The Best Protocol Analyzer

Sniffer Pro

Release 4.7

소프트웨어 사용법

(주) PGPnet

목 차

매뉴얼 설명 vi

도움말 표시 vi

Sniffer Pro 를 위한 다른 매뉴얼 vi

1. **Sniffer Pro 소개** 1

주요 구성 요소....2

2. **네트워크 모니터** 4

모니터 필터 5

모니터 어플리케이션 5

데쉬보드(Dashboard) 6

Dashboard 의 선로 상태 표시기....7

데쉬보드 그래프 관찰 8

데쉬보드 통계자료에 대한 임계값 설정....9

호스트 테이블(Host Table) 10

단일 스테이션 기능....11

매트릭스(Matrix) 14

특정 스테이션 기능....14

어플리케이션 응답 시간(ART, Application Response Time)....16

ART 알람....16

ART 화면에 다른 프로토콜 추가하기 20

히스토리 샘플(History Samples) 22

다중 히스토리 샘플 화면 구성하기....24

프로토콜 분포(Protocol Distribution)....26

글로벌 통계 자료 (Global Statistics)....28

스마트 스크린 (Smart Scan): ATM 어댑터 29

물리 계층 통계 자료 (ATM 어댑터)....30

스위치 (Switch)....31

모니터 알람 33

모니터 데이터 변환하기....33

모니터 데이터에 대한 보고서 생성하기 34

모니터 데이터를 데이터베이스 파일에 저장하기....34

3. **패킷 캡처 하기 (Capturing Packets)** 36

캡처 제어(Capture Controls)....36

캡처 패널(Capture Panel)....37

캡처 버퍼(Capture Buffer) 38

Large Capture Buffer Sizes 39

캡처 버퍼와 관련된 문제점 해결 40

캡처 버퍼의 내용을 파일에 저장하기..40

특정 스테이션에서 캡처 하기..41

캡처 필터 (Capture Filters)..41

캡처 트리거 (Capture Triggers)..42

Expert 옵션 (Expert Options) 42

Expert 계층 및 대상들 (Expert Layers and Objects) 42

Expert 임계 값 (Expert Thresholds)..44

프로토콜 (Protocols) 45

서브넷 마스크 (Subnet Masks) 46

RIP 설정 (RIP Settings)..47

802.11 옵션..49

Access Point 의 16 진수 주소 결정하기 50

4. 캡처 된 데이터를 화면에 표시하기.. 52

디스플레이 필터 (Display Filters)..53

패킷 디스플레이 (Packet Display)..54

디코드 탭(Decode Tab)..54

디스플레이 조작(Navigating the Display) : 키(key)들의 기능 익히기..............55

패킷 선택하기(Selecting Packets)..55

디스플레이 옵션 설정하기(Setting Display Options)..56

Decode 화면에서 프레임 찾기..60

프로토콜 강제 지정 사용하기(Using Protocol Forcing) 64

매트릭스 탭(Matrix Tab)..65

호스트 테이블 탭(Host Table Tab)..67

프로토콜 분포 탭(Protocol Distribution Tab)..69

통계 자료 탭(Statistic Tab) 70

Expert 화면..71

자동 Expert 디스플레이 필터 설정..72

Expert Filter 의 한계 73

Expert Filter 에 대한 주의 사항 73

상황에 따른 설명 메시지 디스플레이 하기 (Displaying Context-Sensitive Explain Message) 74

Expert 화면 재정렬하기 (Rearranging Expert Display)..74

캡처 파일과 함께 Expert Objects 저장하기..75

Save/Load Expert Objects 기능의 주의 사항 75

Expert 데이터베이스의 내용 변환하기 (Exporting the Contents of the Expert Database)......75

Expert 분석기 데이터 자동......76

5. **필터와 트리거 정의하기 78**

필터 정의하기 (Defining Filters)......78

Filter Profile 사용하기 79

주소에 의한 필터링 (Filtering by Address)......82

데이터 패턴에 의한 필터링 (Filtering by Data Pattern)......83

패킷 크기, 프로토콜, 그리고 에러 유형에 의한 필터링 84

캡처 버퍼 옵션 설정하기......85

ATM VPI.VCI 상에서 필터링 하기......86

ATM 스테이션 주소 상에서 필터링 하기 87

Payload 유형으로 필터링 하기 (ATMBook Only)......88

WAN/Synchronous 프레임 유형에 의한 필터링 하기......88

트리거(Triggers) 정의하기......89

6. **주소록 (Address Book) 사용하기 91**

주소록 생성하기......91

수동으로 호스트 네임 입력하기 92

주소록 불러오기......93

주소와 이름의 자동 검색......93

라우터를 위한 자동 검색 설정하기......94

Netware 4.x 네임과 주소 94

Gigabit Ethernet 어댑터에서 자동 검색 사용 95

Full Duplex 10/100 Ethernet 어댑터 또는 Snifferbook Ultra 에서 자동 검색 사용 95

발견된 주소를 주소록에 첨가하기 96

7. **알람(Alarms) 관리하기 98**

알람 로그 98

알람의 중요도 설정하기......99

모니터 알람 99

Expert 알람 100

알람 통보 동작 설정하기......101

알람 동작 활성화 하기 102

알람 신호와 소리......103

8. **Sniffer Pro 도구 사용하기 104**

Ping......104

Trace Route 105
DNS Lookup 106
Finger 106
Who Is 107
Tools 메뉴에 도구 첨가하기 108
9. **패킷 생성기 사용하기 109**
표준 패킷 생성기 사용하기 109
단일 패킷 전송하기 110
캡처 버퍼나 파일 전송하기 111
ATM/Gigabit Ethernet 패킷 생성기 사용 112
단일 패킷 전송하기 112
캡처 버퍼나 파일 전송하기 114
Packet Library 사용 116
Packet Library 에 Packet 저장 117
Packet Library 에서 패킷을 로드 117
Packet Setup 파일과 Buffer Setup 파일 사용하기 118
트래픽을 생성하기 위한 스크립트 사용하기 118
스크립트 파일 저장하기 119

10. **Sniffer Pro 와 함께 Sniffer Reporter Agent 사용하기 120**
11. **네트워크 어댑터들과 어댑터 설정 121**
Sniffer Local Agents 생성하기 122

부록 1: Sniffer Pro 의 스위치 분석 기능 124
지원되는 스위치들 124
스위치 분석의 개념 125
스위치 분석을 위한 설치 125
인터페이스 카드들의 설치 및 구성 126
이 작업을 하는 방법 127
카드 구성하기 – 순서 127
특정 스위치를 Sniffer Pro 의 목록에 추가하기 128
Test 버튼을 이용하여 설정 내용 확인하기 131
부록 2: 데이터 패턴을 이용한 필터 정의 132

머리말

매뉴얼 설명

본 매뉴얼은 Sniffer Pro 의 전반적이고 포괄적 내용 즉, 네트워크 가시성 그리고 윈도우 95/98 과 윈도우 NT 를 위한 문제 해결을 위한 툴에 대한 사용 방법을 제공한다.

도움말 표시

본 소프트웨어를 실행한 후, 화면에 등장하는 작은 메뉴 아이콘에 대한 간단한 설명은 마우스 포인터를 해당 메뉴 아이콘에 올리면 나타난다.

또한 Sniffer Pro 온라인 도움말 목차를 검색할 때와 현재 보고 있는 내용에 관한 그 이상의 정보를 얻고자 한다면, 도움말 표시에 있는 내용을 참조하자.

Sniffer Pro 를 위한 다른 매뉴얼

Table 1. 다른 Sniffer Pro 매뉴얼

매뉴얼	내용
스위치 Expert 연결과 구성 가이드 (Switch Expert connection and configuration Guide)	스위치 Expert 사양을 사용하기 위하여 Sniffer Pro 를 연결하고 구성하는 방법에 대한 설명.
ATM 설치, 연결 그리고 구성 가이드 (ATM Installation, Connection and Configu-ration Guide)	ATM 하드웨어를 사용하고 있을 때, Sniffer Pro 를 설치, 연결, 구성하는 방법 설명. ATM 인터페이스에 대한 설명.
WAN 하드웨어의 설치, 연결 그리고 구성 가이드 (Installing, Connecting, and Configuring WAN Hardware)	LM2000 이나 HSSI 를 사용하고 있을 경우, Sniffer Pro 를 설치, 연결, 구성하는 방법
SnifferBook 사용하기 (Using the SnifferBook)	SnifferBook 을 사용할 경우, Sniffer Pro 를 설치, 연결, 그리고 구성하는 방법.
WANBook 사용하기 (Using the WANBook)	WANBook 을 사용할 경우, Sniffer Pro 를 설치, 연결, 그리고 구성하는 방법
Fast Ethernet Full Duplex Pod 사용하기	Fast Ethernet Full Duplex Pod 를 사용하는 경우, Sniffer Pro 를 설치, 연결, 그리고 구성하는 방법.
Expert Analyzer Output File Format	Expert 분석기 표시로부터 변형된 CSV 파일의 내용에 대한 설명.

1. Sniffer Pro 소개

Sniffer Pro 는 당신에게 다음과 같은 기능을 제공해주는 강력한 네트워크 관측 도구이다.

* 실시간 네트워크 동작 상태 모니터

* 개별 스테이션, 두 스테이션 간의 데이터 송수신, 혹은 일정 비율의 네트워크에 대한 상세 사용량(utilization)과 에러 통계 자료 수집

- 기본 네트워크 분석(baseline analysis)을 위한 시간단위의 사용량 및 에러 정보를 저장
- 시,청각적인 실시간 알람 생성
- 문제가 검출되었을 경우, 네트워크 관리자에게 통보
- 상세한 패킷 분석을 위하여 네트워크 트래픽 캡처
- 네트워크 트래픽에 대한 Expert 분석
- 트래픽 시뮬레이션, 응답 시간 측정, 홉 수 계산, 그리고 문제의 해결을 위하여 활동적인 도구를 가지고 네트워크를 면밀히 조사

Sniffer Pro 는 윈도우 32-비트 멀티테스킹 사양의 이점을 최대로 활용하도록 디자인되었다. 당신은 이 프로그램의 다중 인스턴트와 개별적인 도구들을 실행시킬 수 있으며, 다른 윈도우 어플리케이션들과 함께 안정적으로 실행시킬 수 있다. 직관적인 윈도우 유저 인터페이스는 Sniffer Pro 를 쉽게 배우고 사용할 수 있도록 한다.

Sniffer Pro 는 여러 가지 유형의 네트워크 세그먼트에서도 사용할 수 있다.

- Ethernet
- Gigabit Ethernet
- Fast Ethernet (100BASE-T)
- Wireless LANs (802.11b)
- Token Ring
- ATM
- WAN/Synchronous
  - LM2000 어댑터를 사용하는 RS/V 인터페이스
  - HSSI 어댑터를 사용하는 HSSI 인터페이스
  - SnifferBook 과 이에 대응하는 인터페이스 모듈을 사용하는 RS/V, T1, E1 그리고 ISDN (BRI 와 PRI) 인터페이스
  - WANBook 과 이에 대응하는 인터페이스 모듈을 사용하는 RS/V, T1, E1 그리고 ISDN (BRI 와 PRI) 인터페이스

주요 구성 요소

*그림 1-1*은 Sniffer Pro 의 주요 구성 요소들을 보였다.

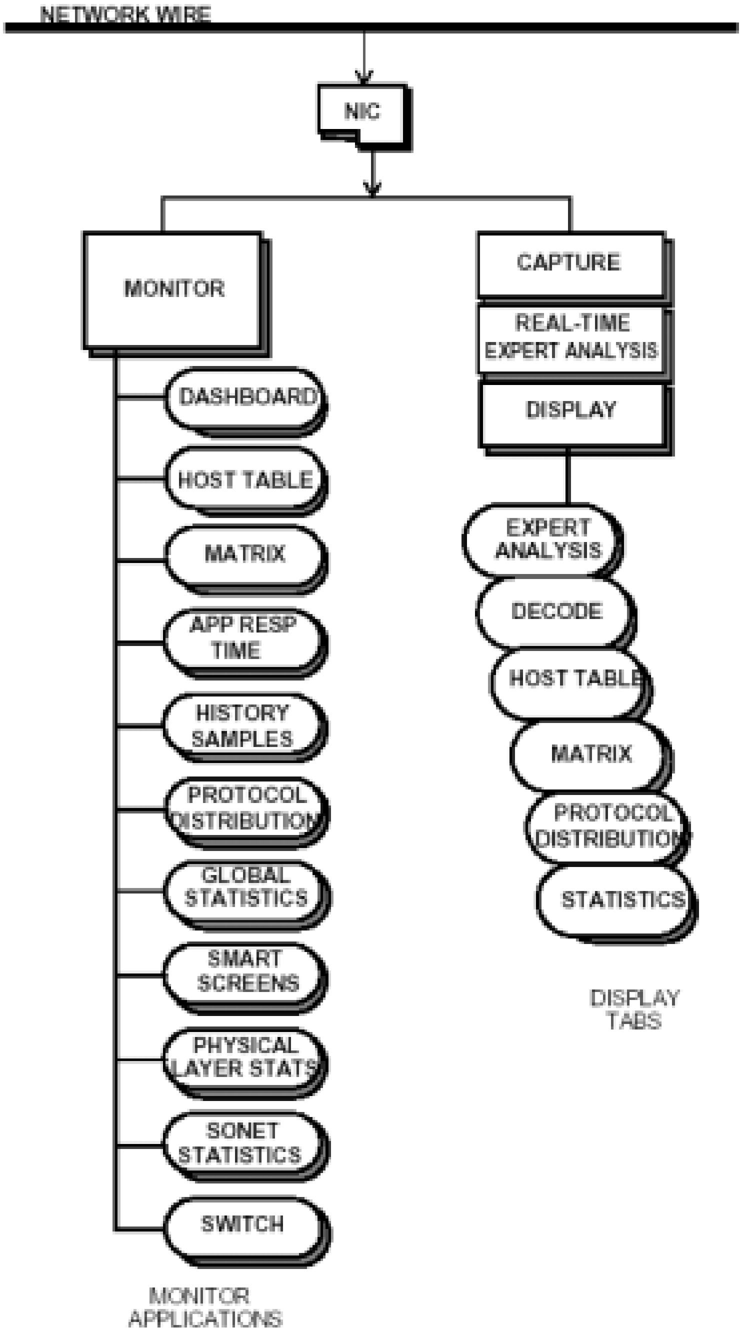


그림 1-1. Sniffer Pro 주요 구성 요소

*그림 1-1*에서는 Sniffer Pro 의 주요 기능을 보여주고 있다.

: *모니터(monitor), 캡처(capture), 실시간 Expert 분석(real-time Expert analysis), 그리고 패킷 디스플레이(display)*

- 모니터는 실시간으로 네트워크 트래픽 데이터를 계산하고 화면에 표시.
- 캡처 기능은 네트워크 트래픽을 캡처하고 실제 데이터를 나중에 분석하기 위하여 버퍼에 (선택적으로 파일에) 저장.
- 실시간 Expert 분석 기능은 캡처하는 동안 네트워크 패킷들을 분석하고 네트워크에 잠재되어 있는 문제들을 경보하며, 이러한 문제들은 symptom 과/혹은 diagnoses 로 분류됨.
- 디스플레이 기능은 캡처 버퍼에 있는 패킷들을 디코드하고 분석하여 그 내용들을 다양한 형태로 화면에 표시.

2. 네트워크 모니터

Sniffer Pro 모니터(monitor)는 통계적인 측정 데이터와 당신의 네트워크 트래픽에 대한 계산치를 저장하고 네트워크 활동의 정확한 그림을 실시간으로 제공한다. 또한 에러가 검출되었을 경우, 당신에게 경보하기 위하여 알람을 생성할 수 있으며, 차후에 트래픽과 장비의 경함 상태를 분석 할 수 있도록 네트워크 활동 상태를 시간별로 저장할 수 있다.

모니터는 다음과 같은 종류의 정보를 제공한다.

- ◆ 일정 시간 간격으로 발생하는 네트워크 트래픽의 프레임/바이트 수, 활용도의 비율(%), 그리고 브로드케스트와 멀티케스트 개수를 포함하는 네트워크 부하에 대한 통계치.
- ◆ 다음 내용을 포함하는 네트워크 에러에 대한 통계치.
  - Ethernet ; CRC errors, runts, oversize packets, fragments, jabbers, alignment errors, collision counts.
  - Gigabit Ethernet; CRC errors, code violations errors, jabbers 및 runts.
  - Token Ring; Ring purge packets, beacon packets, NAUN changes, token errors, soft errors 등등.
  - ATM; CRC errors, length errors 및 timeout errors.
  - Wireless LAN; PLCP errors, length errors 및 timeout errors
- ◆ 프로토콜 사용에 대한 통계 자료.
- ◆ 상위 계층 프로토콜에 대한 어플리케이션 응답 시간 통계 자료.
- ◆ 개별적인 스테이션과 두 스테이션에 사이의 트래픽의 통계 자료
- ◆ 패킷 크기 분포에 대한 통계치

주 ---

네트워크 에러에 대한 통계를 관찰하기 위해서는 지원하는 전용 네트워크 인터페이스 카드(NIC)와 확장된 드라이버가 필요하다. 컴퓨터에 확장된 NDIS 드라이버를 설치하려면, Sniffer Pro 설치 가이드를 참조하라.

모니터에 의하여 수집된 데이터는 당신이 트래픽 과부하, 문제 해결의 장애 요인, 그리고 장애를 발생시키는 장비의 위치를 찾을 수 있도록 도와준다. 또한 그 데이터는 네트워크의 보수와 업그레이드를 위한 회사 리소스의 배치 방법을 결정하는데 중요한 요인이 될 수 있다.

모니터 필터

Sniffer Pro 는 모니터에 미리 정의된 필터들을 적용할 수 있도록 해 준다. 모니터에 적용한 필터는 모든 모니터 어플리케이션에 영향을 준다.

모니터 필터를 사용하여, 당신은 몇 가지 다른 시각으로 네트워크 트래픽을 관찰할 수 있다. 또한 네트워크 문제의 장애 분석에 필요한 데이터에 정밀한 초점을 맞출 수 있으며, 기록 자료를 위하여 수집하는 파일의 크기를 최소화 시킬 수 있다.

필터를 정의하는 방법에 관해서는 *제 5 장 필터와 트리거 정의하기*를 참조하자.

모니터 어플리케이션

모니터 어플리케이션을 이용하여 모니터 데이터를 화면에 표시할 수 있다. 모니터 어플리케이션은 Monitor 메뉴 아래에 목록화 되어 있으며, 또한 주 툴바에서도 사용할 수 있다(*그림 2-1*). 두 개의 특정 ATM 모니터 어플리케이션(Smart Screens, Switch Statistics)은 자신만의 고유한 툴바(*그림 2-1*)를 사용할 수 있으며, 이곳에 있는 Media Options 버튼은 ATM 분석을 위한 설정 옵션을 액세스하기 위하여 사용된다.

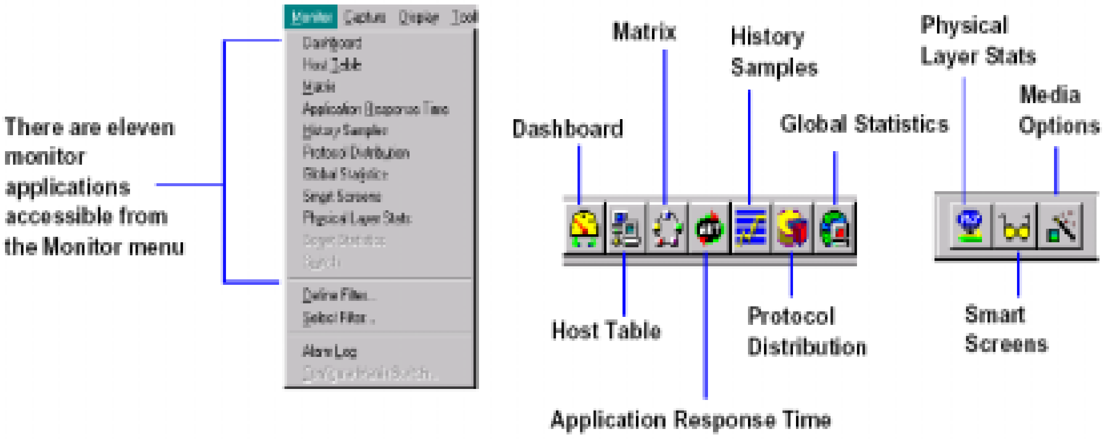


그림 2-1. 모니터 메뉴와 툴바 버튼 (Main 과 ATM)

주 --

모니터 어플리케이션을 사용하려면, 선택한 어댑터에 대한 " logged on" 상태이어야 한다. 만약 로그온 상태가 아니라면, Monitor 메뉴에 있는 모니터 어플리케이션 항목들이 비활성 상태로 보이며, 이것은 해당 항목들을 사용할 수 없음을 의미한다. Log ON 과 Log Off 옵션에 대한 내용은 *11 장, 네트워크 어댑터 설정하기*를 참조하자.

데쉬보드(Dashboard)

네트워크 세그먼트의 네트워크 사용량, 초당 패킷 전송률, 그리고 에러율을 실시간으로 화면에 표시하기 위하여 데쉬보드를 사용한다. 또한 히스토리에서 모니터 할 수 있는 시간별 에러 종류 및 개수, 전송된 패킷의 크기별 분포 등 다양한 종류의 네트워크 상황을 이곳에서 미리 관찰 할 수 있다.

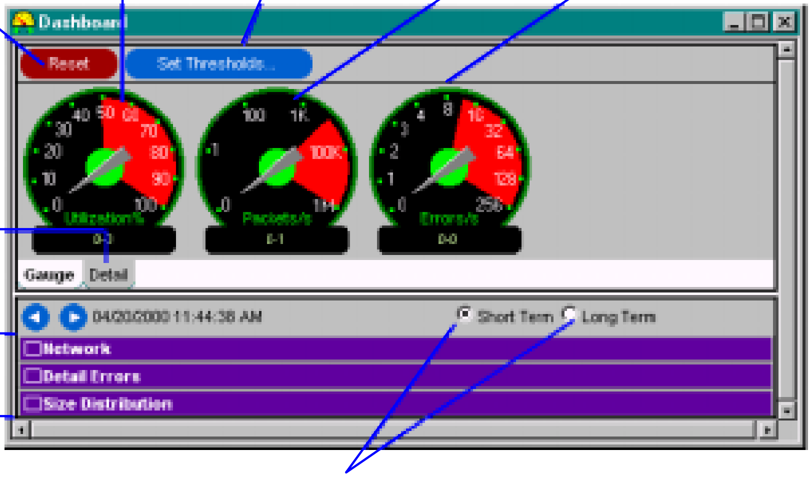
툴바에 있는 Dashboard 아이콘을 클릭하거나 **Monitor** 메뉴에서 **Dashboard** 를 선택하여 데쉬보드 화면을 나타나게 한다.

- 데쉬보드에서는 네트워크 사용량(utilization), 초당 패킷 전송률(packet rate), 초당 에러율(error rate)을 실시간으로 볼 수 있다.
- Detail 탭은 네트워크, 에러 및 패킷 크기 분포에 대한 통계자료를 제공한다.
- 연결된 토폴로지 별로 통계 자료를 수집하기 위하여 다양한 탭이 제공된다. 예를 들어, WAN 어댑터는 Options 대화 상자에서 선택할 수 있는 ‘ encapsulation’ 방법에 따라서 서로 다른 탭을 제공한다. (Frame Relay, HDLC, SDLC 등등)
- WAN 어댑터에서 상단의 “ LED” 들은 해당 선로의 상태를 표시하며, 보다 상세한 내용은 *Dashboard 의 선로 상태 표시기*를 참조하자.
- 네트워크, 에러 및 패킷 크기별 분포에 대한 통계 자료를 선 그래프로 제공한다.
- ATM 어댑터들은 **ATM** 탭을 제공한다. ATM Book 을 사용하고 있을 때, 데쉬보드에 있는 통계 자료들은 다양한 색상으로 나타난다. 파란색의 통계치는 Sniffer Pro PC 상에 있는 소프트웨어를 사용하여 계산된 것들이다.
- 네트워크 통계, 에러 통계 및 패킷 크기 분포에 대한 그래프를 사용자가 다양하게 구성할 수 있다.

누적된 상세한 통계 자료나 중요한 네트워크 파라미터에 대한 초당 평균의 통계치를 보기 위하여 여러 가지 다양한 탭을 사용할 수 있다. 실제 보이는 탭들은 현재 연결되어 있는 어댑터의 종류에 따라 다르다.

데쉬보드에 있는 각각의 항목들(뿐만 아니라 많은 네트워크 통계 자료들)을 위한 알람 임계 값을 설정할 수 있다. 임계 값이 증가되었을 때, 알람 로그에 있는 내용이 만들어진다. 네트워크를 지켜보기 위하여 그 알람 로그를 모니터 할 수 있다.

그림 2-2-1 은 Ethernet 어댑터를 위한 데쉬보드를 보여준다.



모든 카운터를 '0'으로 만들고자 한다면 Reset 을 클릭

네트워크 사용률

데쉬보드 통계자료에 대한 알람 임계값을 설정하려면 이 버튼을 클릭

초당 패킷수

초당 에러수

붉은색 영역은 알람 임계값을 설정한 부분

보다 상세한 통계자료를 보려면 이곳을 클릭

해당 통계자료에 대한 그래프를 보고자 한다면 이곳을 클릭

Network, Detail Errors 및 Size Distribution 그래프의 스케일을 좁게 또는 넓게 하려면 이 버튼을 선택

그림 2-2-1 . 데쉬보드 게이지

Dashboard 의 선로 상태 표시기

트래픽 관찰을 위해 WAN 네트워크 어댑터가 선택되면, 데쉬보드 상단에는 다양한 LED 표시기가 나타난다. 이 LED 들은 표준 RS-232 표시기인 RxC, TxC, RxD, TxD, CTS, RTS, DSR, DTR 및 Clock 을 사용하여 현재 연결된 선로의 상태를 보여준다.

Clock and Data LEDs (RxC, TxC, RxD 및 TxD)

- 황색 – 해당 선로에 신호가 존재함.
- 적색 – 해당 선로에 신호가 존재하지 않음.

Control LEDs (CTS, RTS, DSR, DTR)

- 연두색 – 해당 선로에 신호가 존재함.
- 적색 – 해당 선로에 신호가 존재하지 않음.

“ Clock” LED

- 연두색 – 클록이 존재함.
- 적색 – 클록이 없음. (예를 들어, 선이 연결되어 있지 않기 때문)

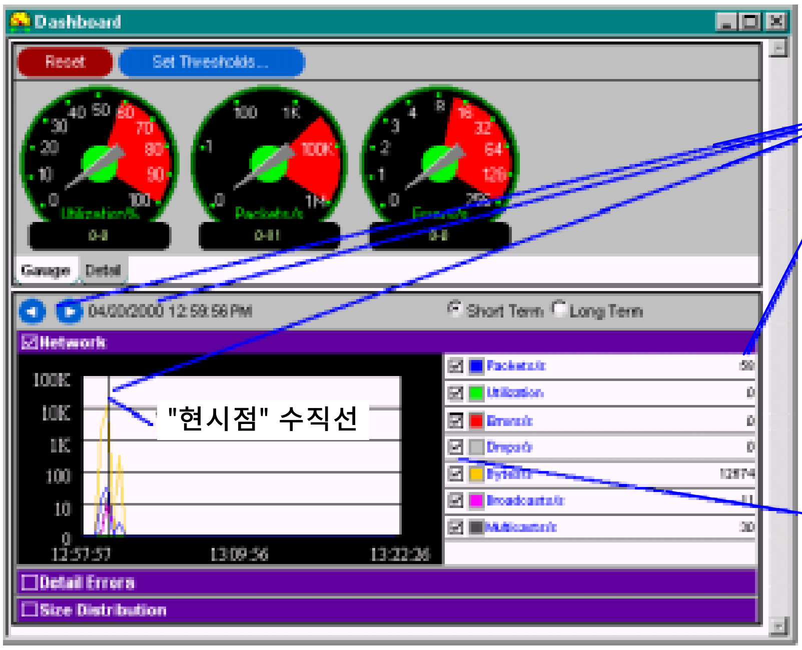
데쉬보드 그래프 관찰

데쉬보드는 또한 Detail 탭에서 볼 수 있는 아래의 3 가지 통계 자료에 대한 그래프들을 제공하며, 사용자의 욕구에 맞춰 구성할 수 있다.

- 네트워크 통계자료(Network statistics)
- 상세한 에러(Detail errors)
- 패킷 크기별 통계자료 (Size Distribution statistics)

원하는 통계자료의 그래프를 보려고 한다면 해당하는 4 각형 박스를 클릭한다. 그러면 선택된 통계자료에 해당하는 그래프가 데쉬보드 하단에 나타난다.

그림 2-2-2 는 Ethernet 어댑터에 대한 네트워크 통계 자료를 보여주고 있다. 네트워크 그래프 내에서 실질적으로 보여지는 통계자료는 선택된 어댑터에 따라 다르게 나타난다. (예를 들면, ATM 어댑터가 설치되어 있다면 Idle Cells, Congested Cells 등과 같은 항목이 그래프 내에 포함될 수 있다.)



"현시점" 수직선

그래프의 "현시점"을 이동시키려면 스크롤 버튼을 클릭한다. "현시점"을 나타내는 수직선이 이동하면 그래프의 우측에 해당 시간의 통계자료가 나타난다. 따라서 "현시점" 수직선을 좌우측으로 이동시키면서 원하는 시간의 통계 자료를 상세하게 볼 수 있다.

그래프 내에 포함시켜서 동시에 관찰하고 싶은 통계 자료는 이곳에서 선택한다.

그림 2-2-2. 사용자가 구성 가능한 데쉬보드 그래프

데쉬보드 그래프를 이용한 작업

데쉬보드에 있는 그래프를 이용하여 다음과 같은 작업을 할 수 있다.

- 그래프의 우측에는 해당 그래프들에 대한 통계자료가 목록으로 구성되어 있다. 통계자료 목록에서 있는 특정 항목에 대한 그래프를 보려고 한다면, 각 항목의 작은 박스를 클릭한다. 선택된 통계자료에 대한 그래프가 서로 다른 색으로 나타날 것이다.

- 선택된 통계자료에 대한 그래프를 다른 모습으로 보려고 한다면, 그래프 우측의 항목에서 원하는 부분에 마우스를 가져가면 대응되는 그래프가 굵게 보여진다.
- 또한 그래프에는 " 현시점(current)" 라고 하는 수직선을 포함하고 있다. 그래프의 우측에 있는 통계자료의 수치는 " 현시점" 수직선의 위치에 따라서 다르게 나타난다. 따라서 현시점 수직선을 다음과 같은 방법으로 이동시키면서 원하는 시간의 데이터를 관찰할 수 있다.

  - 그래프의 상단에 있는 화살표 버튼을 클릭한다.
  - 그래프 내에서 " 현시점" 수직선을 클릭하여 좌우로 이동시킨다.

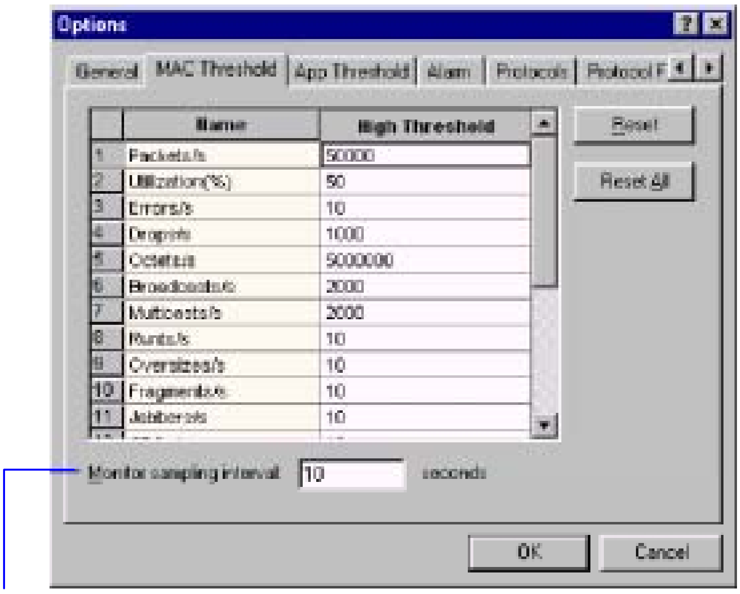
  현시점 수직선이 위치한 곳에 해당하는 시간과 날짜는 그래프 상단에 나타난다.
- 그래프 상단에 있는 Long term(확장)이나 Short term(축소) 버튼을 클릭하여 그래프의 시간 범위를 줄이거나 넓힐 수 있다.

데쉬보드 통계자료에 대한 임계값 설정

데쉬보드 상에서 관찰 가능한 각 항목들(뿐만 아니라 다른 많은 네트워크 통계 자료)에 대한 알람 임계값을 설정할 수 있다. 측정된 값이 임계값을 초과하면, 알람 로그 화면에 해당 정보가 등록된다.

임계 값을 설정하기 위해서는 데쉬보드(*그림 2-2-1*) 상단에 있는 Set Thresholds 버튼을 클릭하거나 Tools 메뉴에서 Options 을 선택하여 Mac Threshold 탭을 클릭한다.

지정된 임계 값을 초과했을 경우, 알람을 적용할 수 있는 여러 가지 네트워크 파라미터들의 목록을 볼 수 있다. 실질적인 파라미터들은 현재 연결되어 있는 어댑터에 따라 다르다. *그림 2-3*는 Ethernet 어댑터에 대한 네트워크 파라미터들을 보여주고 있다.



	Name	High Threshold
1	Packets/s	50000
2	Utilization(%)	50
3	Errors/s	10
4	Drops/s	1000
5	Octets/s	5000000
6	Broadcasts/s	2000
7	Multicasts/s	2000
8	Runts/s	10
9	Oversizes/s	10
10	Fragments/s	10
11	Jabbers/s	10

Monitor sampling interval 10 seconds

각 측정치에 대한 최대 임계값은 이곳에 지정된 시간 간격으로 초당 평균값으로 계산 된다.

그림 2-3. 임계 값 옵션 설정

호스트 테이블(Host Table)

호스트 테이블은 각 네트워크 노드의 트래픽 통계 자료를 실시간으로 수집한다.

- LAN 어댑터에 대해서, 호스트 테이블은 MAC, IP 네트워크, IP 어플리케이션, IPX 네트워크, 그리고 IPX 전송 계층 정보를 누적한다.
- ATM 어댑터에 대해서, 호스트 테이블은 또한 네트워크 상에서 검출된 연결 (PVC 와 SVC 모두)들을 목록으로 나타내는 ATXCNX 탭을 포함하고 있다.
- WAN 어댑터에 대해서, 호스트 테이블은 SDLC, LCN, DLCI, 또는 현재 Options 메뉴에서 선택된 캡슐화 프로토콜에 의존하는 HDLC 링크 계층 정보를 누적한다. 가능하다면 (Frame Relay 에 대해서는), 전송 계층 정보도 제공된다.

주 ---

호스트 테이블에서 계산되는 Frame Relay DLCI 들에 대한 CIR Utilization 통계 자료에 대한 정보는 *Frame Relay DLCI 들의 CIR 사용량에 대한 통계 자료*를 참조하자.

전송 계층 정보를 사용할 수 있을 경우, 특히 Frame Relay 를 위하여 그 정보가 제공된다. 호스트 테이블의 내용은 테이블, 막대 차트(bar chart), 파이형 차트(pie chart) 형태로 볼 수 있다.

- 테이블 형태는 각 네트워크 노드에 대하여 측정한 트래픽 통계 자료를 실시간으로 화면에 표시한다.

  - *Outline table* 은 각 네트워크 노드에서 송수신된 전제 바이트와 패킷들의 개략적인 내용을 제공한다.

  - *Detail table* 은 각 네트워크 노드에서 송수신된 트래픽 부하와 상위 계층 프로토콜 유형에 대하여 정리된 내용을 제공한다.

호스트 테이블의 열에 있는 제목을 클릭하여 내용을 정렬할 수 있다. (예를 들어, 입력된 패킷으로 통계 자료를 정렬하고 싶은 경우, 열에 있는 제목에서 In Pkts 을 클릭한다.) 제목을 두 번 클릭하면, 반대로 정렬된다.

- *막대 차트(bar chart)*는 가장 분주한 x 개의 호스트를 실시간으로 화면에 표시하며, x 는 사용자가 정의할 수 있는 수이다. (기본 값은 10)
- *파이형 차트(pie chart)*는 가장 분주한 x 개의 호스트를 전체 x 개의 트래픽 부하에 대한 상대적인 비율(%)로 화면에 표시한다. x 는 사용자가 정의할 수 있는 수이다. (기본 값은 10)

호스트 테이블의 툴바에 있는 (Properties) 버튼을 클릭하여 설정 내용(업데이트와 정

렬 간격, 그리고 막대와 파이 차트에 있는 최고 x 변수의 값 등)을 입력할 수 있다.

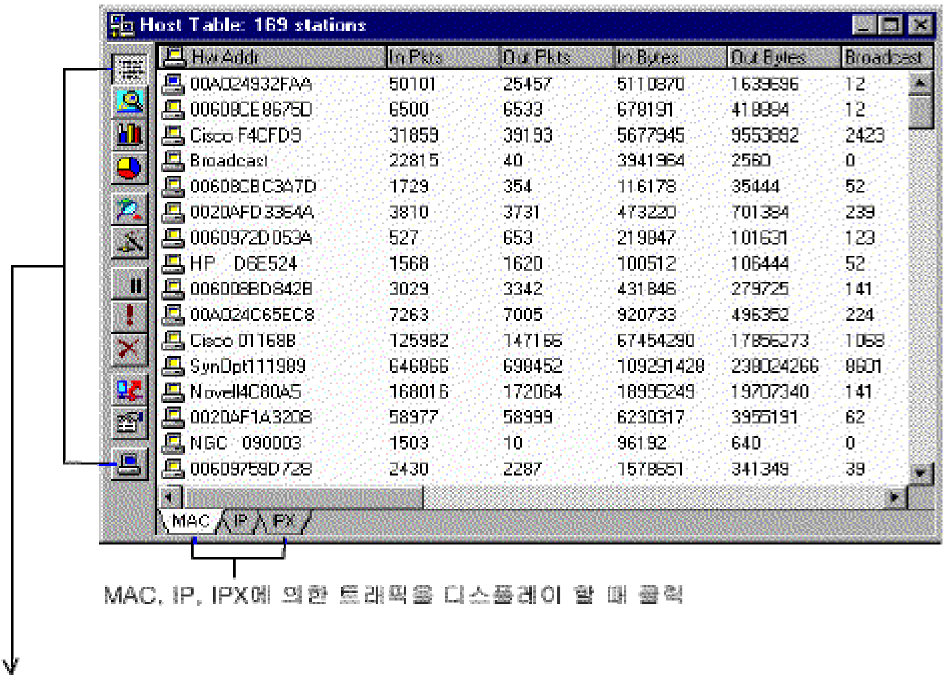
테이블에 있는 통계 자료들은 표와 차트로 변환할 수 있으며, 이러한 내용은 *모니터 데이터 변환하기(Exporting Monitor Data)*에서 설명한다.

단일 스테이션 기능

한 스테이션에서 출발하거나 그 스테이션으로 도착하는 데이터를 캡처 하기 위해서는 우측 테이블에 있는 해당 스테이션 아이콘을 클릭하고 좌측에 있는 버튼 가운데 버튼을 클릭한다. 보다 상세한 정보는 *특정 스테이션에서 캡처 하기(Capturing from Specific Stations)*를 참조하자.

단일 스테이션의 통계 자료를 화면에 표시하려면, 우측 테이블에 있는 해당 스테이션 아이콘을 클릭하고 좌측에 있는 버튼 가운데 버튼을 클릭한다. 단일 스테이션의 통계 자료를 트래픽 맵, 테이블, 막대 차트, 혹은 파이 차트로 볼 수 있다.

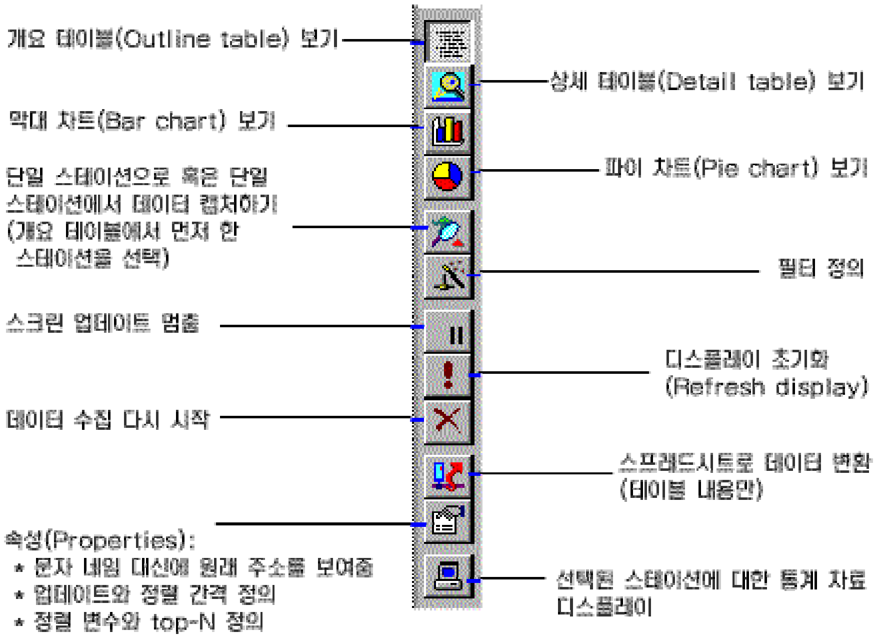
그림 2-4 는 Ethernet 어댑터에 대한 호스트 테이블을 보여주며, 호스트 테이블의 툴바를 설명하고 있다.



Host Table: 169 stations

Hw Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast
00A024932FAA	50101	25457	5110870	1639696	12
00608CE8675D	6500	6533	678191	418884	12
Cisco F4CFD9	31859	39193	5677945	9553892	2423
Broadcast	22815	40	3941964	2560	0
00608CBC3A7D	1729	354	116178	35444	52
0020AFD3364A	3810	3731	473220	701384	239
0060972D053A	527	653	219847	101631	123
HP D6E524	1568	1620	100512	106444	52
006008BD842B	3029	3342	431846	279725	141
00A024C65EC8	7263	7005	920733	496352	224
Cisco 01168B	125982	147166	67454290	17856273	1068
SynOpt111989	646866	698452	109291428	238024266	8601
Novell4C80A5	168016	172064	18995249	19707340	141
0020AF1A3208	58977	58999	6230317	3955191	62
NGC 090003	1503	10	96192	640	0
00609759D728	2430	2287	1578651	341349	39

MAC
IP
IPX
MAC, IP, IPX에 의한 트래픽을 디스플레이 할 때 클릭



개요 테이블(Outline table) 보기
상세 테이블(Detail table) 보기
막대 차트(Bar chart) 보기
파이 차트(Pie chart) 보기
단일 스테이션으로 혹은 단일 스테이션에서 데이터 캡쳐하기 (개요 테이블에서 먼저 한 스테이션을 선택)
필터 정의
스크린 업데이트 멈춤
디스플레이 초기화 (Refresh display)
데이터 수집 다시 시작
스프레드시트로 데이터 변환 (테이블 내용만)
속성(Properties):
* 문자 네임 대신에 원래 주소를 보여줌
* 업데이트와 정렬 간격 정의
* 정렬 변수와 top-N 정의
선택된 스테이션에 대한 통계 자료 디스플레이

그림 2-4. 호스트 테이블 (개요 테이블 보기)과 툴바

Frame Relay DLCI 들의 CIR 사용량에 대한 통계 자료

Options 대화 상자 내에서 **Encapsulation** 옵션이 **Frame Relay** 로 설정되면, 호스트 테이블은 Frame Relay 탭에서 검출된 각 DLCI 별로 **CIR Util(%)** 통계를 제공한다. **CIR Util(%)** 통계는 해당 DLCI 에 제공되는 DLCI 의 CIR(committed information rate)를 기준으로 사용자측에서 네트워크 측으로 전송된 비트 수를 나누어서 계산한다.

이러한 연산이 수행되려면, Sniffer Pro 가 해당 통계 값을 제공하기 위해서 각 DLCI 에 할당된 CIR 을 알고 있어야 한다. Sniffer Pro 는 아래와 같은 두 가지 방법으로 특정 DLCI 에 할당된 CIR 을 알 수 있다.

- 회선 관리 메시지(line management message)를 해석
- Options 대화 상자의 **Bandwidth** 탭에 설정된 값을 참조

주 ---

Bandwidth 탭에 새로운 값을 설정한 후에는 호스트 테이블의 **Frame Relay** 탭에 있는 사용량 통계 값에 새로 설정한 값이 적용되도록 적어도 한번은 Expert 모드에서 캡처를 시작하고 중지해야 한다.

Bandwidth 탭은 여러분의 Frame Relay 회선 상에서 서로 다른 DLCI 에 할당된 CIR (bandwidth) 값을 강제로 지정할 수 있게 한다. Sniffer Pro 는 회선 관리 메시지들을 (link management message) 해석하여 서로 다른 DLCI 에 할당된 대역폭을 검사한다. 그렇지만, 몇몇 회선 관리 프로토콜들(ITU-T 표준 Q.933 Annex A 와 ANSI 표준 T1.617, Annex D)은 회선 관리 메시지들의 일부에 대역폭 정보를 포함하고 있지 않다. 만약 여러분의 네트워크에서 대역폭 정보가 포함되어 있지 않는 회선 관리 메시지를 사용한다면, **Bandwidth** 탭 내에서 다른 DLCI 에 할당된 대역폭을 지정했는지 확인해야 한다.

아래와 같은 경우에는 호스트 테이블의 **Frame Relay** 탭에 있는 DLCI 에 대한 CIR 사용량 값 **N/A** 로 표시될 것이다.

- Sniffer Pro 가 해당 DLCI 에 대한 CIR 을 표시하는 회선 관리 메시지를 관측할 수 없는 경우.
- Options 대화 상자의 Bandwidth 탭에 수동으로 해당 DLCI 의 CIR 을 입력하지 않은 경우.

매트릭스(Matrix)

매트릭스는 네트워크 노드간의 대화에 대한 통계 자료를 실시간으로 수집한다.

- LAN 과 ATM 어댑터에 대해서, 매트릭스는 MAC, IP 네트워크, IP 어플리케이션, IPX 네트워크, 그리고 IPX 전송 계층 정보를 누적한다.
- WAN 어댑터에 대해서, 매트릭스는 SDLC, LCN, 가상 회선(Virtual Circuit), 또는 현재 Options 메뉴에서 선택된 캡슐화 프로토콜에 의존하는 HDLC 링크 계층 정보를 누적한다. 가능한 경우(Frame Relay)에는 전송 계층 정보가 제공된다.

매트릭스 데이터는 트래픽 맵(traffic map), 테이블, 막대 혹은 파이 차트(pie chart) 형태로 볼 수 있다.

- 트래픽 맵은 노드간의 네트워크 트래픽 패턴에 대한 개괄적인 관찰을 실시간으로 제공.
- 매트릭스 테이블 형태는 두 노드 쌍에 대해 측정한 트래픽 통계 자료를 화면에 표시.
  - *Outline table* 은 두 네트워크 노드 쌍에서 송수신된 전제 바이트와 패킷들의 개략적인 내용을 제공한다.
  - *Detail table* 은 두 네트워크 노드 쌍에서 송수신된 대화에 대한 트래픽 부하와 상위 계층 프로토콜 유형에 대하여 정리된 내용을 제공한다.

매트릭스 테이블의 열에 있는 제목을 클릭하여 내용을 정렬할 수 있다. (예를 들어, 패킷으로 통계 자료를 정렬하고 싶은 경우, 열에 있는 제목에서 Packets 항목을 클릭한다.) 제목을 두 번 클릭하면, 반대로 정렬된다.

- 막대 차트는 가장 분주한 x 개의 대화 노드 쌍을 실시간으로 화면에 표시하며, x 는 사용자가 정의할 수 있는 수이다. (기본은 10)
- 파이 차트는 가장 분주한 x 개의 대화 노드 쌍을 전체 x 개의 트래픽 부하에 대한 상대적인 비율(%)로 화면에 표시한다. x 는 사용자가 정의할 수 있는 수이다.(기본은 10)

매트릭스 툴바에 있는 버튼을 클릭하여 설정 내용(트래픽 맵에 사용되는 색상, 막대와 파이 차트에 있는 최고 x 변수의 값, 그리고 업데이트와 정렬 간격 등)을 입력할 수 있다.

테이블에 있는 통계 자료들은 표와 차트로 변환할 수 있으며, 이러한 내용은 *모니터 데이터 변환하기(Exporting Monitor Data)*에서 설명한다.

특정 스테이션 기능

두 특정 스테이션 간의 데이터를 캡처 하기 위해서는 트래픽 맵 혹은 outline 테이블에 있는 스테이션 가운데 하나를 클릭한 후, 매트릭스 테이블 좌측에 있는 버튼 가운데 버튼을 클릭한다. 보다 상세한 정보는 있는 *특정 스테이션에서 캡처 하기(Capturing from*

*Specific Stations)*를 참고하자.

그림 2-5 는 Ethernet 어댑터에 대한 매트릭스 바 차트를 보여주며, 매트릭스 툴바를 설명하고 있다.

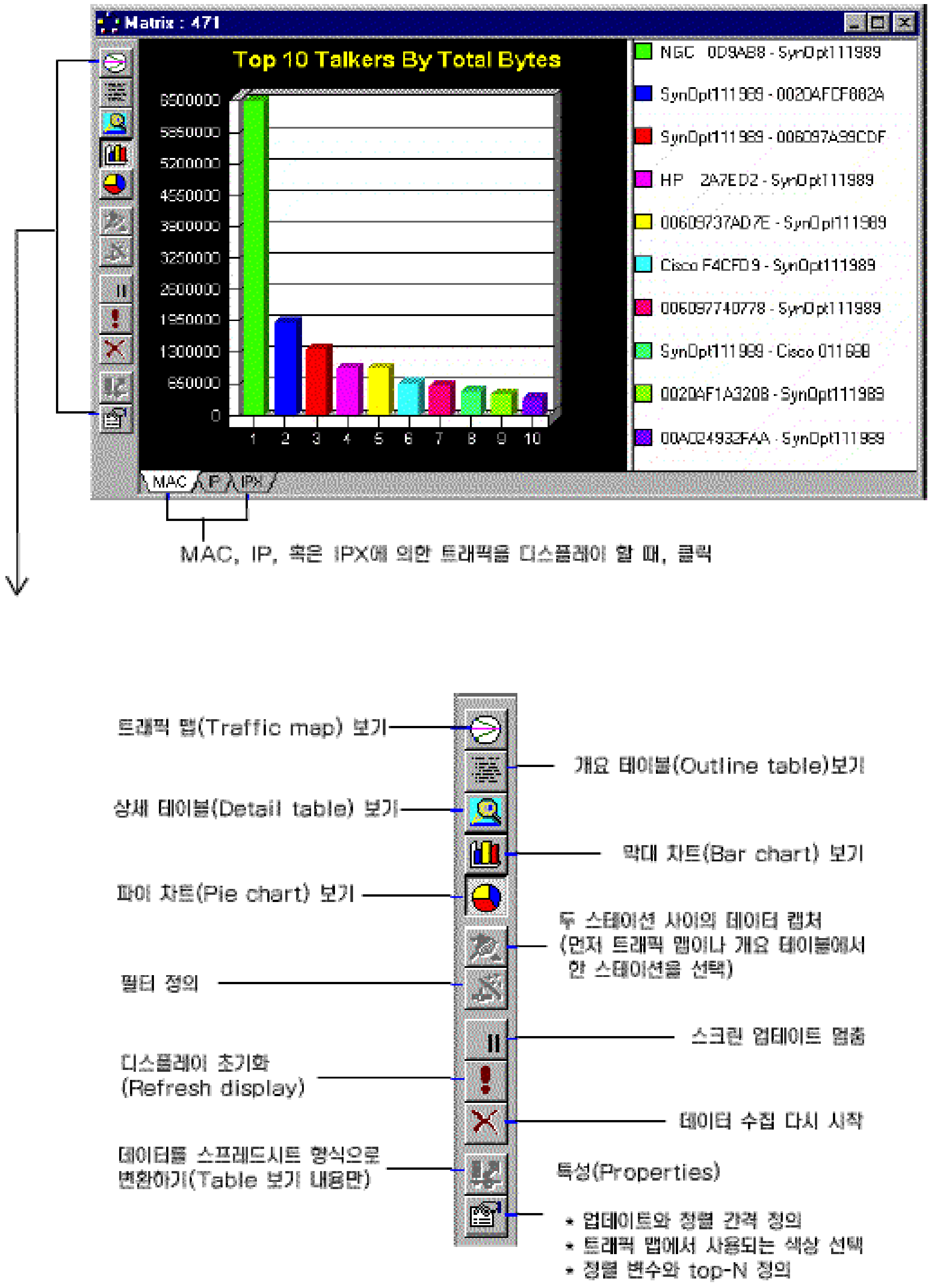

Matrix : 471
Top 10 Talkers By Total Bytes
6500000
5850000
5200000
4550000
3900000
3250000
2600000
1950000
1300000
650000
0
1
2
3
4
5
6
7
8
9
10
🟩 NGC 0D9AB8 - SynOpt111989
🟦 SynOpt111989 - 0020AFCF882A
🟥 SynOpt111989 - 006097A99CDF
🟪 HP 2A7ED2 - SynOpt111989
🟨 00608737AD7E - SynOpt111989
🟦 Cisco F4CFD9 - SynOpt111989
🟥 006097740778 - SynOpt111989
🟩 SynOpt111989 - Cisco 011698
🟩 0020AF1A3208 - SynOpt111989
🟪 00A024932FAA - SynOpt111989
MAC
IP
IPX
MAC, IP, 혹은 IPX에 의한 트래픽을 디스플레이 할 때, 클릭
트래픽 맵(Traffic map) 보기
개요 테이블(Outline table)보기
상세 테이블(Detail table) 보기
막대 차트(Bar chart) 보기
파이 차트(Pie chart) 보기
두 스테이션 사이의 데이터 캡처
(먼저 트래픽 맵이나 개요 테이블에서
한 스테이션을 선택)
필터 정의
스크린 업데이트 멈춤
디스플레이 초기화
(Refresh display)
데이터 수집 다시 시작
데이터를 스프레드시트 형식으로
변환하기(Table 보기 내용만)
특성(Properties)
• 업데이트와 정렬 간격 정의
• 트래픽 맵에서 사용되는 색상 선택
• 정렬 변수와 top-N 정의

그림 2-5. 매트릭스 (막대 차트)와 툴바

어플리케이션 응답 시간(ART, Application Response Time)

ART(Application Response Time) 모니터 어플리케이션은 잘 알려진 TCP/UDP 포트로(예를 들어, HTTP, Telnet, SNMP 등) 연결된 서버와 클라이언트들 사이의 어플리케이션에 대한 응답시간을 실시간으로 측정하고 리포트 한다. 응답시간은 Sniffer Pro 에서 관측되는 요청(request)과 응답(response) 사이의 시간 간격으로 측정된다.

ART 를 실행시키면, 테이블 형식으로 응답시간 정보가 화면에 표시된다. 그렇지만, client-server response time 막대 차트 및 server response time 막대 차트 의 형식으로도 다른 어플리케이션에 대한 응답 시간을 관찰할 수 있다.

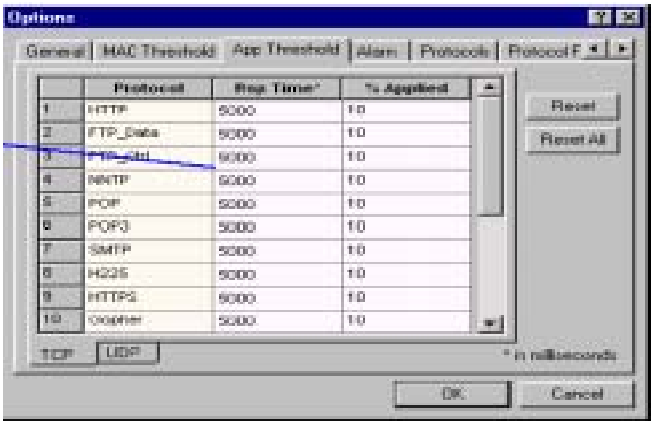
- 테이블 형식의 목록에 있는 내용은 어플리케이션 계층의 연결에 대한 서버 및 클라이언트의 주소, 해당 연결에 대한 응답 시간의 상세한 분포, 전체 트래픽 통계량(server bytes, client octets, retries 및 timeout) 정보를 보여준다.

  ART 는 프로토콜에 의해서 연결을 구성한다. ART Options 대화 상자(ART 창에 있는 Properties 버튼을 클릭하여 볼 수 있는)의 **Display Protocols** 탭에서 사용자가 선택한 각 프로토콜은 ART 창의 하단에 각각의 탭을 가지고 있다. 따라서 ART 창의 하단에서 적절한 탭을 클릭하여 다른 어플리케이션에 대한 연결 상태를 볼 수 있다.
- **Client-Server Response Time** 막대 차트는 ART Options 대화 상자의 **Server-Client** 탭에서 설정한 옵션들에 따라 Server-Client pair 들의 상태를 그래프로 표시한다. 이 옵션들에는 몇 개의 pair 를 그래프에 표시할 것인가와 정렬 방식 및 화면 표시 방법들이 포함되어 있다.
- **Server Response Time** 막대 차트는 ART Options 대화 상자의 **Server Only** 탭에서 설정한 옵션들에 따라 Server 들의 상태를 그래프로 표시한다. 이 옵션에도 몇 개의 pair 를 그래프에 표시할 것인가와 정렬 방식 및 화면 표시 방법들이 포함되어 있다.

ART 알람

어플리케이션 응답시간을 관측하고 수집된 정보를 화면에 표시함과 더불어 ART 는 또한 검출된 어플리케이션 응답 시간이 Options 대화 상자 내의 App Threshold 에 지정된 임계값보다 늦어지는 경우에 알람을 생성한다.

ART 어플리케이션에 의해서 생성되는 알람의 임계값들은 *그림 2-6* 에 보인 Options 대화 상자의 **App Threshold** 탭에서 설정한다.



	Protocol	Rsp Time*	% Applied
1	HTTP	5000	10
2	FTP_Data	5000	10
3	FTP_Ctrl	5000	10
4	NNTP	5000	10
5	POP	5000	10
6	POP3	5000	10
7	SMTP	5000	10
8	H225	5000	10
9	HTTPS	5000	10
10	Gopher	5000	10

* in milliseconds

이곳에 임계값을
지정한다.

그림 2-6. ART 알람들을 위한 임계값 설정

App Threshold 탭은 ART 어플리케이션에 의해 모니터 되는 어플리케이션을 각 행에 포함하고 있다. TCP 나 UDP 에 의해서 구성되는 프로토콜들이 목록에 있다.

각 프로토콜에 대한 Rsp Time 과 % Applied 필드:

- Rsp Time 값은 어느 시점에서 해당 프로토콜이 " slow" 로 처리되는가를 지정한다. 예를 들어, 만약 HTTP 에 대한 Rsp Time 이 5000msec 로 설정되었다면, 어떤 HTTP 요청에 대한 응답 시간이 5000msec 보다 길다면, " slow" 로 처리될 것이다. 주어진 Server-Client 접속에 대한 " slow" 응답 비율이 % Applied 임계값을 초과한다면, 모니터는 해당 접속에 대해서 알람을 생성한다.
- % Applied 값은 특정 프로토콜을 사용하여 접속된 상황에서 Rsp Time 임계값을 초과한 응답이 발생했을 때, 전체 응답 시간에 대해 수용 가능한 최대 비율을 의미한다. 주어진 Server-Client 접속에서 Rsp Time 임계값을 초과한 응답의 비율이 % Applied 에 지정한 값을 초고하면, 모니터는 해당 접속에 대해서 알람을 생성한다.

생성된 알람은 알람 로그에 등록된다. 특정한 알람이 발생했을 때, 취해야 할 동작에 대해서는 Option 대화 상자의 Alarms 탭에서 설정한다. 이와 관련된 내용은 *7 장: 알람 관리*를 참조하자.

그림 2-7 은 현재 네트워크에서 HTTP 에 대한 서버의 어플리케이션 응답시간의 분포를 막대 그래프 형식으로 보여주고 있다.

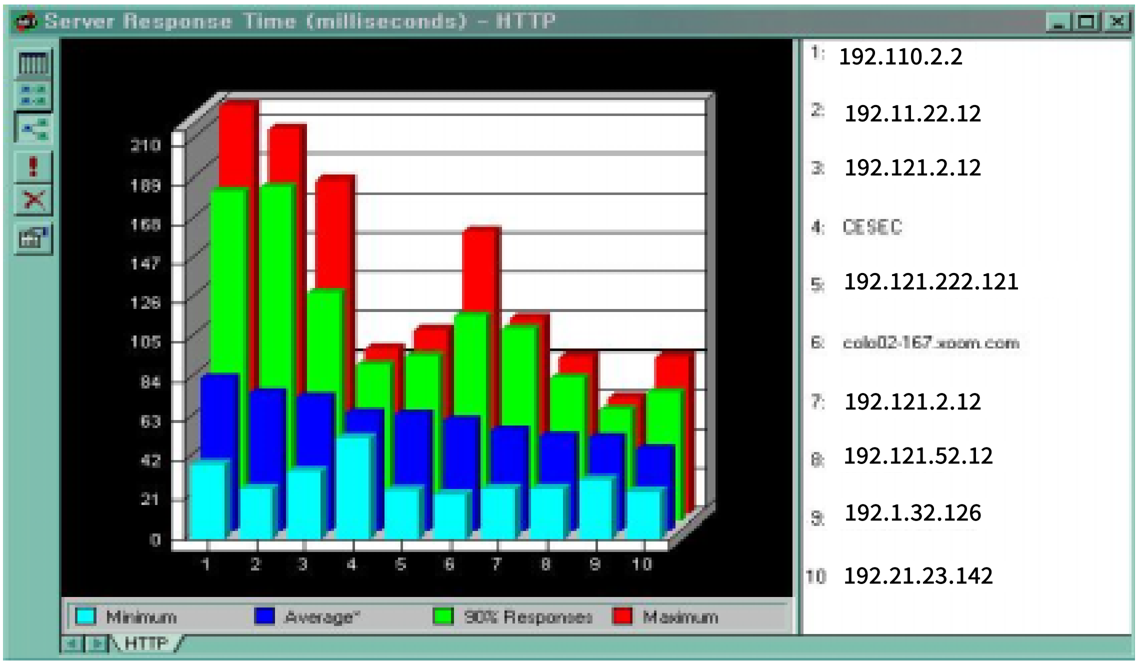


그림 2-7. 서버들의 어플리케이션(HTTP) 응답시간

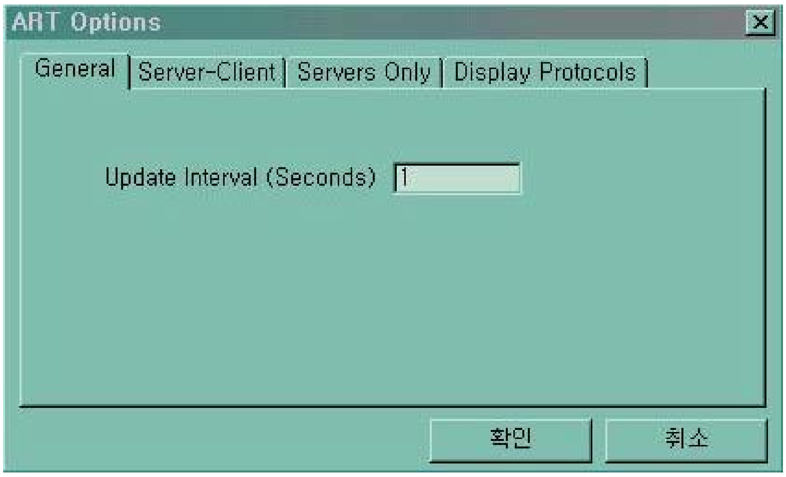
- *그림 2-7* 의 좌측에 있는 툴바에서 ▦ 버튼은 각 클라이언트와 서버 사이의 응답시간 분포를 각 서버와 클라이언트의 주소와 함께 전체적인 트래픽 통계 자료를 정리하여 테이블 형식으로 보여 준다. (server bytes, client octets, retries 및 timeouts)

  ART 는 프로토콜들에 의해서 접속이 구성된다. ART Option 대화 상자(ART 윈도우에서 Properties 버튼을 클릭) 내의 Display Protocols 탭에서 프로토콜을 선택하면 ART 화면의 하단에 각 프로토콜에 대한 탭이 생성된다. 따라서 ART 윈도우의 하단에 있는 탭 가운데 원하는 프로토콜에 해당하는 탭을 선택하여 다른 프로토콜 접속을 관찰할 수 있다.

- 버튼은 Server-Client Response Time 을 관찰하기 위한 것이며, 특정 클라이언트와 서버간의 통신 상태에서 응답시간의 분포를 막대 차트로 보기 위해서 클릭한다. ART Option 대화 상자의 Server-Client 탭을 클릭하여 화면에 표시되는 내용을 구성할 수 있다. 이곳에 나타나는 클라이언트 서버 목록은 응답시간이 가장 늦은 10 개의 쌍이 될 수도 있고, 응답시간이 가장 빠른 10 개의 쌍이 될 수도 있다. 또한 나타나는 클라이언트/서버 쌍의 개수도 사용자가 임의로 지정할 수 있다.

- 버튼은 Server Response Time 을 관찰하기 위한 것이며, 특정 서버의 전체 응답시간의 분포를 막대 차트로 보기위해 클릭한다. 앞에서와 마찬가지로 ART Option 대화 상자의 Server-Client 탭을 클릭하여 화면에 표시되는 내용을 구성할 수 있다.

- 밑에 있는 두개의 버튼은 각각 Refresh 및 Reset 기능을 수행하는 아이콘들이다. 좌측 툴바의 끝에 있는 아이콘은 ART 화면의 구성을 바꾸기 위한 Properties 아이콘이며, 이 버튼을 클릭하면 *그림 2-8*과 같은 ART Options 대화 상자가 나타난다.



ART Options

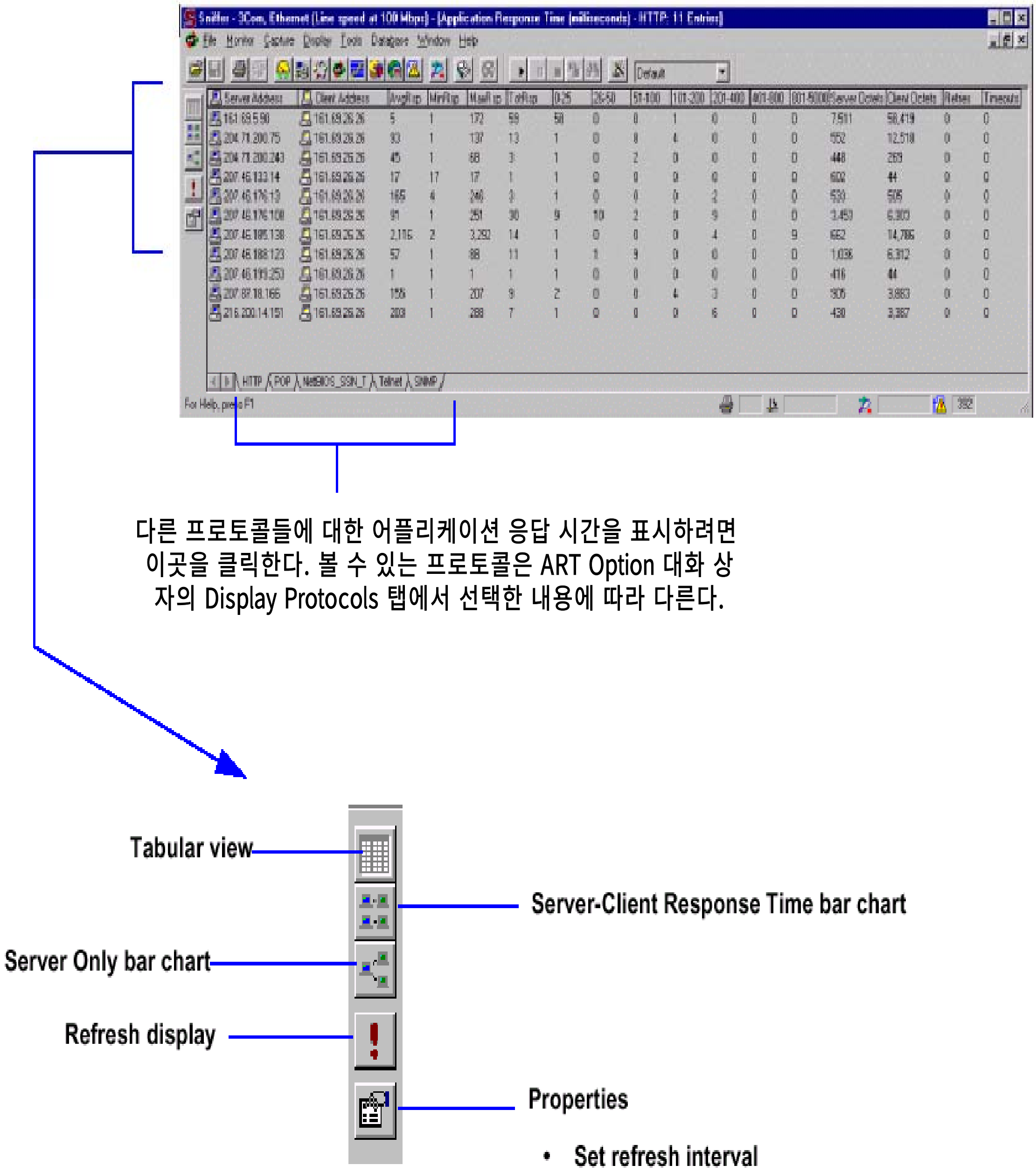
General | Server-Client | Servers Only | Display Protocols

Update Interval (Seconds) 1

그림 2-8. ART Options 대화 상자

- ART 옵션의 General 탭에서는 업데이트 간격을 조절할 수 있다.
- Server-Client 탭에서는 Server-Client Response Time 화면의 구성을 설정하고, Server Only 탭에서는 Server Response Time 화면의 구성을 설정할 수 있다.
- Display Protocols 탭에서는 각 화면에 표시되는 어플리케이션 프로토콜의 종류를 선택할 수 있으며, 이곳에서 ‘x’ 표시가 된 어플리케이션 프로토콜들은 ART 화면의 하단에 자신 만의 탭을 갖게 된다.
  - 이곳에 등록된 프로토콜들은 사용자가 추가 할 수 있으며, 새로운 프로토콜을 추가하기 위해서는 **Tools/Options** 메뉴를 선택했을 때 나타나는 **Options** 대화상자의 Protocols 탭에서 해당 프로토콜을 추가하면 된다.

*그림 2-9*는 테이블 형식으로 표시된 ART 윈도우를 보여주고 있다.



Sniffer - 3Com, Ethernet (Line speed at 100 Mbps) - [Application Response Time (milliseconds) - HTTP: 11 Entries]

Server Address	Client Address	AvgRsp	MinRsp	MaxRsp	TotRsp	0-25	26-50	51-100	101-200	201-400	401-800	801-5000	Server Octets	Client Octets	Retries	Timeouts
161.69.5.90	161.69.26.26	5	1	172	59	58	0	0	1	0	0	0	7,511	58,419	0	0
204.71.200.75	161.69.26.26	93	1	137	13	1	0	8	4	0	0	0	552	12,518	0	0
204.71.200.243	161.69.26.26	45	1	68	3	1	0	2	0	0	0	0	448	269	0	0
207.46.133.14	161.69.26.26	17	17	17	1	1	0	0	0	0	0	0	602	44	0	0
207.46.176.13	161.69.26.26	165	4	246	3	1	0	0	0	2	0	0	530	505	0	0
207.46.176.108	161.69.26.26	91	1	251	30	9	10	2	0	9	0	0	3,453	6,303	0	0
207.46.185.138	161.69.26.26	2,116	2	3,292	14	1	0	0	0	4	0	9	662	14,786	0	0
207.46.188.123	161.69.26.26	57	1	88	11	1	1	9	0	0	0	0	1,036	6,312	0	0
207.46.199.253	161.69.26.26	1	1	1	1	1	0	0	0	0	0	0	416	44	0	0
207.87.18.166	161.69.26.26	156	1	207	9	2	0	0	4	3	0	0	906	3,863	0	0
216.200.14.151	161.69.26.26	203	1	288	7	1	0	0	0	6	0	0	430	3,387	0	0

다른 프로토콜들에 대한 어플리케이션 응답 시간을 표시하려면 이곳을 클릭한다. 볼 수 있는 프로토콜은 ART Option 대화 상자의 Display Protocols 탭에서 선택한 내용에 따라 다른다.

- Set refresh interval
- Set display options for bar charts
- Specify display protocols

그림 2-9. ART 화면과 Toolbar

ART 화면에 다른 프로토콜 추가하기

다른 모든 모니터 어플리케이션에 프로토콜을 추가하는 방법과 동일하게 ART 화면에도 다른 프로토콜을 추가할 수 있다. 아래 과정에 따라서 새로운 프로토콜을 추가해 보자.

==

ART 화면에 다른 프로토콜 추가

1. **Tools** 메뉴에서 **Options** 명령을 선택하여 Options 대화 상자를 나타나게 한다.
2. Options 대화 상자에서 **Protocols** 탭을 클릭한다.
3. Protocols 탭은 새로운 상위 계층 프로토콜들을 모니터하기 위해서 추가(또는 기존 상위 계층 프로토콜들과 관련된 포트 번호들을 교체)할 수 있는 곳이다.
   - 만약 TCP 상에서 동작하는 프로토콜을 추가하려고 한다면, Protocols 탭의 하단에 있는 TCP 탭을 클릭한다.(default)
   - 만약 UDP 상에서 동작하는 프로토콜을 추가하려고 한다면, Protocols 탭의 하단에 있는 UDP 탭을 클릭한다.

주 ---

ART 는 IPS 상에서 동작하는 프로토콜들에 대한 모니터를 지원하지 않는다.

----

4. 하단쪽으로 스크롤 하여 **Name** 셀을 클릭한다. Sniffer 화면에서 표시되는 프로토콜의 이름을 입력한다.
5. Port 셀을 클릭하고 Sniffer Pro 가 해당 프로토콜을 위해서 관찰해야 하는 포트 번호를 입력한다.
6. OK 를 클릭한다. Sniffer Pro 는 수정된 내용을 적용하기 위해서 해당 어플리케이션을 재 시작할 것을 요구한다. 해당 어플리케이션을 다시 시작한다.
7. **Monitor** 메뉴에서 **Application Response Time** 명령을 선택하여 ART 화면을 표시한다.
8. ART Options 대화 상자를 나타나게 하기 위해서 **Properties** 버튼을 클릭한다.
9. ART Options 대화 상자에서 **Display Protocols** 탭을 클릭한다.
10. **Display Protocols** 탭의 하단에 있는 **TCP** 나 **UDP** 탭을 클릭한다. 이곳에 있는 프로토콜 종류는 위의 **3 단계**에서 추가된 프로토콜의 종류에 따라 다르게 나타난다.
11. 앞에서 추가된 프로토콜을 확인하기 위해서 화면을 아래쪽으로 스크롤 하자. 추가된 프로토콜을 ART 화면에 추가하기 위해서 옆에 있는 작은 상자를 클릭한다.
12. ART Options 대화 상자에서 OK 를 클릭한다. ART 어플리케이션은 ART 화면을 닫고 다시 실행해야 한다고 확인 메시지를 보여준다. **Yes** 를 클릭하여 화면을 닫고 다시 열도록 하자.
13. ART 화면은 추가된 새로운 프로토콜 탭을 하단에 추가하여 다시 나타난다.

히스토리 샘플(History Samples)

네트워크 성능에 대한 기초 자료를 작성하기 위하여 일정 시간 동안에 다양한 네트워크 통계 자료를 수집하는 히스토리 샘플을 사용할 수 있다.

기반 네트워크 통계 자료는 비정상적인 네트워크 상태가 발생할 때, 그 상태를 경고하도록 알람 임계 값을 설정하는데 도움이 된다. 또한 히스토리 샘플은 장기간 네트워크의 경향을 분석하는데 사용할 수 있으며, 차후에 네트워크를 확장하고 구성하는 계획에 도움이 될 수도 있다.

동시에 10 개 정도의 히스토리 샘플 처리 과정을 시작할 수 있다. 이러한 샘플은 10 개의 서로 다른 샘플이 되거나, 단기간 그리고 장기간 경향이 동시에 저장될 수 있도록 동일한 샘플의 다중 인스턴트가 될 수도 있다.

히스토리 샘플을 모니터하기 위하여 사용할 수 있는 네트워크 이벤트는 Adapter 대화 상자에서 선택했던 어댑터의 유형에 따라 다양하다. 예를 들어, 토큰 링 네트워크를 모니터 할 때, 다양한 유형의 토큰 링 프레임(예: 탐지 프레임(beacon frames)) 히스토리 샘플을 수집할 수 있다. Frame Relay 네트워크를 모니터 할 때, 다양한 유형의 Frame Relay 프레임(예: LMI 프레임) 히스토리 샘플을 수집할 수 있다. 또한 ATM 네트워클 모니터 할 때, 서로 다른 셀 유형의 히스토리 샘플을 수지할 수 있다.

샘플 데이터는 막대 차트, 선 차트, 영역 차트 등으로 화면에 표시될 수 있다. *그림 2-10* 은 Ethernet 어댑터에 대한 히스토리 샘플을 보여준다.

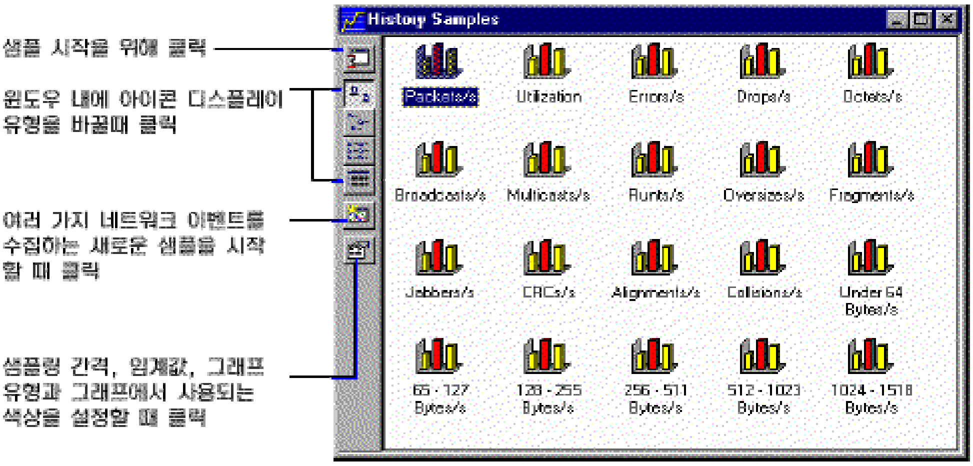
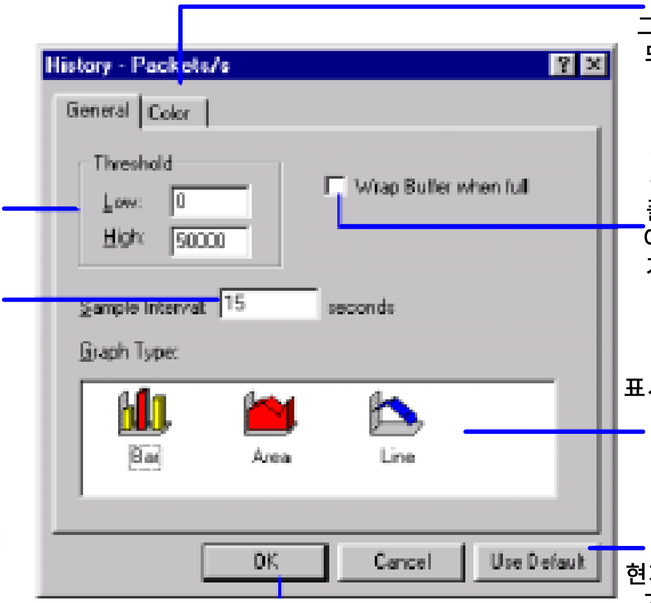


그림 2-10. 히스토리 샘플 윈도우

샘플을 시작하기 전에 샘플링 간격, 상위와 하위 임계 값, 그래프 유형 그리고 그래프에 사용되는 색상을 설정한다. 먼저 히스토리 샘플 윈도우에서 사용하려고 하는 샘플을 선택한다. 그 다음 좌측에 있는 버튼 가운데 (Properties) 버튼을 클릭한다. History properties 대화 상자는 *그림 2-11*에서 보였다.


History - Packets/s

Threshold
Low: 0
High: 90000

☐ Wrap Buffer when full

Sample Interval: 15 seconds

Graph Type:

그래프에서 사용되는 색상 선택

최대 3,600개의 샘플이 수집되었을 경우, 최신 샘플을 계속 수집하여 기존 데이터에 겹겹쳐서 저장 하려고 할 때, 여기를 클릭

표시할 그래프의 유형 선택

현재 설정된 정보를 기본값으로 저장

설정한 내용을 저장

임계값 입력

샘플 간격 입력 (Sniffer는 최대 3,600개의 샘플을 유지한다. 만일 이곳에 15를 입력하면, 15초 간격으로 최대 3,600개의 샘플이 추출되므로 총 15시간 동안의 정보를 관찰할 수 있다.)

그림 2-11. 히스토리 샘플 설정 정보 구성하기.

트래픽을 관찰하는 동안 특정 부분의 화면을 확대하기

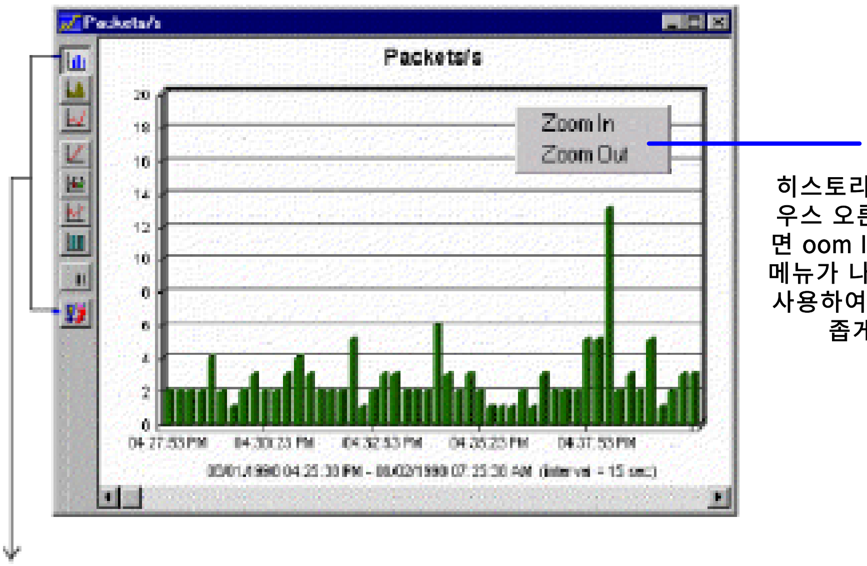
히스토리 샘플 화면에서 데이터를 수집하여 표시하는 동안 특정 부분의 샘플만 집중적으로 관찰하기 위해서 Zoom In \ Zoom Out 화면 메뉴 옵션을 사용할 수 있다. 이 옵션을 사용하여 화면에 표시되는 데이터 구간을 바꾸면 사용자는 짧은 시간 동안의 샘플를 관찰하거나, 장시간의 경향을 관찰할 수 있다.

Zoom In \ Zoom Out 메뉴는 히스토리 샘플들의 그래프가 표시되고 있는 화면의 어느 곳에서나 마우스 오른쪽 버튼을 클릭하면 나타나고, 해당 화면에서 원하는 옵션을 선택한다. *그림 2-12* Packets/s 히스토리 샘플 화면에 Zoom In \ Zoom Out 메뉴가 보이고 있다.

Wrap Buffer when full 옵션이 선택되어 있지 않다면, 최대 샘플 개수가 모두 수집되면, 히스토리 샘플 화면은 자동적으로 중지할 것이다. 더불어서 히스토리 화면을 닫으면 히스토리 샘플 화면도 자동적으로 중지하게 된다.

히스토리 샘플에 대한 데이터는 테이블 형식의 텍스트 파일이나 화면 그대로의 내용으로 저장할 수 있다. 보다 상세한 내용은 *모니터 데이터 변환하기*를 참조하자.

그림 2-12 에서는 막대 차트의 형태로 Packets/s 히스토리 샘플을 보여주며, 툴바를 설명하고 있다.



히스토리 샘플 화면에서 마우스 오른쪽 버튼을 클릭하면 oom In/Zoom Out 화면 메뉴가 나타난다. 이 메뉴를 사용하여 화면을 넓게 또는 좁게 볼 수 있다.

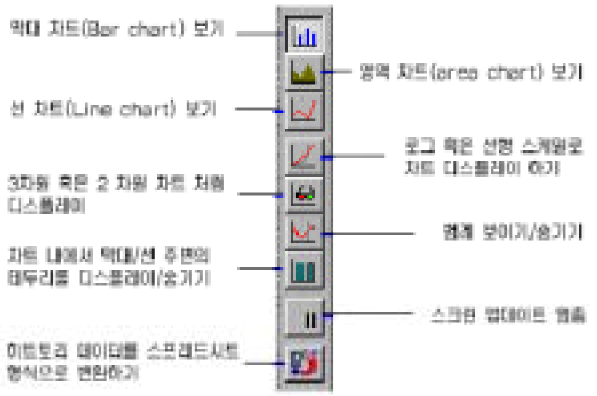
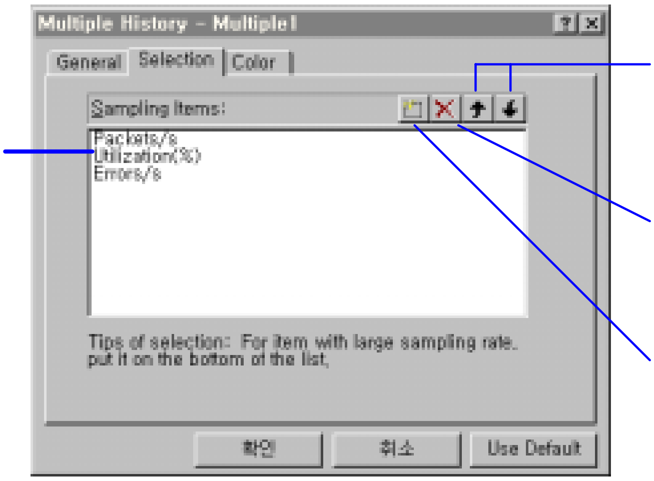

막대 차트(Bar chart) 보기
영역 차트(area chart) 보기
선 차트(Line chart) 보기
로그 혹은 선형 스케일로 차트 디스플레이 하기
3차원 혹은 2 차원 차트 처럼 디스플레이
범례 보이기/숨기기
차트 내에서 막대/선 주변의 테두리를 디스플레이/숨기기
스크린 업데이트 멈춤
히스토리 데이터를 스프레드시트 형식으로 변환하기

그림 2-12. 히스토리 샘플(Packets/s 막대 차트)과 툴바

다중 히스토리 샘플 화면 구성하기

여러 가지 항목의 히스토리 샘플들을 서로 비교하기 위해서 한 화면에 구성할 수 있다. 다중 히스토리 샘플 화면을 구성하려면, 먼저 Multiple History 대화 상자에서 필요한 항목을 선택 또는 삭제해야 한다. 히스토리 샘플 주 화면의 좌측 하단에 있는 Add Multiple History 버튼을 클릭하여 필요한 대화 상자를 화면에 나타나게 한다. 그림 2-13 은 Multiple History 대화 상자이다.

다중 히스토리 샘플 화면에 포함되는 통계 자료 항목들이 이곳에 표시됨



Sampling Items:

Packets/s
Utilization(%)
Errors/s

Tips of selection: For item with large sampling rate, put it on the bottom of the list.

화면에 표시되는 각 샘플 통계 자료의 순서(위치)를 바꾸려면 이 버튼을 사용.

선택된 통계 자료를 삭제하려면 이 버튼을 클릭

추가 하고자 하는 새로운 통계 자료 항목이 있으면 이 버튼을 클릭하여 해당 대화 상자에서 선택

그림 2-13 Multiple History 대화 상자

*그림 2-13*에서 볼 수 있듯이 Multiple History 대화 상자에는 3개의 탭이 있다. General과 Color 탭은 *그림 2-11* 에서 설명한 것과 동일하다. Selection 탭에서는 다중 히스토리 화면에 추가할 통계 자료 항목들을 선택할 수 있으며, 화면 표시되는 방법도 설정할 수 있다. 일반적으로 목록의 제일 하단에는 샘플의 크기가 큰 것을 놓아야 화면에서 뒷부분에 표시될 것이다.

Multiple History Sample 구성을 마친 후, OK를 클릭하면, 히스토리 샘플 주 화면의 하단에 새로 추가된 다중 히스토리 아이콘이 지정된 이름으로 추가된다.

프로토콜 분포(Protocol Distribution)

프로토콜 분포는 네트워크의 전송 그리고 어플리케이션 계층 프로토콜에 기반을 둔 네트워크 사용 현황을 알아보기 위하여 사용할 수 있다. 예를 들어, IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan, 그리고 많은 다른 프로토콜들을 모니터 할 수 있다.

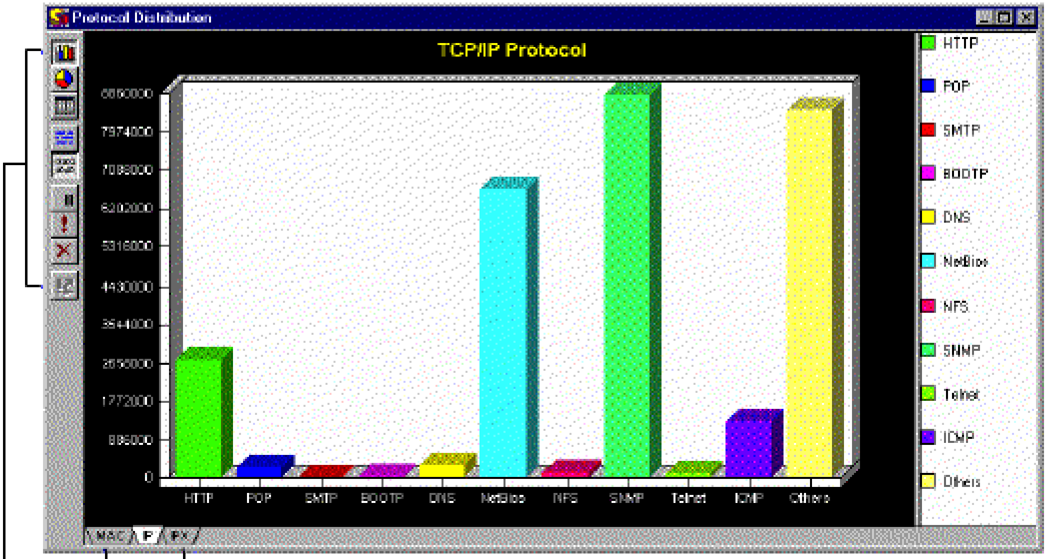
프로토콜 분포는 NFS, FTP, Telnet, SMTP, POP2, POP3, HTTP(WWW), Gopher, NNTP, SNMP, X-Windows, 등 대중적인 IP 어플리케이션을 모니터 한다. 또한 NCP, SAP, RIP, NetBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP, 그리고 SPX 와 같은 IPX 전송 계층 프로토콜을 모니터 한다.

WAN 과 ATM 어댑터를 위해서는 연결 계층 프로토콜에 기반을 둔 네트워크 사용 현황을 모니터하기 위하여 몇 가지 탭이 추가로 제공된다. (예: Frame Relay 회선을 위한 PVC) WAN 탭들은 Options 대화 상자에서 현재 선택된 캡슐화 프로토콜을 기반으로 사용 가능하다.

프로토콜 분포는 테이블, 또는 막대나 파이 차트로 볼 수 있다. 또한 한 프로토콜에 대한 패킷의 수나 비율을 볼 수 있다.

Sniffer Pro 는 프로토콜 분포 데이터를 표 작성이나 차트화 할 수 있도록 형식 변환(export) 기능을 제공하며, 보다 상세한 내용은 *모니터 데이터 변환하기(Exporting Monitor Data)*를 참조한다.

그림 2-14 는 Ethernet 어댑터에 대한 프로토콜 분포 막대 차트를 보여준다.



MAC, IP, 혹은 IPX 별로 프로토콜 분포를 디스플레이 할 경우에 클릭

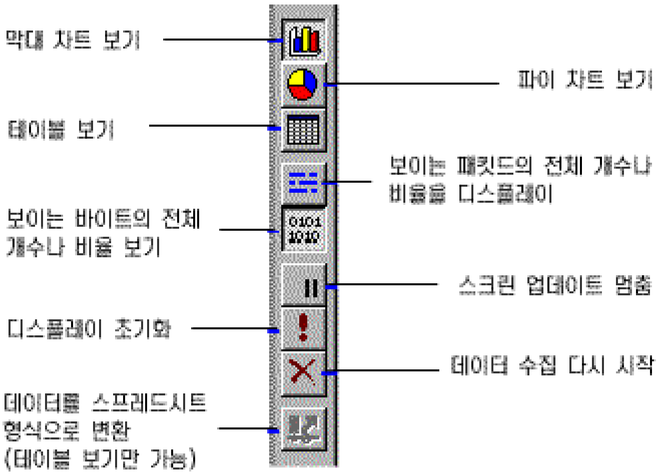


그림 2-14. 프로토콜 분포 (막대 차트)과 툴바.

글로벌 통계 자료 (Global Statistics)

Global Statistics 은 네트워크의 전체 활동 수준과 정확한 크고 작은 패킷들의 트래픽 부하, 그리고 전체 네트워크 성능과 유용성에 대한 각 패킷들의 서로 다른 효과를 이해하는데 도움이 된다.

Global Statistics 는 네트워크 트래픽 분석과 관련된 통계적인 측정치가 포함된 다양한 탭을 제공한다.

- 크기 분포(Size Distribution) 탭은 각 패킷 크기가 발생하는 주기를 모니터 된 전체 트래픽에 대한 비율로 보여준다.
- 활용도 분포(Utilization Distribution) 탭은 10% 단위(0 – 10%, 11% - 20%, … , 21% - 100%)로 그룹화하여 분포된 네트워크 대역폭 소모량을 보여준다.
- WAN Link 탭(WAN 어댑터만)은 WAN 트래픽을 그래프와 테이블의 형태로 보여준다. DTE 와 DCE 에 대하여 Packets/second, Utilization/second, 그리고 Errors/second 가 모두 모니터 되며, 이와 더불어 다양한 에러 프레임 개수와 프레임 크기 분포 개수도 모니터 된다.
- ATM 탭(ATM 어댑터만)은 ATM 트래픽을 그래픽과 테이블 형태로 보여준다. DTE 와 DCE 에 대하여 Packets/second, Utilization/second, 그리고 Errors/second 가 모두 모니터 되며, 이와 더불어 다양한 에러 개수와 크기 분포 개수도 모니터 된다.

글로벌 통계 자료는 막대 혹은 파이 차트로 볼 수 있다.

그림 2-15 는 Ethernet 어댑터에 대한 패킷 크기 분포 그래프를 보여주고 있다.

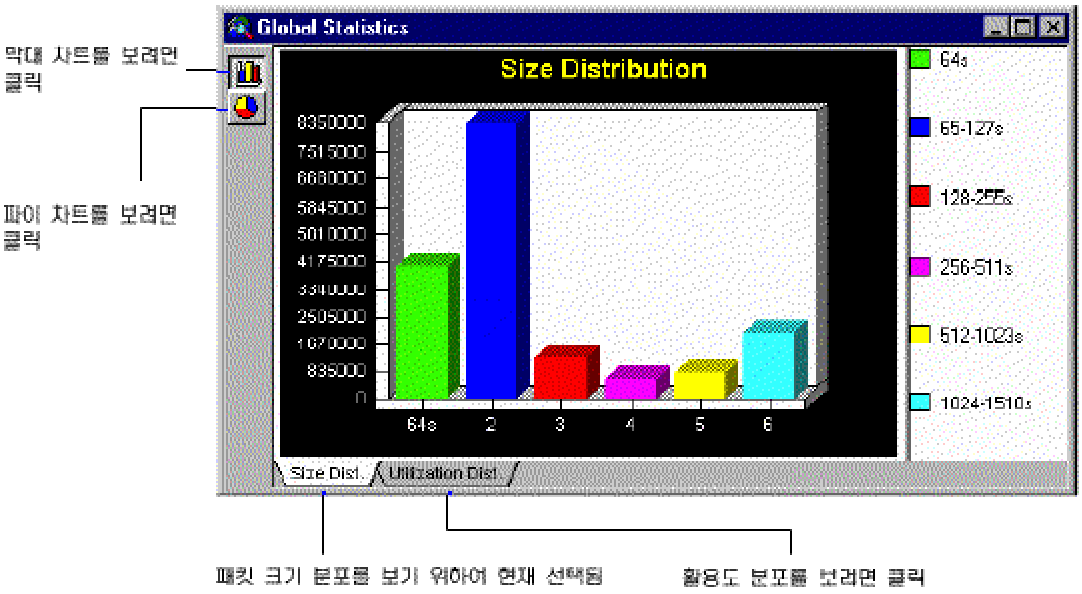


그림 2-15. Global Statistics (막대 차트)

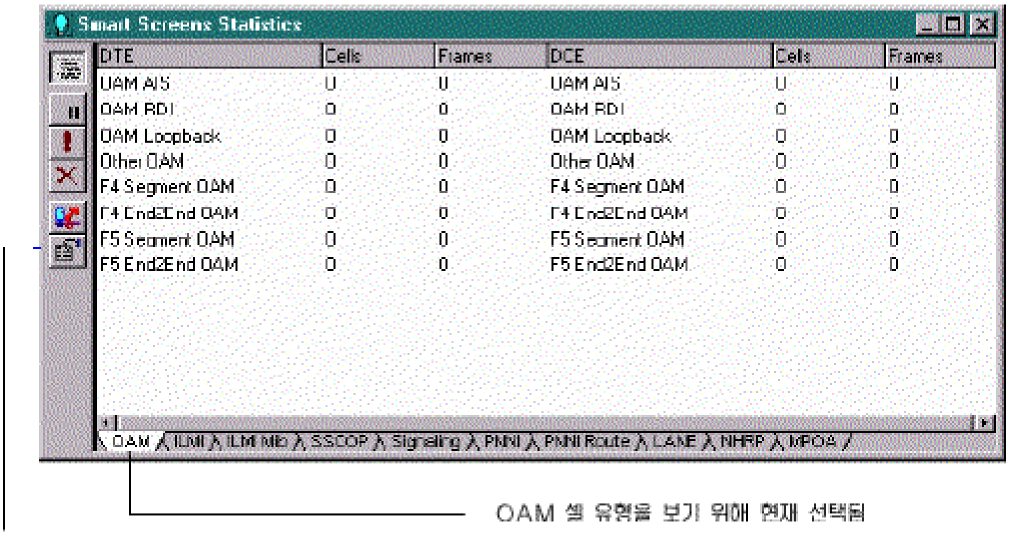
스마트 스크린 (Smart Scan): ATM 어댑터

ATM 스마트 스크린은 다양한 ATM 과 관련된 cell/frame 유형에 대한 개수를 테이블 형태로 제공한다. 서로 다른 일련의 cell/frame 유형에 따라서 다양한 스마트 스크린이 있다. 예를 들어, OAM cell 유형, ILMI cell 유형 등등.

ATM 스마트 스크린을 보려면, **Monitor** 메뉴에서 **Smart Screens** 를 선택하거나 ATM 툴바에서 **Smart Screens** 버튼을 클릭한다.

윈도우 내에는 DTE 와 DCE 에 의하여 분해된 다양한 프레임 유형의 개수가 나타난다. 스마트 스크린 윈도우의 하단에는 지정된 일련의 cell/frame 유형에 따른 서로 다른 프로토콜을 위한 여러 개의 탭이 있다. 해당 cell/fame 유형에 대한 개수를 보기 위하여 각 탭을 클릭할 수 있다.

그림 2-16 은 스마트 스크린 디스플레이 가운데 **OAM** 탭을 보여주고 있다.



DTE	Cells	Frames	DCE	Cells	Frames
UAM AIS	U	U	UAM AIS	U	U
OAM RDI	0	0	OAM RDI	0	0
OAM Loopback	0	0	OAM Loopback	0	0
Other OAM	0	0	Other OAM	0	0
F4 Segment OAM	0	0	F4 Segment OAM	0	0
F4 End2End OAM	0	0	F4 End2End OAM	0	0
F5 Segment OAM	0	0	F5 Segment OAM	0	0
F5 End2End OAM	0	0	F5 End2End OAM	0	0

OAM 셀 유형을 보기 위해 현재 선택됨

스마트 스크린(Smart Screens)에 대한 일반적인 특성을 설정하려면 클릭

다른 프레임/셀 합계를 보려면 이곳에 있는 다른 탭을 클릭

그림 2-16. ATM 스마트 스크린 (OAM 탭)

물리 계층 통계 자료 (ATM 어댑터)

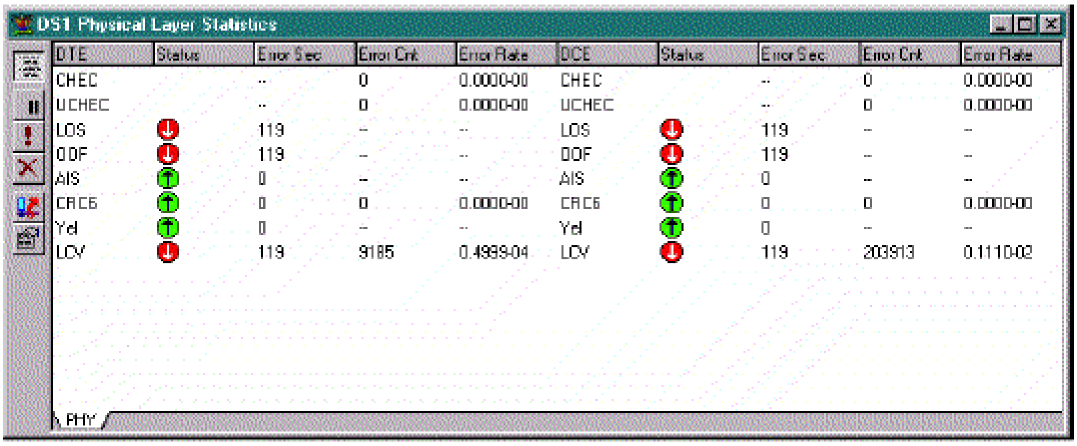
물리적 계층 통계 자료 스크린은 연결된 ATM 물리적 인터페이스의 현제 상태를 모니터하는 카운터와 상태 지시자들을 제공한다. 실제 카운터는 ATM 네트워크(예를 들어, 다중 모드 Fiber STS3c, 단일 모드 Fiber STS3c, UTP-5 STS3c, DS3, E1, E3, OC-3, OC-12 등 등)에 연결하기 위하여 사용되는 인터페이스 도구(혹은 ATM Book 인터페이스 모듈)에 의존한다.

ATM 물리 계층 통계 자료 스크린을 보려면, Monitor 메뉴에서 Physical Layer Stats 를 선택하거나 ATM 툴바에서 Physical Statistics 버튼을 클릭한다. 윈도우 내부의 내용은 DTE 와 DCE 에 의하여 분해된 다양한 물리 계층 통계 자료와 알람의 카운터를 보여준다.

주 --

물리 계층 통계 자료 스크린에 있는 카운터들은 다중 모드 Fiber STS3c, 단일 모드 Fiber STS3c, UTP-5 STS3c, OC-3_물리적_계층_통계 자료 인터페이스 포드(pos)에 대하여 모두 동일하다.

그림 2-17 은 T1 인터페이스 도구에 대한 물리 계층 통계 자료 스크린을 보여준다.



DS1 Physical Layer Statistics

DTE	Status	Error Sec	Error Cnt	Error Rate	DCE	Status	Error Sec	Error Cnt	Error Rate
CHEC		--	0	0.0000-00	CHEC		--	0	0.0000-00
UCHEC		--	0	0.0000-00	UCHEC		--	0	0.0000-00
LOS	↓	119	--	--	LOS	↓	119	--	--
OOF	↓	119	--	--	OOF	↓	119	--	--
AIS	↑	0	--	--	AIS	↑	0	--	--
CRC6	↑	0	0	0.0000-00	CRC6	↑	0	0	0.0000-00
Yel	↑	0	--	--	Yel	↑	0	--	--
LCV	↓	119	9185	0.4999-04	LCV	↓	119	203913	0.1110-02

이 화면은 다른 회선 표시자(indicator)들의 상태를 보여준다. 화살표가 위로 되어 있는 것은 해당 표시자가 에러 상태가 아님을 의미한다. 화살표가 아래로 되어 있는 것은 표시자가 에러 상태에 있음을 의미한다.

그림 2-17. ATM 물리 계층 통계 자료 (T1 pod 에서 보이는 내용)

스위치 (Switch)

주 ---

스위치 통계 자료를 모니터하기 위한 상세한 구성 방법은 부록 1 을 참조하자.

스위치 어플리케이션은 Switch Connection Setting 대화 상자에 선택된 스위치에서 통계 자료를 읽어오고 화면에 표시한다. Switch Configuration List 에 있는 스위치에 Sniffer 를 연결하여 Switch 어플리케이션을 실행하면, Sniffer 는 해당 스위치에 설정되어 있는 MIB 정보를 받아서 화면에 표시한다. 즉, 연결되어 있는 스위치의 모듈, 포트 및 VLAN 정보를 Switch 창에 표시한다. 여기에는 다음과 같은 정보가 제공된다.

- 바이트 수, 유니케스트 패킷, 브로드케스트 패킷, 에러 패킷 그리고 버려진 패킷을 포함하여 각 포트에 입출력 되는 트래픽 통계 자료.
- 스위치 상에 있는 각 모듈과 포토의 이름을 포함한 확인 정보.
- 각 모듈과 포트가 기능 수행, 대기, 혹은 정지 상태인가를 알아보기 위한 동작 상태 정보.

그림 2-18 에 제시한 것처럼, Switch 는 3 개의 부분 창으로 구성되어 있다.

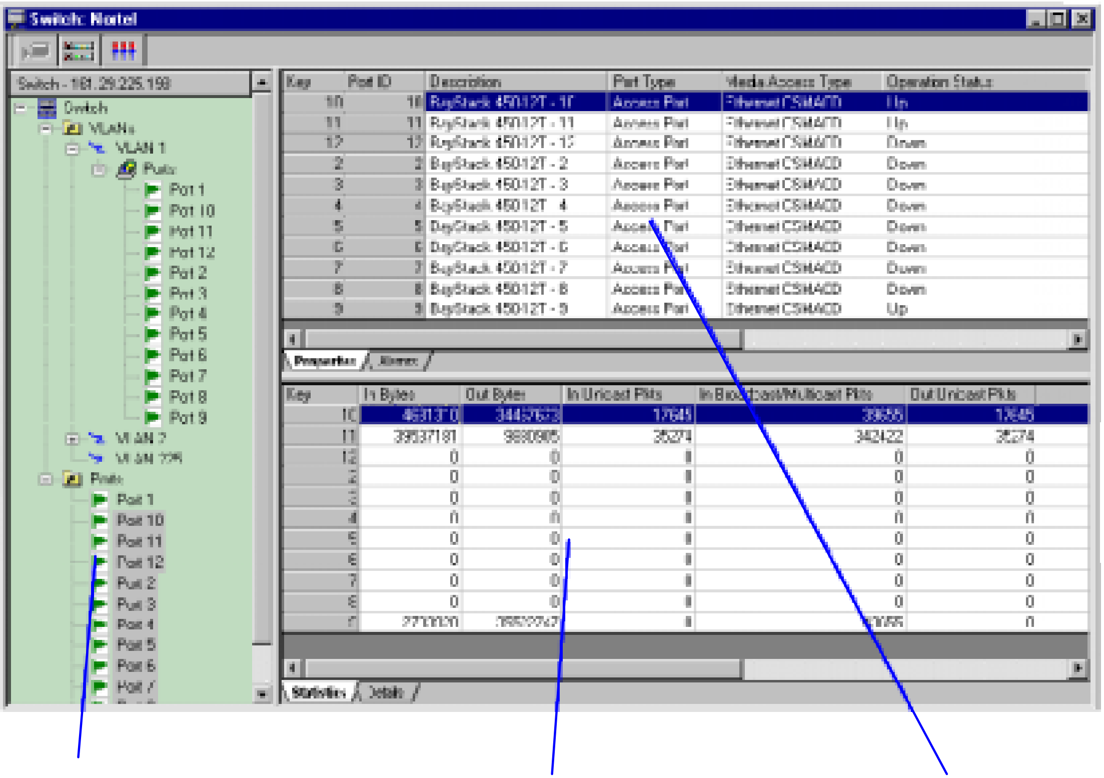
- 좌측 창은 **Module** 및 **VLAN** 기반으로 구성된 스위치의 계층적인 트리 구조를 제공한다.
  - **Module** 폴더는 스위치 상에 있는 모든 모듈들을 상위에서 하위까지 순서대로 표현한다. 또한 각 모듈 항목들은 자신이 포함하고 있는 포트들에 대한 정보를 하위 단에 목록으로 제공한다.
  - **VLAN** 폴더는 해당 스위치에 구성되어 있는 모든 VLAN 목록을 표시한다. 또한 각 VLAN 항목은 자신에게 포함되어 있는 모든 포트들에 대한 정보를 하위 단에 제공한다. 특정 VLAN 에 포함되지 않은 포트들은 VLAN 폴더 하위의 목록에 나타나지 않는다.
- 우측 상단에 있는 Properties(특성) 창에서는 두개의 탭을 제공한다:
  - **Property** 탭은 좌측의 계층 트리 화면에서 선택된 항목의 MIB 을 기반으로 다양한 통계 자료를 제공한다. 예를 들어, 계층 트리 화면에서 Switch 항목이 선택되면, Property 탭에서는 해당 스위치의 전반적인 정보, 즉 모듈, 시리얼 번호, 등을 제공한다. 계층 트리 화면에서 선택된 항목의 종류에 따라서 다양한 정보가 제공된다.
  - **Alarm** 탭에서는 해당 스위치에 임계값 기반(threshold-based) 알람을 설정할 수 있다. 각 알람들은 Interface 와 RMON Statistics MIB 그룹의 통계 자료를 기반으로 운영된다. 즉, 특정 임계값을 초과하는 상황이 발생하면, 스위치는 해당 알람을 Sniffer Pro 쪽으로 전달하고 Alarm Log 에 기록된다. 또한 특정 알람이 검출되었을 때, 해당

스위치 포트에서 즉시 패킷 캡처를 시작할 수 있도록 트리거(일정)를 구성할 수 있다.

◆ 우측 하단의 통계 자료 창에서도 두개의 탭이 제공된다.

- Statistics 탭은 좌측 계층 트리에서 현재 선택된 항목에 대한 MIB 정보를 읽어서 트래픽 통계 자료를 제공한다. 예를 들어, 만약 좌측에서 VLAN 을 선택했다면, Statistics 탭에서는 선택된 VLAN 에 포함된 각 포트에 대한 테이블 항목과, 포트별 트래픽 통계 자료(bytes in/out, unicast in/out, multicast in/out 등등)를 제공한다.
- Detail 탭은 계층 트리에서 선택된 항목에 대한 MIB 정보를 읽어서 상세한 통계 자료를 제공한다.

*그림 2-18*은 스위치 통계 자료 화면의 Module 탭이 활성화된 상태를 보여주고 있다.



Key	Port ID	Description	Port Type	Media Access Type	Operation Status
10	10	BayStack 450-12T - 10	Access Port	Ethernet CSMACD	Up
11	11	BayStack 450-12T - 11	Access Port	Ethernet CSMACD	Up
12	12	BayStack 450-12T - 12	Access Port	Ethernet CSMACD	Down
2	2	BayStack 450-12T - 2	Access Port	Ethernet CSMACD	Down
3	3	BayStack 450-12T - 3	Access Port	Ethernet CSMACD	Down
4	4	BayStack 450-12T - 4	Access Port	Ethernet CSMACD	Down
5	5	BayStack 450-12T - 5	Access Port	Ethernet CSMACD	Down
6	6	BayStack 450-12T - 6	Access Port	Ethernet CSMACD	Down
7	7	BayStack 450-12T - 7	Access Port	Ethernet CSMACD	Down
8	8	BayStack 450-12T - 8	Access Port	Ethernet CSMACD	Down
9	9	BayStack 450-12T - 9	Access Port	Ethernet CSMACD	Up

Key	In Bytes	Out Bytes	In Unicast Pkts	In Broadcast/Multicast Pkts	Out Unicast Pkts
10	46313710	34457673	17645	39655	17645
11	39537181	9880985	35274	342422	35274
12	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0
9	27700020	28552747	0	[illegible]	0

이곳의 계층 트리 구조는 해당 스위치에 대한 Module 별, VLAN 별로 포트를 구성하고 있다. 상위에 있는 항목들을 클릭하면, 하단의 서브 항목들을 볼 수 있다.(예들 들어, Module 항목을 클릭하면, 포트들을 볼 수 있다.)

우측의 두 창에 표시되는 통계 자료들은 이곳에서 선택된 항목에 대한 정보들이 다.

Statisitcs 창에서는 좌측 트리에서 선택된 항목에 대한 트래픽 통계 자료를 위한 두 개의 탭이 있다.

Properties 창은 아래 두 개의 탭을 제공한다.

- Properties 탭은 좌측 트리에서 선택된 항목에 대한 운영 정보 및 구성 정보를 제공한다.
- Alarm 탭에서는 현재 연결된 스위치에 대한 알람을 설정한다.

그림 2-18. 스위치 통계 자료 화면 (Module 탭 활성)

모니터 알람

Sniffer Pro 는 모니터 도중에 비정상적인 네트워크 이벤트를 검출하고 목록에 등록하는 이해하기 쉬운 방법을 제공한다.

알람 관리자는 사용자가 입력한 파라미터들의 임계 값을 초과할 때 해당 이벤트를 alarm log 에 등록한다. 알람 로그에 등록된 이벤트들을 다시 살펴봄으로써 적절한 주의를 요구하는 네트워크 상태를 확인할 수 있다.

알람 로그를 보려면, **Monitor** 메뉴에서 **Alarm Log** 를 선택하거나 Sniffer Pro 메인 툴바에서 알람 로그 버튼 ⚠을 클릭한다.

알람을 구성하고 옵션을 설정에 관한 정보는 *제 7 장. 알람 관리하기(Managing Alarms)* 를 참조하자.

모니터 데이터 변환하기

아래와 같은 어플리케이션에서 표시하는 데이터는 테이블이나 차트의 형태로 변환할 수 있다.

- 데쉬보드 게이지와 탭에 표시되는 내용
- 모니터와 매트릭스 outline 테이블에 표시되는 내용
- 히스토리 데이터
- 프로토콜 분포 테이블에 표시되는 내용
- Smart Screen 테이블에 표시되는 내용
- Physical Layer Statistics 테이블에 표시되는 내용

각 화면의 툴바에서 **Export** 버튼을 사용할 수 있으며, 데이터를 변환하려면 해당 화면에서 버튼을 클릭한다.

데이터는 아래와 같이 몇 가지 형태로 저장할 수 있다.

- (.csv) Comma Separated Value
- (.txt) 탭으로 구분되는 텍스트 파일
- (.prn) 스페이스로 구분되는 텍스트 파일

모니터 데이터에 대한 보고서 생성하기

Sniffer Reporter Agent 는 Sniffer Pro 어플리케이션에 의해 수집된 데이터에 기반을 둔 고객을 위한 다양한 종류의 보고서를 생성하도록 Network Associates 가 제공하며 필요에 따라서 구입해야 하는 어플리케이션이다. 만일 Sniffer Pro PC 에 Sniffer Reporter Agent 가 설치되었다면, Reporter 의 아이콘 📊이 아래와 같은 모니터 어플리케이션에 나타난다.

- 매트릭스
- 호스트 테이블
- 프로토콜 분포
- 글로벌 통계 자료

각 모니터 어플리케이션에 의하여 수집되는 데이터에 기반을 둔 보고서에 대한 설정 대화상자를 나타나도록 하기 위하여 Reporter 의 아이콘을 클릭할 수 있다. Sniffer Reporter Agent 의 사용법에 대한 보다 상세한 정보는 추가로 제공되는 문서나 온라인 도움말을 보기 바란다.

모니터 데이터를 데이터베이스 파일에 저장하기

Sniffer Pro 는 Monitor 어플리케이션에 의해 생성되는 실시간 통계 자료를 확장자가 .CSV 인 파일로 데이터베이스 내에 저장한다. 이 파일들은 Sniffer Pro 프로그램이 설치되어 있는 디렉터리에서 현재 선택된 local 에이전트가 사용하는 폴더의 서브 디렉터리에 저장된다. 이 파일들이 저장된 서브 디렉터리는 Sniffer 가 실행된 날짜별로 서로 다르게 생성된다. 서브 디렉터리의 이름은 트래픽 모니터링을 시작한 시점의 날짜를 기준으로 *yymmdd*(년, 월, 일)형식으로 생성된다.

기본적으로 Sniffer Pro 는 모든 통계 자료에 대한 데이터베이스 파일들을 매 60 분마다 업데이트 한다.

Sniffer Pro 메뉴 바에 있는 **Database** 메뉴는 데이터베이스 파일의 설정 옵션을 제공한다. 모든 통계 자료 혹은 일부 통계 자료에 대한 데이터베이스 수집을 수행하지 않도록 할 수 있으며, 통계 자료에 대한 갱신 간격을 바꾸고, 일부 혹은 모든 데이터베이스 기록을 삭제할 수 있다. 또한 Sniffer Pro 주소록을 데이터베이스 파일에 저장할 수 있다.

Reporter 어플리케이션과 모니터의 데이터베이스 파일

Reporter 는 Sniffer Pro 와 함께 사용할 수 있는 어플리케이션이며, Sniffer Pro 와는 별도로 구매해야 한다. Reporter 를 사용하여 Sniffer Pro 에서 수집된 데이터를 기반으로 다양한 보고서를 생성할 수 있다. Reporter 는 보고서를 생성하기 위해서 모니터 어플리케이션 및 Expert 분석에서 생성된 CSV 파일을 사용한다.

Sniffer Pro 의 모니터 어플리케이션에 의해서 수집된 데이터를 기반으로 보고서들을 생성하기 위해 Reporter 를 사용하려고 한다면, 먼저 Database > Options (Sniffer Pro 의 **Database** 메뉴에서 **Options** 명령을 선택하면 볼 수 있는) 대화 상자의 Database 탭에서 데이터베이스 수집 기능을 활성화 확인해야 한다. Reporter 에서 생성되는 다양한 보고서들은 모니터 어플리케이션에서 수집된 다양한 통계 자료를 기반으로 하기 때문에, 원하는 보고서를 생성하기 위해서는 위 대화 상자에서 모든 통계 자료에 대한 수집 항목을 선택했는지 반드시 확인해야 한다.

3. 패킷 캡처 하기 (Capturing Packets)

통계적인 측정치와 네트워크 트래픽에 대한 계산치를 저장하는 모니터 기능과는 달리 캡처 기능은 네트워크로부터 실질적인 패킷들을 수집하여 캡처 버퍼 내에 저장한다.

캡처하는 동안, Expert 는 패킷들을 분석하고 그 결과를 실시간으로 표시(display)한다. 실시간 Expert 분석을 비활성 상태로 설정하기 위해서는 **Tools** 메뉴에서 **Expert Options** 을 선택하고 **Expert During Capture** 박스가 체크되지 않아야 한다.

캡처가 중지된 후, 캡처 버퍼로부터 패킷들을 디코드하고 표시하기 위하여 Sniffer Pro display 기능을 사용할 수 있으며, 이 기능은 네트워크 처리 내용에 대한 자세한 정보를 제공한다(*packet display*). Display 기능은 또한 Expert 분석을 표시한다(*Expert display*). Packet display 와 Expert display 는 모두 *4 장, Displaying Captured Data* 에서 설명한다.

Sniffer Pro 는 캡처 과정을 제어하고 *capture buffer*(캡처 된 패킷들을 저장)를 구성하며, *capture filter* 를 정의하기 위하여 주 툴바(toolbar)와 **Capture** 메뉴에 *capture controls* 를 제공한다. 또한 캡처 세션의 상태를 볼 수 있도록 capture panel 을 제공한다.

캡처를 시작하기 전에, Expert 데이터의 처리 방법과 표시 방법을 정의하는 Expert 옵션을 구성해야 한다. Expert 옵션은 뒤에서 설명된다.

캡처 제어(Capture Controls)

메인 툴바에 있는 캡처 버튼 또는 **Capture** 메뉴에 있는 메뉴 항목을 사용:

- 캡처 세션을 시작(start), 중지(stop), 잠시 멈춤(pause)
- 캡처 결과를 표시
- 캡처에 사용하는 새로운 필터 생성
- 캡처에 사용하는 필터 선택

*그림 3-1*은 주 툴바에 있는 캡처 버튼을 보여주고 있다.

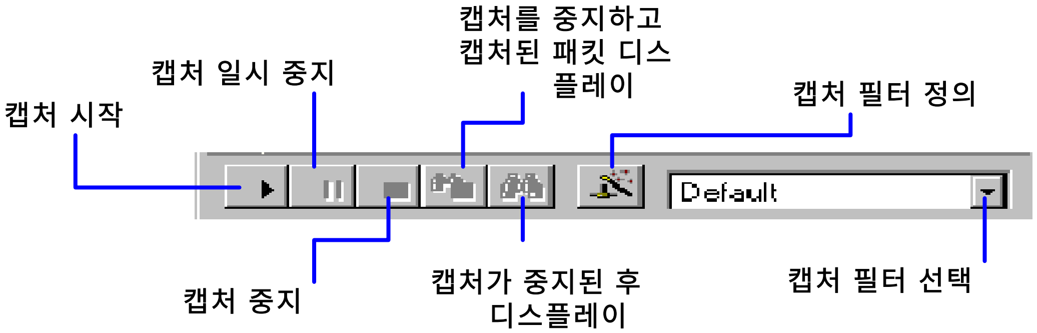


그림 3-1. Capture Controls

또한 Sniffer Pro 는 Capture 메뉴에서 자주 사용되는 기능에 대해 아래와 같이 단축키를 제공한다.

- Start/Stop Capture – F10
- Stop and display capture – F9
- Display a stopped capture – F5

캡처 패널(Capture Panel)

캡처 과정의 상태를 관찰하기 위하여 캡처 패널을 사용하자. 패널에는 두개의 버튼이 제공된다. **Gauge** 탭은 캡처 되는 패킷의 수를 표시하며, 캡처 버퍼가 어떻게 채워지는지를 ‘%’ 비율로 나타낸다. **Detail** 탭은 현재 캡처 세션에 관한 자세한 통계 값들을 보여준다.

만일 Gigabit Ethernet 이나 ATM Book 을 사용하고 있다면, **Channel Info** 탭이 기가비트 Ethernet 인터페이스 카드나 ATM 북 상에서 캡처 버퍼의 상태에 관한 정보를 제공한다.

주 --

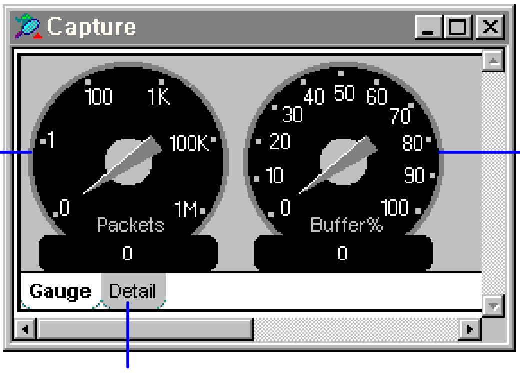
SnifferBook Ultra, Full Duplex Ethernet PCI card 와 Fast Ethernet Full Duplex Pod 에 대한 캡처 패널의 모양은 표준 캡처 패널과 다르다. 만약 위 pod 가운데 하나를 사용하고 있다면, 해당 장비와 함께 제공되는 문서를 참조하기 바란다.

캡처 패널을 열고, **Capture** 메뉴에서 **Capture Panel** 을 선택하거나 주 툴바에서 버튼을 클릭한다.

캡처 패널(Packet Generator 와 데쉬보드처럼)은 장착 가능한 윈도우이다. **Tools** 메뉴에서 **Options** 을 선택하고 **Workspace** 탭을 클릭하거나, 혹은 **Capture Panel** 윈도우를 선택하고 **Docking View** 를 선택하여 이 패널을 Sniffer 데스크 탑 위에 띄울 수 있다. 만일 띄워지지

않는다면, 캡처 패널이 보통 윈도우이다.

*그림 3-2*은 Capture Panel 윈도우를 보여주고 있다.



이 게이지는 캡처된 패킷의 개수를 보여줌

이 게이지는 버퍼가 얼마나 채워졌는가를 (%) 비율로 보여줌

캡처 과정에 대한 자세한 통계 자료를 볼때 클릭. 예를 들어, 버려지거나, 수용되거나, 거부된 패킷의 개수와 프레임 조각 크기를 보여줌

그림 3-2. 캡처 패널 게이지

캡처 버퍼(Capture Buffer)

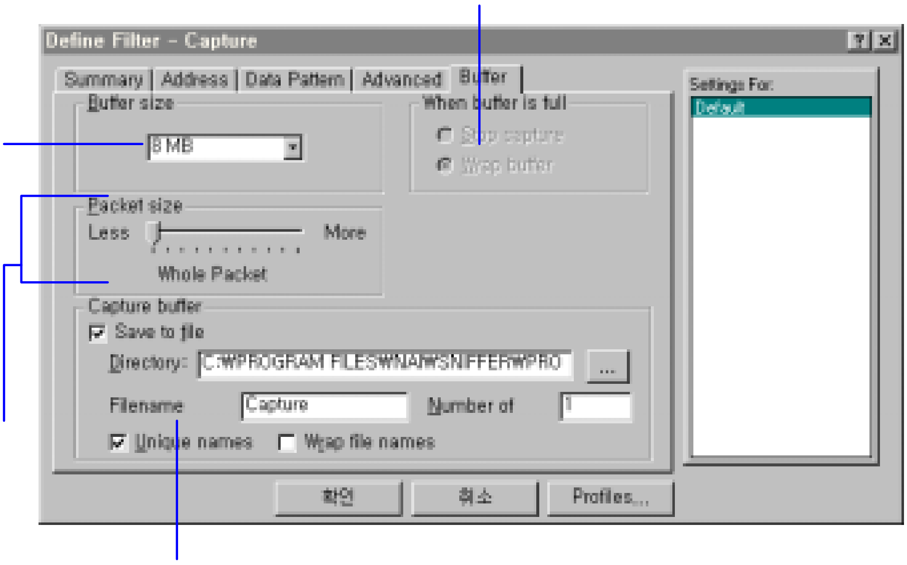
캡처 된 패킷은 *캡처 버퍼(capture buffer)* 내에 저장된다. 캡처 버퍼에 있는 패킷들을 직접 표시하고 분석하거나 디스크에 저장할 수 있다. 또한 미리 저장된 캡처 파일들을 로드하여 화면에 표시할 수 있다(trace files). 캡처 된 데이터는 실시간으로 파일에 스풀 할 수 있다.

비록 데이터가 그 순간에 캡처 된 것이 아니지만, 미리 캡처 된 패킷들을 파일에서 로드함으로써 화면에 표시하고 분석할 수 있다. Sniffer Pro 는 디스크 파일에서 로드 된 데이터를 네트워크에서 직접 캡처 한 데이터처럼 동일한 방법으로 처리한다.

캡처 버퍼 옵션들은 Define Filter 기능에 포함되어 있다. 캡처 버퍼 옵션들을 설정하기 위하여 **Capture** 메뉴에서 **Define Filter** 를 선택한 후, **Buffer** 탭을 클릭하라. (*그림 3-3*)

캡처 버퍼의 크기를 선택하여나 입력. 버퍼 크기를 너무 크게 설정한다면, Sniffer Pro가 메모리를 할당하기 위해 시간 지연이 있을 수 있다. 시스템에서 사용할 수 있는 RAM의 크기 보다 더 큰 버퍼를 지정하지 않도록 주의 하자.

캡처 버퍼가 모두 채워졌을 때, 캡처를 멈추거나 버퍼에 있는 기존 데이터에 겹쳐서 저장(wrap)할 때 선택. Save to File 옵션이 비 활성상태로 되어 있는 경우에만 이 옵션을 선택할 수 있음.



Buffer size: 8 MB

When buffer is full: ○ Stop capture ● Wrap buffer

Packet size

Capture buffer: ☑ Save to file

Directory: C:\PROGRAM FILES\NAI\SNIFFER\PRO

Filename: Capture Number of: 1

☑ Unique names □ Wrap file names

패킷 크기 선택. 버퍼 내에 있는 모든 패킷을 저장할 수 있지만, 특정 크기로 잘라서 저장할 수 있다. (일정 크기로 패킷을 자르면, 디스크 공간을 절약하고, 캡처 파일의 크기를 줄이며, 네트워크 트래픽이 과부하 상태일 때, 프레임 을 상실하는 경우를 제거할 수 있다.

저장되는 파일 이름의 앞부분과 파일의 개수를 입력한다.
(각 파일은 정의된 캡처 버퍼와 동일한 크기가 될 것이다.)

그림 3-3 캡처 버퍼 옵션을 설정하기.

Large Capture Buffer Sizes

이전 버전의 Sniffer Pro 에서는 사용하는 운영 체제의 성능을 고려해서 캡처 버퍼의 최대 크기를 40 MB 로 제한 시켰었다. Windows NT 와 Windows 2000 사용자를 위해서 이번 버전에서는 캡처 버퍼의 크기를 256KB 에서 Sniffer Pro PC 의 물리적인 메모리의 50%(최대 385 MB)까지 사용할 수 있도록 새로운 메모리 설정 기술을 사용한다.

예를 들어, 256 MB RAM 이 장착된 PC 에서는 대략적으로 66 MB 정도가 운영 체제와 Sniffer Pro 에서 사용되며, 나머지 190 MB 의 RAM 을 여분으로 사용할 수 있다. 따라서 190 MB 의 50%, 즉 최대 95 MB 의 RAM 을 캡처 버퍼로 사용할 수 있다.

주 --

Buffer size 드롭 다운 메뉴에서 미리 설정된 버퍼 크기를 선택할 수도 있지만, 사용자가 임의로 새로운 값을 입력할 수 있다.

캡처 버퍼와 관련된 문제점 해결

Sniffer Pro 에서 사용되는 새로운 메모리 설정 기술은 가끔씩 오류 메시지의 원인이 될 수도 있다. 종종 이러한 오류들은 아래와 같이 레지스트리 설정을 수정하여 해결할 수 있다.

NO_MORE_SYSTEM_PTEs

이 오류 메시지는 Windows NT 와 Windows 200 모두에서 발생할 수 있으며, 버퍼 크기가 사용할 수 있는 메모리 양보다 더 크게 선택되었을 경우에 나타날 수 있다. 이러한 메시지가 나타나면, 아래와 같은 작업을 하자.

1. **Start/Run** 을 선택하고 대화 상자에 **regedit** 를 입력하여 Registry Editor 를 시작하자.
2. 다음의 레지스트리 키로 이동하자.
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\SystemPages
3. 새로운 값을 설정하기 위해서 해당 키를 더블 클릭하자.
4. 해당 키에 10 진수 값으로 50,000 을 설정하자.
5. **OK** 를 클릭하자.
6. Registry Editor 를 빠져 나와서 시스템을 재시동하자.

Capture failed: Decrease the capture buffer size and try again

이 오류 메시지는 버퍼 크기가 사용 가능한 메모리 크기보다 더 크게 선택되었을 때, Windows 2000 에서 발생할 수 있다. 이 메시지가 발생하면, 아래와 같은 작업을 하자.

1. **Start/Run** 을 선택하고 대화 상자에 **regedit** 를 입력하여 Registry Editor 를 시작하자.
2. 다음의 레지스트리 키로 이동하자.
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\IoPageLockLimit
3. 새로운 값을 설정하기 위해서 해당 키를 더블 클릭하자.
4. 해당 키에 10 진수 값으로 65,000 을 설정하자.
5. **OK** 를 클릭하자.
6. Registry Editor 를 빠져 나와서 시스템을 재시동하자.

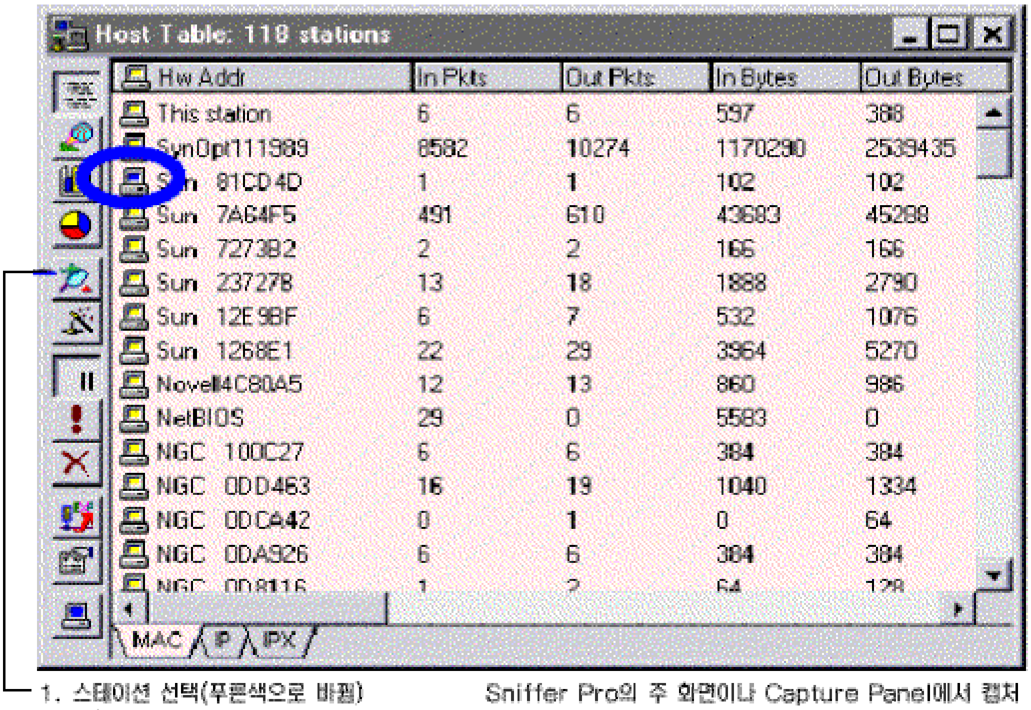
캡처 버퍼의 내용을 파일에 저장하기

캡처 버퍼의 내용은 **Buffer** 탭에서 **Save to File** 항목을 선택하여 버퍼가 가득 채워졌을 경우 자동으로 파일에 저장하도록 할 수 있다. 파일 이름의 머리글과 스풀 되는 파일의 개수를 입력한다. 예를 들어, **Number of files** 필드 내에 5 를 입력하고 **Wrap file names** 를 클릭하면, 6 번째 파일은 첫번째 파일에 겹쳐지게 된다. 만일 **Wrap file names** 를 선택하지 않으며, 캡처는 5 번째 파일이 가득찰 때까지 수행할 것이다.

특정 스테이션에서 캡처 하기

특정 스테이션을 위한 패킷들을 캡처 하기 위하여 모니터의 호스트 테이블 내에서 해당 스테이션을 선택한다. 두개의 특정 스테이션 간의 패킷을 캡처 하기 위해서는 모니터의 매트릭스 표시로부터 캡처 하려는 스테이션 가운데 하나를 선택한다. 그 후, 버튼을 클릭한다. (호스트 테이블 혹은 매트릭스 테이블을 보기 위해서는 Monitor 메뉴에서 Host Table 혹은 Matrix 를 선택하거나 툴바 버튼을 사용.)

그림 3-4 호스트 테이블 내의 한 스테이션에 대하여 캡처하는 방법을 보여주는 예이다.



Hw Addr	In Pkts	Out Pkts	In Bytes	Out Bytes
This station	6	6	597	388
SynOpt111989	8582	10274	1170290	2539435
Sun 81CD4D	1	1	102	102
Sun 7A64F5	491	610	43683	45288
Sun 7273B2	2	2	166	166
Sun 237278	13	18	1888	2790
Sun 12E9BF	6	7	532	1076
Sun 1268E1	22	29	3964	5270
Novell4C80A5	12	13	860	986
NetBIOS	29	0	5583	0
NGC 100C27	6	6	384	384
NGC 0DD463	16	19	1040	1334
NGC 0DCA42	0	1	0	64
NGC 0DA926	6	6	384	384
NGC 0D8116	1	2	64	128

1. 스테이션 선택(푸른색으로 바뀜)
2. 캡처 버튼 클릭

Sniffer Pro의 주 화면이나 Capture Panel에서 캡처 과정을 볼 수 있음.

그림 3-4. 호스트 테이블에서 단일 스테이션 캡처

캡처 필터 (Capture Filters)

단지 필요한 패킷들만 캡처 하기 위하여 *필터들(filters)*을 정의할 수 있기 때문에, 네트워크 문제들을 관측하기 위하여 필요한 데이터에만 초점을 맞출 수 있다.

한 필터를 캡처 과정에 적용하면, 캡처 과정에서 *캡처 필터(capture filter)*를 호출한다. 캡처 필터는 단지 임의의 프레임만을 캡처 버퍼 내에 저장되도록 한다. 캡처 필터를 정의하는

방법에 관한 내용은 *5 장, 필터 정의와 트리거(Defining Filters and Triggers)*를 참조하자.

캡처 트리거 (Capture Triggers)

트리거 내용은 데이터와 시간, 알람, 그리고 특정 네트워크 이벤트에 기초하여 캡처를 시작하고 중지하도록 한다. 업무 시간 이후나 주말과 같이 Sniffer Pro 를 지켜볼 수 없는 상황에서 데이터를 캡처 하기 위하여 혹은 알람에 설정된 조건에 의하여 특정 이벤트가 발생하였을 경우 캡처를 시작하도록 하기 위하여 트리거를 사용한다.

캡처 트리거를 정의하는 방법은 *5 장, 필터 정의와 트리거(Defining Filters and Triggers)*를 참조하자.

Expert 옵션 (Expert Options)

효율적인 네트워크 분석을 위하여, 그리고 자신의 네트워크 프로토콜 환경에 따라서 데이터 캡처를 시작하기 전에 Expert 옵션을 설정해야 한다. Expert 옵션은 다음에서 설명한다.

Expert 계층 및 대상들 (Expert Layers and Objects)

캡처하는 동안, Expert 는 문제가 발생하는 Expert 계층에 따라서 네트워크 문제들을 분류하고 관찰하는 트래픽으로부터 네트워크 대상들의 데이터베이스를 구성한다. (Expert 네트워크 계층화 구조는 OSI 모델과 유사하다. 그러나 두개의 체계가 언제나 일치하지는 않는다.)

Expert 옵션은 다음과 같은 내용으로 설정할 수 있다.

- Expert 처리로부터 특정 계층을 제외 시킴.

  - 네트워크 분석에 필요한 특정 트래픽만을 선택할 수 있도록 하는 캡처 필터를 사용하여 처리 과정에서 특정 Expert 계층을 제외시킬 수 있다. 이러한 내용은 특정 네트워크 문제에 대하여 정밀하게 초점화 할 수 있도록 한다.

  각 Expert 계층에 대한 데이터베이스 내에 생성될 수 있는 대상의 최대 개수를 설정.

- 네트워크 대상을 생성하는데 필요한 메모리의 양을 줄이기 위하여, 각 Expert 계층에 대하여 Expert 가 생성할 수 있는 object 의 최대 개수를 설정할 수 있다.

  - 설정을 도와주기 위하여 Expert 는 각 계층을 위하여 선택된 대상의 개수에 필요한 메모리의 추정된 값을 보여준다.

- 데이터베이스 내에 더 이상의 공간이 없을 경우, Expert 대상을 재 순환할 것인가 아니면 새로운 고려 대상의 생성을 멈출 것인가를 결정한다.

- Expert 는 캡처 버퍼에 누적된 패킷들 내에 있는 정보로부터 네트워크 대상의 데이터베이스를 구성한다.
  - 몇몇 네트워크들은 구조상으로 매우 복잡하기 때문에, 어떤 시점에서 Expert 는 새로운 네트워크 대상을 위하여 더 이상의 메모리를 갖을 수 없을 것이다. 만일 대상을 재 순환하면, Expert 는 새로운 대상을 데이터베이스에 계속 추가하며, 메모리 부족이 발생할 경우, 가장 흥미도가 떨어지는 대상에 겹쳐서 쓴다 (오류와 상관없는 object 가 가장 흥미도가 떨어지는 것). 만일 대상을 재 순화하지 않는다면, Expert 는 메모리 부족 상황에서 새로운 대상의 생성을 중단하며, 그 대신 계속해서 이미 데이터베이스에 저장된 내용이 포함하고 있는 정보를 가지고 트래픽을 해석한다.

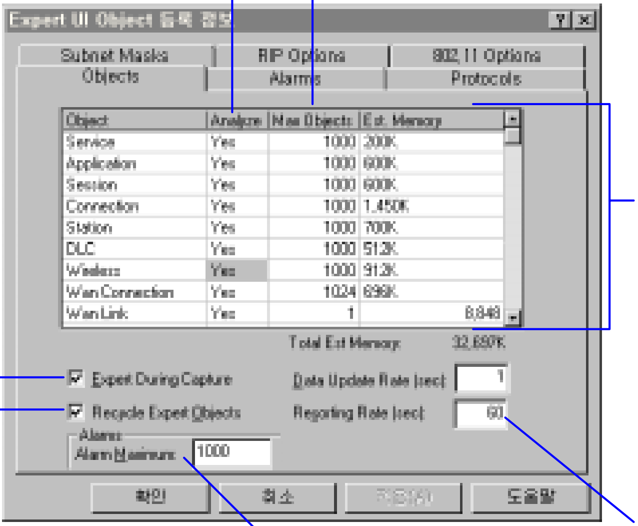
- 캡처하는 동안 실시간 Expert 분석의 enable/disable.
  - 캡처를 시작했을 때, 기본적으로 Sniffer Pro Expert 는 버퍼로 들어오는 패킷을 분석하고 그 결과를 실시간으로 Expert 윈도우에 표시한다.
  - 따라서 캡처 과정동안 Expert 분석기가 생성한 네트워크 object, symptom, diagnoses 을 관찰할 수 있다. 만일 필요하지 않다면, 실시간 Expert 분석은 disable 할 수 있다.

네트워크 대상과 Expert 계층 옵션을 구성하기 위하여, **Tools** 메뉴에서 **Expert Options** 을 선택한다. Expert Options 대화 박스에서 **Objects** 탭을 볼 수 있다. *그림 3-5*를 보자.

Analyze 항목에서 특정 계층을 No로 선택하면, Expert 분석 과정에서 해당 계층을 제외시킬 수 있음.

각 Expert 계층에 대해서 database내에 생성되는 object들의 최대 개수를 지정할 수 있음.

이 항목을 선택하지 않으면, 버퍼에 캡처하는 동안 실시간으로 Expert 분석이 실행되지 않는다.



Object	Analyze	Max Objects	Est. Memory
Service	Yes	1000	200K
Application	Yes	1000	600K
Session	Yes	1000	600K
Connection	Yes	1000	1,450K
Station	Yes	1000	700K
DLC	Yes	1000	512K
Wireless	Yes	1000	912K
Wan Connection	Yes	1024	696K
Wan Link	Yes	1	8,848

Total Est Memory: 32,697K

☑ Expert During Capture — Data Update Rate (sec): 1

☑ Recycle Expert Objects — Reporting Rate (sec): 60

Alarms — Alarm Maximum: 1000

Sniffer Pro는 각 계층에 지정된 개수 만큼의 object를 위해 필요한 메모리 양을 추정하여 하단에 표시함.

이 옵션들은 Expert 화면이 새로운 데이터로 업데이트되는 주기를 표시.

이 체크 박스는 메모리 한계를 초과했을 경우, Expert 시스템이 취해야할 동작을 지정한다.

* 선택된 경우, 데이터베이스에 있는 기존 object에 겹쳐서 기록하여 새로운 object를 생성한다.
* 선택되지 않은 경우, 새로운 object를 생성하지 않고 기존에 데이터베이스에 있는 정보에 따라서 트래픽을 해석함.

이 옵션은 Expert 데이터베이스 내에 생성될 수 있는 알람의 최대 개수를 지정함.

알람이 최대 개수가 되면, Recycle Alarms 옵션이 선택된 경우, Expert는 가장 오래된 알람이나 우선수위가 가장 낮은 알람을 제거하여 새로운 알람이 생성되고, 반대의 경우에는 새로운 알람이 생성되지 않음.

그림 3-5. Expert 대상과 계층 옵션 설정하기

Expert 임계 값 (Expert Thresholds)

Expert 임계 값들은 Expert 가 주어진 네트워크 이벤트에 기초한 증상 혹은 분석 내용을 생성할 것인가를 결정한다.

Expert 임계 값을 바꾸기 위해서는 **Tools** 메뉴에서 **Expert Options** 을 선택하고 **Alarms** 탭을 클릭한다. Alarms 탭은 *그림 3-6*에서 보였다.

중요 정보 --

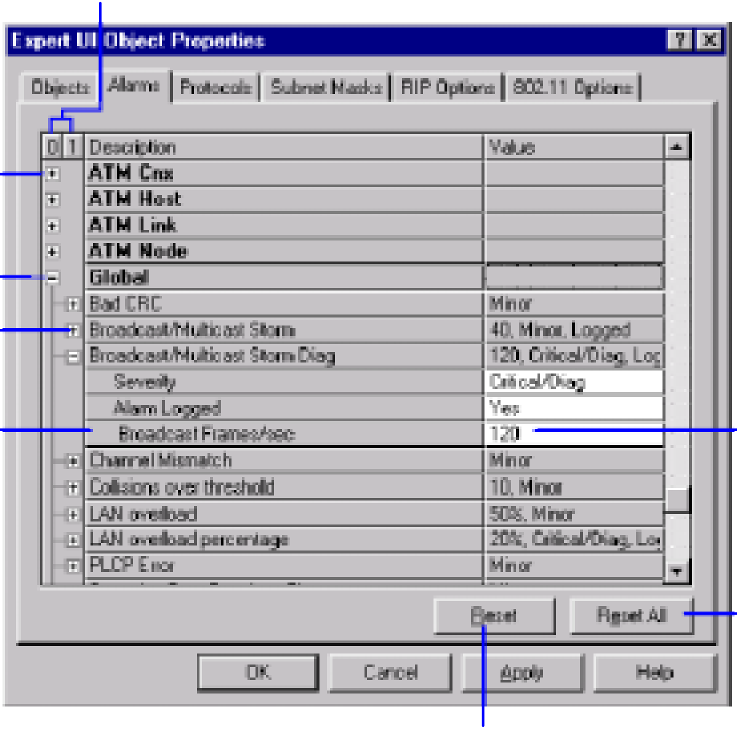
Sniffer Pro 에 적용되는 기본 임계 값은 정확하고 정보가 될 수 있는 증상 및 분석 내용을 검출하도록 주의 깊게 계산되어 왔다. 임계 값을 바꾸기 전에 반드시 자신의 네트워크에 대하여 확실히 이해하고 있어야 한다.

Alarm severity level 과 alarm log 에 관한 정보는 *7 장, Alarms 관리(Managing Alarms)*에

서 설명한다.

Expert 계층을 열고 모든 증상과 분석 내용(알람)을 화면에 나타내려면 +를 클릭

모든 Expert 계층을 확장/축소 하려면 여기를 클릭



Expert UI Object Properties

0	1	Description	Value
⊞		**ATM Cnx**	
⊞		**ATM Host**	
⊞		**ATM Link**	
⊞		**ATM Node**	
⊟		**Global**	
	⊞	Bad CRC	Minor
	⊞	Broadcast/Multicast Storm	40, Minor, Logged
	⊟	Broadcast/Multicast Storm Diag	120, Critical/Diag, Log
		Severity	Critical/Diag
		Alarm Logged	Yes
		Broadcast Frames/sec	120
	⊞	Channel Mismatch	Minor
	⊞	Collisions over threshold	10, Minor
	⊞	LAN overload	50%, Minor
	⊞	LAN overload percentage	20%, Critical/Diag, Log
	⊞	PLCP Error	Minor

임계값 항을 클릭하고 새로운 임계값을 입력할 수 있음.

이 알람에 대한 설정 정보를 화면에 나타나게 하려면 여기를 클릭.

모든 계층에 대한 설정 내용을 기본값들로 초기화

임계값은 설정 목록의 끝 부분에 나타남.

선택된 값을 기존에 설정된 기본값으로 초기화

그림 3-6. Expert 임계 값 설정하기

프로토콜 (Protocols)

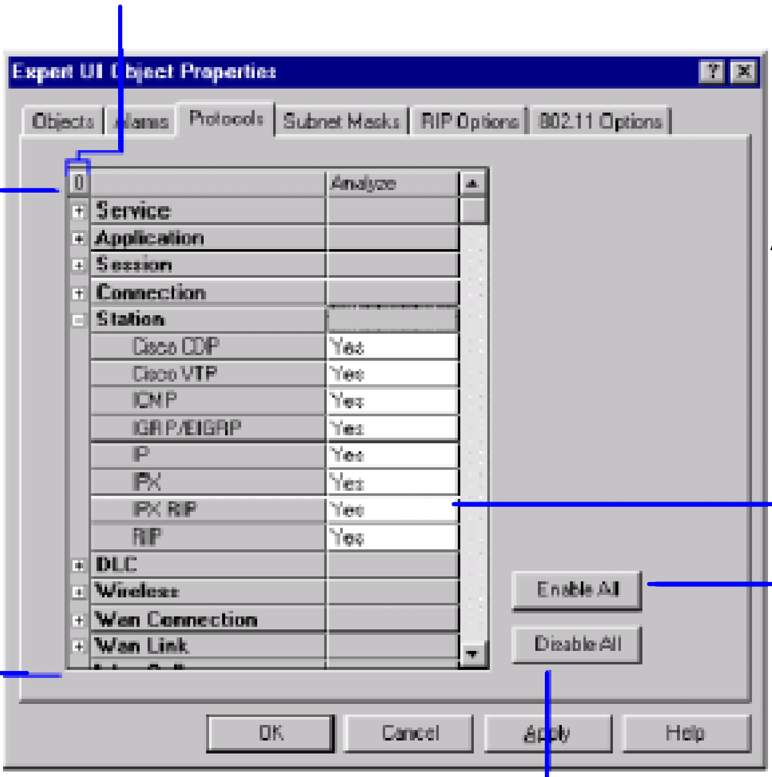
특정 프로토콜에 대해서만 Expert 분석이 필요한 경우 또는 Expert 분석 성능을 향상시키고자 하는 경우에는 Expert 분석이 필요한 프로토콜들만 선택할 수 있다.

Expert 분석이 필요한 프로토콜들을 선택하려면, Tools 메뉴에서 Expert Options 을 선택하고 Protocols 탭을 클릭한다. Protocols 탭은 그림 3-7 에 제시하였다.

Protocols 탭에는 분석되는 Expert 계층별로 프로토콜들이 정리되어 있다. 대화 상자 내에 있는 + 기호를 클릭하면, 각 계층에 속해 있는 프로토콜들을 볼 수 있다. 다음으로 분석이 필요한 프로토콜이 있는 경우에는 Analyze 열에서 Yes 를 선택하고, 분석이 필요하지 않은 프로토콜에 대해서는 No 를 선택하면 된다.

특정 Expert 계층을 열어서 해당 계층의 모든 프토토콜들을 보려면 + 기호를 클릭

모든 Expert 계층들을 확장/축소 하려면 여기를 클릭



0	Analyze
+ Service	
+ Application	
+ Session	
+ Connection	
− Station	
Cisco CDP	Yes
Cisco VTP	Yes
ICMP	Yes
IGRP/EIGRP	Yes
IP	Yes
IPX	Yes
IPX RIP	Yes
RIP	Yes
+ DLC	
+ Wireless	
+ Wan Connection	
+ Wan Link	

Analyze 셀을 클릭하고 Yes 또는 No를 선택

모든 프로토콜들에 대해서 Expert 분석을 수행하지 않으려면 이곳을 클릭

모든 프로토콜들에 대해서 Expert 분석을 수행하려면 이곳을 클릭

그림 3-7. 특정 프로토콜에 대해서 Expert 분석을 활성화

서브넷 마스크 (Subnet Masks)

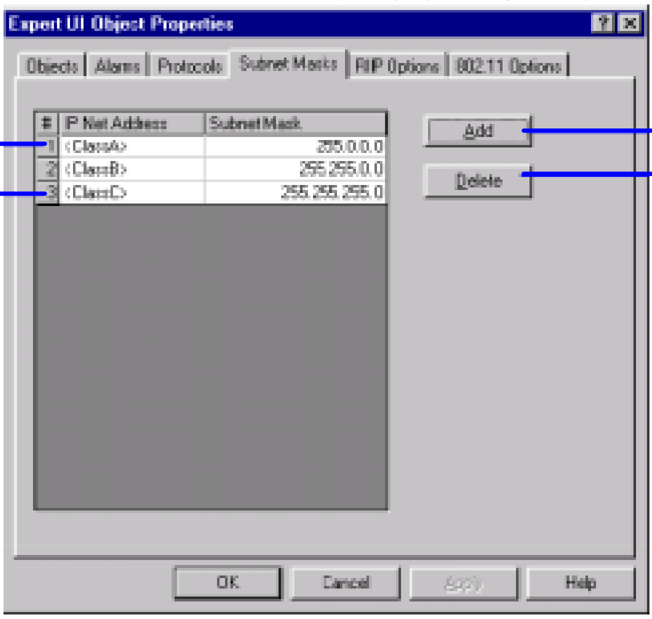
TCP/IP 서브넷 마스크는 전통적으로 IP 주소의 부류에 따른 서브넷 마스크가 되도록 IP 네트워크 주소 내에서 특정 비트들로 예약되어 있다. Expert 는 기본적으로 설정되어 있는 서브넷 마스크를 사용한다.

어떤 네트워크들은 비 전통적인 서브넷 마스크를 사용할 수도 있다. 만일 Expert 가 비 전통적인 서브넷 마스크를 사용하는 네트워크 세그먼트에 접속되어 있다면, Expert 는 가짜 네트워크 대상들과 분석 내용들을 등록할 수도 있다. 이러한 상황은 Expert 가 실질적인 서브넷 마스크 주소라기 보다는 주소 필드 내에의 한 곳에 있는 주소 정보라고 예상하기 때문이다.

만일 네트워크에서 비 전통적인 서브넷 마스크를 사용한다면, Expert 가 프레임을 관찰하는 네트워크를 위한 IP 네트워크 주소와 적절한 서브넷 마스크를 추가해야 한다.

Tools 메뉴에서 Expert Options 을 선택한 후, Subnet Masks 탭을 클릭한다(*그림 3-8*). 새로운 내용을 추가하기 위하여 Add 버튼을 클릭한다. IP Net Address 열에 여러분의 IP 주소를 n.n.n.n 형식으로 입력한다. 단 각각의 n 값은 256 보다 작아야 한다. Subnet Mask 열에 IP 주소와 연관된 서브넷 마스크를 입력한 후, Apply 를 클릭한다.

Expert가 프레임을 관찰하는 네트워크에 대한 IP 주소와 적절한 서브넷 마스크를 추가



#	IP Net Address	Subnet Mask
1	<ClassA>	255.0.0.0
2	<ClassB>	255.255.0.0
3	<ClassC>	255.255.255.0

Expert는 각 클래스의 IP 주소에 대해서 기본적인 서브넷 마스크 설정 정보를 보여준다.

선택된 IP 주소/서브넷 마스크를 테이블에서 삭제

그림 3-8. 서브넷 마스크 설정하기

RIP 설정 (RIP Settings)

Expert 는 캡처 과정 동안 RIP(Routing Information Protocol) 분석을 수행하고 캡처 된 프레임 내에 있는 RIP 과 다른 라우팅 프로토콜들을 세밀하게 분석하여 라우팅 테이블을 구성한다. RIP 분석은 Expert 윈도우에 있는 " Route" 계층에서 보여주며, 통상적인 라우팅 문제를 검출할 수 있도록 한다.

RIP 분석은 ' disable' 하거나 수행하기 원하는 분석 수준(트래픽 총계와 잘못 지정된 프레임, 혹은 단지 트래픽 총계만)을 입력할 수 있다.

Expert 는 네트워크 전반에서 발견된 라우터들 혹은 여러분이 설정한 기본 라우터들을 추적한다. 기본 라우터를 설정할 때, Expert 는 기본 고정 라우터를 게이트웨이로 구성한다. 이러한 라우터에 대한 목적지 IP 주소는 [0.0.0.0]이다. (이곳에는 기본 라우터의 MAC 주소 혹은 IP 주소를 입력할 수 있다.) 이러한 설정은 RIP Expert 가 통보하지 않는 경로를 제공하는 라우터를 알아볼 수 있도록 한다.

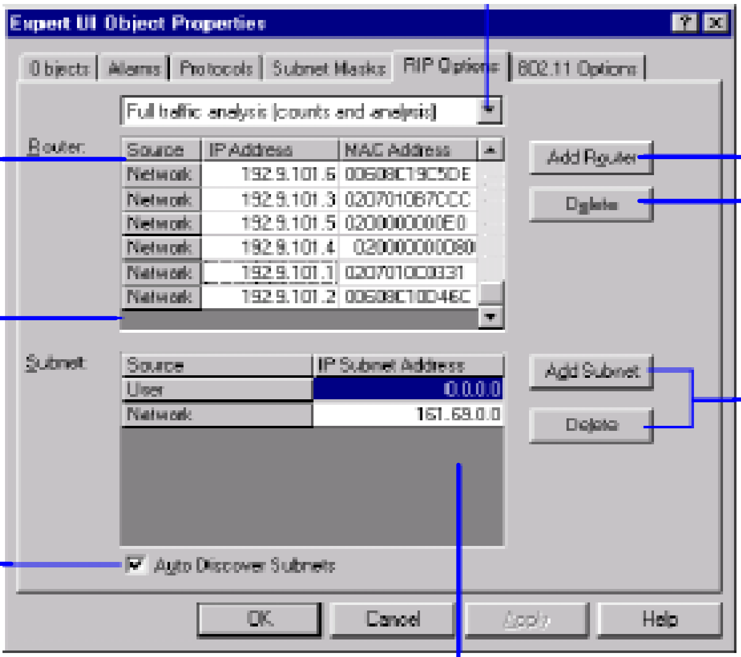
몇몇 호스트들은 기본 게이트웨이로 트래픽을 라우팅 하도록 구성될 수 있지만, 그러한 호스트에서 기본 게이트웨이로의 경로는 결코 통보되지 않을 수도 있다. 고정 기본 라우터를 설정하지 않으며, RIP Expert 는 프레임을 한 호스트에서 기본 게이트웨이로 보내는 것을 잘못 지정된 것으로 옳지 못하게 분석할 것이다. 만일 여러분이 설정했던 기본 경로가 또한 통보되었다면, 그 경로가 테이블 내에 영구히 남아 있기 때문에 다른 경로는 무시된다.

중요 정보---

Expert 에 의하여 분석되는 RIP 패킷들을 위하여 연결 계층과 어플리케이션 계층은 반드시 Expert Properties dialog box 의 **Objects** 탭에 있는 Analyze 에 설정되어야 한다. RIP sits above UDP; RIP 해석기는 반드시 UDP 해석기로부터 호출되어야 한다. Sniffer Pro 는 전송 계층으로 UDP 를 고려; 전송 계층을 위하여, 그리고 해석되는 것 이상으로 적어도 연결 계층은 반드시 선택되어야 한다.

RIP 분석을 설정하거나 ' disable' 하기 위해서는 **Tools** 메뉴에서 **Expert Options** 를 선택한 후, **RIP Options** 탭을 클릭한다. RIP Options 탭은 *그림 3-9*에서 보였다.

실행하고자 하는 RIP 분석의 수준을 선택
* No traffic analysis (RIP disable)는 RIP Expert를 수행하지 않음
* Full Traffic analysis (counts and analysis)는 트래픽을 계산하고 잘못 지정된 프레임을 검출함
* Traffic Counts only는 단지 트래픽만을 계산함



Full traffic analysis (counts and analysis)

Source	IP Address	MAC Address
Network	192.9.101.6	00608C19C5DE
Network	192.9.101.3	0207010B7CCC
Network	192.9.101.5	0200000000E0
Network	192.9.101.4	020000000080
Network	192.9.101.1	0207010C0331
Network	192.9.101.2	00608C10D46C

Source	IP Subnet Address
User	0.0.0.0
Network	161.69.0.0

☑ Auto Discover Subnets

Expert는 캡처는 캡처하는 동안 네트워크 상에서 라우터를 검색하여 검색된 정보를 라우터 테이블 내에서 보여줌.

캡처하는 동안 자동적으로 Expert가 네트워크 상에 있는 서브넷을 검색

라우터 테이블에 기본 라누터를 추가

라우터 테이블에서 임의의 라우터를 제거

서브넷 테이블에 임의의 서브넷을 추가하거나 제거

중요 정보;
RIP Expert는 Subnet Masts 탭에 적절히 설정되어 있는 서브넷 마스크와 IP 서브넷 주소가 필요함.

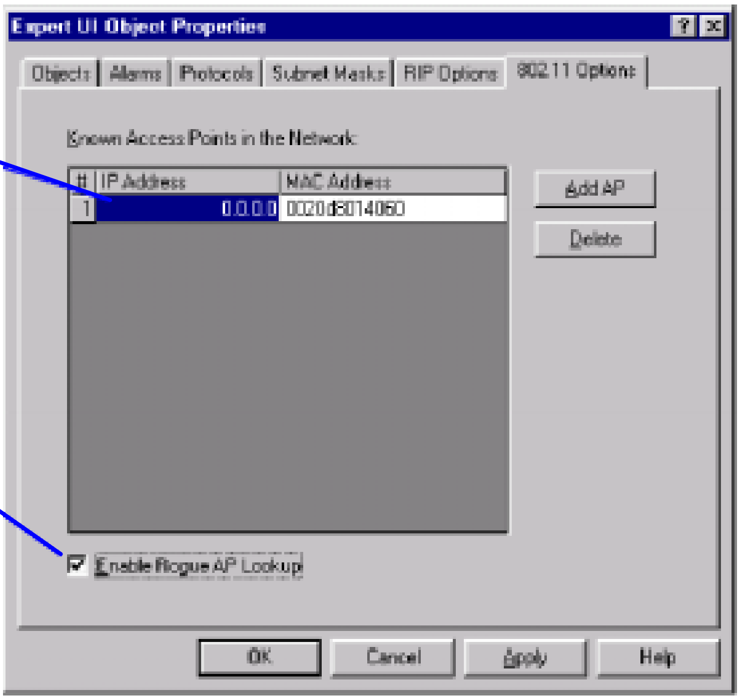
이 테이블은 캡처하는 동안 Expert가 네트워크에서 자동적으로 검색한 서브넷과 사용자가 수동으로 입력한 서브넷 주소를 보여줌.
Source 항은 해당 서브넷이 Expert에 의해 검출된 것인지 또는 사용자가 수동으로 추가한 것인지를 나타냄.

그림 3-9. RIP 옵션 설정하기

802.11 옵션

802.11 Options 탭에 있는 옵션들은 Expert 가 무선 네트워크 상에서 rogue access point 확인 방법을 지정할 수 있다. Enable Rogue AP Lookup 옵션이 선택되면, Expert 는 매번 새로운 액세스 포인트를 검색하여, 사용자가 802.11 Options 탭에 입력한 액세스 포인트의 MAC 주소화 비교한다. 만약 검색된 액세스 포인트 주소가 802.11 Options 탭 내에 입력되어 있지 않다면, Expert 는 Rogue Access Point 알람을 생성한다. 더욱이 Expert 화면에서는 해당 액세스 포인트를 rogue 로 판단할 것이다. (Rogue 라는 말은 Expert Summary 와 Detail 화면 내에서 괄호에 묶여진 채로 나타나게 될 것이다.) 이 기능은 무선 네트워크 환경에서 사용자에게 허용되지 않은 액세스 포인트를 간단히 확인할 수 있는 방법을 제공한다.

그림 3-10 은 Expert Options 대화 상자에서 802.11 Options 탭을 보여주고 있다.



Known Access Points in the Network

#	IP Address	MAC Address
1	0.0.0.0	0020d8014060

☑ Enable Rogue AP Lookup

Add AP 버튼을 클릭하고 사용자의 네트워크 상에서 알고 있는 액세스 포인트의 주소를 이곳에 입력한다. 원하는 개수 만큼의 액세스 포인트를 입력할 수 있다.

Expert가 새로 검색된 액세스 포인트의 주소를 사용자가 입력한 주소 목록에 있는 MAC 주소와 비교하기를 원한다면 이 옵션을 선택한다. 만약 이 옵션이 선택되고 Expert가 이 대화 상자에서 입력되지 않은 주소를 찾아내면, 그 액세스 포인트를 Rogue라고 Expert 화면에 표시할 것이다. 더불어서 Expert는 Rogue Access Point 알람을 생성한다.

그림 3-10. 802.11 Options 탭 설정하기

Expert 의 rogue 확인 기능을 효율적으로 사용하려면, 현재의 무선 네트워크에서 공식적으로 사용되고 있는 액세스 포인트들의 MAC 주소를 먼저 Expert 에게 알려 주어야 한다. 아래의 방법을 따라서 액세스 포인트들의 MAC 주소를 입력한다.

Expert 가 rogue 액세스 포인트들을 확인할 수 있도록 환경 설정

1. Tool/Expert Options 항목을 선택하여 Expert Properties 창의 802.11 Options 탭을 화면에 나타나게 하고 대화 상자 내에서 802.11 Options 탭을 클릭한다.

2. 아래의 과정을 따라서 사용자의 무선 네트워크에서 공식적으로 사용되고 있는 액세스 포인트들의 MAC 주소를 입력한다.
   가. **Add AP** 버튼을 클릭한다.
      802.11 Options 탭에 있는 새 항목의 **MAC Address** 난을 클릭한다.
   나. 무선 네트워크에서 관측되는 액세스 포인트의 MAC 주소를 **MAC Address** 난에 입력한다. 16 진수 형식의 모든 주소 값을 입력해야 한다. 적절한 길이와 형식(12 문자, 16 진수 만)에 맞지 않는 주소는 입력할 수 없다. 만약 사용자의 네트워크에 있는 액세스 포인트들의 16 진수 전체 주소를 알고 있지 않다면, '*Access Point 의 16 진수 주소 결정하기*' 를 참조하자.
   다. 정상적인 MAC 주소가 입력되면, IP Address 난에 IP 주소를 입력할 수 있다.IP 주소는 오직 사용자가 참고하기 위한 정보이며, 액세스 포인트들이 rogue 로 표시될 때, Expert 는 단지 MAC 주소만 비교한다.
   라. 사용자의 무선 네트워크 상에 있는 각 액세스 포인트에 대해 *Step 가*에서 *Step 다*까지를 반복한다.
3. **802.11 Options** 탭에 있는 항목들 가운데 **Enable Rogue AP Lookup** 옵션을 선택한다.
4. Expert Properties 대화 상자에서 **OK** 버튼을 클릭한다.

Rogue AP Lookup 옵션을 선택하고 **OK** 를 클릭했다면, 패킷을 캡처하거나 파일을 불러오는 동안에 Expert 는 새롭게 검색된 액세스 포인트의 MAC 주소를 **802.11 Options** 탭에서 입력한 주소와 비교할 것이다. 비교 결과 검색된 MAC 주소가 목록에 없다면, Expert Summary 와 Detail 화면에 rogue 로 표시될 것이다. 더불어서 검색된 각 rogue AP 에 대해서 **Rogue Access Point** 알람이 생성될 것이다.

Access Point 의 16 진수 주소 결정하기

사용자의 네트워크에서 사용되는 액세스 포인트의 16 진수 주소 전체를 모르고 있다면, 먼저 액세스 포인트 자체를 확인해 볼 필요가 있다. 종종, MAC 주소는 장비 자체에 기록되어 있다.

만약 기록되어 있지 않다면, 사용자는 Expert 화면을 사용하여 해당 주소를 검색할 수 잇다. 그렇지만, 대부분의 Expert 화면은 16 진수 MAC 주소의 앞부분을 공급자 ID 로(즉, 16 진수 0020d8014060 주소는 통상적으로 Expert 화면에서 Netwav014060 으로 표현) 표시하기 때문에, 사용자는 Expert 화면에서 전체 주소가 모두 16 진수로 표시되게 하는 방법을 알아야 한다. 아래 과정으로 이 주소 값을 확인한다.

액세스 포인트의 16 진수 주소 결정

1. 결정하려고 하는 액세스 포인트의 주소를 포함하고 있는 네트워크에서 패킷을 캡처한다. 다른 방법은 해당 네트워크에서 이미 캡처된 파일을 읽어오는 것이다.

2. Expert 화면의 Outline 창에서 Wireless 계층을 선택하고 우측의 Summary 창에서 Station Function 열을 살펴본다. 이 열에는 **Access Point** 라고 하는 항목이 있다. 이 항목을 선택한다.

   Detail 창은 Summary 창에서 선택한 항목에 대한 통계 자료를 보여주도록 자동 업데이트 한다.

3. Detail 창에서 Wireless Address 필드 쪽으로 이동한다. 이 필드는 선택된 액세스 포인트의 MAC 주소를 모두 16 진수의 형태로 보여준다. 일반 문자로 표기되는 주소의 앞 부분이 공급자의 ID 로 표시되어 있지 않다.
4. 네트워크에 있는 모든 액세스 포인트에 대해서 위 과정을 반복하여 각각의 주소들을 모두 16 진수 형태로 찾아낸다.

4. 캡처 된 데이터를 화면에 표시하기

캡처 버퍼나 캡처 파일에 저장된 패킷을 디코드하고 관찰하거나(packet display) Expert 분석 결과를 보기(Expert display) 위하여 *Display* 항목을 사용한다.

캡처 버퍼 및 이와 관련된 Expert 분석 내용을 화면에 표시하려면, 캡처 세션이 활성화되어 있는 동안 메인 툴 바에 있는 ‘ Stop and Display’ 버튼을 클릭하거나 캡처 세션이 종료된 후에 ‘ Display’ 버튼을 클릭한다. 캡처 파일을 열기 위해서는 **File** 메뉴에서 **Open** 을 선택한다.

또한 Expert 표시는 캡처를 시작할 때, Expert 분석을 실시간으로 지켜보기 위하여 활성화시킬 수 있다. (캡처 동안에 실시간 Expert 분석을 하지않기 위해서는 **Tools** 메뉴에서 **Expert Options** 를 선택하고 **Expert During Capture** 박스를 마크하지 않은 상태로 두어야 한다.)

주 --

캡처 결과를 최초로 볼 때, Expert 표시는 캡처 세션동안 분석된 모든 트래픽을 보여준다. 만일 그 내용을 화면에 다시 표시하면, Expert 는 캡처 버퍼에 있는 패킷을 다시 분석하고 그 결과를 화면에 표시한다. 만일 캡처 버퍼가 캡처 동안에 중첩되었다면 화면에 표시된 결과는 다를 수도 있다. 캡처된 패킷들을 파일에 저장할 때, **Save Expert Objects** 옵션을 선택하고 저장된 파일을 다시 불러들일 때 **Load Expert Objects** 옵션을 선택하면, 위 상황이 발생하는 것을 방지할 수 있다.

디코드 된 패킷과 Expert 분석 내용을 화면에 표시하기 전에 디스플레이 필터를 적용할 수 있다. 디스플레이 필터들은 당신의 네트워크 분석에 필요한 특정 데이터 만을 관찰할 수 있도록 해준다. 또한 Expert 데이터가 화면에 표시되는 방법을 지정하도록 Expert 옵션을 설정해야 한다. Expert 옵션들은 *Expert 옵션(Expert Options)*에서 설명되었다.

디스플레이 필터 (Display Filters)

디스플레이 필터는 캡처 된 데이터를 화면에 표시하는데 사용되는 필터이다. 디스플레이 필터는 원하는 데이터를 선택하여 화면에 표시할 수 있도록 한다. 디스플레이 필터 아래와 같은 내용만 보이도록 사용할 수 있다.

- 네트워크 노드 혹은 주소 쌍간에 전송된 패킷들.
- 하나 또는 여러 프로토콜 그룹에 속한 패킷들
- 미리 지정한 데이터 패턴에 맞는 패킷들
- 에러 패킷들
- 임의의 크기 영역에 포함되는 패킷들
- 위의 내용들을 여러 가지로 조합한 사항에 맞는 패킷들

또한 특별한 네트워크 object, symptom 또는 diagnosis 와 관련된 데이터만 디스플레이 하도록 자동 Expert 필터를 지정할 수 있다. 보다 상세한 내용은 *자동 Expert 디스플레이 필터 정의하기*를 참조한다.

디스플레이 필터는 캡처 버퍼의 내용에 영향을 주지 않는다. 이러한 필터들은 단지 일부 데이터가 화면에 표시되지 않도록 하는 것이다.

디스플레이 필터를 적용시키면, 필터링 된 데이터들이 창의 하단의 새로운 탭(filtered n) 에서 보여진다. 원하는 만큼의 디스플레이 필터를 적용할 수 있으며, 각 필터가 적용될 때 마다 창의 하단에 새로운 탭이 추가된다.

창의 하단에 Filterd n 이라고 이름이 붙어서 추가되어 있는 탭에서 마우스 우측 버튼을 클릭하면 해당 창을 닫을 수도 있다. 또한 원하는 탭을 선택한 후에 File 메뉴에 있는 Save As 명령을 선택하여 해당 창에 있는 필터링 된 패킷들을 따로 저장할 수 있다. 이 때에는 필터링 된 프레임들만 포함되어 있는 새로운 창이 생성되며, 나머지는 Save As 대화 상자 에서 필요한 정보를 입력한 후에 저장하면 된다.

필터의 정의 방법에 대한 내용은 *제 5 장 필터와 트리거 정의하기(Defining Filters and Triggers)*를 참조한다.

패킷 디스플레이 (Packet Display)

캡처 버퍼나 캡처 파일의 내용을 디스플레이 할 때, Sniffer Pro 는 프로토콜 해석기 (*protocol interpreters*)를 이용하여 캡처 된 패킷들에 포함되어 있는 상위 레벨 프로토콜을 해석하고 디코드 한다. Sniffer Pro 는 200 종류 이상의 서로 다른 네트워크 프로토콜을 디코드 한다.

디코드 된 데이터는 다양한 형식으로 디스플레이 할 수 있다. 각각의 형식은 디스플레이 윈도우 내에 탭으로 나타난다. 이러한 형식에는 Decode, Matrix, Host Table, Protocol Distribution, Statistic, 그리고 Expert 가 있다.

주 --

Matrix, Host Table, Protocol Distribution, 그리고 Statistics 탭들은 **Display Setup** 대화상자의 **General** 탭에서 **Post analysis tabs** 상자가 체크되어 있어야만, 디스플레이 윈도우의 아래 부분에 나타난다. 이와 비슷하게 Expert 탭은 **Expert tab** 상자가 체크되어 있어야만 나타난다.

디코드 탭(Decode Tab)

디코드 탭은 패킷을 3 가지 색상을 이용하여 *summary, detail, hex* 의 3 가지 창을 보여준다.

- *Summary* 창은 줄단위의 요약된 형태로 캡처 된 패킷의 전체 내용을 보여준다.
- *Detail* 창은 현재 summary 창에서 선택된 패킷의 자세한 내용을 보여준다. 각 계층의 프로토콜이 해석되어 화면에 표시된다.

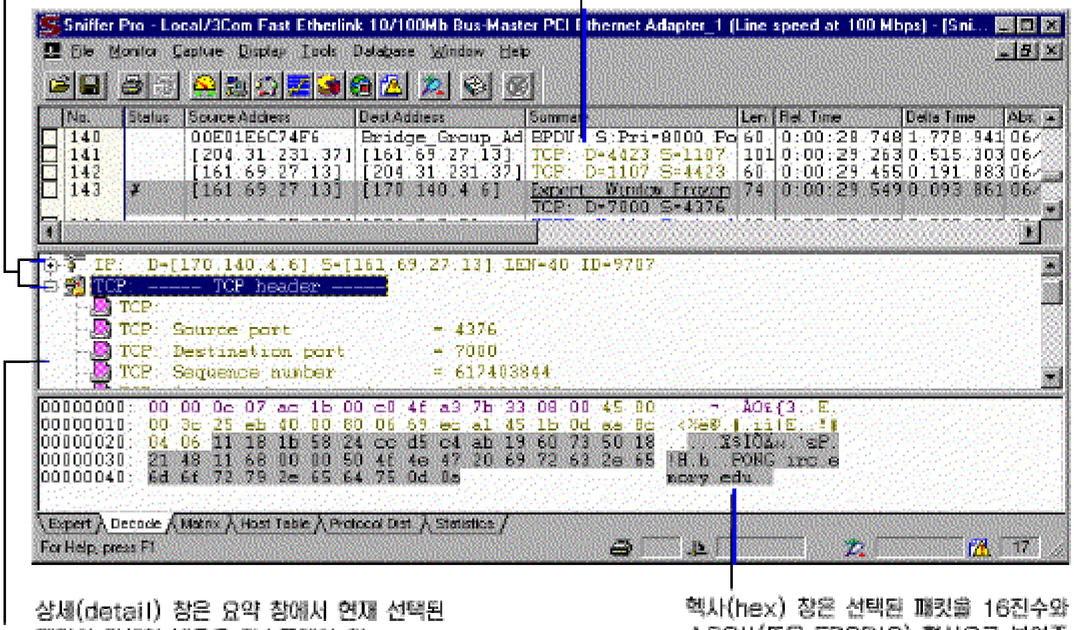
  Detail 프로토콜 창은 완전히 확장된 디코드, 한 라인 요약, 두 가지가 혼합된 형태의 3 가지 시점으로 디스플레이 할 수 있다. 기본적으로 Sniffer Pro 는 detail 창에서 밑줄이 그어진 프로토콜 계층을 확장하여 보여준다. 관찰 영역을 작게 하고 싶다면, 프로토콜 하위계층 줄의 앞에 있는 (-) 기호를 클릭한다. 프로토콜 디스플레이를 다시 확장하려면, (+) 기호를 클릭한다.
- *Hex* 창은 선택된 패킷을 16 진수 코드와 ASCII(혹은 EBCDIC) 형태로 보여준다.

  Summary 창서 한 패킷을, 혹은 detail 창에서 하나의 상세한 프로토콜 필드를 선택한 경우, 패킷 내부에 있는 동일한 16 진수 옥텟(octets)들이 hex 창에 강조되어 나타난다. 이것은 프로토콜 필드 및 패킷 내에서 그에 상응하는 바이트들과의 상관 관계를 빠르게 보여준다.

그림 4-1 은 디코드 디스플레이(Decode display)를 보여준다.

프로토콜 디스플레이를 줄이려면 (-) 기호를 클릭하고 확장하려면 (+) 기호를 클릭

summary 창은 캡처된 패킷의 개요를 라인단위의 요약된 형식으로 보여줌.


Sniffer Pro - Local/3Com Fast Etherlink 10/100Mb Bus-Master PCI Ethernet Adapter_1 (Line speed at 100 Mbps) - [Sni...
File Monitor Capture Display Tools Database Window Help
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
17

No.	Status	Source Address	Dest Address	Summary	Len	Rel. Time	Delta Time	Abs
140		00E01E6C74F6	Bridge_Group_Ad	BPDU: S:Pri=8000 Po	60	0:00:28.748	1.778.941	06/
141		[204.31.231.37]	[161.69.27.13]	TCP: D=4423 S=1107	101	0:00:29.263	0.515.303	06/
142		[161.69.27.13]	[204.31.231.37]	TCP: D=1107 S=4423	60	0:00:29.455	0.191.883	06/
143	✗	[161.69.27.13]	[170.140.4.6]	Expert: Window Frozen TCP: D=7000 S=4376	74	0:00:29.549	0.093.861	06/

```
IP:  D=[170.140.4.6] S=[161.69.27.13] LEN=40 ID=9707
TCP: ----- TCP header -----
  TCP:
  TCP: Source port            = 4376
  TCP: Destination port       = 7000
  TCP: Sequence number        = 617403844
```

```
00000000: 00 00 0c 07 ac 1b 00 c0 4f a3 7b 33 08 00 45 00  .....¬.ÀOε{3..E.
00000010: 00 3c 25 eb 40 00 80 06 69 ec a1 45 1b 0d aa 8c  .<%ë@...iì¡E..ª.
00000020: 04 06 11 18 1b 58 24 cc d5 c4 ab 19 60 73 50 18  .....X$ÌÕÄ«.`sP.
00000030: 21 48 11 68 00 00 50 4f 4e 47 20 69 72 63 2e 65  !H.h..PONG irc.e
00000040: 6d 6f 72 79 2e 65 64 75 0d 0a                    mory.edu..
```

상세(detail) 창은 요약 창에서 현재 선택된 패킷의 자세한 내용을 디스플레이 함.

헥사(hex) 창은 선택된 패킷을 16진수와 ASCII(또는 EBCDIC) 형식으로 보여줌

그림 4-1. 디코드 탭

디스플레이 조작(Navigating the Display) : 키(key)들의 기능 익히기

디스플레이를 조작하기 위하여 아래와 같은 키들을 사용하며, 또한 Display 메뉴에 있는 명령어들을 사용할 수 있다.

Page UP	활성 영역에서 이전 페이지 보기.
Page Down	활성 창에서 다음 페이지 보기.
Cursor Up	활성 창에서 이전 라인 보기.
Cursor Down	활성 창에서 다음 라인 보기.
F2	Summary 창에서 다음으로 선택된 패킷 찾기.
Shift+F2	Summary 창에서 이전에 선택된 패킷 찾기.
Control+F2	해당 패킷을 선택되지 않은 상태에서 선택된 상태로 전환.
F3	지정한 문자열, 데이터 패턴, 상태에 맞는 다음 인스턴트 찾기.
Alt+F3	Search Packet 대화 상자 열기
F4	디코드 디스플레이의 확대/축소
F7	Summary 창에서 이전 패킷 보기
F8	Summary 창에서 다음 패킷 보기

패킷 선택하기(Selecting Packets)

Sniffer Pro는 사용자가 summary 창에서 개별적인 패킷이나 한 그룹의 패킷을 선택할 수

있도록 한다. 패킷을 선택하는 기능은 당신에게 흥미 있는 키 패킷들을 표시할 수 있도록 하며, 따라서 그러한 패킷들을 보다 쉽게 사용할 수 있다. 이 기능을 사용하여 다음과 같은 작업을 할 수 있다.

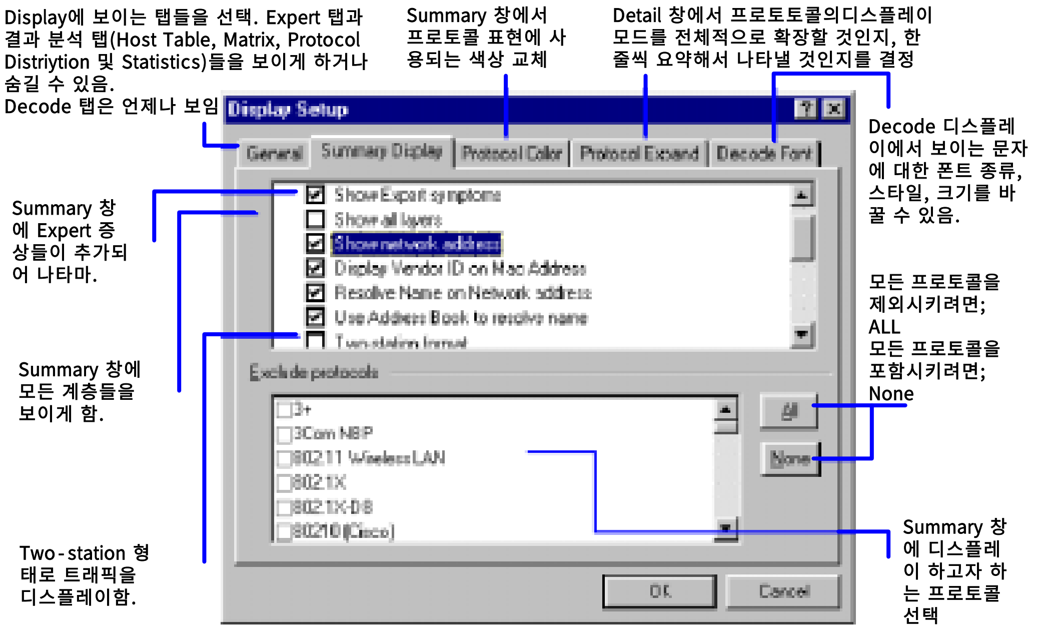
- 선택된 패킷을 관찰하기 위하여 분리된 다른 윈도우에 저장.
- 선택된 패킷을 파일에 저장.
- 선택된 패킷들을 북 마크로 하여, F2 를 이용하여 선택된 한 패킷에서 다음 패킷으로 이동

디스플레이 옵션 설정하기(Setting Display Options)

디코드 디스플레이에 데이터가 디스플레이 되는 방법은 사용자가 정의할 수 있다. 정의할 수 있는 내용은 아래와 같다.

- 어떤 서브 프로토콜을 summary 창에서 제거.(이 항목은 디스플레이 필터에서 보다 좀 더 상세한 통제 방법이다.)
- Summary 주소 필드의 형식 지정 (네트워크 혹은 하드웨어).
- 두 스테이션 디스플레이 형식이 사용되어야 하는지 명시.
- Summary 디스플레이에 보여지는 추가적인 필드의 선택.
- 프로토콜에 따라 summary 창에 디스플레이 되는 패킷들의 색상 코드.
- Detail 디스플레이에 사용되는 폰트 선택.

디스플레이 옵션을 설정기 위해서는 Display 메뉴에서 Display Setup 을 선택한다. *그림 4-2*는 Display Setup 대화 상자를 보여주고 있다.



Display에 보이는 탭들을 선택. Expert 탭과 결과 분석 탭(Host Table, Matrix, Protocol Distriytion 및 Statistics)들을 보이게 하거나 숨길 수 있음. Decode 탭은 언제나 보임

Summary 창에서 프로토콜 표현에 사용되는 색상 교체

Detail 창에서 프로토토토콜의디스플레이 모드를 전체적으로 확장할 것인지, 한 줄씩 요약해서 나타낼 것인지를 결정

Decode 디스플레이에서 보이는 문자에 대한 폰트 종류, 스타일, 크기를 바꿀 수 있음.

Summary 창에 Expert 증상들이 추가되어 나타마.

Summary 창에 모든 계층들을 보이게 함.

모든 프로토콜을 제외시키려면; ALL 모든 프로토콜을 포함시키려면; None

Two-station 형태로 트래픽을 디스플레이함.

Summary 창에 디스플레이 하고자 하는 프로토콜 선택

Display Setup

☑ Show Expert symptoms
□ Show all layers
☑ Show network address
☑ Display Vendor ID on Mac Address
☑ Resolve Name on Network address
☑ Use Address Book to resolve name
□ Two-station format

Exclude protocols

□ 3+
□ 3Com NBP
□ 802.11 Wireless LAN
□ 802.1X
□ 802.1X-D8
□ 80210 (Cisco)

그림 4-2. 디스플레이 옵션 설정

Summary 디스플레이 옵션에 대하여

*그림 4-2*에서 다음과 같은 Summary 디스플레이 옵션을 설정할 수 있다.

Show Expert symptoms
‘ Enable’ 이라면, Summary 디스플레이는 각 프레임에 대하여 검출된 최종 증상(symptom)을 보여준다.

Show all layers
‘ Enable’ 이라면, Summary 관찰은 한 프레임에 저장된 각 프로토콜 레벨을 한 라인에 보여준다. ‘ Disable’ 이라면, 채택된 최상위 프로토콜 레벨에 대하여 한 라인을 보여준다.

Show network address
‘ Enable’ 이라면, Summary 관찰은 네트워크 주소를 보여준다. ‘ Disable’ 이라면, Summary 관찰은 하드웨어(DLC) 주소를 보여준다.

Resolve name on MAC address
‘ Enable’ 이라면, Summary 관찰은 MAC 주소를 숫자로 표시되는 주소가 아닌 이름으로 보여준다.

Resolve name on Network address
‘ Enable’ 이라면, Summary 관찰은 네트워크 주소를 숫자로 표시되는 주소가 아닌 이름으로 보여준다.

Use Address Book to resolve name
‘ Enable’ 이라면, Summary 관찰은 주소록(Address Book)에 이름이 등록된 임의의 스테이션에 대한 주소를 적절한 이름으로 보여준다.

Two-station format
‘ Enable’ 이라면, 디스플레이 영역을 좌, 우측 창으로 분리하여, 두 스테이션 간의 트래픽을 보여준다.

선택적인 필드

Status
프레임과 관련된 플래그(flag)를 보여준다. Status 열에는 어떤 플래그들이 나타날 수 있는지에 대한 내용은 *Summary 화면에서 패킷 상태 표시 기호*를 참조하자.

Absolute time	프레임이 수신되었을 때, 보여준다.
Delta time	현재 프레임과 이전 프레임 사이의 간격을 보여준다.
Relative time	현재 프레임과 표시된 프레임 사이의 간격을 보여준다.
(Len)Bytes	프레임의 길이를 보여준다.
Cumulative bytes	표시된 프레임에서 시작하여 현재 프레임을 포함한 모든 프레임의 길이를 보여준다.

Two-Station 형식에 대하여

네트워크의 활동성을 시험할 때, 두 스테이션 사이의 트래픽에만 초점을 맞추고 싶은 경우가 있다. 이 경우, 두 스테이션을 정의하는 디스플레이 필터를 설정하고 Display Setup 대화 상자의 Summary Display 탭에서 **Two-station format** 을 ‘ enable’ 로 설정한다. 이 대화 상자는 **Display** 메뉴에서 **Display Setup** 을 선택하여 액세스할 수 있다.

두 스테이션 형식은 화면의 왼쪽에 있는 먼저 검출된 한 스테이션에서의 전송과 오른쪽에 있는 다른 스테이션에서의 전송들을 보여준다. 단일 스테이션 디스플레이에서 Source 와 Destination 항목은 제거된다. 그 대신 **From** *xxx* 와 **From** *yyy* 라고 제목 붙은 두 가지 항목이 있다. 프레임은 좌측에 있는 스테이션에서 우측에 있는 스테이션으로 주소가 지정된 채 옮겨지며, 그 반대도 동일하다.

Summary 화면에 있는 패킷 상태 플래그(Status flag)

대부분의 네트워크 토폴로지에서 만약 패킷이 정상적이고 error, symptom, diagnoses 등이 발견되지 않는다면, 아래와 같은 경우를 제외하고 Summary 창에 있는 **Status** 열은 빈 공간으로 남아 있다.

- 무선 LAN 상에서 캡처된 데이터에 대해서는 Status 열에 있는 플래그가 해당 패킷이 캡처된 무선 LAN 채널 번호를 의미한다. 예를 들어, Status 열에 [1]이라고 표시되어 있다면, 이것은 해당 패킷이 무선 LAN 1 번 채널에서 캡처 되었다는 것이다.
- 네트워크 pod(SnifferBook Ultra 와 같은)나 멀티 포트 어댑터 카드(Full Duplex Ethernet PCI card 같은)로부터 캡처된 데이터의 경우에는 **Status** 열의 표시가 해당 패킷이 캡처된 pod 나 card 를 나타낸다. 예를 들어, Status 열에 [A]라고 표시되어 있다면, 이것은 해당 패킷이 pod 나 카드 상에 있는 Port A 에서 캡처 되었음을 의미한다. 이러한 표시는 SnifferBook 이 사용되는 위치에 따라서 DCE 와 DTE 방향이 바뀔 수 있는 Packet over Sonet(PoS)에서 패킷을 캡처하는 경우데 유용한 방법이다.

다음의 내용은 Summary 창의 Status 열에서 사용되는 플래그 목록이다.

- M 해당 패킷이 선택 표기되었음. 특정 패킷을 표기 하면, 다른 패킷을 점검 하다가 표시된 패킷으로 빠르게 돌아올 수 있음.
- A 패킷이 pod 나 어댑터 카드 상에 있는 Port A 에서 캡처 되었음.
- B 패킷이 pod 나 어댑터 카드 상에 있는 Port B 에서 캡처 되었음.
- # 해당 패킷과 관련된 symptom 이나 diagnoses 가 포함되어 있음.
- Trigger 해당 패킷이 event filter trigger 임.
- CRC 정상적인 크기이지만 CRC 에러가 있는 패킷.
- Jabber 패킷이 비정상적으로 크고 CRC 에러가 있는 패킷.
- Runt 패킷 크기는 64 bytes(4 CRC bytes 포함)보다 작지만, CRC 에러는 없음.
- Fragment 패킷 크기는 64 bytes(4 CRC bytes 포함)보다 작고, CRC 에러가 있음.
- Oversize 패킷 크기가 1518(4 CRC bytes 포함)보다 크지만, CRC 에러는 없음.
- Collision Collision 에 의해서 패킷이 손상되었음.
- Alignment 패킷의 길이가 8 bits 의 정수 배수가 아님.
- Dup Address Ring(Token Ring) 내에서 주소가 충돌이 있음
- Frame Copy 도착지 호스트(Token Ring)에서 해당 패킷이 복사되지(수신되지) 않았음.

ATM 어댑터에 대한 상태 플래그

표준 상태 표시와 더불어, ATM 어댑터에서는 아래와 같은 추가적인 표시가 있다.

- AAL5 Length AAL5 length error 가 있음.
- AAL5 Max Seg AAL5 Maximum Segments error 가 있음.
- Timeout Timeout error 가 있음.
- Buffer Buffer error 가 있음.
- Unknown Unknown error 가 있음
- AAL2 0 STF 의 패리티가 전송 에러를 지정함; complete CPS-PDU 가 버려짐.
- AAL2 1 STF 의 시퀀스 번호가 틀림; 만약 OSF 가 47 보다 작다면, 처리 과정은 OSF 에 의해 지정되는 Octet 에서 시작하며, 그렇지 않다면, complete CPS-PDU 는 버려짐.
- AAL2 2 해당 CPS-PDU 내에 오버랩하는(overlapping) CPS-Packet 에 대해 예상되는 octet 수가 STF 내에 포함되어 있는 정보와 대응되지 않음; OSF 의 값이 47 보다 작다면, 처리 과정은 OSF 가 지정하는 octet 에서 시작함.
- AAL2 3 STF 의 OSF 가 48 또는 보다 큰 값을 가지고 있음; complete

CPS-PDU 는 버려짐

- AAL2 4 CPS-Packet 헤더의 HEC(Header Error Control) Code 가 CPS-Packet 헤더 내에 전송 에러가 있음을 지적함; CPS-PDU 내에서 처리되지 않은 정보는 버려짐.
- AAL2 5 수신된 CPS-Packet Payload(CPS-SDU)의 길이가 " Max_SDU_Deliver_length" 에서 지적하는 최대 길이를 초과.
- AAL2 6 일부 CPS-Packet 이 먼저 수신되었으며, CPS-Packet 이 완전하게 재구성되기 전에 에러로 검색되어 버려졌을 것임.
- AAL2 7 일부 CPS-Packet 이 먼저 수신되었으며, CPS-Packet 이 완전하게 재구성되기 전에 에러로 검색되어 버려졌을 것임.
- AAL2 8 수신된 CPS-Packet 헤더의 UUI 필드에 " 28" 또는 " 29" 값이 포함되어 있음. 이 값들은 이후의 표준화를 위해 예약된 것임.
- AAL2 9 수신된 CPS-Packet 헤더 내의 CID 값이 SAP 와 관련 없음.

나머지 상태 에러 메시지 AAL2 IP 0, AAL2 IP 1, AAL2 IP 2 들은 근본적으로 AAL2 0, AAL2, 1 및 AAL2 2 에러이며, 각 에러는 결과적으로 INCOMPLETE PACKET(IP)을 의미한다. 즉, 이러한 에러가 발생했을 때, 한 개의 AAL2 패킷이 ATM 셀들을 가로질러서 재구성 되는 과정 속에 존재하게 된다.

- AAL2 IP 0 STF 의 패리티가 전송 에러를 지적하고 재구성되는 패킷에서 이전 셀이 버려졌을 수도 있음.
- AAL2 IP 1 STF 의 시퀀스 번호가 틀리며, 재구성되는 패킷에서 이전 셀이 버려졌을 수도 있음.
- AAL2 IP 2 해당 CPS-PDU 내에 오버랩하는(overlapping) CPS-Packet 에 대해 예상되는 octet 수가 STF 내에 포함되어 있는 정보와 대응되지 않음. 재구성되는 패킷에서 이전 셀이 버려졌을 수도 있음.

Decode 화면에서 프레임 찾기

Decode 화면에는 수천, 수 만개의 프레임들이 포함되어 있을 수 있기 때문에, 특별히 원하는 프레임을 찾는다는 것은 매우 유용한 기능이 될 수 있다. Sniffer 의 강력한 검색 기능은 문자열, 특정 데이터 패턴, 특정 상태 플래그(status flag), 또는 Expert symptom 이나 diagnosis 등을 이용하여 원하는 프레임을 손쉽게 찾아낼 수 있다.

주 --

프레임들을 검색하는 기능과 더불어 Decode 탭에서 특정 프레임의 번호를 입력하여 해당 프레임으로 이동할 수도 있다. **Display** 메뉴에서 **Go to Frame** 을 선택하고 화면에 나타

나는 대화 상자에서 해당 프레임 번호를 입력하면 된다.

Find Frame 대화 상자에서 프레임 검색을 시작한다. Find Frame 대화 상자는 아래와 같은 방법으로 나타나게 할 수 있다.

- Display 메뉴에서 Find Frame 을 선택.
- Decode 탭 화면에서 마우스 우측 버튼을 클릭하여 나타나는 메뉴에서 Find Frame 을 선택.
- Alt-F3 단축키를 사용

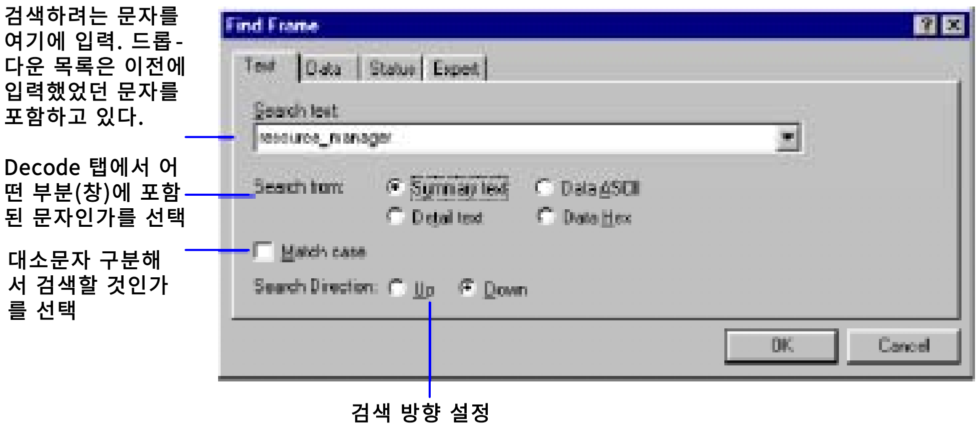
Find Frame 대화 상자에는 아래와 같은 4 개의 박스가 있다.

- Text – Text 탭에서는 특정 문자열이 포함된 프레임을 찾을 수 있다.
- Data – Data 탭에서는 특정 데이터 패턴이 포함된 프레임을 찾을 수 있다.
- Status – Status 탭에서는 특정 상태 플래그(status flag)가 표시된 프레임을 찾을 수 있다.
- Expert – Expert 탭에서는 Expert symptom 이나 diagnosis 가 표시된 프레임을 찾을 수 있다.

다음 단원에서는 앞에서 언급한 각 탭에서의 프레임 검색 방법을 설명한다.

문자열이 포함된 프레임 검색

Find Frame 대화 상자를 열고 Text 탭을 클릭하여 특정 문자열이 포함된 프레임을 찾아낸다. *그림 4-3*은 Find Frame 대화 상자의 Text 탭을 보여주고 있다.


검색하려는 문자를 여기에 입력. 드롭-다운 목록은 이전에 입력했었던 문자를 포함하고 있다.
Decode 탭에서 어떤 부분(창)에 포함된 문자인가를 선택
대소문자 구분해서 검색할 것인가를 선택
검색 방향 설정
Find Frame
Text
Data
Status
Expert
OK
Cancel

Search text: resource_manager

Search from: ● Summary text ○ Data ASCII ○ Detail text ○ Data Hex

□ Match case

Search Direction: ○ Up ● Down

그림 4-3. Find Frame 대화 상자의 Text 탭

찾고자 하는 문자를 입력한 후, OK 버튼을 클릭한다. 만약 해당 문자열 포함된 프레임이 발견되면, Decode 화면에 나타날 것이다. 동일한 문자열이 포함된 다음 패킷을 찾으려면,

F3 키를 누른다.

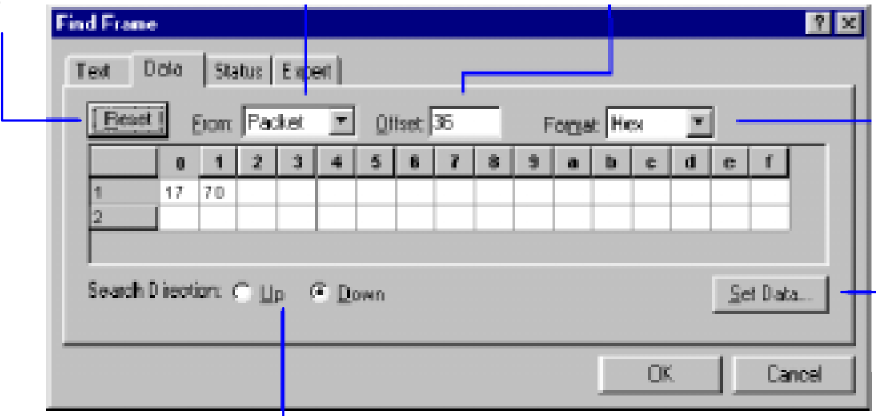
데이터 패턴이 포함된 프레임 검색

데이터 패턴이 포함된 패킷을 찾으려면, Find Frame 대화 상자를 열고 **Data** 탭을 클릭한다. *그림 4-4*에서 Find Frame 대화 상자의 Data 탭을 보였다.

Data 탭에 있는 모든 필드를 초기화

Packet, Protocol 등 데이터 검색 대상 선택

지정된 패턴의 검색 위치에 대한 offset 지정



Find Frame

From: Packet

Offset: 36

Format: Hex

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	17	70														
2																

Search Direction: ○ Up ● Down

검색할 데이터의 형식 지정

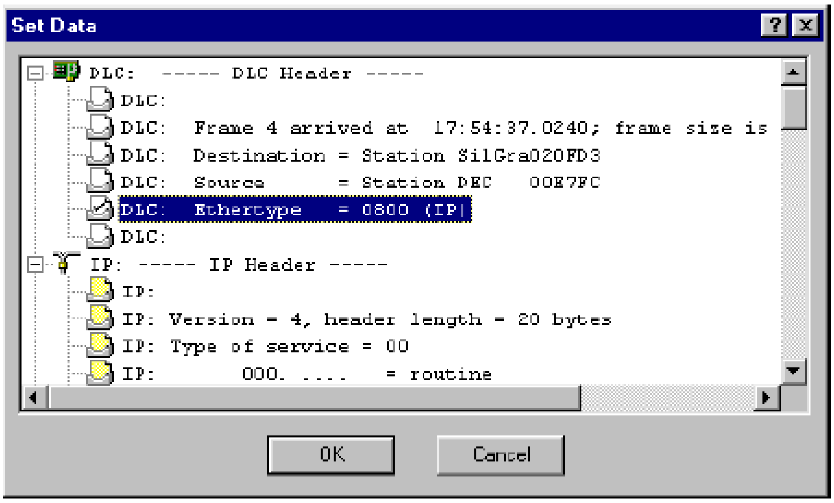
검색 방향 지정

Summary 창에서 선택된 패킷의 모든 디코드 정보를 줄 단위로 보여주는 창을 열기위해 사용. 검색 패턴으로 사용하기 위해 해당 패킷의 디코드 내용 중에 임의의 한 줄을 선택할 수 있음.

그림 4-4. Find Frame 대화 상자의 Data 탭

데이터 패턴을 이용하는 가장 쉬운 검색 방법은 아래와 같이 이미 알고 있는 패킷의 패턴을 사용하는 것이다.

1. 패킷 선택
   - Summary 창에 있는 특정 패킷
   - Detail 창에 있는 프로토콜 필드 또는 데이터 패턴
2. **Display** 메뉴에서 **Find Frame** 명령을 선택하여 (또는 마우스 우측 버튼을 클릭하여 나타나는 메뉴에서) Find Frame 대화 상자를 연다.
3. Data 탭 선택
   - 만약 Summary 창에서 한 패킷을 선택했다면, Data 탭에는 선택된 패킷에 있는 일부 데이터가 이미 포함되어 있을 것이다.
   - Detail 창에서 프로토콜 필드나 데이터 패턴을 선택했다면, Data 탭에는 선택된 필드나 패턴이 이미 포함되어 있을 것이다.
4. **From** 상자에는 **Don' t Care** 로 설정한다.
5. 선택된 패킷의 디코드된 정보를 줄 단위로 포함하고 있는 Set Data 대화 상자를 열기 위해 **Set Data** 버튼을 클릭할 수 있다. (*그림 4-5*)



Set Data

```
⊟ DLC:  ----- DLC Header -----
     DLC:
     DLC:  Frame 4 arrived at  17:54:37.0240; frame size is
     DLC:  Destination = Station SilGra020FD3
     DLC:  Source      = Station DEC    00E7FC
     DLC:  Ethertype   = 0800 (IP)
     DLC:
⊟ IP: ----- IP Header -----
     IP:
     IP: Version = 4, header length = 20 bytes
     IP: Type of service = 00
     IP:       000. ....   = routine
```

그림 4-5. Set Data 대화 상자

6. Set Data 대화 상자에서 한 줄을 선택하고 OK 를 클릭한다.
   선택된 줄에 있는 데이터는 Find Frame 대화 상자의 데이터 패턴 영역에 표시된다. 필요하다면, 데이터와 길이를 수정한다.
7. OK 를 클릭하여 검색을 시작한다.
   패턴이 일치하는 패킷이 발견되면, 해당 패턴을 포함하고 있는 패킷이 Decode 화면에 표시될 것이다. 다음 패킷을 찾으려면 F3 키를 누른다.

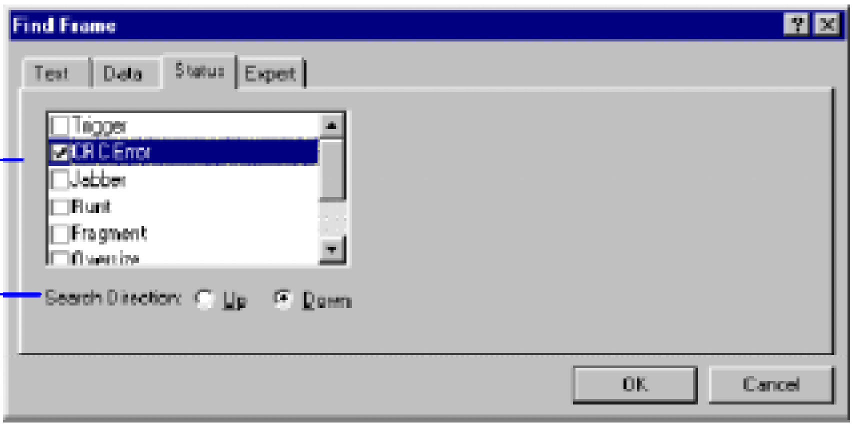
미리 알고 있던 데이터 패턴들을 찾는 것과 더불어, 사용자가 Data 탭 내의 여러 필드에 원하는 데이터 패턴을 입력해 넣을 수도 있다.

상태 플래그(status flag)가 표시된 프레임 검색

Find Frame 대화 상자를 열고 Status 탭을 클릭하면, 특별한 Status 플래그가 표시된 패킷을 검색할 수 있다. *그림 4-6*은 Find Frame 대화 상자의 Status 탭 화면이다.

찾으려고 하는 상태 플래그 선택

검색 방향 지정



Find Frame

□ Trigger
☑ CRC Error
□ Jabber
□ Runt
□ Fragment
□ Oversize

Search Direction: ○ Up ● Down

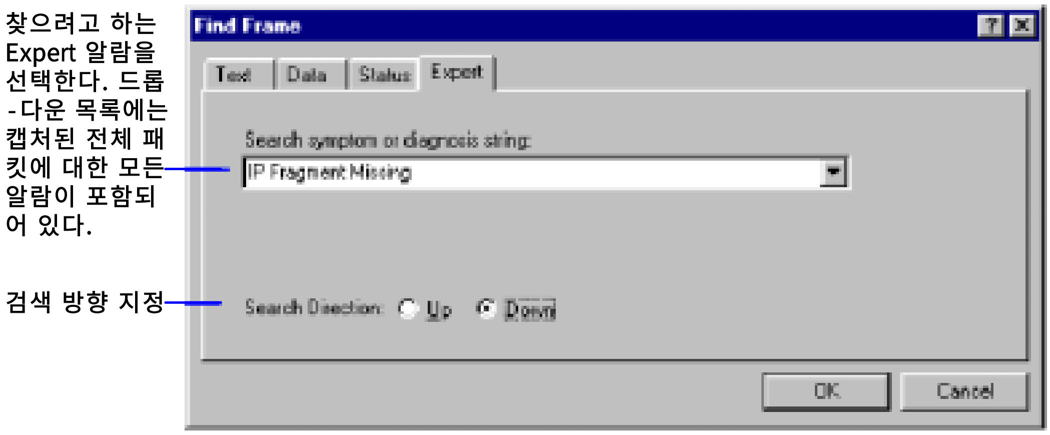
그림 4-6. Find Frame 대화 상자의 Status 탭

찾으려고 하는 플래그를 선택했으며, OK 를 클릭하여 검색을 시작한다. 만약 지정한 플래그가 표시된 프레임이 발견되면, 해당 프레임은 Decode 화면에 표시될 것이다. 계속해서 다음 프레임을 찾으려면, F3 키를 누른다.

여러 가지 패킷 상태 플래그에 대한 설명은 앞에서 설명한 *Summary 화면에 있는 패킷 상태 플래그*를 참고하자.

Expert 알람들이 있는 프레임 검색

Find Frame 대화 상자를 열고 Expert 탭을 클릭하면, 특별한 Expert symptom 이나 diagnosis 가 포함된 패킷들을 검색할 수 있다. *그림 4-7* 은 Find Frame 대화 상자의 Expert 탭을 보여주고 있다.


찾으려고 하는 Expert 알람을 선택한다. 드롭-다운 목록에는 캡처된 전체 패킷에 대한 모든 알람이 포함되어 있다.
검색 방향 지정
Find Frame
Text
Data
Status
Expert
OK
Cancel

Search symptom or diagnosis string: IP Fragment Missing

Search Direction: ○ Up ● Down

그림 4-7. Find Frame 대화 상자의 Expert 탭

찾으려고 하는 Expert 알람을 지정했으면, OK 를 클릭하여 검색을 시작한다. 지정된 Expert 알람이 포함되어 있는 프레임이 발견되면, Decode 화면에 해당 프레임이 표시될 것이다. 계속해서 다음 프레임을 찾으려면, F3 키를 누른다.

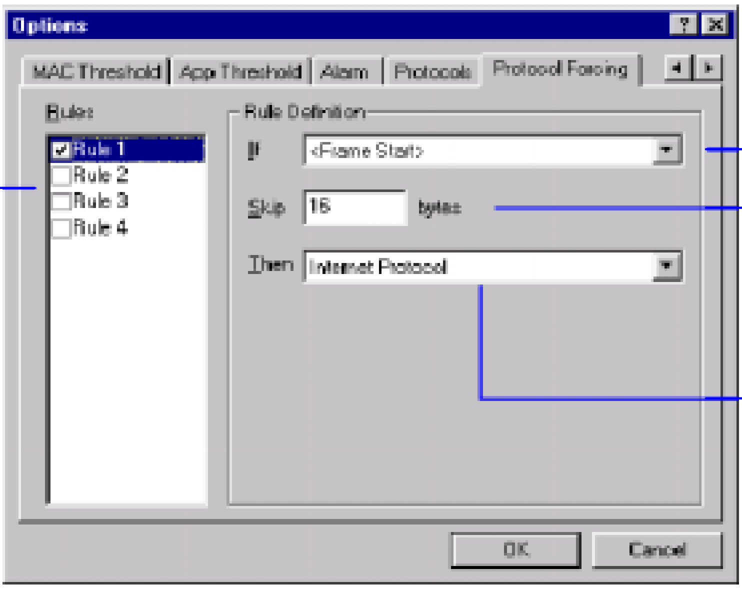
프로토콜 강제 지정 사용하기(Using Protocol Forcing)

프로토콜 강제 지정 기능은 표준적인 프로토콜 그리고 Sniffer Pro 가 어떻게든지 디코드할 수 없을 수도 있는 비 표준적인 프로토콜을 혼합하여 사용하는 프레임을 캡처 할 경우에 유용하다. 예를 들어, 어떤 스테이션에서는 분석할 수 없는 자기 독점적인 하위 계층 패킷 형식 내에 표준 IP 데이터를 네트워크가 포함하고 있을 수도 있다. 프로토콜 강제지정은 기본적으로 당신이 " 만일 이 경우를 만나면, 주어진 만큼의 바이트 수를 건너뛰고(표준 데이터가 있는 곳까지), 이 프로토콜을 적용하라" 하고 분석기에서 알려줄 수 있다.

프로토콜 강제 지정 규칙은 분석기(analyzer)의 Tools 메뉴에서 Options 명령을 선택하면

디스플레이 되는 옵션 대화 상자의 Protocol Forcing 탭에서 입력한다. (*그림 4-8*)

"force from" 처럼 패킷 내에서 특정 프로토콜의 시작 위치를 지정하기 위해 드롭 다운 목록을 사용. 분석기가 이곳에 지정된 조건을 만나면, Skip xx bytes 필드에 입력된 바이트 수만큼 스킵하여, Then 필드에서 선택된 프로토콜 해석기를 사용.



Options

MAC Threshold | App Threshold | Alarm | Protocols | Protocol Forcing

Rules:
☑ Rule 1
□ Rule 2
□ Rule 3
□ Rule 4

Rule Definition
If <Frame Start>
Skip 16 bytes
Then Internet Protocol

4 가지 정도의 규칙을 정의할 수 있음. 선택된 규칙은 활성화되어 디코드되는 데이터에 적용됨.

If 조건이 만족되었을 때, 스킵하는 바이트 수를 지정

"force to"에 의해 적용되는 프로토콜을 지정하기 위해 드롭 다운 목록에서 선택. 즉, 이곳에 지정된 프로토콜이 Skip xx bytes 필드에 입력된 offset 이후에 적용됨.

그림 4-8. 프로토콜 강제 지정의 규칙 정의하기

매트릭스 탭(Matrix Tab)

매트릭스 탭은 네트워크 노드 간의 통신에 대한 통계 자료를 수집한다.

- LAN 에 대해서, 매트릭스 탭은 MAC, IP 네트워크 그리고 IP 어플리케이션, IPX 네트워크, 그리고 IPX 전송 계층 정보를 누적한다.
- WAN 에 대해서, 매트릭스 탭은 Options 대화 상자에서 선택된 캡슐화 프로토콜에 의존하는 SDLC, 가상 회선, 혹은 HDLC 와 같은 연결계층 및 IP 네트워크, IP 어플리케이션, IPX 네트워크, 그리고 IPX 전송계층 정보를 누적한다.

누적된 데이터는 트래픽 맵, 테이블, 혹은 막대나 파이 차트를 이용하여 볼 수 있다.

- *트래픽 맵(traffic map)*은 노드간의 네트워크 트래픽 패턴에 대한 직관적인 관찰을 제공한다. 임의의 프로토콜을 마크하지 않거나 디스플레이 하는 특정 네트워크 노드들을 선택하여 원하지 않는 트래픽을 제거할 수 있다.
- *매트릭스 테이블(matrix table)*은 노드 쌍에 대한 트래픽 총계를 디스플레이 한다.
  - *Outline table* 은 두 네트워크 노드 간에 전송된 전체 바이트와 패킷에 대하여 정리한 내용을 제공한다.
  - *Detail table* 은 상위 계층 프로토콜 유형과 각 통신 노드 쌍 사이에 입출력 되는 트래픽 부하에 대하여 정리된 정보를 제공한다.

특정 열의 제목을 클릭하여 매트릭스 테이블을 정리할 수 있다. 예를 들어, 통계 자료를 패킷 별로 정렬하려면, Packets 열의 제목을 클릭한다. 해당 제목을 두 번 클릭하면 역순으로 정렬된다.

- *막대 차트*는 10 개의 가장 분주한 노드 쌍을 디스플레이 한다.
- *파이 차트*는 10 개의 가장 분주한 노드 쌍을 전체 트래픽 부하에 대한 비율(%)로서 디스플레이 한다.

모든 관찰 내용에는 연결 계층, MAC 계층에서의 대화 트래픽을 디스플레이 할 수 있으며, 단지 IP 혹은 IPX 하나만을 선택적으로 관찰 할 수도 있다. 테이블 형태의 관찰에서 통계 자료는 일반적인 표 형식이나 차트 형식으로 변환할 수 있다.

*그림 4-9*는 매트릭스 화면(막대 차트)과 해당 툴바를 보여주고 있다.

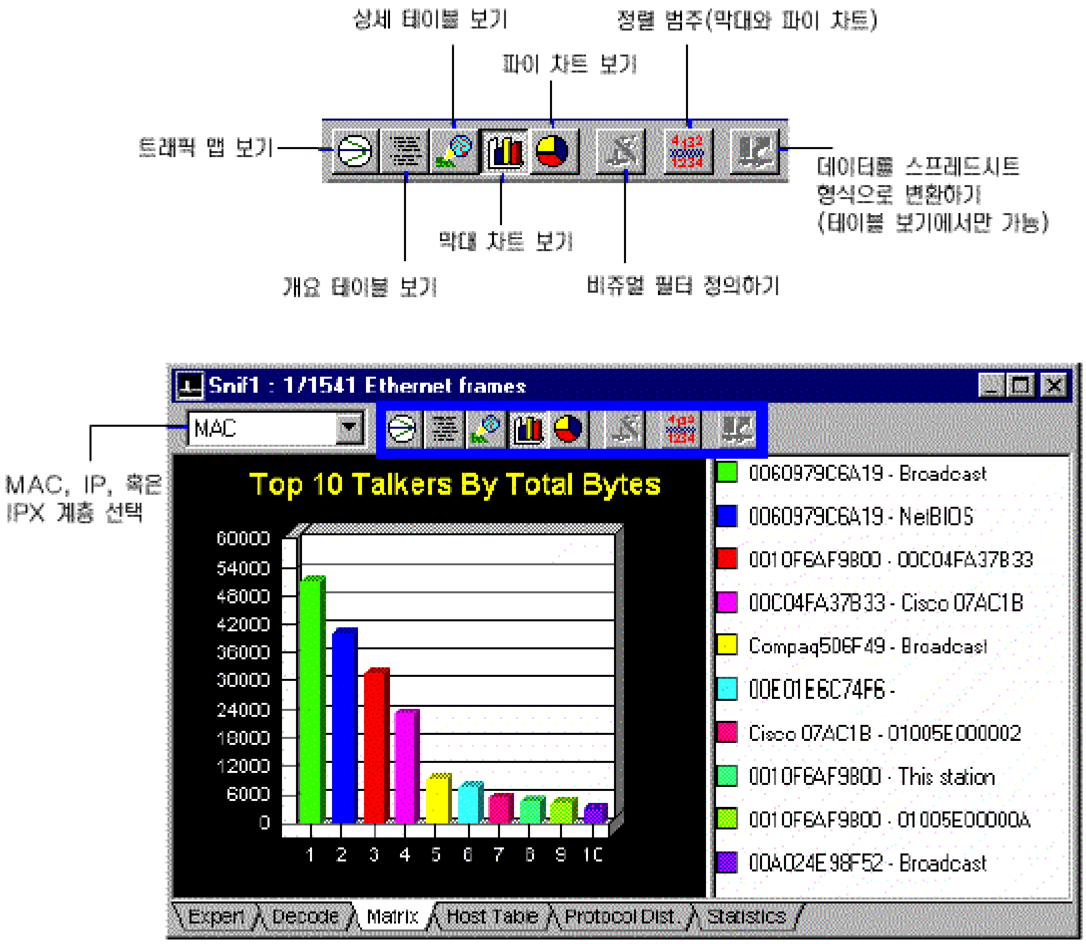


그림 4-9. 매트릭스 화면(막대 차트)과 툴바

호스트 테이블 탭(Host Table Tab)

호스트 테이블은 각 네트워크 노드의 트래픽 통계 자료를 수집한다.

- LAN 에 대해서, 호스트 테이블 탭은 MAC, IP 네트워크 그리고 IP 어플리케이션, IPX 네트워크, 그리고 IPX 전송 계층 정보를 누적한다.
- WAN 에 대해서, 호스트 테이블 탭은 Options 대화 상자에서 선택된 캡슐화 프로토콜에 의존하는 SDLC, 가상 회선, 혹은 HDLC 와 같은 연결계층 및 IP 네트워크, IP 어플리케이션, IPX 네트워크, 그리고 IPX 전송계층 정보를 누적한다.

누적된 데이터는 테이블, 막대 차트, 파이 차트를 이용하여 볼 수 있다.

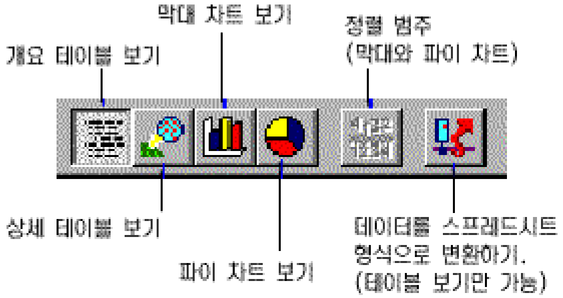
- 테이블은 각 노드에 대한 트래픽 총계를 디스플레이 한다.
  - *Outline table* 은 각 노드에 입출력 된 전체 바이트와 패킷에 대하여 정리한 내용을 제공한다.
  - *Detail table* 은 상위 계층 프로토콜 유형과 각 네트워크 노드에 입출력 되는 트래픽 부하에 대하여 정리한 내용을 제공한다.

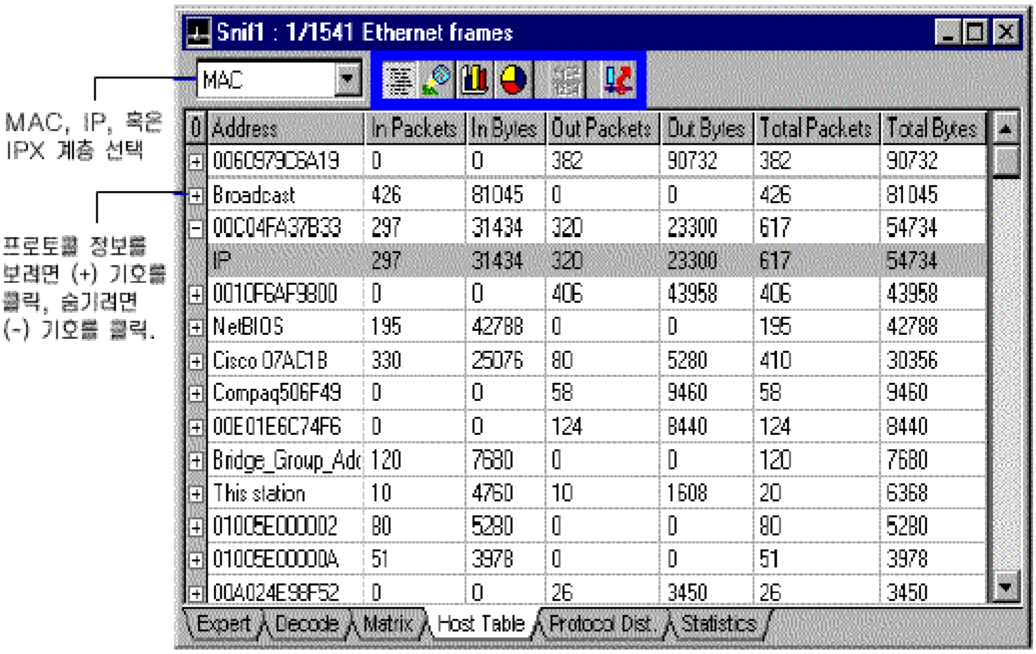
특정 열의 제목을 클릭하여 매트릭스 테이블을 정리할 수 있다. 예를 들어, 통계 자료를 수신 패킷 별로 정렬하려면, In Pkts 열의 제목을 클릭한다. 해당 제목을 두 번 클릭하면 역순으로 정렬된다.

- 막대 차트는 10 개의 가장 분주한 노드들을 실시간으로 디스플레이 한다.
- 파이 차트는 10 개의 가장 분주한 노드들을 전체 트래픽 부하에 대한 비율(%)로서 디스플레이 한다.

모든 관찰 내용에는 연결 계층, MAC 계층에서의 대화 트래픽을 디스플레이 할 수 있으며, 단지 IP 혹은 IPX 하나만을 선택적으로 관찰 할 수도 있다. 테이블 형태의 관찰에서 통계 자료는 일반적인 표 형식이나 차트 형식으로 변환할 수 있다.

그림 4-10 는 호스트 테이블 화면과 해당 툴바를 보여주고 있다.





0	Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
+	0060979C6A19	0	0	382	90732	382	90732
+	Broadcast	426	81045	0	0	426	81045
−	00C04FA37B33	297	31434	320	23300	617	54734
	IP	297	31434	320	23300	617	54734
+	0010F6AF9800	0	0	406	43958	406	43958
+	NetBIOS	195	42788	0	0	195	42788
+	Cisco 07AC1B	330	25076	80	5280	410	30356
+	Compaq506F49	0	0	58	9460	58	9460
+	00E01E6C74F6	0	0	124	8440	124	8440
+	Bridge_Group_Ad	120	7680	0	0	120	7680
+	This station	10	4760	10	1608	20	6368
+	01005E000002	80	5280	0	0	80	5280
+	01005E00000A	51	3978	0	0	51	3978
+	00A024E98F52	0	0	26	3450	26	3450

그림 4-10. 호스트 테이블 화면(상세 테이블)과 툴바

프로토콜 분포 탭(Protocol Distribution Tab)

Protocol Distribution 탭은 네트워크, 전송, 그리고 어플리케이션 계층 프로토콜을 기반으로 네트워크 사용에 대하여 보고한다. 예를 들어, 이 보고자료를 이용하여 IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan, 그리고 다른 많은 프로토콜 들을 모니터 할 수 있다.

프로토콜 분포는 NFS, FTP, Telnet, SMTP, POP2, POP3, HTTP(WWW), Gopher, NNTP, SNMP, X-Windows 등과 같은 대중적인 IP 어플리케이션을 모니터 하며, 또한 NCP, SAP, RIP, NetBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP, 그리고 SPX 와 같은 IPX 전송 계층 프로토콜들을 모니터 한다.

프로토콜 분포는 테이블 혹은 막대나 파이 차트로 볼 수 있다 또한 한 프로토콜에 대한 패킷 혹은 바이트 개수나 비율을 볼 수 있다. Sniffer Pro 는 프로토콜 분포 데이터를 일반적인 테이블이나 차트로 변환할 수 있는 기능을 제공한다. 데이터를 변환하려면, 화면은 테이블 형식이어야 한다.

*그림 4-11*은 프로토콜 분포 화면과 해당 툴바를 보여준다.

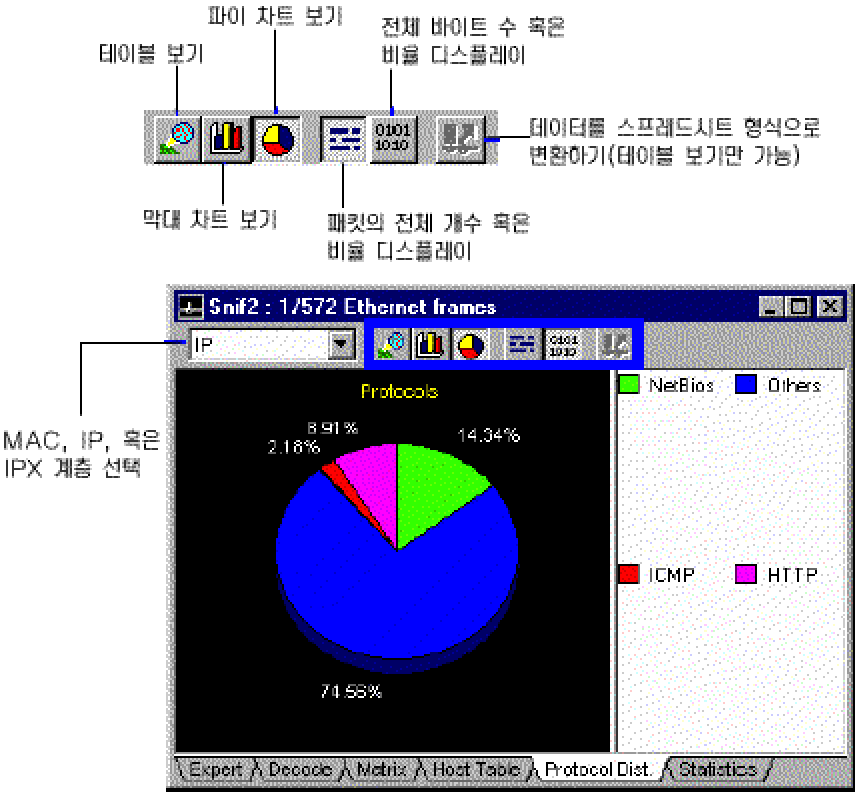

파이 차트 보기
테이블 보기
전체 바이트 수 혹은 비율 디스플레이
데이터를 스프레드시트 형식으로 변환하기(테이블 보기만 가능)
막대 차트 보기
패킷의 전체 개수 혹은 비율 디스플레이
0101 1010
Snif2 : 1/572 Ethernet frames
IP
MAC, IP, 혹은 IPX 계층 선택
Protocols
8.91%
2.18%
14.34%
74.58%
NetBios
Others
ICMP
HTTP
Expert
Decode
Matrix
Host Table
Protocol Dist.
Statistics

그림 4-11. 프로토콜 분포 화면(파이 차트)과 툴바

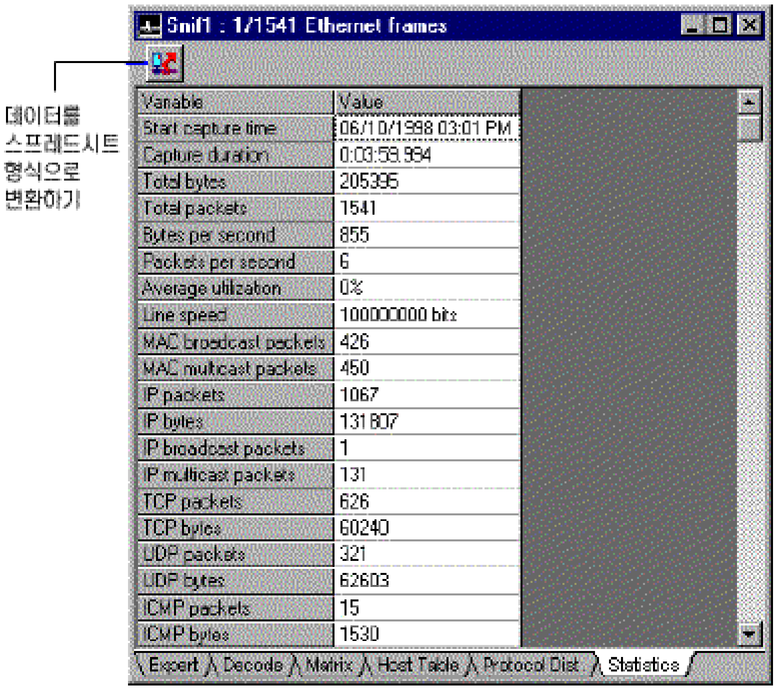
통계 자료 탭(Statistic Tab)

각 캡처 세션에서 Sniffer Pro 는 캡처 주기 동안 네트워크 트래픽을 분석하는데 도와주기 위하여 통계적인 정보를 누적한다. 이러한 정보의 개략적인 내용은 Statistics 탭에 있는 테이블에 디스플레이 된다. 테이블은 아래와 같은 사항들을 디스플레이 한다.

- 캡처 데이터와 시간
- 캡처 동안에 보여지는 트래픽 양
- 활용도 통계 자료

이러한 정보는 Export 버튼을 이용하여 스프레드시트(spreadsheet)용 데이터로 변환할 수 있다.

그림 4-12은 통계 자료(Statistics) 화면을 보여준다.


데이터를 스프레드시트 형식으로 변환하기
Snif1 : 1/1541 Ethernet frames
Expert
Decode
Matrix
Host Table
Protocol Dist.
Statistics

Variable	Value
Start capture time	06/10/1998 03:01 PM
Capture duration	0:03:59.994
Total bytes	205395
Total packets	1541
Bytes per second	855
Packets per second	6
Average utilization	0%
Line speed	100000000 bits
MAC broadcast packets	426
MAC multicast packets	450
IP packets	1067
IP bytes	131807
IP broadcast packets	1
IP multicast packets	131
TCP packets	626
TCP bytes	60240
UDP packets	321
UDP bytes	62603
ICMP packets	15
ICMP bytes	1530

그림 4-12. 통계 자료 화면

Expert 화면

Expert 화면은 Expert 분석 결과를 보여준다. Expert 분석은 캡처하는 동안에 수행될 수 있으며, 그 결과를 실시간으로 보여준다. 또한 캡처 이후에도 디스플레이 기능이 호출되면 발생한다.

Expert 분석하는 동안, Sniffer Pro 는 자신이 관찰한 트래픽으로부터 네트워크 대상들의 데이터베이스를 구성한다. Expert 프로토콜은 네트워크 스테이션, 라우팅 노드, 서브넷, 그리고 캡처 버퍼 내에 있는 프레임과 관련된 연결 등에 대한 모든 학습 내용을 해석한다. 이러한 정보를 이용하여 Sniffer Pro 는 네트워크 상에 존재할 수도 있는 잠재적인 문제들을 지적하고 당신에게 경고한다. 이러한 문제들은 *증상(symptoms)* 혹은 *분석(diagnoses)*으로 분류된다.

- *Symptom* 은 임계 값을 초과하였음을 지적하며, 네트워크 상의 문제점을 지적할 수도 있다.
- *Diagnosis* 는 함께 분석된 몇 가지 증상, 높은 비율의 특정 증상 재발, 혹은 네트워크가 실질적인 문제를 안고 있다고 Expert 가 결론 맺는 특별한 네트워크 이벤트에 대한 단일 인스턴스를 포함할 수 있다. 분석 내용은 즉시 조치되어야 한다.

Expert 분석 결과(증상과 분석)는 Expert 화면 탭과 캡처 과정을 디스플레이 하는 실시간 Expert 창에서 5 가지 작은 창에 보여진다. 5 개의 작은 창은 모든 레벨의 상세한 결과에서 정보를 선택하고 관찰할 수 있도록 제공된다. *그림 4-13* 을 보자.

각각의 작은 창에 대해서 설명하면,

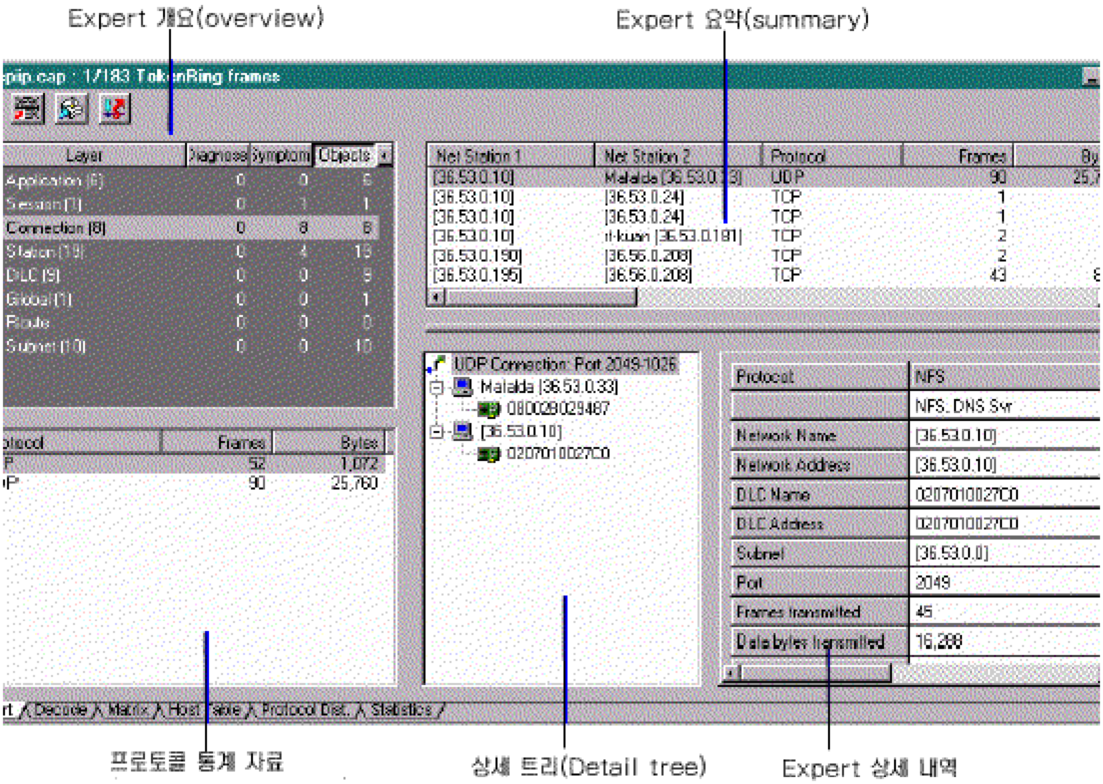
- *Expert 개요(Overview)* 창은 네트워크 분석 계층(ISO 계층과 개념적으로 유사한)과 각 계층에 대한 Expert 개요 통계 자료(대상, 증상, 혹은 분석)를 보여준다. 계층과 통계 유형의 조합을 선택하여, 다른 Expert 창에 보여지는 Expert 분석 데이터를 통제한다.

팁 ---

Expert 개요 창의 우측 상단에 있는 작은 화살표를 클릭하면, Expert 전체 화면을 좁거나 넓게 구성할 수 있다.

- *Expert 요약(Summary)* 창은 Expert 개요 창에서 선택된 계층과 통계에 대하여 키가 되는 요약 정보를 보여준다. 어떤 계층과 통계 유형이 선택되었는가에 따라서 Expert 요약 창에 표시되는 열의 항목은 바뀐다.
- *프로토콜 통계 자료(protocol statistics)* 창은 Expert 개요 창에서 선택된 계층에서 조우한 각 프로토콜에 대한 트래픽 양을 디스플레이 한다. Expert 개용 창이 작을 경우, 이 창은 디스플레이 되지 않는다.

- *상세 트리(detail tree)* 창은 Expert 개요와 요약 창에서 선택된 모든 계층 및 그 하위계층에 대한 구조적인 목록을 보여준다. 윈도우 검색기에서처럼 각 계층은 확장 및 축소가 가능하다. Expert 상세 데이터를 디스플레이 하려면 상세 트리에 있는 항목을 클릭한다.
- *Expert 상세 내역(detail)* 창은 다른 창에서 선택된 데이터에 대한 정보 테이블의 모음이다. 이 창에 표시되는 내용은 다른 창에서 선택된 아이템이 어떤 것인가에 따라서 변할 것이다.



pip.cap : 1/183 TokenRing frames

Layer	Diagnose	Symptom	Objects
Application (6)	0	0	6
Session (1)	0	1	1
Connection (8)	0	8	8
Station (19)	0	4	19
DLC (9)	0	0	9
Global (1)	0	0	1
Route	0	0	0
Subnet (10)	0	0	10

otocol	Frames	Bytes
P	52	1,072
iP	90	25,760

Net Station 1	Net Station 2	Protocol	Frames	By
[36.53.0.10]	Malalda [36.53.0.33]	UDP	90	25,7
[36.53.0.10]	[36.53.0.24]	TCP	1	
[36.53.0.10]	[36.53.0.24]	TCP	1	
[36.53.0.10]	rl-kuan [36.53.0.181]	TCP	2	
[36.53.0.190]	[36.56.0.208]	TCP	2	
[36.53.0.195]	[36.56.0.208]	TCP	43	8

```
UDP Connection: Port 2049-1026
⊟ Malalda [36.53.0.33]
    080029029487
⊟ [36.53.0.10]
    0207010027C0
```

Protocol	NFS
	NFS, DNS Svr
Network Name	[36.53.0.10]
Network Address	[36.53.0.10]
DLC Name	0207010027C0
DLC Address	0207010027C0
Subnet	[36.53.0.0]
Port	2049
Frames transmitted	45
Data bytes transmitted	16,288

그림 4-13. Expert 윈도우 영역

자동 Expert 디스플레이 필터 설정

다음 항목과 관련되어 캡처 버퍼 내의 모든 트래픽을 자동적으로 화면에 출력하는 Expert 디스플레이 필터를 사용할 수 있다:

- Network object
- Symptom 또는 diagnosis

Expert 윈도우의 Summary 영역에서 네트워크 object, symptom 또는 diagnosis 를 선택하고 Expert 윈도우의 좌측 상단에 있는 Define Filter 버튼을 클릭하여 Expert 디스플레

이 필터를 적용한다. 필터 적용 결과로 Expert 는 디스플레이 윈도우 하단에 새로운 탭을 추가한다. 이 탭은 Filtered xx 라고 이름이 붙여지며, xx 는 필터를 적용한 순서대로 붙여지는 번호이다. 이 탭에는 선택한 네트워크 object, symptom 또는 diagnosis 와 관련된 프레임들만 포함하고 있다.

네트워크 object 필터는 각 프레임에 할당된 프레임 번호를 바꾸지 않기 때문에 Filtered 탭에 있는 프레임들은 해당 번호가 바뀌지 않은 채로 (즉, 일정한 간격이 아닌 필터링된 후에도 원래의 프레임 번호로) 표시된다. 따라서 프레임 31- 34 번이 필터에서 제외되면, 프레임 30 번 이후에 바로 프레임 35 번이 나타나게 된다. 만약 필터링된 프레임들을 Save As 명령으로 새 파일에 저장하면, Sniffer Pro 는 모든 프레임들의 번호를 순서대로 재 할당한다.

Expert Filter 의 한계

Expert 필터에는 두 가지 한계점이 있다.

- Broadcast storm 과 같은 몇 개의 symptoms 와 diagnosis 들은 분석기가 필터를 적용할 수 있는 네트워크 object 와 관련이 없다. 이러한 경우에, Define Filter 버튼이 화면의 좌측 상단에 나타나지 않을 수도 있으며, 이것은 Expert 필터를 설정할 수 없다는 것이다.
- 종종 다음 메시지가 나타날 것이다.

  No frames are eligible for display

  이 메시지는 아래와 같은 상황에서 나타난다.

  - 송 수신된 프레임이 없는 object 를 선택했을 경우.
  - 표준 디스플레이 필터를 사용하여 이미 필터링된 object 를 선택했을 경우.

Expert Filter 에 대한 주의 사항

Expert 분석기는 어떤 프레임들이 특정 네트워크 object 와 관련되어 있는지를 결정하기 위해서 몇 가지 알고리즘을 사용한다. 때로는 이 알고리즘들이 참고할 필요가 있는 프레임들을 제거할 수도 있다.

- 몇 가지 접속 유지용 프레임들은 보이지 않을 수도 있다. 예를 들어, 만약 사용자가 Novell Netware 연결 계층에 대해서 Expert 필터를 설정했다면, Expert 분석기는 NCP 계층들과 관련된 모든 프레임들을 보여줄 것이다. 그렇지만, 관련이 없는 몇 가지 접속 유지용(connection maintenance) 프레임들은 보이지 않을 것이다.
- Connection 계층의 object 에 대해서 필터를 설정했을 때, 해당 접속을 초기화하는 프레임들은 보이지 않는다. 이것은 Expert 가 해당 접속이 완료될 때까지 connection object 를 생성하지 않기 때문이다.
- 어플리케이션 계층의 object 에 대해서 필터를 사용하는 경우, TCP 연속 프레임(continuation frame)들은 보이지 않는다.

상황에 따른 설명 메시지 디스플레이 하기 (Displaying Context-Sensitive Explain Message)

Expert 는 Expert 윈도우의 각 작은 영역에 대하여 설명하는 정보를 제공한다. 정보가 필요한 영역의 내부를 클릭하고 F1 키를 누른다.

또한 Expert 는 생성된 각 증상과 분석에 대한 간략한 설명을 제공한다. 증상과 분석에 대한 상세한 설명을 보려 한다면, Expert 상세 내역 창에 나타난 증상/분석의 우측에서 물음표(?)를 클릭한다.

Expert 화면 재정렬하기 (Rearranging Expert Display)

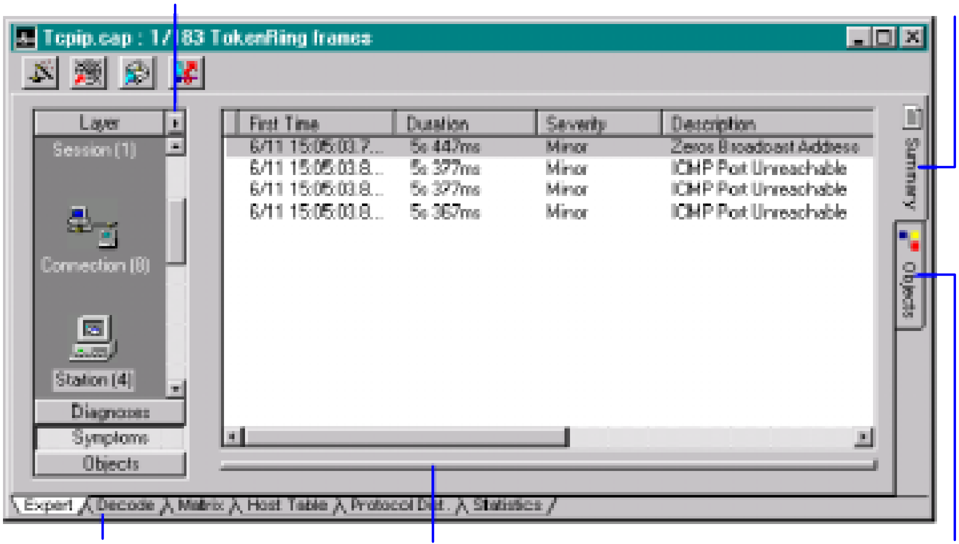
Expert 화면은 당신이 보기에 편리한데로 다음 3 가지 형식으로 바꿀 수 있다.

- 5 개의 작은 창들을 동시에 보기(*그림 4-13*)
- Expert 개요와 요약 창 보기. 이것이 기본 설정이다.
- 상세 트리와 Expert 상세 내역 창 보기.

*그림 4-14*는 기본적인 Expert 화면과 다른 창들을 재배열하는 방법을 보여주고 있다.

Expert 개요 창을 확대하고, 프로토콜 통계 창을 하단에 나오게 하는 버튼

현재 보이는 것처럼 Expert 개요 와 요약 창을 구성하려면 이 탭을 크릭



First Time	Duration	Severity	Description
6/11 15:05:03.7...	5s 447ms	Minor	Zeros Broadcast Address
6/11 15:05:03.8...	5s 377ms	Minor	ICMP Port Unreachable
6/11 15:05:03.8...	5s 377ms	Minor	ICMP Port Unreachable
6/11 15:05:03.8...	5s 367ms	Minor	ICMP Port Unreachable

패킷 디스플레이 탭. 디코드된 패킷을 보기 위한 탭. (캡처가 중지 되었을 경우에만 가능)

동시에 5개의 모든 창을 화면에 보이게 구성하려면 이 막대를 화면의 주간으로 드래그하여 하단의 창을 확대 (그림 4-23)

상세 트리와 Expert 상세 정보 창을 화면에 보이게 하려면 이 Objects 탭을 클릭

그림 4-14. Expert 윈도우 창의 재배열

캡처 파일과 함께 Expert Objects 저장하기

패킷을 캡처하는 동안, Expert 는 프레임 기반으로 Expert object 들을 생성한다. 장시간 캡처하는 동안에 Expert 가 이러한 object 를 생성하기 위해 사용하는 몇몇 프레임들은 새로운 프레임들을 위한 공간을 확보하기 위해서 캡처 버퍼에서 제외되는 경우가 있다. 그렇지만, Expert object 들 자체는 데이터베이스 내에 남아있게 된다.

Save As 대화 상자 내에 있는 **Save Expert Objects** 박스를 선택함으로써 캡처하는 동안에 생성되는 모든 Expert object 들을 캡처 파일과 더불어 저장할 수 있다. 이 옵션이 선택되면, 데이터베이스 내에 있는 모든 Expert object 들은 저장된 캡처 파일 끝부분에 저장된다. 이후에는 Expert objects 가 저장된 캡처 파일을 열 때, **Open** 대화 상자에서 **Load Expert Objects** 상자를 선택한다. 이러한 방법을 이용하면, 캡처된 파일을 다시 열 때, 파일 내부에 포함되어 있는 프레임들과 연관된 Expert object 대신에 캡처하는 동안에 생성되었던 모든 Expert object 를 볼 수 있다.

Save/Load Expert Objects 기능의 주의 사항

- Expert object 들은 오직 .CAP 형식으로 저장된 캡처 파일에만 저장할 수 있다.
- Expert object 들이 저장되지 않은 캡처 파일을 열 때, **Load Expert Objects** 옵션을 선택하면, 에러는 없을 것이다. 해당 파일은 일반적인 상태로 읽혀질 것이다.

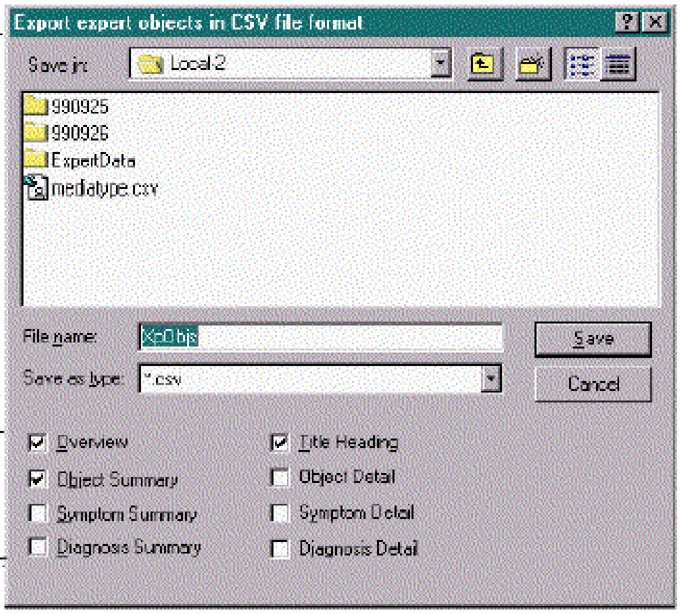
Expert 데이터베이스의 내용 변환하기 (Exporting the Contents of the Expert Database)

네트워크 대상, 증상 그리고 분석과 같은 Expert 분석기의 데이터베이스에 있는 내용은 확장자가 .CSV(comma-separated values)인 파일로 변환할 수 있다. CSV 파일 형식은 대부분의 스프레드시트 프로그램에서 쉽게 사용할 수 있다.

Expert 분석기의 데이터베이스 내용은 두 가지 방법으로 변화할 수 있다.

- **수동**: Expert 윈도우에 있는 Export 버튼을 클릭한 후, 변환하기 원하는 데이터베이스의 위치를 지정하기 위하여 *그림 4-15*에 보인 대화 상자를 사용한다.
- **자동**: 데이터베이스 옵션 대화 상자의 Expert Data 탭에 있는 옵션을 사용한다. 보다 자세한 내용은 다음에 나오는 *Expert 분석기 데이터 자동 변환*을 보아라.

변환된 데이터의 형식은 *Expert 분석기 출력 파일 형식(Expert Analyzer Output File Format)* 매뉴얼에 자세하게 설명되었다.



Expert 데이터베이스의 변환된 내용들을 위한 경로와 파일 이름을 지정

CSV 파일로 변환 하고자 하는 Expert 데이터베이스의 부분을 선택.
각각의 체크 상자는 Expert 윈도우에 있는 작은 창에 대응.

Export expert objects in CSV file format

Save in: Local 2

990925
990926
ExpertData
mediatype.csv

File name: XpObjs

Save as type: *.csv

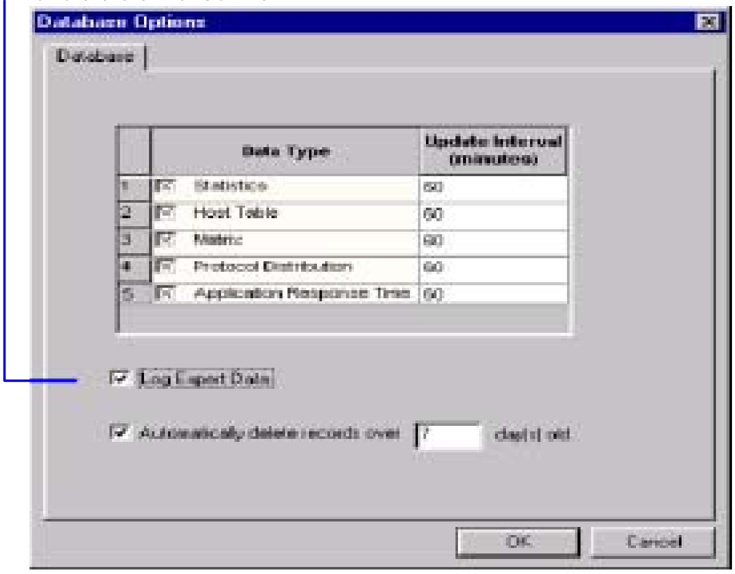
☑ Overview
☑ Object Summary
☐ Symptom Summary
☐ Diagnosis Summary
☑ Title Heading
☐ Object Detail
☐ Symptom Detail
☐ Diagnosis Detail

그림 4-15. Expert 데이터베이스의 내용 변환하기

Expert 분석기 데이터 자동

Sniffer Pro 가 캡처가 끝날 때마다 Expert 데이터베이스의 내용을 자동으로 변환하도록 설정할 수 있다. 그러기 위해서는 데이터베이스 옵션 대화 상자의 **Expert Data** 탭에 있는 **Log Expert Data** 옵션을 선택해야 한다(*그림 4-16*). 이 대화 상자는 Sniffer Pro 의 **Database** 메뉴에서 **Options** 명령을 선택하여 화면에 표시한다.

이 옵션이 선택되면, 매번 캡처가 끝날 때마다 자동적으로 Expert data가 데이터베이스에 저장된다.



Database Options

Database

	Data Type	Update Interval (minutes)
1	☑ Statistics	60
2	☑ Host Table	60
3	☑ Matrix	60
4	☑ Protocol Distribution	60
5	☑ Application Response Time	60

☑ Log Expert Data

☑ Automatically delete records over 7 day(s) old

그림 4-16. Expert Data 의 자동 파일 저장 설정하기

Log Expert Data 옵션이 선택되면, Sniffer Pro 는 캡처가 중지될 때 마다 Expert 분석기의 데이터베이스를 CSV 파일로 변환한다.

자동으로 변환된 파일들은 Sniffer Pro 가 설치된 디렉터리 내에 있는 현재 어댑터에 대한 서브 디렉터리 내에 **ExpertData** 라고 하는 서브 디렉터리에 저장된다. (Select Settings 대화 상자에 정의된 각 어댑터는 이 디렉터리에 자신만의 서브 디렉터리를 갖는다.) 예를 들어, 현재 선택된 어댑터 이름이 Local-2 라고 하면, 자동으로 변환된 파일들은 다음 디렉터리에 저장된다.

\Program Files\NAI\SnifferNT\Program\Local-2\ExpertData\yymmddhhmmexpert.csv

주 --
Sniffer Pro 가 Windows NT 와 Windows 2000 에 설치된 경우에 위 경로가 맞으며, Windows 95/98 시스템에서는 **\Program Fiels\NAI\Sniffer\Program\...**에서 찾는다.

위에서 언급했듯이 저장된 파일들은 *yymmddhhmm*expert.csv 형식으로 이름이 부여된다. 여기에서 *yy*=연도, *mm*=월, *dd*=날짜, *hh*=시간, *mm*=분을 나타낸다.

5. 필터와 트리거 정의하기

당신의 네트워크 분석에 필요한 특정 트래픽만을 골라내기 위하여 *필터(filter)*를 사용하며, 이러한 필터를 이용하여 네트워크 장애 분석에 필요한 데이터에만 정밀하게 초점을 맞출 수 있으며, 수집하는 파일의 크기를 최소화할 수 있다.

*트리거(trigger)*를 사용하여 업무이외의 시간이나 주말과 같이 Sniffer Pro 를 지켜볼 수 없는 상황에서도 데이터를 캡처 할 수 있으며, 알람에 설정된 특정 이벤트가 발생하였을 경우에 캡처를 시작할 수도 있다.

필터 정의하기 (Defining Filters)

Sniffer Pro 에서 사용되는 모든 필터들은 동일한 과정을 걸쳐서 정의된다. 필터의 유형은 사용하는 방법에 따라서 결정된다.

- 어떠한 트래픽을 선택하는가에 대하여 모니터링할 때, 그 필터는 *모니터 필터(monitor filter)*가 된다.
- 어떠한 트래픽을 선택하여 캡처 버퍼에 저장하는가에 대해 확인할 때, 그 필터는 *캡처 필터(capture filter)*가 된다.
- 캡처 버퍼 내에서 특정 데이터를 선택하여 화면에 표시할 때, 그 필터는 *디스플레이 필터 (display filter)*가 된다.

팁 ---

필터를 정의할 때, 이름(**Profile**)을 입력한다. 그 후 이름이 붙여진 필터를 모니터, 캡처, 또는 디스플레이 필터가 되도록 결정(**Monitor**, **Capture** 또는 **Display** 가운데 어떤 메뉴에서 Select Filter 선택하느냐에 따라)한다. 여러 종류의 필터를 쉽게 구별하려면, 확실히 알 수 있는 이름을 사용한다. *Filter Profile 사용하기*를 참고한다.

필터를 정의하려면, **Monitor**, **Capture** 혹은 **Display** 메뉴에서 **Define Filter** 를 선택한다. 또는 많은 Sniffer Pro 윈도우에 있는 버튼을 사용할 수 있다. Filter Settings 대화 박스를 열면, 현재 사용하고 있는 네트워크 어댑터에 따라서 아래의 탭들 가운데 일부 또는 전부가 화면에 보여질 것이다.

- **Summary** 탭은 현재 선택된 필터에 대한 설정 내용을 보여주며, 또한 버퍼 크기와 캡처 중지 혹은 버퍼가 가득 찼을 경우 기존 데이터에 겹쳐서 저장하는 등의 캡처 동작을 표시한다.

- **Address** 탭은 네트워크 노드 주소를 기반으로 필터를 설정할 수 있도록 한다.
- **Data Pattern** 탭은 데이터 패턴을 기반으로 필터를 설정할 수 있도록 한다.
- **Advanced** 탭은 패킷 크기, 프로토콜, 그리고 에러 유형을 기반으로 필터를 설정할 수 있도록 한다.
- **Buffer** 탭은 캡처 버퍼 옵션을 설정할 수 있도록 한다.
- WANBook 을 포함하여 WAN 어댑터에서는 **SDLC, X.25, Frame Relay,** 그리고 **HDLC** 탭이 필터 상에 다양한 WAN 패킷 유형을 설정할 수 있다. 사용할 수 있는 실질적인 탭은 **Options** 대화 박스에 있는 Encapsulation(캡슐화) 옵션의 설정 여부에 따라 다르다.
- ATM 어댑터에서는 **ATM VPI.VCI** 탭이 VPI.VCI 들을 사용하는 네트워크 상에서 특정 VCC 에 필터를 설정할 수 있도록 제공된다. 이러한 필터들은 PVC 상에서 필터들을 설정할 때 유용하다.
- ATM 어댑터에서는 **ATM Station Address** 탭이 특정 ATM 종단 스테이션 주소에 대한 필터를 설정할 수 있도록 제공된다. 이러한 필터는 모든 SVC 상에서 필터를 설정할 때 유용하다.
- Gigabit Ethernet 어댑터에서는 어댑터 카드 상에 있는 각 채널에 대해 필터를 정의하고, auto-negotiation filter 나 다른 옵션들을 설정할 수 있도록 **GB Ethernet** 탭이 있다.
- Full Duplex Ethernet 어댑터에서는 어댑터의 보드 상에 있는 버퍼가 모두 채워졌을 때 실행할 동작을 설정하고, VLAN Protocol Forcing 옵션을 설정할 수 있도록 **Full Duplex Ethernet** 탭이 있다.

Filter Profile 사용하기

정확한 필터를 정의한다는 것은 많은 시간이 필요한 작업이 될 수도 있다. Sniffer Pro 의 필터 프로파일 기능은 필터를 정의하고 나중에 다시 사용할 수 있도록 저장하는 방법을 제공한다. *필터 프로파일(filter profile)*은 Define Filter 대화 상자에 있는 다양한 탭(**Address, Data Pattern, Advanced, Buffer**)에서 정의한 하나 또는 그 이상의 필터 집합체이다.

예를 들어, 오직 특정 라우터로 입출력되는 IP 트래픽에만 관심이 있는 환경에서 Sniffer Pro 를 자주 사용한다고 하자. 이런 경우에 사용자는 해당 라우터의 IP 주소를 입력한 **Address** 필터와 더불어 IP 프로토콜 트래픽만 선택된 **Advanced** 필터가 조합된 필더 프로파일을 생성할 수 있을 것이다. 이처럼 구성한 필터의 조합은 Select Filter 대화 상자에서 저장한 필터 프로파일을 선택함으로써 필요한 경우 언제나 사용할 수 있다.

팁 ---

특정 필터 프로파일에 포함되어 있는 개별적인 필터들의 정보를 보고 싶다면, Define

Filter 를 선택하고 Define Filter 대화 상자의 우측에 있는 Settings For 창에서 해당 필터 프로파일을 선택한다. Define Filter 대화 상자의 Summary 탭에 개별 필터들의 간단한 정보가 표시된다.

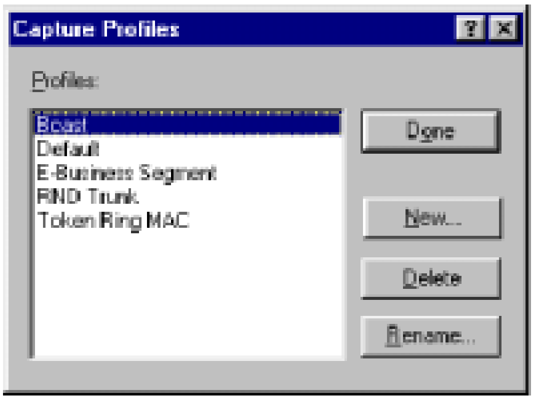
Filter Profile 생성

새로운 필터를 구성할 때마다 Define Filter 대화 상자에 있는 **Profiles** 를 클릭하여 시작했는지 확인할 필요가 있다. 그 다음에 **New** 버튼을 클릭하여 대화 상자를 열면 새로운 이름으로 필터 프로파일을 생성할 수 있다.

필터 프로파일에 이름을 할당했으면, Define Filter 대화 상자의 **Settings For** 창에 그 이름이 추가되고 해당 필터에 대한 설정 내용을 찾을 수 있다. 더불어서, 추가된 필터는 Select Filter 대화 상자에 보이게 되고, 모니터링, 캡처 및 디코드 영역 어디에서든 적용이 가능하게 될 것이다.

필터 프로파일 생성하기

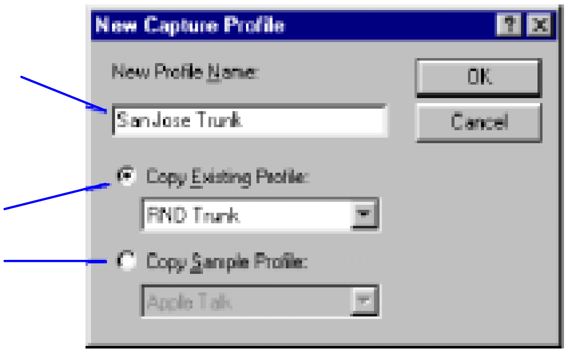
1. Monitor, Capture 또는 Display 메뉴 (구성하려고 하는 필터의 적용 대상에 따라서) 어디에서든 **Define Filter** 명령을 선택한다.
2. Profiles 버튼을 클릭한다.
   Capture Profiles 대화 상자(*그림 5-1*)가 나타나고, 이전에 정의된 필터 프로파일들이 목록에 있다.



Bcast
Default
E-Business Segment
RND Trunk
Token Ring MAC

그림 5-1. Capture profiles 대화 상자

3. 새 필터 프로파일을 만들기 위해 New 버튼을 클릭한다.
   New Capture Profile 대화 상자가 나타난다. (*그림 5-2*)



New Profile Name: San Jose Trunk

● Copy Existing Profile: RND Trunk

○ Copy Sample Profile: Apple Talk

이곳에 필터 프로파일
의 이름을 입력.

기존에 있던 프로파일
이나 Sniffer Pro와 함
께 제공되는 샘플 프로
파일들의 설정 내용을
복사하여 사용 가능.

그림 5-2. New Capture Profile 대화 상자

4. New Capture Profile 대화 상자에서 필터 프로파일을 위한 이름을 입력한다. 더불어서, 이전에 정의했던 프로파일 (**Copy Existing Profile** 옵션) 또는 Sniffer Pro 와 함께 제공되는 많은 샘플들 (**Copy Sample Profile** 옵션) 가운데 하나의 설정 내용을 복사하여 사용할 수 있다.
5. **OK** 를 클릭한다.
6. Capture Profiles 대화상자에서 **Done** 을 클릭한다.

Define Filter 대화 상자의 Settings For 창 내부에 설정한 필터가 보일 것이다. 이제 새로운 필터 프로파일에 대한 필터들을 서정하기 위해 Define Filter 대화 상자의 다른 탭 (**Address, Data Pattern, Advanced** 등등) 들의 내용을 구성할 수 있다.

샘플 프로파일 사용하기

Sniffer Pro 는 다양한 네트워크 트러블슈팅 환경에서 사용할 수 있는 많은 샘플 필터를 제공하고 있다. 사용 가능한 샘플 프로파일들은 New Capture Profile 대화 상자 (*그림 5-2*) 내에 있는 **Copy Sample Profile** 드롭 다운 목록에서 찾을 수 있다. 샘플 필터 프로파일들은 IP 및 IPX 뿐만 아니라, 보다 하위 계층의 프로토콜인 FDDI LLC, Token Ring MAC, Token Ring LLC 등등 다양한 많은 프로토콜들에 대한 필터를 제공한다.

샘플 프로파일에 구성된 개별적인 필터들을 보고자 한다면, 샘플 프로파일을 기반으로 하는 새로운 필터 프로파일을 만들어서 Define Filter 대화 상자의 **Settings For** 탭에 있는 내용을 선택한 후, **Summary** 탭을 클릭하면 볼 수 있다. Summary 탭에서는 선택된 필터 프로파일에 구성된 개별적인 필터들의 목록을 보여줄 것이다.

주소에 의한 필터링 (Filtering by Address)

10 쌍 정도의 네트워크 노드의 주소를 이용하여 캡처 필터나 디스플레이 필터를 구성하려면, Filter Settings 대화 상자의 **Address** 탭에 있는 옵션을 사용한다.

중요 정보--

새로운 필터를 정의하려면, 먼저 **Profiles** 버튼을 클릭하고 새로운 이름을 부여한다. 그 다음 설정 내용을 입력한다.

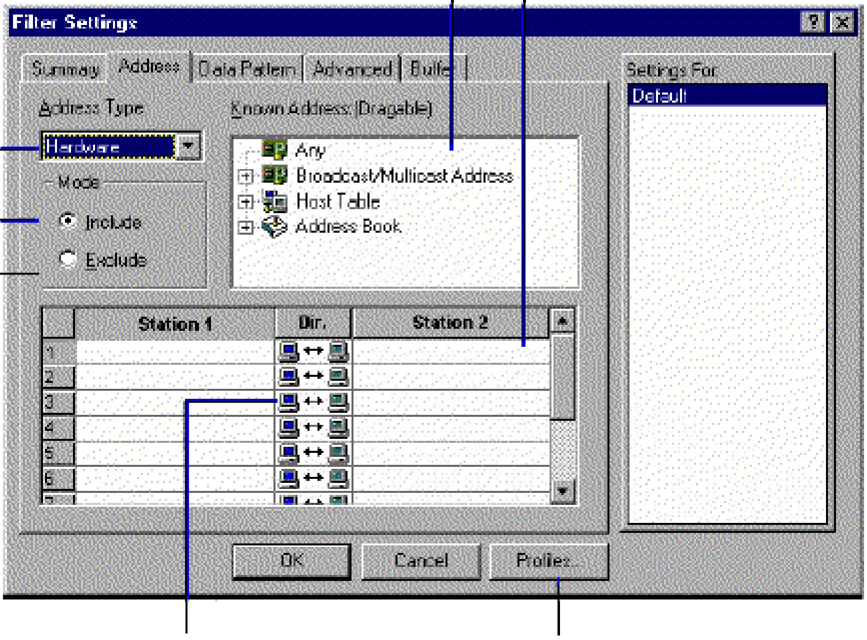
----

*그림 5-3*은 Filter Settings 대화 상자의 **Address** 탭을 보여주고 있다.

Known Address에서 문자로 표시된 주소를 스테이션 1이나 스테이션 2 내부로 드래그 앤 드롭
Known Address는 Broadcast Address, Host Table, 혹은 Address Book에서 가져옴

수동으로 주소를 바로 입력할 수 있음.

주소를 하드웨어 주소(6바이트의 16진수 값) 또는 네트워크 IP, IPX(4 옥텟) 주소로 정의.



지정된 주소에 대한 패킷들을 포함시킬 것인지, 제외시킬 것인지 선택.

Dir 옵션을 설정하여 트래픽의 흐름 방향을 선택

먼저, 새로운 필터에 네임을 부여하기 위해 클릭

그림 5-3. 주소 필터 설정하기

데이터 패턴에 의한 필터링 (Filtering by Data Pattern)

지정한 데이터 패턴에 맞는 패킷만을 캡처 하거나 디스플레이 하는 필터를 정의하려는 경우, Data Pattern 탭을 사용한다. 데이터 패턴 필터는 단일 데이터 패턴만으로 구성하여 단순하게 설정하거나, 부울 함수인 AND, OP, NOT 을 이용하여 연결되는 다중 데이터 패턴을 포함하여 매우 복잡하게 설정할 수 있다.

주---

복잡한 필터는 20 개 이하의 부울 함수와 데이터 패턴으로 제한된다.

보다 상세한 필터 구성 방법은 부록 2 를 참조하자.

데이터 패턴

- 비트 단위의 입부 시퀀스
- 시퀀스의 길이
- 패킷 내에서 그 시퀀스의 옵셋 위치

최대 데이터 패턴의 길이는 32 옥텟(Octets)이다. 옵셋을 패킷의 시작 부분이나 프로토콜 경계 부분에 지정할 수 있다.

디스플레이 디코드 화면에서 필터를 위한 데이터 패턴을 복사할 수 있다. 이러한 작업을 수행하려면, 필터 정의 기능을 호출하기 전에 패킷을 선택한다. Data Pattern 탭에서 Add Pattern 을 선택한 다음 Set Data. 이러한 과정은 선택된 패킷으로부터 데이터 필드를 데이터 패턴 필드에 복사하고, 옵셋과 길이를 계산한다.

복잡한 데이터 패턴 필드를 구성하려면, 부울 연산자를 이용하여 데이터 패턴들을 링크한다. 그 결과는 Data Pattern 탭에 있는 트리와 유사한 다이어그램에 디스플레이 된다.

Data Pattern 탭은 필터 생성을 위한 작업 공간을 디스플레이하며, 현재 데이터 패턴 식을 디스플레이 한다. 화면 아래에 있는 버튼들은 부울 함수 표현과 데이터 패턴을 정의하는 과정을 제어한다.

*그림 5-4*는 Filter Settings 대화 상자의 Data Pattern 탭을 보여주고 있다.

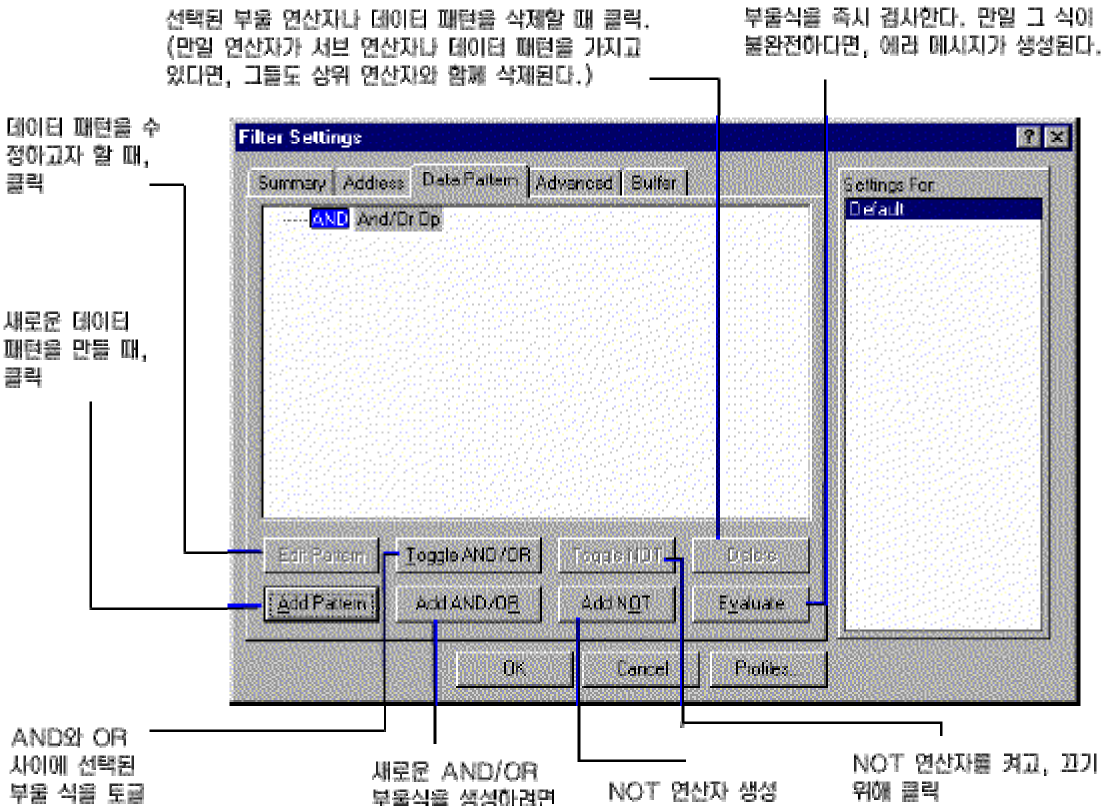

선택된 부울 연산자나 데이터 패턴을 삭제할 때 클릭. (만일 연산자가 서브 연산자나 데이터 패턴을 가지고 있다면, 그들도 상위 연산자와 함께 삭제된다.)
부울식을 즉시 검사한다. 만일 그 식이 불완전하다면, 에러 메시지가 생성된다.
데이터 패턴을 수정하고자 할 때, 클릭
새로운 데이터 패턴을 만들 때, 클릭
Filter Settings
Summary
Address
Data Pattern
Advanced
Buffer
AND And/Or Op
Settings For
Default
Edit Pattern
Toggle AND/OR
Toggle NOT
Delete
Add Pattern
Add AND/OR
Add NOT
Evaluate
OK
Cancel
Profiles...
AND와 OR 사이에 선택된 부울 식을 토글
새로운 AND/OR 부울식을 생성하려면
NOT 연산자 생성
NOT 연산자를 켜고, 끄기 위해 클릭

그림 5-4. 데이터 패턴 필터 설정하기

패킷 크기, 프로토콜, 그리고 에러 유형에 의한 필터링

패킷 크기, 프로토콜 유형이나 에러 유형을 기반으로 하는 필터를 정의하려면 **Advanced** 탭의 옵션들을 사용한다. 패킷들을 특정 패킷 크기와 동일하게, 보다 크게, 혹은 보다 작게 명시하거나 특정 패킷 크기 영역 내에 혹은 해당 영역 이외의 패킷으로 지정할 수 있다.

하나 혹은 그 이상의 프로토콜이나 서브 프로토콜을 필터처럼 동작하게 선택할 수 있다. 만일 어떤 패킷이 선택된 프로토콜 유형 가운데 한가지에 대응된다면, 그 패킷은 필터를 통과하여 지나갈 것이다. 만일 선택된 프로토콜이 없으면, Sniffer Pro 는 모든 프로토콜 유형들을 캡처 한다.

주 ---

만일 당신이 필요한 프로토콜이 프로토콜 목록에 정의되어 있지 않다면, 데이터 패턴 필터 관리 내용을 이용하여 당신 자신의 프로토콜 필터를 정의할 수 있다.

주 ---

목록 내에 있는 모든 프로토콜들이 Expert 에 의해 제공되는 것은 아니다. Expert 를 위하

여 현재 제공되는 프로토콜의 목록은 온라인 도움말을 보아라.

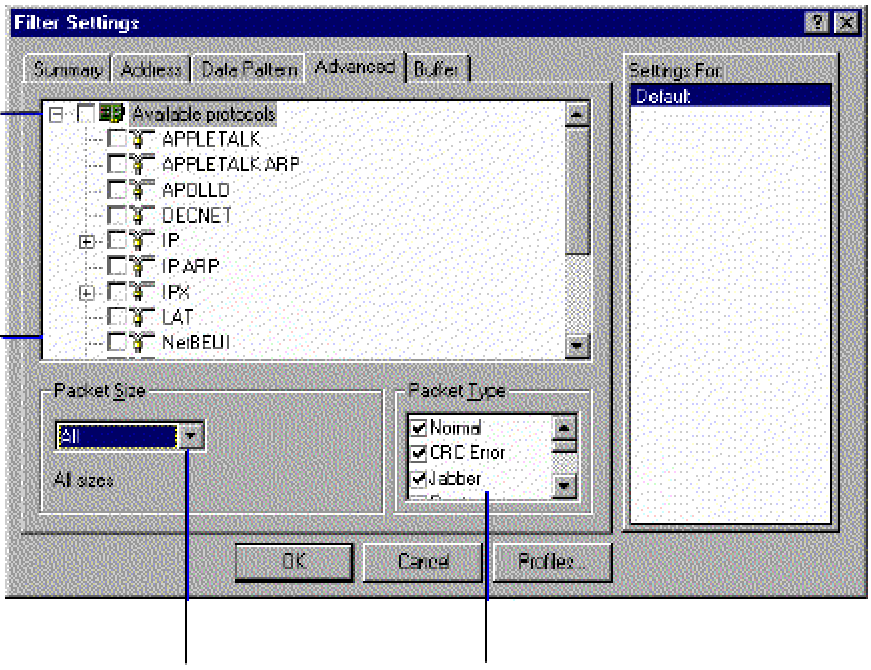
Sniffer Pro 는 CRC 에러, 조각 등을 포함하는 모든 영역의 에러 패킷들을 캡처하고 디스플레이 한다. 에러 유형 필터를 생성하기 위하여 하나 혹은 그 이상의 **Packet Types** 를 선택할 수 있다.

중요 정보 ---

에러 패킷 정보를 수집하기 위해서는 Sniffer Pro 와 함께 제공되는 NAI 확장 네트워크 드라이버 가운데 하나를 설치해야 한다.

----

*그림 5-5*는 Filter Settings 대화 상자의 **Advanced** 탭을 보여주고 있다.



Packet Size: All
All sizes

Packet Type:
☑ Normal
☑ CRC Error
☑ Jabber

필터링하려는 네트워크 프로토콜들을 지정. 표시되는 모든 프로토콜들은 캡처나 모니터 데이터에 포함됨.

필터링하려는 패킷의 크기를 지정.

필터링하려는 에러의 유형들을 지정. 체크되는 모든 에러들은 데이터에 포함됨.

그림 5-5. 상위(advanced) 필터 설정하기

캡처 버퍼 옵션 설정하기

캡처 버퍼를 위한 옵션은 **Buffer** 탭에서 설정한다. 이 설정 내용들은 필터가 단지 캡처 필터로 사용되는 경우에만 사용한다. 캡처 버퍼 설정에 관한 내용은 *캡처 버퍼(Capture Buffer)*에서 설명한다.

ATM VPI.VCI 상에서 필터링 하기

지정된 PVCs(Permanent Virtual Connections)에서 데이터를 캡처기 위한 필터들을 정의할 경우, ATM VPI.VCI 탭을 사용한다. *그림 5-6*는 ATM.VPI.VCI 탭을 보여주고 있다.

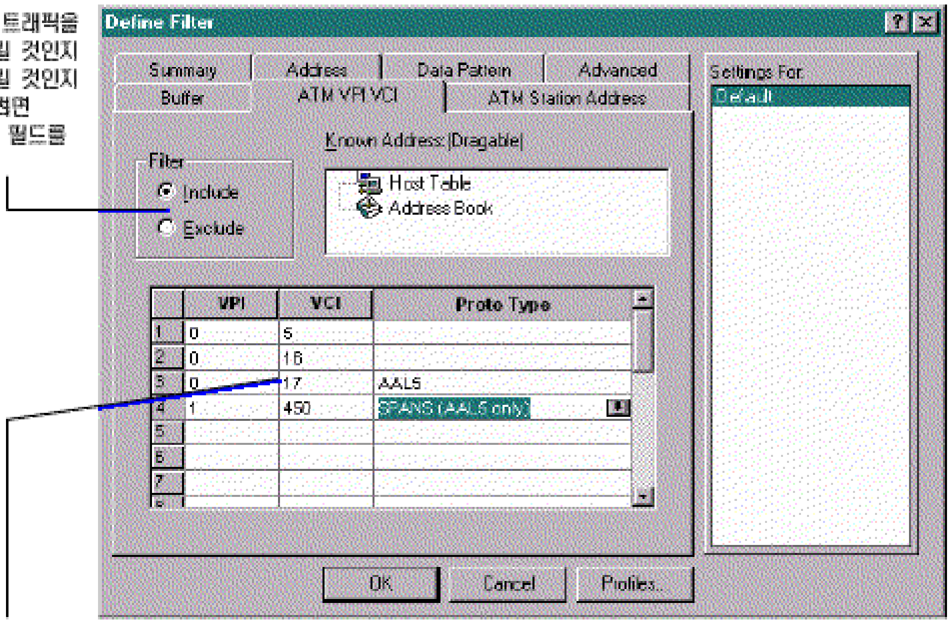
또한 이 탭에서는 지정된 PVC 들에 어떤 유형의 트래픽이 실시간으로 해석되는지 설정할 수 있다. 해당 필드에 VPI.VCI 를 입력하고 프로토콜을 지정하기 위해 Proto Type 필드에 있는 드롭다운 목록을 사용한다. 이 방법은 분석기가 signaling 정보를 알 수 없어서 프로토콜 종류를 추정할 수 없을 때 손쉽게 사용할 수 있다.

주 --

Include, Exclude 설정은 ATM Book 을 위하여 사용할 수 없다. ATM Book 을 위한 PVC 필터들은 기본적으로 Include 필터들이다.

그림 5-6 에서 PVC 필터들은 VPI.VCI 0.5(표준 신호 채널)와 VPI.VCI 0.16(표준 ILMI 채널)에서 트래픽을 캡처 하도록 설정되었다. 또한 Proto Type 필터들은 SPANS, VPI.VCI 1.450 PVC 에서의 모든 트래픽 및 AAL5, 0.17 상에서의 모든 트래픽을 해석할 수 있다.

지정된 트래픽을 포함시킬 것인지 제외시킬 것인지 결정하려면 Filter 필드를 사용



Filter
● Include
○ Exclude

	VPI	VCI	Proto Type
1	0	5	
2	0	16	
3	0	17	AAL5
4	1	450	SPANS (AAL5 only)
5			
6			
7			

캡처에 포함시키거나 제외시키고자 하는 PVC의 VPI.VCIsVPI.VCI를 추가하려면, VPI와 VCI 필드를 사용.
선택된 PVC에 프로토콜 필터를 적용하려면, Proto Type 필드를 사용.

그림 5-6. ATM VPI.VCI 필터 설정하기

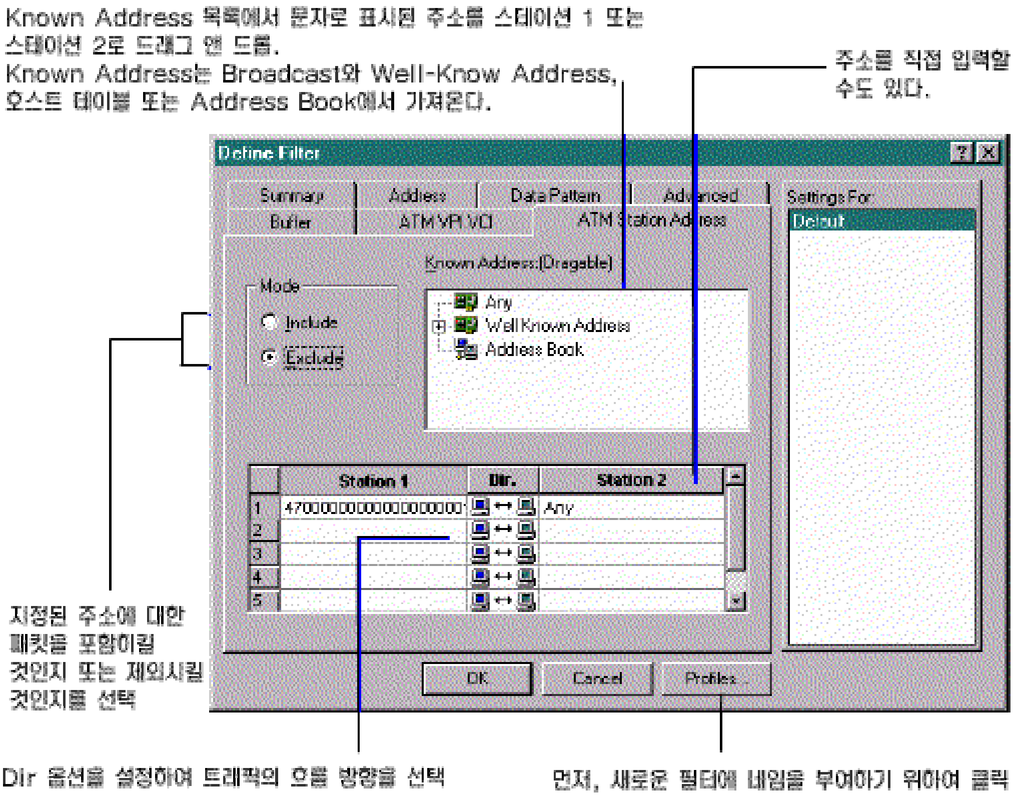
ATM 스테이션 주소 상에서 필터링 하기

SVC(Switched Virtual Connections)들은 서로 다른 PVC 상에서 동적으로 설정되기 때문에, 데이터가 보내어지는 VPI.VCI 와 관계없이 ATM 네트워크 상에서 다른 스테이션 사이에 전송되는 데이터를 캡처하는 방법이 필요하다. ATM Station Address 탭은 이러한 방법을 제공한다.

중요 정보 --

새로운 필터를 정의하려면, 먼저 Profiles 버튼을 클릭하여 새로운 필터에 이름을 부여한다. 그 다음 설정 내용을 구성한다.

그림 5-7은 필터 설정 대화 상자의 ATM Station Address 탭을 보여주고 있다.



Known Address 목록에서 문자로 표시된 주소를 스테이션 1 또는 스테이션 2로 드래그 앤 드롭. Known Address는 Broadcast와 Well-Know Address, 호스트 테이블 또는 Address Book에서 가져온다.

주소를 직접 입력할 수도 있다.

Mode: ○ Include ● Exclude

	Station 1	Dir.	Station 2
1	470000000000000000000	↔	Any
2		↔	
3		↔	
4		↔	
5		↔	

지정된 주소에 대한 패킷을 포함시킬 것인지 또는 제외시킬 것인지를 선택

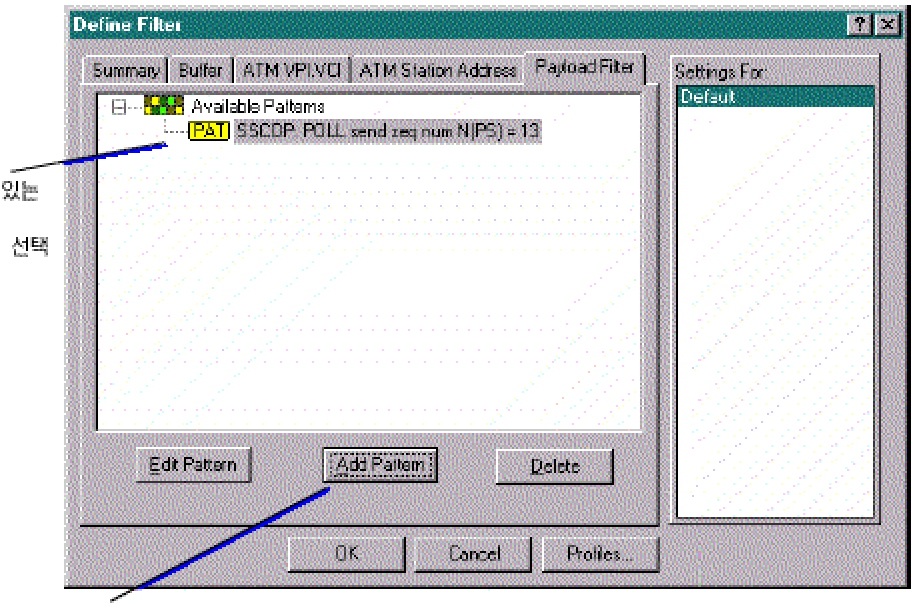
Dir 옵션을 설정하여 트래픽의 흐름 방향을 선택

먼저, 새로운 필터에 네임을 부여하기 위하여 클릭

그림 5-7. ATM Station Address 필터 정의하기

Payload 유형으로 필터링 하기 (ATMBook Only)

만일 ATM Book 을 사용하고 있다면, 당신이 지정한 데이터 패턴 범주에 부합하는 패킷들만 캡처하는 필터들을 설정하기 위하여 Define Filter 대화 상자의 **Payload Filter** 탭을 사용할 수 있다. 패턴 필터들은 각 캡처 된 셀의 첫번째 48 바이트(각 53 바이트 셀의 5 바이트 헤더를 제외한 셀)에 적용한다.



사용할 수 있는 payload 패턴들에서 선택

새로운 패턴을 추가할 수 있는 대화 상자를 열기 위해 여기를 클릭.
Decode 디스플레이에서 프레임을 선택할 수 있으며, 선택된 프레임은 자동으로 추가됨.

그림 5-8. Payload Filter 설정하기 (ATM Book 에서만)

WAN/Synchronous 프레임 유형에 의한 필터링 하기

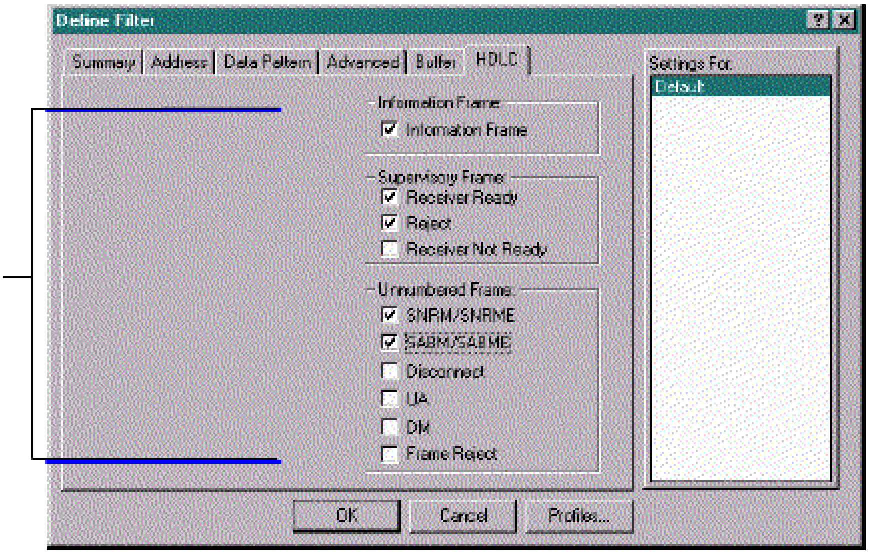
WAN/Synchronous 어댑터가 현재 사용하는 프로브(probe)로 선택되었을 때, Filter Setting 대화 상자에는 새로운 탭이 나타난다. Options 대화 상자 내에 현재 선택된 캡슐화 프로토콜에 따라서 이 탭은 아래 목록 가운데 하나가 될 수 있다.

- SDLC
- X.25
- Frame Relay
- HDLC

이러한 탭들은 캡처에 포함하거나 제외시키고자 하는 다양한 프레임 유형들을 선택하기

위하여 사용한다. 필터처럼 사용할 수 있는 프레임 유형은 현재 활성화된 캡슐화 프로토콜과 일치한다. 예를 들어, 만일 캡슐화 프로토콜로 HDLC/Router/Bridge 가 선택되었다면, HDLC 정보 프레임(Information Frames), 수신기 준비(Receiver Ready) 프레임, 거절(Reject) 프레임 등을 포함하거나 제외시킬 수 있다.

*그림 5-9*는 Filter Settings 대화 상자의 **HDLC** 탭을 보여주고 있다.



Settings For: Default

Information Frame
☑ Information Frame

Supervisory Frame
☑ Receiver Ready
☑ Reject
□ Receiver Not Ready

Unnumbered Frame
☑ SNRM/SNRME
☑ SABM/SABME
□ Disconnect
□ UA
□ DM
□ Frame Reject

필터링하려는 패킷의 유형 들을 지정. 표시된 모든 패킷 유형들은 데이터에 포함됨.

그림 5-9. WAN/Synchronous 프레임 유형 필터 설정하기

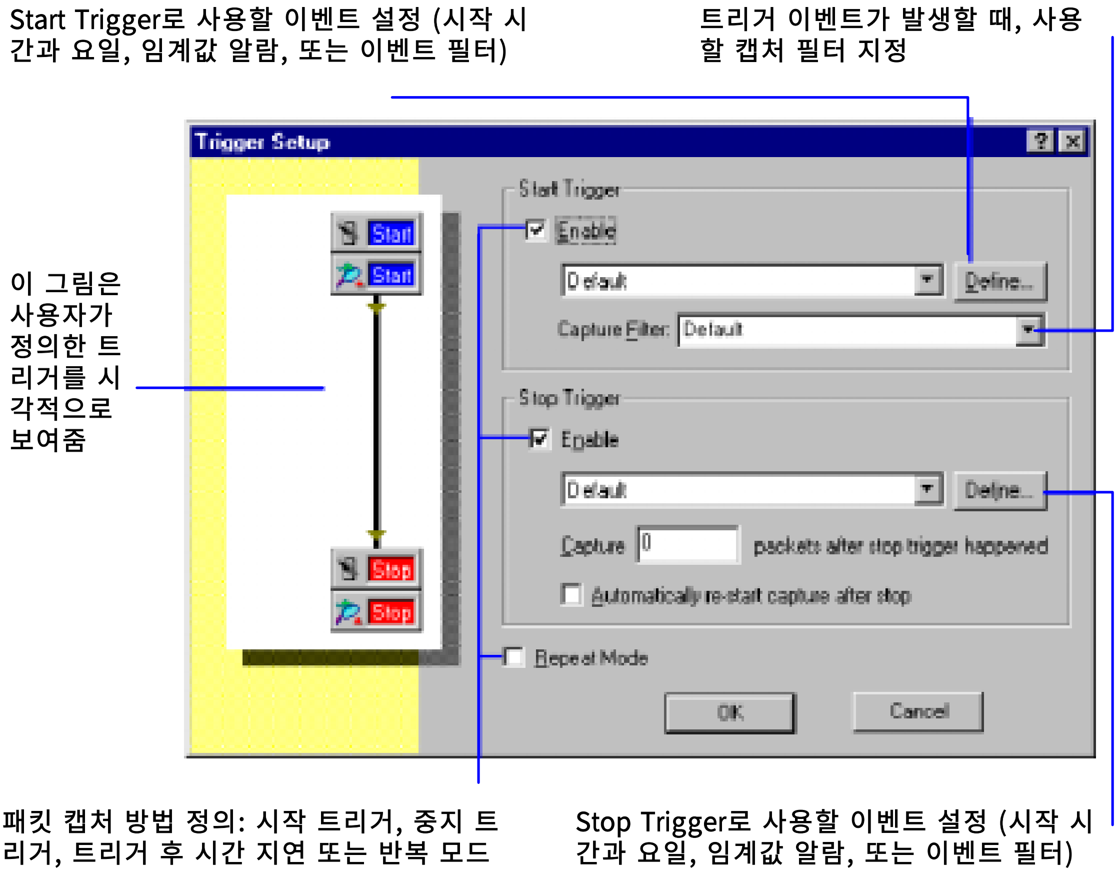
트리거(Triggers) 정의하기

트리거는 날짜와 시간, 알람, 그리고 특정 네트워크 이벤트들을 기반으로 캡처를 시작하고 중지한다. 트리거를 사용하여 업무이외의 시간이나 주말과 같이 Sniffer Pro 를 지켜볼 수 없는 상황에서도 데이터를 캡처 할 수 있으며, 알람 조건과 같이 특정 이벤트가 발생하였을 경우에 캡처를 시작할 수도 있다.

트리거는 다음 세가지 유형으로 정의할 수 있으며, 필터에서처럼, 트리거를 정의하고 이름을 붙이면 차후에 필요한 경우에 다시 사용할 수 있다.

- 시작 트리거(start triggers) : 캡처 세션이 시작하는 시점.
- 중지 트리거(stop triggers) : 캡처 세션이 중지하는 시점.
- 시작과 중지 트리거(start and stop triggers) : 캡처 세션의 시작과 중지 시점을 모두.

트리거를 정의하려면, **Capture** 메뉴에서 **Trigger Setup** 을 선택한다. 트리거 설정을 위한 대화 상자는 다음 *그림 5-10*과 같다.



Start Trigger로 사용할 이벤트 설정 (시작 시간과 요일, 임계값 알람, 또는 이벤트 필터)

트리거 이벤트가 발생할 때, 사용할 캡처 필터 지정

이 그림은 사용자가 정의한 트리거를 시각적으로 보여줌

Trigger Setup

Start Trigger

☑ Enable

Default

Capture Filter: Default

Stop Trigger

☑ Enable

Default

Capture 0 packets after stop trigger happened

□ Automatically re-start capture after stop

□ Repeat Mode

패킷 캡처 방법 정의: 시작 트리거, 중지 트리거, 트리거 후 시간 지연 또는 반복 모드

Stop Trigger로 사용할 이벤트 설정 (시작 시간과 요일, 임계값 알람, 또는 이벤트 필터)

그림 5-10. 트리거 필터 정의하기

6. 주소록 (Address Book) 사용하기

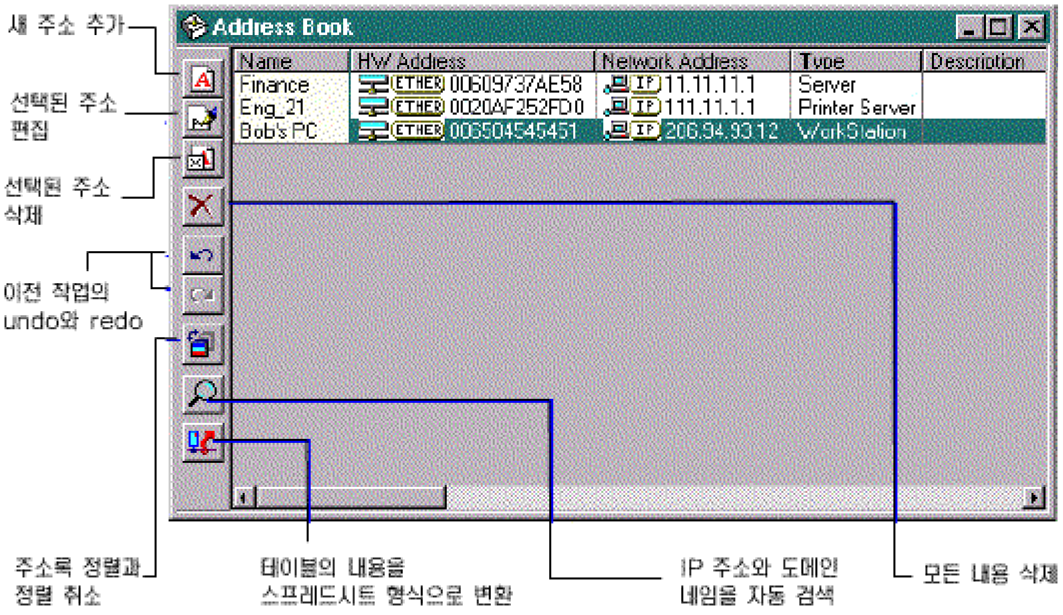
Sniffer Pro 의 주소록은 당신의 네트워크 노드에 친숙하고, 알기 쉬운 호스트 네임을 할당할 수 있게 한다. 문자로 표시된 이름들은 아래와 같은 상황에서 6 바이트 하드웨어 주소, IP 주소, 그리고 ATM 주소의 대체용으로 사용된다.

- 필터 정의
- 캡처 디코드 디스플레이
- Expert 디스플레이
- 호스트 테이블 디스플레이 (모니터와 캡처 모두)
- 매트릭스 디스플레이 (모니터와 캡처 모두)

주소록 생성하기

사용자의 네트워크에 소속되어 있거나 통신하고 있는 호스트들의 이름을 테이블로 보관하기 위하여 주소록을 만든다. 호스트 네임을 수동으로 입력하거나, 외부에 있은 주소 테이블을 불러올 수 있으며, 주소록의 자동 검색 기능을 사용하여 자동으로 검색할 수도 있다.

주소록을 열려면, Tools 메뉴에 있는 Address Book 을 선택하거나, 메인 툴바에서 버튼을 클릭한다.



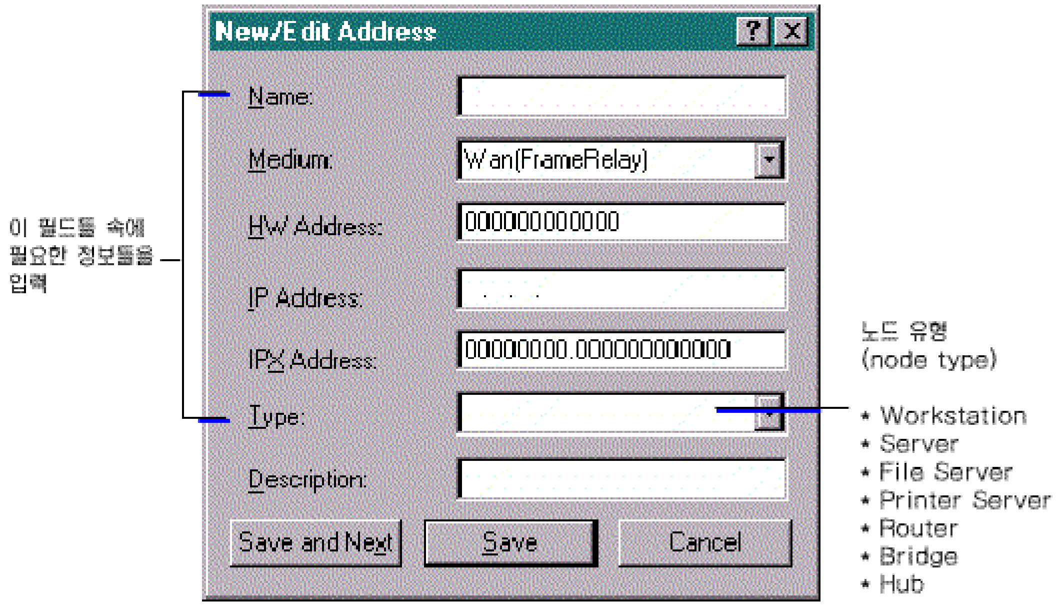
Name	HW Address	Network Address	Type	Description
Finance	ETHER 00609737AE58	IP 11.11.11.1	Server	
Eng_21	ETHER 0020AF252FD0	IP 111.11.1.1	Printer Server	
Bob's PC	ETHER 006504545451	IP 206.94.93.12	WorkStation	

그림 6-1. 주소록 (Address Book)

수동으로 호스트 네임 입력하기

호스트 테이블에서 하드웨어 주소와 IP 주소를 가져옴으로써 자신만의 주소록을 만들 수 있다.

주소록에 새로운 주소를 첨가하려면, **Tools** 메뉴에서 **Address Book** 을 선택한 후, Address Book 툴바에 있는 **New Address** 버튼을 클릭한다. New/Edit Address 대화 상자가 나타나며, 이곳에 새로운 노드에 대한 주소 정보를 입력할 수 있다. *그림 6-2* 를 보자.



New/Edit Address

Name:

Medium: Wan(FrameRelay)

HW Address: 000000000000

IP Address: . . .

IPX Address: 00000000.000000000000

Type:

Description:

이 필드들 속에 필요한 정보들을 입력

노드 유형 (node type)

- Workstation
- Server
- File Server
- Printer Server
- Router
- Bridge
- Hub

그림 6-2. 수동으로 호스트 네임 입력하기

Medium 필드

Medium 필드를 달리 표현하면, *topology* 필드라고 할 수 있다. 즉, Address Book 을 작성하려고 하는 네트워크 종류를 지정하는 곳이다. **Medium** 필드는 Address Book 에 있는 각 항목들이 소속되어 있는 네트워크 종류를 Sniffer 에게 알려주는 것이다.

Medium 필드의 설정 내용은 사용자가 입력할 수 있는 **HW Address** 의 종류를 결정하게 된다. 예를 들어, Medium 필드에 Ethernet 이라고 설정했다면, **HW Address** 필드에는 16 진수 표준 Ethernet 하드웨어 주소를 입력할 수 있다. 그렇지만, **Medium** 필드에 **ATM (Connection)**이라고 설정하면, **HW Address** 필드에 VPI.VCI 값을 입력하는 빈 공간이 제공된다.

주소록 불러오기

Sniffer Pro 는 다른 어플리케이션(NetXRay 와 WebXRay 와 같은)으로부터 혹은 Sniffer Pro 주소록에 있는 로컬 호스트 파일에서 주소 테이블을 불러올 수 있다. 불러오는 주소는 반드시 CSV 형식이어야 하며, Sniffer Pro Program 디렉터리에 제공되는 Visual Basic 스크립트를 이용하여 주소록 안에 불러져야 한다.

주 --

주소록에는 최대 5,000 개의 항목이 입력될 수 있다.

주소 테이블을 불러오려면, **File** 메뉴에서 **Run Script** 를 선택한다. Sniffer Pro Program 디렉터리에서 적당한 스크립트를 선택한 후, **Open** 을 클릭한다. Open 대화 상자에서 .csv 파일을 선택하고 **Open** 을 클릭한다.

주소와 이름의 자동 검색

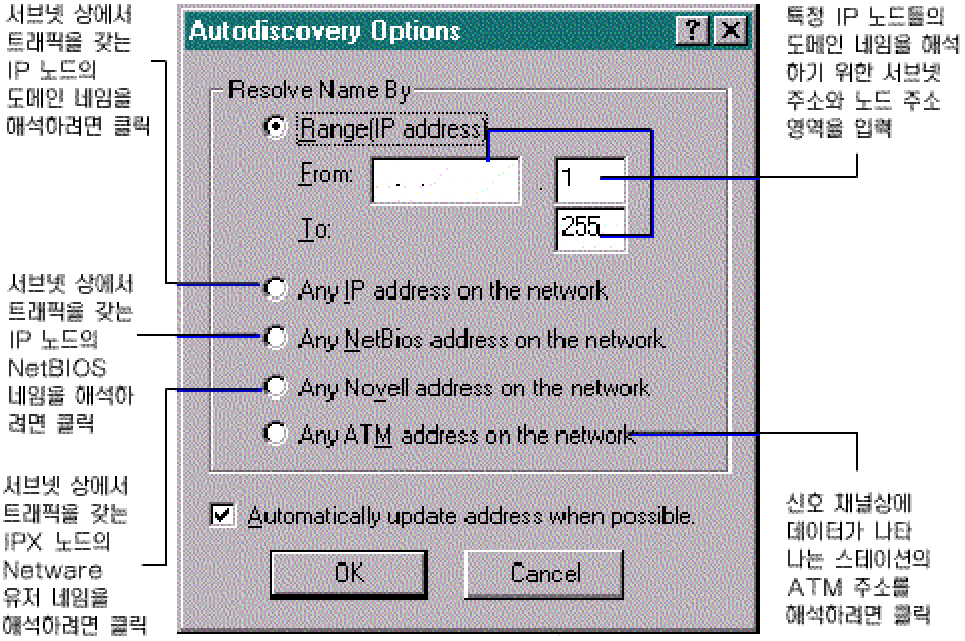
Sniffer Pro 는 다음과 같은 호스트 네임과 주소를 자동으로 검색하고 그들을 주소록에 저장하는 자동 검색 기능을 제공한다.

- 네트워크 노드의 IP 주소, 이와 관련된 하드웨어 주소, 그리고 도메인(domain) 네임
- 네트워크 노드의 NetBIOS 네임과 하드웨어 (MAC 주소)
- IPX 네트워크 노드의 Netware 유저 네임과 하드웨어 (MAC) 주소
- Signaling channel 상에서 보이는 ATM 주소

중요 정보 --

Netware 사용자 이름과 MAC 주소를 자동 검색하는 동안, 반드시 DOS 창으로 통하여 Netware 서버에 로그인하고 *userlist /a* 명령을 입력해야 한다. 이러한 명령은 Sniffer Pro 가 *로그인 유저 네임(login user name)*과 하드웨어 주소를 가져올 수 있도록 하는 것이다.

자동 검색 기능을 사용하려면, 주소록 툴바에 있는 **autodiscovery** 🔍 버튼을 클릭하거나 오른쪽 마우스 버튼을 클릭하고 **Auto Discovery** 를 선택한다. Discovery Option 대화 상자가 나타나면, 해석하기 원하는 주소의 유형을 선택한다. (*그림 6-3*)



서브넷 상에서 트래픽을 갖는 IP 노드의 도메인 네임을 해석하려면 클릭

서브넷 상에서 트래픽을 갖는 IP 노드의 NetBIOS 네임을 해석하려면 클릭

서브넷 상에서 트래픽을 갖는 IPX 노드의 Netware 유저 네임을 해석하려면 클릭

특정 IP 노드들의 도메인 네임을 해석하기 위한 서브넷 주소와 노드 주소 영역을 입력

신호 채널상에 데이터가 나타나는 스테이션의 ATM 주소를 해석하려면 클릭

Autodiscovery Options

Resolve Name By

● Range(IP address)

From: . . . 1

To: 255

○ Any IP address on the network

○ Any NetBios address on the network

○ Any Novell address on the network

○ Any ATM address on the network

☑ Automatically update address when possible.

그림 6-3. Autodiscovery Options 설정하기

라우터를 위한 자동 검색 설정하기

라우터는 다른 서브넷과 당신의 Sniffer Pro 가 상주하는 로컬 세그먼트 사이에 트래픽을 이동시키기 때문에, 라우터의 하드웨어 주소는 해당 라우터를 경유하는 어떤 IP 주소와 관련 있을 것이다. 이것은 자동 검색 과정에서 중복 IP 주소로 나타난다. 자동 검색이 중복 IP 주소들을 찾게 되면, 그 주소를 알람 로그의 내용으로 추가하며, 알람 소리를 낸다. 이와 같은 중복 IP 주소 알람의 실수를 막기위해서는, 먼저 당신 IP 네트워크 라우터의 IP 주소, 하드웨어 주소, 그리고 도메인 네임을 주소록에 수동으로 입력하여, Type 을 Router 로 설정한다.

Netware 4.x 네임과 주소

만일 Novell Netware 4.x 를 사용하고 있다면, Netware 서버로부터 유저 목록을 축적하기 위하여 자동 검색 기능을 사용하는 대신 다음과 같은 처리 과정을 수행할 수 있다. (목록에는 단지 현재 서버에 로그인 된 유저들만 포함할 것이다.)

1. DOS 창에서 다음 명령어를 입력한다.

   Nlist user /a > \ *install-directory*\ program \ novell.txt

주 --

Install-directory 에는 Sniffer Pro 가 설치된 디렉터리로 입력한다.

----

2. Sniffer Pro **File** 메뉴에서 **Run Script** 를 선택한다.
3. **ImpNovAddr.bas** 를 선택한 후, 1 과정에서 생성된 novell.txt 을 선택한다.

Gigabit Ethernet 어댑터에서 자동 검색 사용

Gigabit Sniffer Pro 에서도 다른 Sniffer Pro 네트워크 토폴로지와 동일한 자동 검색 기능을 제공한다. 자동 검색은 Sniffer Pro 가 네트워크 노드들의 이름과 주소를 알아내어 자동으로 주소록에 추가하게 된다.

그러나 Gigabit Sniffer Pro 는 다른 토폴로지와 조금 다르게 동작한다. 주요 차이점은 아래와 같다.

- **Any IP address on the network** 와 **Any IPX address on the network** 옵션 기능은 Gigabit Ethernet 어댑터의 버퍼에서 PC 캡처 버퍼로 데이터 전송이 있는 동안에만 정상적으로 동작한다.
- Range (IP address)를 사용하려면, Sniffer Pro PC 의 Gigabit Ethernet 어댑터가 접속되어 있는 네트워크 세그먼트와 같은 곳에 두 번째 Ethernet 어댑터를 접속해야 한다. Range (IP address)가 지정되면, Gigabit Sniffer Pro 는 두 번째 어댑터를 사용하여 정의된 각 IP 주소에 ping 을 할 것이다. 여전히 Gigabit Ethernet 어댑터의 버퍼에서 PC 캡처 버퍼로 데이터 전송이 있는 동안에만 주소록의 각 항목들이 남아있게 될 것이다.
- **Any NetBios address on the network** 옵션은 Gigabit Sniffer Pro 에서 동작하지 않는다.

Full Duplex 10/100 Ethernet 어댑터 또는 Snifferbook Ultra 에서 자동 검색 사용

Full Duplex 10/100 Ethernet 어댑터 카드와 Snifferbook Ultra 에서도 다른 Sniffer Pro 네트워크 토폴로지와 동일한 자동 검색 기능을 제공한다. 자동 검색은 Sniffer Pro 가 네트워크 노드들의 이름과 주소를 알아내어 자동으로 주소록에 추가하게 된다.

그렇지만, Full Duplex 10/100 Ethernet 어댑터 카드와 Snifferbook Ultra 에서는 다른 토폴로지와 조금 다르게 동작한다. Full Duplex 10/100 Ethernet 어댑터 카드나 Snifferbook Ultra 에서 자동 검색 기능을 사용하려면 아래 사항들을 기억해야 한다.

- 자동 검색은 오직 **Stream** 모드로 캡처가 진행되는 동안에만 동작한다.
- **Any IP address on the network, Any IPX address on the network** 및 Any NetBios address on the network 옵션은 **Stream** 모드로 캡처가 진행되는 동안에만 정상적으로 동작한다.
- Full Duplex 10/100 Ethernet 어댑터 카드에서는 **Range (IP address)** 옵션을 사용할 수 있지만, Sniffrbook Ultra 에서는 사용할 수 없다.

  Full Duplex 10/100 Ethernet 어댑터 카드에서 **Range (IP address)**을 사용하려면, Sniffer Pro PC 의 Full Duplex 10/100 Ethernet 어댑터 카드가 접속되어 있는 네트워크 세그먼트와 같은 곳에 두 번째 Ethernet 어댑터를 접속해야 한다. 더불어서, 이 두 번

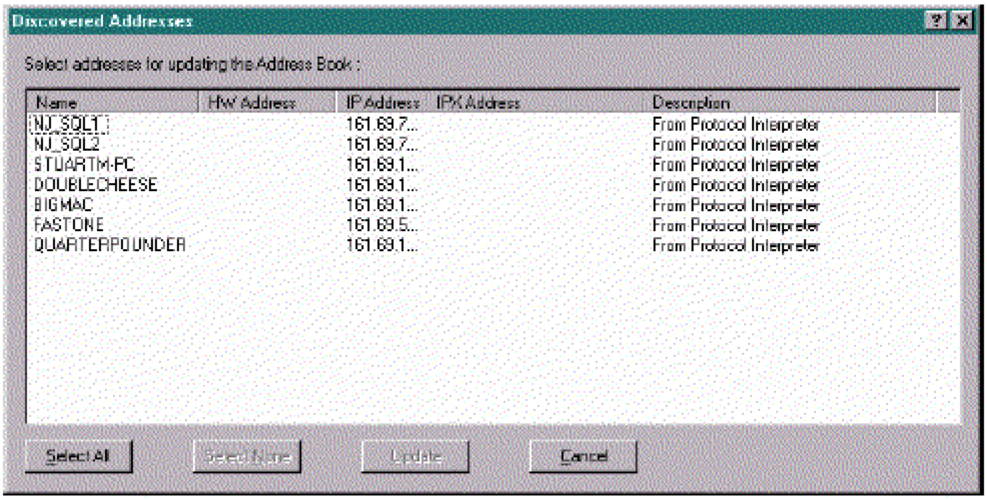
째 어댑터는 반드시 TCP/IP 설정이 되어 있어야 한다. **Range (IP address)**가 설정되면, FDX Sniffer Pro 는 두 번째 어댑터를 이용하여 지정된 IP 주소로 ping 동작을 수행할 것이다. 다른 옵션들과 마찬가지로 **Stream** 모드 캡처가 진행되는 동안에만 가능하다.

발견된 주소를 주소록에 첨가하기

캡처하는 동안에 Expert 분석기는 네트워크 상에서 자동으로 호스트 네임과 주소 쌍을 검색한다. 검색된 주소는 Discovered Address 대화 상자를 사용하여 분석기의 주소록에 첨가할 수 있다.

Expert 에 의하여 검색된 네임과 주소 쌍을 주소록에 첨가하기:

1. 캡처를 마친 후, 디스플레이 윈도우의 Expert 탭을 화면에 나타낸다.
2. 디스플레이 윈도우의 Expert 탭에 있는 **Discovered Addresses** 버튼을 클릭한다. Discovered Address 대화 상자가 나타난다. (*그림 6-4*) 이 대화 상자는 캡처 세션 동안에 검색되었던 새로운 호스트 네임과 주소 쌍들의 목록을 보여준다. 모든 호스트 네임과 주소 쌍이 이미 주소록에 등록되어 있는 것은 아니다.



Select addresses for updating the Address Book :

Name	HW Address	IP Address	IPX Address	Description
NJ_SQL1		161.69.7...		From Protocol Interpreter
NJ_SQL2		161.69.7...		From Protocol Interpreter
STUARTM-PC		161.69.1...		From Protocol Interpreter
DOUBLECHEESE		161.69.1...		From Protocol Interpreter
BIGMAC		161.69.1...		From Protocol Interpreter
FASTONE		161.69.5...		From Protocol Interpreter
QUARTERPOUNDER		161.69.1...		From Protocol Interpreter

그림 6-4. Discovered Addresses 대화 상자

3. 주소록에 첨가하고자 하는 주소들을 목록에서 선택한다. 여러 개의 내용을 선택하기 위하여 표준 Shift-클릭과 Ctrl-클릭 방법을 사용할 수 있다. 또한 선택 과정을 빠르게 하기 위하여 **Select All** 과 **Select None** 버튼을 사용할 수 있다.

4. 주소록에 첨가하려 하는 모는 주소의 선택이 끝나면, **Update** 버튼을 클릭한다.

5. 이제 주소록은 새롭게 추가된 내용들을 보여줄 것이다.

팁 --

Tools 메뉴에서 액세스 되는 Options 대화 상자의 General 탭은 검색된 호스트 네임과 주소 쌍을 저장하는 것에 대하여 재 확인하는 기능을 제공한다. 만일 Prompt to save/update 목록에 있는 Discovered Address 체크 박스를 표시하면, 분석기는 언제나 캡처 윈도우가 닫힐 때, 저장되지 않았던 검색된 주소들을 저장하기 원하는지 물을 것이다.

----

7. 알람(Alarms) 관리하기

Sniffer Pro 알람 기능은 네트워크 알람 이벤트를 검출하고 목록에 추가하는 포괄적인 방법을 제공한다.

- Sniffer Expert 는 데이터를 캡처하는 동안 알람을 생성한다. Expert 는 증상 혹은 분석 내용을 검출하면 이벤트를 알람 로그에 추가할 수 있다.
- 모니터의 알람 관리자는 Sniffer Pro 를 실행하면 자동적으로 시작한다. 이 관리자는 유저가 지적한 파라미터의 임계 값을 초과하면, 해당 이벤트를 알람 로그에 추가한다.
- Switch Statistics 어플리케이션의 **Alarm Config** 탭은 다른 스위치 포트 상에서 임계 값을 기반으로 하는 알람의 설정 방법을 제공한다. 임계 값을 초과하는 상황이 발생하면, 해당 알람들이 Sniffer Pro 에게 다시 보고된다.

특별히 중요한 등급의 알림이 발생할 경우, 전자 메일, 비퍼(beeper) 혹은 페이저(pager)로 당신에게 통보하도록 Sniffer Pro 구성할 수 있다. 알람의 등급은 Critical/Diag, Major, Minor, Waning, 혹은 Informational 의 5 가지 다른 중요도 가운데 하나에 할당 될 수 있다.

알람 로그

모든 알람 이벤트 (모니터 알람과 Expert 알람)들은 alarm log 에 등록되며, 이 목록은 **Monitor** 메뉴에 있는 **Alarm Log** 를 선택하거나, **Alarm** 버튼 ⚠을 클릭하여 화면에 디스플레이 할 수 있다.

각각의 알람 이벤트에 대하여, 알람이 시작되는 노드의 유형(예를 들어, 서버, 브릿지, 허브), 알람의 내역, 발생하는 시기, 중요도 등을 볼 수 있다.

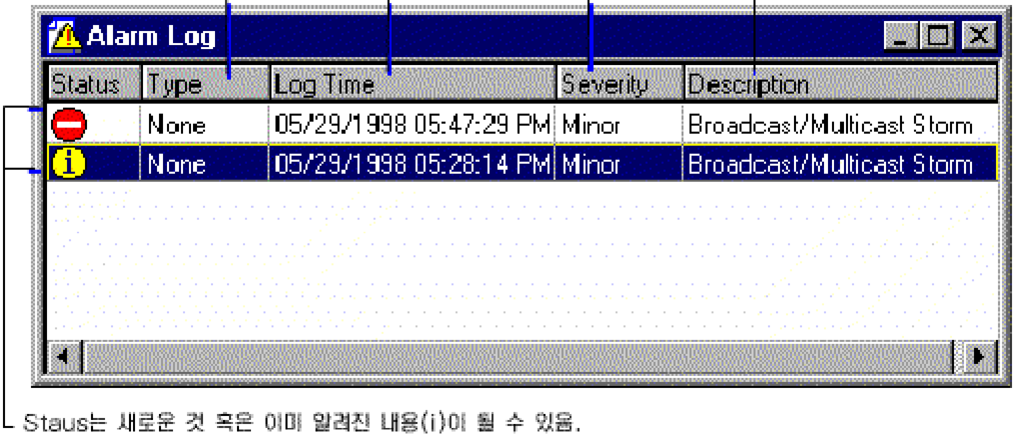
그림 7-1 은 알람 로그를 보여주고 있다.

알람을 트리거하는 노드의 유형(주소록에 정의된 내용)

알람이 트리거되었던 날짜와 시간

이 알람 유형에 할당된 중요도 (1에서 9)

에러 표시



Status	Type	Log Time	Severity	Description
⛔	None	05/29/1998 05:47:29 PM	Minor	Broadcast/Multicast Storm
ⓘ	None	05/29/1998 05:28:14 PM	Minor	Broadcast/Multicast Storm

Staus는 새로운 것 혹은 이미 알려진 내용(i)이 될 수 있음.
이미 알려진 알람으로 설정하려면 알람 항목에서 오른쪽 마우스 버튼을 클릭하여 Acknowledge 선택

그림 7-1. 알림 로그(Alarm Log)

알람의 중요도 설정하기

모니터와 Expert 알람(증상과 분석) 모두에 중요도를 할당할 수 있다.

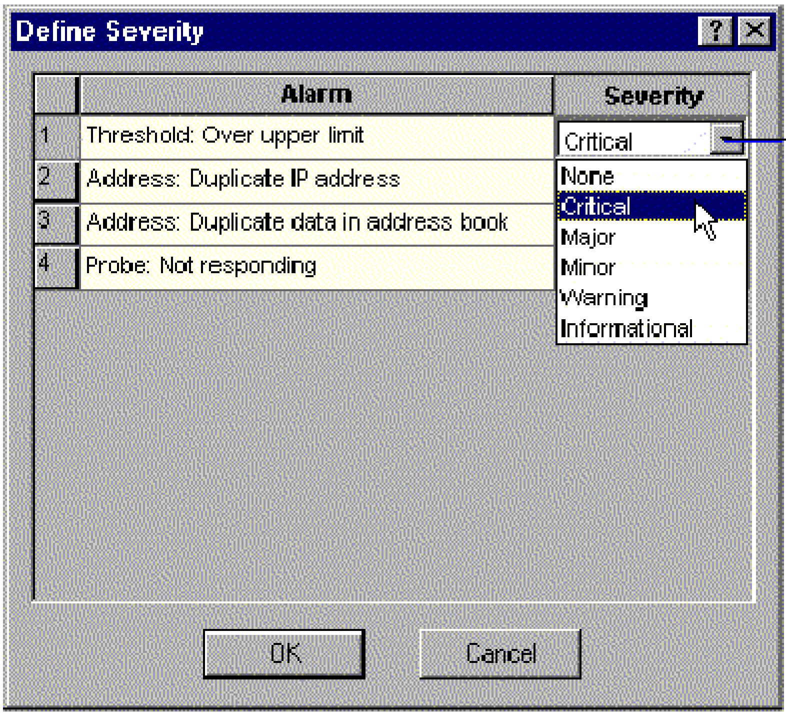
모니터 알람

기본적으로, Sniffer Pro 는 4 개의 이벤트 유형을 정의하고 각각에 중요도를 할당한다. 각 이벤트에 할당되는 기본적인 중요도는 당신이 지정한 네트워크 동작 환경에 적합하도록 바꿀 수 있다. *표 7-1* 은 기본적인 중요도 목록이다.

표 7-1. 기본적인 중요도

알람 이벤트	중요도
임계 값: 한계를 초과	Critical
주소: 복제 IP 주소	Critical
주소: 주소록에 복제 데이터	Informational
프로브: 응답하지 않음	Minor

알람의 중요도를 바꾸려면, **Tools** 메뉴에서 **Options** 을 선택한 후, **Alarm** 탭을 클릭한다. Define Severity 대화 상자를 열기 위하여 **Define Severity** 버튼을 클릭한다. (*그림 7-2*) 알람에 대한 중요도 옵션의 목록을 보기 위하여 Severity 항목을 클릭한다. 사용하기 원하는 것을 선택한 후, **OK** 를 클릭한다.



Define Severity

	Alarm	Severity
1	Threshold: Over upper limit	Critical
2	Address: Duplicate IP address	
3	Address: Duplicate data in address book	
4	Probe: Not responding	

드롭다운 목록에서 중요도를 선택

그림 7-2. 모니터 알람을 위한 중요도 설정하기

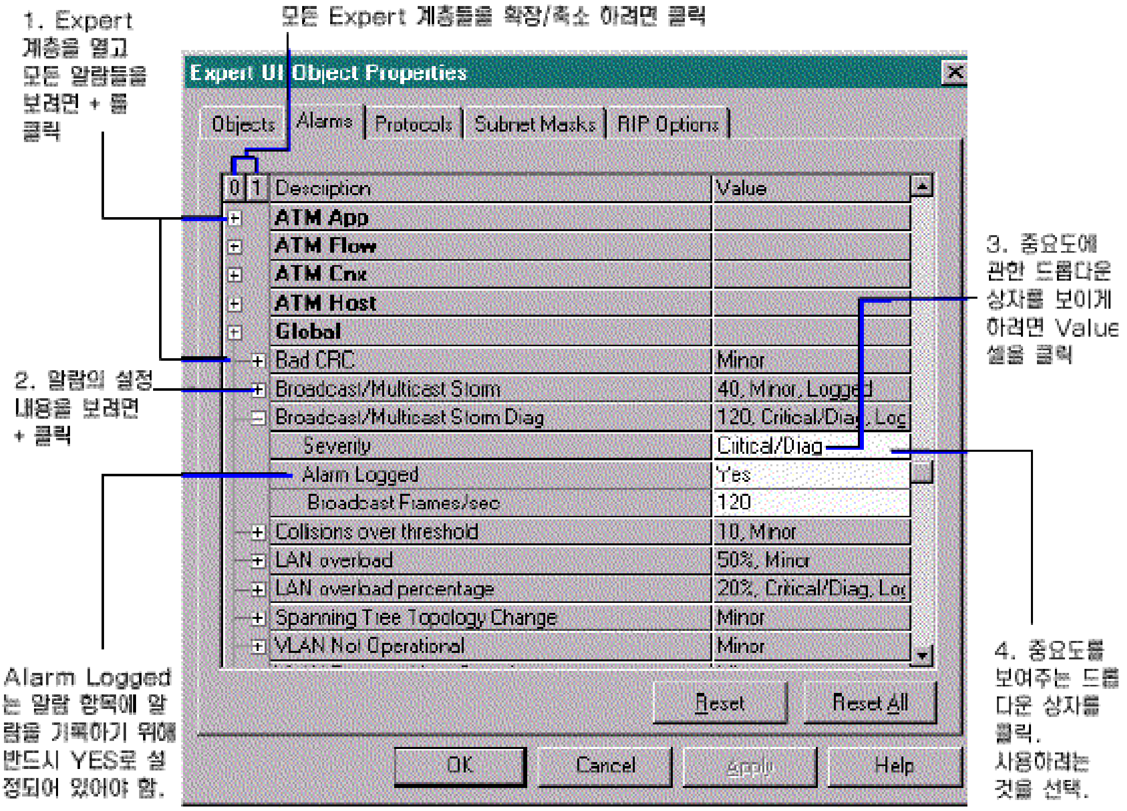
Expert 알람

Expert 알람(symptom 과 diagnosis)은 Critical/Diag, Major, Minor, Waning, 혹은 Informational 의 5 가지 다른 중요도 가운데 하나에 할당 될 수 있다. Symptom 또는 diagnosis 에 대한 중요도는 Expert 윈도우의 summary 창에 디스플레이 한다. 또한 만일 Tools/Expert Options/Alarms 탭에 있는 Alarm Logged 를 YES 로 설정하면 알람 이벤트는 알람 로그에 기록된다.

주 ---

알람이 사용자에게 통보되려면 반드시 알람 로그에 기록되어야 한다. *알람 통보 동작 설정하기*를 참조하자.

Expert 알람에 대한 중요도를 바꾸려면, Tools 메뉴에서 Expert Options 을 선택하고 Alarms 탭을 선택한다. *그림 7-3*은 Alarms 탭을 보여주고 있다.



1. Expert 계층을 열고 모든 알람들을 보려면 + 를 클릭

모든 Expert 계층들을 확장/축소 하려면 클릭

2. 알람의 설정 내용을 보려면 + 클릭

3. 중요도에 관한 드롭다운 상자를 보이게 하려면 Value 셀을 클릭

4. 중요도를 보여주는 드롭다운 상자를 클릭. 사용하려는 것을 선택.

Alarm Logged 는 알람 항목에 알람을 기록하기 위해 반드시 YES로 설정되어 있어야 함.

Expert UI Object Properties

Description	Value
ATM App	
ATM Flow	
ATM Cnx	
ATM Host	
Global	
Bad CRC	Minor
Broadcast/Multicast Storm	40, Minor, Logged
Broadcast/Multicast Storm Diag	120, Critical/Diag, Log
Severity	Critical/Diag
Alarm Logged	Yes
Broadcast Frames/sec	120
Collisions over threshold	10, Minor
LAN overload	50%, Minor
LAN overload percentage	20%, Critical/Diag, Log
Spanning Tree Topology Change	Minor
VLAN Not Operational	Minor

그림 7-3. Expert 알람에 대한 중요도 설정하기

알람 통보 동작 설정하기

알람에 할당할 수 있는 각 중요도(Critical/Diag, Major, Minor, Waning, 혹은 Informational)는 4 가지 이상의 알람 통보 동작에 할당될 수 있다. 이러한 통보 동작들은 하루가운데 특정 시간이나 1 주일 가운데 특정 요일에 동작하도록 설정할 수 있다. 알람이 시작될 때, Sniffer Pro 는 아래와 같은 작업을 수행할 수 있다.

- 사람이 들을 수 있는 알람 신호 소리를 내기
- 전자 메일의 전송
- 비퍼(beeper) 번호 호출
- 알람 문자열을 첨가한 페이저 호출
- 어플리케이션을 열기 위하여 Visual Basic 을 불러오거나 SNMO 콘솔에 SNMP 트랩(trap)처럼 알람 통보를 전송

주 --

비퍼나 페이저를 호출하기 위해서는 컴퓨터에 모뎀이 장착되어 있어야 한다.

통보 동작을 설정하려면, **Tools** 메뉴에서 **Options** 를 선택하고 **Alarm** 탭을 선택한다. Define Actions 대화 상자를 열기 위하여 **Define Actions** 를 클릭한다. (*그림 7-4*) **Add** 를 클릭하고 원하는 유형의 알람 응답을 선택하기 위하여 버튼을 선택한다. 설정 마법사는 위의 설정 과정을 도와줄 것이다.

주 ---

Expert 알람은 통보 과정에 포함되기 위하여 반드시 알람 로그에 기록되어야 한다. Expert 알람을 참조하라.

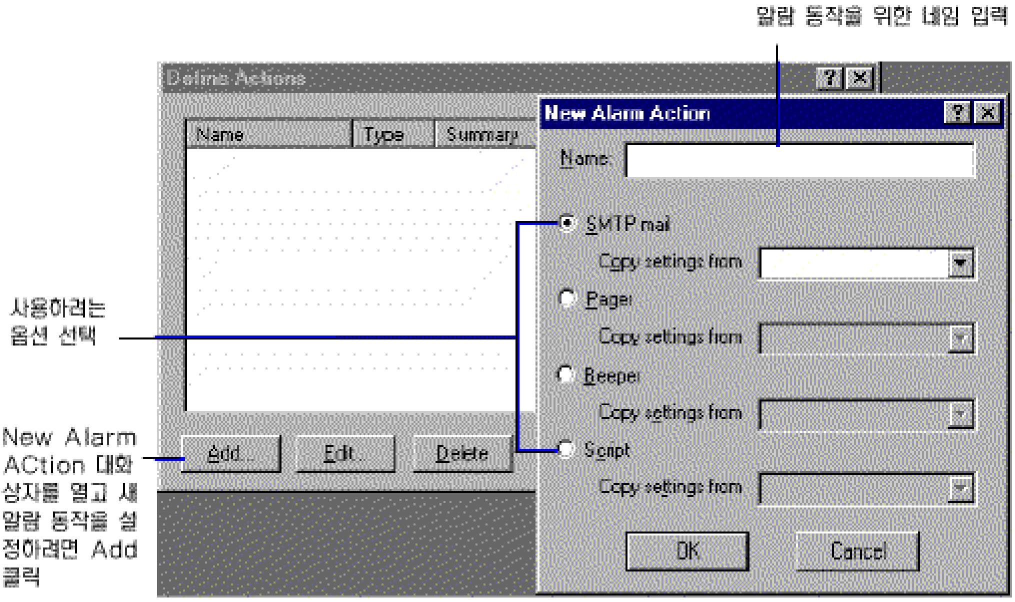


그림 7-4. 알람 통보 동작 설정하기

알람 동작 활성화 하기

알람 동작의 정의를 마친 후, 각 알람에 중요도를 할당해야 한다. 4 가지 이사의 동작에 중요도가 할당될 수 있다. 특수한 중요도를 갖는 알람이 발생하였을 때, 그 알람에 할당된 모든 동작들이 실행된다. (시간과 날짜 설정에 의해 동작 중지 상태가 아니라면)

주 ---

알람 동작이 수행되도록 알람을 ' enable' 해야 한다. 알람 동작을 활성화 하려면 **Alarm** 탭에 있는 **Enable New Alarm** 체크 상자를 체크 한다.

알람 신호와 소리

기본적으로, Sniffer Pro 는 알람이 발생할 때, 한가지 경보 소리를 발생시킨다. 만일 다른 소리가 더 마음에 든다면, 표준 경보음을 확장자가 wav 인 임의의 다른 파일로 교체할 수 있다. 이 작업을 하려면 **Alarm** 탭에서 … 버튼을 클릭하고 파일을 선택한다.

8. Sniffer Pro 도구 사용하기

Sniffer Pro 는 IP 네트워크 문제들을 확인하고 장애 검사를 할 수 있는 몇 가지 일반적인 도구를 포함하고 있다. *Ping, Trace Route, DNS Lookup, Finger* 그리고 *Who Is* 가 그것이다. 이러한 도구들은 **Tools** 메뉴에서 찾을 수 있다. 이번 장에서는 Sniffer Pro 에서 제공되는 도구들을 설명하고 사용자 자신 만의 도구를 첨가하는 방법에 대하여 논의한다.

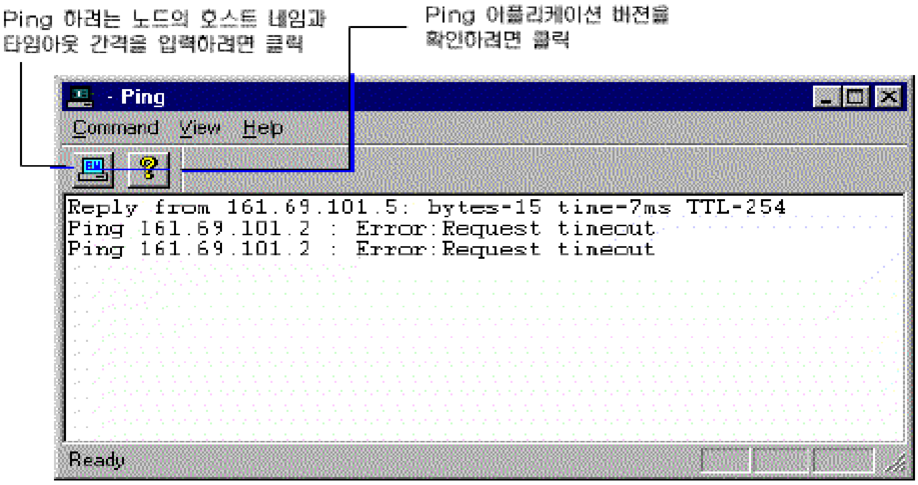
Ping

네트워크 상에서 특정 IP 호스트 노드에 접속이 가능한가 확인하기 위하여 Ping 을 사용한다.

Ping 은 당신이 지정한 호스트나 네트워크 게이트웨이로부터 ICMP ECHO RESPONSE 를 끌어내기 위하여 ICMP 프로토콜의 지정된 ECHO REQUEST 데이터그램을 활용한다.

- 만일 지정한 호스트가 응답하면, Ping 은 송신되고 수신된 바이트 수와 응답 시간, 그리고 TTL (Time to Live)을 화면에 표시한다.
- 만일 정의된 시간 내에 응답이 없으면, Ping 은 **Error: Request timeout** 메시지를 화면에 출력한다. 기본적인 ‘ timeout’ 주기는 300 msec 이다. 이 값은 네트워크의 환경에 따라서 적당한 값으로 조절할 수 있다.

그림 8-1 은 Ping 이 실행된 윈도우를 보여주고 있다.


Ping 하려는 노드의 호스트 네임과 타임아웃 간격을 입력하려면 클릭
Ping 어플리케이션 버전을 확인하려면 클릭
- Ping
Command View Help
Ready

```
Reply from 161.69.101.5: bytes-15 time-7ms TTL-254
Ping 161.69.101.2 : Error:Request timeout
Ping 161.69.101.2 : Error:Request timeout
```

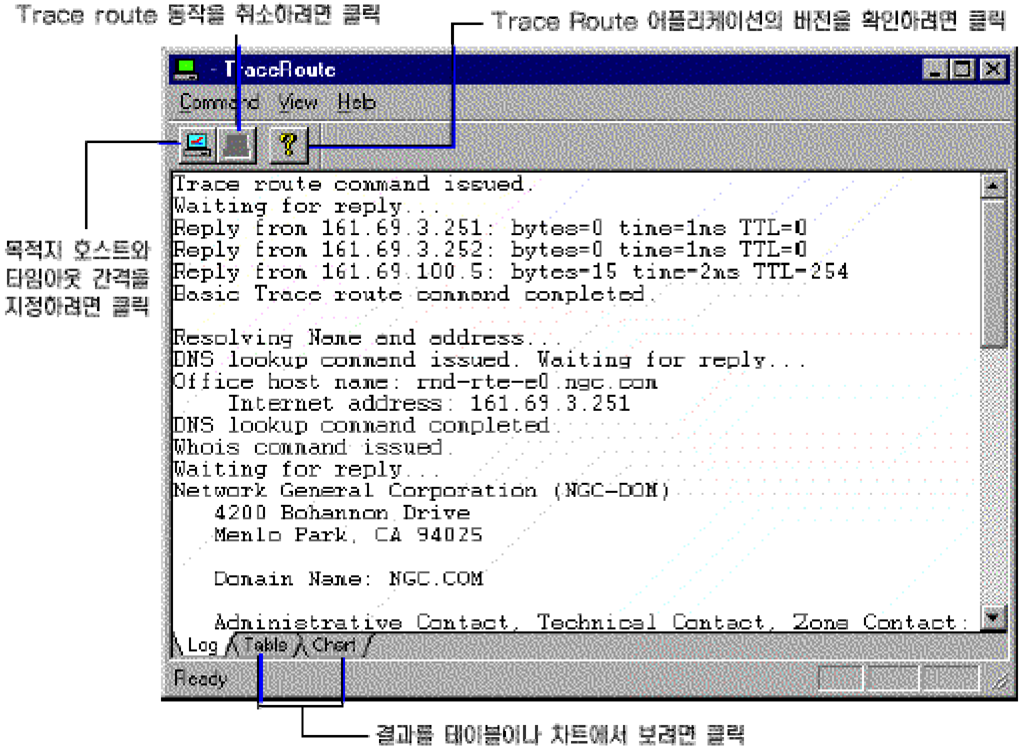
그림 8-1. Ping 실행 윈도우

Trace Route

중간에 있는 모든 라우터들의 IP 주소 및 Sniffer Pro 와 목적지 호스트 사이의 액세스 시간 지연을 확인하기 위하여 Trace Route 를 사용한다.

목적지의 IP 주소 혹은 DNS 네임 및 액세스 중지 시간 간격(기본값은 300 msec)을 입력한다. Trace Route 는 ICMP Trace Route 패킷들을 보낸다. 경로 상에 존재하는 라우터들은 자신의 존재를 보고하며, Trace Route 는 당신의 PC 와 목적지 호스트 사이의 경로를 보여주는 Trace Route 실행 윈도우를 생성하고 결과를 화면에 나타낸다. 또한 Trace Route 실행 윈도우의 아래 부분에 있는 Table 혹은 Chart 탭을 클릭하여 **Table** 이나 **Chart** 내에 있는 결과를 화면에 나타낼 수 있다.

*그림 8-2*는 Trace Route 실행 윈도우를 보여준다.

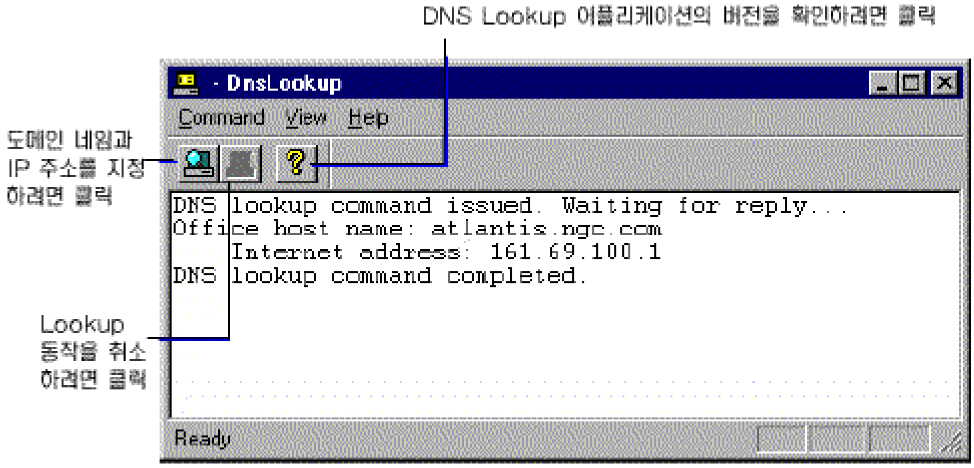

Trace route 동작을 취소하려면 클릭
Trace Route 어플리케이션의 버전을 확인하려면 클릭
목적지 호스트와 타임아웃 간격을 지정하려면 클릭
- TraceRoute
Command
View
Help
Log
Table
Chart
Ready
결과를 테이블이나 차트에서 보려면 클릭

```
Trace route command issued.
Waiting for reply...
Reply from 161.69.3.251: bytes=0 time=1ms TTL=0
Reply from 161.69.3.252: bytes=0 time=1ms TTL=0
Reply from 161.69.100.5: bytes=15 time=2ms TTL=254
Basic Trace route command completed.

Resolving Name and address...
DNS lookup command issued. Waiting for reply...
Office host name: rnd-rte-e0.ngc.com
    Internet address: 161.69.3.251
DNS lookup command completed.
Whois command issued.
Waiting for reply...
Network General Corporation (NGC-DOM)
   4200 Bohannon Drive
   Menlo Park, CA 94025

   Domain Name: NGC.COM

   Administrative Contact, Technical Contact, Zone Contact:
```

그림 8-2. Trace Route 실행 윈도우

DNS Lookup

IP 주소에 대한 도주 네임이나 도주 네임에 대한 IP 주소를 찾고자 할 때, DNS Lookup 을 사용한다. DNS Lookup 은 DNS 호스트에게 조회를 하고 조회 결과를 DNS Lookup 실행 윈도우 내에 나타낸다. *그림 8-3*을 보자.


DNS Lookup 어플리케이션의 버전을 확인하려면 클릭
도메인 네임과 IP 주소를 지정하려면 클릭
Lookup 동작을 취소하려면 클릭
- DnsLookup
Command View Help
Ready

```
DNS lookup command issued. Waiting for reply...
Office host name: atlantis.ngc.com
      Internet address: 161.69.100.1
DNS lookup command completed.
```

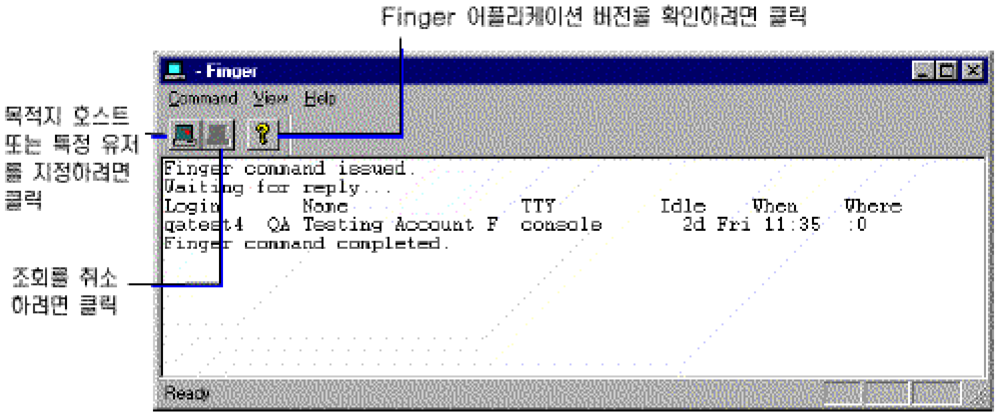
그림 8-3. DnsLookup 실행 윈도우

Finger

지정된 호스트에 로그인 된 사용자에 관한 정보를 디스플레이 하려고 할 때, Finger 를 사용한다. 이 명령어에는 호스트 네임이나 IP 주소를 입력할 수 있다.

특별한 유저에 대한 조회를 하려면, **Query** 필드에 유저네임을 입력한다. 모든 유저들을 보고자 한다면, **Query** 필드를 비워둔다.

Finger 는 조회 결과를 Finger 실행 윈도우 내에 나타낸다. *그림 8-4*를 보자.


Finger 어플리케이션 버전을 확인하려면 클릭
목적지 호스트 또는 특정 유저를 지정하려면 클릭
조회를 취소하려면 클릭
- Finger
Command View Help
Ready

```
Finger command issued.
Waiting for reply...
Login        Name                TTY          Idle    When     Where
qatest4   QA Testing Account F   console        2d Fri 11:35   :0
Finger command completed.
```

그림 8-4. Finger 실행 윈도우

Who Is

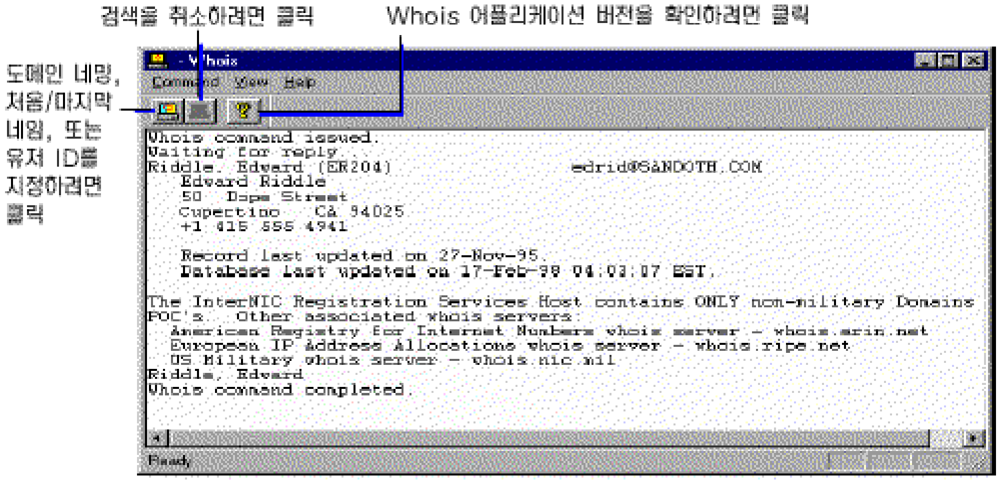
등록된 도메인 네임, 유저 네임, 혹은 유저 ID 에 대한 TCP/IP 디렉터리 내용을 검색하려할 때, Who Is 를 사용한다.

Who Is 검색 대상을 **Query** 필드에 입력한다. 이곳에는 다음과 같은 내용을 입력한다.

- 도메인 네임이면, *name.dom*;
  예를 들어, netscape.com
- 등록된 유저에 대해서는 *Firstname Lastname*
  예를 들어, 홍 길동
- 유저 ID 이면 userid;
  예를 들어, kdhong

또한 **Sever** 필드에 서버를 지정하여 특정 서버에만 검색을 한정시킬 수 있다.

검색 결과는 WhoIs 실행 윈도우에 나타난다. *그림 8-5*를 보자.


검색을 취소하려면 클릭
Whois 어플리케이션 버전을 확인하려면 클릭
도메인 네임, 처음/마지막 네임, 또는 유저 ID를 지정하려면 클릭
- Whois
Command
View
Help
Ready

```
Whois command issued.
Waiting for reply...
Riddle, Edward (ER204)                    edrid@SANDOTH.COM
   Edward Riddle
   50  Dope Street
   Cupertino    CA 94025
   +1 415 555 4941

   Record last updated on 27-Nov-95.
   Database last updated on 17-Feb-98 04:03:07 EST.

The InterNIC Registration Services Host contains ONLY non-military Domains
POC's.  Other associated whois servers:
  American Registry for Internet Numbers whois server - whois.arin.net
  European IP Address Allocations whois server - whois.ripe.net
  US Military whois server - whois.nic.mil
Riddle, Edward
Whois command completed.
```

그림 8-5. Whois 실행 윈도우

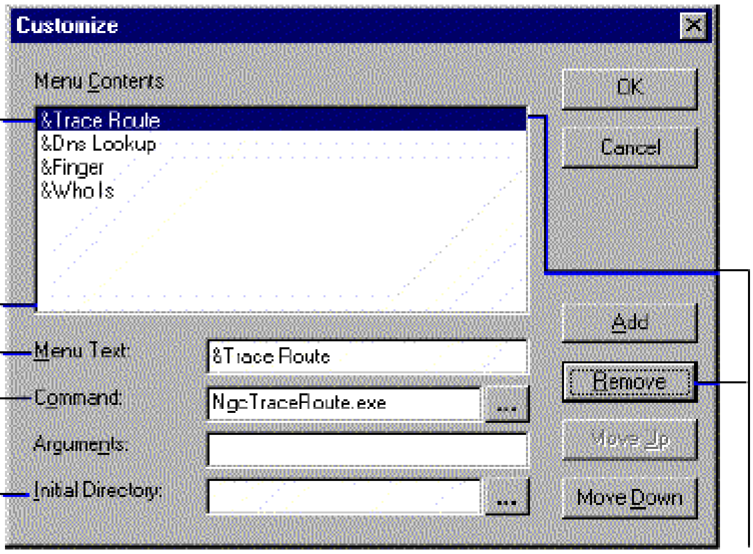
Tools 메뉴에 도구 첨가하기

Sniffer Pro 에서는 기본으로 제공되는 도구들과 더불어 사용자 자신만의 도구를 Tools 메뉴에 첨가할 수 있다. 첨가되는 도구는 사용자 자신의 컴퓨터에 현재 설치되어 있고 액세스 할 수 있는 Window 혹은 DOS 에서 실행 가능한 파일이어야 한다.

새로운 도구를 첨가할 때, 경로, 파일 네임 그리고 프로그램 실행에 필요한 명령어 파라미터들을 입력한다. Tools 메뉴에서 Customize User Tools 를 선택하여 Customize 대화 상자(*그림 8-6*)를 열고, 제공되는 필드들 내에 필요한 정보를 입력한다.

단축키를 할당하려면(Alt + t), 적당한 문자로 표시된 도구 네임 앞에 (&) 문자를 붙인다. 프로그램은 자동적으로 Alt + 번호를 할당하고, 할당된 단축키는 메뉴 아이템의 우측에서 볼 수 있다.

Tools 메뉴에 있는 도구들의 순서를 바꾸고 싶다면, Menu contents 상자에서 특정 도구를 선택하고 Move UP 혹은 Move Down 을 클릭한다.



Menu Contents:
&Trace Route
&Dns Lookup
&Finger
&Who Is

Menu Text: &Trace Route
Command: NgcTraceRoute.exe
Arguments:
Initial Directory:

Tools 메뉴에 보이는 도구들의 순서를 바꾸려면, 해당 도구를 선택하고 Move UP 또는 Movde Down을 클릭

Tools 메뉴에 보이게 되는 도구 네임을 입력

실행가능한 파일네임, 부가적인 파라미터, 그리고 도구의 적절한 시작을 위해 필요한 초기 시작 디렉토리를 입력

선택된 도구를 Tools 메뉴에서 삭제하려면 클릭

그림 8-6. Tools 메뉴에 도구 첨가하기

9. 패킷 생성기 사용하기

패킷 생성기를 사용하여 네트워크에 테스트 패킷을 전송함으로써 다음과 같은 작업을 할 수 있다.

- 장애 측정을 위하여 네트워크 문제를 다시 발생시키고 네트워크 장비나 어플리케이션의 상태 확인
- 실질적인 네트워크 상황을 시뮬레이션 하기 위하여 일정 수준의 네트워크 트래픽 부하를 생성하고 장비와 어플리케이션을 테스트

경 고---

실제 네트워크에 패킷을 전송하는 것은 여러 가지 기대하지 않았던 심각한 결과를 발생시킬 수도 있다. 네트워크에 안전한 패킷을 전송하고 있는지 확인하거나, 패킷 생성기를 사용하기 전에 전체 네트워크에서 해당 네트워크를 독립시켜야 한다.

패킷 생성기는 다른 Sniffer Pro 동작과 함께 CPU 리소스를 공유한다. 트래픽을 생성하고, 패킷을 캡처하며, 동시에 네트워크 부하를 모니터 할 수 있다. 그러나 여러 개의 프로세스를 동시에 띄우는 것은 성능에 영향 줄 수 있다.

중요 정보 ---

ATM 패킷 생성기는 Ethernet, token ring, 등과 같은 네트워크 토폴로지에서 사용되는 패킷 생성기와는 다르다. 이러한 내용은 이후에 다시 설명될 것이다.

표준 패킷 생성기 사용하기

패킷 생성기를 시작하려면, Tools 메뉴에서 Packet Generator 를 선택한다.

패킷 생성기를 이용하여 단일 패킷을 전송할 수 있으며, 이 패킷은 당신이 새로 만든 패킷이나 네트워크에서 캡처 한 패킷이 될 수도 있다. 또한 캡처 버퍼 혹은 캡처 파일의 전체 내용을 전송할 수 있다.

한 패킷, 캡처 버퍼 혹은 캡처 파일을 한번에, 지정된 횟수 만큼 또는 연속해서 전송할 수 있다. 만일 여러 개의 패킷들을 보내거나 연속해서 하나의 패킷을 전송하면, 각 패킷 사이의 지연 시간을 지정할 수 있다. (msec, 혹은 전송하고자 하는 패킷이 차지하는 회선 활용도의 % 비율로 지정 가능)

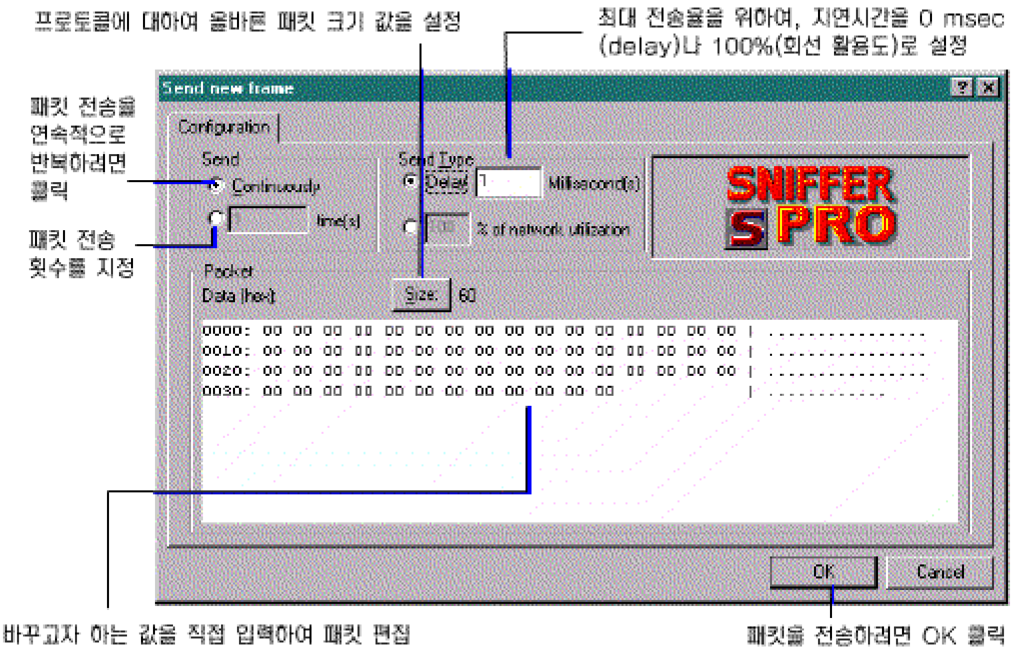
패킷 생성기는 두 가지 관찰 방법을 가지고 있다. Animation view 는 패킷이 전송되고 있을 때 보여진다. Detail view 는 패킷 전송 과정을 상세하게 보여준다.

단일 패킷 전송하기

한 패킷을 전송하기 전에, 보내려고 하는 메시지를 준비해야 한다. 캡처 된 패킷을 사용하거나 당신이 수정했던 캡처 된 패킷을 사용하여 전송할 패킷을 생성할 수 있다.

- 새로운 패킷을 생성하려면, Send new frame 대화 상자를 나타나게 하기 위하여 Packet Generator 윈도우에 있는 Send 1 frame 버튼을 클릭한다. 16 진수 코드는 **Configuration** 탭에서 직접 편집할 수 있다.
- 기존(캡처 된)의 패킷을 선택하거나 기존의 패킷을 편집하려면, 먼저 디코드 화면의 요약(summary) 창에서 패킷을 선택해야 한다. 그 다음, Send current frame 대화 상자를 나타나게 하기 위하여 패킷 생성기 윈도우에서 Send current frame 버튼을 클릭한다. 이곳에 표시되는 16 진수 코드는 **configuration** 탭에서 편집할 수 있다.

대화 상자에 있는 옵션을 선택하여 패킷을 보내는 방법을 제어할 수 있다. *그림 9-1* 은 Send new frame 대화 상자(Send current frame 대화 상자도 동일함)를 보여준다.


프로토콜에 대하여 올바른 패킷 크기 값을 설정
최대 전송율을 위하여, 지연시간을 0 msec (delay)나 100%(회선 활용도)로 설정
패킷 전송을 연속적으로 반복하려면 클릭
패킷 전송 횟수를 지정
바꾸고자 하는 값을 직접 입력하여 패킷 편집
패킷을 전송하려면 OK 클릭
Send new frame
? ×
Configuration
SNIFFER
S PRO
OK
Cancel

Send
● Continuously
○ time(s)

Send Type
● Delay 1 Millisecond(s)
○ % of network utilization

Packet
Data (hex)
Size: 60

```
0000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
0030: 00 00 00 00 00 00 00 00 00 00 00 00             | ............
```

그림 9-1. 단일 패킷 전송하기

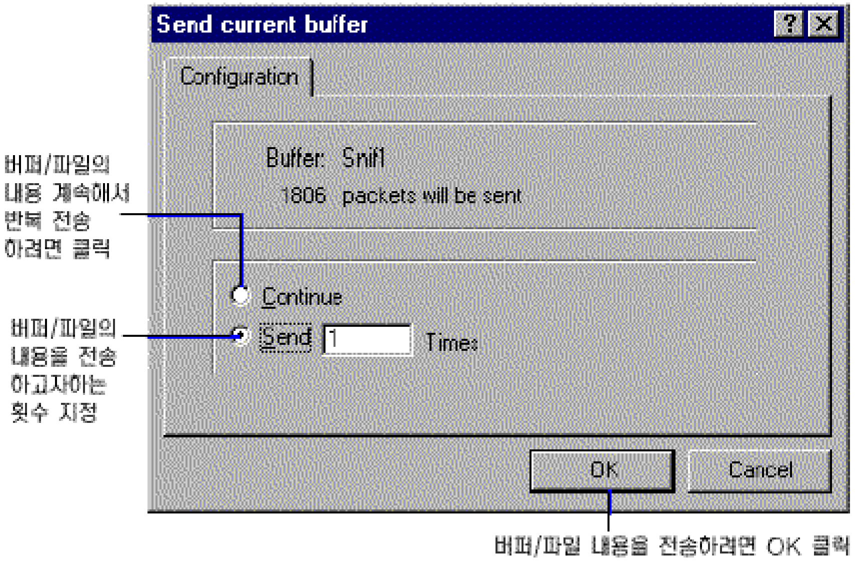
주

최대 전송 비율은 패킷의 크기, 네트워크의 성능, 컴퓨터의 CPU 속도, 그리고 시스템에 다른 프로세스가 동작하고 있는가에 의존한다.

캡처 버퍼나 파일 전송하기

현재의 캡처 버퍼나 캡처 파일을 전송하려면, 먼저 그 내용을 화면에 나타내야 한다. 현재 버퍼를 디스플레이 하려면, **Capture** 메뉴에서 **Display** 를 선택하고, 캡처 파일을 디스플레이 하려면, **File** 메뉴에서 **Open** 을 선택한다. 그 다음 패킷 생성기 윈도우에 있는 Send buffer 버튼을 클릭한다. Send current buffer 대화 상자는 버퍼/파일 내용에 대한 정보를 디스플레이 하여 전송하고자 하는 패킷의 제어 방법을 제공한다.

*그림 9-2*는 Send current buffer 대화 상자를 보여준다.



Send current buffer

Configuration

Buffer: Sniff1

1806 packets will be sent

○ Continue

● Send 1 Times

OK Cancel

버퍼/파일의 내용 계속해서 반복 전송 하려면 클릭
버퍼/파일의 내용을 전송 하고자하는 횟수 지정
버퍼/파일 내용을 전송하려면 OK 클릭

그림 9-2. 현재 버퍼 내용을 전송하기

ATM/Gigabit Ethernet 패킷 생성기 사용

ATM/Gigabit Ethernet 패킷 생성기를 시작하려면, 먼저 현재 모니터 하려고 선택된 것이 ATM 또는 Gigabit Ethernet 어댑터인가를 확인한다. 그 다음, **Tools** 메뉴에서 **Packet Generator** 를 선택한다.

주 --

이번 단원에서는 ATMbook 을 " ATM 어댑터" 로 간주한다. ATMbook 은 패킷 생성 기능을 제공한다.

ATM/Gigabit Ethernet 패킷 생성기를 이용하여, 단일 패킷을 전송할 수 있으며, 이 패킷은 당신이 새로 만든 패킷이나 네트워크에서 캡처 한 패킷이 될 수도 있다. 또한 캡처 버퍼 혹은 캡처 파일의 전체 내용을 전송할 수 있다.

한 패킷, 캡처 버퍼 혹은 캡처 파일을 한번에, 지정된 횟수 만큼 또는 연속해서 전송할 수 있다. 만일 여러 개의 패킷들을 보내거나 연속해서 하나의 패킷을 전송하면, 각 패킷 사이의 지연 시간을 지정할 수 있다.

사용하고 있는 어댑터가 ATM 인가 Gigabit Ethernet 인가에 따라 패킷 생성기는 다른 정보를 제공한다.

ATM 어댑터 – 패킷 생성기 윈도우

- **Detail** 탭은 개별 포트를 기준으로 패킷 전송 과정을 보여준다.
- **Connections** 탭은 ATM/Gigabit 패킷 생성기가 전송하는 각 VPI.VCI 에 대한 상세한 통계 자료를 전송한다.

Gigabit Ethernet 어댑터 – 패킷 생성기 윈도우

- **Detail** 탭에서는 트래픽 생성 과정에 대해 다양한 통계 자료를 제공한다.
- **Size Dist.** 탭에서는 트래픽 생성 과정에서의 상세한 패킷 크기별 분포 자료를 제공한다.

단일 패킷 전송하기

한 패킷을 전송하기 전에, 보내려고 하는 메시지를 준비해야 한다. 캡처 된 패킷을 사용하거나 당신이 수정했던 패킷을 사용하여 전송할 패킷을 생성할 수 있다. 또한 전송하기 위하여 Packet Setup 파일을 열수도 있다. Packet Setup 파일은 저장된 패킷과 패킷이 전송되

는 방법을 정의하는 일련의 옵션들을 포함하고 있다.

- 새로운 패킷을 생성하려면, Packet Setup 대화 상자를 나타나게 하기 위하여 Packet Generator 윈도우에 있는 Send 1 frame 버튼을 클릭한다. 다음으로 Edit Packet 대화 상자를 호출하기 위해 Edit 버튼을 클릭한다. 이 대화 상자에서 전송되는 패킷을를 직접 편집할 수 있다.
- 기존(캡처 된)의 패킷을 선택하거나 기존의 패킷을 편집
  - 디코드 화면의 요약(summary) 창에서 패킷을 선택해야 한다. 그 다음, 디코드 화면에서 우측 버튼을 클릭하면 나타나는 메뉴에서 **Send current frame** 명령을 선택하거나 Packet Setup 대화 상자에서 Send Current Packet 버튼을 클릭한다. 다음에 Edit Packet 대화 상자에서 Edit 버튼을 클릭하여 전송하려는 패킷을 직접 편집할 수 있다.
  - Packet Setup 대화 상자의 **Packet** 메뉴에서 **Load** 명령을 선택하여 Packet Library 에 미리 저장되어 있는 한 패킷을 선택한다.
- 전송하려는 패킷과 관련된 Packet Setup 파일을 선택하려면, Packet Setup 대화 상자를 열기 위하여 Send 1 frame 버튼이나 Send current frame 버튼을 클릭한다. 그 다음, 저장된 Packet Setup(*.pks) 파일을 열기 위하여 **Setup** 메뉴에서 **Open** 명령을 선택한다. 다른 패킷에 대한 Packet Setup 파일에 있는 전송 옵션을 사용하려고 한다면, 위에서처럼 Packet Setup 파일을 열고, 다음에 **Packet** 메뉴의 **Load** 명령을 이용하여 열려있는 Packet Setup 파일과 함께 사용하려고 하는 패킷을 선택한다.

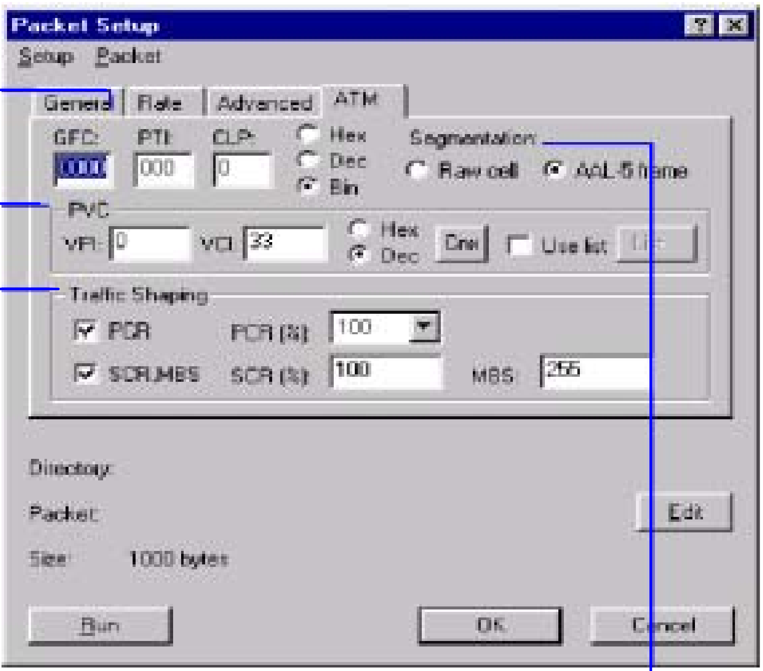
Packet Setup 대화 상자에 있는 옵션들을 정의하여 보내고자 하는 패킷을 처리하는 방법을 제어할 수 있다. Packet Setup 대화 상자는 아래와 같은 탭을 가지고 있다.

- **General** 탭은 선택된 패킷을 몇 차례 보낼 것인가를 지정할 수 있다. ATMbook 이 아닌 ATM 어댑터에서는 선택된 패킷을 전송하려는 포트를 선택할 수 있다.
- **Rate** 탭은 선택된 패킷이 전송되었을 때의 속도를 지정할 수 있게 한다.
- **Address** 탭 (**Gigabit Ethernet only**)에서는 전송되는 패킷 내에 있는 출발 주소와 도착 주소를 Address Book 에서 고정된 6 바이트, 임의로, 순차적인 데이터, 또는 선택적인 한 주소로 바꿀 수 있다.
- **Advanced** 탭은 생성되는 패킷에 대하여 보다 진보적인 옵션을 지정할 수 있다. **ATM** 에서는 임의의 패킷 크기로 생성할 것인가를 지정할 수 있으며, **Gigabit** 에서는 생성되는 패킷에 대한 시퀀스 번호나 타임스탬프(timestamp)을 지정할 수 있다.
- **ATM** 탭 (**ATM only**)에서는 전송되는 트래픽 내에 GFC 필드, PTI 필드, 그리고 CLP 비트의 값을 지정할 수 있다. 이와 더불어, 전송하는 것이 셀인지 프레임인지, 패킷 전송은 어떤 VPI.VCI 에서 수행되는가에 대하여 또한 지정할 수 있으며, 선택된 VPI.VCI 에 대한 트래픽 형성 파라미터들을 설정할 수 있다.
- **Gigabit** 탭 (**Gigabit Ethernet only**)에서는 생성되는 프레임에 몇 바이트의 preamble 이

포함되어 있는가와 자동 CRC 수정이 사용되는가를 지정할 수 있다.

Packet Setup 대화 상자의 Packet 메뉴에 있는 Edit 명령은 전송되는 패킷의 내용을 직접 수정할 수 있다.

*그림 9-3*은 Packet Setup 대화 상자의 ATM 탭을 보여준다.



GFC: 0000
PTI: 000
CLP: 0
○ Hex ○ Dec ● Bin
Segmentation: ○ Raw cell ● AAL-5 frame
PVC
VPI: 0
VCI: 33
○ Hex ● Dec
□ Use list
Traffic Shaping
☑ PCR PCR (%) 100
☑ SCR,MBS SCR (%) 100 MBS 255
Directory:
Packet:
Size: 1000 bytes

전송되는 패킷의 셀 헤더에 있는 GFC 필드, PTI 필드, CLP 비트의 값을 지정 (16, 10 또는 2 진수)

선택된 패킷을 전송하려는 VPI.VCI를 지정. 하나의 지정된 VPI.VCI에서 전송하거나, 전송하려는 15개 이상의 VPI.VCI 목록을 생성하기 위해 List 버튼을 클릭.
또한 잘 알려진 VPI.VCI를 선택하기 위해 주소록을 사용할 수 있슴.

선택된 패킷의 전송율을 제어하기 위한 Traffic Shapping 파라미터를 지정. Traffic Shapping 파라미터들은 Rate 탭에서 Traffic shapping 옵션이 설정되어 있어야만 사용됨.

Raw cell들을 전송할 것인지 AAL5 프레임을 전송할 것인지 지정

그림 9-3. ATM/Gigabit 패킷 생성기에서 단일 패킷 전송하기

주 --

최대 전송 비율은 패킷의 크기, 네트워크의 성능, 컴퓨터의 CPU 속도, 그리고 시스템에 다른 프로세스가 동작하고 있는가에 따라서 다르다.

캡처 버퍼나 파일 전송하기

버퍼 모드에서 ATM /Gigabit 패킷 생성기는 열려있는 캡처 버퍼나 저장된 파일의 내용을 전송한다. 버퍼의 내용을 전송하기 전에 보내려고 하는 버퍼를 구성해야 한다. 전송 버퍼는 Buffer Setup 대화 상자에서 구성한다. 이 대화 상자는 아래와 같은 방법으로 디스플레이 할 수 있다.

- Sniffer Pro 의 **Tools** 메뉴에서 **Packet Generator** 명령을 선택한다.패킷 생성기 윈도우

에 대화 상자가 나타나면, Send Buffer 버튼 을 클릭한다.

- Sniffer Pro 의 Decode 화면에서 오른쪽 마우스 버튼을 클릭하면, 새로운 서브 메뉴가 나타난다. 서브 메뉴가 나타나면, 항목 가운데 Send Current Buffer 옵션을 선택한다.

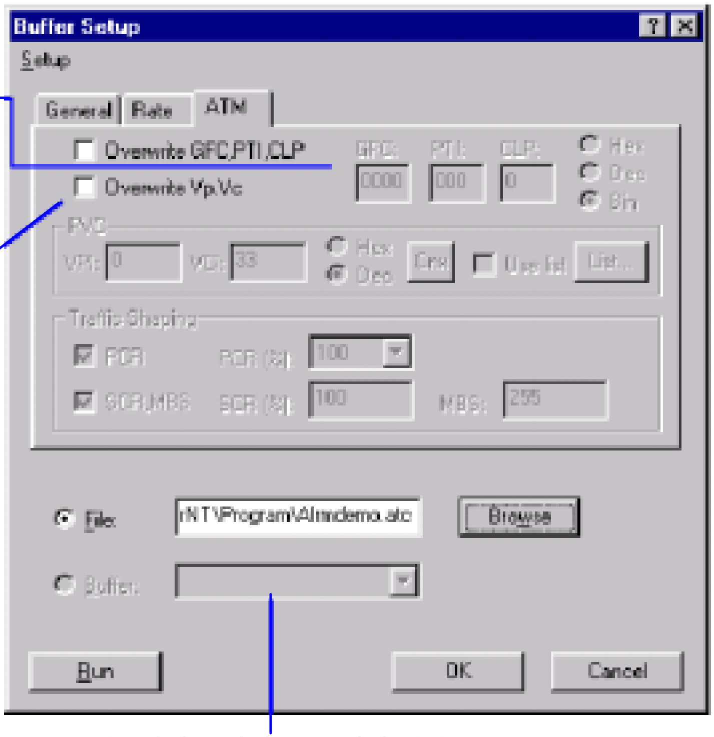
어떤 방법을 선택하든 상관없이, Buffer Setup 대화 상자가 나타난다. Buffer Setup 대화 상자는 전송하려는 버퍼, 전송 간격, 전송되는 포트 등을 구성할 수 있게 한다. Buffer Setup 대화 상자는 다음과 같은 3 가지의 탭을 가지고 있다.

- General 탭은 선택된 패킷을 몇 차례 보낼 것인가를 지정할 수 있다. ATMbook 이 아닌 ATM 어댑터에서는 선택된 패킷을 전송하려는 포트를 선택할 수 있다. Gigabit Ethernet 에서는 버퍼에 있는 모든 데이터를 전송할 것인지 또는 한 포트나 다른 포트에서 수신된 데이터만 전송할 것인지를 정할 수 있다.
- Rate 탭은 선택된 패킷이 전송되었을 때의 속도를 지정할 수 있게 한다.
- ATM 탭 (ATM only)은 선택된 버퍼에 있는 셀들의 헤더를 고객 자신만의 헤더로 겹쳐 쓸(overwrite) 수 있도록 한다. 또한 버퍼 내에서 발견된 VPI.VCI 상에 버퍼를 전송할 것인지, 또는 단지 고객이 선택한 VPI.VCI 상에만 전송할 것인지를 선택할 수 있다.
- Address 탭 (Gigabit Ethernet only)에서는 전송되는 패킷 내에 있는 출발 주소와 도착 주소를 Address Book 에서 고정된 6 바이트, 임의로, 순차적인 데이터, 또는 선택적인 한 주소로 바꿀 수 있다.
- Gigabit 탭 (Gigabit Ethernet only)에서는 생성되는 프레임에 몇 바이트의 preamble 이 포함되어 있는가와 자동 CRC 수정이 사용되는가를 지정할 수 있다.

전송하고자 하는 파일이나 버퍼를 선택할 수 있도록 하는 동일한 정보가 세 가지 탭의 각 하단에 보인다.

- 저장된 ATM 트레이스(trace) 파일을 전송하려 한다면, File 옵션을 선택한다. 전송되는 트레이스 파일의 내용을 살펴볼 수 있는 통상적인 Browse 대화 상자를 디스플레이 하려면 Browse 버튼을 클릭한다.
- 현제 열려 있는 캡처 버퍼를 전송하려 한다면, Buffer 옵션을 선택한다. 드롭 다운 목록은 현제 열려있는 모든 버퍼들과 트레이스 파일들을 포함하고 있다.

*그림 9-4*는 ATM 어댑터에 대한 Buffer Setup 대화 상자를 보여준다.



Buffer Setup

Setup

General | Rate | ATM

☐ Overwrite GFC,PTI,CLP GFC: 0000 PTI: 000 CLP: 0 ○ Hex ○ Dec ● Bin

☐ Overwrite Vp,Vc

PVC VPI: 0 VCI: 33 ○ Hex ● Dec Cnx ☐ Use list List...

Traffic Shaping

☑ PCR PCR (%): 100

☑ SCR,MBS SCR (%): 100 MBS: 255

● File: rNT\Program\Atmdemo.atc Browse

○ Buffer:

선택된 버퍼에 있는 셀의 헤더를 고객 자신의 헤더로 겹쳐 쓰고자 한다면 이 필드를 사용.

버퍼 내에서 이미 발견된 VPI.VCI에 버퍼의 내용을 전달할 것인지, 고객 자신이 선택한 VPI.VCI로만 전송할 것인지를 선택.
만일 버퍼 내에서 발견된 VPI.VCI를 겹쳐 쓰도록 선택한다면, 지정된 한개의 VPI.VCI에 전송을 하거나 전송을 위해 15개 이상의 VPI.VCI를 생성할 수 있음.

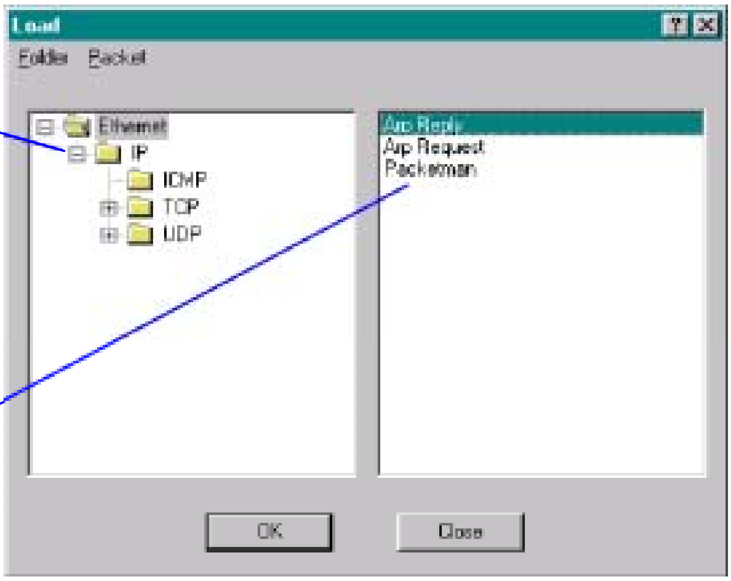
전송하려는 파일 또는 버퍼 선택

그림 9-4. 현재 버퍼에 있는 내용을 전송하기 (ATM 패킷 생성기)

Packet Library 사용

Packet Library 는 사용자가 저장한 패킷들을 분류하여 정리하는 방법을 제공한다. Packet Setup 대화 상자의 Packet 메뉴에서 Load 나 Save 명령을 선택하여 Packet Library 를 연다. 열려진 대화 상자의 구조는 조금 다르겠지만, 저장된 패킷들의 라이브러리를 액세스할 수 있다.

Packet Library 는 MS-Windows Explorer 와 유사한 방법으로 동작한다. 즉, 왼쪽 창에는 폴더의 계층 적인 구조가 보이고 오른쪽 창에서는 왼쪽 창에서 선택한 폴더에 저장되어 있는 패킷들을 보여준다. 기본적으로 Packet Library 는 *그림 9-5* 에서 볼 수 있는 것처럼, 다양한 프로토콜에 대한 집합체로 구성된다.



왼쪽 창은 Packet Library에 있는 폴더들의 계층적인 구조를 제공.

오른쪽 창에는 왼쪽 창에서 선택된 현재 폴더에 포함되어 있는 패킷들을 보여줌.

그림 9-5. Packet Library

아래와 같은 작업을 Packet Library 에서 하기 위해 **Folder** 와 **Packet** 메뉴에 있는 명령어들을 사용한다.

- **Folder** 메뉴에는 **New**, **Rename** 및 **Delete** 명령이 있으며, 각각 Packet Library 의 왼쪽 창에 있는 폴더들을 생성하고, 이름 바꾸기 및 삭제하는 기능이다.
- **Packet** 메뉴에는 **Rename** 및 **Delete** 명령이 있으며, 각각 Packet Library 의 오른쪽 창에 있는 패킷의 이름을 바꾸고 삭제하는 기능이다.

Packet Library 에 Packet 저장

아래와 같은 방법으로 패킷들을 Packet Library 에 저장할 수 있다.

- Packet Setup 대화 상자에 있는 **Packet** 메뉴에서 **Save As** 명령을 실행한다. 이것은 형제 Packet Library 에 로드된 패킷을 저장할 수 있다.
- Sniffer Pro Decode 화면의 Summary 창에 있는 한 프레임을 선택하고 마우스 오른쪽 버튼을 클릭하고 나타나는 메뉴에서 **Add Frame to Pkt. Library** 를 선택한다.

위 두 가지 경우, 그 결과는 동일하다. 대화 상자에서 해당 프레임을 저장할 폴더를 선택하고 저장되는 패킷에 대한 이름을 입력한다.

Packet Library 에서 패킷을 로드

Packet Library 에 패킷을 저장했다면, Packet Setup 대화 상자에 있는 Packet 메뉴에서 Load 명령을 실행하여 언제나 사용할 수 있다. 대화 상자는 *그림 9-5* 에서 보였으며, 로드하려고 하는 패킷을 선택할 수 있다.

Packet Setup 파일과 Buffer Setup 파일 사용하기

ATM/Gigabit 패킷 생성기는 ATM/Gigabit Ethernet 패킷 생성기 대화 상자에 있는 다양한 옵션들을 다르게 정의한 내용을 포함하도록 Packet Setup 파일과 Buffer Setup 파일들을 저장할 수 있게 한다. Packet 과 Buffer Setup 파일들은 새로운 패킷이나 버퍼에 주의 깊게 정의한 설정 내용을 쉽게 적용할 수 있다.

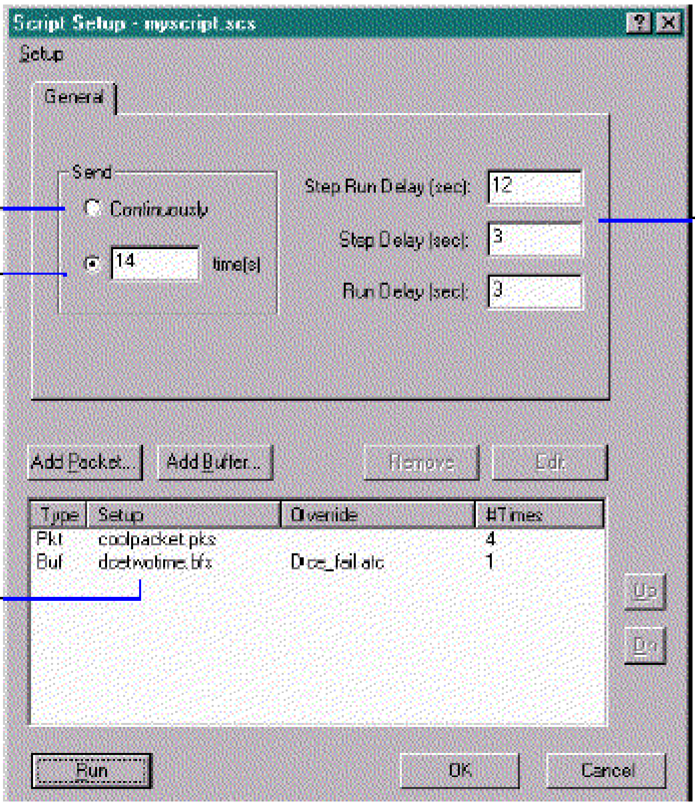
- Packet Setup 파일은 Packet Setup 대화 상자에 있는 **Setup** 메뉴에서 **Save as** 명령을 사용하여 저장한다.
- Buffer Setup 파일은 Buffer Setup 대화 상자에 있는 **Setup** 메뉴에서 **Save as** 명령을 사용하여 저장한다.

트래픽을 생성하기 위한 스크립트 사용하기

ATM/Gigabit 패킷 생성기에는 네트워크 상에 전송하기 위해 저장된 패킷과 버퍼들의 복잡한 조합을 구성할 수 있는 조금 어려운 스크립트 유틸리티가 제공된다. 또한 주어진 패킷과 버퍼에 서로 다른 Packet Setup 파일과 Buffer Setup 파일을 적용하는 다양한 능력을 사용할 수 있다. Packet Generation Script 는 Send Script 대화 상자가 나타나도록 패킷 생성기의 툴바에서 **Send Script** 버튼 을 클릭하여 설정한다.

스크립트는 일련의 스텝들(steps)로 구성한다. 각 스텝은 전송된 패킷이나 전송된 버퍼가 될 수 있다. 패킷 스텝과 버퍼 스텝을 순차적으로 Script Setup 대화 상자 내에 추가하여 스텝들의 목록을 생성한다. 각 스텝은 정해진 횟수만큼 실행하도록 지정할 수 있다. 또한 주어진 한 스텝을 반복하는 시간 지연 **(Step Run Delay)**, 스텝 자신들 사이의 시간 지연 **(Step Delay)**, 각 실행 사이의 시간 지연 **(Run Delay)**. " **실행(run)**" 은 목록에 있는 일련의 전체 스텝들로 구성한다.

*그림 9-6*는 샘플 스크립트에 대한 Script Setup 대화 상자를 보여준다.



Script Setup - myscript.scs

Setup

General

Send

○ Continuously

● 14 time(s)

Step Run Delay (sec):	12
Step Delay (sec):	3
Run Delay (sec):	3

Type	Setup	Override	#Times
Pkt	coolpacket.pks		4
Buf	doetwotime.bfx	Doe_fail.atc	1

스크립트를 계속해서 반복 전송하려면 클릭

스크립트의 전송 횟수 지정.

한 스텝의 반복 간격, 스텝들 자신의 지연 시간, 그리고 전체 스크립트의 실행을 위한 지연 시간을 지정.

이 스크립트 내에 있는 스텝들. 스크립트에 Packet Step을 추가하려면 Add Packet 클릭. 스크립트에 Buffer Step을 추가하려면 Add Buffer 클릭.

그림 9-5. 스크립트 전송하기

스크립트 파일 저장하기

스크립트는 여러 차례 반복해서 사용할 수 있도록 파일로 저장할 수 있다. Script Setup 대화 상자에 있는 Setup 메뉴에서 Save as 를 선택하여 스크립트 파일을 저장한다. 그 다음, 저장된 스크립트 파일은 다시 사용하려 할 때, Script Setup 대화 상자에 있는 Setup 메뉴에서 Open 명령을 클릭하여 열면 된다. 스크립트 파일은 .SCS 확장자로 저장된다.

10. Sniffer Pro 와 함께 Sniffer Reporter Agent 사용하기

Sniffer Reporter Agent 는 Sniffer Pro 어플리케이션에서 수집된 데이터를 기반으로 고객이 조절할 수 있는 다양한 형식의 보고서를 생성하기 위하여 Network Associates 가 제공하는 선택 사항(어플리케이션)이다.

Sniffer Pro 의 **Tools** 메뉴에서 **Reporter** 옵션을 선택하여 Sniffer Pro 내에 Sniffer Reporter Agent 를 설치할 수 있다.

이와 더불어, 만일 Sniffer Reporter Agent 가 Sniffer Pro PC 에 설치되어 있다면, Reporter 아이콘 📊 이 아래와 같은 모니터 어플리케이션의 각 툴바에 나타난다.

- 매트릭스
- 호스트 테이블
- 프로토콜 분포
- 글로벌 통계 자료

해당 모니터 어플리케이션에 의해 수집된 데이터를 기반으로 하는 보고서를 설정하는 대화 상자가 나타나도록 Reporter 아이콘을 클릭할 수 있다.

Sniffer Reporter Agent 의 사용 방법에 대한 더 자세한 정보는 다른 문서나 회사에서 제공하는 온라인 도움말을 참조한다.

11. 네트워크 어댑터들과 어댑터 설정

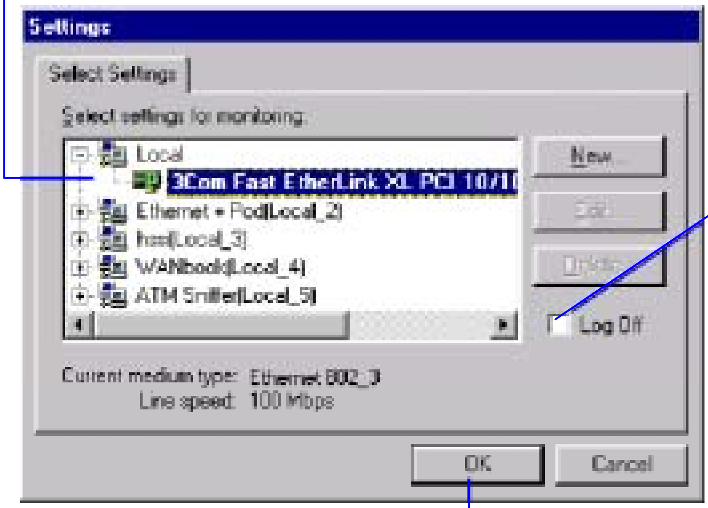
한 개 이상의 NDIS-호환 네트워크 인터페이스 카드가 시스템이 설치되어 있다면, Sniffer Pro 가 어떤 카드를 사용할 것인가를 선택할 수 있다. 또한 **Log On/Log Off** 를 사용하여 선택된 인터페이스 카드가 “ log on” (트래픽 모니터링 기능이 동작하고 데이터를 캡처할 준비가 되어 있는 상태)이나 “ log off” 모드에서 시작하도록 지정할 수 있다.

만일 서로 다른 네트워크 세그먼트가 여러 개의 어댑터에 붙어 있다면, 어떤 세그먼트를 Sniffer Pro 가 한 어댑터에서 다른 어댑터로 스위칭하여 모니터 할 것인가를 선택할 수 있다.

더불어, 여러 개의 Sniffer Pro 인스턴트를 실행하여 각각의 인스턴트가 다른 어댑터를 사용하거나 동일한 어댑터를 사용하도록 설정할 수 있다. 이 방법을 이용하여 여러 개의 세그먼트를 동시에 모니터 할 수 있다.

어댑터를 선택하려면, Files 메뉴에서 **Select Settings** 를 클릭한다. Settings 대화 상자가 나타나며(*그림 11-1*) , 그 대화 상자는 해당 Sniffer Pro PC 를 위하여 정의되었던 로컬 에이전트들이 포함하고 있다. Sniffer Pro 가 모니터하기 위한 대상 네트워크로써 이미 정의된 로컬 에이전트 가운데 하나를 선택할 수 있으며, 또는 모니터에 사용하는 새로운 로컬 에이전트를 정의하기 위하여 **New** 버튼을 클릭할 수 있다.

이 화면에서 네트워크 어댑터 선택



Settings

Select settings for monitoring:

- Local
  - 3Com Fast EtherLink XL PCI 10/1
- Ethernet - Pod(Local_2)
- host(Local_3)
- WANbook(Local_4)
- ATM Sniffer(Local_5)

Current medium type: Ethernet 802_3
Line speed: 100 Mbps

각각의 카드에 대해서 "log off" 또는 "log on"모드를 설정. 이 박스를 체크하여 설정을 바꿀 수 있음.

이 옵션의 이름은 카드에 현재 설정된 내용에 따라 바뀐다. 예를 들어, 여기에서 선택된 카드가 "log on" 모드에서 시작하도록 설정되어 있기 때문에 반대로 Log Off 박스를 체크할 수 있다.

Ok 클릭

그림 11-1. 네트워크 어댑터 선택하기

Sniffer Local Agents 생성하기

Sniffer Pro 의 다중 인스턴트를 실행하려면, 로컬 에이전트(local agents)라고 하는 분리된 내용들을 생성한다. 로컬 에이전트는 각 로컬 에이전트가 주소록, 캡처 필터 설정, 그리고 패킷 디스플레이 옵션과 같은 세션 정보를 소유하고 있는 일련의 설정 내용으로 생각될 수 있다. 각 로컬 에이전트는 독립된 구성 정보를 갖고 있으며, 따라서 한 네트워크에서 다른 네트워크로, 한 세그먼트에서 다른 세그먼트로 이동하여 Sniffer Pro 를 전반적으로 재 구성할 때, 또는 지정된 작업을 위한 옵션을 설정할 때 사용될 수 있다.

팁 --

다양한 네트워크의 장애 분석을 위한 필드 서비스로 이동 가능한 Sniffer Pro 를 사용한다면, 각 클라이언트의 네트워크에 대한 구성 정보를 보관하기 위하여 로컬 에이전트 기능을 사용한다.

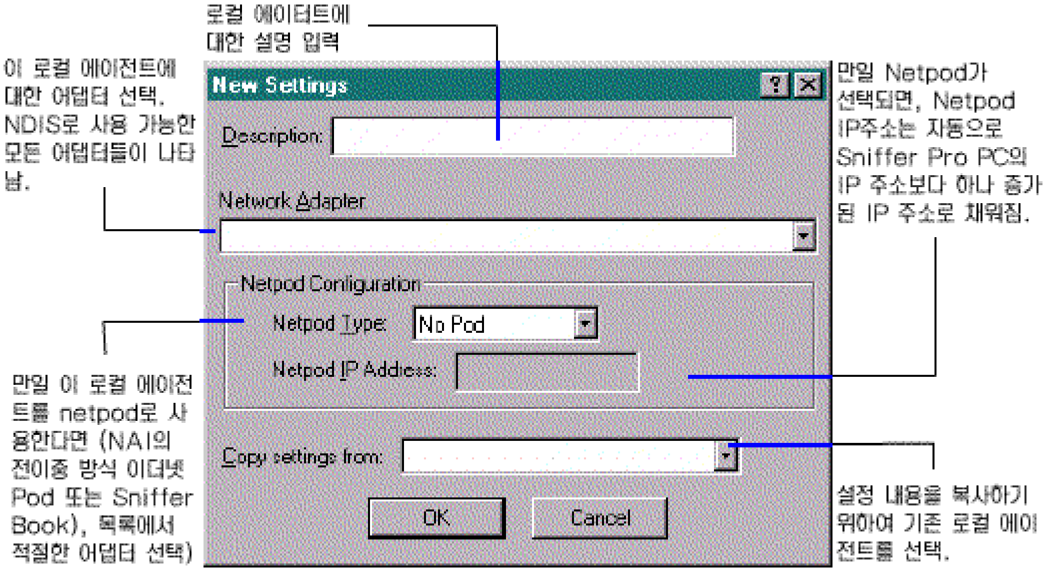
새로운 로컬 에이전트를 생성하려면, File 메뉴에서 Select Settings 를 선택하고 New 버튼을 클릭한다. New Settings 대화 상자는 로컬 에이전트에 대한 네임을 입력하고 당신에게 필요한 재구성 내용의 양을 줄여주기 위하여 기존의 프로브에서 워크 스페이스 설정 내용들을 복사할 수 있도록 해 준다.

중요 정보 --

새로운 로컬 에이전트를 생성할 때, 자동적으로 현재 Sniffer Pro 어플리케이션에 정의된 설정 내용을 사용한다. (주소록, 캡처 필터 설정 내용, 패킷 디스플레이 옵션, 등등)

----

*그림 11-2*는 New Settings 대화 상자를 보여준다.



로컬 에이터트에 대한 설명 입력

이 로컬 에이전트에 대한 어댑터 선택. NDIS로 사용 가능한 모든 어댑터들이 나타남.

만일 이 로컬 에이전트를 netpod로 사용한다면 (NAI의 전이중 방식 이더넷 Pod 또는 Sniffer Book), 목록에서 적절한 어댑터 선택)

만일 Netpod가 선택되면, Netpod IP주소는 자동으로 Sniffer Pro PC의 IP 주소보다 하나 증가된 IP 주소로 채워짐.

설정 내용을 복사하기 위하여 기존 로컬 에이전트를 선택.

New Settings

Description:

Network Adapter

Netpod Configuration

Netpod Type: No Pod

Netpod IP Address:

Copy settings from:

그림 11-2. Local Agent 생성하기

부록 1: Sniffer Pro 의 스위치 분석 기능

Sniffer Pro 는 Cisco Catalyst 스위치들이 제공하는 port mirroring 기능을 손쉽게 사용할 수 있는 기능을 제공한다. Cisco Catalyst 스위치들은 이러한 port mirroring 기술을 SPAN(Switched Port ANalyzer)이라고 한다. SPAN 은 감시와 분석을 위하여 하나 또는 여러 개의 포트에서 지정된 SPAN 포트로 네트워크 트래픽을 복사할 수 있도록 하는 기능이다. 이번 버전에서는 Sniffer Pro 인터페이스로 Cisco 스위치를 구성할 수 있으며, Sniffer Pro 를 사용하여 다음과 같은 작업을 할 수 있다.

- 네트워크 상에 있는 스위치에 연결하고 해당 스위치의 MIB 에 저장된 자세한 통계자료를 자동으로 읽어오기.
  - 이 통계자료는 Sniffer Pro 의 Switch Statistics 화면에 보고된다.
- 스위치 상에 SPAN 포트 설정하기
- 어떤 포트 또는 VLAN 이 해당 SPAN 포트로 미러링(mirroring)되는 가를 지정하기.
  - 이번 버전에서는 단지 한번에 한 개의 포트나 VLAN 을 미러(mirror)할 수 있다.
- 지정된 포트 또는 VLAN 상에서 데이터를 캡처하고 스위치에 대한 전문 분석(Expert analysis) 내용 보기
- 통계 자료나 인터페이스 그룹 내부의 RMON 자료를 기반으로 하는 새로운 알람들을 위하여 스위치에 임계 값을 설정하기.
  - 이러한 알람들은 스위치에서부터 Sniffer Pro 로 보고되어 Alarm log 에 기록된다.
- Sniffer Pro 가 자동으로 SPAN 을 설정할 수 있도록 트리거를 가동하고 알람 보고를 위하여 한 스위치 포트에서 캡처 시작하기.

지원되는 스위치들

Sniffer Pro 에서는 아래와 같은 종류의 Cisco Catalyst 스위치에 대한 미러링 기능과 전문 분석 기능을 제공한다.

Cisco Catalyst 2900	Version 4.5(2)*
Cisco Catalyst 2926	Version 4.5(2)*
Cisco 2900XL series including:	
2916xl and other 4 MB models	Version 11.2(8)SA5 *
2924(M)XL	Version 12.0(5.1)XP *
Cisco Catalyst 4003	Version 4.5(8)*,5.5(1)*,6.1(3)*
Cisco Catalyst 4006	

Cisco Catalyst 5000 series including:	Version 4.5(2)*
WS-C5000	
WS-C5002	
WS-C5500	
WS-C5505	
WS-C5509	
Cisco Catalyst 6000 series including:	Version 5.4(1)*
WS-C6000	
WS-C6002	
WS-C6500	
WS-C6509	
Nortel Baystack 450	Versions: HW:RevB FW:V1.04 SW:V1.0.1.0*

스위치 분석의 개념

스위치로 구성된 네트워크는 네트워크 분석과 관리면에서 특유한 문제점들을 내포하고 있다. 전통적인 매체-공유 네트워크에서는 한 스테이션이 패킷을 전송하고자 할 때, LAN 상에 있는 모든 스테이션이 해당 패킷을 ‘ 관측’ 하게 되며, 그 패킷을 관찰하여 만일 자신에게로 주소가 지정되어 있다면 주소가 지정된 그 스테이션만이 해당 패킷을 자신의 버퍼로 복사하게 된다. 이 경우에는 네트워크 분석이 간단하여 Sniffer Pro 는 선로 상에서 보여지는 각 프레임을 분석할 수 있으며, 네트워크 상의 모든 패킷 교환을 이해하고 해석할 수 있다.

이와는 반대로, 한 스테이션이 스위치로 구성된 네트워크를 경유하여 패킷을 전송하고자 할 때, 해당 스위치는 이 패킷을 요구하는 장비는 어느것인가와 단지 그 스테이션만이 해당 패킷을 수신하기 위하여 어느 곳으로 패킷을 보내야 하는가를 결정한다. 스위치에 있는 각 포트는 단지 이 포트에 연결된 장비를 위하여 패킷을 복제하게 된다. (단, 브로드캐스트와 멀티캐스트는 모든 장비로 목적지가 지정됨) 이러한 동작은 트래픽을 분할하는 효과가 있으며, Sniffer Pro 가 네트워크에 존재하는 모든 트래픽을 완벽하게 관측하기 어렵도록 한다.

스위치 분석을 위한 설치

Sniffer Pro 를 이용하여 스위치로 구성된 환경을 분석하기 위해서는 두개의 네트워크 인터페이스 카드가 필요하다 – 구성 카드(configuration card)와 모니터 카드(monitor card). 다음 그림은 구성 카드와 모니터 카드를 이용하여 Sniffer Pro 를 네트워크 및 스위치에 연결하는 방법을 보여주고 있다.

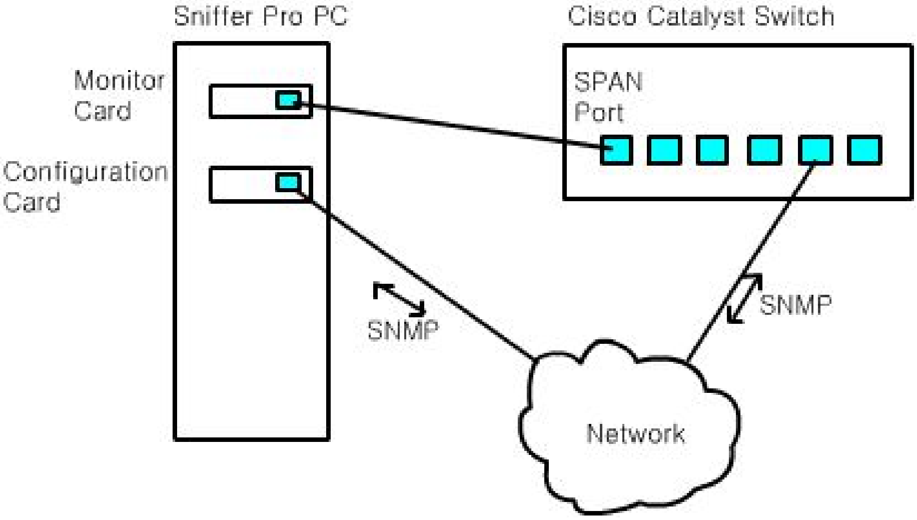


그림 1. 스위치 분석을 위한 Sniffer Pro 의 설치

- Sniffer Pro 는 SNMP 를 사용하여 스위치와 대화하기 위하여 구성 카드를 사용한다. 구성 카드는 반드시 자신의 IP 를 이용하여 해당 스위치를 경유할 수 있는 한 네트워크에 연결되어야 한다.
  - Sniffer Pro 는 구성 카드를 통하여 다양한 구성 명령(configuration command)과 SNMP 요청을 스위치에게 송신한다. 전송되는 내용에는 스위치의 SPAN 포트를 설정하는 명령어뿐만 아니라 스위치의 MIB 에 저장되어 있는 정보(예를 들어, 스위치의 이름, 스위치 상에 있는 포트들에 대한 다양한 통계 자료, 스위치에 있는 소프트웨어와 하드웨어에 대한 정보 등)에 대한 SNMP GET request 가 포함되어 있다.
  - 구성 카드는 또한 Sniffer Pro 의 GET request 에 대한 스위치의 응답을 수신하기 위하여 사용된다. 이러한 응답들은 스위치의 MIB 에 저장된 보고 데이터들이다. Sniffer Pro 의 Switch Statistics 어플리케이션은 이러한 데이터를 시각적으로 보여준다.
- 모니터 카드는 스위치의 SPAN 포트에 직접 연결된다. 이것은 스위치에 의해서 해당 SPAN 포트로 입력되는 모든 트래픽을 캡처 한다. 이번 버전에서 Sniffer Pro 는 한 포트 또는 VLAN 에 있는 모든 포트에 입력되는 트래픽을 캡처 할 수 있다.

인터페이스 카드들의 설치 및 구성

‘ 스위치 분석을 위한 설치’ 에서 보았듯이 전문적인 스위치 분석을 사용하기 위해서는 두개의 이더넷 카드가 필요하다. 하나는 스위치를 구성하기 위하여 또 하나는 스위치에서 트래픽을 캡처 하기 위하여 사용된다. 두개의 이더넷 카드가 설치되면, 스위치에게 SNMP 명령어를 전송하기 위하여 올바른 카드(구성 카드)가 사용되고 있는지를 확인하기위한 방법이 필요하게 된다. 이것은 아래와 같이 각 카드에 어떤 프로토콜을 ‘ bound’ 하는 가에 따라서 구분될 수 있다.

- 구성 카드는 네트워크 상에서 SNMP 를 이용하여 스위치와 통신한다. 이러한 이유로 구성 카드고 사용하고자 하는 카드에는 반드시 TCP/IP 스택이 설치(bound)되어 있어야 한다.
- 모니터 카드는 스위치에 있는 SPAN 포트에 직접 연결되어 있다. SNMP 명령어가 모니터 카드로 송신되지 않도록 하려면, 모니터 카드에 TCP/IP 스택이 설치되어 있지 않아야 한다.
  - 윈도우 95/98 환경에서는 모니터 카드가 동작하기 위해서는 제외한 몇 가지 프로토콜이 설치되어 있어야 한다. 따라서 윈도우 95/98 환경에서 TCP/IP 를 제외한 프로토콜(예를 들어, IPX/SPX)이 모니터 카드에 대해서 설치되어 있는 가를 확인한다.
  - 윈도우 NT 환경에서는 모니터 카드에 더미(dummy) 프로토콜을 설치할 필요가 없다. 그냥 두어도 Sniffer 드라이버가 스스로 모니터 카드에 설치된다.

주: 한 스위치 포트가 SPAN 포트로 지정되면, 해당 포트는 자동적으로 트렁크 포트가 되어 자신이 구성원으로 속해있던 임의의 VLAN 에서 제외된다. 즉, 이 포트를 통한 연결이 상실된다. 따라서 만일 스위치 제어 명령을 모니터 카드를 통하여 SPAN 포트에 잘못 전달하게 되면, 해당 포트는 동작하지 않게 될 것이다. (즉, 해당 스위치와의 연결이 이루어지지 않을 것이다.) 만일 스위치 제어 명령이 잘못된 카드를 통하여 전달되고 있음을 발견했다면, 해당 바인딩(binding)을 되돌리기 보다는 케이블을 교체하는 간단한 방법이 있다. (SNMP 명령어를 전송하는 카드를 SPAN 포트보다는 네트워크에 연결하거나 그 반대로 한다.)

이 작업을 하는 방법

Sniffer Pro 내부에 있는 두개의 이더넷 카드 가운데 오직 하나만 TCP/IP 스택을 가지고 있기 때문에 모든 SNMP 명령어들은 이 카드를 통하여 자동적으로 전송될 것이다. TCP/IP 스택이 설치된 카드가 스위치 상에 있는 SPAN 포트가 아닌 네트워크에 연결되어 있는지 확인해 보자.

카드 구성하기 – 순서

두개의 이더넷 카드를 설치하고 구성하기 위해서 아래 과정을 따라 해보자.

1. Sniffer Pro 가 설치되어 있는 PC 에 두개의 이더넷 카드를 설치하자.
2. 어느 네트워크 인터페이스 카드를 구성 카드로 사용할 것인가를 결정하자. 선택된 카드에 TCP/IP 스택이 설치되어 있는가와 프로토콜 바인딩 상태를 확인하자.
3. IP 주소를 이용하여 모니터 될 수 있는 스위치에 접속할 수 있는 네트워크에 구성 카드

를 연결하자.

4. 두 번째 네트워크 인터페이스 카드는 모니터 카드로 사용된다. 이 카드에 TCP/IP 스택이 설치되어 있지 않은가와 바인딩 상태를 확인하자.
5. 스위치에 있는 어느 포트를 SPAN 포트로 사용할 것인가를 결정하자. SPAN 포트의 모듈 번호와 포트 번호를 기록하자. 나중에 Sniffer Pro 의 스위치 목록에 해당 스위치를 추가할 경우에 이러한 정보가 필요하다. Sniffer Pro 의 모니터 카드를 SPAN 포트에 연결하자.

특정 스위치를 Sniffer Pro 의 목록에 추가하기

인터페이스 카드가 연결되고 구성이 완료되면, 해당 스위치를 Sniffer Pro 의 스위치 목록에 추가하고 그 스위치의 SPAN 포트를 설정하기 위하여 Monitor 메뉴에 있는 Switch 항목을 사용할 준비가 된 것이다. Sniffer Pro 의 Monitor 메뉴에서 Switch 항목을 선택하면, 아래와 같은 대화 상자가 나타난다.

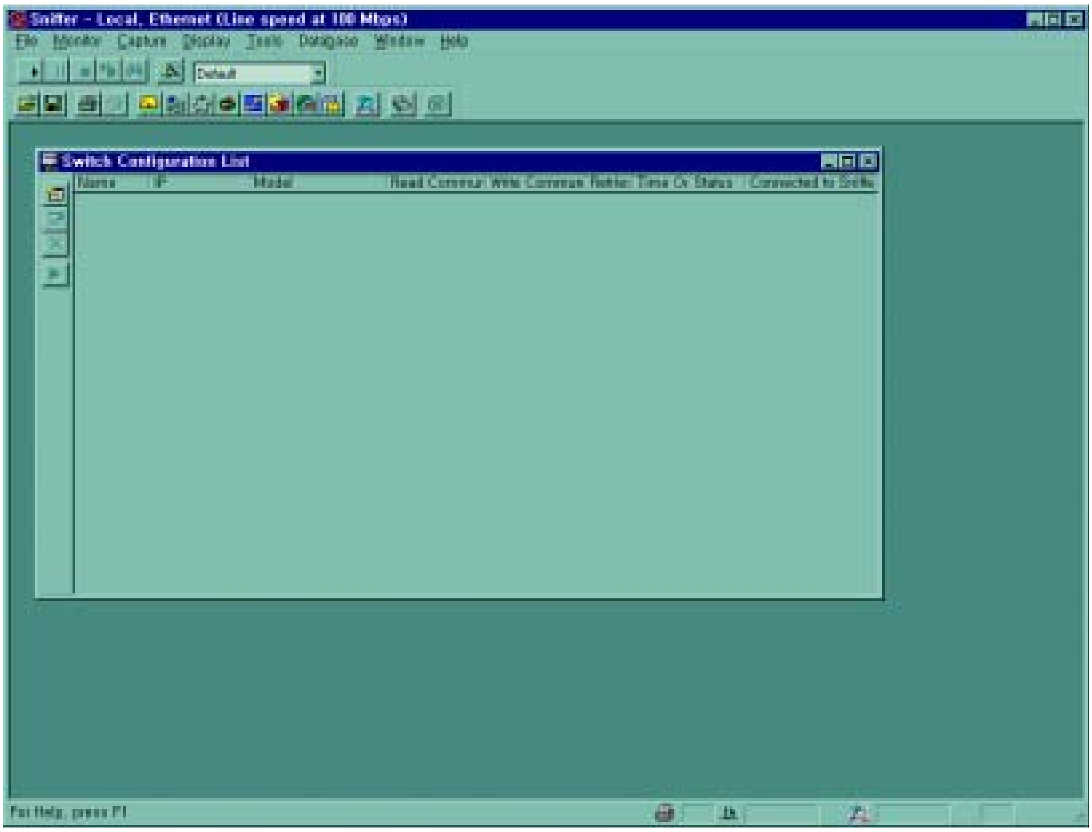
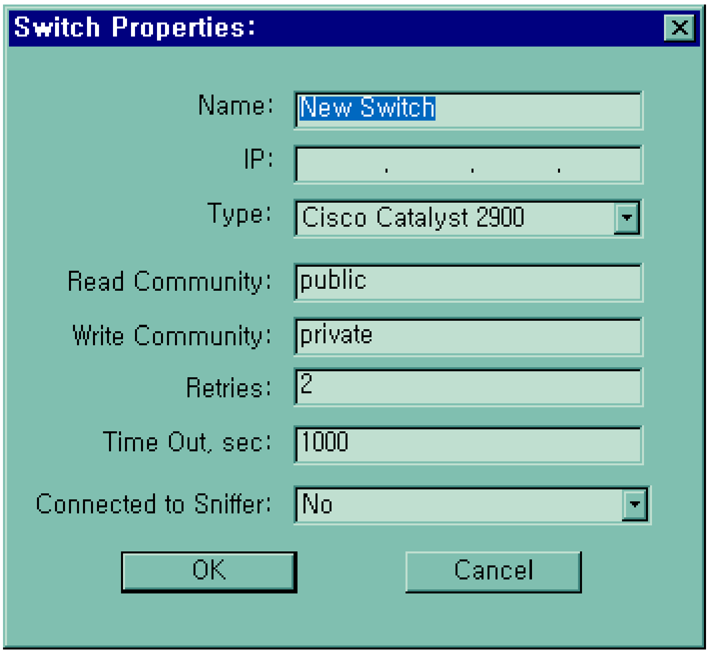

Sniffer - Local, Ethernet (Line speed at 100 Mbps)
File Monitor Capture Display Tools Database Window Help
Default
Switch Configuration List
Name IP Model Read Commun Write Commun Refresh Time Or Status Connected to Sniffe
For Help, press F1

그림 2. Switch Configuration List 대화 상자

위의 그림에서 보는 바와 같이 Switch Configuration List 대화 상자는 초기에 단지 비어

있는 상태이다. 이 대화 상자는 이제 Sniffer Pro 의 스위치 목록에서 특정 스위치들을 추가, 삭제하기 위하여 사용한다. 스위치들을 목록에 추가하게 되면, 각 스위치들이 이 곳에 목록으로 나타난다.

Sniffer Pro 의 목록에 새로운 스위치를 추가하려면 이 대화 상자에서 좌측 상단의 아이콘, 즉 New Entry 버튼을 클릭한다. 그러면 아래 그림과 같은 Switch Properties 대화 상자가 나타난다.


Switch Properties:

Name: New Switch
IP: . . .
Type: Cisco Catalyst 2900
Read Community: public
Write Community: private
Retries: 2
Time Out, sec: 1000
Connected to Sniffer: No

그림 3. Switch Properties 대화 상자

Switch Properties 대화 상자는 목록에 추가되는 스위치를 위하여 동작 파라미터를 설정할 수 있도록 여러 가지 항목을 포함하고 있다. 아래와 같은 옵션을 설정하자.

- Switch Name
  - Sniffer Pro 화면에서 알아볼 수 있는 해당 스위치의 이름을 설정한다. 이 옵션은 단지 Sniffer Pro 의 화면에만 영향을 준다. 즉 이름은 해당 스위치의 어떠한 설정 정보도 변경하지 않는다.
- Switch IP Address
  - Sniffer Pro 가 구성 카드를 통하여 연결하게 되는 해당 스위치의 IP 주소를 지정한다.
- Switch Type
  - 모니터링 하려는 스위치의 종류를 선택한다.
- Read Community
  - 스위치에 있는 RMON MIB 에 대한 Read Community 문자열을 지정한다. Sniffer Pro

가 스위치의 MIB 를 브라우즈 할 수 있도록 이곳에 지정하는 문자열은 스위치에 정의된 Read Community 와 일치해야 한다. Cisco 의 Catalyst 5000 시리즈 제조 과정에서 지정한 이 옵션의 기본값은 ‘ public’ 이다.

- Write Community

  - 스위치에 있는 RMON MIB 에 대한 Write Community 문자열을 지정한다. Sniffer Pro 가 스위치의 구성 내용(SPAN 포트와 관련된 옵션)을 설정할 수 있도록 이곳에 지정하는 문자열은 해당 스위치에 지정된 Write Community 와 일치해야 한다. Cisco 의 Catalyst 5000 시리즈 제조 과정에서 지정한 이 옵션의 기본값은 ‘ private’ 이다.

- Retries

  - Sniffer Pro 가 접속 실패 메시지를 화면에 출력하기 전에 Timeout 에 설정된 시간 간격으로 해당 스위치에 접속을 다시 시도하는 횟수를 지정한다.

  스위치에 접속을 시도할 때(Switch Connection Options 대화 상자에 있는 Test 버튼을 사용하거나 Switch Statistics 어플리케이션을 실행), Sniffer Pro 는 Timeout 에 지정된 시간동안 스위치로부터의 응답을 기다린다. Timeout 값이 경과하면, Sniffer Pro 는 Retries 에 지정된 횟수만큼 다시 연결을 시도하게 된다. 그 이후에도 스위치로부터의 응답이 없다면, 접속 실패(failure) 메시지가 보고된다.

- Timeout

  - Sniffer Pro 가 재접속을 시도하기 전에 해당 스위치로부터의 응답을 기다리거나 접속 실패 메시지를 출력하기 전에 대기하는 시간을 지정한다.

- Analysis Module, Analysis Port

  - 스위치에서 SPAN 포트를 지정하기 위해서는 이곳에 지정된 두개의 옵션, 즉 스위치의 모듈(module) 번호와 포트 번호를 지정한다. SPAN 포트는 지정한 포트에 접근하는 모든 데이터가 감시 또는 분석 하기위해서 동시에 전송되는 포트이다. 또한 SPAN 포트를 때로는 모니터(monitor) 포트나 분석(analysis) 포트라고도 한다.

[주 의] --

Analysis Module 과 Analysis Port 옵션은 스위치에서 새로 설정하는 내용이다. 이러한 설정 내용들은 Switch Statistics 윈도에서 처음으로 캡처를 시작하는 경우에 동작할 것이다. SPAN 포트로 설정된 포트는 다른 어플리케이션이 항상 사용하지 않는 점에 주의하자. 사용하고 있던 포트를 SPAN 포트로 지정하면 그 포트는 현재 사용하던 상태를 잃어버리고 해당 포트에 연결된 다른 장비들에게로의 모든 서비스가 중단된다. 만일 어떤 포트를 SPAN 포트로 지정해야 하는지 모르겠다면, 네트워크 관리자에게 문의하라. 또한 Test 버튼을 사용하여 지금까지 설정한 내용들의 상황을 확인해야 한다.

Test 버튼을 이용하여 설정 내용 확인하기

스위치 구성 옵션들을 모두 설정했다면, 설정한 값들을 확인하기 위하여 Test 버튼을 사용할 것을 권장한다. Test 버튼을 클릭하면 다음에 설명할 내용들에 대한 테스트를 수행한다. 만일 이 가운데 어떤 것이라도 실패하면, 설정 정보를 적절히 바꿀 수 있도록 테스트 실패 상황에 대한 에러 메시지를 출력한다.

[주 의] --

Test 버튼을 클릭하는 것은 실제 스위치 구성 내용을 바꾸지 않는다. Sniffer Pro 는 Switch Statistics 어플리케이션을 실행하여 스위치에 직접 연결할 때까지는 해당 스위치의 어떠한 구성 옵션도 바꾸지 않는다.

- 첫번째 과정으로 IP 주소, Read Community 문자열과 Write Community 문자열을 확인한다. Sniffer Pro 는 해당 IP 주소로 접속을 시도하며, 지정된 Community 문자열을 이용하면 MIB 를 브라우징 하거나 기록이 가능한가를 확인한다.
- 첫번째 과정이 통과되면, 그 다음으로 Sniffer Pro 는 지정된 IP 주소를 갖는 장비가 Sniffer Pro 에서 지원하는 Cisco Catalysit 스위치인가 아니면 다른 네트워크 장비인가를 확인한다.
- 두 번째 과정도 통과되면, 다음으로 Sniffer Pro 는 30 초 동안 SPAN 포트로 지정한 포트를 모니터 한다. 만약 트래픽이 검출되면, Sniffer Pro 는 SPAN 포토로 사용하려고 지정한 포트가 이미 다른 목적으로 사용되고 있다는(SPAN 포트로 지정하면 현재 해당 포트에 연결된 사용자들의 연결이 중단된다는) 경고를 출력한다.

[주 의] --

만약 30 초 동안 트래픽이 검출되지 않는다고 해도 SPAN 포트로 지정된 포트가 전혀 사용하지 않는 포트라고는 보장할 수 없다. 스위치에 연결된 장비가 주어진 시간동안 단지 어떠한 트래픽도 발생시키지 않았을 수도 있다.

Test 버튼을 이용하여 해당 스위치와의 통신이 가능한가를 확인했다면, 이제 Switch Statistics 어플리케이션을 실행하여 현재 Switch Connection Settings 대화 상자에서 선택된 스위치에 연결할 준비가 되었다.

부록 2: 데이터 패턴을 이용한 필터 정의

Define Filter 대화 상자 내에 있는 Data Pattern 탭을 클릭하여 데이터 패턴 필터 탭을 화면에 나타나게 한다. 지정된 데이터 패턴 범주에 속하는 패킷들만 캡처 하도록 데이터 패턴 필터를 정의할 수 있다.

데이터 패턴 필터는 한가지 데이터 패턴이나 AND/OR/NOT 의 부울 함수를 이용한 여러 가지의 데이터 패턴을 이용하여 생성할 수 있다. 복잡하게 구성된 필터는 20 개 이상의 부울 함수와 데이터 패턴들을 포함시킬 수 없다.

데이터 패턴은 특별한 비트 시퀀스, 이러한 비트들의 길이, 그리고 패킷 내에서 해당 패턴의 옵셋(offset) 위치 등으로 정의된다. 옵셋 지정에는 완전한 패킷의 시작부분이나 최초 레벨 프로토콜 영역에서 시작하는 두 가지 선택사항이 있다. 최대 데이터 패턴의 길이는 32 옥텟(octet)이다.

패킷에서 프로토콜 영역이 시작하는 옥텟 위치는 매체의 유형(이더넷, 토큰 링)이나 DLC 유형(이더넷 II, 802.2, 802.3 SNAP)에 따라서 다양하게 나타날 수도 있다. IPX 프로토콜이 좋은 예이다. 이 프로토콜은 이더넷 II 유형의 패킷에서는 옵셋 바이트 14 에서 시작하고, 802.2 유형의 패킷에서는 옵셋 바이트 17 에서 시작한다. Sniffer 는 다양한 형태의 DLC 유형을 인식하며 해당 프로토콜 영역을 올바르게 표시할 수 있기 때문에, 옵셋을 계산하기 위하여 시작 위치로써 프로토콜 계층 영역을 사용하면, 다른 네트워크 매체나 다른 DLC 형식에서도 동일한 패턴 필터를 사용하여 프로토콜 패킷들을 캡처 할 수 있다.

데이터 패턴의 정의를 손쉽게 하도록, Sniffer 는 이미 알고 있는 패킷에서 사용자가 선택한 데이터 패턴을 복사하여 사용할 수 있도록 한다. 이러한 작업을 위하여 이전에 캡처 된 파일을 열면 packet decode viewer 가 보이며, 여기에서 Define Filter 를 호출하기 전에 특정 패킷이 선택된다. 디코드 된 패킷에서 알고 있는 데이터 필드를 데이터 패턴 필드로 복사하려면 Data Pattern 탭에서 Add Pattern/Set Data 를 사용한다. 이러한 과정에서 옵셋과 길이가 자동으로 계산되어 데이터 패턴 공간이 채워지며, 필드 이름을 입력할 수 있게 한다.

복잡한 데이터 패턴 필터를 구성하려면 AND/OR/NOT 부울 함수를 사용한다. 구성된 결과는 논리적인 관계를 보여주기 위하여 트리와 같은 형식으로 화면에 표시된다.

부울 함수를 이용하여 데이터 패턴 필터의 구성을 학습하기 위한 가장 좋은 방법은 간단한 데이터 패턴 필터에서 시작하는 것이다. 첫번째 단계는 부울 함수의 논리적인 관계를 작

성하는 것이다. 그 다음에는 괄호를 사용하여 부울 함수의 동작 순서를 지정하는 것이다. 따라서 최종 함수는 트리 형식으로 구성된다.

다음의 예제는 샘플 필터인 My Subnet 을 구성하는 방법을 단계별로 보인 것이다. (My Subnet 은 또한 샘플 부울 함수로 구성된 샘플 데이터 패턴 필터로써 Sniffer 캡처 목록에 추가된다.)

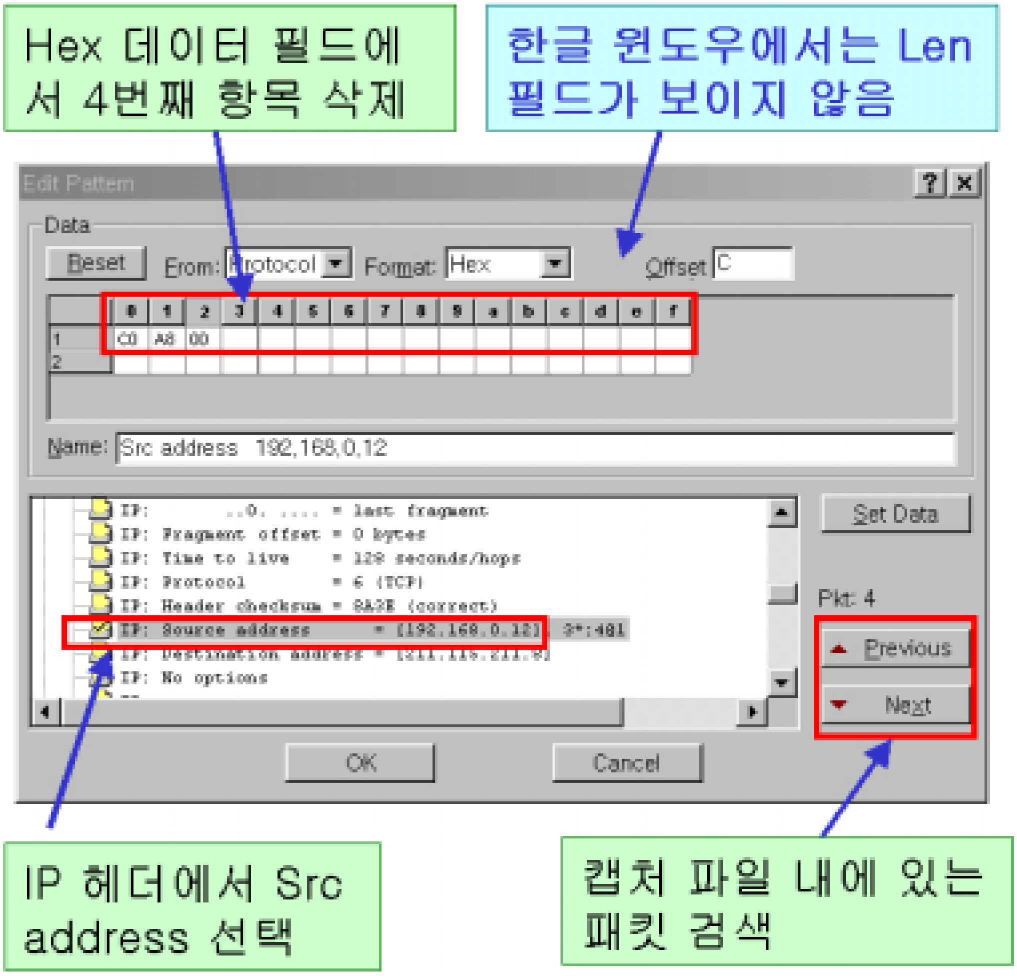
예)서브넷 192.168.0 로 입출력 되는 트래픽을 제외한 모든 IP 트래픽을 캡처 한다고 가정하자.

첫번째 단계는 아래와 같은 동작을 하도록 데이터 패턴의 부울 함수를 작성한다.

Not(Src Subnet 192.168.0 OR Dest Subnet 192.168.0)

만약 이러한 서브넷 주소를 포함하고 있는 패킷이 있다면, 해당 파일을 열고 소스 서브넷 주소 192.168.0 를 포함하고 있는 패킷을 선택한 후, 아래와 같은 단계를 따라서 데이터 패턴 필터를 정의해보자.

1. 필터링하려고는 패턴이 포함되어 있는 캡처 파일을 스니퍼에서 Open 한 후, 메인 툴바에서 Define Filter 아이콘을 클릭한다.
2. Profiles > New 버튼을 클릭하여 새로운 이름을 입력하고 OK 를 클릭한다.
3. Advanced 탭을 클릭한다.
4. Available Protocols 목록 상자에서 IP 를 선택한다. 이것은 동일한 데이터 패턴을 갖는 IP 패킷 이외의 패킷들은 캡처에서 제외시키는 것이다.
5. Data Pattern 탭을 클릭하자. 기본값인 AND 연산자가 화면에 보인다.
6. Add NOT 버튼을 클릭하여 NOT 연산자를 생성한다.
7. 새로 생성된 NOT 항목에서 Add AND/OR 을 클릭하여 NOT 연산자와 연결된 새로운 국부 AND 연산자를 생성한다.
8. Toggle AND/OR 버튼을 클릭하여 AND 를 OR 로 바꾼다.
9. OR 항목에서 Add Pattern 버튼을 클릭하여 Edit Pattern 대화 상자를 호출한다.
10. 상세한 디코드 윈도우를 스크롤 하여 서브넷 192.168.0 를 포함하고 있는 IP source address 로 이동하여 해당 필드를 선택한다.
11. From 목록 상자에서 Protocol 을 선택한다. 이것은 Sniffer 에게 IP 프로토콜 데이터 패킷의 시작 위치에서 IP 주소의 옵셋을 계산하도록 알리는 것이다.
12. Set Data 버튼을 클릭하여 Sniffer 에게 IP address 필드를 채우도록 알린다. Edit Pattern 대화 상자가 아래 *그림 1* 처럼 보일 것이다.



Hex 데이터 필드에서 4번째 항목 삭제

한글 윈도우에서는 Len 필드가 보이지 않음

Edit Pattern

Data

Reset From: Protocol Format: Hex Offset C

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	C0	A8	00													
2																

Name: Src address 192,168,0,12

```
IP:          ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 128 seconds/hops
IP: Protocol        = 6 (TCP)
IP: Header checksum = 8A2E (correct)
IP: Source address      = [192.168.0.12]  3*:481
IP: Destination address = [211.115.211.9]
IP: No options
```

Set Data

Pkt: 4

Previous

Next

OK Cancel

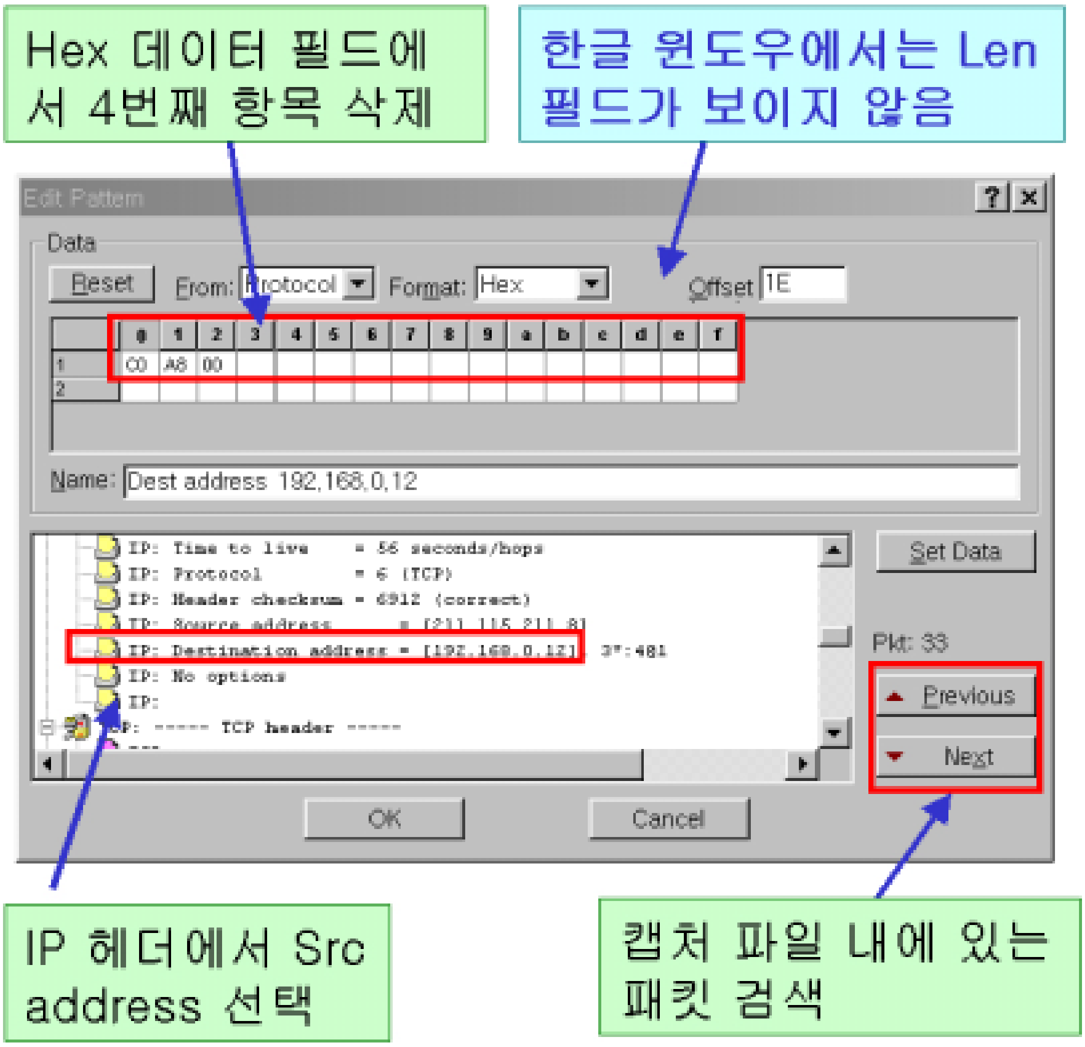
IP 헤더에서 Src address 선택

캡처 파일 내에 있는 패킷 검색

그림 1. Edit Pattern 대화 상자 1

13. Len 필드의 값을 4 에서 3 으로 바꾸고 데이터 패턴 필드에서 4 번째 옥텟을 삭제한다.
 * 주의; 한글 윈도우에 스니퍼를 설치했을 경우에는 Len 필드가 보이지 않는다.
14. Name 필드를 Src Subnet 192.168.0 로 편집한다.
15. OK 를 클릭한다. 새로운 데이터 패턴 Src Subnet 192.168.0 가 생성되었으며, OR 연산자로 연결되었다.
16. OR 연산자를 다시 클릭하여 선택한다.
17. Add Pattern 버튼을 클릭하여 다른 Edit Pattern 대화 상자를 호출한다.
18. Set Data 버튼을 클릭하여 Sniffer 가 Dest Subnet 을 위하여 더미 데이터 패턴을 채우게 하고 OK 를 클릭한다.
19. Define Filter 대화 상자에서 OK 를 다시 클릭하여 필터를 저장한다.
20. Packet Display(Decode 탭 화면)에서 destination IP 서브넷 주소를 포함하고 있는 다음 패킷을 선택한다.
21. 매인 툴바에서 Define Filter 아이콘을 클릭하여 My Subnet 을 위한 대화 상자를 연다.

22. Data Pattern 탭을 클릭하여 이전에 구성된 Data Pattern 필터를 화면에 나타나게 한다.
23. 두 번째 PAT 를 선택하고 Edit Pattern 버튼을 클릭하여 Edit Pattern 대화 상자를 호출한다.
24. 상세한 디코드 윈도우를 스크롤 하여 서브넷 192.168.0 를 포함하고 있는 IP destination address 로 이동하자. 해당 필드를 선택한다.
25. From 목록 상자에서 Protocol 을 선택한다. 이것은 Sniffer 가 IP 프로토콜 데이터 패킷의 시작점에서 목적지 IP 주소의 옵셋을 계산하도록 하는 것이다.
26. Set Data 버튼을 클릭하여 Sniffer 가 IP 주소 필드를 채우도록 한다.
27. Len 필드의 값을 4 에서 3 으로 바꾸고 데이터 패턴 필드에서 4 번째 옥텟을 삭제한다.
28. Name 필드를 Dest Subnet 192.168.0 로 편집한다. Edit Pattern 대화 상자가 *그림 2* 처럼 나타날 것이다.


Hex 데이터 필드에서 4번째 항목 삭제

한글 윈도우에서는 Len 필드가 보이지 않음

Edit Pattern

Data

From: Protocol

Format: Hex

Offset 1E

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	C0	A8	00													
2																

Name: Dest address 192,168,0,12

```
IP: Time to live     = 56 seconds/hops
IP: Protocol         = 6 (TCP)
IP: Header checksum = 6912 (correct)
IP: Source address       = [211.115.211.8]
IP: Destination address = [192.168.0.12]  3":481
IP: No options
IP:
TCP: ----- TCP header -----
```

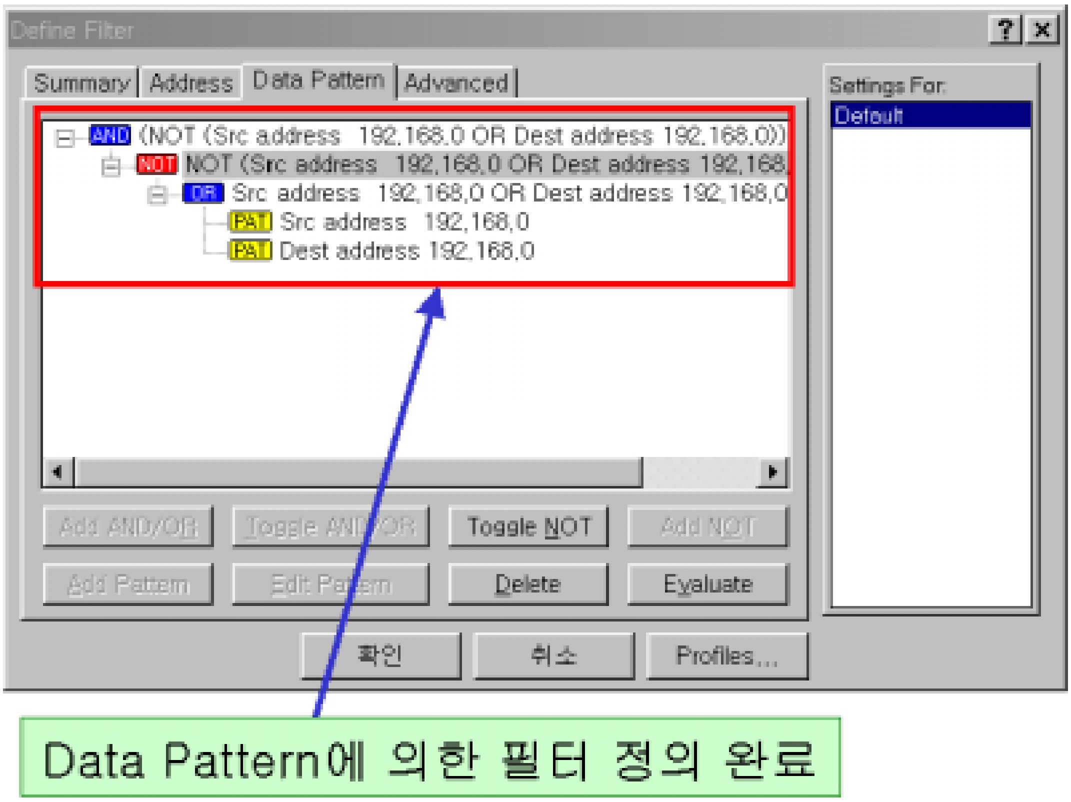
Pkt: 33

IP 헤더에서 Src address 선택

캡처 파일 내에 있는 패킷 검색

그림 2. Edit Pattern 대화 상자 2

29. OK 를 클릭한다. 두 번째 데이터 패턴 Dest Subnet 192.168.0 가 생성되었으며 OR 연산자로 연결되었다.
30. Evaluate 버튼을 클릭한다. 최종 동작 Not(Src Subnet 192.168.0 OR Dest Subnet 192.168.0)이 *그림 3*에서처럼 최상위 부분에 나타날 것이다.



```
AND (NOT (Src address  192.168.0 OR Dest address 192.168.0))
  NOT NOT (Src address  192.168.0 OR Dest address 192.168
    OR Src address  192.168.0 OR Dest address 192.168.0
      PAT Src address  192.168.0
      PAT Dest address 192.168.0
```

Data Pattern에 의한 필터 정의 완료

그림 3. Data Pattern 필터 탭

31. OK 를 클릭하여 필터를 저장한다.