Layer 3 VPNs and Traceroute

Alex Marder, Matthew Luckie, Bradley Huffaker, kc claffy, Jonathan M. Smith
Expected Response Types: Ingress

Reply: i → Probe
Expected Response Types: Egress

Reply: e

Probe
Responses Face the Traceroute Source

Ingress Response

Egress Response
Responses *Do Not* Face Destination

- We don’t expect the interface that would have forwarded the probe to the destination
What is a Layer 3 VPN?

• Virtual IP networks that share the same physical infrastructure
  • VPN uses ISP backbone but separate forwarding tables

• Common uses
  • Connect customer sites together
  • Enable high bandwidth connection to cloud
L3 VPN: Traceroute Example

Traceroute

Network Map
L3 VPN: Packet Sent From $\text{AS}_A$ to $\text{AS}_B$

Traceroute

Network Map
L3 VPN: Traceroute Starts Normally

Traceroute

[Diagram]

Network Map

[Diagram]
L3 VPN: Egress Virtual Forwarding (VRF)

Traceroute

\[
\begin{align*}
\text{a}_{\text{AS}_A} & \rightarrow \text{s}_1_{\text{AS}_S} & \rightarrow \text{b'}_{\text{AS}_B} \\
\end{align*}
\]

Network Map

AS\textsubscript{A}  
AE \rightarrow a \rightarrow a' \rightarrow SE\textsubscript{1} \rightarrow s'\textsubscript{1} \rightarrow s\textsubscript{1} \rightarrow S\textsubscript{1} \rightarrow s'\textsubscript{2} \rightarrow s\textsubscript{2} \rightarrow SE\textsubscript{2} \rightarrow b' \rightarrow b \rightarrow BE

Service Provider

VPN ID

Dest: AS\textsubscript{B}
L3 VPN: Ends Normally

Traceroute

Service Provider

Network Map

Dest: AS_B
Problem With Conventional Interpretation

Traceroute

Interpretation (Assuming Ingress Addresses)
Problem With Conventional Interpretation

Traceroute

162.252.70.103  
Internet2

128.91.238.218  
UPenn

128.91.238.217  
UPenn

Correct Interpretation

162.252.70.103  
Internet2

R₁

?  
R₂

128.91.238.218  
UPenn

128.91.238.217  
UPenn

R₃
Finding Egress VRF Addresses

Adjacent hops with *consecutive* addresses

162.252.70.103
Internet2

R1

R2

128.91.238.218
UPenn

128.91.238.217
UPenn

R3

UPenn
Must Rule Out Two Separate /31s

One /30 Link

Two /31 Links
4 Address Prefixes: Ping Test

128.91.238.216/30

Usable Host Addresses

128.91.238.216
128.91.238.217
128.91.238.218
128.91.238.219

Network

128.91.238.216
128.91.238.217
128.91.238.218
128.91.238.219

Broadcast
Results

Correctness

Coverage

Precision

Recall

R&E 1

R&E 2

Middle

All
Conclusion

• Watch out for egress VRF addresses
  • 6% of middle addresses in ITDK traceroutes

• We can detect them
  • An hopefully account for them