Vacation Scholarship Report - AIGO Network

Jenni Gorham - gorhaj02@student.uwa.edu.au
25/02/2007

Introduction

The Australian International Gravitational Observatory (AIGO) is an interferometric gravitational wave detector located in the Shire of Gingin, Western Australia. This report explores the status of the AIGO network in February 2007 and the issues involved in remotely controlling the Zadko Telescope from a remote location. AIGO is on a two-way satellite plan with Telstra. All internet traffic passes through a single computer running Microsoft ISA Server on Microsoft Windows 2000 Server. This serves as a proxy server, firewall, DHCP server and router. The server connects through a network of ethernet cables and wireless bridges to computers in the main building, end stations, accommodation building, Gravity Discovery Centre (GDC), Southern Cross Cosmos Centre (SCCC) and Zadko Dome (see Figure 1).

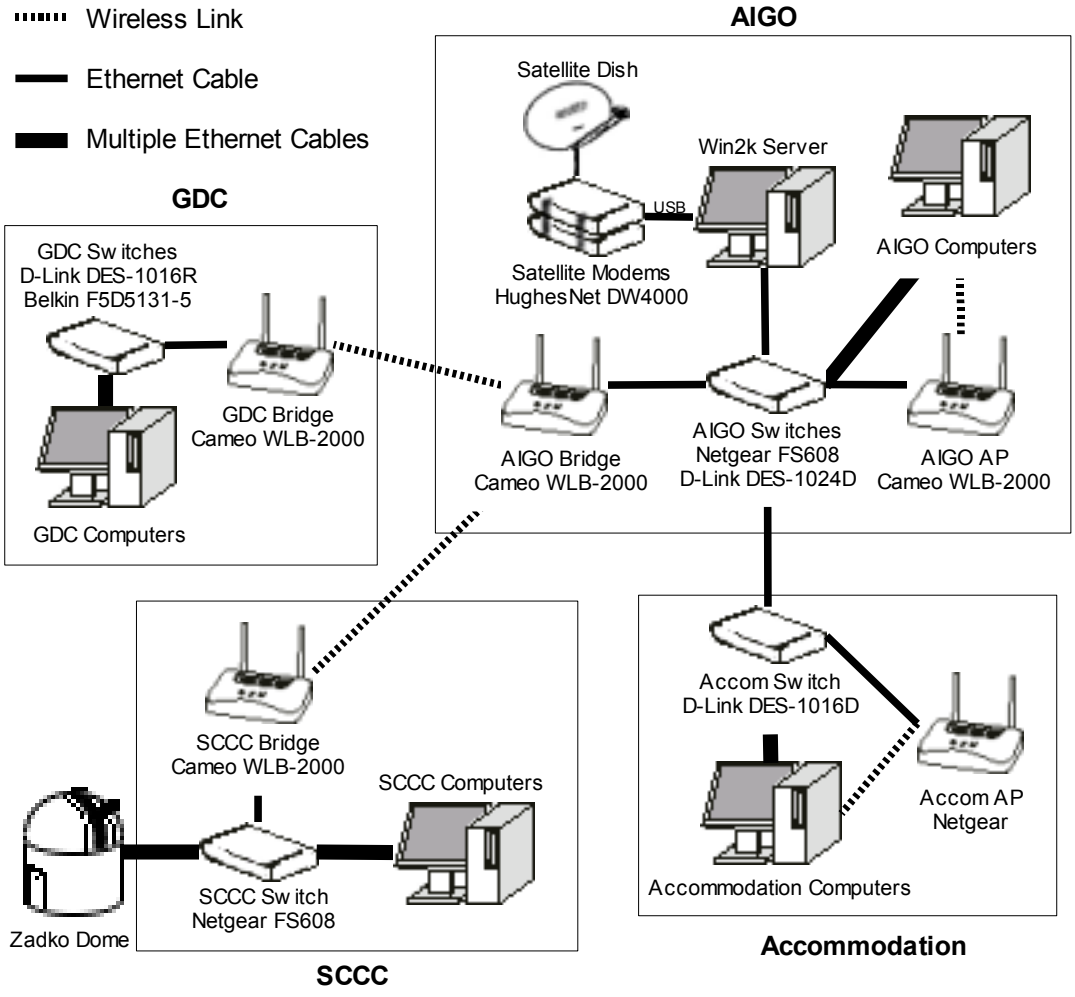

Figure 1: AIGO network diagram

Satellite Connection

The broadband satellite plan from Telstra has speed limits of 512kb/s down and 128kb/s up. The monthly limit is 3GB (uploads plus downloads); this plan is no longer available [1]. The satellite link introduces a long delay in transmissions – a ping to physics.uwa.edu.au takes 0.8 to 2 seconds. The theoretical limit for this delay (limited by the speed of light) is about 0.5s. We are using a DW4000 satellite system (consisting of one modem each for transmitting and receiving). The DW4000 connects to a computer over USB, and only comes with drivers for Windows, so is unsuitable for connecting to a Unix-based server. According to the manufacturer, the DW4000's speed capabilities are as follows: "When properly tweaked, downstream speeds average around 900+ kbps. Upstream varies from around 35-85+ kbps" [2]. In an SFTP transfer of a 17MB file from my laptop in AIGO to my home computer in Perth (on an high-speed ADSL2+ connection), the average upstream speed was approximately 50kb/s. This is far less than the 128kb/s limit that we could have according to our Telstra plan. The win2k server may also be degrading the connection speed. I recommend that we eventually replace the DW4000 with a satellite system that supports higher upload speeds and connects using TCP/IP over an ethernet cable (all modern operating systems support TCP/IP and will require no drivers to connect). The DW6000 is such a system [3].

The Server

The win2k server is a gateway between the local area network (LAN) and the internet. One USB port connects to the DW4000, providing the satellite link, and the ethernet port connects to a network switch, providing connectivity to the LAN. The server is situated in the electronics workshop, and has the local IP address 192.168.0.2.

Dynamic Host Configuration Protocol (DHCP) is a means of automatically configuring the network settings (IP address, gateway etc) of computers in a LAN [4], and is handled by a DHCP server (in this case, the Windows 2000 Server). To configure the DHCP server, go to Start → Programs → Administrative Tools → DHCP on the win2k server. It is set up to allocate addresses in the range 192.168.0.51 to 192.168.0.179 to clients. The rest of the addresses in the 192.168.0.0/24 range are available for static addressing. The DHCP server also has the capacity to permanently reserve an address for a specific computer (based on MAC address).

The Microsoft Internet Security and Acceleration (ISA) Server software provides a firewall, a proxy server and network address translation. To configure the ISA server, go to Start → Programs → Microsoft ISA Server → ISA Management. The proxy server is not in place to speed up web sites through caching, but to prevent people anonymously creating large amounts of traffic (which is very expensive on a satellite plan). As outgoing secure shell (SSH) connections are allowed through the firewall, it is still possible to create large amounts of traffic anonymously (through SFTP, for example), but this was not considered to be a large concern, since file transfers are more likely to be made through HTTP, FTP or P2P protocols, all of which are blocked by the ISA server's firewall.

Computers in the AIGO LAN have addresses in the range 192.168.0.1 to 192.168.0.254, but to a computer on the internet, they all appear to have the address 144.135.51.50. This is achieved by network address translation (NAT), also known as IP masquerading, which is the process of re-writing the source/destination IP addresses of traffic passing through a router [5]. This means that making a connection from a computer on the internet to a specific one inside the LAN is more difficult than usual, because there is no way for the remote computer to specify which local computer it wants to connect to. The way to fix this is called port forwarding (called "server publishing" by the ISA server) which I will explain below.

Jean-Charles Dumas informs me that the win2k server was not working at one point, and was replaced with a Windows XP computer with internet sharing until the win2k server was working again. During this time, internet access was significantly faster. It is therefore my recommendation that the win2k server be eventually replaced, preferably with a computer running GNU/Linux (in which case the satellite modems must be replaced as well, since the DW4000 doesn't support Linux). Linux can provide routing, NAT and a firewall (through netfilter/iptables [6]); a proxy server (through Squid [7]); and a DHCP server, all for free.

Wireless Bridges

The Wireless Access Points (WAPs) used at AIGO can be configured via Simple Network Management Protocol (SNMP) or with a USB cable and provided utility. The Windows drivers are on a CD in Steve's office, and there is an SNMP client for Linux called ap-config, available from the ap-utils package for many distributions. The WAPs can run in 4 different modes: access point, access point client, wireless bridge, or wireless repeater.

The connections from AIGO to the SCCC and GDC are made with wireless bridges. This was done by setting the three bridging WAPs (one in the SCCC, one in AIGO, and one in the GDC) to bridge mode, until January 2007, when connectivity to the SCCC WAP was lost. The signal strength measured by the SCCC WAP was lower than the GDC's, but the GDC bridge has been known to work (albeit slowly and unreliably) at much lower strengths. The only way that was found to restore the connection to the SCCC was to set the AIGO WAP to access point mode, and the SCCC and GDC WAPs to access point client mode. This setup is very similar to using bridge mode, with the most significant difference being a loss in bandwidth, according to http://www.mervin.net.au/wireless/template/PTPlinks.php [accessed on 25/02/07]. This speed reduction is not a problem, since the wireless speed (maximum 11Mb/s for IEEE 802.11b, which is the fastest speed that the current WAPs support) is far greater than the speed of the satellite link (512/128 kb/s down/up). If at some point a higher speed of wireless link is required between computers in the LAN, the WAPs could be upgraded to ones supporting IEEE 802.11g, supporting speeds up to 54Mb/s [8]. *

Description	ESSID	Channel	MAC Address	Manufacturer	IP Address
AIGO Bridge	aigo_wlan	13	00:40:F4:80:B3:86	Cameo Communications	192.168.0.10
SCCC Bridge		13	00:40:F4:80:B3:93	Cameo Communications	192.168.0.11
AIGO AP	aigoap	1	00:40:F4:78:D1:8D	Cameo Communications	192.168.0.13
Accom AP	accomap	6	00:09:5B:3D:73:C0 (wireless)	Netgear	
			00:0E:FF:FF:FF:00 (ethernet)		192.168.0.14
GDC Bridge		13	00:40:F4:81:03:E2	Cameo Communications	192.168.0.15

Table 1: Wireless Access Points in the AIGO LAN.

The bridging WAPs have RP-SMA (reverse polarity SMA) connections to their external antennae [9]. This should be taken into account if they or their antennae need to be replaced. The AIGO bridge has an omnidirectional antenna, and the GDC and SCCC bridges have directional panel antennae. Antennae and WAPs cost about $100-$300 each. WAPs in bridge mode generally only work with other WAPs of the same model, because there is no standard for bridging. Not all WAPs are capable of bridging or running in client mode. Alphastore (www.alphastore.com.au) carries a wide range of WAPs

* A quick explanation of notation: b stands for bit, B stands for byte (8 bits). The SI prefixes are used here in their original sense, not in the binary sense (e.g. when someone says they have a 700MB (megabyte) CD, they mean 700MiB (mebibyte) or 700×2^20 B), i.e. k = 1000, M=1 000 000.

and antennae.

A few weeks after the WAPs' configuration had been changed to remedy the SCCC WAP's failure to bridge, the wireless link to the SCCC was again failing. Pinging 192.168.0.11 (SCCC WAP) would often not work, while pinging 192.168.0.10 (AIGO WAP) and 192.168.0.15 (GDC WAP) would. Pinging the AIGO WAP from the SCCC would always work, but I haven't figured out why. Sometimes an SSH connection from outside the LAN to the dome control computer (through the SCCC WAP) would work, even though the SCCC WAP was unreachable from other parts of the LAN. At the time of writing, a new WAP, model DWL-2100AP from PLE computers [10] has been ordered to replace the defective one. This will most likely not work in bridge mode with the other WAPs, but should work in access point client mode.

Port Forwarding

The Zadko Telescope will need to be controlled remotely by connecting to a Dome Control Computer (DCC) in the Zadko Dome, which in turn connects to the MaxDome control circuit via RS-232. In order to make this connection through the satellite link, a technique known as port forwarding must be used because NAT makes the computers on the LAN effectively invisible to other computers. See [11] for more information about port forwarding. Common application-layer protocols have standard ports assigned to them, for example HTTP uses port 80, SSH uses port 22, and FTP uses 21. For incoming connections of a particular protocol to reach a computer on the LAN, a rule must be set up on the ISA Server to forward the port to the target computer's local IP address. For example, there is a rule to forward incoming SSH connections to the vacuum computer so that it can be logged into remotely.

It is necessary for the target computer to have a fixed IP address. There are two ways to do this: configure the DHCP server to reserve an IP address for it, or disable DHCP on the target computer, giving it an address that isn't in the DHCP address pool, and isn't used by any other computer with a fixed IP address (to find out which addresses were in use I used nmap: 'nmap -sP 192.168.0.1-254'). To reserve an address for a computer, go to Start → Programs → Administrative Tools → DHCP on the Windows 2000 Server. Select Scope, right-click on Reservations and select New Reservation. You must know the MAC address of the target computer. The DEC Alpha DCC that is currently in the dome has DHCP disabled, and is using the static address 192.168.0.3.

To configure the ISA server, go to Start → Programs → Microsoft ISA Server → ISA Management. To forward a port, ISA has to have a protocol definition for it. In ISA Management, go to Servers and Arrays → GINGIN2KSERVER → Policy Elements. If the protocol you wish to forward to the target computer is not defined, right-click on Protocol Definitions and select New → Definition. Then right-click on Publishing → Server Publishing Rules, and select New → Rule. This will forward the port and allow the connection through the firewall. SSH access to the DCC was required, but port 22 is already forwarded to the vacuum computer, so the SSH server was configured to use port 2222 (through the configuration file /usr/local/daemon/openssh/etc/sshd_config), and the ISA server was configured to forward this port to the DCC.

It is now possible to remotely log in to the DCC by using the command 'ssh root@144.135.51.50 -p 2222' in a UNIX-based OS (BSD, Linux, Mac OS X, etc). It is also possible to make connections with other protocols over the SSH connection by using SSH port forwarding. For example, if there was a web server running on the DCC, the HTTP connection could be tunneled over SSH by using the command 'ssh -L localhost:80:localhost:80 root@144.135.51.50 -p 2222'. Then the web server could be accessed by entering the address 'http://localhost' in a web browser. See the SSH manual page for more

information. XDMCP access (graphical remote login) to the DCC was also desired, but I didn't have any success getting that to work using ISA's server publishing, and it uses UDP so it won't work with SSH port forwarding; although an X11 connection can be forwarded through SSH to get remote access to graphical programs running on the DCC.

Firewall Piercing

There is a way to tunnel UDP traffic over an SSH connection, and that is to create a PPP connection over SSH, essentially emulating a full connection [12]. To achieve this, execute the following command from a root shell:

pppd silent updetach 10.0.0.1:10.0.0.2 pty "ssh -t root@144.135.51.50 -p 2222 pppd ipcp-accept-local ipcp-accept-remote"

This will create a ppp interface to the DCC, with the addresses 10.0.0.1 and 10.0.0.2 assigned to your computer and the DCC, respectively. Again using the example of a web server running on the DCC, it will be possible to access it by entering 'http://10.0.0.2' into the address bar of a web browser. It should be possible to get an XDMCP connection to the DCC by using the command "X :1 -query 10.0.0.2 -from 10.0.0.1", but this gives a segmentation fault (after displaying the DCC's hourglass cursor) when executed from my computer, so I'm not sure if it works at all.

Dialup Modem Connection

The satellite link has long delays and may be unreliable, so there is also a modem connected to the DCC which can provide a remote login, or ppp connection. I configured the modem to pick up after the first ring, using C-Kermit and AT commands. The modem is connected to the dome's phone line, with the phone number 9575 7775. If you dial in to the modem with a terminal program (HyperTerminal or Kermit for example), uugetty will provide a login prompt. Uugetty is started by init at boot time per /etc/inittab. A normal PPP connection is possible and I have configured the DCC to assign addresses 10.0.0.1 and 10.0.0.2 to the dialing computer and DCC respectively through the /etc/ppp/options.tty01 configuration file.

Conclusion

There are now two ways to get access to the DCC: through the satellite link, or through the phone line. The satellite link has higher transfer speeds, but longer delays, and traffic must also pass through the wireless bridge, which is currently unreliable, but will hopefully improve once the new WAP is installed. The telephone connection may therefore be the faster way to issue commands to the DCC, but at the cost of a phone call. The satellite link might be better suited to file transfers, as long as the monthly limit of 3GB is not exceeded.

If higher upload speeds and shorter delays are required for the satellite connection, the satellite modems should be replaced with ones supporting faster uploads and OS-independent TCP/IP networking, such as the DW6000 satellite system, and the win2k server should be replaced with a GNU/Linux server or other more efficient system.

References and Suggested Reading

[1] Telstra. *2-way Broadband Satellite service & plans*, [Online], Available from: <http://my.bigpond.com/internetplans/broadband/satellite/2_way_plans/default.jsp> [12/02/07]

[2] DirecWay. *DirecWay DW4000*, [Online], Available from: <http://www.copperhead.cc/DW4000.htm> [12/02/07]

[3] DirecWay. *DirecWay DW6000*, [Online], Available from: <http://www.copperhead.cc/DW6000.htm> [12/02/07]

[4] Wikipedia. (23 February 2007), *Dynamic Host Configuration Protocol*, [Online], Available from: <http://en.wikipedia.org/wiki/DHCP> [25/02/07]

[5] Wikipedia. (22 February 2007), *Network Address Translation*, [Online], Available from: <http://en.wikipedia.org/wiki/Network_address_translation> [25/02/07]

[6] Wikipedia. (23 February 2007), *Netfilter/iptables*, [Online], Available from <http://en.wikipedia.org/wiki/Netfilter/iptables> [25/02/07]

[7] Squid. (21 August 2006), *Squid Web Proxy Cache*, [Online], Available from: <http://www.squid-cache.org/> [25/02/07]

[8] Wikipedia. (22 February 2007), *IEEE 802.11*, [Online], Available from: <http://en.wikipedia.org/wiki/IEEE_802.11> [25/02/07]

[9] Wikipedia. (31 January 2007), *SMA Connector*, [Online], Available from: <http://en.wikipedia.org/wiki/SMA_connector> [01/02/07]

[10] PLE Computers. (2006), *PLE Computers*, [Online], Available from: <http://www.ple.com.au/> [25/02/07]

[11] Wikipedia. (20 February 2007), *Port Forwarding*, [Online], Available from: <http://en.wikipedia.org/wiki/Port_forwarding> [25/02/07]

[12] François-René Rideau. (24 November 2001), *Firewall Piercing mini-HOWTO*, [Online], Available from: <http://tldp.org/HOWTO/Firewall-Piercing/index.html> [25/02/07]