



# Project Särimner

The elevator pitch.

# Backstory

- Today most parts of the Swedish digital crisis infrastructure is physically placed in Stockholm. Lets use “krisinformation.se" as the example here but its not limited to only that.

- This makes it very vulnerable to attacks against the (in most cases) only source of data.

- Vulnerable to cable-cuts, DDOS-attacks, other attacks aswell as attacks and outages on local infrastructure in Stockholm.

# Backstory - Repetition

- Today most parts of the Swedish digital crisis infrastructure is physically placed in Stockholm. Lets use “krisinformation.se" as the example here but its not limited to only that.

- This makes it very vulnerable to attacks against the (in most cases) only source of data.

- Vulnerable to cable-cuts, DDOS-attacks, other attacks aswell as attacks and outages on local infrastructure in Stockholm

- **Possible solutions are:**
  - **Reinforce infrastructure so that the country never looses connectivity with Stockholm**
  - **Distribute information so that it can be served from more places than one.**

# Project Särimner

- *In Norse mythology,* ***Sæhrímnir*** *is the creature killed and eaten every night by the Æsir and einherjar. The cook of the gods, Andhrímnir, is responsible for the slaughter of Sæhrímnir and its preparation in the cauldron Eldhrímnir.*

- *After Sæhrímnir is eaten, the beast is brought back to life again to provide sustenance for the following day. Sæhrímnir is attested in the Poetic Edda, compiled in the 13th century from earlier traditional material, and the Prose Edda, written in the 13th century by Snorri Sturluson.*

# Project Särimner

- “Totalförsvarsplaneringen” is the overall strategic plan for military response in Sweden,  and its assuming that in the event of war, the enemy will try to segregate the country in one or many pieces. Especially cutting away Stockholm.

- PTS (Post- och Telestyrelsen) is of the general view that the robustness of Swedens communication-systems will see a major improvement if operators is interconnecting at as many places as possible and that critical infrastructure is available at many places and not centralized.

# Project Särimner

- Project Särimner is a Proof-of-Concept project to try to figure out if important services to the civilan population of Sweden can work without having contact or even having Stockholm at all.

- Joint project between Netnod and SUNET, financed by PTS
- Over-aching goal is to develop a method of secure and robust communication between the people and owners of critical services
- Consists of two parts.
  - Secure exchange of information amongst “Swedish” ISPs
  - Delivery of important content under a situation of extreme stress on either the population of Sweden or the infrastructure of Sweden.
- Project will run as a PoC in 2018



# Project Särimner

Techy Slides

# Project  Särimner - Part 1 - Content Delivery.

- System must handle quite a lot of traffic.
  - Range in about  1 request per 1 sek per inhabitant of .SE  => 10 millon request/s
  - Always gives an answer, no host does not respond to ping.
- Nodes will primary be proxy for web and serve DNS.
  - Distributed system to solve load + segregation in one go
  - System is always-on to make sure it actually works.
- System must handle to work autonomously
  - Single-nodes must be working without having any connectivity to mothership for “quite some time”
  - POC is set out to be 16 nodes.

# Content delivery under a time with extreme stress…

- To have a “important service” work a few things must work.
  - Routing / IP
  - DNS
  - HTTPS
  - TLS
- The goal is to build a system that solves all or most of this that sits as close to the end-user as possible to increase performance, decrease attack-surface and improve geographical resiliency.

# Content delivery under a time with extreme stress…

- To have a “important service” work a few things must work.
  - Routing / IP
  - DNS
  - HTTP
  - TLS
- The goal is to build a system that solves all or most of this that sits as close to the end-user as possible to increase performance, decrease attack-surface and improve geographical resiliency.

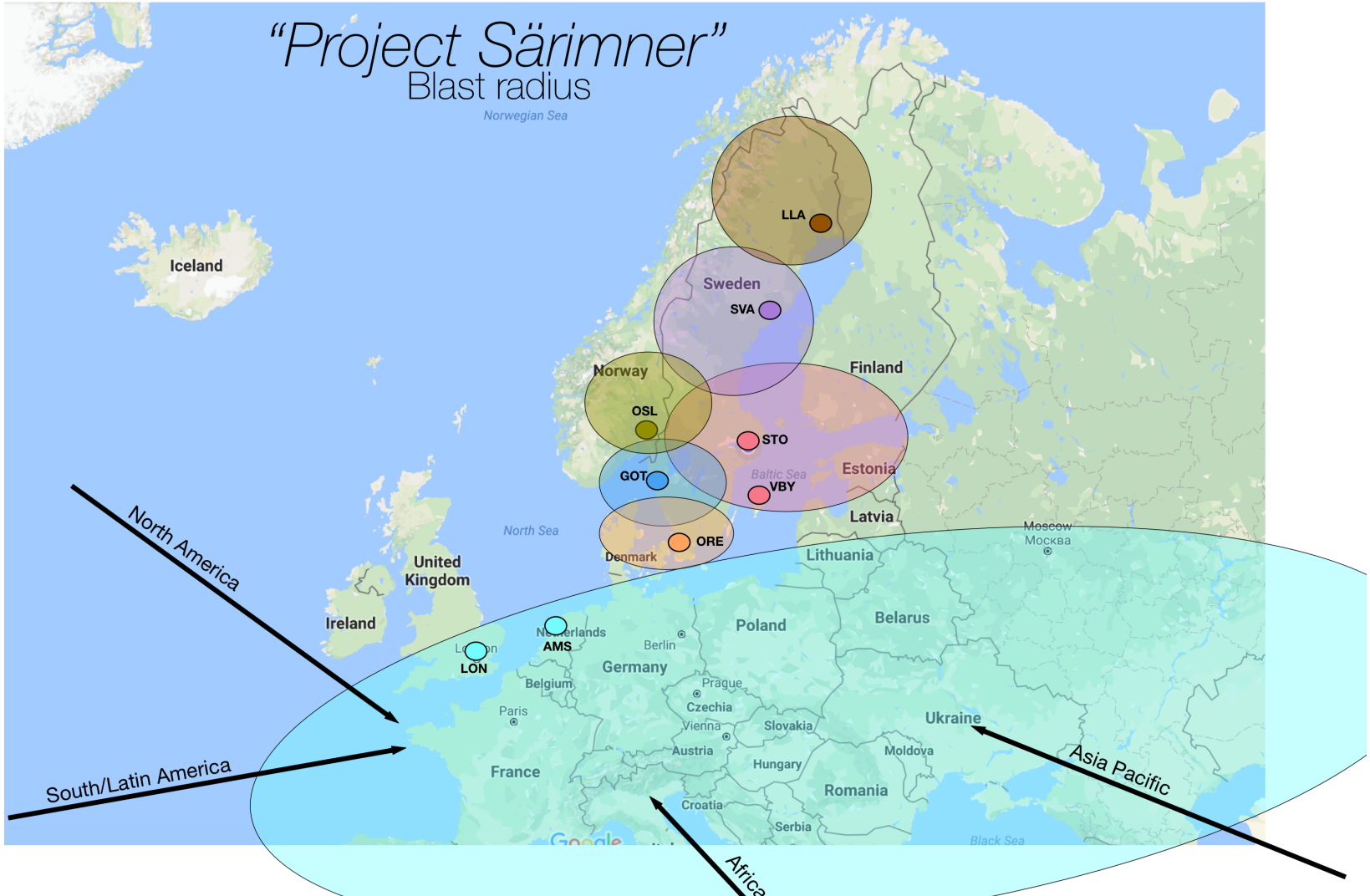
- YES, like any CDN you have ever seen ever.

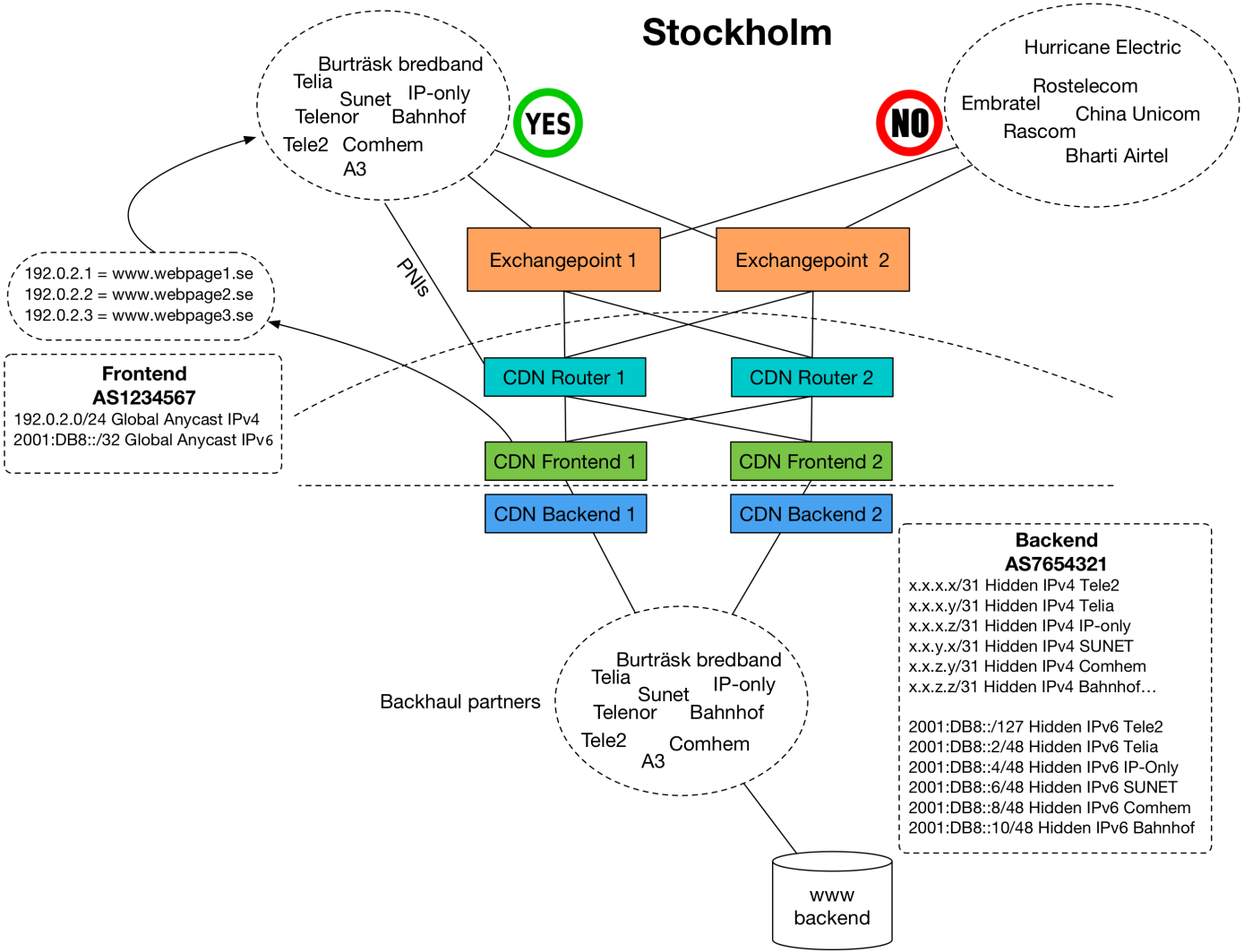
# Content Delivery Nodes

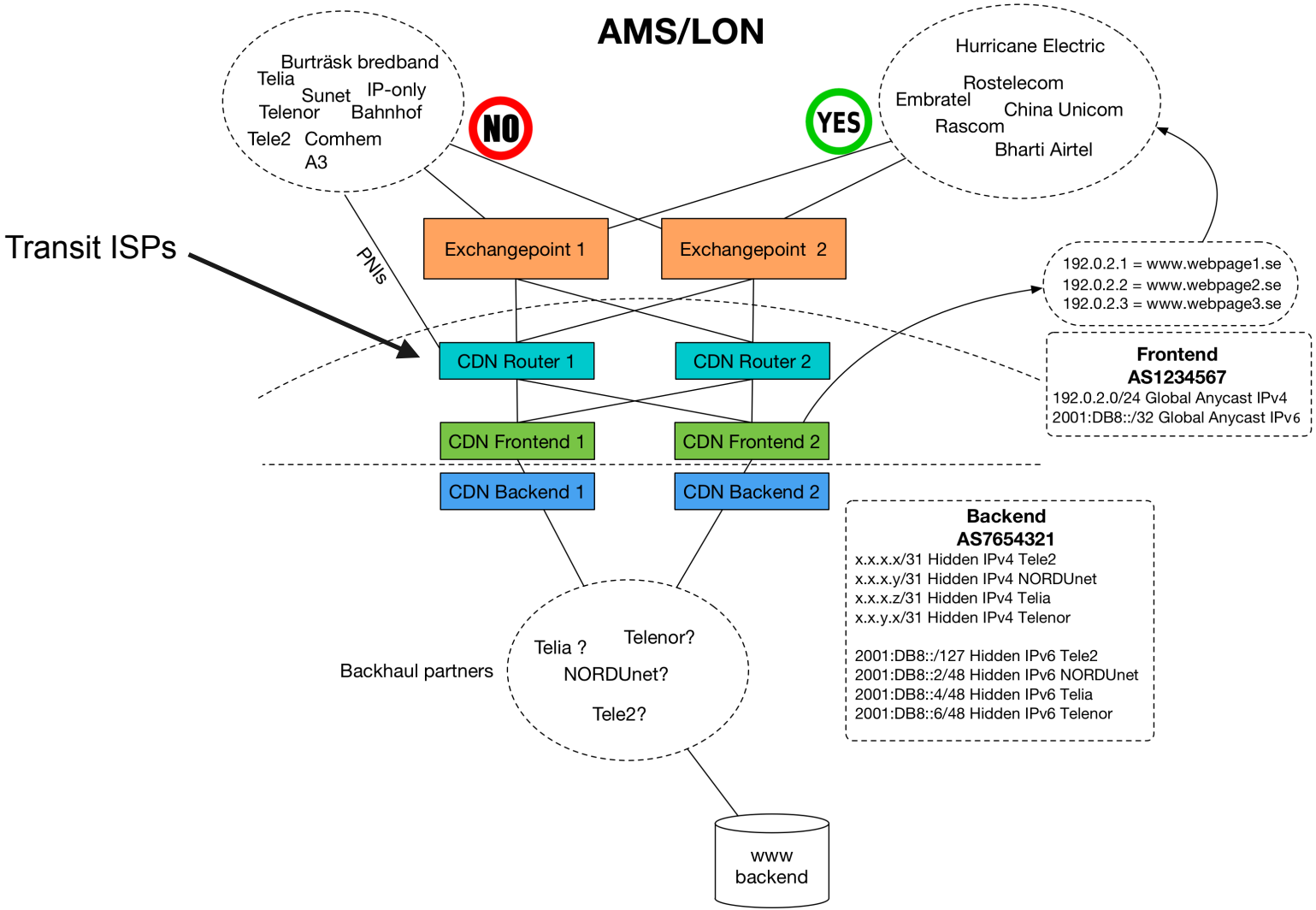
- Stable and hardened. By having this conversation the potential enemy already knows this exists and will try to steal them (physically or logically).
- All nodes should carry all information always.
- In a time of peace and non-stress the nodes should just be caching proxies of the information.
- When not at peace, the nodes will have the possibility to serve cached content for “a while” or fall back to older-versions or sites that has a longer TTL. I.e a more static backup-page.
- Aging, fallback and caching is fully controlled by the content-owner.

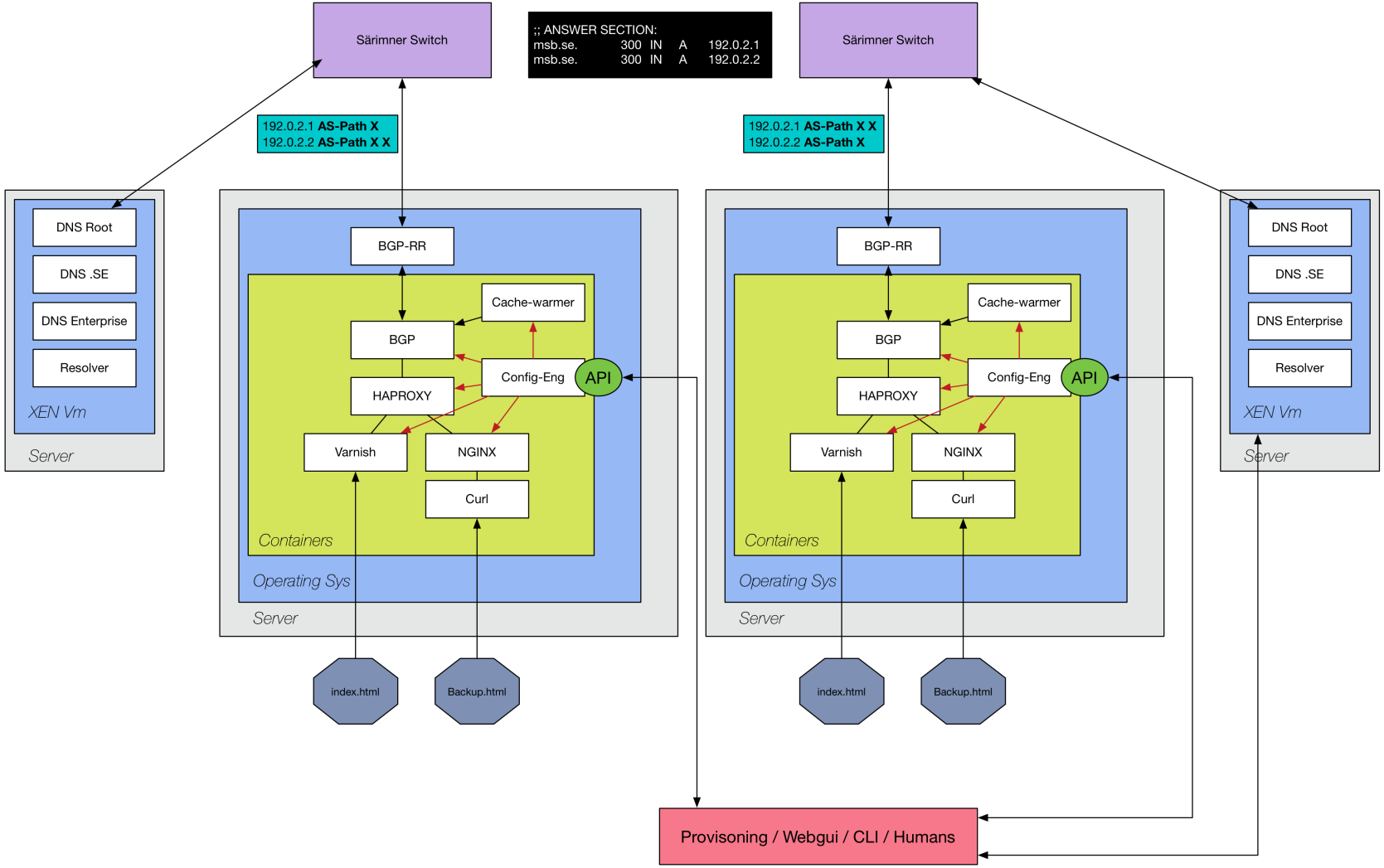
# Nodes

- Is placed at:
  - Netnods IXPs
  - Other IXPs relevant for Sweden, for example STHIX, Norrnod, IXOR, etc
  - As a on-net caching box inside an ISPs network
  - One or other strategic places (islands, isolated areas, etc).
- Exposes DNS and HTTP/HTTPS against the end-user
  - Anycast, all nodes is using the same ASN and the same IP-adresses
  - Authoriative DNS-server for Root, SE, NU etc and more of the DNS-chain
  - Resolver for DNS (perhaps also for external resolvers)
  - Terminates HTTP/HTTPS.
  - Validate and sign that the information given is the actual proper information (no fakenews)
  - Special procedures and protocols to validate the integrity of a node and self-destruct if needed.


"Project Särimner"
Blast radius
Norwegian Sea
LLA
Iceland
Sweden
SVA
Norway
Finland
OSL
STO
GOT
VBY
Baltic Sea
Estonia
Latvia
North Sea
ORE
Denmark
Moscow
Москва
Lithuania
United Kingdom
Ireland
Poland
Belarus
AMS
Berlin
LON
Germany
Belgium
Prague
Czechia
Paris
Vienna
Slovakia
Ukraine
Austria
Hungary
Moldova
France
Romania
Croatia
Serbia
Black Sea
North America
South/Latin America
Asia Pacific
Africa


Stockholm
Burträsk bredband
Telia
Sunet
IP-only
Telenor
Bahnhof
Tele2
Comhem
A3
YES
NO
Hurricane Electric
Rostelecom
Embratel
China Unicom
Rascom
Bharti Airtel
PNIs
Exchangepoint 1
Exchangepoint 2
192.0.2.1 = www.webpage1.se
192.0.2.2 = www.webpage2.se
192.0.2.3 = www.webpage3.se
Frontend
AS1234567
192.0.2.0/24 Global Anycast IPv4
2001:DB8::/32 Global Anycast IPv6
CDN Router 1
CDN Router 2
CDN Frontend 1
CDN Frontend 2
CDN Backend 1
CDN Backend 2
Backend
AS7654321
x.x.x.x/31 Hidden IPv4 Tele2
x.x.x.y/31 Hidden IPv4 Telia
x.x.x.z/31 Hidden IPv4 IP-only
x.x.y.x/31 Hidden IPv4 SUNET
x.x.z.y/31 Hidden IPv4 Comhem
x.x.z.z/31 Hidden IPv4 Bahnhof…
2001:DB8::/127 Hidden IPv6 Tele2
2001:DB8::2/48 Hidden IPv6 Telia
2001:DB8::4/48 Hidden IPv6 IP-Only
2001:DB8::6/48 Hidden IPv6 SUNET
2001:DB8::8/48 Hidden IPv6 Comhem
2001:DB8::10/48 Hidden IPv6 Bahnhof
Backhaul partners
Burträsk bredband
Telia
Sunet
IP-only
Telenor
Bahnhof
Tele2
Comhem
A3
www
backend


AMS/LON
Burträsk bredband
Telia
Sunet
IP-only
Telenor
Bahnhof
Tele2
Comhem
A3
NO
YES
Hurricane Electric
Rostelecom
Embratel
China Unicom
Rascom
Bharti Airtel
Transit ISPs
PNIs
Exchangepoint 1
Exchangepoint 2
192.0.2.1 = www.webpage1.se
192.0.2.2 = www.webpage2.se
192.0.2.3 = www.webpage3.se
CDN Router 1
CDN Router 2
Frontend
AS1234567
192.0.2.0/24 Global Anycast IPv4
2001:DB8::/32 Global Anycast IPv6
CDN Frontend 1
CDN Frontend 2
CDN Backend 1
CDN Backend 2
Backend
AS7654321
x.x.x.x/31 Hidden IPv4 Tele2
x.x.x.y/31 Hidden IPv4 NORDUnet
x.x.x.z/31 Hidden IPv4 Telia
x.x.y.x/31 Hidden IPv4 Telenor
2001:DB8::/127 Hidden IPv6 Tele2
2001:DB8::2/48 Hidden IPv6 NORDUnet
2001:DB8::4/48 Hidden IPv6 Telia
2001:DB8::6/48 Hidden IPv6 Telenor
Backhaul partners
Telia ?
Telenor?
NORDUnet?
Tele2?
www
backend


Särimner Switch
;; ANSWER SECTION:
msb.se. 300 IN A 192.0.2.1
msb.se. 300 IN A 192.0.2.2
Särimner Switch
192.0.2.1 AS-Path X
192.0.2.2 AS-Path X X
192.0.2.1 AS-Path X X
192.0.2.2 AS-Path X
DNS Root
DNS .SE
DNS Enterprise
Resolver
XEN Vm
Server
BGP-RR
Cache-warmer
BGP
Config-Eng
API
HAPROXY
Varnish
NGINX
Curl
Containers
Operating Sys
Server
index.html
Backup.html
BGP-RR
Cache-warmer
BGP
Config-Eng
API
HAPROXY
Varnish
NGINX
Curl
Containers
Operating Sys
Server
index.html
Backup.html
DNS Root
DNS .SE
DNS Enterprise
Resolver
XEN Vm
Server
Provisoning / Webgui / CLI / Humans

# Node platform

- All “nodes” has internal redundancy. A node consists of at least two servers, that always act as “active-active”. Loadbalancing is achieved with RR-DNS and BGP with prepend-tricks.

- Server platform
  - 1RU machines that has all ports on front, 40-50cm deep, 4x10Gbit/s interface, NVMe-storage + hundreds of gigabytes of RAM to save information on RAMDisk as much as possible. HSMs for key-storage.

- Operatingsystem
  - Some flavour of Linux, Secure execution through TPM, everything always encrypted, possibly GRSEC and/or SELINUX and more bells and whistles.

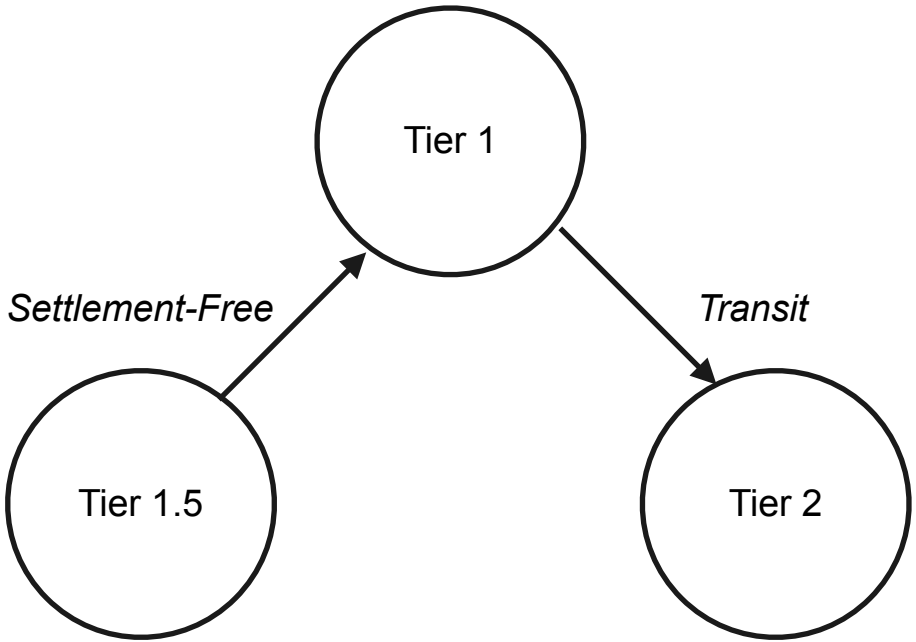
- Applications typically built as containers and/or VMs, Continuous integration and software is typically deployed/upgrade by a full re-provision of the node.

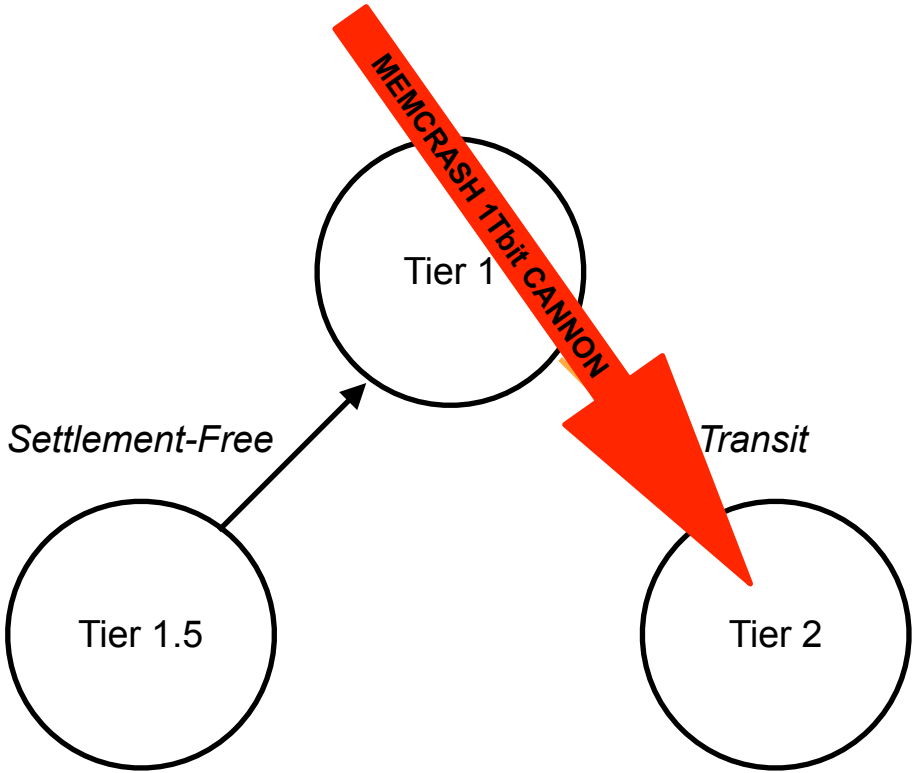
# Timeplan

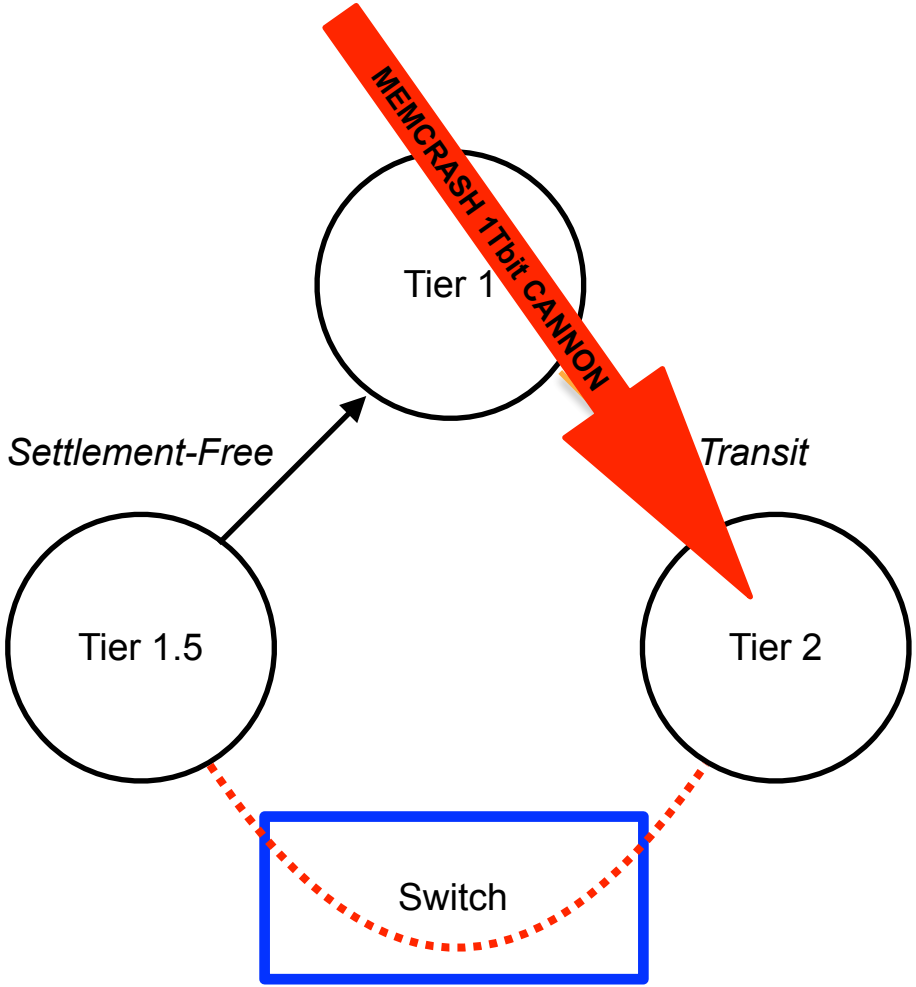
- Stockholm End of Q2 **Bunker(s)** + **Public DC** (Netnod, STHIX, ??)
- Göteborg End of Q3, **Bunker, Public DC?** (Netnod, STHIX)
- Malmö/Öresund End of Q3, **Bunker** (Netnod, STHIX)
- Sundsvall, End of Q4, **Bunker** (Netnod)
- Luleå, End of Q4, **Notviken** (Netnod)
- Visby End of Q4, **“A bunker”**
- Amsterdam, End of Q3, **SARA/Interxion** (AMSIX, NLIX, Asteroid, Transit)
- London, End of Q3, **Equinix HEX67** (LINX, Lonap, Transit)
- Frankfurt, 2019, **Interxion FRA**, (DE-CIX, ECIX, Transit)
- Operator-placed, End of Q4 **You?**
- Other?

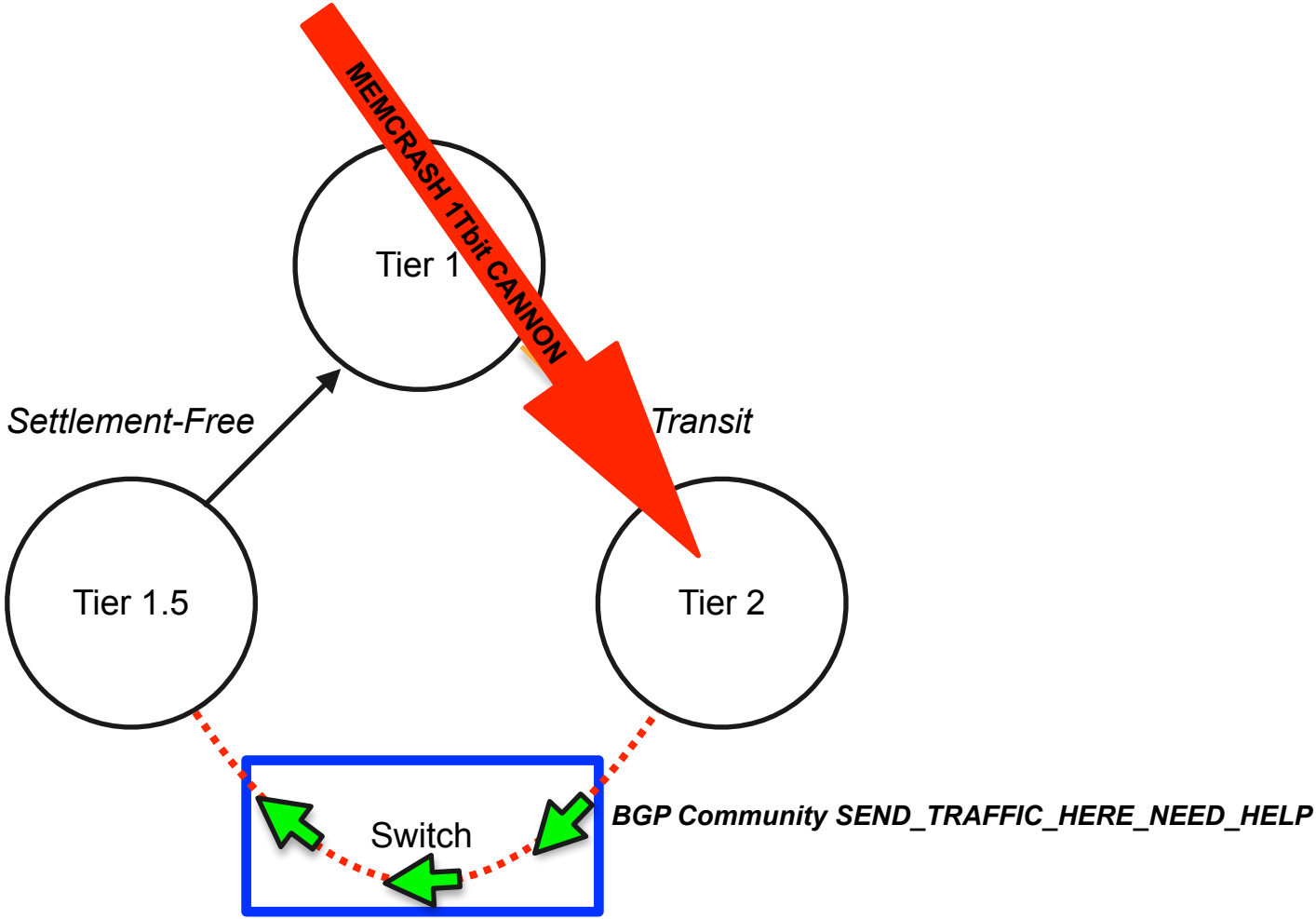
# Project Särimner Part 2 - Interconnection.

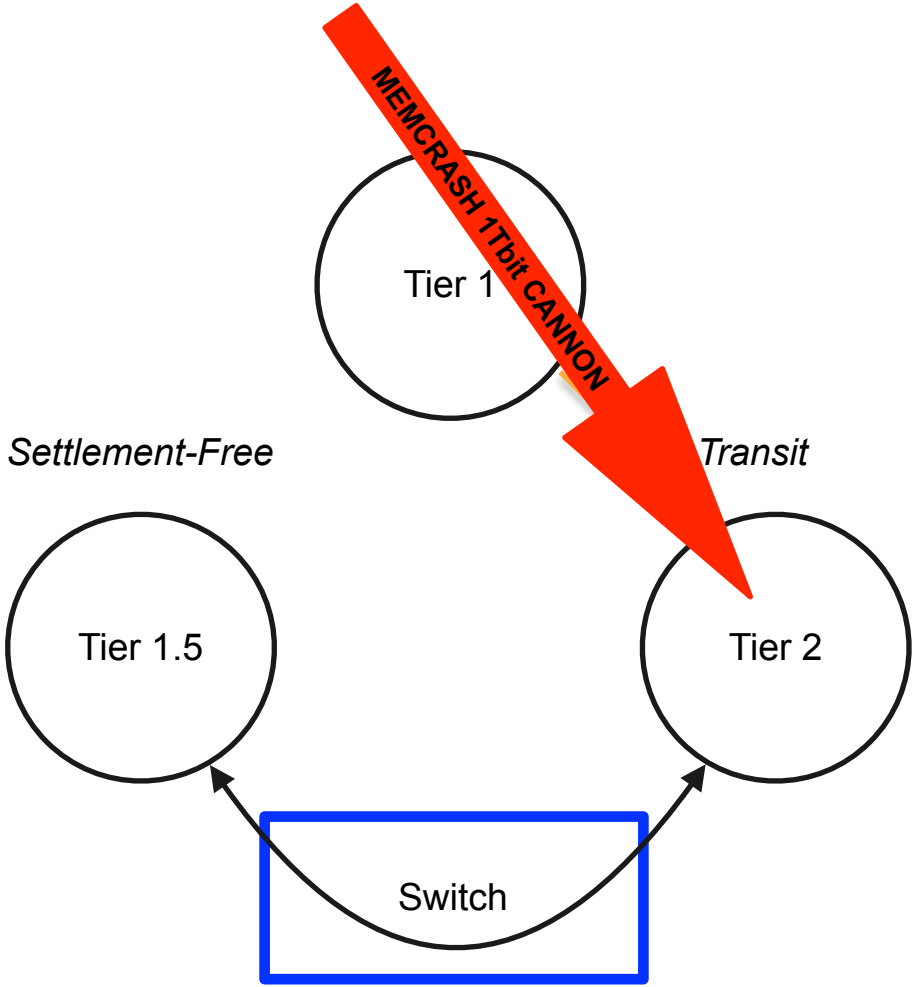
- Traffic-exchange between ISP should work under extreme stress.
  - Separate VLAN/port over current exchanges, dedicated ports between ISPs
  - Could be a copy of fe.nix.cz but adjusted for Sweden
- Could be that Särimner CDN is only available in the “Walled Garden VLAN”.
- Most important thing is trust and method of contact.
- Can’t interfere with day-to-day business and peering-games.
- Can signal “i need help, please send traffic here”, direct or through routeserver.


Tier 1
Settlement-Free
Transit
Tier 1.5
Tier 2


MEMCRASH 1Tbit CANNON
Tier 1
Settlement-Free
Transit
Tier 1.5
Tier 2


MEMCRASH 1Tbit CANNON
Tier 1
Settlement-Free
Transit
Tier 1.5
Tier 2
Switch


MEMCRASH 1Tbit CANNON
Tier 1
Settlement-Free
Transit
Tier 1.5
Tier 2
Switch
BGP Community SEND_TRAFFIC_HERE_NEED_HELP


MEMCRASH 1Tbit CANNON
Tier 1
Settlement-Free
Transit
Tier 1.5
Tier 2
Switch

# Problems…

- Hot potato routing. Can we **actually** do it?
- Can the ISPs actually function without the capital?
  - Backbone
  - Radius/DHCP/DNS
  - BRAS/BNG
- Handle the “keys to the kingdom” (SSL-keys) with state of the art security.
  - Can we force market into short-lived certs? (letsencrypt style…)
- Verify integrity of a node
- Secure boot
- Secure backhauling to Origin.
- Loadbalancing and TE.
- Continue business and operation after PoC is done.



# Techy Questions?

hugge@sunet.se
matte@netnod.se