

A Day in the Life of a *Real* Network Guy (Separating the professionals from the amateurs)

The following story illustrates the challenges real IT network professionals face every day. This is a true story. Every detail of every event is real. It happened between mid June 2003 and mid July 2003, with most of the excitement (at least for a true computer nerd) happening the afternoon of July 15, 2003 and the morning of July 16, 2003.

Definitions

As in any industry, IT network professionals have a unique language. Here are some relevant words and acronyms:

TCP/IP – the set of communication protocols that define the Internet. By now, the Internet connects every nearly every organization in the world to nearly every other organization in the world. Most organizations also use TCP/IP in their own in-house networks.

Ethernet – The de-facto standard technology for local area networks (LANs).

IP Address – Roughly analogous to a street address in the physical world. An IP Address is a number that (more or less) uniquely identifies everything connected to a TCP/IP network. Note that a computer may have more than one IP Address for a variety of reasons. One relevant reason would be if the computer has more than one connection to the network.

DHCP – Dynamic Host Configuration Protocol. This is a way to dynamically assign IP Addresses to network devices that are mobile or that are not always connected to the network.

DNS – Domain Naming System. Since IP addresses are difficult to remember, most networks use DNS servers to translate names to IP Addresses.

RAS – Remote Access Services. This is Microsoft's early name for what it now calls dialup networking. RAS allows a modem connected to a server to become a network interface device.

The Story Begins

It all started one day in mid June, when this organization decided it needed the ability for people to dial directly into its network. Greg Scott of InfraSupport connected a modem to the main server, connected a phone line to the modem and tested the setup. It worked flawlessly.

Overlooked that day was a subtle change in DNS behavior.

The server already had an Ethernet connection with a statically assigned IP Address. But now, after adding the modem and setting up RAS, the server now had two network connections. These were the original Ethernet connection and the new RAS connection. DHCP would dynamically assign an IP Address to the new RAS connection.

Since the server was set to register itself with DNS, it now registered two IP Addresses – the original IP Address of its Ethernet adapter and now the new, dynamically configured IP Address of its RAS adapter. This becomes significant later in the story.

Three weeks later, after the new modem was a long-forgotten detail, this organization needed 3 new Windows 98 workstations added to the network. Our hero configured them, as he had done some many dozens of times before.

As an essential security practice for any organization connected to the Internet, this organization uses a corporate wide antivirus system to help ensure that incoming email does not cause any electronic mischief. The server automatically installs the antivirus software on any new workstation connecting to the network, and continuously installs updates as they become available.

The Fun Begins

As Greg logged into the new workstations and the antivirus installation program started, Greg proudly remembered that day when he set all this up. Had it been only 7 months for this customer? It seemed like so long ago now and the details from one installation mixed with details from so many others. How many times had he done this? He had long since lost count. Even so, this was still so cool – anytime a new workstation connects to this network, it automatically installs an up to date set of antivirus software to protect itself and the network from invasion. The best part – the workstation has no choice. If it logs in, it *will* install the corporate antivirus software, no exceptions. None of that nasty stuff is getting into *this* network.

Greg smiled an inner, confident smile and watched lazily as the first installation screen came up. Suddenly, jolting him wide awake, an ominous warning box popped up out of nowhere on the screen:

TCP/IP not configured. Installation aborted. Please see your network administrator.

Aw nuts! As the blood drained from Greg's face and the adrenaline started pumping, thoughts raced through his mind. What in the world is going on here? What is messed up with these laptops anyway? How could TCP/IP not be installed if this thing can use TCP/IP to get to the server and install the antivirus software? "This makes no sense!" he screamed to himself, as he put on his outward mask of a confident network administrator.

Greg's troubleshooting instincts quickly kicked in, honed by more than 20 years of problem solving. With grim, steely determination, he knew the next steps. First, was the problem related to only this workstation or did all these new systems share the problem? The next system behaved the same way. Hmmmm – maybe they had some problem with the factory installed Windows 98. Let's rebuild Windows 98 on one workstation while we try to probe a little deeper on the other one.

This is a well-known troubleshooting trick in the IT industry, especially with Microsoft products. First reboot it, if that doesn't work then rebuild it. More often than not, it works. So Greg set about reloading Windows 98 on one of the problem workstations.

Meanwhile, could something be wrong environmentally? Perhaps these refurbished workstations were fine but something else was going on in the network. It seemed highly unlikely, but then this problem made no sense. But then again, most problems make no sense until finding the answer – then they are obvious.

The next step, for no particular reason, was to try a ping test. Ping is a handy little program that sends a packet to a system and waits for an echo reply. If the other system replies, this is a good indicator it is online.

The Plot Thickens

Greg pinged the server and, to his horror, he noticed it translated to a different IP Address than he expected. Even worse, it did not reply!

“How is this possible?” he thought to himself. “I hard-coded that server's IP Address myself, but this IP Address from ping looks like it came from DHCP! But if that's the case, how come nobody else is having problems, only the antivirus installation program on these specific workstations? Maybe something is really out of whack on these things. We'll know soon enough once this other one finishes rebuilding.”

Right then, a terrifying thought crossed Greg's mind. “What if the CAB files are also messed up on these workstations, so I am just installing junk on top of junk?” Horrifying images of another all-nighter crept into Greg's mind as he pondered the possibilities.

But something was gnawing at the back of Greg's mind. *This didn't add up. Workstation corruption issues had never behaved this way . . .*

Inspiration Strikes

IT network troubleshooting is science. Develop a hypothesis, try a series of experiments to prove or disprove the hypothesis, and keep refining the experiments until arriving at an acceptable theory that fits the observed results. The process is sometimes ingeniously creative, sometimes maddeningly tedious.

When inspiration struck, the feeling was almost euphoric – *what if the workstations are fine and DNS is messed up?* The euphoria quickly gave way to dread as the consequences of that inspiration sank in – *if DNS is messed up, that could mean the whole network is messed up!*

Greg walked briskly into the server room, sat down at the server, and ran the DNS program. Eagerly anticipating and at the same time dreading the answers he would uncover, Greg's fingers flew over the keyboard as he navigated his way to the organization's Active-Directory integrated DNS zone.

There it was, clear as daylight – two “A” (hostname) records:

```
dellwin2k      A      192.168.0.231
dellwin2k      A      192.168.0.2
```

Greg breathed a sigh of relief while his curiosity started to rise. The workaround seemed simple enough – just get rid of that bogus first DNS entry with the wrong IP Address. Greg removed it, walked back to the workstations, retried the antivirus installation and this time it went smoothly.

But how did that bogus entry get inside DNS on the server? And what's to stop it from happening again?

The rest of the Story

With the immediate workstation problem solved, it was time to figure out why it happened in the first place. That was when Greg remembered the modem from three weeks ago. Of course! Yes, that had to be it – the new modem was now another network attachment and of course it would have its own IP Address! And of course it would register itself with DNS!

To confirm this hypothesis, Greg checked the IP Address DHCP had assigned to the modem. Sure enough, it matched that bogus DNS entry. Mystery solved, and now, with hindsight, blatantly obvious.

Now for the solution – how to ensure that the modem IP Address stays out of DNS? But first, was that the right solution? Could some scenario exist where it makes sense for DNS to have a record of the modem IP Address? Greg reasoned that since the extra DNS entry had already created this problem with the workstation antivirus installation, who knows what other unforeseen problems could come up? Also, this organization had lived for a long time without that DNS entry prior to installing the modem. So it seemed like it was best to permanently get rid of that DNS entry if possible.

Greg checked these Microsoft Knowledge Base articles:

- 198767 – *How to Prevent Domain Controllers from Dynamically Registering DNS Names*
- 275554 – *The Host's "A" Record is Registered in DNS After You Choose Not to Register the Connection*
- 292822 – *Name Resolution and Connectivity Issues on Windows 2000 Domain Controller with Routing and Remote Access Installed*
- 289735 – *Routing and Remote Access IP Addresses Register in DNS*

A complex picture unfolded that looked uglier by the minute. Since this was the only server at this organization, it held the roles of domain controller, RAS Server, DNS Server, and every other kind of server. The Microsoft articles told a complex story about how domain controllers always register all their IP Addresses with DNS, even those dynamically assigned to modems.

To work around the problem, Greg could manually change several registry parameters, which would force the server to not register *any* connections with DNS, including the Ethernet connection. Unfortunately, this would break several other fundamental network services. Microsoft further recommends to not install RAS on domain controllers or DNS servers for this very reason – domain controllers by design register all IP Addresses with DNS.

Suddenly, a very small irritation had the potential to blow up into a major network issue. But surely, some way could be found to mitigate the problem?

As of this writing, July 16, 2003, the best solution so far is to live with the problem. No clean method exists to fix the problem and the symptoms are now well known and easily recognizable. If more serious consequences occur, Greg will revisit the decision and decide a proper course of action.

Conclusion

This story is typical in so many ways. One small, seemingly insignificant network change caused a problem in a seemingly unrelated area several weeks later. Finding the answer turned into an iterative, “peeling the onion” exercise that led in an unexpected direction without a clean solution.

Issues like this separate the real professionals from everyone else.