

— Mirko G. Hammann

Netzwerk-Automation mit dem HP Network Node Manager

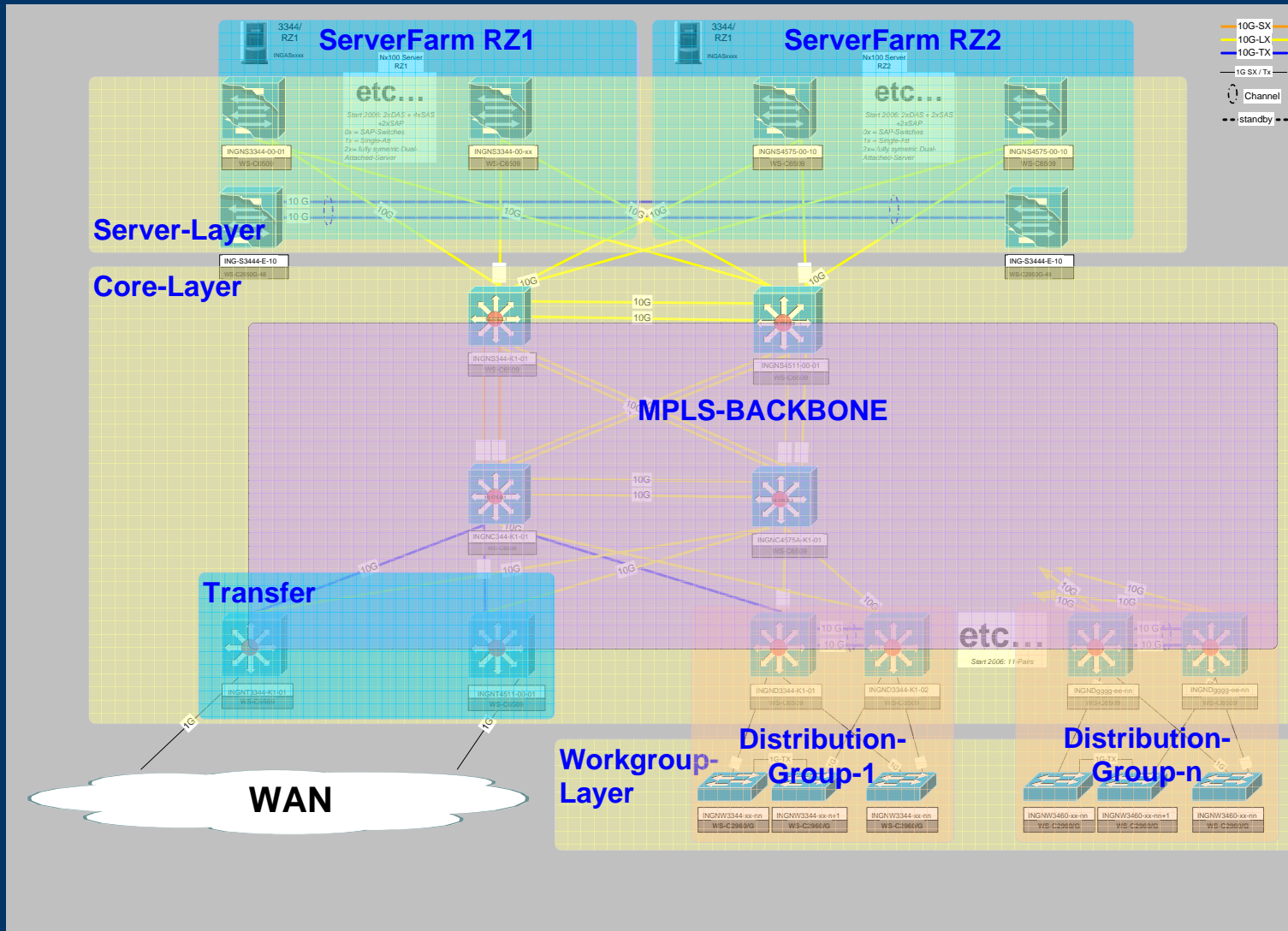
Boehringer Ingelheim

- chemische und pharmazeutische Produktpalette
- bekannte Produkte: Thomapyrin[®], Mucosolvan[®], frubias[®]
- 40.000 Mitarbeiter weltweit, 10.000 Mitarbeiter deutschlandweit
- 3 Standorte in Deutschland: Biberach, Dortmund, Ingelheim
- Netzwerk besteht an den drei Standorten aus 2260 Switches und 476 APs
- interne IT-Abteilung mit 450 Mitarbeitern

Netzwerk-Team

- Erstellen und optimieren von Betriebskonzepten für das Netzwerk
- Überwachung der Funktionsfähigkeit des Netzwerkes
- Instandhaltung der vorhandenen Infrastruktur
- Erweiterung der Infrastruktur
- Konfiguration von Netzwerkkomponenten

BI-Netzwerk



Konfiguration von Workgroup-Switches

Früher:

- eine Standardkonfiguration wurde aufgespielt
- individuelle Einstellungen (z.B. Hostname) wurden manuell angepasst

Nachteile:

- Welche ist die aktuelle Standardkonfiguration?
- bei individuellen Einstellungen können Fehler auftreten (Fehlerfaktor Mensch)
- Installation und Recovery kann nur von Fachpersonal durchgeführt werden

Gründe zur Automatisierung

Welche Vorteile bietet eine automatisierte Konfiguration von Netzwerkkomponenten?

- standardisierte Konfiguration auf allen Komponenten
- einfache, schnelle und kostengünstige Installation und Recovery von Komponenten
- schnelle Integration neuer Komponententypen
- einfache Anpassungen der Konfiguration durch Templates

Voraussetzungen

Welche Voraussetzungen muss ein Switch erfüllen, damit man ihn automatisiert konfigurieren kann?

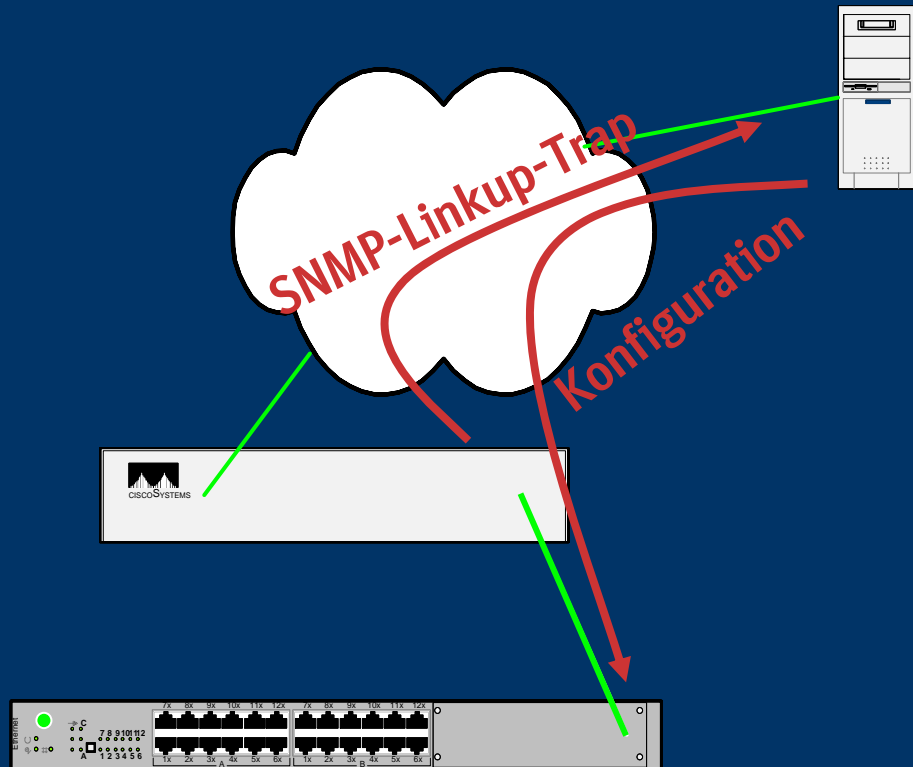
- der Uplink des Switches muss nach Start automatisch aktiviert werden
- der Switch muss nach dem Start über DHCP eine IP-Adresse bekommen
- der Switch muss von der NMM-Station erreichbar sein

Cisco Autoinstall-Prozess

Aktuelle Cisco Workgroup-Switches (z.B. C2960) erfüllen die genannten Voraussetzungen. Sie besitzen einen so genannten Autoinstall-Prozess:

1. Switch ist unkonfiguriert und wird zum ersten Mal angeschaltet
2. Switch aktiviert auf seinem Uplink das native VLAN 1
3. Switch fordert über DHCP eine IP-Adresse an
4. Switch sucht via Broadcast eine Konfigurationsdatei
5. Switch lädt über TFTP eine Konfigurationsdatei

Schematische Übersicht



Nodemanager

All Alarms Browser					
File Actions View					Help
Ack	Corr	Severity	Date/Time	Source	Message
		Normal	Mon Nov 03 07:56:47	10.176.175.16	Cisco_Default Trap: [1] mgmt.mib-2.system.sysUpTime.sysUpTimeInstan
✓		Minor	Mon Nov 03 07:56:53	ingne3344-k1-01.eu.boehringer.com	linkDown on GigabitEthernet2/4 (ifndex=52; ifType=ether:
✓		Minor	Mon Nov 03 07:56:54	ingne3344-k1-02.eu.boehringer.com	linkDown on GigabitEthernet2/4 (ifndex=52; ifType=ether:
		Warning	Mon Nov 03 07:56:55	ingne3344-k1-01.eu.boehringer.com	Port GigabitEthernet2/4 (ifAlias: NW3344-K1-03-TEST_A)
		Minor	Mon Nov 03 07:56:55	ingne3344-k1-01.eu.boehringer.com	rmn Minor linkdown on interface NW3344-K1-03-TEST_A
		Minor	Mon Nov 03 07:56:55	ingne3344-k1-02.eu.boehringer.com	rmn Minor linkdown on interface NW3344-K1-03-TEST_B
✓		Warning	Mon Nov 03 07:57:11	dtmnw9252-01-17.eu.boehringer.com	linkDown on GigabitEthernet0/10 (ifndex=10110; ifType=e
✓	1	Normal	Mon Nov 03 07:57:16	dtmnw9252-01-17.eu.boehringer.com	linkUp on GigabitEthernet0/10 (ifndex=10110; ifType=eth
✓		Warning	Mon Nov 03 07:57:30	dtmnw9252-01-17.eu.boehringer.com	linkDown on GigabitEthernet0/10 (ifndex=10110; ifType=e
✓	1	Normal	Mon Nov 03 07:57:34	dtmnw9252-01-17.eu.boehringer.com	linkUp on GigabitEthernet0/10 (ifndex=10110; ifType=eth
		Warning	Mon Nov 03 07:58:37	ingne3344-k1-01.eu.boehringer.com	Port GigabitEthernet2/4 (ifAlias: NW3344-K1-03-TEST A)
✓	1	Normal	Mon Nov 03 07:58:37	ingne3344-k1-02.eu.boehringer.com	linkUp on GigabitEthernet2/4 (ifndex=52; ifType=etherne
✓	1	Normal	Mon Nov 03 07:58:37	ingne3344-k1-01.eu.boehringer.com	linkUp on GigabitEthernet2/4 (ifndex=52; ifType=etherne
✓		Warning	Mon Nov 03 08:01:57	dtmnw9250k-01-04.eu.boehringer.com	linkDown on GigabitEthernet0/3 (ifndex=10103; ifType=e
✓	1	Normal	Mon Nov 03 08:02:01	dtmnw9250k-01-04.eu.boehringer.com	linkUp on GigabitEthernet0/3 (ifndex=10103; ifType=eth
		Normal	Mon Nov 03 08:02:03	dtmnw9251-01-09.eu.boehringer.com	linkUp on GigabitEthernet0/11 (ifndex=10111; ifType=eth
		Warning	Mon Nov 03 08:02:16	dtmnw9251-01-08.eu.boehringer.com	linkDown on GigabitEthernet0/2 (ifndex=10102; ifType=et
		Warning	Mon Nov 03 08:02:17	dtmnw9250k-01-04.eu.boehringer.com	linkDown on GigabitEthernet0/3 (ifndex=10103; ifType=e

3530 Alarms - Critical:2 Major:33 Minor:58 Warning:1652 Normal:1785 (1338 acknowledged)

Event Configuration

Event Configuration for ingmsov5.eu.boehringer.com

File Edit View Help

Enterprise Identification

Enterprise Name	Enterprise ID
modular	.1.3.6.1.4.1.3181.3.4
meetingplaceEventsV	.1.3.6.1.4.1.7185.3.1.3
switchingTraps	.1.3.6.1.4.1.14179.1.50
bsnTraps	.1.3.6.1.4.1.14179.2.6.3
acNotifications	.1.3.6.1.4.1.17471.0
manager	.1.3.6.1.4.1.17471.1.2
coreServer	.1.3.6.1.4.1.17471.1.3
edgeServer	.1.3.6.1.4.1.17471.1.4
snmpTraps	.1.3.6.1.6.3.1.1.5

Event Identification

Event Name	Event Identif
SNMP_Cold_Start	.1.3.6.1.6.3
SNMP_Warm_Start	.1.3.6.1.6.3
SNMP_Link_Down	.1.3.6.1.6.3
SNMP_Link_Up-Autoinstall-Test	.1.3.6.1.6.3
SNMP_Link_Up_autoinstall	.1.3.6.1.6.3
SNMP_Link_Up	.1.3.6.1.6.3
SNMP_Authen_Failure	.1.3.6.1.6.3
SNMP_EGP_Down	.1.3.6.1.6.3

Event Configurator / Modify Event for ingmsov5.eu.boehringer.com

Event Name	Event Type	Event Object Identifier
SNMP_Link_Up_autoinstall	Link Up	.1.3.6.1.6.3.1.1.5.4

Event Description

A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.

Event Sources (all sources if list is empty)

/etc/opt/OV/share/conf/EventSourceList_AUTOINSTALL.txt

Add From Map

Delete

Delete All

Source

Add

Category Cisco Alarms Forward Event Severity Normal

Event Log Message

```
linkUp on $2 (ifindex=$1; ifType=$3; locIfReason=$4) AUTOINSTALL will run
```

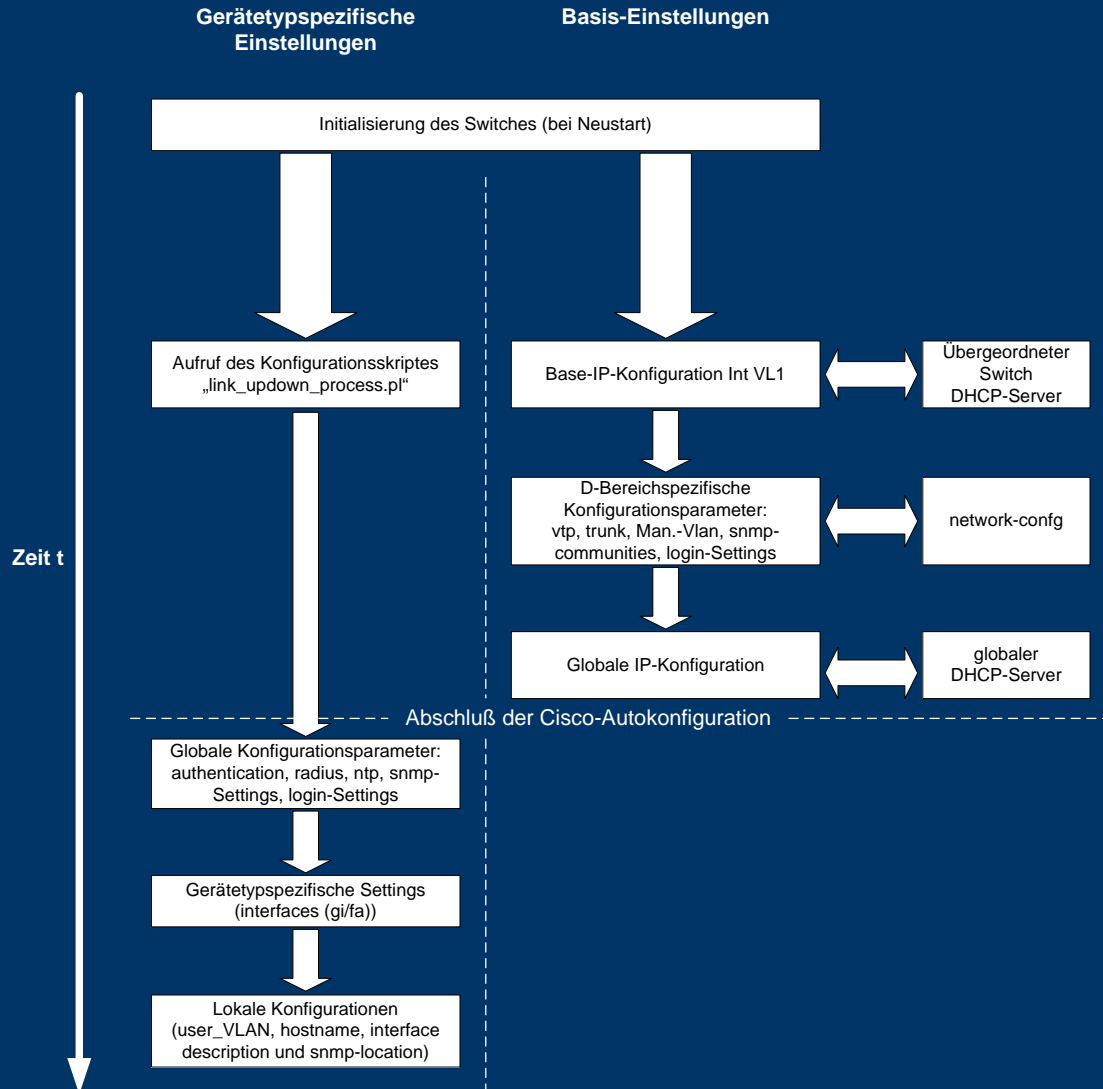
Pop-up Notification (Optional)

Command for Automatic Action (Optional)

```
link_updown_process $x $X $s $r $N $1 IOS up &
```

OK Reset Cancel Help

Prozessablauf



Gefahren

Welche Risiken gibt es bei einer automatisierten Konfiguration?

- bei einem konfigurierten Switch kann die Konfiguration überschrieben werden
- es können zu viele Switches auf einmal das Skript aufrufen (z.B. bei einem Stromausfall)
- falsche Portdescription, die zu falschem Hostname führen
- die Trunksetting können falsch gesetzt sein

Sicherheitsvorkehrungen

Welche Sicherheitsvorkehrungen wurden getroffen, um die Risiken zu minimieren?

- es wird geprüft, ob der Switch eine Konfiguration und einen Hostname besitzt
- es wird nur eine Konfiguration durchgeführt, wenn der Switch als Hostname „ingnwx“ heißt. Diesen Namen hat er von der Cisco Autoinstall Konfiguration erhalten hat.
- Counter verhindern, dass das Skript zu oft gestartet wird
- Timer terminieren nach einer zu langen Wartedauer das Skript
- mit regulären Ausdrücke wird auf die Einhaltung von Namenskonventionen geachtet
- Trunkparameter und IP-Adressen werden auf Plausibilität geprüft

Aktueller Stand

- in zwei Jahren wurden ca. 1500 Switches automatisch konfiguriert
- der Prozess ist an allen drei Standorten in Deutschland etabliert
- die Konfiguration kann durch sitespezifische Einstellungen von jedem Standort aus durchgeführt werden
- alle notwendigen Einstellungen sind für die jeweiligen Standorte und Switchtypen parametrisierbar, es sind keine Codeänderungen notwendig
- aufgetretene Probleme waren größtenteils auf Fehlkonfigurationen zurückzuführen

Ausblick

- Europaweite Nutzung der automatisierten Konfiguration in den nächsten zwei Jahren
- Webinterface zur einfacheren Konfiguration und besseren Übersichtlichkeit
- Integration weiterer Switchtypen

Anhang

Anforderungen – Übergeordneter Switch

- Interface VLAN 1 muss konfiguriert sein, d.h. es muss eine IP-Adresse haben und auf no shutdown gesetzt sein
- dem VLAN 1 muss ein lokaler DHCP-Dienst zugeordnet sein, dabei darf die Lease-Time für den DHCP-Dienst nicht zu groß eingestellt werden
- SNMP-Link-Up-Traps an den Ports müssen eingeschaltet sein
- die Grundkonfigurationsdatei network-config muss auf disk0 abgelegt sein und dem tftp-server zugeordnet werden
- es muss ein Management-VLAN definiert sein, das für die Workgroup-Switches in der Datei network-config initialisiert werden muss
- es muss für jeden Port, an dem ein Workgroup-Switch hängt, eine portdescription gesetzt sein

Anforderungen – Workgroup-Switch

- es darf keine *config.text*, *private-config.text* und *vlan.dat* vorhanden sein
- die IOS-Version auf dem Flash muss größer als 12.2(25)SEE sein (mit Kryptographie und Cisco-Autoinstall-Prozess)

Unterstützte Access Switcher Typen

- es werden folgende Switch-Typen der Firma Cisco werden von dem automatischen Konfigurationsskript unterstützt:
 - WS-C2960-8TC-L
 - WS-C2960G-8TC-L
 - WS-C2960-24TC-L
 - WS-C2960G-24TC-L
 - WS-C2970G-24T-E
 - WS-C3560-8PC-S
 - WS-C3560-24PS-E
 - WS-C3750G-24TS-E

Anforderungen – NNM

- es muss mindestens Perl-Version 5.8.0 installiert sein
- es müssen die folgenden Perl-Module installiert sein: Net::SNMP, Socket, Time::Local
- das Betriebssystem muss HP-UX oder ein vergleichbares Unix- bzw. Linux-Derivat sein
- der primäre Switch muss in die Event Configuration eingepflegt werden
- Unter HP-UX muss darauf geachtet werden, dass der Action-Daemon den Prozess nicht nach 300 Sekunden terminiert. Dies kann unter anderem dadurch verhindert werden, indem man den Prozess für das Skript beim Starten mit „&“ in den Hintergrund versetzt.