SECURE DEVICE INSTALL

draft-wkumari-opsawg-sdi-03

BACKGROUND / DISCLAIMER

- Idea percolating for a while `draft-ietf-anima-autonomic-control-plane` final impetus.
- Designed for **simplicity**
  - implement **and** use

- Examples use Cisco autoinstall, but works with anything with a config.
- Does **not** solve all use cases, solves common one

Use-case

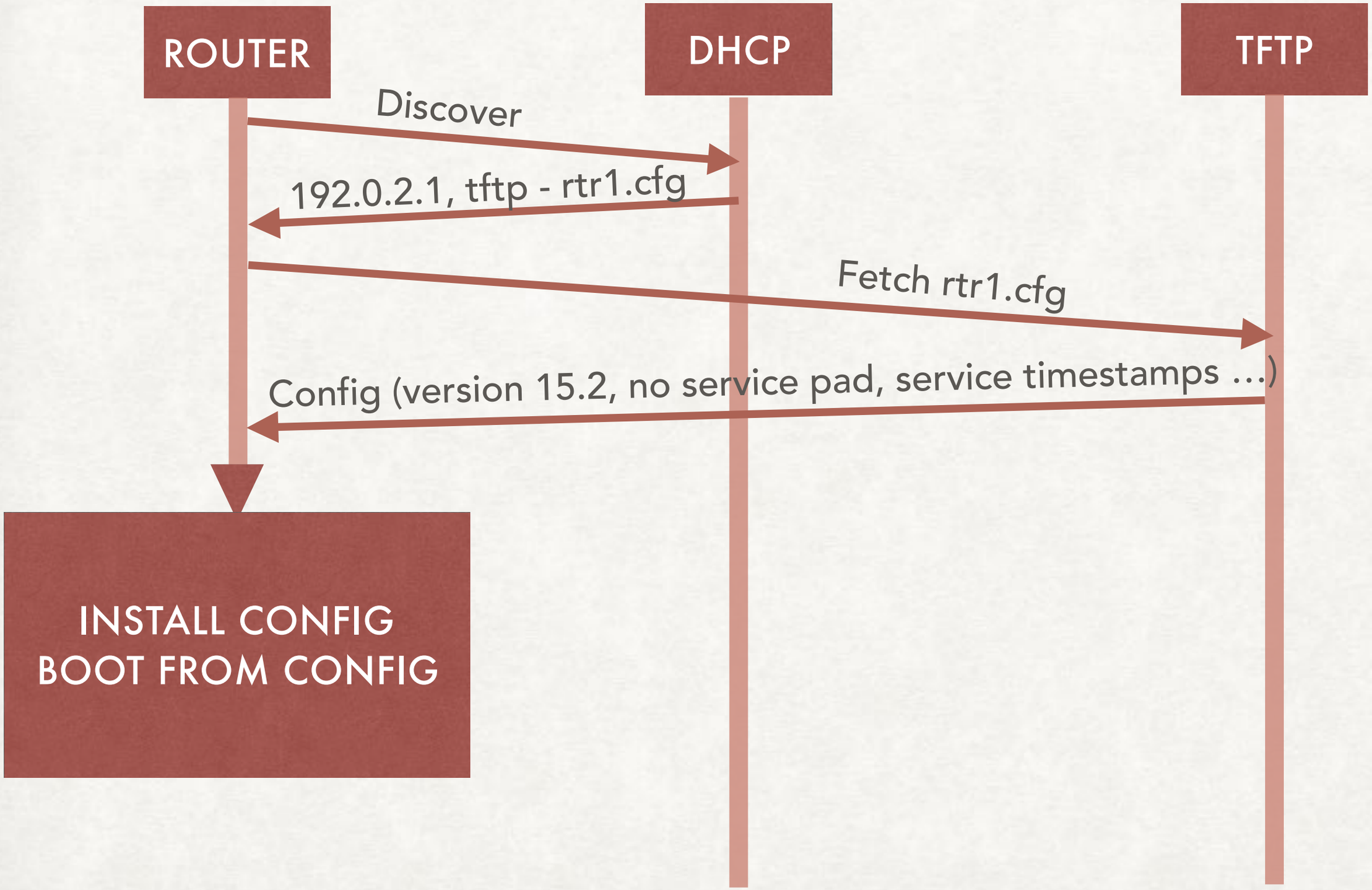
SECURE DEVICE INSTALL

- Ship a device to an Internet Exchange
  - Already have a circuit
- Have device able to be plugged in and Just Work

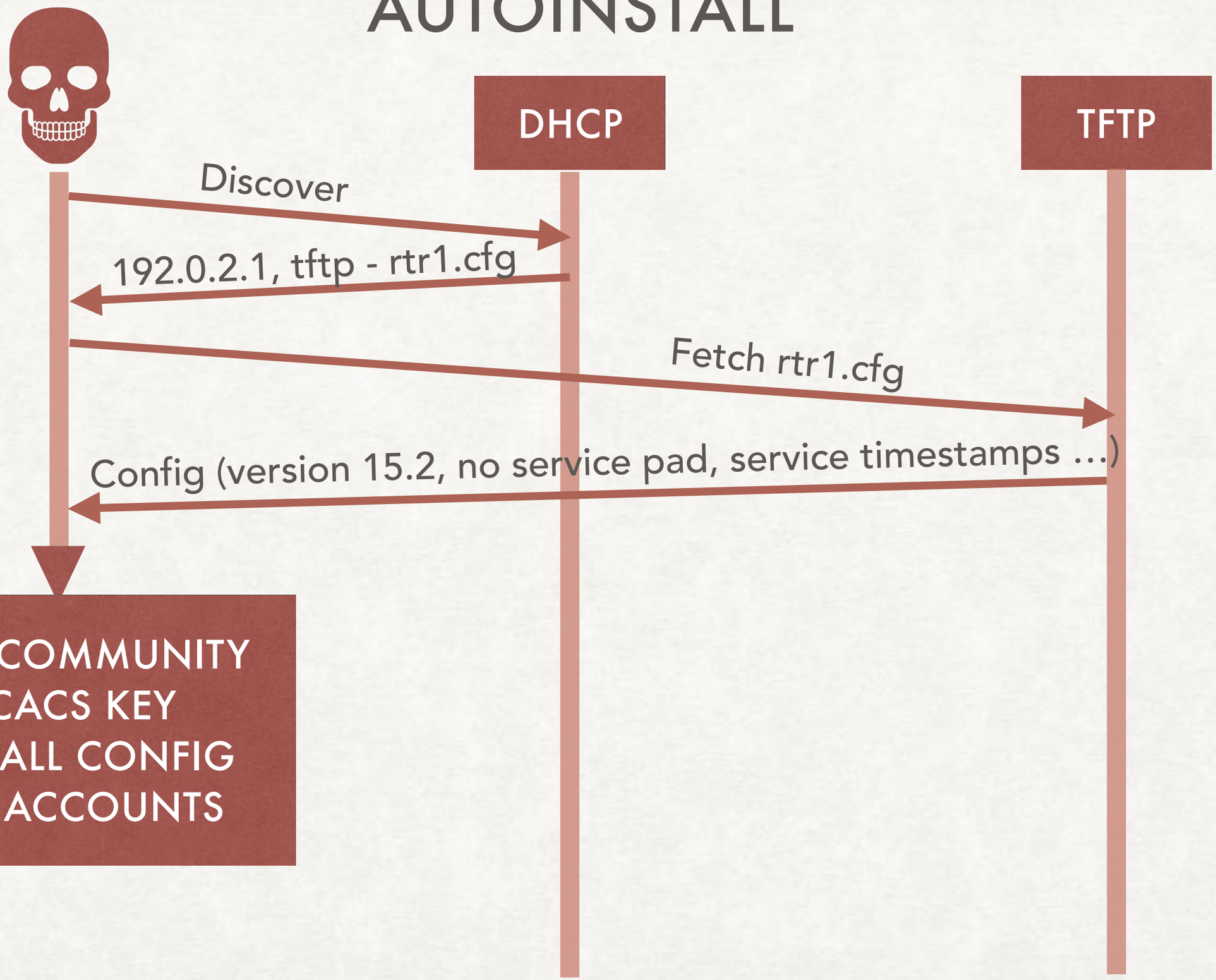
- Great! Use e.g Autoinstall, solved!
- Nope.

Refresher on autoinstall

AUTOINSTALL



AUTOINSTALL



I'm Sad

SECURE DEVICE INSTALL

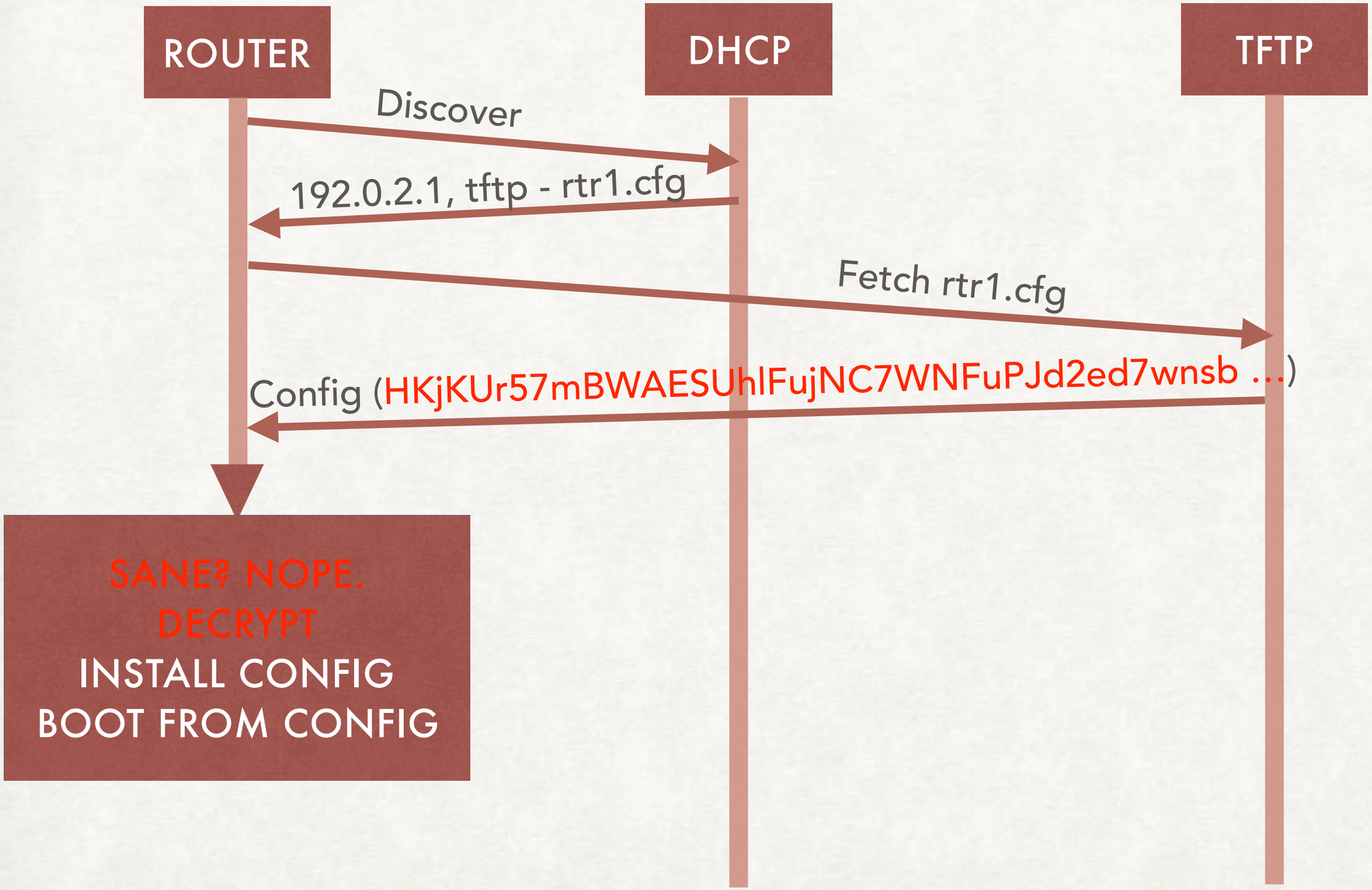
1. Vendors builds device, makes a keypair
2. They publishe public key on http://cert.vendor.example

1. I order a device
2. Vendor says “Thanks, shipping you serial #4217”
3. I fetch http://cert.vendor.example/sn-4217.crt
4. Encrypt config file to key in sn-4217.crt

When device boots, it fetches rtr1.cfg:

1. If rtr1.cfg looks sane, install and boot
2. If not, decrypt with private key, install and boot
3. Done.

SECURE AUTOINSTALL



AUTOINSTALL

Attacker Sad

FAQ

- Why not `draft-ietf-netconf-zerotouch`?!
  - Simplicity.
  - `netconf-zerotouch` better, but more complex
- Why not ANIMA ACP and BRSKI?!
  - Simplicity / control. ANIMA is very heavyweight
- Why not $Vendor $Cool_Product?
  - Simplicity, standardized
- Why not use the 802.1AR IDevID certificate?
  - If you have it and can use it, go right ahead
- Can I delete the cert?
  - Probably? Your choice.

QUESTIONS?

SIMPLE? REALLY!?

```
Step 1: Fetch the certificate.

  $ wget http://keyserv.example/certificates/SN19842256.crt

Step 2: Encrypt the config file.

   $ openssl smime -encrypt -aes-256-cbc -in
SN19842256.cfg\
     -out SN19842256.enc -outform PEM SN19842256.crt
  -----BEGIN PKCS7-----
MIICigYJKoZIhvcNAQcDoIICezCCAncCAxggE+MIIBOgIBADAiMBUxEzARB
gNVBAMMClNOMTk4NDIyNTYCCQDJVuBOb1DANBgkqhkiG9w0BAQEFAASCAQB
ABvM3...
   LZoq08jqlWhZZWhTKs4XPGHUdmnZRYIP8KXyEtHt
   -----END PKCS7——

Step 3: Profit!
```