Laura Chappell presents…™

Introduction to Network Analysis

(Part 1 of 2)

An overview of the functions and advantages of troubleshooting and securing networks using network analyzers.

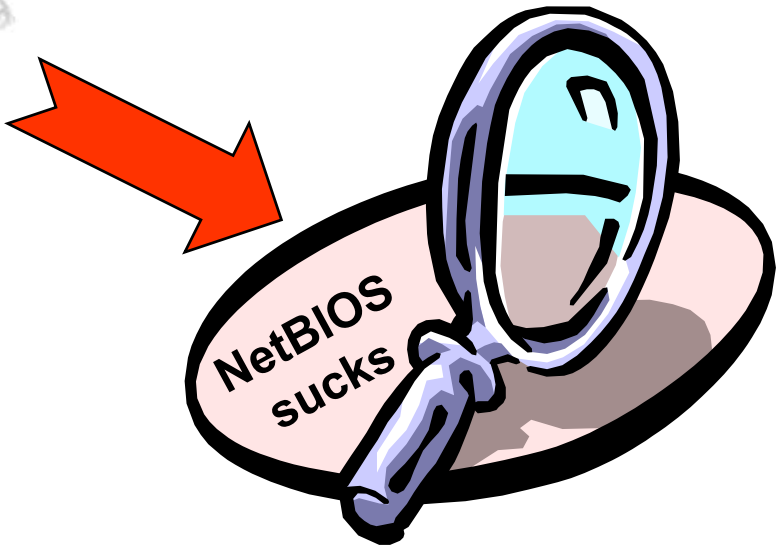
Course Contents

- Analyzer Elements
- Analyzer Placement
- Analyzer GUI
- Trends and Graphs
- Alarms/Alerts
- Trace Buffer
- Reading Traces
- Filters
- Event Logging
- Pattern Analysis
- Packet Generation
- Cyber Crime
- Application Analysis
- Analysis Reporting
- Related Products/Tools
- References/Resources

Why Analyze?

Understand what's going on

Packets don't lie!



What Can You Do With Analysis?

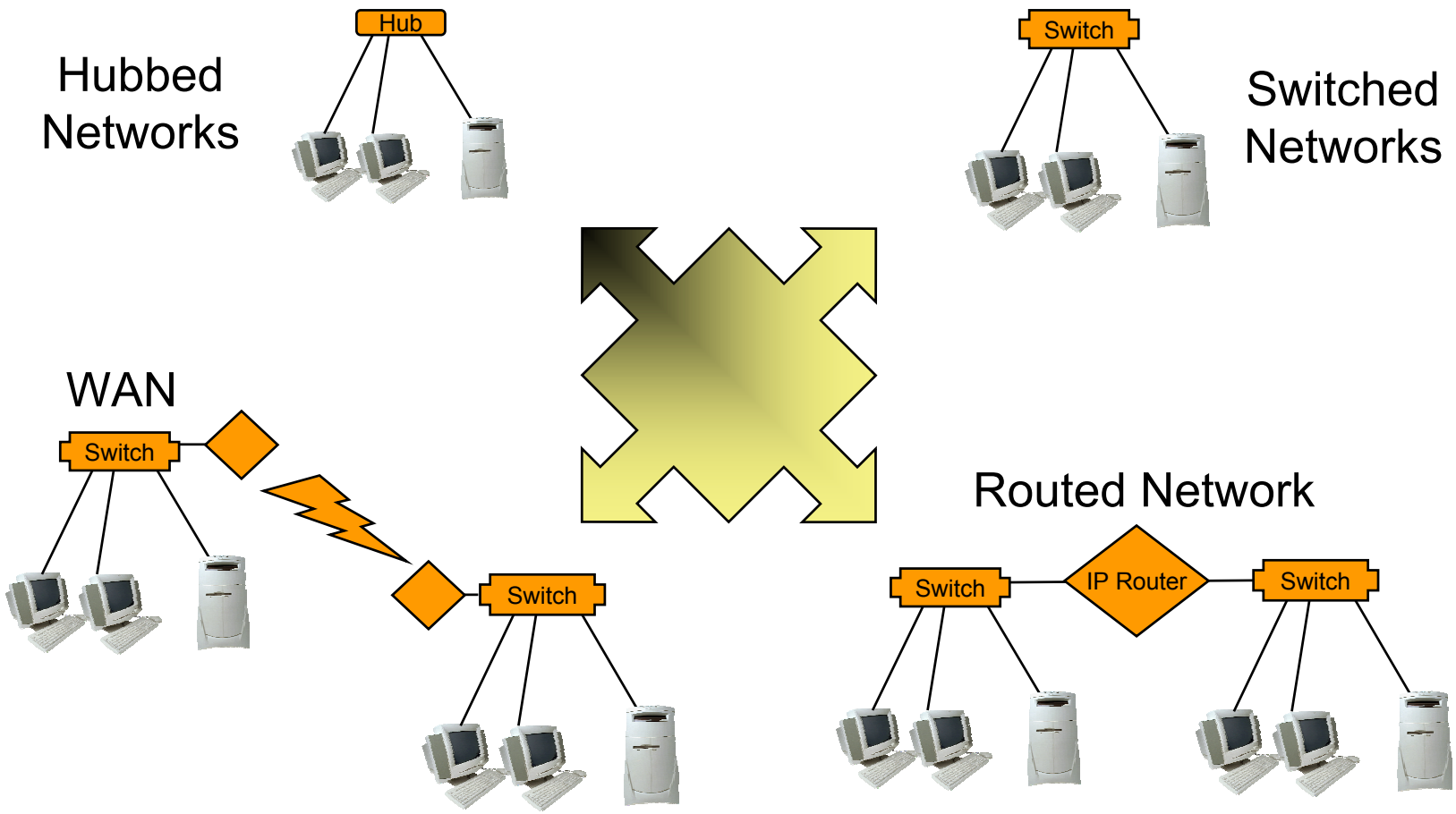
- Learn your network's characteristics
- Know who's using the bandwidth
- Know who's on your network
- Find peak and slow times
- Identify attacks
- Find unsecure applications
- Find 'fat' apps
- Get definitive answers to problems
- Make more money

Reality Check

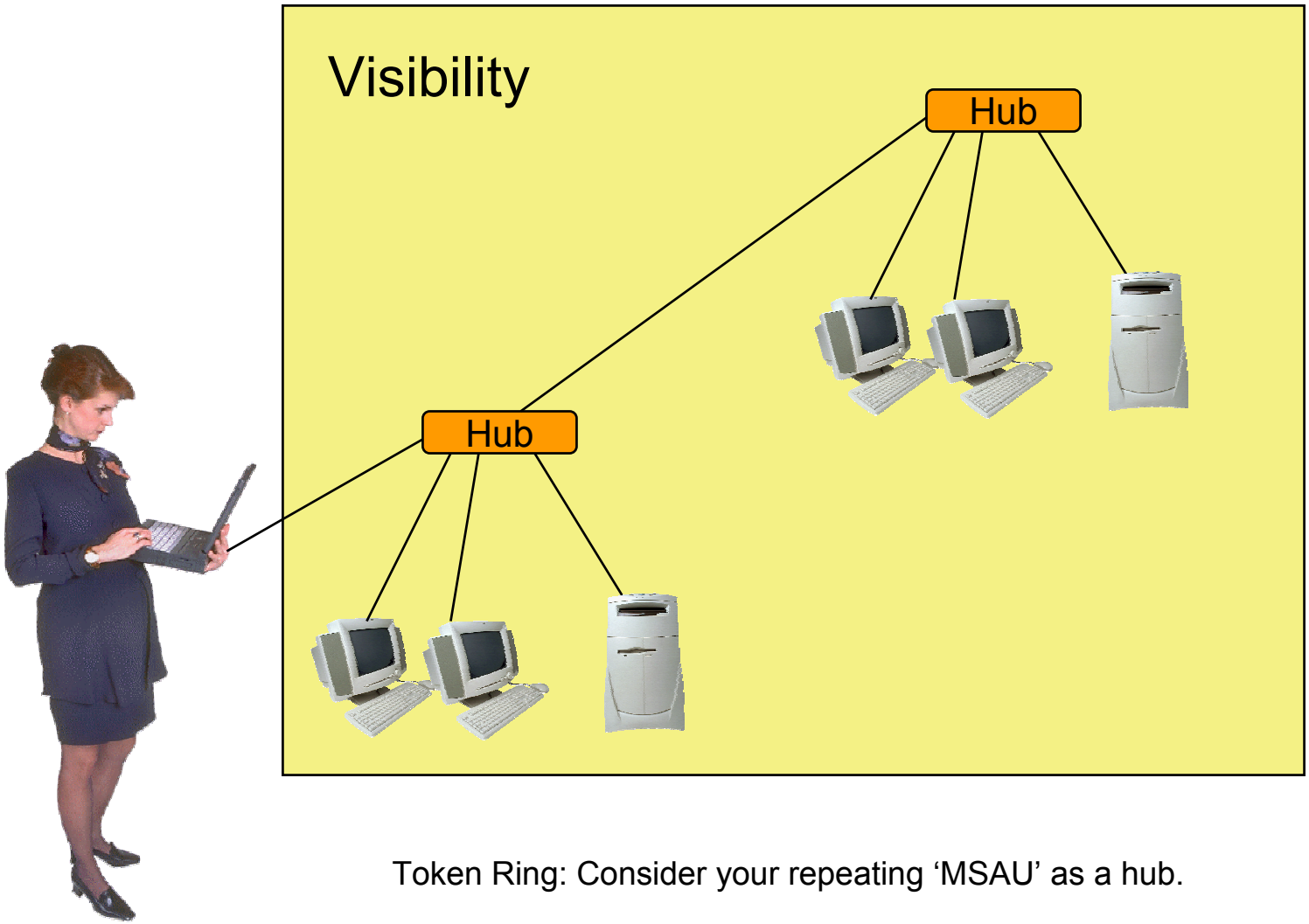
- To analyze well, you must know:
  - basic packet structure
  - basic communications flows
  - analyzer features/functions
  - where your resources are

Data Flows and Analyzer Placement

Data Flow Overview

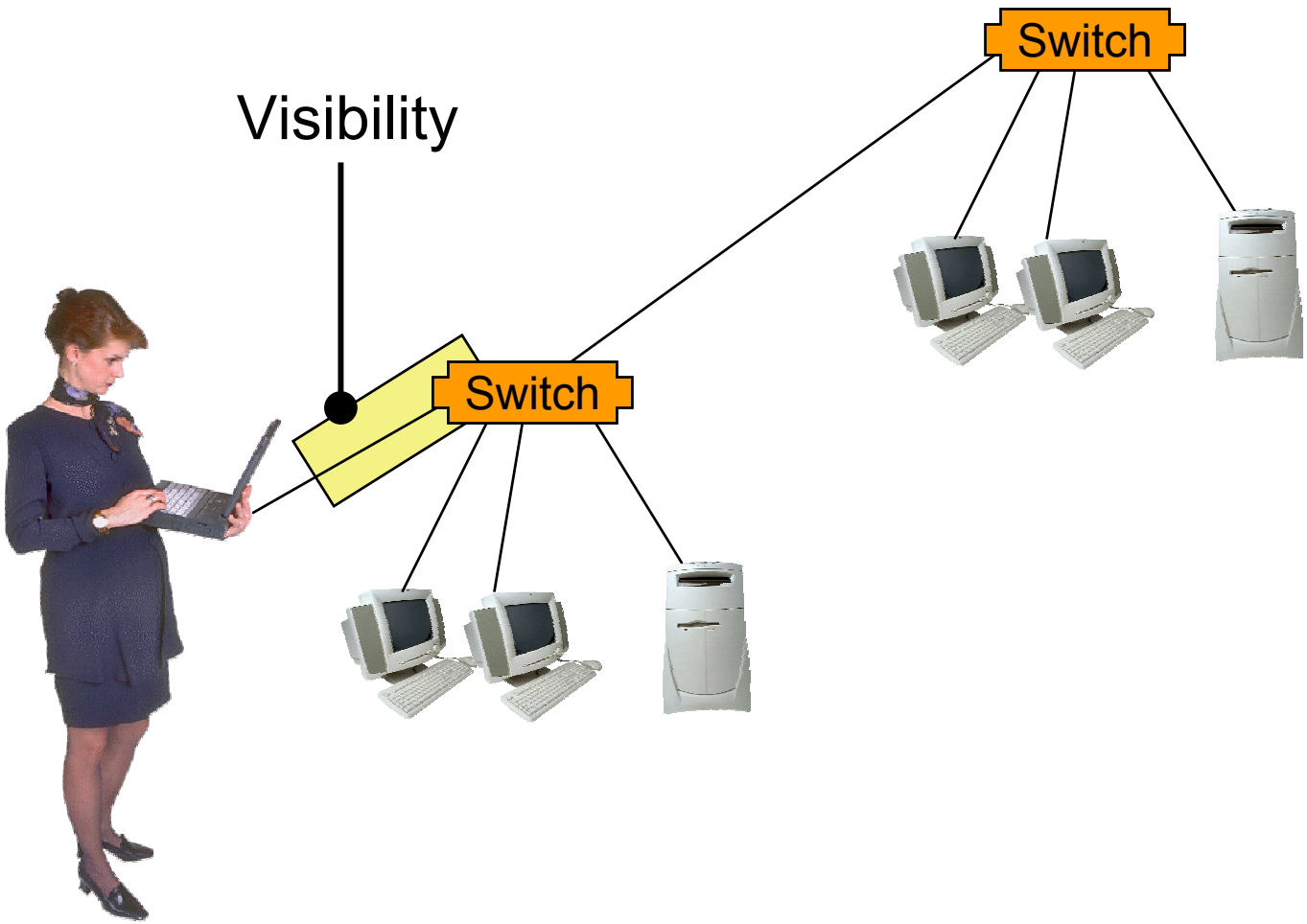


Analyzer Placement: Hubs



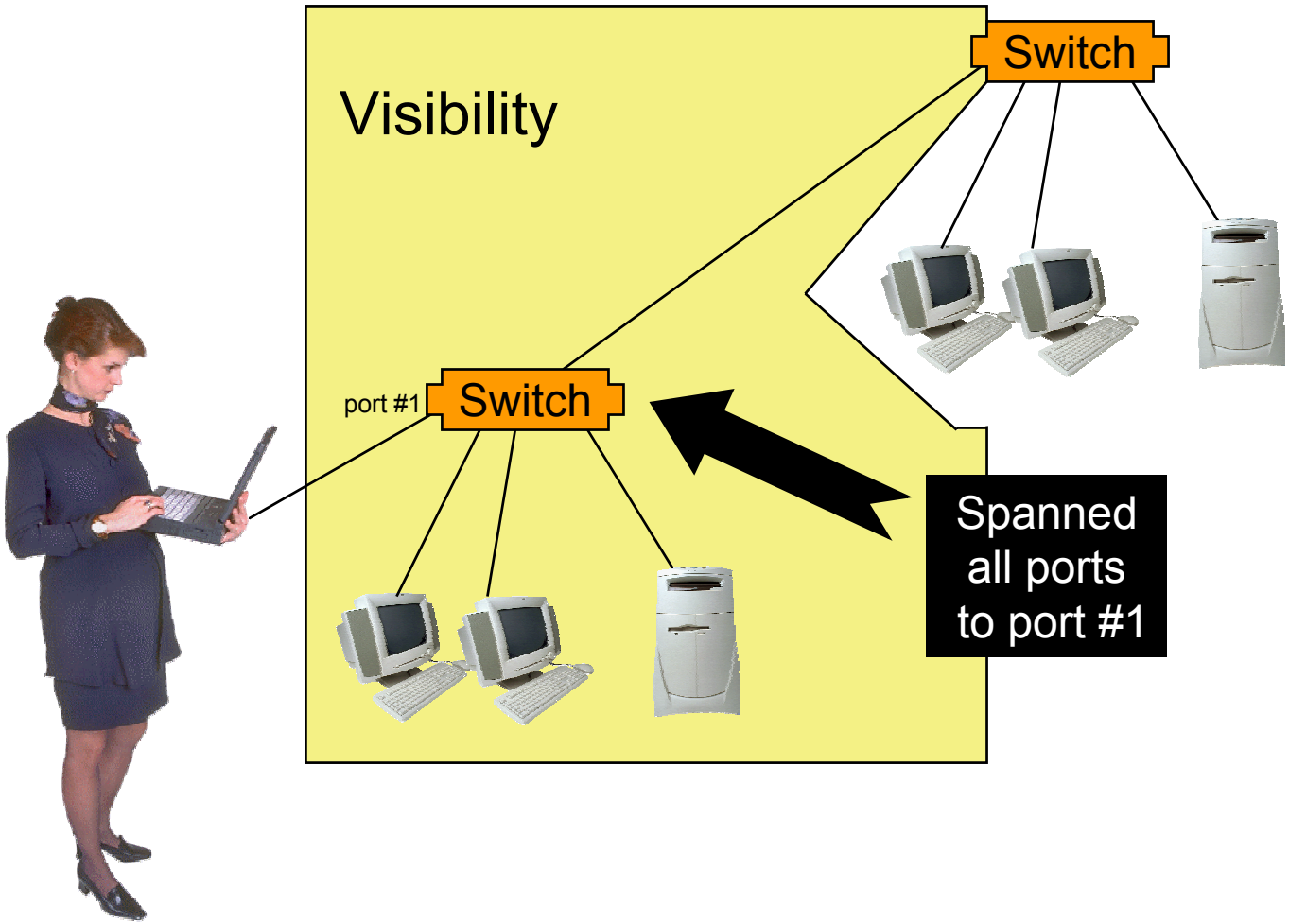
Token Ring: Consider your repeating ‘MSAU’ as a hub.

Analyzer Placement: Switches



Analyzer Placement: Switches

Port Spanning or Mirroring



Port Spanning Examples: Cisco

set span enable

set span disable

set span src_mod/src_port dest_mod/dest_port [rx | tx | both]

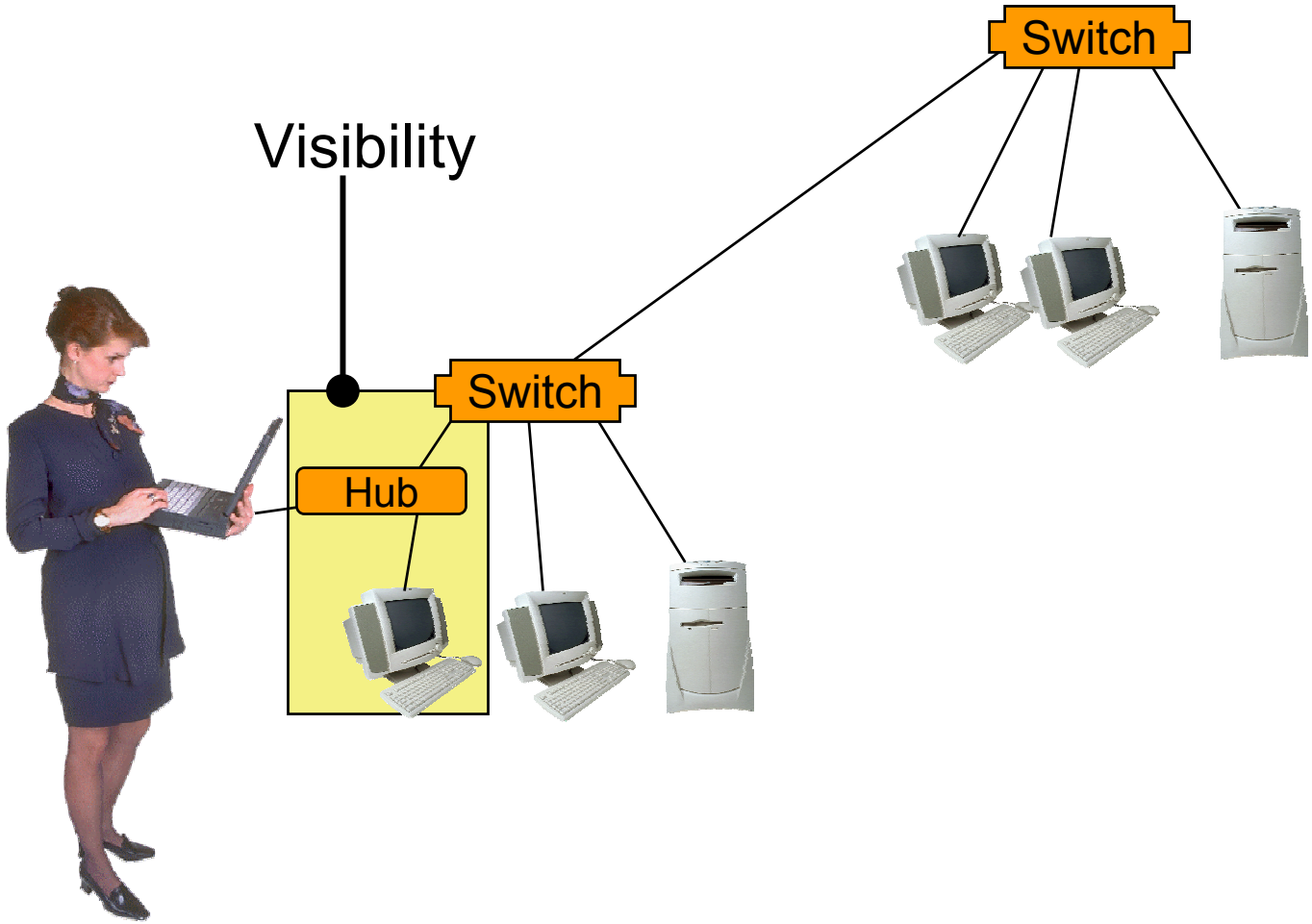
set span src_vlan dest_mod/dest_port [rx | tx | both]

Syntax Description

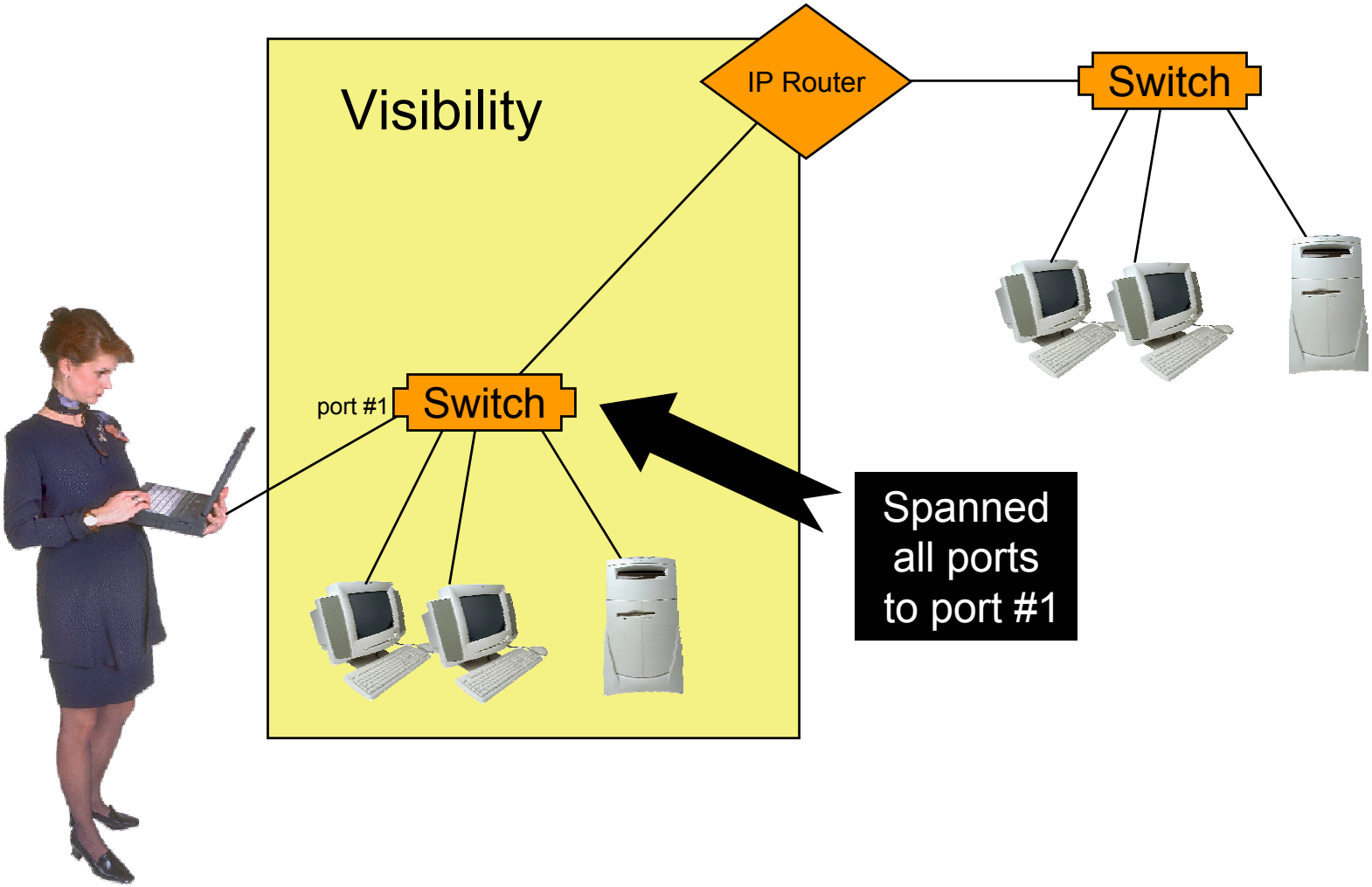
- enable — Port monitoring is enabled.
- disable — Port monitoring is disabled.
- src_mod — The monitored module (source).
- src_port: — The monitored port (source).
- dest_mod — The monitoring module (destination).
- dest_port — The monitoring port (destination).
- src_vlan — The monitored VLAN (source).
- rx — Information received at the destination is monitored.
- tx — Information transmitted from the source is monitored.
- both — Both information that is transmitted from the source and received at the destination is monitored.

Analyzer Placement: Switches

Hubbing Out

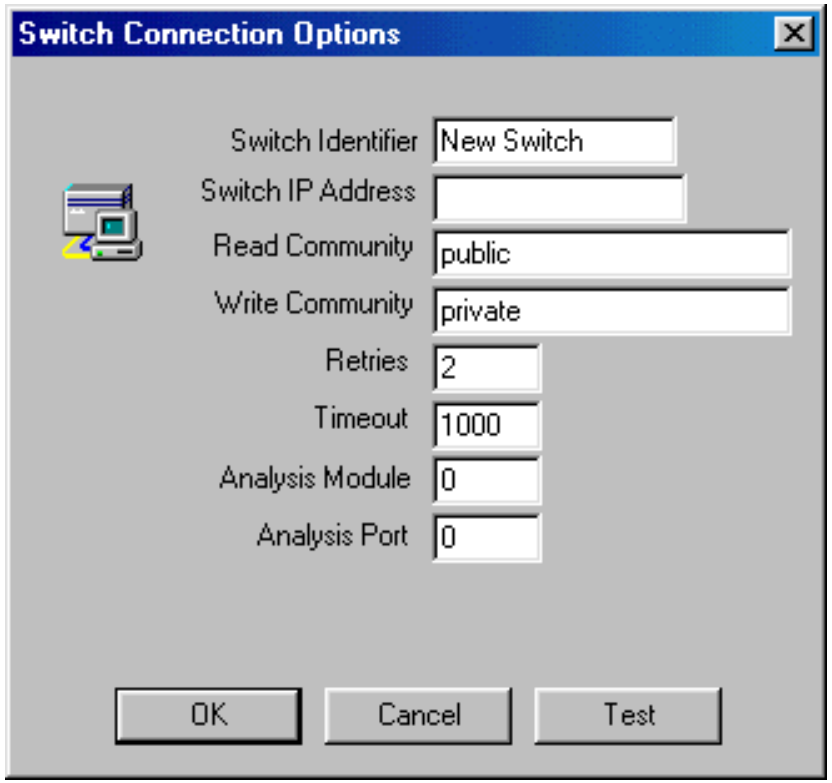


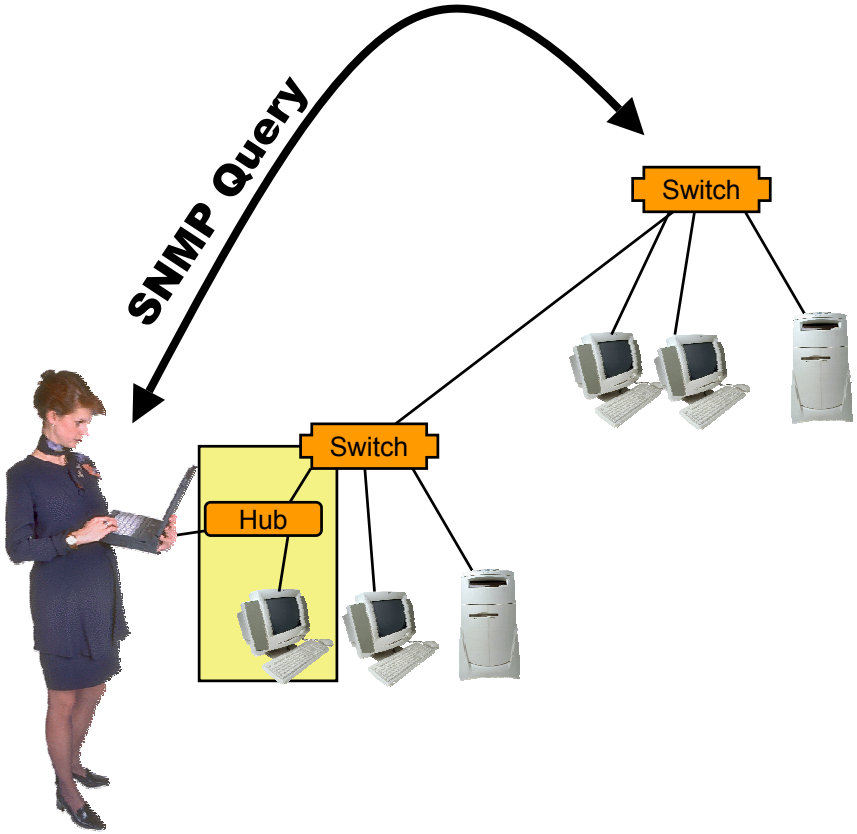
Analyzer Placement: Routers



Switch Statistics

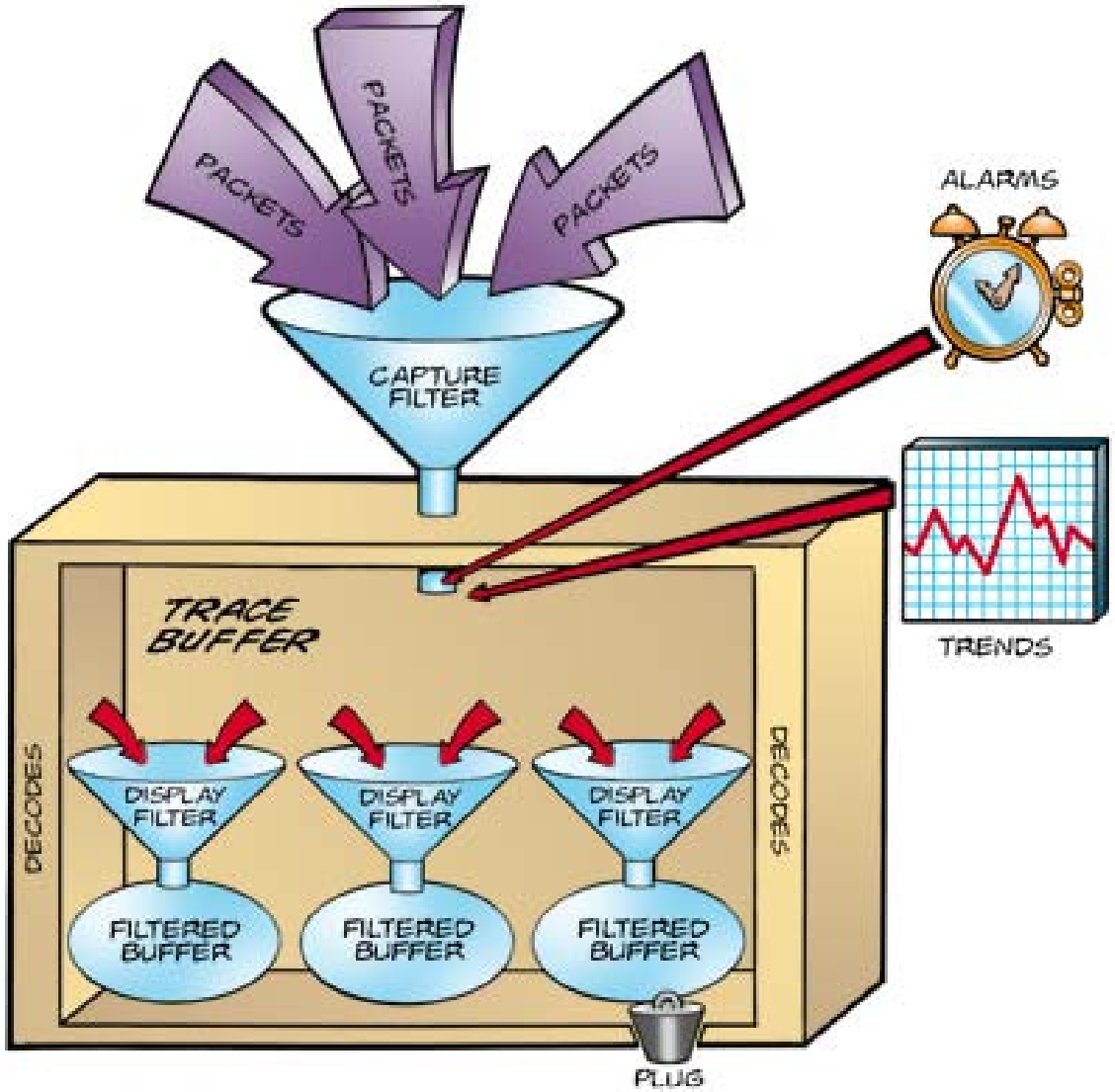
- Some analyzers can perform SNMP queries on switches.





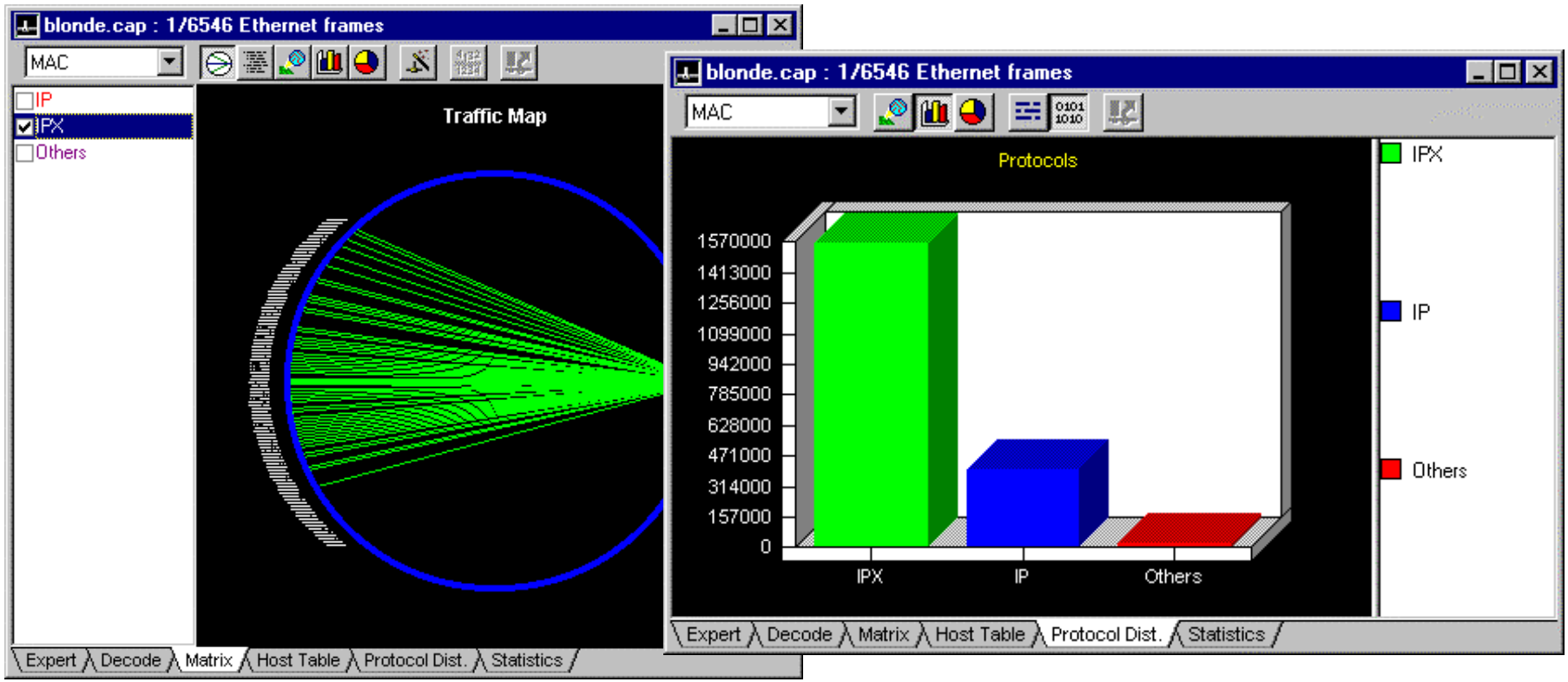
Analyzer Elements

Basic Analyzer Elements



Typical Analyzer - Gone GUI!

- Gauges and graphs
- Alarm/alert idiot lights...



Typical Analyzer - Gone GUI!

- Decodes!

ftp-listfiles.cap: Decode, 10/38 Ethernet Frames

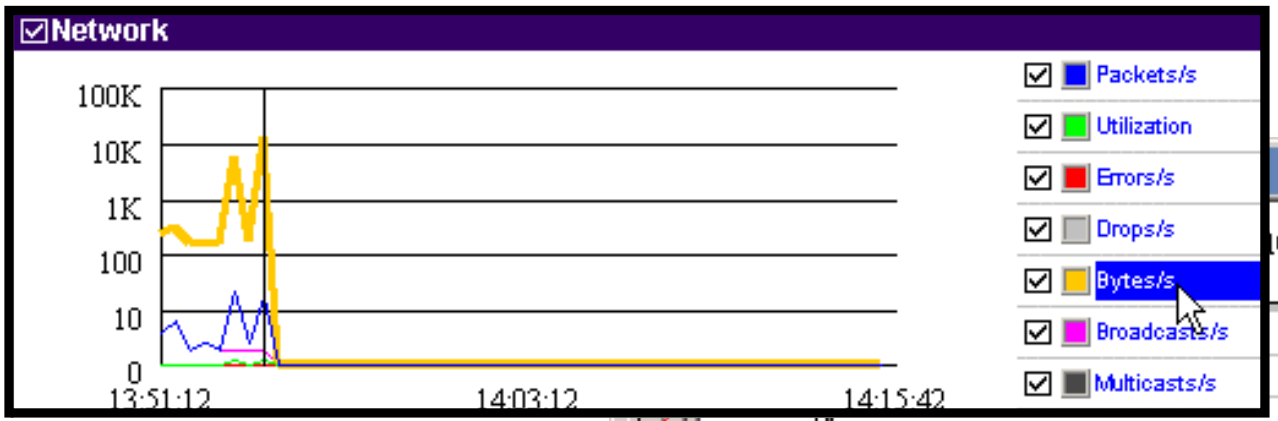
No.	Sta	Source Address	Dest Address	Summary
1	M	00A0CC30C8DE	Broadcast	ARP: C PA=[10.2.0.1] PRO=IP
2		RuntopE15A80	00A0CC30C	ARP: R PA=[10.2.0.1] HA=RuntopE15A80
3		[10.2.0.2]	[10.2.0.1	TCP: D=21 S=1038 SYN SEQ=252836327 LEN
4		[10.2.0.1]	[10.2.0.2	TCP: D=1038 S=21 SYN ACK=252836328 SEQ
5		[10.2.0.2]	[10.2.0.1	TCP: D=21 S=1038 ACK=80707912 WIN=
6		[10.2.0.1]	[10.2.0.2	FTP: R PORT=1038 220-Scott's FTP Ser
7		[10.2.0.2]	[10.2.0.1	TCP: D=21 S=1038 ACK=80707936 WIN=
8		[10.2.0.1]	[10.2.0.2	FTP: R PORT=1038 220-BisonWare Bison
9		[10.2.0.2]	[10.2.0.1	TCP: D=21 S=1038 ACK=80707986 WIN=
10		[10.2.0.2]	[10.2.0.1	FTP: C PORT=1038 USER fred
11		[10.2.0.1]	[10.2.0.2	FTP: R PORT=1038 331 User name OK -
12		[10.2.0.2]	[10.2.0.1	TCP: D=21 S=1038 ACK=80708021 WIN=

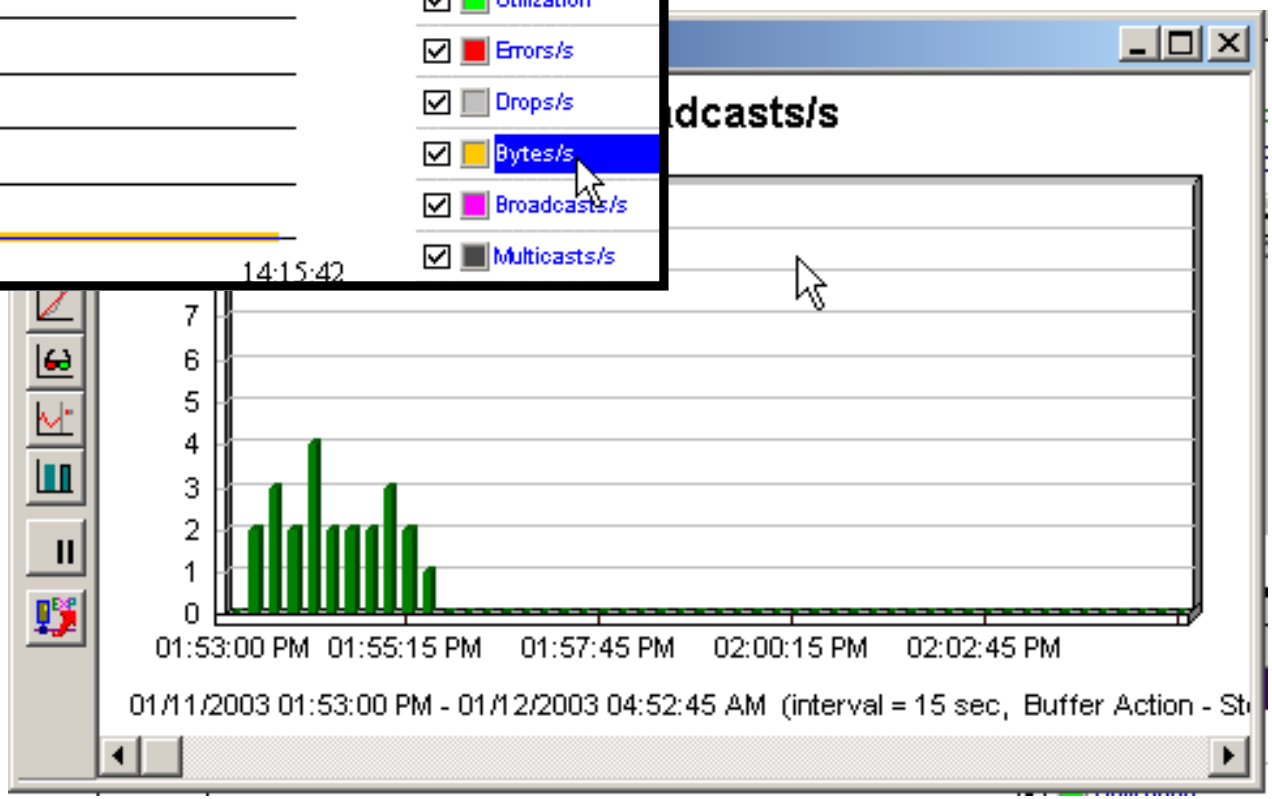
```
    TCP: [11 Bytes of data]
    TCP:
FTP: ----- File Transfer Data Protocol -----
    FTP:
    FTP: Line  1:  USER fred
    FTP:
```

Expert | Decode | Matrix | Host Table | Protocol Dist. | Statistics

Trend Information

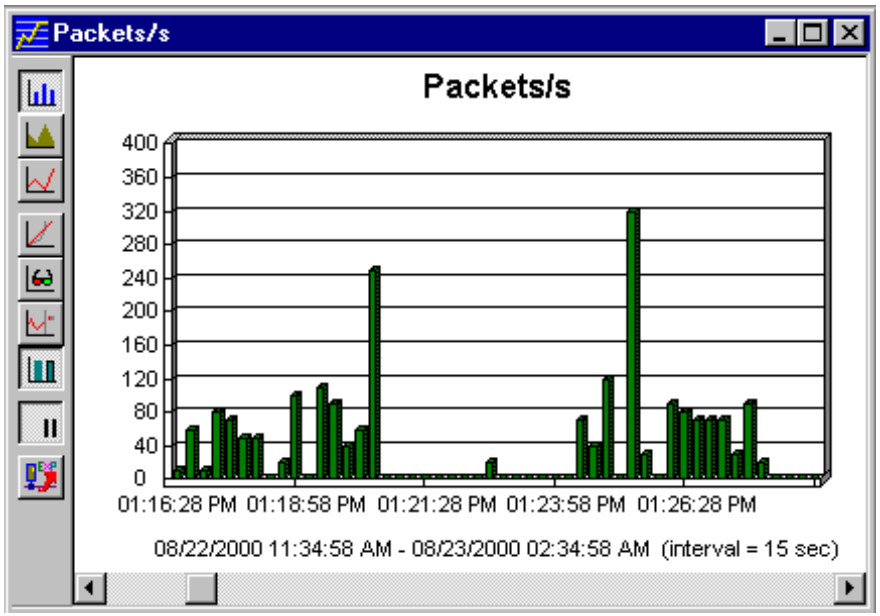
- Short-term trending (15 min – 1 hour)
- Long-term trending (days, weeks, months)



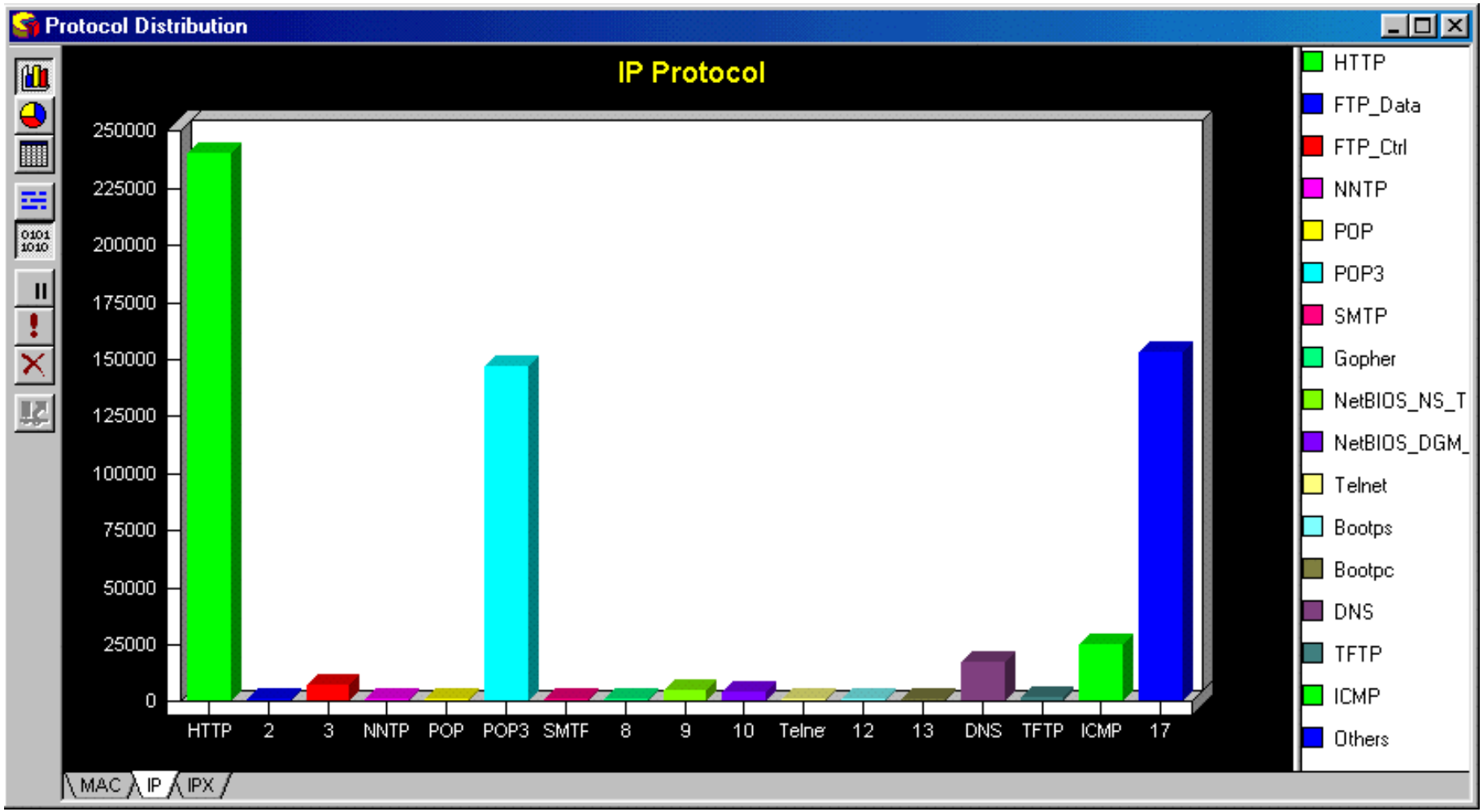


Trends to Watch

- Packet/second
- Utilization %
- Errors/second
- Broadcasts/second
- *Multicasts/second*
- Octets or Kbytes/second
- Packet size distribution



Protocol Information



Alarms/Alerts

- Automatic notification of unusual events
- Watch the thresholds
- Trends enable you to set appropriate thresholds
- Don’t trust all alarms/alerts— research their cause

Capturing Packets

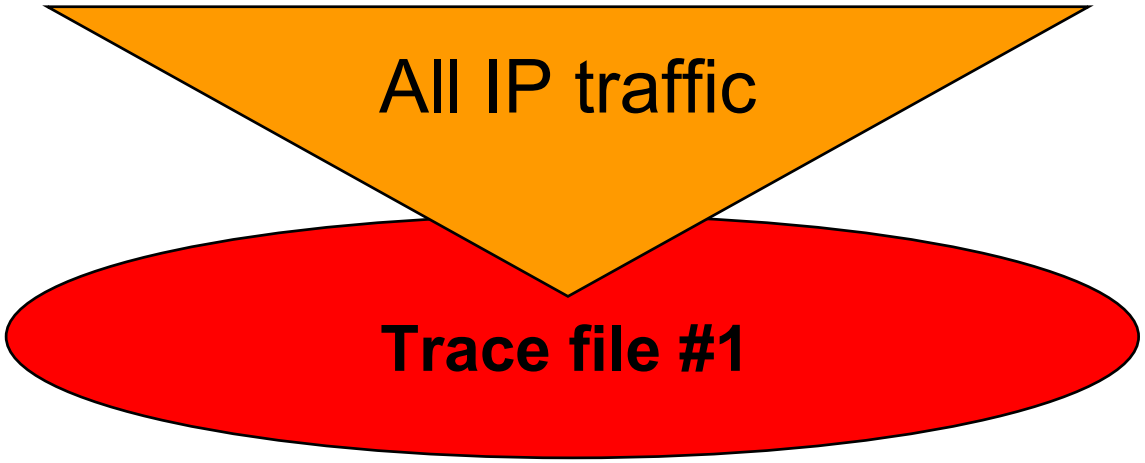
- Basic Capture Processes
- Altering the Buffer
- Using Capture Triggers
- Using Filters
  - Capture filtering (pre-filtering)
  - Display filtering (post-filtering)

Basic Capture Process

- General capture - “laying on of hands”
  - capture all traffic
  - review summary to identify areas of interest
- Specific capture - filtered/focused
  - define capture filters
  - consider trace buffer size
  - consider triggers

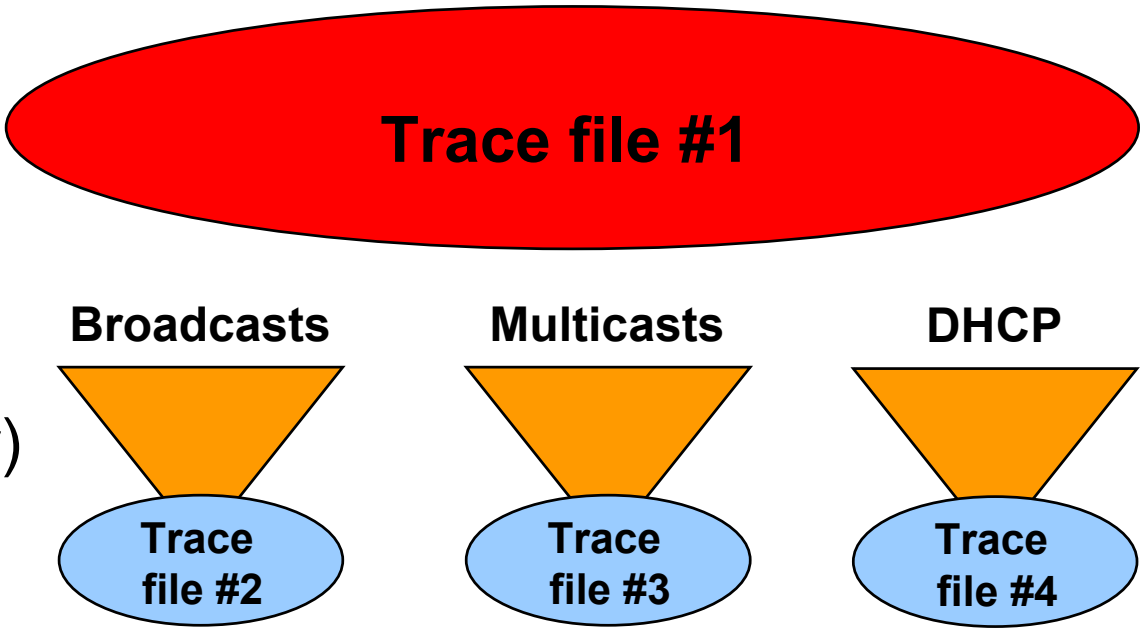
Sample Filter Usage

Pre-filter
(aka Capture Filter)



Sample Filter Usage

Post-filters
(aka Capture Filter)



Reading Traces

Snif2: Decode, 46/167 Ethernet Frames

No.	Sta	Source Address	Dest Address	Summary
43		[12.234.13.8	[80.87.13	HTTP: C Port=1318 GET /tinyimages/
44		[80.87.131.1	[12.234.1	TCP: D=1319 S
45		[12.234.13.8	[80.87.13	TCP: D=80 S=1
46		[12.234.13.8	[80.87.13	HTTP: C Port=1319 GET /images/caf
47		[80.87.131.1	[12.234.1	HTTP: R Port=1316 HTML Data
48		[12.234.13.8	[80.87.13	TCP: D=80 S=1316 ACK=302229018

Summary window

```
HTTP: Line  2:  Accept: */*
HTTP: Line  3:  Referer: http://www.cybercandy.co.uk/aaasm
HTTP:           ffeinated
HTTP: Line  4:  Accept-Language: en-us
HTTP: Line  5:  Accept-Encoding: gzip, deflate
HTTP: Line  6:  User-Agent: Mozilla/4.0 (compatible; MSIE
HTTP:           0)
```

Decode window

```
: 00 3d 40 00 00 47 45 54 20 2f 69 6d 61 67 65  ü.=@..GET /image
8 2f 63 61 66 66 65 69 6e 65 2e 67 69 66 20 48  s/caf
4 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a  TTP/1.1..Accept:
```

Hex window

Expert | Decode | Matrix | Host Table | Protocol Dist. | Statistics

The Summary Window

No.	Sta	Source Address	Dest Address	Summary
1	M	00A0CC30C8DE	Broadcast	ARP: C PA=[10.2.0.1] PRO=IP
2		RuntopE15A8(	00A0CC30C!	ARP: R PA=[10.2.0.1] HA=RuntopE15A80 I
3		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1038 SYN SEQ=252836327 LEN
4		[10.2.0.1]	[10.2.0.2]	TCP: D=1038 S=21 SYN ACK=252836328 SE(
5		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1038 ACK=80707912 WIN=
6		[10.2.0.1]	[10.2.0.2]	FTP: R PORT=1038 220-Scott's FTP
7		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1038 ACK=80707936 WIN=

Packet length	Between Packets	Current Time	From Marked Packet	Bytes from Marked Packet
Len (Bytes)	Delta Time	Abs. Time	Rel. Time	Cumulative Bytes
60	0.000.000	08/05/2000 10:	0:00:00.000	64
60	0.000.063	08/05/2000 10:	0:00:00.000	128
78	0.000.235	08/05/2000 10:	0:00:00.000	210
62	0.000.264	08/05/2000 10:	0:00:00.000	276
60	0.000.377	08/05/2000 10:	0:00:00.000	340
78	0.023.954	08/05/2000 10:	0:00:00.024	422
60	0.196.316	08/05/2000 10:	0:00:00.221	486

Using Summary Information

- Identify general transactions (summary column)
- Latency and throughput testing (time/cumulative bytes)
- First place to look for patterns (summary column)

No.	Status	Source Address	Dest Address	Summary
1	M	00A0CC30C8DB	Broadcast	ARP: C PA=[10.2.0.1] PRO=IP
2		RuntopE15A80	00A0CC30C8DB	ARP: R PA=[10.2.0.1] HA=RuntopE15A80 PRO=IP
3		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 SYN SEQ=182953128 LEN=0 WIN=8
4		[10.2.0.1]	[10.2.0.2]	TCP: D=1033 S=21 SYN ACK=182953129 SEQ=108320
5		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 ACK=10832032 WIN=8760
6		[10.2.0.1]	[10.2.0.2]	FTP: R PORT=1033 220-Scott's FTP Server
7		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 ACK=10832056 WIN=8736
8		[10.2.0.1]	[10.2.0.2]	FTP: R PORT=1033 220-BisonWare BisonFTP serv
9		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 ACK=10832106 WIN=8686
10		[10.2.0.2]	[10.2.0.1]	FTP: C PORT=21 USER fred
11		[10.2.0.1]	[10.2.0.2]	FTP: R PORT=1033 331 User name OK - need pas
12		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 ACK=10832141 WIN=8651
13		[10.2.0.2]	[10.2.0.1]	FTP: C PORT=21 PASS krueger
14		[10.2.0.1]	[10.2.0.2]	FTP: R PORT=1033 230 User logged in OK - Pro
15		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 ACK=10832174 WIN=8618
16		[10.2.0.2]	[10.2.0.1]	FTP: C PORT=21 QUIT
17		[10.2.0.1]	[10.2.0.2]	FTP: R PORT=1033 221 Thank you for visiting
18		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 FIN ACK=10832216 SEQ=1829531
19		[10.2.0.1]	[10.2.0.2]	TCP: D=1033 S=21 FIN ACK=182953161 SEQ=108322
20		[10.2.0.2]	[10.2.0.1]	TCP: D=21 S=1033 ACK=10832217 WIN=8576

Latency Testing

- ACK time = wire latency
- Response time = processing time

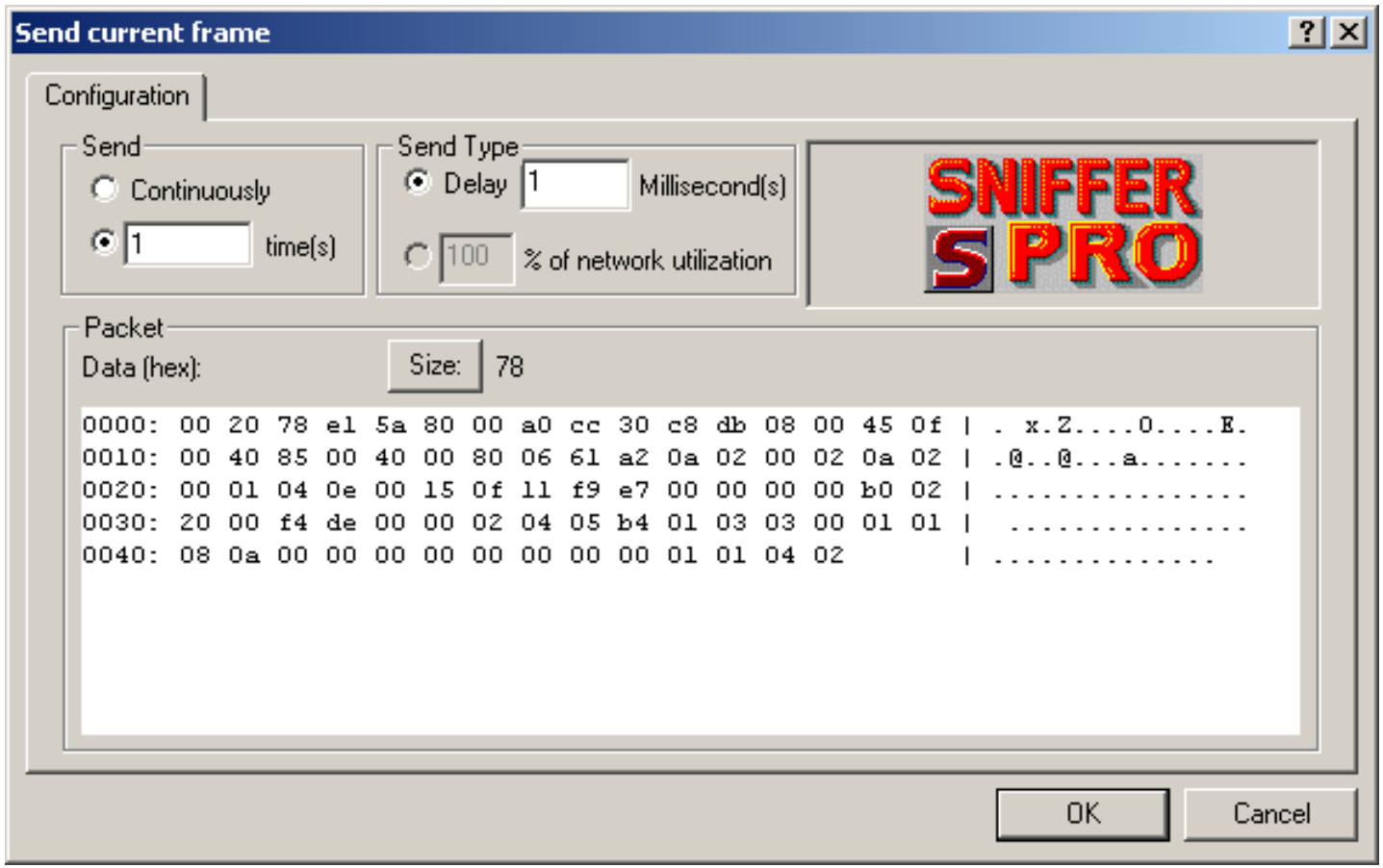
ftp-listfiles.cap: Decode, 10/38 Ethernet Frames

No.	Summary	Delta Time
8	FTP: R PORT=1038 220-BisonWare Bisor	0.000.146
9	TCP: D=21 S=1038 ACK=80707986 WIN=	0.212.825
10	FTP: C PORT=1038 USER fred	5.696.688
11	FTP: R PORT=1038 331 User name OK -	0.005.604
12	TCP: D=21 S=1038 ACK=80708021 WIN=	0.101.999
13	FTP: C PORT=1038 PASS krueger	2.718.684
14	FTP: R PORT=1038 230 User logged in	0.005.800
15	TCP: D=21 S=1038 ACK=80708054 WIN=	0.192.762
16	FTP: C PORT=1038 PORT 10,2,0,2,4,15	1.615.659
17	FTP: R PORT=1038 200 PORT Command Ac	0.007.636
18	FTP: C PORT=1038 NLST	0.024.053

Expert | Decode | Matrix | Host Table | Protocol Dist. | Statistics

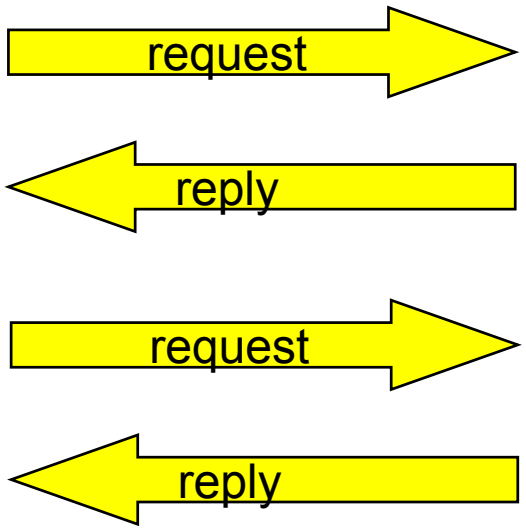
Build/Send Test Packets

- Response times/faults
- Network Saturation



Typical Communication Patterns

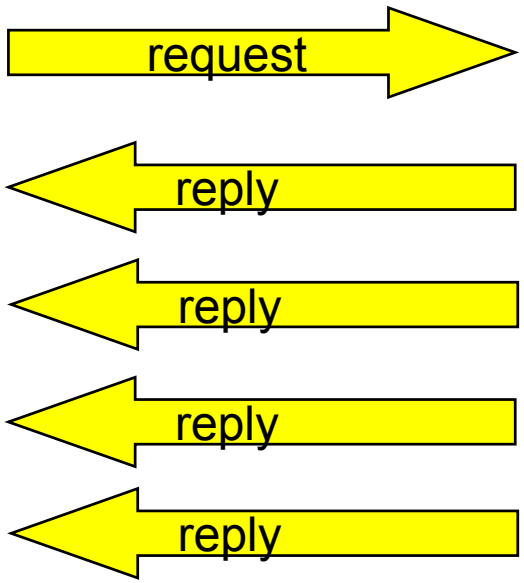
- Good patterns
- Bad patterns
- Lousy stinkin' patterns



For Commands

Typical Communication Patterns

- Good patterns
- Bad patterns
- Lousy stinkin' patterns

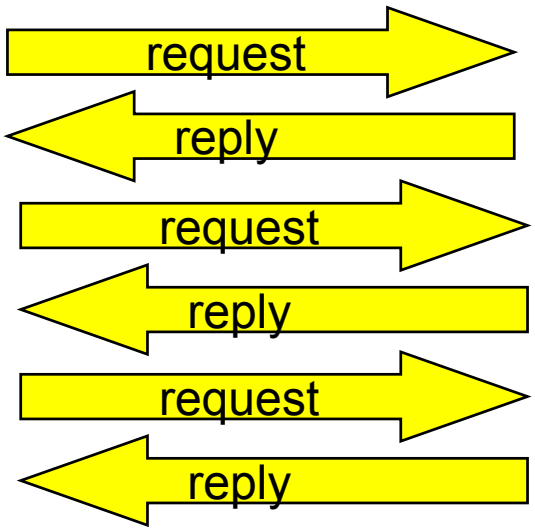


Typical Communication Patterns

Good patterns

Bad patterns

Lousy stinkin' patterns



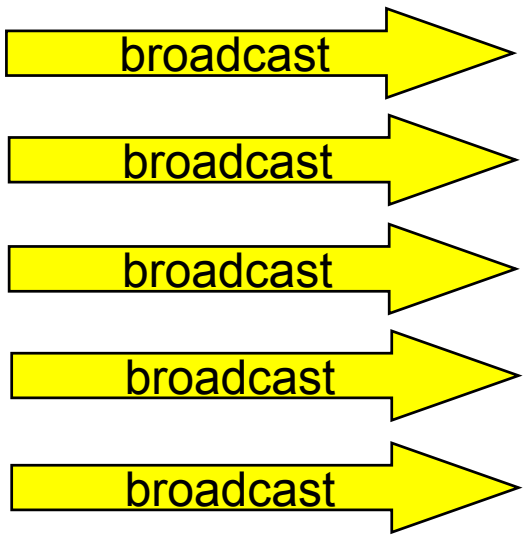
For Data Transfer

Typical Communication Patterns

Good patterns

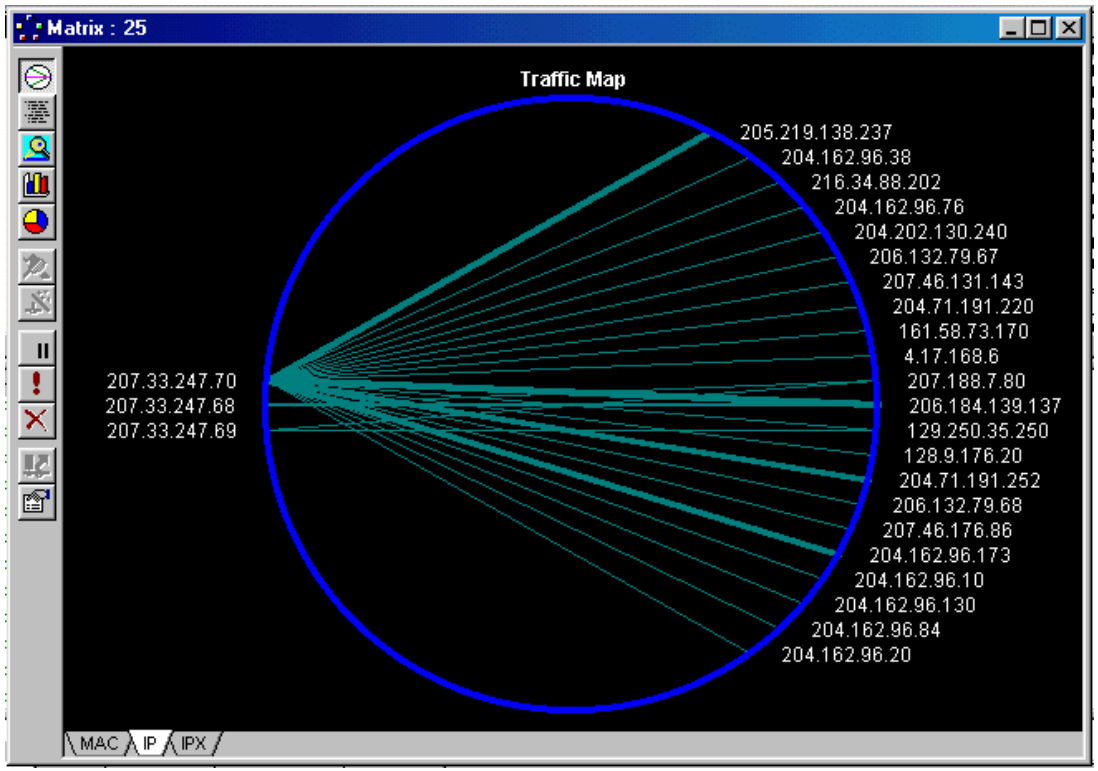
Bad patterns

Lousy stinkin' patterns

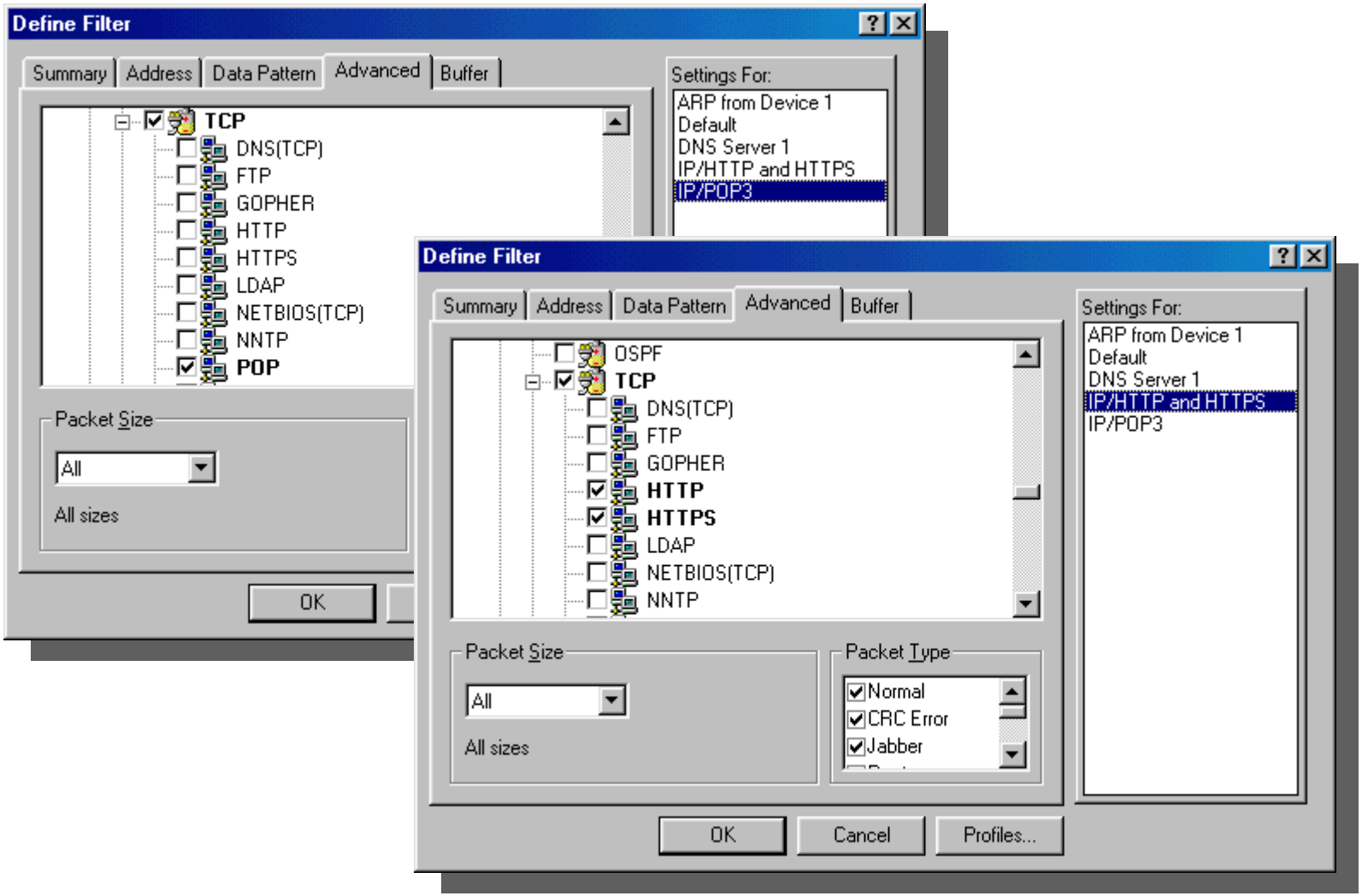


Conversation Matrix

- Point-to-point relationships
- Single point of congestion
- Single point of failure



Protocol Filtering

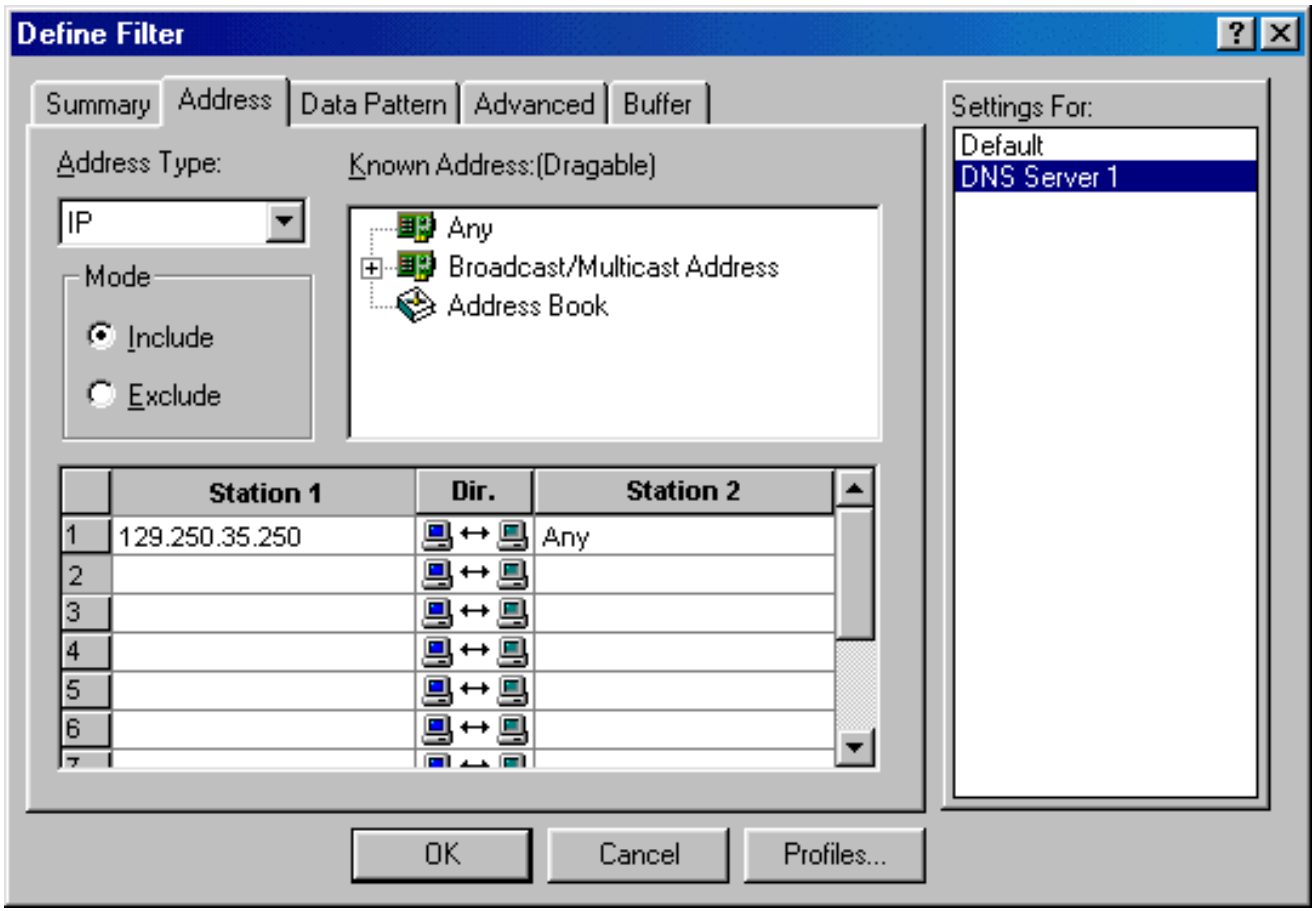


Protocol Filters You Should Have

- ICMP/All
- ICMP/Destination Unreachable
- ICMP/Echo
- ICMP/Redirect
- ARP
- IP/UDP All
- IP/UDP NetBIOS
- IP/UDP SNMP (Trap + Get)
- IP/UDP DHCP + BOOTP
- IP/TCP All
- IP/TCP FTP
- IP/TCP FTP Commands*
- IP/TCP DNS (TCP and UDP)
- IP/TCP Telnet
- IP/TCP Rlogin
- IP/TCP/SMTP
- IP/TCP POP
- IP/TCP HTTP + HTTPS

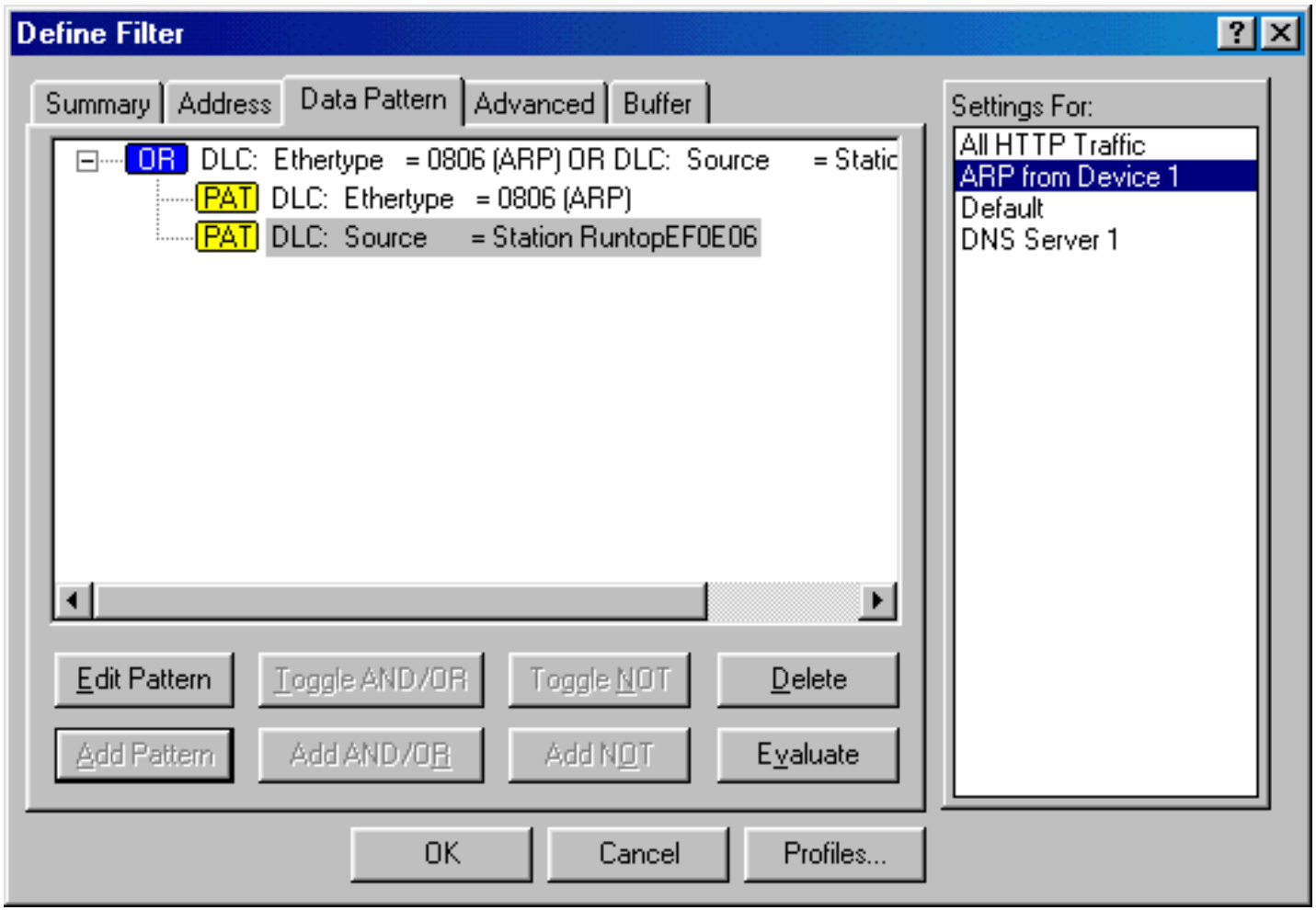
Address Filtering

- MAC-Layer, Network Layer (IP/IPX… etc.)
- Include/exclude



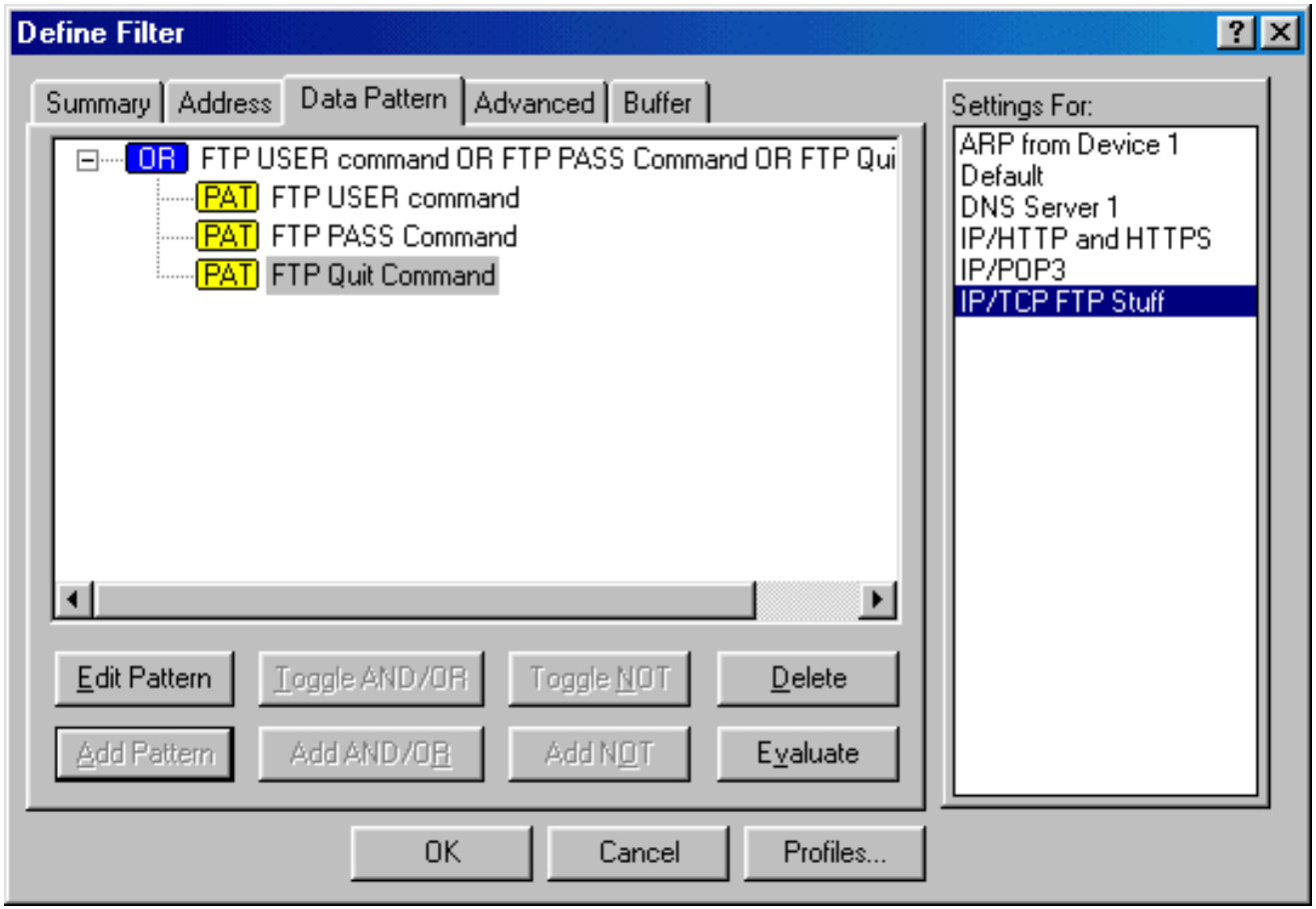
Pattern Filtering

- AND, NOT and OR



Boolean Filtering

- Don't just look for FTP Traffic… look for the commands…



Which Analyzer?

- Ethereal
- Finisar Surveyor
- Network Associates' Sniffer
- Network Instruments Observer
- WildPackets EtherPeek

… others

Conclusion

- Good analysis requires a solid understanding of network communications.
- Analyzers are ideal for troubleshooting and security tasks.
- There are a variety of reports and graphs that can be used to document network performance.
- If you own a network – you should own an analyzer.