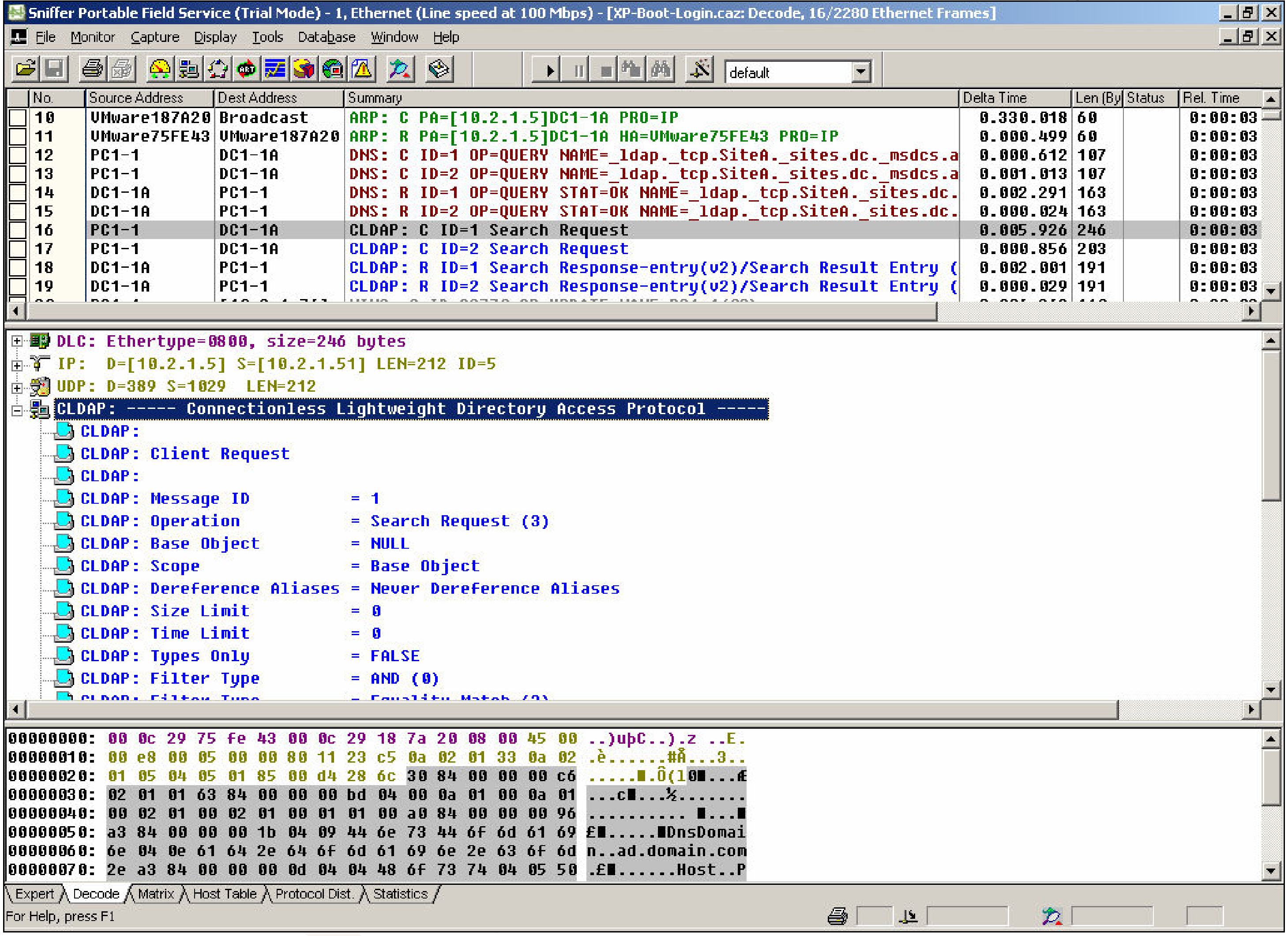
This is considered the ideal decode Summary pane configuration.

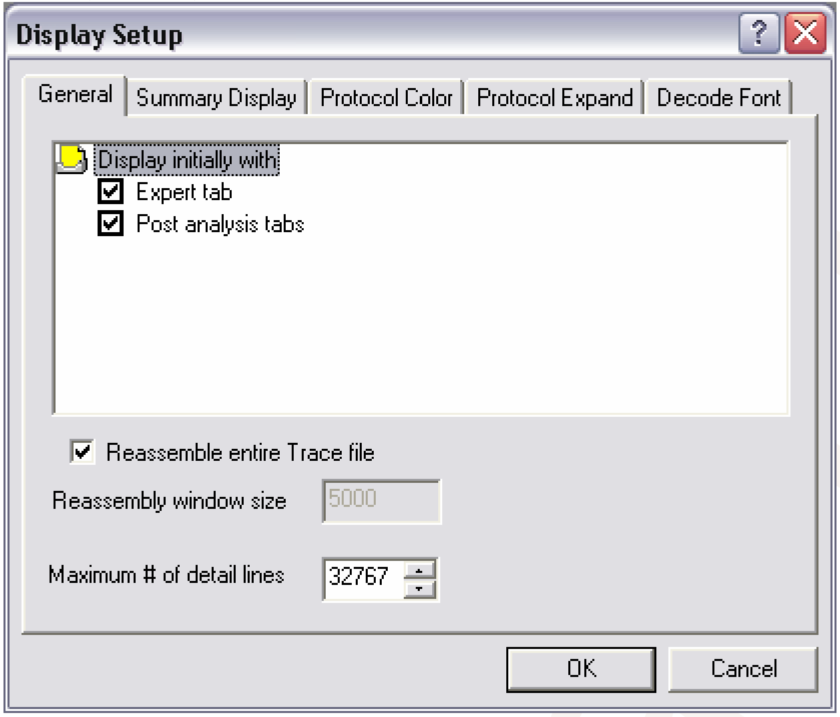

Sniffer Portable Field Service (Trial Mode) - 1, Ethernet (Line speed at 100 Mbps) - [XP-Boot-Login.caz: Decode, 16/2280 Ethernet Frames]
File
Monitor
Capture
Display
Tools
Database
Window
Help
default
Expert
Decode
Matrix
Host Table
Protocol Dist.
Statistics
For Help, press F1

No.	Source Address	Dest Address	Summary	Delta Time	Len (By	Status	Rel. Time
10	VMware187A20	Broadcast	ARP: C PA=[10.2.1.5]DC1-1A PRO=IP	0.330.018	60		0:00:03
11	VMware75FE43	VMware187A20	ARP: R PA=[10.2.1.5]DC1-1A HA=VMware75FE43 PRO=IP	0.000.499	60		0:00:03
12	PC1-1	DC1-1A	DNS: C ID=1 OP=QUERY NAME=_ldap._tcp.SiteA._sites.dc._msdcs.a	0.000.612	107		0:00:03
13	PC1-1	DC1-1A	DNS: C ID=2 OP=QUERY NAME=_ldap._tcp.SiteA._sites.dc._msdcs.a	0.001.013	107		0:00:03
14	DC1-1A	PC1-1	DNS: R ID=1 OP=QUERY STAT=OK NAME=_ldap._tcp.SiteA._sites.dc.	0.002.291	163		0:00:03
15	DC1-1A	PC1-1	DNS: R ID=2 OP=QUERY STAT=OK NAME=_ldap._tcp.SiteA._sites.dc.	0.000.024	163		0:00:03
16	PC1-1	DC1-1A	CLDAP: C ID=1 Search Request	0.005.926	246		0:00:03
17	PC1-1	DC1-1A	CLDAP: C ID=2 Search Request	0.000.856	203		0:00:03
18	DC1-1A	PC1-1	CLDAP: R ID=1 Search Response-entry(v2)/Search Result Entry (	0.002.001	191		0:00:03
19	DC1-1A	PC1-1	CLDAP: R ID=2 Search Response-entry(v2)/Search Result Entry (	0.000.029	191		0:00:03

```
DLC: Ethertype=0800, size=246 bytes
IP:  D=[10.2.1.5] S=[10.2.1.51] LEN=212 ID=5
UDP: D=389 S=1029  LEN=212
CLDAP: ----- Connectionless Lightweight Directory Access Protocol -----
    CLDAP:
    CLDAP: Client Request
    CLDAP:
    CLDAP: Message ID            = 1
    CLDAP: Operation             = Search Request (3)
    CLDAP: Base Object           = NULL
    CLDAP: Scope                 = Base Object
    CLDAP: Dereference Aliases = Never Dereference Aliases
    CLDAP: Size Limit            = 0
    CLDAP: Time Limit            = 0
    CLDAP: Types Only            = FALSE
    CLDAP: Filter Type           = AND (0)
```

```
00000000: 00 0c 29 75 fe 43 00 0c 29 18 7a 20 08 00 45 00 ..)uþC..).z ..E.
00000010: 00 e8 00 05 00 00 80 11 23 c5 0a 02 01 33 0a 02 .è......#Å...3..
00000020: 01 05 04 05 01 85 00 d4 28 6c 30 84 00 00 00 c6 .....█.Ô(l0█...Æ
00000030: 02 01 01 63 84 00 00 00 bd 04 00 0a 01 00 0a 01 ...c█...½.......
00000040: 00 02 01 00 02 01 00 01 01 00 a0 84 00 00 00 96 .......... █...█
00000050: a3 84 00 00 00 1b 04 09 44 6e 73 44 6f 6d 61 69 £█.....█DnsDomai
00000060: 6e 04 0e 61 64 2e 64 6f 6d 61 69 6e 2e 63 6f 6d n..ad.domain.com
00000070: 2e a3 84 00 00 00 0d 04 04 48 6f 73 74 04 05 50 .£█......Host..P
```

Reassemble Entire Trace File **will eliminate line-by-line paging of frames in a very large trace. Increase** ***Maximum Number of Detail Lines*** **displayed in decode Detail pane: important with HTTP, LDAP, etc.**



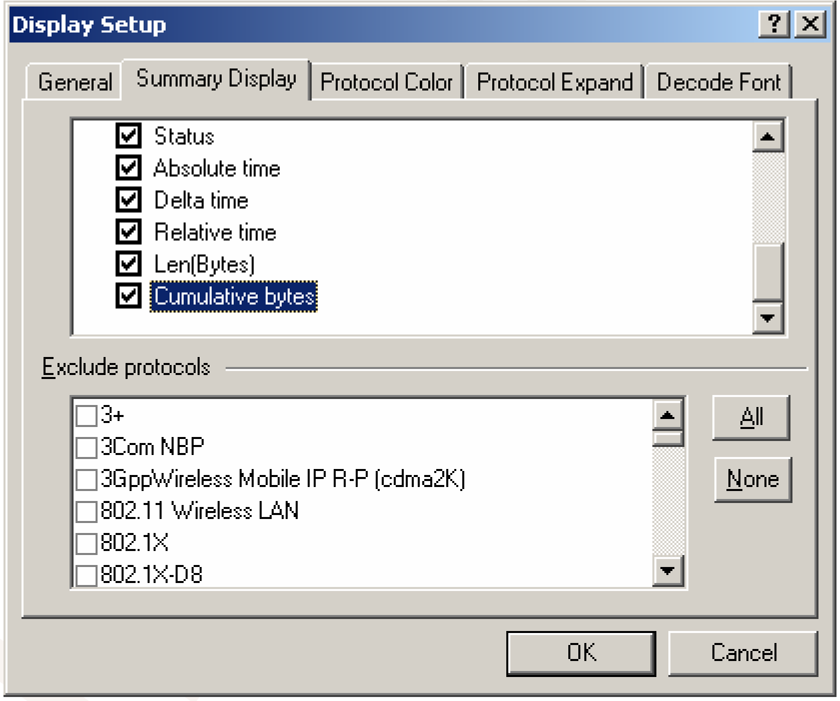
Display initially with
☑ Expert tab
☑ Post analysis tabs

☑ Reassemble entire Trace file

Reassembly window size 5000

Maximum # of detail lines 32767

Enable Cumulative Bytes used with the Mark to gauge file transfer performance.

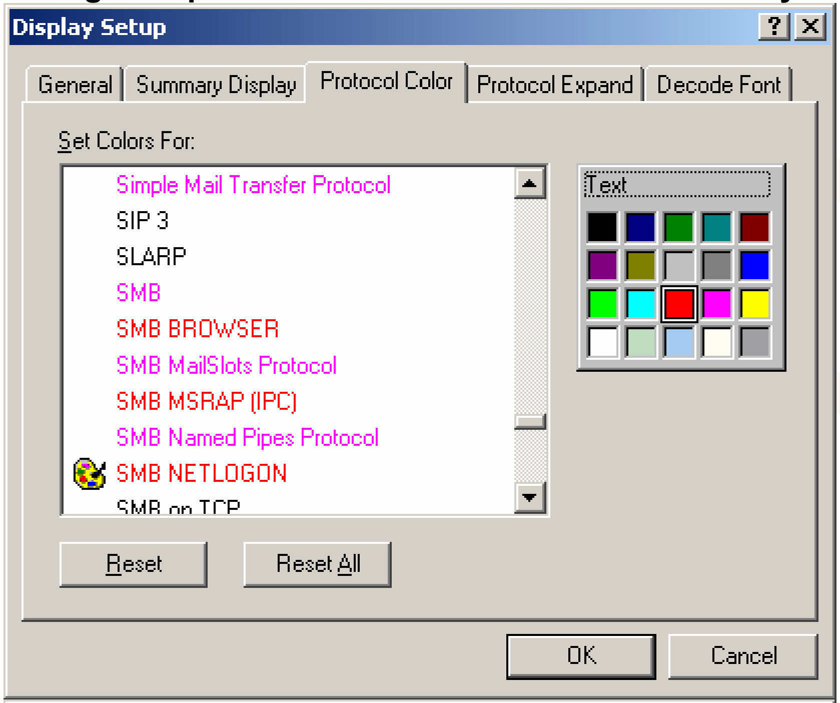


☑ Status
☑ Absolute time
☑ Delta time
☑ Relative time
☑ Len(Bytes)
☑ Cumulative bytes

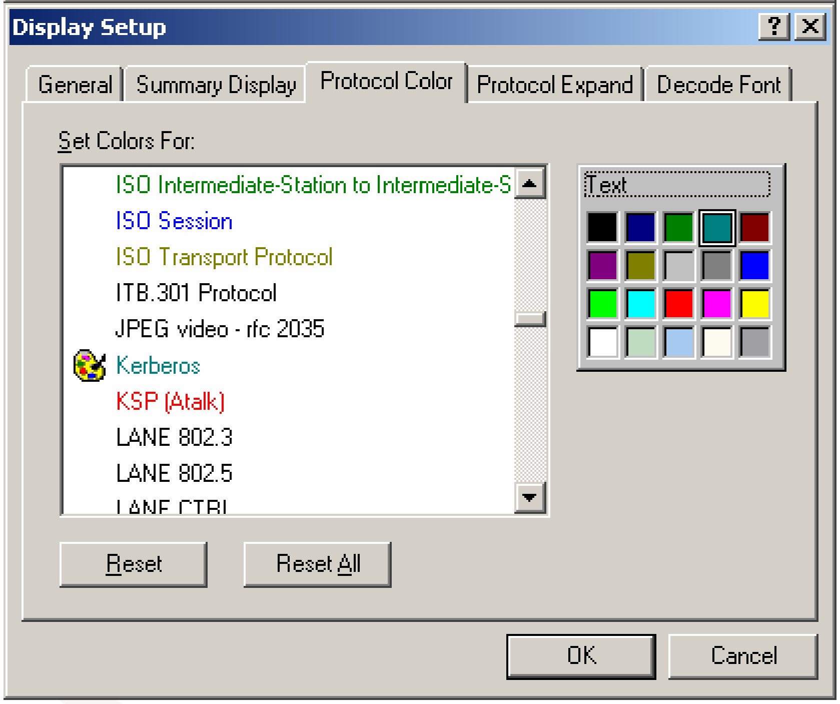
Exclude protocols

□ 3+
□ 3Com NBP
□ 3GppWireless Mobile IP R-P (cdma2K)
□ 802.11 Wireless LAN
□ 802.1X
□ 802.1X-D8

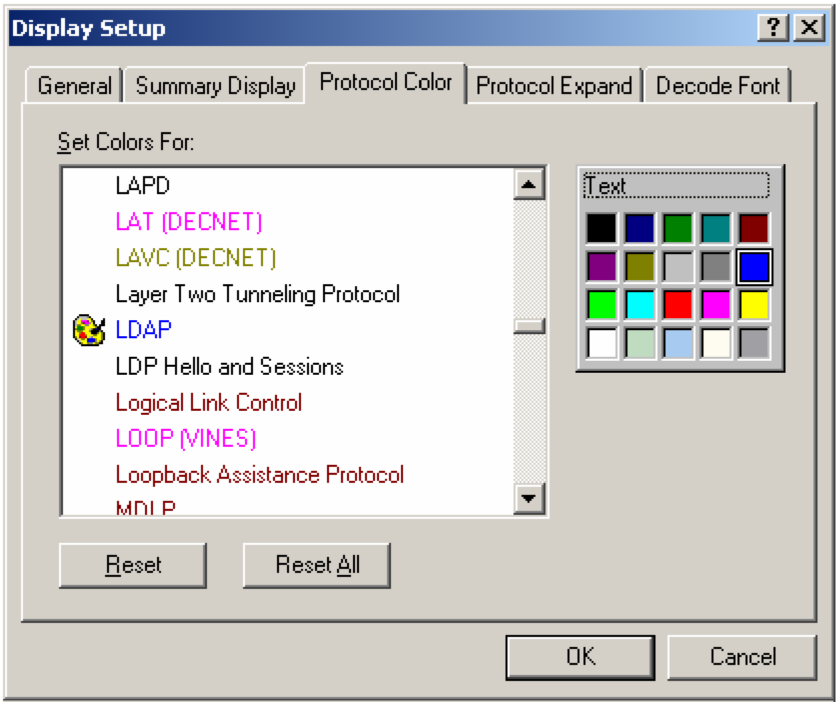
Change the protocol colors to ones that will visually stand out amongst its peers:



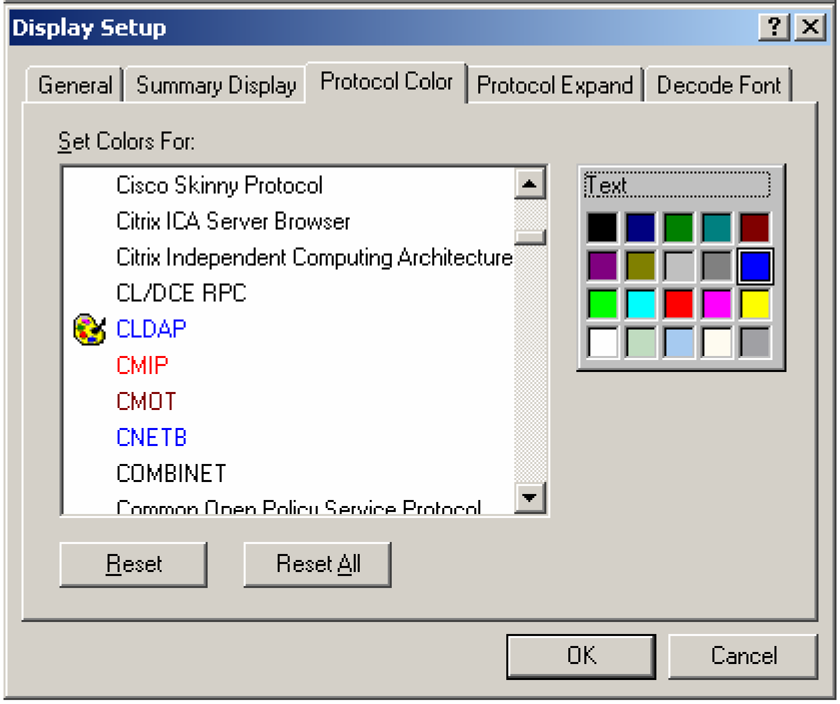
Simple Mail Transfer Protocol
SIP 3
SLARP
SMB
SMB BROWSER
SMB MailSlots Protocol
SMB MSRAP (IPC)
SMB Named Pipes Protocol
SMB NETLOGON
SMB on TCP



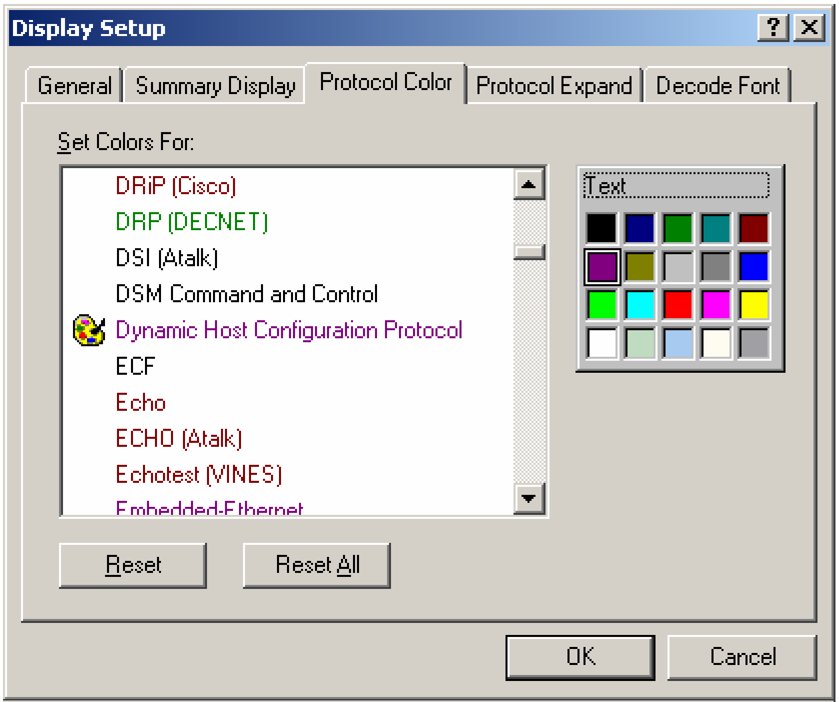
ISO Intermediate-Station to Intermediate-S
ISO Session
ISO Transport Protocol
ITB.301 Protocol
JPEG video - rfc 2035
Kerberos
KSP (Atalk)
LANE 802.3
LANE 802.5
LANE CTRL



LAPD
LAT (DECNET)
LAVC (DECNET)
Layer Two Tunneling Protocol
LDAP
LDP Hello and Sessions
Logical Link Control
LOOP (VINES)
Loopback Assistance Protocol
MDLP



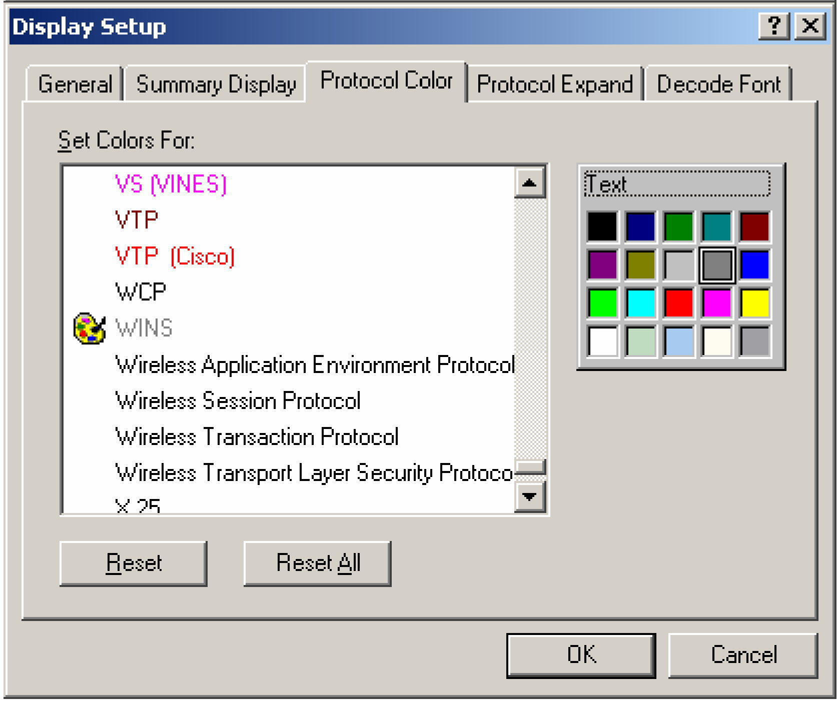
Cisco Skinny Protocol
Citrix ICA Server Browser
Citrix Independent Computing Architecture
CL/DCE RPC
CLDAP
CMIP
CMOT
CNETB
COMBINET
Common Open Policy Service Protocol



Set Colors For:

DRiP (Cisco)
DRP (DECNET)
DSI (Atalk)
DSM Command and Control
Dynamic Host Configuration Protocol
ECF
Echo
ECHO (Atalk)
Echotest (VINES)
Embedded-Ethernet

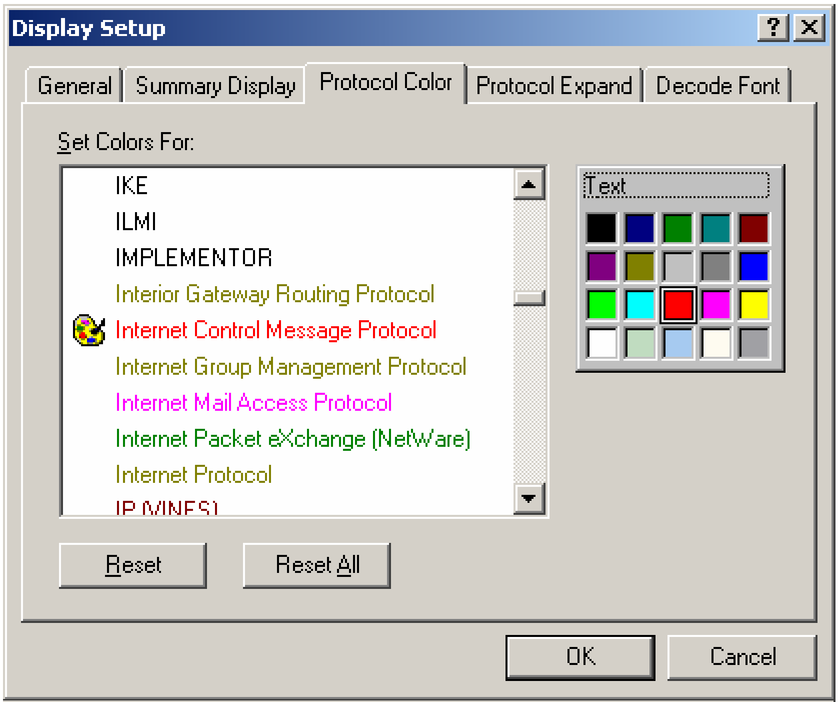
Text



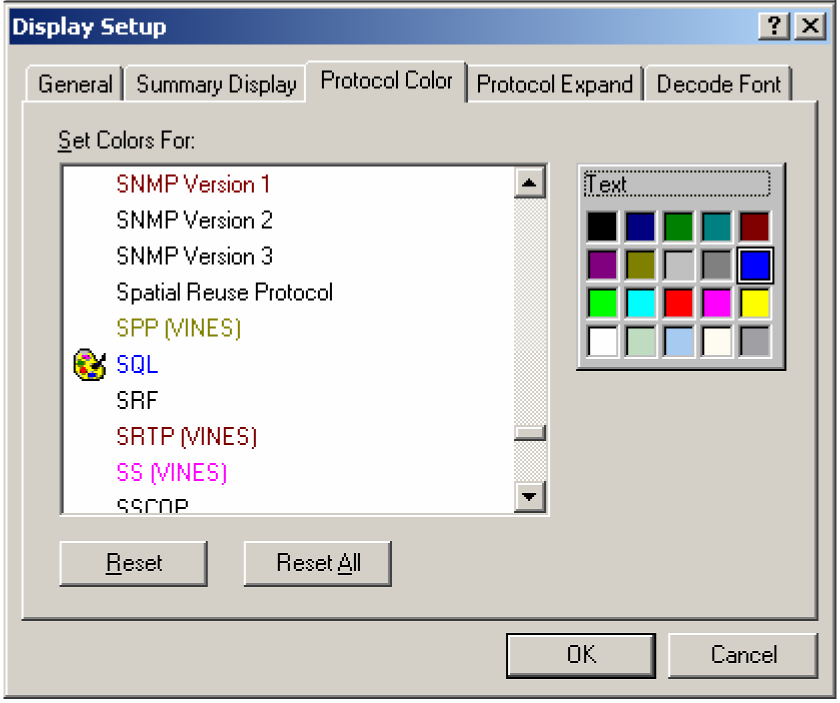
Set Colors For:

VS (VINES)
VTP
VTP (Cisco)
WCP
WINS
Wireless Application Environment Protocol
Wireless Session Protocol
Wireless Transaction Protocol
Wireless Transport Layer Security Protoco
X.25

Text

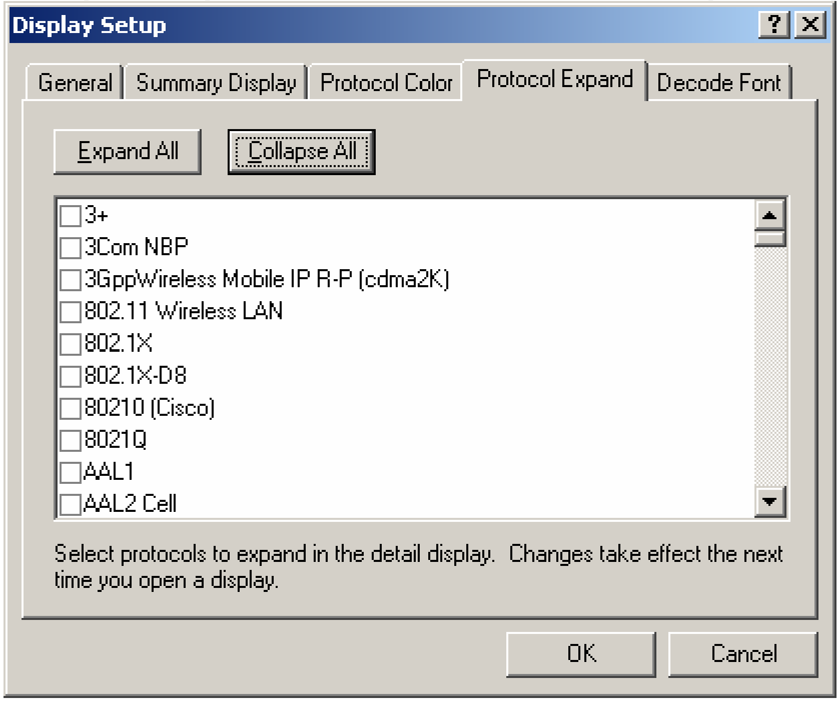


IKE
ILMI
IMPLEMENTOR
Interior Gateway Routing Protocol
Internet Control Message Protocol
Internet Group Management Protocol
Internet Mail Access Protocol
Internet Packet eXchange (NetWare)
Internet Protocol
IP (VINES)



SNMP Version 1
SNMP Version 2
SNMP Version 3
Spatial Reuse Protocol
SPP (VINES)
SQL
SRF
SRTP (VINES)
SS (VINES)
SSCOP

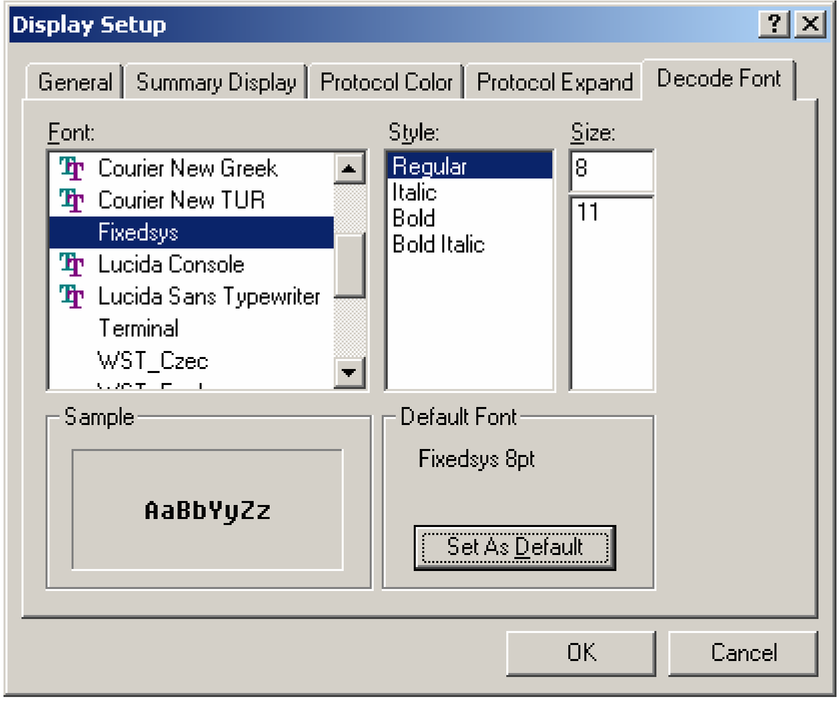
Collapse the protocol list in the decode Detail pane to permit faster viewing.



□ 3+
□ 3Com NBP
□ 3GppWireless Mobile IP R-P (cdma2K)
□ 802.11 Wireless LAN
□ 802.1X
□ 802.1X-D8
□ 80210 (Cisco)
□ 8021Q
□ AAL1
□ AAL2 Cell

Select protocols to expand in the detail display. Changes take effect the next time you open a display.

Change the display font to a crisper one that will permit longer viewing times. Set as Default.



Display Setup

Font: Fixedsys

Style: Regular

Size: 8

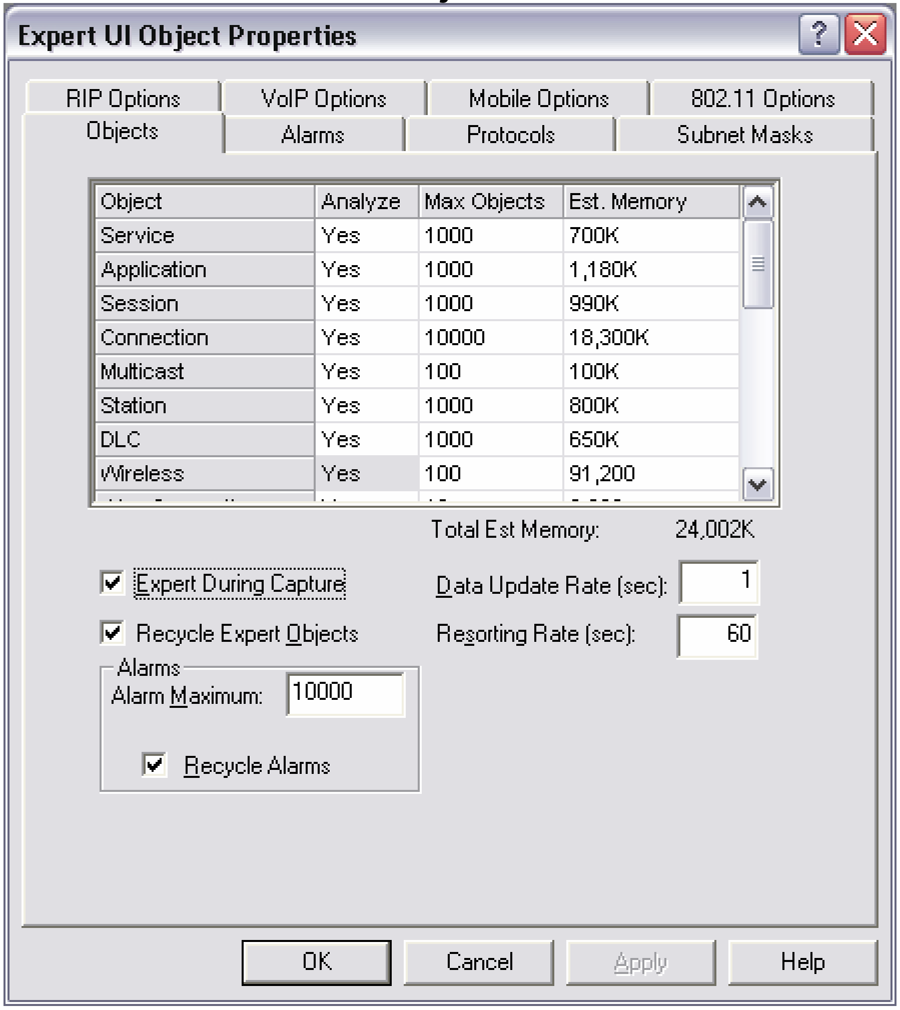
Sample

AaBbYyZz

Default Font

Fixedsys 8pt

Zero out the Wireless, WAN, and ATM *Max Objects* if you're Sniffing Ethernet.
Wireless has been left at 100 below because this user opens Wireless traces on occasion.
Decrease Class D Multicasts to 100, too. No point in wasting memory on resources that will probably not be used to their maximum.
Increase Connection *Max Objects* to at least 5000. Increase to 10,000 on Infinistream.



Object	Analyze	Max Objects	Est. Memory
Service	Yes	1000	700K
Application	Yes	1000	1,180K
Session	Yes	1000	990K
Connection	Yes	10000	18,300K
Multicast	Yes	100	100K
Station	Yes	1000	800K
DLC	Yes	1000	650K
Wireless	Yes	100	91,200

Total Est Memory: 24,002K

☑ Expert During Capture

☑ Recycle Expert Objects

Data Update Rate (sec): 1

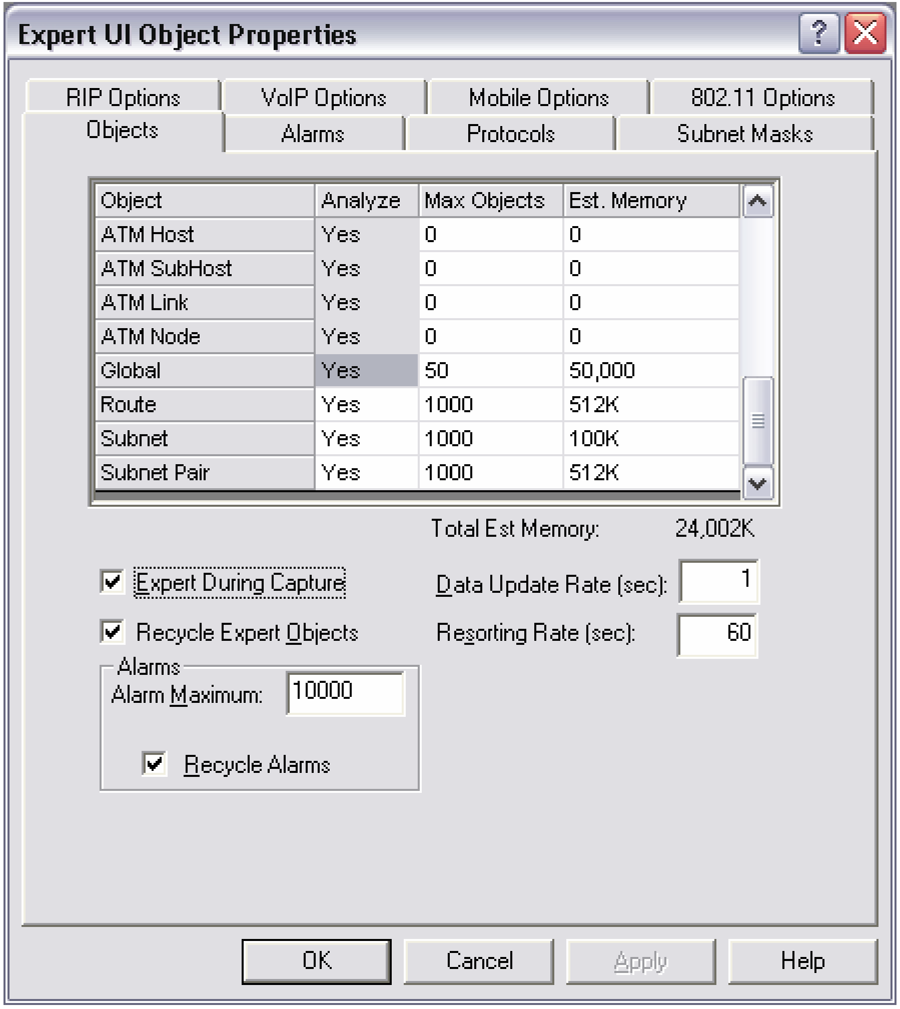
Resorting Rate (sec): 60

Alarms

Alarm Maximum: 10000

☑ Recycle Alarms

Increase *Alarms Maximum* to at least 3000, especially if you're capturing from a Distribution or Core switch. Increase to 10,000 on Infinistream.



Object	Analyze	Max Objects	Est. Memory
ATM Host	Yes	0	0
ATM SubHost	Yes	0	0
ATM Link	Yes	0	0
ATM Node	Yes	0	0
Global	Yes	50	50,000
Route	Yes	1000	512K
Subnet	Yes	1000	100K
Subnet Pair	Yes	1000	512K

Total Est Memory: 24,002K

☑ Expert During Capture

☑ Recycle Expert Objects

Data Update Rate (sec): 1

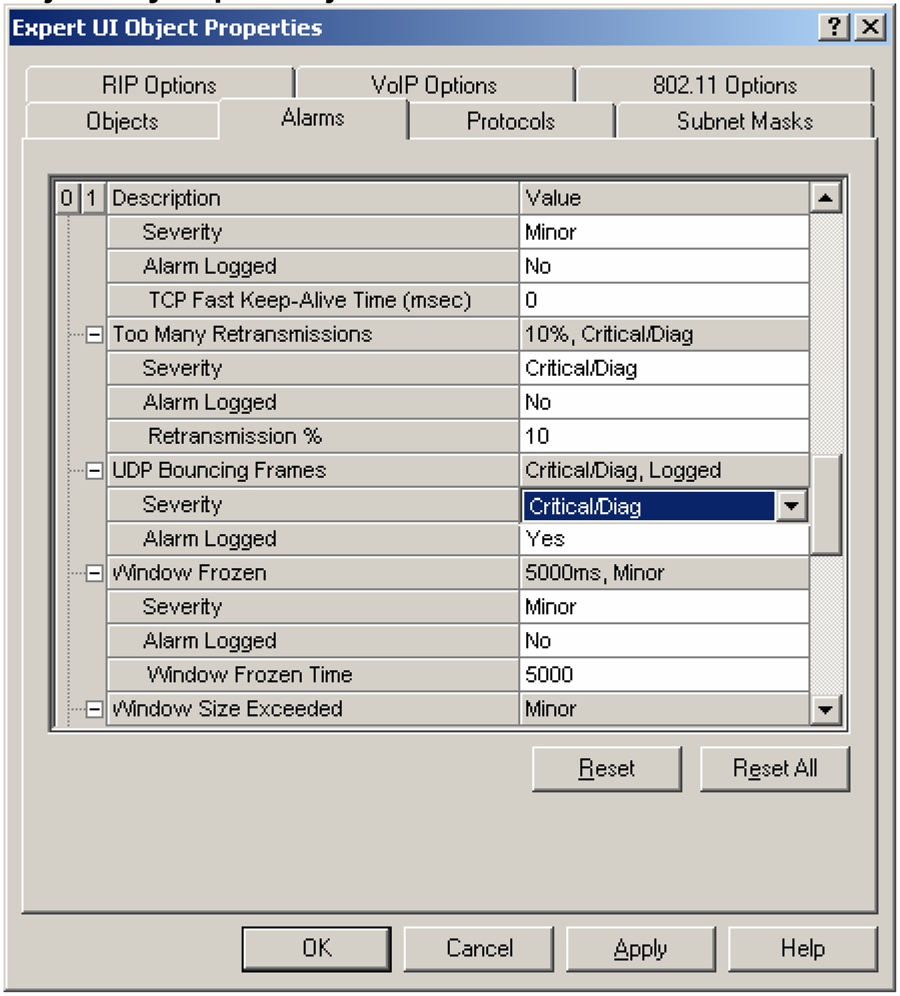
Resorting Rate (sec): 60

Alarms

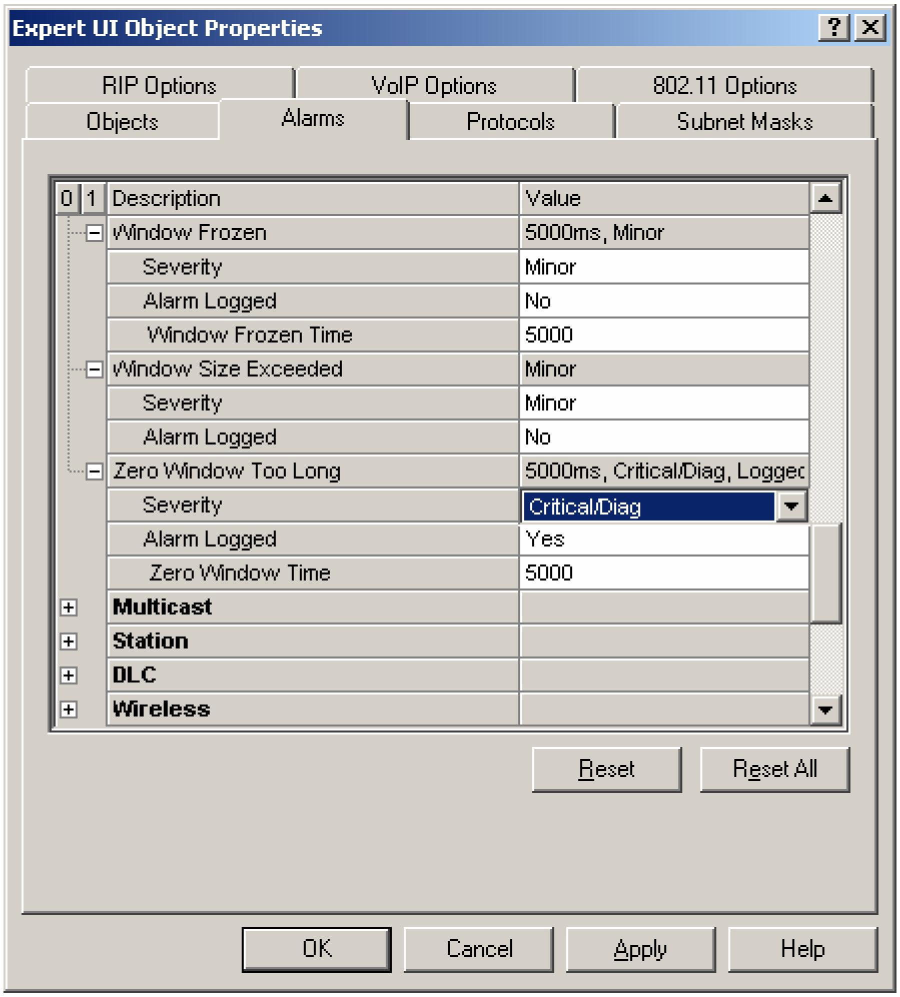
Alarm Maximum: 10000

☑ Recycle Alarms

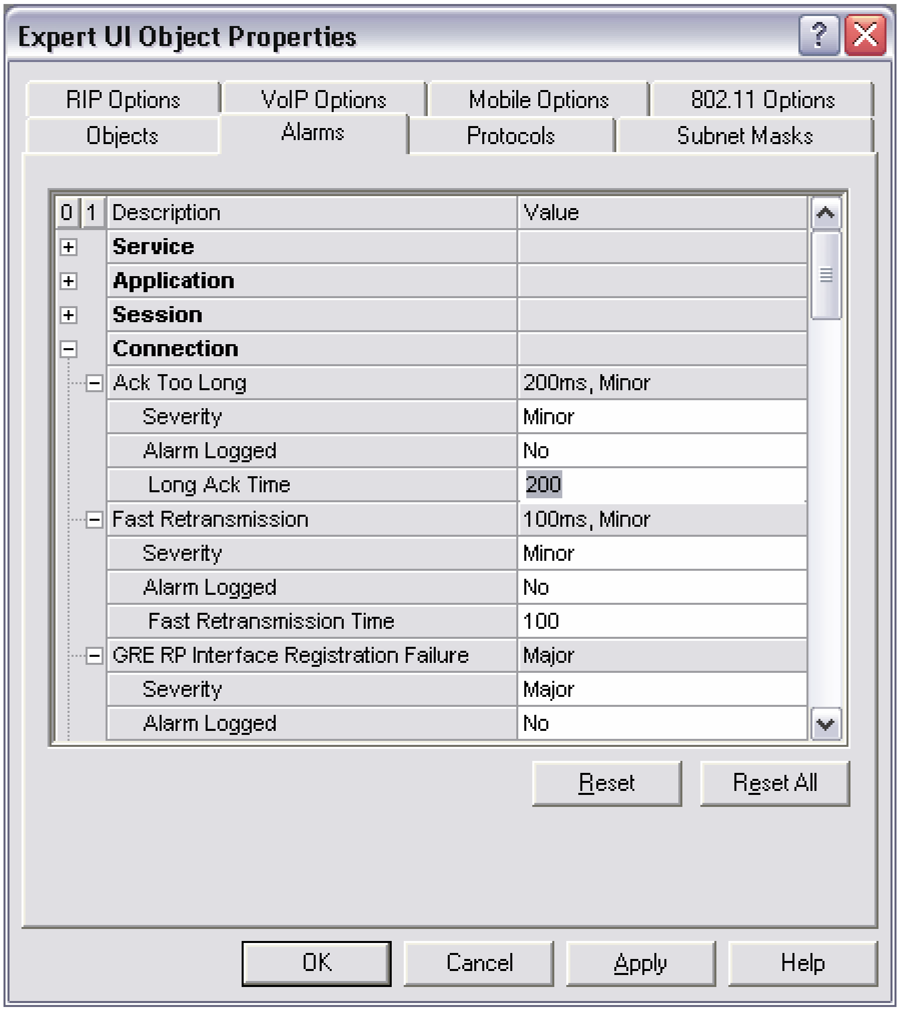
Adjust key Expert Object Alarms.



Description	Value
Severity	Minor
Alarm Logged	No
TCP Fast Keep-Alive Time (msec)	0
⊟ Too Many Retransmissions	10%, Critical/Diag
Severity	Critical/Diag
Alarm Logged	No
Retransmission %	10
⊟ UDP Bouncing Frames	Critical/Diag, Logged
Severity	Critical/Diag
Alarm Logged	Yes
⊟ Window Frozen	5000ms, Minor
Severity	Minor
Alarm Logged	No
Window Frozen Time	5000
⊟ Window Size Exceeded	Minor

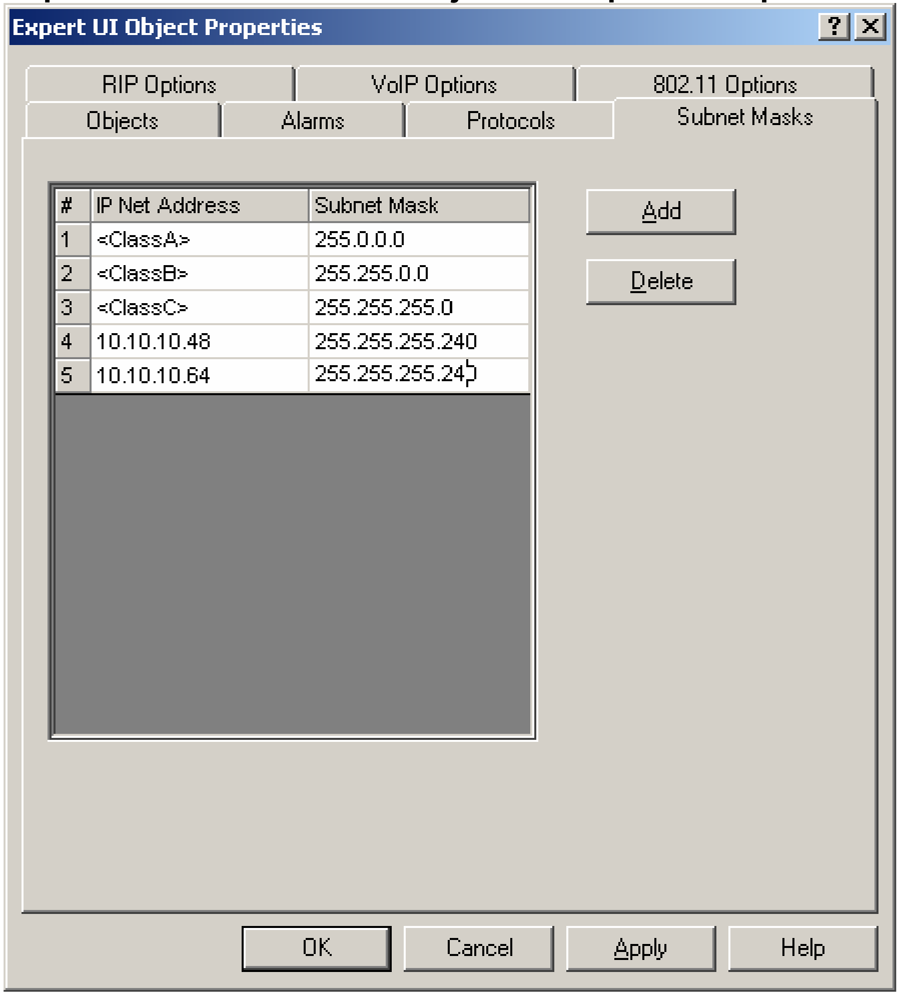


0 1	Description	Value
⊟	Window Frozen	5000ms, Minor
	Severity	Minor
	Alarm Logged	No
	Window Frozen Time	5000
⊟	Window Size Exceeded	Minor
	Severity	Minor
	Alarm Logged	No
⊟	Zero Window Too Long	5000ms, Critical/Diag, Loggec
	Severity	Critical/Diag ▼
	Alarm Logged	Yes
	Zero Window Time	5000
⊞	**Multicast**	
⊞	**Station**	
⊞	**DLC**	
⊞	**Wireless**	



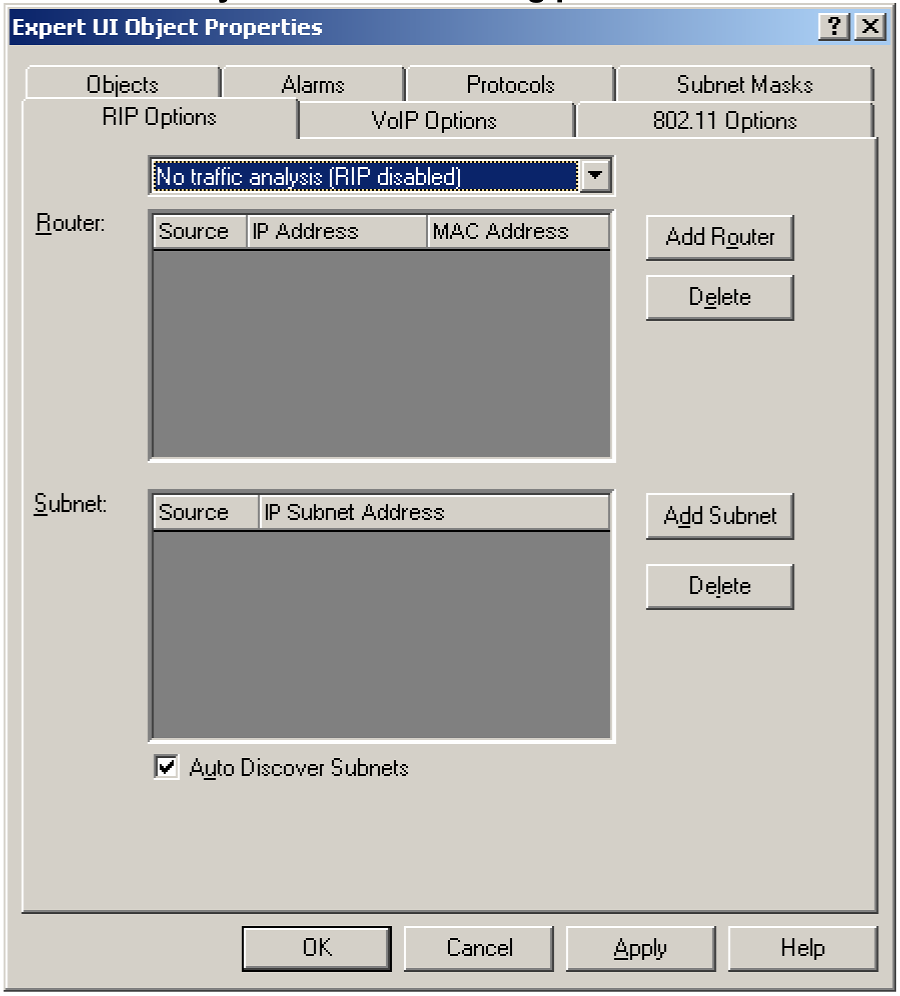
Description	Value
Service	
Application	
Session	
Connection	
Ack Too Long	200ms, Minor
Severity	Minor
Alarm Logged	No
Long Ack Time	200
Fast Retransmission	100ms, Minor
Severity	Minor
Alarm Logged	No
Fast Retransmission Time	100
GRE RP Interface Registration Failure	Major
Severity	Major
Alarm Logged	No

Add the subnet mask(s) only for the subnet you are attached to or SPANning/mirroring.
Five symptoms and diagnoses are dependent upon the correct subnet mask(s) for the attached network.
Expert Overview's Subnet Objects is dependent upon this configuration, too.



#	IP Net Address	Subnet Mask
1	<ClassA>	255.0.0.0
2	<ClassB>	255.255.0.0
3	<ClassC>	255.255.255.0
4	10.10.10.48	255.255.255.240
5	10.10.10.64	255.255.255.240

Disable RIP if you use other routing protocols on the attached network segment.



Expert UI Object Properties

No traffic analysis (RIP disabled)

Router:

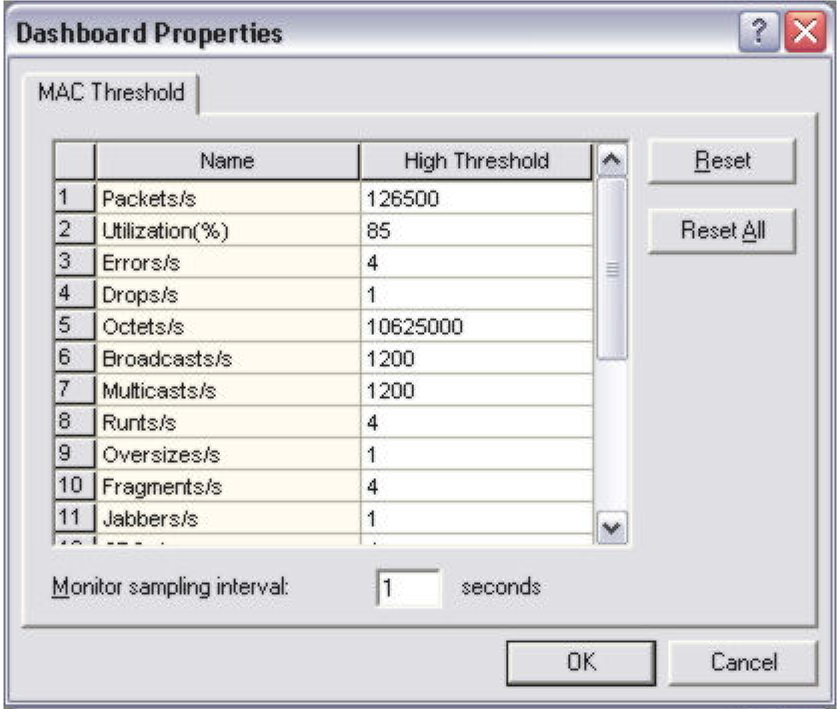
Source	IP Address	MAC Address

Subnet:

Source	IP Subnet Address

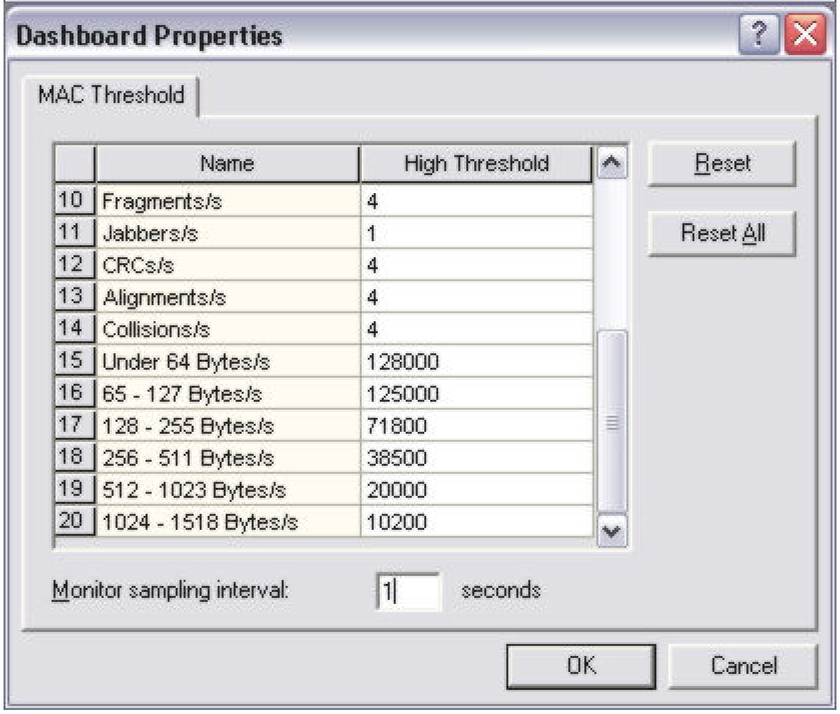
☑ Auto Discover Subnets

Change the Dashboard to suit a 100Mbps switched environment.



	Name	High Threshold
1	Packets/s	126500
2	Utilization(%)	85
3	Errors/s	4
4	Drops/s	1
5	Octets/s	10625000
6	Broadcasts/s	1200
7	Multicasts/s	1200
8	Runts/s	4
9	Oversizes/s	1
10	Fragments/s	4
11	Jabbers/s	1

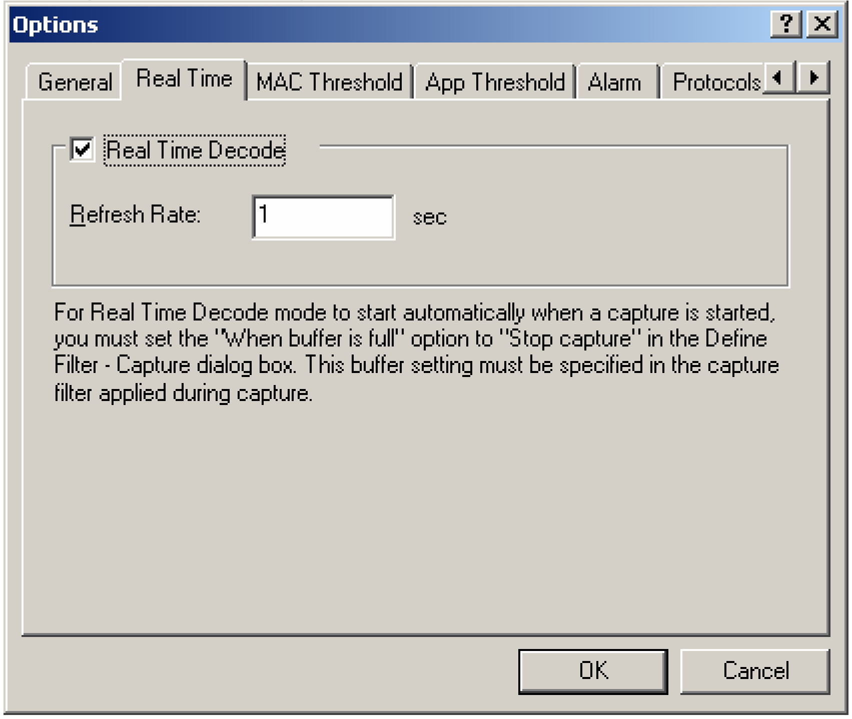
Monitor sampling interval: 1 seconds



	Name	High Threshold
10	Fragments/s	4
11	Jabbers/s	1
12	CRCs/s	4
13	Alignments/s	4
14	Collisions/s	4
15	Under 64 Bytes/s	128000
16	65 - 127 Bytes/s	125000
17	128 - 255 Bytes/s	71800
18	256 - 511 Bytes/s	38500
19	512 - 1023 Bytes/s	20000
20	1024 - 1518 Bytes/s	10200

Monitor sampling interval: 1 seconds

Enable Real Time decodes if you need to see immediately see the results of your network configuration changes, otherwise, disable to save CPU cycles.

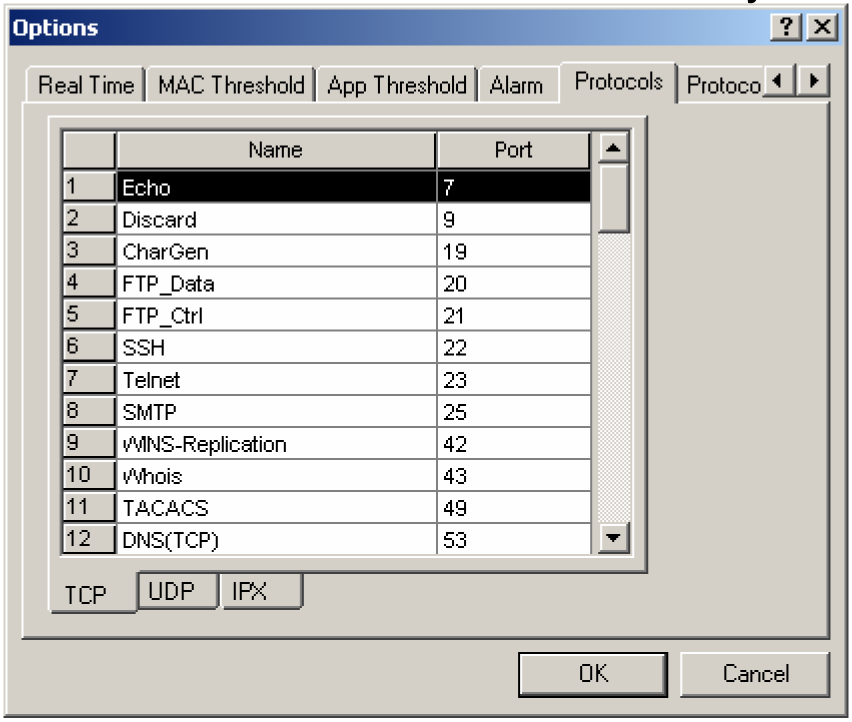


☑ Real Time Decode

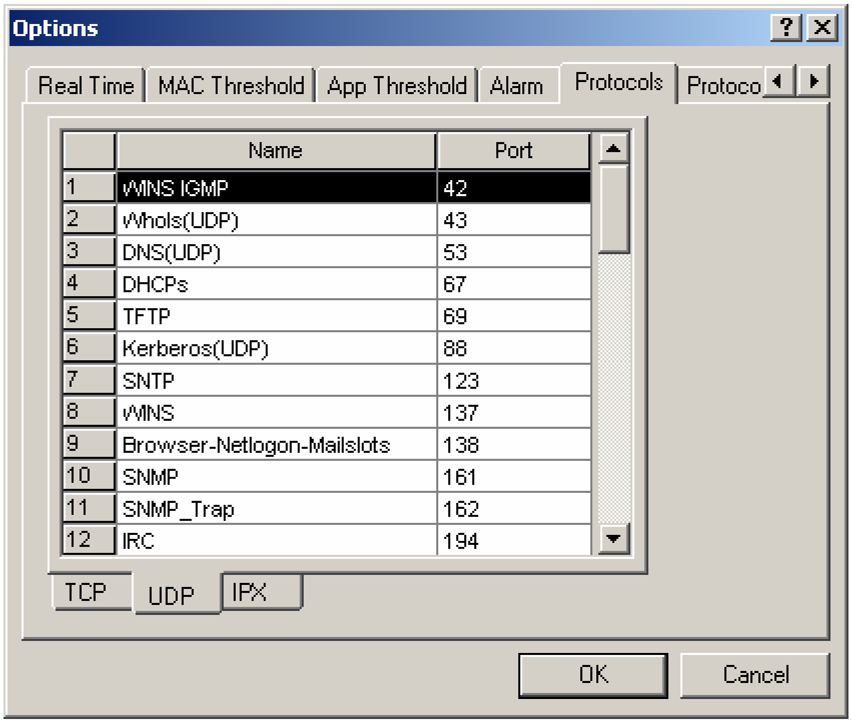
Refresh Rate: 1 sec

For Real Time Decode mode to start automatically when a capture is started, you must set the "When buffer is full" option to "Stop capture" in the Define Filter - Capture dialog box. This buffer setting must be specified in the capture filter applied during capture.

Replace the existing UDP/TCP protocols list with a more comprehensive one using weblink http://www.networkhorizons.com/08-Analyzer_Tweaks/Protocols/Protocols.xls
There is a link to Microsoft for an Excel viewer if you don't have Excel.



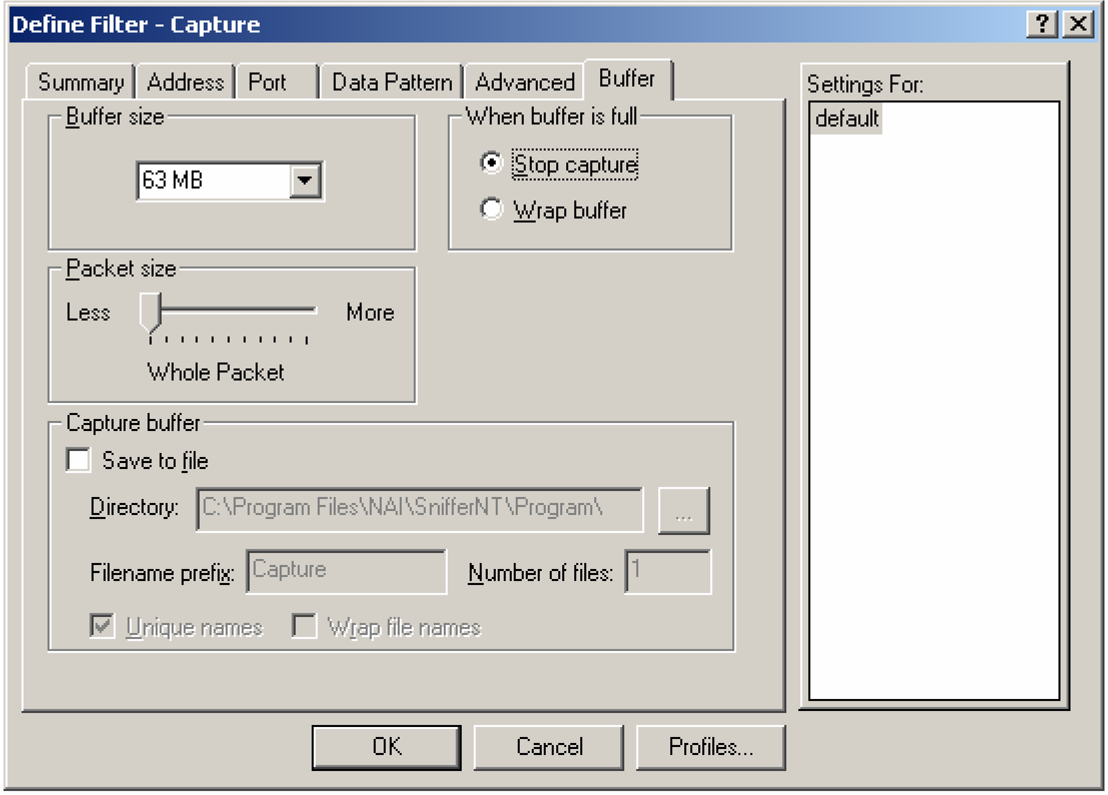
	Name	Port
1	Echo	7
2	Discard	9
3	CharGen	19
4	FTP_Data	20
5	FTP_Ctrl	21
6	SSH	22
7	Telnet	23
8	SMTP	25
9	WINS-Replication	42
10	Whois	43
11	TACACS	49
12	DNS(TCP)	53



	Name	Port
1	WINS IGMP	42
2	WhoIs(UDP)	43
3	DNS(UDP)	53
4	DHCPs	67
5	TFTP	69
6	Kerberos(UDP)	88
7	SNTP	123
8	WINS	137
9	Browser-Netlogon-Mailslots	138
10	SNMP	161
11	SNMP_Trap	162
12	IRC	194

Increase the minimum capture filter *Buffer Size* to 63MB from 8MB (max 384MB. Want more? use Infinistream).

Set *When Buffer is Full* to *Stop Capture* if troubleshooting, set to *Wrap Buffer* if running continuously.



Buffer size: 63 MB

When buffer is full:
● Stop capture
○ Wrap buffer

Packet size: Less — More
Whole Packet

Capture buffer
□ Save to file
Directory: C:\Program Files\NAI\SnifferNT\Program\
Filename prefix: Capture
Number of files: 1
☑ Unique names
□ Wrap file names

Settings For:
default