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

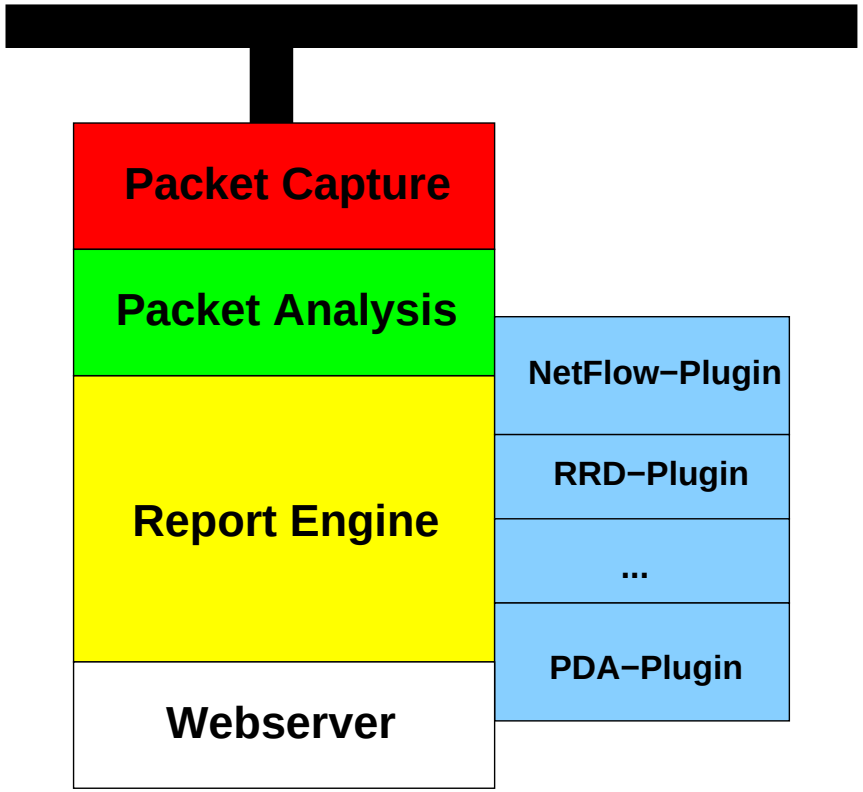
- Unterstützte Protokolle:

  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



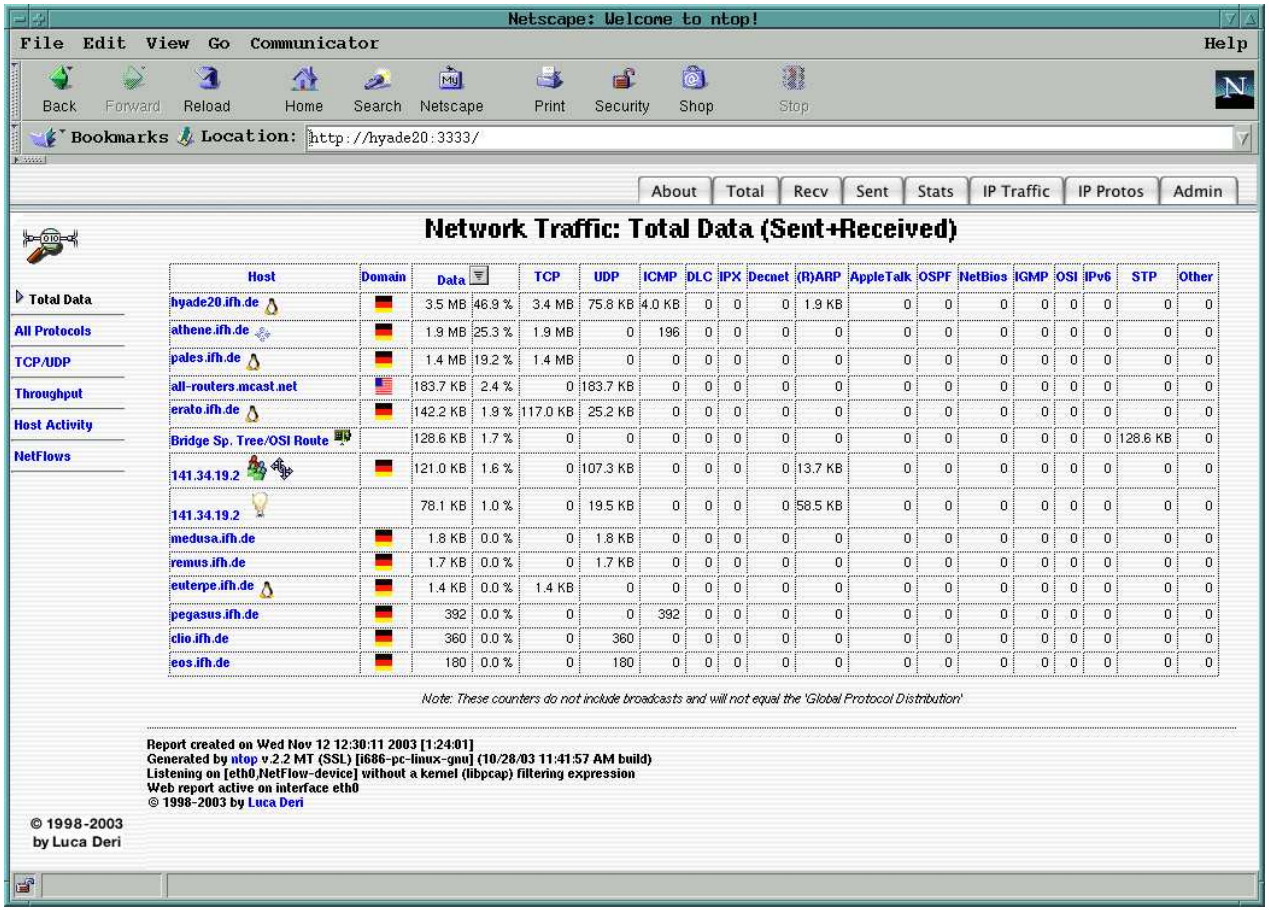
basiert auf libpcap

Plugins

HTTP/HTTPS

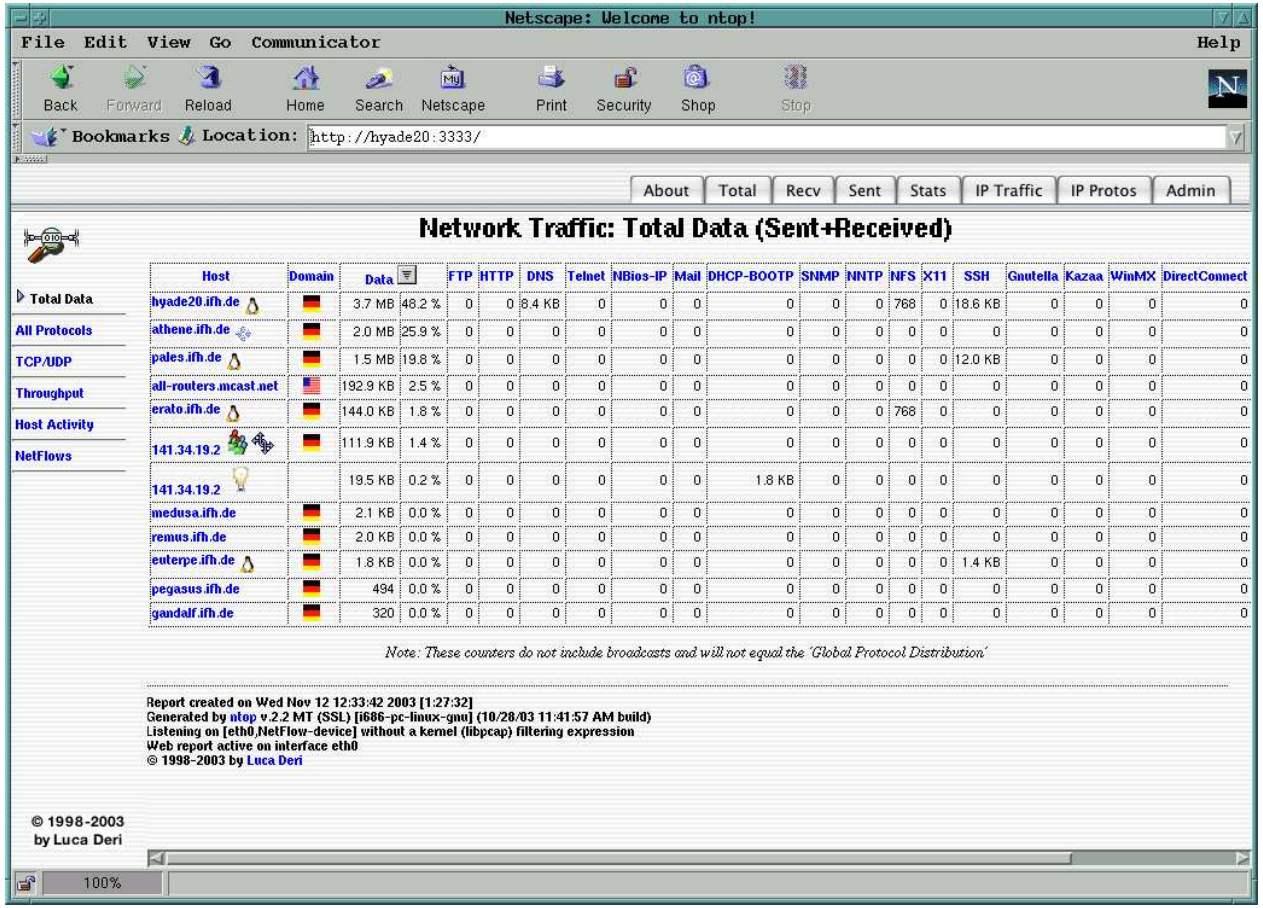
Basic-Features (1)

Total-Data-Statistik



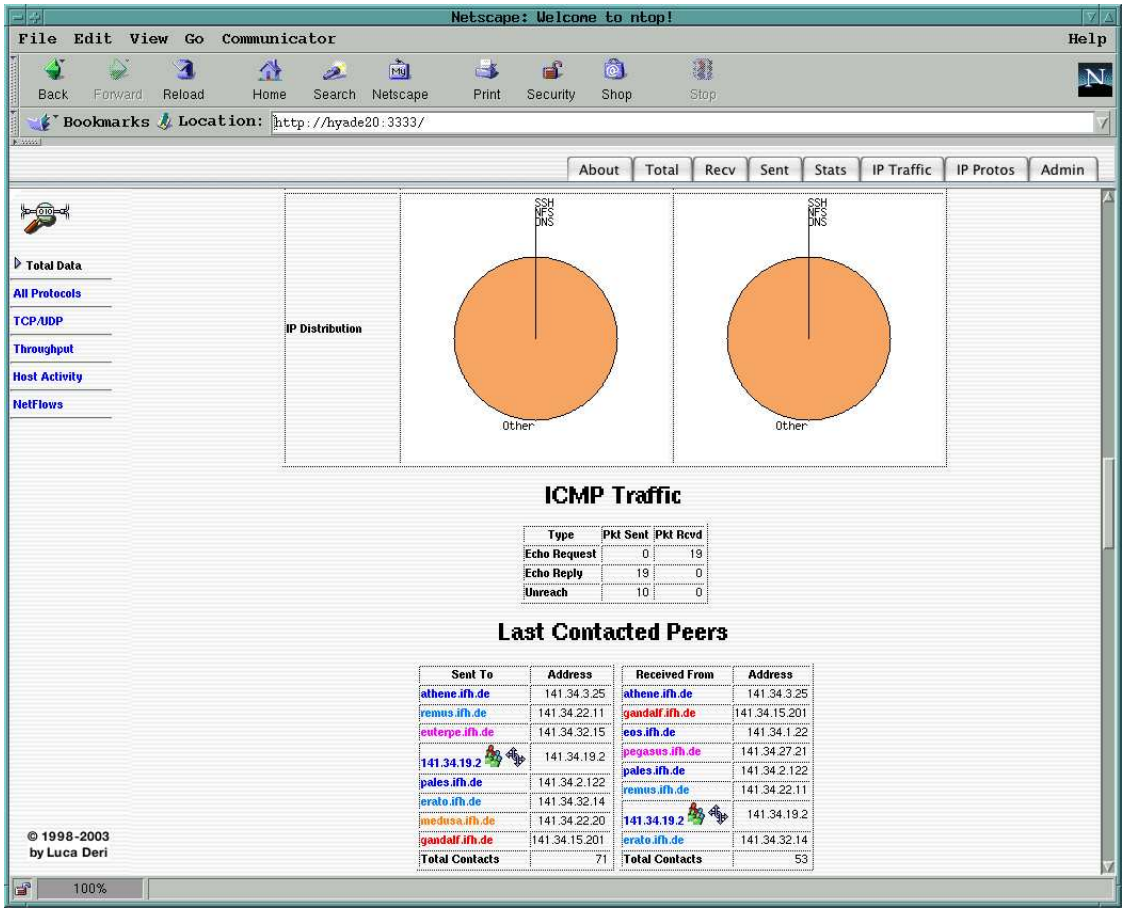
Basic-Features (2)

TCP/UDP-Statistik



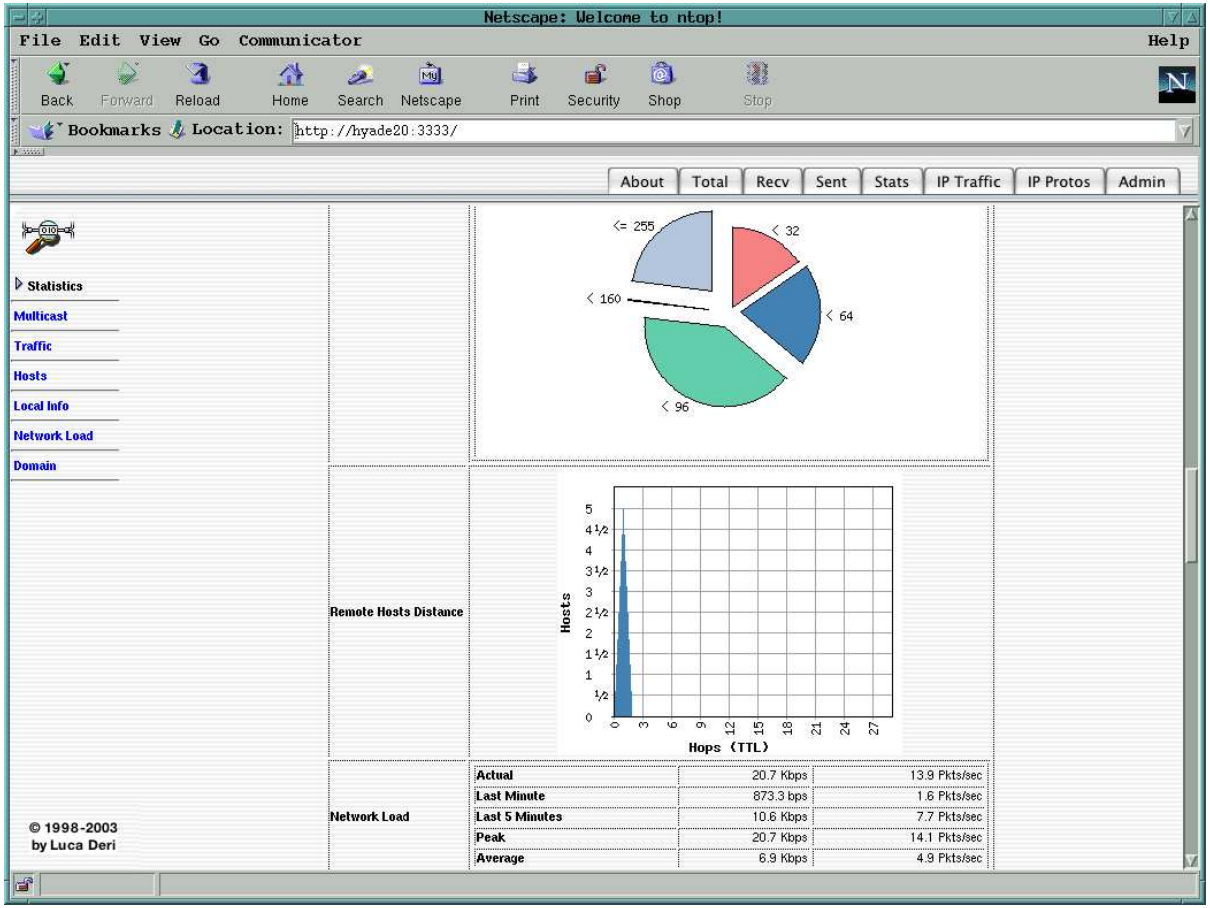
Basic-Features (3)

Host-Statistik



Basic-Features (4)

Netzwerk-Statistik



Advanced Features

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

Administration

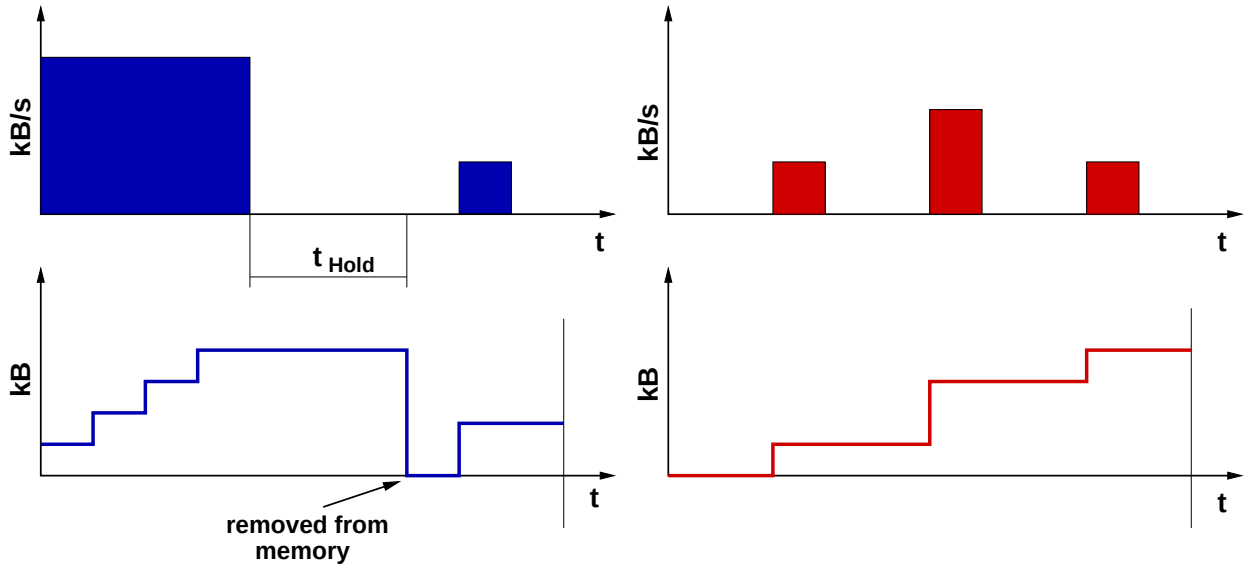
- Zugriffsverwaltung
- Zählerrücksetzung
- Filtereinrichtung
- Datenexport (TXT, XML, PHP, Perl ...)
- Plugin-Konfiguration

Plugins

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

ntop-Datenhaltung im RAM

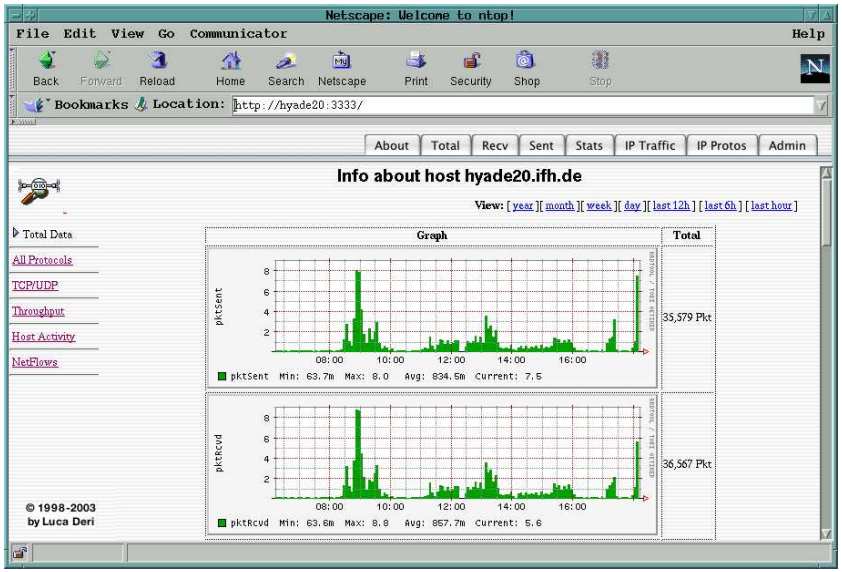
Kein langfristiges Speichern aller Hosts möglich.



Verweildauer im Speicher hängt von Aktivität ab.

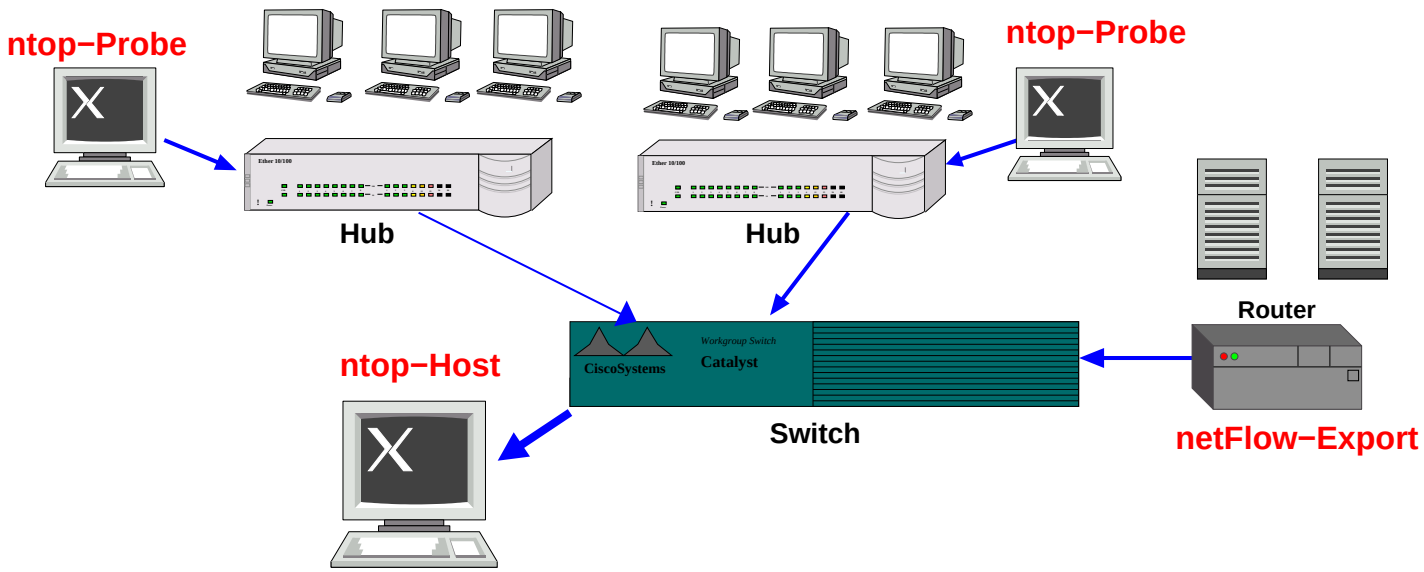
rrdPlugin

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



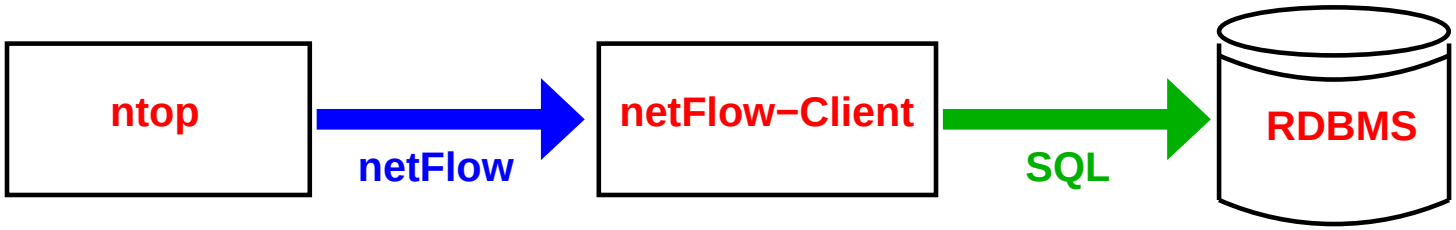
NetFlow-Plugin (1)

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



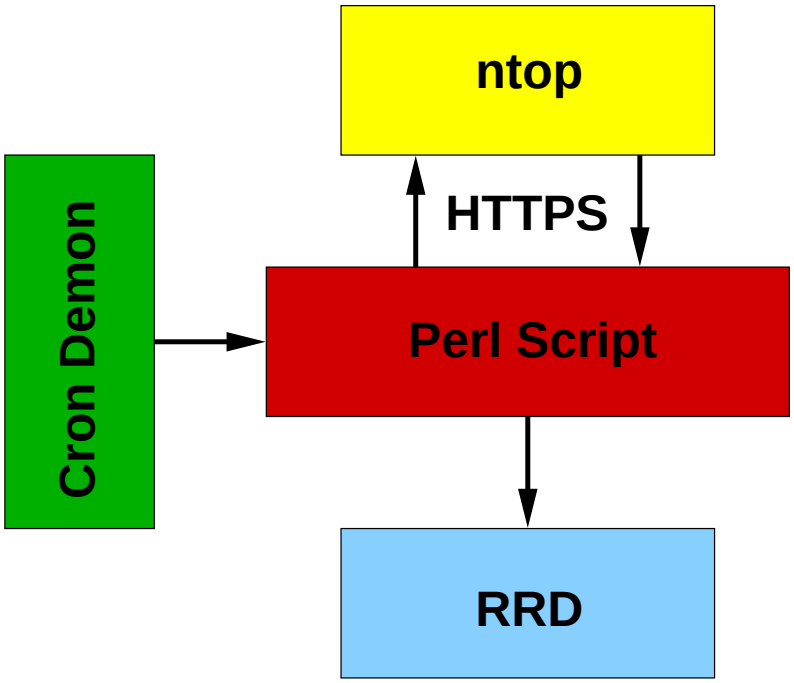
NetFlow-Plugin (2)

- 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`