INTRODUCTION

RFC 2317 is an IETF (Internet Engineering Task Force) document that describes a method of delegating parts of the DNS reverse-mapping tree in a more manageable way, specifically, for parts of the tree that correspond to subnets smaller than /24 in size. The DNS reverse-mapping tree has nodes broken at octet boundaries of IP addresses, which correspond to the old classful network masks. This just means that reverse-mapping zones (and hence, delegation points) fall on /8, /16, or /24 boundaries. With the proliferation of CIDR (Classless Inter-Domain Routing) support for routing, ISPs no longer assign entire Class C networks to customers that only need a handful of addresses. In general, address assignments no longer fall on nice, classful boundaries.

For DNS, a problem comes in to play when an ISP gives a customer an address range that is smaller than a Class C, but that customer also wants to be delegated the DNS reverse-mapping zone. Again, DNS can only deal nicely with mapping a /24 network, but if the ISP has given, for example, a /25, the customer only has half of the Class C. If the customer configures his DNS server to be authoritative for the zone corresponding to a /24 network, half of the possible reverse-mapping records in the zone will not be resolvable.

RFC 2317 defines an approach, considered a best practice, which fixes this issue.

HOW DOES IT WORK?

Looking at this from the customer’s point of view, there are two issues:

1. Other name servers will query the ISP’s name servers for reverse lookups as the ISP owns the zone corresponding to the /24 network that my network is part of, i.e., the delegation path points to the ISP’s name servers.

2. I need to create PTR records on my DNS server, but my name servers are not in the delegation path, so creating a zone corresponding to the /24 network won’t work. So where will the PTR records reside?

Looking at this from the ISP’s point of view:

1. Other name servers will query my name servers for reverse lookups as I own the zone corresponding to the /24 network that contains the network assigned to my customer, but the customer needs to have the PTR records on their DNS server.

2. How can I somehow delegate a reverse-mapping zone to my customer when DNS can only delegate on a classful boundary?

As an example, let’s use the network 172.20.24.0/24, and “split” this network into 32 networks with a prefix of /29. Two customers exist, so let’s look at the one who has been assigned the second /29 subnet, 172.20.24.8/29.
Here’s what this normally looks like:

The customer’s side is the easiest. The customer’s DNS server cannot be configured to be authoritative for the 24.20.172.in-addr.arpa, as they do not own it. RFC 2317 works around this by creating a new subzone for each of the corresponding subnets. In this example, there would be a zone called 8-15.24.20.172.in-addr.arpa, or perhaps 8/29.24.20.172.in-addr.arpa. The name of the new level can be anything, but the customer and the ISP must agree on the naming convention used. Using “8-15” is self-documenting and shows that the last octet of IP addresses covered by this delegated zone start at 8 and end at 15. Using “8/29” shows us the same information, only in prefix notation. Infoblox recommends using the first notation, or range-based notation, as it’s easier to read when looking at a zone definition and also does not cause problems with older BIND 8 name servers with the check-names feature turned on. The prefix notation is often more confusing (e.g., PTR is at 9.8/29.24.20.172.in-addr.arpa). Again, both refer to the same network. The RFC does not say either of these formats must be used, so some ISPs use strings like “subnet1”, “net1”, or any other label. The only rule is that the characters must be legal for BIND (and the DNS One!), that each one be unique (within the /24 subnet), and the customer and ISP agree. In most cases, the convention used is defined as a policy by the ISP.
So, the client DNS machine would end up with a zone called (assuming a label of “8-15”) 8-15.24.20.172.in-addr.arpa, and all of its PTR records would be written to it. Like so:

The ISP would have the same zone defined on its DNS server as a delegation to the customer’s name servers. Also, in the parent /24 zone, 24.20.172.in-addr.arpa in this case, the ISP would place one CNAME for every PTR record that the customer has. Like so:
CNAME and NS records on the ISP side would look like this:


With these records, here’s the resolution path for the queries:

1. An application asks the resolver to reverse map the IP address 172.20.24.9.
2. The resolver queries its local name server for PTR records for 9.24.20.172.in-addr.arpa.
3. The local name server queries the roots, TLD and eventually the ISP name servers for the PTR record for 9.24.20.172.in-addr.arpa.
5. The ISP name server finds that 8-15.24.20.172.in-addr.arpa has been delegated to the customer’s name servers.
6. The final lookup goes to the DNS server at the customer, and the answer for a PTR is found attached to 9.8-15.24.20.172.in-addr.arpa.

CONFIGURATION ON DNS ONE

For an ISP, one would do the following:

1. Create the 172.20.24.0/24 as Authoritative.
2. Split the /24 into /29s.
3. Add the particular /29 you need to delegate as a delegated network, just like any other delegated network.
4. Click on the Advanced button, and check the box for RFC 2317 and fill in the desired label (in this case, that would be “8-15”). The DNS One automatically adds the CNAMEs into the 24.20.172.in-addr.arpa zone.

For an ISP customer, one would do the following:

1. Create the 172.20.24.0/24 as Nonauthoritative.
2. Split the /24 into /29.
3. Add the particular /29 you need as Authoritative.
4. Click on the Advanced button, and check the box for RFC 2317 and fill in the desired label (in this case, that would be “8-15”).

Remember that the ISP and Customer must use the exact same naming convention or the CNAME references to the final PTR records won’t be correct.