

NeDi

Network Discovery that Really Works

Dr. Michael Schwartzkopff, sys4 AG



sys4 AG

Enterprise Experts

What we do ...

- > We solve complex problems
- > We develop custom solutions based on established standards
- > We know which Open Source tools are suitable and reliable
- > Our teams consists of well known experts

Do you know your network?

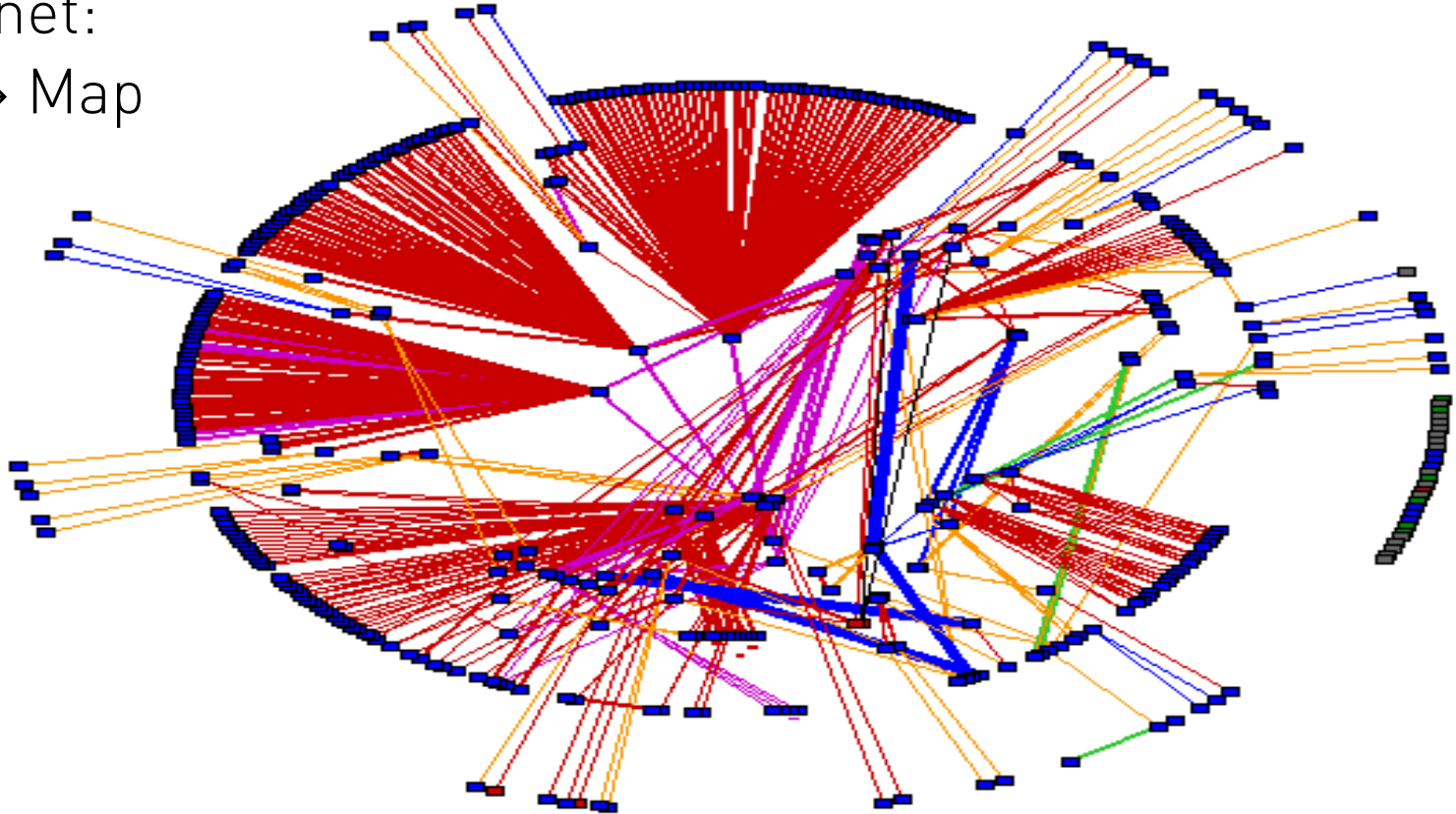
- > Really? All hosts? All devices? Now?
- > Scanning is no solution. Especially with IPv6.
 - > NeDi asks several seed devices for their neighbours.
 - > These neighbours are put on a TODO list.
- > NeDi works recursive through the net.
- > NeDi uses SNMP:
 - > CDP, LLDP, ARP cache, routing table

Simple installation and configuration

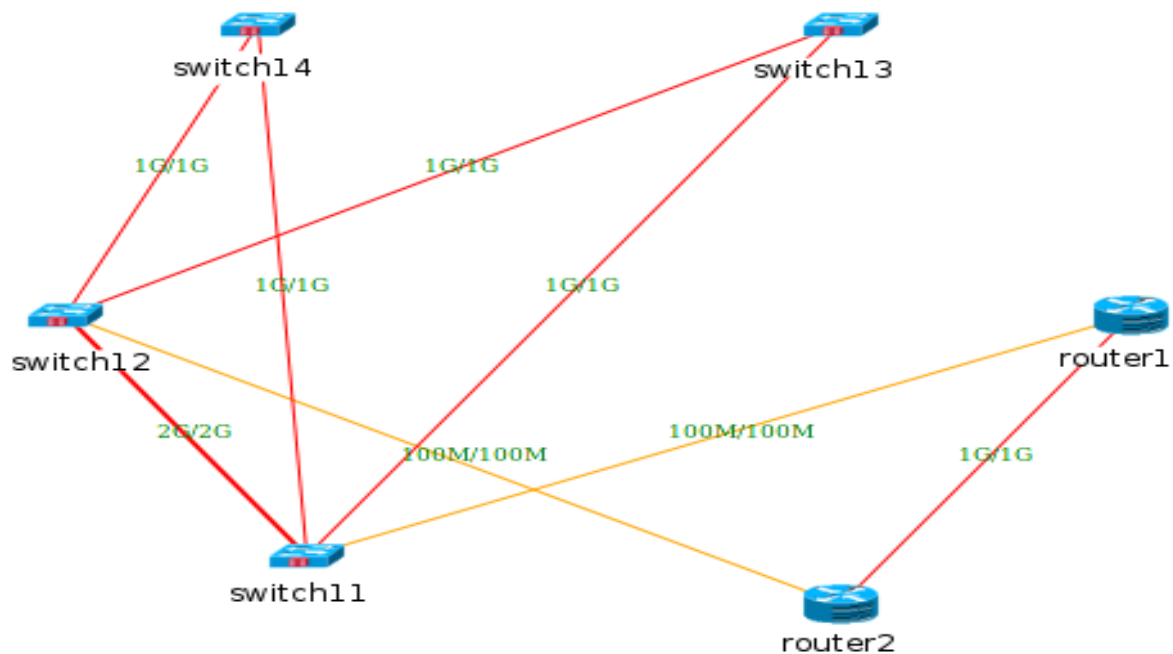
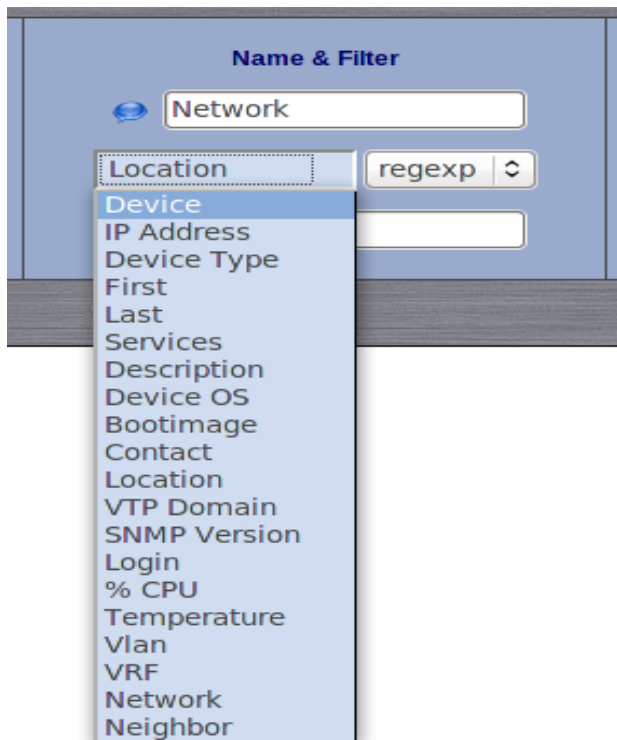
- Unpack the archive to a adequate directory.
- Configure the SNMP community String in *nedi.conf*
- Configure the access to the data base in *nedi.conf*
- Configure your webserver.
- ... and start NeDi:
`nedi -p`
- View the result on the web site.

After one run NeDi knows your net

- > Map of the net:
Topology → Map



Use Filters to Zoom to Parts of the Net



NeDi Collects More Data

- > Walking through the net NeDi collects more data than just neighbourhood:
 - > Devices: Name, IP, OS, version, CPU load, temp, memory
 - > Interfaces: Name, alias, description, statistics
 - > Modules: Modell, serial number, slot, ...
 - > Networks: Name, interfaces, IP, mask, ...
 - > Hosts: name, IP, MAC, VLAN, ...
- > The webinterface offers reports about all data collected:
 - > To what interface *host01* is connected to?
 - > How many ports are unused on *switch01*?

The Database













- > The database scheme of NeDi is very simple.
- > It was designed for speed during discovery, not to avoid redundancies.
- > Display the scheme: *System* → *Export*
- > You can also compile SQL queries here.
- > Of course, you also can use the command line to send requests to the database.

Asset Management

- > NeDi is a perfect basis of an asset management.
- > NeDi finds what really exists on the network.
- > You can use this information to adjust your asset management system.
 - > Are all existing devices listed in your asset management
 - > Do all listed devices still exist?
- > Identify alien equipment in your network.
 - > NeDi is also a tool for the IT security!

Reports

- > Report → Type Distribution














Device Type		
abc Type		Devices
	WS-C4506-E	 79
	WS-C4503-E	 54
	Cisco Wlan AP	 39
	WS-C4948-10GE	 28
	WS-C3560X-48P	 22
	CBS3020-HPQ	 22

- > Possible with all information like software versions, ...

Events

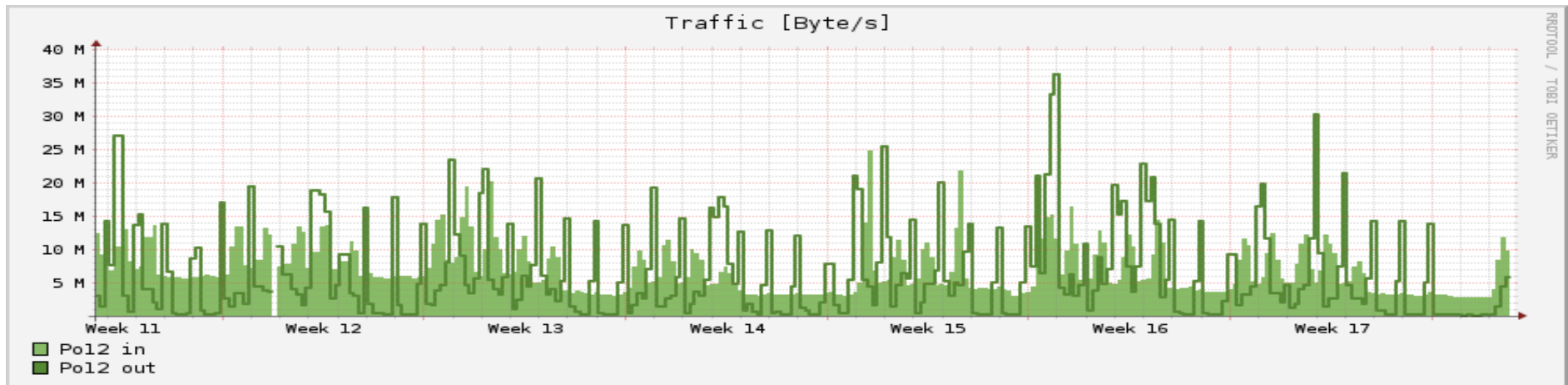
- > NeDi recognizes events in your network.
- > That may be new devices, hosts, or modules.
- > NeDi classifies the events:
 - > Level: Other, Info, Notice, Warning, Alert, Emergency
 - > Class: Traffic, Config, Discover, Device, Security, User, Monitoring, Node
- > The admin configures NeDi to report about specific events (i.e. mail).
- > You also can report events:
 - > When was a specific module installed?
 - > When did a special host appear on the network?

Sample Event

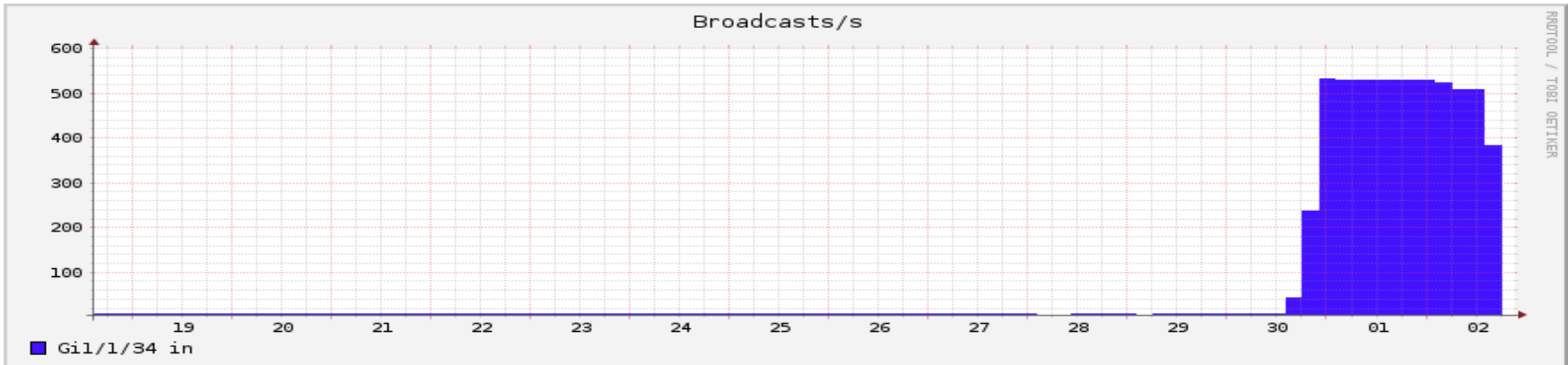
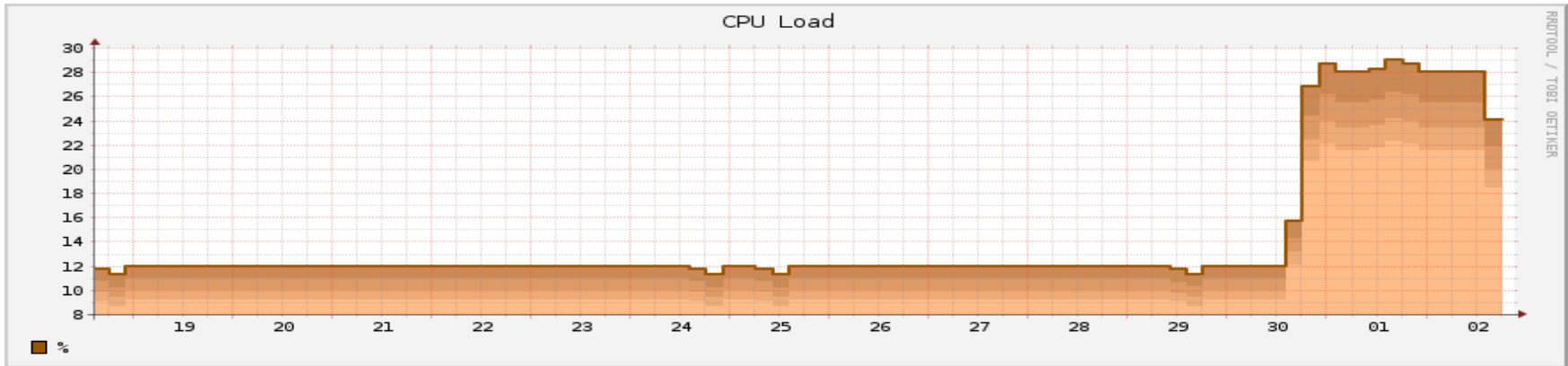
 Source	 Class	 Info
m205s21		New 1000BaseLX SFP module with SN:OPA1438. found in slot GigabitEthernet1/2
m205s21		New 1000BaseLX SFP module with SN:OPA1438 found in slot GigabitEthernet1/1
m205s21		New FRULink 1G Module module with SN:FDO1434. found in slot FRULink Slot 1 - FRULink Module
m205s21		New Switch FRU Fan module with SN: found in slot Fan 1
m205s21		New Switch FRU Fan module with SN: found in slot Fan 0
m205s21		New FRU Power Supply module with SN:LIT1440 found in slot Power Supply 1
m205s21		New FRU Power Supply module with SN:LIT1437 found in slot Power Supply 0
m205s21		Boot image changed from - to c3560e-universalk9-mz.12
m205s21		Serial number changed from noSuchInstance to FDO1441
m205s21		Sysobjid changed from other to 1.3.6.1.4.1.9.1.1229

RRDs for Historic Data

- > NeDi stores all important data in RRDs
 - > Network total: Events, hosts, PoE, interfaces
 - > Device statistics: CPU, temp, memory und MemIO
 - > Interface statistics: Traffic, errors, discards und broadcasts



Graphs Show Errors Fast



Topology

- > The routing tool show the routes through the net. It asks online for the routing tables.
- > Spanning Tree Tabelle
 - > What is the root bridge?
 - > What are the costs of a single interface?
 - > Which ports forwards, which one blocks?
- > In the *link editor* you can add links if NeDi did not discovery the neighbourhood correctly.
- > In the location editor you can add coordinates for locations:
 - > NeDi uses the **sysLocation** OID to locate devices.

New Device Classes

- > NeDi classifies the devices according to their **sysObjectID** (1.3.6.1.2.1.1.2)
- > If NeDi does not know a specific class, you can help it with the *Device Definition Generator*:
 - > NeDi asks for a lot of OIDs and saves it into a definition file.
 - > These files are plain text files.
 - > You can edit it with your preferred editor.

Monitoring

- > NeDi can be used to feed a monitoring system.
- > NeDi can monitor devices on its own.
 - > Request values and send alerts.
 - > Similar to the events from above.
- > NeDi is no replacement for a good monitoring tool like Zabbix, OpenNMS, or nagios.

Config Management

- > If you allow Nedi read access to the command line of your devices, it saves the configuration every discovery run.
- > That makes NeDi a nice config management / backup tool.
- > Special tools like **rancid** can do a little bit more.
 - > Automatic diffs
 - > Versioning (subversion, git, ...)
- > But NeDi is perfect to configure **rancid**.

Write configurations

- > If you allow NeDi write access to the command line of your devices it can change the configuration.
- > Roll-out of mass changes.
 - > i.e. modify ACLs.
- > Interface configuration.
 - > Modify Parameters of interfaces on many devices.
 - > Switch off a port via the GUI.
- > Selection of the devices via the many options.

Discovery

- > NeDi Discovery the neighbourhood via a Logical Link Control Protocol (LLDP)
 - > Cisco's CDP, LLDP, Foundry's FDP
- > But it can discovery *everything* if you you the den ARP Cache of your known devices.
 - > Have fun and run NeDi with ARP cache detection and the community string **public**.
- > Or NeDi can read out the routing tables to discover the next hop.

NeDi – It Works!

- > NeDi helps you to understand your network and to discover vulnerabilities.
- > A discovery run is really fast.
 - > You can optimize the time via some options.
- > NeDi records your network setup and saves all information into its database.
- > The Webinterface allows easy access to all the information.

Thank you very much for your attention!

Contact:

Dr. Michael Schwartzkopff

msl@sys4.de