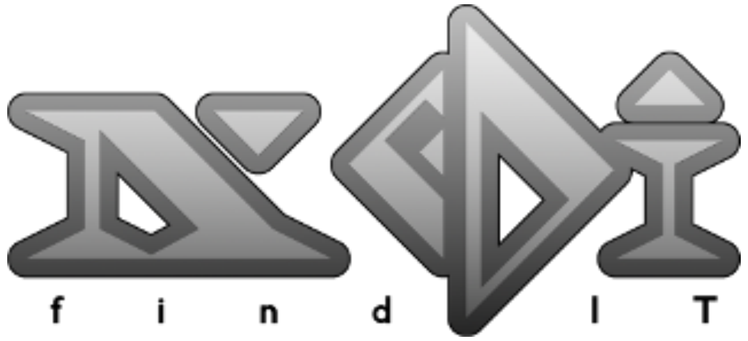


Logstash and Elastic for Networking

www.nedi.ch

ABOUT ME

5 years
7 months

08/2008 - ~~present~~ 4.2014
HP Networking Ambassador
Hewlett Packard
www.hp.com

7 years
3 months

05/2001 - 07/2008
Network & Security Engineer
Paul Scherrer Institute
www.psi.ch

1 year
1 month

04/2000 - 04/2001
Security Engineer
UBS
www.ubs.com

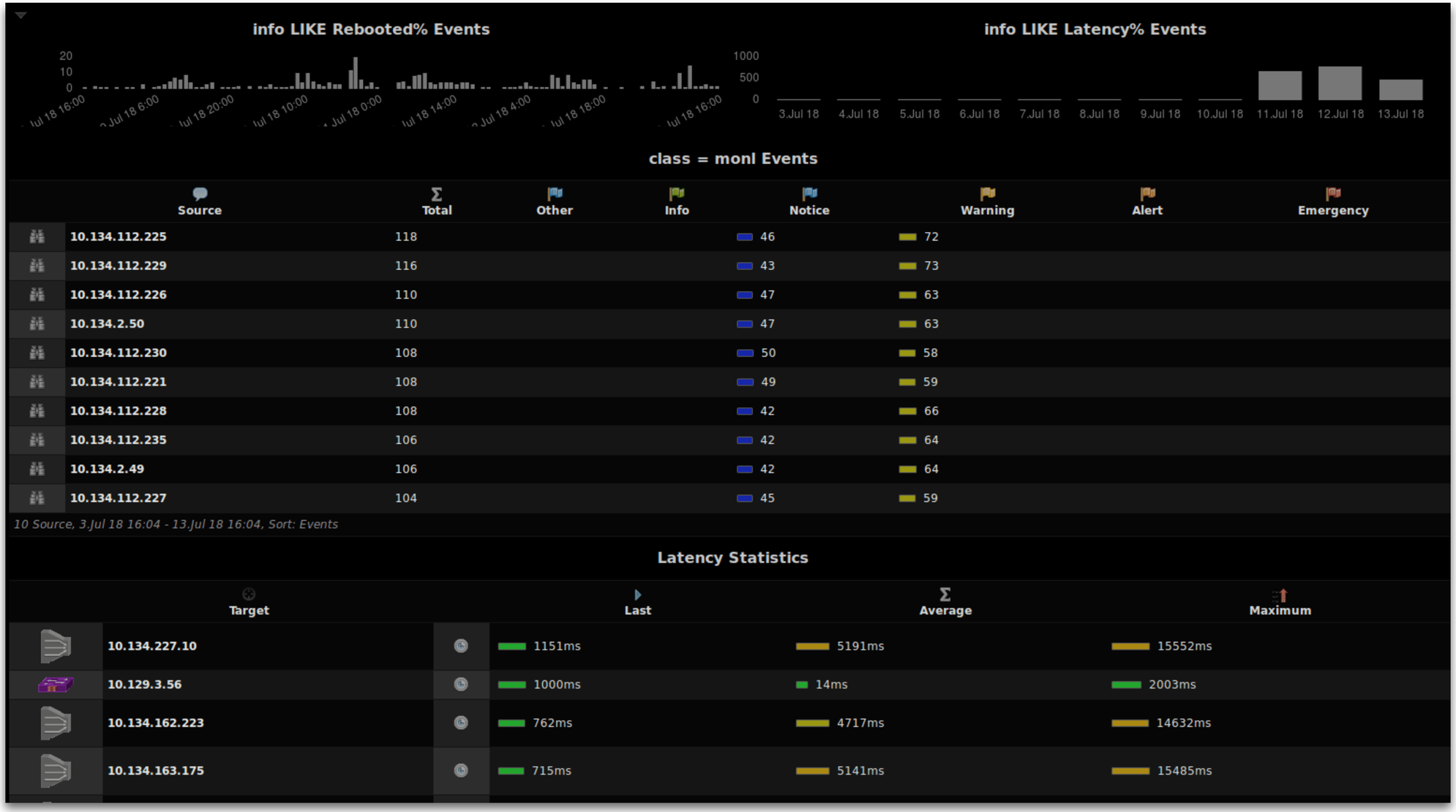
2 years
1 month

12/1997 - 12/1999
Rollout Project Manager
Perot Systems
www.dell.com

3 years
1 month

12/1994 - 12/1997
Network Engineer
SBC (UBS)
www.ubs.com

ABOUT NEDI


info LIKE Rebooted% Events
20
10
0
Jul 18 16:00
Jul 18 6:00
Jul 18 20:00
Jul 18 10:00
Jul 18 0:00
Jul 18 14:00
Jul 18 4:00
Jul 18 18:00
Jul 18 16:00
info LIKE Latency% Events
1000
500
0
3.Jul 18
4.Jul 18
5.Jul 18
6.Jul 18
7.Jul 18
8.Jul 18
9.Jul 18
10.Jul 18
11.Jul 18
12.Jul 18
13.Jul 18
class = monl Events
Source
Total
Other
Info
Notice
Warning
Alert
Emergency
10.134.112.225 118 46 72
10.134.112.229 116 43 73
10.134.112.226 110 47 63
10.134.2.50 110 47 63
10.134.112.230 108 50 58
10.134.112.221 108 49 59
10.134.112.228 108 42 66
10.134.112.235 106 42 64
10.134.2.49 106 42 64
10.134.112.227 104 45 59
10 Source, 3.Jul 18 16:04 - 13.Jul 18 16:04, Sort: Events
Latency Statistics
Target
Last
Average
Maximum
10.134.227.10 1151ms 5191ms 15552ms
10.129.3.56 1000ms 14ms 2003ms
10.134.162.223 762ms 4717ms 14632ms
10.134.163.175 715ms 5141ms 15485ms

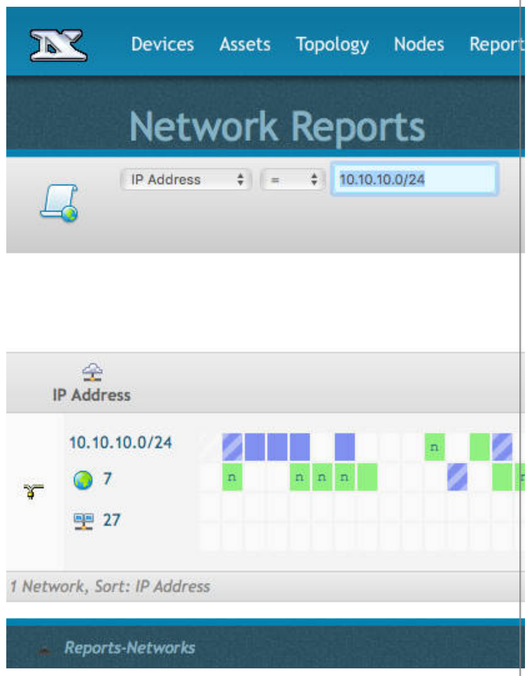
IMPROVED IP INFORMATION

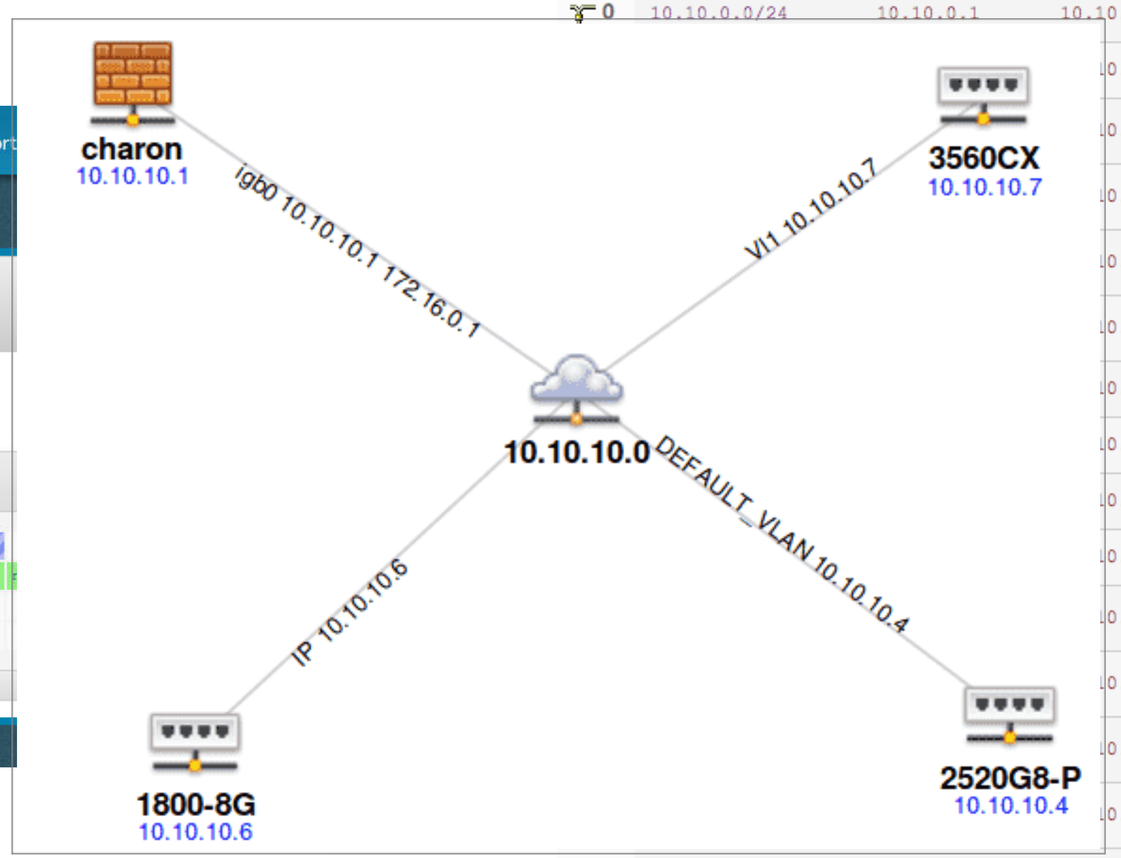
ARP Values

MAC		IP	Update	Services	Operating System	Devices	Port
EDIMAX	74da3825d964	10.10.10.100	10.Apr 19 22:45	SSH-2.0-OpenSSH_6.0p1,nginx/1.2.1,	Debian	charon	igb0
	34ab3731ae83	10.10.10.112	11.Apr 19 9:25			charon	igb0
	b827ebd0b99a	10.10.10.113	11.Apr 19 7:20	SSH-2.0-OpenSSH_7.4p1,	Raspbian	charon	igb0
SAMSUNG	f47b5e0b8b5c	10.10.10.115	11.Apr 19 1:25			charon	igb0
hmd.	ac57755cb432	10.10.10.118	11.Apr 19 8:30		Android 8.0	charon	igb0
	5254006e7f4e	10.10.10.120	11.Apr 19 6:40			charon	igb0
CISCO	000dbd7408ee	10.10.10.124	11.Apr 19 5:40			charon	igb0
CISCO	001bd4a0d4e2	10.10.10.125	11.Apr 19 9:50	SSH-2.0-1.00 ,	Cisco IP Phone	charon	igb0

DHCP-fingerprinting: https://github.com/dumplab/dhcpfingerprint
NeDi Portscan: nedi.pl -sid -O10.10.10.0/24

VERIFY YOUR IPAM





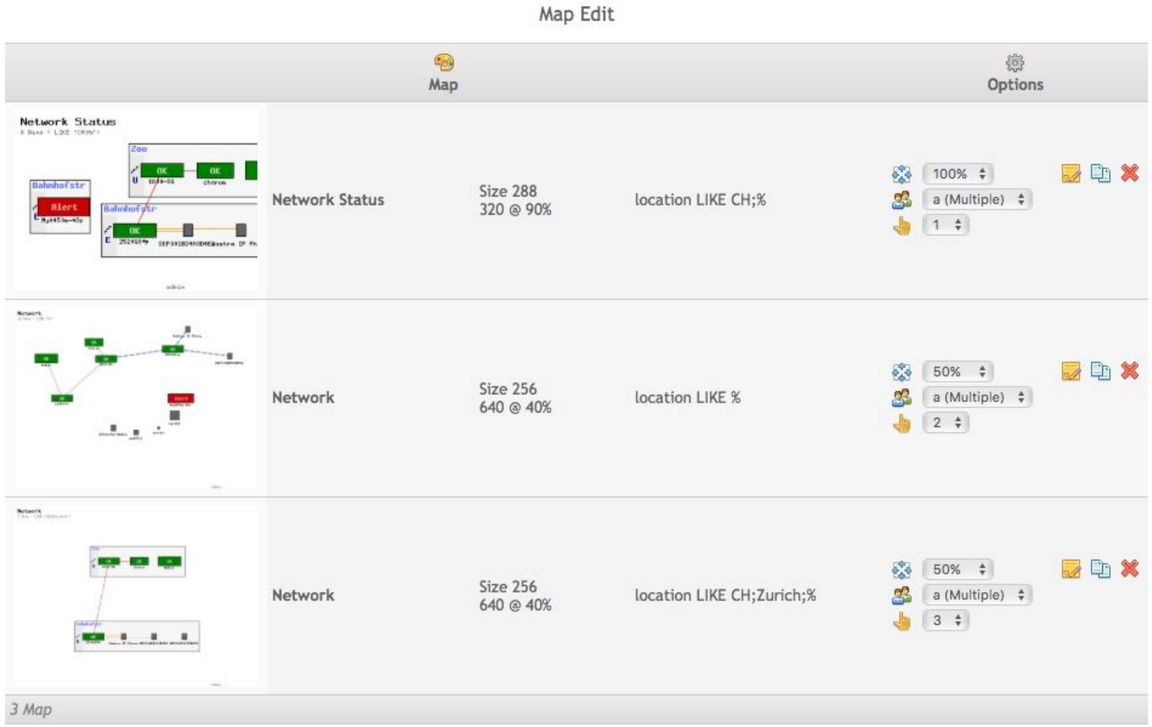
Subnet List

	Network	Start	End	Bcast	Total Population
0	10.10.0.0/24	10.10.0.1	10.10.0.254	10.10.0.255	254
			10.10.1.254	10.10.1.255	508
			10.10.2.254	10.10.2.255	762 1
			10.10.3.254	10.10.3.255	1016 1
			10.10.4.254	10.10.4.255	1270 1
			10.10.5.254	10.10.5.255	1524 1
			10.10.6.254	10.10.6.255	1778
			10.10.7.254	10.10.7.255	2032
			10.10.8.254	10.10.8.255	2286
			10.10.9.254	10.10.9.255	2540
			10.10.10.254	10.10.10.255	2794 25 23 25
			10.10.11.254	10.10.11.255	3048 1
			10.10.12.254	10.10.12.255	3302 1
			10.10.13.254	10.10.13.255	3556 1
14	10.10.14.0/24	10.10.14.1	10.10.14.254	10.10.14.255	3810
15	10.10.15.0/24	10.10.15.1	10.10.15.254	10.10.15.255	4064

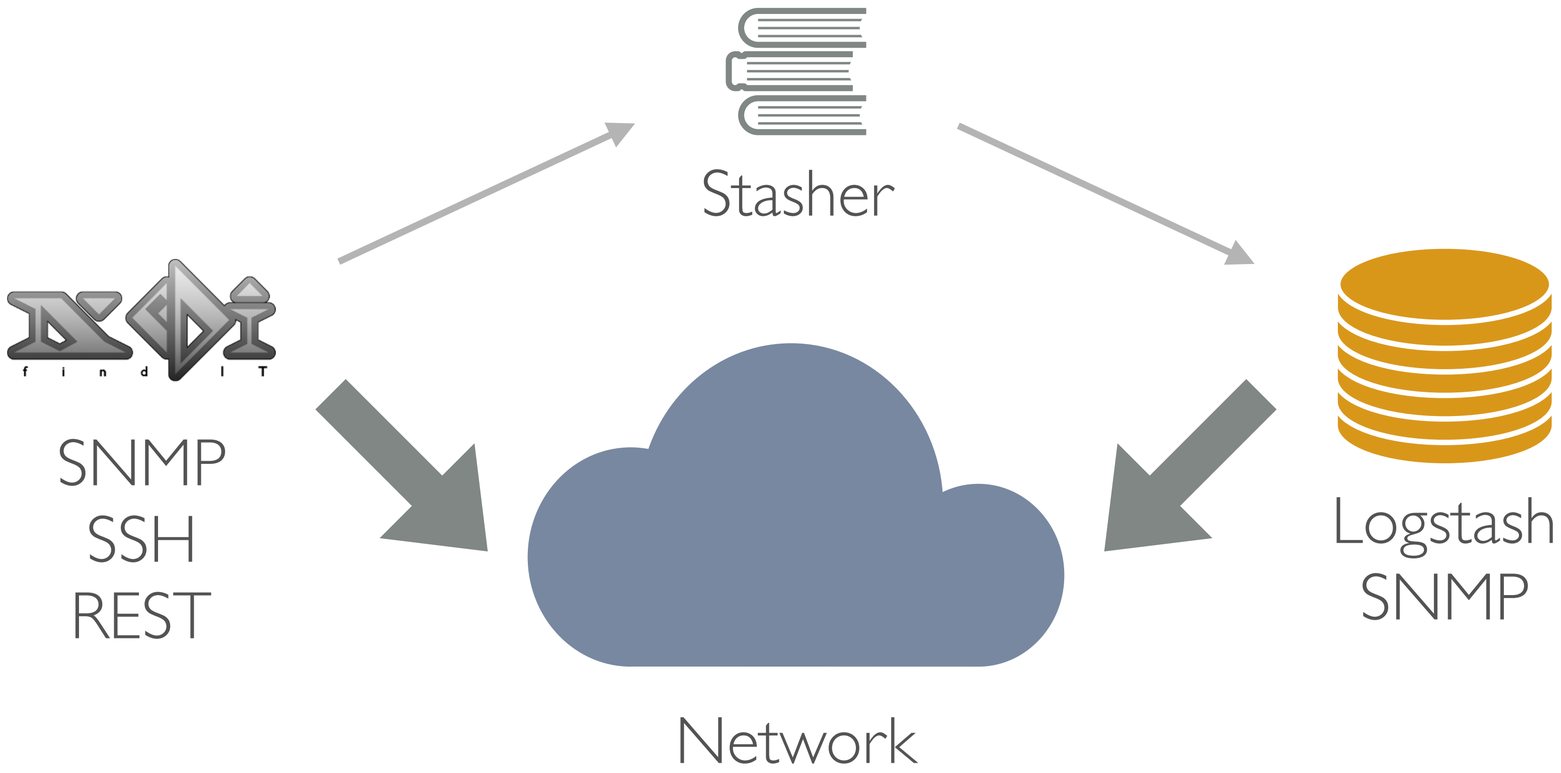
MONITORING

MONITORING MAP

EDITOR



NEDI 2 LOGSTASH



STASHER

```
usage: stasher.pl [Actions]

-U file Use specified configuration (use - to read from stdin)
-O fldr Use specified output folder (default .)
-d opt  b=basic debug,d=DB queries
-v Verbose output
-------------------------------------------------------------
Stasher 0.2 (C) 2019 NeDi Consulting GmbH
```

10_INPUT.CONF

```
input {
  snmp {
    tags => ["NeDi","Switch","Cisco"]
    type => "WS-C2960-8TC-L"
    get  => ["1.3.6.1.4.1.9.9.48.1.1.1.6.1","1.3.6.1.4.1.9.9.109.1.1.1.1.8.1","1.3.6.1.2.1.1.1.0"]
    hosts => ["{host => "udp:10.10.10.3/161" community => "public"}"]
    oid_root_skip => 5
    interval => "${NEDI_SNMP_INTERVAL_OS:60}"
  }
  snmp {
    tags => ["NeDi","Switch","Hewlett-Packard"]
    type => "2520-8G-PoE"
    get  => ["1.3.6.1.2.1.1.1.0","1.3.6.1.4.1.11.2.14.11.5.1.1.2.1.1.1.6.1","1.3.6.1.4.1.11.2.14.11.5.1.9.6.1.0"]
    hosts => ["{host => "udp:10.10.10.4/161" community => "public"}"]
    oid_root_skip => 5
    interval => "${NEDI_SNMP_INTERVAL_OS:60}"
  }
  snmp {
    tags => ["NeDi","Firewall","PC Engines GmbH"]
    type => "begemot-FreeBSD"
    get  => ["1.3.6.1.4.1.2021.4.11.0","1.3.6.1.2.1.1.1.0","1.3.6.1.4.1.2021.11.10.0"]
    hosts => ["{host => "udp:10.10.10.1/161" community => "public"}"]
    oid_root_skip => 5
    interval => "${NEDI_SNMP_INTERVAL_OS:60}"
  }
}
```

20_FILTER_OS.CONF

```
filter {
  # Valid for all types
  mutate {
    rename => [ "[mib-2.system.sysDescr.0]", "[os][description]" ]
  }
  if "WS-C3560CX-8PCS" in [type] {
    mutate {
      rename => [ "[1.3.6.1.4.1.9.9.48.1.1.1.6.1]","[hw][mem-free]" ]
      rename => [ "[1.3.6.1.4.1.9.9.109.1.1.1.1.8.1]","[hw][cpu]" ]
      rename => [ "[1.3.6.1.4.1.9.9.13.1.3.1.3.1004]","[hw][temp]" ]
      rename => [ "[1.3.6.1.2.1.1.1.0]","[os][description]" ]
    }
  }
  if "2520-8G-PoE" in [type] {
    mutate {
      rename => [ "[1.3.6.1.2.1.1.1.0]","[os][description]" ]
      rename => [ "[1.3.6.1.4.1.11.2.14.11.5.1.1.2.1.1.1.6.1]","[hw][mem-free]" ]
      rename => [ "[1.3.6.1.4.1.11.2.14.11.5.1.9.6.1.0]","[hw][cpu]" ]
    }
  }
  if "begemot-FreeBSD" in [type] {
    mutate {
      rename => [ "[1.3.6.1.4.1.2021.4.11.0]","[hw][mem-free]" ]
      rename => [ "[1.3.6.1.2.1.1.1.0]","[os][description]" ]
      rename => [ "[1.3.6.1.4.1.2021.11.10.0]","[hw][cpu]" ]
    }
  }
}
```

30_OUTPUT_ELASTIC.CONF (STATIC)

```
# -----------------------------------------------------------------------------
# Output to Elasticsearch
# -----------------------------------------------------------------------------

output {
  elasticsearch {
    hosts => ["192.168.32.101:9200"]
    user => "elastic"
    password => "admin123"
    index => "snmp-network-%{+YYYY.MM.dd}"
    template => "/etc/logstash/snmp_network/templates/snmp_network.template.json"
    template_name => "snmp_network"
    template_overwrite => "true"
  }
}
```

THANKS!