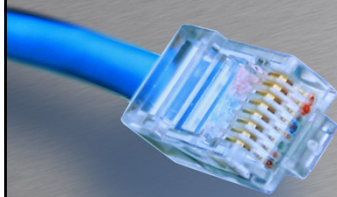


Mirror funktion



HOUSE OF
TECHNOLOGY



- en del af **mercantec**⁺

Wireshark

IP telefoni

Wireshark

- Gratis netværkssniffer
– www.wireshark.org
- Kan opsamle datapakker der kommer til PC
- Pakker skal derfor hen til PC'en
- Husk PoE funktion eller strøm adapter til telefon

Switch med "Port Mirror" funktion

SIP IP telefon 1

SIP IP telefon 2


Kopi af data mellem IP telefon 1 og 2



Mirror Funktion

HOUSE OF TECHNOLOGY
— en del af mercontec*

- Der sendes en kopi af trafik på en eller flere porte til en anden port. (Overvågning)
- Ikke fast standard
 - Cisco: Switched Port Analyzer. (SPAN)
 - 3COM: Roving Analysis Port. (RAP)
 - Zyxel: Port Mirroring




Mirror Funktion

HOUSE OF TECHNOLOGY
— en del af mercontec*

- Eksempel på Port Mirroring på Zyxel
 - Kopier trafik fra port 1,4,5 og 6 til port 3


```
Switch(config)# mirror-port  
Switch(config)# mirror-port 3  
Switch(config)# interface port-channel 1,4-6  
Switch(config-interface)# mirror  
Switch(config-interface)# mirror dir egress
```
- Eksempel på oprettelse af SPAN på Cisco Switch

```
EUC# CONFIGURE TERMINAL  
EUC(config)# MONITOR SESSION 1 SOURCE FASTETHERNET 0/1  
EUC(config)# MONITOR SESSION 1 DESTINATION FASTETHERNET 0/2
```




Network Tap (En anden måde)


HOUSE OF TECHNOLOGY



— en del af mercantec+




- Firmaer der laver Network Taps
 - Black box (Copper Tap)
 - Comcraft
 - Datacom Systems
 - Net Optics
 - Network Critical
 - VSS Monitoring




Cisco 7940

HOUSE OF TECHNOLOGY

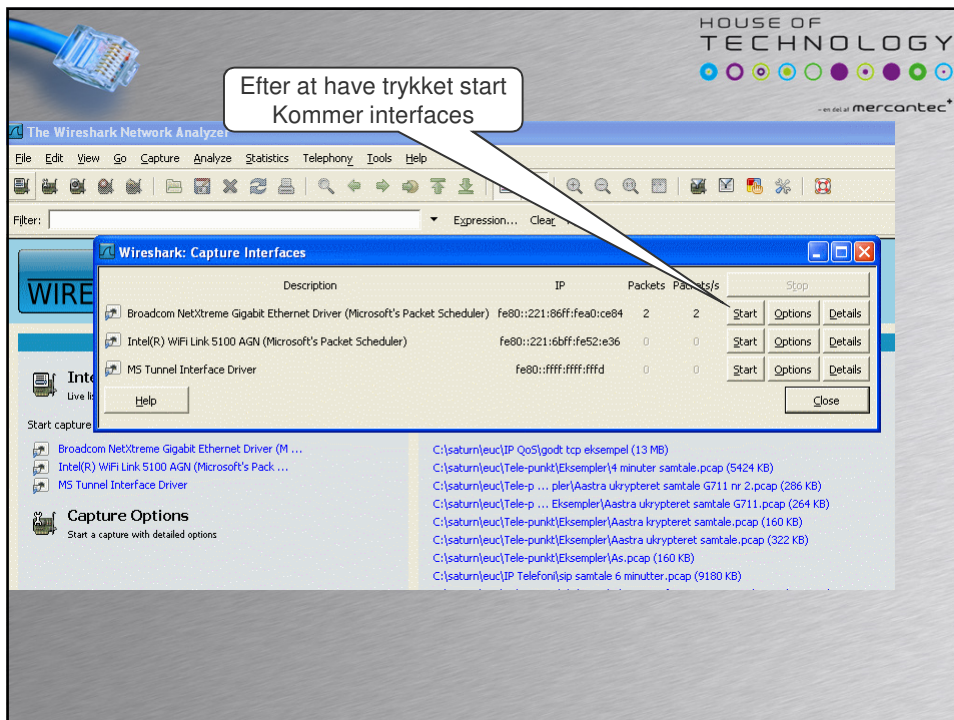
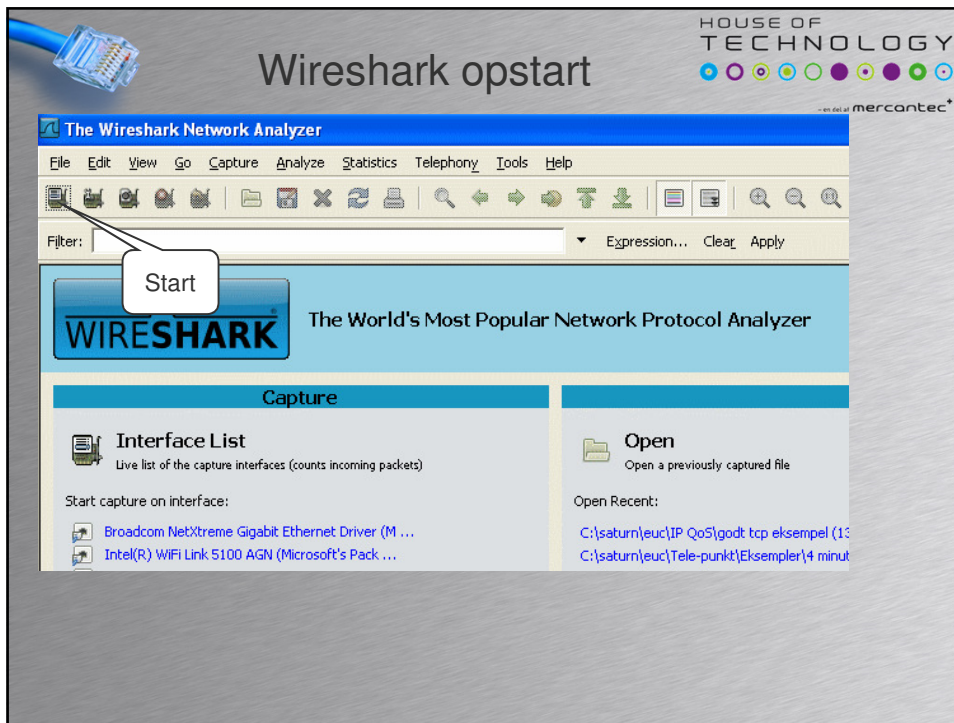


— en del af mercantec+

- Port Mirror på telefonen
- 7940 Telefonerne er sat op til at replikere alle pakker ud af PC porten også



Kopi af data sendes til PC



HOUSE OF TECHNOLOGY
— en del af mercantec+

Brug Telephony menuen

No.	Time	Source	Destination	Protocol	Info
77	3.479853	192.168.139.31	192.168.139.54	RTP	PT=ITU-
78	3.499383	192.168.139.31	192.168.139.54	RTP	PT=ITU-
83	3.597034	192.168.139.31	192.168.139.54	RTP	PT=ITU-
84	3.620473	192.168.139.31	192.168.139.54	RTP	PT=ITU-
85	3.640012	192.168.139.31	192.168.139.54	RTP	PT=ITU-
86	3.659532	192.168.139.31	192.168.139.54	RTP	PT=ITU-
87	3.679039	192.168.139.31	192.168.139.54	RTP	PT=ITU-
88	3.698580	192.168.139.31	192.168.139.54	RTP	PT=ITU-
89	3.718107	192.168.139.31	192.168.139.54	RTP	PT=ITU-
90	3.737647	192.168.139.31	192.168.139.54	RTP	PT=ITU-
91	3.757159	192.168.139.31	192.168.139.54	RTP	PT=ITU-
92	3.780641	192.168.139.31	192.168.139.54	RTP	PT=ITU-
93	3.800157	192.168.139.31	192.168.139.54	RTP	PT=ITU-
94	3.819684	192.168.139.31	192.168.139.54	RTP	PT=ITU-
95	3.839212	192.168.139.31	192.168.139.54	RTP	PT=ITU-

Husk at decode UDP som RTP!