

Over the (n)top

Netzwerküberwachung mit ntop

Stephan Knabe
Hochschule Harz, Wernigerode
stephan.knabe@desy.de

8. März 2004

ntop im Überblick (1)

- Monitoring kleiner bis mittlerer Netzwerke
- OSI-Layer 2, 3, 4 und 5
- Grafische Oberfläche
- Integrierter Webserver
- Umfangreiche tabellarische und grafische Übersichten
- Open Source (GPL)

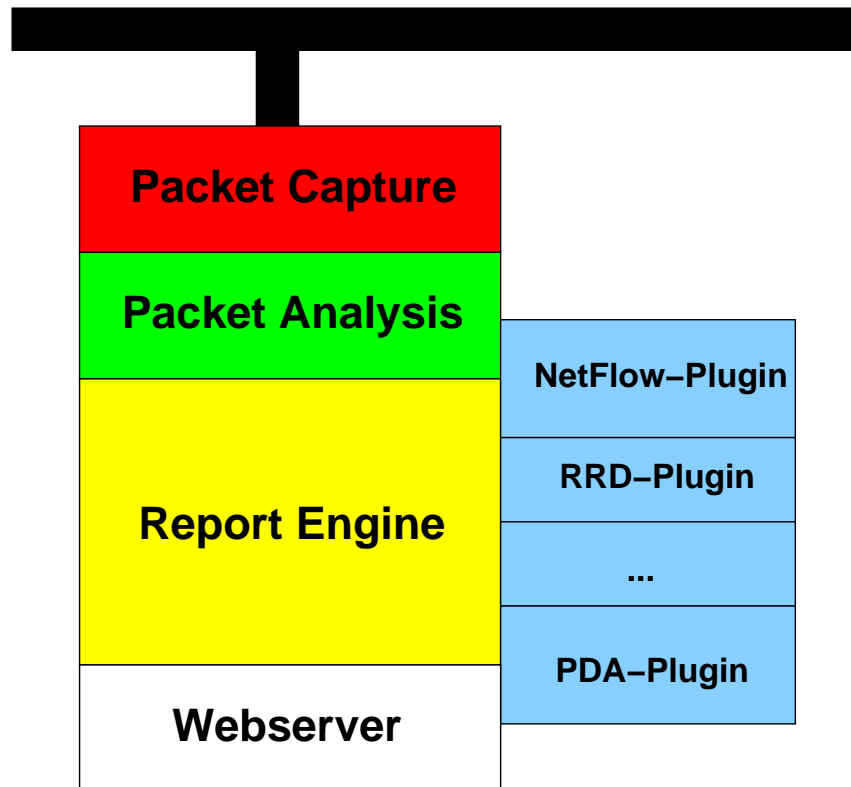
ntop im Überblick (2)

- Unterstützte Netzwerkmedien:
Loopback, Ethernet (inklusive 802.11Q), Token Ring,
PPP/PPPoE, FDDI, ...
- Unterstützte Betriebssysteme:
FreeBSD, Linux, Solaris, IRIX, AIX, MS Windows
- Unterstützte Protokolle:
IP, IPX, DecNet, AppleTalk, Netbios, OSI, DLC ...

ntop im Überblick (3)

- Hauptentwickler Luca Deri und Burton M. Strauss III
- Projekt-Website `www.ntop.org`
- Dokumentation, FAQ, Wiki unter `www.ntopsupport.com`
- Mailinglisten `ntop@unipi.it` und `ntop-dev@unipi.it`
- Aktuelle Releases 2.2c, 3.0pre1 und CVS

Architektur



basiert auf libpcap

Plugins

HTTP/HTTPS

Basic-Features (1)

Total-Data-Statistik

Netscape: Welcome to ntop!

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: http://hyade20:3333/

About Total Recv Sent Stats IP Traffic IP Protos Admin

Network Traffic: Total Data (Sent+Received)

Host	Domain	Data	TCP	UDP	ICMP	DLC	IPX	Decnet	(R)ARP	AppleTalk	OSPF	NetBios	IGMP	OSI	IPv6	STP	Other
hyade20.ifh.de		3.5 MB 46.9 %	3.4 MB	75.8 KB	4.0 KB	0	0	0	1.9 KB	0	0	0	0	0	0	0	0
athene.ifh.de		1.9 MB 25.3 %	1.9 MB	0	196	0	0	0	0	0	0	0	0	0	0	0	0
pales.ifh.de		1.4 MB 19.2 %	1.4 MB	0	0	0	0	0	0	0	0	0	0	0	0	0	0
all-routers.mcast.net		183.7 KB 2.4 %	0	183.7 KB	0	0	0	0	0	0	0	0	0	0	0	0	0
erato.ifh.de		142.2 KB 1.9 %	117.0 KB	25.2 KB	0	0	0	0	0	0	0	0	0	0	0	0	0
Bridge Sp. Tree/OSI Route		128.6 KB 1.7 %	0	0	0	0	0	0	0	0	0	0	0	0	0	128.6 KB	0
141.34.19.2		121.0 KB 1.6 %	0	107.3 KB	0	0	0	0	13.7 KB	0	0	0	0	0	0	0	0
141.34.19.2		78.1 KB 1.0 %	0	19.5 KB	0	0	0	0	58.5 KB	0	0	0	0	0	0	0	0
medusa.ifh.de		1.8 KB 0.0 %	0	1.8 KB	0	0	0	0	0	0	0	0	0	0	0	0	0
remus.ifh.de		1.7 KB 0.0 %	0	1.7 KB	0	0	0	0	0	0	0	0	0	0	0	0	0
euterpe.ifh.de		1.4 KB 0.0 %	1.4 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0
pegasus.ifh.de		392 0.0 %	0	0	392	0	0	0	0	0	0	0	0	0	0	0	0
idho.ifh.de		360 0.0 %	0	360	0	0	0	0	0	0	0	0	0	0	0	0	0
eos.ifh.de		180 0.0 %	0	180	0	0	0	0	0	0	0	0	0	0	0	0	0

Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'

Report created on Wed Nov 12 12:30:11 2003 [1:24:01]
Generated by ntop v.2.2 MT (SSL) [i686-pc-linux-gnu] (10/28/03 11:41:57 AM build)
Listening on [eth0 NetFlow-device] without a kernel (libpcap) filtering expression
Web report active on interface eth0
© 1998-2003 by Luca Deri

© 1998-2003
by Luca Deri

Basic-Features (2)

TCP/UDP-Statistik

The screenshot shows the Netscape Communicator interface with the ntop web interface. The browser's address bar shows the URL `http://hyade20:3333/`. The main content area displays a table titled "Network Traffic: Total Data (Sent+Received)". The table has columns for Host, Domain, Data, and various protocols including FTP, HTTP, DNS, Telnet, NBios-IP, Mail, DHCP-BOOTP, SNMP, NNTP, NFS, X11, SSH, Gnutella, Kazaa, WinMX, and DirectConnect. The "Total Data" row shows 3.7 MB (48.2%) for hyade20.ifh.de. Other rows show data for various protocols and hosts like athene.ifh.de, pales.ifh.de, all-routers.mcast.net, erato.ifh.de, 141.34.19.2, medusa.ifh.de, renus.ifh.de, euterpe.ifh.de, pegasus.ifh.de, and gandalf.ifh.de.

Host	Domain	Data	FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS	X11	SSH	Gnutella	Kazaa	WinMX	DirectConnect
Total Data	hyade20.ifh.de	3.7 MB 48.2 %	0	0	8.4 KB	0	0	0	0	0	0	768	0	18.6 KB	0	0	0	0
All Protocols	athene.ifh.de	2.0 MB 25.9 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TCP/UDP	pales.ifh.de	1.5 MB 19.8 %	0	0	0	0	0	0	0	0	0	0	0	12.0 KB	0	0	0	0
Throughput	all-routers.mcast.net	192.9 KB 2.5 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Host Activity	erato.ifh.de	144.0 KB 1.8 %	0	0	0	0	0	0	0	0	0	768	0	0	0	0	0	0
NetFlows	141.34.19.2	111.9 KB 1.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	141.34.19.2	19.5 KB 0.2 %	0	0	0	0	0	0	1.8 KB	0	0	0	0	0	0	0	0	0
	medusa.ifh.de	2.1 KB 0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	renus.ifh.de	2.0 KB 0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	euterpe.ifh.de	1.8 KB 0.0 %	0	0	0	0	0	0	0	0	0	0	0	1.4 KB	0	0	0	0
	pegasus.ifh.de	494 0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	gandalf.ifh.de	320 0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

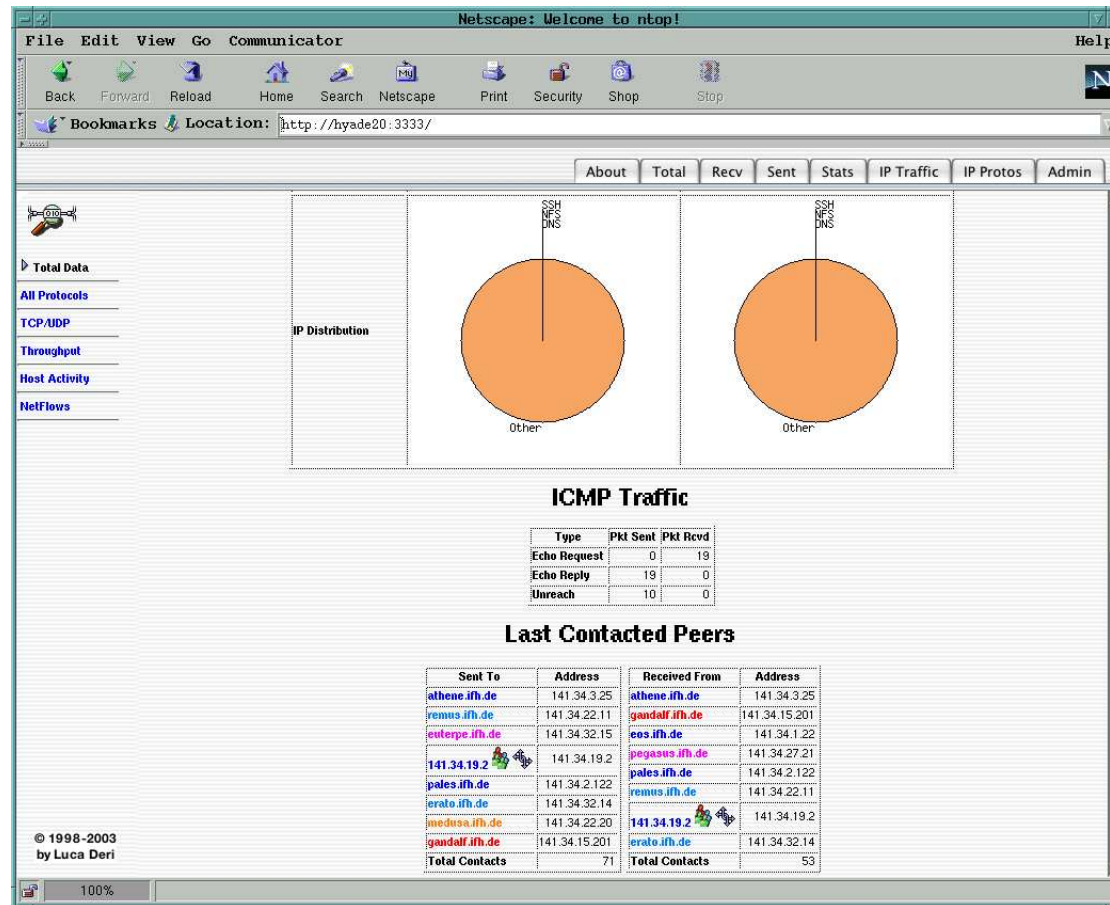
Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'

Report created on Wed Nov 12 12:33:42 2003 [1:27:32]
Generated by ntop v.2.2 MT (SSL) [i686-pc-linux-gnu] (10/28/03 11:41:57 AM build)
Listening on [eth0,NetFlow-device] without a kernel (libpcap) filtering expression
Web report active on interface eth0
© 1998-2003 by Luca Deri

© 1998-2003
by Luca Deri

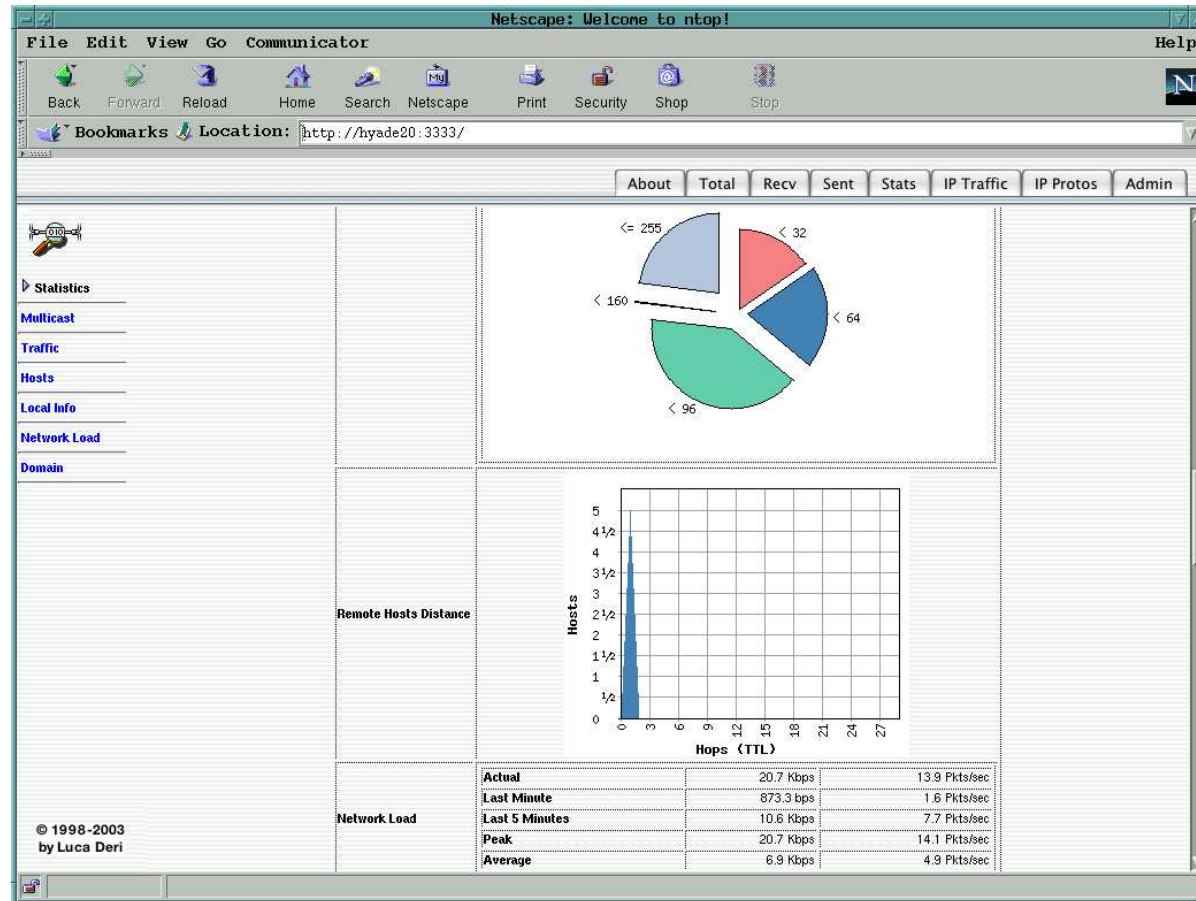
Basic-Features (3)

Host-Statistik



Basic-Features (4)

Netzwerk-Statistik



Advanced Features

- TCP-Connection-Tracking
- Host-Matrix
- VLAN-Übersicht
- Einfache IDS-Features

Administration

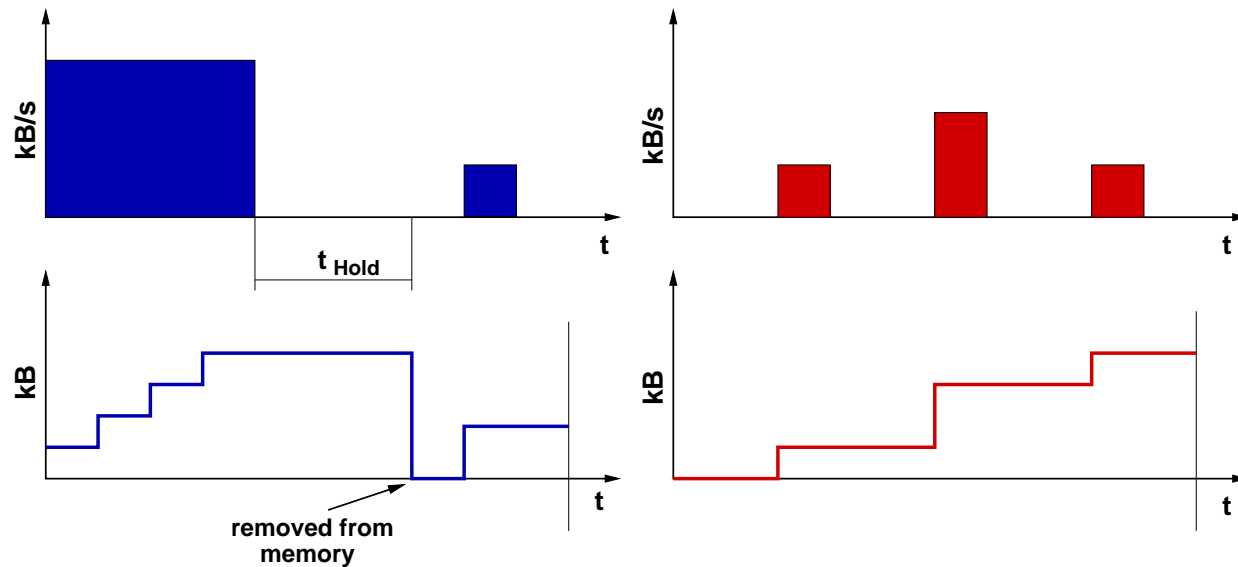
- Zugriffsverwaltung
- Zählerrücksetzung
- Filtereinrichtung
- Datenexport (TXT, XML, PHP, Perl ...)
- Plugin-Konfiguration

Plugins

- NetFlow - Im- und Export von IP-Verbindungsdaten
- rrdPlugin - Datenspeicherung und Langzeitgrafiken
- ICMP-Watch - Detailliertes Monitoring von ICMP-Paketen
- NFS-Watch - NFS-Statistiken
- LastSeen - Statistik der Zeitpunkte von Hostaktivitäten

ntop-Datenhaltung im RAM

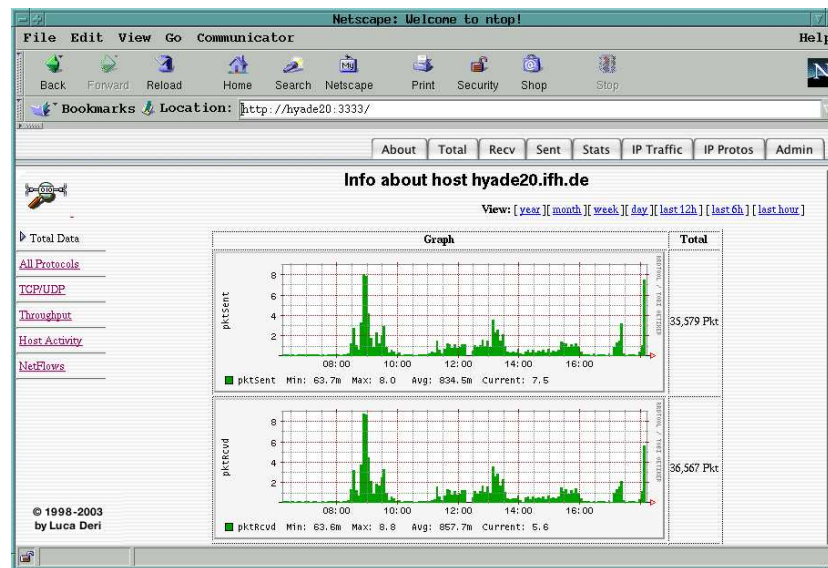
Kein langfristiges Speichern aller Hosts möglich.



Verweildauer im Speicher hängt von Aktivität ab.

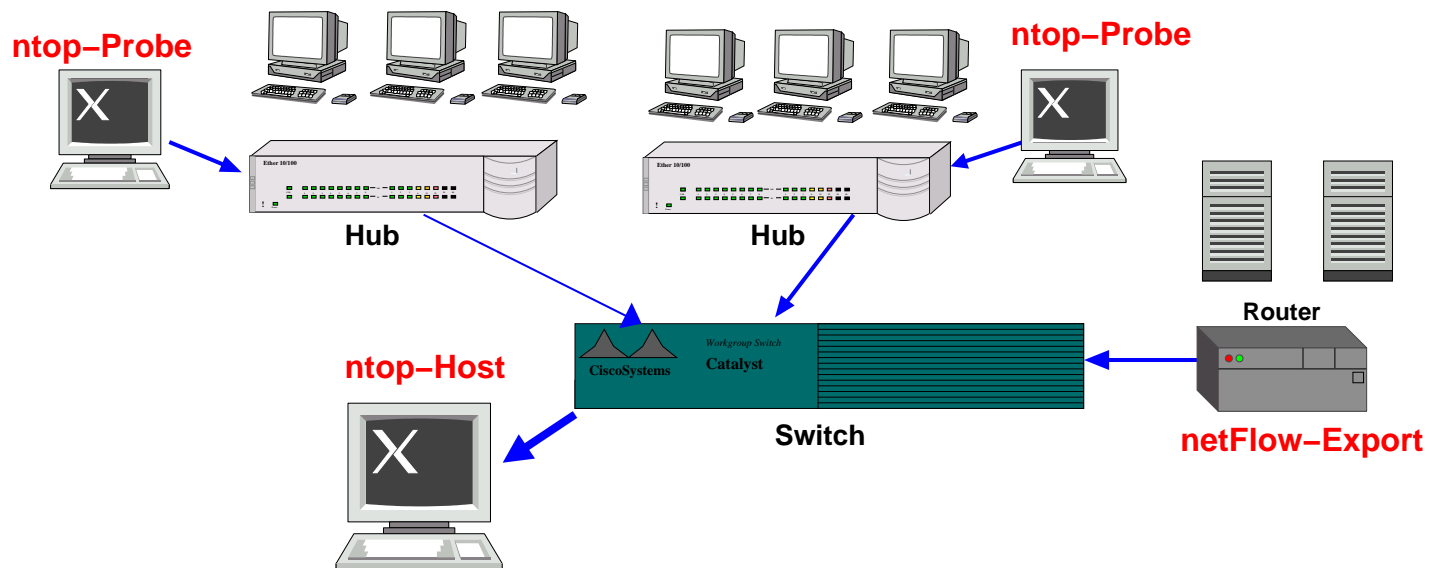
rrdPlugin

- Konfiguration von Speicherort, Daten-Umfang, Detail-Stufen
- Integrierte Graphen für Host- und Netzwerk-Statistiken



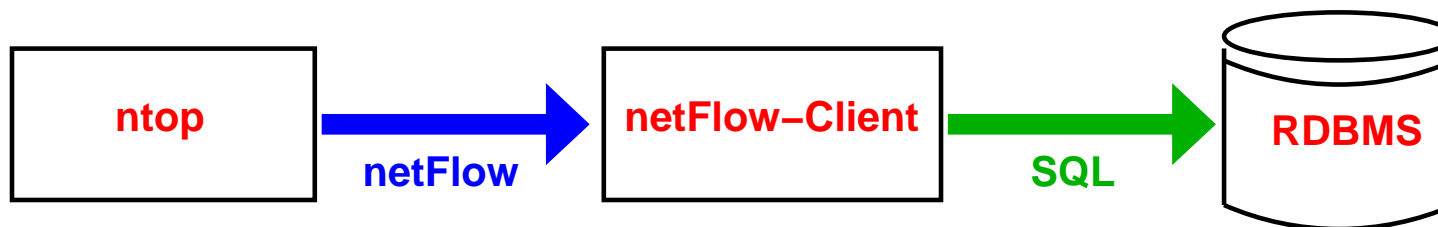
NetFlow-Plugin (1)

- In großen Netzen und Switch-Umgebungen verteiltes Monitoring möglich
- RMON/SMON liefern nur unzureichende Daten



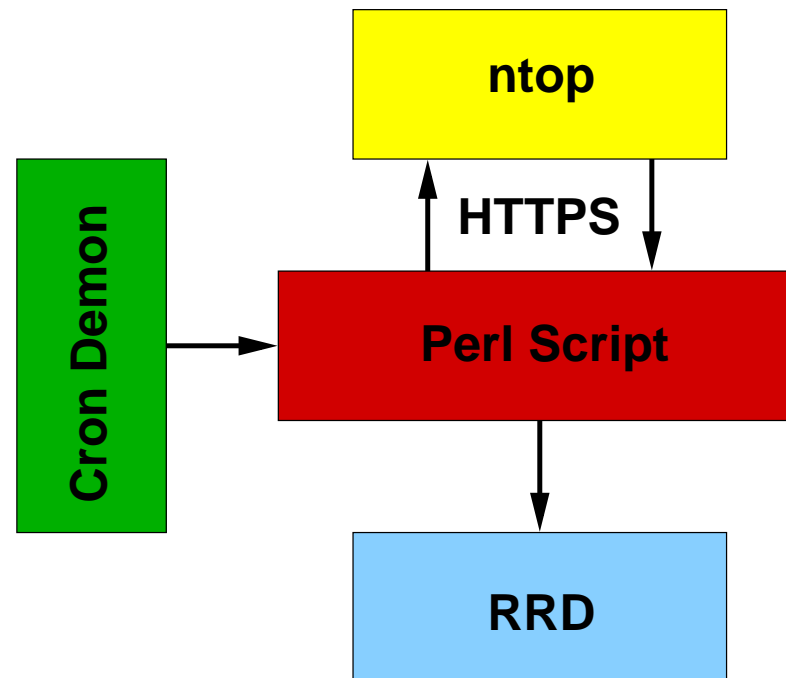
NetFlow-Plugin (2)

- NetFlow unterstützt Im- und Export von Flow-Daten
- Unterstützte Flow-Protokolle sind u.a. NetFlow v5, sFlow, nFlow und NetFlow v9
- Weitere, einfach zu implementierende Schnittstelle zu eigenen Applikationen



Ergänzung um eigene Scripts:

Zeitgesteuertes Auslesen von Zahlenwerten



- Universelles Tool für den alltäglichen Praxiseinsatz
- In größeren Netzwerken als verteilte Lösung möglich
- Verschiedene Schnittstellen zu (eigenen) externen Anwendungen
- Kein Ersatz für IDS oder Protokollanalyse

Ressourcen

- Projekt-Homepage `www.ntop.org /`
`www.ntopsupport.com`
- Informationen zu Flow-Protokollen:
`www.cisco.com, www.sflow.org`
- RRD-Infos `www.mrtg.org,`
`www.rrdtool.org`
- Feedback an `stephan.knabe@desy.de`