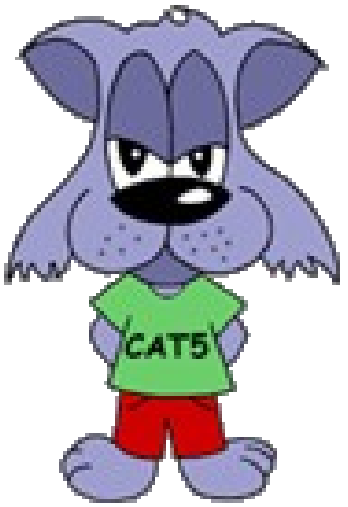
Signalopsamling i netværk

Kristen Nielsen

@ TheCamp.dk 2015



Signalopsamling i netværk

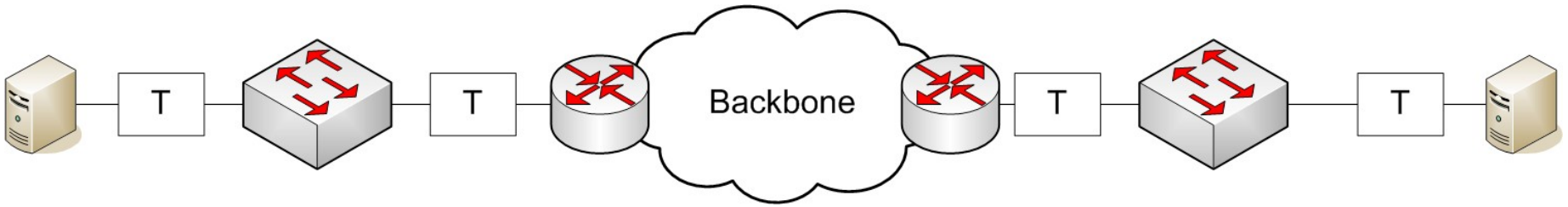
- Hvorfor er signalopsamling interessant
- Hvad er signalopsamling
- Hvad bruges signalopsamling til
- Hvordan kan signalopsamling foretages
- Hvilket udstyr anvendes

Hvorfor signalopsamling.

- Til fejlfindingsformål
- Netværksteknikerens "voltmeter"
- God mulighed for at få et network wide overblik.
- Overvågning

Hvad er signalopsamling

- Opsamling af datatrafik kan ske mange steder
  - På hosts (tcpdump, wireshark)
  - Fra Switche eller routere (spanporte/monitorporte)
  - Fra kabler. (kobberkabler, fiberkabler)
    - Imellem host og switch
    - Imellem switch/router
    - Imellem routere



På host med tcpdump

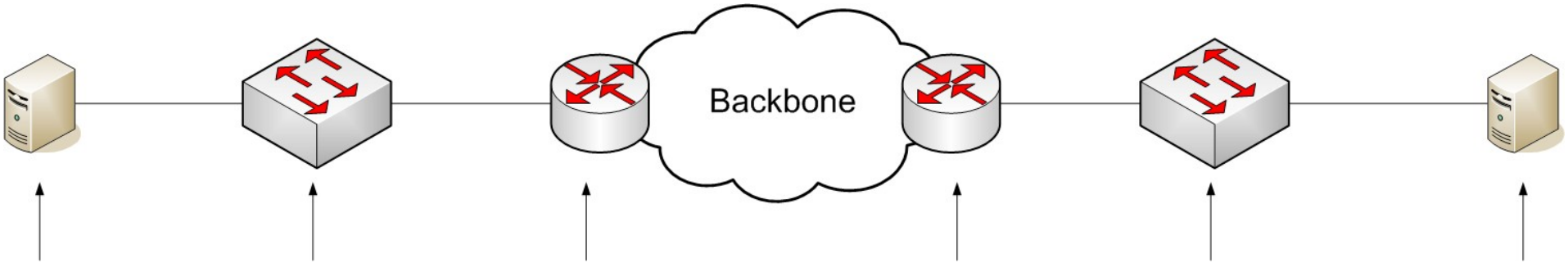
- Log ind på din (unix/linux) maskine og brug tcpdump (solaris: snif)

- Der kan måles trafik fra alle lokale netværksinterfaces på hosten. Dvs det trafik som hosten kan se kan måles.
- Tcpdump har mange options, kan gemme første del af pakken (default) eller hele pakken, gemme til disk, udskrive korte analyser af hver pakke. Osv
- Wireshark laver fuld protokol dekodning.

Måling med switche Spanporte/monitorporte

- Gamle hubs (10-100Mbps) sender alt ud på alle porte.
- Nyere og moderne switche har monitorporte der kan konfigureres til at sende en kopi af trafik fra udvalgte porte til en udvalgt udgang.
  - Kan give overload på den valgte udgang hvis de porte der måles på er højt belastede.
  - rx+tx trafik fra alle måleporte --> tx på monitorport.

Trafikmåling i udstyr



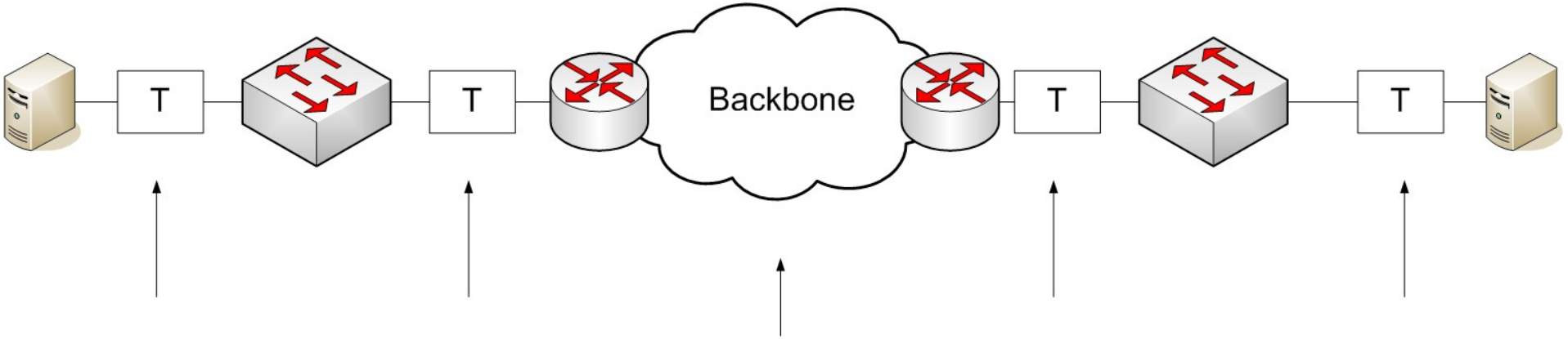
• Switche og routere har ofte mulighed for at sende en kopi af trafik fra udvalgte porte eller VLANS til en monitor port.

• Generelt måles typisk fra Ethernet eller IP og højere protokoller.

• I Switche/Routere
  - Monitorporte (rx, tx both)
  - VLAN monitorering (typisk en retning i VLAN => alt trafik i VLAN)
  - RSPAN (Remote spanport)

• På Hosts
  - Netværkskort (bpf- Berkeley Packet Filter el. lign)
  - Tcpdump
  - Wireshark

Trafikmåling på linjen med taps

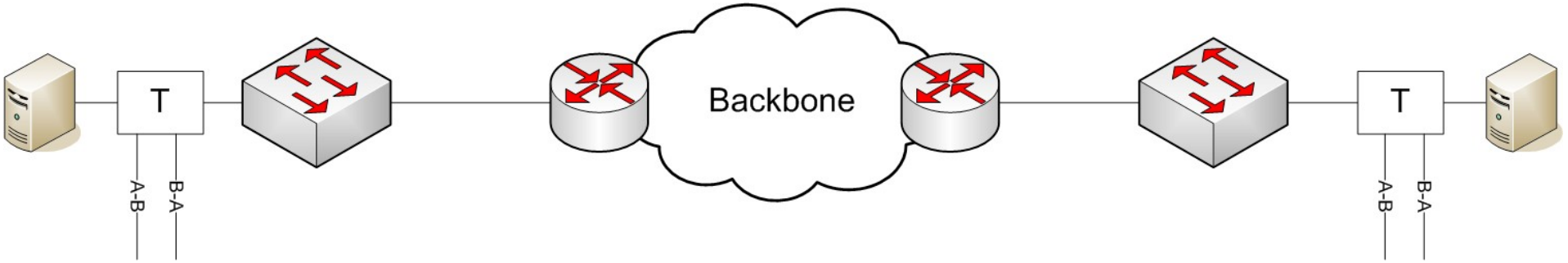


- Signaler på linjen / mediet kopieres på elektrisk eller lys niveau.
- Alle protokoller også de aller laveste måles.
- Timing på mediet afspejles præcist.

Måling af trafik på kabler.

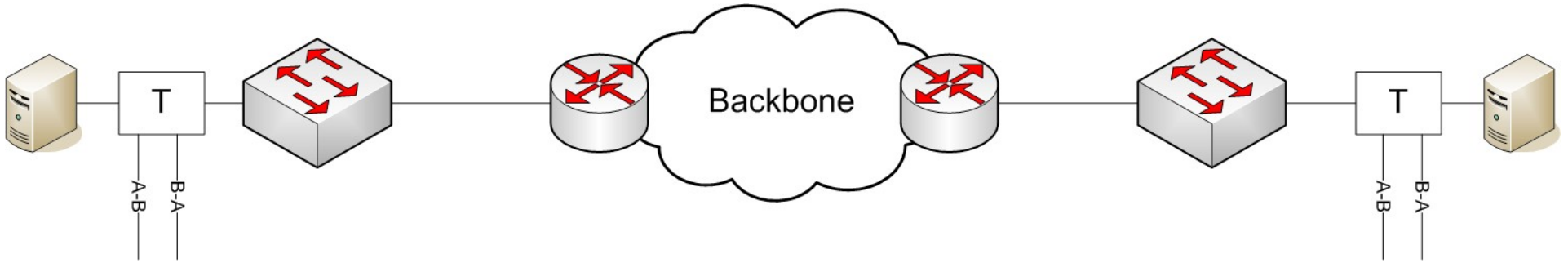
- For at måle trafik på kabler kræves en såkalt tap som kan kopiere signalerne på kablet til en ekstra udgang.
- Tappe skal passe til kablerne og til linjehastigheden i disse.
- Typisk/ofte er der 2 udgange for hvert kabel der tappes, en til hver retning. RX og TX (eller A -> B og B -> A retningen).
-

Signalopsamling med wiretaps



- Tappe findes i mange varianter – og skal passe til mediet der skal tappes.
- Sidder i signalvejen og laver en kopi af signalet. (kan typisk ikke detekteres)
- Signaler fra retning A → B og B → A kopieres typisk ud til hver sin udgang.
  - 1 Gbps linie kan ved max belastning i begge retninger give 2 Gbps ud.

Komplicerede traces

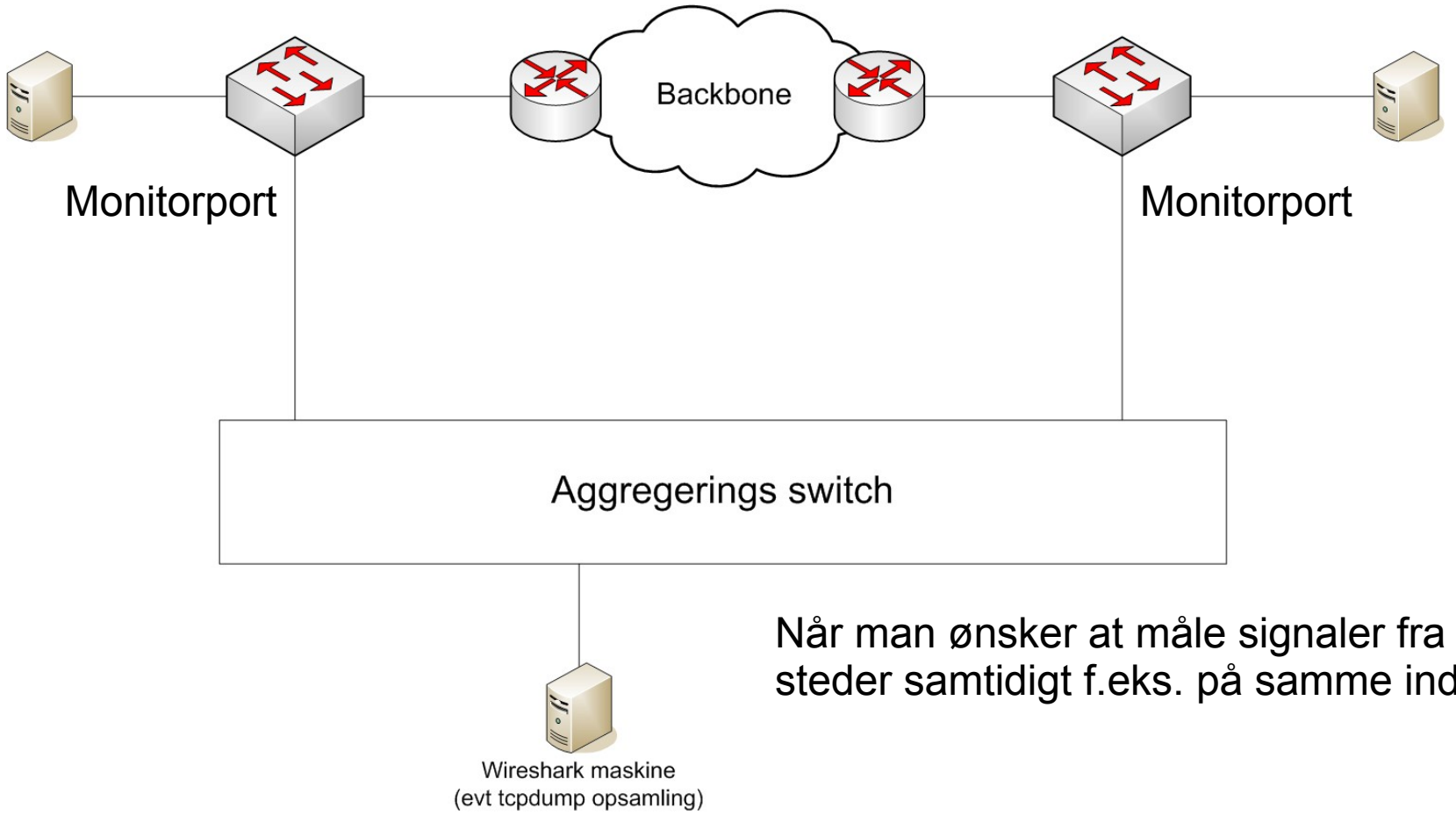


- Hvis man leder efter fejl i større netværk, vil man gerne se et samlet signal flow.
- Tracefiler optaget forskellige steder i netværket (.cap) filer kan pre merges med programmet mergecap. Wireshark kan også samle filer direkte. Timestamp anvendes til sorteringen.
- Tracewrangler kan forbehandle og evt. anonymisere tracefiler.

Håndtering af målesignaler

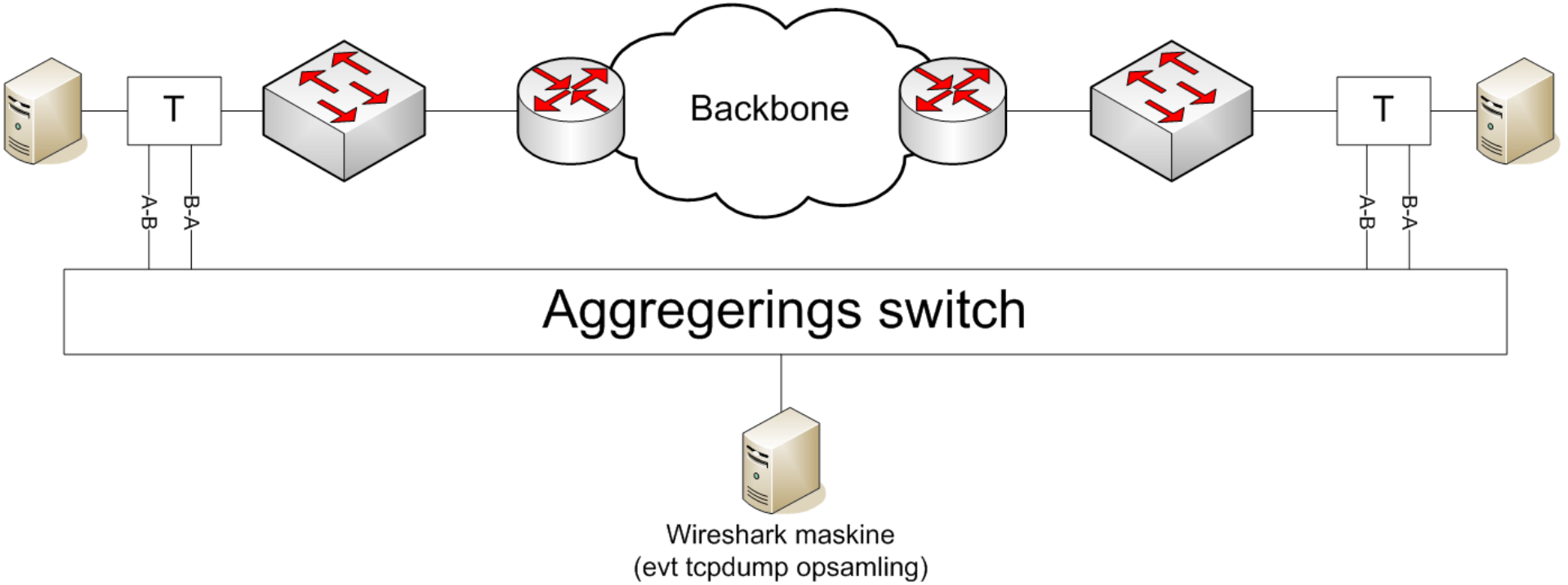
- Målesignaler kan ikke (let) sendes igennem almindelige switche da disse vil forsøge at håntere disse som almindelig trafik.
- Der anvendes istedet direkte feed til en server der analyserer signalet.
- Signalerne kan også aggregeres inden de sendes til en analyseserver.
- Der findes en række produkter der laver aggregering af målesignaler.
- Ofte koster de kassen.

Aggregering af signaler



Når man ønsker at måle signaler fra flere steder samtidigt f.eks. på samme indgang.

Opsamling til specielle formål



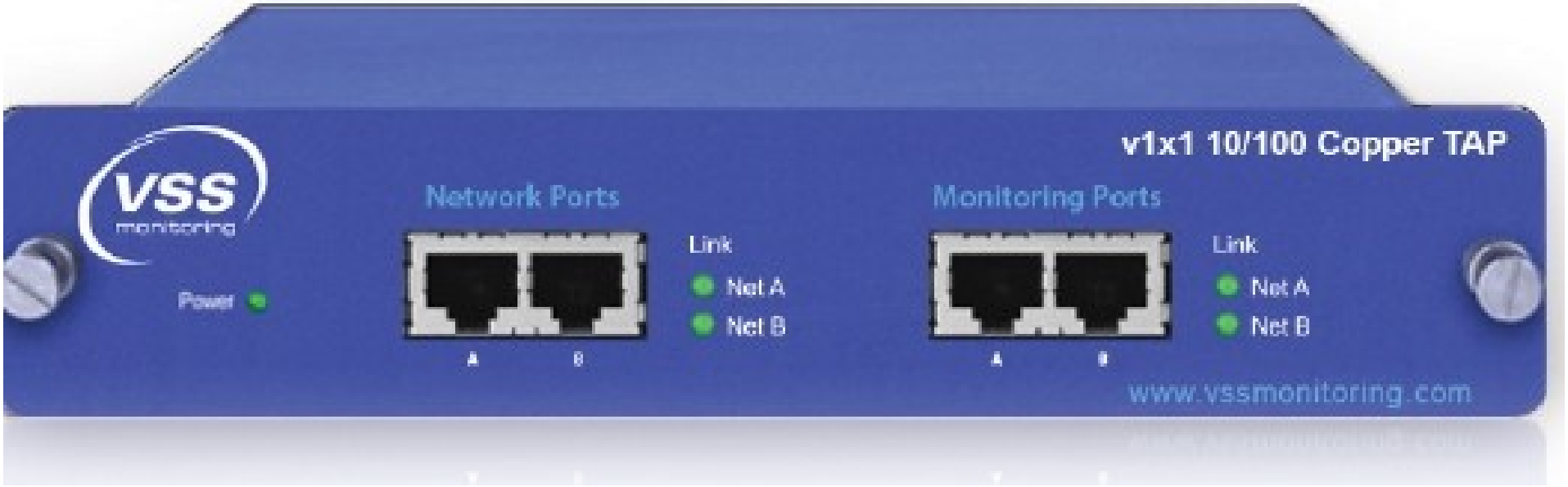
- Hvis der ønskes et målesignal med signalerings trafik i netværket vil man gerne undgå flere kopier af pakker i signalet.
- f.eks. ved at opsamle pakker i A → B retning ved hver host.
- Ved mere komplicerede setups kan man være nød til at filtrere på IP og retning.

Signalopsamlingsudstyr

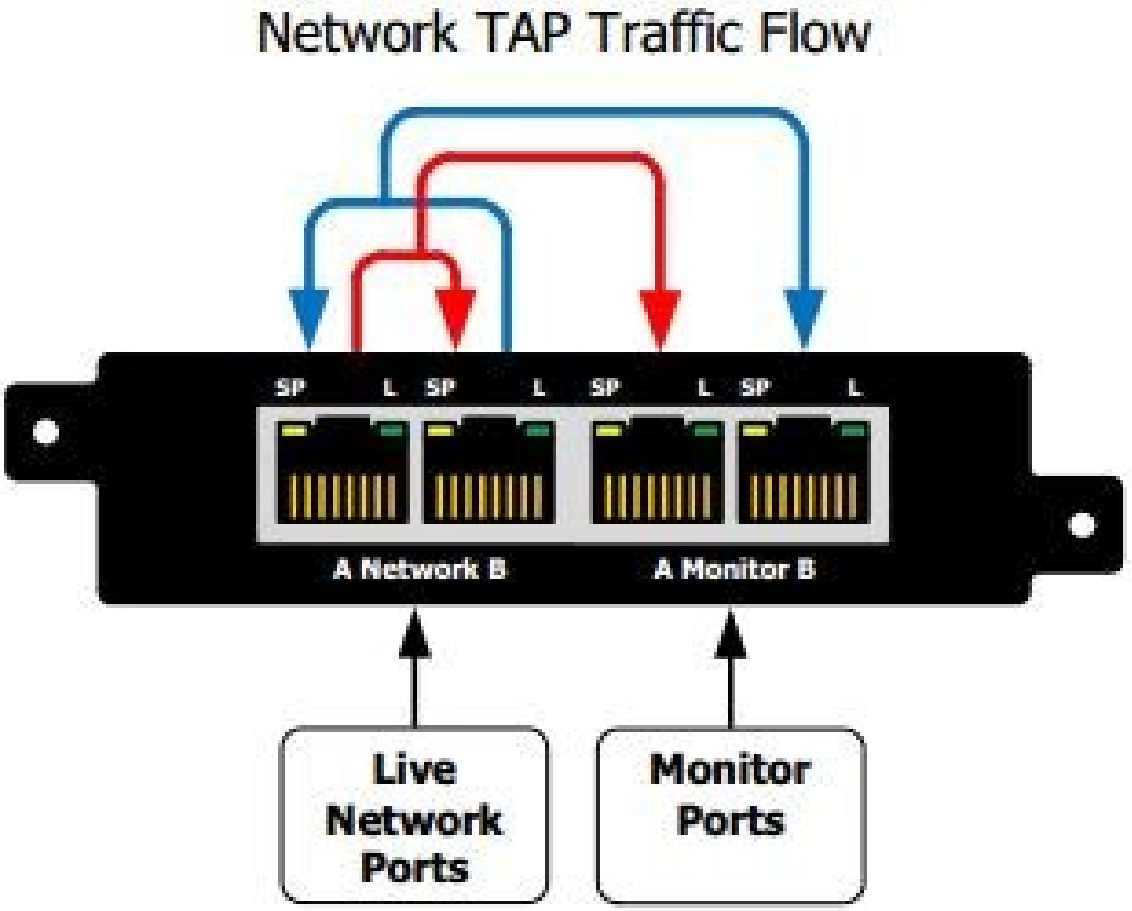
- Tappe, elektriske og optiske
- Aggregerings switche

Kobbertap

- 10/100 Mbps
- Bryder ikke linjen ved power off
- 2 udgange 1 til hver trafikretning



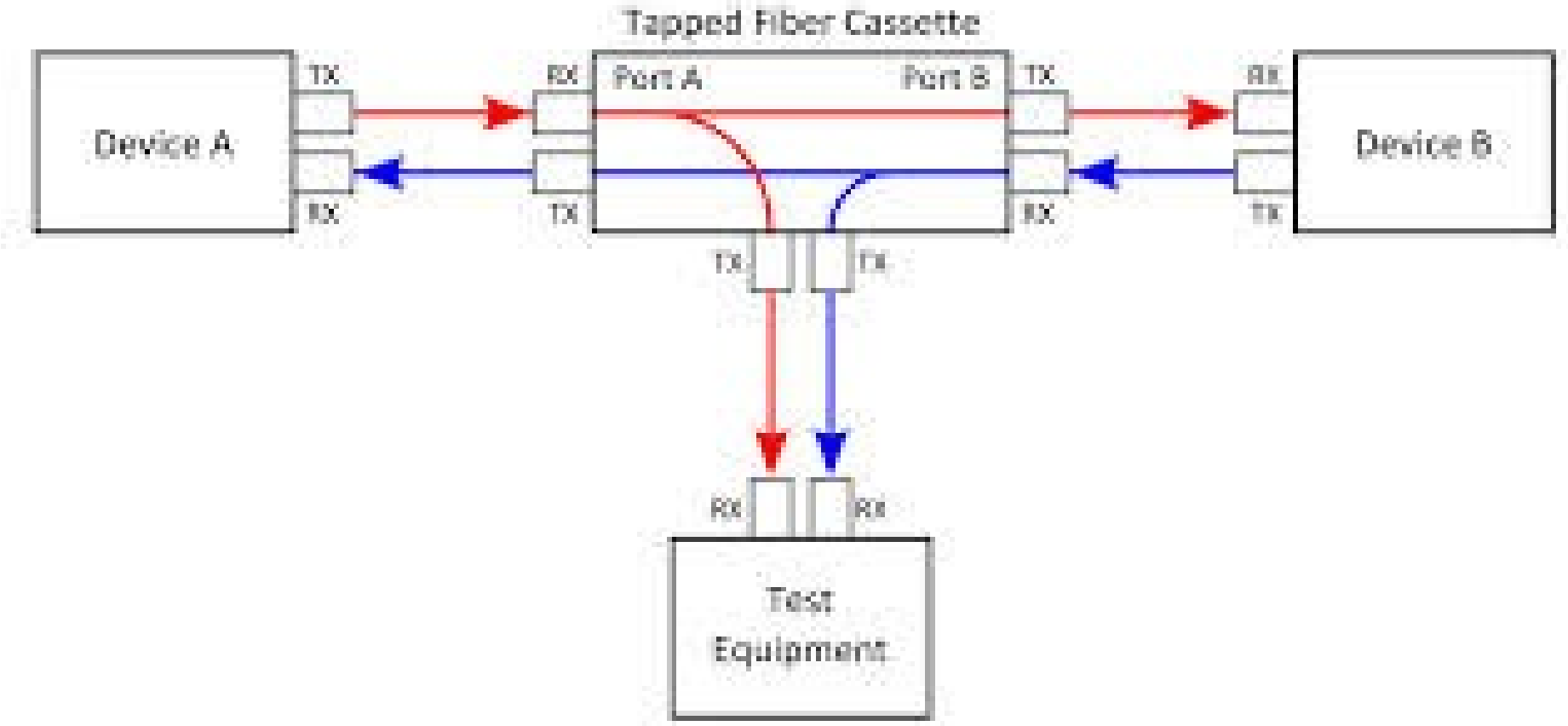
Kobbertap


Network TAP Traffic Flow
SP
L
SP
L
SP
L
SP
L
A Network B
A Monitor B
Live Network Ports
Monitor Ports

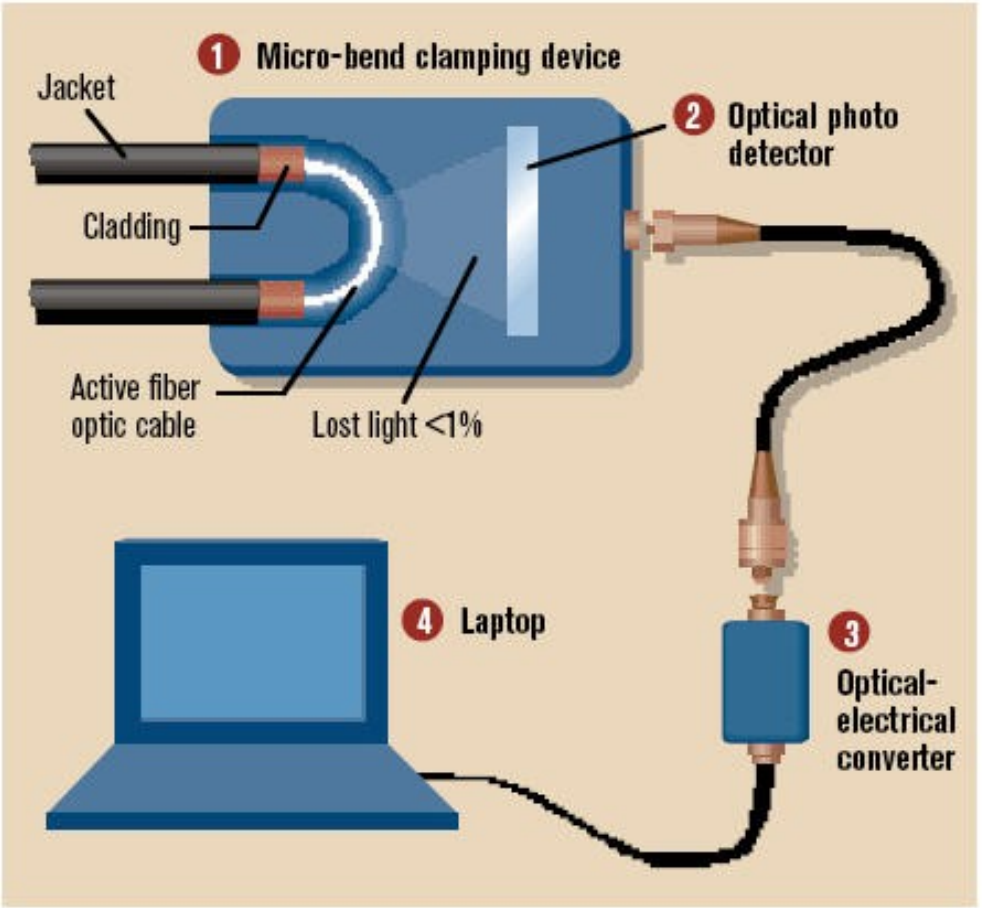
Fibertap

GIGA TAP 1 PORT

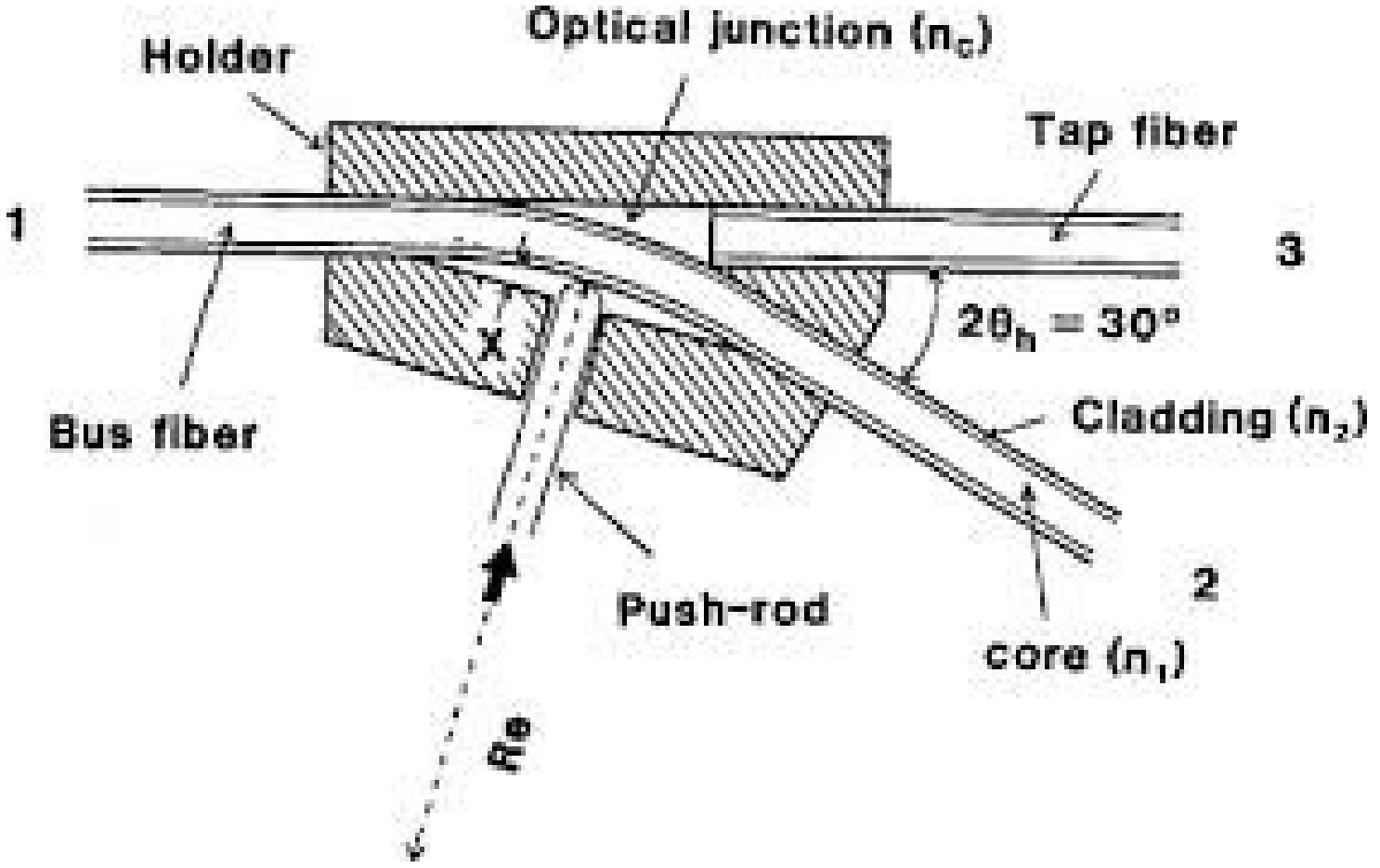
Fibertap


Tapped Fiber Cassette
Device A
TX
RX
RX
TX
Port A
Port B
TX
RX
TX
RX
RX
TX
Device B
TX
TX
RX
RX
Test
Equipment

Fibertap


1 Micro-bend clamping device
Jacket
2 Optical photo detector
Cladding
Active fiber optic cable
Lost light <1%
4 Laptop
3 Optical-electrical converter

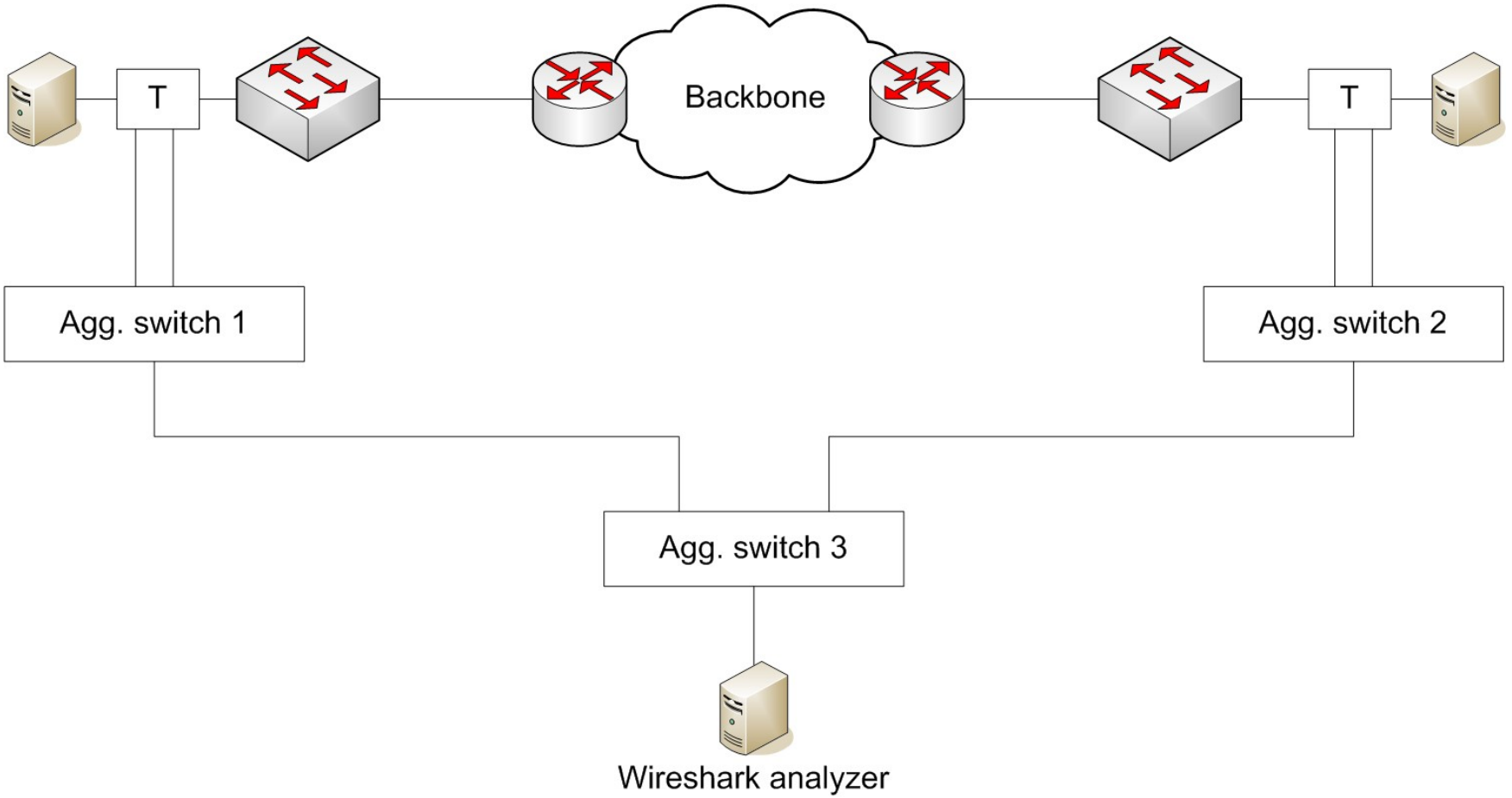
Fibertap


Optical junction (n_c)
Holder
Tap fiber
1
3
$2\theta_h = 30°$
Bus fiber
Cladding (n_2)
Push-rod
2
core (n_1)
Re

Aggregerings switche

- Den billige løsning
- VSS.com udstyr
- Gigamon udstyr

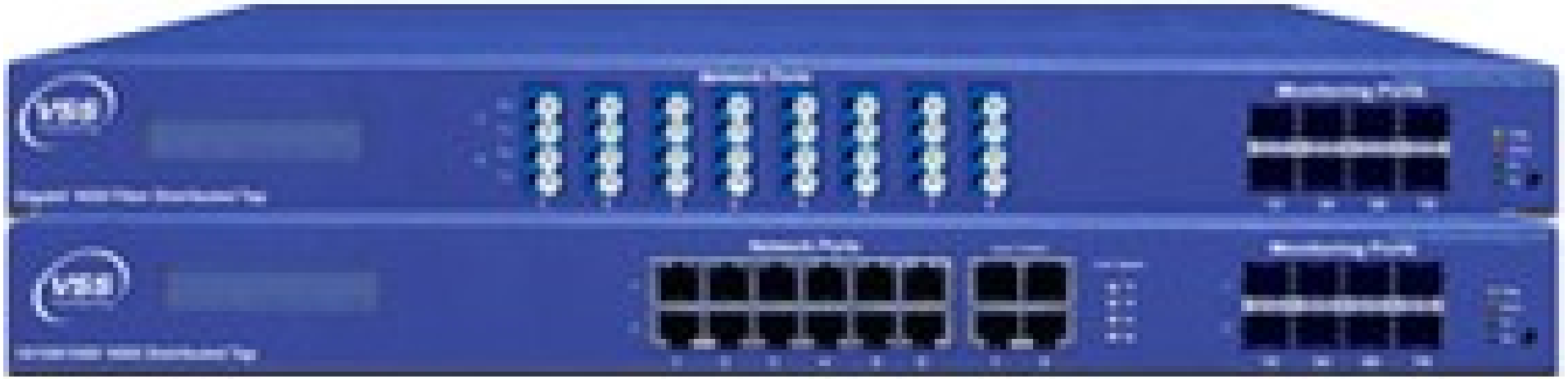
Aggregerings switche (DIY)

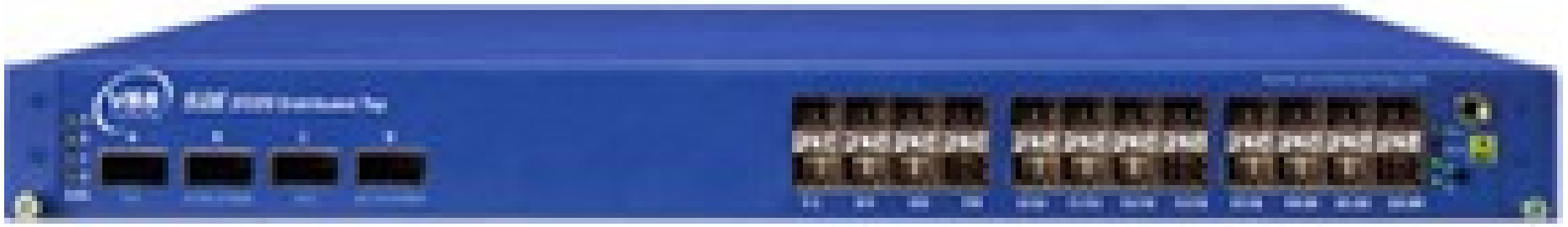


- Standard switche KAN anvendes med lidt snilde.
- Slå alt switching og vlan fra, brug monitor port config fra ind til ud.
- Ignorer fejl logs især duplicate mac addr eller tilsvarende.

VSSmonitoring.com udstyr

- Tap og tap+aggregering i mange varianter.





Gigamon aggregeringsudstyr

Gigamon G-serie

- Web eller CLI interface.
- Simpelt signalaggregering
- Fiber (SFP) eller kobber (RJ45)
- 20 x 1G , 4 x 10G porte
- Porte kan konfigureres til monitor (ind) eller tool (ud)
- Filtre på div features ip, port, mv. Imellem ind- og udgang.

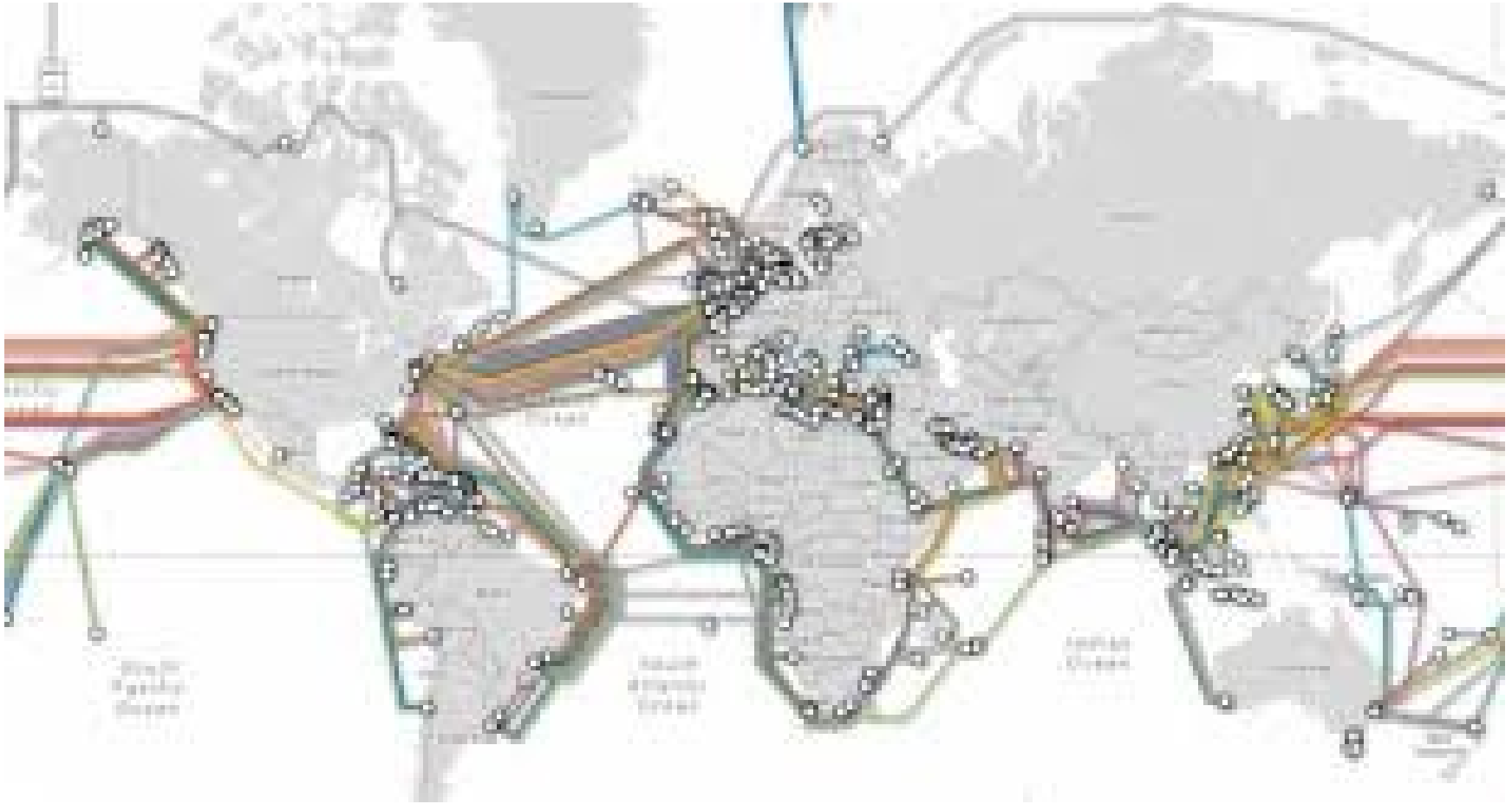
Gigamon aggregeringsudstyr

- Gigamon HD (blade system)
- Web eller CLI interface.
- Timestamping (ekstra ntp timestamp i pakken)
- SSL dekrypteing (kræver certifikat)
- Tunnelling (over IP net)
- Source port labeling.
- Dedublikering
- osv

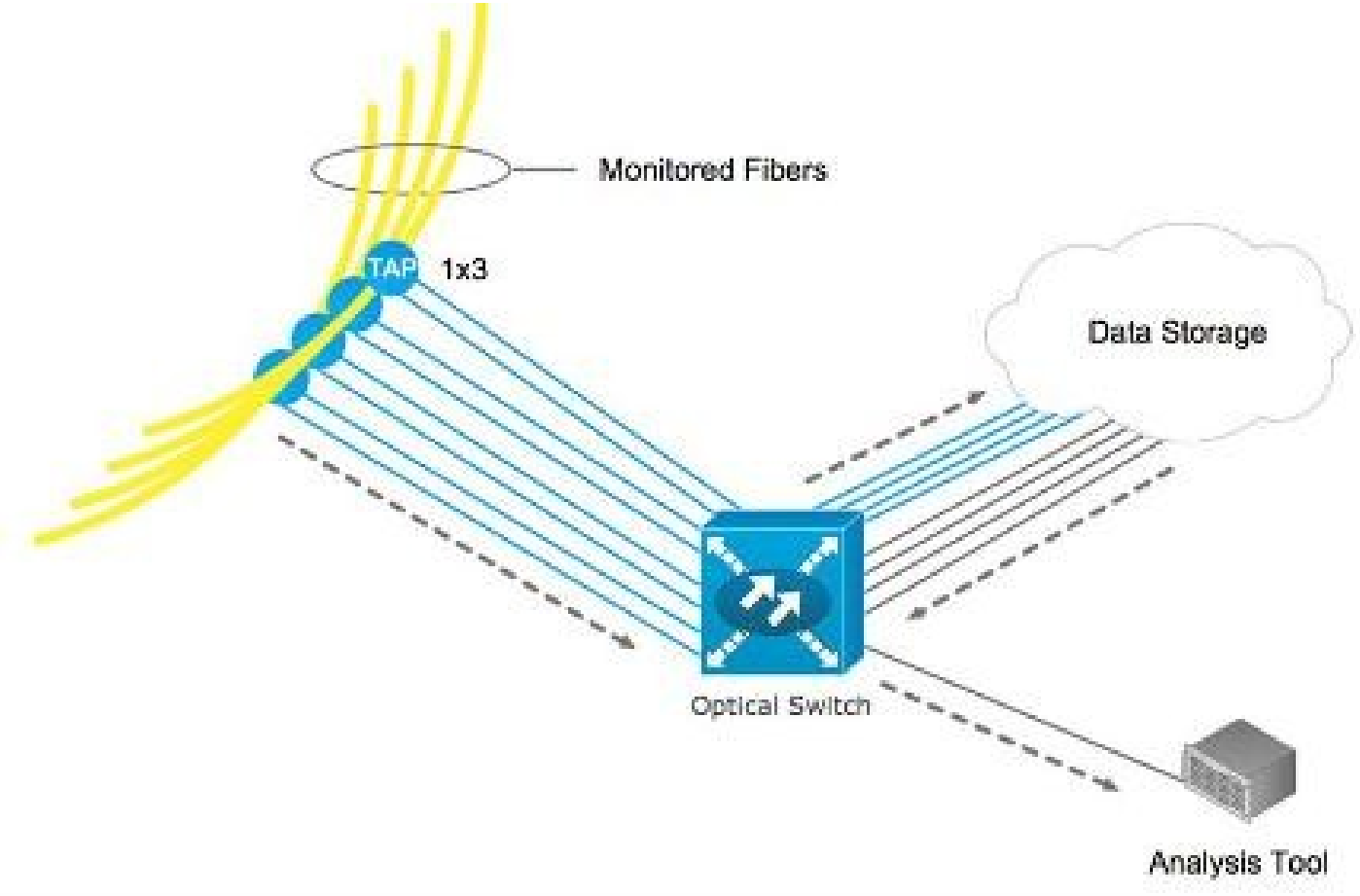
Signalopsamling udfordringer

- Multi colur optical taps.
  - Hver fiber indeholder flere bølgelængder (farver)
  - Hver farve har fuld fiberkapacitet.
- GB/TB traffic analyse. Trafikken bliver voldsom.
- Opsamling på systemer over stor geografi.
  - Lokalt, nationalt, world.

Større setups



Større setups



Spøgsmål.

Og tak for jeres opmærksomheden.