DHCP configuring applications

- Threat or danger?

Purpose of DHCP options

- Original goals:
  - Configure IP parameters
  - Configure services needed to get online
  - Configure other services

IP parameters

- IP address (allocated)
- Prefix length (DHCPv4)
- MTU (rarely used)
- Default IP TTL (is it ever used?)
- Etc.

Network services

- Network doesn't work without these
  - DNS
  - Default routes (DHCPv4)
  - Other routes (DHCPv4)
  - Source address selection policy

- NTP
- SIP
- SMTP
- POP
- LPR

Application services

- Protocols like DNS and NTP are network-local
- Protocols like SMTP, POP and IMAP are not
- SIP is an edge case

Is DHCP a good choice?

NTP: a good candidate?

- NTP looks like a good candidate
  - Time is universal, so a local server is good
  - Time is needed for security protocols
- Problems
  - Flawed security model: should I trust Motel 7 to give me the correct time?
  - Most operating systems have a hard-coded FQDN for NTP configuration, and do not consult DHCP.
- So this is a mixed bag

SMTP, POP, IMAP

- Protocols like these are user-centric, not network-centric.
- I definitely don't want Motel 7 to deliver SMTP, POP or IMAP service to me.
- Protocols of this type need to be configured some other way—DHCP is clearly inappropriate.

What about SIP?

- SIP is a nice edge case.
- Maybe you want to use a different SIP server within a large company, when roaming from site to site.
- However, in the general case, the SIP server DHCP gives you will not work, and DHCP doesn't provide a way for you to know when to use the DHCP-provided server and when not to.
- So in fact, SIP is an example of a protocol that should *not* be configured using DHCP

But wait, there's more

- Currently some SIP phones configure using DHCP
- Rather than using DHCP-provided SIP address each time they renew their lease, they capture a SIP configuration the first time they connect, and retain it forever.
- This is a hack: it works, but it's not really following the DHCP flow
- It's also not secure—I can pwn your phone if I'm on the wire when you plug it in the first time, and wiretap all your calls from then on.

Conclusion

- DHCP is only appropriate for configuring applications in very restricted cases.
- The model of using DHCP to configure arbitrary applications should not be followed in the future, even though it is in current use in some cases.
- We need to carefully consider the use model for each proposed DHCP option to make sure that we think it's a good idea.

Why talk about this?

- There is a very typical controversy when defining DHCP options: should the option send one or more IP addresses, or one or more FQDNS?
- Application protocols often want DNS, because it is felt to offer more control.
- However, for a variety of reasons, DHCwg recommends *not* using FQDNs.
- This recommendation has gotten massive pushback from the apps area.

Should DHCP use FQDN?

- If it's to support user-centric apps, that's not a reason, because user-centric apps shouldn't be configured using DHCP.
- NTP is a more interesting case.
- PCP is also an interesting case.
- Both NTP and PCP however have tried to do a hybrid model: IP *and* DNS.

Current DHCwg advice

- Prefer to use IP address—places fewer demands on client.
- Use FQDN in situations where it makes more sense, but be clear about why it makes more sense.
- Absolute worst thing to do is both, because it creates interoperability issues

Interoperability issues

- DHCP doesn't support MTI on the server
  - Administrators are free to configure or not configure any particular option
- Clients can't anticipate which is configured.
- Clients must therefore request both
- If server is configured with both, it must send both.
- Now client has to decide which one to use, and the DHCP packet contains unneeded information.

Way forward

- Option 1: continue with current DHCwg consensus: recommend IP, allow FQDN, recommend against using both
- Option 2: extend DHCP to support requesting option A or option B, rather than option A and option B.