

# Network Measurements

Victor S. Frost

Dan F. Servey Distinguished Professor  
Electrical Engineering and Computer Science

University of Kansas

Phone: (785) 864-4833

e-mail: [vsfrost@ku.edu](mailto:vsfrost@ku.edu)

<http://www.ittc.ku.edu/~frost>

# Why measure?

- Wide area network behavior is unpredictable
  - Many factors are pushing and pulling the infrastructure
  - Constant change is normal
- Many applications have minimum performance requirements
  - Reliability,
  - predictability, ...
- Network managers adjust systems to conditions

# Why measure?

- Support network life cycle
  - Design and planning
    - Specify requirements
    - Understand network demands
    - Design & predict performance
  - Development
    - Detailed system evaluation using prototypes
    - Validate system design
  - Deployment
    - Measure baseline performance
    - Determine that design meets expectations.
  - Production
    - Continuous monitoring of network performance wrt design specifications
    - Monitor changing loads.
  - Evolution
    - Respond to changing loads and customer requirements,
    - Predict system performance under future loads

# Why measure?

- Advance the understanding of networks
  - The Internet is a HUGE network of networks & Scientists love to study/model complex systems
  - Explore emergent behaviors
  - Develop new traffic models
  - Understand impact of new technologies
  - Diagnose problems
  - Understand “why” the networks perform as observed

# Why measure?

- Measurement perspectives
  - Technical
    - Identify new features
    - Identify need for new protocols
  - Commercial
    - Network operators
    - Equipment vendors
  - Social
    - How does society use networks?
    - What is the impact on society?
  - Policy
    - Determine the availability of the network- penetration
    - Truth in advertising network capabilities.
    - Improve the availability of information for consumers about their broadband service (goal of the FCC's Measuring Broadband America (MBA) program)

<https://broadbandnow.com/Kansas>

<https://www.fcc.gov/general/measuring-broadband-america>

# Why Measure?

- Measurement perspectives (continued)
  - Developer
  - Operator
  - Regulator
  - Researcher
- Security

# Who is measuring?

- End users – very limited visibility
- Enterprises
  - Campuses
  - Global companies
- ISP (tier 2) – limited visibility
- Major Carriers (tier 1)
- Researchers

# When to measure?

- Diurnal traffic cycle
- Capture specific events, e.g., Mother's day
- Time scales,  $\mu\text{sec}$  to months
- Passive measurements are usually continuous but with a fixed sampling rate; important characteristics can be missed
- Active measurements are typically discrete
  - Sometimes a “once and done”
  - Sampling is a consideration
  - Important characteristics can be missed

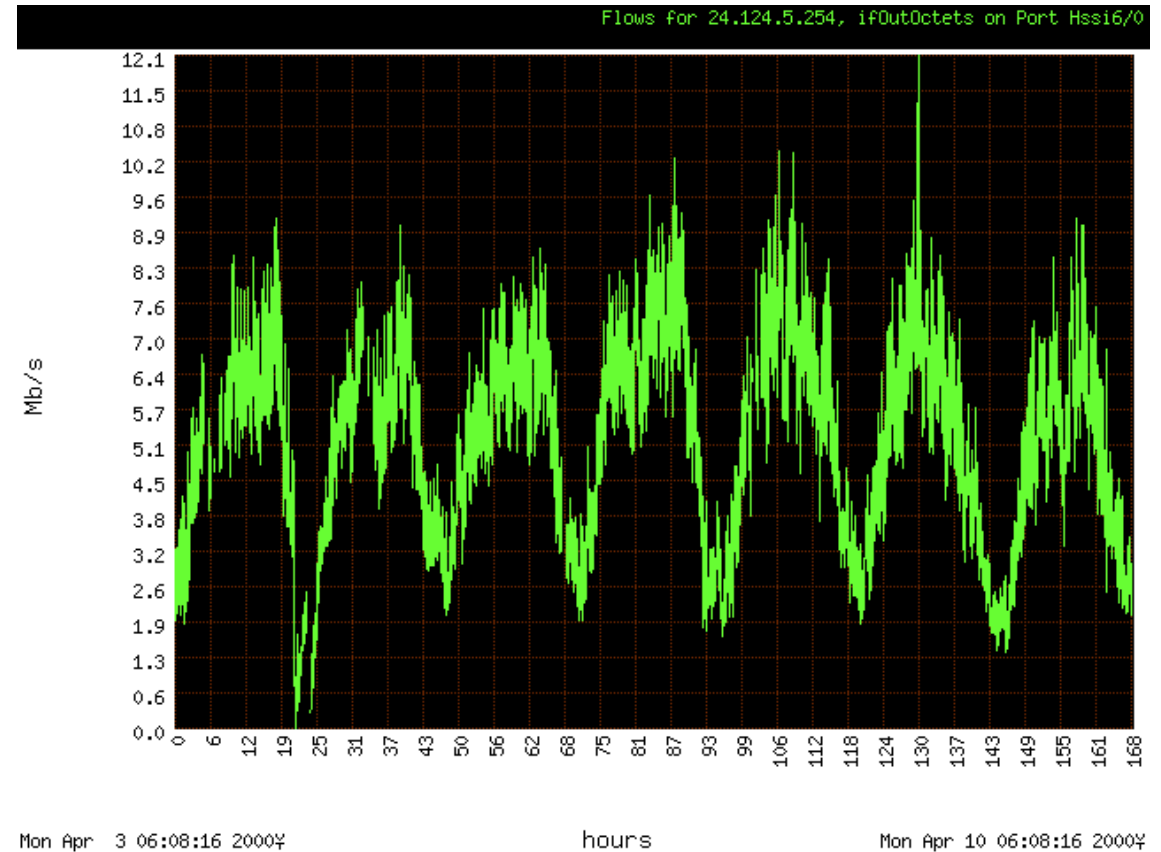
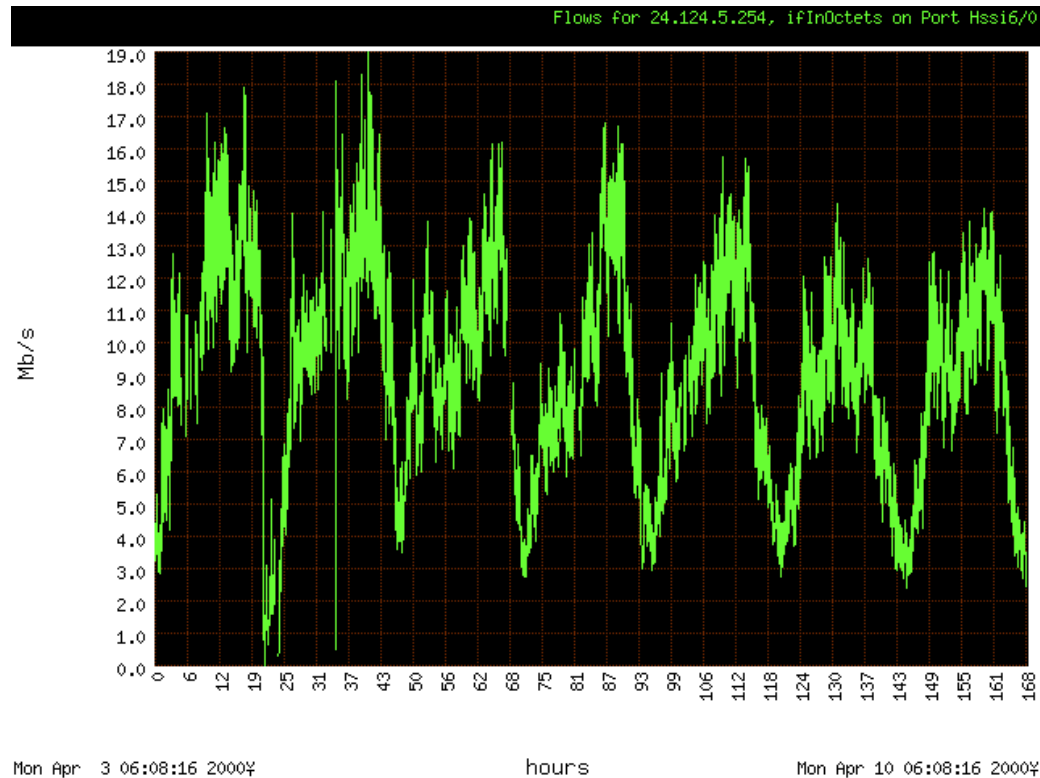


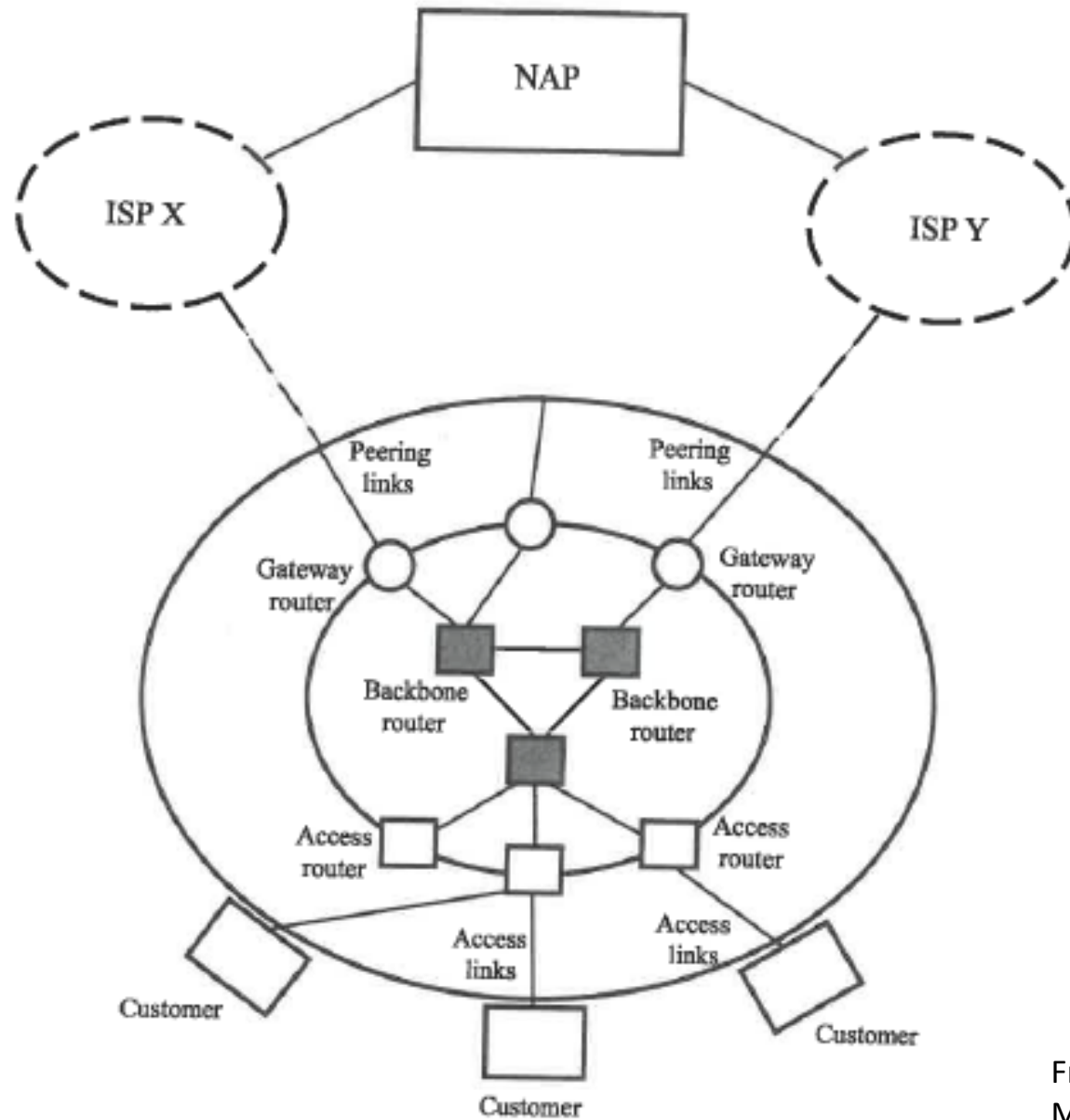
# Where to measure?

- End user equipment
  - PC's
  - Routers
  - Special boxes, e.g., BISmark an OpenWRT-based platform to perform measurements of ISP performance and traffic inside home networks  
<https://www.measurementlab.net/tests/bismark/>
- Enterprise routers
- ISP (tier 2)
- Major Carriers (tier 1)

# Tier 2 measurements.

## Time of day variations

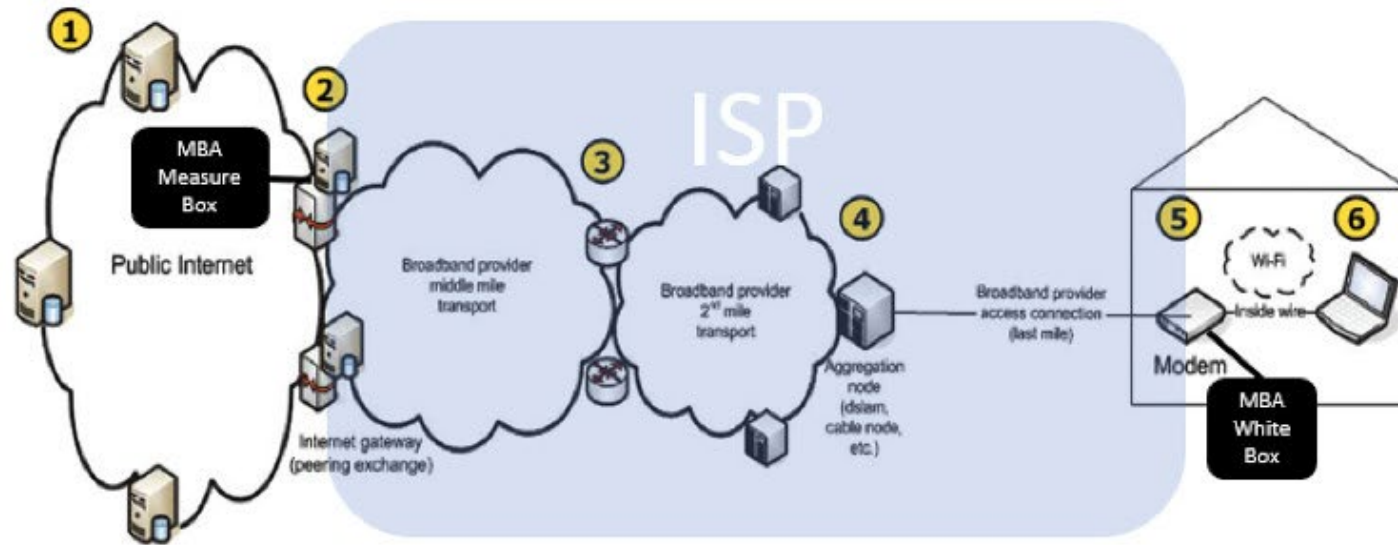




**Figure 4.1** Measurement locations in an ISP.

From: Internet Measurement: Infrastructure, Traffic and Applications, by Mark Crovella, Balachander Krishnamurthy  
Published by John Wiley & Sons Inc, 2006

*Exhibit 4-I:  
Simplified View of  
Internet Network  
and Connections*

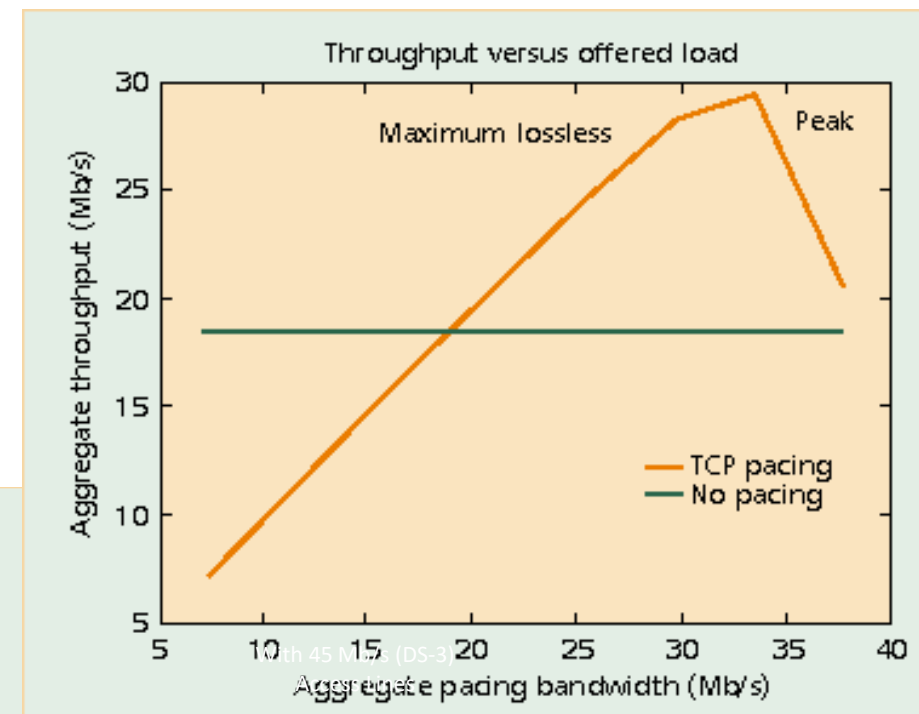
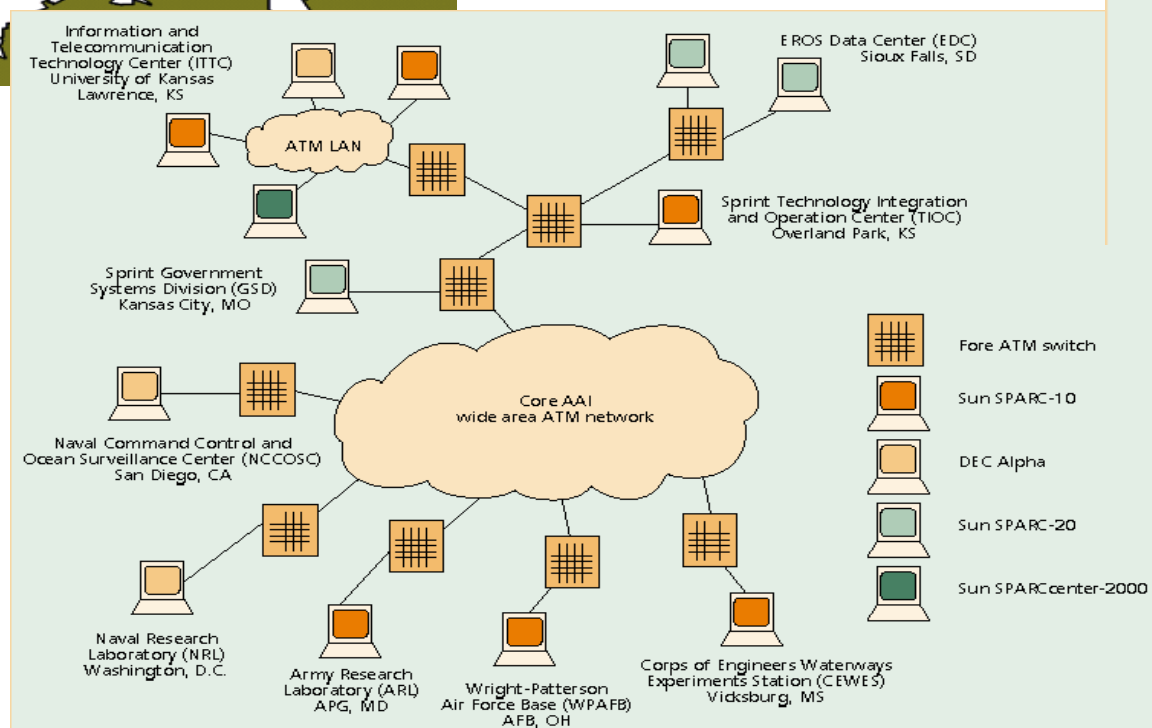
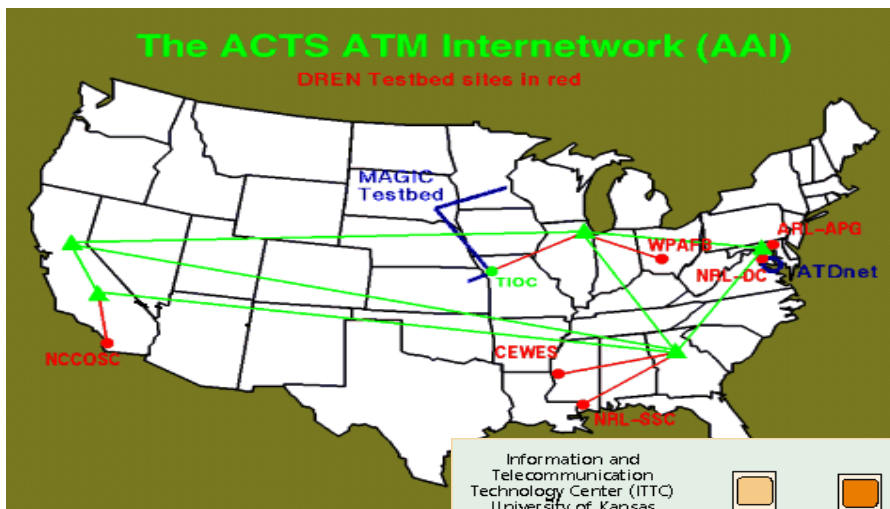


#### DEFINITIONS

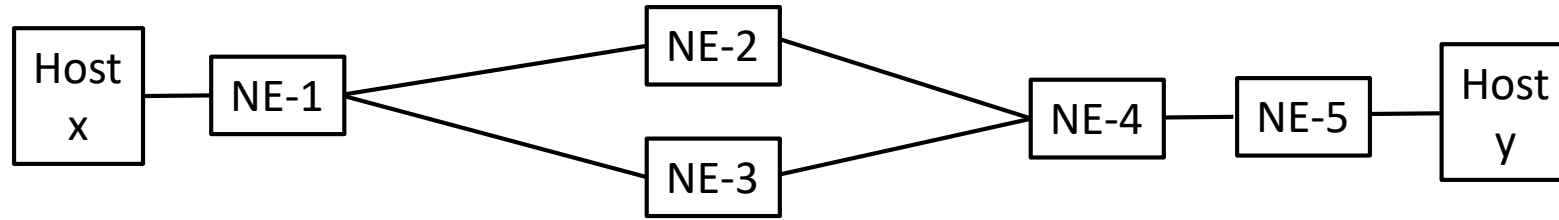
- 1 Public Internet content:** public Internet content that is hosted by multiple service providers, content providers and other entities in a geographically diverse (worldwide) manner
- 2 Internet gateway:** closest peering point between broadband provider and public Internet for a given consumer connection
- 3 Link between 2nd mile and middle mile:** broadband provider managed interconnection between middle and last mile
- 4 Aggregation node:** First aggregation point for broadband provider (e.g. DSLAM, cable node, satellite, etc.)
- 5 Modem:** Customer premise equipment (CPE) typically managed by a broadband provider as the last connection point to the managed network (e.g. DSL modem, cable modem, satellite modem, optical networking terminal (ONT), etc.)
- 6 Consumer device:** consumer device connected to modem through internal wire or Wi-Fi (home networking), including hardware and software used to access the Internet and process content (customer-managed)

From: <https://www.cybertelecom.org/broadband/speed.htm>

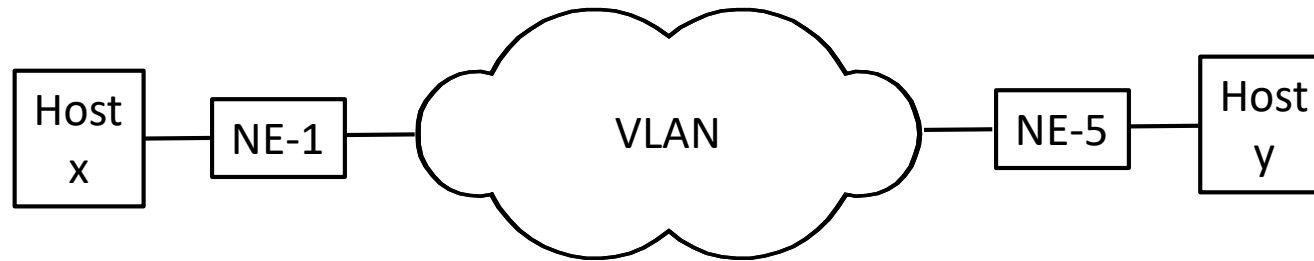
# Network Performance Example



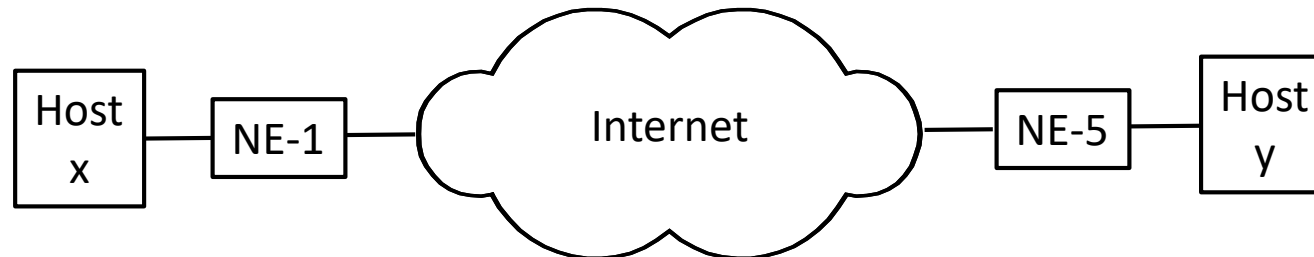
# Views of the network



Physical-Layer 1



VLAN-Layer 2



IP-Layer 3

- Visibility depends upon the layer where the measurement are taken
- Hides:
  - Firewalls
  - NATS
- For example, a route change at the PHY layer may not be measured by traceroute

# Measurement Challenges?

- "Poor observability"
  - Arising from administrative barriers
  - Security concerns
  - Privacy concerns
- Layered architecture
- Hidden layers
  - Firewalls
  - Traffic Shapers
  - NATs
  - Proxies

# Measurement Challenges?

- Data consistency
  - Data collected for the same characteristic using Different methods does not always agree
  - For example:
    - Internet speed test from M-Lab <https://www.measurementlab.net/>
    - Internet speed test from Ookla <https://www.speedtest.net/>
- Clock synchronization
- Calibration is difficult
- Representativeness- are the results from a measurement (at one time using one infrastructure) be used to characterize the network Firewalls
  - Traffic Shapers
  - NATs
  - Proxies



# Measurement Challenges?

- Repeatability is difficult
  - Networks are dynamic
  - There are some public repositories of data
  - <https://www.measurementlab.net/>
  - <https://www.caida.org/>
- Mass quantity of data
  - Link speeds increasing
  - Number of users increasing
  - Number of applications are increasing
  - Measurements across several layers maybe required
- Appropriate statistical techniques must be applied

# Where to save the measured data:

## Repositories of Network Measurements

- Center for Applied Internet Data Analysis (CAIDA)  
<https://www.caida.org/>
- “Founded in 1997, the Center for Applied Internet Data Analysis (CAIDA) conducts network research and builds research infrastructure to support large-scale data collection, curation, and data distribution to the scientific research community. CAIDA is based at the San Diego Supercomputer Center, located on the UC San Diego campus in La Jolla, CA”

# Where to save the measured data:

## Repositories of Network Measurements

- Center for Applied Internet Data Analysis (CAIDA)
  - Contains extensive measurement data sets see(Jan 2022)  
[https://www.caida.org/catalog/media/2022\\_caida\\_measurement\\_data\\_infrastructure\\_overview/caida\\_measurement\\_data\\_infrastructure\\_overview.pdf](https://www.caida.org/catalog/media/2022_caida_measurement_data_infrastructure_overview/caida_measurement_data_infrastructure_overview.pdf)
  - Topologies
  - Flows
  - Traces
  - Network Telescope, a /8 network domain with no legitimate flow, collects data on anomalous traffic

# Where to save the measured data:

## Repositories of Network Measurements

- RIPE Labs <https://labs.ripe.net/>
  - “RIPE Labs has been bringing people from all corners of the community together to share and discuss news and ideas about network operations, measurements and tools, Internet governance, industry events and community matters.”
  - Routing
  - Test traffic measurements
  - Reachability

# Where to save the measured data:

## Repositories of Network Measurements

- M-Lab <https://www.measurementlab.net/>
  - “M-Lab aims to advance Internet research by empowering consumers with useful information about their Internet performance. By providing free, open Internet measurement data, researchers, regulators, advocacy groups, and the general public can get a better sense of how the Internet is working for them, and how to maintain and improve it for the future.”
- The State of the Internet Reports | Akamai see <https://www.akamai.com/our-thinking/the-state-of-the-internet>

# How to measure?

- Active methods – send traffic into the network and measure response
  - Ping
  - Tracetroute
  - Speed tests
- Passive methods – Log traffic
  - Wireshark
  - Simple Network Management Protocol (SNMP)
- Many tools are available. See
  - <http://www.icir.org/models/tools.html>
  - [A Survey on Internet Performance Measurement Platforms and Related Standardization Efforts](#)
  - [Survey of End-to-End Mobile Network Measurement Testbeds, Tools, and Services](#)
- Use testbeds
  - Emulation of the network and/or traffic
  - [GENI \(Global Environment for Network Innovations\)](#)
  - [WINLAB \(Wireless Information Network Laboratory\)](#)
  - [EMULAB](#)
  - [COSMOS \(Cloud Enhanced Open Software Defined Mobile Wireless Testbed for City-Scale Deployment\)](#)
  - [FABRIC](#)

# Measurement environment

Real-world Network Real-world Traffic “In the wild”	Emulated Network Real-world Traffic
Real-world Network Emulated Traffic	Emulated Network Emulated Traffic

# Role of time

- Network events occur:
  - At geographically distributed locations
  - In different network elements.
  - Running different OS
  - With different clocks
- Determining the true time is a hard problem.



# Time

- Let clock  $j$  report “apparent time”= $C_j(t)$  at true time  $t$ .
- Let  $\theta_j(t) = C_j(t) - t =$  time offset
- Desire  $\theta_j(t)$  small
- Apparent time changes with time, causes skew; let  $\gamma_j(t) = \frac{dC_j(t)}{dt}$
- Want
  - $\gamma_j(t) \rightarrow 1$
  - Or  $C_j(t)$  linear so skew rate =  $\gamma_j(t) = \gamma_j$
  - Skew (parts/million) =  $1 - \gamma_j$
  - Time resolution,  $\Delta t$ ,  $C_j(t) = C_j(i\Delta t)$

# Time sources

- Stratum 0

These are high-precision timekeeping devices such as atomic clocks, GNSS (including GPS) or other radio clocks. They generate a very accurate pulse per second signal that triggers an interrupt and timestamp on a connected computer. Stratum 0 devices are also known as reference clocks. NTP servers cannot advertise themselves as stratum 0. A stratum field set to 0 in NTP packet indicates an unspecified stratum.

- Stratum 1

These are computers whose system time is synchronized to within a few microseconds of their attached stratum 0 devices. Stratum 1 servers may peer with other stratum 1 servers for sanity check and backup. They are also referred to as primary time servers.

- Stratum 2

These are computers that are synchronized over a network to stratum 1 servers. Often a stratum 2 computer queries several stratum 1 servers. Stratum 2 computers may also peer with other stratum 2 computers to provide more stable and robust time for all devices in the peer group.

- Stratum 3

These are computers that are synchronized to stratum 2 servers. They employ the same algorithms for peering and data sampling as stratum 2, and can themselves act as servers for stratum 4 computers, and so on.

# Time sources

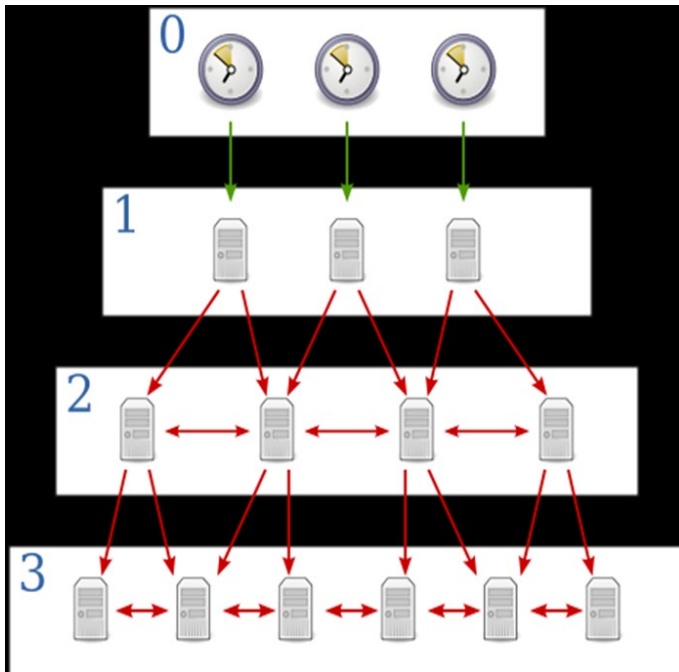
- GPS
  - Time resolution order of  $.1\mu\text{s}$  to  $1\mu\text{s}$
- NTP (Network Time Protocol)
- NIST Radio servers –broadcasts time 24/7
  - WWV
  - WWVH
  - WWVB
  - Time resolution 1ms to 10ms
- PC
- Software clock
  - Time resolution order of 10ms
  - Skew  $\sim 50\mu\text{s}/\text{sec} = 50 \text{ ppm}$
- Time stamp counter (TSC)
  - Time resolution order of  $1\mu\text{s}$
  - Skew  $\sim .1\mu\text{s}/\text{sec} = .1 \text{ ppm}$

# Time sources

- NTP (Network Time Protocol)
  - Time servers and clients
  - Clients sends request to server
  - Organized in hierarchy

(Top level is stratum 1 of NTP)

Stratum 0  
(reference clocks)



Current NTP configuration on Windows systems

```
H:\>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0010772s
Root Dispersion: 0.3380753s
ReferenceId: 0x81ED0CE9 (source IP: 129.237.12.233)
Last Successful Sync Time: 1/11/2022 1:24:45 PM
Source: time1.ku.edu,0x9
Poll Interval: 15 (32768s)
```

Precision = time resolution= $\Delta t$

The root is this PC's stratum 1 NTP server.

Root Dispersion = maximum amount of variance between the NTP server and its known time-source

Root Delay = RTT to server

See <https://blog.meinbergglobal.com/2021/02/25/the-root-of-all-timing-understanding-root-delay-and-root-dispersion-in-ntp/>

# Example: Ping

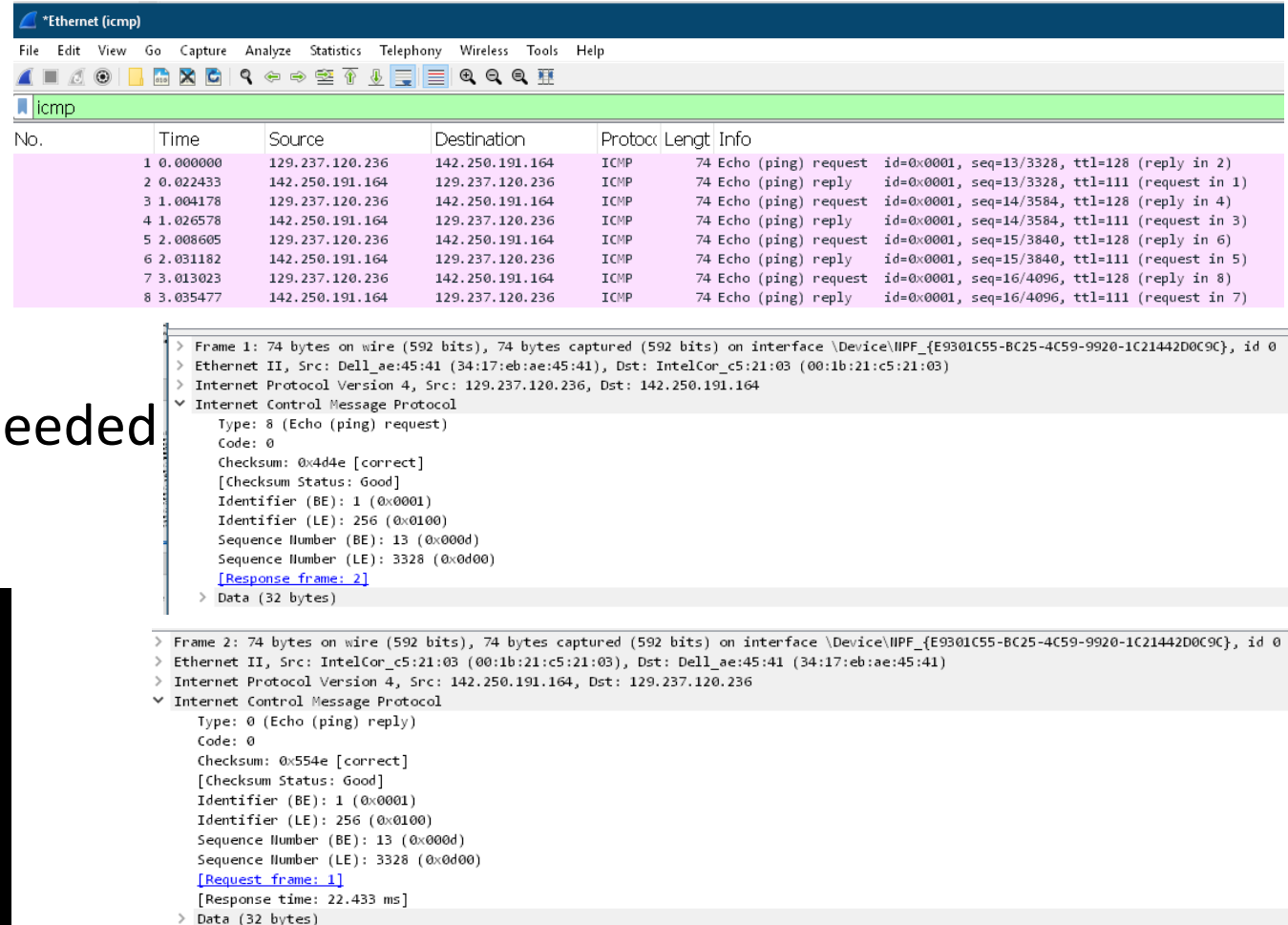
- Ping
  - Measures RTT
  - Sends ICMP ECHO packet to target
  - Target returns ICMP REPLY packet
  - No Specialized software/hardware needed
  - Not all devices respond to ping

```
H:\>ping www.google.com

Pinging www.google.com [142.250.190.68] with 32 bytes of data:
Reply from 142.250.190.68: bytes=32 time=22ms TTL=111
Reply from 142.250.190.68: bytes=32 time=22ms TTL=111
Reply from 142.250.190.68: bytes=32 time=21ms TTL=111
Reply from 142.250.190.68: bytes=32 time=22ms TTL=111

Ping statistics for 142.250.190.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 22ms, Average = 21ms
```

## Passive Measurements of flow using Wireshark



The image shows a Wireshark packet capture of an ICMP Echo (ping) request and its corresponding reply. The top pane displays a list of packets, and the bottom pane shows the detailed view of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	129.237.120.236	142.250.191.164	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 2)
2	0.022433	142.250.191.164	129.237.120.236	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=111 (request in 1)
3	1.004178	129.237.120.236	142.250.191.164	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 4)
4	1.026578	142.250.191.164	129.237.120.236	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=111 (request in 3)
5	2.008605	129.237.120.236	142.250.191.164	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 6)
6	2.031182	142.250.191.164	129.237.120.236	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=111 (request in 5)
7	3.013023	129.237.120.236	142.250.191.164	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 8)
8	3.035477	142.250.191.164	129.237.120.236	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=111 (request in 7)

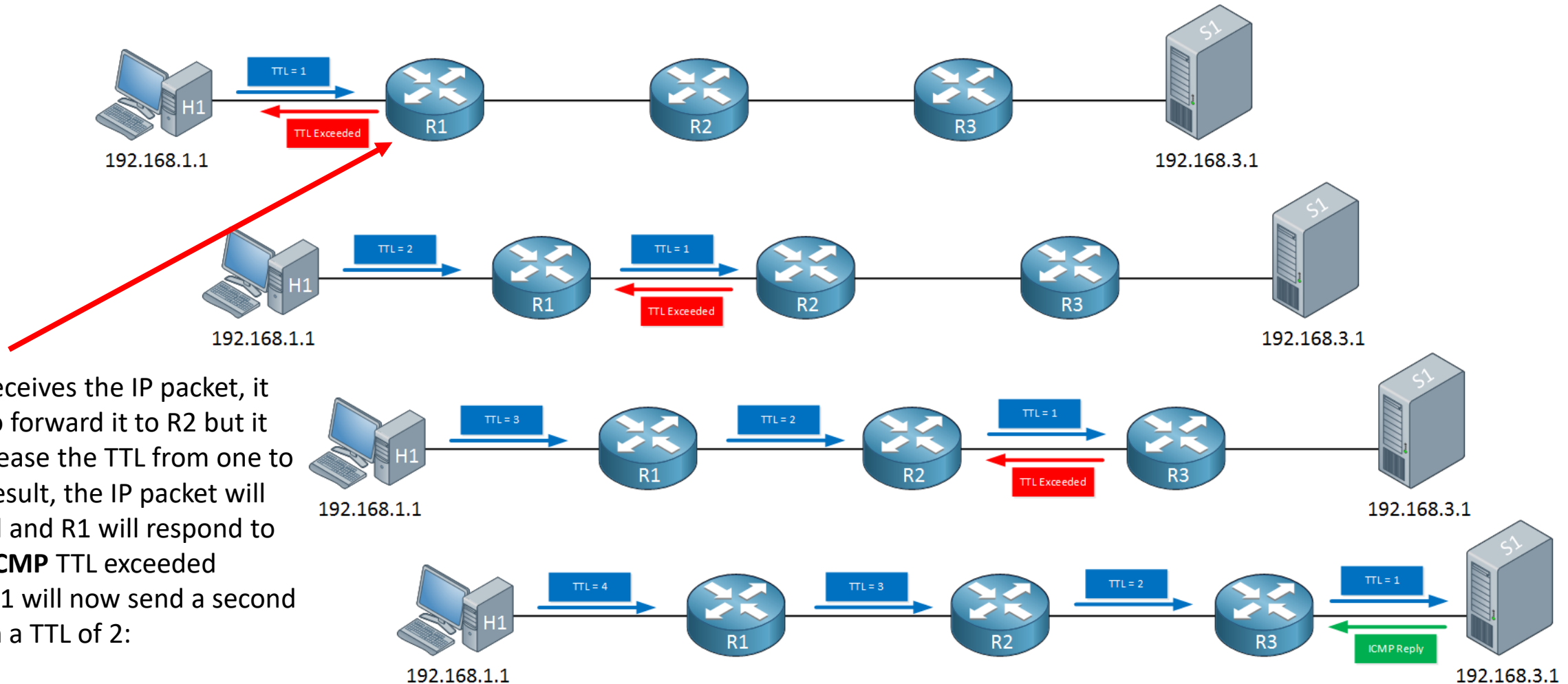
The detailed view of the first packet (Frame 1) shows the following information:

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{E9301C55-BC25-4C59-9920-1C21442D0C9C}, id 0
- Ethernet II, Src: Dell\_ae:45:41 (34:17:eb:ae:45:41), Dst: IntelCor\_c5:21:03 (00:1b:21:c5:21:03)
- Internet Protocol Version 4, Src: 129.237.120.236, Dst: 142.250.191.164
- Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0x4d4e [correct]
  - [Checksum Status: Good]
  - Identifier (BE): 1 (0x0001)
  - Identifier (LE): 256 (0x0100)
  - Sequence Number (BE): 13 (0x000d)
  - Sequence Number (LE): 3328 (0x0d00)
  - [Response frame: 2]
- Data (32 bytes)

The detailed view of the second packet (Frame 2) shows the following information:

- Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{E9301C55-BC25-4C59-9920-1C21442D0C9C}, id 0
- Ethernet II, Src: IntelCor\_c5:21:03 (00:1b:21:c5:21:03), Dst: Dell\_ae:45:41 (34:17:eb:ae:45:41)
- Internet Protocol Version 4, Src: 142.250.191.164, Dst: 129.237.120.236
- Internet Control Message Protocol
  - Type: 0 (Echo (ping) reply)
  - Code: 0
  - Checksum: 0x554e [correct]
  - [Checksum Status: Good]
  - Identifier (BE): 1 (0x0001)
  - Identifier (LE): 256 (0x0100)
  - Sequence Number (BE): 13 (0x000d)
  - Sequence Number (LE): 3328 (0x0d00)
  - [Request frame: 1]
  - [Response time: 22.433 ms]
- Data (32 bytes)

# Example: Traceroute



When R1 receives the IP packet, it will want to forward it to R2 but it has to decrease the TTL from one to zero, as a result, the IP packet will be dropped and R1 will respond to H1 with a **ICMP** TTL exceeded message. H1 will now send a second packet with a TTL of 2:

Modified From:

<https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/traceroute>

# Example: Traceroute

```
H:\>tracert www.google.com

Tracing route to www.google.com [142.250.190.68]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    gw-vlan110.ittc.ku.edu [129.237.123.254]
  2  <1 ms    <1 ms    <1 ms    129.237.160.18
  3  <1 ms    <1 ms    <1 ms    vl406.dptvss01.net.ku.edu [129.237.2.170]
  4  <1 ms    <1 ms    <1 ms    ae5-0.comp-br-01.net.ku.edu [129.237.2.74]
  5   2 ms     1 ms     1 ms    comp-br-01-ae8-untrust.net.ku.edu [129.237.2.14]
  6   1 ms     1 ms     1 ms    kanren-ku-comp-border.peer.net.kanren.net [164.113.216.5]
  7   2 ms     1 ms     1 ms    bb-kc-walnut-et7-0-0-0.bb.net.kanren.net [164.113.193.114]
  8   *        2 ms     3 ms    e0-3.core2.mci1.he.net [184.105.253.141]
  9   2 ms     2 ms     2 ms    100ge12-1.core1.mci3.he.net [184.105.213.34]
 10  12 ms    11 ms    12 ms    100ge15-2.core1.dal1.he.net [184.105.64.213]
 11  12 ms    12 ms    13 ms    port-channel6.core3.dal1.he.net [184.104.196.169]
 12  12 ms    12 ms    12 ms    ipv4.de-cix.dfw.us.as15169.google.com [206.53.202.109]
 13  33 ms    12 ms    12 ms    108.170.252.130
 14  12 ms    12 ms    12 ms    216.239.63.207
 15  18 ms    19 ms    19 ms    142.251.229.27
 16  23 ms    23 ms    23 ms    216.239.40.14
 17  22 ms    22 ms    22 ms    216.239.63.32
 18  22 ms    22 ms    22 ms    108.170.244.1
 19  22 ms    22 ms    22 ms    142.251.60.203
 20  22 ms    22 ms    22 ms    ord37s34-in-f4.1e100.net [142.250.190.68]

Trace complete.
```

# Example: Traceroute

- Only finds source (S) to destination (D) S->D
- D->S maybe different
- Assumes path stable during execution
- Router interfaces have IP addresses, so visibility into IP network path not router topology

```
H:\>tracert www.ku.edu

Tracing route to ku.edu [129.237.135.76]
over a maximum of 30 hops:

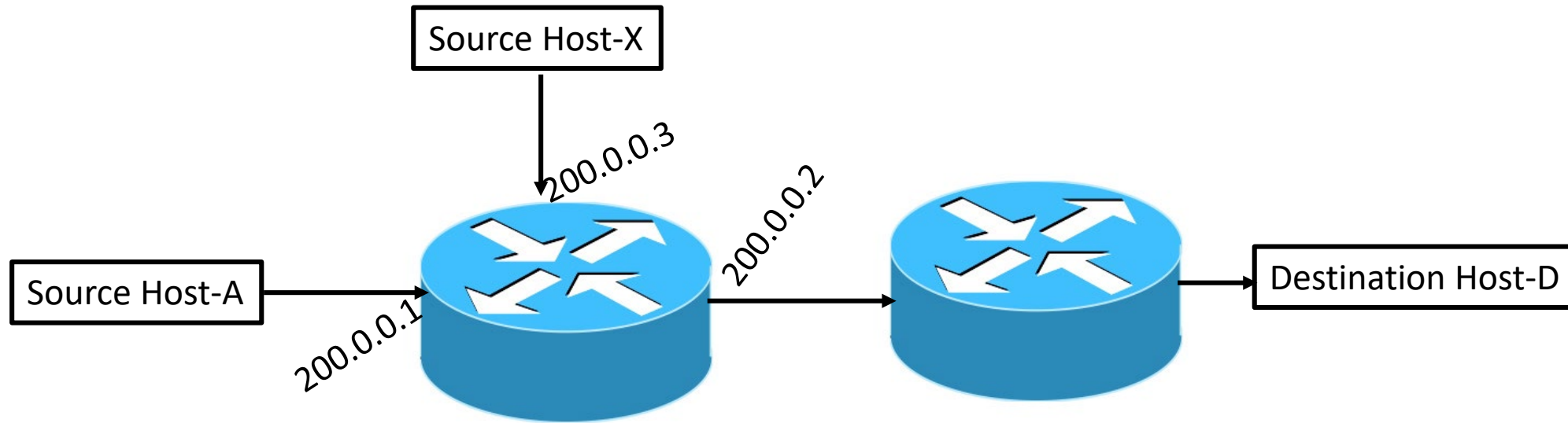
  1  <1 ms    <1 ms    1 ms  gw-vlan110.ittc.ku.edu [129.237.123.254]
  2  <1 ms    <1 ms    <1 ms  129.237.160.18
  3  <1 ms    <1 ms    1 ms  vl406.dptvss01.net.ku.edu [129.237.2.170]
  4   9 ms    1 ms     <1 ms  ae5-0.comp-br-01.net.ku.edu [129.237.2.74]
  5  23 ms   108 ms   143 ms  xe-0-0-1-0.comp-sr-01-2.net.ku.edu [129.237.2.230]
  6  <1 ms    <1 ms    <1 ms  129.237.135.76

Trace complete.
```





# Example: Traceroute



Traceroute A->D  
200.0.0.1->200.0.0.2.....  
Traceroute X->D  
200.0.0.3->200.0.0.2.....

No way to tell that The path  
shares a router

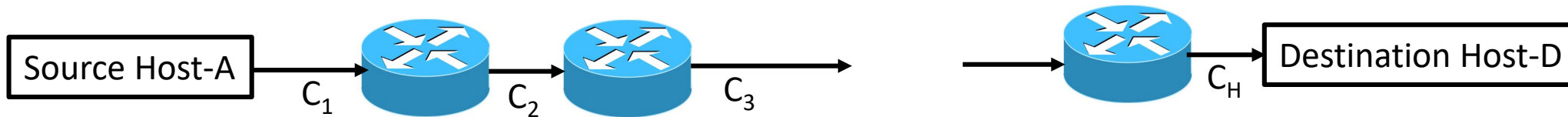
More advanced methods are  
needed to generate a router  
level topology using traceroute.  
Alias resolution methods are  
used to discover if two interfaces  
share the same router.

# Throughput measurements

- Applications
  - Server selection
  - Configuration of overlay networks
  - Verification of SLAs
  - Adjust coding for streaming media

# Throughput measurements

- Definitions of throughput
  - Units b/s, Bytes/sec, packets/sec
  - Maximum uncongested throughput,  $C_{\max} = \min(C_j)$  for  $j=1\dots H$



# Throughput measurements

- Definitions of throughput
  - Available throughput =  $C_a$ 
    - Let  $u(t) = 1$  if path is busy else  $u(t) = 0$
    - Then over a  $T$  send interval the average path utilization

$$\bar{u} = \frac{1}{T} \int_t^{t+T} u(\eta) d\eta$$

and the available throughput is

$$C_a = (1 - \bar{u}) C_{Max}$$

- Bulk transfer throughput = CB
  - Rate a new single, log-lived TCP connection obtains over the path.

# Throughput measurements

- Throughput measurement techniques
  - For TCP must consider the impact of slow start
  - Used in FCC's Measuring Broadband America Program
    - Uses multiple TCP sessions to mitigate TCP window flow control limitations
    - Sustained download speed: throughput in Mbps utilizing three concurrent TCP connections measured at the 25-30 second interval of a sustained data transfer
    - Sustained upload speed: throughput in Mbps utilizing three concurrent TCP connections measured at the 25-30 second interval of a sustained data transfer
    - Burst download speed: throughput in Mbps utilizing three concurrent TCP connections measured at the 0-5 second interval of a sustained data transfer
    - Burst upload speed: throughput in Mbps utilizing three concurrent TCP connections measured at the 0-5 second interval of a sustained data transfer

# Throughput measurements

- Download

- The client establishes multiple connections with the server over port: 8080. The client requests the server to send an initial chunk of data.
- The client calculates the real-time speed of the transfers, then adjusts the chunk size and buffer size based on this calculation to maximize usage of the network connection.
- As the chunks are received by the client, the client will request more chunks throughout the duration of the test.
- During the first half of the test, the client will establish extra connections to the server if it determines additional threads are required to more accurately measure the download speed.
- The test ends once the configured amount of time has been reached.

- Upload

- The client establishes multiple connections with the server over the defined port and sends an initial chunk of data.
- The client calculates the real-time speed of the transfers and adjusts the chunk size and buffer size based on it to maximize usage of the network connection, and requests more data.
- As the chunks are received by the server, the client will send more chunks throughout the duration of the test.
- During the first half of the test, the client will establish extra connections to the server if it determines additional threads are required to more accurately measure the upload speed.
- The test ends once the configured amount of time has been reached.

From: <https://help.speedtest.net/hc/en-us/articles/360038679354-How-does-Speedtest-measure-my-network-speeds->

# Throughput measurements

- There are different measurement techniques and definitions
  - Hard to compare
  - Be aware of differences

# A capacity estimation technique: Variable Packet size (VPS) Probing

- Premise: The RTT from Ping contains two components, propagation times and service times
- Assumptions
  - No queueing
  - One link is forward and reverse path
  - Forward and reverse paths have same capacity
  - Then RTT as a function of message length (L) is a line

$$RTT(L) = \frac{L}{C} + \tau + \frac{L}{C} + \tau = \frac{2L}{C} + 2\tau$$

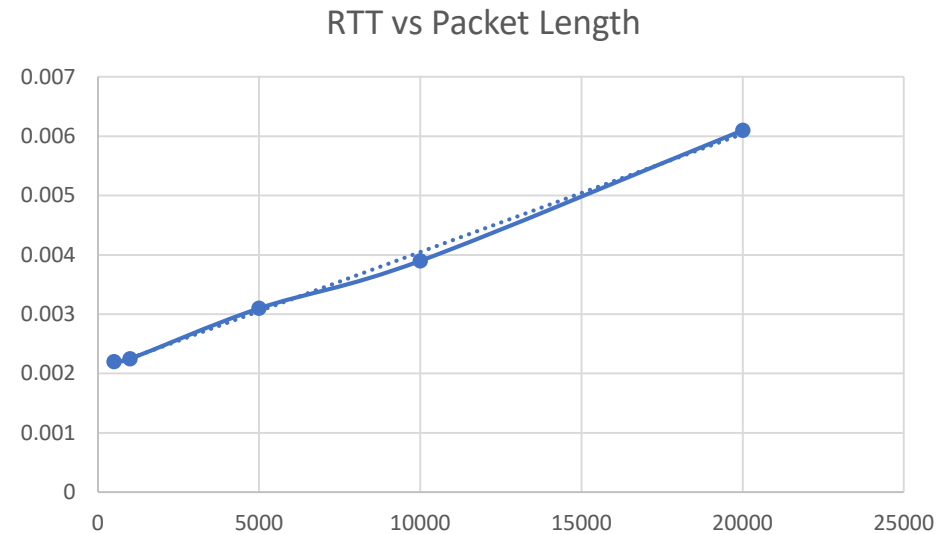
- Measure RTT using different L and solve for C, slope = 2/C



# A capacity estimation technique: Variable Packet size (VPS) Probing

- Example: Length vs RTT

Length ((bits)	RTT (sec)
500	0.0022
1000	0.00225
5000	0.0031
10000	0.0039
20000	0.0061

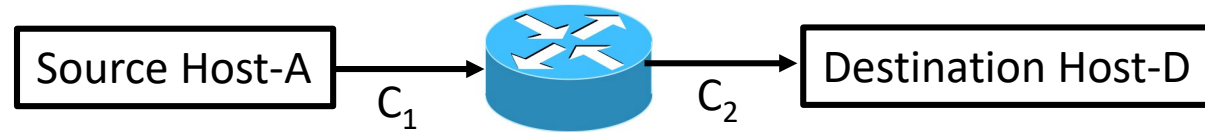


$$RTT(L) = 2.1 + 2 * 10^{-7} L(ms)$$

$$C = 10Mb / s$$

# A capacity estimation technique: Variable Packet size (VPS) Probing

- Example: multiple links



- Step 1
  - Set TTL=1 and use ICMP to measure
  - Estimate  $C_1$   $RTT_1(L) = \alpha_1 + \beta_1 L$

- Set 2
  - Set TTL=2 and use ICMP to measure

$$RTT_2(L) = \frac{L}{C_1} + 2\tau_1 + 2\tau_2 + \frac{L}{C_2} = \alpha_2 + \beta_2 L$$

= fixed delay + delay as a function of L

Step 3 find  $C_2$  where

$$C_2 = \frac{1}{\beta_2 - \beta_1}$$

In general

$$C_i = \frac{1}{\beta_i - \beta_{i-1}}$$

# A throughput estimation technique: Variable Packet size (VPS) Probing

- Issues with VPS probing
  - Assumes no cross traffic and light load (little queueing)
  - Time resolution of ICMP for high capacity links
  - Hidden queues (intermediate layer 2 networks)

# Estimating packet loss rate (PLR)

- Transmit  $N$  packets out of which  $n$  are observed as lost.
- Assuming statistically independent losses
- Simple and unbiased estimator for PLR is  $\hat{p} = \frac{n}{N}$
- $\hat{p}$  is binomially distributed
- Assuming  $N \gg 1$  and  $n \ll N$  and  $\bar{n}$  = expected number of losses in  $N$  packet transmissions.  $P[n_L < \bar{n} < n_U] = 0.954$

where

$$n_L = n + 2 - \sqrt{n+1} \quad n_U = n + 2 + \sqrt{n+1}$$

- Example:  $n = 10$   $P[8.6 < \bar{n} < 15.3] = 0.954$

# Estimating packet loss rate (PLR)

- Example continued:

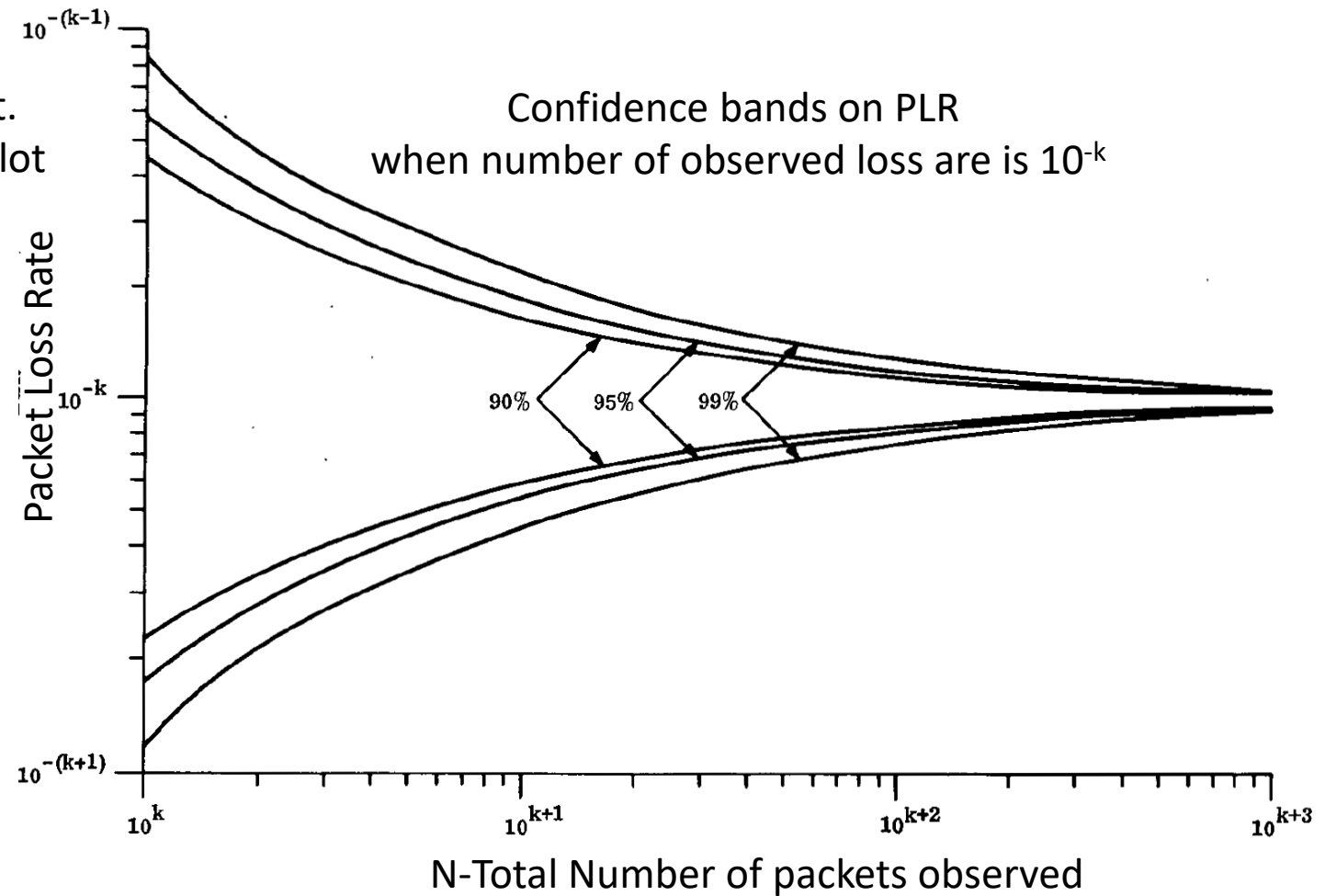
- If true PLR =  $10^{-5}$  then to get  $n=10$   $N=10^6$  and

$$P\left[\frac{8.6}{10^6} < \bar{n} < \frac{15.3}{10^6}\right] = P\left[\frac{8.6}{10^6} < \hat{p} < \frac{15.3}{10^6}\right] = P[8.6 * 10^{-6} < \hat{p} < 15.3 * 10^{-6}] = 0.954$$

- The range of the lower and upper limits are about a factor of 2

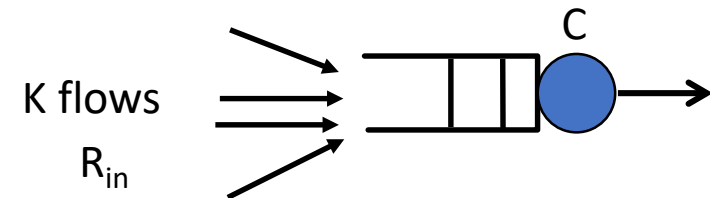
# Estimating packet loss rate (PLR)

For other confidence limits use this plot.  
 $n=10$  corresponds to  $N=10^{k+1}$  on this plot

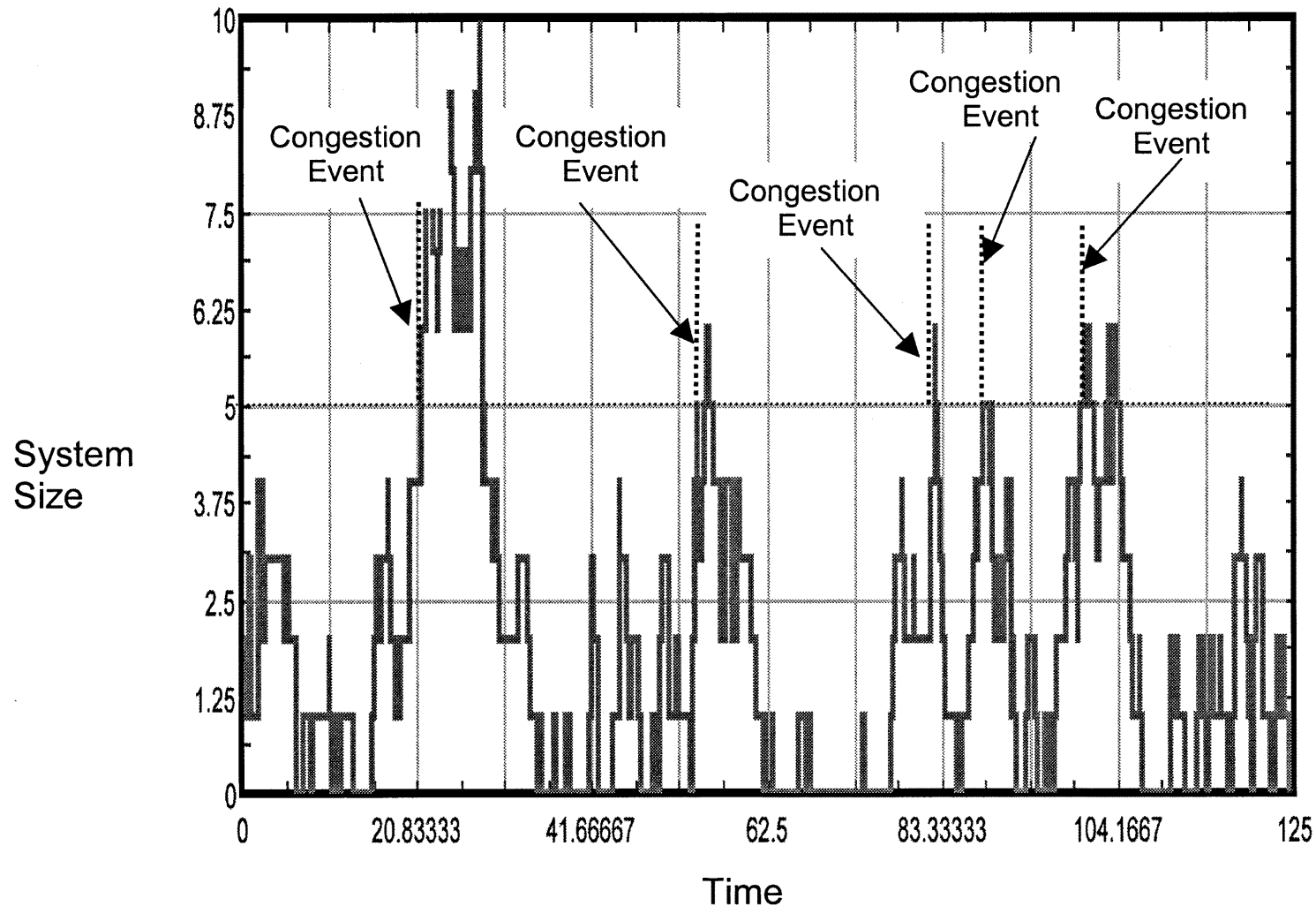


# Estimating packet loss rate (PLR)

- PLR in the Internet can be small
  - Requiring lots of probes.
  - Trade-offs
    - Probe rate
    - Measurement accuracy
    - impact the traffic on the path
    - Timeliness of results
- Losses occur when a queue is “congested”
- When  $R_{in} > C$  for Time > time to empty buffer (Q bits) then congested,  
buffer size Q typically  $RTT * C$
- Congestion metrics
  - PLR
  - Frequency of congestion events (loss episode frequency)
  - Length of congestion events (loss episode duration)



# Congestion events



From: Quantifying the temporal characteristics of network congestion events for multimedia services, V.S. Frost  
[IEEE Transactions on Multimedia](#) , Volume: 5, [Issue: 3](#), Sept. 2003



# Congestion events

- Approximation to predict the average time between congestion events for M/G/1 case; general message length distributions with finite variance.
- Let  $\lambda$  = arrival rate     $\mu$  = service rate

$$C_s^2 = \text{squared coefficient of variation} = \frac{\text{Var}[S]}{(E[S])^2} \quad S = \text{Service time}$$

$$P_b = \text{Prob}[X(t)=b] = \text{State probability and } \frac{1}{P_b} = \text{Mean recurrence time}$$

Let  $\tau$  = time between congestion events

$$E[\tau] \approx \frac{(1 + C_s^2)}{2P_b(\mu - \lambda)}$$

$$\Lambda = \text{Frequency of congestion events} = \frac{1}{E[\tau]}$$

# Congestion events

- Congestion rate for a flow traversing M routers
- Assume congestion events at each router for statistically independent.
- Then the frequency of congestion events for the flow is the sum of the frequency of congestion events at each router

$$\Lambda_T = \sum_{k=1}^M \Lambda_k$$

# Congestion events: Example

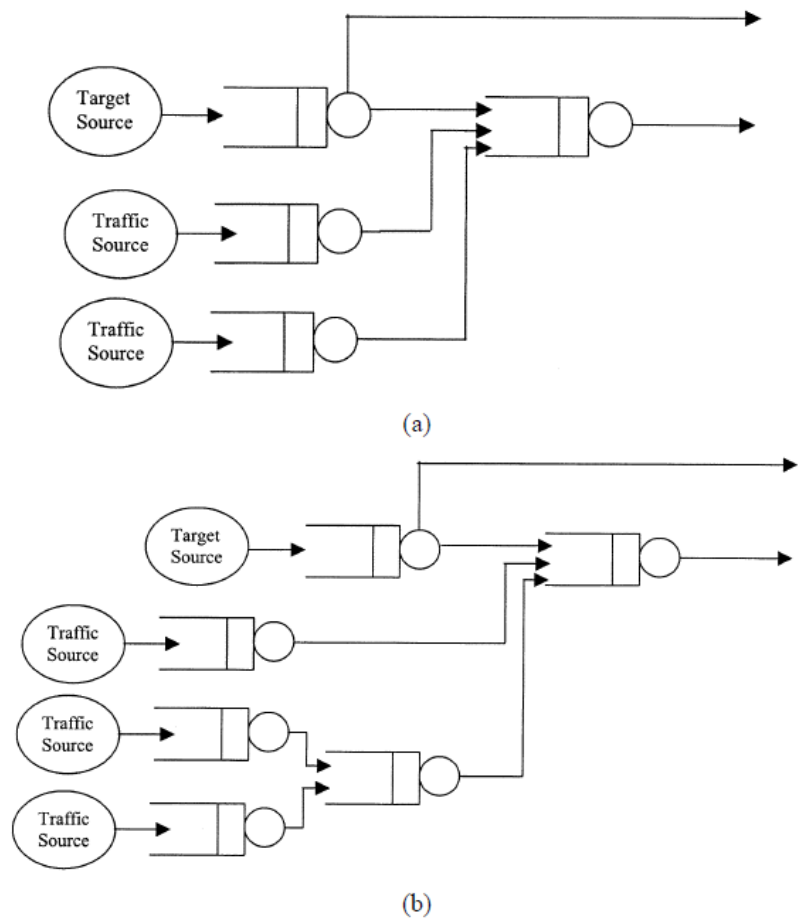


Fig. 8 (a) Network topology 1. (b) Network topology 2.

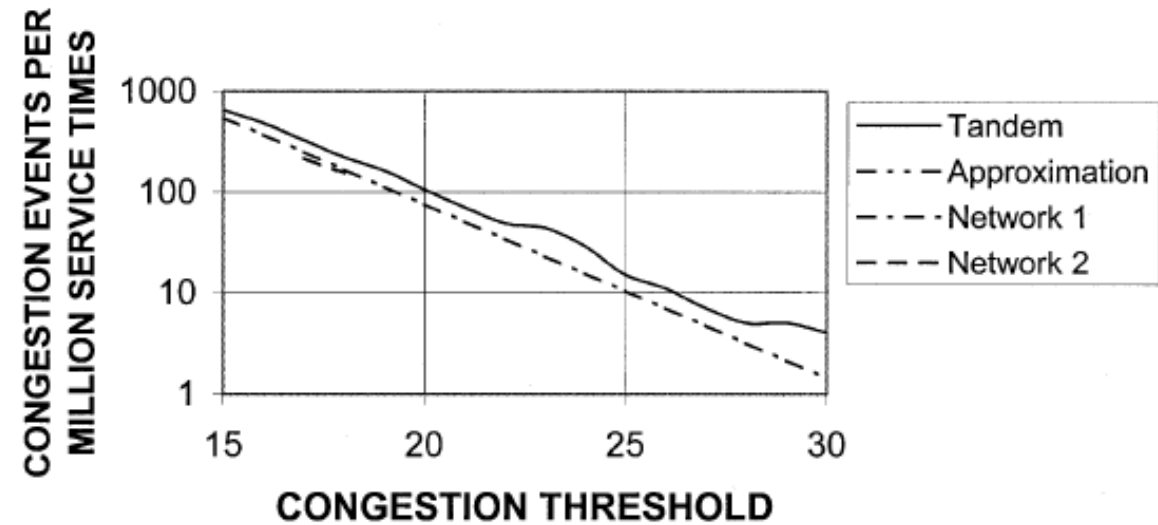


Fig. 9. Networks with M/H(2) Traffic-load 0.55.  
H(2)=hyperexponential service times

# Tools: Packet loss and more

- Wireshark -filters
  - tcp.analysis.lost\_segment
  - tcp.analysis.retransmission
- PingPlotter <https://www.pingplotter.com/> 14 day free trial
- EMCO Ping Monitor <https://emcosoftware.com/ping-monitor>
- Paessler PRTG Network Monitor <https://www.paessler.com/prtg>
- perfSONAR <https://www.perfsonar.net/>
- M-lab <https://www.measurementlab.net/>

# Anonymization of network measurements

- Network measurements
  - Contain valuable information
    - Collected
      - internally, .i.e., not to be shared
      - with sharing in mind, e.g., to be deposited in a repository
      - at different layers of the protocol stack
      - At different physical locations in the network
    - Maybe company sensitivity or proprietary
    - May contain private end user information
- Sharing of network measurements contributes to advancing the technology
- Organizations are deterred from sharing measurements.
- To facilitate collection and data sharing , measurements can be anonymized.

# Anonymization of network measurements

- Definitions

- “Article 3 (1) of Regulation (EU) 2018/1725: “personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”.

[https://edps.europa.eu/data-protection/data-protection/glossary/p\\_en](https://edps.europa.eu/data-protection/data-protection/glossary/p_en)

- Name
    - SSN
    - E-mail address
    - Office phone number

# Anonymization

- Definitions
  - World Wide Web Consortium
    - “most information referring to an individual is “identifiable”
- Personally identifiable information (PII)
- Anonymity is the absence of identity
- Identity
  - Information wrt groups
  - Proprietary information
    - Locations of routers
    - Physical paths of communications links, e.g., fibers
    - Traffic patterns
    - Network performance

# Anonymization

- Why anonymize measured data
  - Privacy
  - Restrict access to business information of interest to competitors
  - Security
- Risks to sharing measure data
  - Identification of vulnerable links, open to attack.
  - Disclosure of propriety information, network topology and specific physical routes by reverse engineering
  - Privacy, release of payload content
  - Sequential inferencing, knowledge of some fields can be use to infer anonymized information.



# What Information to Anonymize

- Identity-related
  - IP addresses
  - Host names
  - URLs
  - User names
- PII
  - Name
  - Passwords
  - Credit card numbers
  - Search histories
  - Payload
- Organization-specific
  - Network addresses, prefixes
  - AN numbers
  - Locations of peering points
  - Traffic patterns
- Business and Security-sensitive
  - Router topology
  - Firewall rules
  - BGP policies

# How to Anonymize Network Measurements

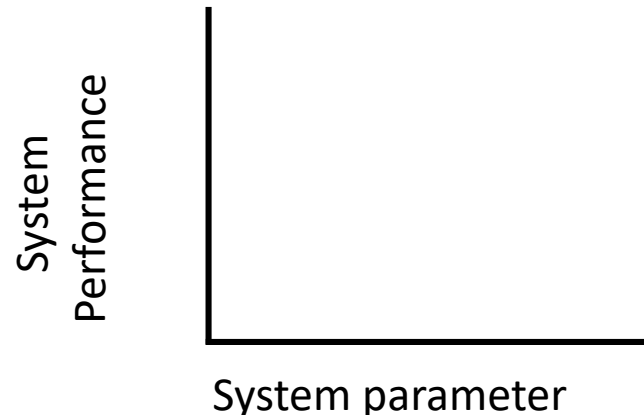
- Delete fields
  - Examples,
    - payload
    - full IP address
    - Port numbers
- Aggregation
  - Examples, replace
    - full IP address with network prefix
    - Port numbers with “generic” place holder
- Encryption
- Barriers to gathering and distributing network measurements continues to be a topic of interest, e.g.,
  - Challenges in measuring the Internet for the public Interest by David Clark and kc claffy  
[https://papers.ssrn.com/sol3/Delivery.cfm/SSRN\\_ID3902179\\_code798307.pdf?abstractid=3898347&mirid=1](https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3902179_code798307.pdf?abstractid=3898347&mirid=1)
  - Workshop on Overcoming Measurement Barriers to Internet Research (WOMBIR 2021)  
<https://www.caida.org/workshops/wombir/2104/>

# Methodology of Testing and Measurements

- Planning
  - Define each step
  - Be organized
    - Who
    - Where data is stored
  - Document each step, make measurements repeatable as possible
  - Have clearly stated objectives

# Methodology of Testing and Measurements

- Develop a detailed test plan
  - Identify needed resources
    - People
    - Equipment
    - Software tools
  - Assign responsibilities
  - Create a test configuration diagram
  - Create and document the methodology
  - Identify test points with list of associated measurements
  - Develop a testing schedule
    - Project time line
    - Milestones
  - Outline test report, including
    - Deliverables
    - Expected plots



# Methodology of Testing and Measurements

- During testing and measurements
  - Maintain an activity log
  - Maintain a problem resolution log
- Data Interpretation
  - Process collected data (data reduction/summary)
  - Sanity check measurements
    - Meet expectations
    - Reasonability
  - Sanity check measurements during data collection (do not wait until the end)
- Data Presentation- Executive summary
  - Objectives
  - Conclusions
  - Lessons learned