IPv6 hálózatmenedzsment - NetFlow v9 architektúrával

Campus IPv6 Workshop, Budapest

András Kovács, NIIF <akov@niif.hu>
János Mohácsi, NIIF <mohacsi@niif.hu>

2006.09.28.

IPv6 hálózatmenedzsment

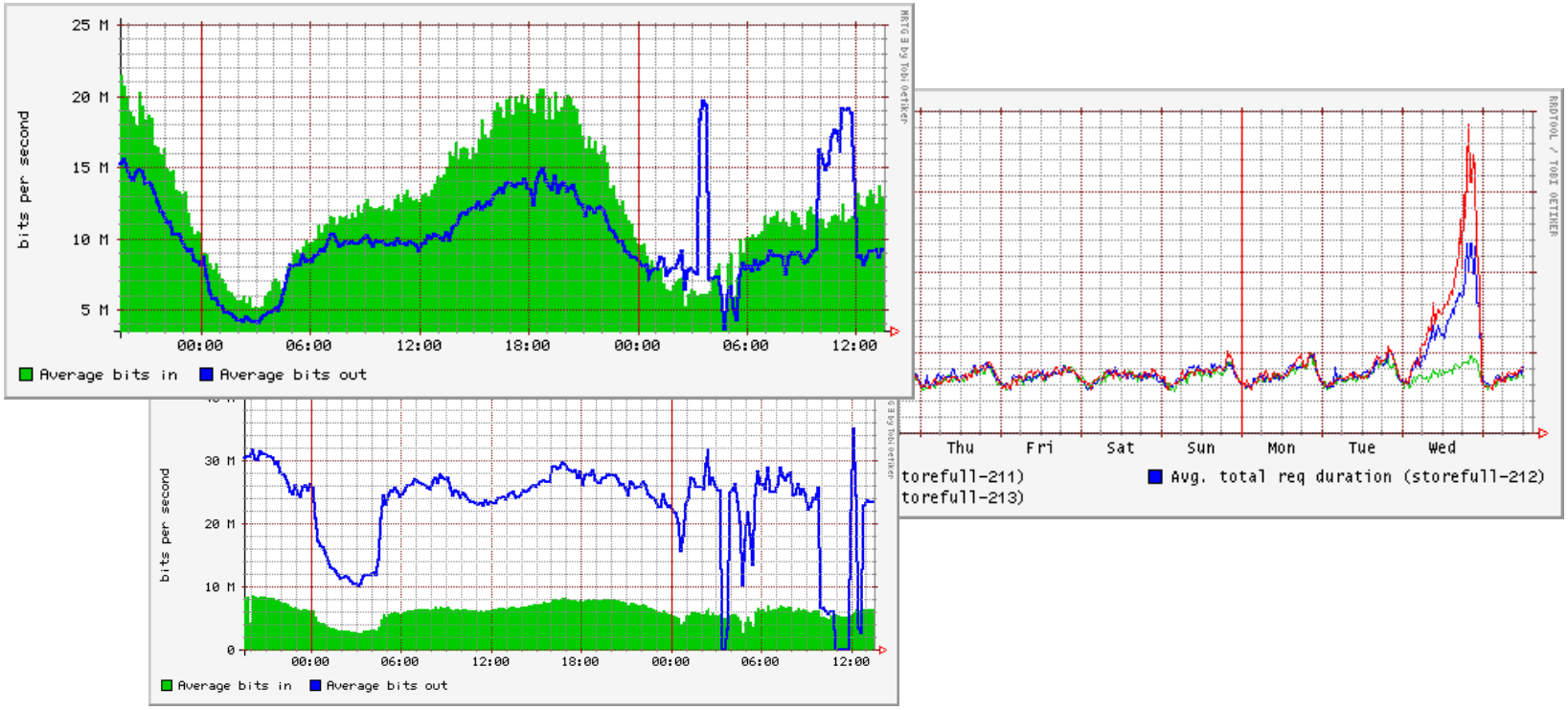
- Hálózat menedzsment
  - Leltár jellegű nyilvántartás az eszközökről és HW/SW konfigurációjukról
  - Topológia
  - Biztonság
  - Felügyelet
  - Jelentés készítés az SLA szerint
- IPv6?
  - Dual stack IPv6 hálózat – viszonylag egyszerű
  - Csak IPv6 – jelenleg nem jelentős
- Egyszer az IPv4-et már nem lesz érdemes megtartani
  - Képesnek kell lenni IPv6-on menedszselni a hálózatot

Dualstack hálózatmenedzsment

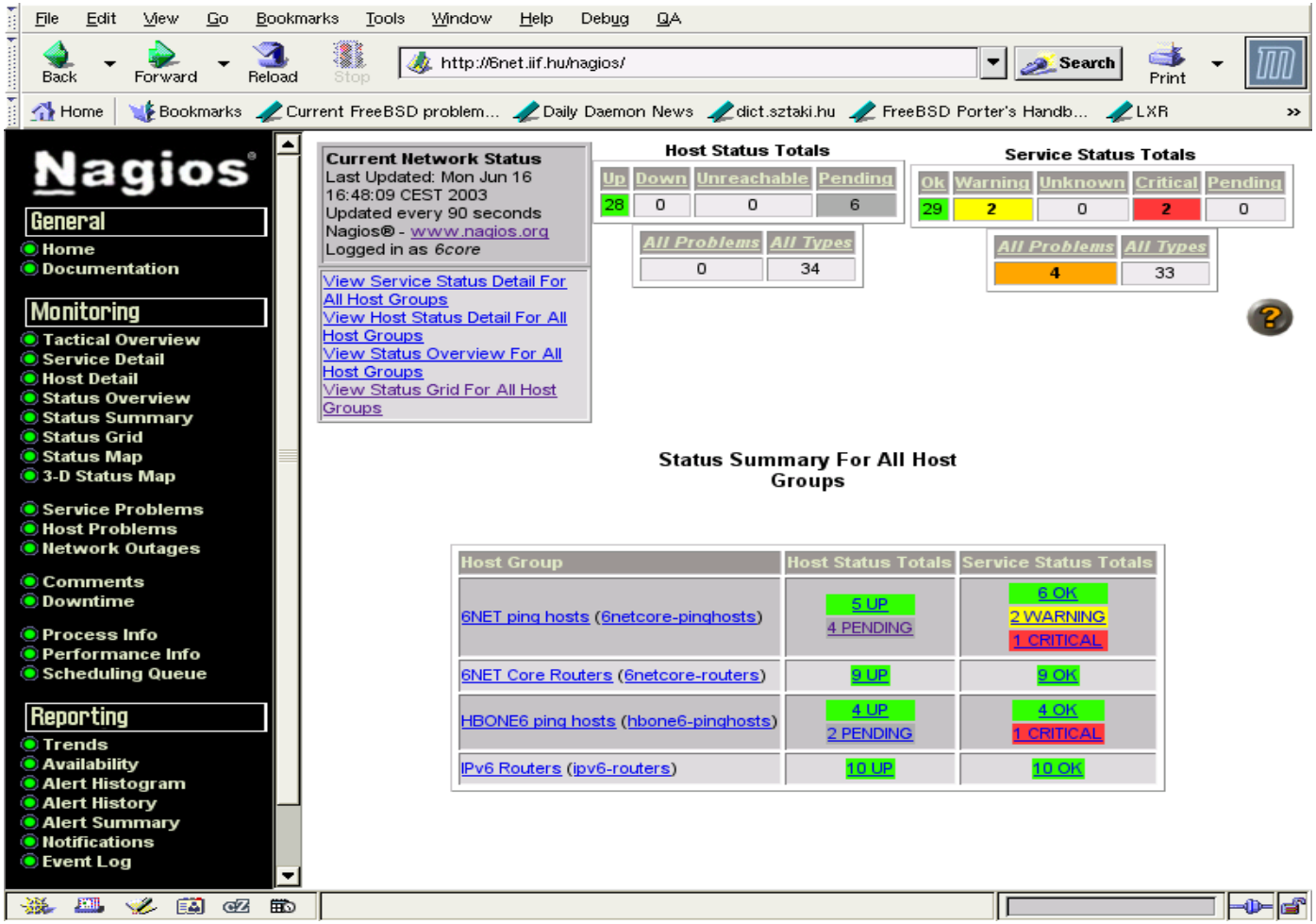
- A hálózat menedzsment egy része mehet IPv4-en – de mehet IPv6-on is
  - Konnektivitás (telnet/ssh)
  - Menedzsment eszközök: leltár, konfiguráció, számlálók, routing információk – SNMP MIB
- Ami mindenképen szükséges
  - MIBs IPv6 támogatás
  - NetFlow (v9)
  - Eszközök IPv6-os címeket támogató változata

IPv6 forgalom mérés -Cricket / MRTG

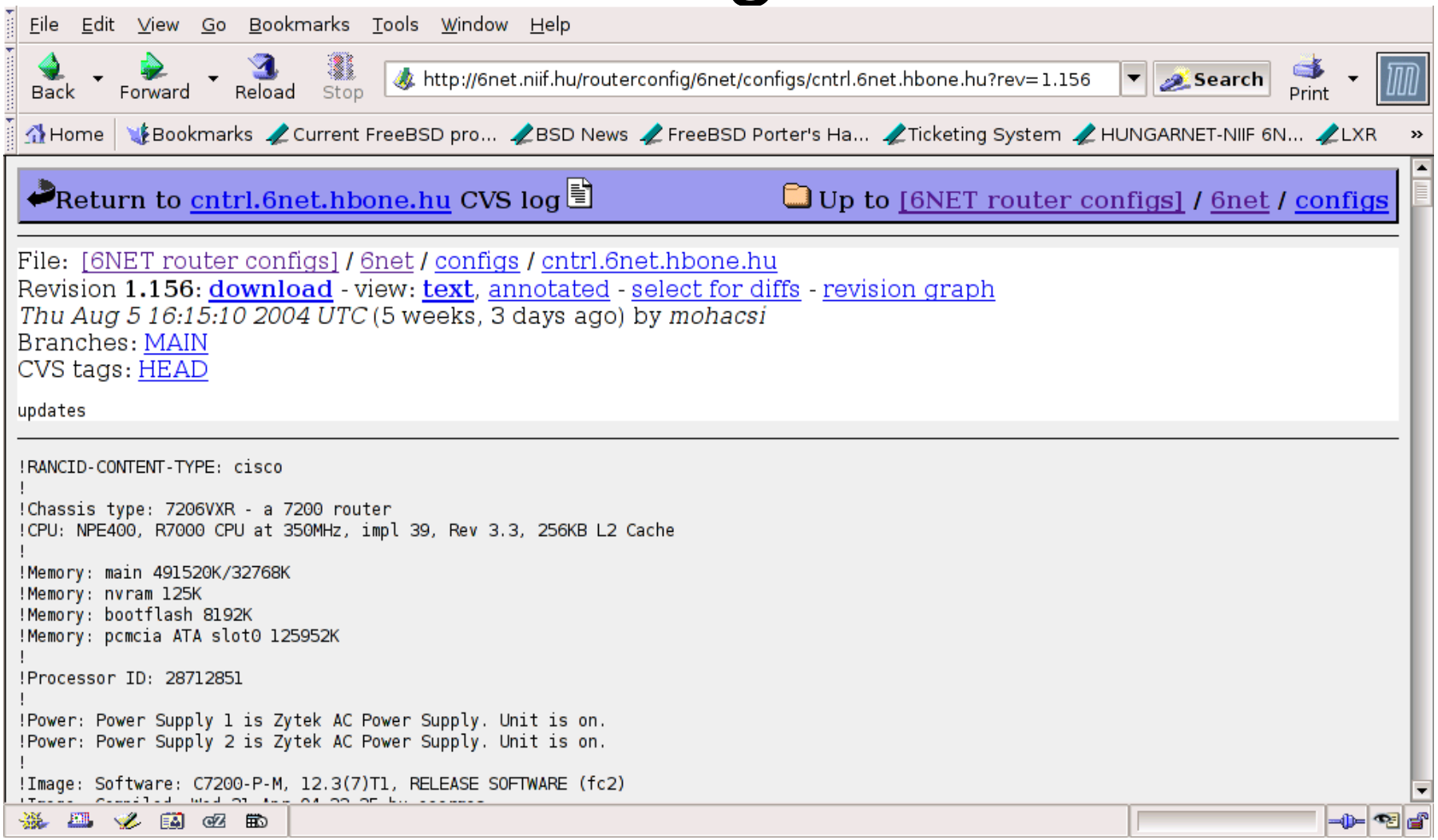
- IPv6-os forgalom külön mérése – MIB definiált – implmentáció nincs



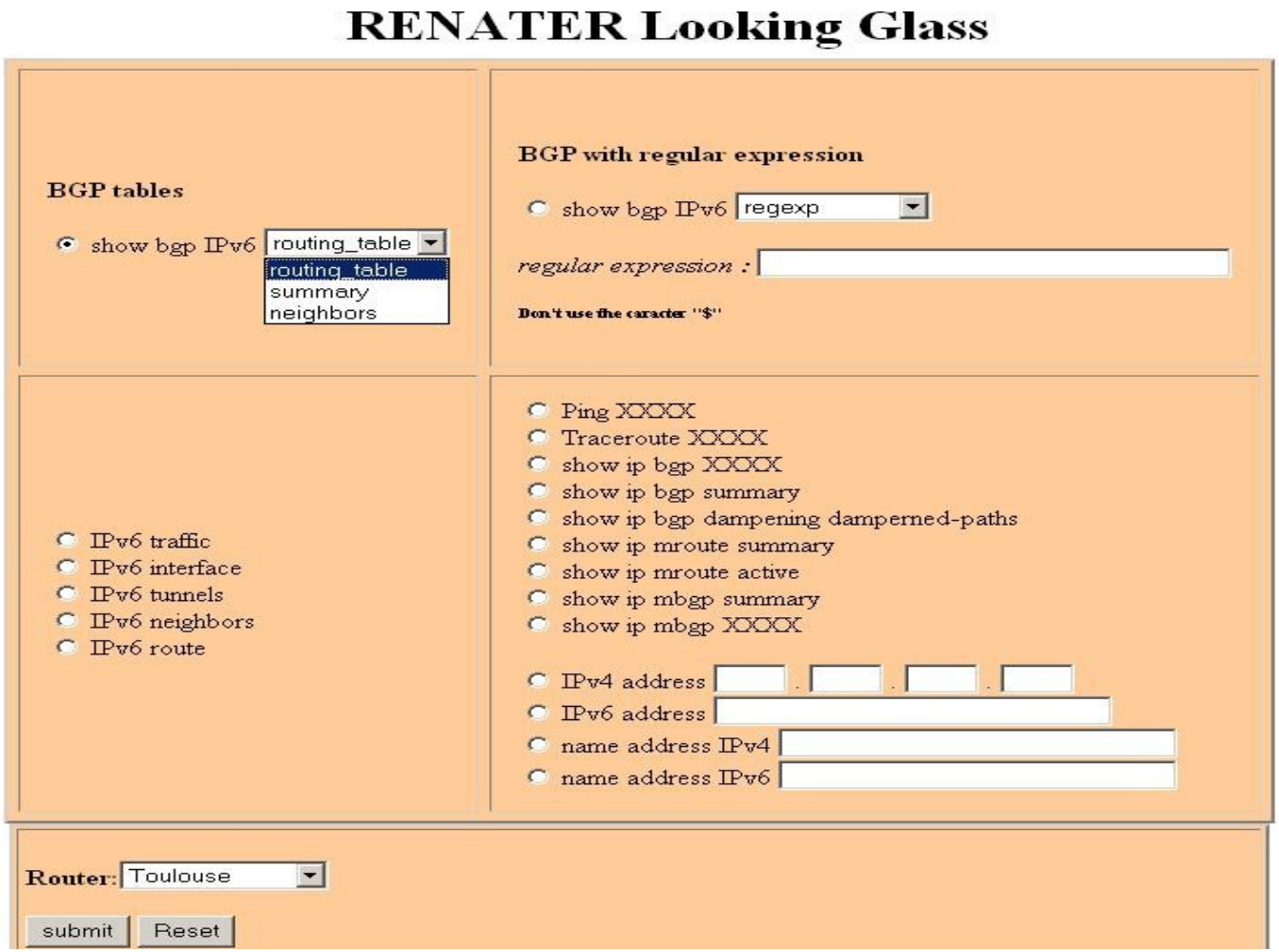
Nagios IPv6


File Edit View Go Bookmarks Tools Window Help Debug QA
Back Forward Reload Stop
http://6net.iif.hu/nagios/
Search Print
Home Bookmarks Current FreeBSD problem... Daily Daemon News dict.sztaki.hu FreeBSD Porter's Handb... LXR
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Current Network Status
Last Updated: Mon Jun 16 16:48:09 CEST 2003
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as 6core
View Service Status Detail For All Host Groups
View Host Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Grid For All Host Groups
Host Status Totals
Up Down Unreachable Pending
28 0 0 6
All Problems All Types
0 34
Service Status Totals
Ok Warning Unknown Critical Pending
29 2 0 2 0
All Problems All Types
4 33
Status Summary For All Host Groups
Host Group
Host Status Totals
Service Status Totals
6NET ping hosts (6netcore-pinghosts)
5 UP
4 PENDING
6 OK
2 WARNING
1 CRITICAL
6NET Core Routers (6netcore-routers)
9 UP
9 OK
HBONE6 ping hosts (hbone6-pinghosts)
4 UP
2 PENDING
4 OK
1 CRITICAL
IPv6 Routers (ipv6-routers)
10 UP
10 OK

Eszköz/konfiguráció leltár



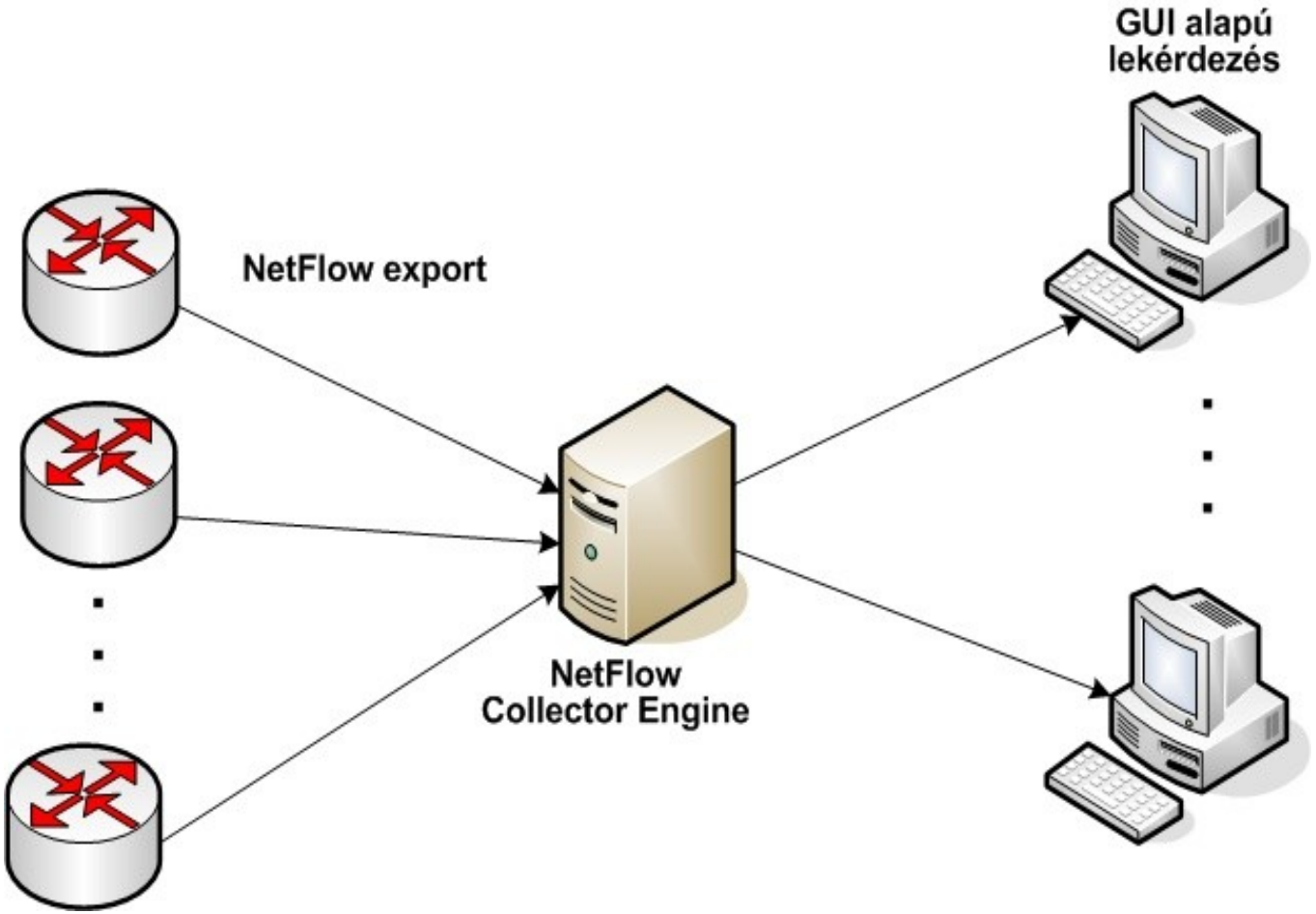
Looking Glass



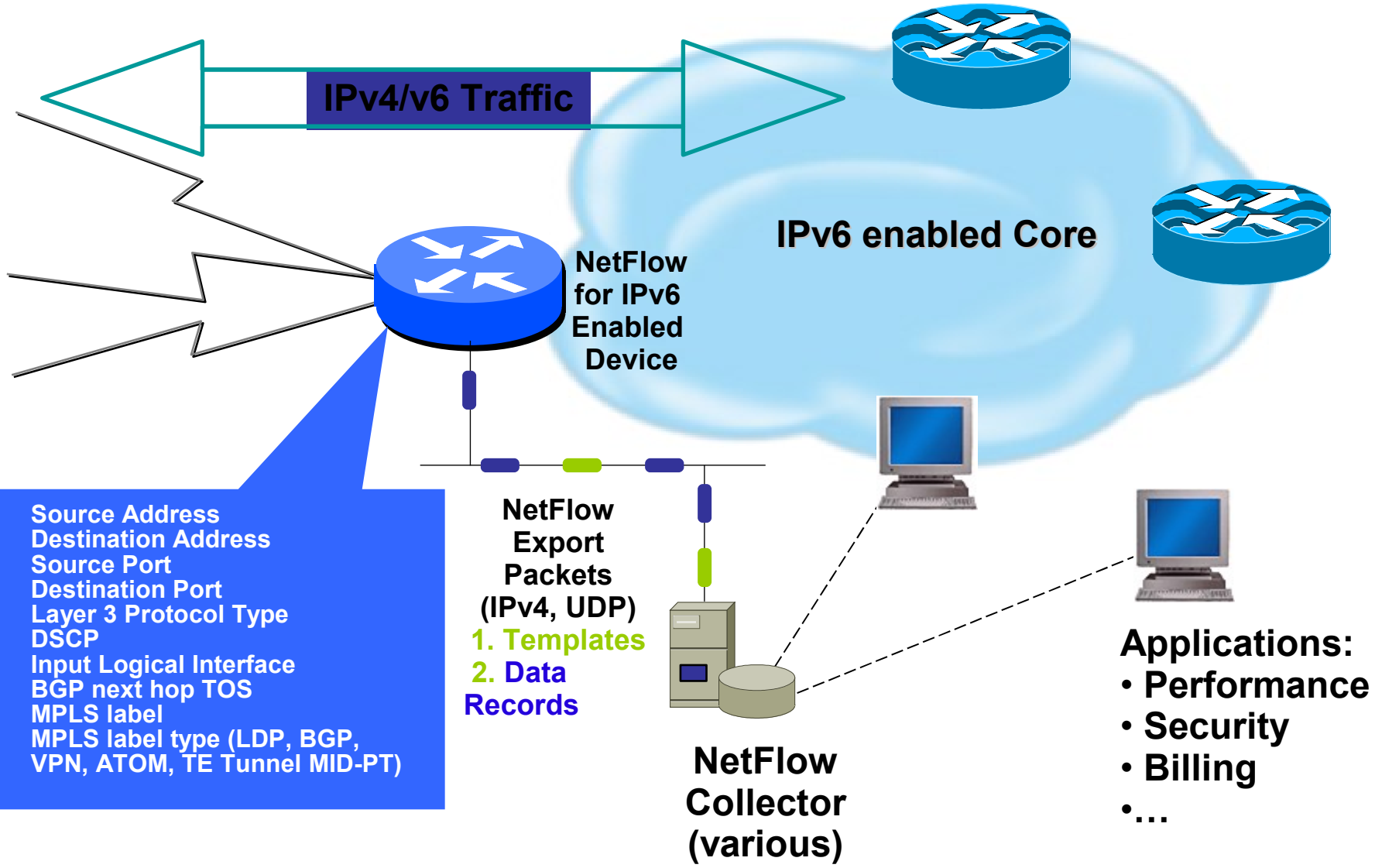
LAN IPv6 menedzsment

Lásd a következő előadást

Mi az a Netflow?

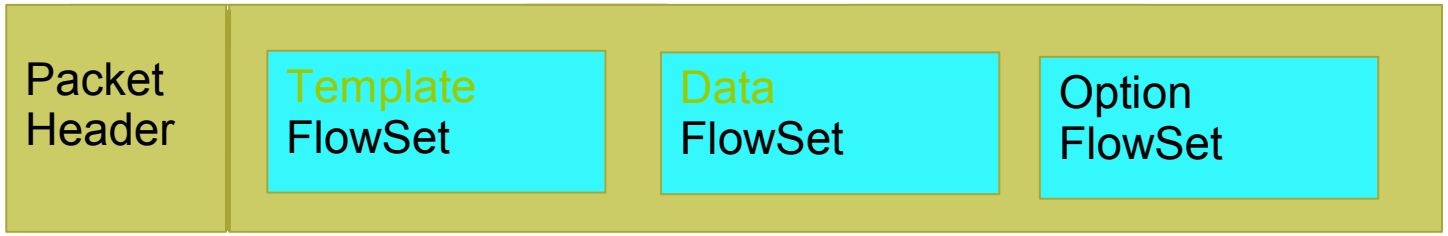


NetFlow IPv6 támogatás

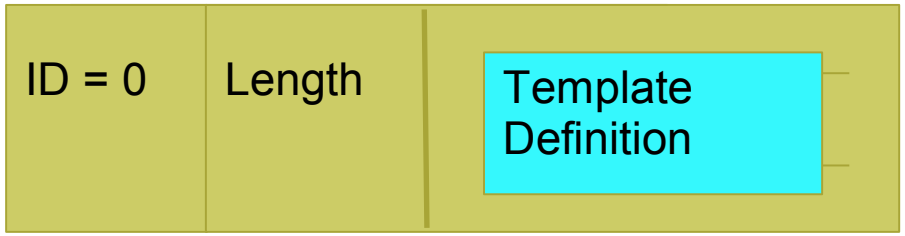


NetFlow Version 9

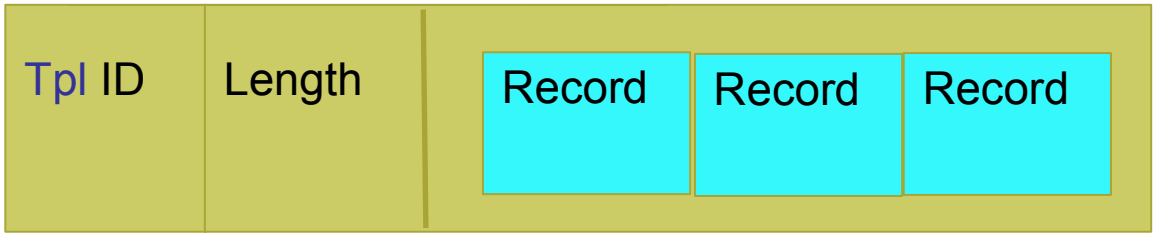
Packet



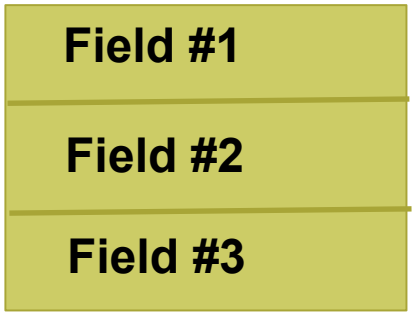
Template Definition (Template FlowSet)



Flow Records (Data FlowSet)



Record

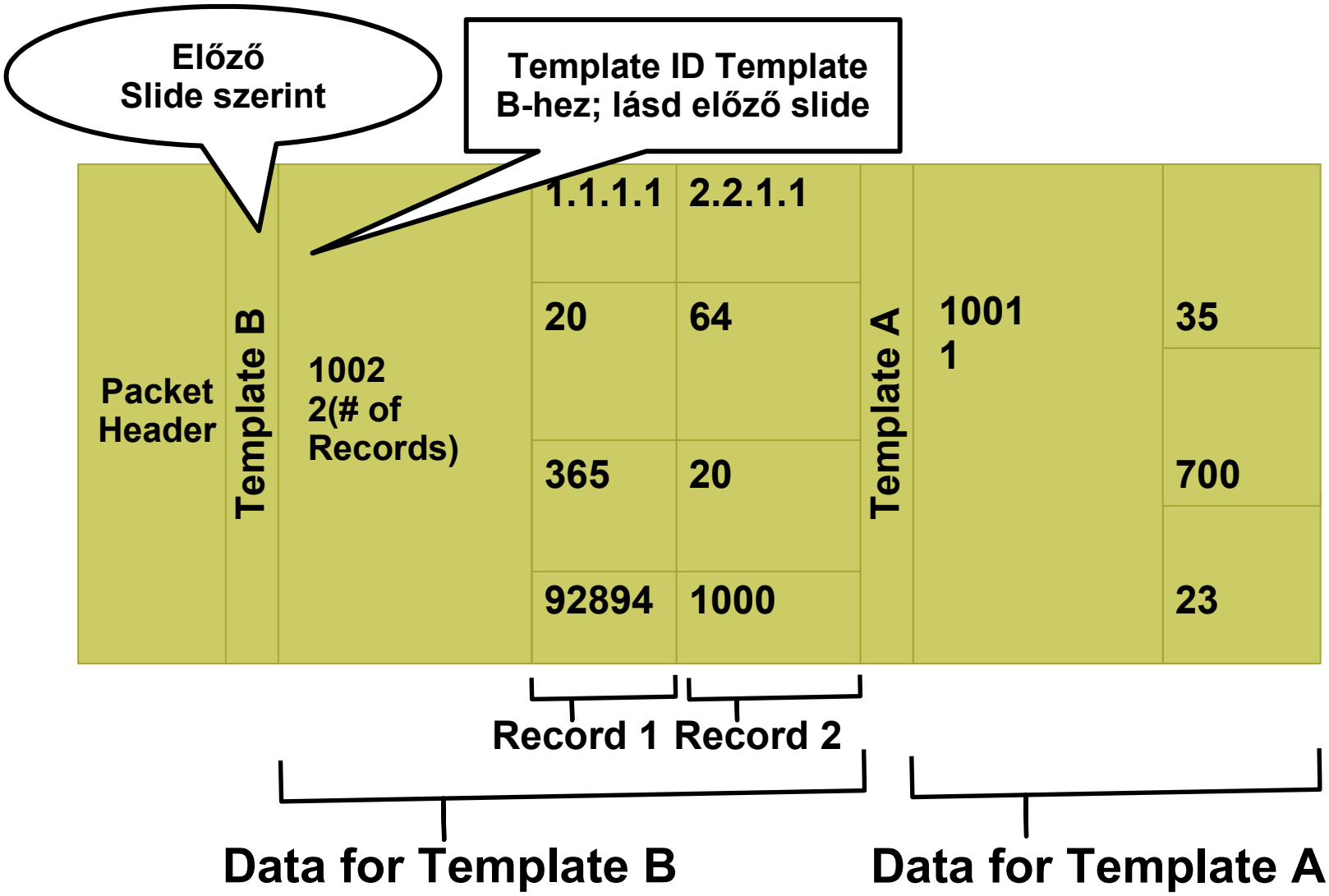


NetFlow Version 9
Példa Template Definition

Template A
Flow Set ID (0 for Template)
Length of Template Structure
1001 (Template ID)
3 (# of Fields)
SRC_AS_NUMBER
2
DST_AS_NUMBER
2
L4_PROTOCOL
2

Template B
Flow Set ID (0 for Template)
Length of Template Structure
1002 (Template ID)
4 (# of Fields)
SRC_IP_PREFIX
4
SRC_AS_NUMBER
2
PACKET_COUNT
2
BYTE_COUNT
2

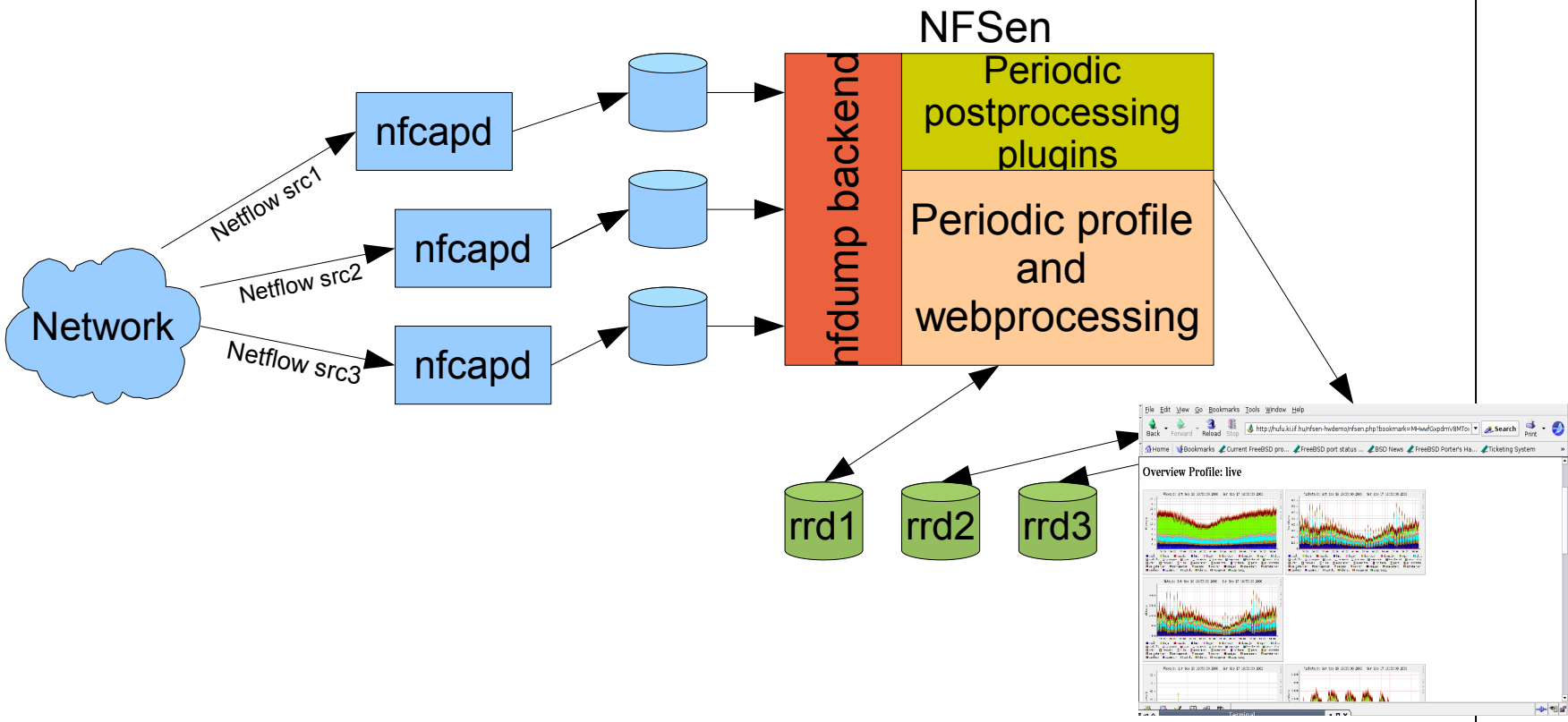
Példa Exportált csomag



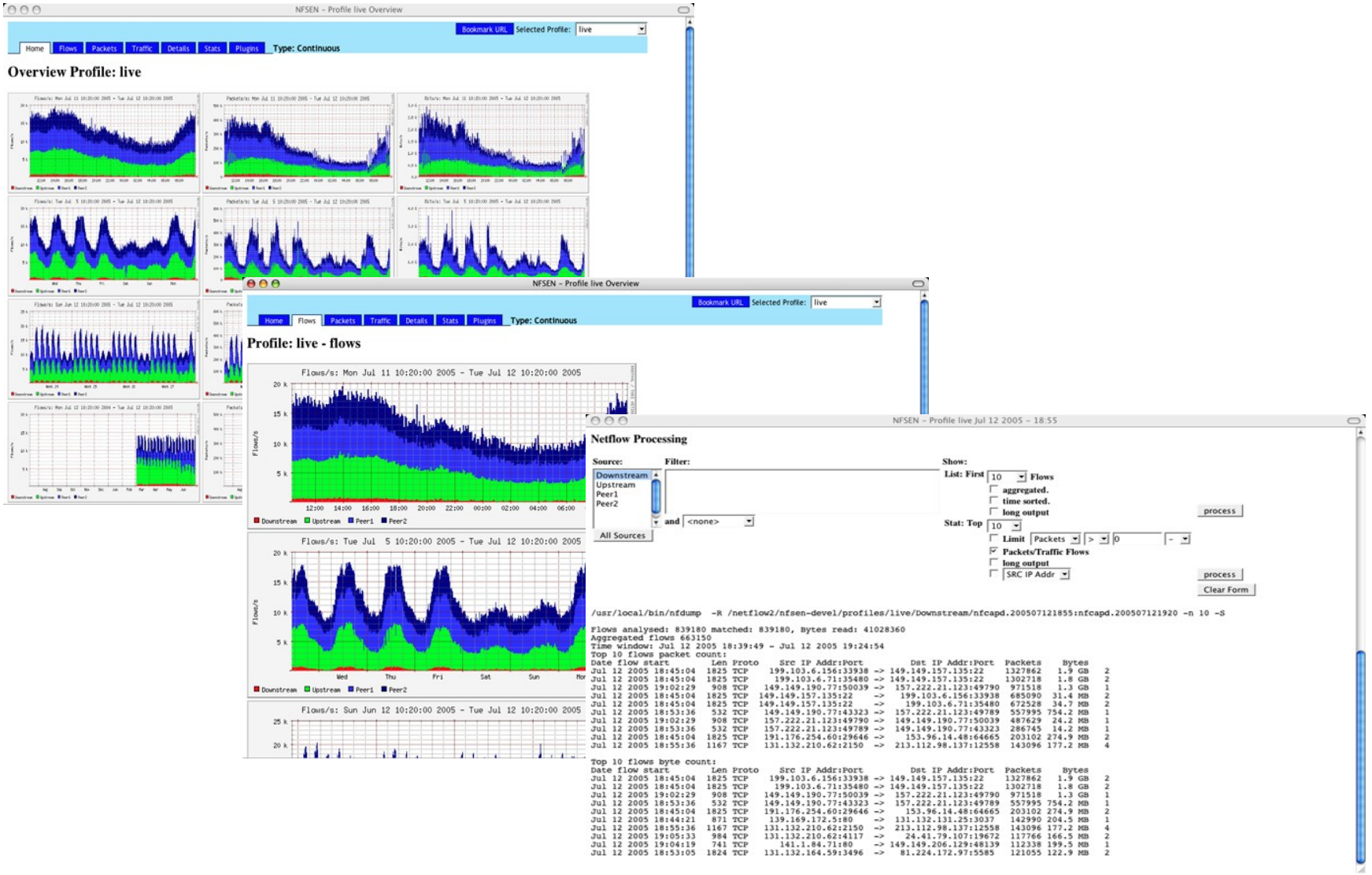
IPFIX vs NetFlow v9 és IPv6

- IETF IPFIX WG -IPFIX
  - Majdnem Netflow v9
  - SCTP az elsődleges transzport
- Cisco
  - Netflow IPv6 támogatás Cisco IOS 12.3(7)T után
    - Netflow v9-al kompatibilis
    - IPv4 transzport az netflow exportálásra
    - Netflow adatgyüjtők
      - Nerdd
      - Flowd
      - NFSen

NfSen/nfdump architektúra



NFSen Netflow kimenet



Az SCTP protokoll

- **Stream Control Transmission Protocol (SCTP)**
  - 2000: IETF Signaling Transport (SIGTRAN)
  - RFC 2960 és RFC 3286
- **Mire jó az SCTP?**
  - TCP- és UDP- szerű működés egyben (és több)
  - Üzenethatárok megtartása (pl. rekordok átvitele)
  - Egy kapcsolaton belül N számú stream
  - Multihoming, hibatűrés
  - …és még több
  - Ideális: sok, üzenet alapú adat megbízható/nem megbízható átvitelére
- **További információ:**
  - Magyar nyelvű leírás: http://ipv6.niif.hu/m/SCTP_tutorial
  - SCTP socket programozás: http://ipv6.niif.hu/m/SCTP_socket

NetFlow + SCTP I.

- **IETF IP Information Export (IPFIX):**
  - 2003: IPFIX protokoll = Cisco IOS NetFlow v9 (+)
  - 2005: SCTP implementálása kötelező, default IPFIX transzport
- **Cisco SCTP support:**
  - NetFlow export + SCTP: 12.4T
  - Konfiguráció példával: http://ipv6.niif.hu/m/SCTP_cisco_config

```
interface GigabitEthernet0/0
 . . .
 ipv6 flow egress
 . . .

ipv6 flow-export destination 195.111.98.214 50000 sctp
```

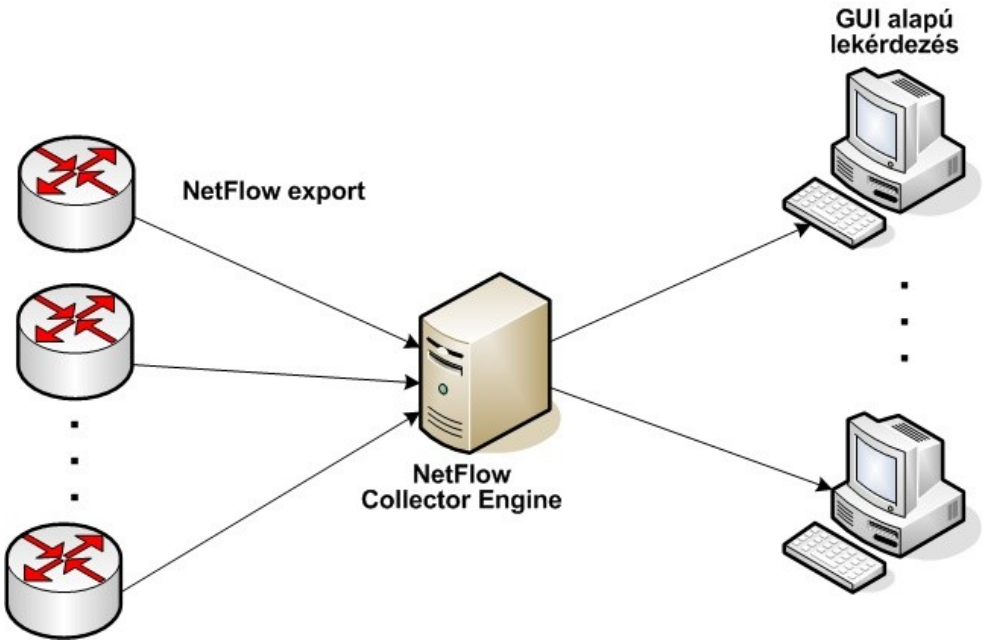
  - Új konfig szintaxis (!), IPv4-nél is

NetFlow + SCTP II.

- **NetFlow + SCTP tesztek:**
  - Cisco 7206 VXR router, IO-GE és PA-FE kártyák
  - IOS verzió: 12.4(9)T
- **Tapasztalatok:**
  - Teszthez elmegy, de instabil
  - Memory leak
  - Megfelelően bonyolult setup-nál: router reload
  - IPv6 + SCTP feletti export: nem implementált
  - NetFlow v9 template konfig: nem implementált
  - Aggregation cache-ek (pl. AS, source prefix): részben működnek csak

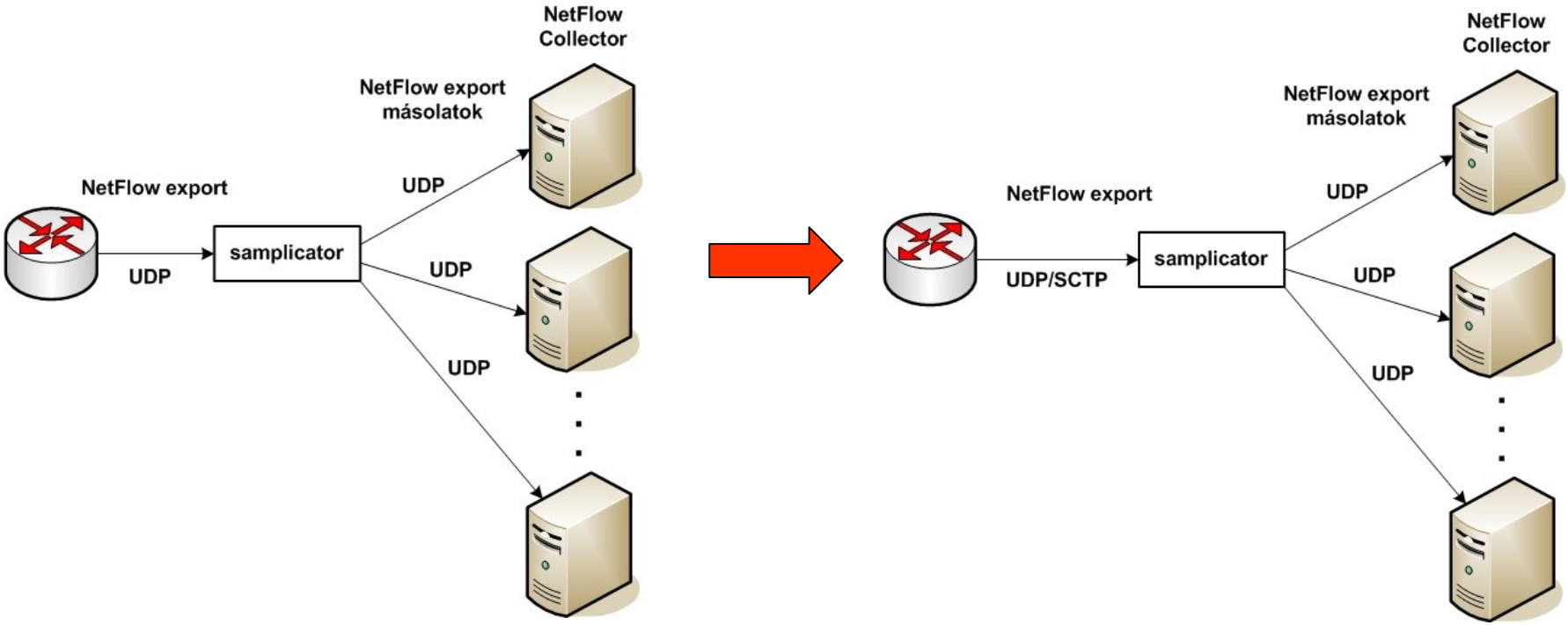
NetFlow + SCTP III.

- **SCTP-képes NetFlow collector-ok:**
  - Cisco CNS NetFlow Collection Engine
  - ipflow
  - ???
- Hogyan tudna az én kedvenc xy netflow collector-om SCTP-t?
- **NetFlow modell:**



Samplicator

- **Mi a samplicator?**
  - Szabad forrású segédprogram NetFlow export-ok többszörözéséhez
  - http://www.switch.ch/tf-tant/floma/sw/samplicator/
  - SCTP-képes samplicator: a Campus6 projekt keretében, router oldali SCTP implementáció teszteléséhez



?

http://ipv6.niif.hu