

What is Nyx?

Contributed by Administrator
 Wednesday, 11 July 2007
 Last Updated Monday, 06 August 2007

(Nyx: Greek. mythology, the goddess of the night)

Nyx is high performance network monitoring utility that allows for almost realtime IP and MAC address searching across your entire corporate network infrastructure. Written in Java, using Tomcat and MySQL as operating platform and SNMP for monitoring.

Nyx comes with an extensible and highly customizable XHTML user interface and an open XML query language for interfacing third party applications.

What is Nyx?

Your network size is above-average? Your environment is open and your users have a large degree of freedom? You've lost overview who is actually using your infrastructure from where?

Then you need Nyx! Nyx is a monitoring tool, capable of localising IP- and MAC-addresses in your network and printing out - in almost realtime - the switch ports these addresses belong to. Nyx has also a history log, so you can easily review past incidences.

Advantages Controlling who is using your network infrastructure where and when in a large, open environment is nearly impossible! Chasing errors and abuse cases can be a full time job.

Nyx provides the ability to overview all IP- and MAC-addresses in your network, log their chronological and local use and evaluate them. Using Nyx gives you the ability to track all enddevice connections to the network. Unauthorized devices or other "trouble makers" can be located in seconds and be plugged out from the network.

How Nyx works Nyx uses the SNMP-protocol to scan the network devices (switches and routers) on a regular basis and store the gathered information in a SQL-style database. The data are access from a webbased frontend (servlet), correlated and presented in a human readable form to the user.

Features

- highly parallel scanning of network devices
- scanning almost in real time (one scan cycle in a 5 minute window)
- designed for large and extra large networks (>100k end devices, >1k network devices)
- usable also in small networks
- periodical survey and logging of the network status
- recognition of up- and downlink ports for data reduction in search results
- VLAN (IEEE 802.3Q) capable (depending on the network devices)
- extendable to any SNMP capable type of network device
- database with all your network devices
- completely implemented in object oriented Java
- easy extensible module based programming style
- customizable web frontend based on XSLT

System requirements: database server: minimum:

- dualcore Xeon, 3GHz
 - 4GB RAM
 - fast built in disc array
 - 200GB of free disc space
 - min. 100 MBit/s Ethernet
 - MySQL 5.0
- recommended:

- quadcore Xeon, 3GHz
- 8GB RAM
- fast built in disc array
- 200GB of free disc space
- 1 GBit/s Ethernet

frontend- / application server:

minimum:

- single- or dualcore Xeon, 3GHz
- 2GB RAM
- 1 GBit/s Ethernet
- Apache Tomcat 5

Front- and application server can also be installed on two servers (default: on the same).

network devices:

- SNMP v1 capable, min. BRIDGE-MIB, better Q-BRIDGE-MIB
- device must tolerate SNMP scan in a 5 minutes cycle
- device abstraction must be developed for each type of network device
- min. 1 switch and 1 router (or 1 layer 2/3 device) current supported devices:

- HP Procurve series: 25xx, 26xx, 28xx, 4000M, 41xGL, 530x, 6108
- Cisco 6500 series
- F5 Big-IP