|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range Value | Description | Example |
| 1. | Interface Type | 1,2,3 | 1-File, 2- Local network adapter, 3- Network adapter on remote machine. | 2 |
| 2. | Snaplen | 1-65535 | Snaplen is the amount of data captured by each frame. The Snaplen ranges from 0-65535. | 65535 |
| 3. | Time out | 0001-Infinity | The time to wait for a packet at an interface. It is in milliseconds | 2000 |
| 4. | Promiscuous Mode | y/n | Promiscuous Mode.  Promiscuous mode(y) - captures all the traffic frames that pass through the given interface. The no option (n) Captures only frames that are sent and received by that interface | y |
| 5. | Count | 0-Infinity | Count –No of frames to be captured. Ranges from 0 to ∞. | 0 |
| 6. | Format | Hex/Dec | The display format for captured frames | hexadecimal |
| 7. | Callback function | TclScript | A Tcl Script that will be called on packet capture event. Applicable only for “loop” option | puts “%H %D” |
| 8. | Filter | WinPcap capture | Capture Filter. This is same as WinPcap capture filter. | “tcp | icmp” |
| 9. | Dump File | Dump File or capture file | The file where the capture frames are to be stored on “loop” option | tcap0DumpFile |
| 10. | Device ID | Local or remote machine. | Adapter Identification | \Device\NPF\_{A6EEB94A-2E91-4F4F-AAEB-1A39BEC3BF0F} |
| 11. | Local IP or Remote IP | Local IP or Remote IP | Adapter’s IPv4 address. | 192.168.1.8 |
| 12. | Subnet Mask | IP Net mask | Subnet Mask of the adapter | 255.255.255.0 |
| 13. | Sample Method | |  |  | | --- | --- | | 0,1,2 |  | |  |  | |  |  | |  |  | |  |  | |  |  | | Sample method is applied after the filtering packets for identifying the subset of the packets captured.  0-defines no sampling  1-defines one packet is returned out of N packets.  2- Defines 1 packets is returned to the user after N milli second | 0 |
| 15. | Remote Interface Number | Interface Number (Integer) | Remote Interface Number | 3 |
| 16. | Remote Host Name | Name of the host machine | Name of the remote host | Haris-HP |
| 17. | Remote Port Number | Port Number | Port number of “rpcapd” on remote host | 3000 |

Tcap list

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1. | Device ID | Device ID String | Device ID of local or remote machine | rpcap://\Device\NPF\_{A6EEB94A-2E91-4F4F-AAEB-1A39BEC3BF0F} |
| 2. | Device Manufacturer | Vendor of Network adaptor | Name of the device manufacturer | Realtek interface controller. |
| 3. | IP address and Subnet Mask | IP Address and Net mask | IP address and subnet mask of local or remote machine | 192.168.1.13 255.255.255.0 |

Tcap Stats

Capture Statistics

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1. | Packets Received | 0-Infinity | The first element is number of packets received. | 1389 |
| 2. | Packets Dropped | 0-Infinity | The second element is packets dropped due to insufficient buffer size. | 0 |
| 3. | Packets dropped (Adaptor) | 0-Infinity | Third element is number of packets dropped by the adaptor. | 15205120 |

Tcap version

Tcap version

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1 | Versions of Tcl | Null | version of Tcl shell, | {Tcl 8.5} |
| 2 | WinPcap Library | Null | Version of WinPcap built | {WinPcap version 4.1.3 (pac)} |
| 3 | Tcap Version | Null | Tcap version | {Tcap 1.2} |

Tcap capture

Tcap capture <handle >

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1 | Header | Frame Header | Time stamp in HH:MM:SS | 19:19:16 |
| Micro Secs | 034532 |
| Length of packets on wire | 1494 |
| Length of packets presented | 1494 |
| 2. | Data | Hexadecimal or decimal String. | Frame data represented by hexadecimal or decimal. | {00 1e 65 5d 6e 96 e8 de 27 67 8a 5a 08 00 45 00 05 c8 3b fe 40 00 79} |

Tcap loop

Tcap loop <handle>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1 | Header | Frame Header | Time stamp in HH:MM:SS | 18:17:16 |
| Micro Secs | 034532 |
| Length of packets on wire | 3321 |
| Length of packets presented | 3321 |
| 2. | Data | Hexadecimal or decimal | Frame data represented by hexadecimal or decimal. | {00 1f 66 5d 6e 96 e8 de 27 67 8a 5a 08 00 45 00 05 c9 3b ff 40 09 79} |

Tcap opening handle on remote machine

Tcap open -host <rpcapd server host> [-port <server port>]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1 | Tcap Handle | tcap0 – tcap10 | Handle for capturing frames remote network adapter | tcap open –ho … |

Tcap handle creating using interface Id.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1 | Interface ID | 0-10 | Handle is opened by using interface Identity of local or remote machine | Tcap open –id \Device\NPF\_{A6EEB94A-2E91-4F4F-AAEB-1A39BEC3BF0F} |

Tcap handle using interface number

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1 | Interface number | 1,2,3 | Handle is creating using interface number 1, 2, 3.  1 –for wifi  2-ethernet  3-bluetooth | Tcap open –if 1 |

Tcap open handle with ipv6 address

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Name | Range | Description | Example |
| 1 | IPv6 address | 128 bit Alpha numeric value. | Handle is created using ipv6 | Tcap open –i6 fe80::714a:2760:dcdc:c97a%11 |