Abstract

Management of large networks usually follows a hierarchical model with responsibility for various functions delegated to organizations or individuals. At Virginia Tech, Communications Network Services handles most network management tasks except the assignment of IP addresses to individual users and the registration of individual hosts. These functions are delegated to Network Liaisons, or NLs. This document describes the functions of the NL and provides some basic instruction on performing the required tasks.

Throughout this document, the terms “department” and “departmental” are used to identify a particular group of network users and not necessarily what the University considers an official department. These terms may refer to anything from an entire college to a sub-group of a department.

Questions or comments about this document can be sent to hostmaster@vt.edu. General questions can be sent to CNS at ask-cns@vt.edu.

A summary of the slides from the Network Liaison Class are at http://rdweb.cns.vt.edu/~benchoff/dnl-slides/dnm-slides.html.

This document is also available in HTML and PostScript from http://www.cns.vt.edu. The online version has hypertext links to a number of other documents.
Contents

ii
1 Network Liaison’s Functions

Each department with connections to Virginia Tech’s internetwork must have a Network Liaison or NL. The NL is an interface between the department and CNS network management. The responsibilities of the NL include:

- Requesting protocol addresses from network management and assigning them to individual users
- Sending host name registration information to network management.
- Joining the vt-dnet mailing list and forwarding information to users in the department as needed
- Maintaining a database of all hosts in the department and their system managers

In addition to the items above, the NL may also wish to:

- Join local mailing lists for other protocols used in the departmental LAN
- Provide first-level troubleshooting to users in the department

The rest of this document will attempt to provide some background information on each of these topics.

A list of NLs can be found at http://rdweb.cns.vt.edu/public/info/network-liaisons.html

1.1 CSO Name Server

All NLs should be sure their office, department, and home phone numbers are correct in the CSO name server. A Virginia Tech Personal userID (PID) is not required at this time, but it is suggested that each NL get a PID and set mail forwarding appropriately. Future mailing lists, host registration applications, etc. may rely on PIDs. If you are currently using POP to read mail from mail.vt.edu, you have a PID.

1.2 Alternates

Since the NL is the only person who can request addresses and register hosts, most departments will want to designate an alternate NL to assume these responsibilities if the primary NL is unavailable. The alternate NL should have access to all of the required information.

It is particularly important that the data maintained by the NL be passed along if the NL is no longer going to perform that function. Without accurate host name and address information, the new NL will have to reconstruct all of the data.
1.3 vt-dnet

The vt-dnet mailing list is used for network management to send information to NLs. It is very important that the NL read this list and forward any relevant information to users in their department. Anyone can subscribe to the list by sending mail to listserv@listserv.vt.edu with the text “subscribe vt-dnet Your Name”. Items of importance on this list may include:

- Announcements of scheduled network downtime
- Announcements of network changes requiring some intervention from system managers (changes of addresses, etc.)
- Changes in procedures

1.4 Getting Started

In order to register as the NL for a department, send mail to hostmaster@vt.edu with your name, department, and the sub-domain that will be used for your IP addresses. (Sub-domains are discussed later.)

2 Network Protocol Addresses

A communications protocol is the set of standards used by two processes that communicate with each other. It can be thought of as a set of rules or the language for communication. One host may use several protocols to communicate over the network. Each of these protocols must provide a way to identify a particular host on the network. That method of identification is the network address and each protocol uses its own form of address. An address is just a series of numbers that uniquely identifies an endpoint of a connection. For example, a telephone number is an address on the public switched telephone network. Just like telephone numbers, addresses used by communications protocols must be assigned so that one particular endpoint can be found from anywhere on the network. Network addresses may be divided into subnetworks, much like the telephone system is divided by area codes and exchanges. Protocols commonly used on Virginia Tech’s network include IP, IPX, and AppleTalk.

In order for a host to communicate, it must use an address that is assigned to it based on its location in the network. This assignment may be automatic (as with AppleTalk) or it may require configuration by the system manager (as with IP). Since numeric addresses are inconvenient for people to use and remember, addresses may be associated with names. Naming hosts is discussed later in this document.
2.1 Internet Protocol (IP)

IP stands for Internet Protocol. It is the protocol that is used throughout the worldwide Internet (estimated to interconnect more than 20 million hosts), and is the only protocol that is supported on all parts of Virginia Tech’s network. It is well-documented and designed to work under the worst network conditions. It is also designed to take advantage of high-bandwidth networks and offers better performance and reliability than other protocols. (It should be noted that although IP is generally the best protocol, particular implementations of IP may be inferior to other protocols on specific platforms or for specific applications.)

Each host running IP must have an IP address. An IP address is usually expressed as four numbers (each less than 255) separated by periods, e.g. 128.173.3.7. As discussed above, an IP address is determined by the location of the network connection. A particular IP address is only valid within one subnet. In most cases, one subnet will serve one or a few buildings. When requesting addresses, be sure to specify the building where they will be used so that CNS can assign an address in the proper subnet.

The NL requests IP addresses by sending mail to hostmaster@vt.edu indicating the number of addresses needed, building, and sub-domain (the subdomain is part of the host name, and is discussed later). It is usually a good idea for the NL to have a few spare addresses for testing and future assignment. It is important that the NL understand where the assigned addresses will work. The NL then passes this information on to the individual users requesting addresses. The NL should be sure to give the user other configuration information such as gateway, netmask, broadcast address, domain name servers, time servers, etc.

2.2 Local Area Network (LAN) Protocols

Many LAN protocols are in use on the campus internetwork. These protocols are not necessarily designed to take advantage of high-performance networks or to support large numbers of hosts. In order to simplify installation and configuration, management functions required for reliable operation on large networks are often omitted. CNS routes and manages the most popular and widely-used LAN protocols.

IPX

IPX is routed on parts of Virginia Tech’s network and managed by CNS. More information on Virginia Tech’s implementation of IPX can be found at http://rdweb.cns.vt.edu/public/notes/ipx/.

AppleTalk

AppleTalk is routed on parts of Virginia Tech’s network and managed by CNS. AppleTalk users should contact zonemaster@vt.edu for information on establishing zones. Any de-
partment considering running an AppleTalk router should also contact zonemaster@vt.edu before starting.

Other Protocols

All of the protocols discussed so far are routed on Virginia Tech’s network. The process of routing uses devices (routers) specifically designed to interconnect networks running a particular protocol or set of protocols. Routers participate directly in the communication and exchange information about the structure of the network with each other. This is the most efficient and reliable means of communication.

Another method of interconnecting network segments is bridging. Bridging floods all traffic throughout all segments of the network without knowing the location of the destination node. Once the bridges learn the location of a node, traffic is only forwarded on the segments necessary. This requires all of the bridges to track a list of all devices communicating on the network. Bridging consumes much more bandwidth than routing and doesn’t support the features required to isolate and control problems.

In addition to the routed protocols listed above, some segments of the network are interconnected with bridges and will support protocols other than the routed protocols. Bridging is being turned off as rapidly as possible and applications that use protocols other than IP, IPX, or AppleTalk will no longer work when that happens. The most common protocol that will no longer be available is NetBEUI. NetBEUI is the native transport for NetBIOS on Ethernet. NetBIOS can also be transported over IP and that is the suggested transport.

3 IP Domain Names

Hosts using IP identify each other by network addresses. People usually prefer to use names for hosts rather than addresses. The mapping between host names and addresses is handled by servers of the Domain Name System (DNS). These domain name servers manage the Internet-wide “domain name space”, which includes top-level domain names, such as edu, com, and org; second-level domain names, such as vt.edu, sun.com, and npr.org (which are delegated to individual organizations); and further divisions as desired by these organizations.

The DNS must handle millions of host names and therefore each server does not keep track of all of the host names. Instead, domain names are divided up among the various organizations that need them. This division into “sub-domains” allows an organization to assign host names within its sub-domain by putting the data in its domain name server. Our local name servers handle the host names for Virginia Tech, which must end in .vt.edu. Hosts outside of Virginia Tech can look up vt.edu hosts by querying our local name servers.
Local division of the name space requires that there be at least two more parts in front of the .vt.edu, a department sub-domain and a host name.

The department sub-domain is selected by the NL and the department. Usually this is the common abbreviation for the department, such as cs.vt.edu for the Computer Science department. If one NL managed all of the hosts for the College of Education, these hosts could all be registered under a single sub-domain like ed.vt.edu.

The host name is selected by the NL or individual user. It identifies a particular host (computer) within a department sub-domain.

A typical domain name looks like this: vtvml.cc.vt.edu. The host name is vtvml, the department sub-domain is cc (the Computing Center in this case), and vt.edu is Virginia Tech’s top-level domain. A department may also elect to further subdivide their domain names by using additional designators before their department sub-domain, for example laplace.mprg.ee.vt.edu. In this case, Electrical Engineering has elected to designate hosts in the mprg group within their own sub-domain.

A domain name:

- is not case sensitive, but it is suggested that only lower-case letters be used to minimize problems.
- must begin with a letter (“a”-“z”).
- may also contain digits, periods, or hyphens (“0”-“9”, “-”, “.”).
- may not contain any other characters (such as “/” or “_”).
- may not contain spaces.

All hosts on campus running IP (anything with an IP address) should have a domain name registered in the vt.edu domain. This is not strictly required, but several things make it very important:

- A growing number of sites will not communicate with hosts that are not registered in the DNS.
- Network troubleshooting procedures are simplified when machines are named.
- Address conflicts (duplication) are more likely to be noticed if hosts are registered.

The names associated with the IP addresses assigned to a department are registered by the NL. That process is described in more detail later.

An entry in the DNS is called a resource record, or RR. The type of RR that matches host names to IP addresses is an address RR (A RR). In addition to address resource records (A RR), there are a few other RRs that can be added to the DNS.
3.1 Aliases (CNAME RRs)

Hosts registered in the DNS can have aliases. Aliases are useful when a department offers some sort of service for use by other people on the network. The use of an alias allows the service to be moved to some other host without users needing to reconfigure their clients. For example, the machine ebud.cns.vt.edu is the home for the CNS WWW server. The alias www.cns.vt.edu resolves to ebud.cns.vt.edu. (In this case www.cns.vt.edu is the alias and ebud.cns.vt.edu is the canonical host name. The alias is bound to the canonical host name with a CNAME RR.) If this service is moved to another host, the alias can be changed to resolve to the new host name and users do not have to reconfigure their clients. This is very helpful if a host provides multiple services (ftp, www, gopher, etc.) If it is later necessary to move one or more of these services to another host and each service has its own alias, the transition doesn’t require reconfiguration of the clients.

Aliases are not used to create short host names. The process of allowing just the host name to be used (rather than the fully-qualified domain name) is done by the resolver code on a particular client. This is typically done by setting the domain path.

3.2 Mail eXchangers (MX RRs)

A Mail eXchanger is a host that receives mail for another domain name. MX records can be used to forward mail when a host is down, provide mail service for a domain that is not a host, or forward mail for a host which does not have a SMTP server.

In general, mail should be sent to people at their pid@vt.edu addresses and not individual workstation addresses. Individuals can have their PID mail forwarded to any location they choose without changing anything in the DNS.

Operating a mail server is time consuming and complicated. Unless including the departmental name in the address is considered to be of great importance, a department wishing to run its own mail server can have the individual users forward their PIDs to the mail server without having any special records in the name server.

3.3 Update Times

The name servers are usually restarted on Tuesdays and Thursdays. Data should be submitted to hostmaster@vt.edu by 10am to be included in the update. Note that the updates are sometimes delayed or done early. If the timing of an update is critical due to the change of a server name, please indicate that in your request. Hostmaster can either notify you when the change is done or schedule a special update.
3.4 Nslookup and DIG

There are a number of tools available to query the name servers and check the database. Under Unix, nslookup is a standard part of most systems and dig can be built on most systems. There are similar commands available for Windows and Macintosh.

There is a TXT RR in each departmental data file called nsdata. your_subdomain. vt.edu which will indicate when the file was last updated. Here is an example of looking up the record with nslookup.

```
benchoff:~/tmp> nslookup
Default Server: moniker.cc.vt.edu
Address: 128.173.4.113

> set querytype=any
> nsdata.ee.vt.edu
Server: moniker.cc.vt.edu
Address: 128.173.4.113

```

3.5 Other Domains

Departments sometimes host web sites for professional organizations or as part of research projects. CNS does not provide domain name service for non-vt.edu domain names. The Blacksburg Electronic Village, most domain registrars, and many local ISPs will provide domain name service for a small fee.

- Aliases are registered in the non-vt.edu domain which resolve to vt.edu host names.
- The addresses will reverse to vt.edu host names.
- It is the department’s responsibility to see that the domain is properly registered and paid for.

3.6 vt.edu Domain Names

There are a few cases where domain names are registered without a departmental sub-domain label, e.g. www.vt.edu. Hosts registered like this must be the official source of some service provided for the University and requests for such host names are reviewed before they are put in the name server. One exception is an MX record for the departmental sub-domain, which can be registered for any department.
3.7 Registering Host Names

Each host with an IP address should be registered in the domain name server. The NL can register hosts by sending a plain text file in the format described below to hostmaster@vt.edu. Every time a host is added, changed, or deleted, the NL must send the entire updated list to hostmaster@vt.edu.

The data files submitted to hostmaster are processed by a program and they must be in a particular format. This section describes that format and it is important that it be followed carefully.

The NL can request a copy of the current DNS entries for a department by sending mail to hostmaster@vt.edu. This list will only include addresses that are registered in the name server.

File Format

The file must be ASCII text and must not be formatted by the user’s mail agent to wrap or be encoded as a MIME attachment.

Each record in the file must have the following format:

hostname:ip:mxhost,(mxhost...):alias,(alias...):hw:os:mac:comment

Field descriptions (all host names should be fully qualified):

hostname (required) (sample: vtvm1.cc.vt.edu) See the discussion of the required format of host names earlier in this document.

ip (sample: 128.173.4.1) The IP address of the host being registered.

mxhost the mail exchanger for THIS host. May be a list of hosts separated by commas. (optional)

alias comma separated list of aliases (optional)

hw Hardware type. (optional)

os Operating system. (optional)

mac MAC (Ethernet) address. Use dashes and not colons for the address (like 08-00-0b-27-5f-ed). (optional)

comment Use any fields you like from here out
General Notes

- No fields should include spaces until you get to the comment field
- All domain names should be fully qualified (like vtvm1.cc.vt.edu, not vtvm1)
- List hosts in numeric order by IP address
- Put records without IP addresses first in the file
- Do not include multiple zones (If you have both 128.173 addresses and 198.82 addresses, do not combine them in the same file.)
- Do not include multiple sub-domains (If you manage several departments, do not combine the data for deptx.vt.edu and depty.vt.edu.)
- Send the complete list of hosts for your department. All existing data will be replaced.
- Each record must be one line. Do not break long records over multiple lines. (Be careful that your mail program doesn’t do this.)
- Do not include signatures in the mail file.
- If you are not using a particular field, be sure to include the colons out to the last field that you use.
- Do not use leading zeros in ip addresses: use 128.173.4.1, not 128.173.004.001.
- Include your sub-domain on the subject of your mail.

Sample records

The following section contains several sample records. There is a record, description, and the resulting entry in the name server. The name server RRs are included for information only. Don’t worry if you don’t understand what they are.

Example 1 Host and IP address only.

groupw.cns.vt.edu:128.173.5.9: (This is what the line in the data file would look like.)

This record is just a host name and IP address. The MX record will point to the host listed and the HINFO will be blank. This will take care of what needs to be done for most hosts.
Example 2 MX record only.

cns.vt.edu::groupw.cns.vt.edu,morse.cns.vt.edu:
In this case, there is no host for cns.vt.edu. It is used for mail only. This will generate two MX records for cns.vt.edu. The first one will point to groupw.cns.vt.edu and the second one will point to morse.cns.vt.edu. Note that the IP address field is not used, but the colons that delimit it are still there. (The hosts morse.cns.vt.edu and groupw.cns.vt.edu are registered somewhere else in the file with their ip addresses.)


Example 3 Host with IP address and MX hosts.

groupw.cns.vt.edu:128.173.5.9:groupw.cns.vt.edu,morse.cns.vt.edu:
This will point mx records for groupw to itself and morse.

groupw.cns.vt.edu. IN A 128.173.5.9

Example 4 Host with IP address and Aliases

This will add CNAME RR (aliases) for morse. Aliases are useful if you provide some sort of service with a host. If you choose to move the service to some other host, all that needs to be changed is the CNAME. Note that the MX field is not used here, but the colons that delimit it are still there.

morse.cns.vt.edu. IN MX 0 morse.cns.vt.edu.

Example 5 Host with IP address and Ethernet MAC address

This record has the MAC (Ethernet) address filled in. This info is not used in the name server. It is something that NLs should be keeping track of for their own purposes. Note that the address does not contain colons (like 08:00:00:00:00:00:00), dashes are used.

```
morse.cns.vt.edu. IN MX 0 morse.cns.vt.edu.
```

**Example 6** Host with HINFO data

```
morse.cns.vt.edu:128.173.12.12:::DecStation:Ultrix-4.2:
morse.cns.vt.edu. IN HINFO DecStation Ultrix-4.2
morse.cns.vt.edu. IN MX 0 morse.cns.vt.edu.
```

Here the host type and operating system are listed. Note that these two fields do not contain blanks. These fields are not used for much, and are considered to be a security problem by some. Use of these fields is totally up to you.

**Example 7** Hostname, IP address, MX records, Aliases, etc.

```
morse.cns.vt.edu. IN HINFO DecStation Ultrix4.2
morse.cns.vt.edu. IN MX 0 morse.cns.vt.edu.
```

**Example 8** Sample File

Here is a short sample of what a file sent to hostmaster might look like.

```
# DNS data for cns.vt.edu
# (lines that begin with # are comments.)
#
# MX record for sub-domain. Most departments won't use this.
# morse will receive mail for cns.vt.edu
cns.vt.edu::morse.cns.vt.edu
morse.cns.vt.edu:128.173.12.8
```

11
# A few services run on this host:
#
# Regular hosts, just name and address
berg.cns.vt.edu:128.173.12.10
hovhaness.cns.vt.edu:128.173.12.11
# End of data file

3.8 Static Host Table

Domain name service has been the Internet standard for several years. If your host requires a static host table, please contact the vendor and encourage them to add a resolver that uses DNS. CNS no longer maintains or distributes static host files.

4 Database

Each NL should keep track of all of the hosts in the department. Information should include user name, system manager, room number, portal number, ip address, MAC address, and any other fields the NL finds useful. The data for entry in the name server can be generated as a report from this database.

5 Reporting Problems

Network problems should be reported to the CNS Network Operations Center at (540) 231-6780. This number is answered between 0800 and 1700 Monday through Friday. Users in a department should first report problems to their NL if possible.

When reporting a problem, the following information will be required:

- Problem description
- Contact information (building,room,phone,e-mail)
- Problem location (building,room,portal number)
- Network information (addresses, host names)
- Description of problem

The following questions will help determine the source of the problem:
• Has it ever worked? When did it quit working?
• Do other people nearby have the same problem?
• Have there been recent changes to the host (upgrades, etc.)?
• Do other machines work when connected to the portal?
• Is the problem with one protocol or all?
• Can the host ping its default gateway by IP address?
• Can the host ping things off of your subnet by number? by name?

6  Other Topics

A number of other topics are important to system and network management but are well beyond the scope of this document. A few of these are mentioned in this section.

6.1  System Management

All computers require system management. The operating system and applications must be updated from time to time, and various configuration changes must be made when network changes are made. Backups of important data should be done frequently.

6.2  Security

The network layer for the communications path between two endpoints may pass through many segments or devices. In the case of remote access, some of these pieces may be under the control of hostile third parties. For this reason, the network layer is not an appropriate place to create security mechanisms. Applications must assume that all network traffic may be monitored, intercepted, or forged and implement security at the higher layers. The most secure solution is to use applications that do end-to-end encryption between the client and server.

A secure replacement for rlogin/rsh/rcp is ssh. PGP offers file and e-mail encryption and digital signatures. Neither of these products is officially supported by the Computing Center, but both are in widespread use on campus.

Access Control

Any kind of security based on network addresses or domain names is probably not secure at all. The question of how to determine Virginia Tech users by IP address or domain
name comes up frequently when someone wants to restrict access to a resource to Virginia Tech users. Neither of these is a valid solution. There may be cases where non-University users originate connections from vt.edu domain names or where University users are using domain names or addresses that are not Virginia Tech’s. Use of domain names or IP addresses can narrow the number of authorized users to “reasonably local” people, but will exclude some potentially valid users.

Dynamic Host Configuration

It may be desirable to use dynamic host configuration (DHCP or BOOTP) in some situations. CNS offers DHCP as a service on most of the network. See [DHCP at Virginia Tech](#) for more information.

It is acceptable for a department to run a DHCP server so long as two things are done:

- Only known MAC addresses (registered with the server owner) should be configured.
- The server owner must maintain log archives to be able to identify what client was using a particular address at any given time.

DHCP/BOOTP requests are not routed off of the local subnet. A free DHCP server can be obtained from [Internet Software Consortium](#).

Public Access

A host that is used by a large number of people (e.g. in a lab) presents special problems. The system manager should assure that there are access controls in place to be able to trace a particular activity back to the responsible party or to limit what can be done from the host.

6.3 Acceptable Use

Acceptable use of information systems at Virginia Tech is described by [Acceptable Use Of Information Systems At Virginia Tech](#) and a number of State and Federal laws. From time to time, incidents such as threatening e-mail or denial of service attacks must be investigated by University personnel or law enforcement. It is important that the NL for a sub-domain know who the system manager is for all hosts in the sub-domain and pass along any information related to problems to that person. The system manager is expected to know who was using the host at a particular time or to be able to secure the host against unauthorized use. It is expected that the individual user responsible for problems can be found.

A typical case would be that an outside organization contacts someone in CNS to report a network abuse situation. CNS will pass this report along to the NL for the sub-domain.
of the machine and the NL will pass it along to the system manager. The system manager is expected to work with the original complainant and resolve the situation. Support is available from the Computing Center and CNS for some phases of this resolution.

In cases of persistent abuse that is not corrected, or on-going incidents, CNS may shut off the connection to a host until the system manager is able to correct the problem.

6.4 References/Additional Information

- [Acceptable Use Of Information Systems At Virginia Tech](#) outlines general policies about information systems at Virginia Tech.

- [Recommendations and Policy for Win95 Setup and Security](#) from the Computing Center’s WWW server outlines many important configuration issues for MS Windows.

- [IETF Standard 13 (RFC 1034) Domain Concepts and Facilities](#) is an introduction to the Domain Name System.

- [IETF Standard 11 (RFC 822) Standard for the Format of Internet Text Messages](#) specifies the format of mail messages and has some requirements for the format of domain names.

- [DNS and BIND, 2nd Edition](#), Paul Albitz & Cricket Liu, O’Reilly and Associates – This is a good reference on what DNS is all about.

News

Virginia Tech’s news server [news.vt.edu](http://news.vt.edu) carries many news groups that can be helpful to system administrators. Some of the groups are local (vatech.*) and some are world-wide. It is probably worthwhile for a system manager to read at least the local newsgroups that are relevant.

Mailing lists

Mailing lists are another good source of information. Much like news groups, there are both local and international lists that cover useful topics. A local list that is probably worth subscribing to is TECHSUPPORT, which is the “support for support” list. You can subscribe by sending mail to listserv@listserv.vt.edu with the text subscribe techsupport Your Name.