

[an error occurred while processing this directive]

What Next? October 22, 1997

<thump><thump><thump>

Quiet please, quiet please... I know you're all excited but If we can just have a moment of your time... This won't take but a minute and then the festivities may begin.

First off, you're all invited to #rc5 on EFNnet. A live, virtual party is being held right now in celebration of our victory over RC5-56. This is one party you will not want to miss.

However, the obvious question to arise is "what next?" I'm sure you're all wondering what new magic distributed.net has up its sleeve. We've flexed our collective computing muscles and stomped 56-bit RC5 into submission. Far from becoming obsolete, distributed.net now has a much-renewed sense of vigor. We've tasted our first victory-and we LIKE IT.

As it stands, the solution came at an awkward time for us as the V3 protocol is still not ready to enter the coding stage. We are still working out the details of the specification and do not want to rush the design stage. It would be tragic to inadvertently miss something critical in our rush to get the specification out the door. Since a V3 client is most-likely weeks away from reality, we've opted to issue a point-release V2 client and divert all our energies to attacking 64-bit RC5.

Don't let your efforts stagnate! The last thing any of us want is for us to lose our momentum. We've all worked so hard to build distributed.net and in the process we've created what is easily the largest computer in the world. Lets roll out the 64-bit clients and keep adding processors!

A suite of V2 64-bit RC5 clients is available right now and the new 64-bit RC5 server network is in place and waiting for you to feed it with blocks. I invite everyone to hop over to ftp.distributed.net and grab a set. As you shut down your 56-bit clients, you'll be in the perfect position to pop in a 64-bit client to replace it. (note that we will be handling teams differently for RC5-64 and when you set up your clients you should use your own, personal email address and not a team address)

Beyond RC5, yes, we are still working on developing the V3 protocol and will be releasing a full client set to allow distributed.net as a whole to work on not only RC5-64 but a variety of other focused tasks. However, V3 client development will be a very different process than the V2/V1 development cycle we've seen in the past. The V3 client-server specifications and protocol will be a publicly published standard. This means that anyone will be able to use the protocol documentation to build their own, trusted, secure client modules. The days of limited source distribution and secrecy are soon to be gone forever.

On a related-note, there are many people who have wondered if 64-bit RC5 is really feasible. It is, as we all know, a much larger task than 56-bit RC5. Many people have wondered if it's even worth attempting. It's worth mentioning however that at our present rate the estimated time to complete 64-bit RC5 is actually less than our estimated time to complete 56-bit RC5 was back in April. We've already proven how the effort can grow wildly beyond all expectations and there is no reason whatsoever to think that this trend will not continue. As long as you know of at least one computer that's not running the client, there's room for growth. As V3 rolls out and the clients become exponentially more secure, easier to install, easier to maintain, and easier to track it will consequently also become far easier to recruit new machines and new members. Plus, the plans that we have for the stats server will blow you away!

Congratulations! All of us were here for the first of many distributed.net victories and all of us are pioneers in a long and ongoing effort to broaden the impact and reach of distributed computing technologies. It's an oft-said and rarely accurate saying, but for us it is quite applicable: The possibilities are endless!

Adam L. Beberg - Client design and overall visionary
Jeff Lawson - keymaster/server network design and morale booster
David McNett - stats development and general busybody

[an error occurred while processing this directive]