

MEASUREMENTS

OVERVIEW:

- WHAT IS BEING MEASURED?
 - GOALS
 - TECHNIQUES
 - TOOLS

WHAT IS BEING MEASURED?

DELAY

- ONE-WAY
- ROUND-TRIP

DELAY VARIATION

- JITTER

THROUGHPUT

- AVERAGE
 - PEAK
- CAPACITY

LOSS

GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

TRAFFIC ENGINEERING

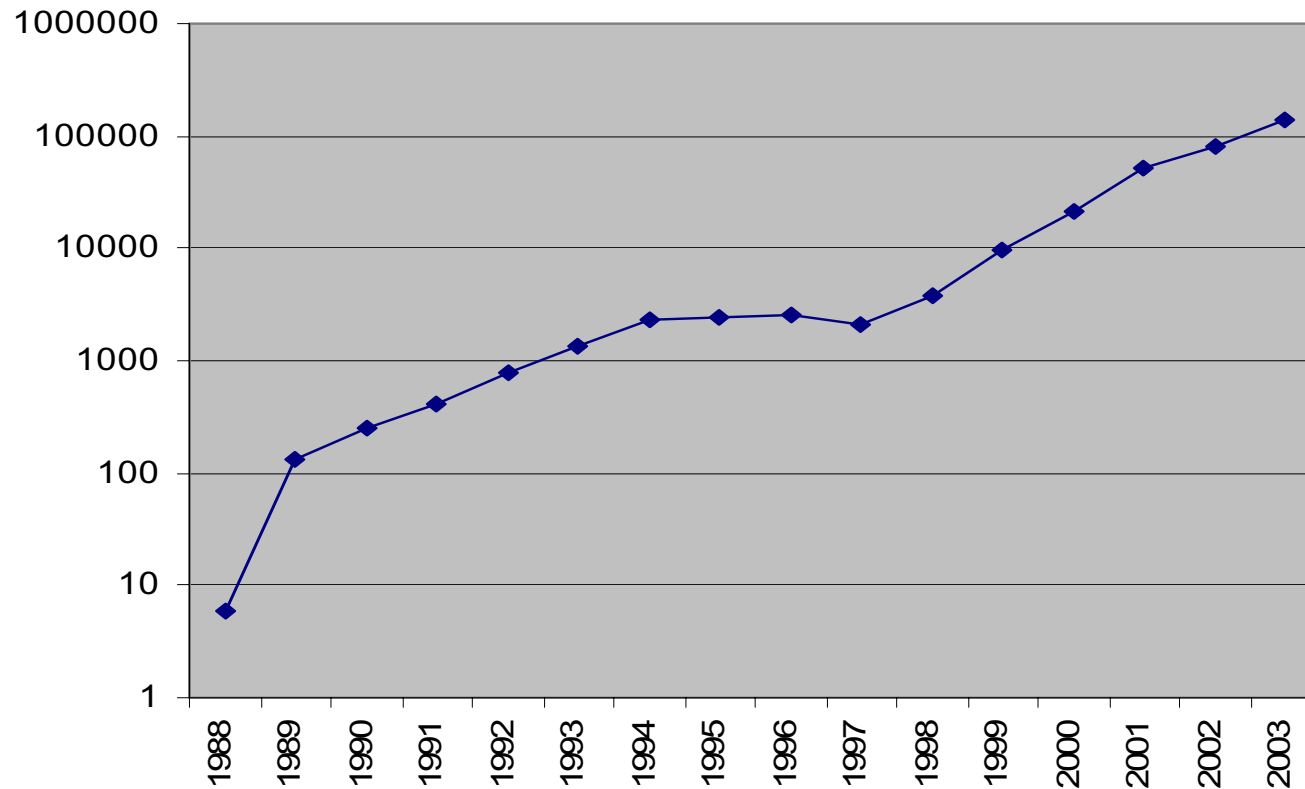
NETWORK DIMENSIONING

ACCOUNTING

NETWORK TOMOGRAPHY

INTRUSION DETECTION - INCIDENTS - 1

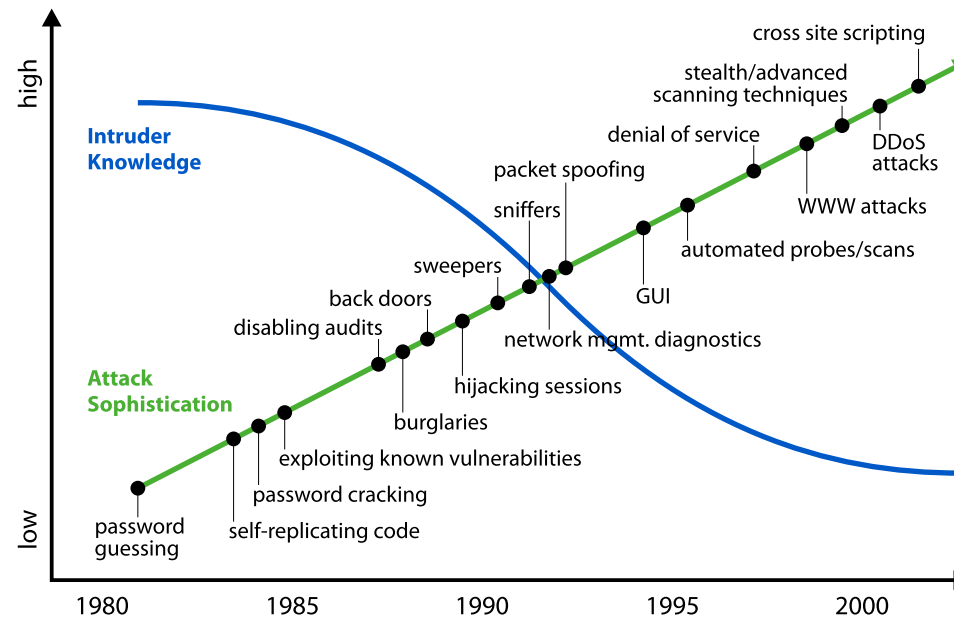
NUMBER OF REPORTED INCIDENTS



SOURCE: www.cert.org/stats/cert_stats.html

INTRUSION DETECTION - INCIDENTS - 2

ATTACK SOPHISTICATION VERSUS INTRUDER'S KNOWLEDGE



SOURCE: D1.4 SCAMPI PROJECT

- WORMS
- DDoS ATTACKS
 - SPAM
- PHISHING

INTRUSION DETECTION - APPROACHES

DETECT BIT PATTERNS

- EXAMPLE: PUBLIC, *.EXE
 - SNIFFER
 - SNORT

DETECT PACKET SEQUENCES

- SNIFFER / HOST
- HORIZONTAL - VERTICAL (PORT) SCANS
 - TCP CONNECTION ATTEMPTS

DETECT SUSPICIOUS BEHAVIOUR

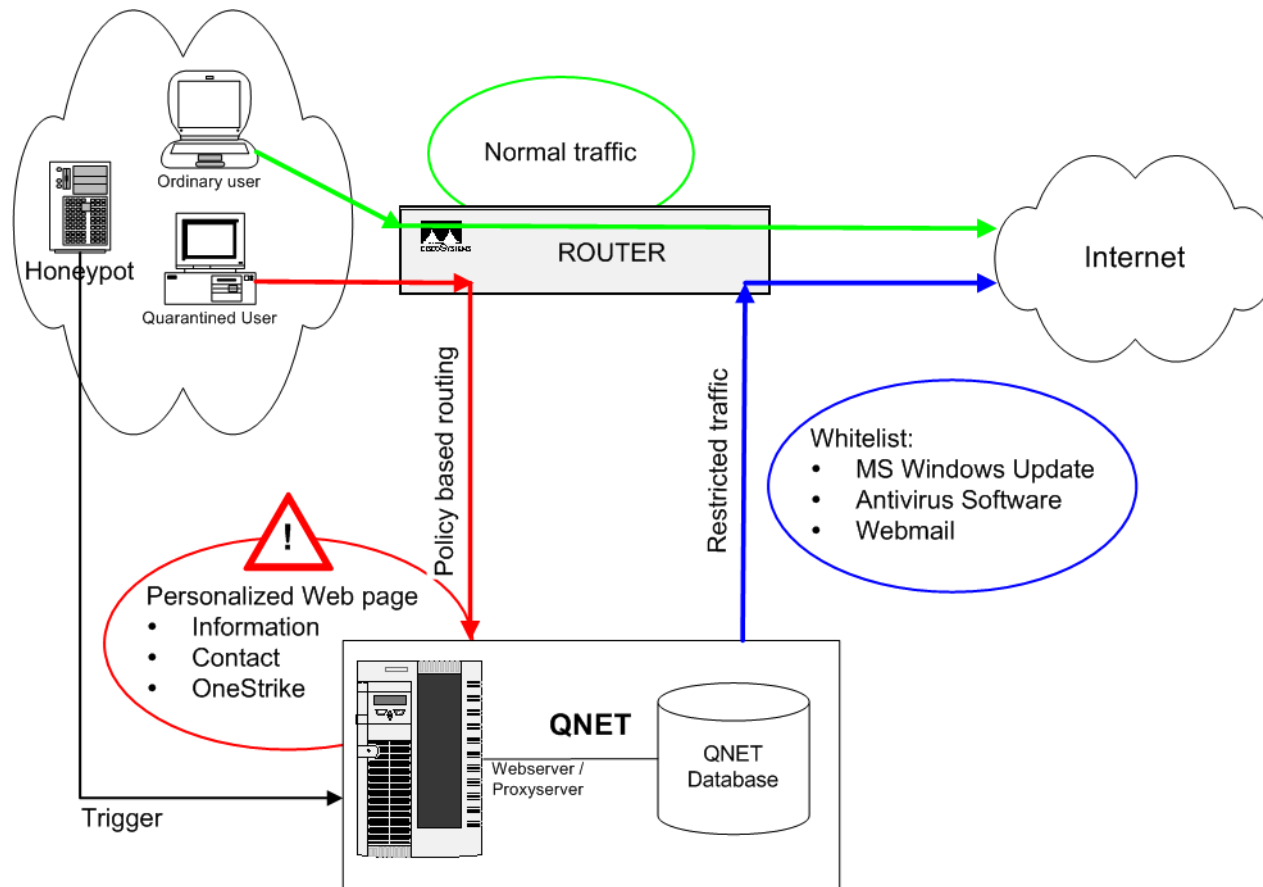
- HOST
- (DISTRIBUTED) HONEYPOT

ANALYZE LOG FILES

- HOST
- MAIL AND WEB LOGS

INTRUSION DETECTION - HONEYPOT

EXAMPLE: UT



BACKGROUND RADIATION

CATEGORIES:

NON-PRODUCTIVE:

- MISCONFIGURATIONS

MALICIOUS:

- SCANS
- WORMS
- BACKSCATTER FROM FLOODING ATTACKS
- DENIAL OF SERVICE (DOS) ATTACKS

BACKGROUND RADIATION

Study by Pang, Yegneswaran, Barford, Paxson & Peterson
2004, Lawrence Berkeley National Laboratory (LBL)

Questions:

- What protocols
 - What ports
- How is the variation in time
- What are the main worms

BACKGROUND RADIATION

Measurement approach:

- Measure traffic destined for unused Internet addresses
 - Passive filtering to cope with large amounts of data
 - Active responders to solicit further traffic

Traces from three locations:

- University of Wisconsin (UW)
- Lawrence Berkeley National Laboratory (LBL)
 - Class A network

BACKGROUND RADIATION

WHAT PROTOCOLS?

Protocol	UW-1		LBL-P		Class A	
	Rate	%	Rate	%	Rate	%
TCP	928	95.0%	664	56.5%	130	88.5%
ICMP	4.00	4.2%	488	39.6%	0.376	0.3%
UDP	0.156	0.8%	45.2	3.8%	16.5	11.3%

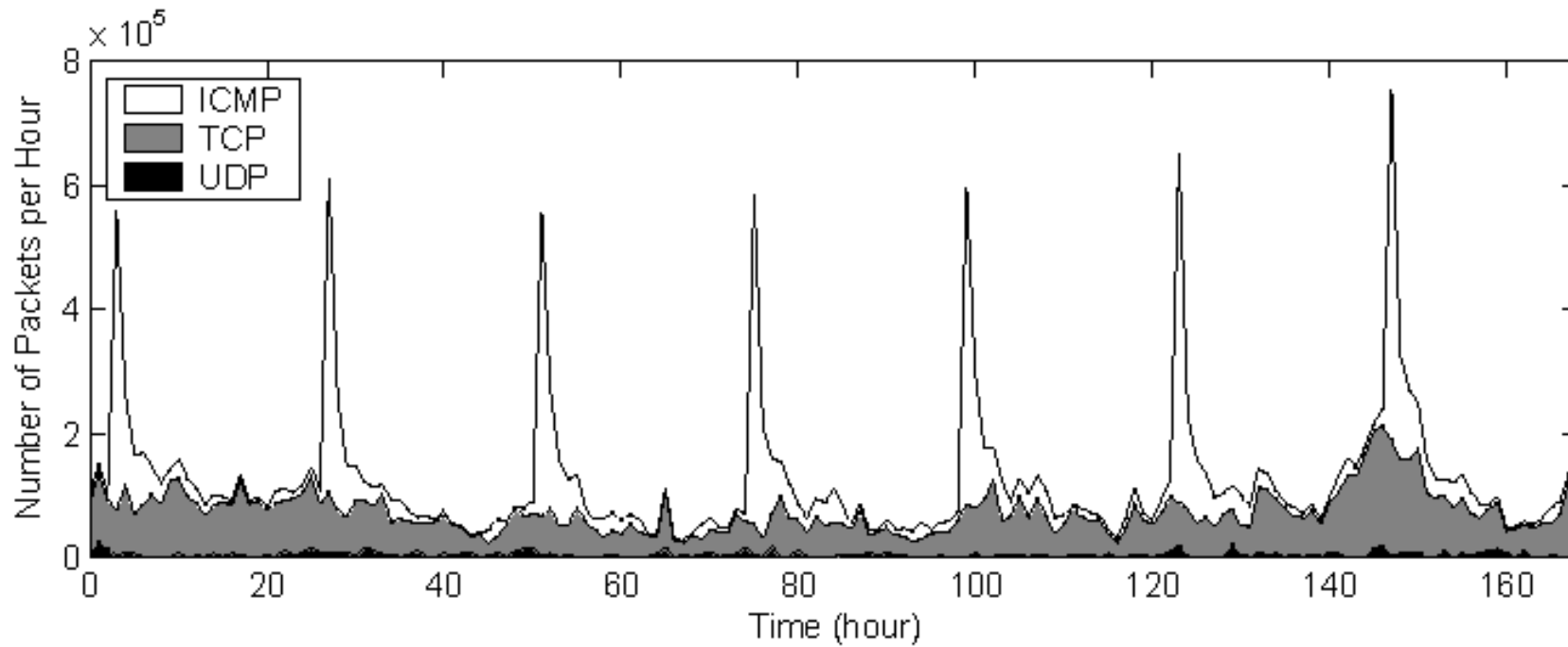
BACKGROUND RADIATION

WHAT PORTS?

TCP Port	# Source IP (%)	# Packets (%)
445	43.4%	19.7%
80	28.7%	7.3%
135	19.1%	30.4%
1025	4.3%	5.8%
2745	3.2%	3.6%
139	3.2%	11.1%
3127	2.7%	3.2%
6129	2.2%	2.4%

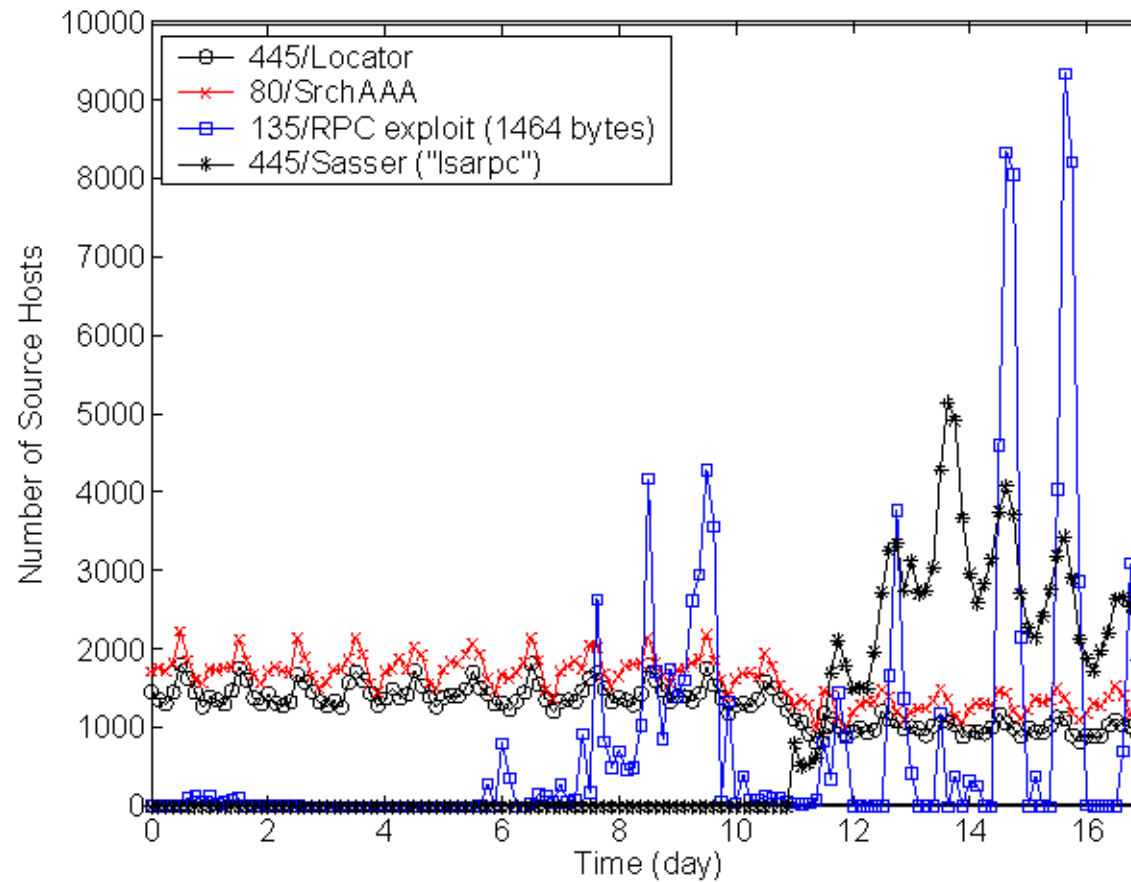
BACKGROUND RADIATION

HOW IS THE VARIATION OVER TIME?
(PER PROTOCOL)



BACKGROUND RADIATION

HOW IS THE VARIATION OVER TIME?
(PER ATTACK)



GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

TRAFFIC ENGINEERING

NETWORK DIMENSIONING

ACCOUNTING

NETWORK TOMOGRAPHY

LAWFULL INTERCEPTION

RECENT PROPOSALS IN US & EUROPE

NOVEMBER 2004, COUNCIL OF THE EU:

- (a) Data necessary to trace and identify the source of a communication which includes personal details, contact information and information identifying services subscribed to.
- (b) Data necessary to identify the routing and destination of a communication.
- (c) Data necessary to identify the time and date and duration of a communication.
- (d) Data necessary to identify the telecommunication.
- (e) Data necessary to identify the communication device or what purports to be the device.
- (f) Data necessary to identify the location at the start and throughout the duration of the communication.

SOURCE: <http://register.consilium.eu.int/pdf/en/04/st14/st14190.en04.pdf>

GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

TRAFFIC ENGINEERING

NETWORK DIMENSIONING

ACCOUNTING

NETWORK TOMOGRAPHY

TRAFFIC ENGINEERING

MODELLING OF NETWORK TRAFFIC

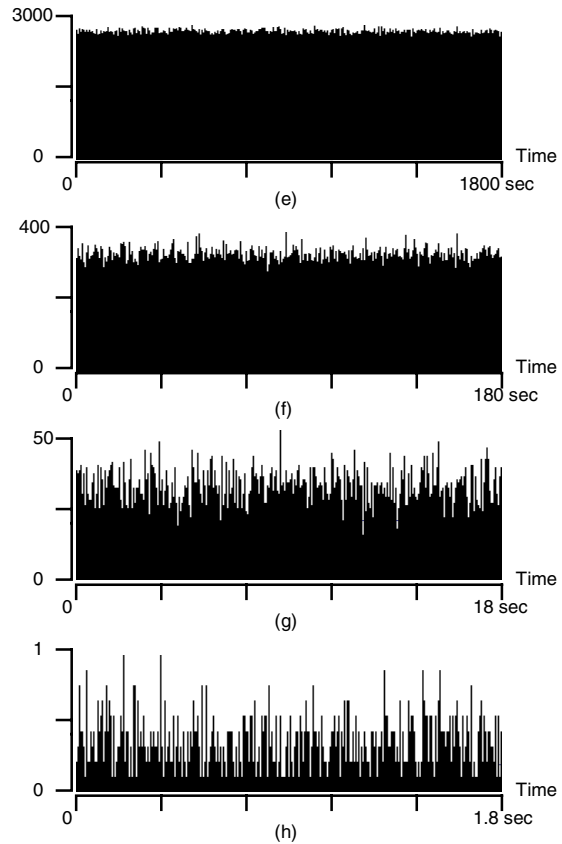
POISSON ARRIVAL PROCESS

GAUSSIAN TRAFFIC MODELS

SELF-SIMILARITY / LONG RANGE DEPENDANCE

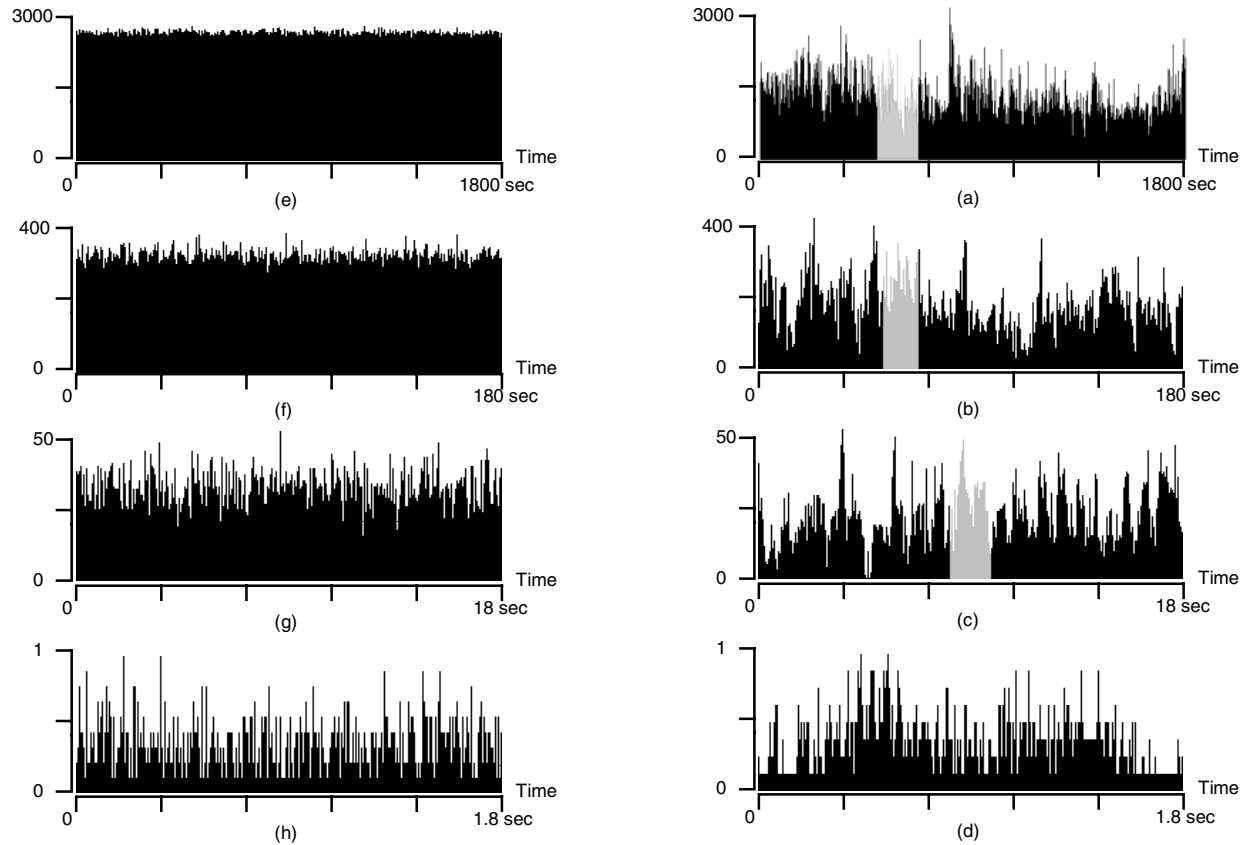
HEAVY TAIL DISTRIBUTION

TRAFFIC ENGINEERING - SELF SIMILARITY



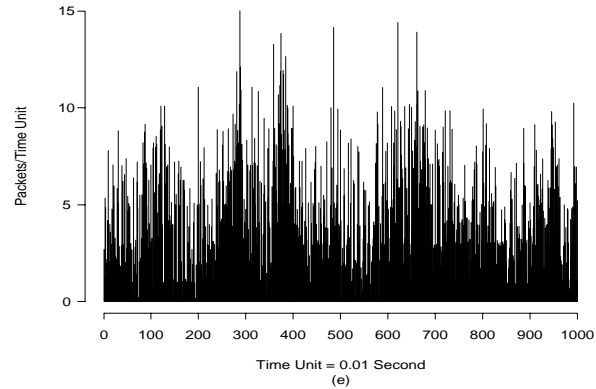
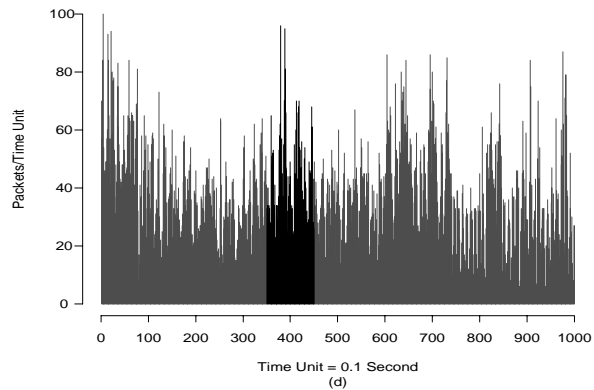
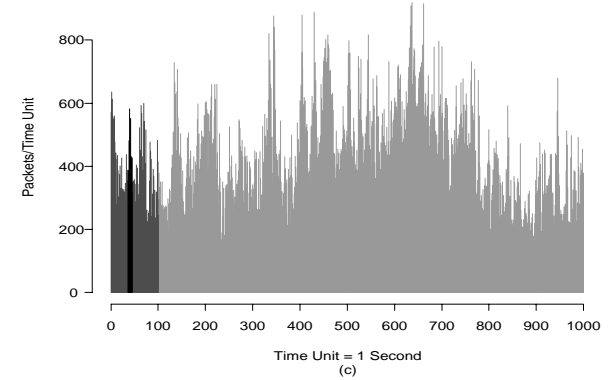
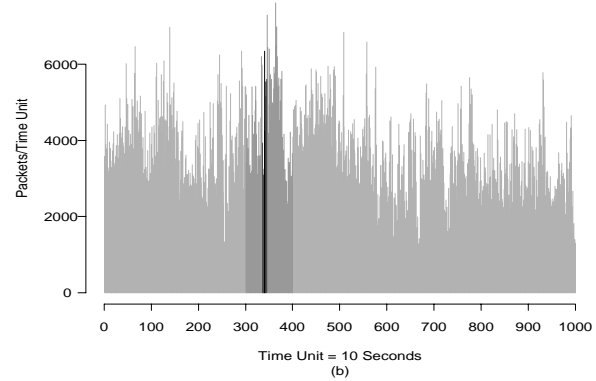
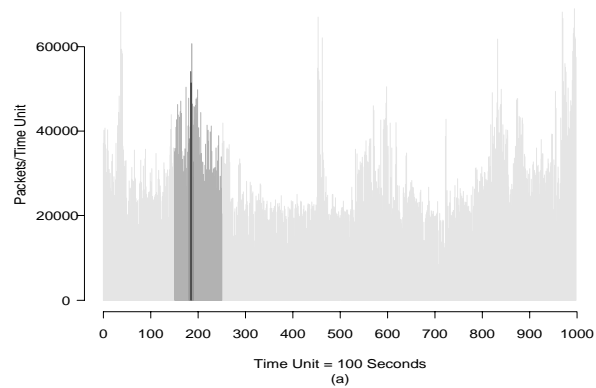
*SOURCE: Traffic Characterisation for Telecommunication Networks
Attila Vidács, Zsolt Kenesi, Ákos Rétfalvi, Péter Pozsgai, Sándor Molnár - BUTE, Budapest, 1999*

TRAFFIC ENGINEERING - SELF SIMILARITY



*SOURCE: Traffic Characterisation for Telecommunication Networks
Attila Vidács, Zsolt Kenesi, Ákos Rétfalvi, Péter Pozsgai, Sándor Molnár - BUTE, Budapest, 1999*

TRAFFIC ENGINEERING - SELF SIMILARITY



*SOURCE: On the self-similar nature of Ethernet traffic (extended version)
WE Leland, MS Taqqu, W Willinger, DV Wilson - IEEE/ACM Transactions on Networking, 1994*

GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

TRAFFIC ENGINEERING

NETWORK DIMENSIONING

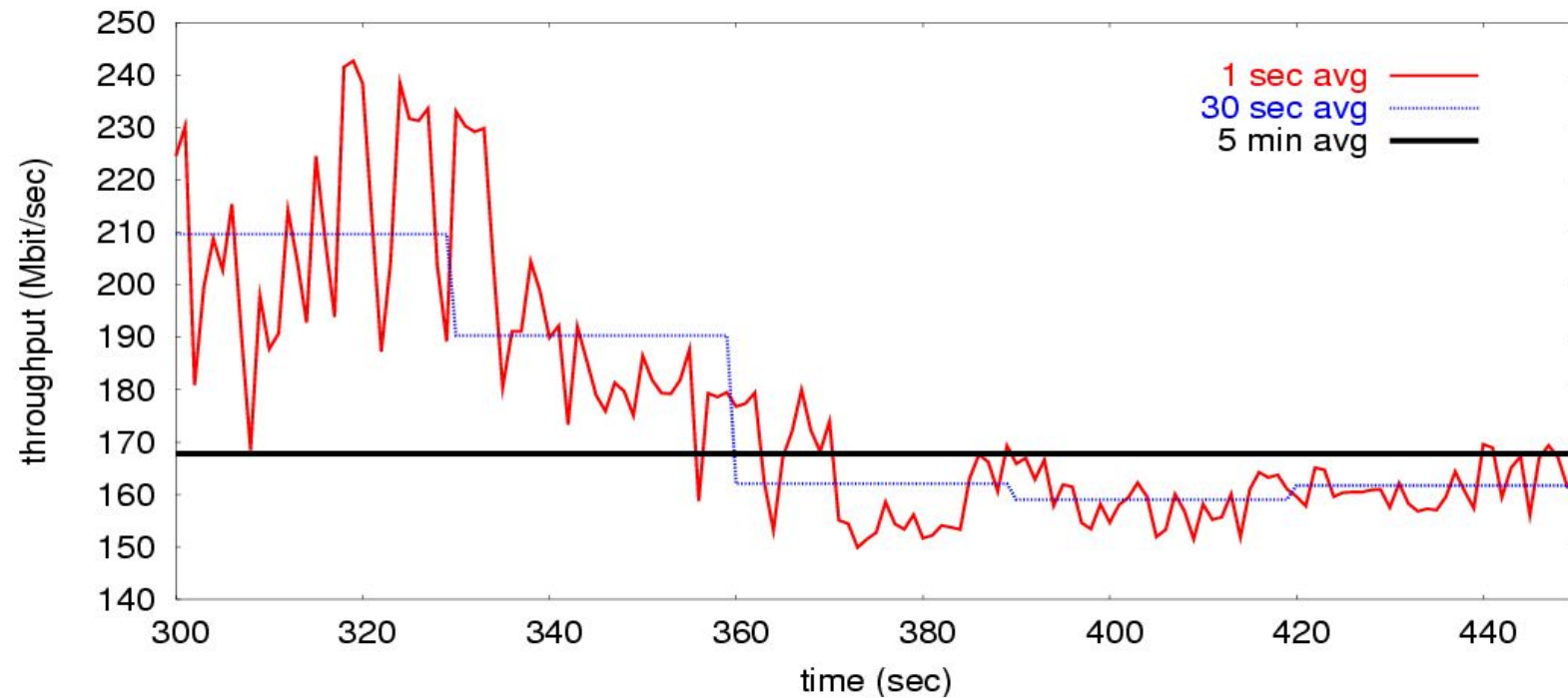
ACCOUNTING

NETWORK TOMOGRAPHY

NETWORK DIMENSIONING

CAPACITY OF LINKS

5 MIN. MRTG - 1 SECOND



GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

TRAFFIC ENGINEERING

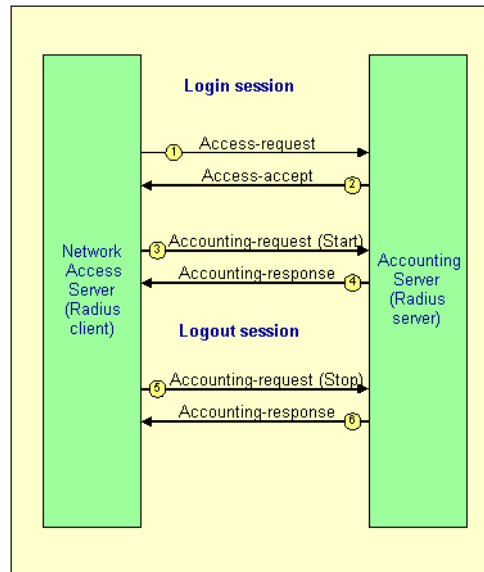
NETWORK DIMENSIONING

ACCOUNTING

NETWORK TOMOGRAPHY

ACCOUNTING

RADIUS



STOP:

- CURRENT TIME
- SESSION TIME
- INPUT OCTETS
- OUTPUT OCTETS
- INPUT PACKETS
- OUTPUT PACKETS
- DISCONNECT REASON

GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

TRAFFIC ENGINEERING

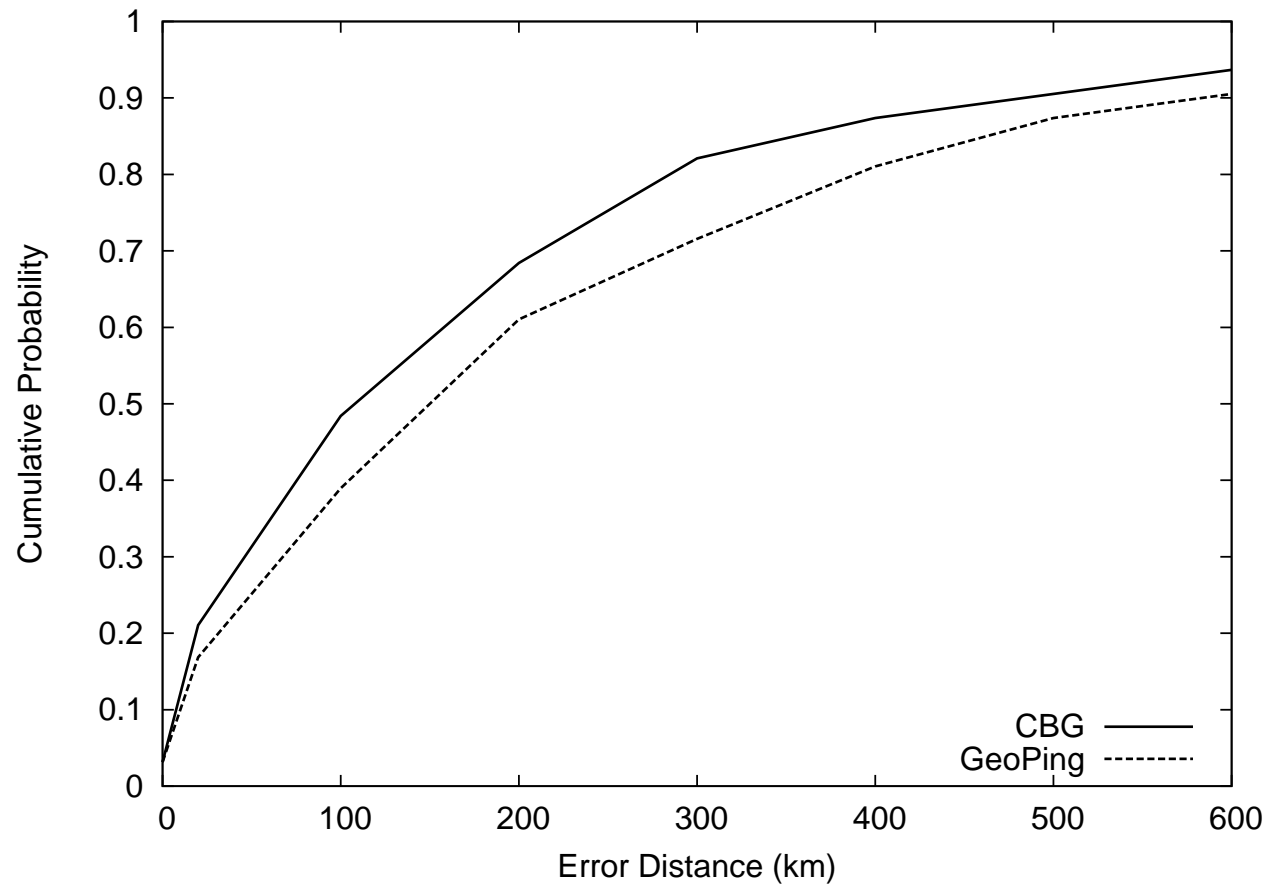
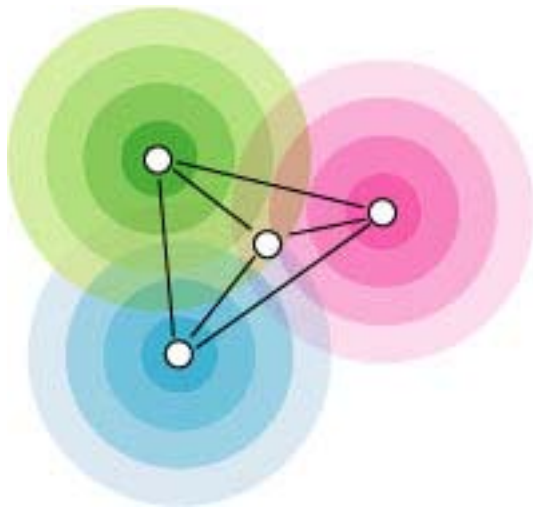
NETWORK DIMENSIONING

ACCOUNTING

NETWORK TOMOGRAPHY

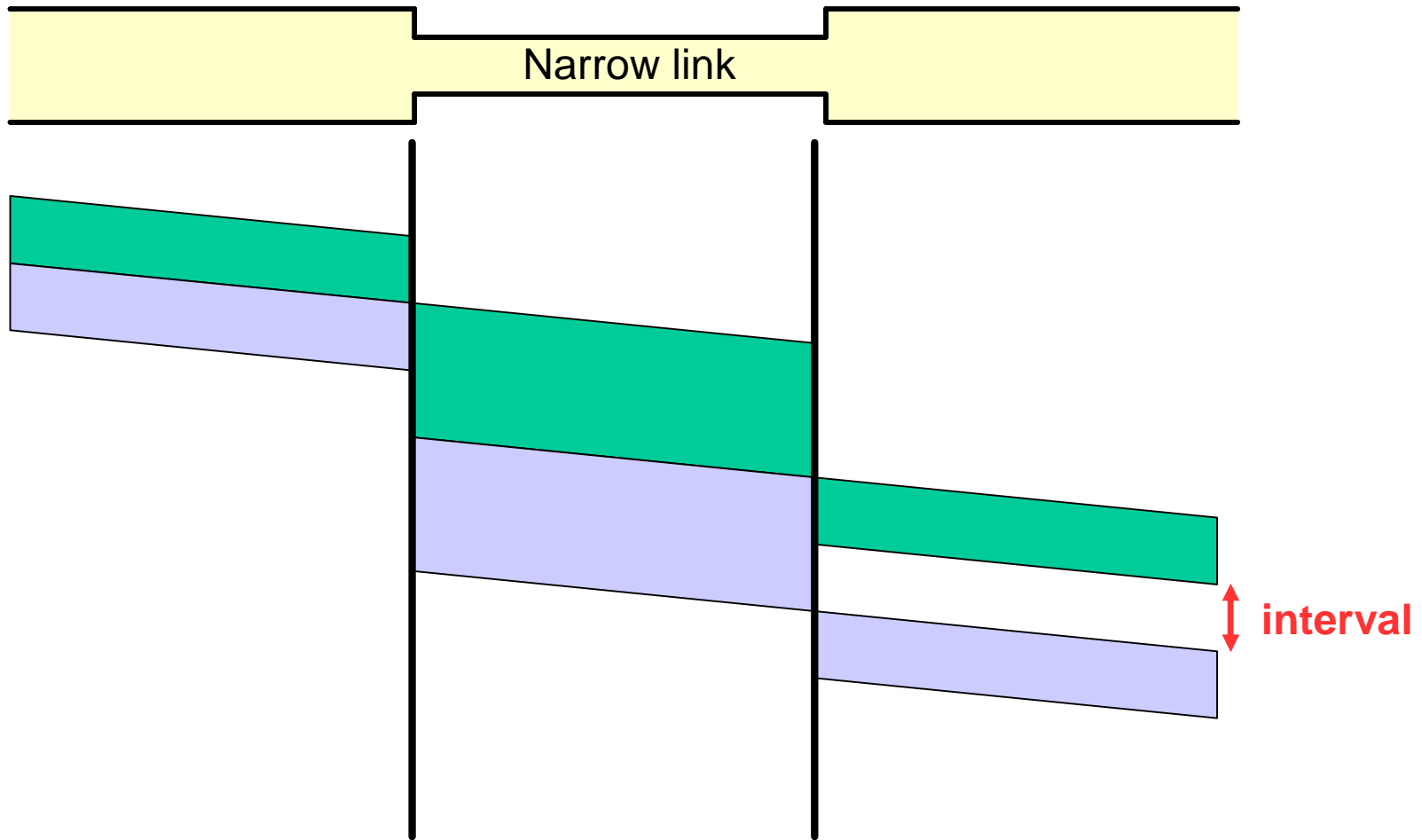
NETWORK TOMOGRAPHY

EXAMPLE: GEO-LOCATION OF INTERNET HOSTS

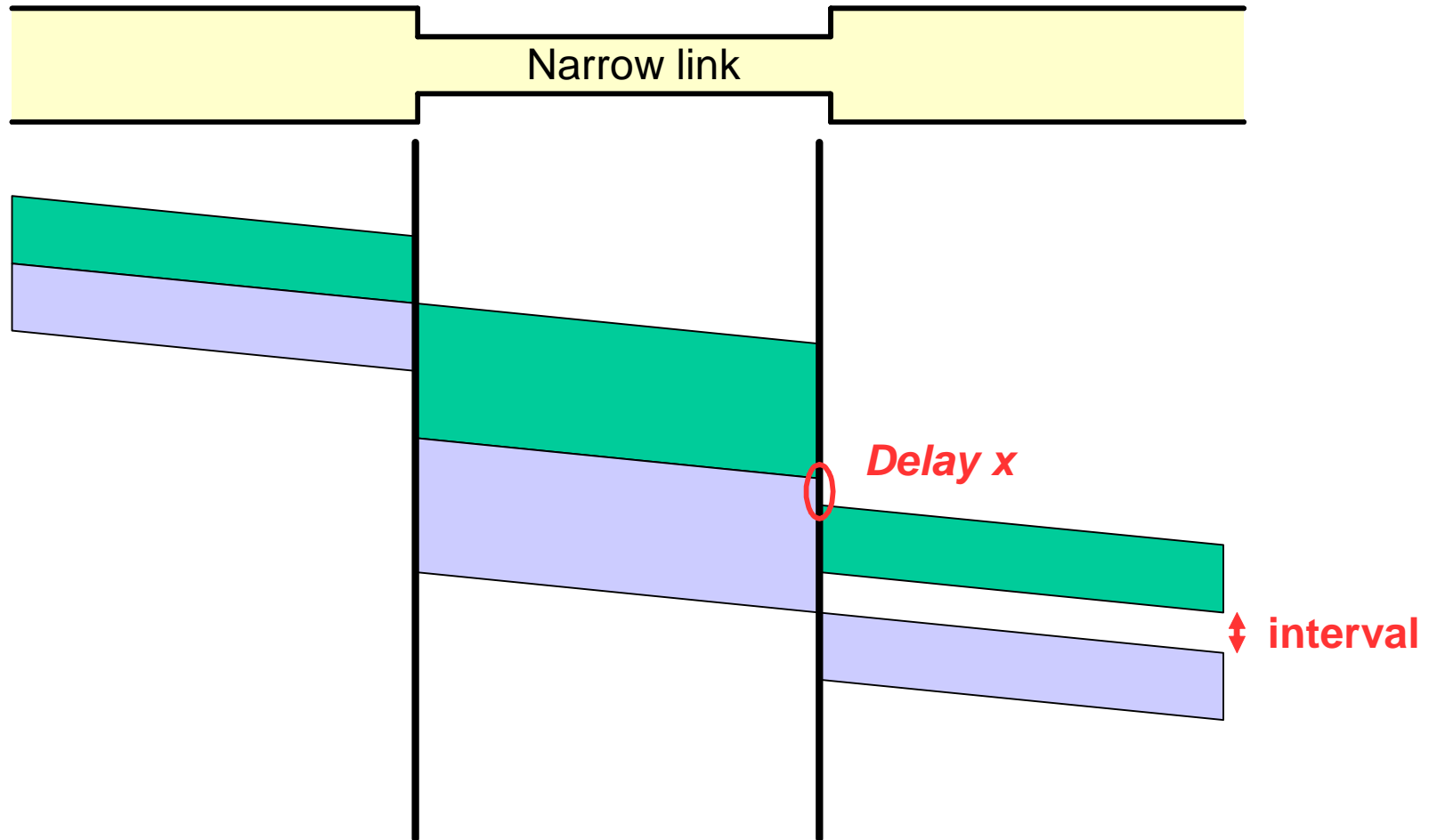


SOURCE: *Constraint-Based Geolocation of Internet Hosts* - B Gueye, A Ziviani, M Crovella, S Fdida
Proc. of the ACM Sigcomm Internet Measurement Conference, 2004

BANDWIDTH ESTIMATION



BANDWIDTH ESTIMATION



TECHNIQUES

ACTIVE MEASUREMENTS

- PING
- TRACEROUTE
- TCP/IP HEADER OPTIONS
- RIPE / SURVEYOR

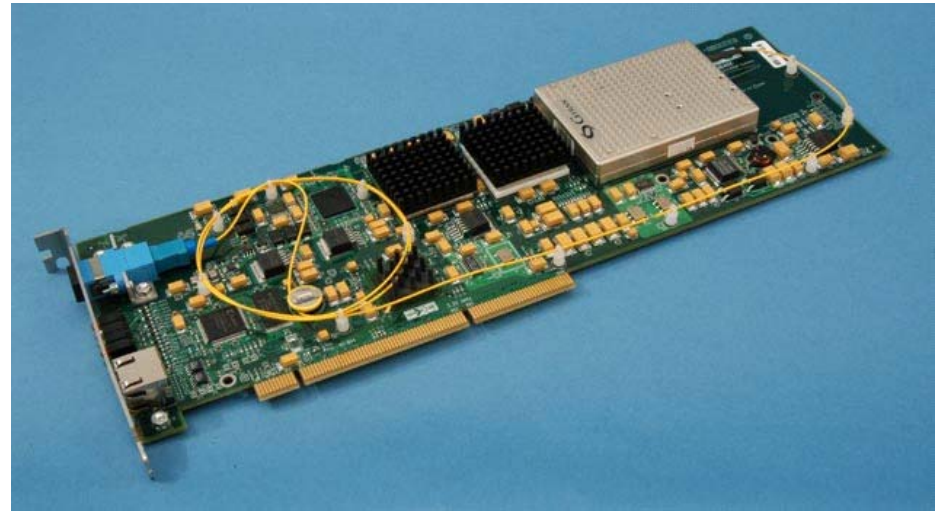
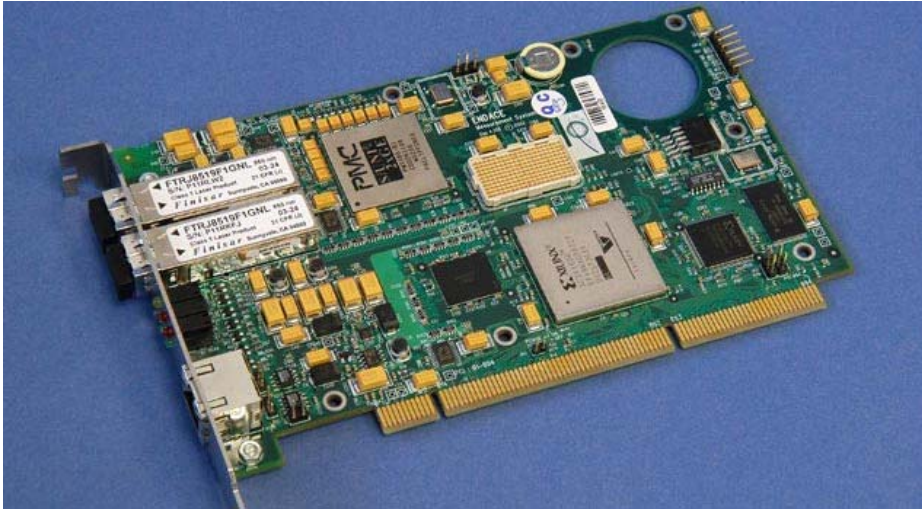
PASSIVE MEASUREMENTS

- PACKET CAPTURING
- TCPDUMP / NETFLOW / NETRAMET
- MIBs

PACKET SAMPLING

- TRAJECTORY SAMPLING

EXAMPLE: MEASUREMENT CARDS



EXAMPLE: TCPDUMP

CAN BE USED TO CAPTURE NETWORK TRAFFIC

NOT ONLY TCP

MANY CAPTURE OPTIONS AND FILTERS

MANY DISPLAY OPTIONS

PACKET CAPTURE (PCAP) LIBRARY

EXAMPLE: WIRESHARK

The screenshot displays the Wireshark interface with a packet capture of an HTTP GET request. The main pane shows a list of packets, with packet 16 selected. The packet list pane shows the following details:

No.	Time	Delta	Source	Destination	Protocol	Info
13	14.817570	14.817570	192.168.0.10	192.168.0.2	TCP	1242 > 80 [SYN] Seq=1404510823 Ack=0 win=65536
14	14.817689	0.000119	192.168.0.2	192.168.0.10	TCP	80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404510824
15	14.818178	0.000489	192.168.0.10	192.168.0.2	TCP	1242 > 80 [ACK] Seq=1404510824 Ack=3661615104
16	14.819035	0.000857	192.168.0.10	192.168.0.2	HTTP	GET / HTTP/1.1
17	14.975815	0.156780	192.168.0.2	192.168.0.10	TCP	80 > 1242 [ACK] Seq=3661615105 Ack=1404511234
23	19.382555	4.406740	192.168.0.10	192.168.0.2	TCP	1242 > 80 [FIN, ACK] seq=1404511234 Ack=3661615105
24	19.382634	0.000079	192.168.0.2	192.168.0.10	TCP	80 > 1242 [ACK] Seq=3661615105 Ack=1404511234
52	54.234482	34.851848	192.168.0.2	192.168.0.10	HTTP	HTTP/1.1 403 Forbidden (text/html)
53	54.235272	0.000790	192.168.0.10	192.168.0.2	TCP	1242 > 80 [RST] Seq=1404511235 Ack=366044707
54	58.137063	3.901791	192.168.0.10	192.168.0.2	TCP	1244 > 135 [SYN] Seq=1414452237 Ack=0 win=65536
55	58.137176	0.000113	192.168.0.2	192.168.0.10	TCP	135 > 1244 [SYN, ACK] Seq=3672465192 Ack=1414452237
56	58.137527	0.000351	192.168.0.10	192.168.0.2	TCP	1244 > 135 [ACK] Seq=1414452238 Ack=3672465192
57	58.137992	0.000465	192.168.0.10	192.168.0.2	DCERPC	Bind: call_id: 57 UUID: IOXIDResolver
58	58.188933	0.050941	192.168.0.2	192.168.0.10	DCERPC	Bind_ack: call_id: 57 accept max_xmit: 5840
59	58.189601	0.000668	192.168.0.10	192.168.0.2	IOXIDR	ComplexPing request AddToSet=0 DelFromSet=1
60	58.202631	0.013030	192.168.0.2	192.168.0.10	IOXIDR	ComplexPing response -> Unknown (0x00000778)
61	58.203457	0.000826	192.168.0.10	192.168.0.2	TOXIDR	ComplexPing request AddToSet=0 DelFromSet=1

The packet details pane for packet 16 shows the following structure:

- Frame 16 (464 bytes on wire, 464 bytes captured)
- Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
- Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
- Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, Ack: 3661615105, Len: 410
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Host: 192.168.0.2\r\n
 - User-Agent: Mozilla/5.0 (windows; U; windows NT 5.0; en-US; rv:1.5) Gecko/20031007\r\n
 - Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.5\r\n
 - Accept-Language: en-us,en;q=0.5\r\n
 - Accept-Encoding: gzip,deflate\r\n
 - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
 - Keep-Alive: 300\r\n
 - Connection: keep-alive\r\n

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 0b 5d 20 cd 02 00 04 61 4a 1e 95 08 00 45 00  ..]....aJ....E.
0010 01 c2 d1 6d 40 00 80 06 a6 6b c0 a8 00 0a c0 a8  ...m@... .k.....
0020 00 02 04 da 00 50 53 b7 22 68 da 3f d0 01 50 18  ....PS. "h?.?P.
0030 ff ff 46 26 00 00 47 45 54 20 2f 20 48 54 54 50  ..F&..GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e  /1.1..Host: 192.
0050 168.0.2  User-Age
```

The filter bar at the bottom shows the filter: tcp. The status bar indicates the file is 'few packets.cap' (24 KB) and the capture is at position 104 D: 19 M: 0.

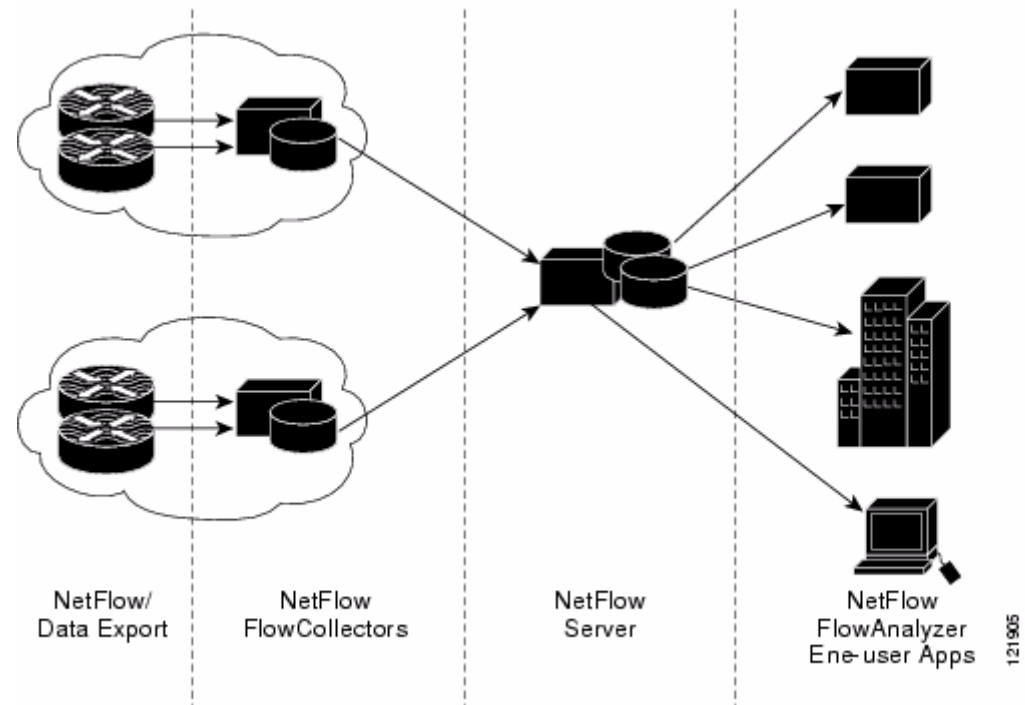
EXAMPLE: NETFLOW

- CISCO
- IETF-IPFIX

FLOW:

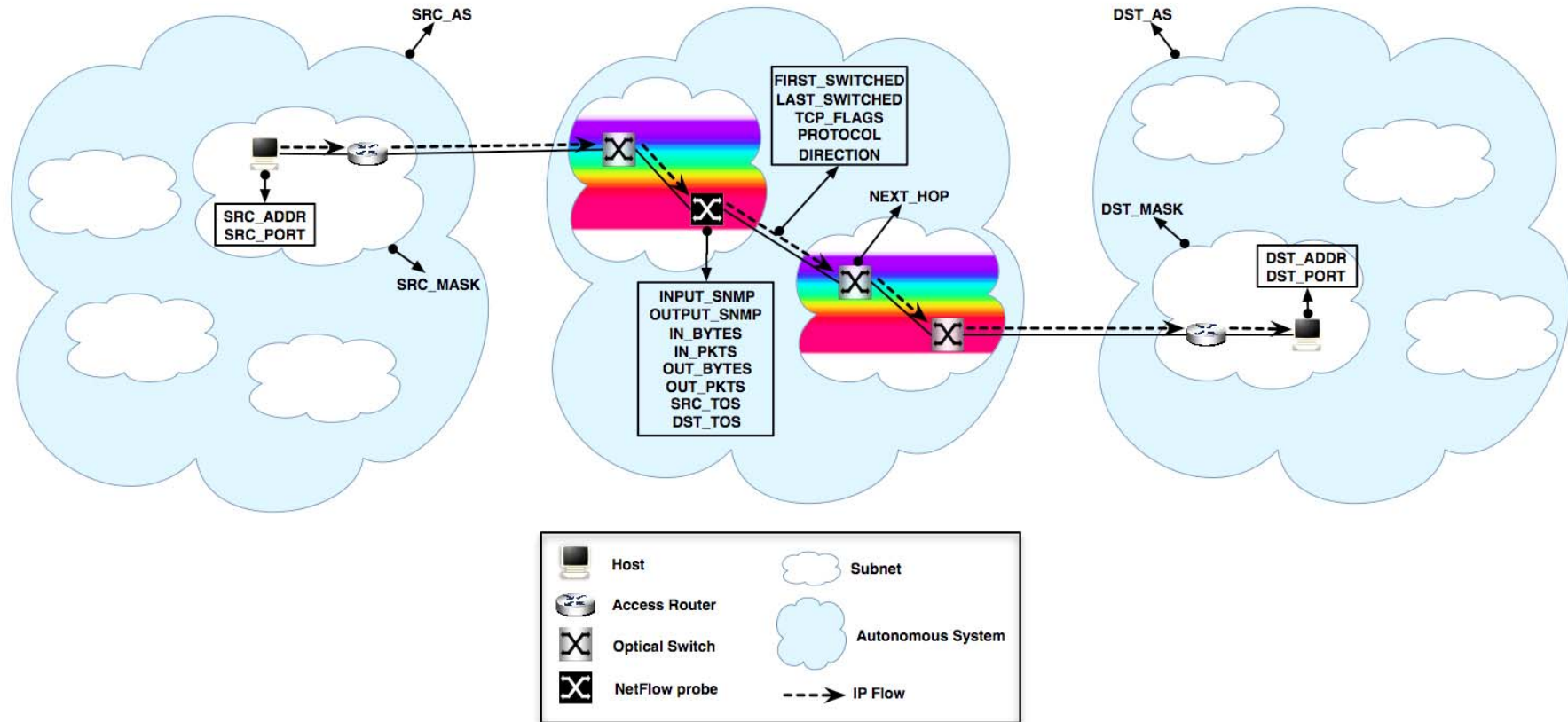
- SOURCE IP ADDRESS
- DESTINATION IP ADDRESS
 - SOURCE PORT NUMBER
- DESTINATION PORT NUMBER
 - LAYER 3 PROTOCOL TYPE
 - TOS BYTE
- INPUT LOGICAL INTERFACE (IFINDEX)

EXAMPLE: NETFLOW



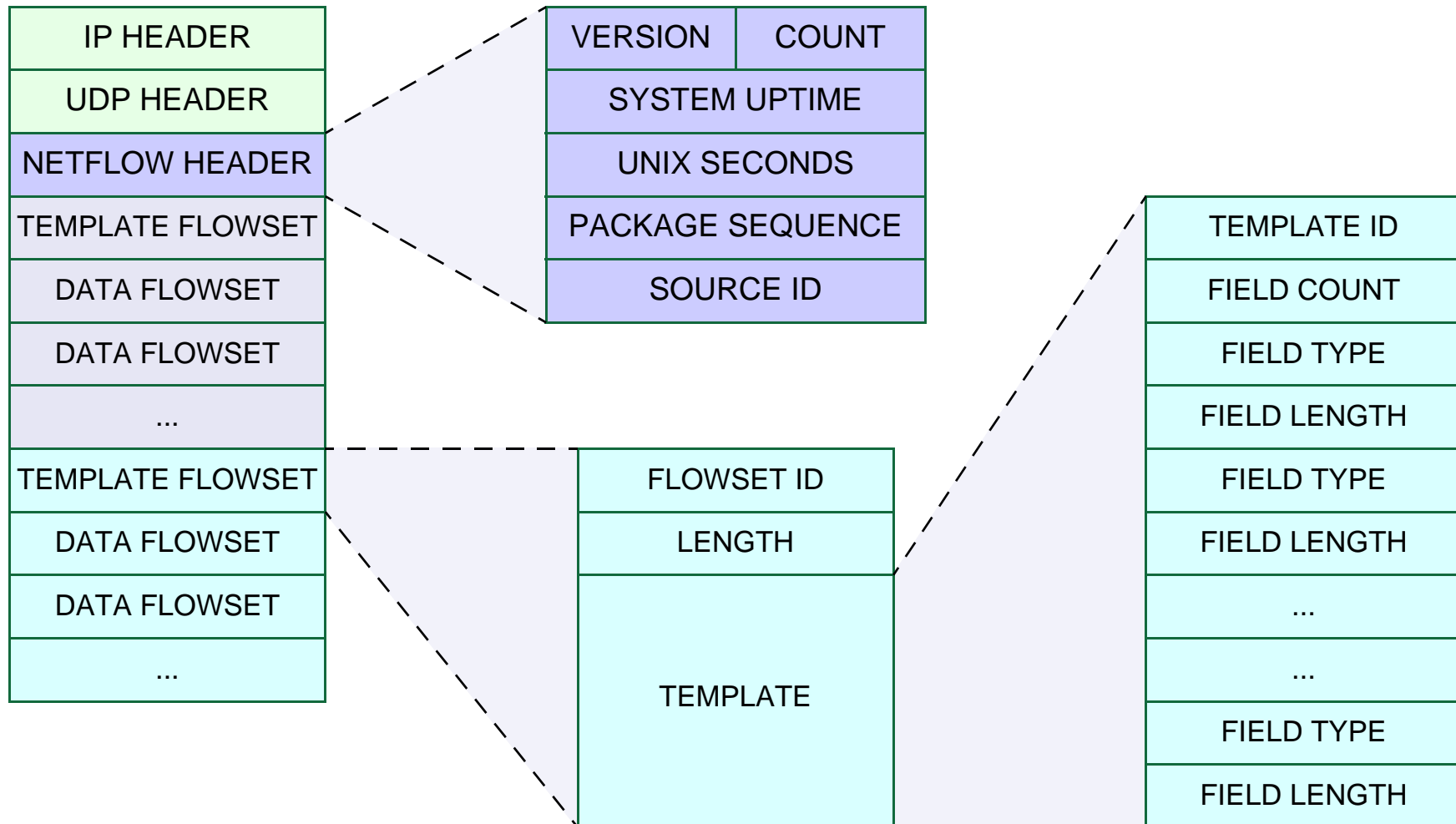
SOURCE: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm>

EXAMPLE: NETFLOW



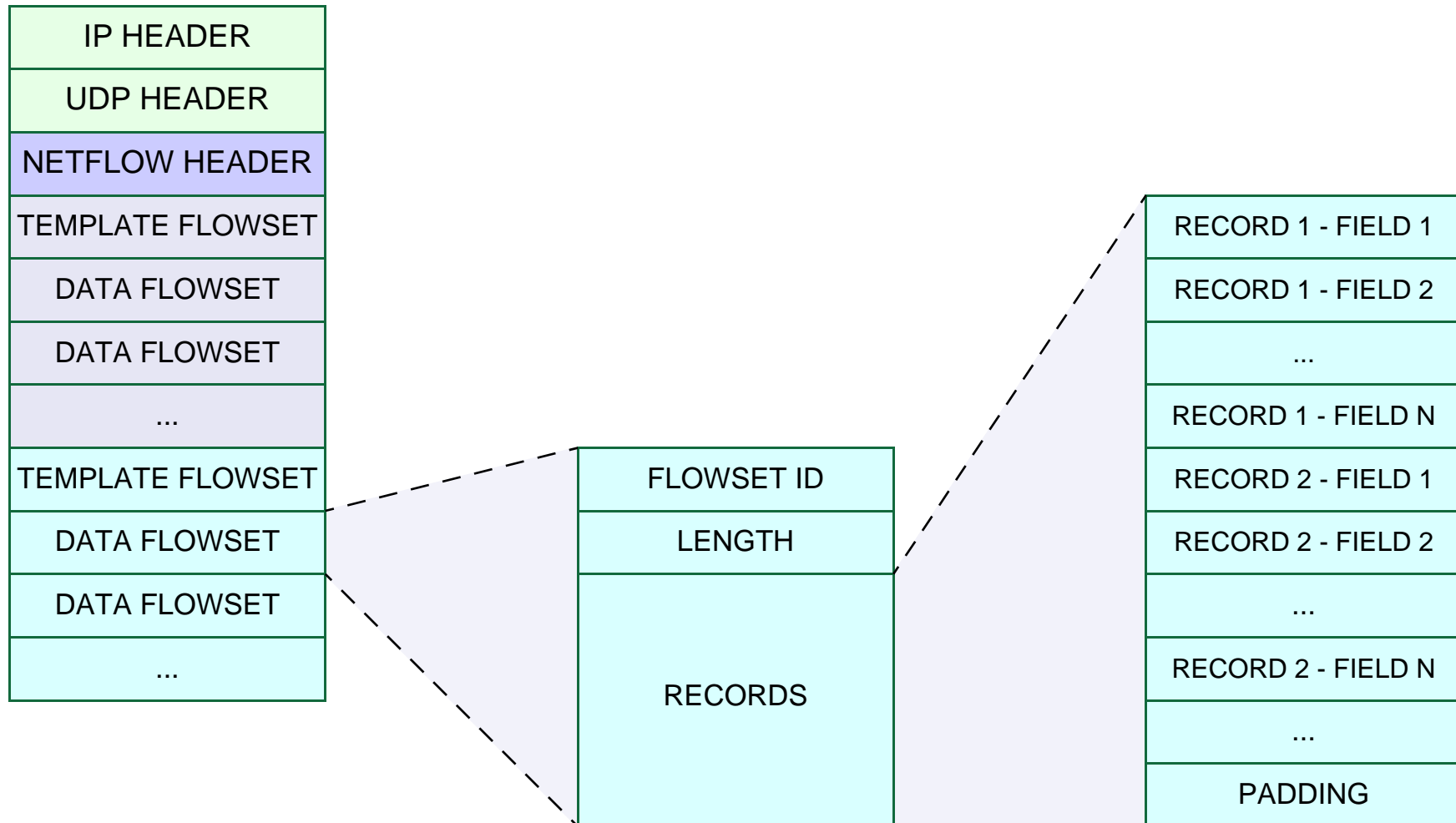
CAPTION

EXAMPLE: NETFLOW V9 (1)



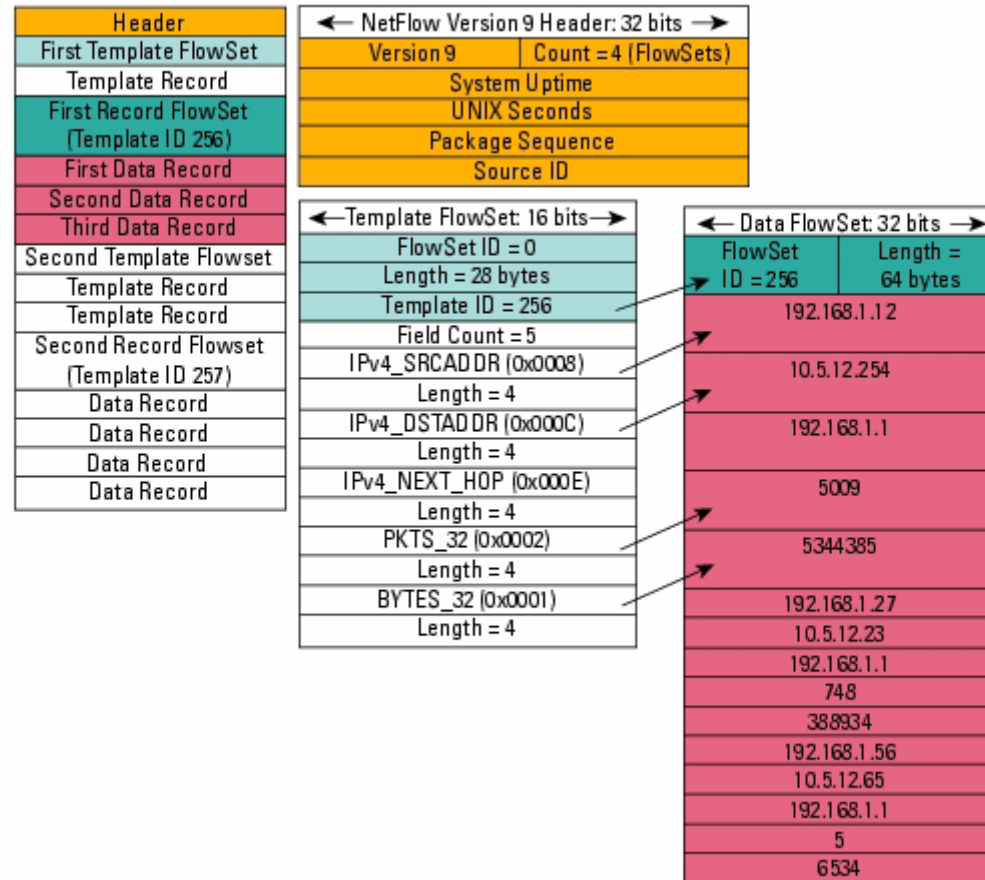
SOURCE: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/tflow_wp.htm#wp1002063

EXAMPLE: NETFLOW V9 (2)



SOURCE: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/tflow_wp.htm#wp1002063

EXAMPLE: NETFLOW V9 (3)



SOURCE: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/tflow_wp.htm#wp1002063