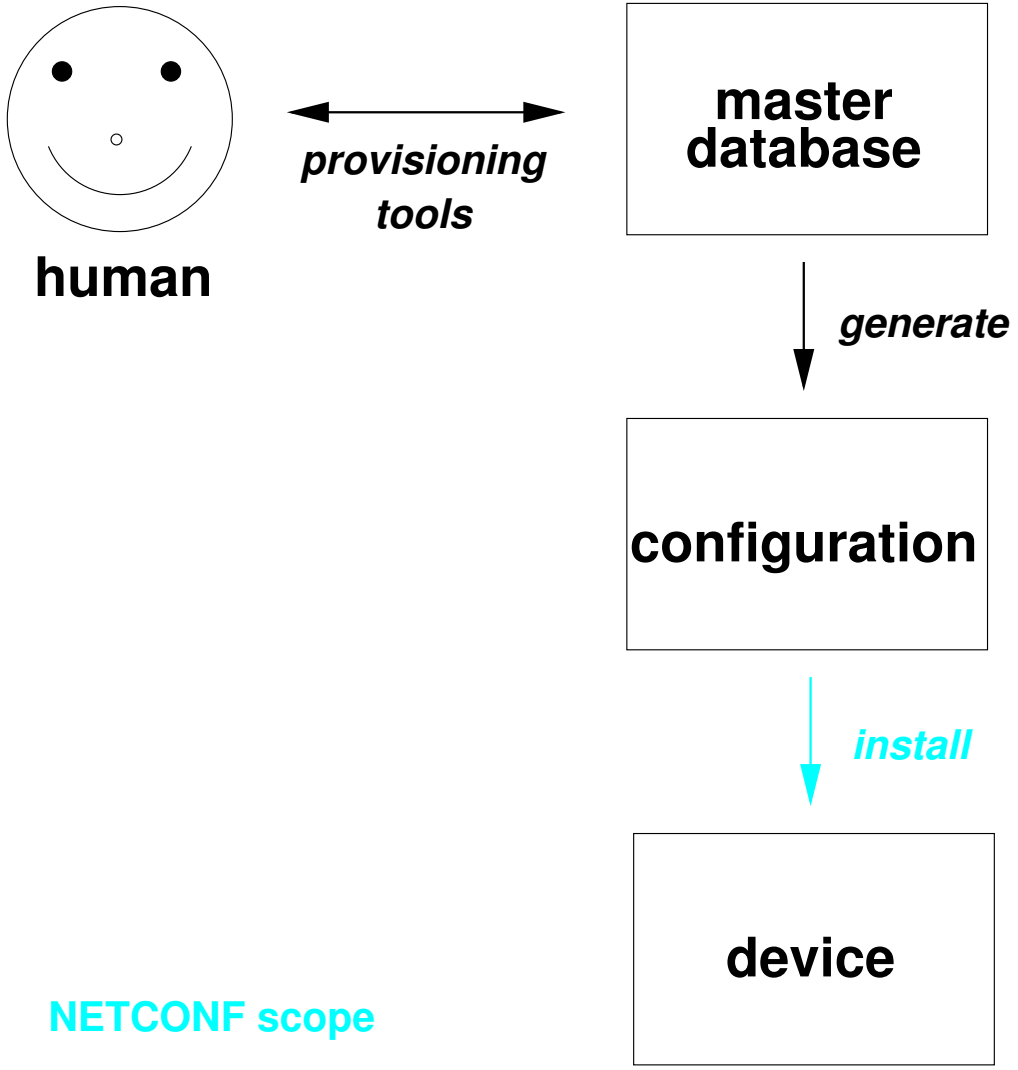
NETwork CONFiguration

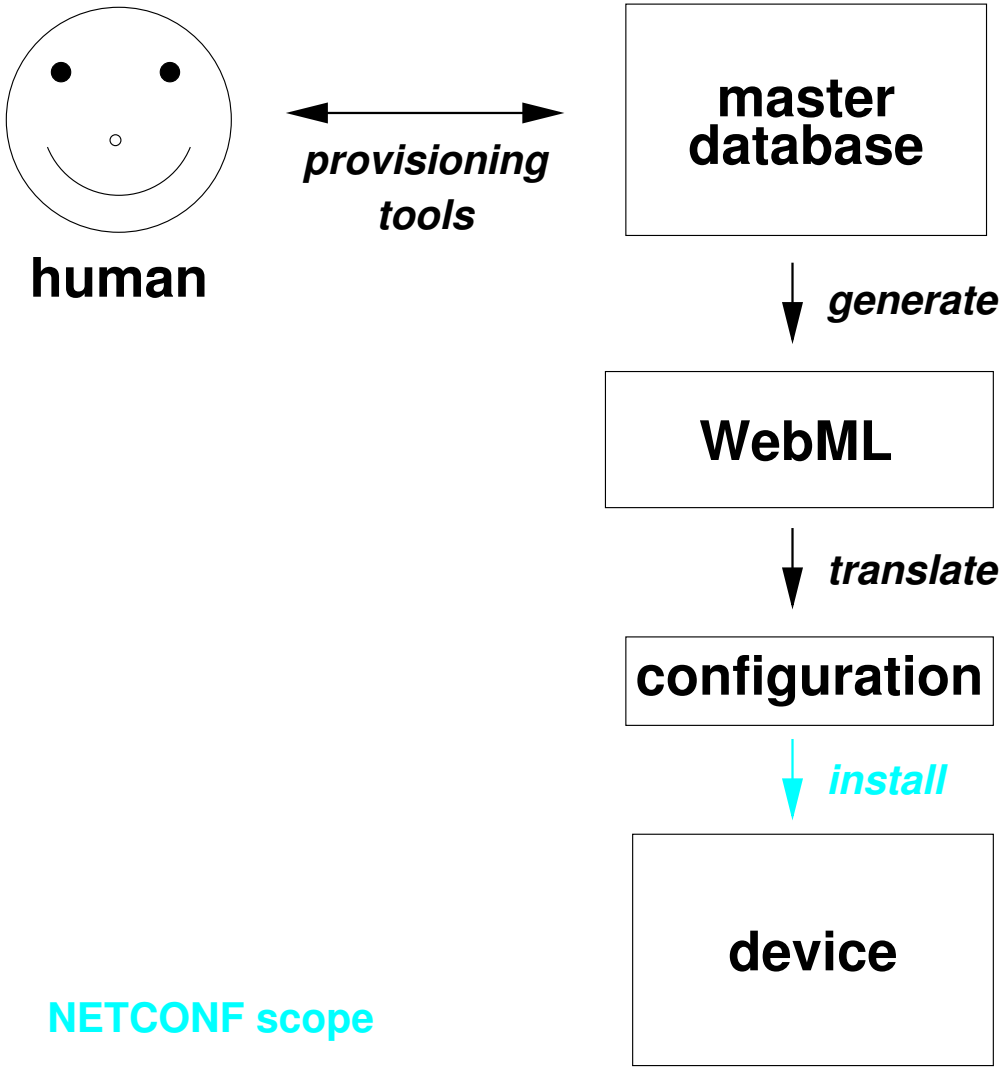
Simon Leinen, SWITCH <simon@switch.ch>

- Approaches to the Network Configuration Problem
- Prior and current IETF activities
- Discussion of practices and requirements

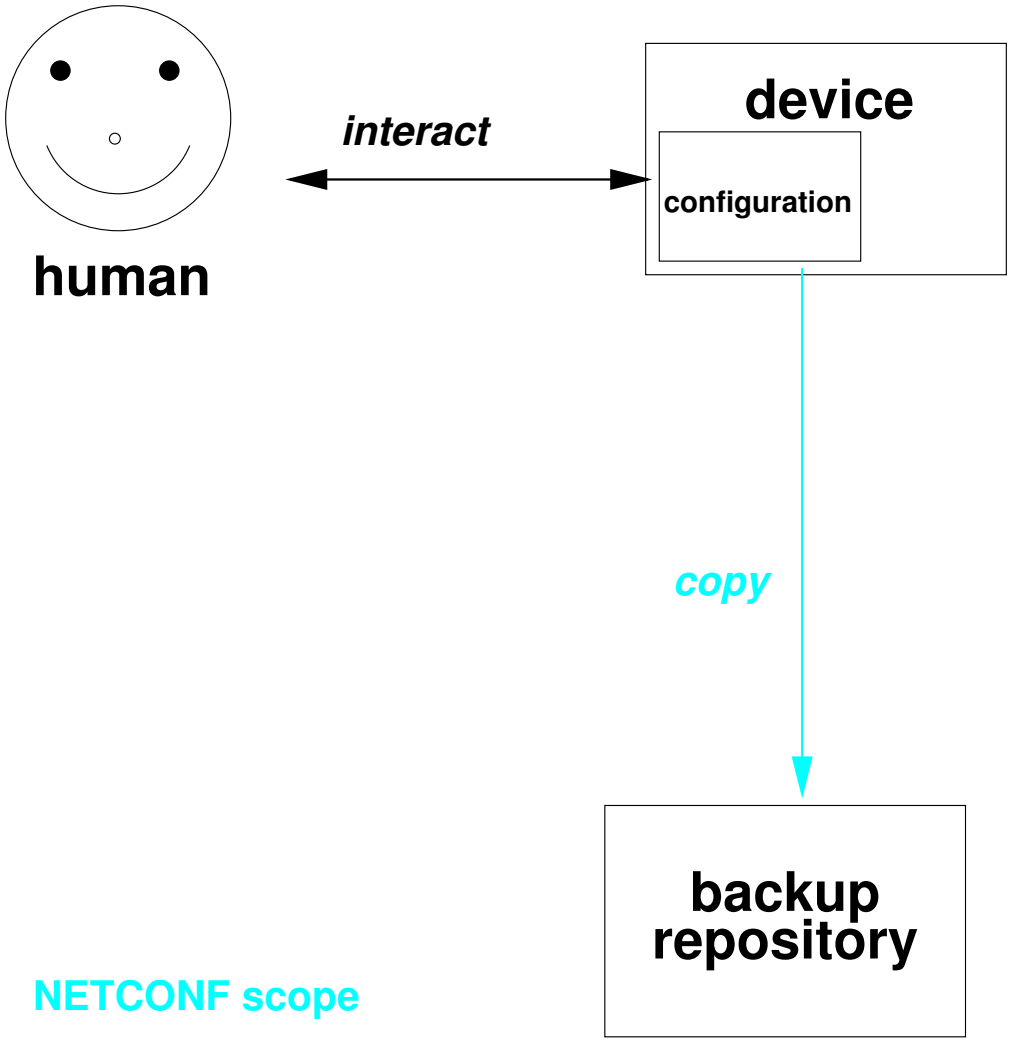
"Generate Everything" Approach



Generate with Intermediate Repr.



"The Network is the Record"



Specialized Script Examples

- convert-entire-network-from-is-is-to-ospf.py
- turn-up-new-customer-connection.sh
- update-server-filter-lists.tcl
- configure-peering-from-ripe-db.pl
- ...

These could all use NETCONF to extract and install pieces of configuration.

NETCONF WG pre-history

- 1990: SNMPv1, MIB-1
- 1990-2000:
  - SNMP evolution (SNMPv3 Full Standard in 2003)
  - Proliferation of standard and enterprise MIBs
  - Work on alternative approaches
    - DTMF/CIM, DEN, WBEM, COPS-PR/PIBs...
- ca. 2000: Perceived disconnect between
  - Network management protocol work in the IETF and
  - Network operators community
- 2001: IETF meets operators
  - NANOG 22, RIPE 40
    - focus on backbone network operators
  - LISA-XV
    - focus on campus/enterprise operators

NETCONF pre-history

- June 2002: IAB Network Management Workshop
  - 25 participants (protocol developers and operators)
  - Documented in RFC 3535
- Some observations:
  - SNMP used for monitoring, but not configuration
  - SNMP MIBs lag (years) behind feature implementation
  - SNMP doesn't distinguish config from non-config data
  - Operators use (proprietary) CLI for many tasks
    - In particular those involving configuration(s)
    - Problems with unstable and hard-to-parse CLI

IETF NETCONF Working Group

- Chartered May 2003
  - One outcome of IETF/operator dialog
- Current charter:
  - Standardize a protocol for network configuration
    - based on XML
- NOT in current charter:
  - Information model (schema) for device configurations
    - ...but see upcoming NetML talk
- Chairs:
  - Andy Bierman (Cisco, SNMP veteran)
  - Simon Leinen (SWITCH, operator)
- Web page:
  - http://www.ops.ietf.org/netconf/

NETCONF WG status

- Will meet for the third time at IETF 59
  - Seoul, February/March 2004
- Four WG drafts:
  - draft-ietf-netconf-prot-01.txt
    - NETCONF Configuration Protocol
  - draft-ietf-netconf-beep-00.txt
    - BEEP Application Protocol Mapping for NETCONF
  - draft-ietf-netconf-soap-00.txt
    - NETCONF Over SOAP
  - draft-ietf-netconf-ssh-00.txt
    - Using the NETCONF Configuration Protocol over Secure Shell (SSH)
- Design team to work on those

draft-ietf-netconf-prot-01.txt

Concepts

- Configuration datastores
  - running (mandatory)
  - startup
  - named files
- Sessions
  - Provide security association
- Multiple channels per session
  - Management
  - Operations
    - RPC (Remote Procedure Calls)
  - Notifications (opt.)

draft-ietf-netconf-prot-01.txt (cont.)

- Operations
  - <get-config>
  - <edit-config>
  - <copy-config>
  - <delete-config>
  - <get-state>
  - <kill-session>

draft-ietf-netconf-prot-01.txt (cont.)

- Capabilities
  - Permit annoucement of extensions (like in BGP)
- Current proposed standard capabilities
  - #manager
  - #agent
  - #writable-running
  - #candidate
  - #startup
  - #validate
  - #notifications
  - #url

<get-config>

```
<rpc message-id="106" xmlns="http://ietf.org/xmlconf/1.0/base">
  <get-config>
    <source><running/></source>
    <config xmlns="http://example.com/schema/1.2/config">
      <users>
        <user>
          <name>fred</name>
        </user>
      </users>
    </config>
    <format>xml</format>
  </get-config></rpc>

<rpc-reply message-id="106" xmlns="http://ietf.org/xmlconf/1.0/base">
  <config xmlns="http://example.com/schema/1.2/config">
    <users>
      <user>
        <name>fred</name>
        <type>admin</type>
        <full-name>Fred Flintstone</full-name>
      </user>
    </users>
  </config></rpc-reply>
```

<edit-config>

```
<rpc message-id="107" xmlns="http://ietf.org/xmlconf/1.0/base">
  <edit-config>
    <target>
      <running/>
    </target>
    <config xmlns="http://example.com/schema/1.2/config">
      <interface>
        <name>Ethernet0/0</name>
        <mtu>1500</mtu>
      </interface>
    </config>
  </edit-config>
</rpc>

<rpc-reply message-id="107" xmlns="http://ietf.org/xmlconf/1.0/base">
  <ok/>
</rpc-reply>
```

<copy-config>

```
<rpc message-id="108" xmlns="http://ietf.org/netconf/1.0/base">
  <copy-config>
    <source>
      <running/>
    </source>
    <target>
      <url>ftp://example.com/configs/testbed-dec10.txt</url>
    </target>
    <format>text</format>
  </copy-config>
</rpc>

<rpc-reply message-id="108" xmlns="http://ietf.org/netconf/1.0/base">
  <ok/>
</rpc-reply>
```

NETCONF Current Issues

- Choice of substrate (transport/"session") layer
  - SSH - operators like it
  - SOAP - developers like it
  - BEEP - protocol designers (router vendors) like it
  - ...unable to select single mandatory substrate yet.
- Notifications
  - Should they be part of the protocol?
  - If so, should they be mandatory?
- Extent of alignment to Web Services protocols
  - SOAP/WSDL
- Granular locking
- Naming within configurations

Further reading

- http://www.ops.ietf.org/netconf/
  - Please consider joining the Mailing List!
- NANOG 28 XML-based configuration BOF
  - Rob Enns' presentation has nice examples
- http://www.liberouter.org/
  - "Netopeer" DTDs for device configuration
  - Includes tools to convert IOS into XML.

A few questions for you...

A few questions for you...

- Do you configure network devices?
  - Read: do you have enable on your routers?
  - (or are you responsible for people doing so)

A few questions for you...

- Do you configure network devices?
- Are you supported by automated systems?
  - Revision management (e.g. RANCID)
  - Scripts that check configs
  - Scripts that generate (partial) configs
  - Higher-level provisioning tools

A few questions for you...

- Do you configure network devices?
- Are you supported by automated systems?
  - Revision management (e.g. RANCID)
  - Scripts that check configs
  - Scripts that generate (partial) configs
  - Higher-level provisioning tools
- If not, would such tools help you?
- If yes, are you happy with them?
- ...

Notifications?

- Should a mechanism for asynchronous notifications be integrated with the configuration protocol?

- Or are existing mechanisms sufficient (CLI/syslog/SNMP traps)?

Directionality

- Do you configure devices that you cannot initiate connections to?
  - Like devices behind firewalls or NATs
- ...so the device would connect to you and request to be configured.