Extended Ping (XPING)

draft-bonica-intarea-eping-04

R.Bonica, R.Thomas, J.Linkova, C.Lenart

IETF 98 - Intarea

March 28, 2017

Your Old Friend, PING

- Ping is a lightweight tool that network operators use to determine the status of a remote interface
  - No credentials required
- Relies on ICMP Echo Request / Echo Response
- Does not actually exercise the probed interface
  - ICMP Echo Request may enter the box through another interface
  - ICMP Echo Reply may leave the box through another interface
- Requires reachability from the Pinging node to the probed interface
  - SAD !

Your New Friend, XPING

- Does not require reachability from the Pinging node to the probed interface
- Requires reachability from the Pinging node to some (i.e., any) interface that is local to the probed interface
  - We call this interface the “destination interface”
- Therefore, applicable in many scenarios where node executing XPING
  - Has a route to the destination interface
  - Does not have a route to the probed interface
- In all of these scenarios, the nodes executing XPING is not directly connected to the probed interface
  - If it were, it would have a direct route to the probed interface

XPING Scenarios

- XPING Node queries the status of Router Interface A
- Scenario I
  - XPING node supports IPv4
  - Router loopback interface is numbered from IPv4 global address space
  - Router Interfaces A through Z are unnumbered
- Scenario II
  - XPING node supports IPv6
  - Router loopback interface is numbered from IPv6 global address space
  - Router Interfaces A through Z are numbered from IPv6 link local address space

XPING Scenarios: Continued

- Scenario III
  - XPING node supports IPv4 and IPv6
  - All router interfaces are numbered from IPv4 global address space and from IPv6 global address space
  - Only the loopback address is advertise by any routing protocol

How Does XPING Work?

- Two new ICMP messages
  - Extended Echo Request
  - Extended Echo Reply
- Distinguish between the destination and probed interfaces
- Defined for ICMPv4 and ICMPv6

Extended Echo Request

- IP Header Fields
  - Source Address – Same as ICMP Echo Request
  - ***Destination Address – Identifies the destination interface***
- ICMP Fields
  - ***Type – TBD by IANA***
  - Code, Checksum, Identifier, Sequence Number – Same as ICMP Echo Request
  - ***ICMP Extension Structure: Identifies the probed interface***
    - See RFC 4884

Extended Echo Request: 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 IIO identifies the probed interface by address, the destination address and probed interface need not be from the same address family. Examples follow:
  - Destination address is IPv4; Probed address is IPv6
  - Destination address is IPv6; Probed address is MAC
- In most cases, a single IIO can identify the probed interface
- In some corner cases, two are required
  - One identifies by IPv6 link-local, the other by MAC

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

XPING User View: Query By Name

```
reji@R11_re0:~ # xping -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
```

XPING User View: Query By IPv6 Link-Local

```
reji@R11_re0:~ # xping -I 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

- XPING 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

Status

- Many comments addressed
  - Thanks to Jonathan Looney
- Prototype complete
  - Thanks to Reji Thomas
- Two new co-authors
  - Thanks Jen Linkova and Chris Lenart

Next Steps

- Vigorous, passionate debate, marked by
  - Polarization
  - Name-calling
  - Gratuitous scandal
- Call for adoption