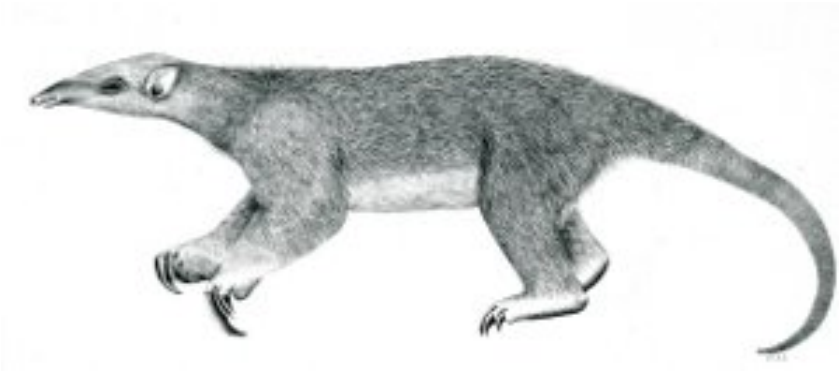
Tranalyzer2

basicFlow

Overall Flow Info + L3/4 addressing



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	1: sensorID on / 0: sensorID off	
BFO_HDRDESC_PKTCNT	0	1: Enables / 0: Disables pkt count for header description	
BFO_MAC	1	1: Enables / 0: Disables MAC address output	
BFO_ETHERTYPE	1	1: Enables / 0: Disables EtherType output	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	
BFO_MPLS	0	0: Do not output MPLS information, 1: Output MPLS labels, 2: Output MPLS headers as hex, 3: Output decoded MPLS headers	
BFO_L2TP	0	1: Enables L2TP header information	
BFO_GRE	0	1: Enables GRE header information	
BFO_PPP	0	1: Enables PPP header information	
BFO_ETHIP	0	1: Enables ETHIP header information	
BFO_TEREDO	0	1: Enables Teredo IP, Port information	
BFO_SUBNET_TEST	1	1: Enables subnet test	
BFO_SUBNET_TEST_GRE	0	1: Enable subnet test on GRE addresses	IPV6_ACTIVATE!=1
BFO_SUBNET_TEST_L2TP	0	1: Enables subnet test on L2TP addresses	IPV6_ACTIVATE!=1
BFO_SUBNET_TEST_TEREDO	0	1: Enables subnet test on Teredo addresses	
BFO_SUBNET_HEX	0	Country code and who information representation: 0: Two human readable columns (two letters country code and who), 1: One column, hex ID output	
BFO_SUBNET_ASN	0	1: Autonomous System Numbers on, 0: ASN off	
BFO_SUBNET_LL	0	1: Latitude, longitude and reliability, 0: no output	
BFO_MAX_HDRDESC	4	Max. number of headers descriptions to store 0: switch off output	T2_PRI_HDRDESC=1
BFO_MAX_MAC	2	Max. number of different MAC addresses to store	

		0: switch off output
BFO_MAX_MPLS	3	Max. number of MPLS Header pointer to store 0: switch off output
BFO_MAX_VLAN	3	Max. number of Ethertypes to store 0: switch off output

1.2.2 utils.h

The following flags can be used to control the output of the plugin: If SUBRNG or WHOEN is changed, the basicFlow plugin

Name	Default	Description
SUBRNG	0	Subnet definition 1: Begin - End / 0: CIDR only
WHOLEN	20	length of WHO record

MUST be recompiled with `'./autogen.sh -f'`.

1.2.3 bin2txt.h

Additional configuration options can be found in $T2HOME/utils/bin2txt.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_HDRDESC_DEPTH>0, the following columns are displayed:

numHdrDesc	U8	Number of different headers descriptions	
numHdrs	RU16	Number of headers (depth) in hdrDesc	BFO_HDRDESC_PKTCNT=1
hdrDesc_PktCnt	RS_U64	Headers description and packet count	
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_DEPTH>0, the following column is displayed:			
ethVlanID	U16R	VLAN IDs	BFO_VLAN=1
ethVlanHdr	RH32	VLAN headers (hex)	BFO_VLAN=2
If BFO_MPLS>0 and BFO_MAX_MPLS_DEPTH>0, the following column is displayed:			
mplsLabels	RU32	MPLS labels	BFO_MPLS=1
mplsTagsHex	RH32	MPLS tags (hex)	BFO_MPLS=2
mplsLabel_ToS_S_TTL	R(U32_U8_U8_U8)	MPLS tags detail	BFO_MPLS=3
If BFO_PPP=1, the following column is displayed:			
pppHdr	H32	PPP header	
If BFO_L2TP=1, the following columns are displayed:			
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	
l2tpSrcIPASN	U32	L2TP source IP ASN	BFO_SUBNET_TEST_L2TP=1&&BFO_SUBNET_ASN=1
l2tpSrcIPCC	S/H32	L2TP source IP country code	BFO_SUBNET_TEST_L2TP=1
l2tpSrcIPWho	S	L2TP source IP organisation name	BFO_SUBNET_TEST_L2TP=1&&BFO_SUBNET_HEX=0
l2tpSrcIPLat_Lng_relP	F_F_F	L2TP source IP latitude, longitude and reliability	BFO_SUBNET_TEST_L2TP=1&&BFO_SUBNET_LL=1
l2tpDstIP	IP4	L2TP destination IP address	
l2tpDstIPASN	U32	L2TP destination IP ASN	BFO_SUBNET_TEST_L2TP=1&&BFO_SUBNET_ASN=1
l2tpDstIPCC	S/H32	L2TP destination IP country code	BFO_SUBNET_TEST_L2TP=1
l2tpDstIPWho	S	L2TP destination IP organisation name	BFO_SUBNET_TEST_L2TP=1&&BFO_SUBNET_HEX=0
l2tpDstIPLat_Lng_relP	F_F_F	L2TP destination IP latitude, longitude and reliability	BFO_SUBNET_TEST_L2TP=1&&BFO_SUBNET_LL=1
If BFO_GRE=1, the following columns are displayed:			
greHdr	H32	GRE header	
greSrcIP	IP4	GRE source IP address	
greSrcIPASN	U32	GRE source IP ASN	BFO_SUBNET_TEST_GRE=1&&BFO_SUBNET_ASN=1

Column	Type	Description	Flags
greSrcIPCC	S/H32	GRE source IP country code	BFO_SUBNET_TEST_GRE=1
greSrcIPWho	S	GRE source IP organisation name	BFO_SUBNET_TEST_GRE=1&& BFO_SUBNET_HEX=0
greSrcIPLat_ Lng_relP	F_F_F	GRE source IP latitude, longitude and reliability	BFO_SUBNET_TEST_GRE=1&& BFO_SUBNET_LL=1
greDstIP	IP4	GRE destination IP address	
greDstIPASN	U32	GRE destination IP ASN	BFO_SUBNET_TEST_GRE=1&& BFO_SUBNET_ASN=1
greDstIPCC	S/H32	GRE destination IP country code	BFO_SUBNET_TEST_GRE=1
greDstIPWho	S	GRE destination IP organisation name	BFO_SUBNET_TEST_GRE=1&& BFO_SUBNET_HEX=0
greDstIPLat_ Lng_relP	F_F_F	GRE destination IP latitude, longitude and reliability	BFO_SUBNET_TEST_GRE=1&& BFO_SUBNET_LL=1
If BFO_TEREDO=1, the following columns are displayed:			
trdoDstIP	IP4	Nxt Teredo Flow: Dest IPv4 address	
trdoDstIPASN	U32	Teredo destination IP ASN	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_ASN=1
trdoDstIPCC	S/H32	Teredo destination IP country code	BFO_SUBNET_TEST_TEREDO=1
trdoDstIPWho	S	Teredo destination IP organisation name	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_HEX=0
trdoDstIPLat_ Lng_relP	F_F_F	Teredo destination IP latitude, longitude and reliability	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_LL=1
trdoDstPort	U16	Nxt Teredo Flow: Destination port	
If BFO_TEREDO=1 and IPV6_ACTIVATE>0 then the following lines are displayed:			
trdo6SrcFlgs	H8	Teredo IPv6 source address decode: Flags	
trdo6SrcSrvIP4	IP4	Teredo IPv6 source address decode: Server IPv4	
trdo6SrcSrvIP4ASN	U32	Teredo IPv6 source address decode: Server IPv4 ASN	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_ASN=1
trdo6SrcSrvIP4CC	S/H32	Teredo IPv6 source address decode: Server IPv4 country code	BFO_SUBNET_TEST_TEREDO=1
trdo6SrcSrvIP4Who	S	Teredo IPv6 source address decode: Server IPv4 who	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_HEX=0
trdo6SrcSrvIP4Lat_ Lng_relP	F_F_F	Teredo IPv6 source address decode: Server IPv4 latitude, longitude and reliability	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_LL=1
trdo6SrcCPIP4	IP4	Teredo IPv6 source address decode: Client Public IPv4	
trdo6SrcCPIP4ASN	U32	Teredo IPv6 source address decode: Client Public IPv4 ASN	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_ASN=1
trdo6SrcCPIP4CC	S/H32	Teredo IPv6 source address decode:	BFO_SUBNET_TEST_TEREDO=1

Column	Type	Description	Flags
		Client Public IPv4 country code	
trdo6SrcCPIP4Who	S	Teredo IPv6 source address decode: Client Public IPv4 who	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_HEX=0
trdo6SrcCPIP4Lat_Lng_relP	F_F_F	Teredo IPv6 source address decode: Client Public IPv4 latitude, longitude and reliability	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_LL=1
trdo6SrcCPPort	U16	Teredo IPv6 source address decode: Client Public Port	
trdo6DstFlgs	H8	Teredo IPv6 dest. address decode: Flags	
trdo6DstSrvIP4	IP4	Teredo IPv6 dest. address decode: Server IPv4	
trdo6DstSrvIP4ASN	U32	Teredo IPv6 dest. address decode: Server IPv4 ASN	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_ASN=1
trdo6DstSrvIP4CC	S/H32	Teredo IPv6 dest. address decode: Server IPv4 country code	BFO_SUBNET_TEST_TEREDO=1
trdo6DstSrvIP4Who	S	Teredo IPv6 dest. address decode: Server IPv4 who	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_HEX=0
trdo6DstSrvIP4Lat_Lng_relP	F_F_F	Teredo IPv6 dest. address decode: Server IPv4 latitude, longitude and reliability	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_LL=1
trdo6DstCPIP4	IP4	Teredo IPv6 dest. address decode: Client Public IPv4	
trdo6DstCPIP4ASN	U32	Teredo IPv6 dest. address decode: Client Public IPv4 ASN	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_ASN=1
trdo6DstCPIP4CC	S/H32	Teredo IPv6 dest. address decode: Client Public IPv4 country code	BFO_SUBNET_TEST_TEREDO=1
trdo6DstCPIP4Who	S	Teredo IPv6 dest. address decode: Client Public IPv4 who	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_HEX=0
trdo6DstCPIP4Lat_Lng_relP	F_F_F	Teredo IPv6 dest. address decode: Client Public IPv4 latitude, longitude and reliability	BFO_SUBNET_TEST_TEREDO=1&& BFO_SUBNET_LL=1
trdo6DstCPPort	U16	Teredo IPv6 dest. address decode: Client Public Port	

Standard six tuple output including geolabeling:

srcIP	IP	Source IP address	
srcIPASN	U32	Source IP ASN	BFO_SUBNET_TEST=1&& BFO_SUBNET_ASN=1
srcIPCC	S/H32	Source IP country code	BFO_SUBNET_TEST=1
srcIPWho	S	Source IP organisation name	BFO_SUBNET_TEST=1&& BFO_SUBNET_HEX=0
srcIPLat_Lng_relP	F_F_F	Source IP latitude, longitude and reliability	BFO_SUBNET_TEST=1&& BFO_SUBNET_LL=1
srcPort	U16	Source Port	

Column	Type	Description	Flags
dstIP4	IP	Destination IP address	
dstIPASN	U32	Destination IP ASN	BFO_SUBNET_TEST=1&& BFO_SUBNET_ASN=1
dstIPCC	S/H32	Destination IP country code	BFO_SUBNET_TEST=1
dstIPWho	S	Destination IP organisation name	BFO_SUBNET_TEST=1 BFO_SUBNET_HEX=0
dstIPLat_Lng_relP	F_F_F	Destination IP latitude, longtable and reliability	BFO_SUBNET_TEST=1&& BFO_SUBNET_LL=1
dstPort	U16	Destination port	
l4Proto	U8	Layer 4 protocol	

1.3.1 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.

1.3.2 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
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
2^{15} (=0x00000000 00008000)	IPv6
2^{16} (=0x00000000 00010000)	IPvX bogus packets

	flowStat	Description
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)	Authentication Header (AH)
2^{31}	(=0x00000000 80000000)	—
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)
2^{38}	(=0x00000040 00000000)	IPv4 1. fragment out of sequence or missing
2^{39}	(=0x00000080 00000000)	Fragmentation sequence not completed when flow timeout
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 not capable to do e.g. IPv4/6 config
2^{44}	(=0x00001000 00000000)	PPPL3 header not readable, compressed
2^{45}	(=0x00002000 00000000)	—
2^{46}	(=0x00004000 00000000)	—
2^{47}	(=0x00008000 00000000)	—
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)	Time slip possibly due to NTP operations on the capture machine
2^{52}	(=0x00100000 00000000)	`liveXtr` : if set dumps the packets from this flow to a new pcap

	flowStat	Description
2^{56} (=0x01000000 00000000)		Tor address detected
2^{57} (=0x02000000 00000000)		A packet had a priority tag (VLAN tag with ID 0)
2^{63} (=0x80000000 00000000)		PCAP packet length > MAX_MTU in *ioBuffer.h*, caplen reduced

1.3.3 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)).

1.3.4 trdoFlags

The trdoFlags column is to be interpreted as follows:

trdoFlags	Description
2^0 (=0x01)	Group/individual
2^1 (=0x02)	Universal/local
2^2 (=0x04)	0
2^3 (=0x08)	0
2^4 (=0x10)	0
2^5 (=0x20)	0
2^6 (=0x40)	Currently Unassigned
2^7 (=0x80)	Behind Nat, new version do not set this bit anymore

1.3.5 Geo labeling

The country coding scheme is defined in utils/cntrycd.txt. The special values [0-9][0-9] are used to represent private addresses or special address ranges such as teredo or multicast:

- 00: 10.0.0.0/8 (private)
- 01: 172.16.0.0/16 (private)
- 02: 192.168.0.0/16 (private)
- 03: 169.254.0.0/16 (link-local)
- 04: 224.0.0.0/8 (multicast)
- 01: fe80::/10 (link local)
- 02: fc00::/7 (private)
- 03: ::ffff:0.0.0.0/96
- 04: ff00::/8 (multicast)
- 10: 2001::/32 (teredo)

The text format of the subnets4.txt and subnets6.txt files is defined as follows:
A '-' in the first column (prefix/mask) denotes a non-CIDR range. In this case, Tranalyzer reads the 2nd column instead of the 1st when SUBRNG=1 in utils.h. If SUBRNG=0, the 2nd column is ignored and only CIDR ranges are accepted.

The text files subnets4.txt and subnets6.txt can be edited and manually converted as follows:

```
#       3       20190114
# prefix/mask   seMask  start_ip-end_ip coCode  asn     probability     long    lat
    country_code    organisation
10.0.0.0/8      8       10.0.0.0-10.255.255.255 0x01003690      0       1.000000        666.000000
          666.000000      00      private_reserved
172.16.0.0/12   12      172.16.0.0-172.31.255.255       0x01003690      0       1.000000
    666.000000      666.000000      01      private_reserved
192.168.0.0/16  16      192.168.0.0-192.168.255.255     0x01003690      0       1.000000
    666.000000      666.000000      02      private_reserved
169.254.0.0/16  16      169.254.0.0-169.254.255.255     0x01003690      0       1.000000
    666.000000      666.000000      03      private_reserved
224.0.0.0/8     8       224.0.0.0-224.255.255.255       0x01002c68      0       1.000000
    666.000000      666.000000      04      Multicast
1.0.0.0/24      24      1.0.0.0-1.0.0.255       0x0e000000      0       0.980000        145.179990
          -37.700000      au      regional internet registry for the asia-pacific region
1.0.1.0/24      24      1.0.1.0-1.0.1.255       0x31000000      0       0.970000        666.000000
          666.000000      cn      chinanet fujian province network
1.0.1.0/24      22      1.0.1.0-1.0.3.255       0x31000000      0       0.980000        119.309990
          26.059990       cn      chinanet fujian province network
1.0.100.0/22    22      1.0.100.0-1.0.103.255   0x73000000      0       0.980000        133.050000
          35.470000       jp      --
-   22      9.111.0.15-9.112.2.116   0x54000000      0       0.980000        13.050000
    225.470000      us      IBM
......
```

`./utils/subconv -4 subnets4.txt` and `./utils/subconv -6 subnets6.txt`

1.4 Packet File Output

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

Column	Description	Flags
flowInd	Flow index	
flowStat	Flow status	
time	Time	
relTime	Duration since start of pcap or interface sniffing	
pktIAT	Packet inter-arrival time	
flowDuration	Flow duration	
numHdrs	Number of headers (depth) in hdrDesc	T2_PRI_HDRDESC=1
hdrDesc	Headers description	T2_PRI_HDRDESC=1
ethVlanID	VLAN number (inner VLAN)	
srcMac	Source MAC address	
dstMac	Destination MAC address	
ethType	Ethernet type	
srcIP	Source IP address	
srcIPCC	Source IP country code	BFO_SUBNET_TEST=1
srcIPWho	Source IP organisation name	BFO_SUBNET_TEST=1
srcPort	Source port	
dstIP	Destination IP address	
dstIPCC	Destination IP country code	BFO_SUBNET_TEST=1
dstIPWho	Destination IP organisation name	BFO_SUBNET_TEST=1

Column	Description	Flags
dstPort	Destination port	
l4Proto	Layer 4 protocol	