Smart Proxy - Bug #18269

DHCP allocates wrong address or no addresses if hosts do not respond to icmp

01/26/2017 12:14 PM - Martyn Smith

Status:	New		
Priority:	Normal		
Assignee:			
Category:	DHCP		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.13.2
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

We are using foreman-proxy and dhcp isc on a server in a secure subnet that is servicing DHCP requests via DHCPRELAY for multiple subnets. Many of these subnets have no direct communication with the DHCP server except via the relay.

The subnets are setup with the following config in /etc/dhcp/dhcpd.conf

```
subnet 10.250.130.192 netmask 255.255.255.240 {
pool {
failover peer "dhcppeer";
range 10.250.130.195 10.250.130.206;
deny dynamic bootp clients;
}
option routers 10.250.130.193;
}
```

We've then entered a subnet with a start and end address of 10.250.130.195 and 10.250.130.206 in foreman. On using IP autosuggest for these subnets we get the following in the proxy.log

D, [2017-01-25T17:47:32.504604 #20035] DEBUG -- : accept: 10.250.143.9:47062
D, [2017-01-25T17:47:32.507528 #20035] DEBUG -- : Rack::Handler::WEBrick is invoked.
D, [2017-01-25T17:47:32.508451 #20035] DEBUG -- : verifying remote client 10.250.143.9 against trusted_hosts katello-dev.solutions.localdns1.solutions.local
D, [2017-01-25T17:47:32.508748 #20035] DEBUG -- : Loading subnets for 127.0.0.1
D, [2017-01-25T17:47:32.509025 #20035] DEBUG -- : Loading subnet data for 10.250.130.192/255.255.255.240
D, [2017-01-25T17:47:32.509200 #20035] DEBUG -- : trying to find an ip address, we got {:to=>"10.250.130.206", :from=>"10.250.130.195"}
D, [2017-01-25T17:47:32.511267 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.197
D, [2017-01-25T17:47:32.512040 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.512135 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.198
D, [2017-01-25T17:47:32.513028 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.513126 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.199
D, [2017-01-25T17:47:32.513962 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.514083 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.200
D, [2017-01-25T17:47:32.514799 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.514898 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.201
D, [2017-01-25T17:47:32.515542 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.515643 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.202
D, [2017-01-25T17:47:32.516243 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.516414 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.203
D, [2017-01-25T17:47:32.517020 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.517111 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.204
D, [2017-01-25T17:47:32.517815 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.517910 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.205
D, [2017-01-25T17:47:32.518539 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.518638 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.206
D, [2017-01-25T17:47:32.519212 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:47:32.519361 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.195

D, [2017-01-25T17:47:32.519960 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
W, [2017-01-25T17:47:32.520055 #20035] WARN -- : No free IPs at 10.250.130.192/255.255.255.240
I, [2017-01-25T17:47:32.521864 #20035] INFO -- : 10.250.143.9 - - [25/Jan/2017 17:47:32] "GET /dhcp/10.250.130.192/unused_ip?from=10.250.130.195&to=10.250.130.206 HTTP/1.1" 200 11 0.0138

and no ip address is suggested.

If we remove the start and end address we get an ip address allocated by autosuggest, however, it always appears to suggest the first address which is not in the address pool and is the router address. The log for that request is below.

D, [2017-01-25T17:46:07.461799 #20035] DEBUG -- : accept: 10.250.143.9:47058
D, [2017-01-25T17:46:07.465218 #20035] DEBUG -- : Rack::Handler::WEBrick is invoked.
D, [2017-01-25T17:46:07.466170 #20035] DEBUG -- : verifying remote client 10.250.143.9 against trusted_hosts katello-dev.solutions.localdns1.solutions.local
D, [2017-01-25T17:46:07.466563 #20035] DEBUG -- : Loading subnets for 127.0.0.1
D, [2017-01-25T17:46:07.466861 #20035] DEBUG -- : Loading subnet data for 10.250.130.192/255.255.255.240
D, [2017-01-25T17:46:07.467121 #20035] DEBUG -- : trying to find an ip address, we got {:to=>nil, :from=>nil}
D, [2017-01-25T17:46:07.469323 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.194
D, [2017-01-25T17:46:07.470478 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.470577 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.195
D, [2017-01-25T17:46:07.471200 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.471372 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.197
D, [2017-01-25T17:46:07.472019 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.472111 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.198
D, [2017-01-25T17:46:07.473152 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.473245 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.199
D, [2017-01-25T17:46:07.473973 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.474064 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.200
D, [2017-01-25T17:46:07.474756 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.474848 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.201
D, [2017-01-25T17:46:07.475540 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.475634 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.202
D, [2017-01-25T17:46:07.476403 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.476497 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.203
D, [2017-01-25T17:46:07.477117 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.477208 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.204
D, [2017-01-25T17:46:07.477838 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.477967 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.205
D, [2017-01-25T17:46:07.478601 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.478704 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.206
D, [2017-01-25T17:46:07.479426 #20035] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-25T17:46:07.479538 #20035] DEBUG -- : Searching for free IP - pinging 10.250.130.193
D, [2017-01-25T17:46:09.506491 #20035] DEBUG -- : Found free IP 10.250.130.193 out of a total of 13 free IPs
I, [2017-01-25T17:46:09.508771 #20035] INFO -- : 10.250.143.9 - - [25/Jan/2017 17:46:09] "GET /dhcp/10.250.130.192/unused_ip HTTP/1.1" 200 23 2.0428

We've tried this on a pingable subnet - i.e. the local one and it works correctly, however, this means it cannot work inside our infrastructure without opening ICMP up to every subnet from the dhcp servers.

History

#1 - 01/26/2017 12:27 PM - Anonymous

Autosuggest relies on icmp or tcp echos for detection of unused addresses. You will need to manually assign ip addresses if a given subnet isn't reachable from smart-proxy machine.

#2 - 01/27/2017 04:01 AM - Martyn Smith

Perhaps this should be a feature request then. It's behaviour in the circumstances seemed anomalous so I raised it as an issue.

I think that in environments requiring a high level of security it's unlikely that every network manager will allow icmp or tcp ping to be allowed which will prevent foreman being used as the IPAM system. Could we not get the existing leases by parsing the leases file in the first instance rather than by pinging? We could then also use ping be a supplementary check in networks that would allow it?

#3 - 01/30/2017 08:47 AM - Martyn Smith

Update:

This does appear to remain an issue in my environment if you can ping some hosts on the subnet and the subnet is remote and uses DHCPRELAY.

A local subnet works correctly.

Example:
DHCP range 10.250.130.192 /28 with the pool 10.250.130.195 - 206
Allocated on the subnet

10.250.130.193 - router (ICMP blocked)
10.250.130.194 - unallocated
10.250.130.195 - allocated and host pingable

and the rest of the range unallocated until the broadcast address 10.250.130.207

With being able to ping from the subnet and to the subnet to every address except the router, and with no ip start and end in the subnet in foreman. The router address gets auto-suggested. This is expected based on Dmitri's post.

However, with a start and end ip entered matching the DHCP pool of 10.250.130.195 to 206, this fails to auto-suggest an ip at all. This does not appear to be expected based on ICMP being enabled.

#4 - 01/30/2017 12:18 PM - Anonymous

> However, with a start and end ip entered matching the DHCP pool of 10.250.130.195 to 206, this fails to auto-suggest an ip at all. This does not appear to be expected based on ICMP being enabled.

Could you post debug-level log from smart-proxy please?

#5 - 01/30/2017 12:26 PM - Martyn Smith

The log is the same as the one posted initially.

D, [2017-01-30T13:20:13.537045 #26591] DEBUG -- : close: 10.250.143.9:58332
D, [2017-01-30T13:21:20.236850 #26591] DEBUG -- : accept: 10.250.143.9:58336
D, [2017-01-30T13:21:20.240253 #26591] DEBUG -- : Rack::Handler::WEBrick is invoked.
D, [2017-01-30T13:21:20.241142 #26591] DEBUG -- : verifying remote client 10.250.143.9 against trusted_hosts katello-dev.solutions.localdns1.solutions.local
D, [2017-01-30T13:21:20.241436 #26591] DEBUG -- : Loading subnets for 127.0.0.1
D, [2017-01-30T13:21:20.241722 #26591] DEBUG -- : Loading subnet data for 10.250.130.192/255.255.255.240
D, [2017-01-30T13:21:20.242016 #26591] DEBUG -- : trying to find an ip address, we got {:to=>"10.250.130.206", :from=>"10.250.130.195"}
D, [2017-01-30T13:21:20.243743 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.197
D, [2017-01-30T13:21:20.245256 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.245355 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.198
D, [2017-01-30T13:21:20.246214 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.246309 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.199
D, [2017-01-30T13:21:20.247001 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.247097 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.200
D, [2017-01-30T13:21:20.247677 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.247779 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.201
D, [2017-01-30T13:21:20.249179 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.249275 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.202
D, [2017-01-30T13:21:20.249886 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.250068 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.203
D, [2017-01-30T13:21:20.250651 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.250746 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.204
D, [2017-01-30T13:21:20.251701 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.251805 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.205
D, [2017-01-30T13:21:20.252506 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
D, [2017-01-30T13:21:20.252597 #26591] DEBUG -- : Searching for free IP - pinging 10.250.130.206
D, [2017-01-30T13:21:20.253287 #26591] DEBUG -- : Found a pingable IP address which does not have a Proxy::DHCP record
W, [2017-01-30T13:21:20.253381 #26591] WARN -- : No free IPs at 10.250.130.192/255.255.255.240
I, [2017-01-30T13:21:20.255245 #26591] INFO -- : 10.250.143.9 - - [30/Jan/2017 13:21:20] "GET /dhcp/10.250.130.192/unused_ip?from=10.250.130.195&to=10.250.130.206 HTTP/1.1" 200 11 0.0145

It seems odd in that it never appears to check ips 10.250.130.195 and 196

#6 - 01/30/2017 12:50 PM - Anonymous

Could you clarify "no direct communication" please? Is that achieved via firewall (or similar) that sends back tcp RST packets? Is there no route between two networks? Trying to understand why there are "Found a pingable IP" messages in the log...

#7 - 01/30/2017 12:55 PM - Anonymous

It seems odd in that it never appears to check ips 10.250.130.195 and 196

This is likely due to code persisting the index of the last free ip address that was suggested. One of the issues there is that the code doesn't take range in the account, so it will start checks from (index + 1)th address in the list of free addresses.

#8 - 01/30/2017 05:04 PM - Martyn Smith

My statement was a little confusing. By no direct communication I was refering to the original DHCPDISCOVER and DHCP OFFER which were relayed via the DHCP relay agent in the firewall. The firewall was initially dropping all ICMP communications howeverm it now only blocks ICMP responses on it's own interface sp ICMP response from any other machines on the subnet are successful.

#9 - 01/30/2017 05:13 PM - Anonymous

How does the firewall handle tcp echoes? Specifically opening a tcp connection from the smart-proxy host to a host in one of the "restricted" subnets: does it send an RST back, silently drops a packet, or perhaps some other way?

#10 - 01/31/2017 04:11 AM - Martyn Smith

TCP echos are still blocked so the firewall would just drop.

#11 - 01/31/2017 04:52 AM - Anonymous

Could you try opening a tcp connection from smart-proxy to a host in a restricted subnet (to any port)? What error are you getting back?