91/03/05

Computing and Network Services
Guidelines for IP Networking at CU-Boulder

These guidelines have been developed in response to an observed need for clear statements of how systems should be configured when connected to the Campus network. These guidelines have been developed from a variety of sources including the Internet Engineering Task Force (IETF), the National Science Foundation (the owners of the NSFNET, by which we connect to the rest of the Internet), the Westnet Steering Committee, and large body of collective local wisdom derived from experience with a number of Campus and wide-area networks.

You, as a user and a system administrator, are required to:

- Work within these guidelines.

- Stay aware of changes and developments to the network and to these guidelines by monitoring the "cu-ip-guide" mailing list and the "netstat" mailing list / news group.

91/03/05

Computing and Network Services
Guidelines for IP Networking at CU-Boulder

Executive Summary -

Host Name/Address	**- If you talk IP on the net, you must have both**
Broadcast Address	**- 128.138.0.0 on backbone**
Directed Broadcasts	**- Turn them OFF!!!!!**
Subnet Mask	**- 255.255.255.0**
Default Gateway	**- 128.138.238.36 for backbone systems**
Routing Protocol	**- RIP** **- Do NOT run "routed"**
Trailers	**- Turn them off**
Name Servers	**- 128.138.238.34 ccnucb** **- 128.138.238.154 cujo** **- 128.138.238.18 boulder**
Rwho Daemon	**- Don’t run it on backbone**
File Serving	**- Limited cross mounting OK** **- No diskless serving on backbone**
Mail	**- Use fully qualified host names** **- Use a good configuration file** **- Always have a "postmaster" alias**
Loopback Interface	**- 127.0.0.1**
Terminal Servers	**- No unrestricted dial-up access**
Miscellaneous Services	**- Don’t run tftp, bootp, timed, or daytime**
X-Terminals	**- The jury is still out**

Host Name/Address -

If your system uses the Internet Protocol on the campus network, you must have an approved host name and IP address. If you are on the campus backbone, send your application for a name and address to hostmaster@spot. Host addresses must be unique, in fact you must have a different IP address for every interface. Host names must be unique within the colorado.edu domain, including the DECnet nodes in area 33.

Broadcast Address -

The currently acceptable broadcast address on the campus backbone is 128.138.0.0.

Although this is an older style of broadcast address, it is required because there are a number of hosts on the network that run the older flavor of Berkeley Unix and cannot handle the newer form of broadcast address. In addition, we have more than one subnet on the campus backbone, and any broadcast address which includes the subnet number will cause problems.

The broadcast address 255.255.255.255 should really be the best and safest choice for a broadcast address and is the first choice in the Host Requirements RFC (RFC 1122). However, most Unix systems derived from Berkeley cannot generate packets with this address. In addition, there are a few 3B2 systems that respond badly to that IP address.

Nemeth, Snyder, and Seebass discuss this matter in "The UNIX System Administration Handbook." Please do not be persuaded by the book to use something other than the addresses given above.

Specifically, DO NOT USE any of the following:

0.0.0.0	(very old style)
128.138.238.255	(causes SEVERE storms)
128.138.238.0	(causes minor storms)
128.138.255.255	(causes medium storms)

On most Unix systems, the broadcast address is set as an argument on the "ifconfig" command at boot time. This usually occurs in one of the /etc/rc* files. Most systems do not provide an acceptable default value for the broadcast address, so make sure that you set it.

Directed Broadcasts -

Some systems allow the possibility of doing "directed broadcasts". No system on the campus backbone should rebroadcast these packets. The forwarding of "directed broadcast" packets (IP addresses of 128.138.238.255) is the mechanism for the most severe broadcast storms on the backbone.

When configuring your SunOS 4.1 system, turn off "directed broadcasts" by setting the kernel configuration parameter IP_DIRBROADCAST=0.

Subnet Mask -

The proper subnet mask for the Boulder campus is 255.255.255.0.

A few of hosts on the network still cannot deal with subnets and therefore have a subnet mask of 255.255.0.0. This discrepancy will generally cause problems when you try to send packets from those hosts to a host on some other subnet.

The problem is that the unsubnetted host expects that all other hosts whose addresses begin 128.138 are on the same, big Ethernet, and that host will issue an ARP (Address Resolution Protocol) request to find the Ethernet address for the desired IP address. One solution is for the gateway to the subnet to respond to ARP requests for hosts on subnets behind the gateway (called "proxy" ARP), but only cisco routers and some modified Unix systems, such as boulder and cujo, will do this. Until recently, we provided a limited "promiscuous" ARP facility on ccnucb which answered ARP requests for hosts on other subnets, but we stopped doing this because we needed ccnucb for other purposes and with the proper subnet mask, this was no longer necessary.

A number of hosts are unable to broadcast a packet using the broadcast address of 128.138.0.0 and a subnet mask of 255.255.255.0. This is because the host compares the third byte of the destination address with its own address, determines that the packet is destined for subnet zero rather than 238, and forwards the packet on to the default gateway. Where, presuming it was an rwho packet, it gets dropped.

This is also called the "netmask" or "network mask" on some flavors of Unix. Like the broadcast address, the subnet mask is normally set as an argument on the "ifconfig" command at boot time. The usual default is to do no subnetting (255.255.0.0), so you will need to make sure that you have set it to 255.255.255.0 (ffffff00 in hex).

Since we use eight bits for the subnet, this allows us to have 254 subnets (can’t use 0 or 255). This leaves room for 254 hosts on each subnet (can’t use 0 or 255 here either). At this time we have assigned over one-fifth of the available subnets. In the future, it will probably be necessary to use eight or nine bits for the subnet (allowing 510 or 1022 subnets), but this would reduce the number of bits available for representing host numbers on each subnet to seven or six 6 (allowing 126 or 62 hosts per subnet). In general, a limit of even 62 hosts per subnet would not appear to be a problem although there are currently four subnets with more than 62 hosts on them.

Another future alternative will probably involve variable subnet sizes. This cannot be implemented currently due to software restrictions on most Unix systems and limitations due to the RIP protocol.

Default Gateway -

If you are setting up a host (or gateway) on the campus backbone, your best choice for a default gateway is the cisco router which connects us to the Internet. Its current address is 128.138.238.36. Its name is cu-westnet-gw.

To set a default gateway on a host on the campus backbone, you will probably need to put a command such as

```
route add default 128.138.238.36  2
```

in the appropriate /etc/rc* file so that it will add the route at boot time.

If you are setting up a subnet behind a single gateway, use the address of the gateway’s interface on your subnet as the address for the default gateway for all the hosts on the subnet.

Routing Protocol -

The routing protocol used on the Boulder campus backbone is called RIP, the Routing Information Protocol. It is a rather simple protocol, using a hop count as its only metric.

Most Unix systems provide a routing daemon called "routed," which speaks RIP. Probably the worst failing of "routed" is that it re-advertises routing information (albeit with the hop count incremented by one) out an interface, even though that interface was the only source by which "routed" heard about that routing information. This means that when the "real" source of routing information about a network stops sending out information about that net, "routed" will tell everyone that IT does know a route, even though it really doesn't.

Do not run "routed" on any host connected to the campus backbone unless you are running it in the "quiet" mode (the -q flag). This will mean that if you are running a gateway, it will not advertise anything, not even that it knows the way to your subnet.

If you want to do advertisements of your subnet, you must run something better than "routed". There is a program called "gated" which does implement RIP properly. "gated" also implements several other protocols (which you probably don't really care about), and it has a lot of features for controlling the information advertised by your host and the information believed from other sources. You can also set a default gateway in the "gated" configuration file. The source code for "gated" is available.

If you have a gateway on which you cannot run "gated", an alternative is for us to put a static route to your subnet on the default gateway. This means that any host on the campus backbone which tries to get to your subnet will send the packet to the default gateway. The default gateway, if it is a cisco, will forward the packet on to the gateway to your subnet, based upon a static routing table entry, and will send a "host redirect" packet back to the originating host, telling it to send all future packets for that host via the gateway to your subnet. Not all hosts respond to "host redirect" messages, but any good IP implementation will.

Cisco routers do RIP properly, as do other routers. Perhaps you should consider installing a real router in front of your subnet, thereby freeing up the CPU cycles of your own machine for things other than passing packets and managing routing tables.

Trailers -

The cisco gateways do not understand the concept of "trailers". It is safest to turn them off for your host.

Like the broadcast address, the choice of trailers or not is normally set as an argument on the "ifconfig" command at boot time. Most Berkeley systems turn trailers on by default. If you find that you can telnet to some off-campus host, but that you cannot do a file transfer, send mail, or even scroll through a couple screens full of output, then you should check to be sure that trailers are off.

Name Serving -

So far in this guide we have expressed all the IP addresses as four eight-bit numbers. There are several mechanisms for translating between symbolic names and IP addresses.

The oldest, and least desirable mechanism is a "host table". Most Unix systems provide this capability. The table usually resides in the file /etc/hosts. The use of this mechanism is discouraged because it does not scale to the current internet environment. On systems with NIS (Sun's Network Information Service), this table is hashed and propagated to the clients.

The newer, and preferred mechanism is the Domain Name System (DNS). The most common implementation of this is the Berkeley Internet Name Daemon (BIND) which is provided by the program "named". The DNS is a distributed name service with the information for each domain (e.g., Colorado.EDU) managed by someone within that domain, rather than by a central organization.

The primary name server for Colorado.EDU is "boulder". Secondary name servers for this domain are ccnucb, cujo, and nnsc.nsf.net.

rwho Daemon -

We encourage you not to run the rwho daemon, or at least to run it in "listen-only" mode.

The rwho daemon broadcasts packets with information about how long your machine has been up, what the load average is, and who is currently logged on. This information is not all that useful, and the rwho packets add to the general clutter of broadcast traffic on the Ethernet. Every system on the backbone must process every broadcast packet that it sees on the Ethernet, even if it has no use for the information in that packet.

If you do run the rhwo daemon, please try to have the host name without the .Colorado.EDU domain name tacked on. Every host on the campus backbone is in that domain, and the .Colorado.EDU qualification just adds to the visual clutter in the ruptime listing. If you cannot eliminate the domain name from your rwho broadcast, please do not do rwho broadcasts.

File Serving -

Cross-mounting and dumping NSF partitions across the campus backbone are currently acceptable, but only in low use circumstances. Swapping, paging, or operating system access across the campus backbone is prohibited. It is not acceptable to run diskless clients or their servers across the campus backbone, just as it is not acceptable to run a Local Area VAX Cluster on or across the campus backbone.

Mail -

Your system probably has a "sendmail" service. Attempting to run this without first establishing a suitable sendmail configuration file (usually /usr/lib/sendmail.cf or /etc/sendmail.cf) can be damaging to the network service and other hosts. There are different sendmail.cf files for different philosophies about mail, and you may wish to elect one way or another. In any event, mail between hosts on the network must use fully-qualified host names in sender and recipient addresses. This usually means that the sendmail.cf file must at least be changed to define the domain as "colorado.edu".

If you subscribe to UnixOps service, they will provide a suitable sendmail.cf file for your system.

Loopback Interface -

Most Unix systems require a "loopback" interface in order for all the networking software to work properly. Some system define this for you automatically, but some do not. Do not operate your system without a properly configured loopback interface.

You usually see if a loopback interface has been defined by using the

netstat -i -n

command to see all the interfaces. One, usually named "lo0" should be there with the address of 127.0.0.1 and a network number of 127.0.0.0. You should be able to use the command:

/etc/ifconfig lo0 127.0.0.1 up

to configure a loopback interface.

Terminal Servers -

Currently there are no restrictions on running terminal servers on or across the campus backbone. We do not, however, permit unrestricted terminal access off campus via the internet. For example, if you have a terminal server with dial-up ports, you must prevent those ports from accessing off-campus hosts directly. In order to get off campus, every user must be validated in some manner. You might think about extending this to the campus network also.

X-terminals -

At this time, it is not clear if the load imposed on an Ethernet by reasonable X-terminal activity is something that can be handled easily by the campus backbone. We are looking for data.

Miscellaneous Services -

Unix provides a number of services across the network. Many of them are enabled by default, but several of these should be disabled. In particular, unless you have a specific reason to the contrary, please do not provide tftp, bootp, time, or daytime services.

The tftp service usually represents a security problem for your host, and it is in your best interest to disable that feature. In addition, some devices on the backbone use this service, and it wastes their resources to handle gratuitous responses from your system.

The bootp service is not so much a security problem for you, but several devices on the backbone use this service, and it a waste of resources for you to be processing those messages (and even responding to them) without having the information to provide a useful response.

The time and daytime services expect that you have an accurate clock on your system. If you do not have a clock synchronized to WWV and are not running the Network Time Protocol, then you will only be contributing to the network noise by providing these services. Of the 58 systems responding to a recent test, only 13 were within two seconds of the correct time, and 14 were over 10 minutes off, with five being at least six hours off.

These services are frequently provided through the "inet daemon". On many Unix systems, these services can be disabled by editing the /etc/inetd.conf file (or some similarly named file). Put a # in colunm one of any lines related to these services.

Exceptions -

We can probably make temporary exceptions to some of these network guidelines, but we do require that you discuss them with us and obtain our approval before deviating from these guidelines.

Contact hostmaster@spot before violating any of these guidelines. In particular, we will want to mitigate any negative consequences for the network as a whole.

References -

There are a number of interesting and useful documents stored in the "pub" directory accessable on spot via anonymous ftp. For example "tcp-ip-intro.doc" gives a nice introduction to the internet protocols.

There is a collection of documents called "Request for Comments". Many of these are in the "pub/rfc" directory. Some of the relevant RFC's are:

- 1178 Choosing a name for your computer
- 1177 FYI on Questions and Answers: Answers to commonly asked "new internet user" questions
- 1175 FYI on where to start: A bibliography of internetworking information
- 1173 Responsibilities of host and network managers: A summary of the "oral tradition" of the Internet
- 1122 Requirements for Internet hosts - communication layers
- 1118 Hitchhikers guide to the Internet

For assistance, call -

Please consider contracting with UnixOps for assistance with installation. They are also eager to provide a variety of other contract services related to managing Unix systems.

Here is a list of some relevant phone numbers. All have prefix 492.

- 6096 UnixOps
- 1615 CNS advisors
- 3887 Jon Giltner
- 4409 Doug Kerry
- 3872 Jeff Scarborough
- 4905 David Wood

Updates to this Document -

These guidelines are not cast in concrete. As the environment changes, and as we continue to learn more about networking, we will undoubtedly make changes to these guidelines.

If you want to be added to an electronic mailing list to receive updates to this guide, please send a mail message to cu-ip-guide-request@spot.Colorado.EDU.

This document is available on-line via anonymous ftp on spot as the file "cu-ip-guide.txt" and "cu-ip-guide.ps" in the "pub" directory.