



IPv6 hálózatmentedzsmen - NetFlow v9 architektúrával

Campus IPv6 Workshop, Budapest

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

2006.09.28.



IPv6 hálózattmenedzsment

- 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 menedzselni a hálózatot

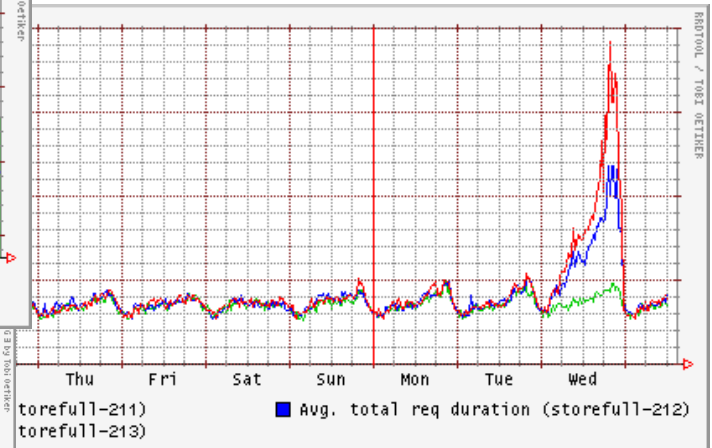
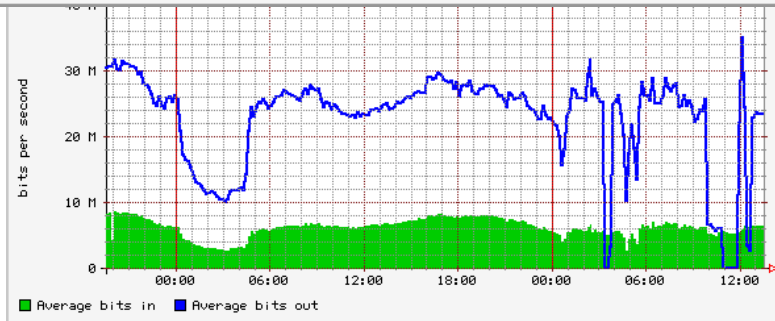
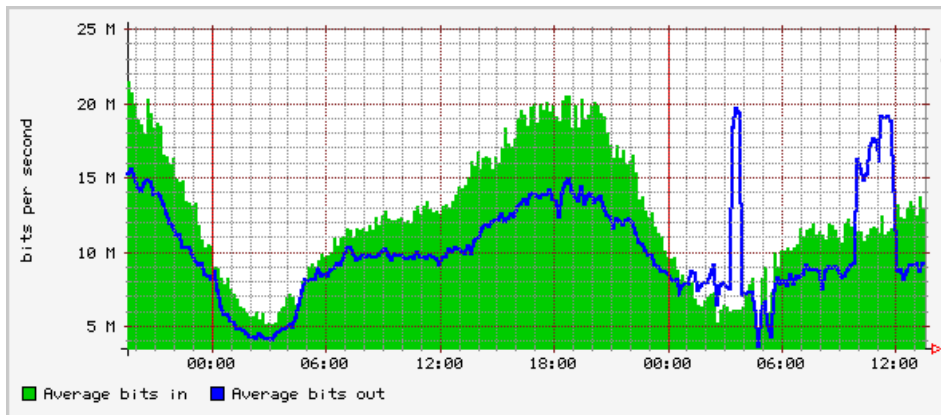


Dualstack hálózatmenedzsment

- 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 mindenképpen szükséges
 - MIBs IPv6 támogatás
 - NetFlow (v9)
 - Eszközök IPv6-os címekeket támogató változata

IPv6 forgalom mérés -Cricket / MRTG

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



Nagios IPv6

The screenshot displays the Nagios web interface in a browser window. The browser's address bar shows the URL `http://6net.iif.hu/nagios/`. The interface includes a navigation menu on the left with sections for General, Monitoring, and Reporting. The main content area is divided into several sections:

- 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.
- Host Status Totals:**

Up	Down	Unreachable	Pending
28	0	0	6

All Problems: 0 **All Types:** 34
- Service Status Totals:**

Ok	Warning	Unknown	Critical	Pending
29	2	0	2	0

All Problems: 4 **All Types:** 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

The interface also features a search bar, a print button, and a help icon (question mark) in the top right corner. The browser's taskbar at the bottom shows various system icons.

Eszköz/konfiguráció leltár

The screenshot shows a web browser window with the following elements:

- Address Bar:** `http://6net.niif.hu/routerconfig/6net/configs/cntrl.6net.hbone.hu?rev=1.156`
- Navigation:** Back, Forward, Reload, Stop buttons.
- Search:** Search button.
- Print:** Print button.
- Bookmarks:** Home, Bookmarks, Current FreeBSD pro..., BSD News, FreeBSD Porter's Ha..., Ticketing System, HUNGARNET-NIIF 6N..., LXR.
- Breadcrumb:** Return to [cntrl.6net.hbone.hu](#) CVS log | Up to [\[6NET router configs\]](#) / [6net](#) / [configs](#)
- File Path:** [\[6NET router configs\]](#) / [6net](#) / [configs](#) / [cntrl.6net.hbone.hu](#)
- Revision 1.156:** [download](#) - view: [text](#), [annotated](#) - [select for diffs](#) - [revision graph](#)
- Commit Info:** Thu Aug 5 16:15:10 2004 UTC (5 weeks, 3 days ago) by *mohacsi*
- Branches:** [MAIN](#)
- CVS tags:** [HEAD](#)
- updates**
- Configuration Output:**

```
!RANCID-CONTENT-TYPE: cisco
!
!Chassis type: 7206VXR - a 7200 router
!CPU: NPE400, R7000 CPU at 350MHz, impl 39, Rev 3.3, 256KB L2 Cache
!
!Memory: main 491520K/32768K
!Memory: nvram 125K
!Memory: bootflash 8192K
!Memory: pcmcia ATA slot0 125952K
!
!Processor ID: 28712851
!
!Power: Power Supply 1 is Zytek AC Power Supply. Unit is on.
!Power: Power Supply 2 is Zytek AC Power Supply. Unit is on.
!
!Image: Software: C7200-P-M, 12.3(7)T1, RELEASE SOFTWARE (fc2)
```

Looking Glass

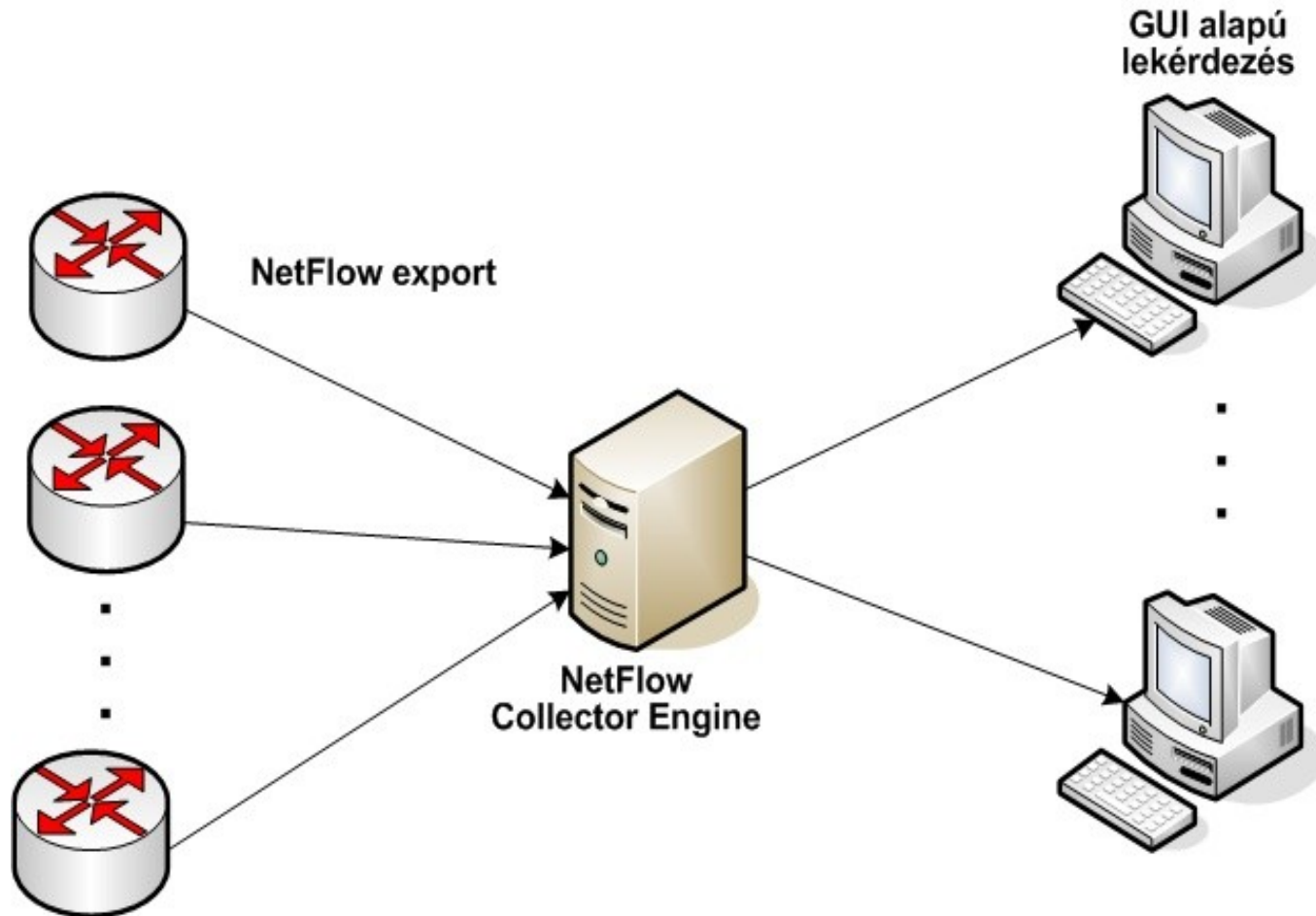
RENATER Looking Glass

<p>BGP tables</p> <p><input checked="" type="radio"/> show bgp IPv6 <input type="text" value="routing_table"/></p> <ul style="list-style-type: none">routing_tablesummaryneighbors	<p>BGP with regular expression</p> <p><input type="radio"/> show bgp IPv6 <input type="text" value="regex"/></p> <p>regular expression : <input type="text"/></p> <p>Don't use the character "\$"</p>
<p><input type="radio"/> IPv6 traffic</p> <p><input type="radio"/> IPv6 interface</p> <p><input type="radio"/> IPv6 tunnels</p> <p><input type="radio"/> IPv6 neighbors</p> <p><input type="radio"/> IPv6 route</p>	<p><input type="radio"/> Ping XXXXX</p> <p><input type="radio"/> Traceroute XXXXX</p> <p><input type="radio"/> show ip bgp XXXXX</p> <p><input type="radio"/> show ip bgp summary</p> <p><input type="radio"/> show ip bgp dampening dampened-paths</p> <p><input type="radio"/> show ip mroute summary</p> <p><input type="radio"/> show ip mroute active</p> <p><input type="radio"/> show ip mbgp summary</p> <p><input type="radio"/> show ip mbgp XXXXX</p> <p><input type="radio"/> IPv4 address <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></p> <p><input type="radio"/> IPv6 address <input type="text"/></p> <p><input type="radio"/> name address IPv4 <input type="text"/></p> <p><input type="radio"/> name address IPv6 <input type="text"/></p>
<p>Router: <input type="text" value="Toulouse"/></p> <p><input type="button" value="submit"/> <input type="button" value="Reset"/></p>	

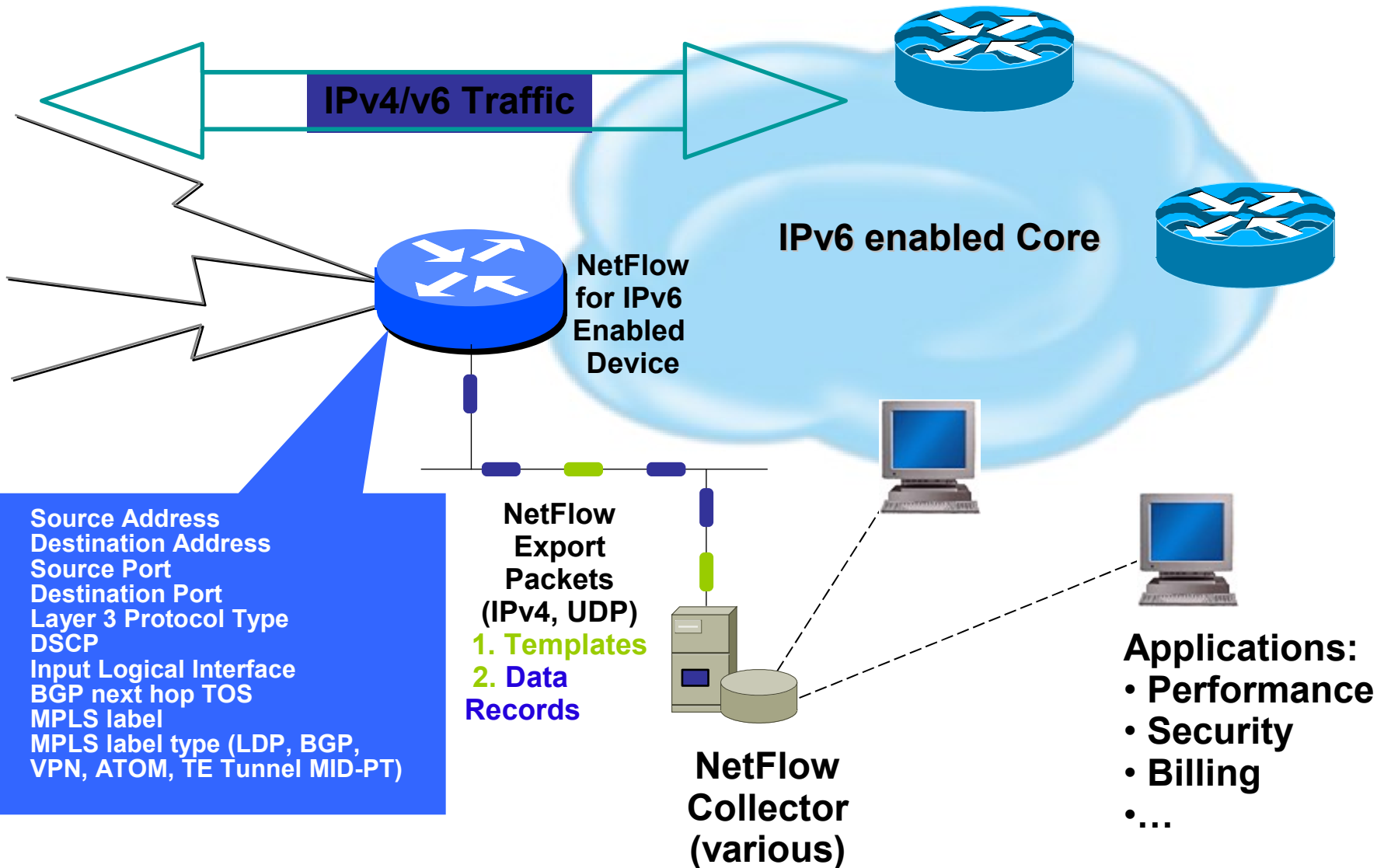
LAN IPv6 menedzsment

Lásd a következő előadást

Mi az a Netflow?



NetFlow IPv6 támogatás

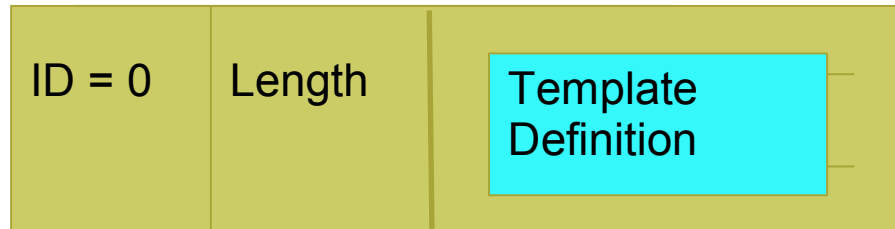


NetFlow Version 9

Packet



Template Definition (Template FlowSet)



Flow Records (Data FlowSet)



Record



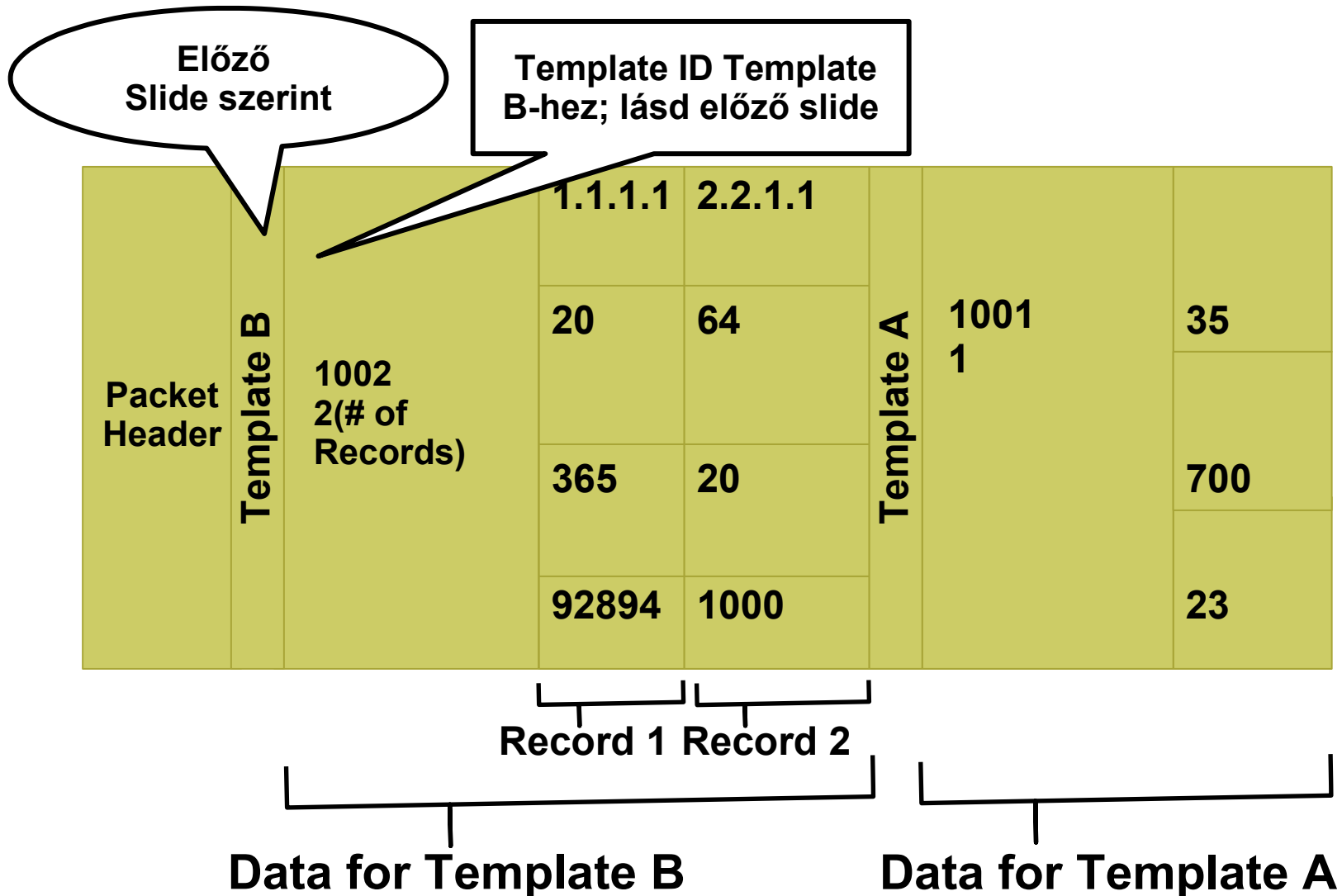
NetFlow Version 9

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

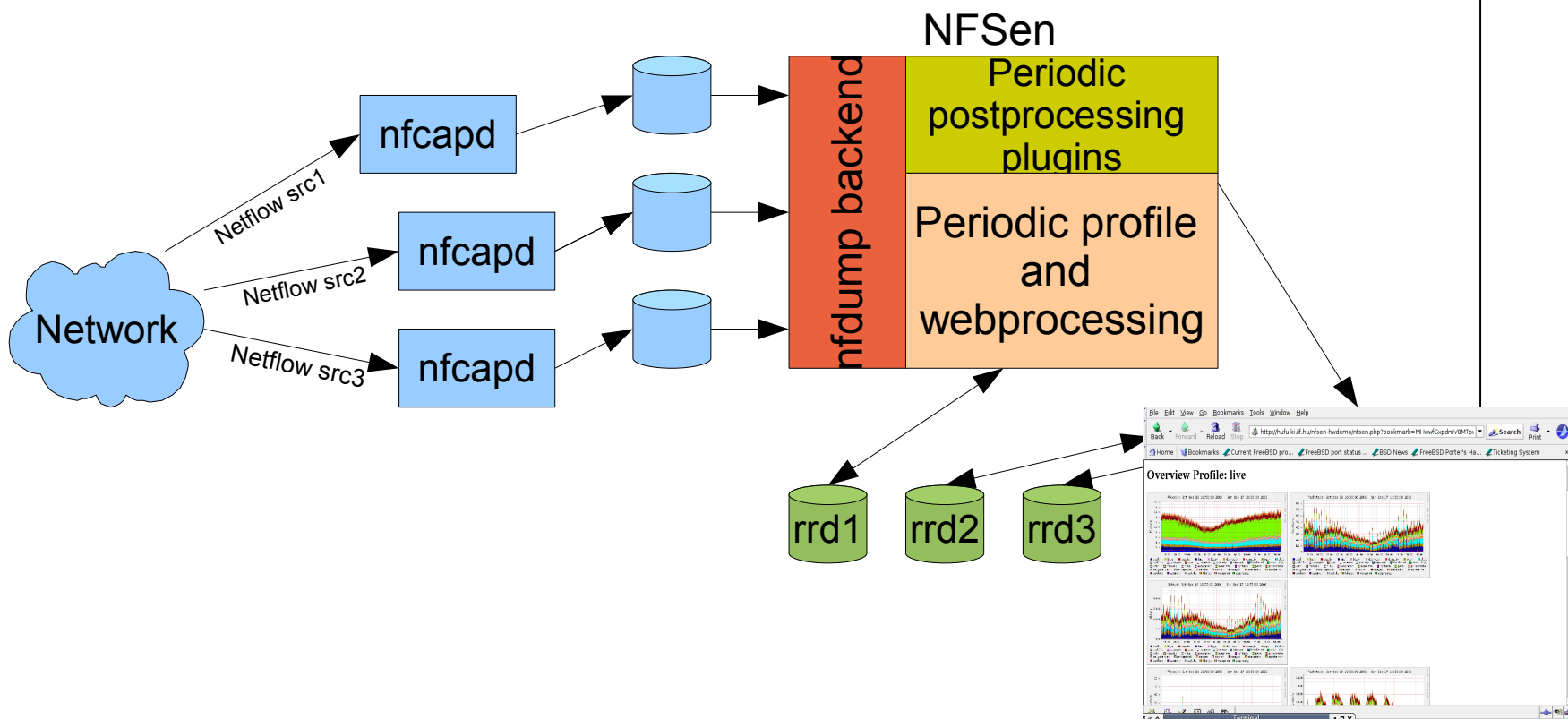
Példa Exportált csomag



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 adatgyűjtők
 - Nerd
 - Flowd
 - NFSen

NfSen/nfdump architektúra





NFSen Netflow kimenet

NFSen - Profile live Overview

Home | Flows | Packets | Traffic | Details | Stats | Plugins | Type: Continuous

Bookmark URL Selected Profile: live

Overview Profile: live

NFSen - Profile live Overview

Home | Flows | Packets | Traffic | Details | Stats | Plugins | Type: Continuous

Bookmark URL Selected Profile: live

Profile: live - flows

NFSen - Profile live Jul 12 2005 - 18:55

Home | Flows | Packets | Traffic | Details | Stats | Plugins | Type: Continuous

Bookmark URL Selected Profile: live

Netflow Processing

Source: Filter: Show: List: First 10 Flows
 aggregated
 time sorted
 long output process

Stat: Top 10
 Limit Packets > 0
 Packets/Traffic Flows
 long output
 SRC IP Addr process
Clear Form

```
/usr/local/bin/ndump -R /netflow2/nfsen-devel/profiles/live/Downstream/nfcapd.200507121855:nfcapd.200507121920 -n 10 -s
```

Flows analysed: 839180 matched: 839180, bytes read: 41028360
Aggregated flows 663150
Time window: Jul 12 2005 18:39:49 - Jul 12 2005 19:24:54

Top 10 flows packet count:

Date flow start	Len	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes
Jul 12 2005 18:45:04	1825	TCP	199.103.6.156:33938	149.149.157.135:22	1327862	1.9 GB
Jul 12 2005 18:45:04	1825	TCP	199.103.6.71:35480	149.149.157.135:22	1302718	1.8 GB
Jul 12 2005 19:02:29	908	TCP	149.149.190.77:50039	157.222.21.123:49790	971518	1.3 GB
Jul 12 2005 18:45:04	1825	TCP	149.149.157.135:22	199.103.6.156:33938	685090	31.4 MB
Jul 12 2005 18:45:04	1825	TCP	149.149.157.135:22	199.103.6.71:35480	672528	34.7 MB
Jul 12 2005 18:45:04	532	TCP	149.149.190.77:43323	157.222.21.123:49789	557995	754.2 MB
Jul 12 2005 19:02:29	908	TCP	157.222.21.123:49790	149.149.190.77:50039	487629	24.2 MB
Jul 12 2005 18:53:36	532	TCP	157.222.21.123:49789	149.149.190.77:43323	286745	14.2 MB
Jul 12 2005 18:45:04	1825	TCP	191.176.254.60:29646	153.96.14.48:64665	203102	274.9 MB
Jul 12 2005 18:55:36	1167	TCP	131.132.210.62:2150	213.112.98.137:12558	143096	177.2 MB

Top 10 flows byte count:

Date flow start	Len	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes
Jul 12 2005 18:45:04	1825	TCP	199.103.6.156:33938	149.149.157.135:22	1327862	1.9 GB
Jul 12 2005 18:45:04	1825	TCP	199.103.6.71:35480	149.149.157.135:22	1302718	1.8 GB
Jul 12 2005 19:02:29	908	TCP	149.149.190.77:50039	157.222.21.123:49790	971518	1.3 GB
Jul 12 2005 18:53:36	532	TCP	149.149.190.77:43323	157.222.21.123:49789	557995	754.2 MB
Jul 12 2005 18:45:04	1825	TCP	191.176.254.60:29646	153.96.14.48:64665	203102	274.9 MB
Jul 12 2005 18:44:21	871	TCP	139.169.172.5:80	131.132.131.25:3037	142990	204.5 MB
Jul 12 2005 18:55:36	1167	TCP	131.132.210.62:2150	213.112.98.137:12558	143096	177.2 MB
Jul 12 2005 19:05:33	984	TCP	131.132.210.62:4117	24.41.79.107:19672	117766	166.5 MB
Jul 12 2005 19:04:19	741	TCP	141.1.84.71:80	149.149.206.129:46139	112338	199.5 MB
Jul 12 2005 18:53:05	1824	TCP	131.132.164.59:3496	81.224.172.97:5085	121055	122.9 MB



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 konfigurációs szintaxis (!), IPv4-nél is



NetFlow + SCTP II.

- **NetFlow + SCTP tesztek:**

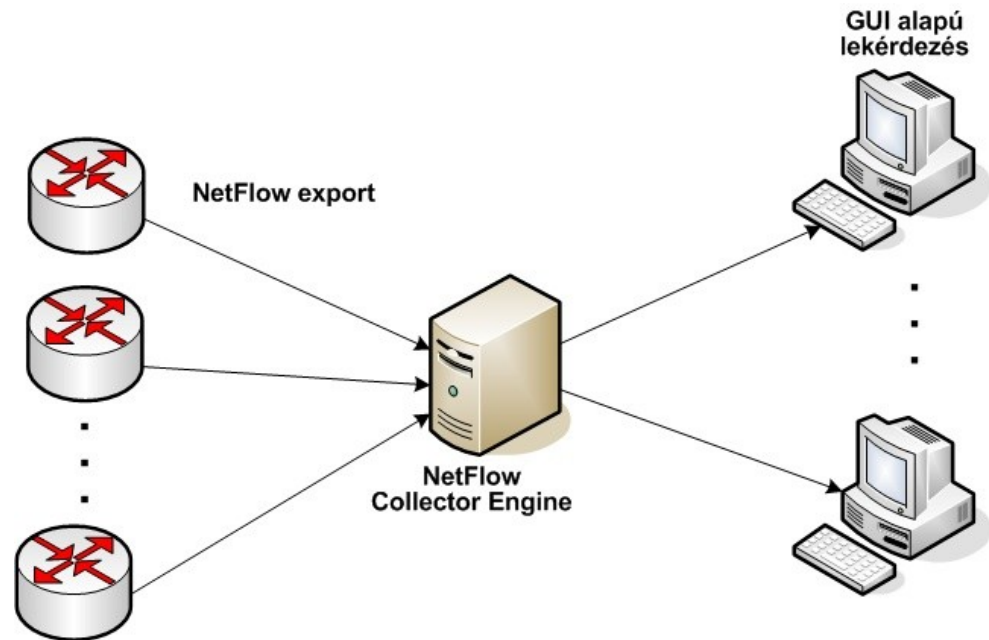
- Cisco 7206 VXR router, IO-GE és PA-FE kártyák
- IOS verzió: 12.4(9)T

- **Tapasztalatok:**

- Teszthez elmegy, de instabil
- Memory leak
- Megfelelően bonyolult setup-nál: router reload
- IPv6 + SCTP feletti export: nem implementált
- NetFlow v9 template konfiguráció: nem implementált
- Aggregation cache-ek (pl. AS, source prefix): részben működnek csak

NetFlow + SCTP III.

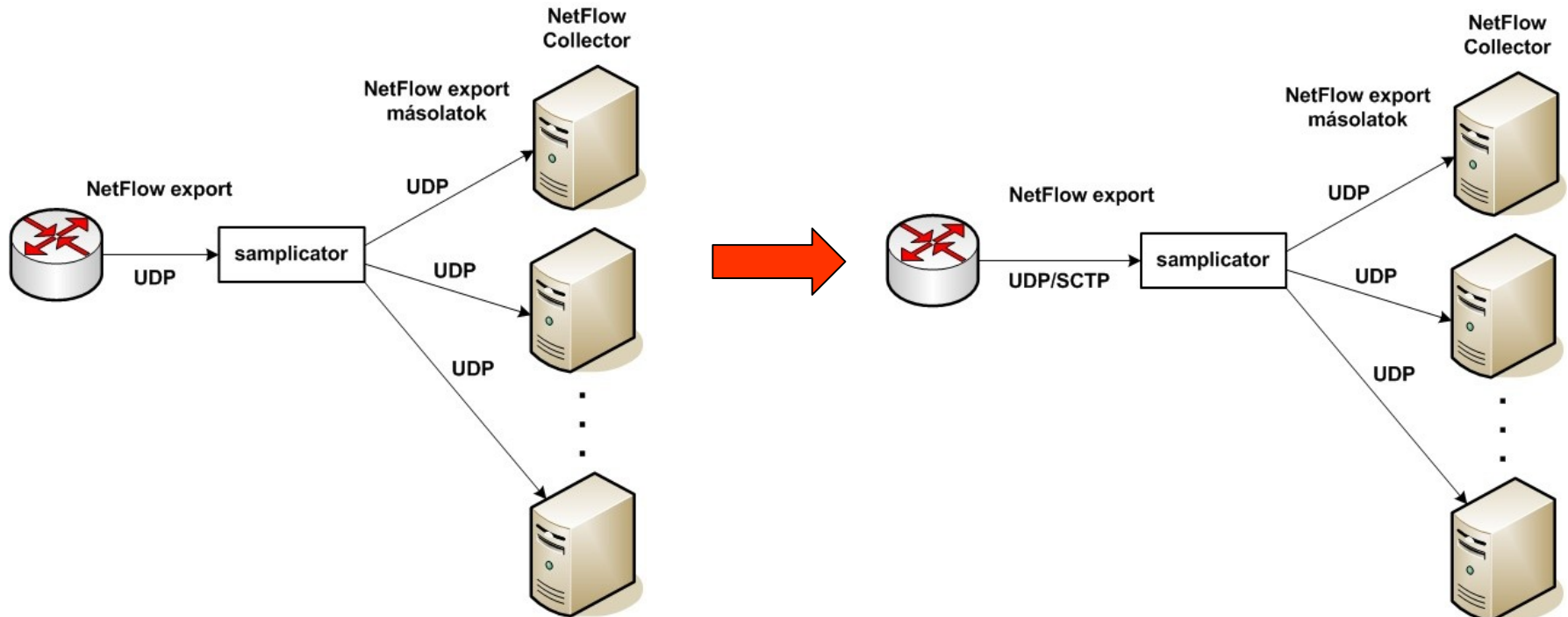
- **SCTP-képes NetFlow collector-ok:**
 - Cisco CNS NetFlow Collection Engine
 - ipflow
 - ???
- Hogyan tudna az én kedvenc xy netflow collector-om SCTP-t?
- **NetFlow modell:**



Samplerator

- **Mi a samplerator?**

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





?

<http://ipv6.niif.hu>