Backing up Network Devices

Julien Goodwin
@laptop006
jgoodwin@studio442.com.au

How many of you have?

- Switches / Routers / Firewalls / etc.
- A backup copy of the OS image?
- A copy of the config when deployed?
- A copy of the current config?
- A copy of the *actual* current config?
- Notifications whenever config changes?
- Automated documentation & verification of config & deployment?

Step 1: The OS

- Create a file repository, archive all current versions of relevant OS'
- As preparation for an upgrade ensure both new and current version are in archive
- If a failure might cut you off from archive copy to a USB drive or similar

Step 2: The Config

Manual – Random

- “Every now and again” copy config to files / wiki
- Means you will miss changes

Manual – Change

- Store archive of config on every change
- What happens when someone does an un-managed change?

Automatic – Push

- On config change send config to repo
- Silent failures
  - If offline
  - If admin turns off
- Limited Support
  - Juniper JunOS
  - Cisco IOS 12.4+
- Often no / limited version control

Automatic – Pull

- Central service pulls config on schedule
- Can notify on failures
  - Including cases of admin manipulation

Rancid

Really Awesome New Cisco config Differ

What?

“RANCID monitors a device's configuration, including software and hardware (cards, serial numbers, etc) and uses CVS or Subversion to maintain history of changes.”

http://www.shrubbery.net/rancid/

What Devices?

- Cisco IOS / IOS-XR / IOS-XE
- Juniper JunOS
- Juniper ScreenOS
- Foundry IronWare & derivatives
- Extreme ExtremeWare (not XOS)
- Quagga
- and more...

How?

- Launched via cron job
- Uses telnet / SSH to connect to devices
- Runs set commands, stores output in files
- Commits to a VCS (CVS / SVN)
- E-mails diffs to a set alias

Logins

- Password only
- For Cisco IOS handles enable password
- Use login classes to prevent any abuse

Benefits

The basics

- Configuration history
- Hardware inventories
- Filesystem details

Version Inventory

```
   Make          OS            Model      Version
=======-===========-================-============
Juniper       JunOS            J6350    10.0R2.10      border1.richmond.vic.au.editure.net
Juniper       JunOS            J4350    10.0R2.10            border2.nm.vic.au.editure.net
  Cisco         IOS    AIR-AP1231G-A  12.3(8)JEC2              ap1.internal.schools.net.au
  Cisco         IOS   AIR-AP1232AG-N  12.3(8)JEC2              ap2.internal.schools.net.au
Juniper       JunOS           SRX650    10.2R3.10           nm-fw-01.nm.vic.au.editure.net
  Cisco         IOS     WS-C2950G-48 12.1(22)EA13         nm-sw-01.internal.schools.net.au
  Cisco         IOS     WS-C2950G-48 12.1(22)EA13         nm-sw-02.internal.schools.net.au
Extreme ExtremeWare       Summit48si      7.6.4.4         nm-sw-03.internal.schools.net.au
Extreme ExtremeWare       Summit48si      7.6.4.4         nm-sw-04.internal.schools.net.au
Juniper       JunOS       EX4200-48T      9.5R3.7     nm-sw-stack-01.nm.vic.au.editure.net
  Cisco         IOS WS-C2960G-48TC-L   12.2(50)SE                  switch.s9.myschools.net
Foundry    IronWare     ServerIronGT  10.2.00dTD2                lb1.vicdir.schools.net.au
Foundry    IronWare     ServerIronGT  10.2.01cTD2                lb2.vicdir.schools.net.au
Juniper       JunOS          SRX240H    10.2R3.10           pm-fw-01.pm.vic.au.editure.net
Extreme         XOS        X450a-48t    12.0.1.11            sw-ext1.vicdir.schools.net.au
Extreme         XOS        X450a-48t    12.0.1.11            sw-int1.vicdir.schools.net.au
```

Basic Configuration

```
Hostname                              DNS    NTP    SNMP
========================================================
        border2.nm.vic.au.editure.net yes    yes     yes
  border1.richmond.vic.au.editure.net yes    yes     yes
              switch.s9.myschools.net yes    yes     yes
     nm-sw-03.internal.schools.net.au yes    yes     yes
     nm-sw-01.internal.schools.net.au yes    yes     yes
 nm-sw-stack-01.nm.vic.au.editure.net yes    yes     yes
          ap1.internal.schools.net.au yes    yes     yes
       nm-fw-01.nm.vic.au.editure.net yes    yes     yes
          ap2.internal.schools.net.au yes    yes     yes
     nm-sw-04.internal.schools.net.au yes    yes     yes
     nm-sw-02.internal.schools.net.au yes    yes     yes
            lb1.vicdir.schools.net.au yes    yes     yes
            lb2.vicdir.schools.net.au yes    yes     yes
```

Verify Reverse DNS

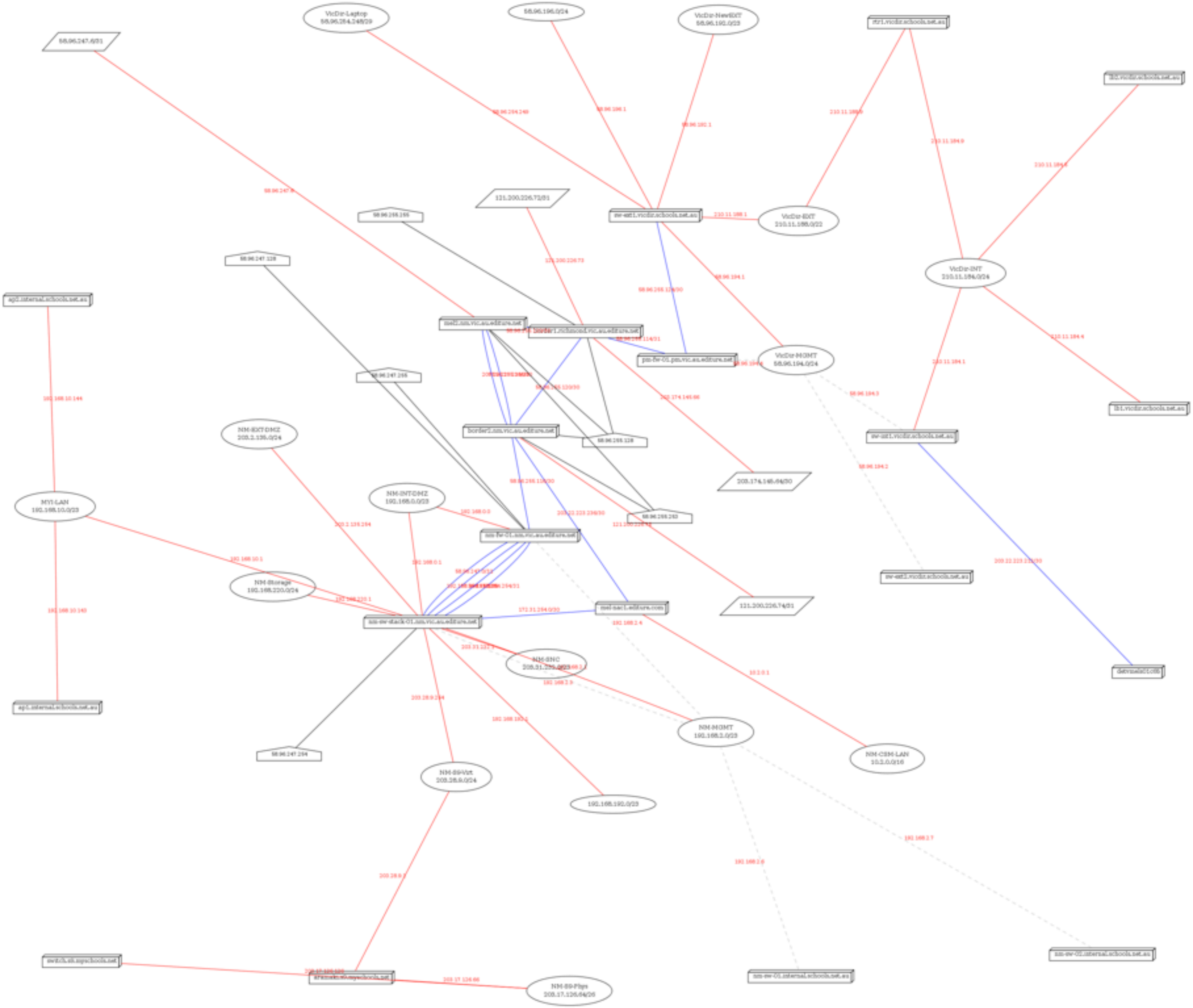
- Extract all interface addresses
- Look them up
- Display them

Verify HA Configurations

- Compare two devices config
- (Ab)use SED/AWK/Perl to remove expected differences
- Diff the result

Automated Network Diagram

- Iterate through configs, extract addresses:
  - Interface
  - Loopback
  - Virtual
  - NAT pools
- Map with graphviz or similar



Tuesday, 25 January 2011

Linking other tools

- Add to Nagios for health monitoring
- Add to MRTG/Cacti/Munin/etc. for interface & environmental monitoring
- Auto-generate DNS zones

Pushing

- Rancid can also be used as a basis for pushing configs
- Makes reverting easier
- Or pushing new configs from a template system

Auto-Discovery

An Aside...

Auto Discovery

- Automatic finding of new devices
- Add them to existing management tools
- But should you?

Next Steps

Config Generation

Templates

- Common standard bits of config
- For Example:
  - Login config
  - Routing protocols
  - SNMP

Netomata Config Generator

What?

- Template based config generator
- Similar to many HTML template languages
- Uses ERB
    - Great for puppet users

Inputs

- Templates
- Device Information Database

What can you manage?

- Hosts
  - /etc/network/interfaces (etc.)
- Devices
  - Cisco config, policies, VLAN databases
  - DNS Zones

Developing Templates

1. Choose a token device
2. Create a template to match config
    - For IOS type remember “no XXX” commands
3. Choose a similar devices
4. Manipulate template until all devices work
5. Move to a new type of device
6. Goto 1

Notch

What?

- CLI Abstraction Layer
- Written in Python
- Primarily out of Google Sydney

Tools

- PUNC - Rancid replacement
- Mr. CLI - clusterssh for routers

References

- Nanog talks
  - Rancid – NANOG26 http://bit.ly/hDSEaL
  - Netomata – NANOG49 http://bit.ly/f3Vpwe
- Notch – http://code.google.com/p/punc/