토콜 구조(200)가 도시된다. 네트워크 N1(106) 및 라우터(108)간의 트래픽의 데이터 링크 계층 프로토콜(202), 즉 이 실시예의 경우 이더넷(Ethernet)은 밀폐형 IPX, IP, ARP, 즉 다른 네트워크 계층(204) 트래픽을 포함한다. IP 트래픽은 밀폐형 UDP, TCP, ICMP, 즉 다른 전송 계층(206) 트래픽을 포함한다. TCP 트래픽은 Web, FTP, 도메인 네임 서비스, 즉 다른 어플리케이션 계층(208) 트래픽을 포함한다.

<32> 본 발명에 따른 네트워크 모니터(102)는 하나 또는 복수의 프로토콜 계층의 이러한 트래픽에 관한 다양한 실시간 통계를 생성할 수 있는 방법으로 네트워크 트래픽을 수집하여 분석하는 하드웨어 및 소프트웨어(후술됨)를 포함한다. 네트워크 모니터(102)에 의해 생성되는 실시간 통계는 서비스 분석의 품질 및 양, 서비스 품질 및 서비스의 양에 기초한 과금(billing), 동적 네트워크 자원 할당 및 계획, 데이터 콘텐츠에 기초한 고객 프로필 작성, 네트워크 보안 분석 및 세션 재생을 가능하게 한다. 예시적인 통계는 바이트 카운트, 비트 카운트, 일방향(one-way) 지연 또는 라운드 트립 지연, 응답 시간, 재전송 바이트, 호스트마다의 개시 바이트, 호스트마다의 종료 바이트, 개시-종료 호스트 쌍 카운트, 웹 중단율, 처리율, 굿풋(goodput), 및 지연 또는 손실로 인한 재전송 바이트의 분율을 포함한다. 이러한 통계는 데이터 링크 계층과 어플리케이션 계층간의 하나 또는 복수의 프로토콜 계층에 제1 통신 회선상의 트래픽에 기초하여 선택적으로 제공될 수 있다.

<33> 도 3에 도시되는 예시적인 네트워크 모니터(302)의 동작은 도 4의 흐름도를 참조하여 기술된다. 네트워크 모니터(302)는 제1 접속(312)에 의해 제1 통신 회선(308)에 결합되는 제1 네트워크 인터페이스(304)와 제2 접속(314)에 의해 제2 통신 회선(310)에 결합되는 제2 네트워크 인터페이스(306)를 포함한다. 제1 인터페이스(304)는 제1 통신 회선(308)으로부터 제1 데이터(비트스트림)를 수신하며, 그 비트스트림은 패킷으로 분리된다(단계 404). 본 명세서에서 사용되는 용어인 분리(seggregate)는 이전에 정의된 패킷이 비트스트림으로부터 추출된다는 것을 의미한다. 비트스트림은 인터페이스(304) 또는 호스트 컴퓨터(316)에 의해서 패킷으로 분리될 수 있다. 패킷은 메모리(318)에 저장되며, 이 메모리는 이 실시예에서 계층적이며, 단기(short-term) 메모리(320) 및 적어도 장기(longer-term) 메모리(322)를 포함한다. 프로세서 및 조회 엔진(316)은 사용자 인터페이스(324)에 의해 선택적으로 제어되며, 도 4를 참조하여 후술되는 바와 같이 패킷을 처리한다.

<34> 예시적인 실시예에서는, 네트워크 모니터(302)가 역지로 개입하지 않는 방법으로 제1 통신 회선(308)에 결합된다. 즉, 통신 회선상의 트래픽의 흐름을 직접적으로 역지로 개입하지 않는다. 네트워크 모니터(302)는, 예를 들

면 제1 접속(312)을 스위치 또는 라우터의 포트, 즉 잭에 꽂음으로써 통신 회선(308)을 차단하고, 제1 접속(312)이 결합되는 Y-커넥터를 설치함으로써 광 스플리터를 사용하며, 제1 접속(312)을 허브에 접속함으로써 또는 네트워크 모니터(302)를 중앙국의 모니터링 잭에 접속함으로써 통신 회선(308)에 결합될 수 있다.

<35> 프로세서 및 조회 엔진(316)은 패킷을 레코드로 변환하며, 그 변환된 레코드를 메모리에 저장한다(단계 414 내지 단계 422). 프로세서 및 조회 엔진(316)은 패킷에 대응하는 통계를 생성하는(단계 406 내지 단계 412) 적절한 프로그래밍을 포함한다. 패킷에 대한 통계 생성이 다양한 방법으로 이루어질 수 있지만, 소정의 타임어 구간, 즉 "샘플링 시간" 이외에 수신되는 패킷 세트를 처리하여(단계 406), 그에 대응하는 통계를 생성하는(단계 408) 방법이 바람직하다. 이러한 처리 동안에, 그 생성된 통계는 적절한 프로그래밍에 의해 적당한 시간 주기로 메모리에 저장되며, 이러한 구간은 패킷 세트에 대응하는 시간 주기와 동일한 순서인 것이 바람직하다.

<36> 후술되는 바와 같이, 패킷을 레코드로 변환함으로써 생성되는 통계가 광범위하게 다양해진다. 레코드는 각 패킷의 타입을 우선 결정하고(단계 414), 그 결정된 타입에 기초하여 그 패킷을 필터링함으로써(단계 416) 생성된다. 각 패킷에 관한 인덱스를 생성하고(단계 418), 그 패킷을 인덱싱된 레코드로 변환하여(단계 420), 메모리에 저장한다(단계 422). 다른 통계는 패킷에 관하여 이전에 생성된 통계를 사용하여 생성되며(단계 426), 레코드는 표시 장치와 같은 하나 또는 더 많은 어플리케이션(단계 428)과, 다른 통계에 기초하여 네트워크 루팅을 동적으로 조절하는 라우터(단계 430)와, 그 생성된 통계에 기초하여 결정되는 서비스의 품질 또는 양에 기초하여 클라이언트에게 요금을 부과하는 과금 서비스에 제공된다(단계 432).

<37> 도 4에 도시된 어플리케이션의 처리는 TCP 패킷을 밀폐시키는 밀폐형 IP 패킷을 포함한 이더넷 통신 회선에 관하여 설명되며, TCP 패킷은 웹 트래픽을 밀폐시킨다(도 2 참조). 이더넷 비트스트림은 통신 회선으로부터 수신되어(단계 402) 패킷으로 분리된다(단계 404). 패킷은 세트로 나누어지며, 각각의 세트는 연속적인 1초 시간 주기(예시적인 시간 주기) 중 한 기간 동안에 수신되는(단계 406) 패킷을 포함한다. 각각의 1초 시간 주기(예시적인 통계) 동안에 수신되는 복수의 비트가 계산된다(단계 408). 연속적인 통계는 다음의 1초 시간 주기에 대응하는 다음의 패킷 세트를 수신하여(단계 412) 그 패킷내의 복수의 비트를 계산함으로써(단계 408) 연속적인 시간 주기 동안에 생성된다. 각각의 1초 시간 주기 동안의 비트 카운트는 통계가 생성될 때 메모리에 저장된다(단계 412).

<38> 각 패킷의 타입(예를 들면, IP, ARP, ...)이 결정된다(단계 414). 사용자가 IP 패킷의 트래픽을 분석하기만을 원하는 경우, 패킷은 IP 패킷만을 통과시키도록 필터링된다(단계 416). 네트워크 모니터가 각각의 IP 패킷을 수신하는 시간은 각각의 IP 패킷의 인덱스로서 사용된다(단계 418). 인덱싱된 레코드는 각각의 IP 패킷에 대하여 생성되어(단계 420) 메모리에 저장된다(단계 422). 제1 필드 F1으로서의 인덱스와 제2 필드 F2로서의 패킷을 갖는 예시적인 레코드는 이하에 기술된다.

표 1

<39>	F1:인덱스(수신 시간)	F2: 패킷 또는 패킷의 일부
------	---------------	------------------

<40> 또한, 필터는 IP 패킷만을 통과시키는 필터링(단계 416)에 부가하여, 제2 필드 F2의 IP 부분만을 레코드가 포함하도록 이더넷 오버헤드 부분을 절단함으로써 패킷의 일부만, 예를 들면 IP 부분만을 통과시키는데 사용될 수 있다. 또, 레코드는 각각이 소스 어드레스 또는 목적지 어드레스와 같은 IP 패킷의 일부에 대응하는 복수의 필드를 포함하며, 복수의 필드 중 임의의 하나 이상의 필드에 기초하여 필터링을 실행할 수 있다.

<41> 임의수의 통계는 저장된 레코드로부터만, 즉 단계 406 내지 단계 412에서 생성되는 패킷에 대한 통계와 결합하여 생성될 수 있다. 이 실시예에서, 관련 기술에 알려진 다른 통계는 각각의 연속적인 분(minute)동안에 수신되는 모든 패킷내의 비트수에 대한 수신된 IP 패킷의 비트 갯수의 비율을 포함한다(단계 426). 이러한 통계의 계산은 본 발명에 따르면 용이하게 행해질 수 있다. 그 이유로는, 저장된 패킷이 이미 모든 IP 패킷으로 되어 있고 수신 시간에 의해 인덱싱되기 때문이다. 따라서, 레코드를 인덱스로 분류하고, 각각의 연속 분동안 레코드 세트를 판독하고, 각각의 레코드 세트에 비트수를 부가함으로써 계산이 실행된다. 분당 모든 패킷내의 비트 수는 매 1초를 기초로 하여 60개 그룹(1분과 동일함)에서 생성된 이전에 계산된 비트 카운트를 합함으로써 계산될 수 있다. 따라서, 다른 통계는 저장된 레코드 및 저장된 통계를 사용하여 생성될 수 있으며, 이것에 의해 요구되는 추가 계산의 횟수 및 그러한 다른 통계를 생성하는데 걸리는 시간이 감소된다.

<42> 본 발명에 따른 네트워크 모니터에 의해 실행되는 필터링 및 저장 방법에 관한 특정 실시예는 도 4를 참조하여 상기 기술되었다. 본 발명에 따른 네트워크 모니터(500)의 데이터 수집 및 분석 방법의 유연성은 도 5에 도시된

데이터 흐름도를 참조하여 이하에서 설명된다.

- <43> 입력되는 비트스트림은 패킷타이저(502)에 의해 패킷화된다. 그 비트스트림의 부호화는 알려진 프로토콜에 대하여 자동적으로 실행되거나 또는 사용자 지정 파라미터에 따라 고객, 즉 독점 프로토콜에 대하여 실행될 수 있다. 예를 들면, 새로운 데이터 링크 계층 프로토콜이 도입되는 경우, 네트워크 모니터(500)는 사용자 인터페이스(520)를 사용하여 실행되는 사용자 정의 프로토콜에 응답하는 적절한 프로그래밍을 포함한다. 따라서, 본 발명에 따른 네트워크 모니터(500)는 입력되는 비트스트림을 패킷화하도록 새로운 프로토콜의 패킷 구조를 인식한다. 네트워크 모니터는 상위의 프로토콜 계층을 통하여 데이터 수집 및 분석을 실행할 수 있다. 이러한 유연성은 데이터 링크 계층에 제한되지 않는다. 즉, 본 발명에 따른 네트워크 모니터(500)는 다른 프로토콜 계층에서 고객 프로토콜에 대하여 통신 데이터를 수집 및 분석할 수 있다.
- <44> 패킷은 경로 A를 사용하여 단기 메모리(510)에 직접 저장될 수 있다. 이로 인해 통신 회선으로부터 수신되는 모든 데이터를 저장하기가 유용하다. 단기 메모리(508)는 오버플로우를 방지하기 위해 장기 메모리(510)에 주기적으로 데이터를 전달한다. 단일 단기 메모리(508) 및 단일 장기 메모리(510)만을 가지는 것에 대하여 전술되고 있지만, 본 발명의 교시는 복수의 메모리 장치를 포함한 다른 계층적 메모리에 적용 가능하다. 예를 들면, 메모리는 랜덤 액세스 메모리(RAM), 디스크 메모리 및 테이프 메모리를 포함한다. RAM이 채워진 경우, 데이터는 디스크 메모리로 전달된다. 디스크 메모리가 채워진 경우에는, 데이터는 테이프 메모리로 전달된다. 테이프 메모리가 채워진 경우에는, 테이프는 저장 목적으로, 예를 들면 연속적인 또는 장기 데이터 기억 장치로 교체된다. 메모리(508, 510)간에 양 화살표로 도시되는 바와 같이, 양 메모리에 저장되는 데이터는 분석을 위해 또는 후술되는 어플리케이션(522~530) 중 하나에 대하여 나중에 검색될 수 있다.
- <45> 메모리에 모든 패킷을 직접 저장하는 것은 보안 어플리케이션(528)에 있어서 바람직할 수 있다. 예를 들면, 네트워크 모니터는 1주일 주기로 모든 통신 데이터를 저장하고 가장 오래전에 저장된 데이터를 오버라이트하도록 프로그래밍될 수 있다. 보안 침해가 생성한지 1주일 이내에 검출되는 경우, 저장된 데이터는 침해의 소스 및 범위를 결정하기 위해 네트워크 모니터에 의해 분석될 수 있다.
- <46> 또한, 패킷화된 데이터는 패킷타이저(502)에 의해 인덱스 생성기(504)에 제공될 수 있다. 인덱스 생성기(504)는 하나 이상의 수신된 패킷에 대응하는 인덱스를 생성한다. 패킷에 대응하는 인덱스의 일례는 네트워크 모니터에 의해 수신되는 시간을 나타내는 시간 스탬프(time stamp), 패킷의 타입(프로토콜 및/또는 계층), 패킷의 사이즈, 패킷 번호(1, 2, 3, ...), 인터페이스 번호, 어플리케이션 및 관련 세션을 포함한다. 레코드 생성기(506)는 패킷 및 생성된 인덱스를 수신하여 생성된 인덱스를 포함하는 레코드를 생성한다. 또는, 레코드 생성기(506)는 수신된 패킷과 이전에 메모리(508, 510)에 저장된 기존의 레코드와 결합한다. 또한, 레코드 생성기는 경로 C를 통해 직접적으로 패킷을 수신하여, 그 패킷을 포함하는 인덱싱되지 않은 레코드를 생성하거나 또는 메모리(508, 510)에 저장된 기존의 레코드에 그 패킷을 결합한다.
- <47> 예를 들면, 단일 레코드는 ATM 세션에 대응하여 생성될 수 있다. ATM 세션에 대응하는 제1 셀(고정 사이즈 패킷)이 수신되는 경우, 인덱싱하여 인덱싱된 레코드를 생성하고 그것을 메모리(508, 510)에 저장한다. 인덱스는, 예를 들면 ATM 세션의 식별자일 수 있다. ATM 세션에 대응하는 다른 셀이 반드시 제대로 수신되지 않은 경우, 레코드 생성기(506)는 경로 C를 통해 이러한 셀을 직접 수신하고, 메모리(508, 510)로부터의 이전에 저장된 인덱싱된 레코드를 관독하여, 그 인덱싱된 레코드에 새롭게 수신되는 셀을 결합한다. 통상의 ATM 세션에 속하는 패킷을 단순히 결합하는 것에 부가하여, 레코드 생성기(506)는 정확한 순서로 레코드 내에 수신된 셀을 정렬하기도 한다.
- <48> 레코드/패킷 타입 식별기(512)는 레코드 생성기(506) 또는 메모리(508)로부터 패킷 또는 레코드를 수신하여, 그 수신된 패킷 또는 레코드에 대응하는 "타입" 또는 "특성"을 식별함으로써 특성을 부여한다. 패킷 또는 레코드의 타입 또는 특성은 범용 식별자이고 사용자 인터페이스(520)를 통해 프로그래밍될 수 있다. 패킷 또는 레코드 타입 또는 특성의 일례는 대응하는 비트 또는 바이트 수, 그것의 프로토콜 계층, 특정 프로토콜 계층에서의 프로토콜 타입, 소스 어드레스, 목적지 어드레스, 및 최종 사용자 ID 및 어플리케이션 ID를 포함한다. 레코드 또는 패킷은 레코드/패킷 타입 식별기(512)에 의해 식별되는 특성 또는 타입에 기초하여 패킷 타입 필터(516)에서 필터링된다. 필터링된 레코드 또는 패킷은 인덱싱되고, 인덱싱되어 레코드로 변환되거나 또는 메모리(508, 510)에 직접 저장된다.
- <49> 시간 주기 필터(514)는 레코드 생성기 또는 메모리(508, 510)로부터 레코드 또는 패킷을 수신하여, 그것을 네트워크 모니터에 의해 통신 회선으로부터 수신되는 시간에 기초하여 필터링한다. 레코드 또는 패킷은 각각의 연속적인 시간 주기 동안에 네트워크 모니터에 의해 수신되는 패킷에 대응하는 그룹으로 분리된다. 통계 생성기

(518)는 각각의 연속적인 시간 주기 동안에 수신되는 패킷에 대응하는 각각의 연속적인 시간 주기에 관한 통계를 생성한다.

- <50> 필터링된 패킷 및 생성된 통계는 메모리에 저장될 수 있다. 도 5의 기능 블럭간의 경로는 메모리의 콘텐츠가 다른 필터링 또는 통계 생성을 실행하는데 다시 사용될 수 있다는 것을 나타낸다. 따라서, 본 발명에 따른 네트워크 모니터는 이전에 생성된 통계 또는 저장된 패킷에 기초하여 통계를 생성함으로써 데이터를 반복적으로 수집 및 분석한다.
- <51> 상기한 바와 같이, 고객 프로토콜에 대하여 네트워크 모니터를 프로그래밍하는 것에 부가하여, 사용자 인터페이스(520)는 네트워크 모니터내의 기능 블럭의 동작 파라미터를 정의한다. 예를 들면, 사용자는 인덱스 생성기(504)에 의해 사용되는 인덱스, 시간 주기 필터(514)에 의해 사용되는 시간 주기, 연속적인 시간 주기 각각에 대하여 통계 생성기(518)에 의해 생성되는 통계를 규정한다.
- <52> 네트워크 모니터(500)에 의해 생성되는 수집 데이터 및 이에 대응하는 분석은 하나 이상의 어플리케이션(522~530)에 제공될 수 있다. 예를 들면, 표시 장치(522)는 도 10 내지 도 28의 표시 스크린에 관하여 이하에서 후술되는 사용자 세션에 응답하여 통계, 레코드 또는 패킷을 표시한다.
- <53> 네트워크 모니터(500)에 의해 생성되는 통계는 네트워크 관리자 또는 라우터(524)에 제공되어, 네트워크 성능에 대응하는 통계에 응답하는 네트워크의 "산출 관리(yield management)"로도 알려진 통신 및 네트워크 대역폭 관리의 동적 루팅을 허용한다. 이미 상기한 바와 같이, 한쪽 지연을 측정하고 상이한 프로토콜 계층의 프로토콜마다 트래픽 통계를 제공함으로써, 본 발명에 따른 네트워크 모니터는 네트워크 관리자로 하여금 측정된 흐름에 따라 네트워크 자원의 크기 순으로 적절하게 분류할 수 있도록 트래픽 흐름의 양을 정함으로써 이러한 비대칭을 식별할 수 있다.
- <54> 통신 네트워크는 본 발명에 따른 네트워크 모니터가 임의의 프로토콜 계층의 트래픽 흐름을 분석하기에 적절한 프로그래밍을 포함하기 때문에 서비스 계층에서 최대한으로 활용될 수 있다. 상이한 서비스가 상이한 서비스 요구 조건을 갖지만, 이 서비스는 종종 단일 통신 네트워크에 통합되기도 한다. 그럼에도 불구하고, 실시간 멀티미디어, IP 상의 음성, 데이터 및 인트라넷과 같은 서비스 각각은 고유 네트워크 서비스 요구 조건을 갖는다. 예를 들면, IP 상의 음성에 대하여, 음성 전송 성능 저하의 낮은 허용 한계로 인해 데이터의 지연 또는 손실을 포함한 낮은 서비스 품질은 허용될 수 없다. 역으로, 데이터 전송은 재전송을 통한 에러 복구에 기인하여 손실 환경을 처리할 수 있다. 예시적인 라우터(524)는 서비스 요구 조건에 따른 상이한 서비스에 대응하는 트래픽을 루팅하도록 구성된다.
- <55> 본 발명에 따른 네트워크 모니터는 각각의 서비스 및/또는 사용자에게 대응하는 흐름을 식별하여 상이한 서비스와의 상호 작용 분석을 위해 제공하는 프로그래밍된 특징을 포함한다. 이러한 정보는 라우터에 의해, 예를 들면 최적 네트워크 토폴로지, 루트 또는 서비스 분리 등을 실시간 또는 비(非)실시간 결정하고, 그 자신의 특유의 서비스 품질의 요구 조건에 각기 모든 서비스를 제공하기에 적절한 최적의 구성을 이루는데 사용될 수 있다.
- <56> 과금(billing) 시스템(526)은 상이한 서비스 및 상이한 호스트에 대응하는 서비스 통계의 품질 및/또는 양을 수신하여 그에 따라 클라이언트에게 요금을 부과하도록 구성될 수 있다. 이로 인해 이전에 측정되지 않은 서비스에 대하여 균일 비율의 과금(flat rate billing)을 제공하기 보다는 상기 통계에 기초하여 클라이언트에게 요금을 부과할 수 있다. 예를 들면, 클라이언트는 IP 통신상의 음성에 대하여 무한 인터넷 서비스를 사용할 수 있다. 본 발명에 따르면, 네트워크 모니터(500)는 IP 호출상의 음성의 갯수, 지속 기간 및 목적지에 대하여 특정 클라이언트에 대한 통계를 생성할 수 있다. 통계는 과금 시스템(526)에 의해 과금 정보로 변환되고, 그에 따라 클라이언트에게 요금을 부과한다. 따라서, IP 호출상의 음성에 인터넷을 사용하는 인터넷 가입자에게는 비인터넷(non-internet) 전화 서비스를 위해 행해지는 호출의 양, 지속 기간 및 목적지에 따라 요금이 부과될 수 있다. 동일하게는, 전자 상거래 처리 횟수, 증권 거래(stock trades) 횟수, 실시간 증권 쿼트(stock quotes)에 대한 요구 횟수 및 다른 처리 횟수에 기초하여 클라이언트에게 요금이 부과될 수 있다. 또는, 클라이언트는 제공되는 서비스의 양에 따른 상이한 부과 요금을 포함한 서비스 계약을 하며, 그에 따라 클라이언트에게 요금이 부과된다. 또한, 네트워크 모니터는 최소 서비스 표준 또는 서비스 레벨 계약을 보증하는 서비스 계약에 순응하도록 사용될 수 있다.
- <57> 상기한 바와 같이, 수집된 데이터는 보안 어플리케이션(528)이 보안 침해를 식별하고, 부적절한 네트워크 사용 또는 불법 활동을 식별하는데 사용될 수 있다. 예를 들면, 패킷은 서버에 파일 전송된 특정 파일을 식별하고, 누가 특정 기계 또는 서버에 텔넷[TELNET: TELEcommunication NETwork] 접속되었는지를 식별하고, 일단 접속되

면 타입핑된 것을 볼수 있도록 필터링될 수 있다.

- <58> 네트워크 모니터로부터의 통계는 사용자 또는 사용자 그룹의 프로필을 작성할 수 있도록 사용자 또는 사용자 그룹에 대응되어야 한다. 인터넷 광고는 사용자에게 새로운 질의에 대한 답변을 요구함으로써 생성되는 고객 프로필에 기초하여 고객에게 전송된다. 본 발명에 따른 네트워크 모니터는 각 고객 프로필을 작성하도록 그 콘텐츠에 기초하여 각각의 수신된 패킷을 필터링한다. 예를 들면, 필라델피아 고객을 모니터링하는 노드는 인터넷에 접속하기 전에 모든 사용자로부터의 모든 패킷을 조사한다. 또한, 사용자에게 되돌아온 트래픽은 패킷내의 특정 텍스트 또는 사용자가 방문한 웹 사이트를 조사(필터링)함으로써 분석될 수 있다. 사용자 또는 사용자마다의 프로필은 그 필터링된 데이터에 기초하여 사용자에 관련된 사용자의 타겟 콘텐츠, 예를 들면 타겟 이메일로 생성될 수 있다. 상기한 필터링 방법은 불법 활동을 검출하거나 또는 선택된 사용자의 활동을 모니터링하기 위해 통신을 모니터링하도록 법 시행 기관 또는 보안국에 의해 동일하게 사용될 수 있다.
- <59> 또한, 네트워크 모니터는 재생 장치(530)에 데이터를 제공하여 통신 회선으로부터 모니터링되는 클라이언트 세션을 재생하는데 사용될 수도 있다. 모든 수신 패킷은 기록되며 특정 세션에 기초하여 필터링될 수 있다. 세션은 그것들 자신의 패킷에 포함되는 정보 또는 SDR(sessions directory protocol)과 같은 특정 패킷 또는 채널에 수신되는 세션 정보에 기초하여 식별될 수 있다. 세션에 대응하는 패킷은 사용자에게 처음에 나타났던 형태로 재생될 수 있다.
- <60> 네트워크 모니터는 독점 또는 고객 프로토콜을 사용하여 트래픽을 전송하는 통신 회선을 모니터링하도록 사용자에게 의해 구성될 수 있다. 네트워크 모니터와 통신 회선간의 적절한 물리 계층 인터페이스에 따라서 사용자는 사용자 인터페이스를 사용하여 독점 프로토콜 파라미터를 처리한다. 파라미터는 비트스트림으로부터 패킷을 분리하도록 네트워크 모니터에 대하여 통신 회선 상에 전송되는 비트스트림내의 패킷의 구조를 정의한다. 또한, 추가 파라미터는 네트워크 모니터가 그 패킷 필드의 콘텐츠에 기초한 통계를 제공하기 위해 고객 질의로 구성될 수 있도록 패킷내의 필드를 정의하기도 한다. 동일하게는, 네트워크 모니터는 링크 계층보다 더 높은 상위층의 고객 프로토콜에 대응하여 데이터를 수신하여 분석하도록 프로그래밍될 수 있다.
- <61> 예시적인 네트워크에서, 데이터 전송 프로토콜은 시간 스탬프 필드를 포함하도록 각각의 패킷에 대하여 제공한다. 소스에서 목적지로 전송되는 패킷은 소스에 의한 전송 시간을 나타내는 시간 스탬프 필드의 시간 스탬프 값을 포함한다. 패킷이 목적지로 수신되는 경우, 목적지에서는 현재 시간 값에서 시간 스탬프 값을 감산함으로써 소스에서 목적지까지의 일방향 전송 지속 기간 또는 지연을 계산할 수 있다. 이 프로토콜은 분리 네트워크 모니터의 패킷 쌍을 일치시키기 위해 네트워크 모니터간의 통신 요구를 제거함으로써 보다 단순한 일방향 전송 지연 및 서비스 품질 측정을 허용한다.
- <62> 소스와 목적지간의 복수의 분리 중간 전송 경로를 포함한 네트워크에 있어서, 한 쪽의 중단간 전송 지속 기간 정보는 소스와 목적지 사이에서 병목 현상이 일어나는 특정 지점에 관련된 정보를 제공하지 않는다. 개선된 병목 현상 진단을 위하여, 본 발명에 따른 네트워크 모니터는 중단간 지연을 계산하기 보다는 소스와 목적지 사이에서 중간 분리 전송 경로 중 하나의 경로에 결합될 수 있다. 네트워크 모니터는 네트워크를 통과하는 패킷으로부터의 시간 스탬프 값을 소스에서 목적지로 수신할 수 있다. 시간 스탬프 값은 중간 지속 기간 값을 결정하기 위해 네트워크 모니터에 의한 패킷의 수신 시간의 현재 시간에 대하여 감산될 수 있다. 중간에 이격되어 있는 하나 이상의 모니터는 상기한 바와 같이 네트워크의 병목 지점을 알아내는데 사용될 수 있다. 예시적인 실시예에서, 각각의 소스, 목적지 및 네트워크 모니터는 전송 지속 기간을 계산하는데 사용되는 현재 시간을 수신하기 위해 GPS(global positioning satellite) 인터페이스를 포함한다.
- <63> 본 발명에 따른 네트워크 모니터가 제공할 수 있는 매트릭스 중 하나는 특정 소스-목적지 쌍, 특정 소스 또는 목적지의 중단된 접속의 갯수와, 특정 소스 또는 목적지의 총 접속에 대한 중단된 접속의 정량에 관한 정보의 지시(indication)이다. 장애를 겪는 TCP(transmission control protocol) 서버를 식별하는 예시적인 방법은 도 6의 흐름도(600)를 참조하여 설명된다.
- <64> 당업자에게 알려진 바와 같이, 서버가 클라이언트에게 전송할 데이터가 없는 경우, TCP 세션은 서버에 의해 폐쇄된다. TCP 세션이 클라이언트에 의해 폐쇄되는 경우, 이것은 세션이 영구적으로 중단되는 것을 나타낸다. 일례로서 웹을 사용하는 경우, 클라이언트(브라우저를 사용하는 사용자)는 단순히 소망하는 데이터에 대한 요구에 관한 클라이언트가 생각이 바뀌었다는 이유로 또는 소망하는 데이터를 수신할 때 지연에 기인한 클라이언트의 성급함으로 인해 세션을 폐쇄할 수 있다.
- <65> 네트워크 모니터는 통신 회선으로부터 패킷을 수신하여(단계 602), 그 패킷이 TCP 세션에 속하는지를 식별한다

(단계 604). 네트워크 모니터는 패킷내의 프로토콜 필드를 식별하여 복호화함으로써 그 패킷이 TCP 패킷인지의 여부를 식별하고, 수 개의 전송 계층 프로토콜 중 어느 하나에 패킷이 속하는지를 식별할 수 있다. 일단 패킷이 TCP로서 식별되면, TCP 클라이언트 및 TCP 서버가 식별된다(단계 606). 패킷을 검사하여 개방되어 있는지 또는 TCP 접속을 초기화했는지를 결정한다(단계 608). 패킷이 개방되어 있거나 또는 TCP 세션의 패킷을 초기화한 경우, 이전에 식별된(단계 608) TCP 서버에 대한 TCP 세션의 총 갯수의 카운트가 증가된다(단계 610).

- <66> 패킷이 개방 패킷인 경우, 네트워크 모니터는 그 패킷이 TCP 접속을 폐쇄하였는지를 다음에 결정한다(단계 612). 패킷이 개방 패킷이 아닌 경우에는 네트워크 모니터는 다음 패킷을 얻는다(단계 602). 그렇지 않으면, 네트워크 모니터는, 예를 들면 FIN 비트를 검사함으로써 서버에 의해 접속이 폐쇄되었는지를 결정하거나(단계 614) 또는 클라이언트에 의해 접속이 폐쇄되었는지를 결정한다. 서버에 의한 폐쇄는 세션의 정상 종료를 나타내고, 네트워크 모니터는 다음의 패킷을 얻는다(단계 602). 서버 이외의 다른 것에 의한 폐쇄는 세션의 영구 종료를 나타내며, 특정 서버에 대응하는 영구 폐쇄 카운트가 증가된다(단계 616). 특정 서버의 총 TCP 세션에 대한 영구 폐쇄의 비율을 계산하여(단계 620), 소정의 임계 값과 비교한다(단계 622). 영구 폐쇄의 비율이 소정의 임계 값을 초과하는 경우, 특정 서버는 "장애 서버"로서 식별된다(단계 624).
- <67> 당업자에게 알려진 바와 같이, 어떤 네트워크에서 특정 TCP 세션에 대응하는 모든 패킷은 동일 통신 회선을 통과하지 않고, 이에 따라서 단일 네트워크 모니터 인터페이스에 의해 검출될 수 없다. 네트워크 모니터는 서버 또는 클라이언트에 근접하게 또는 그 서버상에 배치되어 모든 패킷을 "캐치(catch)"한다. 또는, 복수의 네트워크 모니터 인터페이스는 상기한 바와 같이 패킷에 대응하는 레코드를 저장하는데 사용된다. 저장된 레코드를 분석하여 서버가 "장애를 겪고"있는지의 여부를 결정한다. 예시적인 실시예에서, 원격 네트워크 모니터는, 예를 들면 필터를 사용하여 FIN 패킷을 각각 조사하고, FIN 패킷을 검출하였을 때 FIN 패킷의 콘텐츠를 포함한 메시지를 중앙 모니터로 전송되고, 중앙 모니터는 "장애 서버" 결정을 행한다.
- <68> 중단 접속을 측정하여 장애 서버를 식별하는 것에 관한 교시가 TCP 세션에 관하여 상기 기술되었지만, 이러한 교시는 통상 다른 프로토콜 및 다른 프로토콜 계층에 적용 가능하며, 장애를 겪는 TCP 서버를 식별하는 것에 한정되지 않는다. 예를 들면, 또다른 프로토콜에서 세션은 클라이언트인 서버이든지 간에 동일 노드에 의해 개방 및 폐쇄될 수 있다. 또한, 세션 페이로드는 세션 제어 메시지에 의거하여 분리 통신 링크로부터의 분리 패킷 또는 분리 통신 링크상의 분리 패킷으로 전송될 수 있다.
- <69> 도 7에 도시된 또 다른 실시예에서, 본 발명에 따라 통신을 모니터링하는 시스템(710)은 도 7에 도시된 바와 같이 네트워크내의 각각의 통신 회선에 각각 결합되는 하나 이상의 네트워크 모니터를 포함한다. 제1, 제2 및 제3 네트워크 모니터(700, 710 및 720)는 제1, 제2 및 제3 통신 회선(702, 712 및 722)에 각각 결합된다. 각각의 네트워크 모니터(700, 710 및 720)는 도 5에 도시된 데이터 흐름도에 관하여 상기한 바와 같이 각각의 통신 회선으로부터 수신되는 데이터를 수집하여 분석한다.
- <70> 독립적인 데이터 수집 및 분석을 제공하는 것에 부가하여, 복수의 네트워크 모니터(700, 710 및 720)를 포함하는 시스템은 개선된 네트워크 성능 분석을 제공하기 위해 다른 네트워크 모니터에서 수신된 데이터들을 상호 관련시킨다. 예를 들면, 일방향 지연은 제1 통신 회선(702)으로부터 제2 통신 회선(712)으로 통과하는 데이터에 대하여 계산된다.
- <71> 일방향 지연을 계산하는 예시적인 방법은 도 8에 도시된 흐름도에 의해 기술된다. 통상적으로, "동일" 패킷은 두 개의 분리 네트워크 모니터에서 식별되며, 패킷이 각각의 모니터에 의해 수신되는 시간의 차는 일방향 지연을 계산하는데 사용된다. "동일" 패킷은 분리 네트워크 모니터 사이에서 변화하는 패킷의 일부를 제로화함으로써 식별된다.
- <72> 각각의 제1 및 제2 네트워크 모니터(700, 710)는 각각의 통신 회선(702, 712)로부터 데이터를 수신한다(단계 802 및 단계 806). 패킷타이저(502)는 수신된 데이터를 패킷으로 분리하고(단계 803 및 단계 807), 각자의 인덱스 생성기(504)는 각 패킷의 수신 시간(시간 스탬프)과 각 패킷을 상호 관련시킨다. 레코드 생성기(506)는 각 패킷에 대응하는 시간 스탬프와 데이터 패킷의 고유 부분(UDP)을 포함한 레코드를 생성하여, 그 레코드를 메모리(508, 510)에 저장한다(단계 804 및 단계 808).
- <73> UDP는 데이터 유닛을 특유하게 식별할 수 있는 수신된 패킷의 일부이다. 예를 들면, 이더넷 통신 회선 및 IP 페이로드에 있어서, 이더넷 헤더는 그 패킷으로부터 제거되고, IP ttl 및 체크섬 필드는 제로로 되며, IP 헤더 및 20개의 연속 바이트는 저장되고, 레코드 생성기(506)에 의해 UDP 레코드에 통합된다. UDP는 상이한 프로토콜에 대하여 상이하며 사용자 인터페이스를 사용하여 프로그래밍될 수 있다.

- <74> 제1 네트워크 모니터(700)의 UDPD 레코드는 제2 네트워크 모니터(710)의 레코드와 비교하여 UDPD의 쌍을 일치시킨다(단계 810). 제1 및 제2 네트워크 모니터는 통신 링크(730)를 통해 통신할 수 있다. 통신 링크(730)는 모니터링되는 네트워크를 통한 네트워크 모니터의 통신(대역 내의 통신)에 의해 실시될 수 있다. 또는, 통신 링크(730)는, 예를 들면 전화선, 무선 접속 또는 위성 접속에 의한 네트워크 밖의 통신(대역 밖의 통신)에 의해 실시될 수도 있다.
- <75> 각각의 일치되는 UDPD의 쌍에 대하여, 제2 네트워크 모니터로부터의 대응하는 시간 스탬프 ts2는 제1 네트워크 모니터로부터의 대응하는 시간 스탬프 ts1에서 감산된다. 이 시간 차(ts1-ts2)는 제2 네트워크 모니터(710)에서 제1 네트워크 모니터(700)로 통과하는 UDPD에 대응하는 데이터의 지속 기간을 나타낸다. UDPD를 계산함으로써 동일 또는 다른 통신 프로토콜을 사용하는 제1 및 제2 통신 회선(702, 712)간의 임의의 페이로드의 전송 지속 기간은 상기한 방법에 따라 결정될 수 있다.
- <76> 예시적인 실시예에서, 시간 차(ts1-ts2)는 제1 통신 회선(702)의 지연을 고려하도록 정규화된다(단계 814 및 단계 816). 지연은 수학적 1로 나타나는 바와 같이 제1 통신 회선을 통과하는 UDPD에 대응하는 패킷의 지연 xmit-delay를 시간 차에서 감산함으로써 정규화된다.

수학식 1

정규화된 네트워크 지연=(ts1-ts2)-(링크 속도/패킷 길이)

- <77>
- <78> 여기서, 링크 속도는 제1 통신 회선(712)의 전송 속도이고, 패킷 길이는 UDPD를 포함하는 제1 통신 회선상의 패킷 길이이다. 계산된 네트워크 지연은 대기 지연 및 전송 지연에 기인하는 구성 성분을 포함한다. 도 5에 도시된 데이터 흐름도에 의해 도시되는 바와 같이, 통계 생성기(518)는 생성되는 UDPD 레코드인 패킷을 수신하고, 그 패킷내의 비트의 갯수를 계산하여 정규 계산을 위한 UDPD 레코드에 통합하기 위해 이 통계를 레코드 생성기에 제공한다. 라운드 트립 시간은 제1 네트워크 모니터로부터 제2 네트워크 모니터로의 지연을 동일하게 계산하고, 이 지연에 제2 네트워크 모니터로부터 제1 네트워크 모니터로의 지연을 부가함으로써 추정될 수 있다.
- <79> 계산된 전송 지연의 정확도는 제1 및 제2 네트워크 모니터(700, 710)의 시간 클럭의 동기에 의존한다. 네트워크 모니터는 각 클럭에 동기하도록 통신 회선(730)을 통해 통신한다. 예시적인 실시예에서, 네트워크 모니터는 통상의 시간 소스(740)로부터 시간 신호를 수신함으로써 동기된다. 예시적인 실시예에서, 시간 지연은 10마이크로초 보다 작은 정확도 레벨로 생성된다. 즉, 계산된 지연과 실제 지연간의 차는 10마이크로초보다 작다. 바람직한 실시예에서, 통상의 시간 소스(740)는 글로벌 위치 지정 위성(GPS)과 같은 글로벌 위성의 시스템이고, 각 네트워크 모니터(700, 710)는 하나 이상의 글로벌 위치 지정 위성으로부터 시간 신호를 수신하기 위한 수신기를 포함한다. 모니터링되는 두 개의 통신 회선이 상호 근접해 있는 경우, 제1 및 제2 네트워크 모니터(700, 710) 중 하나는 마스터 GPS 수신기를 포함하며, 나머지는 그 마스터 GPS 수신기에 결합되는 슬레이브 GPS 수신기를 포함한다.
- <80> 예시적인 네트워크 모니터는 모니터링되는 통신 회선에 결합되는 네트워크 인터페이스 카드(NIC) 상에 인터페이스 컴퓨터를 구비하는 호스트 컴퓨터와 함께 실시된다. 상기한 바와 같이, NIC에 의해 수신되는 데이터는 호스트 컴퓨터로 전송되기 전에 처리될 수 있다. 또한, 상기한 바와 같이, 네트워크 모니터는 통신 회선으로부터 데이터를 수신하는 시간을 이용하여 네트워크 통신 통계 또는 매트릭스를 생성한다. 데이터가 통신 회선으로부터 수신되는 시간을 정확하게 기록하기 위해, 인터페이스 컴퓨터는 그 데이터와 수신 시간(시간 스탬프)을 상호 관련시킨다. 호스트 컴퓨터 보다는 인터페이스 컴퓨터를 구비함으로써 인터페이스 컴퓨터로부터 데이터를 전송하는 경우 지연으로 인한 수신 시간의 부정확도는 감소 또는 제거된다.
- <81> 예시적인 실시예에서, 인터페이스 컴퓨터는 인터페이스 클럭을 포함하고, 호스트 컴퓨터는 호스트 클럭을 갖는다. 호스트 클럭 및 인터페이스 클럭은 호스트 컴퓨터로 하여금 시간 스탬프를 이용하여 수신된 데이터에 대응하는 통계를 정확하게 생성시키게 동기된다. 예시적인 실시예에서, 인터페이스 클럭은 카운터로서 실시된다. 각 패킷이 통신 회선으로부터 수신되는 경우, 그 수신된 패킷을 카운터의 현재 값과 상호 관련시킨다. 그 패킷은 카운터 값을 갖는 호스트 컴퓨터에 나중에 전송된다. 호스트 컴퓨터는 절대 시간 기준과 동기되는 호스트 클럭을 포함한다. 상기한 바와 같이, 절대 시간 기준은 글로벌 위치 지정 위성에 의해 제공될 수 있다.
- <82> 호스트 클럭 및 인터페이스 클럭은 인터페이스 컴퓨터에 의해 각 패킷에 관련된 카운터 값을 절대 시간 기준과 상호 관련시킴으로써 동기된다. 인터페이스 클럭과 호스트 클럭을 동기시키는 방법은 호스트 컴퓨터 및 인터페이스 컴퓨터 각각에 대하여 도 9a 및 도 9b의 흐름도를 참조하여 기술된다. 통상적으로, 호스트 컴퓨터는 인터

페이스 컴퓨터로부터 인터페이스 클럭 카운터의 값을 주기적으로 요구하고 그 인터페이스 클럭 카운터의 값을 이용하여 호스트 클럭과 그 카운터를 상호 관련시킨다.

<83> 도 9a 및 도 9b를 참조하여, 호스트 컴퓨터가 인터페이스 컴퓨터로부터 패킷 세트를 수신하는 경우(단계 902), 호스트 컴퓨터는 인터페이스 컴퓨터에 "카운터 읽기(get counter)" 메시지를 전송함으로써 인터페이스 컴퓨터로부터 카운터 값을 요구(단계 906)하기 시작한다. 예시적인 실시예에서, 인터페이스 컴퓨터는 메모리 직접 접근(DMA) 동작에 의해 호스트 컴퓨터의 메모리에 패킷 세트를 저장하고, 그 호스트 컴퓨터를 인터럽트하여 패킷 전송을 지시하게 한다. 호스트 컴퓨터가 패킷 세트를 수신하지 않은 경우, 호스트 컴퓨터는 카운터 값을 요구한(단계 906) 후에 타임아웃 기간동안 패킷을 대기한다(단계 904). 호스트 컴퓨터는 인터페이스 카운터 값을 요구한 경우 호스트 클럭 시간을 기록한다(단계 906).

<84> 인터페이스 컴퓨터가 호스트 컴퓨터로부터 "카운터 읽기" 메시지를 수신한 경우, 인터페이스 컴퓨터는 현재 휴지 상태(idle)인지 또는 통신 회선으로부터 데이터를 수신하고 있는지를 결정한다(단계 922). 휴지 상태가 아닌 경우, 인터페이스 컴퓨터는 호스트 컴퓨터에 "다시 시도(try again)" 메시지를 전송한다(단계 924). 휴지 상태인 경우에는, 인터페이스 컴퓨터는 카운터 값을 판독하고, 그 판독된 카운터 값에서 미리 계산된 인터럽트 서비스 시간을 감산하여 조정 카운터 값을 생성한다. 인터페이스 컴퓨터는 그 조정 카운터 값을 호스트 컴퓨터로 전송한다(단계 928).

<85> 미리 계산된 인터럽트 서비스 시간은 인터페이스 컴퓨터가 호스트로부터 카운터 요구를 수신했을 때로부터 인터페이스 컴퓨터가 그 조정 카운터 값을 호스트 컴퓨터에 제공할 때까지의 시간의 지속 기간에 해당한다. 미리 계산된 인터럽트 서비스 시간은, 예를 들면 인터페이스가 카운터에 대한 요구를 수신하였을 때로부터 인터페이스가 카운터 값을 제공할 때까지의 시간의 지속 기간을 측정하기 위해, 로직 분석기를 사용하여 실험적으로 결정될 수 있다. 실험상의 지연 측정을 정상 동작동안의 지연에 일치시키기 위해 인터페이스가 휴지 상태에 있는 것으로 식별되는 경우 실험상의 요구가 인터페이스에 제공되며, 인터페이스는 휴지 상태에 있는 경우 정상 동작동안의 요구만을 처리한다. 당업자에게 알려진 바와 같이, 인터페이스 컴퓨터의 응답 시간은 동작 동안의 평균 서비스 사용 시간을 생성하도록 반복적으로 취해질 수 있다.

<86> 카운터 값이 수신된 경우 호스트 컴퓨터는 호스트 컴퓨터 클럭에 대한 인터페이스 클럭 카운터의 상대 도수의 추정을 계산한다(단계 912). 상대 도수는 동기 루틴의 다음 실행때까지 인터페이스 컴퓨터로부터 수신되는 패킷과 관련된 카운터 값을 상호 관련시키는데 사용될 수 있다. 예시적인 실시예에서, 호스트 컴퓨터는, 호스트 컴퓨터가 인터페이스로부터 카운트를 수신하였을 때로부터 호스트 컴퓨터가 상대 도수를 계산할 때까지의 지연을 고려하기 위해 상대 도수를 계산하기 전에 단계 906에서 기록된 시간에서 호스트 인터럽트 서비스 시간을 감산한다.

<87> 예시적인 실시예에서, 각각이 각각의 통신 회선에 결합되는 복수의 네트워크 인터페이스는 단일 유닛으로서 실행되며, 공통 클럭을 공유한다. 따라서, 공통 클럭과만의 동기는 호스트 클럭을 각각의 통신 회선 중 임의의 선로부터 수신된 데이터와 관련된 시간 스탬프와 동기시킨다.

<88> 도 10 내지 도 28은 네트워크 모니터에 의해 수집 및 분석되는 데이터를 표시하고 본 발명에 따른 네트워크 모니터에 의한 데이터 분석을 제어하는 그래픽 사용자 인터페이스(GUI)를 나타내는 예시적인 스크린 표시이다. 도 10에 도시된 표시는 테이블 프레임(1010), 제1 프레임(1030), 버튼 프레임(1050)을 포함한다. 테이블 프레임(1010)은 사용자 선택용으로 선택 가능한 박스 및 텍스트 입력 박스를 갖는 제1 부분(1011)과, 수신 데이터에 대응하는 통계 테이블을 갖는 제2 부분(1012)을 포함한다. 선택 가능한 버튼, 박스 및 필드 아래에 나타나는 테이블(1023)은 분석되는 특정 데이터에 대응하는 엔트리를 포함한다. 플롯 프레임(1030)은 수신 데이터에 대응하는 통계를 나타내는 플롯(1032, 1034)을 포함한다. 버튼 프레임(1050)은 사용자 구성 가능한 버튼 세트를 포함한다.

<89> 테이블 프레임(1010)의 제1 부분(1011)의 텍스트 입력 박스는 고정되어 있어, 옵션의 사용자 선택을 방지하고 텍스트 박스로의 사용자 입력을 방지한다. 도 10에서 표시되는 옵션 및 박스와 관련된 기능은 이하에 기술된다.

<90> 1. 스타트: 개시 필드(1013)는 트래픽이 분석되어 그 분석 결과가 GUI에 표시되는 개시 시간을 나타낸다.

<91> 2. 정지: 정지 필드(1014)는 트래픽이 분석되어, 그 분석 결과가 GUI에 디스플레이되는 종료 시간을 나타낸다. 따라서, 개시/정지 필드(1013, 1014)는 트래픽이 분석되어 GUI를 통해 사용자에게 제공되는 시간을 나타낸다. 개시 및 정지 필드(1013, 1014)의 콘텐츠는 복수의 형식으로 표시될 수 있다. 예를 들면, 콘텐츠는 도 10에서 데이터 형식으로 도시된다. 또는, 콘텐츠는 현재 시간에 상대적인 시간을 나타내는 +/- 시간으로서 표시될 수 있다.

으며, 용어 "현재(NOW)"는 현재 시간을 나타내는데 사용되고, 용어 "네버(NEVER)"는 데이터가 연속적으로 갱신되어야 하는 것을 나타내는데 사용될 수 있다.

- <92> 3. 윈도우: 윈도우 필드(1015)는 제2 프레임(1030)에 플롯팅되는 값을 계산하는 시간 주기를 나타낸다. 예를 들면, 사용자가 윈도우 필드로 "1"을 입력하면, 플롯 필드의 값은 매초마다 플롯팅된다. 사용자는 그 값을 플롯의 분해능을 나타내기 위해 적절한 단위를 사용하여 윈도우 필드에 입력할 수 있다(예컨대, 수평 눈금의 단위가 시간인 경우 시간 분해능을 나타내는 1s, 1ms, 100 μ s, ...). 빈 윈도우 필드(1015)는 수평 눈금의 분해능이 자동적으로 설정되어야 함을 나타낸다.
- <93> 4. 톱(Top) N: 톱 N(1016)은 테이블 프레임(1010)의 제2 부분(1012)에 나타나는 테이블(1023)에 대한 최대 갯수의 엔트리를 나타낸다. 톱 N이 10인 경우, 테이블(1023)은 내림차순으로 특정 컬럼 값에 의해 소트되는 10개의 로우를 포함한다. 톱 N이 -10인 경우에는, 테이블(1023)은 올림차순으로 특정 컬럼 값에 의해 소트되는 10개의 로우를 포함한다(즉, 이것은 보텀 N의 개념이다).
- <94> 5. 필터: 필터 윈도우(1017)는 표시될 데이터에 적용되는 필터를 기술한다. 예를 들면, 필터는 링크 계층 프로토콜 IEEE802.3에 따라 패킷의 결과를 표시하는 "프로토콜 IEEE802.3"일 수 있다. IP 트래픽만을 나타내도록 이전에 필터링된 데이터에 대하여, 호스트 10.0.0.1의 필터는 호스트가 10.0.0.1인 소스 또는 목적지에 IP 트래픽의 결과를 표시한다. 또한, 여러가지의 복잡한 필터도 가능하다.
- <95> 6. Do DNS: Do DNS 체크박스(1018)는 테이블(1023)의 엔트리를 수치 표시로부터 텍스트 표시로 변환한다. 예를 들면, IP에서 수치 표시(IP 어드레스)는 호스트를 식별하는데 사용된다. DNS(Domain Name Sever)는 IP 어드레스의 수치 표시로부터 텍스트 표시로의 매핑을 포함한다. 예를 들면, IP 어드레스 10.0.0.1은 텍스트 표시 foo.niksun.com으로 변환된다. DNS 이외의 프로토콜에 대하여, 체크박스에 주어지는 라벨은 등가 함수에 따라 변화한다.
- <96> 7. 도움말: 선택되는 각 필드 다음에 오는 도움말 버튼(1019)은 문맥 의존 도움말을 표시한다. 예를 들면, 필터(1017) 다음에 오는 도움말 버튼이 선택되는 경우, 필터에 대한 도움말 윈도우가 팝업(pop up)된다.
- <97> 8. 재생: 재생 버튼(1020)은 모든 프레임의 콘텐츠를 재생한다.
- <98> 9. 전진 및 후진 버튼: 테이블 프레임(1010)의 제1 부분(1011)에서 전진(1021) 및 후진(1022) 버튼은 배열된 모든 프레임의 콘텐츠를 유지하는 추가 특징을 갖는 브라우저의 "전진" 및 "후진" 버튼과 동일한 기능을 한다. 대조적으로, 브라우저의 "전진" 및 "후진" 버튼을 클릭하면, 프레임 단위로 전방 및 후방으로 이동하여, 여러 프레임간의 대응 관계를 느슨하게 한다.
- <99> 플롯 프레임(1030)은 플롯(1032, 1034), 텍스트 입력 박스 및 선택 가능한 박스 및 버튼을 포함한다. 텍스트 박스 및 선택 가능한 박스는 임의적으로 고정되어 있어, 옵션의 사용자 선택을 방지하고 텍스트 박스내의 사용자 입력을 방지한다. 도 10에 도시된 플롯 프레임(1030)에 표시되는 박스 및 옵션과 관련된 기능은 이하에 기술된다.
- <100> 1. 갱신 테이블 및 플롯: 이 버튼(1036)은 통합 방식으로 테이블 및 프레임을 갱신한다. 예를 들면, 사용자는 마우스로 플롯의 일부를 선택함으로써 줌인하는 경우, 이 버튼을 클릭하면 그 플롯 및 테이블을 줌인되는 선택된 시간 범위 동안에 갱신한다.
- <101> 2. 바이트/패킷 카운트[및 비트/패킷 비율: 및 사용율]: 이 버튼(1037)은 선택시에 3개의 옵션("바이트/패킷 카운트", "비트/패킷 속도" 및 "사용율") 중 하나로 변화한다. 또한, 플롯은 임의 윈도우상의 바이트/패킷 카운트에서 비트 및 패킷 속도(즉, 초당 비트 또는 패킷의 수), 그에 따른 사용율로 변화한다. 예시적인 실시예에서, 바이트 플롯은 링크 속도(즉, 초당 비트에서 링크 또는 채널 또는 가상 회로 용량으로 나뉜 비트 속도)에 상대적인 정규 값을 표시한다.
- <102> 3. 토글 부모 플롯: 이 버튼(1038)은 후술되는 바와 같이 플롯의 라인을 토글한다.
- <103> 4. 평균 토글 플롯: 평균 토글 플롯 버튼 선택시 플롯의 y축의 평균 값(도시되지 않음)이 표시되었는지의 여부가 토글된다.
- <104> 5. 재생/전진/정지/고속 전진/되감기/고속 되감기/일시 정지 버튼: 이러한 버튼(1040)은 플롯을 규정 시간외에도 갱신하고 시간에 따라 스크롤할 수 있도록 스크린상의 플롯의 실행을 제어한다. 테이블 프레임(1010)의 테이블(1032)은 플롯(1032, 1034)과 일치하도록 갱신되어야 한다.

- <105> 6. 톱 플롯(Top plot): 도 10에 도시된 톱 플롯(1032)은 바이트/초의 링크 레벨 비트 속도이다.
- <106> 7. 보텀 플롯(Bottom plot): 도 10에 도시된 보텀 플롯(1034)은 패킷/초의 링크 레벨 패킷 속도이다.
- <107> 테이블 프레임(1010)의 테이블(1023)은 개시(1013) 및 정지(1014) 필드에 의해 명기되는 구간에서 활동되는 것으로 알려진 프로토콜에 기초하여 자동적으로 생성된다. 도 10에서, 테이블(1023)은 개시와 정지 시간 사이에서 264K(K=1000) IP 패킷 및 919 APR 패킷이 네트워크 모니터에 의해 수신됨을 나타낸다. IP 패킷 및 ARP 패킷은 각각 99M(M=1,000,000) 및 55K 바이트를 포함한다.
- <108> 테이블(1023)의 엔트리는 선택된 필드에 의해 데이터를 소트하도록 선택 가능하다. 예를 들면, 테이블의 헤드 패킷이 클릭되는 경우, 테이블은 활동의 내림차순으로 패킷 컬럼에 의해 소트되고 이 헤더가 다시 클릭되는 경우에는 올림차순으로 소트된다. 다른 테이블 헤드를 선택하면 동일하게 엔트리를 소트한다.
- <109> 도 11은 본 발명의 줌잉 기능을 도시하고 있다. 도 10에서의 7:18/12:02 개시/정지 시간 주기는 도 11에서 9:00/10:00 시간 주기로 좁아진다. 테이블(1023) 및 플롯(1032, 1034)은 그에 따라 갱신된다. 개시(1013) 및 정지(1014) 필드는 플롯(1032, 1034)의 시간 주기에 관하여 필드(1013, 1014)의 수동 입력, 또는 예를 들면 마우스에 의한 그래픽 선택에 의해 조정될 수 있다. 선택시, 선택된 구간으로 표시를 줌잉(zooming)한다. 플롯을 줌잉하면 사용자에게 의해 선택된 구간 동안에 플롯이 재생성된다. "테이블 및 플롯 갱신" 버튼(1036)을 선택하면 테이블 프레임(1010)의 데이터를 플롯(1032, 1034)과 동기시킨다. 또한, 사용자가 "자동-동기" 특징(도시되지 않음)을 선택하게 되면, 플롯은 자동적으로 갱신될 수 있다. "테이블 및 플롯 갱신" 버튼(1036)은 사용자가 데이터를 갱신하지 않고도 소망의 시간 주기의 수 배를 줌잉하는 것을 허용한다. 이것은 최종 구간이 선택될 때까지 네트워크 모니터에 의한 불필요한 처리를 감소하는 단점이 있다.
- <110> 도 10의 테이블(1023)의 엔트리로 기입된 프로토콜은 선택된 프로토콜 내에 포함되는 프로토콜을 기입하도록 사용자에게 의해, 예를 들면 하이퍼 링크로서 선택 가능하다. 도 10에 도시된 테이블(1023)의 IP 엔트리를 선택 또는 클릭하면 도 12와 같이 표시된다. 이러한 선택에 의해 도 10에 도시된 플롯 프레임(1030)의 플롯(1032, 1034)은 도 12의 플롯(1232, 1243)의 IP 트래픽만을 나타내도록 자동적으로 갱신된다.
- <111> 플롯은 링크 계층으로부터의 모든 트래픽 및 막대 도표로서 IP 트래픽을 나타낸다. 이러한 이중 표시 포맷은 이전 레벨(이 실시예에서 이더넷)의 모든 트래픽과 비교되는 한 레벨(이 실시예에서 IP)의 모든 트래픽 중에서 각각의 트래픽에 대한 그래픽 표시를 제공한다.
- <112> 또한, 테이블 프레임(1210)의 테이블의 콘텐츠는 IP 트래픽에 대응하도록 갱신된다. 테이블(1223)은 "개시"와 "정지" 시간 사이에서 모니터링되는 링크에 사용중인 모든 IP 프로토콜을 기입한다. 이 특정 경우에, TCP, UDP 및 ICMP IP 프로토콜만이 알려져 있다. 또한, IP 호스트에 의한 활동이 표시된다. 테이블 프레임(1210)을 스크롤 다운함으로써, 소스 호스트에 의한 IP 카운트의 테이블은 톱 N=2인 경우에 대하여 도 13에 도시된 바와 같이 된다.
- <113> 도 13에서, 트래픽은 호스트에 의해 생성되는 트래픽에 대하여 소스 호스트 테이블(1302)에 표시되고, 호스트에 의해 수신되는 트래픽에 대해서는 목적지 호스트 테이블(1304)에 표시되고, 호스트에 의해 생성되고 수신되는 트래픽에 대해서는 호스트 테이블(1306)에 표시된다. 테이블 프레임(1310)의 링크(1308)를 클릭하면 도 14에 도시된 "호스트-쌍" 테이블(1402)의 표시가 생성된다.
- <114> 호스트-쌍 테이블(1402)에는 각각의 식별된 쌍에 대해서 호스트 쌍 중에서 전송된 패킷 및 바이트의 총 갯수를 기입한다.
- <115> 또, 10.0.0.47과 같은 "목적지 호스트"(도 14에서의 1404)를 선택하면 호스트 10.0.0.47이 목적지인 트래픽만을 나타내도록 선택된 "목적지 호스트"에 의한 트래픽이 필터링된다. 이것은 도 15에 나타나며, 도 15에서 테이블(1502)은 10.0.0.47이 목적지인 트래픽과, 개시 및 정지 구간 동안에 모니터링되는 트래픽에 대하여 이 실시예에서의 호스트 128.32.130.10으로부터의 모든 트래픽을 나타낸다.
- <116> 따라서, 호스트 128.32.130.10만이 "개시" 및 "정지" 시간 동안에 10.0.0.47에 트래픽을 전송하는 것을 볼 수 있다. 플롯 프레임(1530)의 플롯(1532, 1534)이 막대 도표(1535)로서 두 개의 호스트간의 활동을 나타내고, 선 도표(1536)로서 모든 IP 트래픽을 나타내고 있는 것에 주목하자. 또한, 색은 플롯 또는 테이블의 데이터를 식별하는데 사용될 수 있다.
- <117> 도 12의 테이블(1223)의 TCP 엔트리가 선택되는 경우, 프로토콜 스택을 고려하면, 테이블 프레임(1610)은 각각의 아래 어플리케이션(1612)에 대한 TCP 레벨 카운트를 포함하도록 도 16에 도시된 바와 같이 갱신된다. 예를

들면, 정해진 시간 주기 동안에 수신되는 21 MB를 포함하는 27K HTTP(웹)가 있다.

- <118> 도 16에서, "TCP 흐름" 버튼(1604)이 선택되는 경우, 모든 TCP 흐름은 도 17에 도시된 바와 같이 시간 지속 기간 및 성능 매트릭스와 함께 표시된다. TCP 흐름은 두 개의 호스트간의 하나의 TCP 세션에 속하는 패킷 세트를 포함한다. 각각의 흐름은 플롯팅되거나 또는 대응하는 패킷은 "플롯" 버튼(1702) 또는 "pks" 버튼(1704)을 각각 선택함으로써 보여지며, 소망의 TCP 흐름에 대응한다. Do DNS 옵션이 선택되는 경우, 모든 TCP 호스트 IP 어드레스가 각각의 네임(예컨대, foo.niksun.com)으로 교체되는 것에 주목하자. 사용자는 특정 호스트, 예컨대 10.0.0.47를 식별하는 것과 같이 다른 링크를 클릭함으로써 흐름을 집합시킨다. 사용자가 10.0.0.47을 클릭하면, 호스트 10.0.0.47에 대하여 집합된 흐름은 도 18에 도시된 바와 같이 표시된다.
- <119> 도 18은 호스트 10.0.0.47으로부터 개시하는 모든 TCP 흐름을 도시하고 있다. 도 18에 도시된 표시는 도 17에 표시된 데이터에 호스트 10.0.0.47에 대하여 선택적인 필터를 적용함으로써 생성된다. 도 18의 다른 호스트(하이퍼링크)를 클릭함으로써 다른 필터를 동일하게 적용할 수 있다. 예를 들면, "용어 호스트" 컬럼에서 사용자가 호스트 10.0.0.5(1802)를 선택하면, 호스트 10.0.0.47(소스로서)과 호스트 10.0.0.5간의 모든 TCP 흐름이 표시된다.
- <120> "TCP 성능" 선택은, 예를 들면 TCP 성능 테이블을 생성하기 위해 도 16에 도시된 스크린 표시에 제공될 수 있다. "TCP 성능" 하이퍼링크를 클릭함으로써, TCP의 성능 테이블(1902)은 도 19에 도시된 바와 같이 표시된다. 전체 테이블 프레임은 도 19에 명확하게 표시된다. 표시는, TCP 클라이언트와 서버 두 개를 실행하는 최악의 경우(톱 N 값이 2인 경우) "장애를 겪는 TCP 클라이언트" 테이블과 "장애를 겪는 TCP 서버" 테이블을 포함한다. 개시 및 정지 필드에 의해 규정되는 시간 주기 동안에 테이블은 각각의 TCP 클라이언트 또는 서버에 대해 이하의 측정을 나타낸다.
- <121> 1. 접속 횟수(No. of Connection): 이것은 클라이언트 또는 서버와의 TCP 접속의 총 횟수이다.
- <122> 2. TCP 데이터 바이트: 이것은 모든 TCP 접속에 의해 전송되는 데이터의 총 갯수를 나타낸다.
- <123> 3. TCP 굵푼(바이트/초): 이것은 TCP 페이로드 처리율(어플리케이션 처리율) 또는 TCP 굵푼을 나타낸다. 즉, 어플리케이션 바이트의 총 갯수는 접속 횟수에 대하여 평균화된 바이트를 전송하는데 걸리는 시간으로 나누어진다.
- <124> 4. TCP 처리율(바이트/초): 이것은 TCP 접속에 전송되는 바이트의 총 갯수를 시간으로 나눈 것(TCP 흐름 속도)이다.
- <125> 5. Avg RTT: 이것은 접속 횟수에 대한 클라이언트와 서버간의 평균 라운드 트립 시간을 나타낸다.
- <126> 6. Avg 응답: 이것은 서버로부터 클라이언트까지의 평균 응답 시간을 나타낸다.
- <127> 7. 재전송 %: 이것은 (혼잡, 손실 또는 지연, 또는 소정의 다른 이유) 재전송되는 TCP 바이트의 백분율을 나타낸다.
- <128> TCP 성능 테이블은 사용자 인터페이스를 통해 다른 매트릭스를 부가하거나 또는 기존의 매트릭스를 삭제하도록 조정될 수 있다.
- <129> 도 16의 http 하이퍼링크를 선택하면 도 20에 도시된 바와 같이 웹 트래픽(http)에 대한 통계가 표시된다.
- <130> "http 성능" 선택은, 예를 들면 http 성능 테이블을 생성하기 위하여 도 20의 스크린 표시에 제공될 수 있다. "http 성능" 하이퍼 링크를 클릭함으로써, http의 성능 테이블(2102)은 도 21에 도시된 바와 같이 표시된다. 전체 테이블 프레임은 명확하게 하기 위해 도 21에 표시된다. 표시는 WWW 클라이언트 및 서버 두 개를 실행하는 최악의 경우(톱 N 값이 2인 경우) "장애를 겪는 WWW 클라이언트" 테이블 및 "장애를 겪는 WWW 서버" 테이블을 포함한다.
- <131> http 성능 테이블(2102)의 매트릭스는 온라인 생성되어, 장애를 겪는 WWW 클라이언트 및 장애를 겪는 WWW 서버로서 사용자에게 표시되거나 또는 즉각적인 조치를 위해 네트워크 관리 시스템에 직접 공급될 수 있다. 이 매트릭스는 불량 서버 및 접속을 식별하도록 네트워크 관리자에게 도움을 줄 수 있다. 또한, 이러한 정보는 웹 서버 운영자에게 더 많은 대역폭을 구매하거나 또는 그의 서버를 고정시킬 것을 통지하기 위한 기초로서 사용될 수도 있다. 또한, 클라이언트에게 더 많은 대역폭을 필요로 하거나 또는 다른 서비스 공급자를 선택할 필요가 있다는 것을 통지하는데 사용될 수도 있다. 따라서, 이 매트릭스는 사용자에게 제공되는 서비스 품질을 향상시키는데 사용될 수 있고, 궁극적으로는 네트워크 관리자에게 다른 이득을 제공할 수 있다. 예를 들면, 테이블에서 "장애

를 겪는 WWW 서버", 기입된 제2 서버(204.162.96.10)는 약 33%의 웹 중단을 갖는다. 이것은 이 웹 사이트에서 고객의 33%의 잠재적인 손실을 나타낸다.

<132> 테이블 프레임(1610)은 각각의 아래의 어플리케이션(1612)의 TCP 레벨 카운트를 포함하도록 도 16에 도시된 바와 같이 갱신된다. 예를 들면, 지정된 시간 주기 동안에 수신되는 21 MB를 포함한 27K HTTP(웹)가 있다.

<133> 도 12에 도시된 UDP 하이퍼링크(1240) 선택시에 프로토콜 스택을 고려하면 도 22에 도시된 표시는 UDP 트래픽의 레벨을 나타내도록 제공된다. 테이블 프레임(2210)에서, 표시되는 "UDP 레벨 카운트" 테이블은 각 UDP 어플리케이션 또는 UDP 포트의 활동을 나타낸다. 예를 들면, 표시는 69 KB를 포함한 453 도메인 패킷이 있음을 나타낸다.

<134> UDP 대역폭 사용이 총 IP의 약 0.32%에 불과하다는 것에 주목하자[도 12에 도시된 테이블(1223) 참조]. 따라서, 플롯 프레임은 UDP 트래픽(블루)을 작게 한 IP 트래픽(레드 그래피)만을 도시한다. "토글 부모 표시"를 클릭함으로써, 사용자는 IP의 플롯(부모 플롯)이 제거될 때 UDP 트래픽(도시되지 않음) 상에만 Y축을 zoom할 수 있다.

<135> 도 22에 도시된 "MBONE" 버튼(2202)을 선택하면, 도 23에 도시된 바와 같이 MBONE(Multimedia backbone) 세션의 어플리케이션 계층 분석이 표시된다.

<136> 도 22에 도시된 버튼 프레임(2250)의 "패킷 보기(view packet)"를 선택하면 도 24에 도시된 바와 같이 모든 패킷의 덤프가 제공된다. 도 24에 도시된 표시에서 링크는 사용자로 하여금 데이터 스트림을 마음대로 필터링하게 한다. 사용자가 10.0.0.12(2402)를 클릭하면, 덤프의 다음 스크린은 10.0.0.12로부터의 패킷 및 10.0.0.12에 관한 패킷만을 포함한다. 다음 스크린에서, 사용자가 10.0.0.5를 선택하면, 갱신된 표시가 10.0.0.12와 10.0.0.5 사이에서의 패킷만을 나타낸다. 또한, 사용자는 포트를 선택함으로써 그 덤프를 수식(qualify)한다. 패킷을 덤프하는 다양한 옵션은 스크린 표시의 상부의 셀렉션(2404)으로부터 덤프 타입을 선택함으로써 적용될 수 있다.

<137> 도 22에 도시된 버튼 프레임(2250)내의 "권고" 버튼(2206)을 선택하면, 네트워크에 대한 실시간 용량 또는 대역폭 권고가 표시된다. "권고" 버튼(2206) 선택 검출시에 네트워크 모니터는 사용자에게 보여지는 데이터를 해석하기 위해 수학적 모델을 사용하여 어플리케이션에 의한 대역폭 사용(또는 다른 타입의 트래픽) 또는 특정 서비스 품질을 얻기 위한 링크/스위치 용량 설정에 관한 권고를 제공한다. 몇 개의 이러한 통계(2502)는 도 25에 도시되어 있다. 사용자는 손실율 및 최대 지연과 같은 소망의 서비스 품질을 입력하여, 분석된 트래픽의 타입에 대한 소망의 서비스 품질을 지원하는데 요구되는 용량에 관한 권고를 취득한다. 도 25 및 26은 제공될 수 있는 권고를 도시하고 있다.

<138> 예시적인 실시예에서, 사용자는 특정 서비스 품질의 레벨을 위해 네트워크 자원의 "크기"를 정하고자 하는 "사용중-기간(busy-period)" 및 특정 어플리케이션을 선택한다. 네트워크 모니터의 적절한 서브루틴은 특정 어플리케이션 트래픽을 분석하고 "모델 파라미터"를 추출하거나 또는 추정한다. 수학적 모델을 사용하여 서비스 품질 파라미터(예컨대, 패킷 손실율, 네트워크 지연, 프레임 속도 등)는 물론 모델 파라미터를 추정함으로써, 모델은 통계학적 다중화 이득, 용량 요구 조건 및 버퍼 할당과 같은 통계를 계산하여, 네트워크 사용율을 최대로 하기 위해서 사용자에게 서비스/라우터 구성, 네트워크 자원 또는 서버 파라미터의 최적 권고를 제공하는 한편, 서비스 품질 요구 조건을 충족시킨다. 이러한 권고는, 통계가 모든 패킷 또는 상이한 서비스에 속하는 패킷 세트에 대하여 갱신되는 실시간에 기초하여 계산되며, 피드백은 최적의 구성에서 각 흐름의 경로를 따라 네트워크 구성 요소에 제공되어, 동적 자원 할당을 가능하게 하여 서비스 품질 요구 조건을 충족시키게 된다.

<139> 그래픽의 x-축(2602)은 사용자의 갯수를 나타내고, y-축(2604)은 비트/초의 용량을 나타낸다. 소망의 사용자 수에 대하여, 용량은 차트를 판독하거나 또는 대응하는 테이블 결과의 표시로부터 판독될 수 있다. 도 27은, Do DNS 버튼이 선택되어 IP 어드레스가 그들의 등록 네임으로 분해(resolve)되는 경우에 대하여 도 22에서와 동일한 표시를 나타내고 있다.

<140> 도 28은 도 22에 도시된 버튼 프레임(2250)내의 "통계" 버튼(2208) 선택시에 표시되는 통계를 나타내는 표시이다. "통계" 버튼(2208) 선택시에 네트워크 모니터는 사용자에게 현재 보여지는 데이터에 기초하여 여러 통계를 계산한다. 예시적인 통계는 패킷 크기 분포, 프로토콜 분포, 클라이언트마다의 대역폭 사용, 도메인에 의한 대역폭 사용, 서버마다의 평균 응답 시간, 서버와 클라이언트 쌍간의 평균 라운드 트립 시간 및 성능 매트릭스를 포함한다.

<141> 본 발명은 호스트 컴퓨터와 인터페이스 컴퓨터간의 특정 분배 기능에 한정되지 않는다. 호스트 컴퓨터 및 인터페이스 컴퓨터의 기능은 단일 컴퓨터에 의해 실행될 수 있다. 본 발명에 따른 네트워크 모니터를 갖는 인터페이스

스는 사용자 인터페이스에 한정되지 않고, 모니터링되는 네트워크 또는 다른 통신 회선에 의한 것일 수 있다.

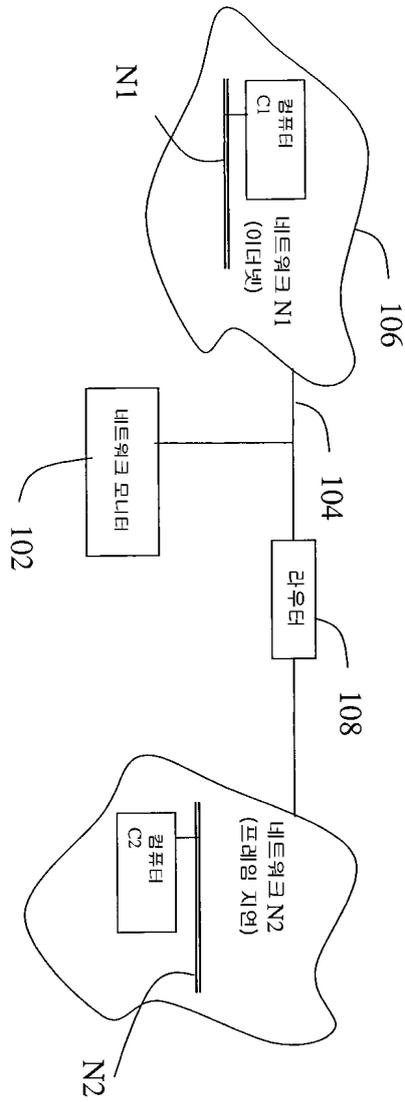
<142> 본 발명은 임의의 특정 실시예에 관하여 상기되어 있지만, 이 상기한 상세한 설명에 한정되지 않는다. 오히려, 상기한 상세한 설명에 있어서 본 발명의 사상으로부터 벗어나지 않고 본 발명의 범위 내에서 다양한 변경이 이루어질 수 있다.

도면의 간단한 설명

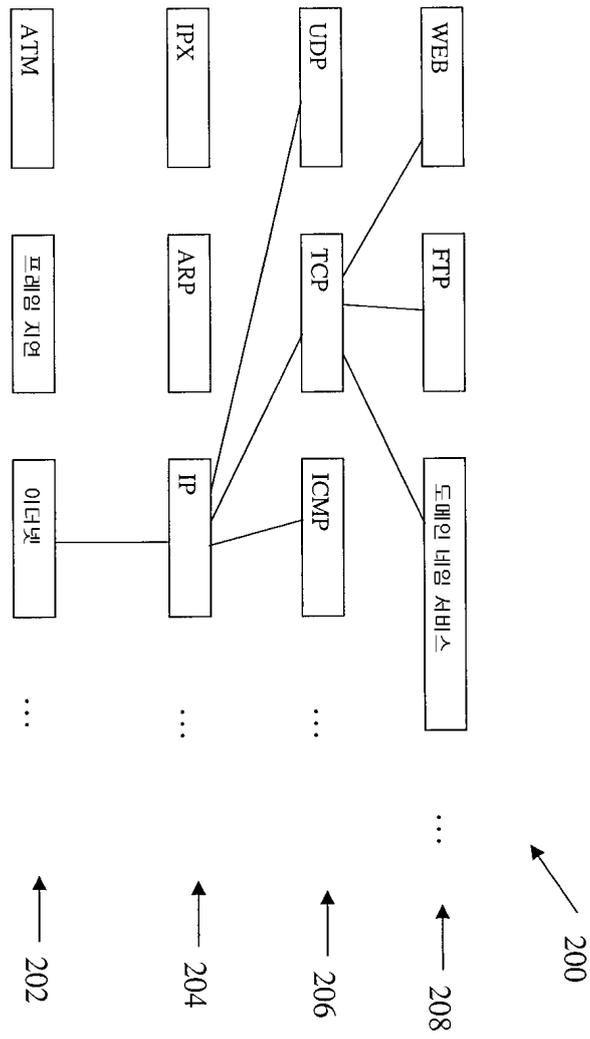
- <18> 도 1은 통신 회선에 결합되는 본 발명에 따른 네트워크 모니터를 도시하는 도면이다.
- <19> 도 2는 예시적인 프로토콜 계층을 도시하는 도면이다.
- <20> 도 3은 본 발명에 따른 예시적인 네트워크 모니터의 블럭도이다.
- <21> 도 4는 본 발명에 따른 통신 회선을 모니터링하는 예시적인 방법을 도시하는 플로우차트이다.
- <22> 도 5는 본 발명에 따른 네트워크 모니터의 데이터 수집 및 분석 방법의 많은 변경을 기술하는 데이터 흐름도이다.
- <23> 도 6은 장애 서버를 식별하는 방법을 도시하는 플로우차트이다.
- <24> 도 7은 네트워크에서 두 개의 분리된 통신 회선에 결합되는 본 발명에 따른 네트워크 모니터를 사용하는 네트워크를 도시하는 도면이다.
- <25> 도 8은 전송 지연을 결정하는 방법을 도시하는 플로우차트이다.
- <26> 도 9a는 인터페이스 컴퓨터와 동기하는 호스트 컴퓨터의 동작을 도시하는 플로우차트이다.
- <27> 도 9b는 호스트 컴퓨터와 동기하는 인터페이스 컴퓨터의 동작을 도시하는 플로우차트이다.
- <28> 도 10 내지 도 28은 모니터링 파라미터를 수신하는 사용자 인터페이스를 도시하고, 통신 분석 정보를 표시 및 제공하는 방법을 도시하는 스크린 표시가다.

도면

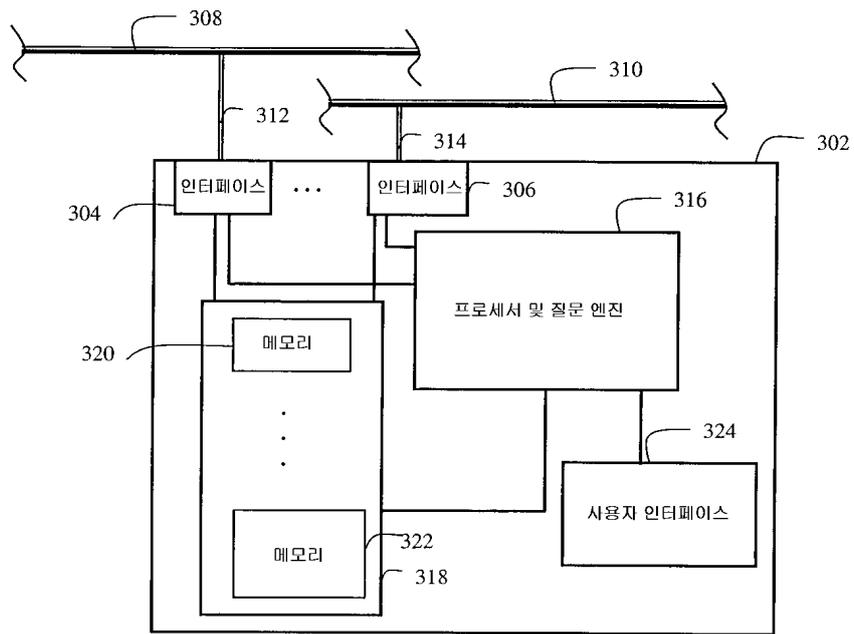
도면1



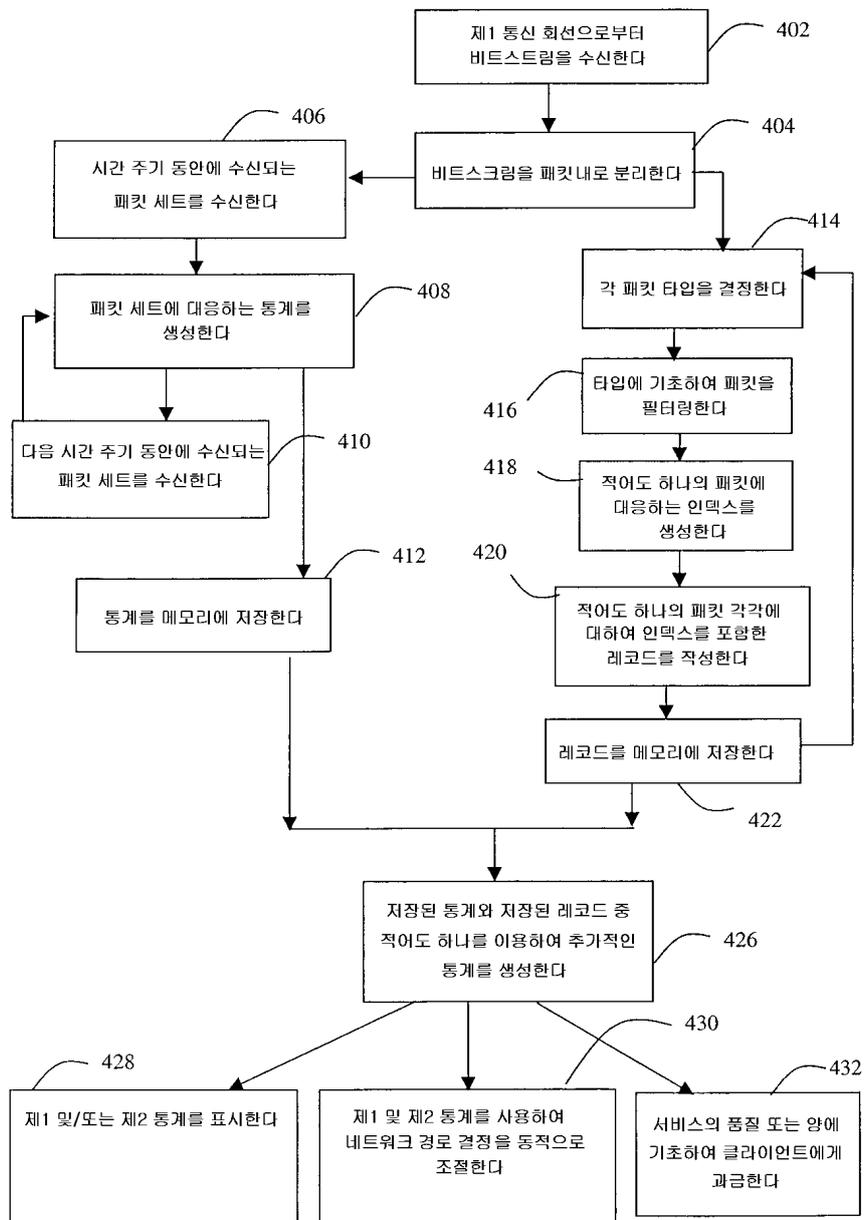
도면2



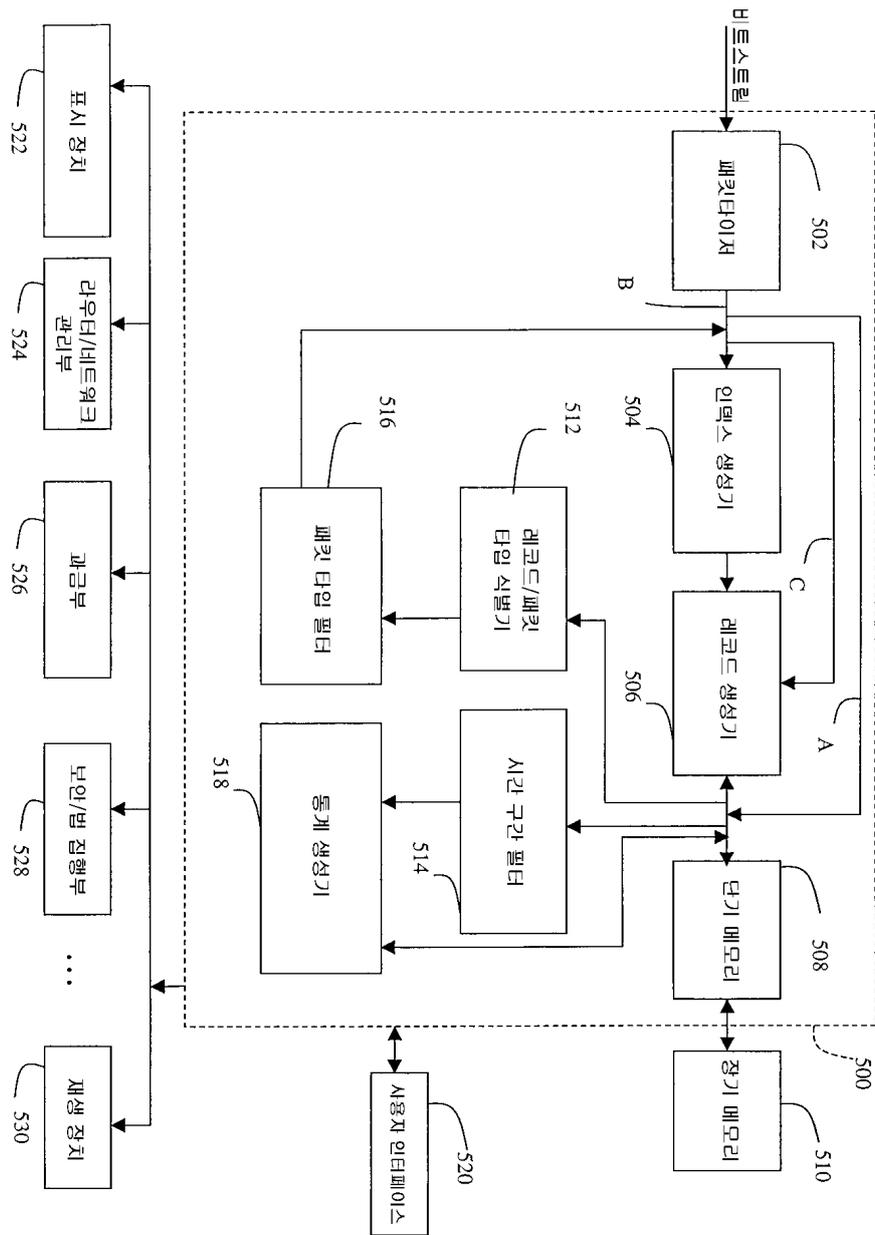
도면3



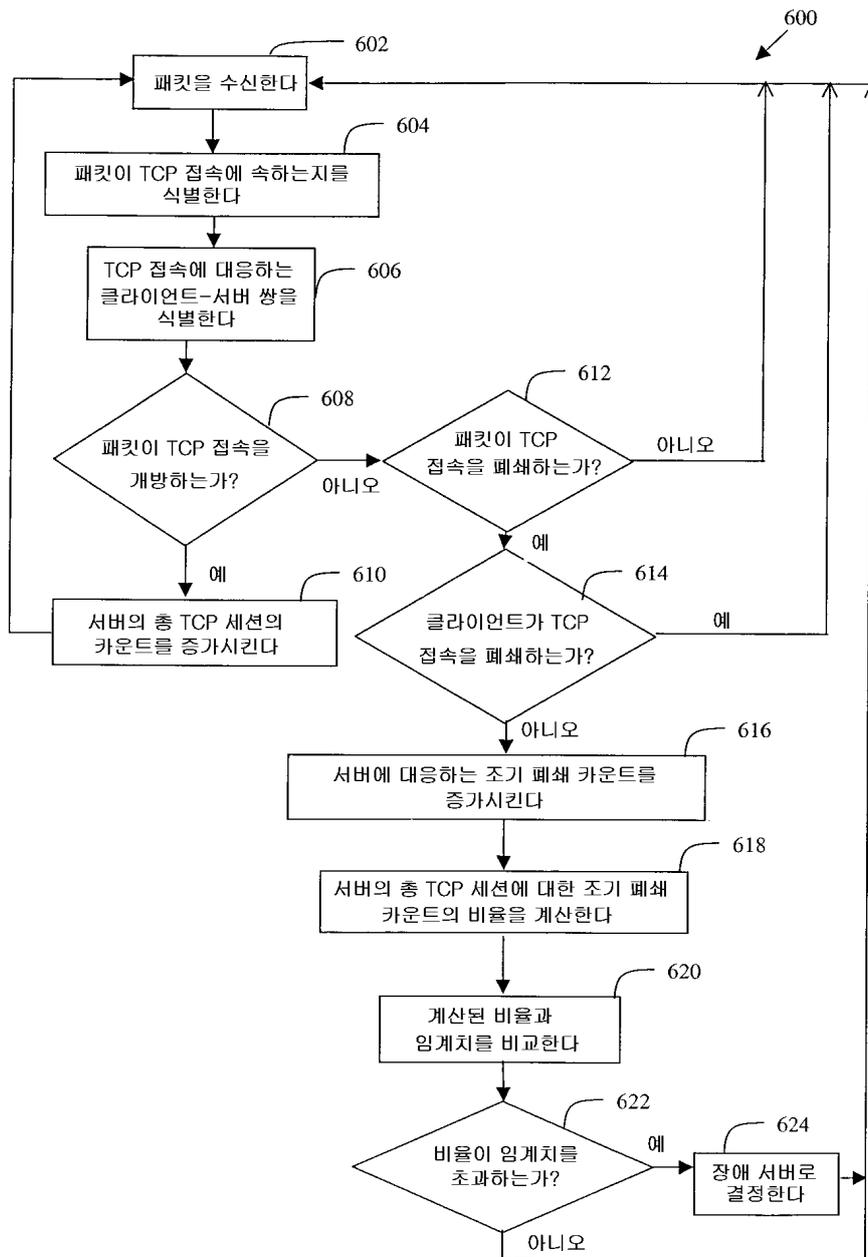
도면4



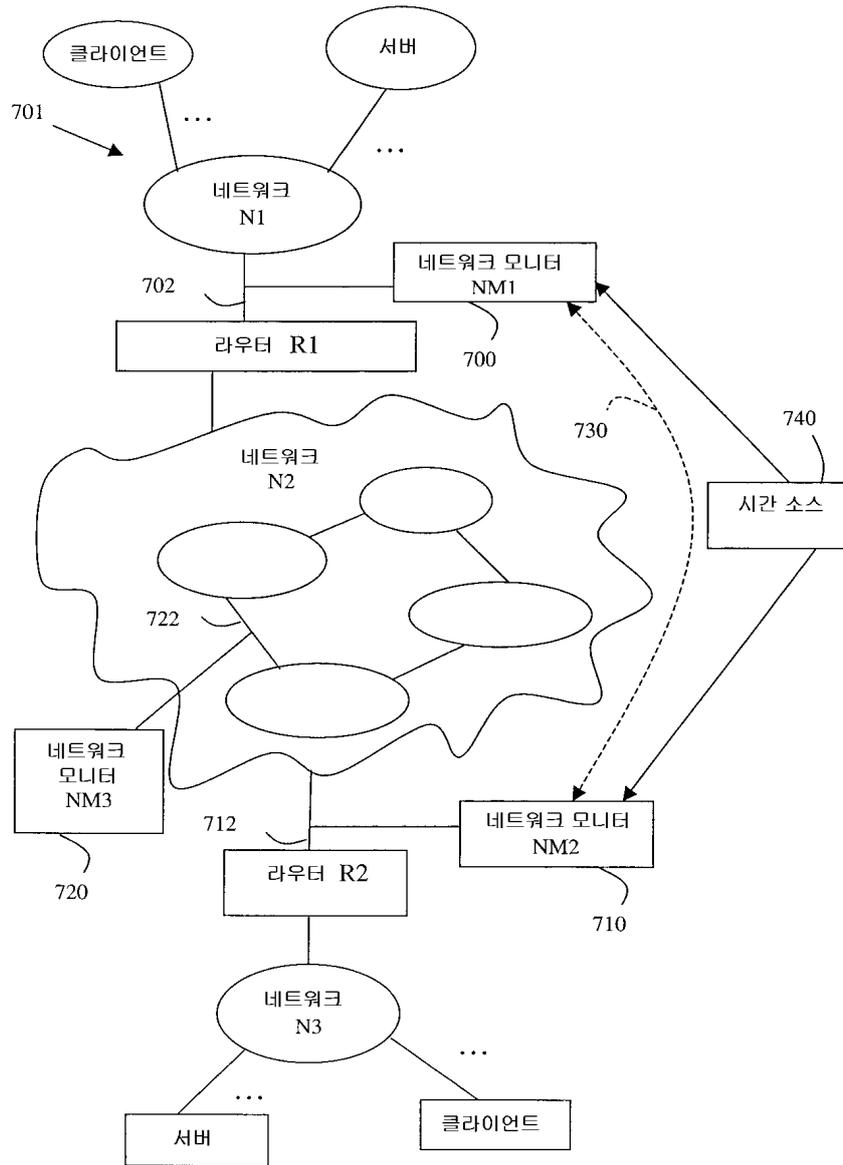
도면5



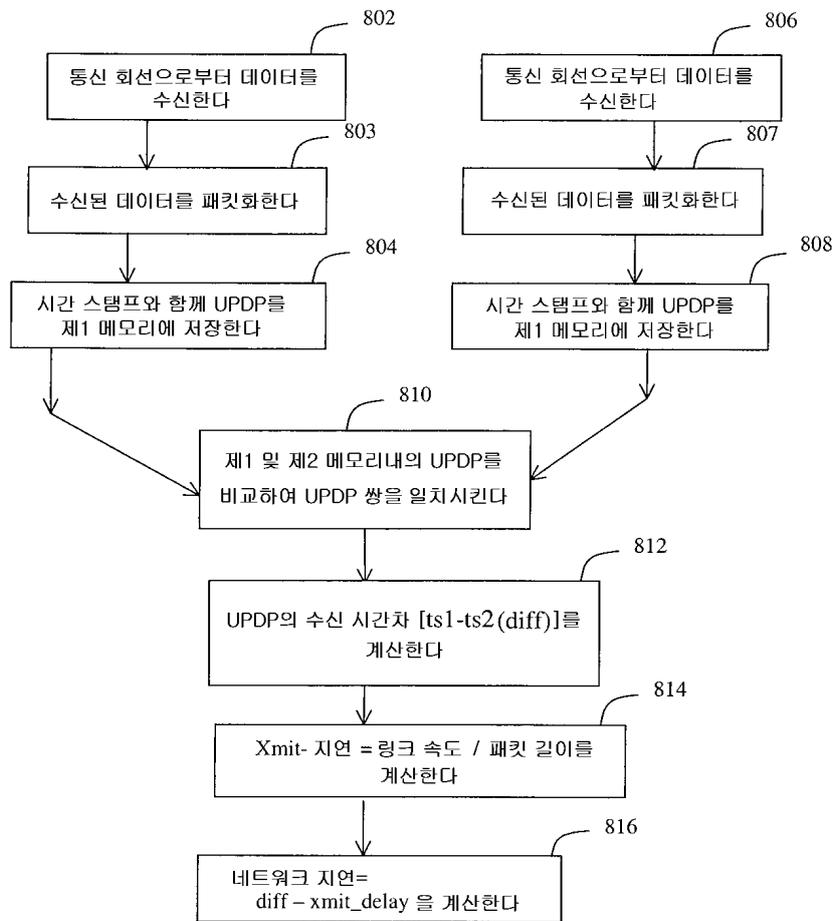
도면6



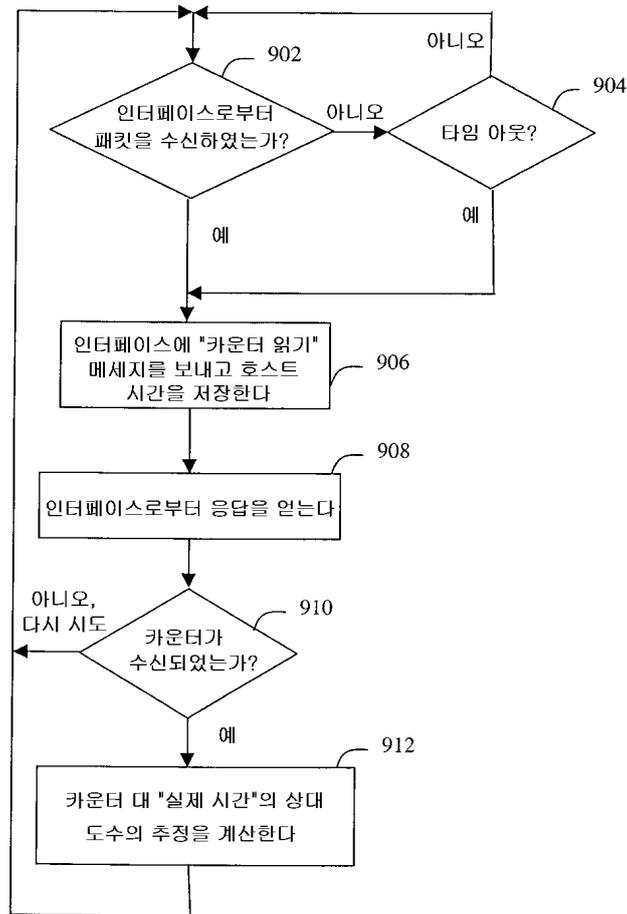
도면7



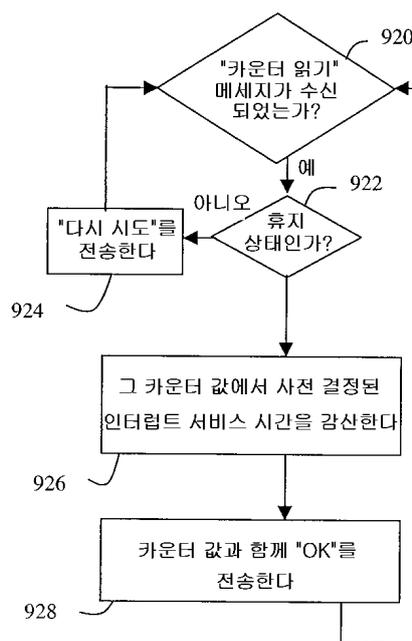
도면8

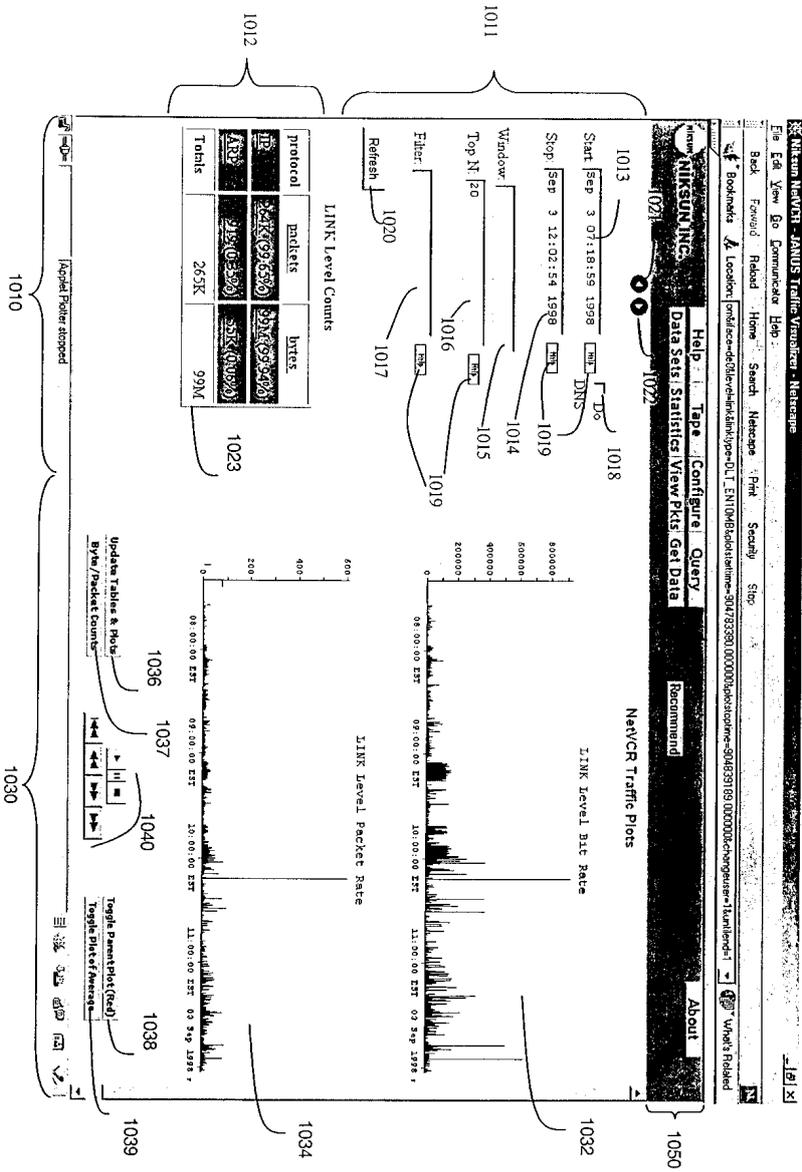


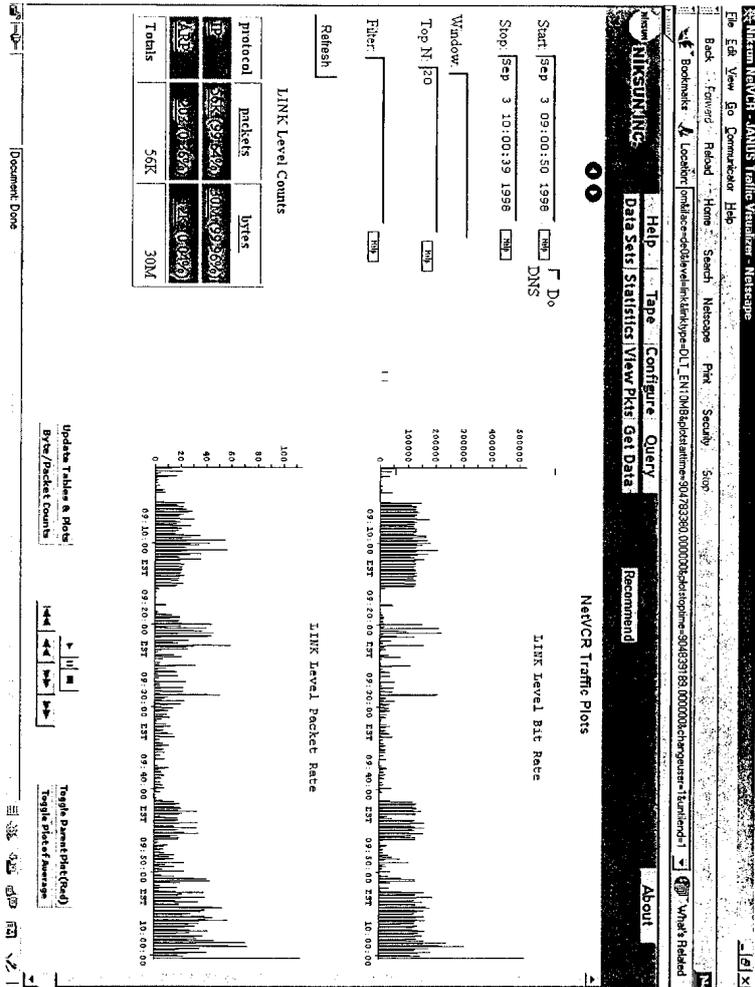
도면9a



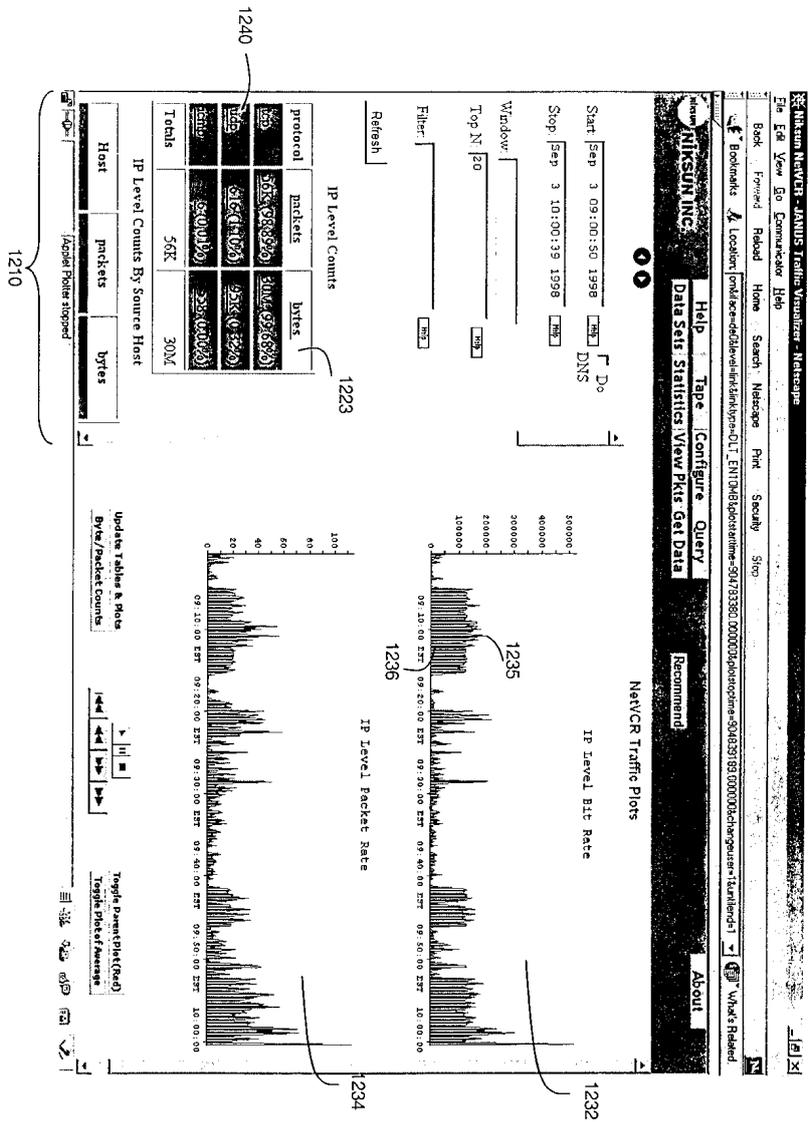
도면9b

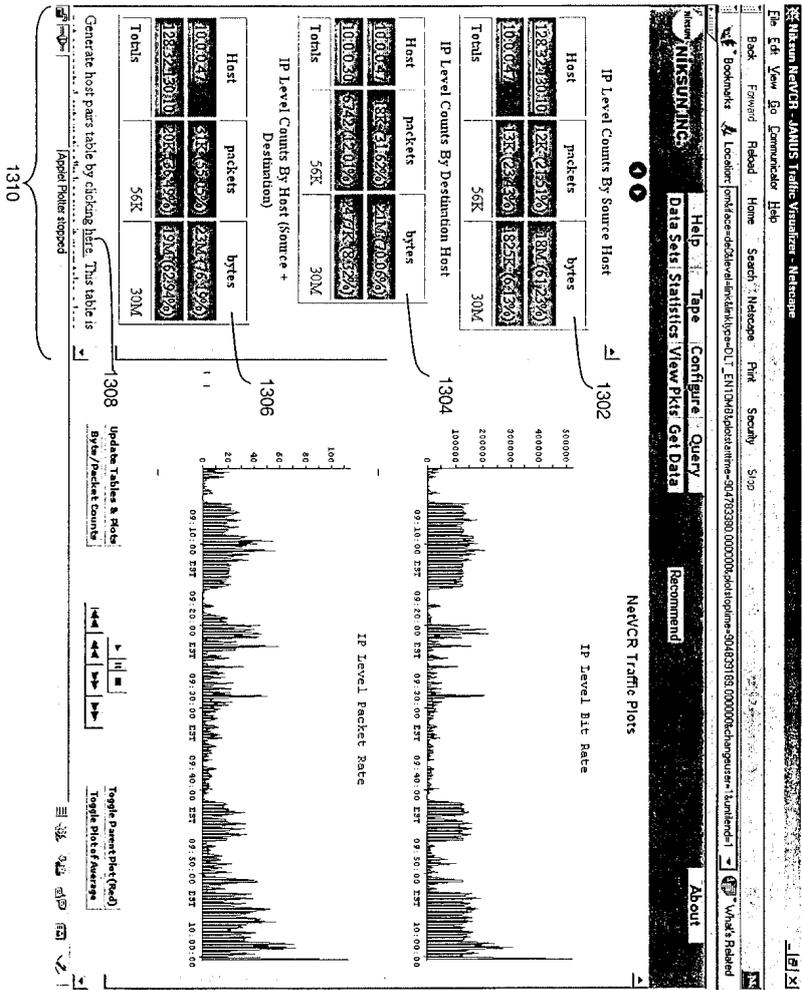


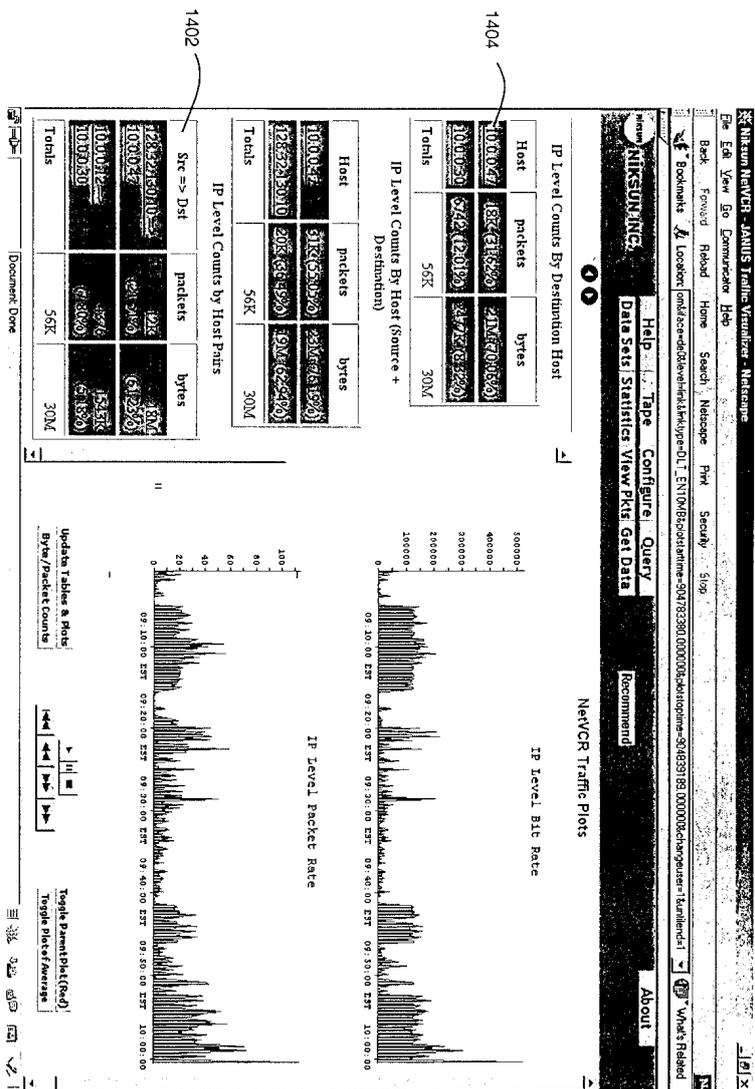


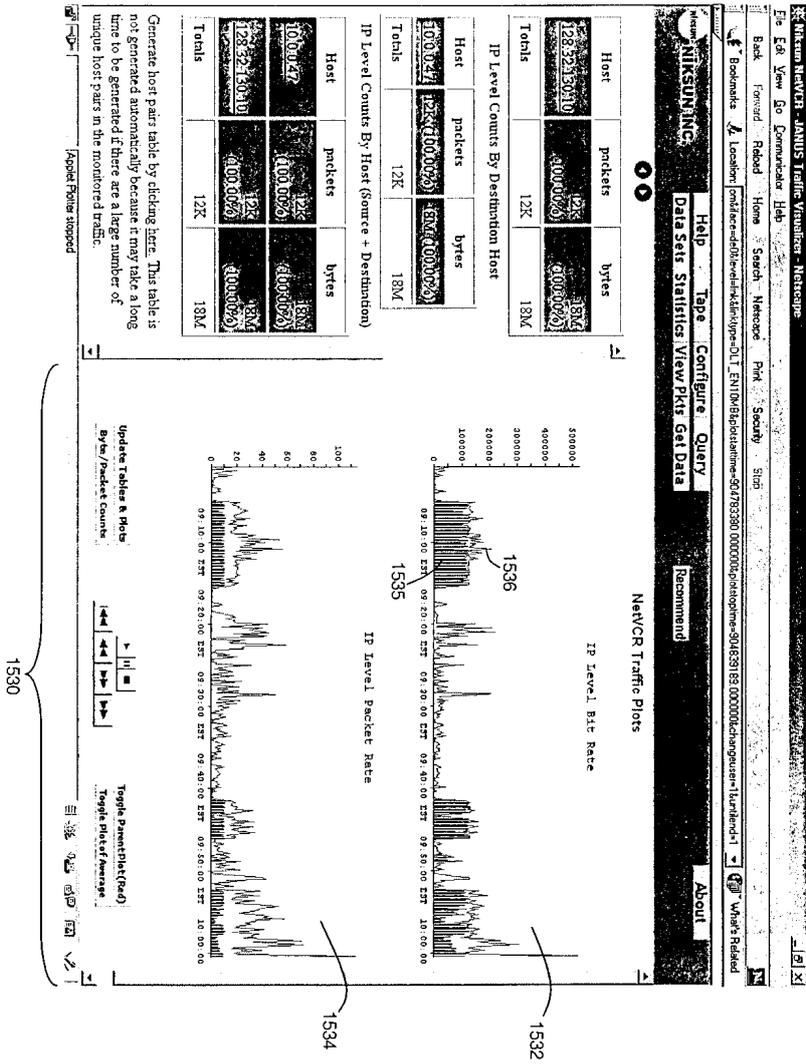


도면12

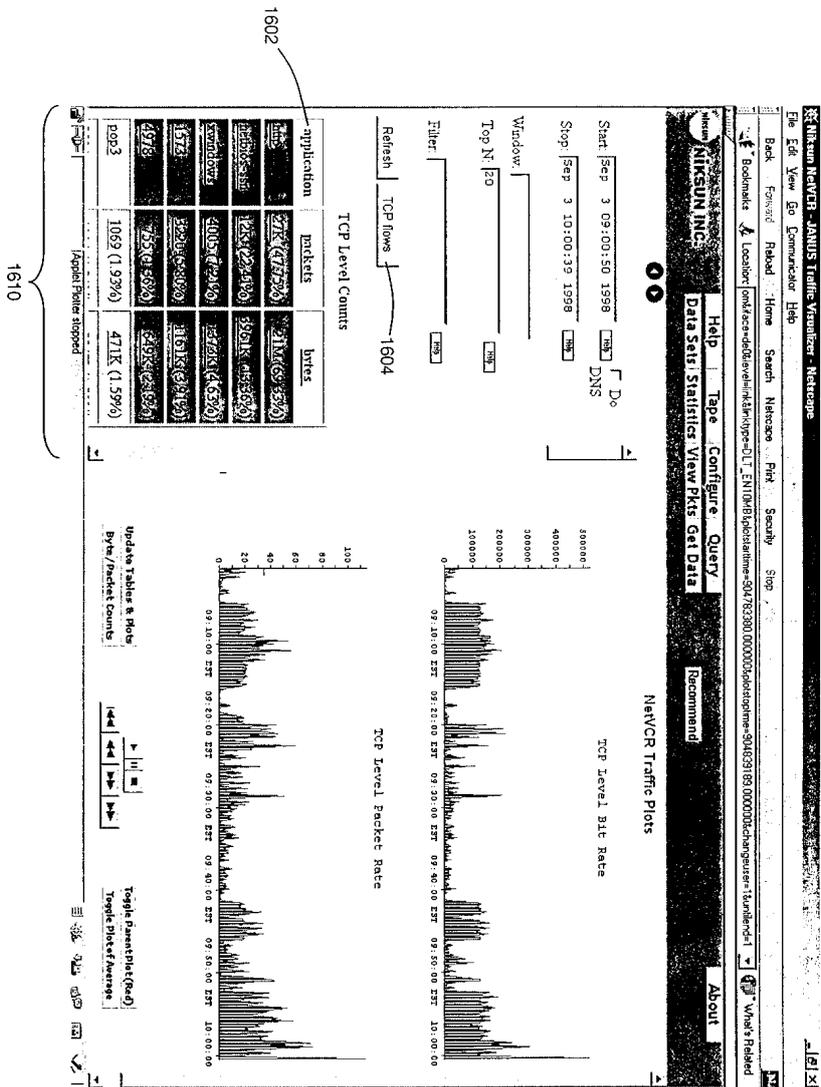








도면16



도면17

*** TCP Flow for data from Sep 3 08:00:50 1998 to Sep 3 10:00:59 1998 - Netscape

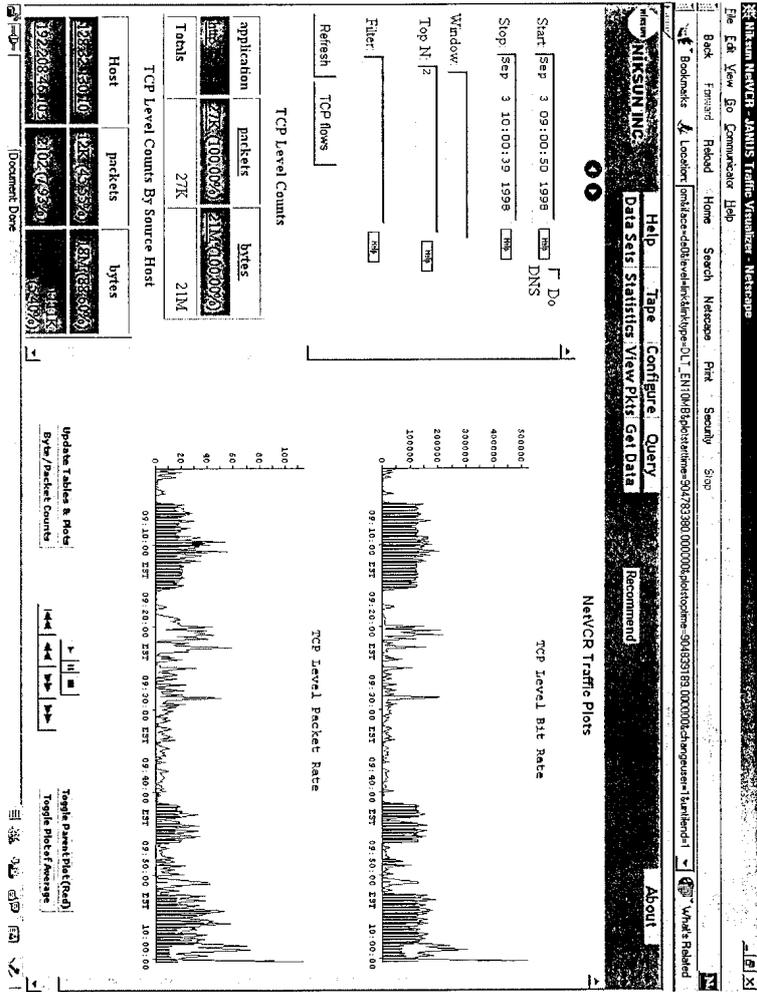
File Edit View Go Communicator Help

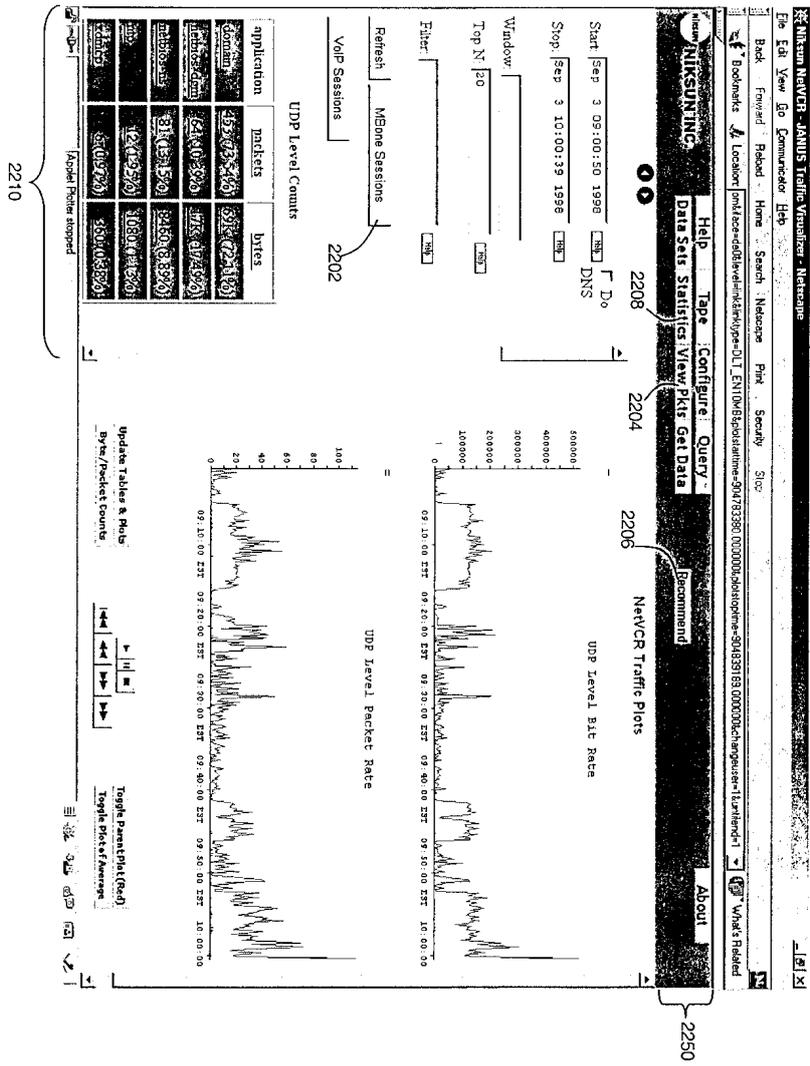
Back Forward Reload Home Search Helpcase Print Security Stop

Backbone Location [xatmnet-cs++4-03-240023490+1988atmnet-gome-Sep+3+102340023493+1988gokwindow-tlog_in-Zdaturerul-licprows -] What's Related

TCP Flows											
Start	Stop	Orig host	Orig port	Orig bytes	Term host	Term port	Term bytes	RTT (sec)	Response (sec)	Rxcount	Rxbytes
1704	1702										
pkts	pkts	1706									
Sep 3 09:01:04 1998	Sep 3 09:02:43 1998	10.0.0.47	33392	89	10.0.0.5	ephcst	12043	N/A	N/A	0	0
Sep 3 09:02:23 1998	Sep 3 09:02:26 1998	10.0.0.101	gocemmh	644	10.0.0.30	netbios-ssn	710	0.000345	0.000252	0	0
Sep 3 09:03:45 1998	Sep 3 09:03:46 1998	10.0.0.40	2572	43	10.0.0.5	pop3	221	0.000933	0.380737	0	0
Sep 3 09:05:06 1998	Sep 3 09:05:07 1998	10.0.0.47	33388	361	128.32.130.10	hnp	0	N/A	N/A	0	0
Sep 3 09:06:07 1998	Sep 3 09:06:17 1998	10.0.0.40	2574	322	207.25.71.29	hnp	42357	0.426337	0.481845	892	0
Sep 3 09:06:09 1998	Sep 3 09:06:13 1998	10.0.0.40	2575	753	207.25.71.29	hnp	126	0.980415	1.017279	0	0
Sep 3 09:06:09 1998	Sep 3 09:06:13 1998	10.0.0.40	2576	752	207.25.71.29	hnp	126	0.998335	0.937072	0	0
Sep 3 09:06:09 1998	Sep 3 09:06:21 1998	10.0.0.40	2577	1076	207.25.71.29	hnp	18243	1.004437	1.171244	373	0
Sep 3 09:06:11 1998	Sep 3 09:06:17 1998	10.0.0.40	2578	759	207.25.71.29	hnp	126	1.170077	1.488473	0	0

Document View





Nixsum NetVCR Janes Bandwidth Advisor - NetScape

File Edit View Go Command Window Help

Back Forward Reload Home Search Netscape Print Security Size

Bookmarks Lockset [http://www.nixsum.com/line/230poc/202/068/20/poc/206/220/poc/207/10/poc/208/06 - View's Related

Nixsum NetVCR Bandwidth Advisor

Statistics Start Time Sep 3 09:00:50 1998
 Statistics End Time Sep 3 10:00:30 1998
 Recorder stcgl.nixsum.com
 Interface de0
 Protocol Layer Name UDP

Hurt Parameter Estimate: 0.722652

Packets/Sec Factor Estimate: 178.089

Total number of Bytes: 89413 bytes	Total number of Packets: 591 packets
Peak Rate in Bits/Sec: 24368 bps	Peak Rate in Packets/Sec: 20 pps
Average Rate In Bits/Sec: 201.098 bps	Average Rate In Packets/Sec: 0.16334 pps

← 2502 →

Bandwidth Requirements

Max. No. Of Sources: 50

Loss Rate Advisor

Bit Loss Rate: 1e-05

도면25

