Network Measurement and Metrics

Dr. Bernardi Pranggono

Advanced Network Engineering

Weeks 26/27

Network Measurement

- Organisations increasingly depend on their networks so it is important to know how well they perform.
- If you don't measure it, you have no objective record or benchmark of how it behaves.
- This could make it difficult to judge whether changes in the network have improved its performance, or degraded it.

Why measure?

- Produce a record of performance
- Establish a baseline for performance
- View trends
- Reveal problems and faults
- Make sure you get what you pay for

Baselines

- A baseline is a measurement that is derived from the collection of data over an extended period during varying but typical types of workloads and user connections.
- The baseline is an indicator of how individual system resources or a group of resources are used during periods of normal activity.
- Routine monitoring over periods ranging from days to months allows you to establish a baseline for system performance.

Techniques and Methodologies

- Setting up meaningful measurements requires careful consideration of the techniques (active or passive), which measurements (metrics) to make and where and when to make them

- Standard methodologies can be applied to allow you to compare performance over periods of time to reveal problems such as bottlenecks or faults.

Passive or Active Measurement

- **Passive measurement**

  Observes normal network traffic without perturbing the network.

  Used to measure traffic flows, i.e. counting number of packets or bytes travelling through routers or links between specified sources and destinations.

- **Active measurement**

  Sends test traffic into the network to measure parameters.

  e.g. to measure a network's maximum carrying capacity by sending packets through it or its latency by sending Ping (ICMP) packets onto a network to determine round trip delay.

N.B. *Clearly you need to be aware that active measurements impose extra traffic onto a network and can distort its behaviour in the process, thereby affecting measurement results.*

Sampling

- When observing packets on a network, the goal is to use measuring tools that can keep up with the traffic at the measurement point, without missing any packets for any reason; this task gets harder and harder as the traffic rate increases.

- If the rate is too high for all packets to be observed reliably, the measurement tool should at least report the number of packets which were missed. In this situation there may be no alternative but to sample the packets, i.e. to base the measurement on a specified subset of the packets - in other words, to 'sample' the network traffic.

Sampling

- Sampling rate: How often should we measure?

- Should we measure with fixed interval (non-adaptive)
- Should we measure with variable interval (adaptive)

- Adaptive sampling works better (an active area of research).

Where to measure?

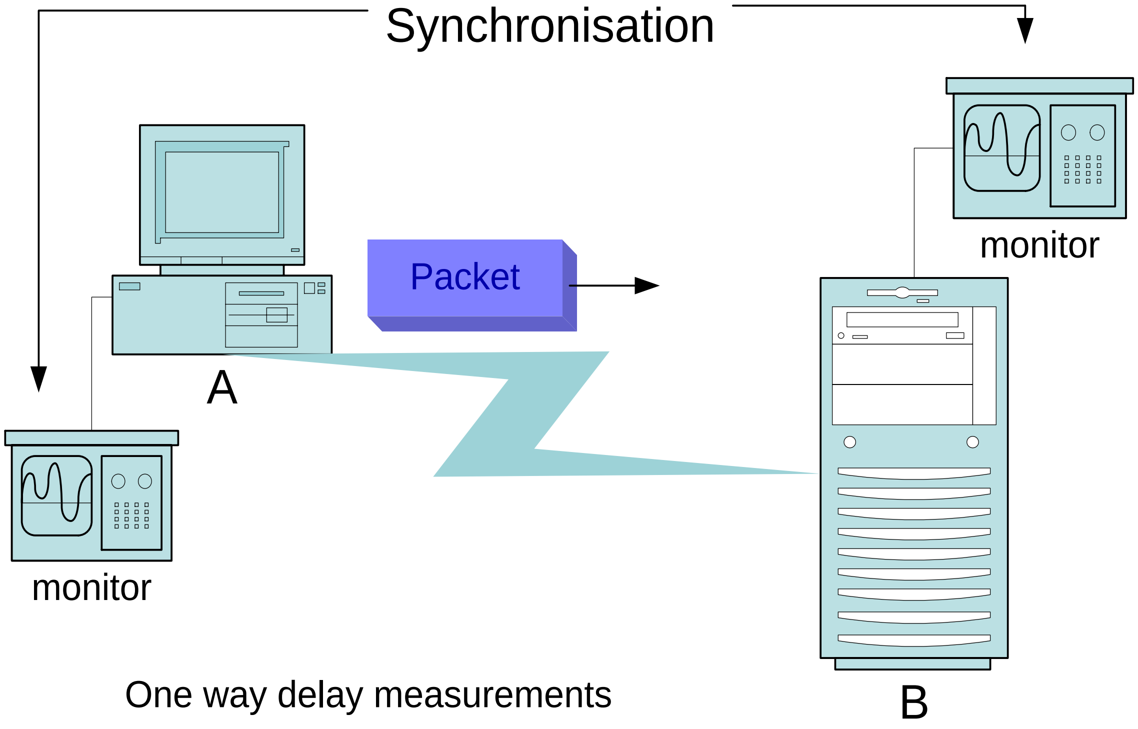
- The place or places in the network where they are actually made is important

- Measurements rely on observations at one or more places in the network.

- They could be made at:
  - a single point
  - many points or
  - at the Edge of network

Multipoint Placement Problems 1

- To measure the time a packet takes to travel from host A to host B, you'll have to record the times at which the packet leaves A and arrives at B using accurate, synchronised clocks.



One way delay measurements

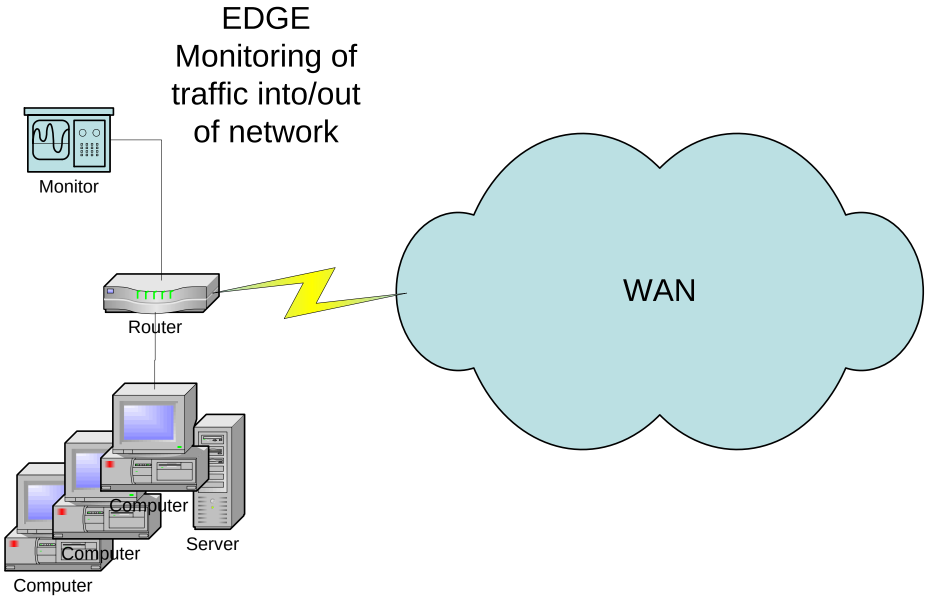
Multipoint Placement Problems 2

- For measuring traffic flows through a large network you might consider observing flows at many points, so as to gather detailed information about the paths packets take through the network.

- This is not a good idea, since it is difficult to correlate measurements of flows taken simultaneously at even a few different places.

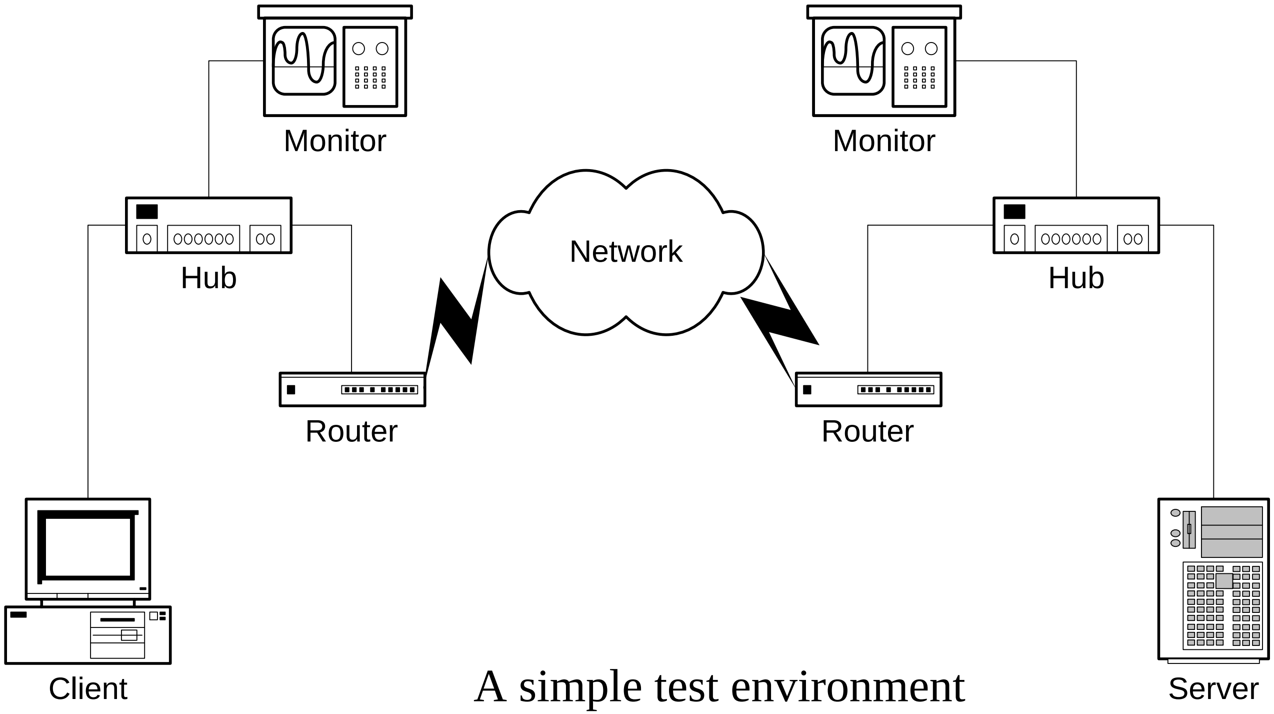
Edge Monitoring

It is much simpler to measure traffic at the ingress/egress links of a network, e.g. at border routers, avoiding the complexities of having to follow individual packets on their various paths through the network, while still allowing you to produce a traffic matrix showing overall traffic flows through it.



EDGE Monitoring of traffic into/out of network

Simple Test System



A simple test environment

Quantities to Measure

- Speed of transmission (raw data rate)
- Throughput (effective data rate)
- Bandwidth (network or channel capacity)
- Latency (response time, round trip delay)
- Packet loss
- Quality
- Signal strength (of wireless signals)
- Signal loss and noise/interference

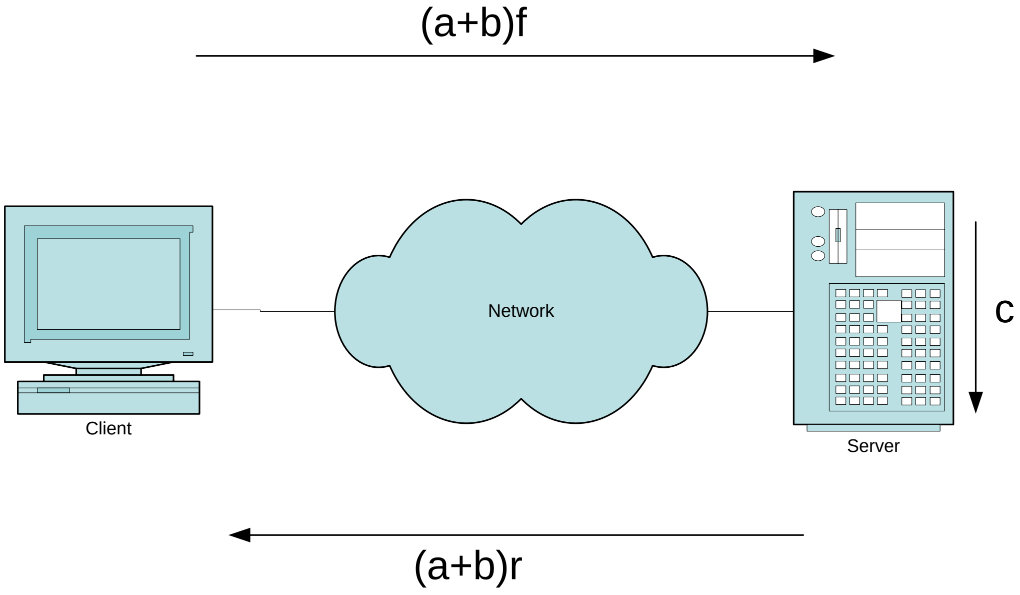
Metrics - What to measure?

Metrics are measurement values that can be used to indicate how well a network is performing.
Common metrics include:

- Latency (Delay)
- Jitter (Delay Variance)
- Throughput
- Bandwidth
- Utilization
- Packet loss
- Availability
- Reliability

Latency

Latency can be defined as the time taken for a packet to make the round trip from your end-user's computer to the distant server and back.



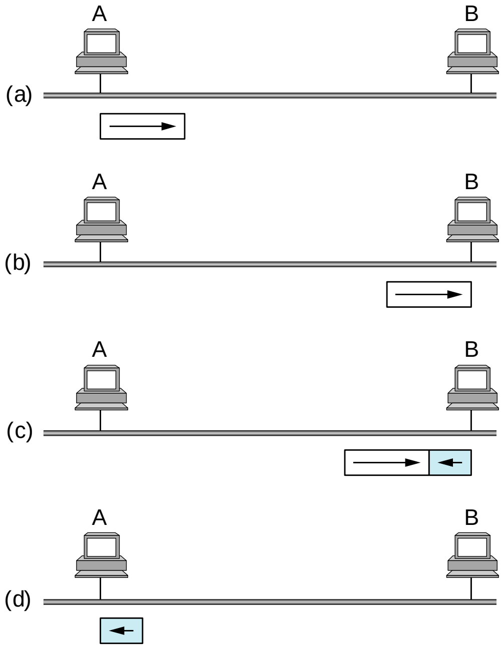
Latency = Total round trip delay = (a+b)f + c + (a+b)r

Latency in Networks

- Delay depends on distance and devices between end points
- A single segment Ethernet LAN exhibits low latency (<1ms)
- A satellite or long distance WAN links may exhibit high latency (>100ms)
- Excessive delay can seriously effect network performance, particularly when the TCP protocol is employed

Ethernet Latency and Design

- Must be considered when installing Ethernet (IEEE 802.3) LANs
- The maximum diameter of a LAN segment must ensure worst case collision detection can occur before a minimum sized frame is transmitted
- Designers must take care not too exceed the maximum round trip delay (slot-time) otherwise collisions may not be detected before the minimum frame size (64bytes = 512 bits) is transmitted.



International Internet Latency

e.g. UK to Japan

```
Pinging www.yahoo.co.jp [202.229.198.216] with 32 bytes of
data:

Reply from 202.229.198.216: bytes=32 time=286ms TTL=234
Reply from 202.229.198.216: bytes=32 time=286ms TTL=234
Reply from 202.229.198.216: bytes=32 time=287ms TTL=234
Reply from 202.229.198.216: bytes=32 time=284ms TTL=234

Ping statistics for 202.229.198.216:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 284ms, Maximum = 287ms, Average = 285ms
```

Q. What does TTL refer to in the reply packets?

Q. How does packet size effect RTT?

National Internet Latency

- UK to UK

```
Pinging www.yahoo.co.uk [217.12.3.11] with 32 bytes of data:

Reply from 217.12.3.11: bytes=32 time=21ms TTL=249
Reply from 217.12.3.11: bytes=32 time=21ms TTL=249
Reply from 217.12.3.11: bytes=32 time=24ms TTL=249
Reply from 217.12.3.11: bytes=32 time=20ms TTL=249

Ping statistics for 217.12.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 24ms, Average = 21ms
```

N.B. Measuring latency (round trip delay) using a tool such as Ping may not accurately reflect the performance users perceive as most applications don't use the ICMP (ping) packets to transfer data.

Performance Stats Example

- **International telecom companies such as C&W publish latency figures for their Global Internet Backbone as an indication of network quality.**

  e.g.

  The objectives for the average monthly roundtrip latency for backbone traffic within C&Ws Internet network:

  Intra-Japan Less than 35 ms

  Japan-US Less than 180 ms

  N.B. *performance results can usually be found on the company web site*

  Q. What is the one way maximum delay for acceptable quality Voice traffic?

Data Rate and Throughput

- Data Rate (raw transmission speed) =

  total amount of data that can be transmitted through including overhead per unit time.

- 'Throughput' is the rate at which useful data is sent through the network

- Throughput is expressed in bits per second (bps), bytes per second (Bps) or packets per second (pps) and depends on many factors

Q. What is max raw transmission speed for Fast Ethernet and why is the effective throughput data rate always less than this?

Data Rate Units and Prefix

- Data rate is typically measured in multiples of the unit *bit per second* or *byte per second.*
- A **kilobit per second** (**kbit/s**, **kb/s**, or **kbps**) is a unit of data transfer rate equal to:
- 1000 bits per second or 125 bytes per second.
- A **megabit per second** (**Mbit/s**, **Mb/s**, or **Mbps** is a unit of data transfer rate equal to:
- 1,000,000 bits per second or 1,000 kilobits per second or 125,000 bytes per second.
- A **gigabit per second** (**Gbit/s**, **Gb/s**, or **Gbps**) is a unit of data transfer rate equal to:
- 1,000 megabits per second or 1,000,000 kilobits per second or 1,000,000,000 bits per second or 125,000,000 bytes per second

N.B KB prefix for file size often refers to 1024 bytes so be careful when measuring file throughput. Also M usually means 1024x1024 =1048,576

Throughput and Packet Size

- Throughput is a function of packet (or frame size at data link level)
- The longer the packets, the higher the throughput
- The shorter the packets, the more effect packet headers and inter-packet gaps have on throughput.

Bandwidth

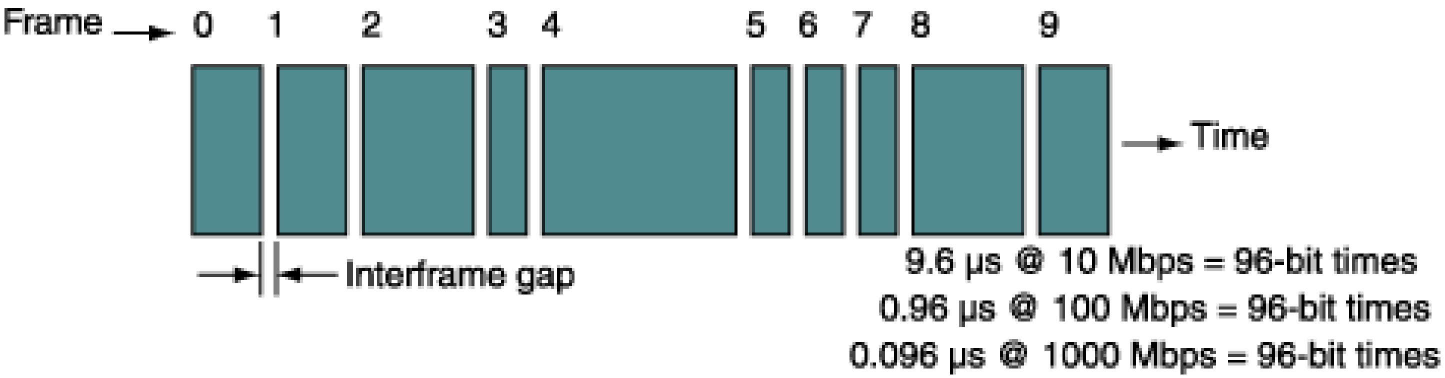
- Bandwidth is used to indicate the data carrying capacity or maximum throughput of a channel

- Example: For Basic Ethernet (10BaseT) the Bandwidth is the raw transmission speed = 10Mbps

Q. What is it for a: IEEE 802.11 g, n and ac WLAN, ADSL2+

Example Ethernet Throughput

- Ethernet frames have a maximum data payload of 1500 Bytes and are separated by an interframe gap.


Frame
0
1
2
3
4
5
6
7
8
9
Time
Interframe gap
9.6 µs @ 10 Mbps = 96-bit times
0.96 µs @ 100 Mbps = 96-bit times
0.096 µs @ 1000 Mbps = 96-bit times

- Calculate the maximum effective data rate (bps) for a 10BaseT LAN segment.

Assume no contention or packet loss

Q. What other overheads does an Ethernet Frame have?
(See Performance Monitoring and Analysis PPT)

Bandwidth and Link Capacity

- What determines the maximum rate at which data can be transmitted across a network link?

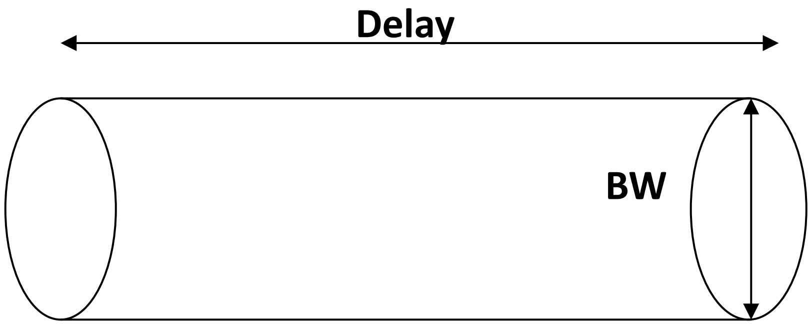
- Is it Bandwidth, Delay (latency) or Both? Does it depend on the transmission protocol used i.e. TCP or UDP.

- All may contribute to the maximum data rate achievable.

Capacity of a Link

The capacity of the link (logical pipe)is given by:

path bandwidth in bits per second x round-trip time (RTT) in seconds



- This is known as the bandwidth-delay product (BDP).
- The pipe can be fat (high bandwidth) or thin (low bandwidth) or short (low RTT) or long (high RTT).
- Pipes that are fat and long have the highest BDP.

Q: for a T3 link with RTT = 100ms, BDP = ?

TCP Window Size and Throughput

- The standard size of the Window field in the TCP header is 16 bits, allowing a TCP peer to advertise a maximum receive window size of 65,535 bytes = default for XP.

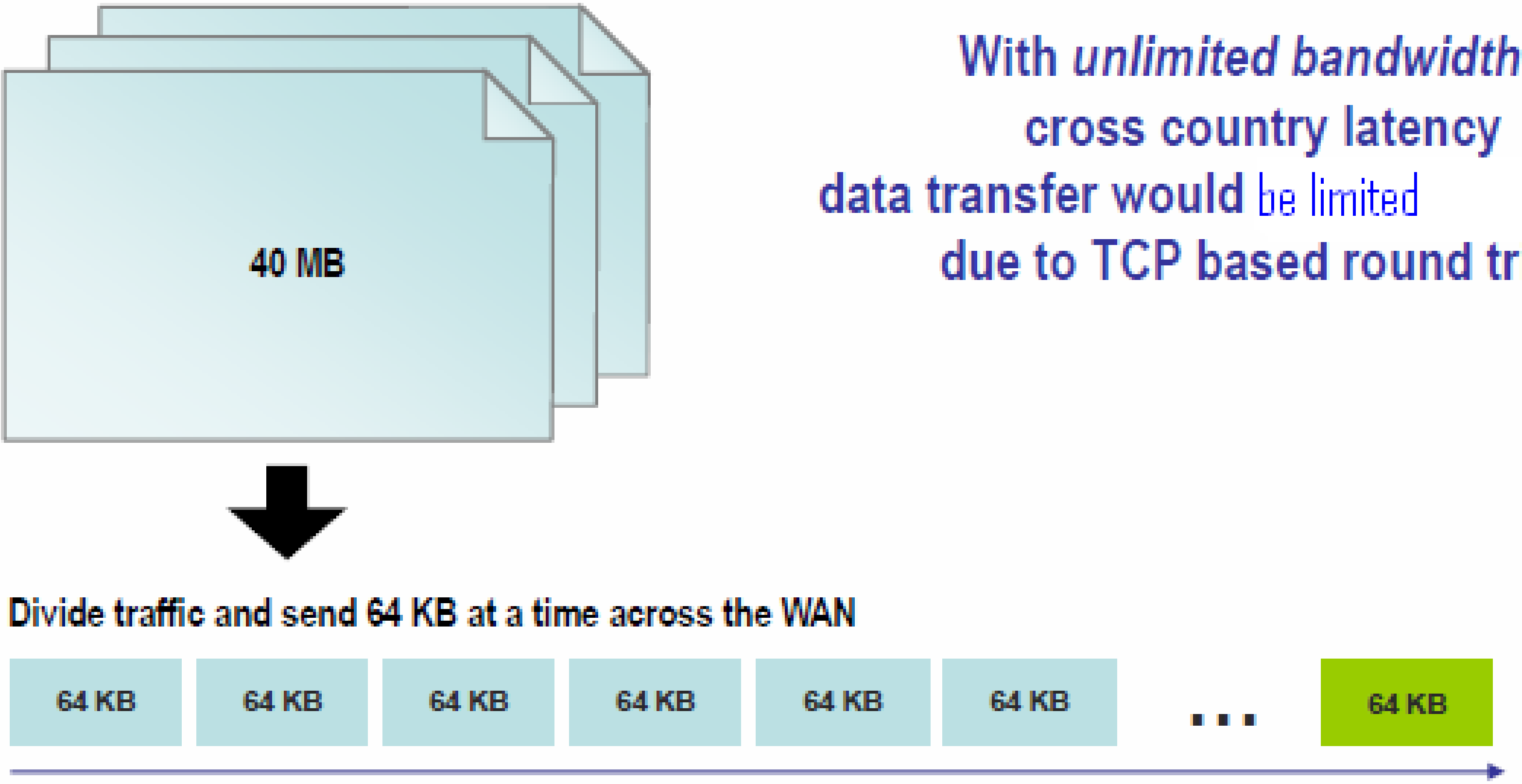
- You can calculate the approximate throughput for a given TCP window size from the following formula:

  Throughput = TCP max Receive Window size / RTT

Q: What is the throughput for a T1 link with RTT=160ms with RWIN = default window size for Win2000 of 8096Bytes?

TCP Chattiness Example

Send a 40 MB file across the WAN



With *unlimited bandwidth &*
cross country latency
data transfer would be limited
due to TCP based round trips

Divide traffic and send 64 KB at a time across the WAN

TCP Throughput Example 1

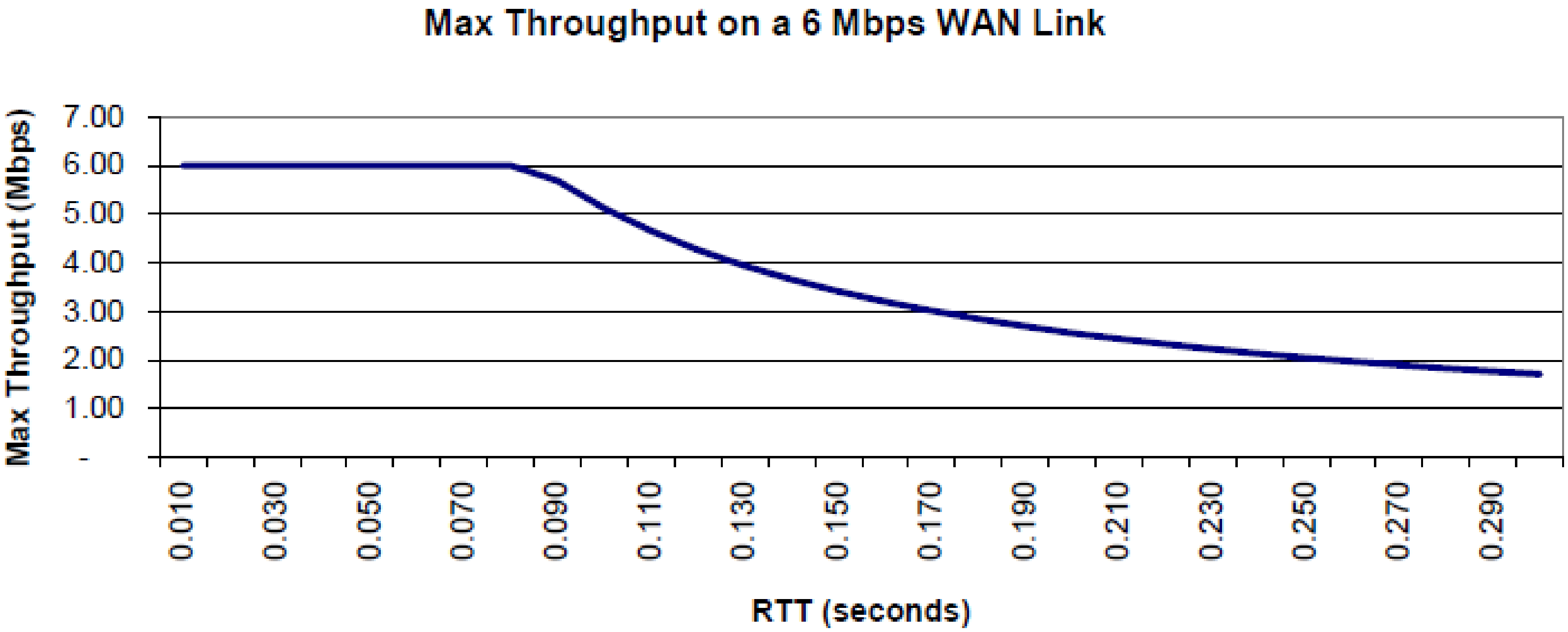


Figure illustrates the effective throughput of a 6 Mbps link (i.e. 4 x T1 lines) for a TCP connection with a 64 Kbytes maximum window and increasing latency. For low latencies, the link reaches its bandwidth-determined throughput, but for latencies larger than about 80 ms the first latency bottleneck is narrower than the bandwidth bottleneck.

TCP Throughput Example 2

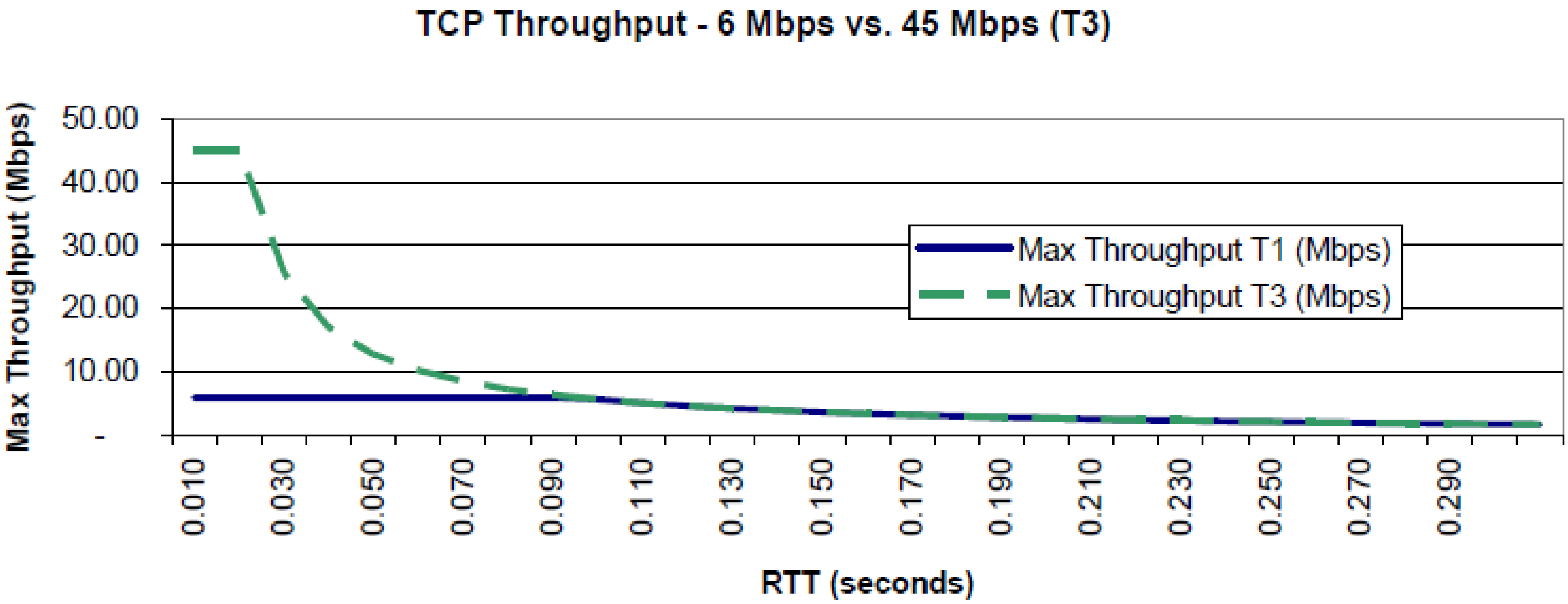


Figure illustrates the same data as example1, but has added a similar curve for a 45 Mbps T3. On this scale of graph, the 6 Mbps links throughput looks flat – but more alarming is that the T3 rapidly declines to a level indistinguishable from the 6 Mbps link as latency increases. At a latency of 90 ms or above and these small TCP windows, a T3 will not offer a single connection any more capacity than a 6 Mbps.

Network Utilization

- Network Utilization for a Network is a measure of the amount of bandwidth consumed as a percentage of the total available.

%U= (Bandwidth used/total Bandwidth available)x100%

Q. What is the %utilisation of a Fast Ethernet that transports data at 75Mbps?

Link Utilization

- Internet and WAN service is normally provided by one or more physical links.

- Each link has a maximum data rate known as the ‘access rate’ of the link.

- Link utilization = (throughput/access rate)x100%

Committed Information Rate

- Some links such as T1 and E1 leased line services, have a well-defined physical maximum speed (1.544 Mbps for T1 and 2.048 Mbps for E1)
- Other links, e.g. Frame Relay PVCs, have a second rate, the 'Committed Information Rate (CIR)'
- Committed information rate or CIR in a Frame relay network is the average bandwidth for a virtual circuit guaranteed by an ISP to work under normal conditions
- At any given time, the bandwidth should not fall below this committed figure
- For short term, the allowed rate may exceed the CIR to allow bursty traffic, known as the Excess Information Rate (EIR)

Broadband Access Speed

- Maximum data rates for upload and download are quoted by ISPs e.g. 256K/8M
- Download speed never achieves the maximum specified due to line quality (S/N ratio and contention ratio (up to 50:1)
- SLAs are rarely available for broadband Internet access except for SDSL
- Some ISPs use traffic shaping to throttle broadband access at specific times

Update on Business Broadband

- Many ISPs including BT and Virgin are offering higher speed broadband access

- Virgin offers very cheap cable connections of up to 100 Mbps for small business

- BT offers ADSL2+ copper and FTTC and FTTP fibre optic connections up to 80Mbps

- Annex M offers high upstream at the expense of a little download speed

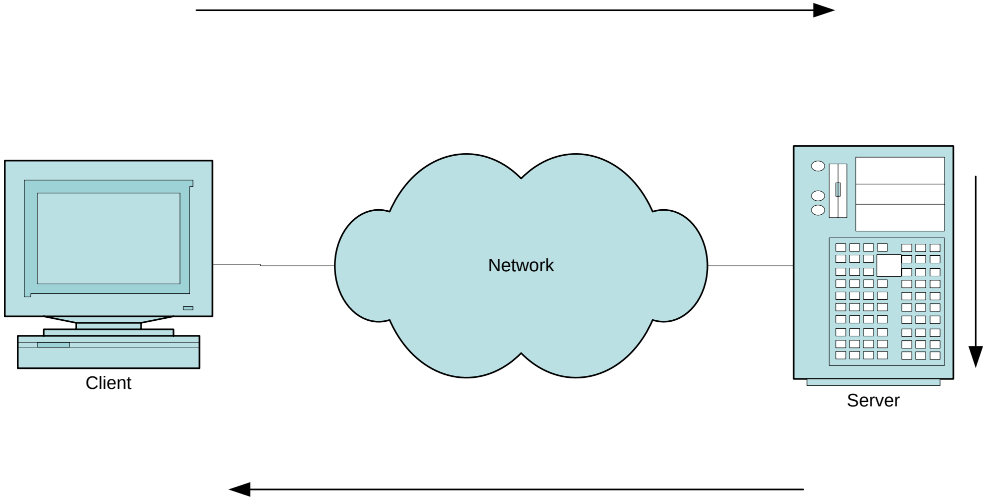
Packet Loss

- Network 'packet loss' is the fraction of packets lost in transit from client to server and back during a specified time interval, expressed as a percentage of the packets sent to the server during that interval.
- Packet losses vary from 0% (on an uncongested path) through 5 to 15% (severe congestion).
- Higher loss rates will most likely make the network unusable for normal purposes.
- Buffer or queue overflows as well as network faults can result in packet loss

Packet Loss Definition

Packet loss during a specific time interval =

no. of lost packets/total packets sent x 100%



Effects of Packet Loss

A moderate level of packet loss (say a few percent) is not in itself an indication of network failure, since:

- Some real-time services, e.g. Voice over IP, can tolerate some packet loss, but once a packet is lost there's no point in trying to recover it.
- TCP resends lost packets, and it also uses packet loss as a signal to decrease the sending rate. This behaviour is described as 'network-friendliness.'
- Many services will continue to operate effectively in the face of some packet loss.

How TCP/IP deals with packet loss

- **TCP** is a connection oriented reliable protocol and deals with packet loss by ARQ methods – Each packet has a sequence number and is acknowledged. So lost or corrupted packets can be retransmitted.

- **UDP** is a connectionless unreliable protocol so discards corrupted packets and has no facility to deal with lost packets

- **Examples:**
- Web transactions employ services of TCP
- VoIP (Voice over IP) employs services of UDP

Quality of Service (QoS)

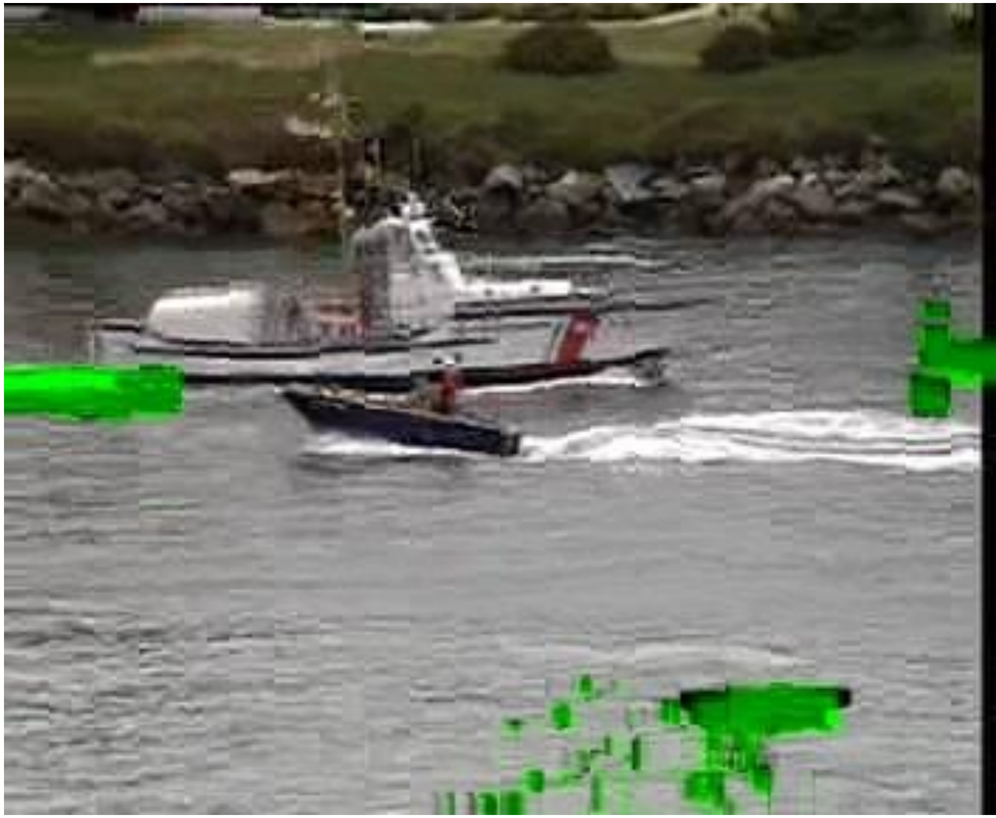
- 'Streaming' applications (such as Voice over IP and video conferencing) work best when there is little variation in end to end packet delay time.
- Although such applications can tolerate occasional packet losses, variation in delays can cause noticeable degradation in the user-perceived quality of their service.
- Metrics such as forward delay, packet loss, round trip delay and delay variance (or jitter) are becoming more important with the advent of real time communication which require a certain level of QoS.
- The IETF and ITU are producing models and standards for metrics which relate to QoS of networks.
- R-Factor and MOS are used to assess overall QoS

Packet loss, VoIP and Video

- VoIP and video conferencing operate in real time and employs the RTP (Real Time Protocol) to send digitised voice or video.
- Packet loss or corruption is likely when sending voice or video across the Internet or over a wireless network, but there is no point trying to correct corrupted packets or re-send lost packets.
- The effects of corrupted or lost packets are transitory, but they may be detectable by the listener or viewer as distorted voice or video (looks like interference or blocking of pictures).
- QoS will determine what is acceptable

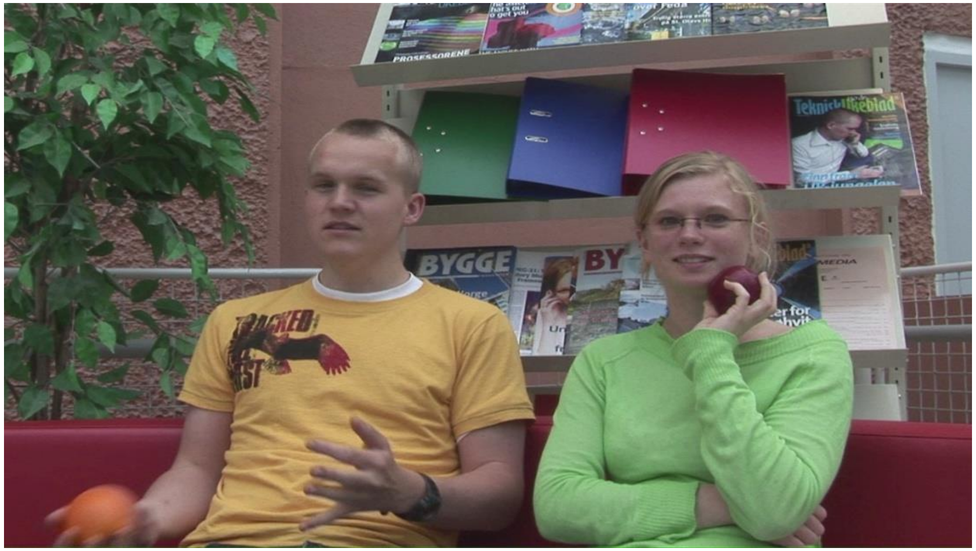
Effects of packet loss on a video

IP TV



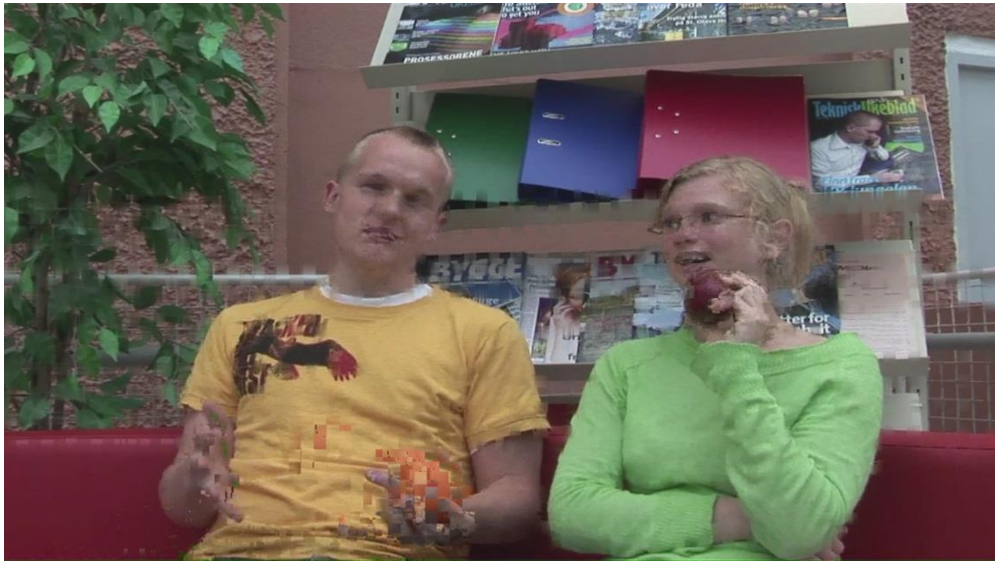
Packet loss can be more detrimental to compressed video with interdependent frames because errors potentially propagate across many frames.

Packet loss in HD video



1st frame sent

5% packet loss



QoS and Jitter

- 'Streaming' applications (such as Voice over IP) work best when there is little variation in their transmission time delay.

- Excessive delay between the sending of packets and their reception on the receiving end can cause for uneven, difficult-to-hear voice communication.

Q. In a VoIP system, what do jitter buffers do?

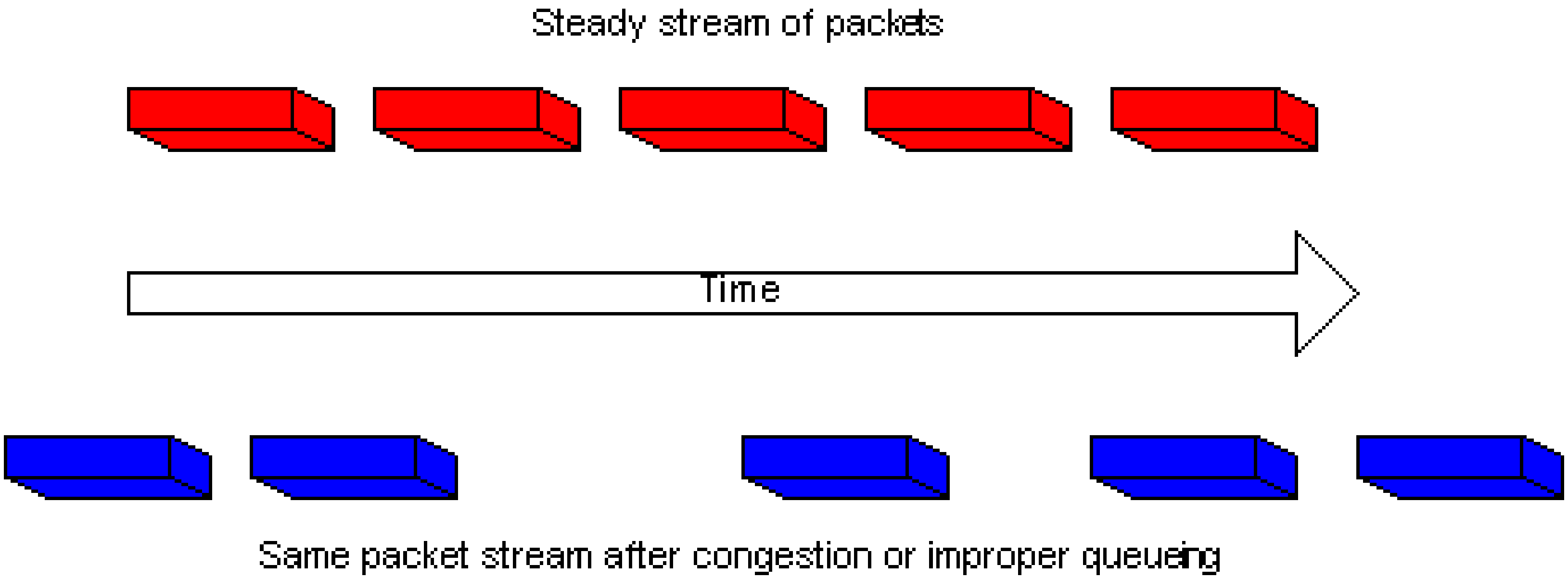
Delay Variance

- Variation in delay is given by:

$$D(n,n-1)=[R(n)-S(n)]-[R(n-1)-S(n-1)]$$

Where D(n,n-1) is the difference in transit time for packets n and n-1, S represents the time when packets (n,n-1) were sent, and R represents the time when packets (n,n-1) were received.

Packet Jitter



Availability

- Shows 'the ability of an *item* to be in a state to perform a *required function* at a given *instant of time* or at any *instant of time* within a given *time interval,* assuming that the external resources, if required, are provided'.

- From the user point of view, 'availability' over a specified time interval is the percentage of that interval during which the system was available for normal use.

Types of Availability

- **'Service availability:'** being able to send packets for a specified service - say WWW request packets - to a particular Internet host, and to receive answering packets

- **'Host availability:'** being able to send packets, say ping packets, to a particular Internet host, and to receive answering packets

- **'Network availability:'** being able to send packets from your network to the Internet, and to receive answering packets

Tests for Availability

- **Web service availability test:** download specified pages from target web server using web browser, measure latency, packet loss and throughput.

- **Host availability test:** ping to the target host, having made sure that it will respond to ICMP packets.

- **Network availability test**: traceroute to the target host, so as to determine whether there is connectivity to the target network**.**

Availability Measurement Example

Network Availability measurement used by C&W

The network availability objective is 100% as calculated with the following formula:

Availability = (uptime/total time) x 100
= (total time – down time) / total time x 100

MTTR=Mean Time To Restore
MTBF=Mean Time Between Failure

Un-availabilty

- Network faults are the most common cause for a loss of availability, e.g. a backbone fibre cable may be cut, or some piece of network equipment may fail.

- Another cause of unavailability is scheduled downtime, i.e. time specified by the provider for maintenance or upgrades. A service definition should make it clear whether or not scheduled downtime is considered 'unavailable' time.

Reliability

- Reliability is a measure of how often you get a response back that is wrong, or get a part that is defective. A 'wrong' response in a network would be a corrupted packet, which is not the same as getting no response - that would indicate a loss of availability.

  E.g. a server going down unexpectedly for 10 min is a reliability issue whereas taking it down deliberately is an availability issue
- Network transport protocols (TCP) provide checks on the correctness of the transferred data; if corruption is detected (by transport-layer software), the packets concerned are retransmitted, so that the user sees only a slower overall transfer rate.
- Such a lowered rate reduces the quality of the service, possibly to the point where that service should be considered unavailable.

Service Level Agreements

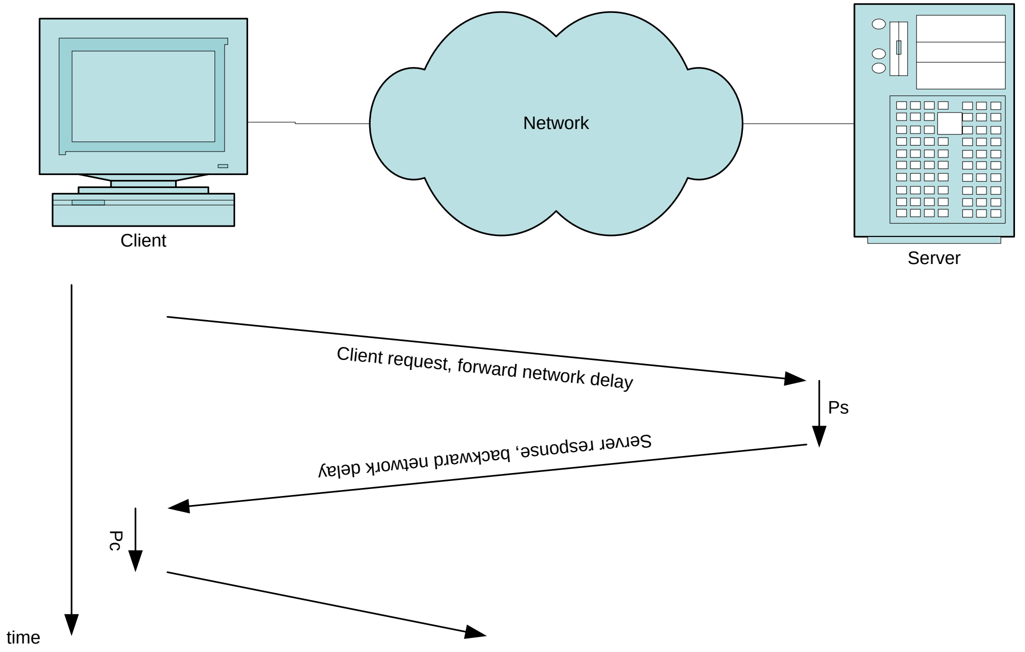
- Contract drawn up between service supplier and customer
- Specifies what is acceptable in terms of availability and quality of service
- Customer compensated if service falls below agreed level

Q. How long can a service be unavailable if the SLA is 99.99% ?

Application Rate Model

- Gives an indication of overall system performance
- It can be shown that that for a single transaction:

$$AppRate = N/(R_T+P_c+(2N/BW_c)+P_s+(2N/BW_s)).$$


Client
Network
Server
Client request, forward network delay
Ps
Server response, backward network delay
Pc
time

How to increase AppRate

- Decrease the client and server processing times
- Reduce the number of packets used
- Reduce the network delays
- Increase the size of the packets
- Increase the bandwidth

TCP Bandwidth and Packet loss

The formula models the TCP congestion avoidance algorithm and provides an upper bound to TCP session throughput as follows:

$$BW = (MSS/RTT)*C/(\sqrt{p})$$

Where:

BW: Bandwidth i.e. throughput (bytes per second)
MSS: Maximum Segment Size- Typically 1460 bytes.
RTT: Round Trip Time as measured by TCP (seconds)
p: packet loss rate
C: constant assumed to be 1.

Simulators and Emulators

- Riverbed Modeler (aka OPNET), NS-2 and COMNET simulator packages allow you to model network scenarios and see the effects of different value metrics on network performance.
- The commercial simulator Riverbed Modeler is particularly useful with its user friendly front end for performing ‘what if’ scenarios to see the effects of upgrading network components before you actually do it for real. *Riverbed Modeler Academic edition is available as a free download for students studying on network courses.*
- NISTNET, INE and Shunra emulators provide a more realistic method of mimicking network operation.

Riverbed Modeler Simulation Examples

Look at the Panko IT GURU network simulation exercises:

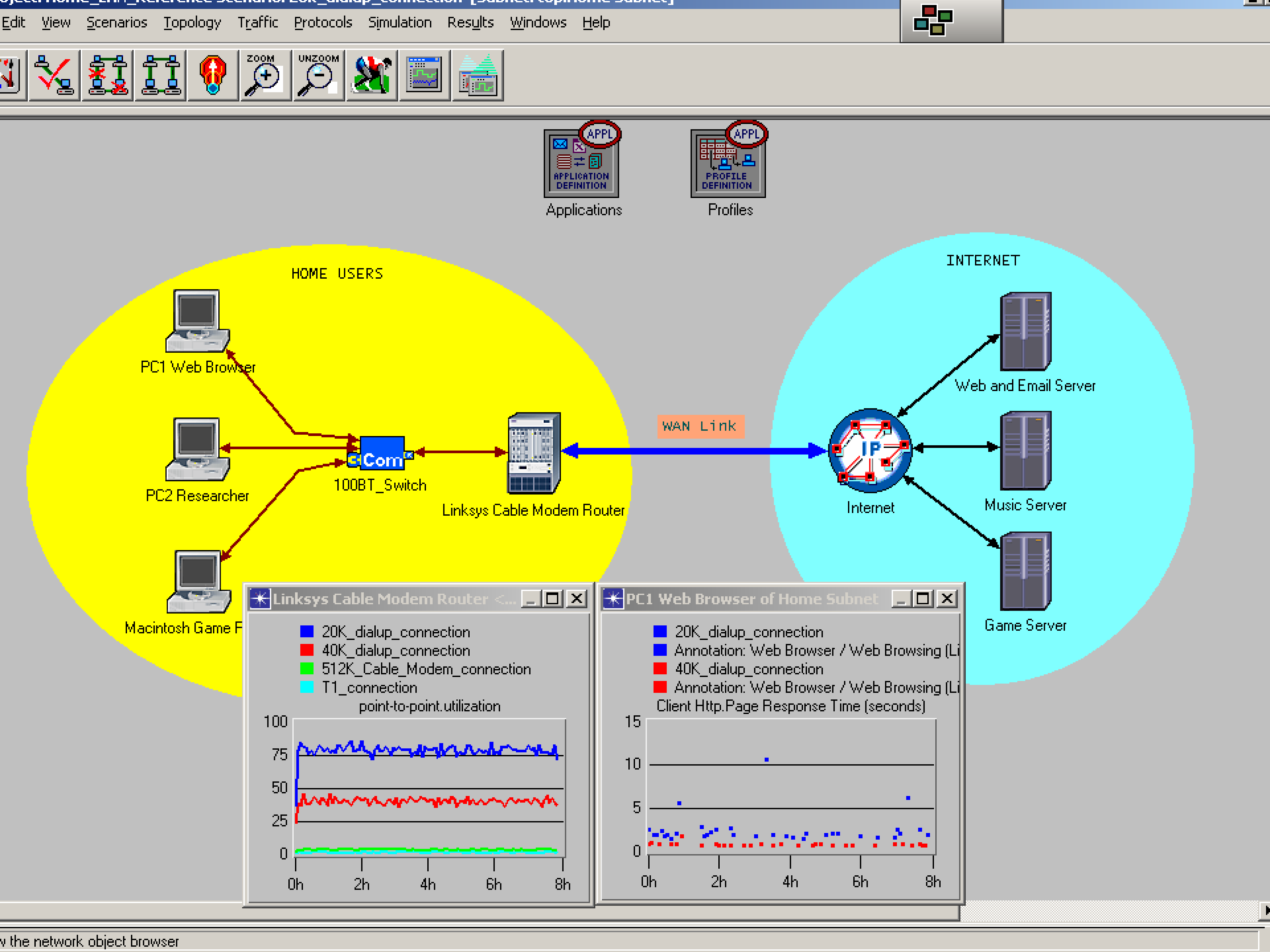
- Lab 1 ‘Evaluating Internet connection choices for a small Home PC network’

  This simulation shows web client accessing a web server using various access methods to see the effect on utilization and response times

- Lab 5 ‘Predicting the impact of TCP window size’

  This simulation will be used in the WAN monitoring and optimization laboratory to show the effects on throughput of received windows size on throughput across high latency WAN links.

- Changing the model variables for the various components allows you to see the effects on performance – ‘what if’ scenarios. Often called ‘change simulation’


Edit
View
Scenarios
Topology
Traffic
Protocols
Simulation
Results
Windows
Help
ZOOM
UNZOOM
APPL
APPLICATION DEFINITION
Applications
APPL
PROFILE DEFINITION
Profiles
HOME USERS
PC1 Web Browser
PC2 Researcher
Macintosh Game F
Com
100BT_Switch
Linksys Cable Modem Router
WAN Link
INTERNET
IP
Internet
Web and Email Server
Music Server
Game Server
Linksys Cable Modem Router <...
20K_dialup_connection
40K_dialup_connection
512K_Cable_Modem_connection
T1_connection
point-to-point.utilization
100
75
50
25
0
0h
2h
4h
6h
8h
PC1 Web Browser of Home Subnet
20K_dialup_connection
Annotation: Web Browser / Web Browsing (Li
40K_dialup_connection
Annotation: Web Browser / Web Browsing (Li
Client Http.Page Response Time (seconds)
15
10
5
0
0h
2h
4h
6h
8h
v the network object browser

Study Resources

- Baselines and Bottlenecks https://www.youtube.com/watch?v=D_HaWESYnvU
- Utilization Statistics https://www.youtube.com/watch?v=E7mVKZuDWfE
- Quality of Service https://www.youtube.com/watch?v=ObZVvYjfiBw