دستور Ping

Ping یک ابزار مدیریتی شبکه های کامپیوتری است که به منظور آزمودن دسترسی پذیری یک میزبان روی شبکه پروتکل اینترنت (IP) استفاده می شود و برای سنجش زمان رفت و برگشت پیام ها ی فرستاده شده از میزبان مبدا تا کامپیوتر مقصد به کار می رود. نام آن از اصطلاحات ناوبری و تشخیص فاصله توسط صوت فعال (Active Sonar) برگرفته شده که پالسی از صوت را فرستاده و به پژواک آن گوش می دهد تا اشیا را در زیر آب تشخیص دهد.

Ping به وسیله ارسال بسته های درخواست پژواک پروتکل پیام کنترلی اینترنت (ICMP) به میزبان مقصد و انتظار برای پاسخ ICMP، عمل می کند. در فرآیند، زمان ارسال تا دریافت (Round-trip time) اندازه گیری شده و از دست دادن بسته ها ضبط می شود. نتیجه آزمایش به شکل خلاصه آماری بسته های پاسخ دریافت شده، شامل زمان های رفت و برگشت حداقل، حداکثر و میانگین و گاهی انحراف از میانگین، چاپ می شود.

بسته به پیاده سازی واقعی، ابزار Ping با سوئیچ های خط فرمان متفاوتی برای فعال سازی حالت های عملکرد ویژه، اجرا می گردد. برای مثال انتخاب ها شامل، مشخص کردن اندازه بسته، عملکرد تکراری خودکار برای ارسال تعدادی مشخص از بسته ها می شود. بسیاری از سیستم عامل ها ابزار مکملی با نام Ping6 برای میزبان های IPv6 ارائه می کنند اما برخی سیستم ها این قابلیت را درون ابزار Ping دارند.

دیتاگرام IP

	Bits 0–7	**Bits 8–15**	**Bits 16–23**	**Bits 24–31**
سرآیند IP (20 bytes)	Version/IHL	نوع سرویس	طول	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	آدرس IP مبدا			
	آدرس IP مقصد			
سرآیند ICMP (8 bytes)	نوع پیام	کد	Checksum	
	داده سرآیند			
سربار ICMP (*دلخواه*)	داده سربار			

جدول ۵ – بسته ICMP

درخواست پژواک(Echo Request)

درخواست پژواک(Ping) یک پیام ICMP است که انتظار می رود به شکل پاسخ پژواک(Pong) در بازگشت دریافت شود. میزبان باید به تمام درخواست های پژواک پاسخ پژواکی دهد که شامل همان داده دریافت شده در پیام درخواست می شود.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
8 = نوع								0 = کد								Checksum سرآیند															
شناسه																شماره رشته															
داده																															

جدول ۶– بسته درخواست پژواک

پاسخ پژواک(Echo Reply)

پاسخ پژواک(Pong) یک پیام ICMP است که در جواب به یک درخواست پژواک صادر می شود و برای تمام میزبان ها و مسیریاب ها اجباری است.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0 = نوع								0 = کد								Checksum سرآیند															
شناسه																شماره رشته															
داده																															

جدول ۷– بسته پاسخ پژواک

نحوه ی به کار بردن دستور Ping در ویندوز

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count]
[-w timeout] [-R] [-S srcaddr] [-4] [-6] target [/?]
```

-t : تا قطع کردن دستور توسط کاربر(Control+C) دستور ping میزبان مشخص شده ادامه می یابد.

-a : آدرس IP را به نام میزبان تبدیل می کند.

-n *count* : مشخص کردن تعداد بسته های ارسالی که به صورت پیش فرض ۴ است.

-l *size* : تعیین اندازه داده های ارسالی بسته، مقدار پیش فرض ۳۲ بایت است و حداکثر تا مقدار ۶۵۵۲۷ بایت

-f : جلوگیری از چند قطعه شدن درخواست های پژواک ICMP توسط مسیریاب ها میان مبدا و مقصد(فقط IPv4)

-i *TTL* : تنظیم زمان طول عمر (Time to Live)، حداکثر مقدار ۲۵۵

-v *TOS*: تنظیم نوع سرویس (Type of Service). از ویندوز ۷ به بعد عملکردی ندارد

-r *count* : مشخص کردن تعداد گام ها میان مبدا و مقصد. حداکثر مقدار ۹ (فقط IPv4)

-s *count* : گزارش زمان برای هر درخواست پژواک دریافت شده و پاسخ ارسال شده، حداکثر مقدار ۴ (فقط IPv4)

-w *timeout* : تعیین زمان انتظار در واحد میلی ثانیه برای هر پاسخ

-R : دنبال کردن مسیر حرکت بسته (فقط IPv6)

-S *srcaddr* : تعیین آدرس مبدا

-4 : مجبور کردن دستور به کاربرد IPv4، ضروری فقط در هنگام استفاده از نام میزبان

-6 : مجبور کردن دستور به کاربرد IPv6، ضروری فقط در هنگام استفاده از نام میزبان

مثالی از دستور Ping

خطوط زیر خروجی اجرای Ping با مقصد www.example.com برای ۵ بسته است.

```
$ ping -c 5 www.example.com
PING www.example.com (93.184.216.119): 56 data bytes
64 bytes from 93.184.216.119: icmp_seq=0 ttl=56 time=11.632 ms
64 bytes from 93.184.216.119: icmp_seq=1 ttl=56 time=11.726 ms
64 bytes from 93.184.216.119: icmp_seq=2 ttl=56 time=10.683 ms
64 bytes from 93.184.216.119: icmp_seq=3 ttl=56 time=9.674 ms
64 bytes from 93.184.216.119: icmp_seq=4 ttl=56 time=11.127 ms

--- www.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.674/10.968/11.726/0.748 ms
```

بعد از اتمام بسته های ping نتایج جمع بندی شده اند. مثلا کوتاهترین زمان رفت و برگشت ۹,۶۷۴ میلی ثانیه، میانگین ۱۰,۹۶۸ میلی ثانیه و حداکثر زمان ۱۱,۷۲۶ میلی ثانیه بوده است. اندازه گیری انحراف معیار ۷۴۸ میلی ثانیه ای دارد.

دستور Tracert

دستور tracert یک ابزار عیب یابی شبکه های کامپیوتری برای نمایش مسیر و اندازه گیری تاخیر انتقال بسته ها از طریق پروتکل اینترنت(IP) است. تاریخچه مسیر به شکل زمان های رفت و برگشت بسته های دریافتی از هر میزبان پی در پی(گره راه دور) در مسیر، ضبط می شود؛ مجموع زمان های میانگین در هر گام، کل زمان صرف شده برای برقراری اتصال را نشان می دهد. Tracert تا زمانیکه تمام (سه) بسته ارسالی بیش از دوبار از بین رود،

سپس اتصال از بین می رود و مسیر قابل ارزیابی نیست. دستور Ping، از سوی دیگر، تنها زمان رفت-برگشت نهایی تا نقطه مقصد را محاسبه می کند.

دستور tracert روی تعدادی از سیستم عامل های امروزی مثل Apple Mac OS، Unix و ویندوز، وجود دارد. سیستم عامل های مبتنی بر ویندوز NT، عملکرد این دستور را با pathping نیز ازائه می کنند. برای IPv6 این ابزار گاهی به نام tracert6 یا traceroute6 می باشد.

پیاده سازی دستور tracert

به طور پیش فرض، traceroute، رشته ای از بسته های UDP به آدرس یک میزبان مقصد ارسال می کند؛ همچنین بسته های درخواست پژواک ICMP و TCP SYN نیز می توانند استفاده شوند. مقدار TTL که با نام محد وده گام نیز شناخته می شود، در تعیین مسیریاب های میانی که تا مقصد باید از آنها گذشت، به کار می رود. مسیریاب ها مقدار TTL بسته را در هنگام مسیریابی، یک واحد کاهش می دهد و بسته هایی را که TTL آنها به صفر می رسد، نادیده گرفته، پیام خطای ICMP «تجاوز از زمان ICMP» بازمی گرداند. مقادیر پیش فرض معمول برای TTL در ویندوز ۱۲۸ و در سیستم عامل های مبتنی بر یونیکس ۶۴ است.

Traceroute بوسیله ارسال بسته ها با افزایش تک واحدی مقدار TTL که از یک شروع می شود، کار می کند. اولین مسیریابی که بسته را دریافت می کند، مقدار TTL را کاهش می دهد و بسته را به دلیل داشتن TTL برابر صفر ، حذف می کند. مسیریاب یک پیغام تجاوز از زمان ICMP به مبدا می فرستد. مقدار TTL مجموعه بسته های بعدی برابر ۲ داده شده، بنابراین اولین مسیریاب بسته ها را عبور می دهد اما مسیریاب دوم آنها را حذف کرده و با پیغام تجاوز از زمان ICMP پاسخ می دهد. به این طریق، traceroute پیام های تجاوز از زمان ICMP بازگشتی را برای ساخت لیستی از مسیریاب هایی که بسته ها از آن می گذرند، استفاده می کند، تا زمانیکه به مقصد رسیده و پیام پاسخ پژواک ICMP بازگردد.

فرستنده به مدت تعداد ثانیه های مشخصی، منتظر پاسخ می ماند. اگر بسته ای در زمان مورد انتظار پاسخ داده نشد، در خروجی یک ستاره نمایش داده می شود. پروتکل اینترنت به اینکه بسته ها مسیر یکسانی به مقصد مشخصی را طی کنند، نیاز ندارد، در نتیجه میزبان هایی که لیست می شوند ممکن است میزبان هایی باشند که دیگر بسته ها از آن گذشته اند. اگر میزبان در گام شماره N پاسخ ندهد، گام در خروجی نادیده گرفته می شود.

نحوه ی به کار بردن دستور Tracert در ویندوز

```
tracert [-d] [-h MaxHops] [-w TimeOut] [-R] [-S srcaddr] [-4] [-6] target [/?]
```

-d : مانع تبدیل آدرس IP به نام میزبان می شود، که اغلب باعث نتیجه دادن سریعتر می شود.

-h *MaxHops* : مشخص کردن تعداد حداکثر گام ها تا مقصد. مقدار پیش فرض ۳۰ است.

-w *timeout* : تعیین زمان انتظار در واحد میلی ثانیه برای هر پاسخ قبل از اتمام زمان

-R : دنبال کردن مسیر رفت-برگشت (فقط IPv6)

-S *srcaddr* : تعیین آدرس مبدا (فقط IPv6)

-4 : مجبور کردن دستور به کاربرد IPv4

-6 : مجبور کردن دستور به کاربرد IPv6

مثالی از دستور tracert

خروجی زیر نتیجه اجرای tracert با مقصد www.google.com است.

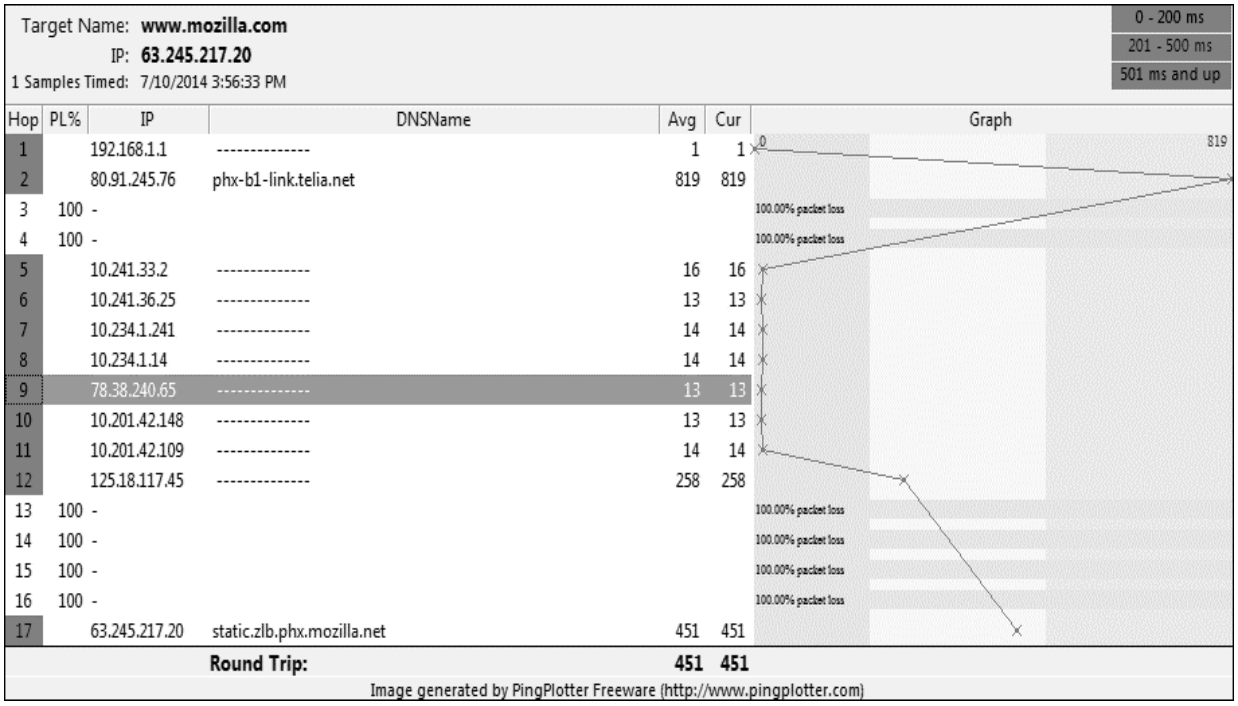
```
Tracing route to static-redirect.zlb.phx.mozilla.net [63.245.217.20]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    78 ms    77 ms    76 ms  91.98.0.1.pol.ir [91.98.0.1]
  3    77 ms    77 ms    77 ms  10.241.33.2
  4    76 ms    78 ms    76 ms  10.241.36.25
  5    76 ms    75 ms    78 ms  10.234.1.241
  6    78 ms    76 ms    75 ms  10.234.1.14
  7    77 ms    77 ms    77 ms  78.38.255.13
  8    79 ms    78 ms    79 ms  10.201.42.148
  9    79 ms    78 ms    78 ms  10.201.42.109
 10   321 ms   329 ms   325 ms  125.18.117.45
 11     *        *        *     Request timed out.
 12     *      445 ms   448 ms  las-b3-link.telia.net [213.248.98.237]
 13     *      448 ms   447 ms  las-bb1-link.telia.net [213.155.137.56]
 14   450 ms   446 ms   443 ms  phx-b1-link.telia.net [80.91.245.76]
 15     *      450 ms   459 ms  mozilla-ic-140268-phx-b1.c.telia.net
[213.248.104.202]
 16   443 ms   457 ms   466 ms  xe-0-0-1.core1.phx1.mozilla.net [63.245.216.18]
 17   456 ms   462 ms   460 ms  static.zlb.phx.mozilla.net [63.245.217.20]

Trace complete.
```

استفاده از دستور ping و tracert در یک محیط گرافیکی

برنامه ی PingPlotter استفاده از این دو دستور را در یک محیط گرافیکی ارائه می دهد و دیگر لازم نیست برای استفاده از آنها نتیجه را در محیط سیاه و سفید اعلان فرمان مشاهده کرد. مزایای استفاده از این ابزار بسیار زیاد است. از جمله این موارد می توان به ارائه چندین trace به مقصد های متفاوت و سپس مشاهده مسیر طی شده به مقصد مورد نظر به وسیله گرافها اشاره کرد. trace آدرس هایی که اخیرا استفاده شده اند در سمت چپ ذخیره و قابل مشاهده اند. همچنین نتایج را می توانید هم در قالب متن و هم در قالب تصویر ذخیره کنید.



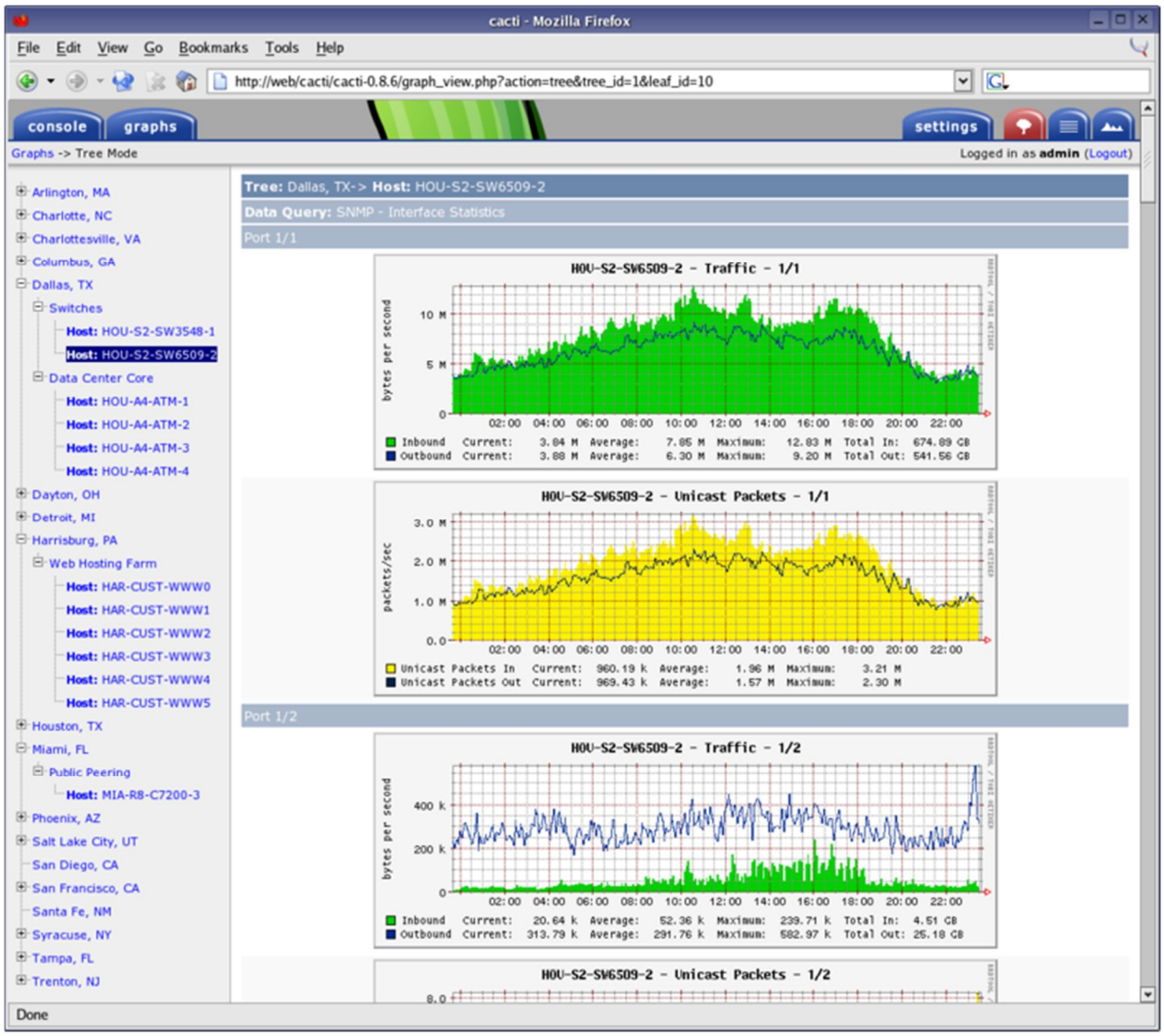
شکل ۵ – نمونه ای از خروجی برنامه PingPlotter

آشنایی با نرم افزار cacti

Cacti یک ابزار نظارت شبکه و گرافیکی مبتی بر وب و منبع باز به عنوان واسط برای ابزار ثبت داده استاندارد صنعتی منبع باز RRDTool است. Cacti به کاربر اجازه می دهد تا سرویس ها را در بازه زمانی از پیش تعیین شده سرکشی(Polling) نموده و داده های حاصل را رسم کند. این نرم افزار معمولا برای ترسیم داده های سری زمانی مواردی مثل بار پردازنده و بهینه سازی پهنای باند شبکه به کار می رود. یک کاربرد رایج بررسی ترافیک شبکه با سرکشی یک واسط مسیریاب با سوئیچ شبکه از طریق پروتکل SNMP است.

این نرم افزار می تواند چندین کاربر را اداره کند، که هریک مجموعه نمودار خود را دارند، در نتیجه گاهی به وسیله ارائه دهندگان میزبانی وب (به خصوص سرورهای اختصاصی، سرورهای شخصی مجازی) برای نمایش آمار پهنای

باند مشتریان خود استفاده می گردد. این نرم افزار می تواند برای تنظیم مجموع داده های خودش بکار رود که اجازه می دهد تنظیم(setup)های خاصی بدون هیچ ترکیب بندی دستی RRDTool بررسی شود. Cacti می تواند برای بررسی هر منبعی از طریق اسکریپت Shell و فایل های اجرایی، توسعه یابد.



شکل ۶ – تصویری از محیط برنامه cacti

Cacti می تواند یکی از نرم افزار های "cmd.php"، نسخه ی php مناسب برای نصب کوچک تر (smaller installation) ، "Spine" یک سرکشی کننده (Poller) مبتنی بر زبان C قابل گسترش تا هزاران میزبان، استفاده کند.

ویژگی های نرم افزار cacti

ویژگی های این نرم افزار شامل موارد زیر است:

- نمودارهای نامحدود
- پشتیبانی تکمیل(auto-padding) خودکار نمودار ها
- تغییر داده نمودار
- منابع داده انعطاف پذیر
- جمع آوری داده روی یک گستره زمانی غیراستاندارد
- اسکریپت های جمع آوری داده دلخواه
- پشتیبانی SNMP به صورت داخلی(built-in)
- قالب(template)های نمودار
- قالب های منبع داده
- قالب های میزبان
- نمایش درختی، لیستی و پیش نمایشی داده های نمودار
- امنیت و مدیریت مبتنی بر کاربر