# **TCP/IP** repetition

# Formål

Formålet med denne øvelse er at få et praktisk kendskab til programmet *Wireshark* og opfriske viden om Internet Protokollen. Programmet Wireshark anvendes til netværks analyse og protokol analyse. Programmet er opdelt i en monitor del og en capture del. Monitor delen bruges til at overvåge nettet og få statistiske oplysninger om nettet. Capture delen bruges til at opsamle data pakker (fx Ethernet) fra nettet og analysere protokollerne der er i pakkerne. Som måleobjekt bruger vi pc'erne og kommandoen PING. Bagerst i øvelse er der en hjælpeside som forklarer capture skærmens opbygning.

### Opgaver

1. I skal først undersøge hvilken IP adresse jeres computer har. Fra kommando prompten ( vælg Start | Kommandoprompt ) startes programmet IPCONFIG

Noter hvilken IP adresse maskinen har nu:

2. Start programmet Wireshark på computeren, vælg følgende:

#### Start | Alle Programmer | Wireshark

Programmet skal bruge mindst et netkort til dataopsamling, vælg et kort fra interface listen. Wireshark sætter netkortet i promiscuous mode, hvilket betyder at netkortet opsamlet alt hvad der kommer på nettet.



Herefter skal opsamlingen startes, k	lik på et <b>Netkort</b>		
<u>File Edit View Go Capture Analyze Statistics</u> 1	elephony Iools Help		
	+ + * 7 ½   E 🖬 🔍 q 🛛   🕷 🛛	<b>5</b> % <b>3</b>	
Filter:	✓ Expression Clear Apply		
WIRESHARK The World's I	Most Popular Network Protocol Analyzer		
Capture	Files		
Live list of the capture interfaces (counts incoming packets	) Open Open a previously captured file		Wel Visit the
Start capture on interface: Broadcom NetXtreme Gigabit Ethernet Driver Microsoft	Open Recent: C:\Users\rasmus\Docu e-punkt\Eksempler\4 minuter samt	ale.pcap (5424 KB)	Usei E
Microsoft Microsoft	C:\Users\rasmus\Documents\A19-DHCP.pcap (4421 Bytes)	(1052 kb)	Seci Work w
Start a capture with detailed options	A rich assortment of example capture files on the wiki		
Capture Help			-
We will be a successful capture setup			
			•
Ready to load or capture No Pac	kets	Profile: Default	1

Prøv nu at sende en PING til computer ved siden af din. Start fra kommando prompten og indtast følgende: **PING IP adresse** på nabo maskinen.

Når PING kommandoen er færdig klikkes på Stop Capture.

Noter TTL (Time To Live) værdien for en af de pakker som du sender, altså PING Req:

Noter TTL værdien for en af de pakker som du modtager, altså PING Reply: \_\_\_\_\_



# Display filter

Som du kan se i den foregående opsamling er der datapakker fra mange af de andre computere. For at fjerne dem skal der opsættes et filter, der filtrere alle pakker væk som ikke er til din computers fysiske adresse (MAC adresse). Alle pakker opsamles stadig, men kun de pakker du ønsker at se vises på skærmen.

Overst i Wireshark vinduet befinder **Display Filter** indstillingerne sig. Skriv et nyt filter og klik på Apply knappen.

<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> Analyze	<u>Statistics</u>	Telephony <u>T</u> ools	<u>H</u> elp					
	M (M (M (M	🖻 🖬 💥 🔮	) 占   🔍	🗢 🛸 🌍 7	<u>↓</u>   <b>           </b>	$\Theta$ $\Theta$ $\Theta$	m   👹	🖹 🛃 💥   💢		
Filter	:	K			▼ Expression (	Clear Apply				
No.	Time		Source		Destination		Protocol	Info		
	40 4.200940		192.1	00.100.10	195.100.123.	200	CRIDIN	Name query NB	LERMAKTC>	
	47 4.355734		HonHa	iPr_18:87:37	Broadcast		ARP	Who has 192.16	8.139.1?	Tell
	48 4.469410		Usi_8	c:30:f5	Broadcast		ARP	Who has 192.16	8.139.106?	Te
	49 4.780383		Wistr	on_98:fd:e5	Broadcast		ARP	Who has 192.16	8.139.95?	те
	50 4.789139		Intel	Cor_11:53:ef	Broadcast		ARP	Who has 192.16	8.139.106?	TE
	51 5.004783		192.1	68.139.66	192.168.139.	255	NBNS	Name query NB	WIN-8EDPXB	541L
	52 5.048321		192.1	68.139.128	239.255.255.	250	SSDP	M-SEARCH * HTT	P/1.1	
	53 5.272401		Veste	lкo_81:0a:2f	Broadcast		ARP	Who has 192.16	8.139.106?	Tŧ

Hvis man fx kun vil se ping og den forudgående arp kan man skriv "icmp || arp". "||" betyder eller når man programmere. Og vil her vise både ping(ICMP) og arp pakker.

<u>Eile Edit View Go Ca</u>	pture <u>Analyze</u> <u>Statistics</u> Telephony <u>T</u> ools	<u>H</u> elp	
	8 🖬 🗶 🎯 📇   🔍 🔶 🔶 😽		୧, ୧, ୧, ፻   ₩ ⊠ 🎭 🖗 🙀
Filter: icmp    arp		▼ Expression	Clear Apply
No.         Time           0         0.847669           8         0.847669           8         0.847950           14         2.347637           17         2.422390           18         2.426373           28         2.685760           36         3.666529           37         3.667071           38         3.667074           39         3.821101           40         3.843472           41         3.843979           42         3.911641           43         4.166300	Source C15C0_7C:D4:41 C15C0_7C:D4:41 C15C0_7C:D4:41 C15C0_7C:D4:41 C15C0_7C:D4:41 AsustekC_04:c4:01 AsustekC_04:c4:01 C15C0_7C:D4:41 QuantaC0_38:a2:88 QuantaC0_38:a2:88 AsustekC_04:c4:01 QuantaC0_38:a0:92 C15C0_7C:D4:41 C15C0_7C:D4:41 IntelCor_4f:2b:1e HonHaiPr_18:87:37	tination Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast	ARP who has 192.168.139.06? TE ARP who has 192.168.139.00? TE ARP who has 192.168.139.106? TE
44 4.213242 47 4.355734 48 4.469410 49 4.780383 50 4.789139	IntelCor_45:e8:d4 HonHaiPr_18:87:37 Usi_8c:30:f5 Wistron_98:fd:e5 IntelCor_11:53:ef	Broadcast Broadcast Broadcast Broadcast Broadcast	ARP who has 192.168.139.106? Te ARP who has 192.168.139.106? Te ARP who has 192.168.139.106? Te ARP who has 192.168.139.106? Te ARP who has 192.168.139.106? Te
<ul> <li>➡ Frame 55: 60 byte</li> <li>➡ Ethernet II. Src:</li> <li>0000 ff ff ff ff ff</li> <li>0010 08 00 06 04 00</li> <li>0020 00 00 00 00 00</li> <li>0030 00 00 00 00 00</li> <li>➡ File: "C:\Users\rasmus\App</li> </ul>	s on wire (480 bits), 60 bytes ca wistron 98:fd:e5 (00:26:2d:98:fd f ff 00 26 2d 98 fd e5 08 06 00 0 10 00 26 2d 98 fd e5 c0 a8 8b 0 00 c0 a8 8b 6a 00 00 00 00 0 00 00 00 00 00 00 ppData\Local\Tem Packets: 66 Displayed: 27 M	aptured (480 H d:e5). Dst: BH 018 3a8 00 Marked: 0 Dropped:	bits) roadcast (ff:ff:ff:ff:ff) 

## Opsamling af netværkstrafik med filter

Du skal nu prøve at opsamle en PING kommando igen, men denne gang med filteret aktiveret. For at få det hele med skal du slette ARP cachen, som er computerens dynamiske tabel til oversættelse af IP adresser til MAC adresser.

For at slette ARP cachen på computeren indtastes fra kommando prompten: ARP -d

Start opsamlingen igen og prøv at sende en PING til computer ved siden af din. Når PING kommandoen er færdig stoppes capture.

For at se indholdet af ARP cachen indtastes følgende fra kommando prompten: ARP -a

Noter indholdet af ARP cachen:

Noter rækkefølgen af de opsamlede pakker (skriv en forkortet tekst fra kolonnen Summary):

Undersøg hvilke protokoller en PING-anmodning (Echo Request) indeholder:



Hvilken information hentes i det første DNS-opslag ?

Hvilken information hentes i de efterfølgende DNS-opslag ?

