Adventures in DHCP

October 13, 2021

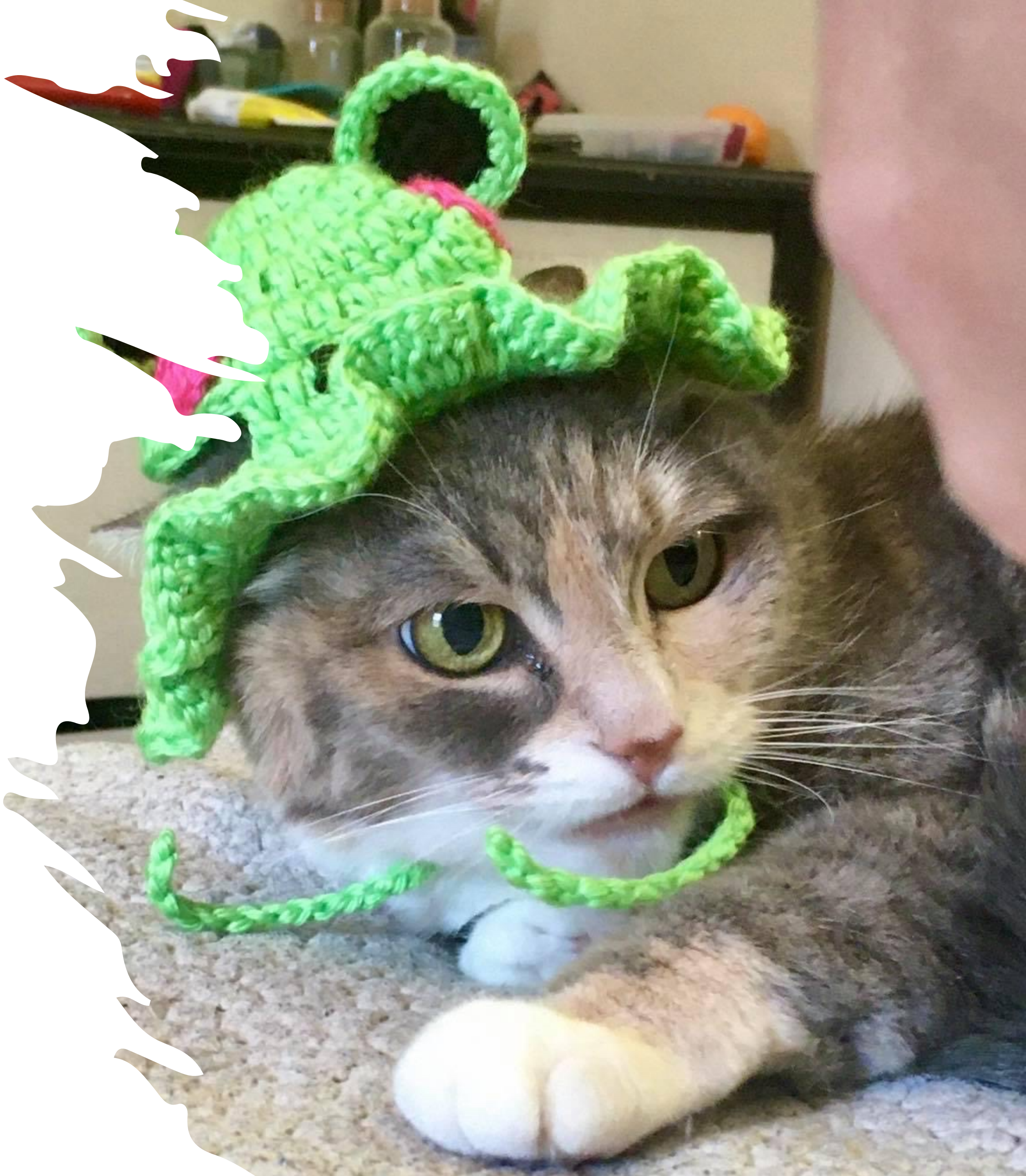
Eric Brown, Network Infrastructure & Services, Virginia Tech

What is DHCP?

- Dynamic Host Configuration Protocol
- When you connect this is how the network gives you a valid address and other information
- Statically addressed hosts can use to obtain other information

Why am I talking about DHCP at DCSS?

- DHCP is decades old.
- We've been running it for almost as long.
- Why do you care? Isn't this just some low-level network nerd stuff?
- Truth is, when it's working you don't care, nor should you (too much)
- Failure experiences range from "can't connect" to "very weird symptoms"



Even old, working technology needs continual refinement and evolution because all the things around it change.

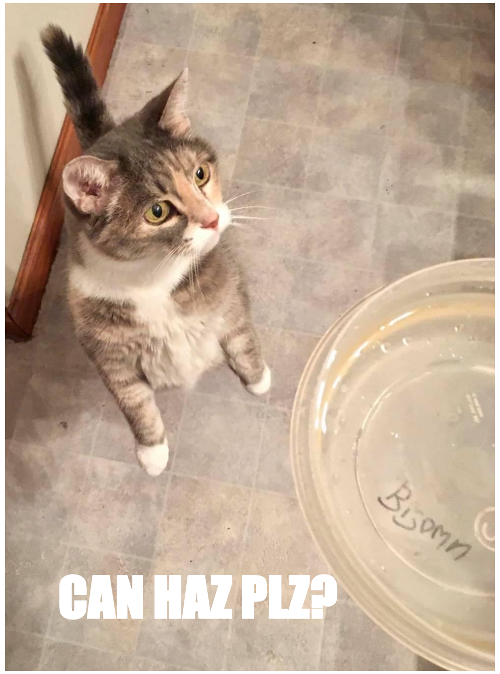
Topics

- How does it work? A simplified process
- A war story about two recent problems
- A change of service

- And some cute cat pictures so you don't lose interest

Simplified process [Binding phase]

Network	Client
	1 Connects and sends DISCOVER message
2 Responds with OFFER message	
	3 Sends REQUEST message
4 Completes transaction with ACKNOWLEDGE msg	



Simplified process part 2 [Renewing phase]

… Time passes and the address comes up for renewal

Network	Client
	1 Sends another REQUEST message
2 Responds with another ACKNOWLEDGE message	

It’s really more complicated

- The “network” is a lot of things working together
  - DHCP servers (with redundancy and failover)
  - DHCP agents
  - Other elements that “snoop” DHCP for protection, performance, and security
- Not all client behavior is the same
- Lots of corner cases for streamlining and resilience

War story #1: Can’t connect

- **Report**: some sites won’t load when first connected
- **Investigation**: working sites are IPv6, suspect DHCP
- **Troubleshooting**: packet capture – no OFFER from network, but client sends INFORM message before DISCOVER
- **Cause**: DHCP agent (our routers) holding state and dropping OFFER
- **Fix**: small config change and several rounds of router upgrades

- **Refinement and Evolution**: changing client and agent behavior requires attention

War story #2: Renew failure

- **Report**: users getting dropped connections
- **Investigation**: logs show repeating REQUEST and ACKNOWLEDGE messages, network going into DDoS protection for DHCP
- **Problem**: clients seem to be ignoring ACKNOWLEDGE message
- **Observation**: DHCP server address different between REQUEST and ACKNOWLEDGE?! This is possible in our configuration
- **Hypothesis**: client firewall is blocking response. Windows Defender Shields Up fits the symptoms, but also other OSs
- **Counter-Hypothesis**: valid server behavior per RFC, consider other causes

War story #2: Renew failure

- **Test 1**: craft "corrected" ACKNOWLEDGE message ← fixed!
- **Test 2**: modify Windows Defender with allow connection rule from DHCP server ← fixed!

- **Fix**: iptables source NAT rules to force server response from "correct" address

- **Refinement and Evolution**: tighter security controls forced a narrower implementation than allowed by standards

A change of service

- **Old Service Policy**: wired DHCP requires registered MAC address
  (MAC address is the hardware identifier of the system)
- **Rational**: find responsible party to investigate suspicious traffic
- **Complication**: randomized MAC address, ease of spoofing, little additional value, not required on residential network

- **Refinement and Evolution**: remove policy and operate as open pool

  "Recent technological developments and other initiatives have significantly decreased the accounting and security value provided by this application and introduced some potential client usability issues."
  KB0012569: https://4help.vt.edu/sp?id=search&q=KB0012569

Open-pool DHCP service

- Everything is great now, right?
- WRONG!
- **Problem**: some depts run own DHCP servers and used MAC registration to avoid conflict
- **Need**: a way to avoid getting an Offer from the Open-pool DHCP service

N.B. departmental DHCP servers need registration

Another service: DHCP Exclusion

- **Preferred**: Set client-id or vendor-class to “NIS_IGNORE”
- **DHCP Exclusion Tool**: Register MAC address
  https://portal.nis.vt.edu/#/exclusion-devices

- Did we gain anything?
  - Improved usability for most
  - Eliminate a local fork of DHCP server software
  - Only managing 130 exclusions versus 34,000 registrations

- **Collaborate**: Considering running DHCP? Please talk to us first

Questions/Contact

- eric.brown@vt.edu
- 231-8696

All cat photo credits: @Shiitakeposting on Facebook