



TU-STIFTELSEN
NETNOD
STUPI
FMV
SUNET
FROBBIT

Nätverket för svensk Internet- Infrastruktur

NSII – Nätverket för Svensk Internet-Infrastruktur



- Medlemmar:
 - FMV, Frobbit, Netnod, STUPI, SUNET och TU-Stiftelsen
- Vi har några av världens ledande experter inom områdena DNS, tid, routing och systemarkitektur knutna till oss.
- Vi kommer också att försöka samla den övriga svenska kompetensen inom detta område.
- Genom olika projekt hoppas vi att kunna knyta till oss nästa generations Svenska infrastrukturutvecklare.

Kort om medlemmarna

- **FMV**
- **Netnod**
 - Ansvarig för drift av kritisk Internetinfrastruktur i Sverige samt gemensamma tjänster
 - Internetknutpunkter, .SE, i.root-servers.net, distribution av svensk tidsskala
- **TU-Stiftelsen**
 - Ägare till Netnod
 - Tänk som legal hemvist för NSII (om det behövs)
- **SUNET**
 - Det svenska universitetsnätet
- **STUPI**
 - Peter Lötberg, internationellt erkänd ledade utvecklare av Internetteknologier
- **Frobbit**
 - Patrik Fältström, internationellt erkänd expert på applikationer, DNS och IP-Telefoni

NSII – Svenskt Kompetenscentrum för Internetteknologi

- **NSIIs kompetenscentrum är ett samarbete mellan forskning, myndigheter och industri.**
- **Syftet är att säkerställa fortsatt kompetens i Sverige kring drift, design och utveckling av IP-baserade nät och Internetteknologi.**
- **Centrumet strävar efter att Sverige även i fortsättningen skall ha världsledande kompetens inom Internetområdet, oberoende av omvärlden.**
- **Centrumet skall även bedriva forskning kring säkerställande av IT-infrastruktur, samt Sveriges oberoende vid krissituationer.**

Behovet av att utveckla Sverige

- **Sverige har tidigare under många år varit högt rankat för utvecklingen av Internet teknologi**
 - Har varit av strategisk nytta för samhälle och industri
 - Finns idag ingen eller mycket dålig återväxt av kompetens
- **Sverige saknar en nationell struktur för bevarandet och utvecklandet av kritisk kompetens**
 - Kan på sikt utgöra ett hot mot infrastruktur stabilitet och industrins utveckling
- **NSII är ett initiativ för att industri, myndigheter och forskning skall försöka fylla tomrummet efter en nationell plan**

NSII – Testbädd

- NSIIs ursprungliga medlemmar driver sedan år 2000 en testbädd i Stockholm.
- Vid testbädden bedrivs idag ett antal projekt, bl.a. vad gäller redundans, och driftstabilitet för kritiska resurser så som myndigheter och gemensamma tjänster på Internet.
- Testbädden bedrivs idag på tre diversifierade strukturer; 622 Mbit/sek, 2,4 Mbit/sek och 10 Gbit/sek, och används idag som ett av de första näten i Sverige för transport av produktionstrafik med IPv6, nästa generations Internetprotokoll.
- Testbädden distribuerade redan 2001, som ett av de första i världen, TV via IP multicast.
- Testbädden används idag för modellering av multipla anslutningar för kritiska tjänster, samt för tester kring DNS, routing, trafikstudier, prestandamätning samt för distribution av tid via Internet.

NSII Utveckling

- **Fortsätta att snabbt knyta fler partners till nätverket**
- **Utveckla de tankar som finns som projekt och realisera resultat**
 - Hitta finansiering
 - Engagera nästa generations utvecklare i genomförandet

NSII Resurser

- **Initiativtagarna till NSII har idag en god uppfattning om ett antal områden där det krävs utveckling i Sverige**
- **NSII skall främst ses som ett nätverk för kompetens**
- **NSII vill hjälpa till hitta finansiering för de projekt som initieras**
- **NSII fungerar som rådgivare till de projekt som startas**
- **NSII är tänkt att kunna fungera som rådgivare samt tankesmedja för problemställningar som medlemmar kan tänkas ha**

NSII - Robust infrastruktur för myndigheter

- **Kommunikation mellan myndigheter sker idag i allt större utsträckning via IP baserade tjänster**
- **Tidigare samlade bedömningar saknas för nya kommunikationssätt**
 - Beroende på tredje part
 - Komplexa beroenden (IP-Telefoni tex)
- **Tekniker för att garantera tillgänglighet och säkra robusta kommunikationer i tider av kris är komplexa**
 - Med visionen om 24h-myndighet gäller detta även i "normala" driftssituationer
- **Projektförslag inlämnat till Vinnova för fråga om finansiering**
 - Intresse finns från Verva samt SOS Alarm
 - Inkluderar pilotimplementation, implementations beskrivning samt revideringsdokument

NSII - Tjänsteknutpunkt

- **Distribution av vissa tjänster mellan operatörer är idag ett problem**
 - Dels ett tekniskt problem vad gäller skalbarhet
 - Dels ett affärsmässigt problem
- **NSII vill utnyttja sin testbädd till att pröva samt utveckla teknologier för standardisering inom innehålls distribution (främst IPTV)**
 - Även samarbete med svenska tillverkare av bredbandsprodukter för utvecklandet av slutkundsutrustning
- **NSII vill utveckla affärsmodellerna tillsammans med de olika aktörerna för att öka tjänsteutbudet till slutkunden**

NSII - sårbarhet i gränsrouting systemet

- PTS genomför tester på testbädden angående tänkbara sårbarheter i gränsrouting systemet
- Testbädden utgör en bra simulering av det verkliga Internet och stora operatörsnät.

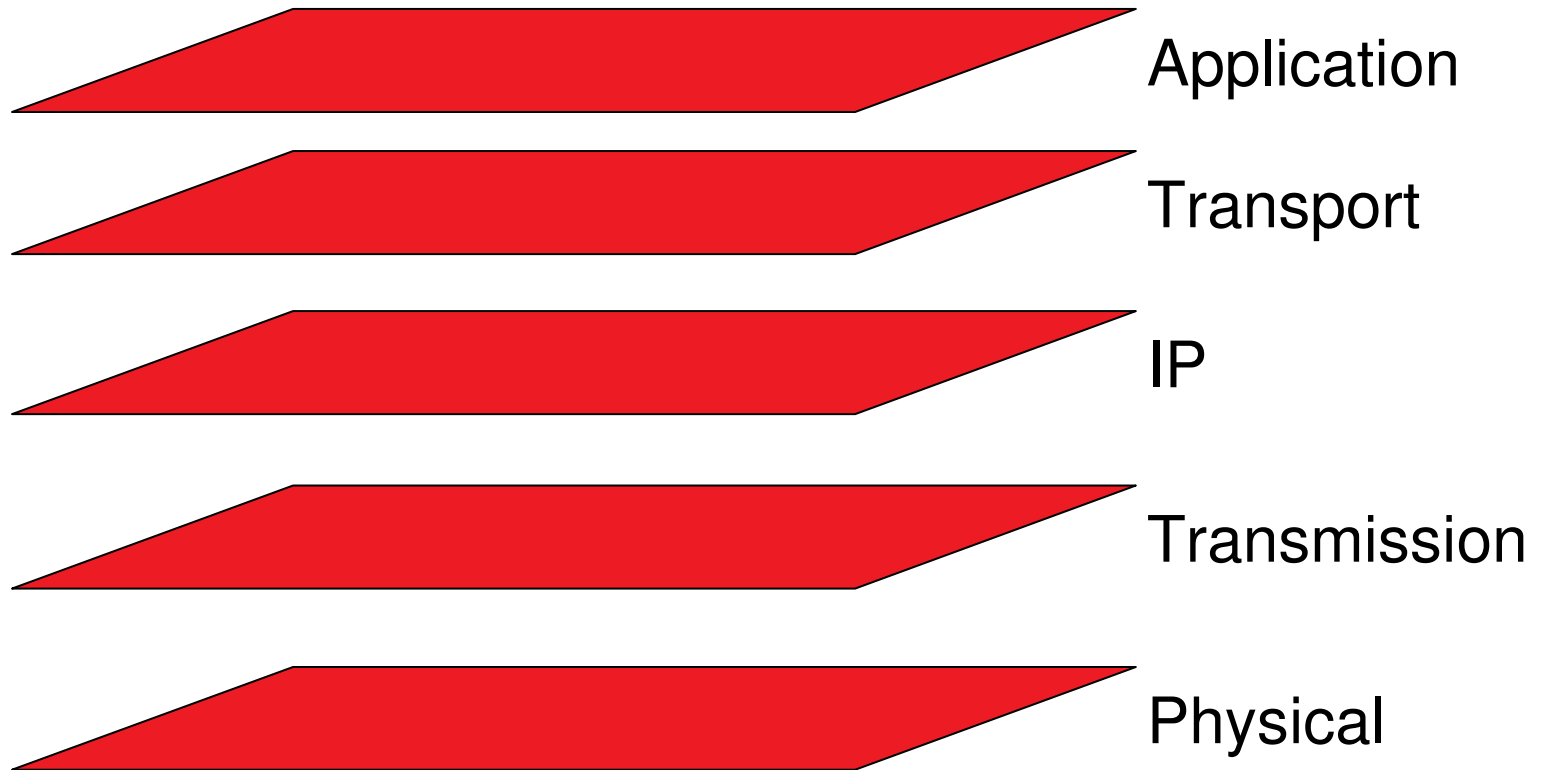
NSII - IPv6

- **NSII och deltagare i NSII deltar också aktivt i utvecklandet av nästa generations Internetprotokoll, IPv6**
 - Bla genom att leda flera arbetsgrupper inom IETF
- **Utveckling av tekniker för robusthet och stabilitet för sessioner och routing i IPv6**
- **Genom tester på testbädden i Stockholm**
- **Utvecklandet av tjänster**
 - NTP över IPv6
- **NSII avser även att utbilda och sprida kunskap om IPv6 i Sverige**

Example: Layers in the protocol stack

- Or...how can one implement robustness...

The layers...



Application

- **An application have to managed the fact that the connection/session might break**
- **A “soft restart” of the session**
- **Like if a users IMAP client is dying, it can “simply” reopen the connection**

TCP / Session layer

- One can have an early termination of the session flow
- Load balance on multiple backend servers
- Make sure backend servers that are down are not in use do not get any requests

IP Layer

- **Routing solve link failures**
- **Anycast solve many problems regarding load balancing globally**

Transmission

- **Failover in for example SDH**
- **Can, when needed, do failover faster than IP**

Physical layer

- **Two transmission paths (two fibers for example) should not run in the same duct**
- **Documentation is needed**
- **Alternate physical layers are needed for failover ability on transmission or IP**

What is the problem?

- **Not everyone understand how to build a robust service**
- **When people think they do, they expect 100% uptime**
 - Instead, one should decide for example “handle 50 hits/s in normal mode, 500/s in reduced mode, then die”
 - After an attack, look at whether the implementation or requirements where wrong
- **Most people implement robustness on only one layer**
- **What happens if one have flap in one layer that is replicated on some other layer?**
 - Oscillations?

With that as a background...

