PROBE: A Utility For Probing Interfaces

Draft-ietf-intarea-probe-01
R. Bonica, R. Thomas, J. Linkova, C. Lenart, M. Boucadair
IETF 99 - Intarea
July 20, 2017
Your Old Friend, PING

- Ping tests bidirectional connectivity between a probing interface and a probed interface
  - Probing interface sends an ICMP Echo Request to the probed interface
  - If the Echo Request arrives at the probed interface, the probed interface returns an ICMP Echo Reply
  - If the Echo Reply arrives at the probing interface, PING succeeds
  - Otherwise, PING fails

- PING does not always exercise the probed interface
  - Echo Request can enter the probed node through an interface other than the probed interface
  - Echo Reply can exit the probed node through an interface other than the probed interface
PING Shortcomings

- PING cannot distinguish among the following failures
  - The Echo Request is lost on route to the probed interface
  - The probed interface is down
  - The Echo Reply is lost on route to the probing interface

- PING requires bidirectional reachability between the probing and probed interfaces. Therefore, it cannot be used when
  - The probed interface is unnumbered
  - The probing and probed interfaces are numbered from different address families
Your New Friend, PROBE

- Distinguishes between proxy and probed interfaces

- Probing interface
  - Sends an ICMP Extended Echo Request to a proxy interface
  - Extended Echo Request identifies the probed interface by address, ifName, or IfIndex

- Proxy interface
  - Receives an Extended Echo Request
  - Determines the status of the probed interface
  - Returns an ICMP Extended Echo Reply
    - Extended Echo Reply reports the status of the probed interface

- Probed interface
  - Can reside on the same node as the proxy interface
  - Can be directly connected to the node upon which the proxy interface resides
Determining Status of the Probed Interface

• If the probed interface resides on the same node as the proxy interface
  • Status is a function of ifOperStatus

• If the probed interface is directly connected to the node upon which the proxy interface resides
  • Probed interface is up if its address is found in the ARP Table or IPv6 Neighbor Cache
  • Probed interface is assumed not to exist if its address is not found in either of the above-mentioned tables
PROBE versus Ping

• PROBE tests bidirectional connectivity between the probing and proxy interface
  • On failure, PROBE does not receive an Extended Echo Reply

• PROBE tests the status of the probed interface
  • On failure, PROBE receives an Extended Echo Reply reporting that probed interface does not exist or is not active

• Given bidirectional connectivity to any interface on a node, PROBE can query the status
  • Of any interface that resides on the node
  • Of any interface that is directly connected to the node
Extended Echo Request

• IP Header Fields
  • Source Address – Same as ICMP Echo Request
  • Destination Address – Identifies the proxy interface

• ICMP Fields
  • Type – TBD by IANA
  • Code, Checksum, Identifier, Sequence Number
    • Same as ICMP Echo Request
    • Sequence number is only 8 bits long
  • Local (L) Flag
    • Set: the probed interface resides same node as the proxy interface
    • Clear: the probe interface is directly connected to the node upon which the proxy interface resides
  • ICMP Extension Structure: Identifies the probed interface
    • See RFC 4884
ICMP Extension Structure

• Contains one or two *Interface Identification Objects (IIO)*
  • Each Identification Object identifies the probed interface by name, index or address
  • When the Local flag is clear, the IIO must identify the probed interface by address

• When the IIO identifies the probed interface by address, it can use any address family
  • ICMPv4 Extended Echo Request can identify probed interface by IPv6 address
  • ICMPv6 Extended Echo Request can identify probed interface by IPv4 address

• In most cases, a single IIO can identify the probed interface
  • In some corner cases, two are required
Extended Echo Reply

• Returns the following information about the probed interface
  • Operational status
  • Active forwarding protocols (IPv4, IPv6)
• Does not return any other information about the probed interface
  • Administrative status
  • MTU
  • Forwarding statistics
  • Routing and management protocol information
  • Other identifying information
    • Interface name, interface description
Use Cases

• The probed interface is unnumbered
• The probing and probed interfaces are not directly connected to one another. The probed interface has an IPv6 link-local address, but does not have a more globally scoped address
• The probing interface runs IPvX only while the probed interface runs IPvY only
• For lack of a route, the probing node cannot reach the probed interface.
PROBE User View: Query By Name

reji@R11_re0:~ # probe -I ge-0/0/0.0 10.10.10.2
PING 10.10.10.2 (10.10.10.2): 56 data bytes
8 bytes from 10.10.10.2 via ge-0/0/0.0: icmp_seq=0 ttl=64
Extended Ping Results
Queried for status of Interface name : ge-0/0/0.0
Status:
   IPv4 ACTIVE
   IPv6 ACTIVE
--- 10.10.10.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
reji@R11_re0:~ # probe -l fe80::1 10.10.10.2
PING 10.10.10.2 (10.10.10.2): 56 data bytes
8 bytes from 10.10.10.2 via ge-0/0/0.0: icmp_seq=0 ttl=64
Extended Ping Results
Queried for status of Interface address : fe80::1
Status:
  IPv4 ACTIVE
  IPv6 ACTIVE
--- 10.10.10.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
Security Considerations - Threats

• PROBE may be used to discover interface names and ifIndex patterns
• This information can be used to infer other information
• For example, if the probed interface name is fe-0/0/0
  • It is probably running Vendor X software
  • It probably has bandwidth of 10 or 100 mbps
  • It probably has MTU of 1500 bytes
Security Considerations - Mitigations

- Nodes disable ICMP Extended Echo by default
  - Enabled by configuration
- Nodes disable each type of query by default (by address, by name, by index)
  - Enabled by configuration
- If a node enables a particular query type, it can define prefixes from which that type of query will be accepted
- PROBE MUST NOT leak information about one VPN inter another
  - Proxy and probed interface must be in same VPN
Status

• Many comments addressed
  • Thanks to Jeff Haas, Sowmini Varhadhan Jonathan Looney and Carlos Pignataro

• New ability to probed directly connected interfaces
  • Thanks to new author, Med Boucadair

• Working prototype
  • Thanks to Reji Thomas
Next Steps

• WG Last Call