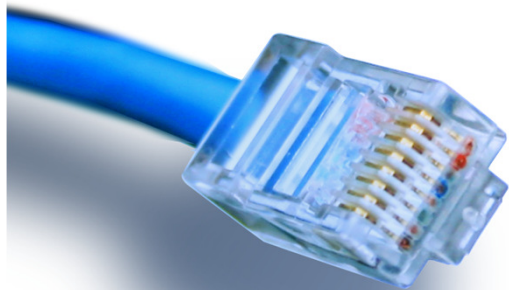


HOUSE OF
TECHNOLOGY



- en del af **mercantec**⁺



Netværksmålinger

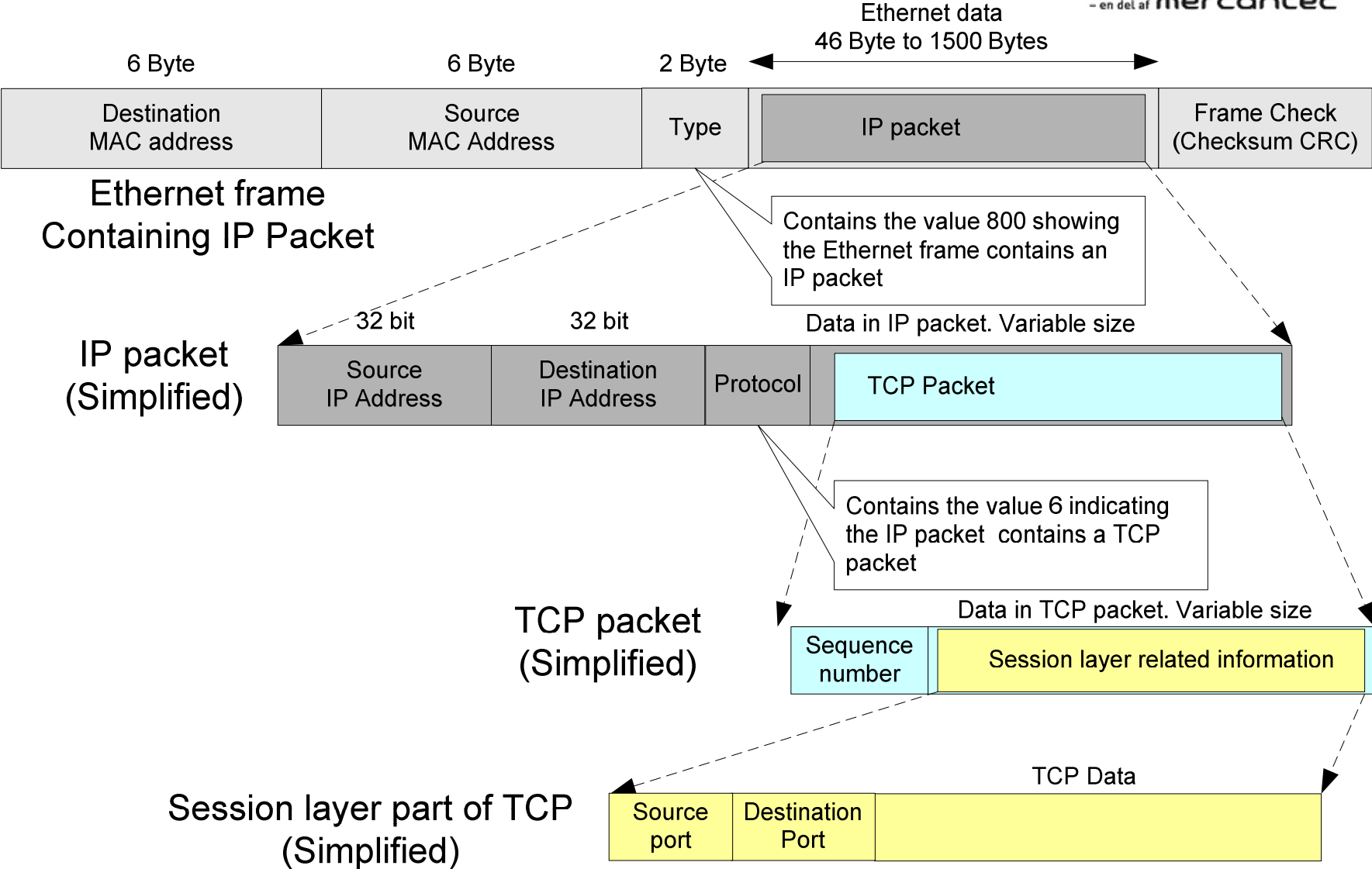
- en introduktion!

Netteknik

TCP - IP - Ethernet



- en del af **mercantec**⁺



DNS eksempel

- På en ældre Windows 7 pc sker følgende default ved DNS opslag:
 - HOSTS filen kigges igennem
 - DNS + DNS Suffix checkes
 - LLMNR aktiveres (Sender 2 requests på hhv. IPv4 og IPv6)
 - NetBIOS spørger ud på nettet (Sender op til 3 “queries”)

```
C:\Users\rasmus>ping media

Pinger media [10.1.0.20] med 32 byte data:
Svar fra 10.1.0.20: byte=32 tid<1ms TTL=128
Svar fra 10.1.0.20: byte=32 tid<1ms TTL=128
Svar fra 10.1.0.20: byte=32 tid<1ms TTL=128
Svar fra 10.1.0.20: byte=32 tid<1ms TTL=128

Ping-statistikker for 10.1.0.20:
    Pakker: Sendt = 4, modtaget = 4, tabt = 0 (0% tab),
    Beregnet tid for rundtur i millisekunder:
        Minimum = 0ms, Maksimum = 0ms, Gennemsnitlig = 0ms
```

DNS opslag set i Wireshark

The image shows a Wireshark network traffic capture. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 25 is highlighted in yellow, showing a NetBIOS Name Service (NBNS) query from 10.1.0.20 to 10.1.0.173. The packet details pane below shows the structure of this query, including the transaction ID (0xcaa4), flags (0x0110), and a single question for MEDIA<20> (Server service).

No.	Time	Source	Destination	Protocol	Length	Info
18	7.72615600	10.1.0.173	8.8.8.8	DNS	76	Standard query 0x194a A media.elmholtz.eu
19	7.84162400	8.8.8.8	10.1.0.173	DNS	151	Standard query response 0x194a No such name
20	7.84300200	fe80::1448:22c7:5ea:ff02::1:3	224.0.0.252	LLMNR	85	Standard query 0x59ff A media
21	7.84314600	10.1.0.173	224.0.0.252	LLMNR	65	Standard query 0x59ff A media
22	7.94348200	fe80::1448:22c7:5ea:ff02::1:3	224.0.0.252	LLMNR	85	Standard query 0x59ff A media
23	7.94356100	10.1.0.173	224.0.0.252	LLMNR	65	Standard query 0x59ff A media
24	8.14365500	10.1.0.173	10.1.0.255	NBNS	92	Name query NB MEDIA<20>
25	8.14382300	10.1.0.20	10.1.0.173	NBNS	104	Name query response NB 10.1.0.20
26	8.14730700	wistronI_1a:e1:6a	Broadcast	ARP	42	Who has 10.1.0.20? Tell 10.1.0.173
27	8.14739800	universa_6c:0f:0f	wistronI_1a:e1:6a	ARP	60	10.1.0.20 is at 00:16:41:6c:0f:0f

Frame 24: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

- Ethernet II, Src: WistronI_1a:e1:6a (3c:97:0e:1a:e1:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 10.1.0.173 (10.1.0.173), Dst: 10.1.0.255 (10.1.0.255)
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- NetBIOS Name Service
 - Transaction ID: 0xcaa4
 - Flags: 0x0110 (Name query)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - MEDIA<20>: type NB, class IN
 - Name: MEDIA<20> (Server service)
 - Type: NB
 - Class: IN

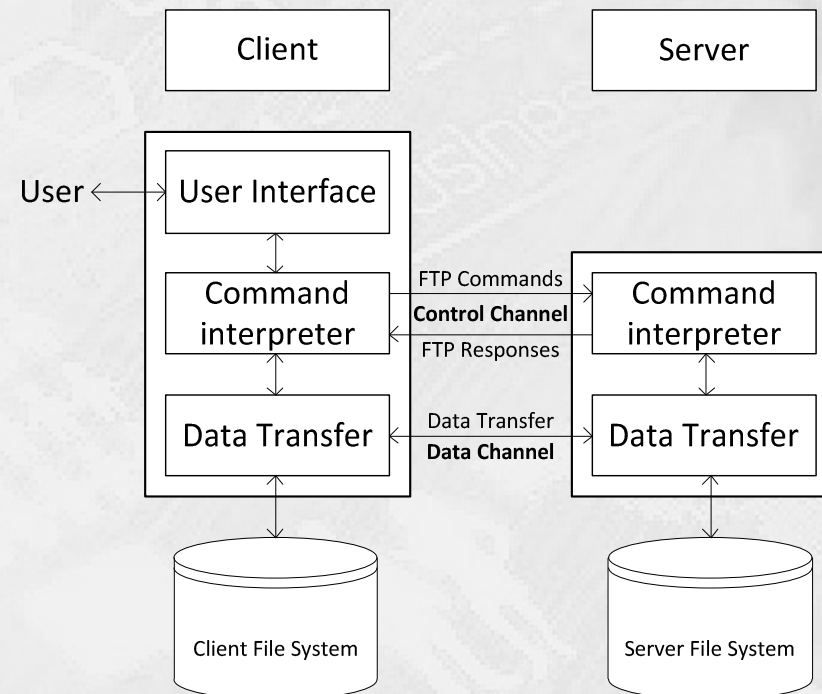
- LLMNR:
 - En Microsoft-designet protokol som kan bruges på netværk hvor der ingen DNS service er
 - Dette er blot én af de mange protokoller der servicerer "zero-configuration networks" (Plug'n Play-netværk)
 - Defineret i RFC 4795.
 - LLMNR multicaster UDP messages på port 5355
 - IPv4 - 224.0.0.252
 - IPv6 - FF02::1:3
 - Den belaster firma-netværket og har ingen reel funktion her ;-)
 - På Windows 7 kan LLMNR disables via en "registry key entry":
 - HKLM/Software/Policies/Microsoft/WindowsNT/DNSClient/
 - Create a DWORD called "EnableMulticast" with a value of 0

File Transfer Protocol

- FTP:
 - Client/Server protokol som benyttes til at overføre filer mellem systemer på Internettet eller andre IP netværk
 - Defineret i RFC 959
 - Benytter TCP forbindelser til at overføre filerne
 - Understøtter brugen af username/password
 - Filerne sendes ukrypteret, så alle der opfanger pakkerne kan se data
 - Benytter både en kontrol og en data kanal til at sende med:
 - **Control:** Benyttes til at oprette sessionen samt til at kontrollere selve overførslen af data
 - **Data:** Benyttes til at overføre filer samt mappestruktur-info
 - Understøtter to forskellige "operation modes":
 - **Active:** Serveren kontakter klienten for at etablere sessionen
 - **Passive:** Klienten kontakter serveren for at etablere sessionen

FTP Channels

- Control channel
 - Authenticates with the server
 - Negotiates FTP parameters (Supported extensions)
 - FTP commands (dir, get, put, bye)
- Data Channel
 - Transfers files and directory listings



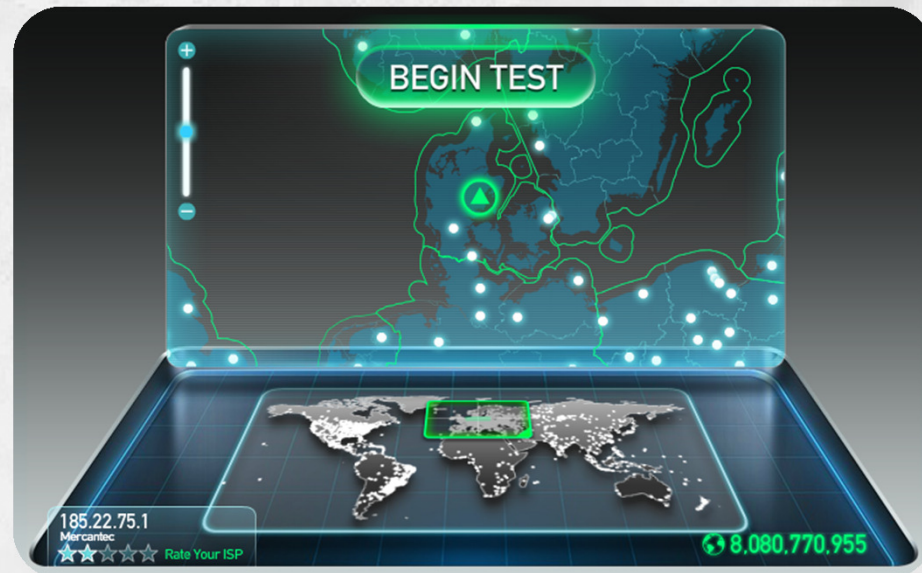
Eksempler på netværksmålinger

- Application layer file transfer
- Network layer latency
- Transport layer bandwidth (TCP/UDP)
- Transport layer latency

- Netværkets 'performance' angiver hvor godt et netværk eller en netværksenhed yder under specifikke betingelser
- Ofte skal netværksadministrator måle og dokumentere et netværks 'baseline' (have et sammenligningsgrundlag til senere)
- Hvis vi måler på en enkelt enhed kalder vi den for en DUT – en enhed under test
- Den samme enhed yder ofte forskelligt når vi måler på den og skifter mellem de forskellige lag i OSI-modellen:
 - Applikationslaget filoverførsel
 - Netværkslaget forsinkelse
 - Transport lags båndbredde (TCP / UDP)
 - Transport lags forsinkelse

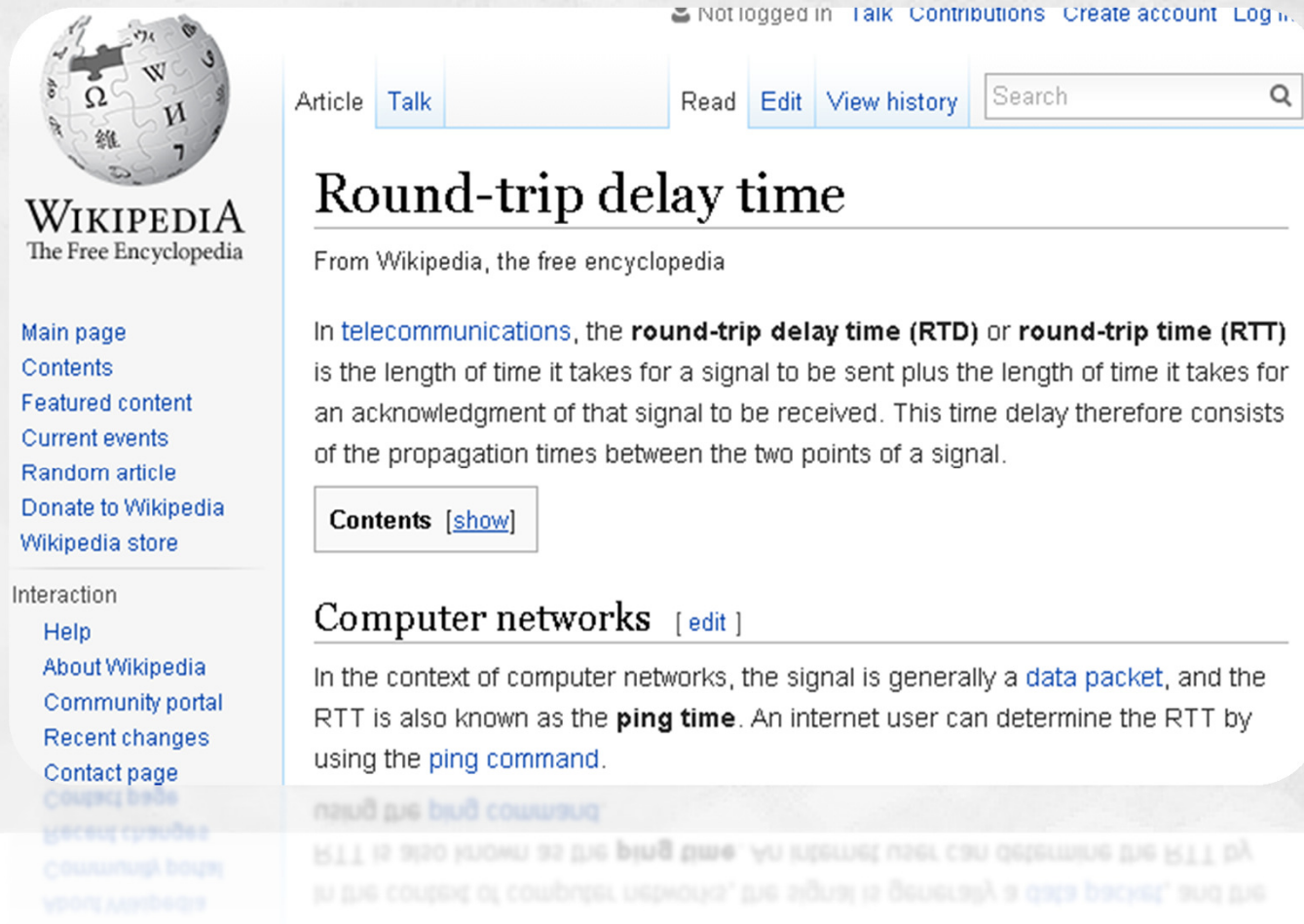
Filoverførsler & WAN-speed

- Overfør en stor fil fra en lagerenhed på dit netværk til din egen pc
 - - og tag tid på overførslen! Simpelt – men effektivt ;-)
 - 'Flaskehalsen' kan dog stamme fra Disk I/O
 - og ikke nødvendigvis fra netværket ;-)
- Check din WAN hastighed:
 - <http://www.speedtest.net/>
 - <http://hastighedstest.tdc.dk/>



Network Layer Latency

- Ping en enhed på netværket og notér tiderne!
 - Simpelt og effektivt ;-)



The screenshot shows the Wikipedia article for "Round-trip delay time". At the top, it says "Not logged in" and provides links for "Talk", "Contributions", "Create account", and "Log in". Below this, there are tabs for "Article" and "Talk", and buttons for "Read", "Edit", and "View history". A search box is also present. The main heading is "Round-trip delay time". Below the heading, it says "From Wikipedia, the free encyclopedia". The main text explains that in telecommunications, the round-trip delay time (RTD) or round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received. This time delay therefore consists of the propagation times between the two points of a signal. There is a "Contents" section with a "show" link. Below that, there is a section for "Computer networks" with an "edit" link. The text under "Computer networks" explains that in the context of computer networks, the signal is generally a data packet, and the RTT is also known as the ping time. An internet user can determine the RTT by using the ping command.

Transport Layer Bandwidth

- Brug en server og en klient på to enheder til at overføre data
- Iperf er et fantastisk værktøj til at teste netværk performance på tværs af en Device Under Test (DUT)
- Iperf skaber en netværks 'socket' og overfører tilfældige data fra hukommelsen
- Eleminerer problemet med 'flaskehalsen' fra Disk I/O
- Jperf er en Java GUI til Iperf, der kører på Windows
- Iperf og Jperf er gratis og OpenSource 😊
- Konfigurer én computer som serveren og én computer som klient – og start målingerne!
- Se links her:
 - <https://github.com/codefutures/jperf>
 - <http://www.firewall.cx/networking-topics/general-networking/970-network-performance-testing.html>

Jperf Server

The screenshot shows the JPerf 2.0.2 graphical user interface. At the top, the title bar reads "JPerf 2.0.2 - Network performance measurement graphical tool". The main window is divided into several sections:

- Configuration Section:** Contains the "Iperf command" field with the text `bin/iperf.exe -s -P 0 -i 1 -p 5001 -fk`. Below it, the "Choose IPerf Mode:" section has the "Server" radio button selected. To the right, there are input fields for "Server address", "Port" (set to 5,001), "Parallel Streams" (set to 1), "Listen Port" (set to 5,001), and "Num Connections" (set to 0). A "Client Limit" checkbox is also present. On the far right, there are "Run IPerf!" and "Stop IPerf!" buttons. Two white arrows with black outlines are overlaid on the image: arrow "1" points to the "Server" radio button, and arrow "2" points to the "Run IPerf!" button.
- Application layer options:** A blue-bordered panel containing various settings such as "Enable Compatibility Mode" (unchecked), "Transmit" (set to 10), "Output Format" (set to kBits), "Report Interval" (set to 1 seconds), "Testing Mode" (Dual and Trade options), "test port" (set to 5,001), and "Print MSS" (unchecked).
- Transport layer options:** A blue-bordered panel for selecting the protocol. "TCP" is selected. Under TCP, there are options for "Buffer Length" (2 MBytes), "TCP Window Size" (56 KBytes), "Max Segment Size" (1 KBytes), and "TCP No Delay" (unchecked). Under "UDP", there are options for "UDP Bandwidth" (1 MBytes/sec) and "UDP Buffer Size" (41 KBytes).
- Bandwidth Graph:** A large black area with a white grid. The y-axis is labeled "Bandwidth" and ranges from 0.0 to 1.0. The x-axis is labeled "Time" and ranges from -19 to 1. The graph is currently empty, indicating no data has been recorded yet.
- Output Section:** A white text area labeled "Output" at the top, which is currently blank. Below it are "Save", "Clear now", and "Clear Output on each Iperf Run" buttons.

Jperf Client



JPerf 2.0.2 - Network performance measurement graphical tool

JPerf

Iperf command: `bin/iperf.exe -c 127.0.0.1 -F -i 1 -p 5001 -f k -t 10`

Choose iPerf Mode: Client Server

127.0.0.1 Port 5,001

Parallel Streams: 1

Listen Port: 5,001

Client Limit:

Num Connections: 0

Run IPerf!

Stop IPerf!

Application layer options

Enable Compatibility Mode

Transmit: 10

Bytes Seconds

Output Format: KBits

Report Interval: 1 seconds

Testing Mode: Dual Trade

test port: 5,001

Representative File:

Print MSS

Transport layer options

Choose the protocol to use

TCP

Buffer Length: 2 MBytes

TCP Window Size: 56 KBytes

Max Segment Size: 1 KBytes

TCP No Delay

Bandwidth

Tue, 13 Nov 2012 00:07:07

#224:
5683741.00KBits/s

Output

[224]	4.0- 5.0 sec	665104 KBytes	5448532 Kbits/sec
[224]	5.0- 6.0 sec	655904 KBytes	5373166 Kbits/sec
[224]	6.0- 7.0 sec	679656 KBytes	5567742 Kbits/sec
[224]	7.0- 8.0 sec	692376 KBytes	5671944 Kbits/sec
[224]	8.0- 9.0 sec	693816 KBytes	5683741 Kbits/sec

Save Clear now Clear Output on each Iperf Run

Transport Layer latency

- Windows **Resource Monitor** kan bruges til at se Transport Layer latency
- Hver TCP-pakke bliver 'acknowledged', og Windows overvåger den tid det tager at modtage denne ACK
- Windows Resource Monitor viser også procentdelen af de tabte pakker i en TCP-session
- Disse oplysninger er meget nyttige når vi har brug for at tage et kig ind i en eksisterende TCP-forbindelse

Open Resource Monitor

Resource Monitor is a tool that you can use to monitor the usage of CPU, hard disk, network, and memory in real time.

Applies to Windows 7

- Open Resource Monitor by clicking the **Start** button . In the search box, type **Resource Monitor**, and then, in the list of results, click **Resource Monitor**.  If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

Transport Layer Latency

The screenshot shows the Windows Resource Monitor application with the 'Network' tab selected. The 'Processes with network activity' table lists ONENOTE.EXE (PID 2628) with 104 B/s sent and 81 B/s received. The 'Network Activity' summary shows 0 Kbps network I/O and 0% network utilization. The 'TCP Connections' table, filtered for ONENOTE.EXE, shows two connections with 0% packet loss and a latency of 210 ms. The right-hand side of the window displays three network performance graphs: 'Netværk' (10 Kbps), 'TCP-forbindelser' (20), and 'Bluetooth-netværksforb...' (100%).

Processnavn	PID	Afsendelse (B/sek.)	Modtagelse (...)	I alt (B/sek.)
ONENOTE.EXE	2628	104	81	185
svchost.exe (NetworkSer...	1436	19	23	42
System	4	15	5	20
OUTLOOK.EXE	2544	5	3	7

Processnavn	PID	Lokal adresse	Lokal port	Fjernadresse	Fjernport	Pakketab (%)	Ventetid (ms)
ONENOTE.EXE	2628	10.1.0.178	53334	65.54.191.33	443	0	210
ONENOTE.EXE	2628	10.1.0.178	53337	64.4.37.224	443		