Tranalyzer2

basicFlow

Overall Flow Information

Tranalyzer Development Team

Contents

1 basicFlow

1.1 Description

The basicFlow plugin provides host identification fields and timing information.

1.2 Configuration Flags

1.2.1 basicFlow.h

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
`BFO_SENSORID`	0	Output sensorID	
`BFO_HDRDESC_PKTCNT`	0	Include packet count for header description	
`BFO_MAC`	1	Output MAC addresses	

`BFO_ETHERTYPE`	1	Output EtherType	`IPV6_ACTIVATE=2||`
			`ETH_ACTIVATE>0`

`BFO_VLAN`	1	0: Do not output VLAN information, 1: Output VLAN numbers, 2: Output VLAN headers as hex 3: Output decoded VLAN headers as `TPID_PCP_DEI_VID`	
`BFO_MPLS`	0	0: Do not output MPLS information, 1: Output MPLS labels, 2: Output MPLS labels as hex, 3: Output MPLS headers as hex, 4: Output decoded MPLS headers	
`BFO_GRE`	0	Enable GRE output	
`BFO_L2TP`	0	Enable L2TP output	
`BFO_PPP`	0	Enable PPP output	
`BFO_LAPD`	0	Enable LAPD output	`LAPD_ACTIVATE=1`
`BFO_TEREDO`	0	Enable Teredo output	
`BFO_SUBNET_IPLIST`	0	Display a list of IP aggregated	
`BFO_SUBNET_TEST`	1	Enable subnet test	
`BFO_SUBNET_TEST_GRE`	0	Enable subnet test on GRE addresses	`IPV6_ACTIVATE!=1`
`BFO_SUBNET_TEST_L2TP`	0	Enable subnet test on L2TP addresses	`IPV6_ACTIVATE!=1`
`BFO_SUBNET_TEST_TEREDO`	0	Enable subnet test on Teredo addresses	
`BFO_SUBNET_HEX`	0	Output the country code and organization as one 32-bit hex number	
`BFO_SUBNET_ASN`	0	Output Autonomous System Numbers (ASN)	

Name	Default	Description	Flags
BFO_SUBNET_LL	0	Output position (latitude, longitude and reliability)	
BFO_MAX_HDRDESC	4	Max. number of headers descriptions to store	T2_PRI_HDRDESC=1
BFO_MAX_MAC	2	Max. different MAC addresses to store	
BFO_MAX_IP	2	Max. different IP addresses to store	
BFO_MAX_MPLS	3	Max. MPLS headers/tags to store	
BFO_MAX_VLAN	3	Max. VLAN headers/numbers to store	

1.2.2 bin2txt.h

Additional configuration options can be found in `$T2HOME/utils/bin2txt.h`. Refer to `tranalyzer2` documentation for more details.

1.2.3 subnetHL.h

Additional configuration options can be found in `$T2HOME/utils/subnetHL.h`. Refer to `tranalyzer2` documentation for more details.

1.3 Flow File Output

The basicFlow plugin outputs the following columns:

Column	Type	Description	Flags
dir	C	Flow direction A / B	
flowInd	U64	Flow index	
sensorID	U32	Sensor ID	BFO_SENSORID=1
flowStat	H64	Flow status and warnings	
timeFirst	TS	Date time of first packet	
timeLast	TS	Date time of last packet	
duration	U64.U32	Flow duration	
If T2_PRI_HDRDESC=1 and BFO_MAX_HDRDESC>0, the following columns are displayed:			
numHdrDesc	U8	Number of different headers descriptions	
numHdrs	R(U16)	Number of headers (depth) in hdrDesc	
hdrDesc	RS	Headers description	BFO_HDRDESC_PKTCNT=0
hdrDesc_pktCnt	R(S_U64)	Headers description and packet count	BFO_HDRDESC_PKTCNT=1
srcMac	R(MAC)	Source MAC address	BFO_MAC=1
dstMac	R(MAC)	Destination MAC address	BFO_MAC=1

ethType	H16	Ethernet type	BFO_ETHERTYPE=1&&
			(ETH_ACTIVATE>0||
			IPV6_ACTIVATE=2)

Column	Type	Description	Flags
If BFO_VLAN>0 and BFO_MAX_VLAN>0, the columns described in Section 1.3.1 are displayed here.			
If BFO_MPLS>0 and BFO_MAX_MPLS>0, the columns described in Section 1.3.2 are displayed here.			
If BFO_PPP=1, the columns described in Section 1.3.3 are displayed here.			
If LAPD_ACTIVATE=1 and BFO_LAPD=1, the columns described in Section 1.3.4 are displayed here.			
If BFO_L2TP=1, the columns described in Section 1.3.5 are displayed here.			
If BFO_GRE=1, the columns described in Section 1.3.6 are displayed here.			
If BFO_TEREDO=1, the columns described in Section 1.3.7 are displayed here.			
Standard five tuple output including geo-information			
srcIP	IP	Source IP address	BFO_SUBNET_IPLIST=0
srcIP	R(IP)	Source IP addresses	BFO_SUBNET_IPLIST=1
If BFO_SUBNET_TEST=1, the following columns are displayed:			
srcIPASN	U32	Source IP ASN	BFO_SUBNET_ASN=1
srcIPCOC	H32	Source IP country organization code	BFO_SUBNET_HEX=1
srcIPCC	SC	Source IP country	
srcIPCnty	S	Source IP county	CNTYCTY=1
srcIPCity	S	Source IP city	CNTYCTY=1
srcIPOrg	S	Source IP organization	BFO_SUBNET_ORG=1
srcIPLat_Lng_relP	F_F_F	Source IP lat., long. and reliability	BFO_SUBNET_LL=1
srcPort	U16	Source Port	
dstIP	IP	Destination IP address	BFO_SUBNET_IPLIST=0
dstIP	R(IP)	Destination IP addresses	BFO_SUBNET_IPLIST=1
If BFO_SUBNET_TEST=1, the following columns are displayed:			
dstIPASN	U32	Dest. IP ASN	BFO_SUBNET_ASN=1
dstIPCOC	H32	Dest. IP country organization code	BFO_SUBNET_HEX=1
dstIPCC	SC	Dest. IP country	
dstIPCnty	S	Dest. IP county	CNTYCTY=1
dstIPCity	S	Dest. IP city	CNTYCTY=1
dstIPOrg	S	Dest. IP organization	BFO_SUBNET_ORG=1

Column	Type	Description	Flags
dstIPLat_Lng_relP	F_F_F	Dest. IP lat., long. and reliability	BFO_SUBNET_LL=1
dstPort	U16	Destination port	
l4Proto	U8	Layer4 protocol	

1.3.1 VLAN

If BFO_VLAN>0 and BFO_MAX_VLAN>0, the following additional column is displayed:

Column	Type	Description	Flags
vlanID	R(U16)	VLAN IDs	BFO_VLAN=1
vlanHdr	R(H32)	VLAN headers (hex)	BFO_VLAN=2
vlanTPID_	R(H16_	VLAN tag protocol identifier (TPID),	BFO_VLAN=3
PCP_	U8_	priority code point (PCP),	
DEI_	U8_	drop eligible indicator (DEI),	
VID	U16)	VLAN identifier (VID)	

1.3.2 MPLS

If BFO_MPLS>0 and BFO_MAX_MPLS>0, the following additional column is displayed:

Column	Type	Description	Flags
mplsLabels	R(U32)	MPLS labels	BFO_MPLS=1
mplsLabelsHex	R(H32)	MPLS labels (hex)	BFO_MPLS=2
mplsHdrsHex	R(H32)	MPLS headers (hex)	BFO_MPLS=3
mplsLabel_ToS_S_TTL	R(U32_U8_U8_U8)	MPLS headers details	BFO_MPLS=4

1.3.3 PPP

If BFO_PPP=1, the following additional column is displayed:

Column	Type	Description	Flags
pppHdr	H32	PPP header	

1.3.4 LAPD

If BFO_LAPD=1 and LAPD_ACTIVATE=1, the following additional column is displayed:

Column	Type	Description	Flags
lapdSAPI	U8	LAPD SAPI	
lapdTEI	U8	LAPD TEI	

1.3.5 L2TP

If BFO_L2TP=1, the following additional columns are displayed:

Column	Type	Description	Flags
l2tpHdr	H16	L2TP header	
l2tpTID	U16	L2TP tunnel ID	
l2tpSID	U16	L2TP session ID	
l2tpCCSID	U32	L2TP control connection/session ID	
l2tpSrcIP	IP4	L2TP source IP address	
If BFO_SUBNET_TEST_L2TP=1, the following columns are displayed:			
l2tpSrcIPASN	U32	L2TP source IP ASN	BFO_SUBNET_ASN=1
l2tpSrcIPCOC	H32	L2TP source IP country organization code	BFO_SUBNET_HEX=1
l2tpSrcIPCC	SC	L2TP source IP country	
l2tpSrcIPCnty	S	L2TP source IP county	CNTYCTY=1
l2tpSrcIPCity	S	L2TP source IP city	CNTYCTY=1
l2tpSrcIPOrg	S	L2TP source IP organization	BFO_SUBNET_ORG=1
l2tpSrcIPLat_Lng_relP	F_F_F	L2TP source IP lat., long. and reliability	BFO_SUBNET_LL=1
l2tpDstIP	IP4	L2TP destination IP address	
If BFO_SUBNET_TEST_L2TP=1, the following columns are displayed:			
l2tpDstIPASN	U32	L2TP dest. IP ASN	BFO_SUBNET_ASN=1
l2tpDstIPCOC	H32	L2TP dest. IP country organization code	BFO_SUBNET_HEX=1
l2tpDstIPCC	SC	L2TP dest. IP country	
l2tpDstIPCnty	S	L2TP dest. IP county	CNTYCTY=1
l2tpDstIPCity	S	L2TP dest. IP city	CNTYCTY=1
l2tpDstIPOrg	S	L2TP dest. IP organization	BFO_SUBNET_ORG=1
l2tpDstIPLat_Lng_relP	F_F_F	L2TP dest. IP lat., long. and reliability	BFO_SUBNET_LL=1

1.3.6 GRE

If BFO_GRE=1, the following additional columns are displayed:

Column	Type	Description	Flags
greHdr	H32	GRE header	
greSrcIP	IP4	GRE source IP address	
If BFO_SUBNET_TEST_GRE=1, the following columns are displayed:			
greSrcIPASN	U32	GRE source IP ASN	BFO_SUBNET_ASN=1
greSrcIPCOC	H32	GRE source IP country organization code	BFO_SUBNET_HEX=1
greSrcIPCC	SC	GRE source IP country	
greSrcIPCnty	S	GRE source IP county	CNTYCTY=1

Column	Type	Description	Flags
greSrcIPCity	S	GRE source IP city	CNTYCTY=1
greSrcIPOrg	S	GRE source IP organization	BFO_SUBNET_ORG=1
greSrcIPLat_Lng_relP	F_F_F	GRE source IP lat., long. and reliability	BFO_SUBNET_LL=1
greDstIP	IP4	GRE destination IP address	
If BFO_SUBNET_TEST_GRE=1, the following columns are displayed:			
greDstIPASN	U32	GRE dest. IP ASN	BFO_SUBNET_ASN=1
greDstIPCOC	H32	GRE dest. IP country organization code	BFO_SUBNET_HEX=1
greDstIPCC	SC	GRE dest. IP country	
greDstIPCnty	S	GRE dest. IP county	CNTYCTY=1
greDstIPCity	S	GRE dest. IP city	CNTYCTY=1
greDstIPOrg	S	GRE dest. IP organization	BFO_SUBNET_ORG=1
greDstIPLat_Lng_relP	F_F_F	GRE dest. IP lat., long. and reliability	BFO_SUBNET_LL=1

1.3.7 Teredo

If BFO_TEREDO=1, the following additional columns are displayed:

Column	Type	Description	Flags
trdoDstIP	IP4	Next Teredo flow: dest IPv4 address	

If BFO_SUBNET_TEST_TEREDO=1, the following columns are displayed:

trdoDstIPASN	U32	Teredo dest. IP ASN	BFO_SUBNET_ASN=1
trdoDstIPCOC	H32	Teredo dest. IP country organization code	BFO_SUBNET_HEX=1
trdoDstIPCC	SC	Teredo dest. IP country	
trdoDstIPCnty	S	Teredo dest. IP county	CNTYCTY=1
trdoDstIPCity	S	Teredo dest. IP city	CNTYCTY=1
trdoDstIPOrg	S	Teredo dest. IP organization	BFO_SUBNET_ORG=1
trdoDstIPLat_Lng_relP	F_F_F	Teredo dest. IP lat., long. and reliability	BFO_SUBNET_LL=1
trdoDstPort	U16	Next Teredo flow: destination port	

If IPV6_ACTIVATE=0, then no further column is displayed.

Teredo IPv6 source address decode

trdo6SrcFlgs	H8	Flags	
trdo6SrcSrvIP4	IP4	Server IPv4	

If BFO_SUBNET_TEST_TEREDO=1, the following columns are displayed:

trdo6SrcSrvIP4ASN	U32	Server IP ASN	BFO_SUBNET_ASN=1
trdo6SrcSrvIP4COC	H32	Server IP country organization code	BFO_SUBNET_HEX=1
trdo6SrcSrvIP4CC	SC	Server IP country	
trdo6SrcSrvIP4Cnty	S	Server IP county	CNTYCTY=1
trdo6SrcSrvIP4City	S	Server IP city	CNTYCTY=1
trdo6SrcSrvIP4Org	S	Server IP organization	BFO_SUBNET_ORG=1
trdo6SrcSrvIP4Lat_Lng_relP	F_F_F	Server IP lat., long. and reliability	BFO_SUBNET_TEST_LL=1
trdo6SrcCPIP4	IP4	Client public IPv4	

If BFO_SUBNET_TEST_TEREDO=1, the following columns are displayed:

trdo6SrcCPIP4ASN	U32	Client public IP ASN	BFO_SUBNET_ASN=1
trdo6SrcCPIP4COC	H32	Client public IP country organization code	BFO_SUBNET_HEX=1
trdo6SrcCPIP4CC	SC	Client public IP country	
trdo6SrcCPIP4Cnty	S	Client public IP county	CNTYCTY=1
trdo6SrcCPIP4City	S	Client public IP city	CNTYCTY=1
trdo6SrcCPIP4Org	S	Client public IP organization	BFO_SUBNET_ORG=1
trdo6SrcCPIP4Lat_Lng_relP	F_F_F	Client public IP lat., long. and reliability	BFO_SUBNET_LL=1

Column	Type	Description	Flags
trdo6SrcCPPort	U16	Client public port	
	Teredo IPv6 destination address decode		
trdo6DstFlgs	H8	Flags	
trdo6DstSrvIP4	IP4	Server IPv4	
If BFO_SUBNET_TEST_TEREDO=1, the following columns are displayed:			
trdo6DstSrvIP4ASN	U32	Server IP ASN	BFO_SUBNET_ASN=1
trdo6DstSrvIP4COC	H32	Server IP country organization code	BFO_SUBNET_HEX=1
trdo6DstSrvIP4CC	SC	Server IP country	
trdo6DstSrvIP4Cnty	S	Server IP county	CNTYCTY=1
trdo6DstSrvIP4City	S	Server IP city	CNTYCTY=1
trdo6DstSrvIP4Org	S	Server IP organization	BFO_SUBNET_ORG=1
trdo6DstSrvIP4Lat_Lng_relP	F_F_F	Server IP lat., long. and reliability	BFO_SUBNET_LL=1
trdo6DstCPIP4	IP4	Client public IPv4	
If BFO_SUBNET_TEST_TEREDO=1, the following columns are displayed:			
trdo6DstCPIP4ASN	U32	Client public IP ASN	BFO_SUBNET_ASN=1
trdo6DstCPIP4COC	H32	Client public IP country organization code	BFO_SUBNET_HEX=1
trdo6DstCPIP4CC	SC	Client public IP country	
trdo6DstCPIP4Cnty	S	Client public IP county	CNTYCTY=1
trdo6DstCPIP4City	S	Client public IP city	CNTYCTY=1
trdo6DstCPIP4Org	S	Client public IP organization	BFO_SUBNET_ORG=1
trdo6DstCPIP4Lat_Lng_relP	F_F_F	Client public IP lat., long. and reliability	BFO_SUBNET_LL=1
trdo6DstCPPort	U16	Client public port	

1.3.8 flowInd

It is useful to identify flows when post processing operations, such as sort or filters are applied to a flow file and only a B or an A flow is selected. Moreover a packet file generated with the -s option supplies the flow index which simplifies the mapping of singular packets to the appropriate flow.

1.3.9 flowStat

The flowStat column is to be interpreted as follows:

flowStat	Description
2^{00} (=0x00000000 00000001)	Inverted flow, did not initiate connection
2^{01} (=0x00000000 00000002)	No Ethernet header

flowStat	Description
2^{02} `(=0x00000000 00000004)`	Pure L2 flow
2^{03} `(=0x00000000 00000008)`	Point to Point Protocol over Ethernet Discovery (PPPoED)
2^{04} `(=0x00000000 00000010)`	Point to Point Protocol over Ethernet Service (PPPoES)
2^{05} `(=0x00000000 00000020)`	Link Layer Discovery Protocol (LLDP)
2^{06} `(=0x00000000 00000040)`	ARP
2^{07} `(=0x00000000 00000080)`	Reverse ARP
2^{08} `(=0x00000000 00000100)`	VLANs
2^{09} `(=0x00000000 00000200)`	MPLS unicast
2^{10} `(=0x00000000 00000400)`	MPLS multicast
2^{11} `(=0x00000000 00000800)`	L2TP v2/3
2^{12} `(=0x00000000 00001000)`	GRE v1/2
2^{13} `(=0x00000000 00002000)`	PPP header after L2TP or GRE
2^{14} `(=0x00000000 00004000)`	IPv4 flow
2^{15} `(=0x00000000 00008000)`	IPv6 flow
2^{16} `(=0x00000000 00010000)`	IPvX bogus packet
2^{17} `(=0x00000000 00020000)`	IPv4/6 in IPv4/6
2^{18} `(=0x00000000 00040000)`	Ethernet over IP
2^{19} `(=0x00000000 00080000)`	Teredo tunnel
2^{20} `(=0x00000000 00100000)`	Anything in Anything (AYIYA) tunnel
2^{21} `(=0x00000000 00200000)`	GPRS Tunneling Protocol (GTP)
2^{22} `(=0x00000000 00400000)`	Virtual eXtensible Local Area Network (VXLAN)
2^{23} `(=0x00000000 00800000)`	Control and Provisioning of Wireless Access Points (CAPWAP), Lightweight Access Point Protocol (LWAPP)
2^{24} `(=0x00000000 01000000)`	Stream Control Transmission Protocol (SCTP)
2^{25} `(=0x00000000 02000000)`	SSDP/UPnP
2^{26} `(=0x00000000 04000000)`	Encapsulated Remote Switch Packet ANalysis (ERSPAN)
2^{27} `(=0x00000000 08000000)`	Cisco Web Cache Communication Protocol (WCCP)
2^{28} `(=0x00000000 10000000)`	SIP/RTP
2^{29} `(=0x00000000 20000000)`	Generic Network Virtualization Encapsulation (GENEVE)
2^{30} `(=0x00000000 40000000)`	IPsec Authentication Header (AH)
2^{31} `(=0x00000000 80000000)`	IPsec Encapsulating Security Payload (ESP)
2^{32} `(=0x00000001 00000000)`	Acquired packet length < minimal L2 datagram
2^{33} `(=0x00000002 00000000)`	Acquired packet length < packet length in L3 header
2^{34} `(=0x00000004 00000000)`	Acquired packet length < minimal L3 header
2^{35} `(=0x00000008 00000000)`	Acquired packet length < minimal L4 header
2^{36} `(=0x00000010 00000000)`	IPv4 fragmentation present
2^{37} `(=0x00000020 00000000)`	IPv4 fragmentation error (refer to the `tcpFlags` plugin for more details)

flowStat	Description
2^{38} (=0x00000040 00000000)	IPv4 1. fragment out of sequence or missing
2^{39} (=0x00000080 00000000)	Packet fragmentation pending or Fragmentation sequence not completed when flow timed-out
2^{40} (=0x00000100 00000000)	Flow timeout instead of protocol termination
2^{41} (=0x00000200 00000000)	Alarm mode: remove this flow instantly
2^{42} (=0x00000400 00000000)	Autopilot: flow removed to free space in main hash map
2^{43} (=0x00000800 00000000)	Stop dissecting, error or unhandled protocol
2^{44} (=0x00001000 00000000)	Consecutive duplicate IP ID
2^{45} (=0x00002000 00000000)	PPPL3 header not readable, compressed
2^{46} (=0x00004000 00000000)	IPv4 header length < 20 bytes
2^{47} (=0x00008000 00000000)	IP payload length > framing length
2^{48} (=0x00010000 00000000)	Header description overrun
2^{49} (=0x00020000 00000000)	pcapd and PD_ALARM=1: if set dumps the packets from this flow to a new pcap
2^{50} (=0x00040000 00000000)	Land attack: same srcIP && dstIP && srcPort && dstPort
2^{51} (=0x00080000 00000000)	Timestamp jump, probably due to multi-path delay or NTP operation
2^{52} (=0x00100000 00000000)	RESERVED, do not use
2^{55} (=0x00800000 00000000)	Subnet tested for that flow
2^{56} (=0x01000000 00000000)	Tor address detected
2^{57} (=0x02000000 00000000)	A packet had a priority tag (VLAN tag with ID 0)
2^{58} (=0x04000000 00000000)	IPv4 packet
2^{59} (=0x08000000 00000000)	IPv6 packet
2^{62} (=0x40000000 00000000)	Flow duration limit, same findex for all subflows
2^{63} (=0x80000000 00000000)	PCAP packet length > MAX_MTU in *ioBuffer.h*, caplen reduced

1.3.10 hdrDesc

The hdrDesc column describes the protocol stack in the flow in a human readable way. Note that it gives the user a lookahead of what is to be expected, even if not in the appropriate IPv4/6 mode. For example, in IPv4 several different headers stacks can be displayed by one flow if Teredo or different fragmentation is involved. T2 then dissects only to the last header above the said protocol and sets the *Stop dissecting* bit in the flow status (2^{41} (=0x00000400 00000000)).

1.3.11 lapdFType

The lapdFType column is to be interpreted as follows:

lapdFType	Description
0	Information frame
1	Supervisory frame
3	Unnumbered frame

1.3.12 lapdFunc

The `lapdFunc` column is to be interpreted as follows:

lapdFunc	Description
`REJ`	Supervisory frame – REJect
`RNR`	Supervisory frame – Receive Not Ready
`RR`	Supervisory frame – Receive Ready
`CFGR`	Unnumbered frame – ConFiGuRe
`DISC`	Unnumbered frame – DISConnect
`DM`	Unnumbered frame – Disconnected Mode
`FRMR`	Unnumbered frame – FRaMe Reject
`SABME`	Unnumbered frame – Set Asynchronous Balanced Mode Extended
`SIM`	Unnumbered frame – Set Initialization Mode
`TEST`	Unnumbered frame – Test
`UA`	Unnumbered frame – Unnumbered Acknowledgement
`UI`	Unnumbered frame – Unnumbered Information
`UP`	Unnumbered frame – Unnumbered Poll
`XID`	Unnumbered frame – eXchange IDentification

1.3.13 trdo6SrcFlgs and trdo6DstFlgs

The `trdo6SrcFlgs` and `trdo6DstFlgs` columns are to be interpreted as follows:

trdo6{Src,Dst}Flgs	Description
2^0 (=0x01)	Group/individual
2^1 (=0x02)	Universal/local
2^2 (=0x04)	—
2^3 (=0x08)	—
2^4 (=0x10)	—
2^5 (=0x20)	—
2^6 (=0x40)	Currently unassigned
2^7 (=0x80)	Behind NAT, new versions do not set this bit anymore

1.3.14 Geo labeling

The country and organization coding scheme are defined in the following files:

- `utils/subnet/whoCntryCds.txt`
- `utils/subnet/whoOrgCds.txt`

The special country code (CC) values `[0-9][0-9]` are used to represent private addresses or special address ranges such as Teredo or multicast:

CC	IPv4 addresses	IPv6 addresses	Description
00	0.0.0.0/32	::/128	Unspecified address
01	127.0.0.0/8	::1/128	Loopback address
02	169.254.0.0/16	fe80::/10	Link-local address
03		fc00::/7	Unique local address
04	10.0.0.0/8		Private network
05	172.16.0.0/12		Private network
06	192.0.0.0/24		Private network
07	192.168.0.0/16		Private network
08	198.18.0.0/15		Private network
10	224.0.0.0/4	ff00::/8	Multicast
11	255.255.255.255/32		Broadcast
20	100.64.0.0/10		Shared address space
21	192.0.2.0/24		TEST-NET-1
22	198.51.100.0/16		TEST-NET-2
23	203.0.113.0/24		TEST-NET-3
24	240.0.0.0/4		Reserved
25		100::/64	Discard prefix
26		2001:20::/28	ORCHIDv2
27		2001:db8::/32	Address used in documentation and example source code
60	192.88.99.0/24		Reserved (formerly used for IPv6 to IPv4 relay)
61		::ffff:0:0/96	IPv4 mapped address
62		::ffff:0:0:0/96	IPv4 translated address
63		64:ff9b::/96	IPv4/IPv6 translation
64		2001::/32	Teredo tunneling
65		2002::/16	The 6to4 addressing scheme (now deprecated)

The country organization codes (BFO_SUBNET_HEX=1) can be decoded with t2netID, e.g., t2netID 0x138020a5. Try t2netID --help for more information.

1.4 Packet File Output

In packet mode (-s option), the basicFlow plugin outputs the following columns:

Column	Type	Description	Flags
flowInd	U64	Flow index	
flowStat	H64	Flow status	
time	TS	Date time of packet	
relTime	U64.U32	Duration since start of pcap or interface sniffing	RELTIME=1
pktIAT	F	Packet inter-arrival time	
pktTrip	F	Packet round-trip time	
flowDuration	F	Flow duration	
numHdrs	U16	Number of headers (depth) in hdrDesc	T2_PRI_HDRDESC=1
hdrDesc	S	Headers description	T2_PRI_HDRDESC=1
vlanTPID_ PCP_	H16_ U8_	VLAN tag protocol identifier (TPID), priority code point (PCP),	BFO_VLAN=3

Column	Type	Description	Flags
DEI_	U8_	drop eligible indicator (DEI),	
VID	U16	VLAN identifier (VID)	
vlanHdr	H32	VLAN headers	BFO_VLAN=2
vlanID	U16	VLAN numbers	BFO_VLAN=1
If BFO_MPLS>0 and BFO_MAX_MPLS>0, one of the following column is displayed:			
mplsLabels	R(U32)	MPLS labels	BFO_MPLS=1
mplsLabelsHex	R(H32)	MPLS labels (hex)	BFO_MPLS=2
mplsHdrsHex	R(H32)	MPLS headers (hex)	BFO_MPLS=3
mplsLabel_ToS_S_TTL	R(U32_U8_U8_U8)	MPLS headers details	BFO_MPLS=4
srcMac	MAC	Source MAC address	
dstMac	MAC	Destination MAC address	
ethType	H16	Ethernet type	
If LAPD_ACTIVATE=1 and BFO_LAPD=1, the following six columns are displayed:			
lapdSAPI	U8	LAPD SAPI	
lapdTEI	U8	LAPD TEI	
lapdFType	U8	LAPD frame type	
lapdFunc	S	LAPD command (U-Frame) or Supervisory frame type	
lapdNR	U8	LAPD Receive Sequence Number	
lapdNS	U8	LAPD Send Sequence Number	
srcIP	IP	Source IP address	
srcIPCC	SC	Source IP country	BFO_SUBNET_TEST=1

srcIPOrg	S	Source IP organization	BFO_SUBNET_TEST=1&&
			BFO_SUBNET_ORG=1

srcPort	U16	Source port	
dstIP	IP	Destination IP address	
dstIPCC	SC	Destination IP country	BFO_SUBNET_TEST=1

dstIPOrg	S	Destination IP organization	BFO_SUBNET_TEST=1&&
			BFO_SUBNET_ORG=1

dstPort	U16	Destination port	
l4Proto	U8	Layer 4 protocol	

1.5 Post-Processing

The t2whois program provides an offline whois and geolocation query option using T2 subnet files. It can be found in $T2HOME/utils/t2whois/ and can be compiled by typing make. The use of the program is straightforward:

```
t2whois 1.2.3.4
```

Try t2whois -h for more information.