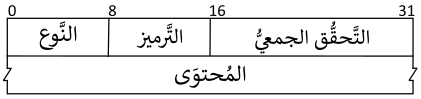
آی‌سی‌ام‌پی

پروتکل کنترل پیام‌های اینترنتی (آی‌سی‌ام‌پی) یکی از پروتکل‌های اصلی بستهٔ پروتکل‌های اینترنت می‌باشد. مورد اصلی استفاده از آن در سیستم عاملهای کامپیوترهای متصل به شبکه، برای ارسال پیام‌های خطا، برای مثال، سرویس مورد درخواست در دسترس نمی‌باشد یا اینکه میزبان یا روتر غیرفعال، است. از آی‌سی‌ام‌پی می‌توان برای رله کردن دستورها استفاده نیز کرد.[۱]



آی سی ام پی

آی‌سی‌ام‌پی[۲] متکی بر آی‌پی برای انجام کارهای خود است و خود بخشی جدایی ناپذیر از آی‌پی می‌باشد. این سیستم با سیستم‌های حمل و نقل داده مثل تی‌سی‌پی یا یودی‌پی متفاوت است و برای ارسال و دریافت داده استفاده نمی‌شود. این پروتکل به‌طور معمول در نرم‌افزارهای کاربردی شبکه استفاده نمی‌شود، مگر در چند استثنا مانند پینگ یا تریس‌روت.

آی‌سی‌ام‌پی برای پروتکل اینترنت نسخه ۴ (IPv4) به عنوان ICMPv4 نیز شناخته می‌شود. پروتکل اینترنت نسخه ۶ نیز از سیستم نامگذاری مشابه استفاده می‌کند: ICMPv6.

مشخصات فنی

پروتکل کنترل پیام‌های اینترنتی بخشی از پروتکل اینترنت می‌باشد، همان‌طور که در ریکوست فور کامنتس (آراف‌سی) ۷۹۲ تعریف شده‌است. پیام‌های آی سی‌امپی برای یافتن ایرادها در شکل داده‌های پروتکل اینترنت (همان‌طور که در آراف‌سی ۱۱۲۲ مشخص شده‌است) یا تشخیص یا مسیریابی در اینترنت ایجاد می‌شوند. خرابی‌ها و اشکالات به منبع اصلی انتشاردهندهٔ داده بازمی‌گردد.[۱]

مثالی از آی‌سی‌امپی پیام طول عمر بیشتر از حد مجاز شد، است. هر دستگاه حاضر در شبکه (مثلاً یک روتر) که داده‌های اینترنتی را منتقل می‌کند، باید به اندازه یک واحد از طول عمر داده ارسال شده تحت پروتکل اینترنت کم کند. در صورتی که طول عمر (تی‌تی‌ال) به ۰ رسید، پیامی مبنی بر پایان یافتن طول عمر در حین انتقال از طریق آی‌سی‌امپی برای دستگاه مبدأ ارسال می‌شود.

با توجه به اینکه هر پیام آی‌سی‌امپی به صورت مستقیم دردادهٔ پروتکل اینترنت بسته‌بندی می‌شود، مانند یودی‌پی پروتکلی نامطمئن است.

اگرچه پیام‌های آی‌سی‌امپی به صورت پیشفرض دردادهای پروتکل اینترنت وجود دارند، ولی پردازش این پیام‌ها به خصوص است و با پردازش معمول پروتکل اینترنت فرق دارد، در واقع به صورت زیر مجموعه‌ای از پروتکل اینترنت مورد تجزیه و تحلیل قرار می‌گیرند. همیشه لازم است که داده‌های موجود در پیام آی‌سی‌امپی بررسی شوند و برای دستگاه مبدأ به عنوان نتیجه ارسال شوند.

بسیاری از ابزارهای معروف شبکه با استفاده از آی‌سی‌امپی کار می‌کنند. دستور تریس‌روت با استفاده از بسته‌های یودی‌پی با تی‌تی‌ال از پیش تعیین شده، به دنبال خطاهای طول عمر در حین ارسال پایان یافت یا مقصد در دسترس نیست، به عنوان پاسخ می‌گردد. پینگ از اکوریکوست و اکوریپلای که پیام‌های آی‌سی‌امپی می‌باشند بهره می‌برد.

ساختار بخشی آی‌سی‌امپی

سربرگ

سربرگ آی‌سی‌امپی بعد از سربرگ آی‌پی۴ شروع می‌شود. تمامی بسته‌های اطلاعاتی آی‌سی‌امپی دارای یک سربرگ ۸ بایتی و قسمت دادهٔ متغیر می‌باشند. ۴ بایت اول سربرگ برای همهٔ بسته‌ها یکسان است. اولین بایت برای نوع آی‌سی‌امپی می‌باشد. بایت دوم برای کد آی‌سی‌امپی است. بایت‌های ۳ و ۴ برای کنترل سلامت آی‌سی‌امپی می‌باشد. ۴ بایت بعدی بر اساس نوع و کد آی‌سی‌امپی متفاوت است.[۱]

خطاهای آی‌سی‌امپی دارای قسمتی برای داده‌ها هستند که شامل کل سربرگ آی‌پی و ۸ بایت اول بسته‌ای که برای آن خطا ایجاد شده‌است. در این حالت بستهٔ آی‌سی‌امپی در یک دادهٔ دیگر پروتکل اینترنت قرار می‌گیرد.[۱]

Bits	۷–۰	۱۵–۸	۲۳–۱۶	۳۱–۲۴
۰	نوع	کد	کنترل	
۳۲	بقیهٔ سربرگ			

- **نوع** -- نوع آی‌سی‌امپی
- **کد** -- مشخصات بیشتر از نوع آی‌سی‌امپی
- **کنترل** -- در اینجا داده‌ای که برای کنترل خطا قرار گرفته‌است از سربرگ و دادهٔ آی‌سی‌امپی محاسبه می‌شود. الگوریتم با سیستم کنترل سلامت بسته‌های آی‌پی نسخه ۴ یکی می‌باشد.
- **بقیه سربرگ** -- این ۸ بایت براساس نوع و کد آی‌سی‌امپی متفاوت هستند.

توسعه دادن اطلاعات

توسعه داده‌های قرار گرفته در بستهٔ آی‌سی‌امپی به صورت زیر صورت می‌گیرید:

- پینگ در لینوکس ۵۶ بایت به ۸ بایت سربرگ آی‌سی‌امپی اضافه می‌کند.
- ping.exe ویندوز ۳۲ بایت به ۸ بایت سربرگ می‌افزاید.

لیستی از پیام‌ها کنترلی قابل استفاده

نوع	کد	معنی پیام
0 -- اکو پاسخ	۰	پاسخ اکو (مورد استفاده به پینگ)
۱ و ۲		*محفوظ*
۳ -- مقصد قابل دسترس	۰	شبکه مقصد غیرقابل دسترس
	۱	میزبان مقصد غیرقابل دسترس
	۲.	پروتکل مقصد غیرقابل دسترس
	۳	پورت مقصد غیرقابل دسترس
	۴.	تکه‌تکه شدن لازم است، و پرچم DF مجموعه
	۵	مسیر شکست خورد منبع
	۶	شبکه مقصد ناشناخته
	۷	مقصد نامعلوم میزبان
	۸	میزبان منبع جدا شده
	۹.	شبکه اداری ممنوع است
	۱۰	میزبان اداری ممنوع است
	۱	قابل دسترسی برای شبکه TOS
	۱۲	میزبان قابل دسترسی برای TOS
	۱۳	ارتباطات اداری ممنوع است
۴ -- اطفا منبع	۰	فرونشاندن منبع (کنترل ازدحام)
۵ -- تغییر مسیر پیام	۰	شکل داده تغییر مسیر برای شبکه
	۱	برای تغییر مسیر شکل داده هاست
	۲.	برای تغییر مسیر شکل داده TOS و شبکه
	۳	برای تغییر مسیر شکل داده و میزبان TOS
۶		جایگزین آدرس میزبان
۷		*محفوظ*
8 -- اکو درخواست	۰	درخواست اکو
۹ -- روتر آگهی	۰	روتر آگهی

۱۰—روتر درخواست	۰	کشف روتر / انتخاب / درخواست
۱۱—زمان بیش از	۰	عکسبرداری تمام شده در حمل و نقل
	۱	قطعه reassembly زمان بیش از
۱۲—پارامتر مشکل: بد هدر آی.	۰	اشاره گر نشان دهنده خطا
	۱	گم شده گزینه مورد نیاز
	.۲	طول بد
۱۳—برچسب زمان	۰	برچسب زمان
۱۴—پاسخ از برچسب زمان	۰	پاسخ از برچسب زمان
۱۵—درخواست اطلاعات	۰	درخواست اطلاعات
۱۶—پاسخ اطلاعات	۰	اطلاعات پاسخ
۱۷—آدرس درخواست ماسک	۰	آدرس درخواست ماسک
۱۸—آدرس پاسخ ماسک	۰	آدرس پاسخ ماسک
۱۹		محفوظ *است* برای امنیت
۲۰ از ۲۹		برای آزمایش *این سایت متعلق به* نیرومندی
۳۰ -- Traceroute	۰	درخواست اطلاعات
۳۱		شکل داده خطا تبدیل
۳۲		میزبان موبایل تغییر مسیر
۳۳		از کجا، آیا، شما (در اصل به معنای برای IPv6)
۳۴		در اینجا، من هستم، (در اصل به معنای برای IPv6)
۳۵		موبایل درخواست ثبت نام
۳۶		پاسخ همراه ثبت نام
۳۷		دامنه درخواست نام و نام خانوادگی
۳۸		دامنه پاسخ نام و نام خانوادگی
۳۹		پرش الگوریتم کشف پروتکل ساده مدیریت کلید برای پروتکل اینترنت
۴۰		Photuris، شکست‌های امنیتی
۴۱		آی‌سی‌ام‌پی برای پروتکل‌های تحرک تجربی مانند Seamoby [RFC4065]
۴۲ از ۲۵۵		*محفوظ*

همچنین مشاهده کنید

- پی ام تود
- آی‌سی‌ام‌پی نسخه ۶
- آی‌آردی‌پی
- حمله اسمارف
- تیسیپی
- پینگ
- تریس‌روت
- آی‌سی‌ام‌پی تونل

منابع

1. *Forouzan, Behrouz A. (2007). Data Communications And Networking (https://archive.org/details/datacommunicatio00foro_184) (Fourth ed.). Boston: McGraw-Hill. pp. 621 (https://archive.org/details/datacommunicatio00foro_184/page/n657)-630. ISBN 0-07-296775-7.*

2. *Postel, J. (September 1981). Internet Control Message Protocol (https://tools.ietf.org/html/rfc792). IETF. RFC 792. https://tools.ietf.org/html/rfc792.*

- ایانا پارامترهای آی‌سی‌ام‌پی (http://www.iana.org/assignments/icmp-parameters) [۱] (https://web.archive.org/web/20081026045758/http://freebie.fatpipe.org/~mjb/Drawings/UDP_ICMP_Headers.png) و *شبکه‌های کامپیوتری -- پایین روش بالا* توسط Kurose و راس

Wikipedia contributors, "ICMP," Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=ICMP

پیوندهای دیگر

- مراجع ۷۹۲، *پروتکل پیام کنترل اینترنت*
- آی‌سی‌ام‌پی نمودار توالی (http://www.eventhelix.com/RealtimeMantra/Networking/Icmp.pdf) بایگانی‌شده (https://web.archive.org/web/20201106230229/http://www.eventhelix.com/RealtimeMantra/Networking/Icmp.pdf) در ۶ نوامبر ۲۰۲۰ توسط Wayback Machine
- مراجع ۱۱۲۲، *مورد نیاز برای میزبان اینترنت -- لایه ارتباطات*
- مراجع ۱۷۱۶ ، به سمت *مورد نیاز برای روتر آی پی*
- آی‌سی‌ام‌پی فیلترینگ در فایروال (https://web.archive.org/web/20080519015614/http://www.daemon.be/maarten/icmpfilter.html)
- ایانا (http://www.iana.org/assignments/icmp-parameters)

آخرین ویرایش ۵ ماه پیش **توسط Yaser rezai انجام شده**

ویکی‌پدیا