Suggestions for Network Configuration at Mt. Waliguan Observatory (WLG)

John Ogren, NOAA/CMDL, Boulder, USA

October 25, 2004

The basic requirements for the computer network at the WLG GAW station include:

– firewall protection against unauthorized access
– support for multiple computers to share the station's single internet connection
– secure remote connection to any computer in the WLG internal network from authorized external computers.

NOAA/CMDL uses Linux on the aerosol data acquisition computer planned for the WLG aerosol upgrade, and needs to connect to this computer from Linux computers at CMDL's offices in Boulder, USA. This need provides the motivation for CMDL to contribute resources to assist the WLG staff in upgrading the WLG network for secure remote access.

If adequate funding is available, the simplest solution for configuring the WLG computer network is to hire an expert network consultant and purchase commercial-grade networking hardware. Such a solution would require minimal networking expertise on the part of the WLG technical staff. On-going support of the network would be provided by the consultant.

An alternate approach is for the WLG technical staff to develop the necessary expertise to implement and support the network in-house. This solution minimizes the procurement and support costs for the network, but requires more staff time to learn how to implement and support the network. The following discussion gives suggestions for in-house network development and support. The emphasis is on using low-cost hardware and free software as much as possible.

DISCLAIMER: I am a scientist and engineer, but not a networking professional. We have implemented the suggestions described below in a test network at NOAA/CMDL, and am confident that they will meet the needs of the WLG network. However, I cannot guarantee that they will work, and the WLG technical staff must conduct their own analysis of the feasibility and suitability of these recommendations. Fortunately, the low procurement costs of the hardware and software will allow evaluation of these recommendations for less than USD $200. The suggestions below are my personal opinions, and do not constitute an endorsement by the U.S. Federal Government for any specific products.

1. A Linksys WRT54G or WRT54GS router provides the functionality required at WLG, cheaply enough that one or more spares can be kept at the station in case of lightning damage. This device currently costs around USD $70 (see http://www.pricescan.com/items/item146116.asp). A detailed description and technical specifications of the router are located at http://www.linksys.com/products/product.asp?grid=33&scid=35&prid=601. This router supports both wired and wireless connections. Wireless support is not required at WLG at present, but might prove to be useful for connecting guest

computers to the network in the future. The WRT54G is recommended specifically because of the additional functionality that is provided by the optional Sveasoft firmware (see below).

2. A firmware upgrade for the WRT54G is available from Sveasoft at http://www.sveasoft.com/modules/phpBB2/index.php. This upgrade costs USD $20 and provides advanced features not present in the standard Linksys firmware. Features in the Sveasoft firmware relevant to the WLG network include advanced firewall configuration, port forwarding, port translation, and a secure command-line interface.
3. A graphical firewall configuration tool for the Sveasoft firmware called “Firewall Builder” is available for Windows 2000 and XP at http://www.netcitadel.com and costs USD $50. This program simplifies the job of configuring the firewall on the router, for example, to define which external computers are allowed access to the network and to define the mapping of port numbers to services on specific computers on the network. A free version of Firewall Builder is available for Linux at http://sourceforge.net/project/showfiles.php?group_id=5314, and is included on the NOAA/CMDL LiveCPD bootable aerosol data acquisition system CD-ROM (available at ftp://ftp.cmdl.noaa.gov/aerosol/etc/cpd/cpdlive.iso). An illustrated (but somewhat outdated) example of the use of Firewall Builder with the Linksys WRT54G router is available at http://www.fwbuilder.org/archives/cat_slides.html#000157.
4. The WRT54G router provides 4 ethernet ports for the LAN. Additional ports can be provided by connecting a network switch to one of the LAN ports on the router.
5. Secure connections to computers on the WLG local network from external computers can be achieved using a combination of the *SSH* (Secure Shell) and *VNC* (Virtual Network Computing) client and server software for both Windows and Linux systems. The *SSH* software provides secure, compressed and encrypted connections over the public internet, while the *VNC* software allows graphical display of the remote computer's screen and control of the remote computer's keyboard and mouse.

   a. Links for downloading software.
   - http://www.realvnc.com has client and server software for *VNC* connections for both Windows and Linux.
   - http://sshwindows.sourceforge.net/ has the OpenSSH client and server software for *SSH* connections for Windows computers.
   - ftp://ftp.cmdl.noaa.gov/aerosol/etc/cpd/wlg has custom software written by NOAA/CMDL that facilitates using *SSH* to establish secure *VNC* connections to Windows and Linux servers from Windows and Linux clients.

   b. Router configuration.
   The router must be configured to forward incoming *SSH* connections to the appropriate computer. In the example below, incoming connections on ports 10100-10120 are forwarded by the router to port 22 (*SSH*) on the instrument computers at WLG with local network addresses in the range 192.168.1.100 - 192.168.1.120, respectively.

   c. Windows server configuration.

Windows computers on the WLG local network must run both *SSH* and *VNC* servers. In addition, the CMDL-supplied *sleep.exe* program must be available in a directory in the server's path, such as C:\windows\system32; this program provides a short delay needed while the VNC connection is being established. The *VNC* server must be configured for access without a password and to listen for incoming connections <u>only</u> on the local machine, as the *SSH* server provides authentication for the connection. This configuration information is entered by clicking “Start” -> ”Programs” -> ”RealVNC” -> ”VNC Server” -> “Configure”, and then selecting “No Authentication or Encryption” on the “Authentication” tab and checking “Only accept connections from the local machine” on the “Connections” tab.

d. <u>Linux server configuration.</u>
The CMDL Linux-based aerosol data acquisition computer comes pre-configured for secure graphical access using *VNC* over an *SSH* connection. The normal (insecure) port used by the *VNC* server is blocked by the firewall on the Linux server, so that the only access is through an encrypted connection via the *SSH* server.

e. <u>Windows client configuration.</u>
Both SSH and VNC client software are needed for remote Windows clients to connect to a Windows or Linux server at WLG. CMDL has written the *svnc.exe* program to make it easy to make a connection. The SSH client *ssh.exe* (part of the OpenSSH package) and VNC client *vncviewer.exe* programs must be available in a directory in the Windows path on the client computer. The syntax for running *svnc* to connect to a remote Windows or Linux server is

```
svnc -C -p port -l user servername
```

where *port* is the port number used for the connection, *user* is the username on the server, and *servername* is the name or IP address of the WLG internet connection. For example, if the WLG internet connection is named wlg-gaw.dyndns.org, a connection to the Windows computer at 192.168.1.105 on the WLG local network would be made with the command

```
svnc -C -p 10105 -l user wlg-gaw.dyndns.org
```

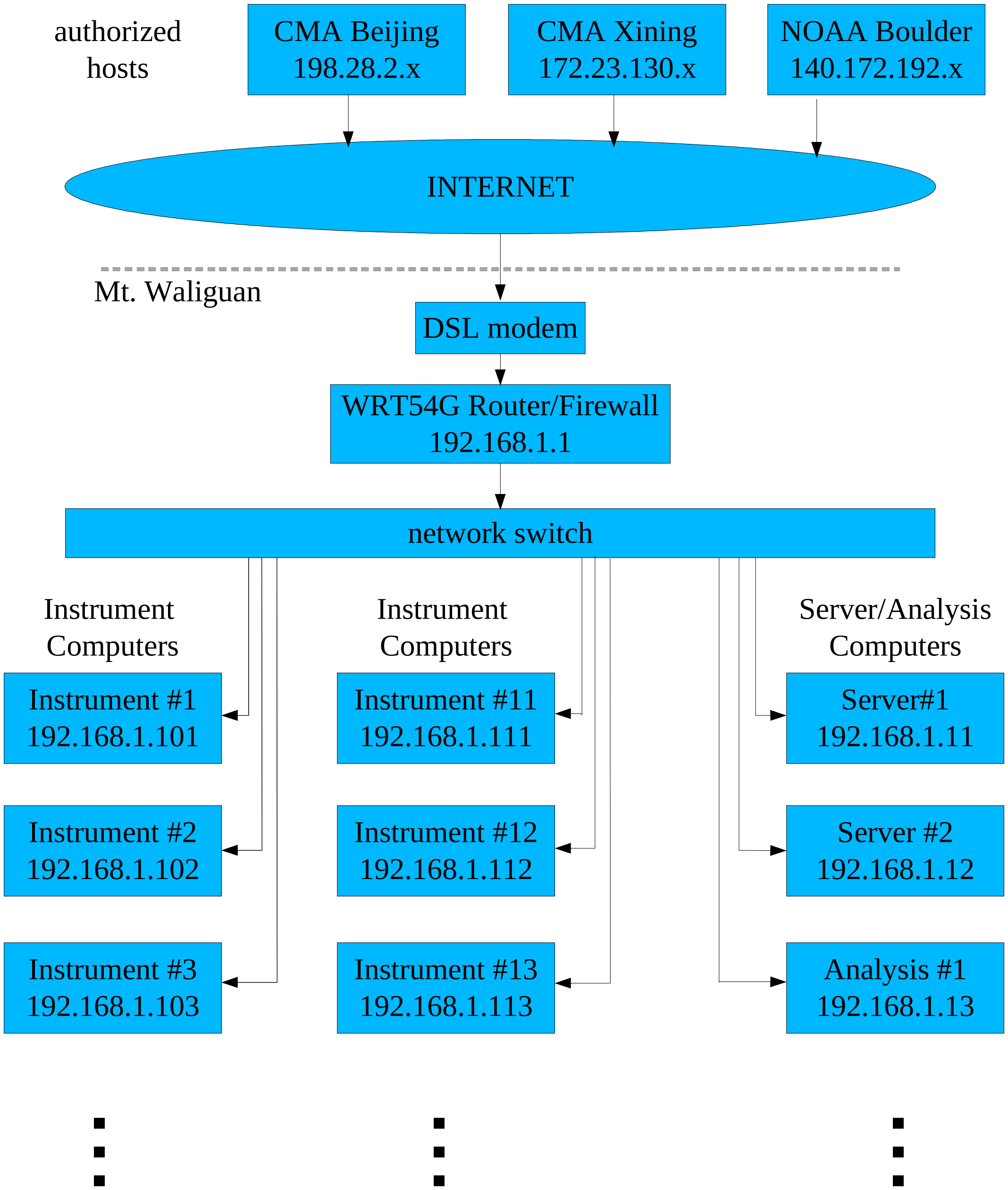
The command can be associated with an icon on the Windows client's desktop, so that the remote computer can be accessed by simply double-clicking on an icon.

f. <u>Linux client configuration.</u>
A short bash script *svnc* is available on the CMDL ftp server to simplify the process of connecting to a remote Windows or Linux host from a Linux client. The syntax is the same as for the *svnc.exe* Windows program. The *ssh* and *vncviewer* programs must be in the user's path for this bash script to work.

6. Additional help for configuring *SSH* and *VNC* to work together can be downloaded at these sites:
http://pigtail.net/LRP/printsrv/cygwin-sshd.html
http://pigtail.net/LRP/vnc/index.html
http://archive.erdelynet.com/ssh-l/2002-09/msg00027.php
http://www.jfitz.com/tips/ssh_for_windows.html

7. Secure file transfers between Windows computers can be done with the ‘sftp’ or 'scp' software included in the OpenSSH package.
8. The WRT54G router supports pass-through of VPN connections, in the case that the WLG technical staff determines that VPN is the preferred solution to securing the remote connections to the WLG network. VPN connections are not used by the SSH+VNC solution described above.
9. The Linux computer to be used for aerosol data acquisition will use a GPS receiver for maintaining an accurate system clock. Windows computers on the WLG network can automatically synchronize their clocks to the GPS time standard with the free NetTime program, available at http://sourceforge.net/project/showfiles.php?group_id=10109.
10. The WRT54G router will work with the current part-time internet connection at the WLG site, which uses a DSL modem and the PPPoE transport mechanism. The router can be configured to disconnect from the internet if the connection has been inactive for a specified period of time, and to reconnect automatically if any of the networked computers attempts to connect to an external IP address.
11. The WRT54G router supports Dynamic DNS, which allows external access to the internal network using a fixed hostname, even though the external IP address of the network changes. See http://www.dyndns.org/services/dyndns/ for more information. By configuring one of the WLG computers to upload data at a specified time every hour, there will be a time window once per hour when external access to the network is possible. The aerosol computer will come pre-configured to upload data every 6 hours, and this can easily be changed to upload data every hour. If external access to the network is required at arbitrary times, the account with the WLG Internet Service Provider will need to be changed to a permanent connection. In this case, it would be simplest to have a static IP address assigned by the ISP.

Network Configuration


authorized hosts
CMA Beijing 198.28.2.x
CMA Xining 172.23.130.x
NOAA Boulder 140.172.192.x
INTERNET
Mt. Waliguan
DSL modem
WRT54G Router/Firewall 192.168.1.1
network switch
Instrument Computers
Instrument #1 192.168.1.101
Instrument #2 192.168.1.102
Instrument #3 192.168.1.103
Instrument Computers
Instrument #11 192.168.1.111
Instrument #12 192.168.1.112
Instrument #13 192.168.1.113
Server/Analysis Computers
Server#1 192.168.1.11
Server #2 192.168.1.12
Analysis #1 192.168.1.13

Revision Notes

original September 6, 2004

revised October 10, 2004

- change recommendations for secure VNC connections based on results of additional tests and software development at CMDL

revised October 25, 2004

- use OpenSSH client rather than putty on Windows
- add -C switch to arguments to *svnc*, to compress data sent over the internet.