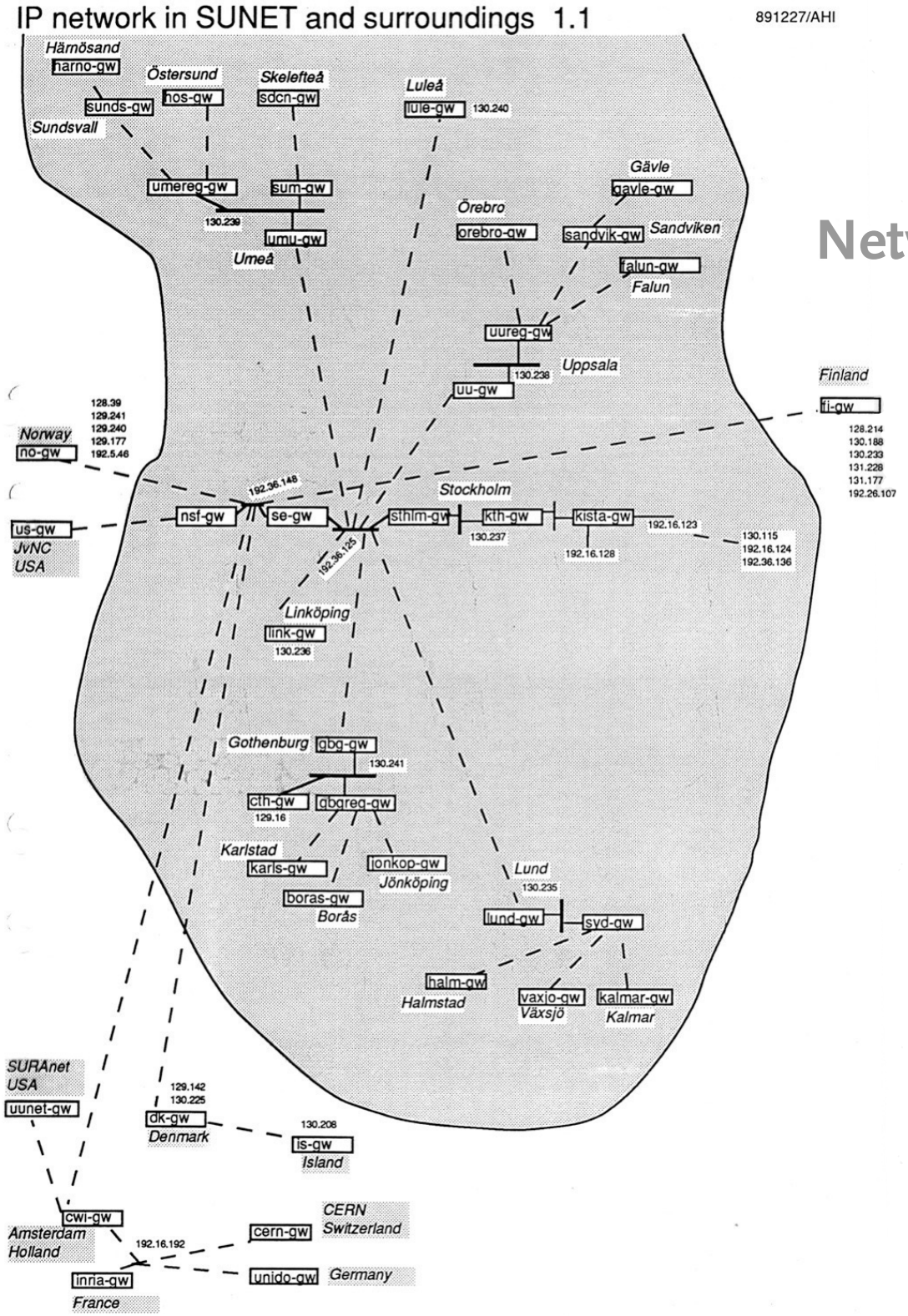
Patrik Fältström

Head of Research and Development

Netnod

A NEW WORLD

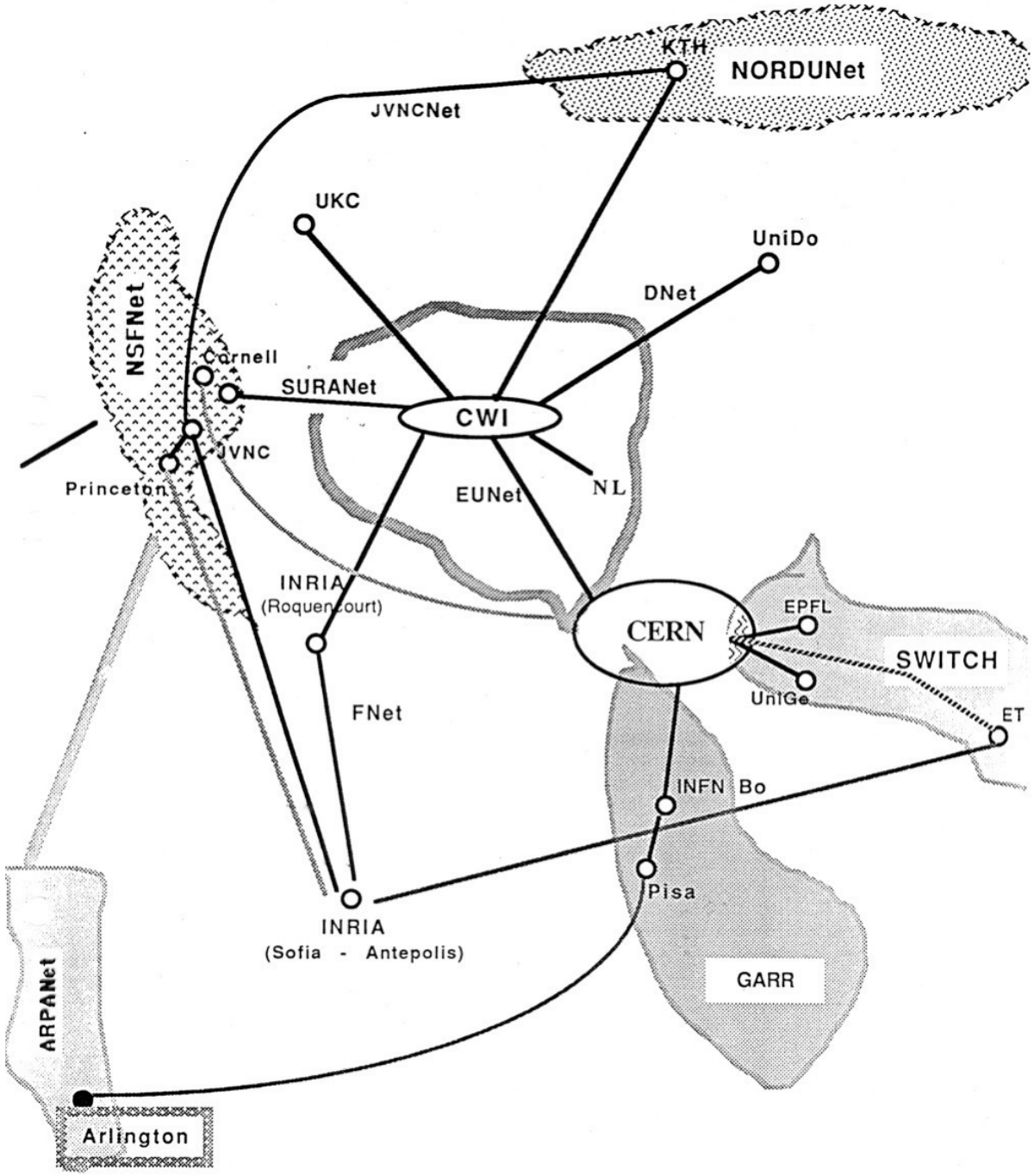
Network in Sweden December 1989



Cisco and µ-vax together with Vitalink bridges created long distance connections

Star-shaped network (64kbps links), with multi-port transceivers as local “LAN” segments

Connection via 64kbps satellite to JvNC in US and to Amsterdam



Networks in Europe December 1989

All connections to NSFNet

"Default Network" was pointing at NSFNet

5 connections over the Atlantic: Stockholm, Amsterdam, Sofi-Antipolis and Pisa

4 large networks: NorduNet, EUNet, Switch and Garr

Computers and Internet

Everything is in the future a computer, a networked computer of course!

At its simplest your TV, your phone, your address book, your agenda, your micro-wave, you car, your... and your laptop are all networked computers

The Internet belongs to all of us - or at least we all own a bit of it

Each of us has our own personal Internet and some of it we may choose to share

Increasingly each of us runs part of the infrastructure

My piece of the Internet?

When a person or organization connect to “the Internet”, the network and services provided end up being a piece of the Internet

Protection (and robustness) start at home

You have a lock on your door, and do not ask road authorities to keep burglars out!

More about this later…

Implications

Your fibre owner might not be your access provider

Your access provider might not be your Internet provider

Your Internet provider might not be your telephony provider

You can be your own telephony provider

Who is responsible for what?

NETNOD

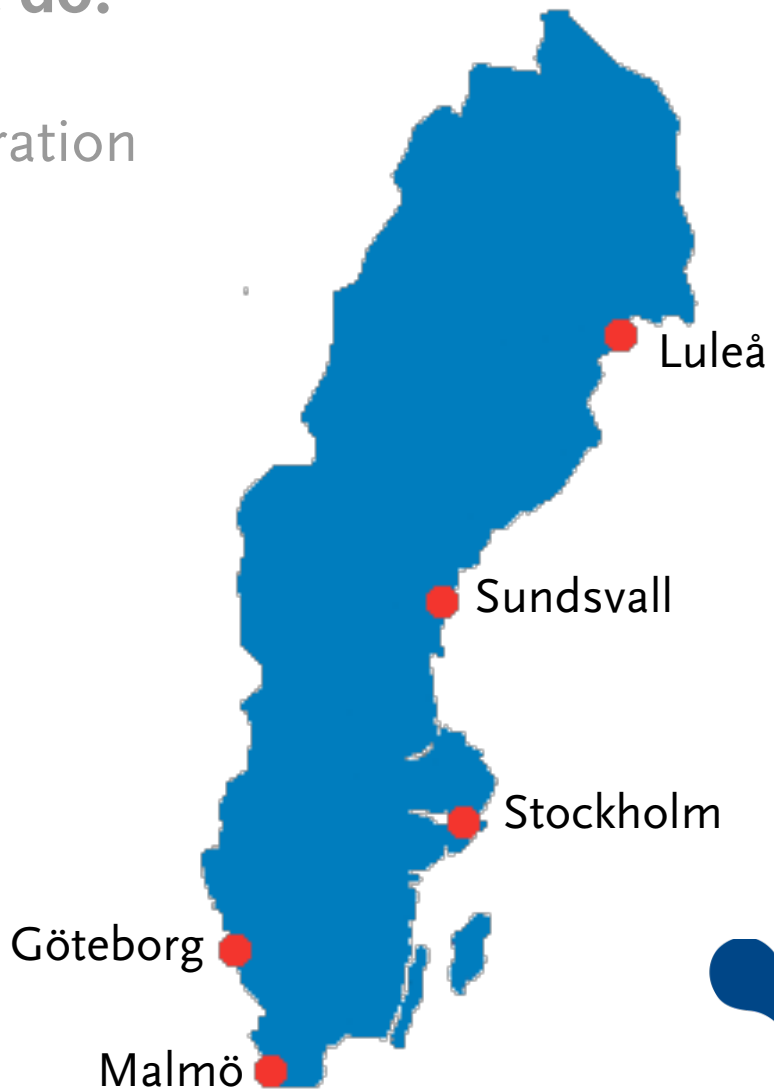
What is Netnod, and what do we do?

By a foundation fully owned incorporation

Not for profit

Provides:

- **IX in 6 locations**
- **DNS in 55 locations**
- **NTP-service in 4 locations**



Netnod history

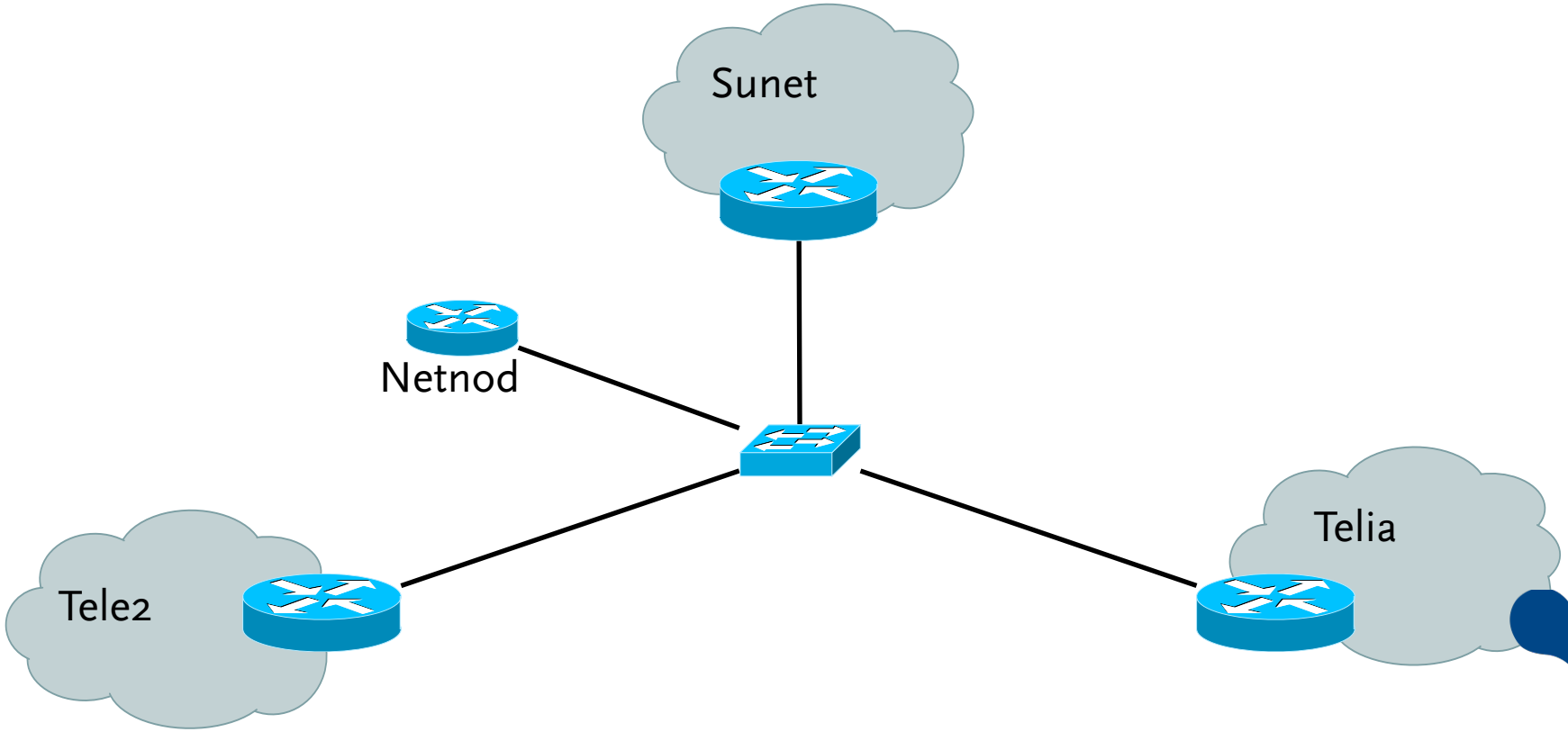
1992-1996 there was a distributed IX at Royal Institute of Technology

1996 the TU-foundation was created

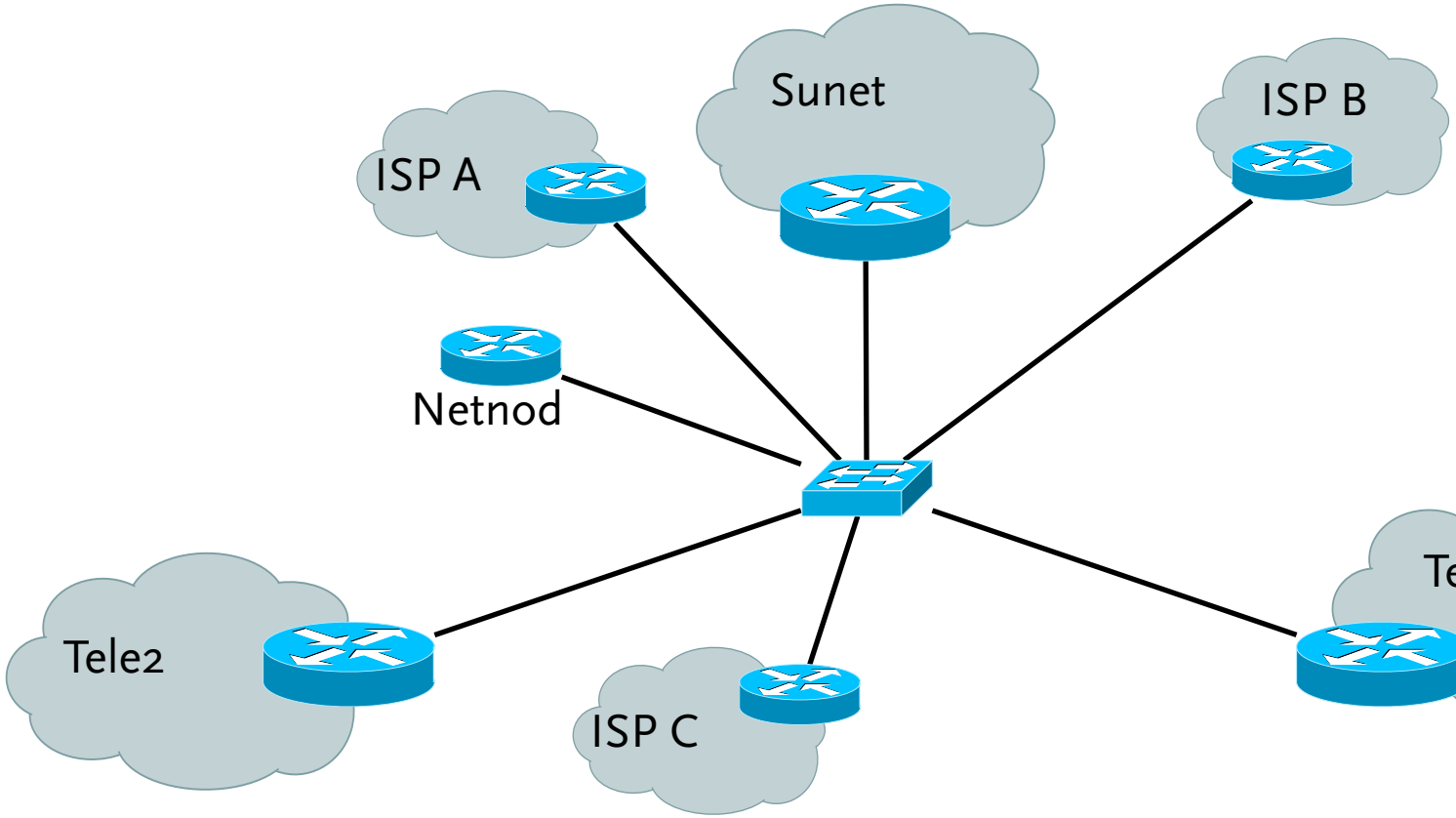
Goal was increased robustness and security

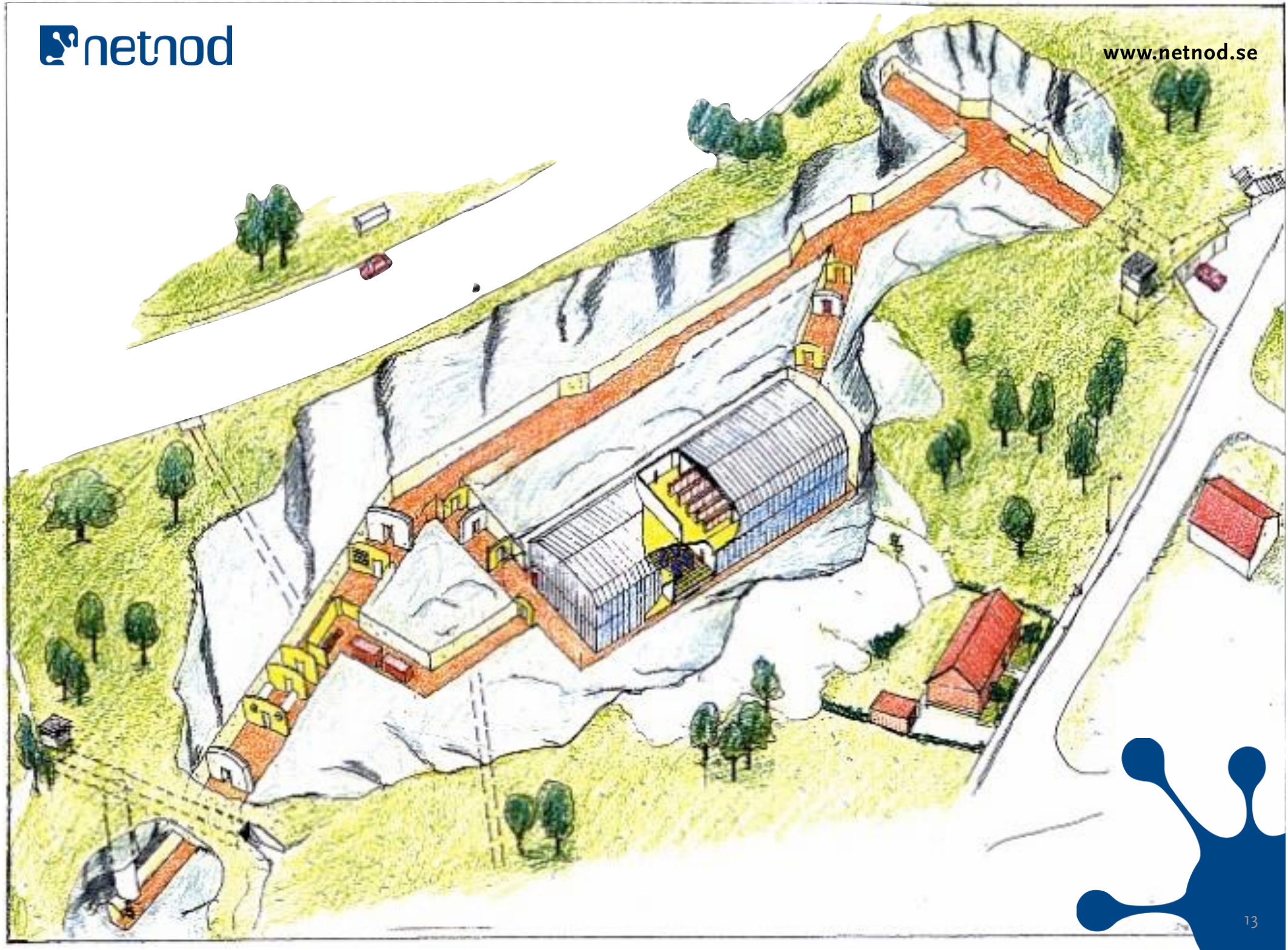
The IX was moved to bunkers in the mountains

Netnod was created



The model did grow




netnod
www.netnod.se

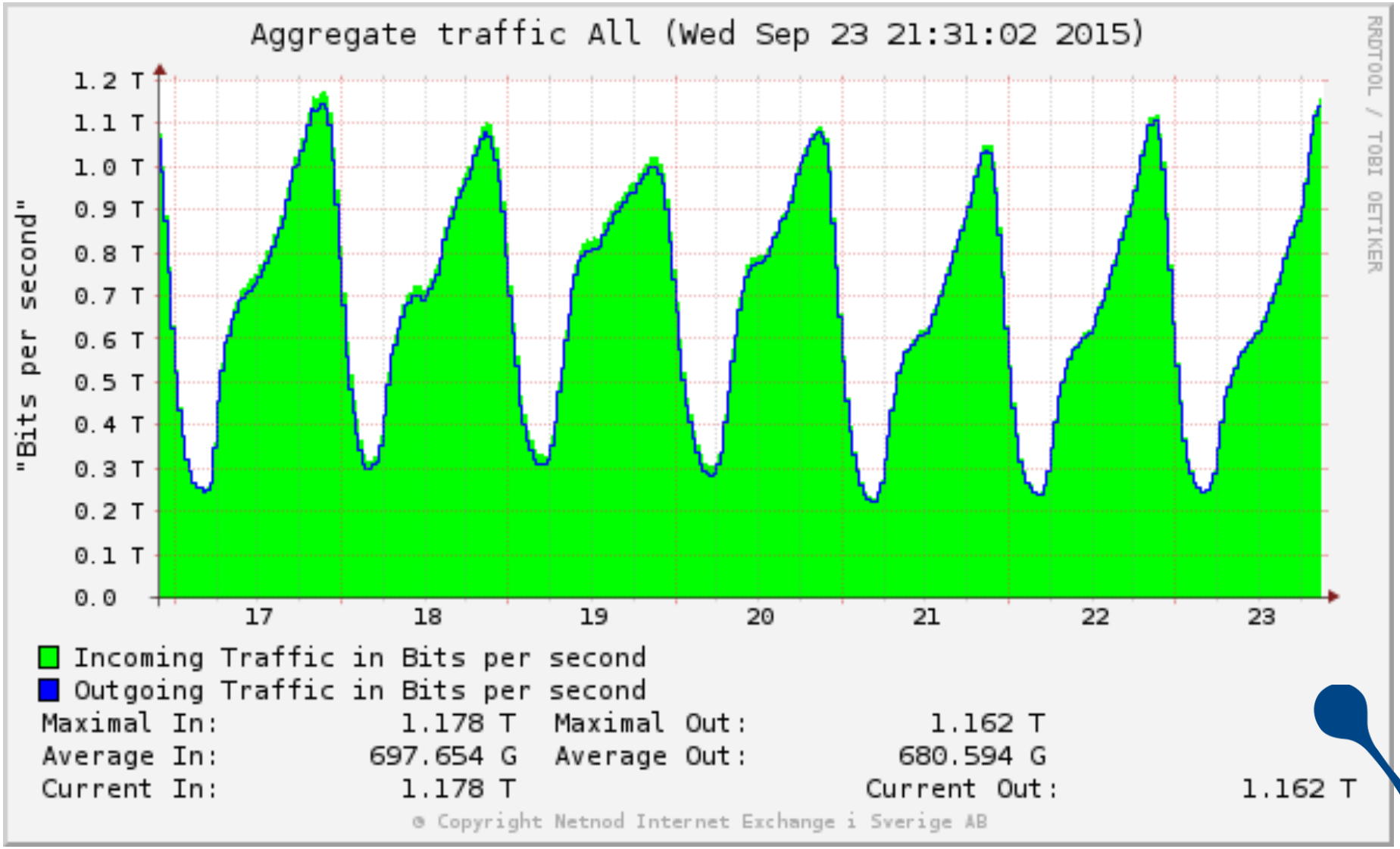
netnod

Mountain bunkers

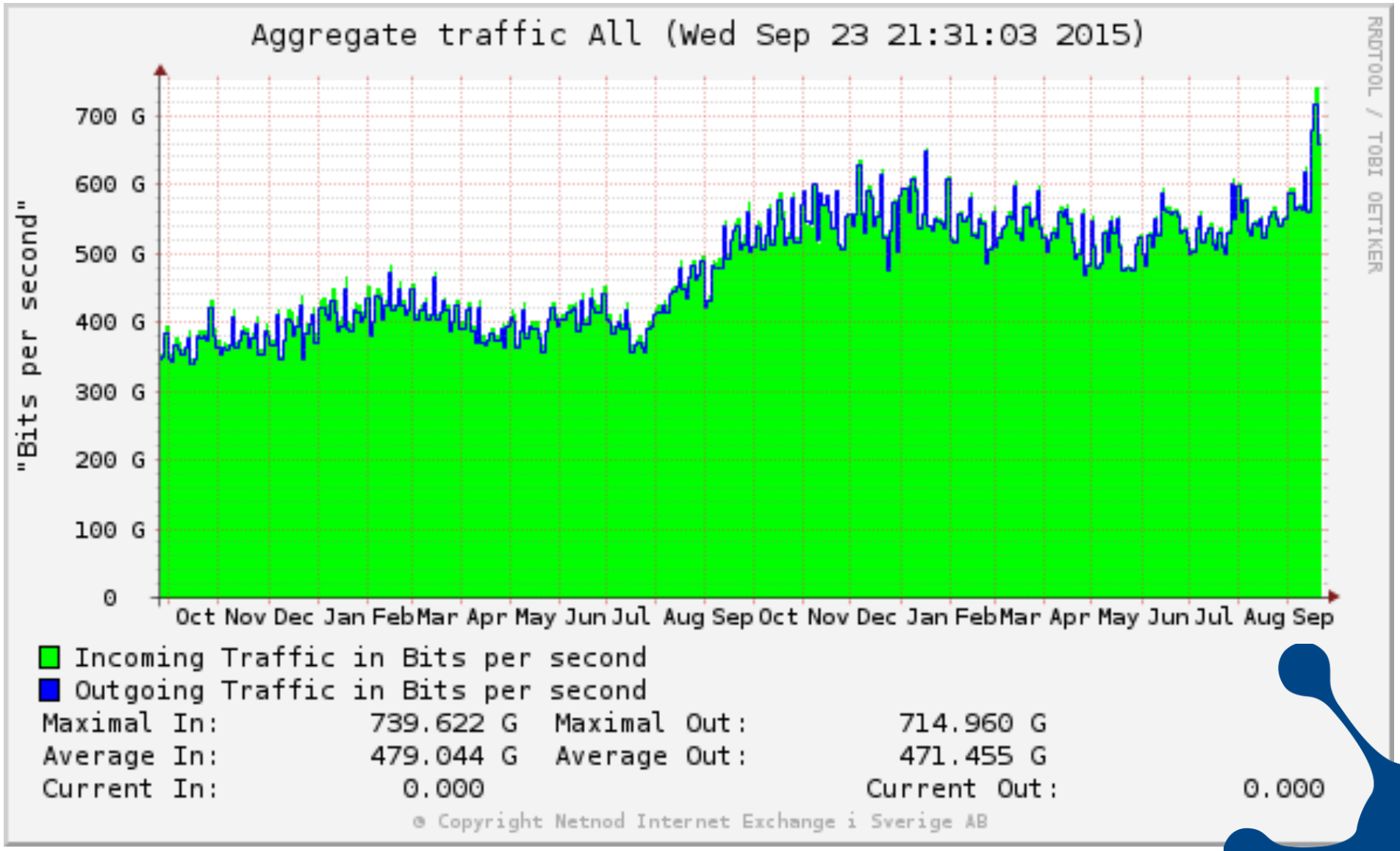
Regulator PTS provides colocation service

Specifically created for telecom

Traffic last week



Traffic last two years, 24h average



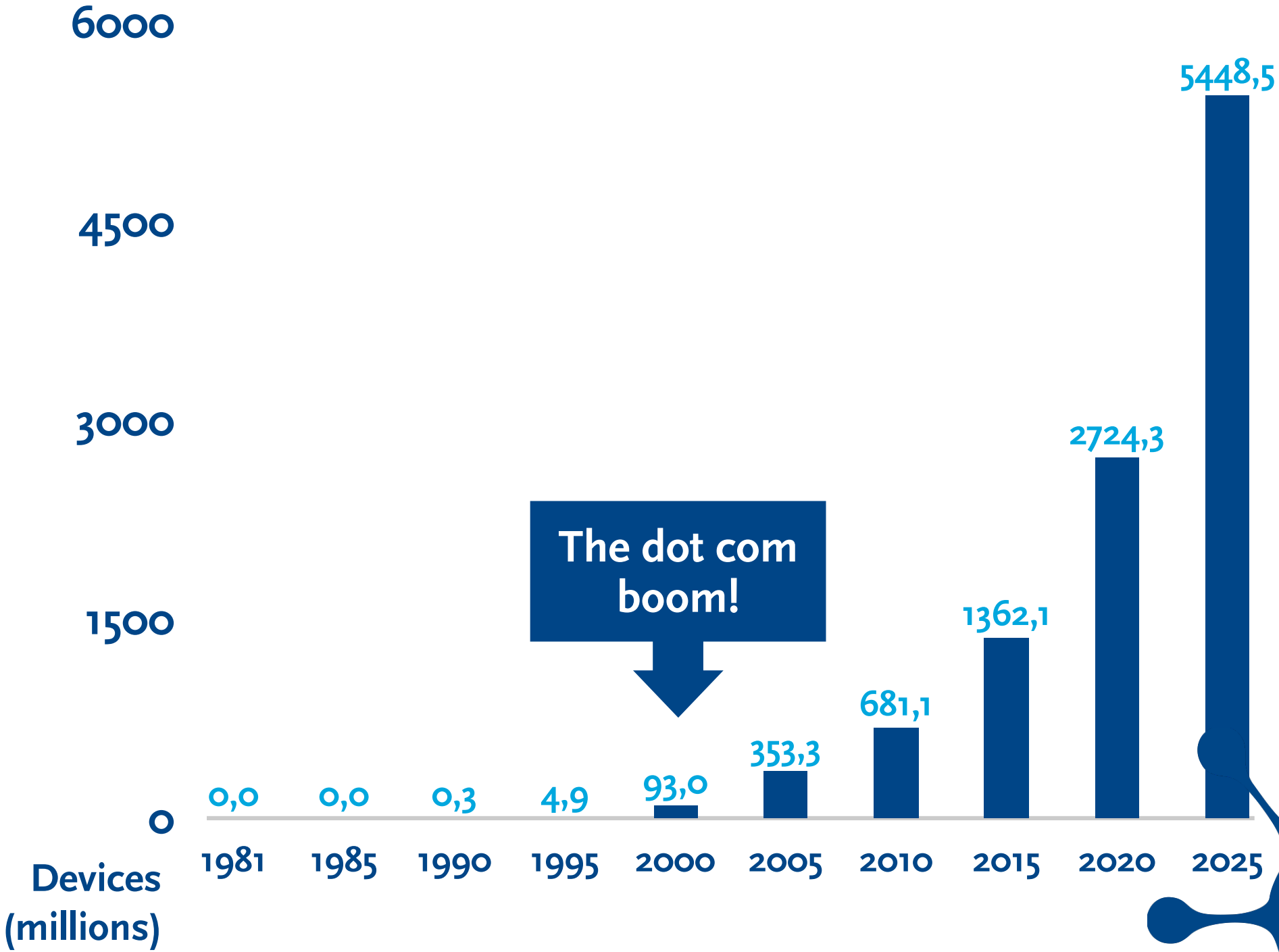
DNS services hosted all over the world

EXAMPLE — MOVING PACKETS

What can possibly go wrong?

We move into third phase of Internet

1980–1995	Era of deregulation and competition, Internet arrives
1995–2010	Early days of Internet, service providers, social networking, mobile Internet
2010–2025	Internet takes off...


6000
4500
3000
1500
0
Devices (millions)
0,0
0,0
0,3
4,9
93,0
353,3
681,1
1362,1
2724,3
5448,5
1981
1985
1990
1995
2000
2005
2010
2015
2020
2025
The dot com boom!

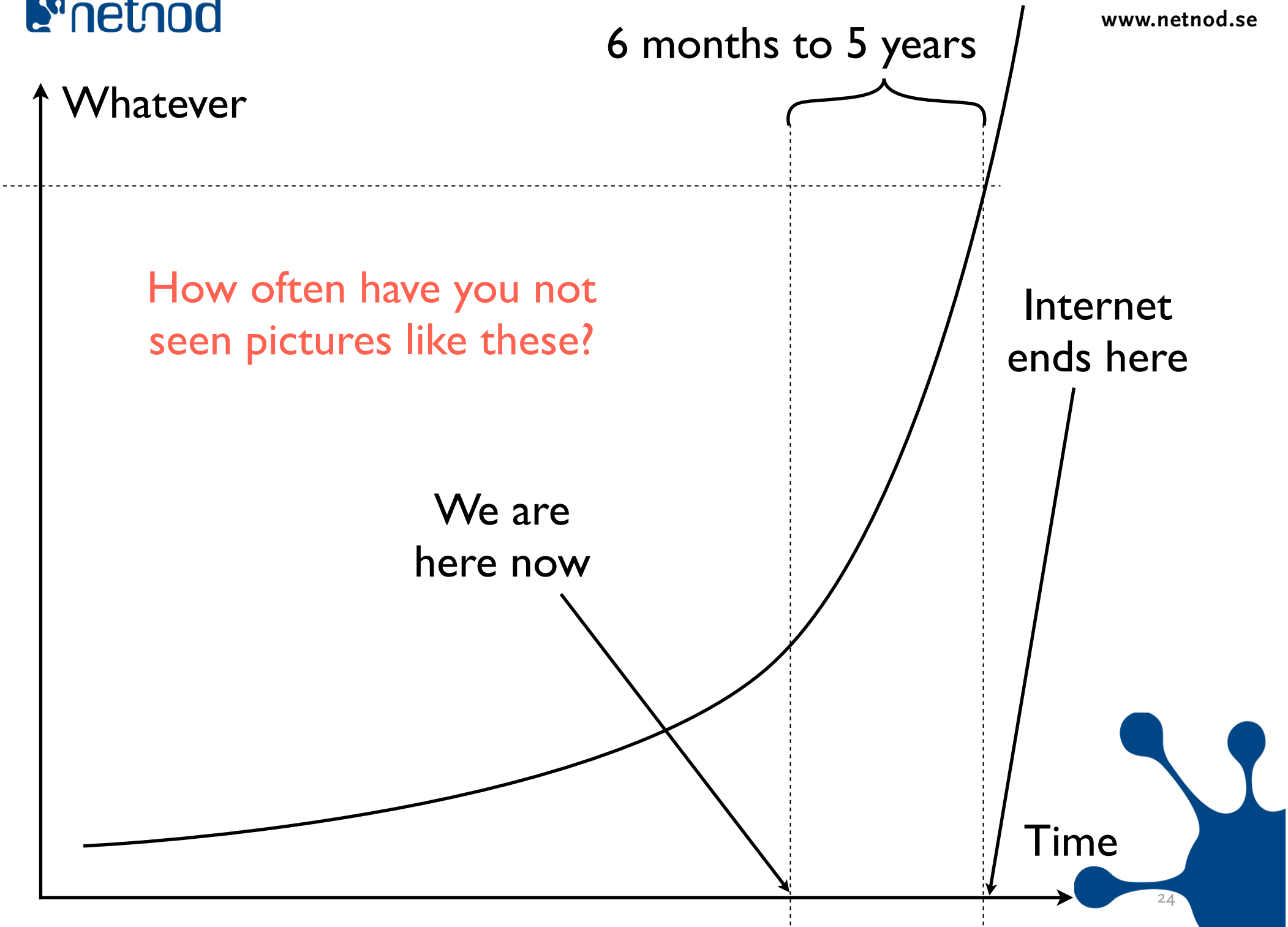
Video Will Become the Predominant Traffic

1995: Web Overtakes Gopher, FTP

2000: Peer-to-Peer Overtakes Web

2013: Video Content Overtakes Peer-to-Peer

2025: Video Communication Overtakes Video Content


6 months to 5 years
Whatever
How often have you not seen pictures like these?
Internet ends here
We are here now
Time

We have a few different problems:

Do we know what will break?

Do we know when it will break?

Can we increase ability for the system to withstand stress?

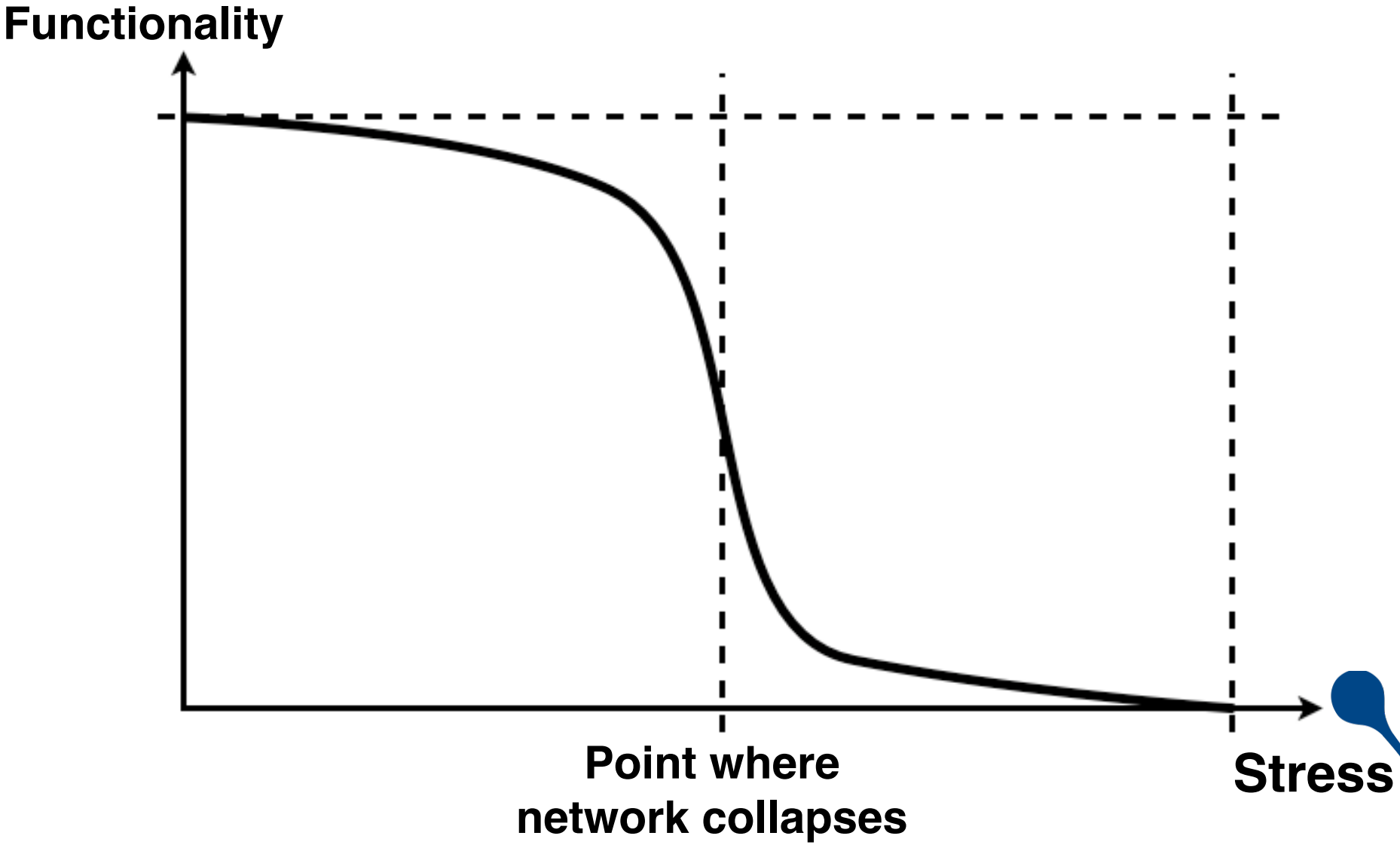
What do we do when things breaks?

Can partially functioning systems withstand all traffic?

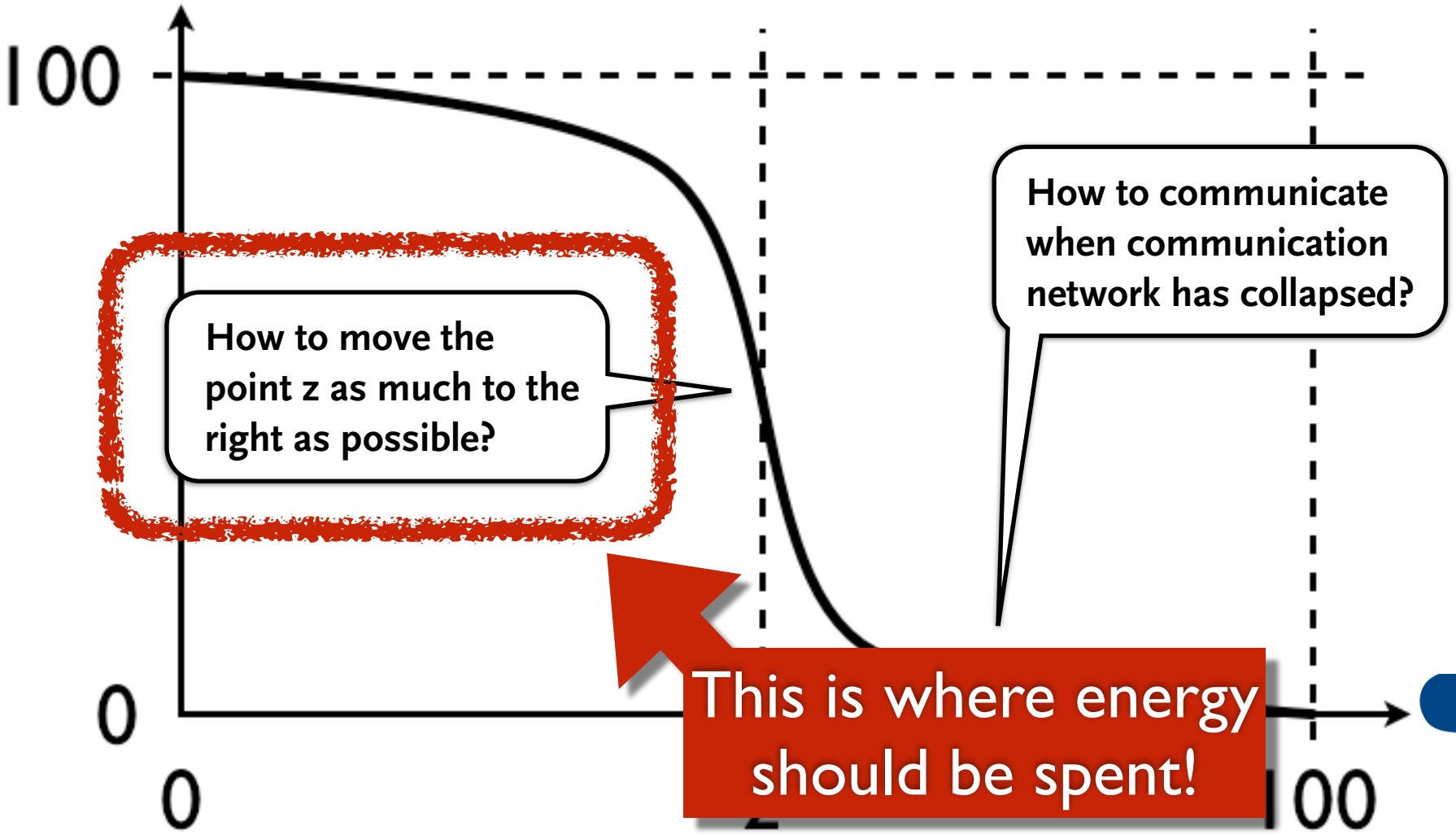
Can we minimize the amount of unwanted traffic?

What is unwanted traffic?

Degradation in a packet based network...



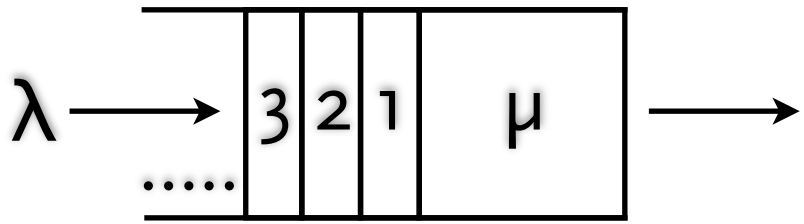
Two different questions that should not be mixed:

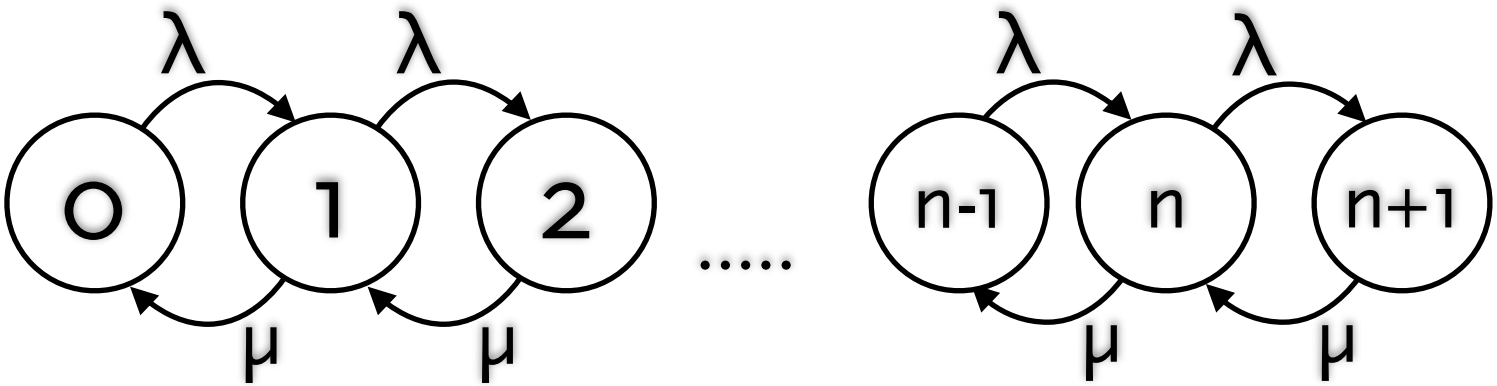


Packet based networks?

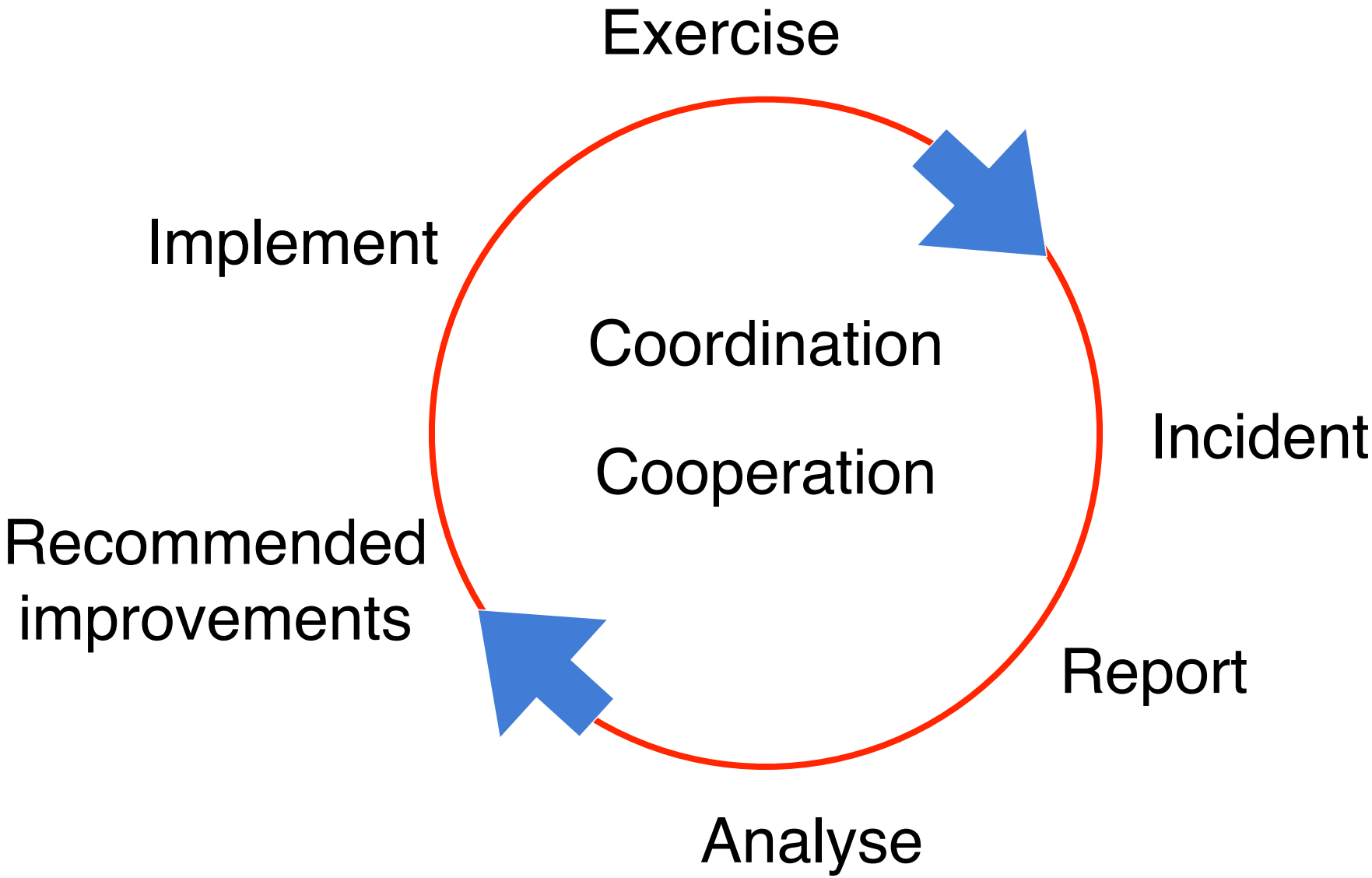
In each network element you see an M/M/1 queuing mechanism

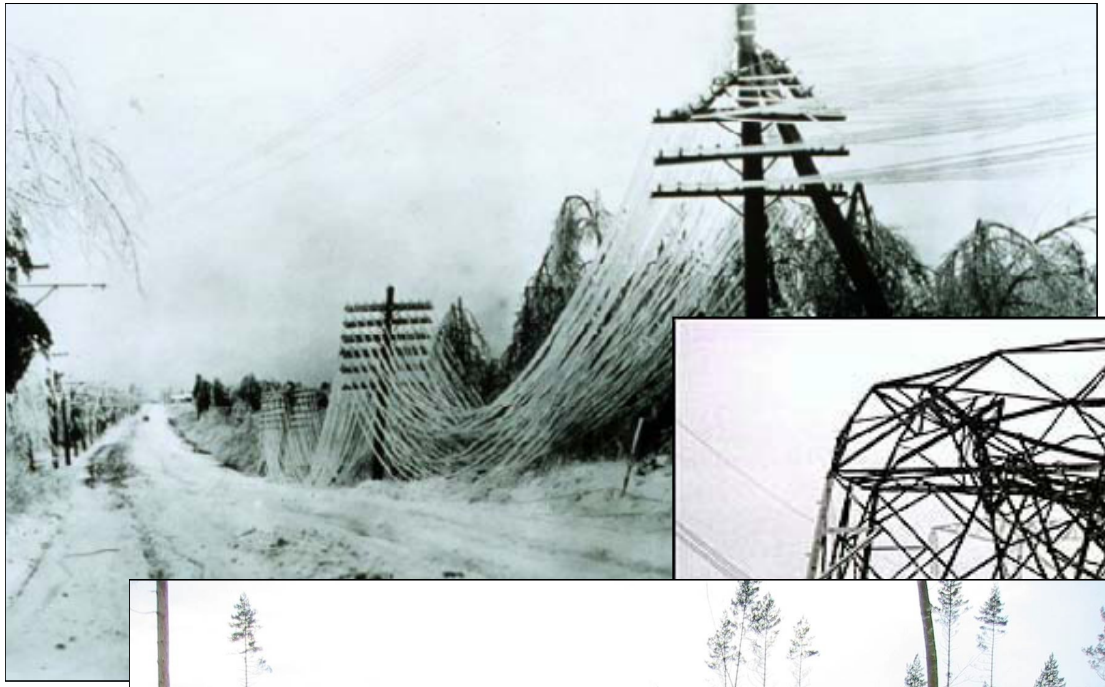
Relatively simple to show how more effective packet based systems (M/M/1/K with combined poisson and exponential distribution) are than traditional TDM





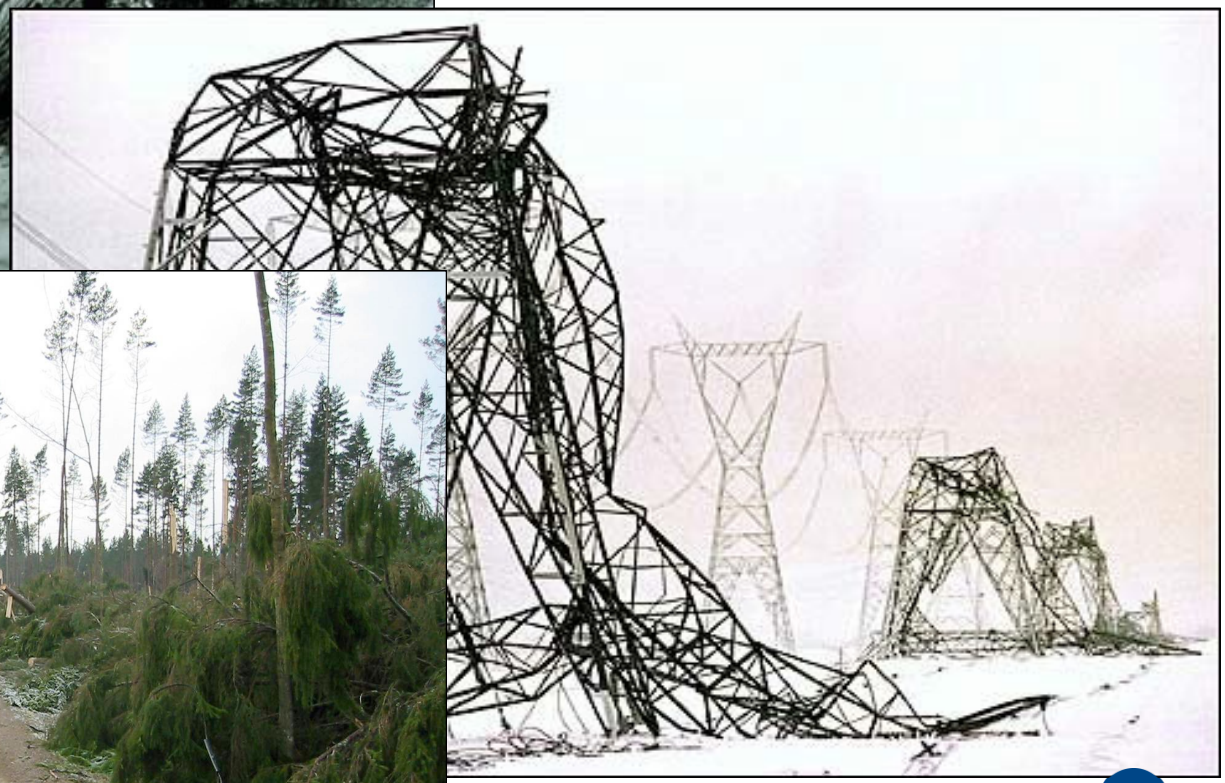
Circle of life



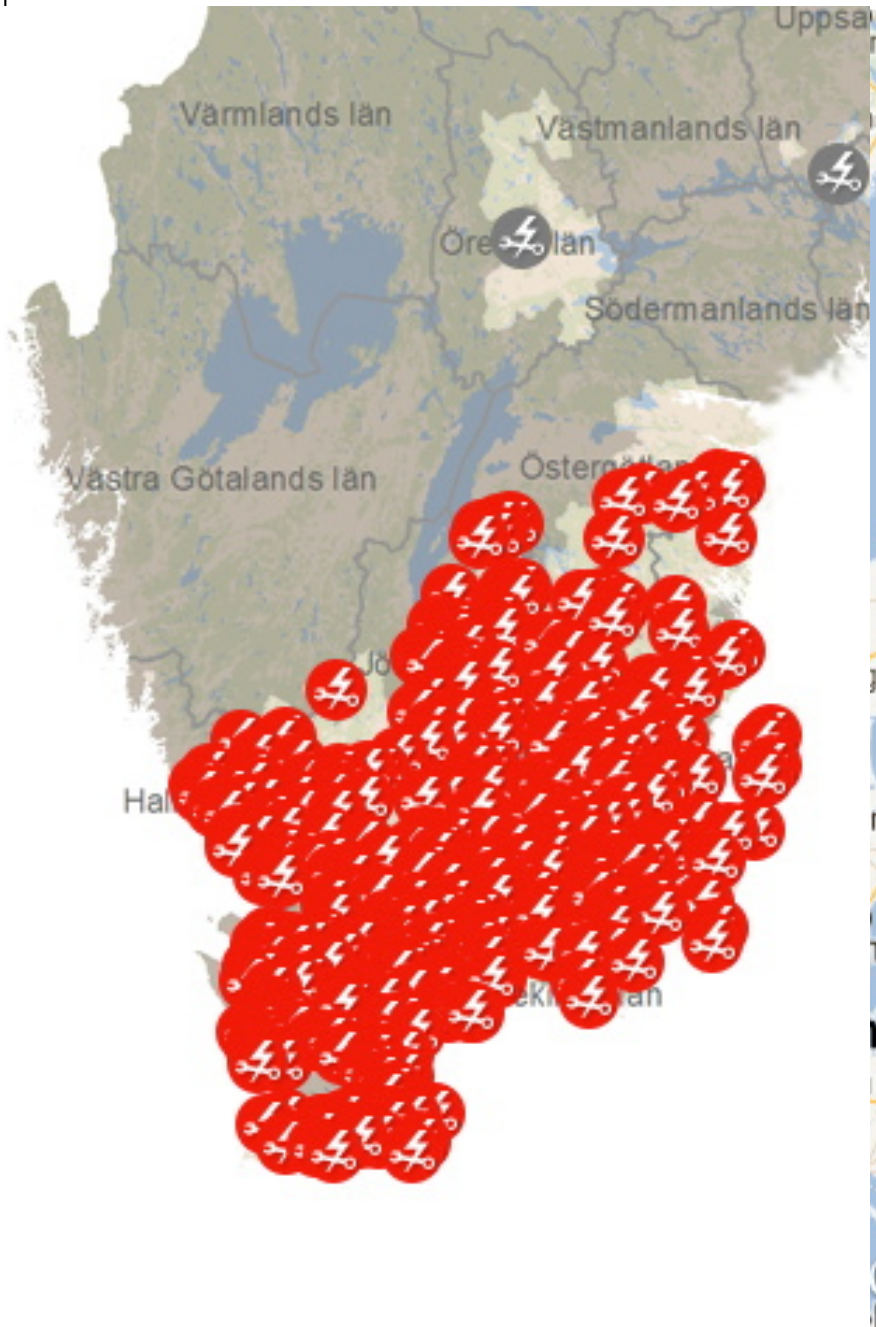


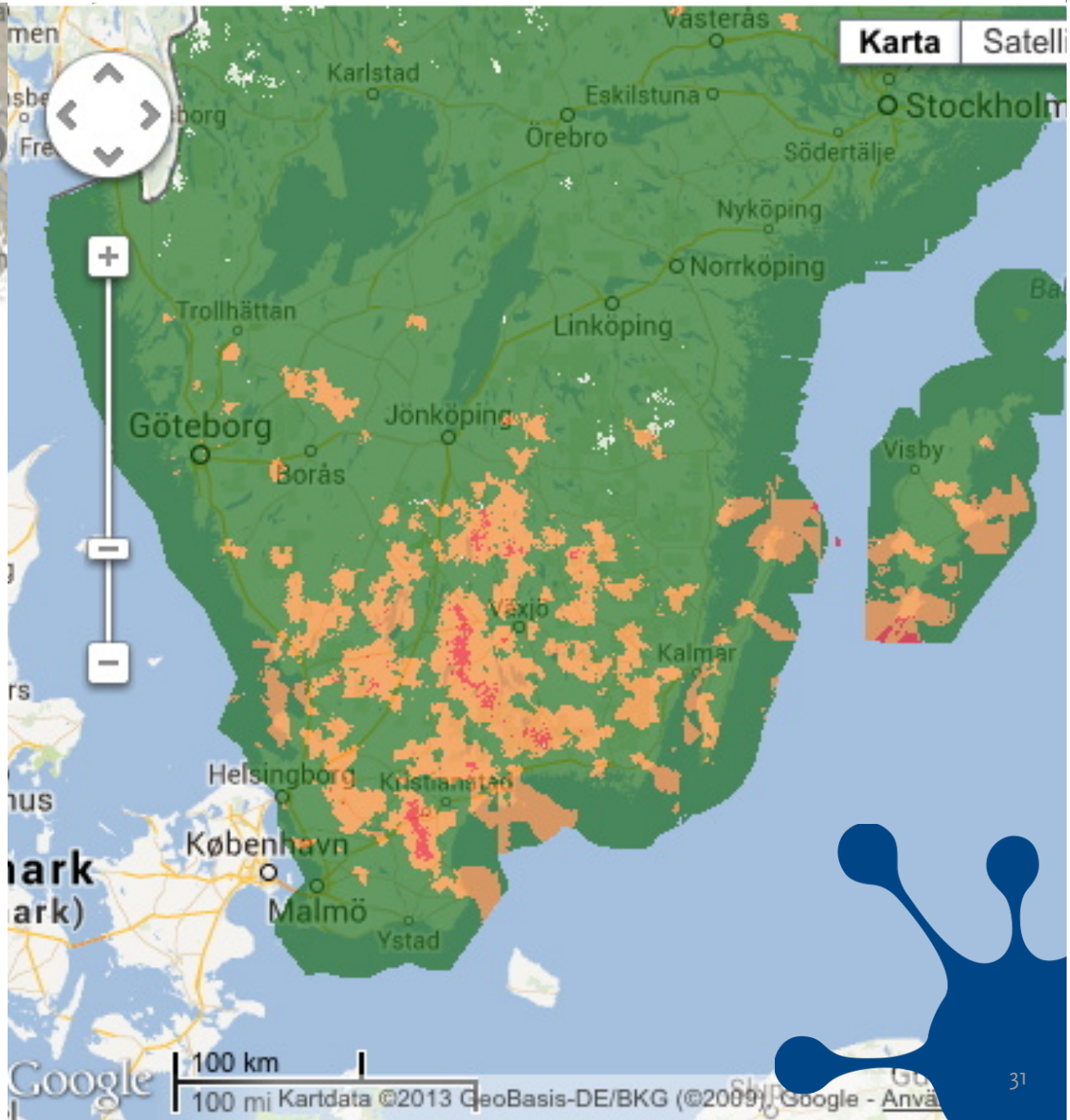
1921 - Sweden

1998 - Canada



2005 - Sweden


Värmlands län
Västmanlands län
Örebro län
Södermanlands län
Västra Götalands län


Karta
Satelli
Karlstad
Eskilstuna
Stockholm
Örebro
Södertälje
Nyköping
Norrköping
Trollhättan
Linköping
Göteborg
Jönköping
Borås
Visby
Växjö
Kalmar
Helsingborg
Kristianstad
København
Malmö
Ystad
100 km
100 mi
Kartdata ©2013 GeoBasis-DE/BKG (©2009), Google - Anvä


206
00010409 LEDIG
Sumetzberger
206
206
201
206

How to build a network?

Redundancy, redundancy, redundancy...

- **If there is packet drop, it should not be in your network**

This implies a few basic things:

- **At least two paths for every packet**
- **Enough capacity in single path for all traffic**
- **Minimize dependency on external parties**
- **Know before things happens what will break**
  - **...and prepare for it!**

What happens?

A physical disturbance is still the most common problem

- Fibre break
- Software upgrade / crashing router or switch
- Power outage
- Surprisingly high amount of traffic

What happens?

A physical disturbance is still the most common problem

- Fibre break
- Software upgrade / crashing router or switch
- Power outage
- Surprisingly high amount of traffic

SENASTE NYTT

NYHETER

"Så minns vi Göran Stangertz" 13:38

Misstänkt kvinnomord efter brand 13:24

Göran Stangertz har avlidit 13:20

Evakueringen inför superstormen har börjat 13:07

"Frankenstorm' kan stoppa SAS 12:52

Linda, 24: "Tog allt vi ägde och gick uppåt" 12:45

SD:s väljare väljer KD 12:13

Klitjko kan avgöra ukrainska valet 11:38

Dagens Äckel finns i tonårsflickornas rum 11:33

Skriv ditt bästa minne av Göran Stangertz 10:51

I dag ska Anonymous slå till – igen

Hackarna hotar Sverige på nytt

I dag tänker Anonymous slå till mot Sverige – igen.

Hackarna ska bland annat planera att ta ner sajterna för FRA, polisen och Antipiratbyrån.

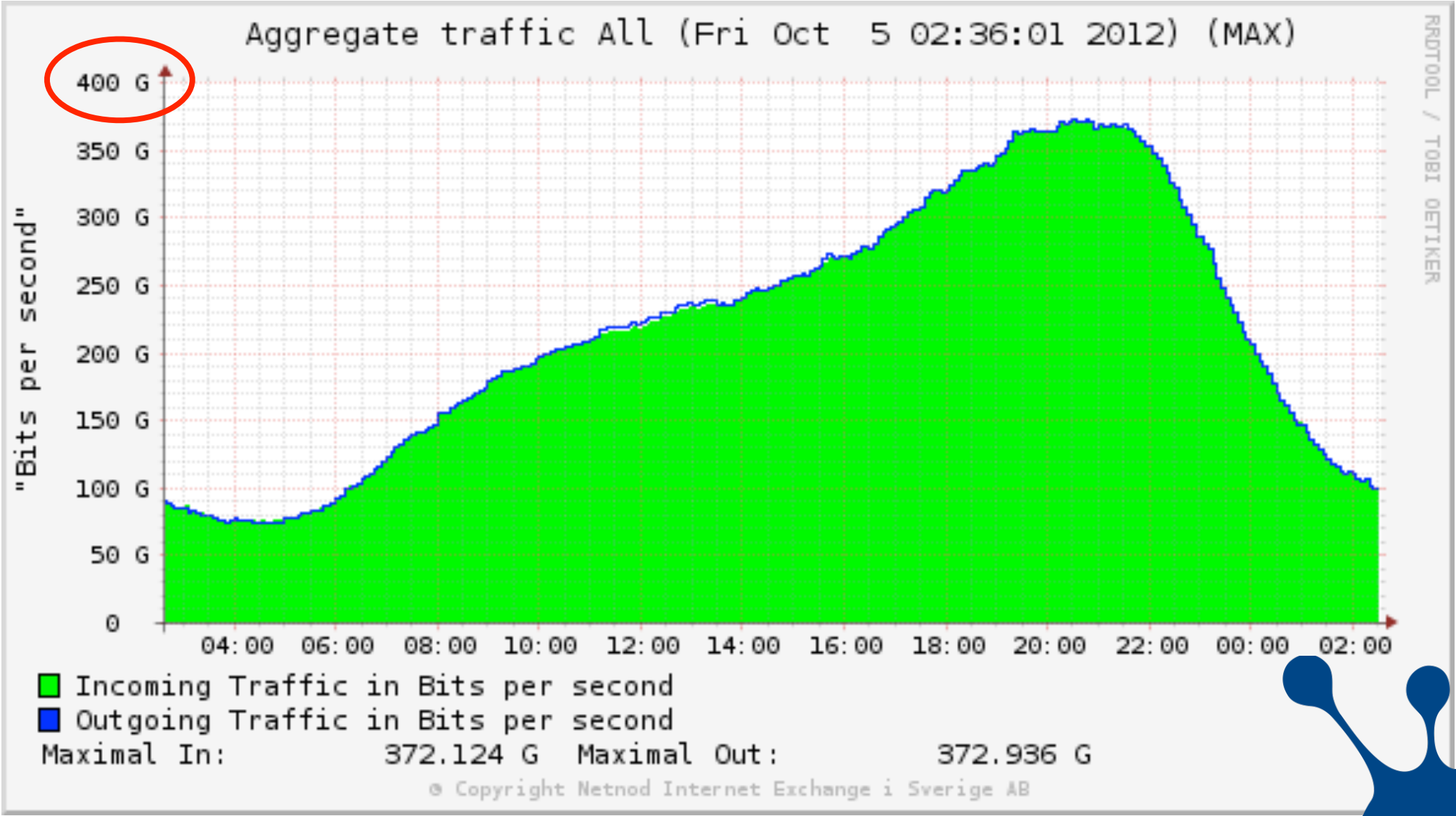
– Vi kommer att göra det största som någonsin

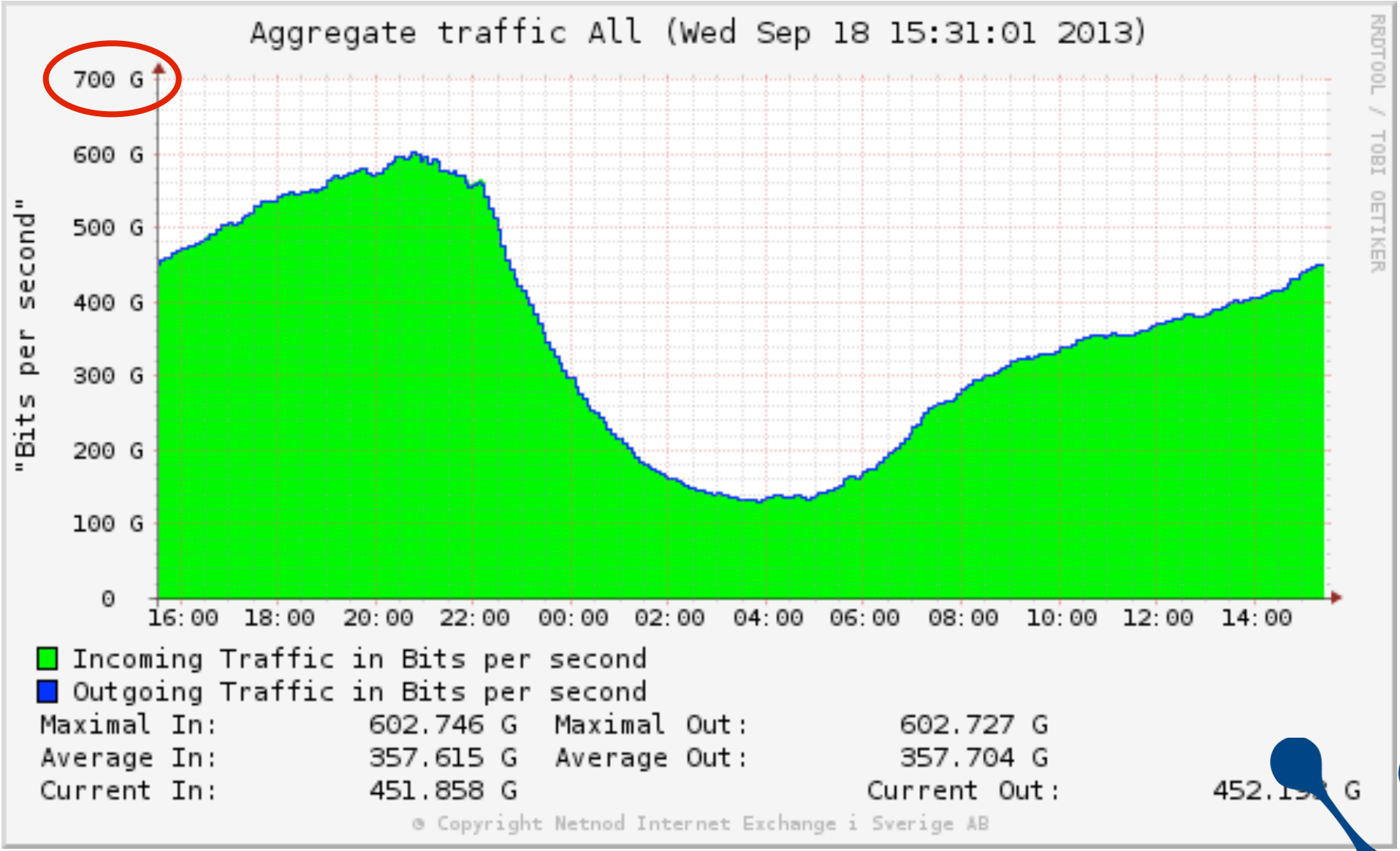
MEST LÄST IDAG

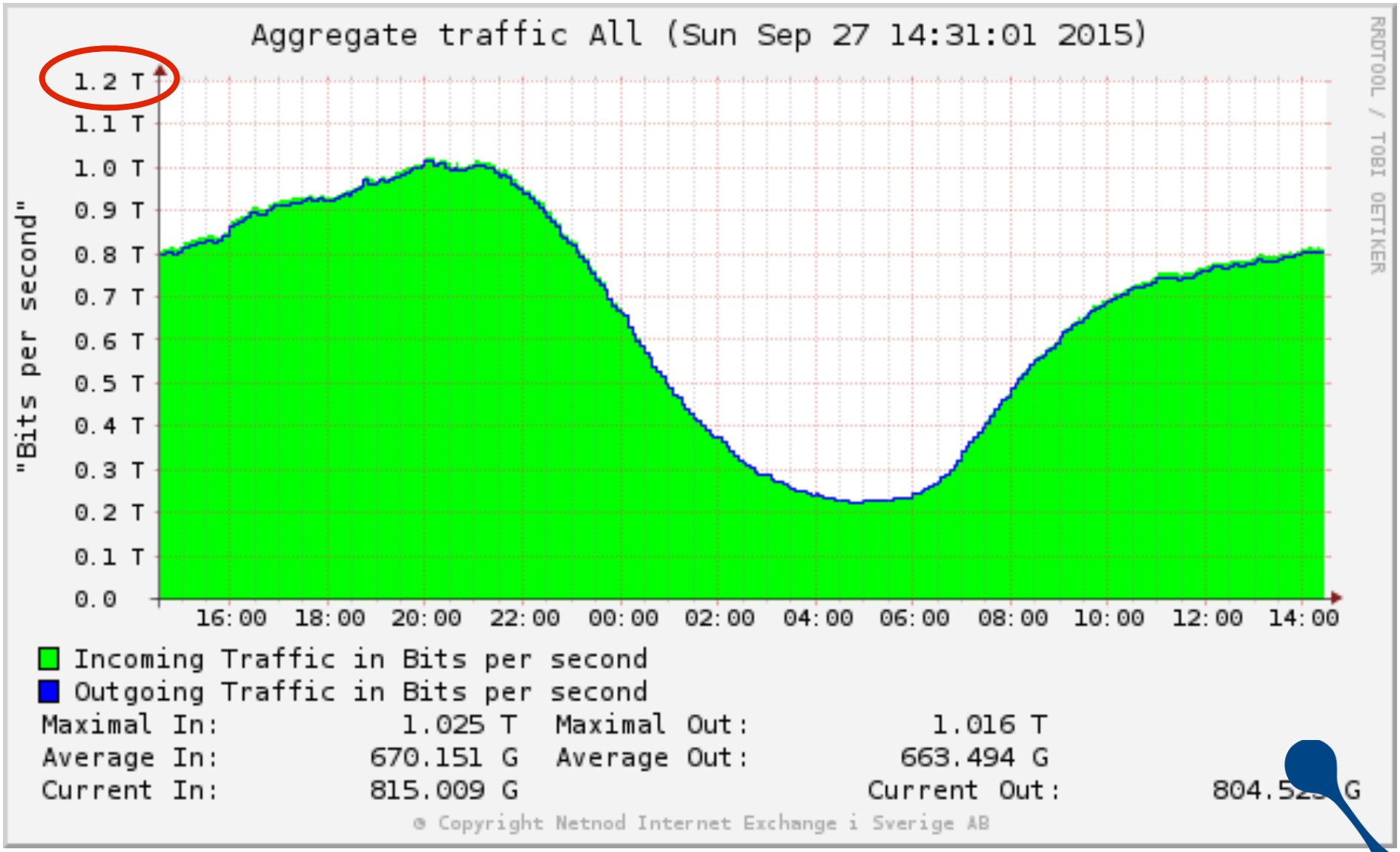
Göran Stangertz har av
TV+TEXT Skådespelaren och regiss
Stangertz har avlidit. Han blev 68

Franke sto
stoppa SAS
Ovädret Sandy
flygbola

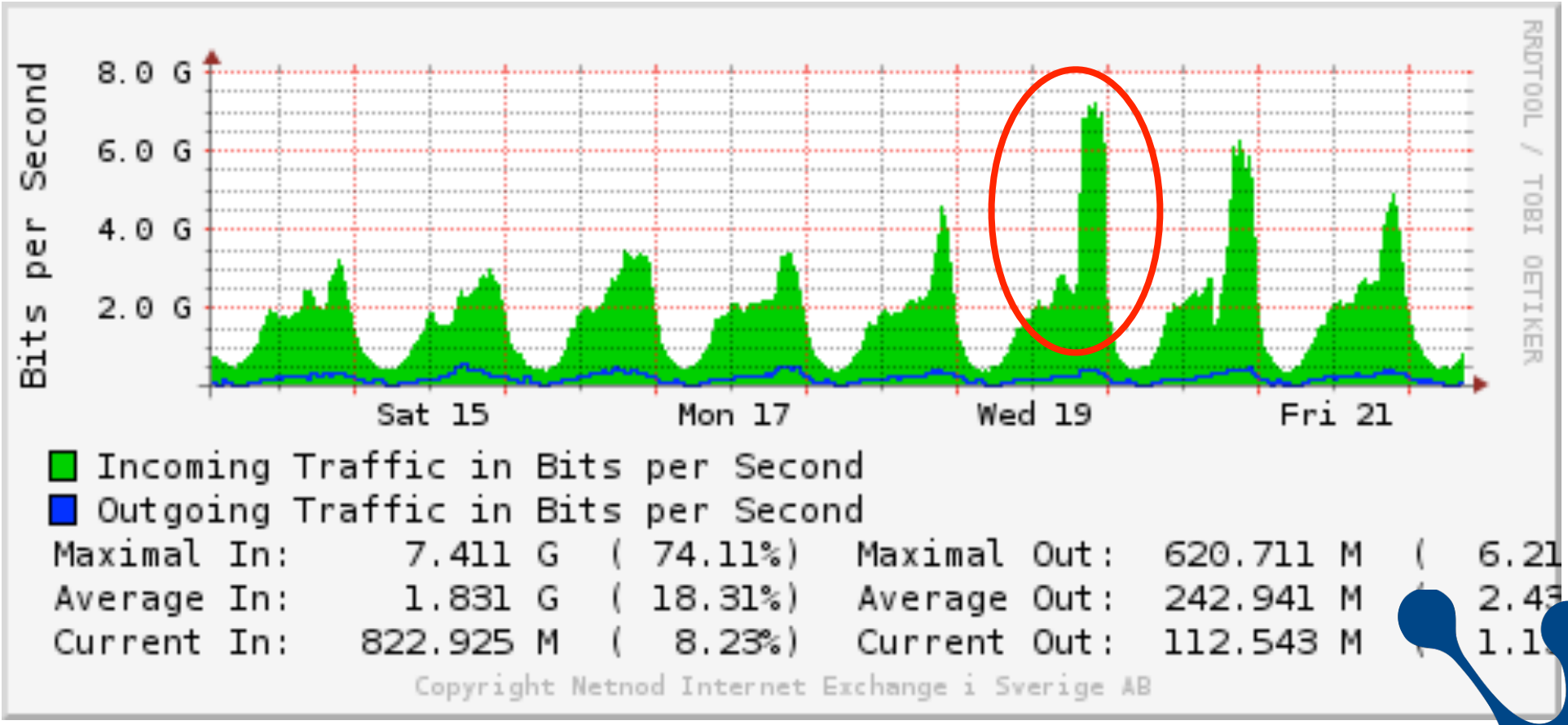
SD:
De
Moder

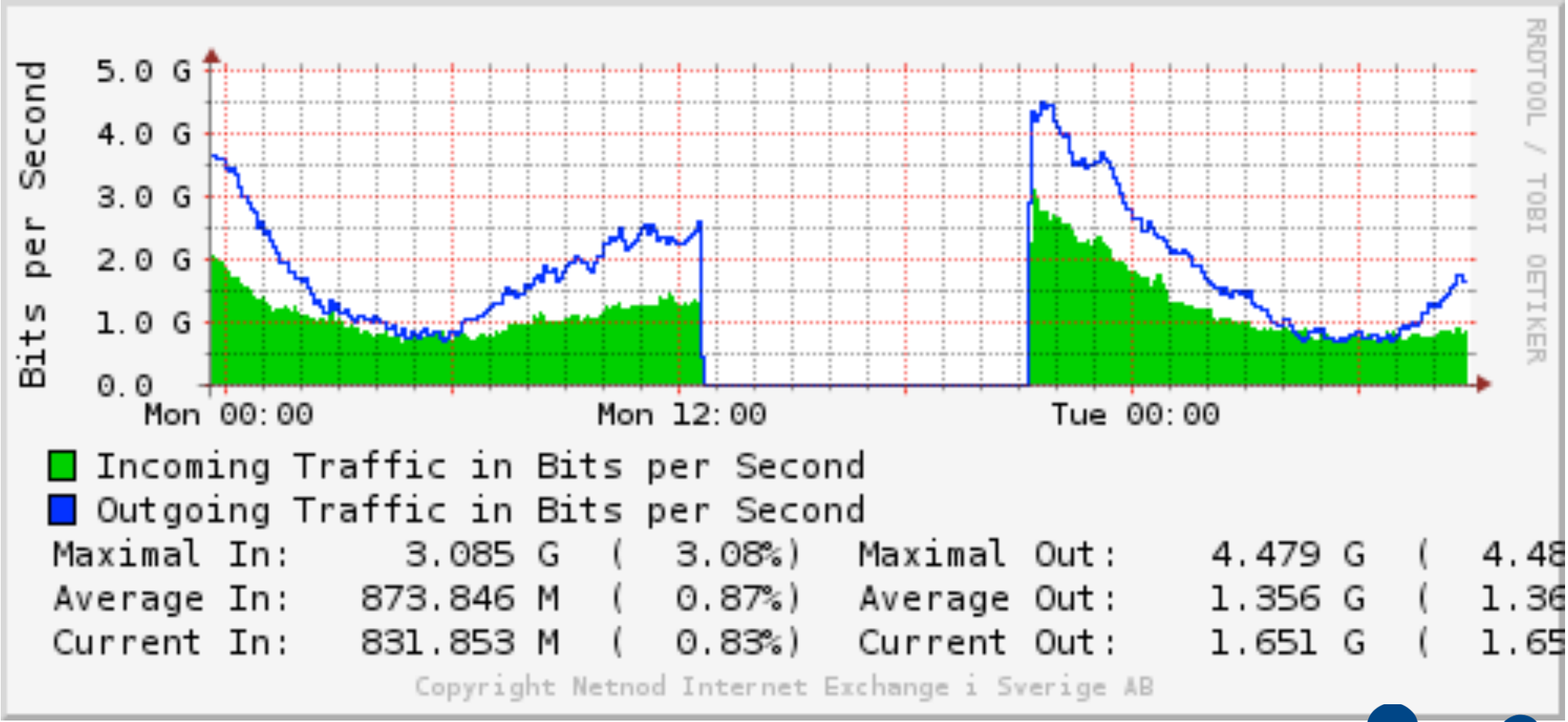

Aggregate traffic All (Fri Oct 5 02:36:01 2012) (MAX)
"Bits per second"
400 G
350 G
300 G
250 G
200 G
150 G
100 G
50 G
0
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
RRDTOOL / TOBI OETIKER
Incoming Traffic in Bits per second
Outgoing Traffic in Bits per second
Maximal In: 372.124 G
Maximal Out: 372.936 G
© Copyright Netnod Internet Exchange i Sverige AB

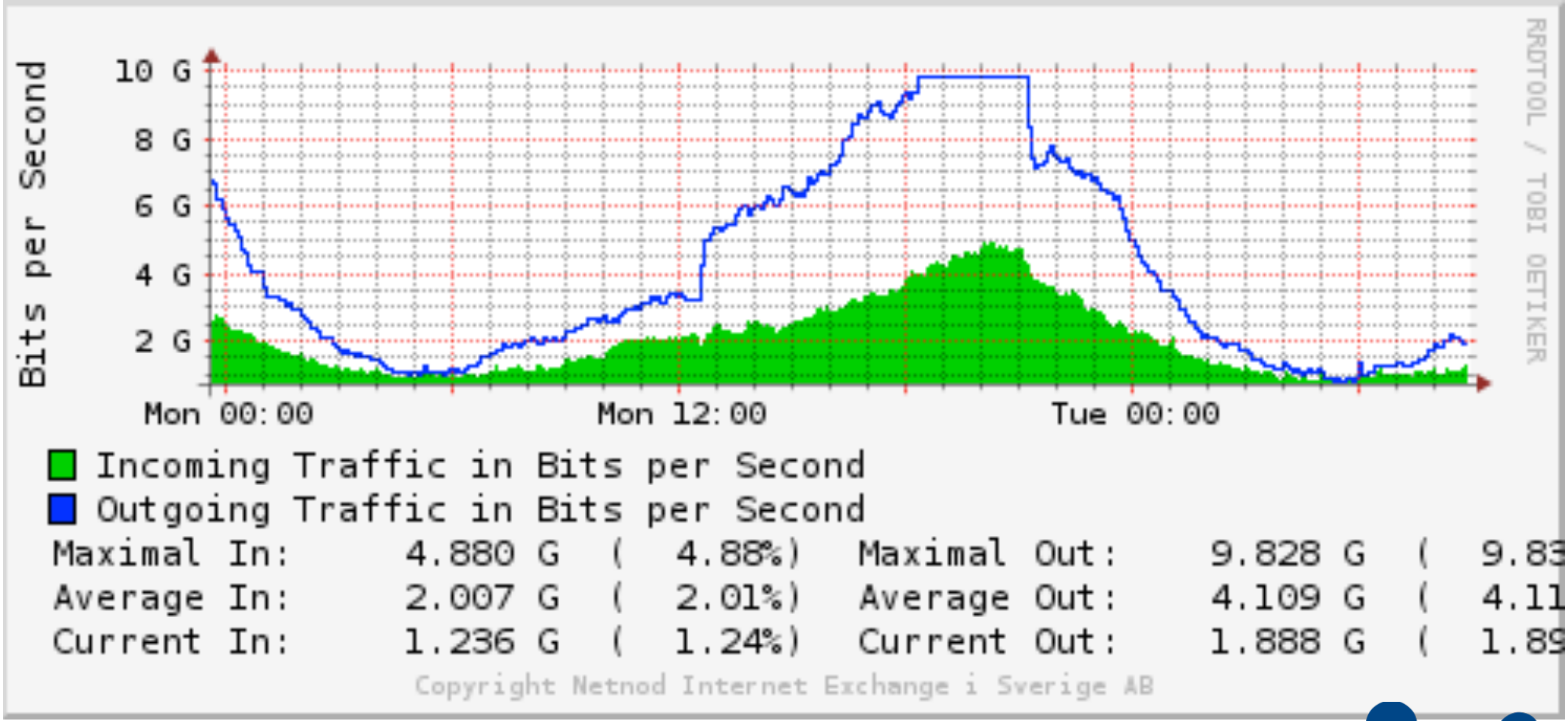

Aggregate traffic All (Wed Sep 18 15:31:01 2013)
"Bits per second"
700 G
600 G
500 G
400 G
300 G
200 G
100 G
0
16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00
RRDTOOL / TOBI OETIKER
Incoming Traffic in Bits per second
Outgoing Traffic in Bits per second
Maximal In: 602.746 G
Maximal Out: 602.727 G
Average In: 357.615 G
Average Out: 357.704 G
Current In: 451.858 G
Current Out: 452.1
© Copyright Netnod Internet Exchange i Sverige AB

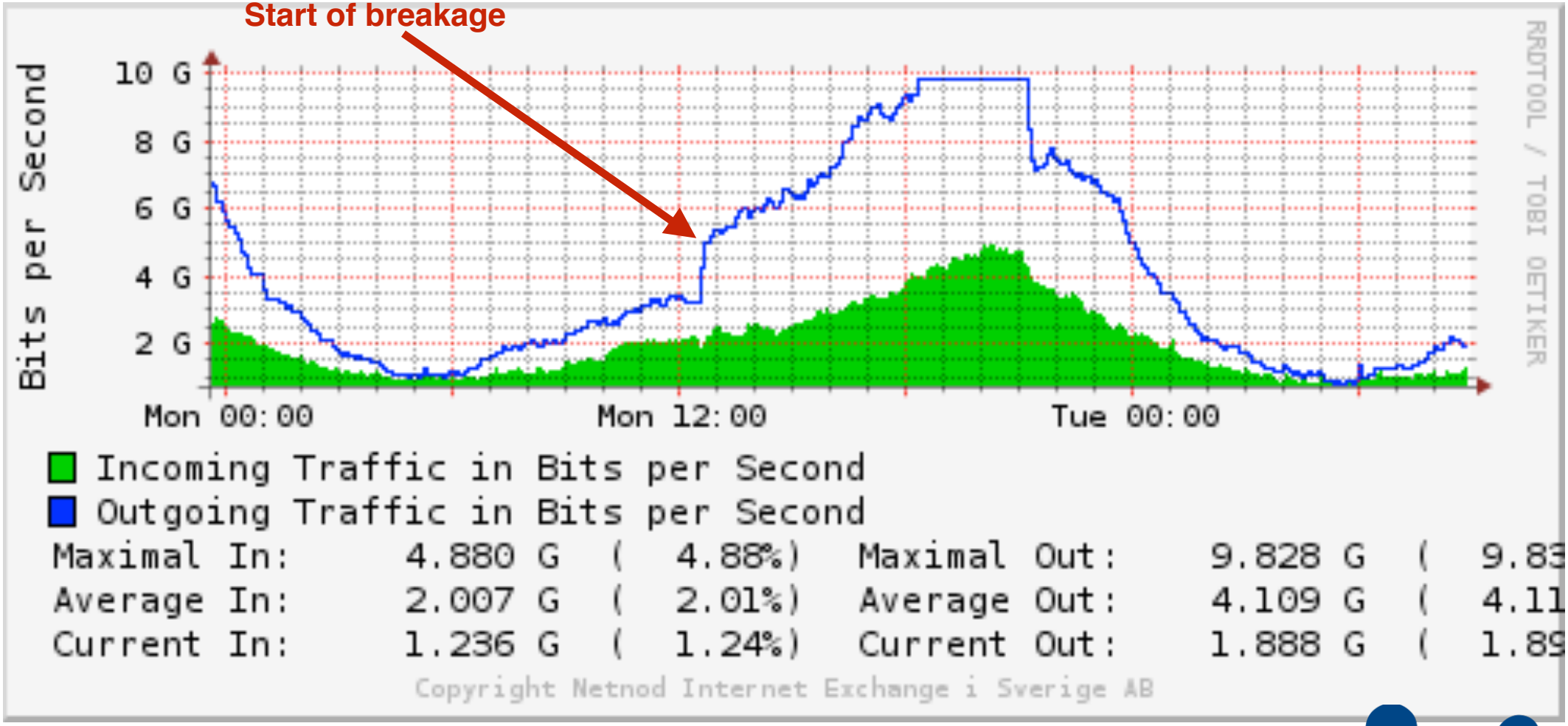

Aggregate traffic All (Sun Sep 27 14:31:01 2015)
"Bits per second"
1.2 T
1.1 T
1.0 T
0.9 T
0.8 T
0.7 T
0.6 T
0.5 T
0.4 T
0.3 T
0.2 T
0.1 T
0.0
16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00
RRDTOOL / TOBI OETIKER
Incoming Traffic in Bits per second
Outgoing Traffic in Bits per second
Maximal In: 1.025 T
Maximal Out: 1.016 T
Average In: 670.151 G
Average Out: 663.494 G
Current In: 815.009 G
Current Out: 804.52
G
© Copyright Netnod Internet Exchange i Sverige AB

One customer...mid october...

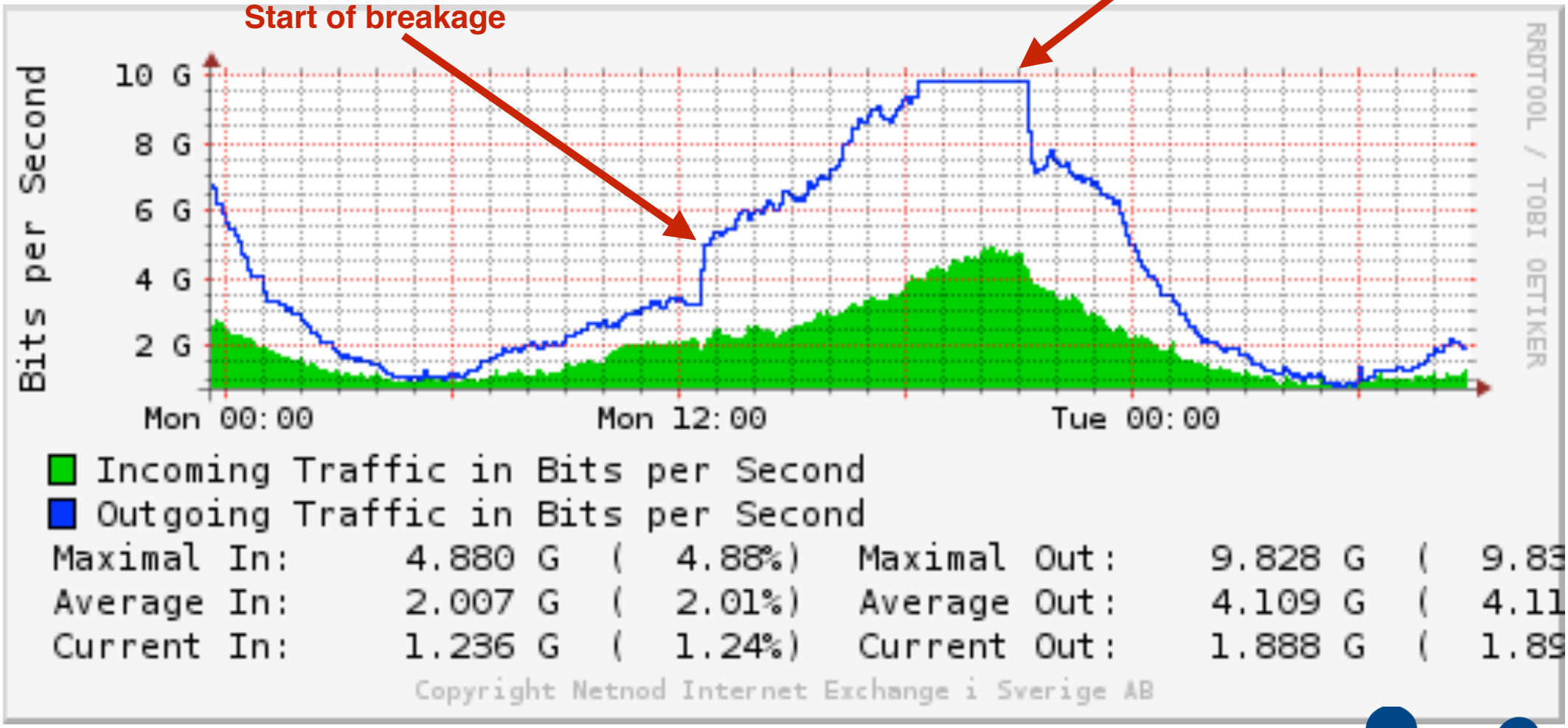



Bits per Second
5.0 G
4.0 G
3.0 G
2.0 G
1.0 G
0.0
Mon 00:00
Mon 12:00
Tue 00:00
RRDTOOL / TOBI OETIKER
Incoming Traffic in Bits per Second
Outgoing Traffic in Bits per Second
Maximal In: 3.085 G (3.08%) Maximal Out: 4.479 G (4.48
Average In: 873.846 M (0.87%) Average Out: 1.356 G (1.36
Current In: 831.853 M (0.83%) Current Out: 1.651 G (1.65
Copyright Netnod Internet Exchange i Sverige AB


Bits per Second
10 G
8 G
6 G
4 G
2 G
Mon 00:00
Mon 12:00
Tue 00:00
RRDTOOL / TOBI OETIKER
Incoming Traffic in Bits per Second
Outgoing Traffic in Bits per Second
Maximal In: 4.880 G (4.88%) Maximal Out: 9.828 G (9.83
Average In: 2.007 G (2.01%) Average Out: 4.109 G (4.11
Current In: 1.236 G (1.24%) Current Out: 1.888 G (1.89
Copyright Netnod Internet Exchange i Sverige AB


Start of breakage
Bits per Second
10 G
8 G
6 G
4 G
2 G
Mon 00:00
Mon 12:00
Tue 00:00
RRDTOOL / TOBI OETIKER
Incoming Traffic in Bits per Second
Outgoing Traffic in Bits per Second
Maximal In: 4.880 G (4.88%) Maximal Out: 9.828 G (9.83
Average In: 2.007 G (2.01%) Average Out: 4.109 G (4.11
Current In: 1.236 G (1.24%) Current Out: 1.888 G (1.89
Copyright Netnod Internet Exchange i Sverige AB

Clear sign of packet drop in network



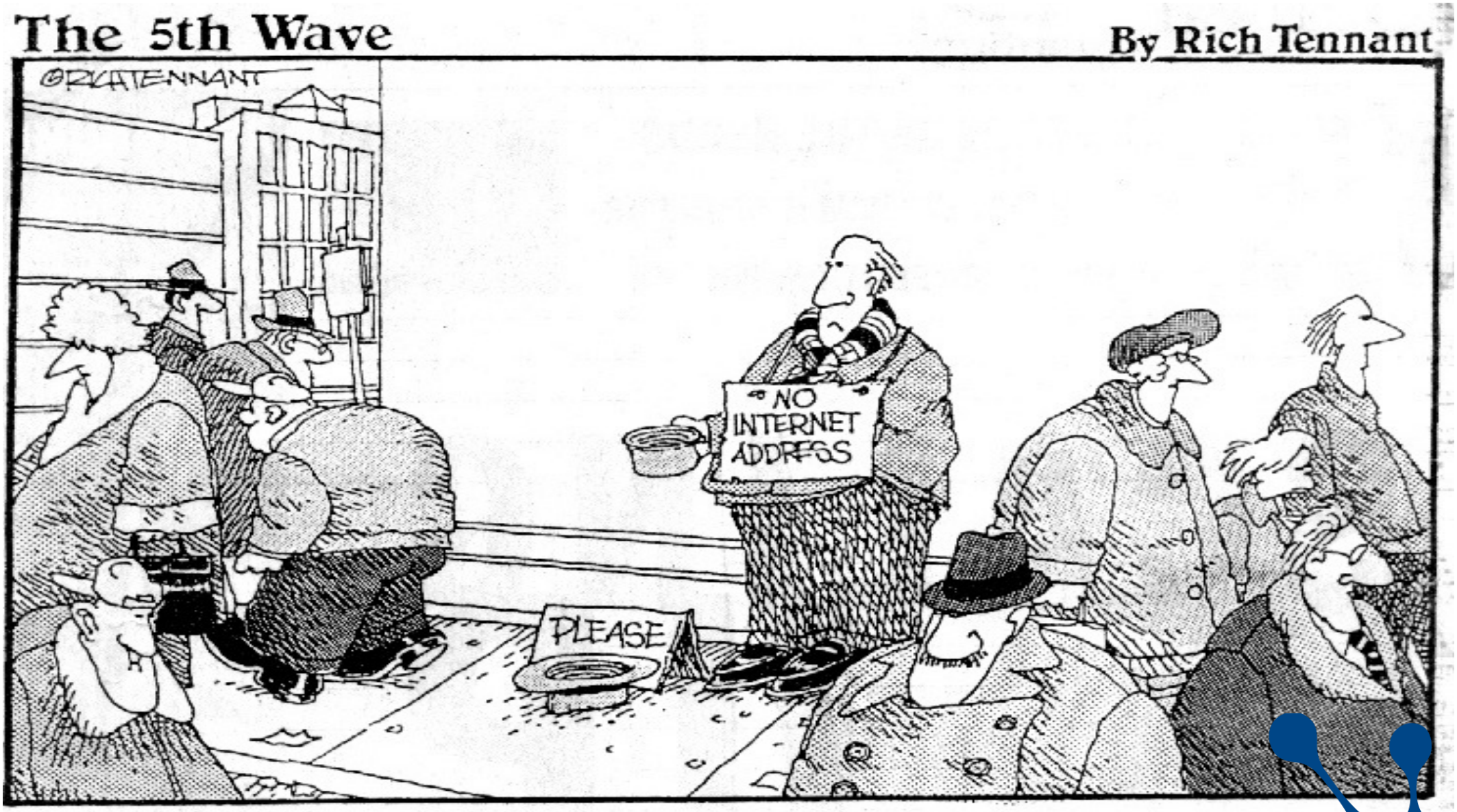
Bits per Second
BRUTOOL / TOOT OPTIVER
33
11
39

Lessons learned

Lesson 1: Build a redundant, robust network!

EXAMPLE — IPV6

Is there anybody out there?

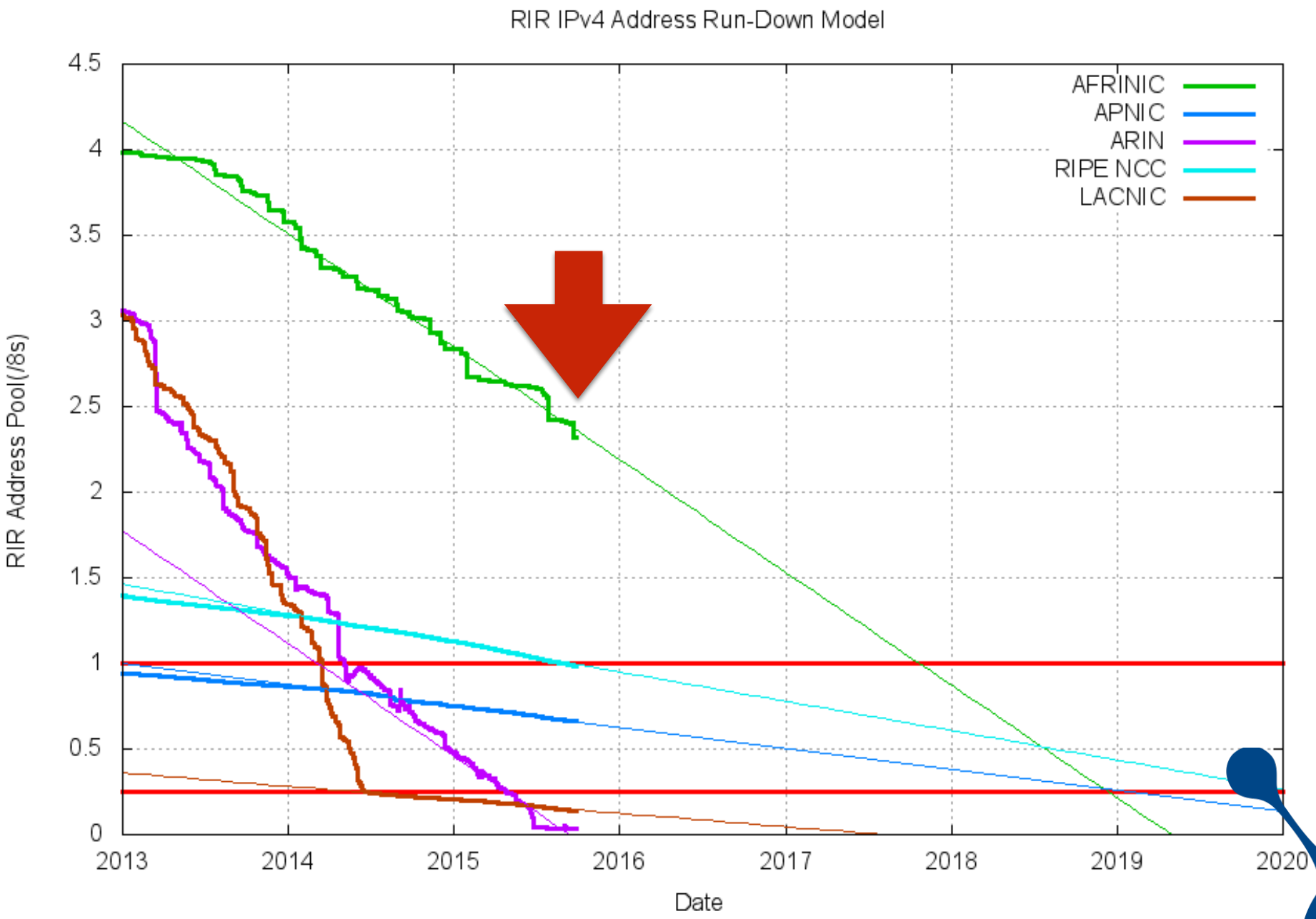

The 5th Wave
By Rich Tennant
©RICHTENNANT
NO INTERNET ADDRESS
PLEASE

Addressing

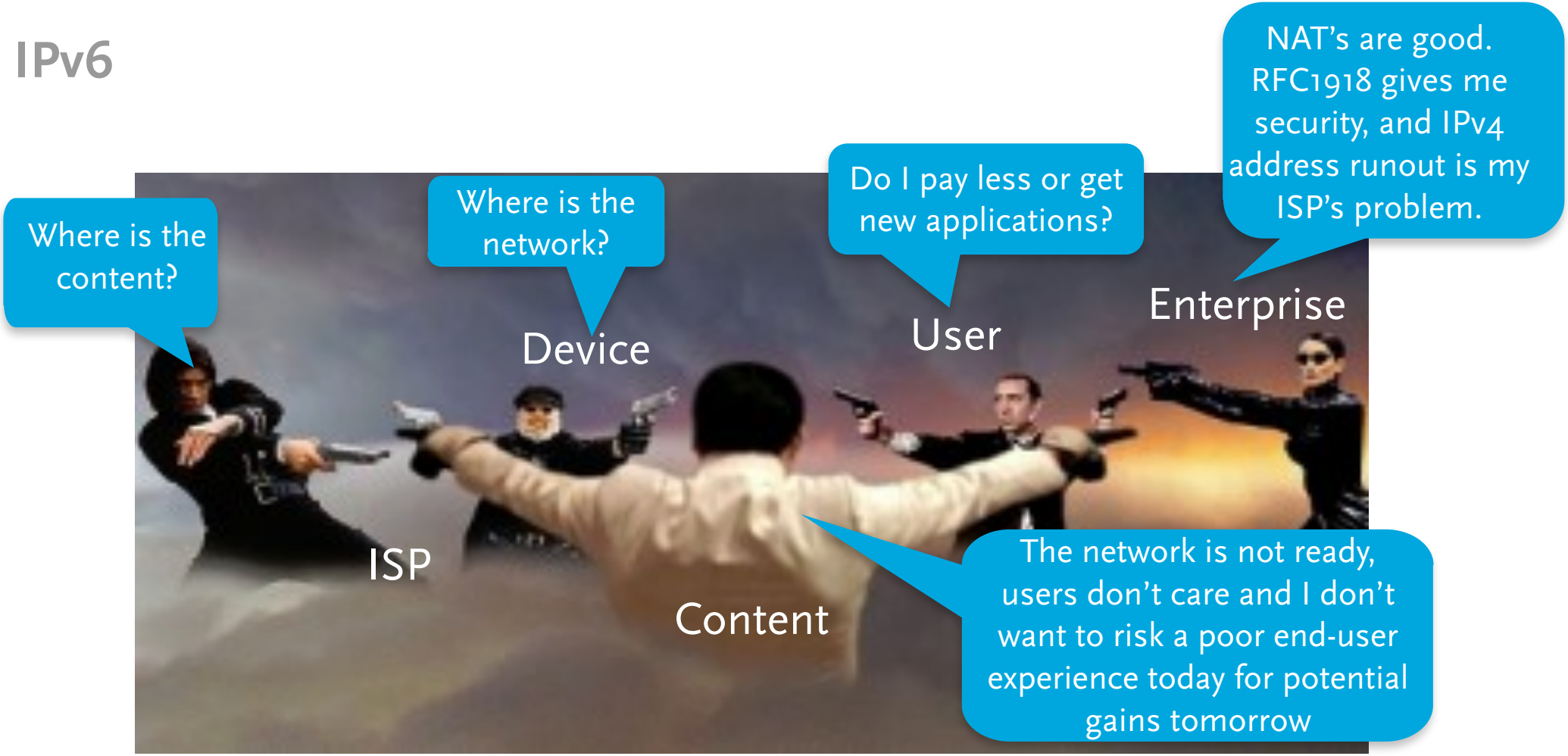
We are running out of IPv4 addresses!
Have we not heard this before?
Yes, but...

It is harder and harder to get IPv4 addresses
1. Create a LIR, pay €3000/year and get one (1) /22
2. Buy a company that have IPv4 addresses
3. Buy addresses on the open market $10/address

Why?


RIR IPv4 Address Run-Down Model
RIR Address Pool(/8s)
Date
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
2013
2014
2015
2016
2017
2018
2019
2020
AFRINIC
APNIC
ARIN
RIPE NCC
LACNIC

IPv6



"A deadlock, stalemate, impasse; a roughly equal (and frequently unsatisfactory) outcome to a conflict in which there is no clear winner or loser,"

Addressing, move from IPv4 to IPv6

Phase 1

Anyone can get addresses from their RIR/LIR

Phase 2

Anyone can buy addresses
Increased number of use of unannounced IP address space

Phase 3

Prices for addresses turns out to be very high
People start using others addresses

Addressing, move from IPv4 to IPv6

Phase 1

Anyone can get addresses from their RIR/LIR

Phase 2

Anyone can buy addresses
Increased number of use of unannounced IP address space

Phase 3

Prices for addresses turns out to be very high
People start using others addresses

Lessons learned

Lesson 1: Build a redundant, robust network!
Lesson 2: Use IPv6, everywhere!

EXAMPLE — CERTIFICATES

Is this a valid page?

What names are in use?

Look at root servers and resolvers?

- **We had a look at i-root during 24 hours**

162 million unique TLDs queried for
65 million are 10 characters long
Created real problems even counting the counters...memory issues...

- **Easy to look at the most common ones**

What do the long tail say?
Look at RD flag and QType?
Other things?

com	298667604
net	170919539
local	115912656
home	45600753
org	43616366
internal	42269815
localdomain	27669054
arpa	27178051
localhost	22019549
lan	18476248
domain	17505162
ru	174[illegible]

Example: Internal Server Names

Designed for “internal only” type applications.

- **Often used by Microsoft Exchange, Active Directory:**

www.corp, www.accounting, mail.test

Doesn’t end in a TLD

- **Can’t be used on the Internet**
- **Nowhere to send the validation email**

Until a TLD is created with that name

Certificate request

```
Data:
 Version: 0 (0x0)
  Subject: C=US, ST=VA, L=Dulles,
    O=Dulles Steel and Forge Supplies,
    OU=IT - Internal WWW Site.,
    CN=www.site/emailAddress=paf@frobbit.se
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
      Modulus (2048 bit):
        00:da:ef:bd:d0:ee:db:...
```

Helpful...

Manage Certificates | Tools | Help | New Features | Repository | Report EV Abuse | Feedback

1-year Standard SSL

Select | Submit | What now?

Where is your certificate going to be hosted?

- Web Hosting, Grid Hosting, Website Builder, Quick Shopping cart, or Dream Design Team
- Dedicated Server or Virtual Dedicated Server, with Simple Control Panel
- Third Party, or Dedicated Server or Virtual Dedicated Server, without Simple Control Panel

Enter your Certificate Signing Request (CSR) below: CSR Help


```
-----END CERTIFICATE REQUEST-----
```


Certificate issuing organization: Learn more

Go Daddy

The requested common name, **www.site**, is not a fully-qualified common name, and must be used on an internal server. Please confirm that this certificate is not meant to be World Wide Web-accessible, otherwise please use a fully-qualified common name.

☑ This certificate will be used on an internal server

Effective August 8, 2011, some certificates will require re-validation every three years. For more information, please click here to review the Subscriber Agreement.

Next | Cancel

Thanks!

Certificate:

Version: 3 (0x2)
Serial Number:
27:e7:22:63:59:11:b0
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=Arizona, L=Scottsdale,
O=GoDaddy.com, Inc., OU=http://certificates.godaddy.com/repository, CN=G
Daddy Secure Certification Authority/serialNumber=07969287
Validity
Not Before: Oct 2 23:56:35 2012 GMT
Not After : Oct 2 23:56:35 2013 GMT
Subject: O=www.site, OU=Domain Control Validated,
CN=www.site
X509v3 Subject Alternative Name:
DNS:www.site, DNS:site

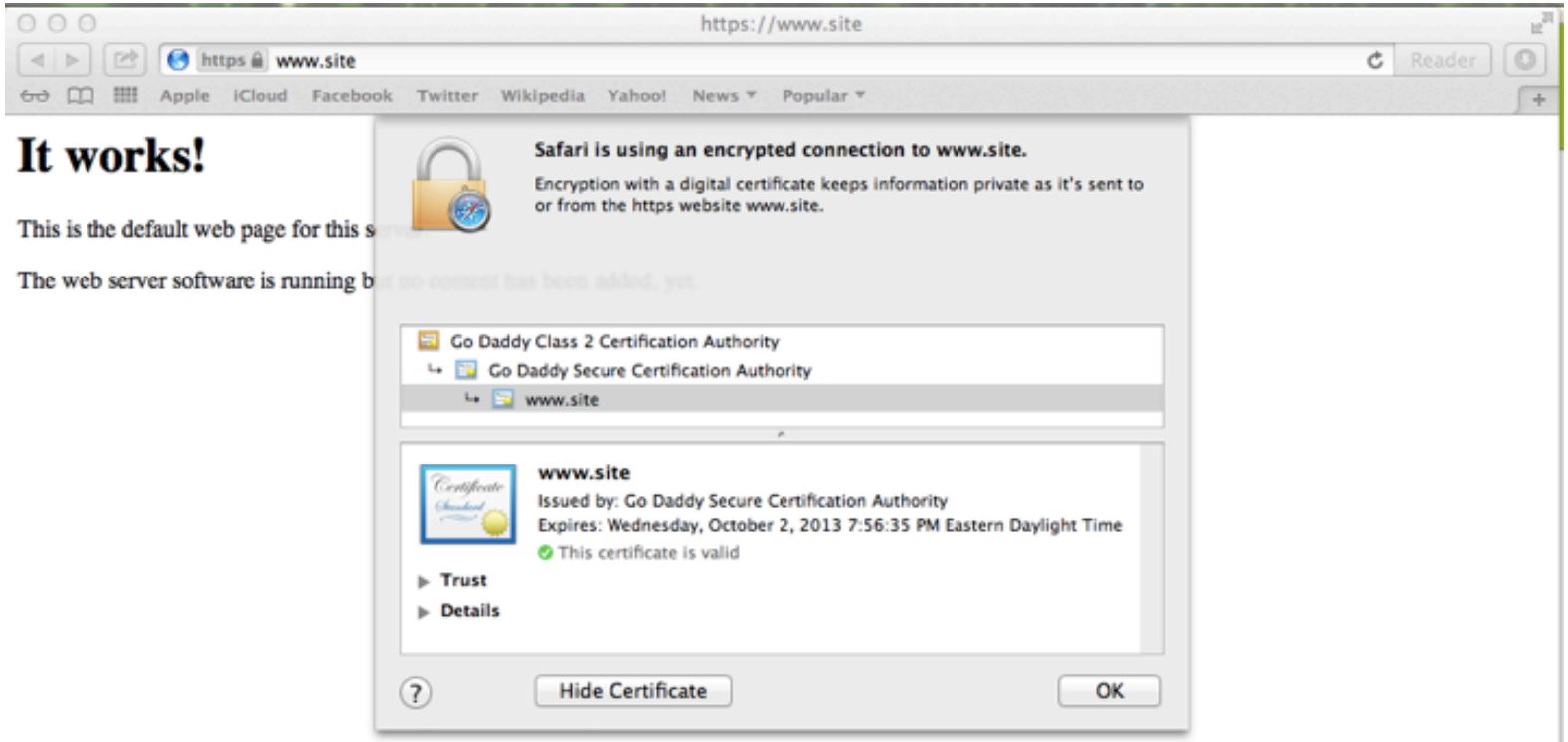
Testing

Setup a fake root

Delegated **.site** to myself

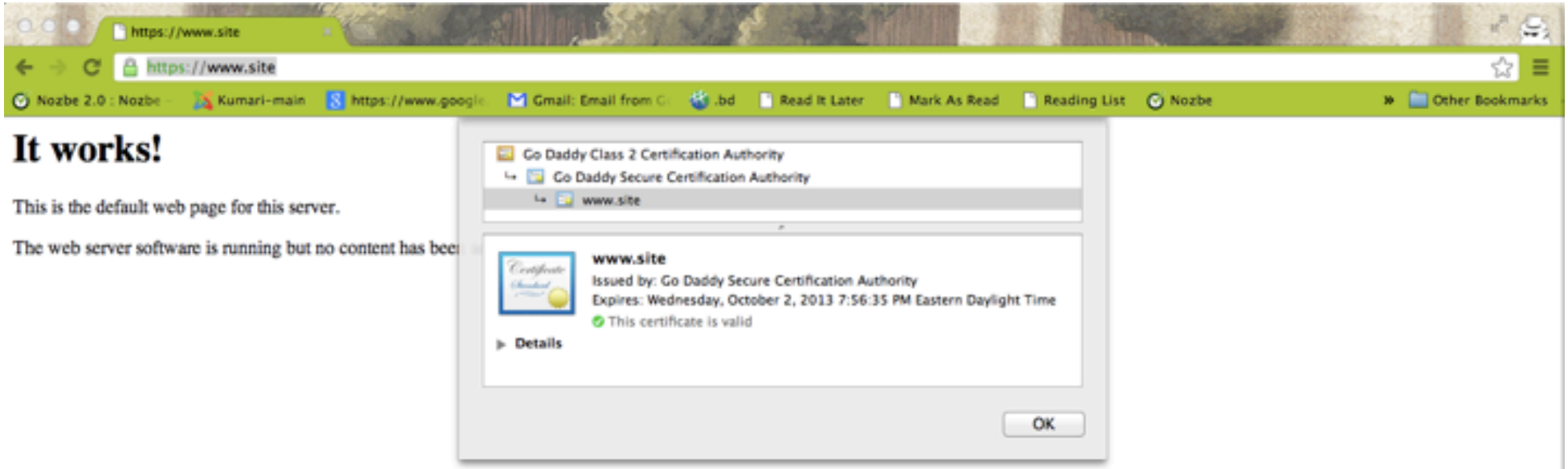
Setup a webserver, serving the cert

Doh!


https://www.site
https www.site
Reader
Apple iCloud Facebook Twitter Wikipedia Yahoo! News Popular
It works!
This is the default web page for this s
The web server software is running b
Safari is using an encrypted connection to www.site.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.site.
Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
www.site
www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time
This certificate is valid
Trust
Details
Hide Certificate
OK

Doh!

Doh!


https://www.site
https://www.site
Nozbe 2.0 : Nozbe
Kumari-main
https://www.google
Gmail: Email from G
.bd
Read It Later
Mark As Read
Reading List
Nozbe
Other Bookmarks
It works!
This is the default web page for this server.
The web server software is running but no content has bee
Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
www.site
www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time
This certificate is valid
Details
OK

Investigations by SSAC

SSAC formed a work party

Researched prevalence of non-FQDN certs

- Using the EFF SSL Observatory data
  - **At least 157 CAs have issued such certs**
  - **Lower bounds estimate**
- CA/B Forum is aware of the issue
  - **3 year from signing to revocation**

Conclusion:

- ICANN must immediately do something

ICANN Actions

ICANN Security Team took the lead

- "Coordinated Vulnerability Disclosure"
- Contacted CA/B Forum Chair Jan 23, 2014
- Briefed CA/B Forum Feb 5, 2014
- Ballot 96 at CA/B Forum passed Feb 26, 2014
  - 30 / 120 day period (instead of 3 years)

SAC057 published Mar 15, 2014

- During 120 day period, delegate to 127.0.53.53

Solved? Nope...

Not all CAs are members of the CA/B Forum

- **So not bound by these agreements**
- **But generally trustworthy / follow guidelines**

Revocation ineffective*

- **Blocking CRL / OSCP / air-gapped networks**

* : http://www.imperialviolet.org/2011/03/18/revocation.html

Lessons learned

Lesson 1: Build a redundant, robust network!
Lesson 2: Use IPv6, everywhere!
Lesson 3: Choose certificates and domain names carefully!
Lesson 4: Do not use search path in stub resolvers!

EXAMPLE — HARDWARE

What are you using?

Heart Bleed

Not very nice…

- **Security mechanism itself had issues**
- **One very dominant piece of software**
- **Questionable disclosure policy uses**

I hope we did learn something…

FBI Criminal Investigation: Cisco Routers

The overall classification of this presentation is
UNCLASSIFIED

Section Chief Raul Roldan

Supervisory Special Agent Inez Miyamoto

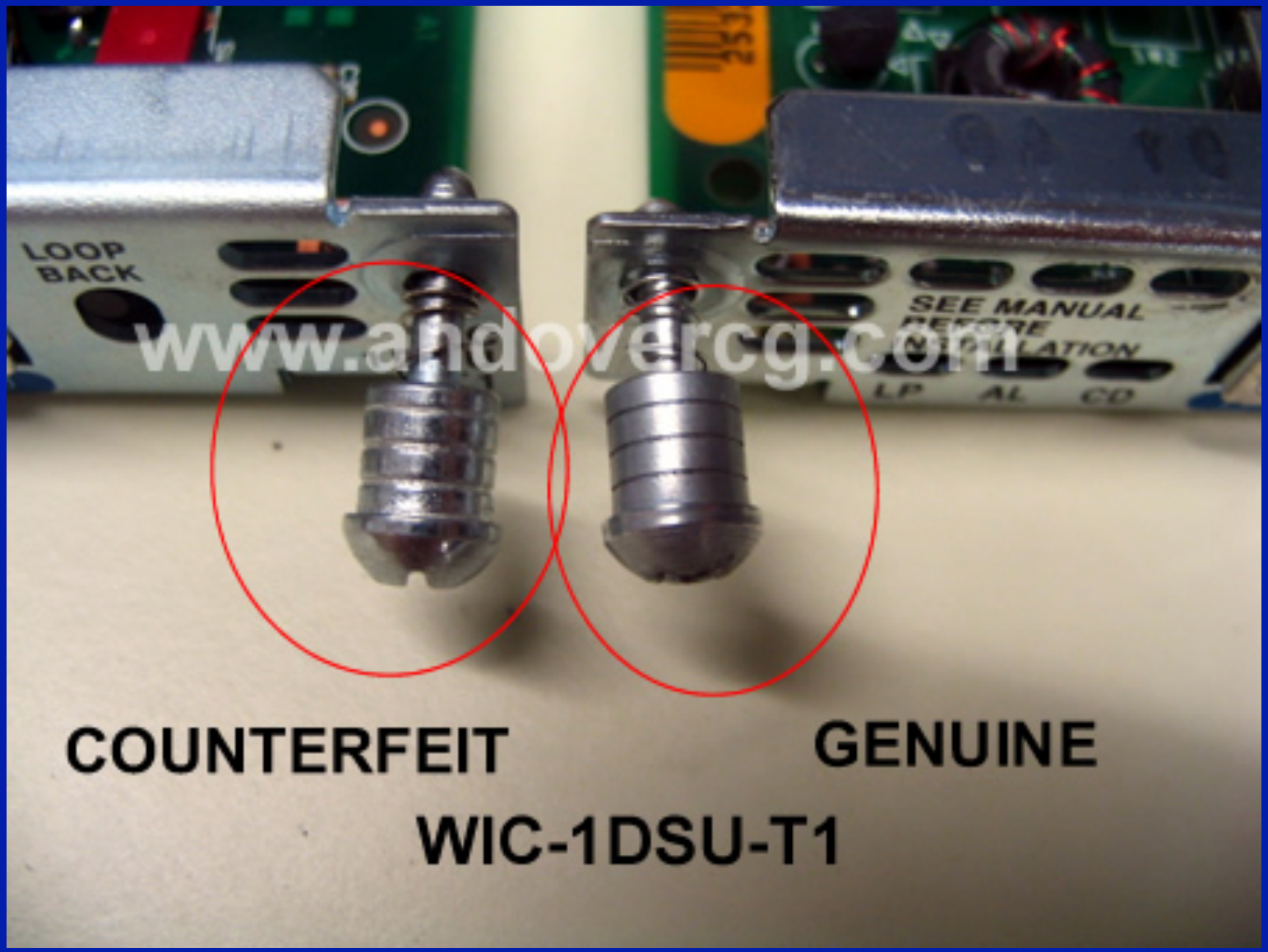
Intelligence Analyst Tini Leon

January 11, 2008

Counterfeit Products

Source: <http://www.usedcisco.com/press-my-esm_used_cisco_identifying_fake_chisco.aspx>

Counterfeit Products



Source: <http://www.usedcisco.com/press-my-esm_used_cisco_identifying_fake_chisco.aspx>

netnod

Hacking News | Malware | Cyber Attack | Vulnerabilities | NSA Spying | e.g. Hacking Fac

The Hacker News™

Security in a serious way

+1,590,250 G+1 1.5M

230,550 Follow

Lenovo Caught (3rd Time) Pre-Installing Spyware on its Laptops

Thursday, September 24, 2015 Swati Khandelwal

G+1 381 Like 5.6k Share 2708 Tweet 1802 Share 50 ShareThis 6637

Lenovo has once again been caught installing spyware on its laptops and workstations without the user's permission or knowledge.

Popular Stories

Aw, Snap! This 1 Can Crash Your

Deleting Whats Before 90 Days Jail

Lenovo Caught (Installing Spywa

iOS 9 Hack: How Photos and Con Passcode

Apple's Biggest Malicious iOS St CIA?

The World's Firs Shipping ay!

Facebo He's Ho to G 'Dis

netnod

Cryptech

CRYPTECH.IS

Trying to make the Internet a little bit safer

Much more nice!

- **CRYPTECH.IS is a loose international collective of engineers trying to improve assurance and privacy on the Internet. It is funded diversely and is administratively quartered outside the US.**
- **...are actively seeking use cases for an initial project which is to produce a design of an open and auditable HSM and supporting software.**
- **...are also considering the issues around assurance of a tool-chain, from compiler to operating system and as close to the hardware as we can reasonably get.**
- **...are seeking collaborative funding.**

Contact Leif Johansson at SUNET!

leifj@sunet.se

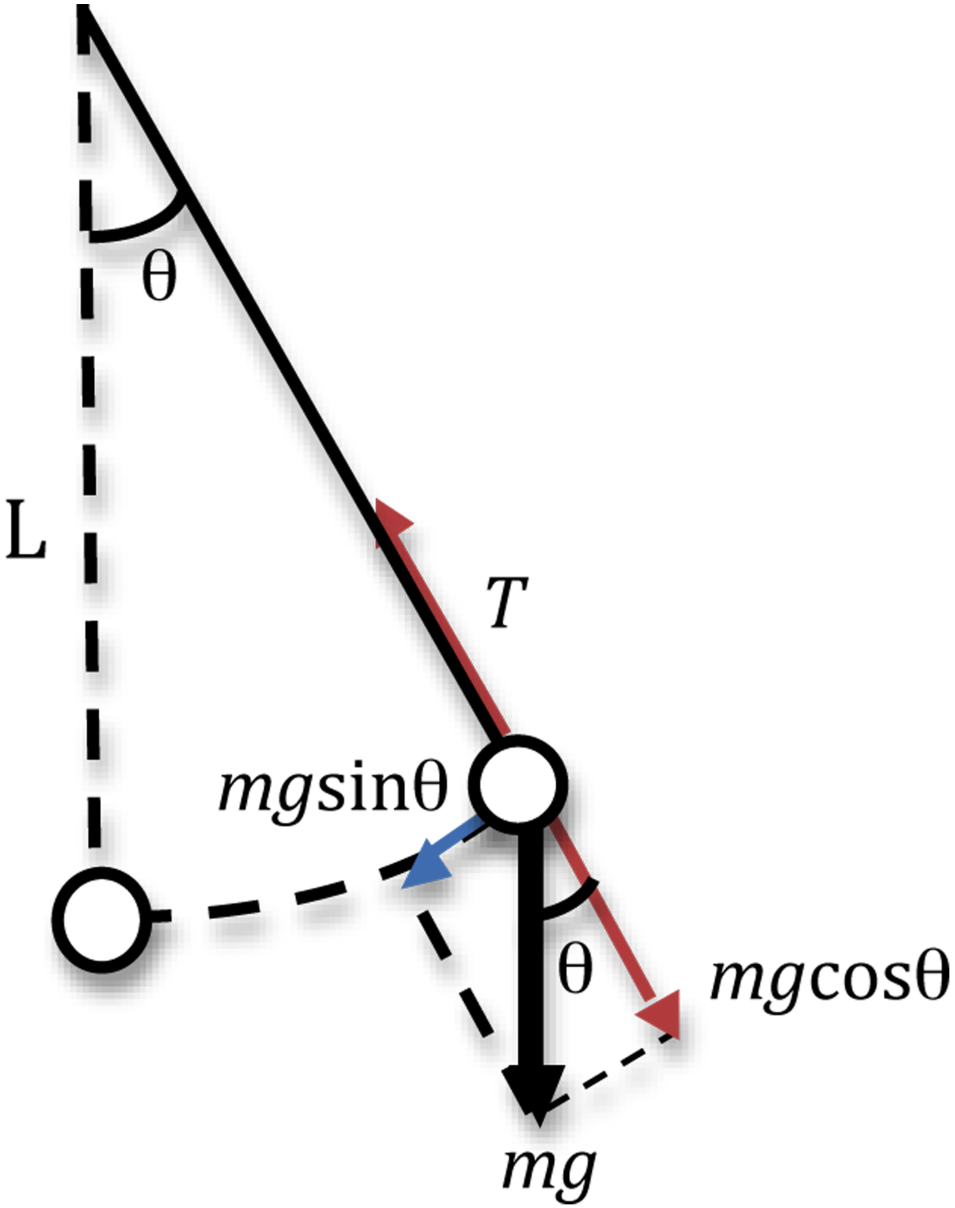
Lessons learned

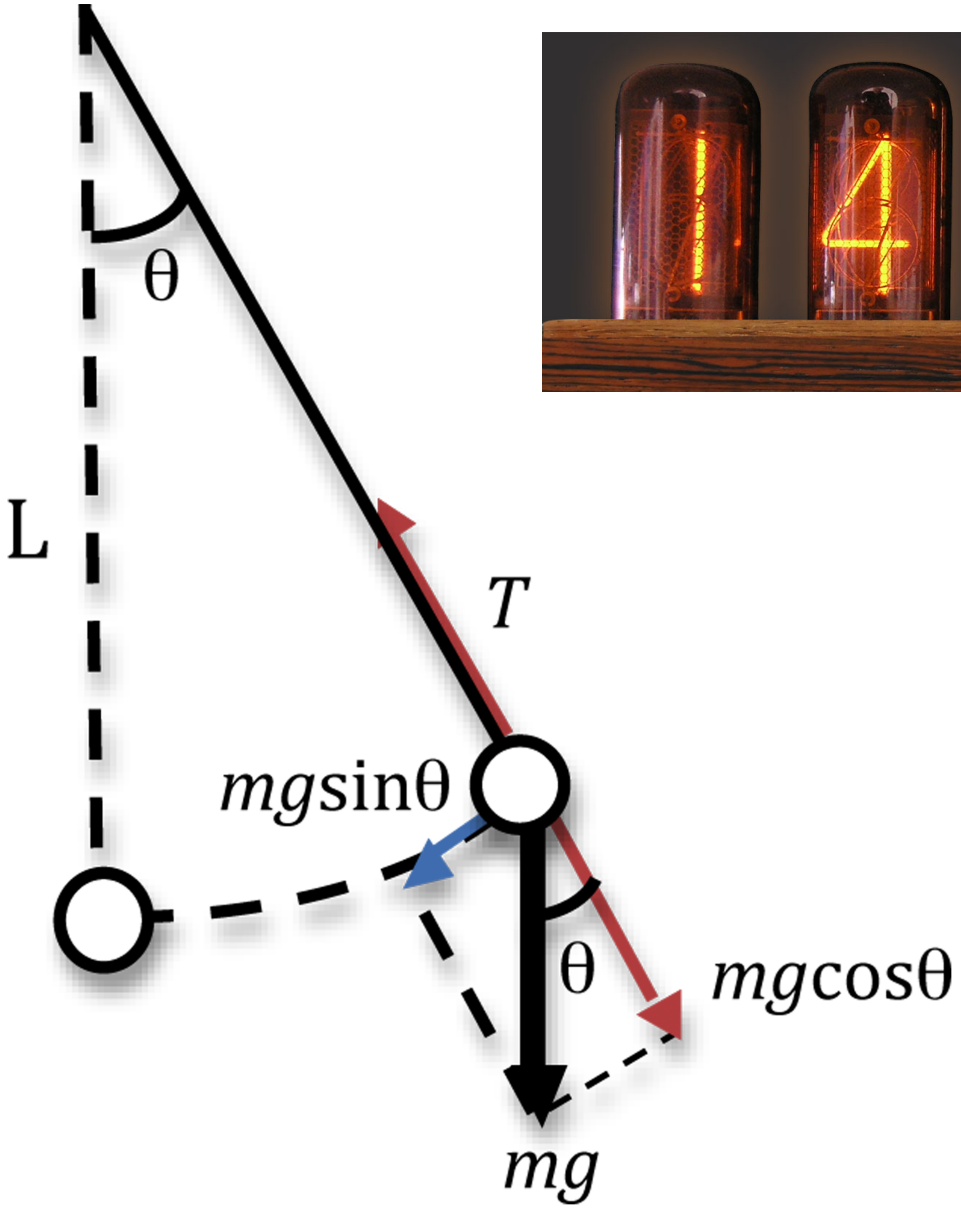
Lesson 1: Build a redundant, robust network!
Lesson 2: Use IPv6, everywhere!
Lesson 3: Choose certificates and domain names carefully!
Lesson 4: Do not use search path in stub resolvers!
Lesson 5: Be careful with what you install!

EXAMPLE — TIME

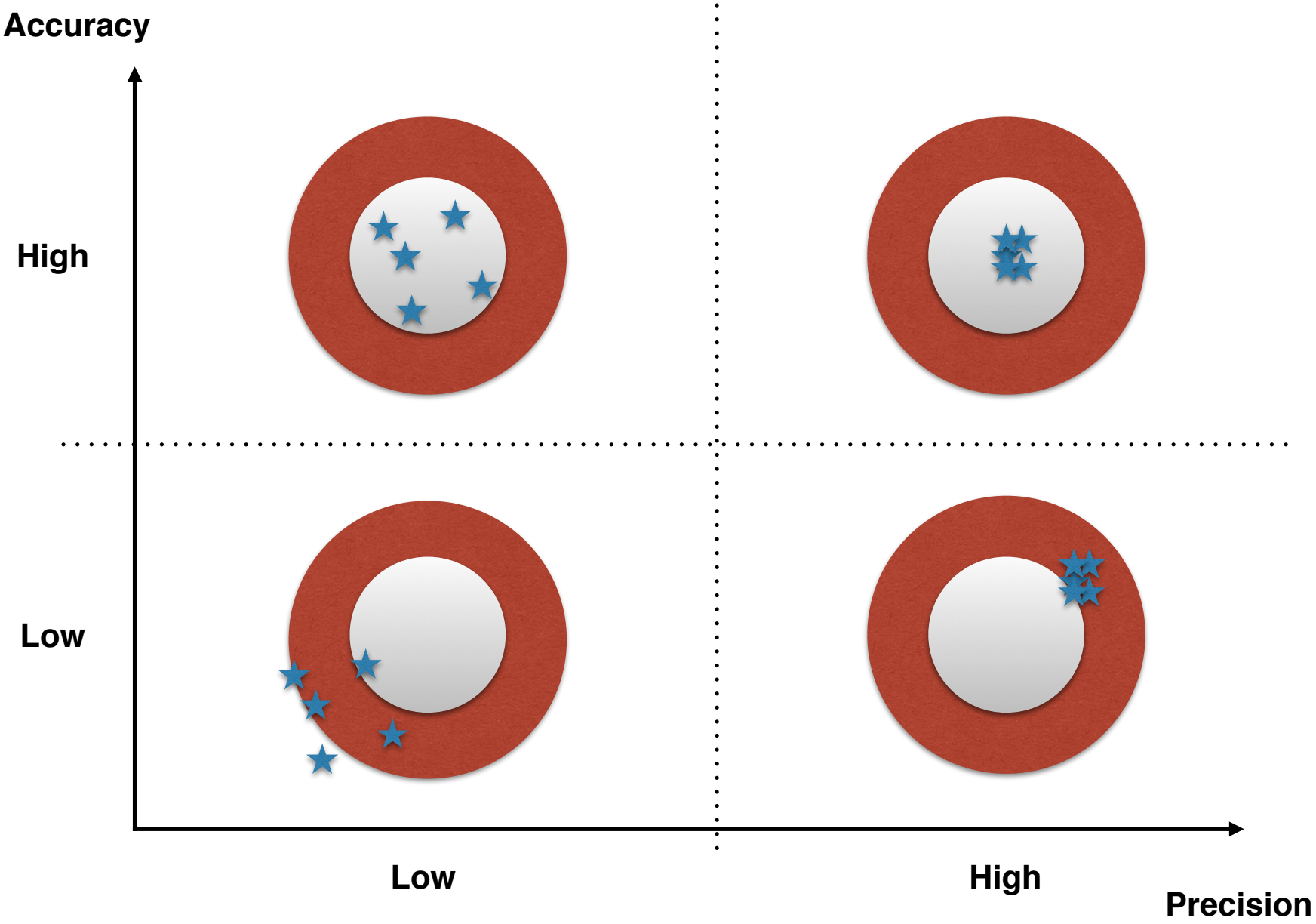
When did things go wrong?

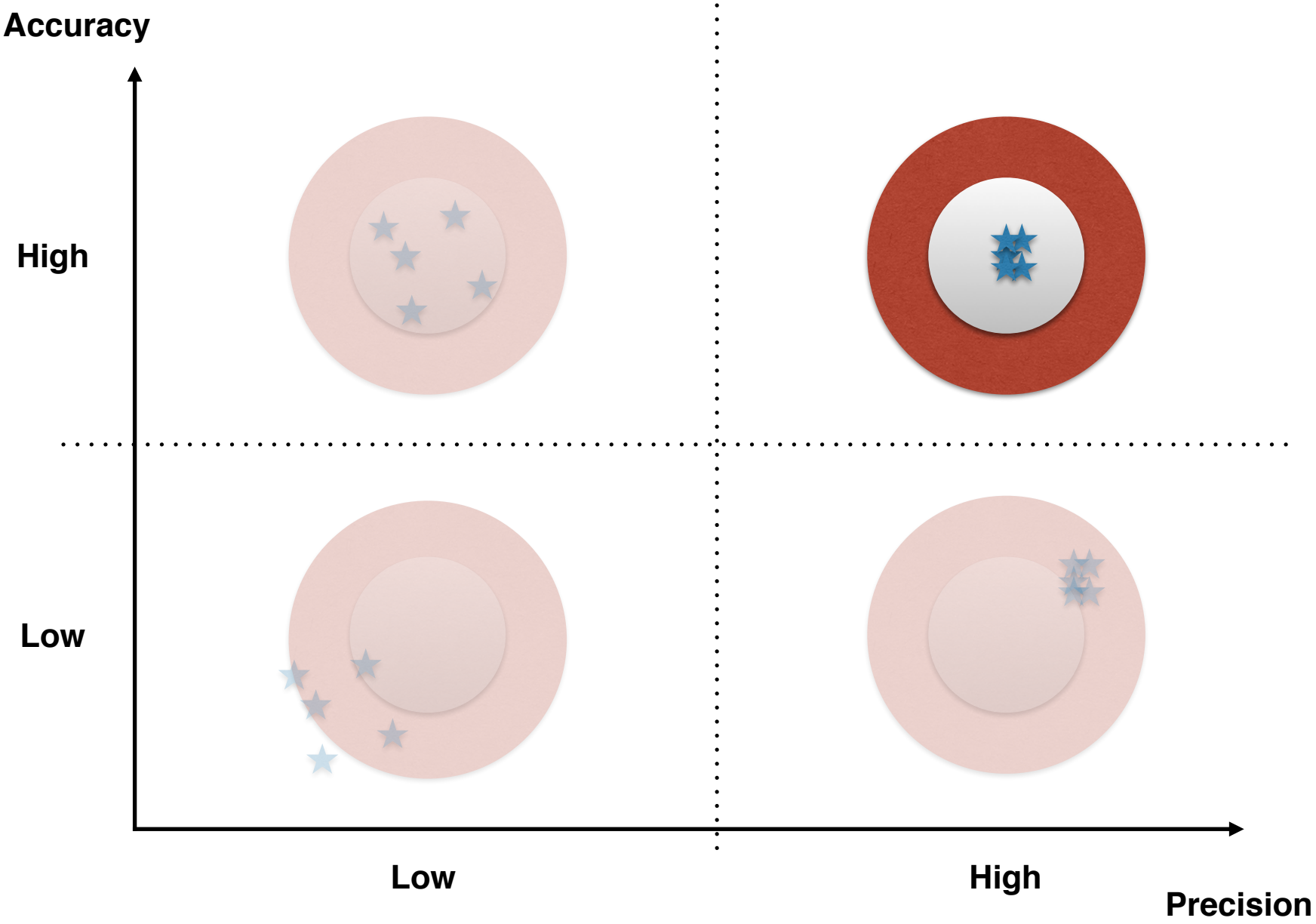

LONDON
MOSKVA
NEW YORK
TOKYO

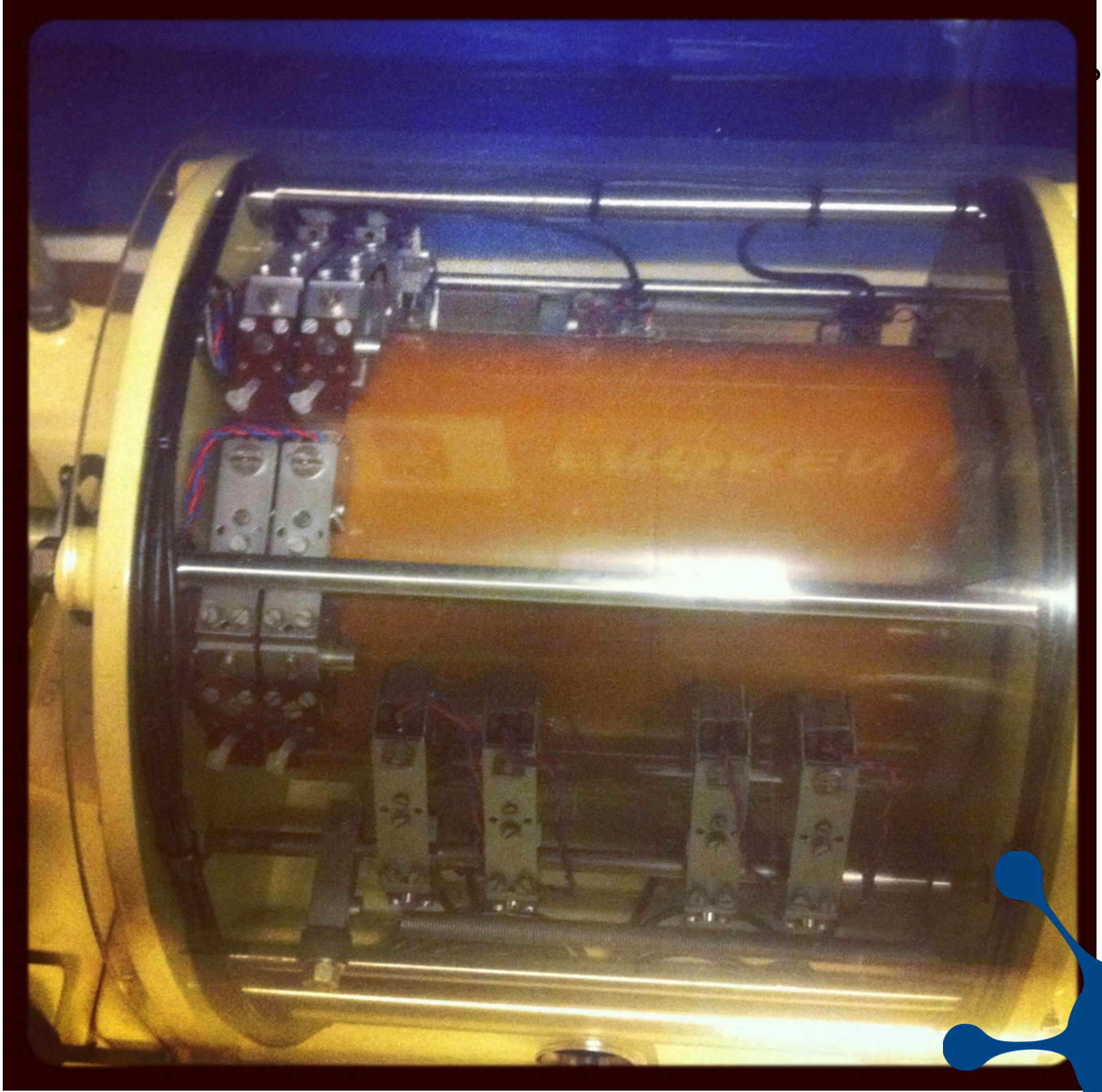

θ
L
T
mgsinθ
θ
mgcosθ
mg


θ
L
T
mgsinθ
θ
mgcosθ
mg

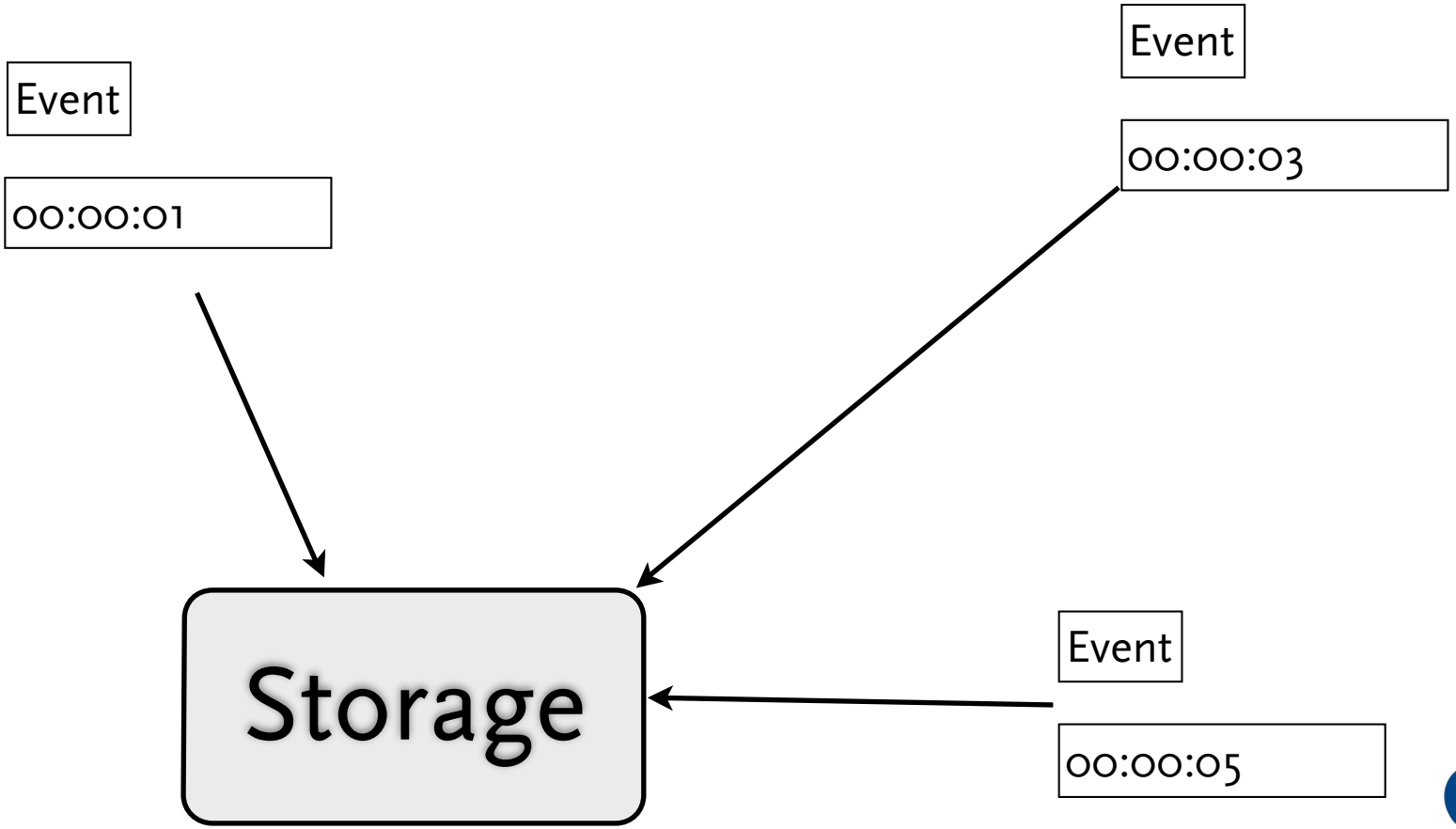

14124


Accuracy
High
Low
Low
High
Precision

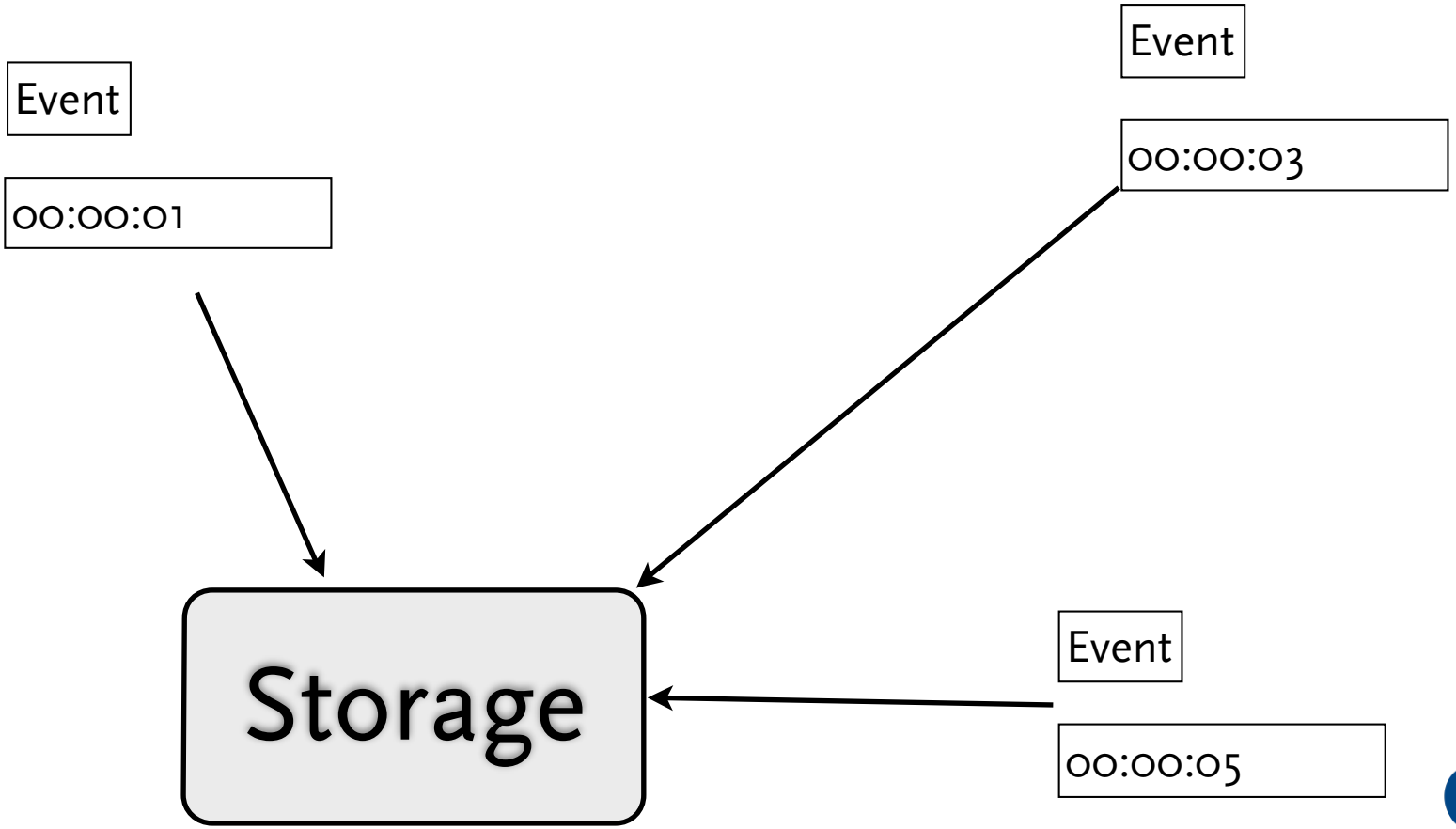

Accuracy
High
Low
Low
High
Precision



Multiple non-synchronized events



Multiple non-synchronized events



In what order did the events take place?

More seriously...

If one have any kind of transaction system, the time stamps must be precise enough that the **order** of the transactions is non-disputable.

1 kap. 5 § Handelsbalken (1736:0123 2):

- **5 § Säljer man tvem ett; gälde skadan åter, (och böte tio daler,) och den behålle godset, som först köpte.**

EuroSOX - Information Lifecycle Management:

- **Operational aspects of ILM include backup and data protection; disaster recovery, restore, and restart; archiving and long-term retention; data replication; and day-to-day processes and procedures necessary to manage a storage architecture.**

Not always easy

Often a second is close enough

In electronic services more precision is needed

There have been a few incidents

- **Procurement was stopped 7 min early**
- **Fax with response to RFP was rejected**
- **Data from surveillance cameras could not (directly) be used**
- **Differentiated charging of road fees**

Not always easy

Often a second is close enough

In electronic services more precision is needed

There have been a few incidents

- **Procurement was stopped 7 min early**
- **Fax with response to RFP was rejected**
- **Data from surveillance cameras could not (directly) be used**
- **Differentiated charging of road fees**

Not

Oft

In e

The

- Pro
- Fax
- Da
- Dif

Space weather and Internet

+We use more and more fiber for transmission

- +We decrease use of copper for transmission
- +We decrease use of satellites and radio links

-Higher speed requires higher precision frequency in end nodes

- ✓We do have to take into account relativity theory

-More players involved require more synchronised timestamps

- ✓We need to agree on what time it is
- -We must be able to have better precision in timestamps

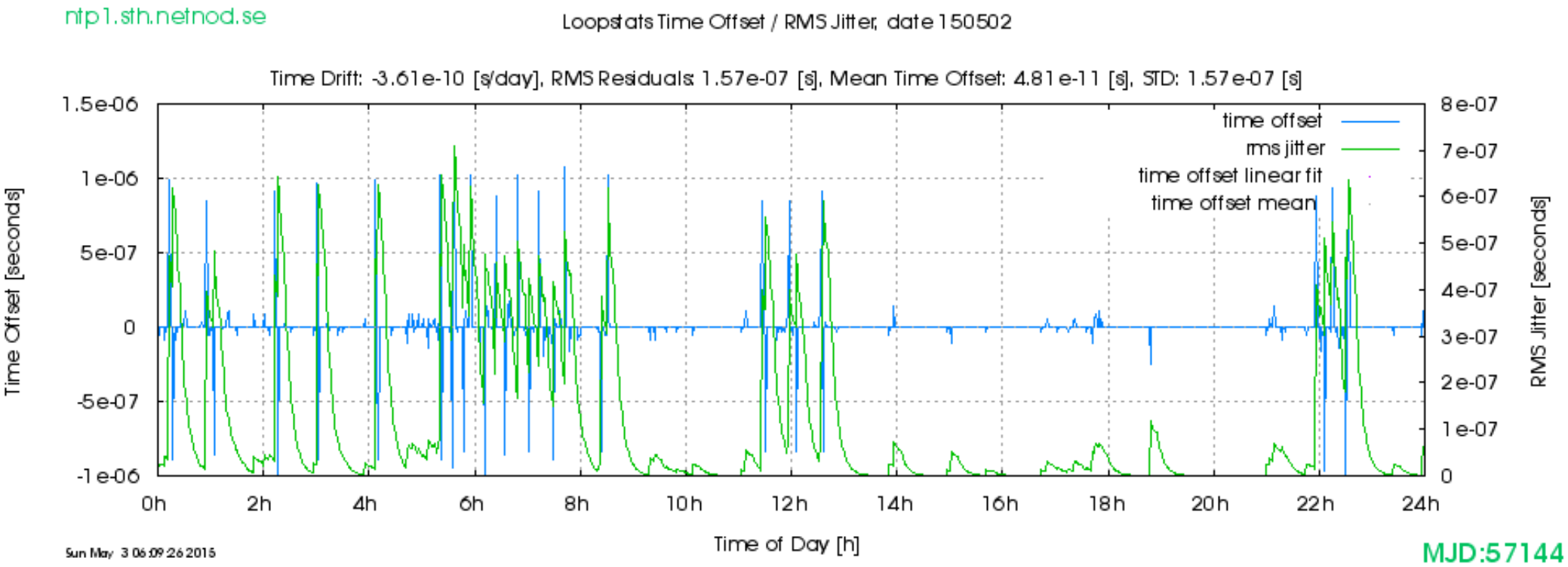
-Increased dependency of GNSS

- -People use more and more GPS
- -Even though transmission is more robust, time distribution is not

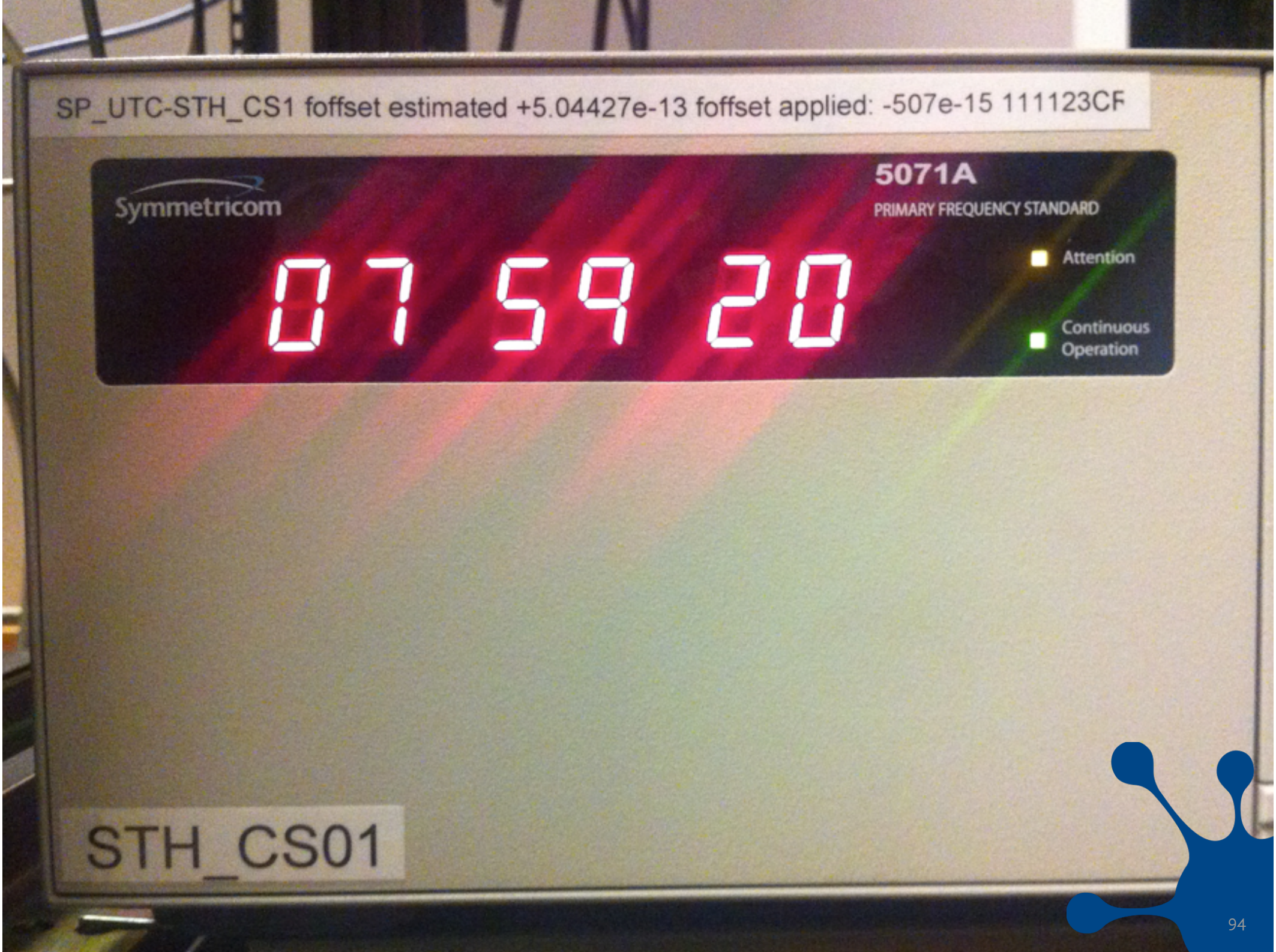
+SAMFI (MSB, PTS etc) have said *Time distribution is important*

- +We at Netnod do what we can to help!

What precision do we reach?



As you can see, we today stay within 10^{-6} seconds
New design is targeted at much better quality


SP_UTC-STH_CS1 foffset estimated +5.04427e-13 foffset applied: -507e-15 111123CF
Symmetricom
5071A
PRIMARY FREQUENCY STANDARD
07 59 20
Attention
Continuous Operation
STH_CS01

Lessons learned

Lesson 1: Build a redundant, robust network!
Lesson 2: Use IPv6, everywhere!
Lesson 3: Choose certificates and domain names carefully!
Lesson 4: Do not use search path in stub resolvers!
Lesson 5: Be careful with what you install!
Lesson 6: Use a reliable time source!

References:

From Sundials to Atomic Clocks: Understanding Time and Frequency, Jespersen, James and Jane Fitz-Randolph, (http://tf.nist.gov/general/pdf/1796.pdf – 26 MB, 306 pages) 2nd (revised) edition, Mineola, New York: Dover Publications, 1999 ISBN 0-16-050010-9

Longitude: The True Story of a Lone Genius Who Solved the Greatest Scientific Problem of His Time, Dava Sobel 1995, Walker Publishing Company, Inc., New York, ISBN 0-8027-1312-2

Elektronisk signering, En antologi, Redaktör: Jon Kihlman. Stockholm, Sweden: Nordstedts Juridik, 2013. ISBN: 978-913901731-8

Patrik Fältström - paf@netnod.se