Remote Windows NT Administration Using Windows CE Handheld Devices

Craig Stacey
Argonne National Laboratory

Abstract

As a systems administrator on call at any time of day, I want to explore ways to manage the environment and handle emergencies remotely. In this paper, I look at a number of options for remote administration using compact devices. While the most obvious form of remote administration is a laptop computer, not every organization has the budget to provide these to their systems administrators. Also, in some situations, even a laptop computer is too large to carry around conveniently. Therefore, I evaluated three devices to determine their usefulness for remote administration. While concentrating on Windows CE devices, I included a Palm Computing handheld for comparison purposes.

1. Overview of MCS environment

The computing environment in the Mathematics and Computer Science Division of Argonne National Laboratory consists of nearly a thousand computers, including supercomputers, servers, workstations, desktop machines, and laptops. Our Windows infrastructure consists of 13 production NT servers, eight Samba servers, eight experimental NT cluster servers, approximately 90 NT/2000 workstations, and 30 or so machines running Win95/98/2000 (mostly laptops).

The systems group that manages these machines consists of eight full time administrators, three of whom are at least partially responsible for the Windows environment. As with all other systems administrators, I have plenty to do, and our user expectations are high. This paper will deal with an experiment in remote administration: namely, using Windows CE devices to remotely administer our Windows servers.

2. Why use a handheld?

I did this experiment for a couple of reasons. First, it seemed like a great academic exercise. There's a certain challenge that comes from administering your organization's web server or Primary Domain Controller via a small handheld computer. However, there's also the allure of being truly able to administer servers remotely without having to carry around a laptop.

The advantage of such a model, should it prove successful, is an ability to carry a pocket-sized device and yet have full remote terminal capabilities. You'd not have to leave other situations for some emergencies, instead using your handheld device to solve the problem over a phone line, Ethernet, or wireless link. The usefulness of this becomes very apparent when you're at some social event or in a meeting.

It was only recently that our division's budget was large enough to supply the systems administrators with laptop computers. The cost of a Windows CE device is much lower than that of a notebook, and may be more palatable to some organizations.

3. The Experiment

There are a number of things to consider in this support model. My focus in this experiment was on security, functionality, usability, portability, and efficiency.

For each device tested, I performed a series of tests to try to accomplish common administration tasks, plus some emergency procedures. The following are the functions I tried to do with each handheld:

- Change user password
- Disable/Enable user account
- Change file ACLs
- Stop / Start web services
- Reboot server
- Powercycle server
- Send and receive email (of course)

As most NT Administrators are aware, most of these tasks can be accomplished from the commandline, but I wanted to be able to access the GUI as well, in case something went wrong with the telnet daemon.

3.1 The tools of remote systems administration

SSH: Ultimately, SSH is a necessity. In the case of our environment, unencrypted logins are rejected at our gateway router, so without a method of secure login, nothing can be done offsite. Therefore, for a device to be considered a viable option, SSH must be available.

VNC: In the GUI-intensive world of Windows, Virtual Network Computing (VNC) is a godsend. Allowing remote control of the desktop via the GUI is a tool I've come to rely on, and is, for many tasks, a vital part of remote administration.

Windows Terminal Server: When possible, the use of Windows Terminal Server is preferred to VNC. It's much faster, and does not have the SSH overhead for security.

SSL capable web browser: For some functions, a web browser is enough to accomplish some administrative tasks, thanks to some tools we employ at MCS, as well as Microsoft-supplied tools.

Ataman Telnet/RSH daemon: We've been very happy with this software package. While telnet, rlogin and rsh are blocked at our gateway router, they are allowed within our switched network. This allows us to integrate our Windows environment into parts of our automated unix administration tasks.

Perl and NT Resource Kit: Of course, perl is used extensively on our servers for administration. Combined with the Windows NT Resource Kit tools, a set of commandline tools exist for controlling and administering our servers, which can be quite desirable over a slow phone link.

Baytech Power strips: These remotely controlled power strips are wonderful. If a server is wedged beyond hope, being able to power cycle it remotely is quite helpful. You need to confirm the PC will come back after a hard power cycle. On some ATX motherboards, this is simply a BIOS setting. On some of our machines, though, I discovered I couldn't make the machine automatically come back, so I had to enable and use Wake-On-LAN.

3.2 The devices I tried

I should note that just as this paper was finished, Microsoft unveiled the next generation of Windows CE device, called PocketPC. Unfortunately, as of this writing, I've yet to experiment with these devices, so it's possible some of the statements I make do not apply to this new version. I've noted in the device listings which version of the operating system they are running.

I've been testing with two different Windows CE devices (one handheld, one palm sized) using a variety of connection methods including 56K modem, 802.11 wireless, 10BaseT Ethernet, and CDPD wireless modem. I have also, for the sake of completeness, looked at options under the Palm Computing platform using a Palm III.

The Computers:

The Handheld PC ("H/PC") is an NEC MobilePro 800. The device has 32MB RAM, a MIPS 4000 processor, built-in 56K modem, USB, IR port, one Type II PCMCIA and one CompactFlash PC Card slot. It runs Windows CE, Handheld PC Edition Version 3.0.

The Palm-sized PC ("P/PC") I tested is a Casio Cassiopeia E105. The device has 32MB RAM, a MIPS R4000 processor, IR Port, 65K color, and one CompactFlash Type II slot.

The Palm Computing Platform device used was a 3Com Palm III running PalmOS 3.1.

The Accessories:

I used Aironet 802.11b (aka 802.11 High Rate) wireless cards and access points to test the wireless connectivity. These were ideal as they were one of the first to market with an 11Mbit 802.11 standard wireless card, and had Windows CE drivers available right away. Preliminary tests with Lucent WaveLAN cards and drivers were problematic, but it's entirely possible these issues have been resolved. 802.11 Wireless cards are, at present, only available as a PCMCIA Type II card, and therefore will not work with the P/PC.

For wired ethernet, I used Socket Communications ethernet cards. These were the best card to use due to the fact they were designed with Windows CE in mind and have a very low power consumption. One of the cards tested was a CompactFlash ethernet, which meant I could use it with the P/PC.

The H/PC had its own built-in 56K modem. For the P/PC, I used the Casio 56K CompactFlash card modem designed for the E105. A standard Palm modem was used for the Palm III.

For wide-area wireless, a Novatel Wireless SAGE CDPD modem was used. This is an external device with a serial connection, allowing it to be used with all of the tested devices. CDPD connectivity is available in most major cities in the US. It has a bandwidth of 9600 bps.

3.3 Keeping it secure

We have a policy within our organization that states "External network connections to MCS resources shall not use clear text reusable passwords for authentication." In enforcing this policy, our gateway router rejects well-known services that use cleartext passwords, including telnet, POP, IMAP, and FTP. In addition, because we won't trust rlogin and rsh connections from offsite, and because additional authentication is sent cleartext, we block those protocols as well. Therefore, our only real method of performing tasks in any of the above protocols involves Secure Sockets Layer (SSL) or Secure Shell (SSH).

Our policy defines an external network connection as one that originates outside our gateway routers. We trust that our internal network is secured, as most traffic inside is sent over a switched network, making packet sniffing ineffective. We do still encourage encryption where possible, but it is not required. Our dialup connections originate outside the router, technically, but because the first point on the router is an address inside our network, we treat these dialups as if they are secured.

4. The Results

H/PC (NEC MobilePro 800):

Because this has both a CF card slot and a Type II PC card slot, I could test every connection method, and all were solid. The built-in modem was quite convenient, and I found I often left the wireless card in the unit rather than tether it with a wire. This did consume more power, but with no hard disk, the battery life of this notebook-sized device was still quite impressive.

The SSH client for Windows CE I used is SSHCE, a product currently in beta testing written by mov software (http://www.movsoftware.com). It's not the best SSH client I've used, but it's the only one for Windows CE, and it allowed me to login from offsite. From that remote login, I was able to reboot or powercycle the server, change user passwords, edit various configuration files, make registry changes, and use other administration tools all from the commandline.

VNC for Windows CE works surprisingly fast, and the 800x600 display on this handheld was quite nice for this. Double-clicking with a stylus is an art to be mastered, but I found my work with this, and with the other handhelds, was improved by the use of a fingertip stylus. All in all, once a machine is up and running, VNC was a good option. Technically, VNC meets our secure access policy, as the challenge and response are encrypted. However, once the session is active, all data is sent cleartext, thus any passwords I type in that VNC session are snoopable. Therefore, we at MCS recommend to our users that any VNC sessions be tunnelled through SSH. Unfortunately, SSHCE does not support port forwarding as of this writing, so that's not an option. I therefore limited our VNC experiments to onsite wireless, or offsite dialup.

What blew me away was Windows Terminal Server Client for Windows CE. This was fast and a joy to work with. I'd often forget I was using a WinCE device, as it looked and felt like a Windows 2000 machine. This was, by far, the most usable method, and I even relied on it for a couple of weeks while my laptop was being repaired.

By using the web-based administration feature of IIS, plus a handy user administration tool written by Mike Gomberg, I was also able to accomplish certain tasks using a browser, such as web service stop and start, password changes and account activation/deactivation.

Impressions:

Ultimately, this was the most usable of the devices. Not surprisingly, it is also the largest of the devices. In fact, there are now a number of micro notebooks running Windows 98 or 2000 that are smaller than this. It does have a standard laptop beat in terms of weight and battery life, as well as overall price, but if you're committing to carrying something of this size, you might be better served by getting a micro notebook like a Sony Vaio or an IBM Thinkpad 240.

P/PC (Casio Cassiopeia E-105)

I had the most hope for this device. It's compact, has a fantastic battery life, and a nice display. Unfortunately, the people writing tools for Windows CE aren't concentrating on the P/PC line. It seems a lot of the programs available for this are games and entertainment oriented. At the time of writing, the only version of SSHCE I received was written only for the H/PC. A P/PC and PocketPC version is now available, and I've requested a copy of the beta. At the time of the experimentation,

however, there were no SSH clients available. Aside from SSH, another stumbling block was the lack of a Windows Terminal Client for the P/PC. The absence of an encrypted connection method is is problematic, but not insurmountable. It simply requires I use a secure dialup for any offsite activity. This means the Sage CDPD modem was not really usable for this device.

I don't view this as a great setback, as the Sage modem is larger than the P/PC itself, and part of the appeal of this small device is that it's something you could conceivably have with you at all times.

VNC for Windows CE works, although it's obviously not designed for a screen that small; you can't see the entire hostname dialog box, for example, but if you trust your stylus typing or Jot writing, you can connect. It's pretty slow, especially over a dialup. I'd say it's something mostly useful in emergency situations, but not something you want to use every day.

TelnetCE from ActiveBridge has been working quite well, and I was able to use it over our secure phone link. This allowed me access to the commandline tools I like to use in administering the servers.

I'm not sure why Microsoft chose not to install a web browser on the P/PC devices, and I'm sure this has been rectified with the PocketPC. IBrowser, a free program from Foliage software (http://www.foliage.com) can perform most web browsing tasks, but it does not include SSL capability. They offer a $34.99 upgrade to Ibrowser Plus which allows https connections to work, and with that tool, the same web-based admin tasks can be accomplished on the P/PC as with the H/PC.

Impressions:

This was, by far, the most promising device. Compact enough to carry with me wherever I went, this could be the device that would get me out of having to make the long drive to work if something went wrong after hours. The battery life is incredible, and with the release of the PocketPC platform, it's possible more serious development will happen for these devices.

Alas, the lack of a Terminal Server client for the P/PC hurts. Were this tool available, the P/PC could be so much more useful as a remote administration tool. As it is, though, it's a handy device. The model I tested did not have a built-in modem, so a modem CF card and dongle were required. This is not a lot of extra baggage, and indeed the P/PC is the smallest of the configurations I tested. I look forward to trying out the new

PocketPCs, in the hopes that these are even more useful.

Palm Computing (Palm III)

In an effort to make sure I was fair and evenhanded, I tried using a Palm III for various administrative tasks. A color palm was not available during testing, so the lack of color on the screen, while certainly annoying in VNC, is not anything you can't get around if you need to.

Top Gun SSH (http://www.isaac.cs.berkeley.edu/pilot/) for the Palm III is not bad. Certainly, it's no worse than SSHCE in terms of speed and screen refreshes. Like SSHCE, it lacks port forwarding, so using VNC is restricted to secure phone line use. This isn't especially problematic, as our testing of the Palm III involved only Palm Modem tests. PalmVNC was a bit slow and buggy, and I didn't find it terribly useful, although it would certainly work in a pinch.

ProxiWeb by ProxiNet (http://www.proxinet.com) is a free SSL capable browser for Palm III. Using this, I could accomplish all the same web-based admin tasks as I could on the P/PC and H/PC.

Impressions:

The Palm is usable at the same fundamental level as the other two devices. Ultimately, if I can use the device to get a unix shell on one of our workstations at MCS, I can accomplish any of the emergency tasks I'd need to, and many of the day-to-day tasks. The Palm III certainly allows me to accomplish that. With the advent of the wireless Palm VII, I'm sure it becomes a much more viable remote administration tool. I look forward to experimenting with that model.

4.1 What worked well

On each of these devices, I was able to gain access to a command shell, which, as stated before, allowed me to accomplish just about everything I needed to. A good knowledge of the tools available for the commandline is handy. An added benefit of using these devices is also storing references and documentation on them.

They all did a passable job of running VNC, allowing me to perform GUI intensive tasks, including restarting a wedged telnet daemon.

Secure web-based administration went fine, although in the case of the P/PC it required the purchase of a product that really should be included.

Terminal Server Client is a wonderful program, and turned the H/PC into a full powered notebook computer. It's fast, efficient and secure.

4.2 What's missing

Obviously, Terminal Server Client would have been quite handy on either the P/PC or the Palm III. I hope Microsoft will at least develop a client for the PocketPC. Such a move could turn the PocketPC from a neat toy to a vital systems administration tool.

A port-forwarding SSH client would also be useful for those of us who work on sites that are paranoid about security.

5. Conclusions

Wireless internet access is becoming very common, and it would be nice for systems administrators to have access to the right devices and software to maintain their machines remotely. I hope developers at Microsoft and their hardware partners are envisioning the PocketPC to evolve into a wireless Windows terminal. Were that to happen, I can't imagine anyone who does this for a living not having one at his or her side. We're not there yet, but we could get there in the very near future. With the tools available today, you're essentially a phone call away from your machines at any time.

It's an interesting support model, and one that I think other systems administrators should think about. It's not right for every situation, but it's proven useful on more than one occasion, and is especially helpful in emergencies.

6. Author and Project Information

Craig Stacey is a systems administrator in the Mathematics and Computer Science Division at Argonne National Laboratory. His email address is stace@mcs.anl.gov.