cping: Concurrent ping and traceroute

https://www.prinmath.com/ham/cping.zip

Willem AC0KQ

What does cping do?

- Concurrent ping and traceroute
  - Ping multiple targets with history
  - Traceroute with history
- Real time monitoring of network
  - One sample per second with several minute history
- Features
  - Open source (Runs on Linux, OSX and Windows)
  - curses based so can be run remotely
  - Switch between traceroute and ping to troubleshoot
  - Adjust display for screen side

ping

- Target, address and statistics on
- Colored numbers is ping times

traceroute

- Runs continuously
- Numbers show time in ms
  - 3=3ms 3=30ms 3=300ms +=>1000ms X=lost
- History shows consistentcy
- Progression shows where problems are

Configuration file

- *cping.cfg* or */etc/cping.cfg*
  - Use first found
- Target/name pairs
  - Specify targets by IP or DNS
  - Rest of line is the name
- Group and indent by **>**
- Comment lines #

```
66.109.209.1   SkyBeam
8.8.8.8        Google
10.11.100.1    Principia
>Backbone
10.16.7.1      RattleSnake
10.16.0.1      CSU
10.16.2.1      BuckhornNC
10.16.8.1      BuckHornRM
10.16.1.1      HorseThNC
10.30.40.1     HorseThRM
>North
10.16.3.1      Budweiser
10.16.4.1      UNC
10.16.6.1      USC
>East
10.30.81.1     Eldorado
10.30.115.1    Westcreek
10.0.10.1      Blackforest
>West
10.30.60.1     Badger
10.30.150.1    Mosquito
10.30.160.1    Upper Dowd
```

Command line parameters

Usage: cping [-vbanrgxthS] [-N count] [-p us] [-f file] [-o file]

-b White lettering on black background
-a Show address in ping table
-n No hops on ping table
-r Scroll pings left to right
-p microseconds between pings [default 1000]
-f config file [default cping.cfg or /etc/cping.cfg]
-o output file
-N Stop after this many pings
-s seconds between ping
-S silent
-x show numeric ping character
-t show ping time stats
-v show cping version
-h help

Keystrokes

- Add more or less information as needed
  - Ping memory is unchanged
- Scrolling works in traceroute mode also
  - Starts new history

↑	**Scroll up**
↓	**Scroll down**
←	**Select previous router**
→	**Select next router**
Enter	**Traceroute to router**
Esc	**Return to ping screen**
i	**Invert colors**
r	**Reverse direction**
t	**Toggle time statistics**
s	**Toggle sound**
a	**Toggle address**
n	**Toggle hop count**
c	**Toggle character**
h	**Help**
q	**Quit program**

Internet Control Message Protocol (ICMP)

- RFC 792 (1981)
- Used for debugging and error messages
- Replies generated from IP stack (OS)
  - Unreachable
  - TTL exceeded
  - Redirect
- Used by ping and traceroute

Anatomy of an ICMP Packet

IP Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

- Header data: 16 bit ID, 16 bit sequence number
- Payload: timestamp (returned in reply)

How does it know?

- Uses a single IP socket to send and receive
- Source IP says who replied
- ID identifies ping program
  - traceroute and ping use different IDs
- Sequence helps count
- Payload contains time stamp for when sent
  - Returned in reply (measures round trip time)
- Time to Live (TTL) sets how far it can go
  - Used by traceroute to determine path

Future developments

- TCP pings
  - Half open just tickles TCP stack
  - Can be used to monitor services
- Expand feature
  - Ping multiple devices as a site
  - Ping devices on a link

Download from

https://www.prinmath.com/ham/cping.zip

Download contains source code
Linux, OSX and Windows executables
and update-cping script

Questions?