DT172G - Nätverksanalys

Lennart Franked

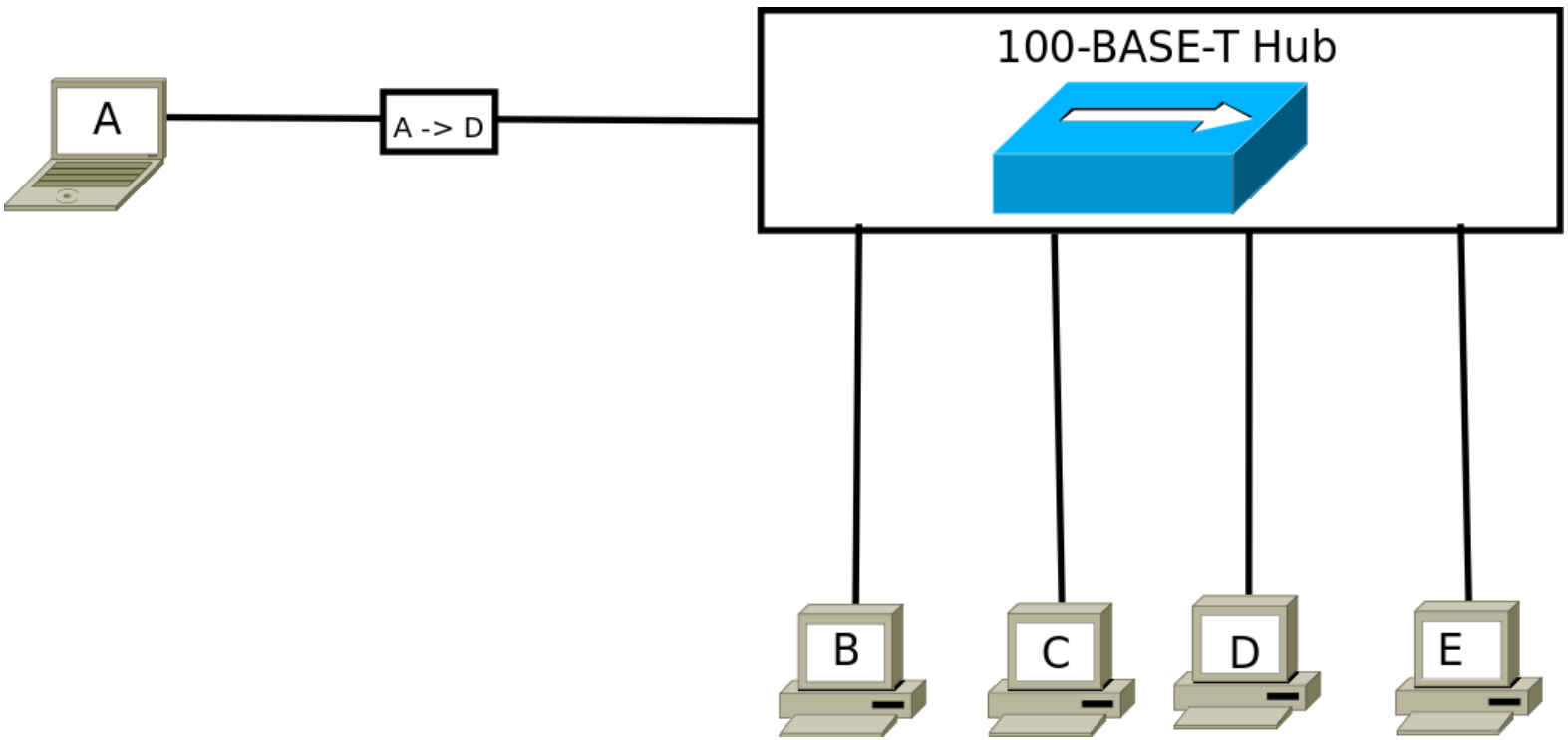
Avdelningen för informationssystem och -teknologi (IST)
Mittuniversitetet

19 september 2017

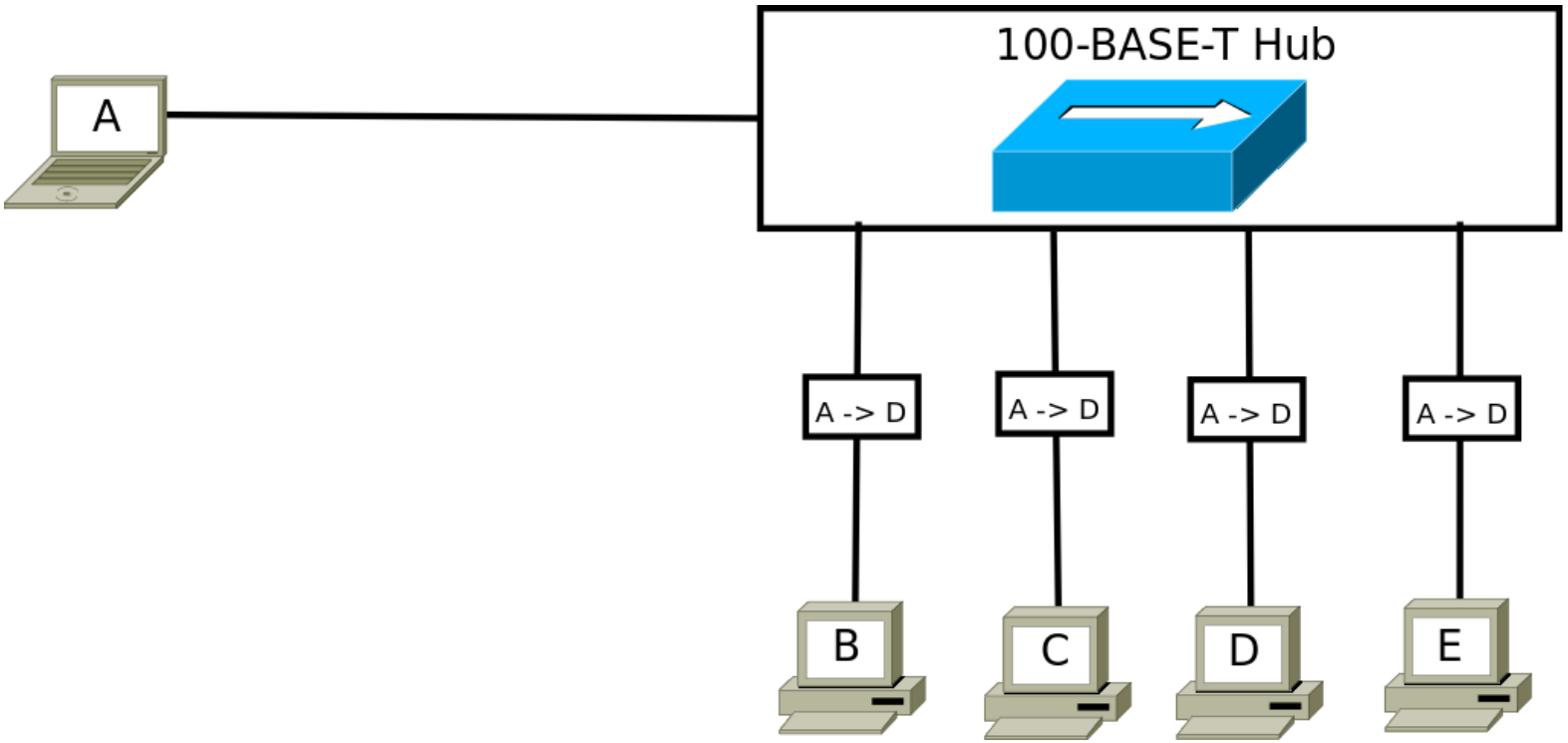
Läsanvisningar

Inför *föreläsning tre* bör ni ha läst [4, kap 2] för att fördjupa era kunskaper kring hur den hårdvara som finns i ett nätverk fungerar. Samt bör ni ha läst [1], [2]. Praktiska exempel på hur Port Mirroring konfigureras kan ni hitta på [3].

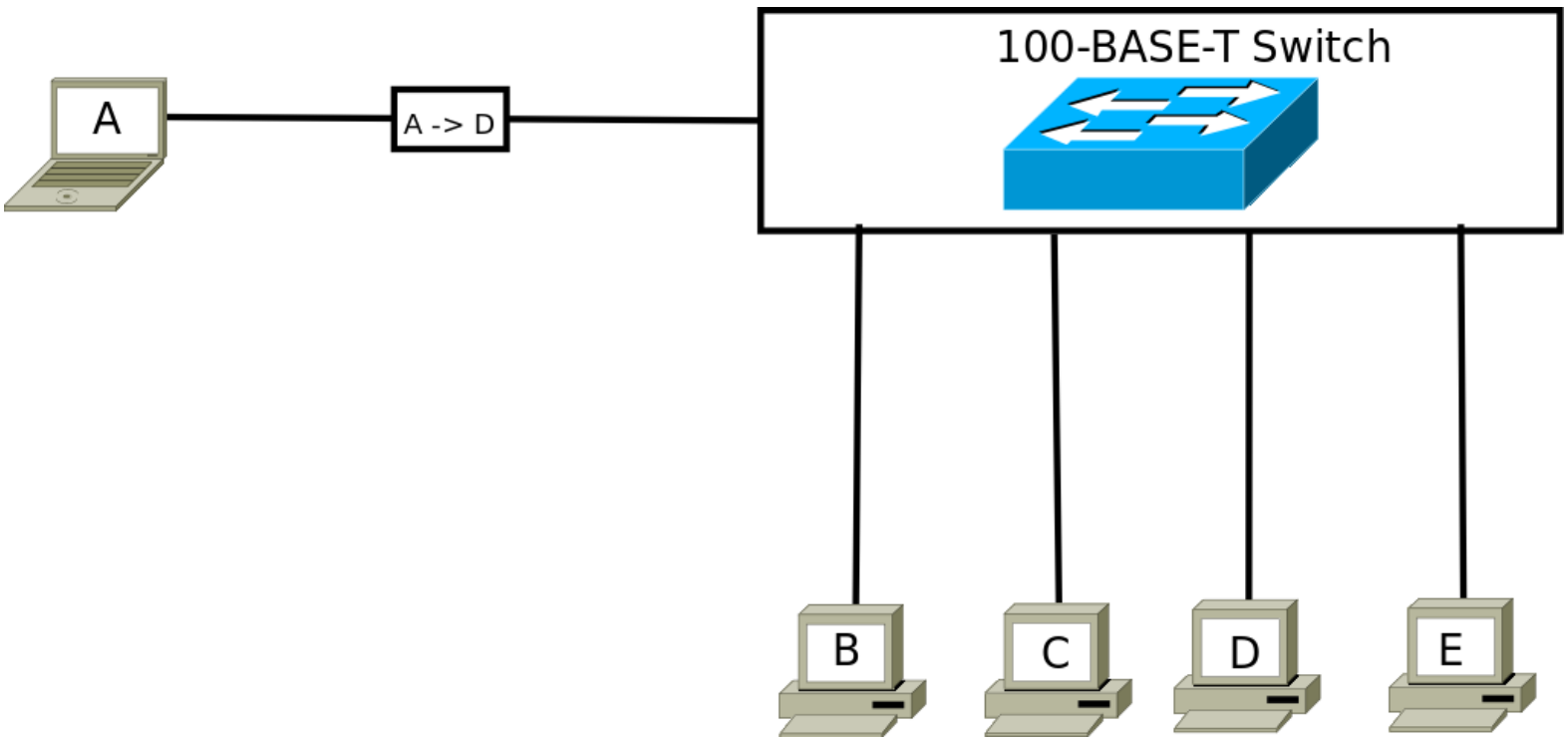
Innehåll



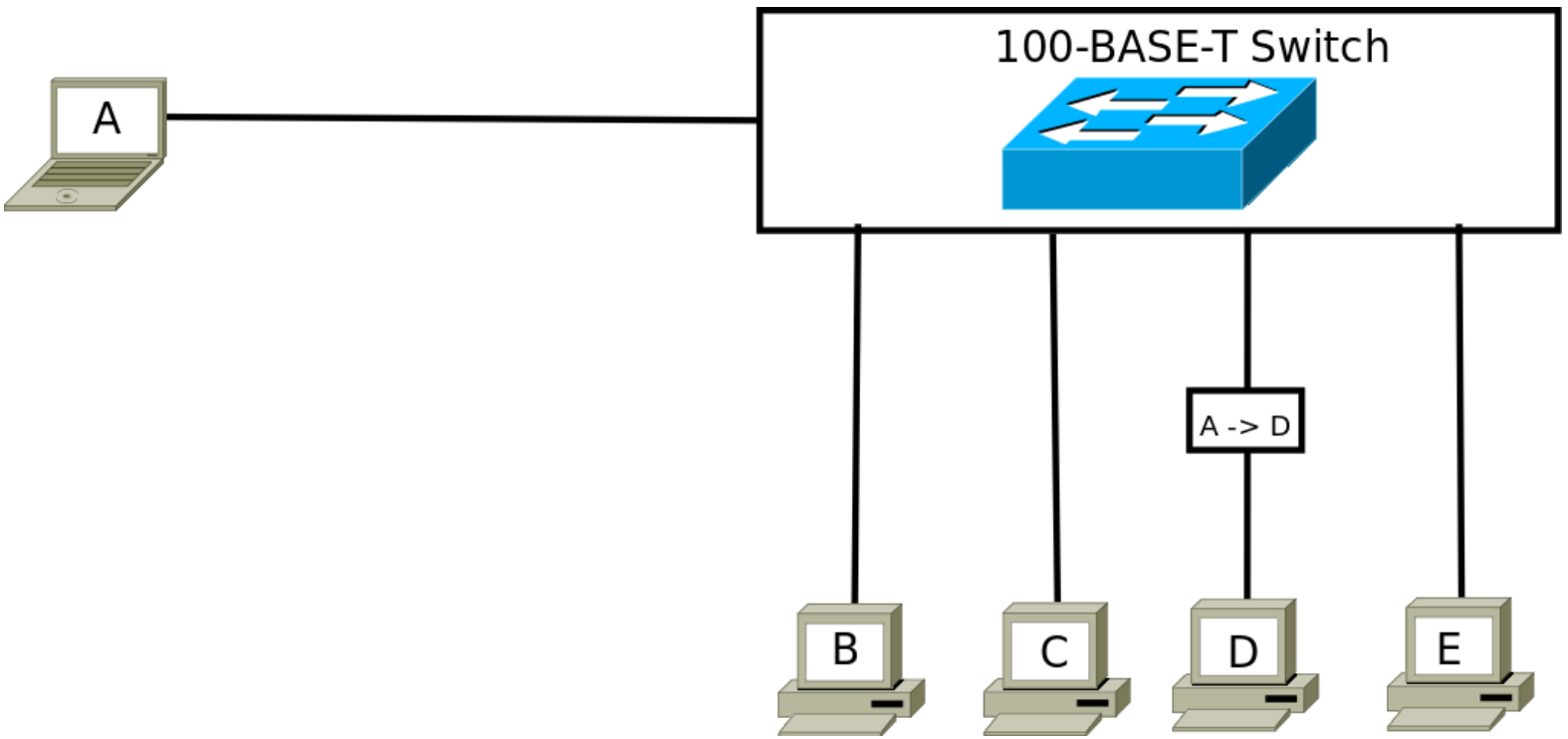
Figur: HUB



Figur: HUB



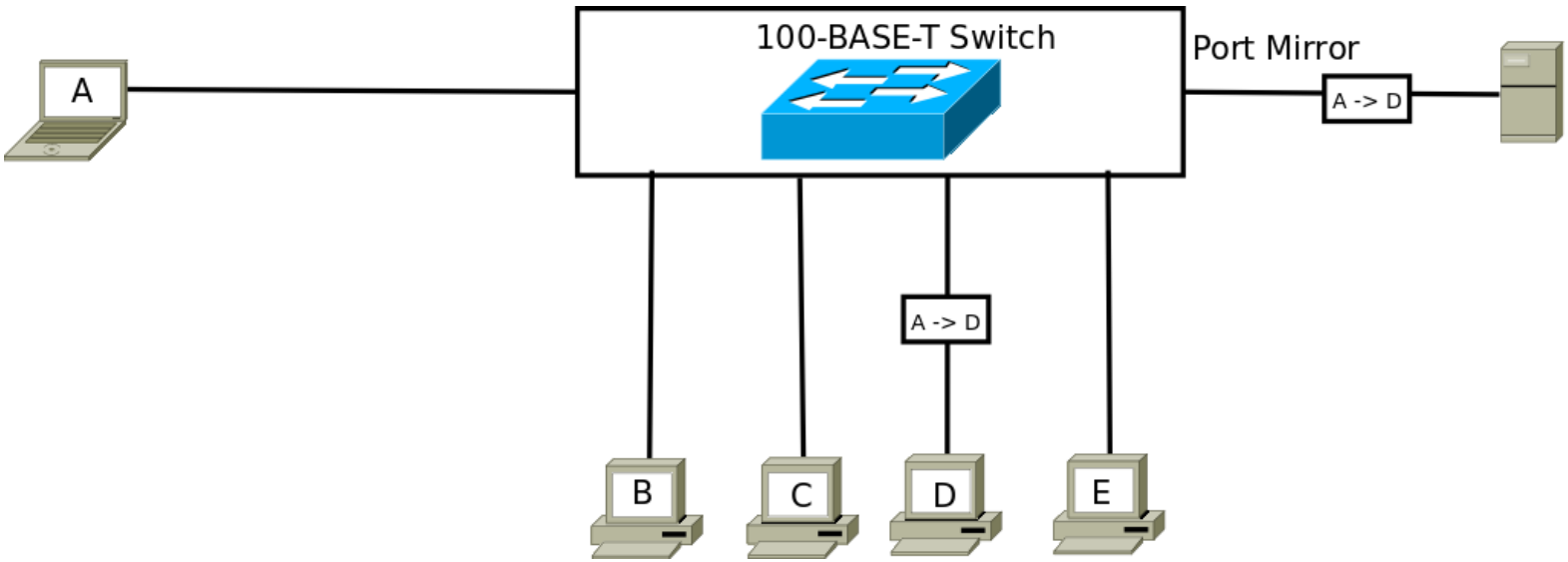
Figur: Switch



Figur: Switch

Spegelport

- Skickar en kopia av paketen ut på en dedikerad port.
- Enbart vissa portar
- Brukar gå att bestämma typ av paket som skall speglas (Rx, Tx, RxTx)
- Vissa implementationer går även att välja portar på andra switchar.
- Även möjlighet att filtrera på VLAN.
- Exempel: Cisco Switched Port ANalyzer (SPAN)



Figur: Port Mirroring

PCAP

Bibliotek används för att samla in datatrafik på ett nätverkskort

- Libpcap
- Winpcap

- Wireshark
- Tshark
- TCPDump
- Genererar utdatafiler i .pcap(2) format

- TShark
  - Textbaserad version av Wireshark
- TCPDump
  - Klassiker som varit med sedan 1987
  - Fungerar likt Tshark

Lämpar sig väl då man vill samla in stora mängder data för senare analys.

- Bra verktyg för att få en god överblick över nätverksanvändningen på en dator.
- Kan generera grafer, följa sessioner, plocka fram statistik...

Lämpar sig väl för analys av kortare sessioner eller efteranalys av en större insamling.

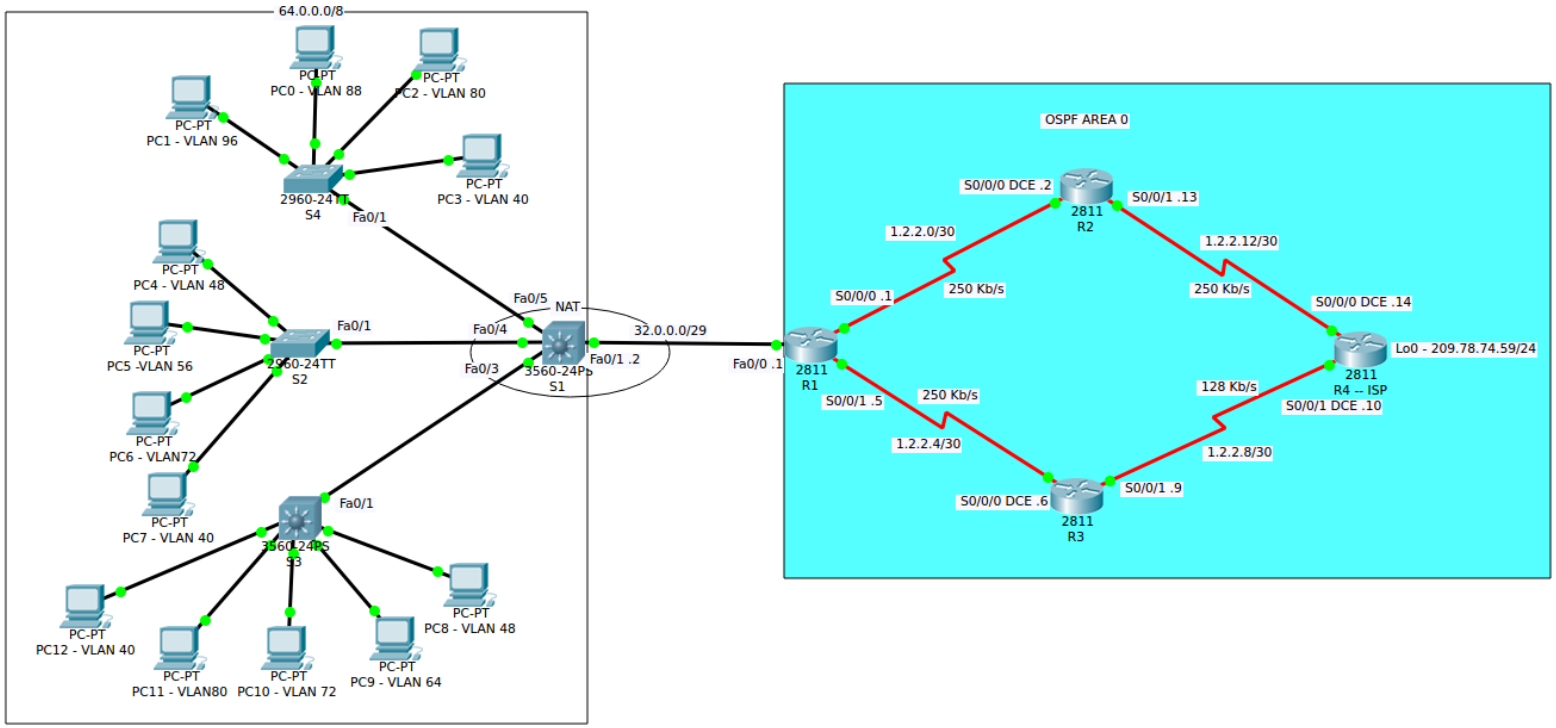
Laborationer

Vi kommer i laborationerna i denna kurs att arbeta med både de textbaserade datainsamlingsverktygen och Wireshark.

Vart bör man samla in data

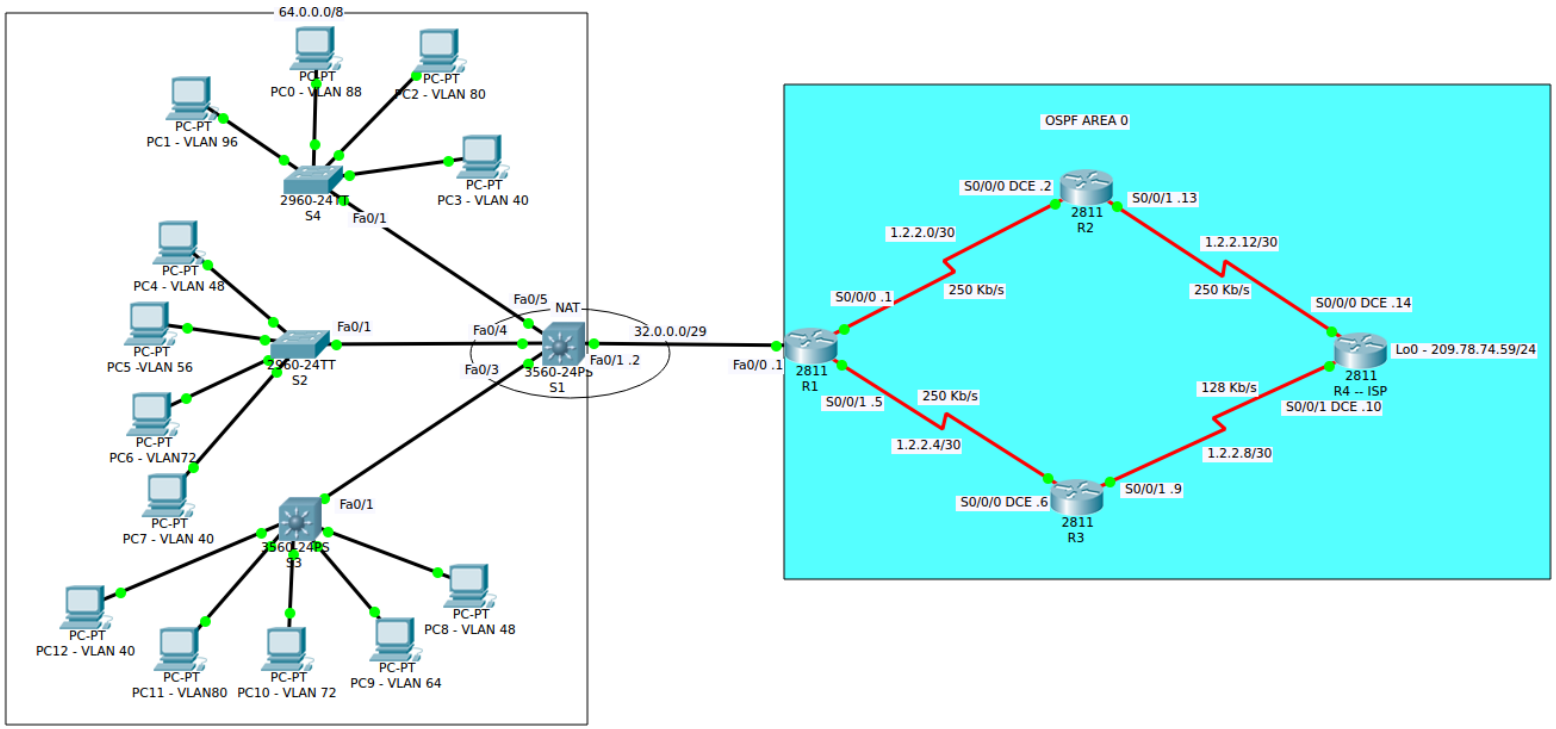
Beroende på syfte med insamling måste vi bestämma vart i nätverket vi vill fånga in trafiken.

- Så nära den enhet/punkt i nätverket vi kan komma



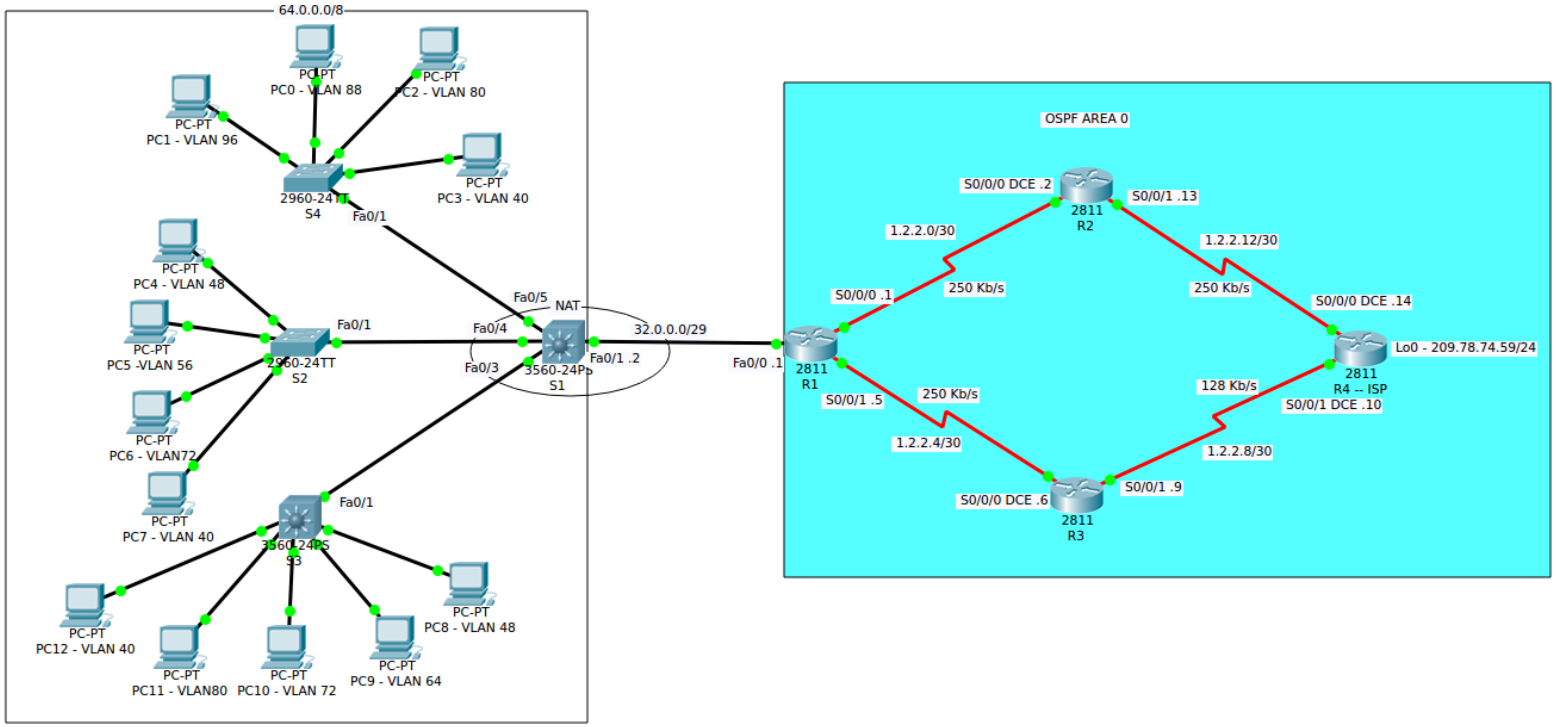
Figur: Insamlingsagent

- Optimalt vid en 'flaskhals' eller vid en samlingspunkt



Figur: Placera insamlingsagent

- Beroende på enhet och typ av information.
  - Före och efter en enhet
  - Mottagare och avsändare
  - Enbart mottagare eller avsändare



Figur: Placera insamlingsagent

Referenser

- "Network Tap". Wiki. 2013. URL: http://en.wikipedia.org/wiki/Network_tap.
- Tim O'Neill. "SPAN Port or TAP? CSO Beware". 2007. URL: http://www.lovemytool.com/blog/2007/08/span-ports-or-t.html.
- *Port Monitoring*. Accessed: 2015-09-15. URL: http://www.cisco.com/c/en/us/tech/lan-switching/port-monitoring/index.html.
- Mani. Subramanian, Timothy A. Gonsalves och N. Usha Rani. *Network management : principles and practice*. Noida, India: Dorling Kindersley, 2011. ISBN: 978-81-317-3404-9.