MEASUREMENTS

OVERVIEW:

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

WHAT IS BEING MEASURED?

DELAY
- ONE-WAY
- ROUND-TRIP

DELAY VARIATION
- JITTER

THROUGHPUT
- AVARAGE
- PEAK
- CAPACITY

LOSS

GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

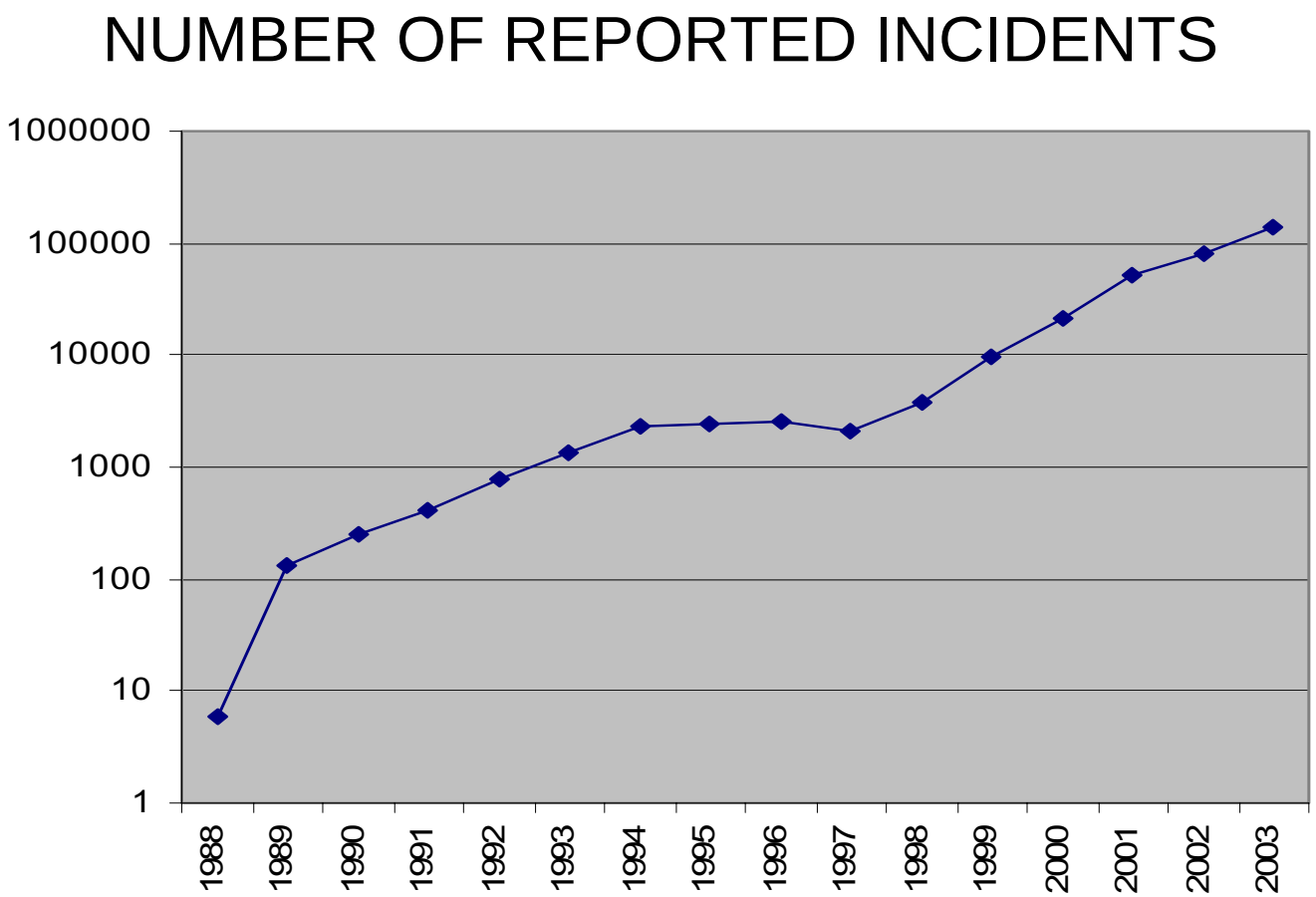
TRAFFIC ENGINEERING

NETWORK DIMENSIONING

ACCOUNTING

NETWORK TOMOGRAPHY

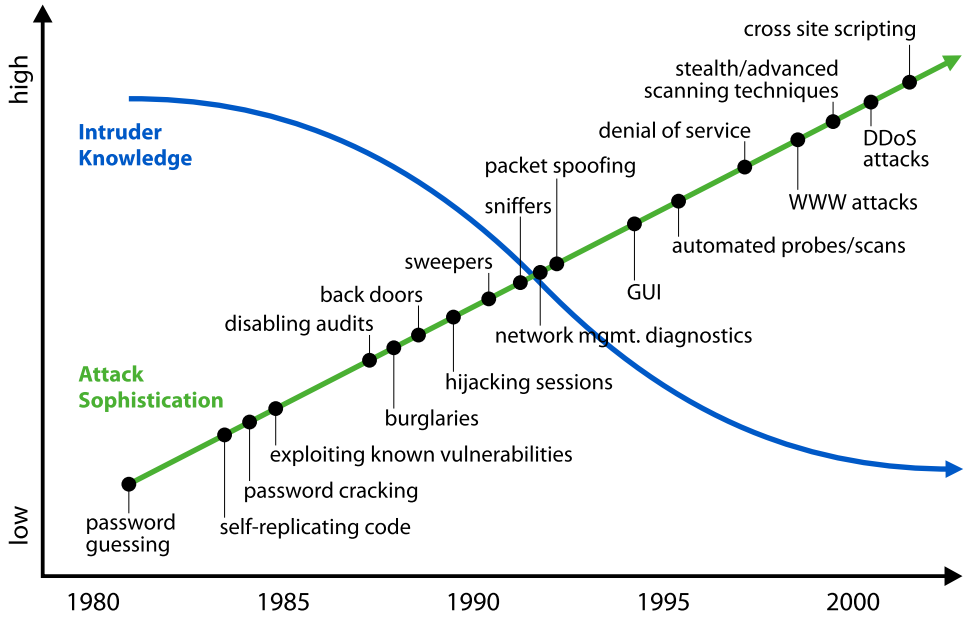
INTRUSION DETECTION - INCIDENTS - 1



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

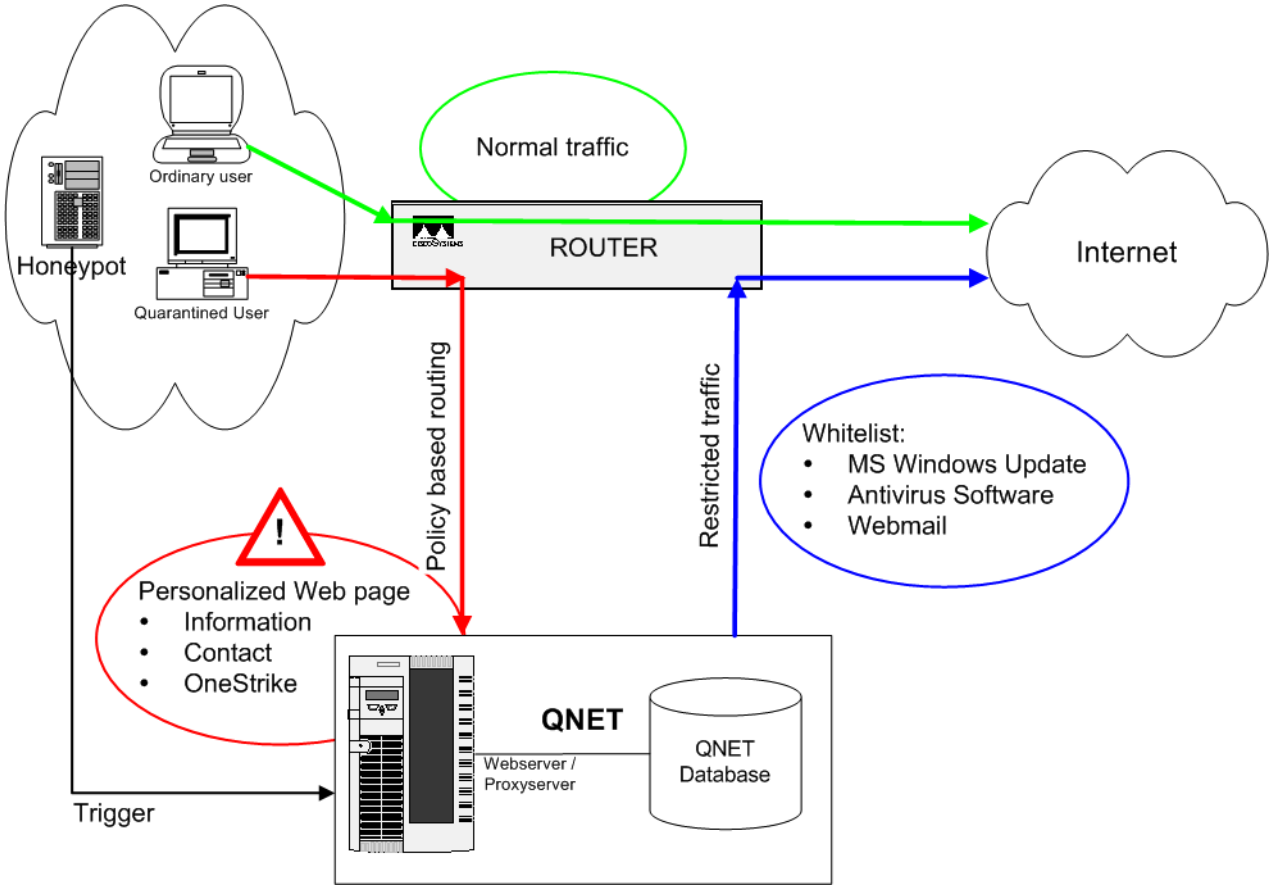
- HOST
- (DISTRIBUTED) HONEYPOT

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

Reference: Characteristics of Internet Background Radiation
R Pang, V Yegneswaran, P Barford, V Paxson, L Peterson Proc. of the ACM Sigcomm Internet Measurement Conference
Taormina, Sicily, Italy 2004

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%

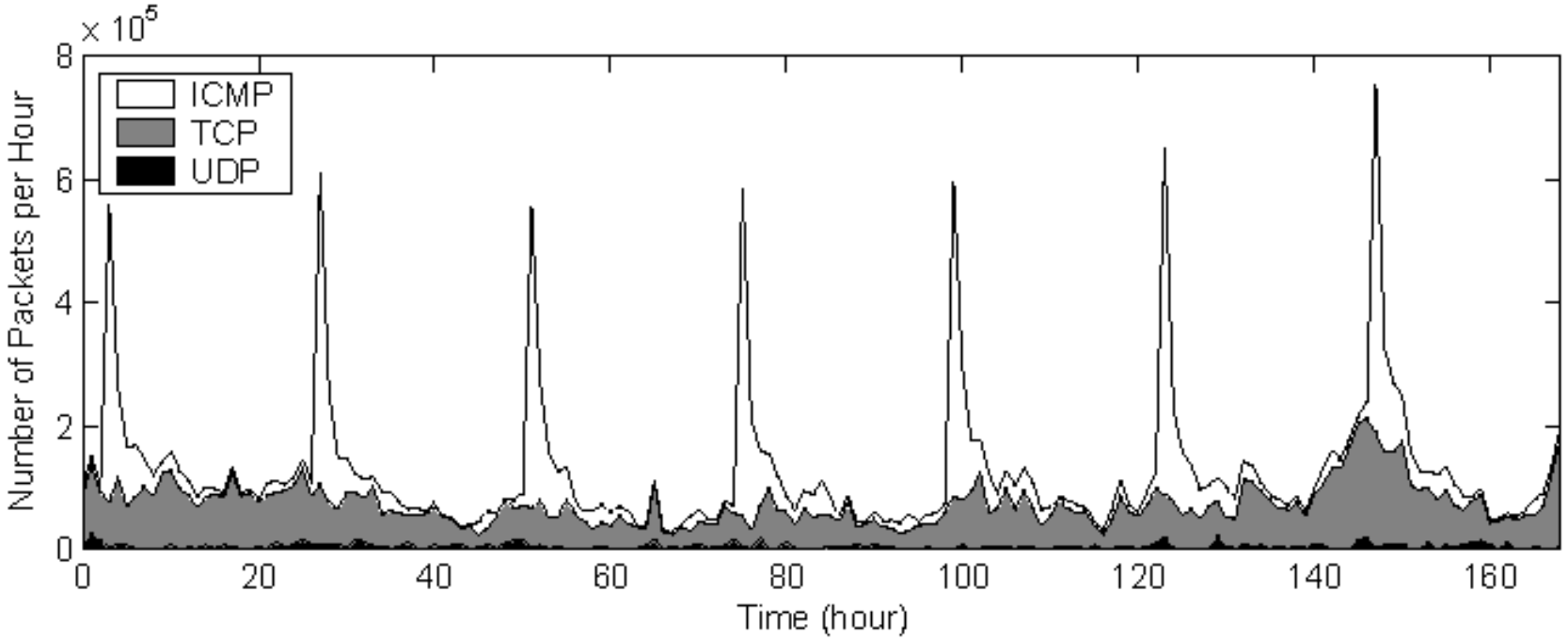
BACKGROUND RADIATION

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%

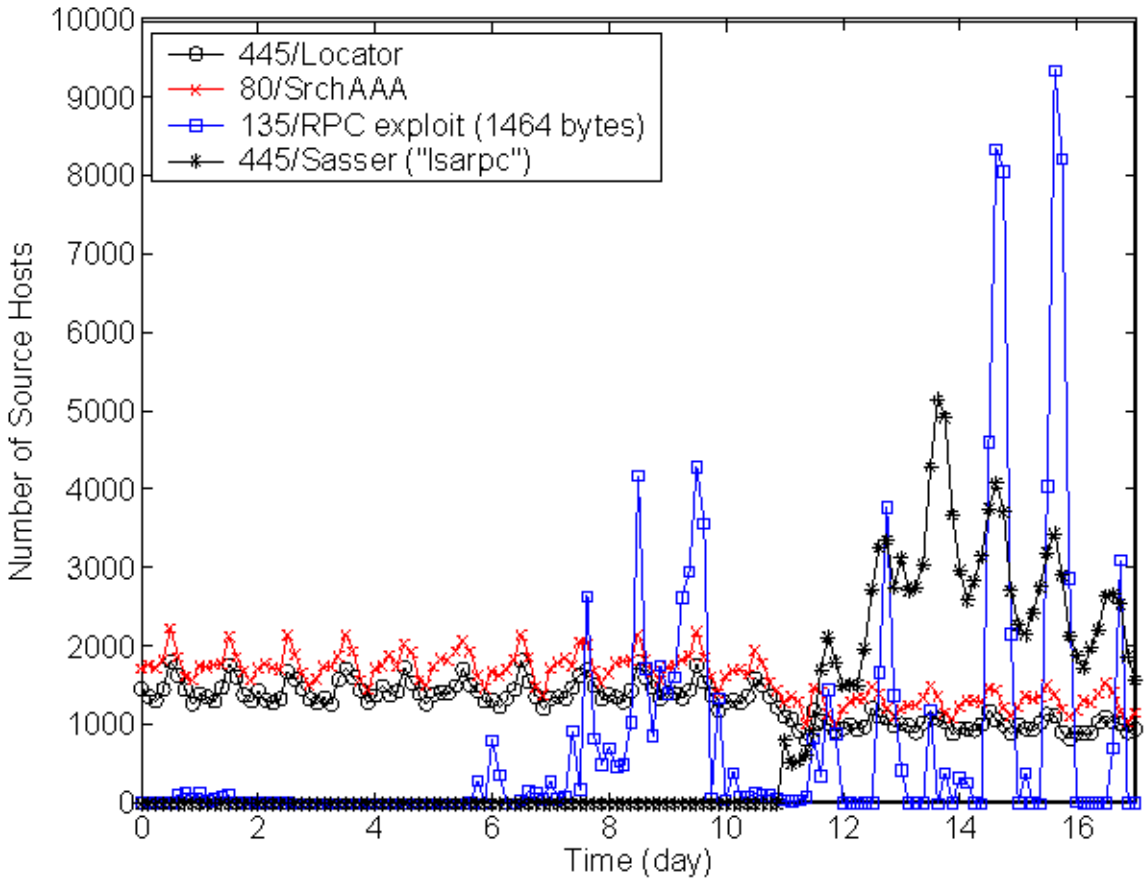
BACKGROUND RADIATION

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

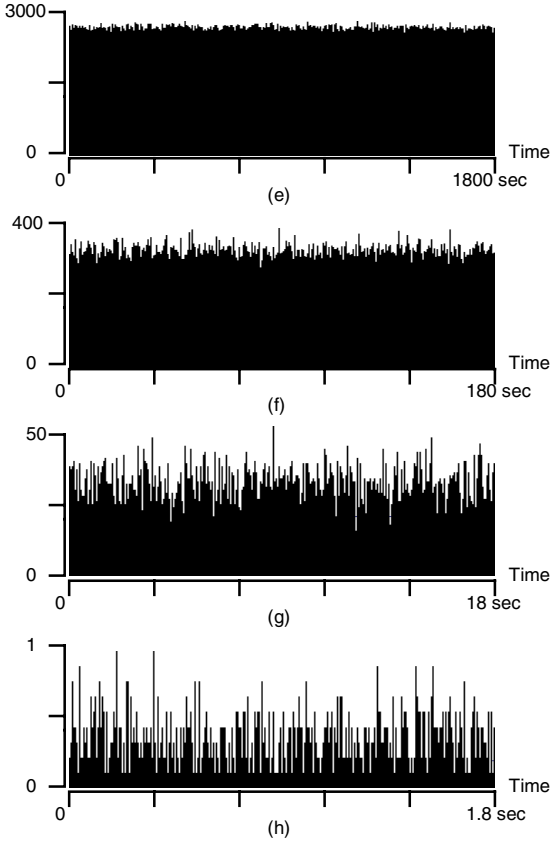
POISSON ARRIVAL PROCESS

GAUSSIAN TRAFFIC MODELS

SELF-SIMILARITY / LONG RANGE DEPENDANCE

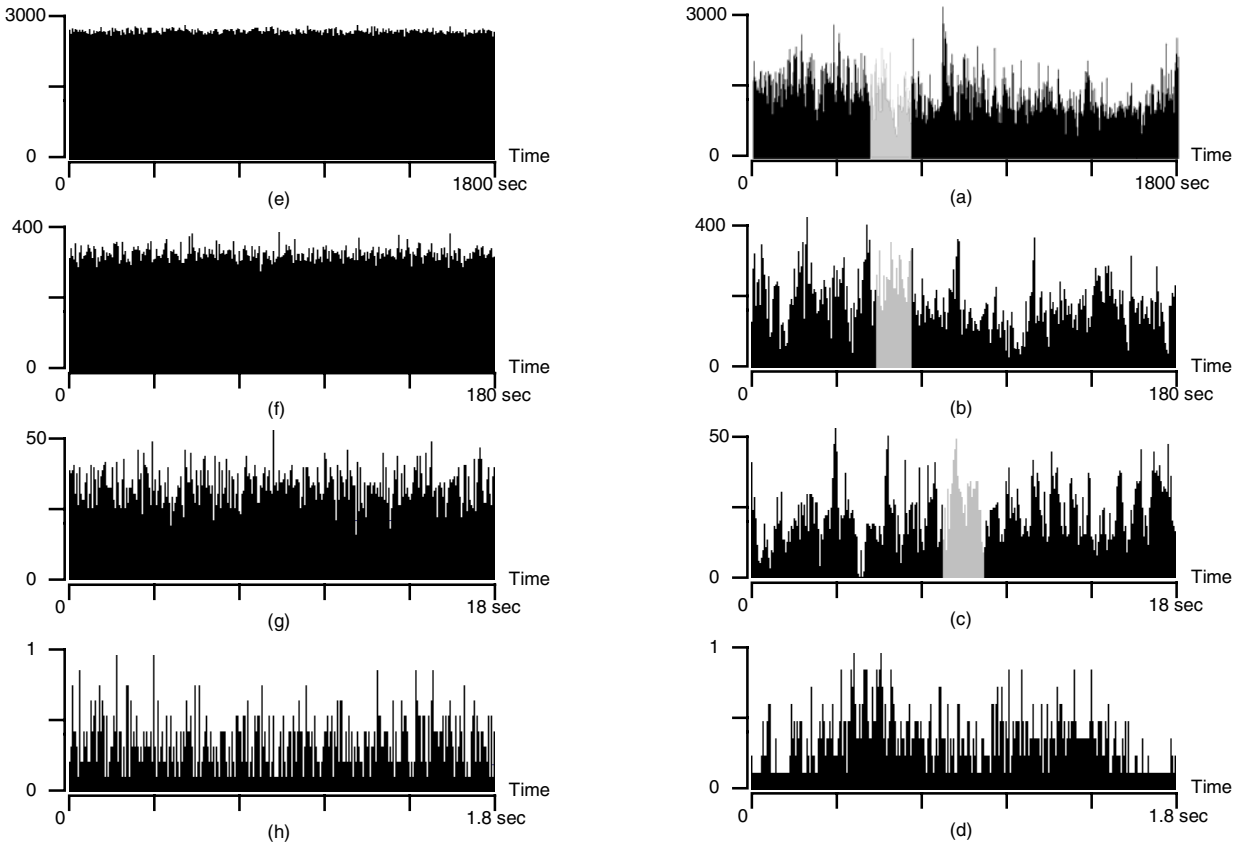
HEAVY TAIL DISTRIBUTION

TRAFFIC ENGINEERING - SELF SIMILARITY



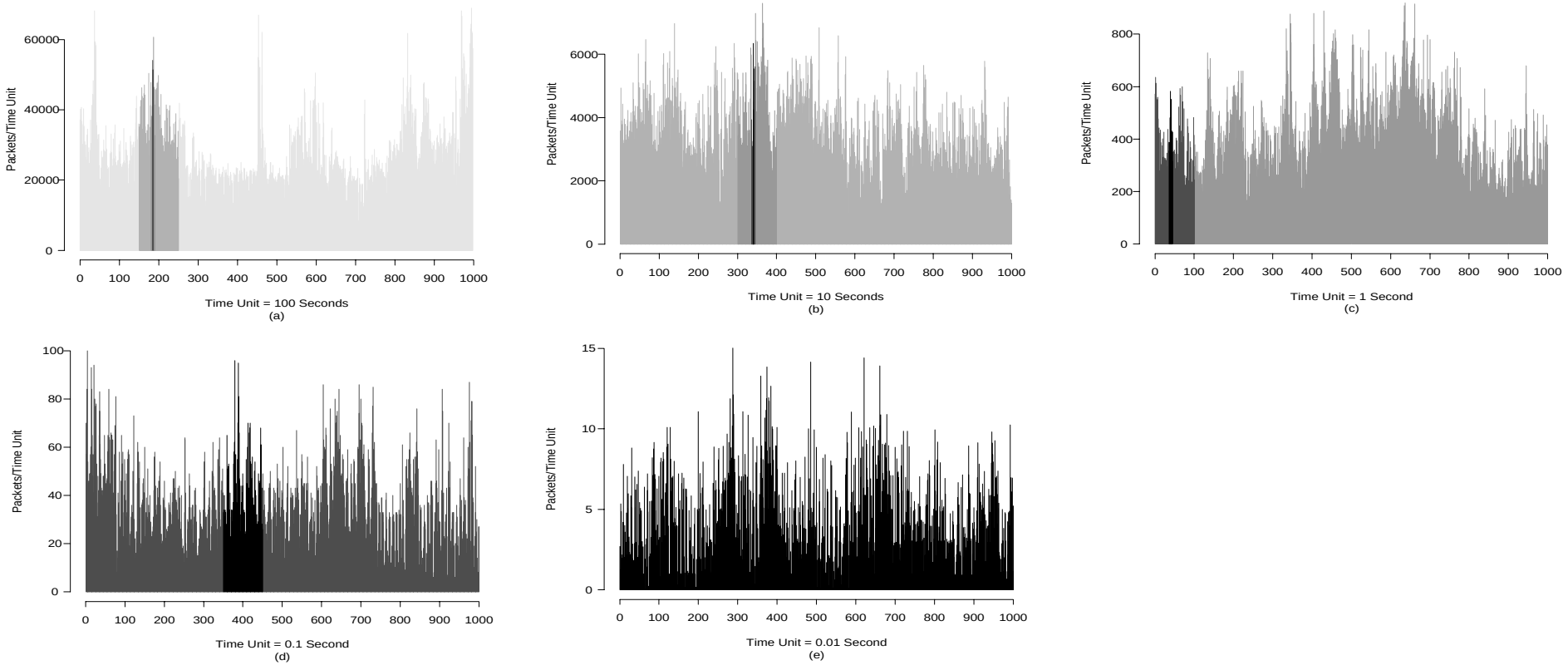
SOURCE: Traffic Characterisation for Telecommunication Networks
Attila Vidács, Zsolt Kenesi, Ákos Rétfalvi, Péter Pozsgai, Sándor Molnár - BUTE, Budapest, 1999

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

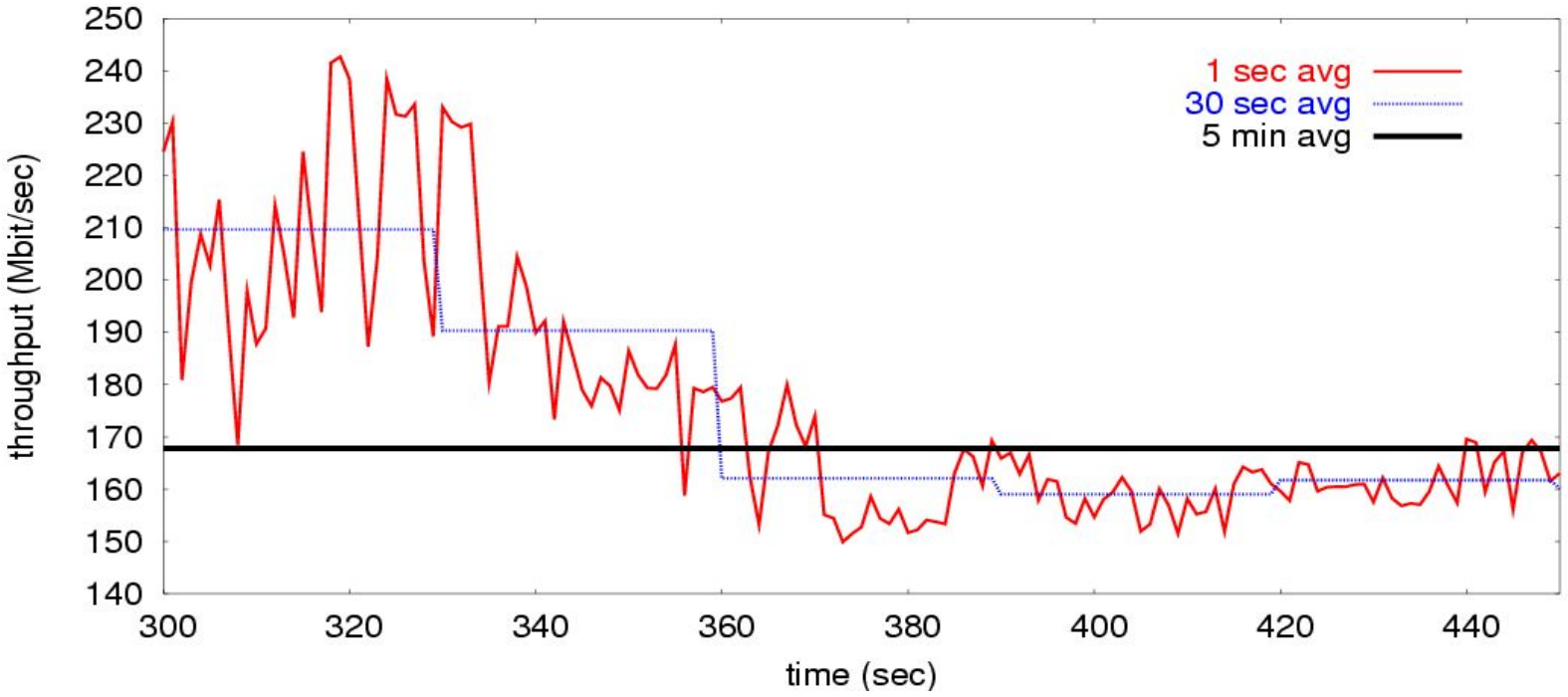
ACCOUNTING

NETWORK TOMOGRAPHY

NETWORK DIMENSIONING

CAPACITY OF LINKS

5 MIN. MRTG - 1 SECOND



GOALS OF MEASUREMENTS

INTRUSION DETECTION

LAWFULL INTERCEPTION

TRAFFIC ENGINEERING

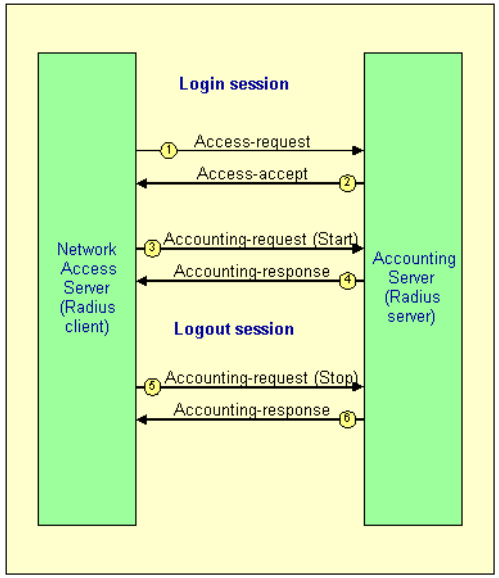
NETWORK DIMENSIONING

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

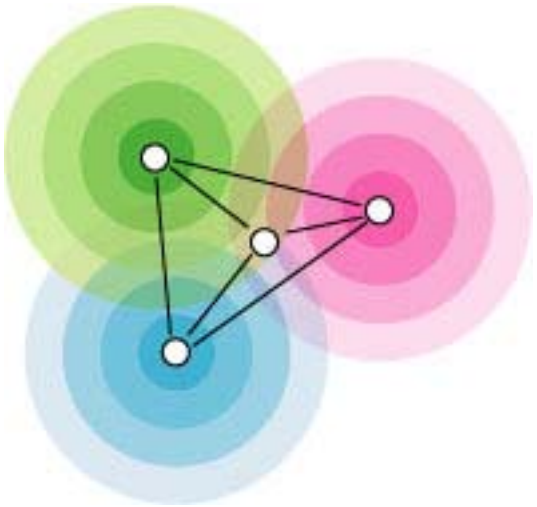
NETWORK DIMENSIONING

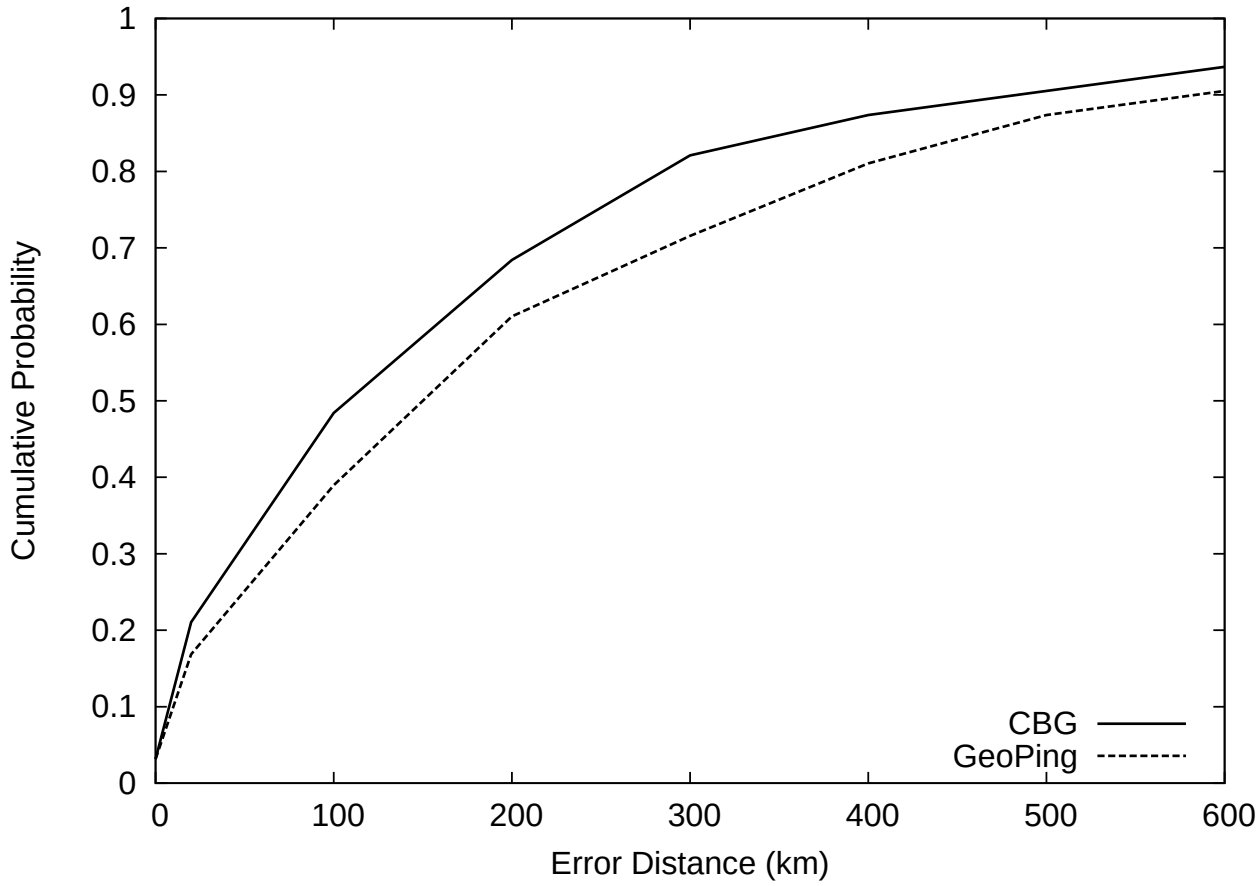
ACCOUNTING

NETWORK TOMOGRAPHY

NETWORK TOMOGRAPHY

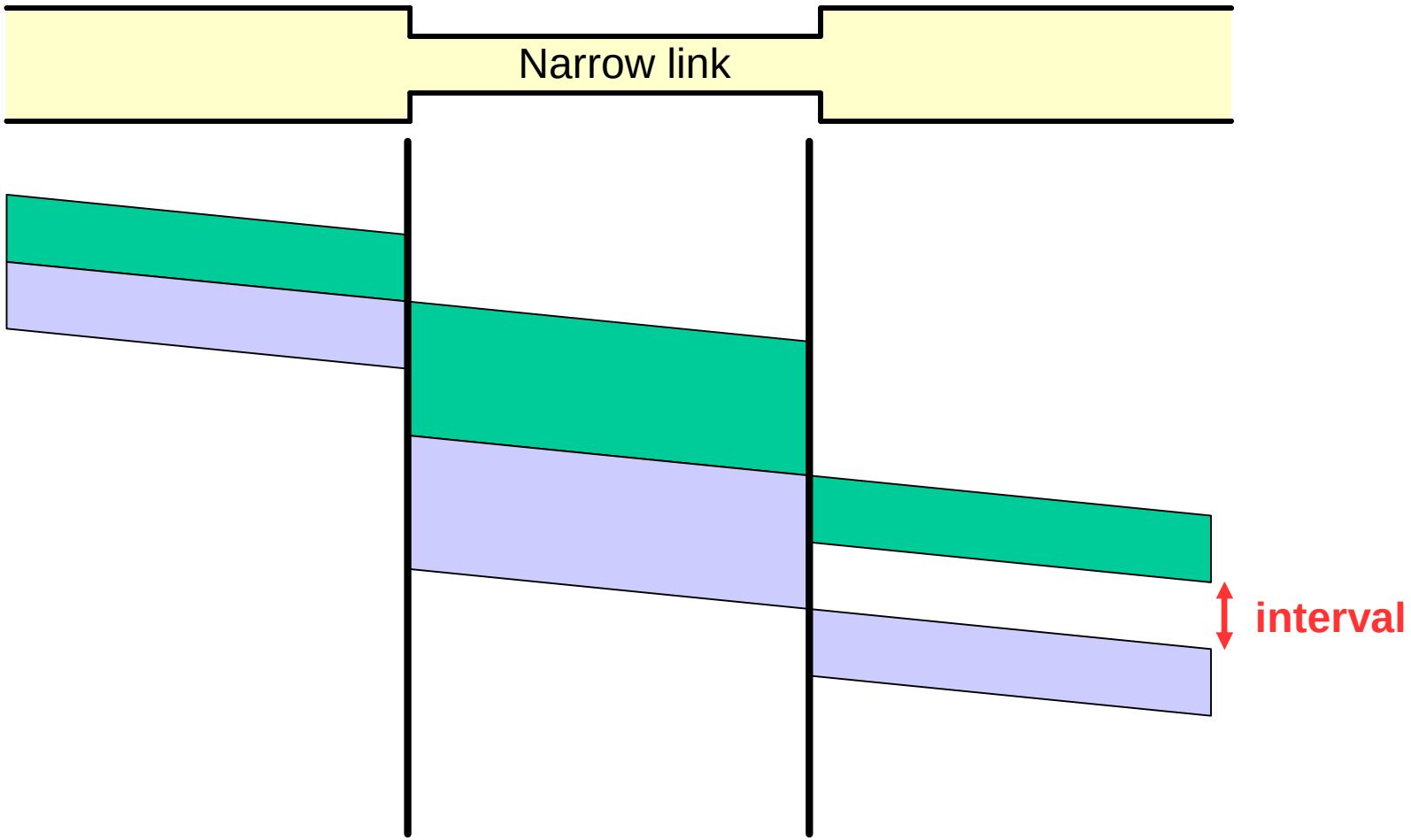
EXAMPLE: GEO-LOCATION OF INTERNET HOSTS



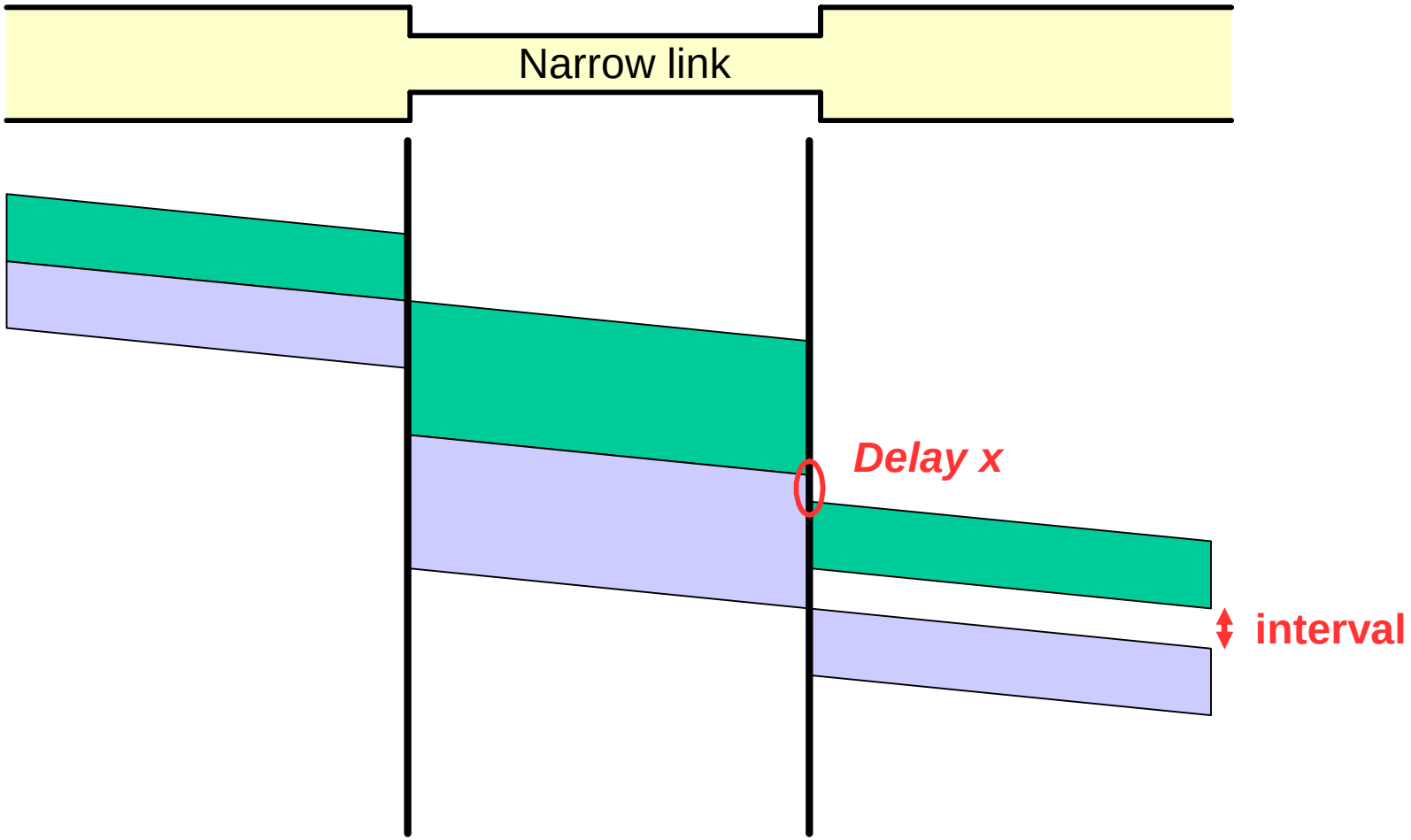


SOURCE: Constraint-Based Geolocation of Internet Hosts - B Gueye, A Ziviani, M Crovella, S Fdida
Proc. of the ACM Sigcomm Internet Measurement Conference, 2004

BANDWIDTH ESTIMATION



BANDWIDTH ESTIMATION



TECHNIQUES

ACTIVE MEASUREMENTS

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

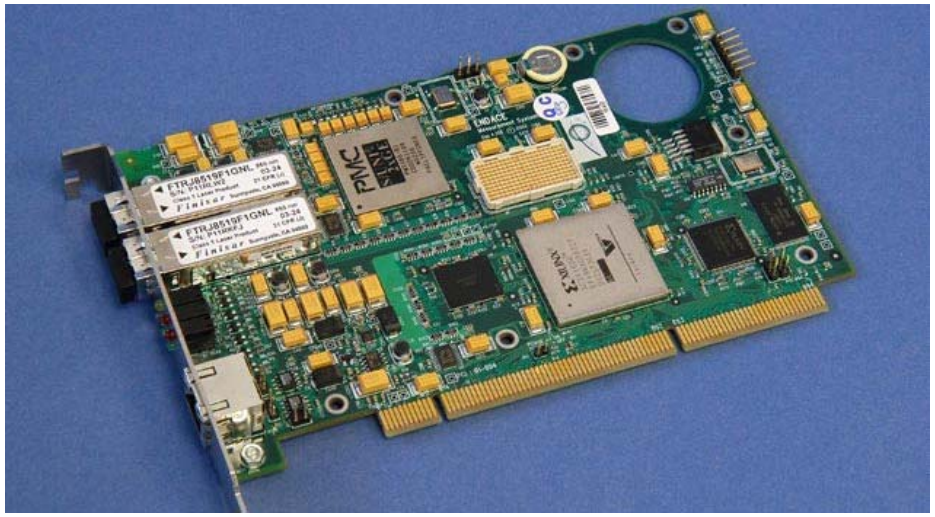
PASSIVE MEASUREMENTS

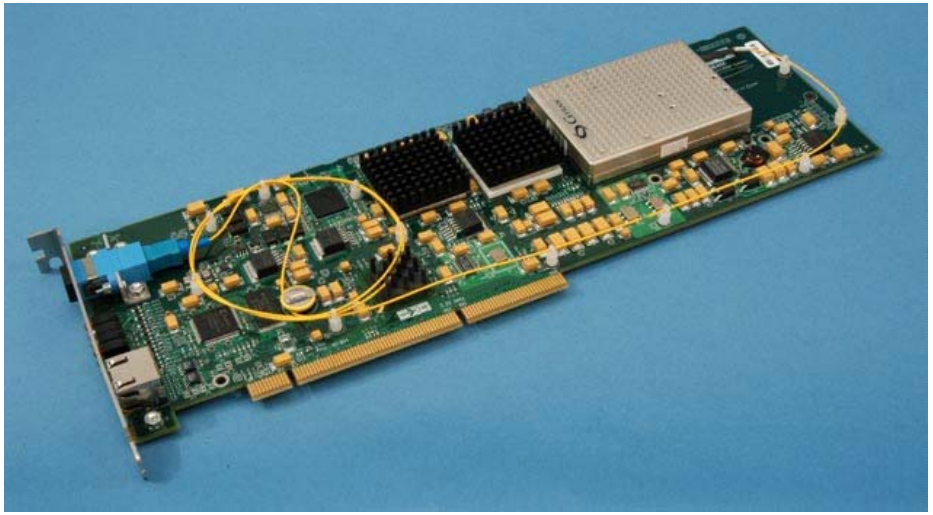
- PACKET CAPTURING
- TCPDUMP / NETFLOW / NETRAMET
- MIBs

PACKET SAMPLING

- TRAJECTORY SAMPLING

EXAMPLE: MEASUREMENT CARDS





EXAMPLE: TCPDUMP

CAN BE USED TO CAPTURE NETWORK TRAFFIC

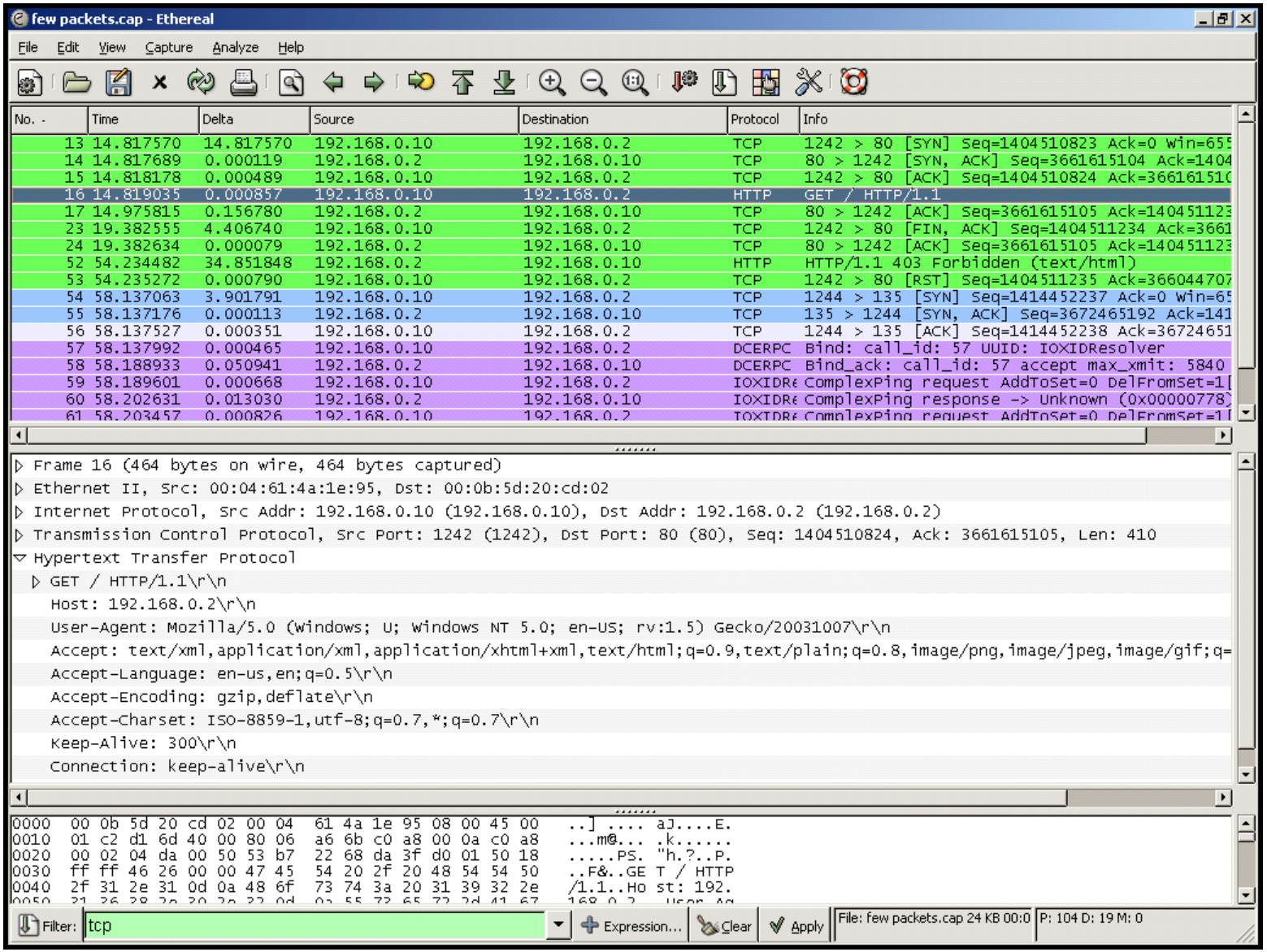
NOT ONLY TCP

MANY CAPTURE OPTIONS AND FILTERS

MANY DISPLAY OPTIONS

PACKET CAPTURE (PCAP) LIBRARY

EXAMPLE: WIRESHARK



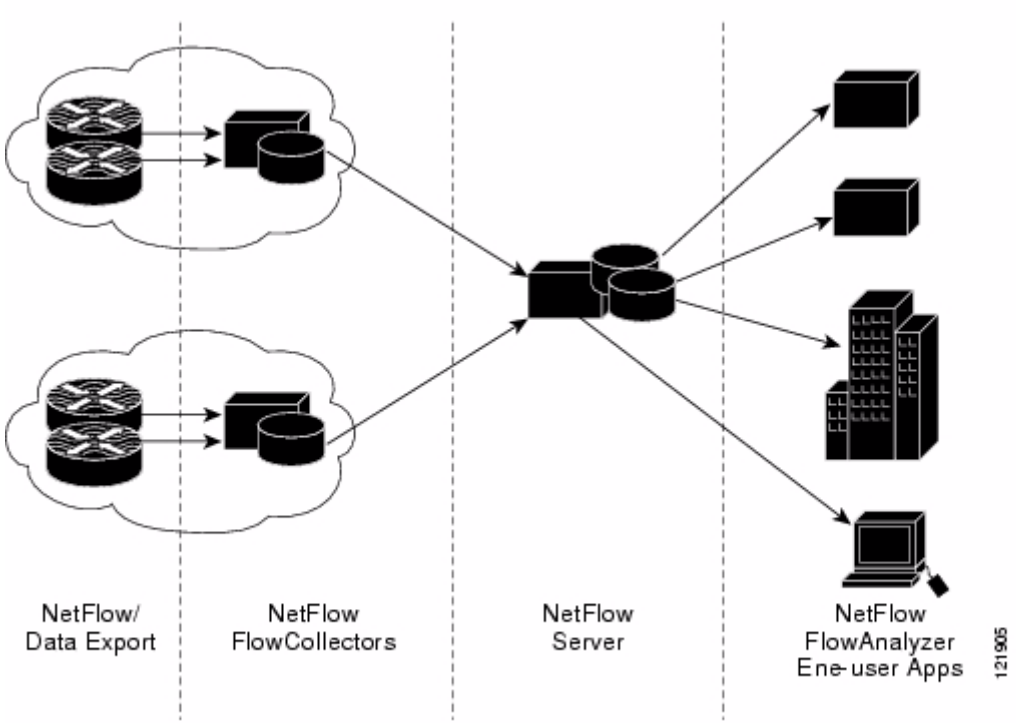
EXAMPLE: NETFLOW

- CISCO
- IETF-IPFIX

FLOW:

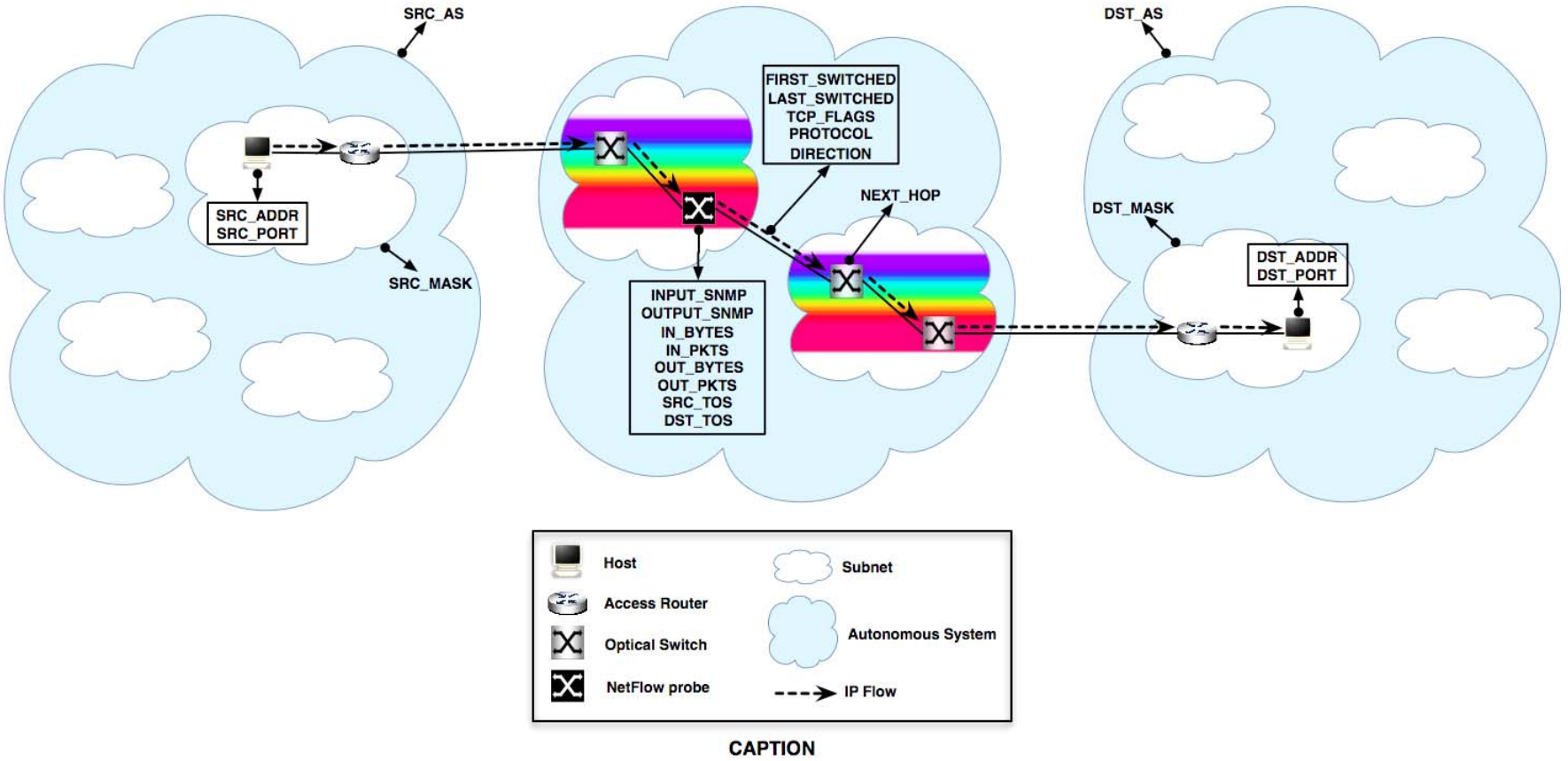
- SOURCE IP ADDRESS
- DESTINATION IP ADDRESS
- SOURCE PORT NUMBER
- DESTINATION PORT NUMBER
- LAYER 3 PROTOCOL TYPE
- TOS BYTE
- INPUT LOGICAL INTERFACE (IFINDEX)

EXAMPLE: NETFLOW



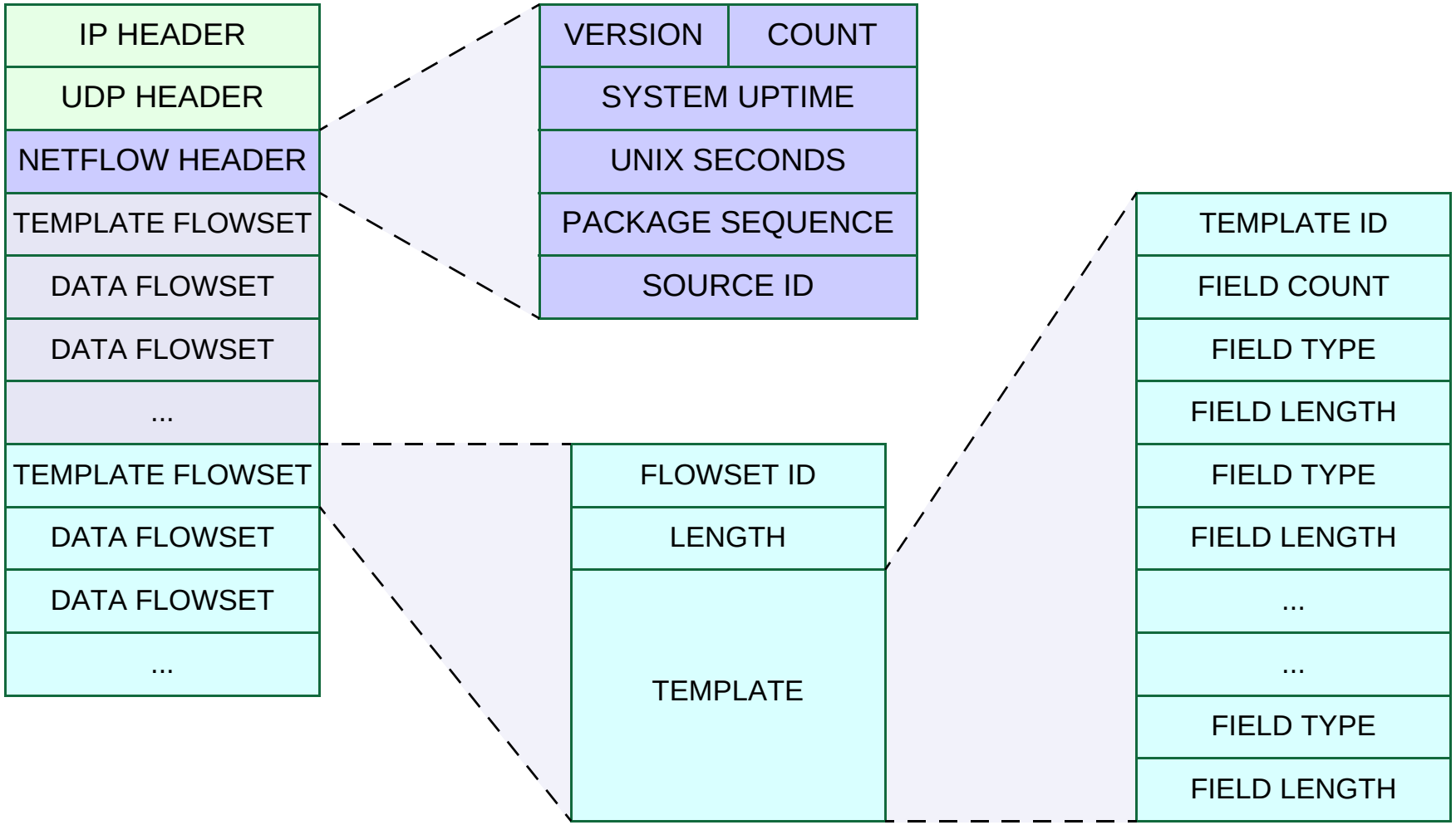
SOURCE: http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm

EXAMPLE: NETFLOW



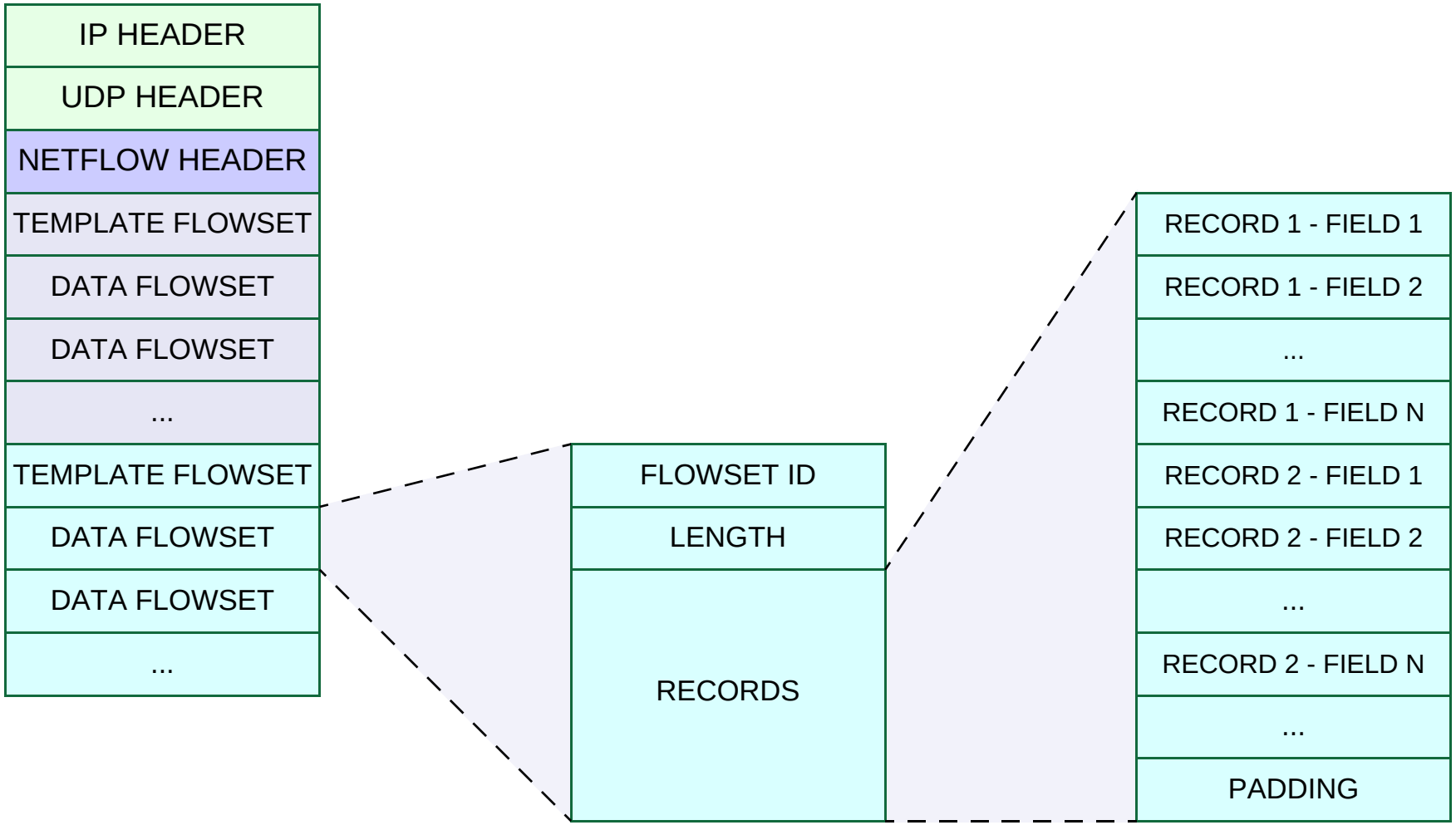
CAPTION

EXAMPLE: NETFLOW V9 (1)



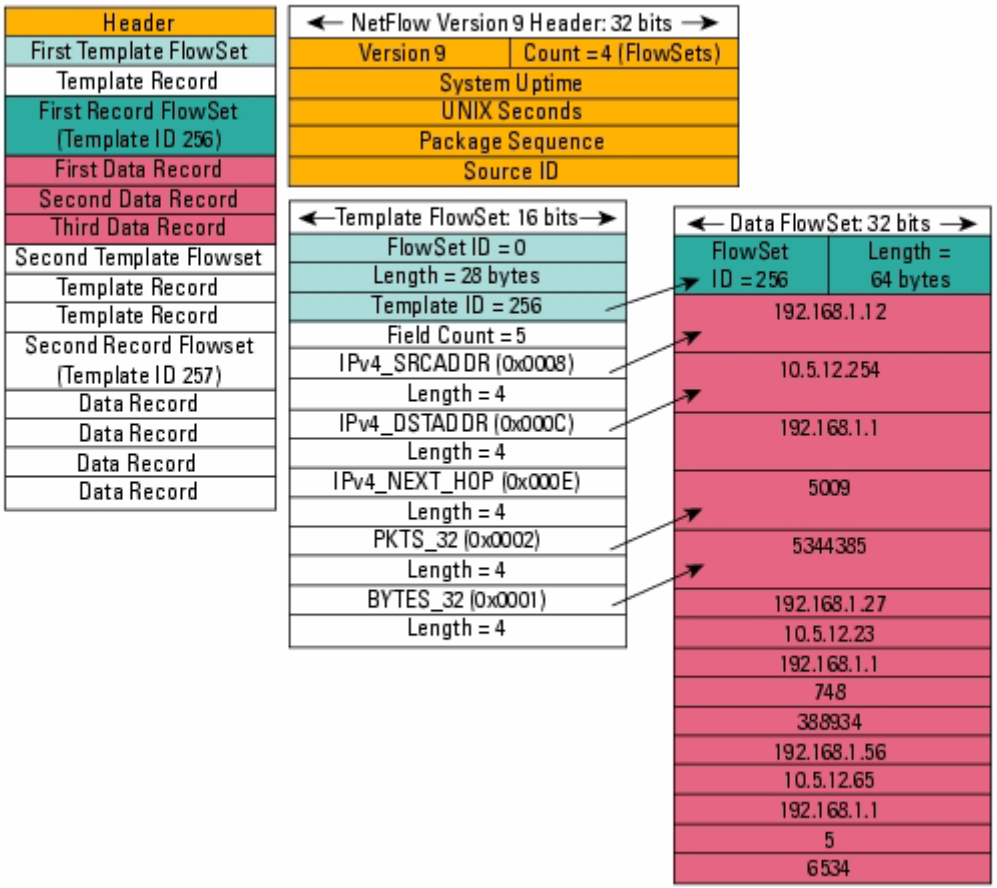
SOURCE: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/tflow_wp.htm#wp1002063

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