

**Notat**

01.11.04

/ibl

---

<b>Vedrørende:</b>	Pakkestørrelser på sundhedsdatanettet
<b>Fordeling:</b>	MedCom
<b>Skrevet af:</b>	Martin Bech og Ib Lucht
<b>Version nr.:</b>	1.0

---

**Generelt om pakkestørrelser på sundhedsdatanettet**

Baseret på nogle få tilfælde hvor transmissionsproblemer i forbindelse med sundhedsdatanettet har kunnet afhjælpes ved at ændre på pakkestørrelsen på IP-trafikken, har man vedtaget at gøre det til en generel anbefaling at benytte en maksimal pakkestørrelse (MTU) som er mindre end standard.

**Baggrund**

Netværkstrafik, baseret på IP-protokollen, består af pakker, der hver især kan have en størrelse op til et maksimum, kaldet MTU (Maximum Transmission Unit size). For almindelige ethernet er MTU standardmæssigt 1500 bytes. Sender man alligevel en større pakke, vil det berørte netværksudstyr normalt sørge for at det bliver delt op i mindre pakker. Dette kaldes fragmentering, og forhandles på plads af netværksudstyret ved at sende nogle bestemte ICMP-pakker.

Med VPN-forbindelser, som dem Sundhedsdatanettet består af, vil der pga. VPN-protokollerne blive hæftet nogle bytes ekstra information på hver pakke, og en pakke, der i forvejen har maksimal størrelse vil kræve fragmentering. Det er ikke noget særligt for sundhedsdatanettet, men gælder for alle lignende systemer, hvor man bruger VPN-tunneler. Der er imidlertid det generelle problem, at de ICMP-pakker, som dette afstedkommer, (igen pga. VPN-konfigurationen) aldrig kommer frem til den maskine, der har genereret pakkerne, og IP-fragmentering kan derfor ikke forventes at virke.

Dette gælder også selvom den pågældende type ICMP-pakker faktisk bliver sluppet gennem sundhedsdatanettets centrale knudepunkt, og det hjælper heller ikke på dette problem at åbne i ens egen kantrouter eller firewall.

**Anbefalingen**

For at være sikker på ikke at opleve dette problem, bør man sætte MTU på både servere og klientmaskiner til 1400 bytes eller derunder.

Har man brug for vejledning i, hvordan dette gøres på noget konkret udstyr, er man velkommen til at kontakte UNI•C for vejledning.