



TransPort  
Training  
Program

# TT005 – Protocol analyser and Event log

Using the Analyser Trace  
Understanding the Event Log

# Analyser Trace

- TransPort routers have a built in protocol analyser
- Captures both transmitted and received data
- Is able to trace:
  - Serial data, PPP negotiations & PPP frames,
  - Ethernet frames, IP packets, DSL PVC cells,
  - ISDN call setup (D channel), ISDN data (Bearer), X.25,
  - IKE negotiations, IPsec traffic (ESP & IKE Float),
  - Wi-Fi management & Wi-Fi data packets
- Filters can be applied to filter include or exclude specific:
  - MAC addresses, TCP/UDP port numbers,
  - IP protocols, IP addresses,
  - discarded packets, loopback packets

# Analyser Trace

- Trace data is presented in an easy to read format.
- Uses circular logging.
- Oldest trace data is at the top, most recent is at the bottom.
- Trace data can also be viewed and analysed with Wireshark Protocol Analyser©

<https://www.wireshark.org/>



Trace data is compressed and stored in a virtual file named ana.txt, the contents of this file will be cleared if the power is removed from the router.

# Analyser Trace

- To configure the Analyser Trace, browse to ***Management - Analyser > Settings***
- The options displayed will depend on the router hardware and firmware.
- The following slides will cover the most commonly used features.

The CLI configuration of the Analyser Trace uses a combination of:  
'ana 0' commands

And physical or logical interface commands ETH/PPP/TUN/OVPN/Wi-Fi to enable tracing on the required interface.

Configuration from the GUI will automatically configure the interface settings as well as the analyser trace settings.

# Analyser Trace – Configuration

- Maximum packet size (anything larger is truncated)
- Log size (180KB maximum)
- Protocol layers (only required for ISDN/X.25 tracing)
- IKE (IKE negotiations for IPsec VPNs)
- QMI (Qualcomm Management Interface)
- Serial Interfaces (Physical ASY & Virtual for W-WAN)
- Wi-Fi Management & Beacons
- Wi-Fi Data Packets

The maximum size of the pseudo file “ana.txt” that is used to store the captured data packets. Once the maximum size is reached, the oldest captured data packets are overwritten when new packets are captured.

The maximum value is 180Kb, but the data is compressed so more than 180Kb of trace data will be captured.

The checkboxes shown under this heading are used to select the serial interfaces over which packets will be captured and included in the analyser trace. The list of available interfaces will include the physical serial interfaces, internal virtual serial interfaces (if present) and interfaces used by built-in WWAN and/or PSTN modems.

# Analyser Trace – Configuration

- Ethernet Interfaces = Layer 2 tracing on the specified interface  
Captures Ethernet frames with headers & shows VLAN tags
- PPP Interfaces = Layer 2 tracing of PPP negotiations & PPP data  
Can be used to understand why a PPP link fails to establish
- IP Sources = Layer 3 tracing on the specified interface  
Captures IP traffic and headers, shows addressing, port, higher layer protocol, checksums & sequence numbers to name a few.

# Analyser Trace – Configuration

- Filters can be used to make the trace data very specific. On a busy router, the ana.txt file will fill up and overwrite old data very quickly.
- Filters can be used to specify MAC addresses, TCP/UDP port numbers, IP protocol numbers & IP addresses.
- To EXCLUDE traffic, enter the relevant text into the filter box.  
For example, to filter out HTTP traffic (port 80) using TCP/UDP Ports:

A screenshot of a configuration window titled "IP Packet Filters". The window has a white background and a thin border. At the top, the title "IP Packet Filters" is displayed in a blue, sans-serif font. Below the title, the text "TCP/UDP Ports:" is shown in a black, sans-serif font. To the right of this text is a small, rectangular input field with a thin border, containing the number "80".

**IP Packet Filters**

TCP/UDP Ports:

# Analyser Trace – Configuration

- To INCLUDE traffic, enter the relevant text into the filter box prefixed with a tilde symbol ~
- Filtering in exclusively captures the specified traffic, filtering out all but the specified traffic.

To filter in telnet traffic (port 23) and only see this traffic in the trace, using TCP/UDP Ports:



The image shows a configuration window titled "IP Packet Filters". Inside the window, there is a label "TCP/UDP Ports:" followed by a text input field containing the value "~23".

# Analyser Trace – Configuration

Multiple values are comma separated, without spaces.

<b>IP Packet Filters</b>	
TCP/UDP Ports:	<input type="text" value="~22,23,8022,8023"/>

Multiple filters are cumulative.

To filter in telnet & SSH but exclude traffic from the 10.10.10.0/24 subnet:

<b>IP Packet Filters</b>	
TCP/UDP Ports:	<input type="text" value="~22,23"/>
IP Protocols:	<input type="text"/>
IP Addresses:	<input type="text" value="10.10.10.0/24"/>

# Analyser Trace – Configuration

- MAC addresses are specified in HEX with OS specific separators (such as : or -) removed.

00-05-9A-3C-7A-00 becomes 00059A3C7A00

## Ethernet Packet Filters

MAC Addresses:

- MAC addresses can be wild-carded by shortening the HEX  
To specify only network interface cards with the same OUI of 00059A

## Ethernet Packet Filters

MAC Addresses:

# Analyser Trace – Configuration

Know the relevant commonly used Well Known Port Numbers:

- 20 FTP – Data
- 21 FTP – Control
- 22 SSH Remote Login Protocol
- 23 Telnet
- 25 Simple Mail Transfer Protocol (SMTP)
- 53 Domain Name System (DNS)
- 69 Trivial File Transfer Protocol (TFTP)
- 80 HTTP
- 123 Time service
- 110 POP3
- 161 SNMP
- 179 Border Gateway Protocol (BGP)
- 443 HTTPS

# Analyser Trace – Configuration

Know the relevant commonly used Well Known Protocol Numbers:

- 1 ICMP
- 4 IPv4
- 6 TCP
- 17 UDP
- 47 GRE
- 50 ESP (IPsec)
- 51 AH (IPsec)
- 108 IP payload compression
- 112 VRRP
- 115 L2TP

# Analyser Trace – Trace Output

- The trace data in text format is viewed from  
***Management - Analyser > Trace***
- Wireshark PCAP files are downloaded by clicking the  
hyperlinks shown in  
***Management - Analyser > PCAP (e.g. Wireshark) traces***  
The traces are IP, Ethernet, PPP & Wi-Fi

# Tracing PPP Negotiations

## Local to Remote

```
----- 19-8-2014 14:27:06.020 -----  
FF 03 C0 21 01 00 00 12 01 04 05 DC 02 06 00 00 ...!.....  
00 00 07 02 08 02 .....
```

### PPP 1 From LOC TO REM

```
FF 03      ADD/CTL  
C0 21      Protocol:    LCP  
01         Code:        CFG REQ  
00         ID:          0  
00 12      Len:         18  
Options:  
01         MRU          05 DC  
02         ACCM         00 00 00 00  
07         PFC  
08         ACFC  
-----
```

## Remote to Local

```
----- 19-8-2014 14:27:06.690 -----  
FF 03 C0 21 01 EF 00 13 01 04 05 D4 03 05 C2 23 ...!.....#  
05 05 06 1C 64 F7 3D .....d.=
```

### PPP 1 From REM TO LOC

```
FF 03      ADD/CTL  
C0 21      Protocol:    LCP  
01         Code:        CFG REQ  
EF         ID:          239  
00 13      Len:         19  
Options:  
01         MRU          05 D4  
03         Authentication C2 23 05  
05         Magic Number 1C 64 F7 3D  
-----
```

# Tracing PPP Negotiations

## Local to Remote

```
----- 19-8-2014 14:27:06.690 -----
FF 03 C0 21 02 EF 00 13 01 04 05 D4 03 05 C2 23 ...!.....#
05 05 06 1C 64 F7 3D .....d.=
```

### PPP 1 From LOC TO REM

```
FF 03      ADD/CTL
C0 21      Protocol:    LCP
02         Code:        CFG ACK
EF         ID:          239
00 13      Len:         19
Options:
01         MRU          05 D4
03         Authentication C2 23 05
05         Magic Number 1C 64 F7 3D
-----
```

## Remote to Local

```
----- 19-8-2014 14:27:06.690 -----
FF 03 C0 21 04 00 00 0E 02 06 00 00 00 07 02 ...!.....
08 02 ..
```

### PPP 1 From REM TO LOC

```
FF 03      ADD/CTL
C0 21      Protocol:    LCP
04         Code:        CFG REJ
00         ID:          0
00 0E      Len:         14
Options:
02         ACCM         00 00 00 00
07         PFC
08         ACFC
-----
```

# Tracing Ethernet Frames - ARP

## Local to Remote

## Remote to Local

```

----- 19-8-2014 15:58:33.920 -----
FF FF FF FF FF 00 04 2D 04 87 CE 08 06 00 01 .....
08 00 06 04 00 01 00 04 2D 04 87 CE C0 A8 00 04 .....
00 00 00 00 00 00 C0 A8 00 01 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

```

ETH From LOC TO REM          IFACE: ETH 0
FF FF FF FF FF FF Dst. MAC
00 04 2D 04 87 CE Src. MAC
08 06 Type: ARP
ARP:
00 01 HW Type: Ethernet (1)
08 00 Prot Type: IP (2048)
06 HW Size: 6
04 Prot Size: 4
00 01 Opcode: Request (1)
00 04 2D 04 87 CE Src. MAC
C0 A8 00 04 Src IP: 192.168.0.4
00 00 00 00 00 00 Dst. MAC
C0 A8 00 01 Dst IP: 192.168.0.1
-----

```

```

----- 19-8-2014 15:58:33.920 -----
00 04 2D 04 87 CE 00 1D 70 CE 81 F3 08 06 00 01 ..-...p.....
08 00 06 04 00 02 00 1D 70 CE 81 F3 C0 A8 00 01 .....p.....
00 04 2D 04 87 CE C0 A8 00 04 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

```

ETH From REM TO LOC          IFACE: ETH 0
00 04 2D 04 87 CE Dst. MAC
00 1D 70 CE 81 F3 Src. MAC
08 06 Type: ARP
ARP:
00 01 HW Type: Ethernet (1)
08 00 Prot Type: IP (2048)
06 HW Size: 6
04 Prot Size: 4
00 02 Opcode: Reply (2)
00 1D 70 CE 81 F3 Src. MAC
C0 A8 00 01 Src IP: 192.168.0.1
00 04 2D 04 87 CE Dst. MAC
C0 A8 00 04 Dst IP: 192.168.0.4
-----

```

# Tracing IP Packets – Telnet setup

```
----- 19-8-2014 16:07:01.700 -----
45 00 00 34 07 0C 40 00 00 06 72 5E C0 A8 00 05
C0 A8 00 04 EF 10 00 17 18 A2 72 BA 00 00 00 00
80 02 20 00 53 38 00 00 02 04 05 04 01 03 03 02
01 01 04 02
```

```
E..A.:@...P^.....
.....f.....
...58.....
.....
```

```
IP (In) From REM TO LOC          IFACE: ETH 0
45          IP Ver: 4
          Hdr Len: 20
          TOS: Routine
          Delay: Normal
          Throughput: Normal
          Reliability: Normal
00 34      Length: 52
07 0C      ID: 1804
40 00      Frag Offset: 0
          Congestion: Normal
          Don't Fragment
          Last Fragment
80          TTL: 128
06          Proto: TCP
72 5E      Checksum: 29278
C0 A8 00 05 Src IP: 192.168.0.5
C0 A8 00 04 Dst IP: 192.168.0.4
TCP:
EF 10      SRC Port: ??? (61200)
00 17      DST Port: TELNET (23)
18 A2 72 BA SEQ Number: 413299386
00 00 00 00 ACK Number: 0
80 02      Flags
          Data Offset 32
          SYN
20 00      Window: 8192
53 38      Checksum: 21304
00 00      URG Ptr: 0
02          TCP_OPT: MSS (1460)
01          TCP_OPT: NOOP
03          TCP_OPT: ??? (3)
01          TCP_OPT: NOOP
01          TCP_OPT: NOOP
04          TCP_OPT: ??? (4)
```

## Remote to Local

```
----- 19-8-2014 16:07:01.700 -----
45 00 00 2C 08 8C 00 00 FA 06 36 E6 C0 A8 00 04
C0 A8 00 05 00 17 EF 10 04 8F BE 81 18 A2 72 8B
60 12 20 00 B9 62 00 00 02 04 05 78
```

```
E.....6.....
.....f.....
...b.....x
```

```
IP (Final) From LOC TO REM          IFACE: ETH 0
45          IP Ver: 4
          Hdr Len: 20
          TOS: Routine
          Delay: Normal
          Throughput: Normal
          Reliability: Normal
00 2C      Length: 44
08 8C      ID: 2188
00 00      Frag Offset: 0
          Congestion: Normal
          May Fragment
          Last Fragment
FA          TTL: 250
06          Proto: TCP
36 E6      Checksum: 14054
C0 A8 00 04 Src IP: 192.168.0.4
C0 A8 00 05 Dst IP: 192.168.0.5
TCP:
00 17      SRC Port: TELNET (23)
EF 10      DST Port: ??? (61200)
04 8F BE 81 SEQ Number: 76529281
18 A2 72 8B ACK Number: 413299387
60 12      Flags
          Data Offset 24
          SYN
          ACK
20 00      Window: 8192
B9 62      Checksum: 47458
00 00      URG Ptr: 0
02          TCP_OPT: MSS (1400)
```

## Local to Remote

# Tracing IP Packets – Telnet, TCP 3 Way Handshake

```
----- 19-8-2014 16:07:01.700 -----
45 00 00 28 07 00 40 00 80 06 72 69 C0 A8 00 05  E..(.@...rI...
C0 A8 00 04 EF 10 00 17 18 A2 72 BB 04 8F BE 82  .....P.....
50 10 FB 90 F5 52 00 00 00 00 00 00 00 00 00  P....R.....
```

```
IP (In) From REM TO LOC      IFACE: ETH 0
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:            Normal
          Throughput:       Normal
          Reliability:      Normal
00 28       Length:         40
07 00       ID:            1885
40 00       Frag Offset:   0
          Congestion:      Normal
          Don't Fragment
          Last Fragment
80          TTL:           128
06          Proto:         TCP
72 69       Checksum:      29289
C0 A8 00 05 Src IP:        192.168.0.5
C0 A8 00 04 Dst IP:        192.168.0.4
TCP:
EF 10       SRC Port:      ??? (61200)
00 17       DST Port:      TELNET (23)
18 A2 72 BB SEQ Number:   413299387
04 8F BE 82 ACK Number:   76529282
50 10       Flags
          Data Offset      20
          ACK
FB 90       Window:        64400
F5 52       Checksum:      62802
00 00       URG Ptr:       0
-----
```

Remote to Local

```
----- 19-8-2014 16:07:01.710 -----
45 00 00 4A 08 8E 00 00 FA 06 36 C0 A8 00 04  E..J.....6....
C0 A8 00 05 00 17 EF 10 04 8F BE 93 18 A2 72 BB  .....P.....
50 18 20 00 68 5A 00 00 00 00 0A 52 05 6D 6F 74 65  P..kZ....Remote
20 43 6F 6E 6E 65 63 74 69 6F 6E 2E 0D 0A 00 0A  Connection.....
55 73 65 72 6E 61 6D 65 3A 20  Username:
```

```
IP (Final) From LOC TO REM      IFACE: ETH 0
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:            Normal
          Throughput:       Normal
          Reliability:      Normal
00 4A       Length:         74
08 8E       ID:            2190
00 00       Frag Offset:   0
          Congestion:      Normal
          May Fragment
          Last Fragment
FA          TTL:           250
06          Proto:         TCP
36 C6       Checksum:      14022
C0 A8 00 04 Src IP:        192.168.0.4
C0 A8 00 05 Dst IP:        192.168.0.5
TCP:
00 17       SRC Port:      TELNET (23)
EF 10       DST Port:      ??? (61200)
04 8F BE 93 SEQ Number:   76529299
18 A2 72 BB ACK Number:   413299387
50 18       Flags
          Data Offset      20
          PSH
          ACK
20 00       Window:        8192
6B 5A       Checksum:      27482
00 00       URG Ptr:       0
```

Local to Remote

# Extended logging

- The Analyser Trace can be written to a USB flash drive for capturing data over an extended time frame.
- A secondary log file is created on U:
- CLI based configuration only:  
ana 0 logdrive u  
ana 0 logfile big\_ana.txt  
ana 0 logsizek 102400

# Hands-On Practical Session - Analyser

- Using the Analyser Trace...
- Enable the Analyser Trace, set the capture log size to its maximum value.
- Enable IP tracing on the Ethernet interface connected to the LAN and the PPP WAN interface.
- Send some data through the router, browse a web page & review the trace data.
- Try and find the DNS lookups.

# Hands-On Practical Session - Analyser

- Configure the trace so it only captures DNS lookups. We need to capture the request from the PC to router and router to DNS server along with the reply packets.
- Do a DNS lookup from your PC using the router as the DNS server.

You can use the Windows 'nslookup' command

```
nslookup <host> <DNS_server>
```

```
nslookup www.bbc.co.uk 192.168.1.1
```

# Hands-On Practical Session - Analyser

- Download the relevant Wireshark PCAP file
- Review the trace data in WireShark

The screenshot shows the Wireshark interface with a PCAP file named 'dfdfdf.pcap'. The main pane displays a list of network packets. The selected packet (No. 6) is a DNS Standard query response from 62.24.134.2 to 92.11.2.226. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	92.11.2.226	62.24.134.2	DNS	59	Standard query request 0xad21 A www.bbc.co.uk
2	0.030000	62.24.134.2	92.11.2.226	DNS	117	Standard query response 0xad21 A www.bbc.co.uk: type A, class IN
3	0.030000	62.24.134.2	92.11.2.226	DNS	117	Standard query request 0xad21 A www.bbc.co.uk
4	0.040000	92.11.2.226	62.24.134.2	DNS	59	Standard query request 0xad21 A www.bbc.co.uk
5	0.070000	62.24.134.2	92.11.2.226	DNS	136	Standard query response 0xad21 A www.bbc.co.uk: type CNAME, class IN, cname www.bbc.net.uk
6	0.070000	62.24.134.2	92.11.2.226	DNS	136	Standard query response 0xad21 A www.bbc.co.uk: type A, class IN, addr 212.58.246.94

The packet details pane for the selected packet (No. 6) shows the following information:

- Queries
  - www.bbc.co.uk: type A, class IN
- Answers
  - www.bbc.co.uk: type CNAME, class IN, cname www.bbc.net.uk
    - Name: www.bbc.co.uk
    - Type: CNAME (Canonical NAME for an alias) (5)
    - Class: IN (0x0001)
    - Time to live: 65
    - Data length: 14
    - CNAME: www.bbc.net.uk
  - www.bbc.net.uk: type A, class IN, addr 212.58.246.94
  - www.bbc.net.uk: type A, class IN, addr 212.58.246.95

# End of Hands-On Practical Session

# The Event Log

- The **event log** (eventlog.txt) is a file containing system events.
- Uses circular logging.
- Newest events are at the top, oldest at the bottom.
- Is stored in battery backed RAM and retained if power is removed.
  
- WR21 has no NVRAM so clears the event log if the power is disconnected but retains the information if rebooted.

# The Event Log

- Each line in the event log contains:
  - Time of the event based on system time
  - Date of the event based on system date
  - Brief description of the event
- Extra information for some events may also include:
  - The interface that generated the event
  - The protocol that generated the event
  - Source and destination IP address
  - The user who triggered the event
  - A phone number (ISDN, PSTN, SMS)

# The Event Log

**Management - Event Log**

```
14:21:37, 13 Dec 2010,Time set/changed OK
14:21:37, 13 Dec 2010,Par change by username, sntp 0 server to
14:21:37, 13 Dec 2010,Time set/changed OK
14:21:39, 13 Dec 2010,SNTP Client,Retries Exceeded
14:20:59, 13 Dec 2010,SNTP Client,Time Set Request
14:20:41, 13 Dec 2010,SNTP Client,Retries Exceeded
14:20:01, 13 Dec 2010,SNTP Client,Time Set Request
14:19:53, 13 Dec 2010,SNTP Client,Retries Exceeded
14:19:13, 13 Dec 2010,SNTP Client,Time Set Request
14:18:57, 13 Dec 2010,WEB Login OK by username lvl 0
14:18:38, 13 Dec 2010,GP socket connected: 10.1.47.30:771 -> 10.1.3.13:59927
14:18:37, 13 Dec 2010,Wi-Fi 0 Access Point up
14:18:34, 13 Dec 2010,USB-2 device 1 connected: EHCI root hub
14:18:34, 13 Dec 2010,USB-1 device 1 connected: EHCI root hub
14:18:32, 13 Dec 2010,ETH 19 up
14:18:32, 13 Dec 2010,ETH 18 up
14:18:32, 13 Dec 2010,ETH 17 up
14:18:32, 13 Dec 2010,ETH 16 up
14:18:32, 13 Dec 2010,ETH 15 up
14:18:32, 13 Dec 2010,ETH 14 up
14:18:32, 13 Dec 2010,ETH 13 up
14:18:32, 13 Dec 2010,ETH 12 up
14:18:32, 13 Dec 2010,ETH 11 up
14:18:32, 13 Dec 2010,ETH 10 up
```

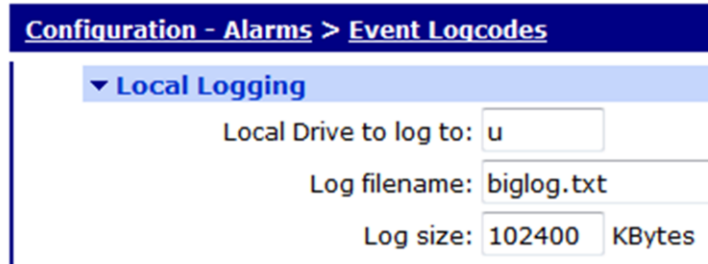
Copyright © Digi International, Inc. All rights reserved.

# The Event Log

- The event log can be obtained in various ways:
- GUI: Management - Event Log
- CLI: type eventlog.txt
- FTP: download the eventlog.txt from the router
- Debug.txt: The event log is part of the debug.txt file.

# Extended logging

- The event log can be written to a USB flash drive for logging events over an extended time frame.
- A secondary log file is created on U:



The screenshot shows a web-based configuration interface. At the top, there is a dark blue header with the text "Configuration - Alarms > Event Logcodes". Below this, a light blue section titled "Local Logging" is expanded. It contains three input fields: "Local Drive to log to:" with the value "u", "Log filename:" with the value "biglog.txt", and "Log size:" with the value "102400" and "KBytes" next to it.

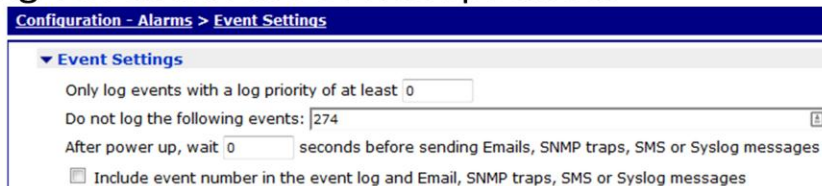
CLI based configuration:  
event 0 logdrive u  
event 0 logfile biglog.txt  
event 0 logsizek 102400

# Event Triggered Alerting

- Events can be used to trigger alerts.
- Alerts can be one of or a combination of:
  - Email notification
  - SNMP trap
  - SMS
  - Syslog message
- Alerts can be restricted to a specific Entity/Number
- Email alerts can have the event log and/or analyser trace attached. Other files from the router can be specified too.

# The Event Log Configuration

- Configured from **Configuration - Alarms > Event Settings**
- Unwanted events can be filtered out.
- To INCLUDE events, enter the relevant text into the filter box prefixed with a tilde symbol ~
- Filtering in exclusively captures the specified events, filtering out all but the events specified.



The screenshot shows a web interface for configuring event settings. At the top, there is a breadcrumb trail: "Configuration - Alarms > Event Settings". Below this, a section titled "Event Settings" is expanded. It contains several configuration options: "Only log events with a log priority of at least 0" with a text input field containing "0"; "Do not log the following events: 274" with a text input field containing "274" and a small square icon to its right; "After power up, wait 0 seconds before sending Emails, SNMP traps, SMS or Syslog messages" with a text input field containing "0"; and a checkbox labeled "Include event number in the event log and Email, SNMP traps, SMS or Syslog messages" which is currently unchecked.

Log priority:

0 = show all events

1 – 9 = 1 most important, 9 least important.

Entering 5 would display events with priority 0-5

The event filtered out here is:

274Wi-Fi client %a probing %c

A delay can be added so if the router reboots, it will wait until connectivity is established before sending an alert.

Including event numbers can be included in the event log view, but in the majority of cases these are not required.

# Logcodes.txt

- The event log relies on the presence of the logcodes.txt to make the output readable and easy to understand.
- Contains a list of:
  - Event numbers, descriptive text and associated variables
  - Reason numbers, descriptive text and associated variables
  - Event priority numbers and reason priority number, where applicable. 0 – 9 where 0 is most important and 9 is least important.

## [EVENTS]

01,0,Power-up[%c]

## [REASONS]

1,,Reboot command

2,,Reboot command via web

# Logcodes.txt

- Without the logcodes.txt, the event log looks like this:

Management - Event Log						
11:32:41,	20	Aug	2014,	Code:240,	Reason:0,	Com:,Ent:Wi-Fi,Add:0,Sapi:0
11:32:40,	20	Aug	2014,	Code:5,	Reason:3,	Com:,Ent:PPP,Add:1,Sapi:0
11:32:39,	20	Aug	2014,	Code:7,	Reason:0,	Com:username,Ent:WEB,Add:0,Sapi:0
11:32:38,	20	Aug	2014,	Code:60,	Reason:1,	Com:,Ent:TCP,Add:0,Sapi:0
11:32:38,	20	Aug	2014,	Code:148,	Reason:1,	Com:,Ent:ETH,Add:0,Sapi:0
11:32:38,	20	Aug	2014,	Code:4,	Reason:0,	Com:,Ent:ETH,Add:2,Sapi:0
11:32:38,	20	Aug	2014,	Code:4,	Reason:0,	Com:,Ent:ETH,Add:1,Sapi:0
11:32:38,	20	Aug	2014,	Code:4,	Reason:0,	Com:,Ent:ETH,Add:0,Sapi:0
11:32:37,	20	Aug	2014,	Code:189,	Reason:0,	Com:802.11 n WLAN,Ent:USBHOST,Add:3,Sapi:2
11:32:36,	20	Aug	2014,	Code:189,	Reason:0,	Com:EHCI root hub,Ent:USBHOST,Add:3,Sapi:1
11:32:36,	20	Aug	2014,	Code:189,	Reason:0,	Com:EHCI root hub,Ent:USBHOST,Add:2,Sapi:1
11:32:36,	20	Aug	2014,	Code:189,	Reason:0,	Com:EHCI root hub,Ent:USBHOST,Add:1,Sapi:1
11:32:36,	20	Aug	2014,	Code:58,	Reason:1,	Com:,Ent:TCP,Add:0,Sapi:0
11:32:36,	20	Aug	2014,	Code:147,	Reason:1,	Com:,Ent:ETH,Add:0,Sapi:0
11:32:36,	20	Aug	2014,	Code:256,	Reason:0,	Com:,Ent:FWCTRL,Add:0,Sapi:0
11:32:35,	20	Aug	2014,	Code:1,	Reason:2,	Com:,Ent:DEBLOG,Add:0,Sapi:0
11:32:35,	20	Aug	2014,	Code:144,	Reason:0,	Com:(not present),Ent:DEBLOG,Add:0,Sapi:1
11:32:35,	20	Aug	2014,	Code:70,	Reason:0,	Com:,Ent:DEBLOG,Add:0,Sapi:0
11:32:30,	20	Aug	2014,	Code:3,	Reason:0,	Com:,Ent:CMD,Add:0,Sapi:0
11:32:30,	20	Aug	2014,	Code:5,	Reason:3,	Com:,Ent:PPP,Add:1,Sapi:0
11:32:35,	20	Aug	2014,	Code:5,	Reason:3,	Com:,Ent:PPP,Add:1,Sapi:0
11:32:25,	20	Aug	2014,	Code:5,	Reason:3,	Com:,Ent:PPP,Add:1,Sapi:0
11:32:25,	20	Aug	2014,	Code:16,	Reason:1,	Com:,Ent:PPP,Add:0,Sapi:0
11:32:22,	20	Aug	2014,	Code:7,	Reason:0,	Com:username,Ent:WEB,Add:0,Sapi:0
11:32:15,	20	Aug	2014,	Code:5,	Reason:3,	Com:,Ent:PPP,Add:1,Sapi:0
11:32:05,	20	Aug	2014,	Code:5,	Reason:3,	Com:,Ent:PPP,Add:1,Sapi:0

Refresh

Clear Log

Open in New Window

# Modifying Logcodes.txt

- Browse to **Configuration - Alarms > Event Logcodes**

Configuration - Alarms > Event Logcodes

Event Settings

Event Logcodes

The logcodes describe the logged events. It is possible to configure each event / reason with a specific priority which can be used to control when that event / reason causes an alarm to be created.

Event Description	Filter	Event Priority	Reasons	Reason Priority
			1 <a href="#">Reboot command</a>	
			2 <a href="#">Reboot command via web</a>	
			3 <a href="#">Message shortage reboot</a>	
			4 <a href="#">Buffer shortage reboot</a>	
			5 <a href="#">Buffers excessive</a>	
			6 <a href="#">MsgLog</a>	
			7 <a href="#">High CPU usage</a>	
			8 <a href="#">Locked task %c</a>	
			9 <a href="#">Watchdog timeout</a>	
			10 <a href="#">Reboot command via iDigi Server</a>	
			11 <a href="#">Python script watchdog</a>	
			12 <a href="#">ESPAD request</a>	
			13 <a href="#">ASY transmit watchdog</a>	
			14 <a href="#">Device Cloud SMS command</a>	
			15 <a href="#">Power failure</a>	
1 <a href="#">Power-up[%c]</a>				
2 <a href="#">Clear Event Log</a>		1		

Review the information on the slide and point out the:

Event Number

Event Description

Event Priority

Reason Number

Reason Description

Reason Priority column (configured reason priorities will show here)

The Filter column will display 'On' if the event is filtered out. Shown in next slide.

# Modifying Logcodes.txt

- Click on the 'Event' or 'Reason' to modify.
- The 'Alarm Priority' is used for alerting.
- The 'Log Priority' is used to include or exclude events from the event log.

Configuration - Alarms > Event Logcodes

Event Settings

Event Logcodes

Event: Clear Event Log

Do not log this event

Log Priority: 0

Alarm Priority: 1

Alarm Priority is dependent on the event being logged by Entity   All  instance 0

Priority only applies to

PPP 0  PPP 1  PPP 2  PPP 3  
 PPP 4  PPP 5  PPP 6  PPP 7

Store a snapshot of the Traffic Analyser trace on the log drive  
If this event creates an Email alarm

Attach a snapshot of the Traffic Analyser trace  
After this event:  Leave the Analyser trace  
 Freeze the Analyser trace  
 Delete the Analyser trace

Attach a snapshot of the Event Log  
After this event:  Leave the Event Log  
 Delete the Event Log

Attachment List ID: 0

If this event creates a Syslog alarm, use

Syslog Priority: Info  
Syslog Facility: User

Apply

It's the alarm priority that is the important one.

The alarm priority is used in conjunction with (for example) "Send an email notification when the event priority is at least".

The Log priority allows you to include or exclude events from the event log and is rarely if ever changed from default.

The log priority is used in conjunction with *Configuration - Alarms > Event Settings > Email Notifications > Only log events with a log priority of at least xx.*

The default value of 0 means all events will be included (or logged) in the event log.

Draw attention to the options to attach the event log and analyser trace.

Mention the Attachment List ID and to specify the file list at the bottom of the previous page (main logcodes window). File names are comma separated.

# Saving Log Codes Changes

- After making a change, click Apply, then 'Save All Event Code Changes'.
- Changes are saved to the file **logcodes.dif**

Configuration - Alarms > Event Logcodes

[Save All Event Code Changes](#)

The logcodes describe the logged events. It is possible to configure each event / reason with a specific priority which can be used to control when that event / reason causes an alarm to be created.

Event Description	Filter	Event Priority	Reasons	Reason Priority
			1 <a href="#">Reboot command</a>	
			2 <a href="#">Reboot command via web</a>	
			3 <a href="#">Message shortage reboot</a>	
			4 <a href="#">Buffer shortage reboot</a>	
			5 <a href="#">Buffers excessive</a>	
			6 <a href="#">MsgLog</a>	
			7 <a href="#">High CPU usage</a>	
			8 <a href="#">Locked task %c</a>	
			9 <a href="#">Watchdog timeout</a>	
			10 <a href="#">Reboot command via iDigi Server</a>	
			11 <a href="#">Python script watchdog</a>	
			12 <a href="#">ESPAD request</a>	
			13 <a href="#">ASY transmit watchdog</a>	
			14 <a href="#">Device Cloud SMS command</a>	
			15 <a href="#">Power failure</a>	
1 <a href="#">Power-up[%c]</a>		5		

At boot up the logcodes.txt and logcodes.dif are merged to create the modified view of the log codes.

# Sending Email Alerts

- Email alerts can be sent, but extra configuration is required.
- See 'QN01 - Configure a Sarian or Digi Transport router to send an automatic email on a specific event' more information.

Configuration - Alarms > Event Settings

▼ Event Settings

Only log events with a log priority of at least

Do not log the following events:

After power up, wait  seconds before sending Emails, SNMP traps, SMS or Syslog messages

Include event number in the event log and Email, SNMP traps, SMS or Syslog messages

▼ Email Notifications

Send email notifications

Send an email notification when the alarm priority is at least

Send a maximum of  emails per day

**0 emails have been sent today**

Use email template file

Email To:

Email From:

Email Subject:

In order to send email notifications, a SMTP account must be configured.

Also see:

QN34: Configuring Syslog alerting on a TransPort router

QN35: Configuring SMS Alerts on a Transport Router

QN36: Configuring SNMP Traps on a Transport Router

# Sending Email Alerts

## Configuration - Alarms > SMTP Account

### SMTP Account

Hostname or IP address of your SMTP Server:  Port

Username:

Password:

Confirm password:

Display "Email From" as:

Attachment size limit:

If the email template does not contain one, use "Reply To" address:

Route using:  Routing table  
 Interface

Resend the email after  seconds if the first attempt fails

# Hands-On Practical Session – Event Log

- View the logcodes.txt from the CLI
- Experiment with the filtering options to include and exclude events from the Event Log.
- Modify an Event Logcode in the GUI, save the change and review the file logcodes.dif
- If time allows, configure Email, Syslog or SMS alerting

Also see:

QN34: Configuring Syslog alerting on a TransPort router

QN35: Configuring SMS Alerts on a Transport Router

QN36: Configuring SNMP Traps on a Transport Router

# End of Hands-On Practical Session