Routers on UTnet

The Network Information Center
of the University of Texas at Austin (UT NIC)

September 1990

Document version 3.1

Introduction

The first section of this document describes UTnet routers and explains why routers are being installed on the UTnet campus network system. The first section is written for those who want to know the basics of what a router is and the effect that router installations will have on campus network operations and on the attached host computers.

The second section describes the effect that router installations have on the campus network. If you do not need to know about the innermost workings of the campus network system, you are strongly encouraged to stick to the first section and forego the gory details.

Host adminstrators and network administrators who brave section two will also benefit from reading about the effect of subnet routers on host network configuration. Host configuration for networks with routers is described in the document *UTnet Guide to TCP/IP Host Configuration.* This guide should be consulted for details on the effect of routers on host operations.

Section 1 — Router Installations on UTnet

1. What is a Router?

A router is a device that establishes a connection between a building network and the campus backbone network system. Routers are a form of network packet switch. You will sometimes see them referred to as subnet routers, or as gateways.

When the UTnet broadband system was first installed, DEC LAN Bridge 100s were used as the packet switch located at the building entrance, which is the point at which the campus backbone network attaches to the building network. Some of the LAN bridges are now being replaced with routers.

1.1. Why are Routers Being Installed?

Routers are being installed on UTnet to improve its operation. Routers improve network operations in several ways, including:

- Increased isolation from general network traffic and from problem traffic on the backbone system. Better isolation helps keep the network system operational by limiting the number of computers that can be affected by network traffic or by incorrect packets encountered on the backbone network.
- The ability to add new network technology to the backbone system without disturbing the building networks. The newer and faster network technologies to be used in the future are different from the Ethernet technology currently used as the backbone transport mechanism. Routers make it possible to attach the building Ethernets to non-Ethernet backbone networks without affecting the building networks.
- Limiting the number of broadcast packets present on the backbone. The host population of UTnet has been growing rapidly, and as the host population grows, so does the level of broadcast packets on the backbone. By intercepting broadcast packets and limiting their propagation, routers make it possible to continue adding hosts to the UTnet network system without overloading the hosts due to ever-increasing rates of broadcast packets.

1.2. The Effects of Installing a Router

Until now, all departmental/building networks were attached to the UTnet backbone system with LAN Bridge 100 packet switches. These Ethernet bridges provide isolation from physical network problems, and also provide a level of network traffic isolation. However, the Ethernet bridges do not provide any isolation from broadcast packets.

Another feature of the Ethernet bridge is that it has no affect on the actual routing mechanisms of the various network protocols traveling over the UTnet. Instead, the bridge operates at the Ethernet level of network operations, and simply forwards packets based on their Ethernet addresses.

The installation of routers operating at the routing level of network operations has an affect upon the network protocols which also function at that layer. Section 2 of this document describes the impact made by the installation of a router in much more detail.

1.3. What Happens When a Router is First Installed

When a router is first installed, there is a one-time possibility that some hosts may experience a disruption of network communications. However, this disruption will only last a short time. It is caused by the fact that certain tables that are automatically created and maintained by hosts running the TCP/IP protocols will be temporarily incorrect.

In most cases these tables, known as ARP tables, will automatically clear themselves within a few minutes. After that, network communications will proceed normally, without further disruptions. It is important to note that any disruption that occurs will only happen once — at the moment that a router is first installed.

Some hosts do not clear their ARP tables automatically, and if these hosts are having problems after a router installation they will have to be rebooted. Rebooting a host will clear the ARP table, since the table is automatically maintained in host memory by the network software on the host. Once the host is rebooted, it will automatically build correct ARP table entries, and communications will proceed normally.

It takes anywhere from five minutes to up to an hour for any incorrect ARP table entries to correct themselves. As noted above, some hosts may have to be rebooted if they continue to have problems communicating.

After the one-time disruption that can occur when a router is installed, there is nothing else that requires any change on the host computers. Network operations will be as rapid as before.

Section 2 — Router Operations in Detail

Router operations are explained in greater detail in this section. In order to understand this section you should be familiar with the concepts of IP subnets, and IP routing, including the Ethernet Address Resolution Protocol (ARP). These items are also discussed in the document *UTnet Guide to IP Addresses and Routing.*

A list of books and other documents that also describe these matters may be found in the *Network Manager's Reading List: TCP/IP, UNIX, and Ethernet.* Further information about the documents cited may be found here, in the section ‘‘Access to Further Information.’’

This section contains a quick description of several complex and interactive elements of network routing, including IP subnets and the ARP protocol. The whole subject of router operation and the effect of routers on the evolving campus and external network systems is large, and that which is described here is only a small part of the entire picture. In fact, this section should probably be headed with the (in)famous comment found in some early Unix source code: ‘‘You are not expected to understand this.’’

If you find that you do not understand the tangle of network routing entities described here, do not be perturbed. The most important item described in this section has to do with the physical location of hosts, once a router is installed. As for the rest, all that one really needs to know has already been described in Section 1, or may be found in the *UTnet Guide to TCP/IP Host Configuration.*

2. Routers and Subnets

Campus routers are installed to control the flow of packets on the campus network system, and to enforce the subnet architecture in use on campus. Subnets, in turn, divide the campus IP address space up into locally administered subnetworks. Typically a department is given one (or more) subnet addresses for its hosts, and these subnet addresses identify the hosts as belonging to that department and as being assigned to that department's network cable.

2.1. TCP/IP Subnet Assignments

From the point of view of the departmental network, *the* major change that occurs when a router is installed is the enforcement of the subnet architecture on the UTnet system.

When each departmental network was attached to the backbone system with a LAN Bridge, the departmental network was given an IP address that included a unique departmental subnet number. This was actually a pseudo-subnet IP address, as described in the *UTnet Guide to IP Addresses and Routing.* By ‘‘psuedo-subnet,’’ we mean that while bridging was in effect, the subnet address was an administrative aid to identifying the network segment and the hosts attached to that segment.

The subnet address on UTnet may be found by examining the third octet of the four-octet IP address. The first two octets of the address make up the network number for UTnet, which is **128.83.** Thus, a host with the address of 128.83.186.1 is host 1, on subnet number 186, on the UT campus network of 128.83.

Once a router is installed the pseudo-subnets currently in use on a departmental network become true subnets for IP routing purposes. Since the correct subnet numbers for a given department have already been assigned, there is usually no need for host addresses to change once a router is installed.

2.2. Subnet Addresses Are Limited to a Single Network Segment

Although there is no need to change host addresses when routers are installed, it is important to understand that once a router is in place, the pseudo-subnet addresses that were once ignored by LAN bridges now become an essential part of the routing process on the campus network. The routers move TCP/IP packets around the network based on the packet’s IP address, which includes the subnet address.

This has important implications for correct network operation in a department. The most important affect is that **all hosts with the same subnet address must be on the network segment assigned to that subnet address.**

In other words, by attaching a router to a building network segment, we enforce the subnet address of that segment. The router is configured with the subnet addresses of the segments to which it is attached. Once the router is started up, it will determine which segment a packet must be sent to by virtue of the subnet address included in the packet’s destination IP address. This means that packets sent to a given subnet address will arrive on one and only one network segment.

2.2.1. Keep Hosts on the Same Network Segment

Each subnet number on campus is limited to one and only one network segment once a router is installed. This is necessary since the IP address, including the subnet address, is the piece of information the routers use to determine which network segment a packet must be sent to.

Consider the case of a host belonging to department A that is using an IP address with department A’s subnet address. If, for some reason, that host is moved to department B's building and is on a network segment that supports department B (and therefore uses department B's subnet address), then that host will no longer be able to communicate once a router is installed. In other words, the host in this example will have functioned as long as LAN bridges were in place, but as soon as a network router is installed and the subnet addresses begin being used for network operations, the incorrectly addressed host will stop working.

In the vast majority of cases this will not be a problem, since most departments have kept their hosts on the correct network segment. But if a host with department A's address has been loaned to department B for some reason, and department B's network is in another building or on a different network segment, then there will be a problem. The problem is easily resolved by giving the host a new IP address that correctly reflects the subnet address of the network segment to which the host is attached.

2.2.2. Multiple Departments Can Still Share a Single Ethernet

A given building network segment can still support multiple departmental subnet addresses without any problems. A given building Ethernet cable/network segment may support several departments, each having a different subnet number. This is currently the case in several buildings at UT Austin, and this configuration will continue to work after routers are installed.

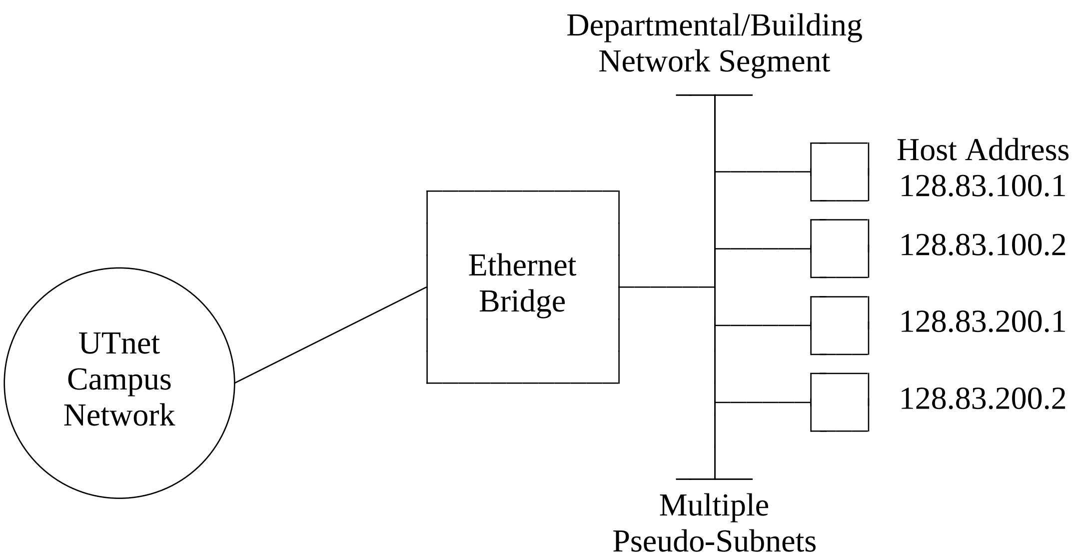

Figure 1. Ethernet Bridge and Pseudo-Subnets

In Figure 1, we show a single building network supporting hosts addressed on two different subnets. The network is attached to the campus system with an Ethernet bridge.

This figure shows a typical installation on campus as of this writing. The Ethernet bridge does not use the subnet addresses of the hosts for routing purposes, which is why we call them pseudo-subnets when a bridge is in use.

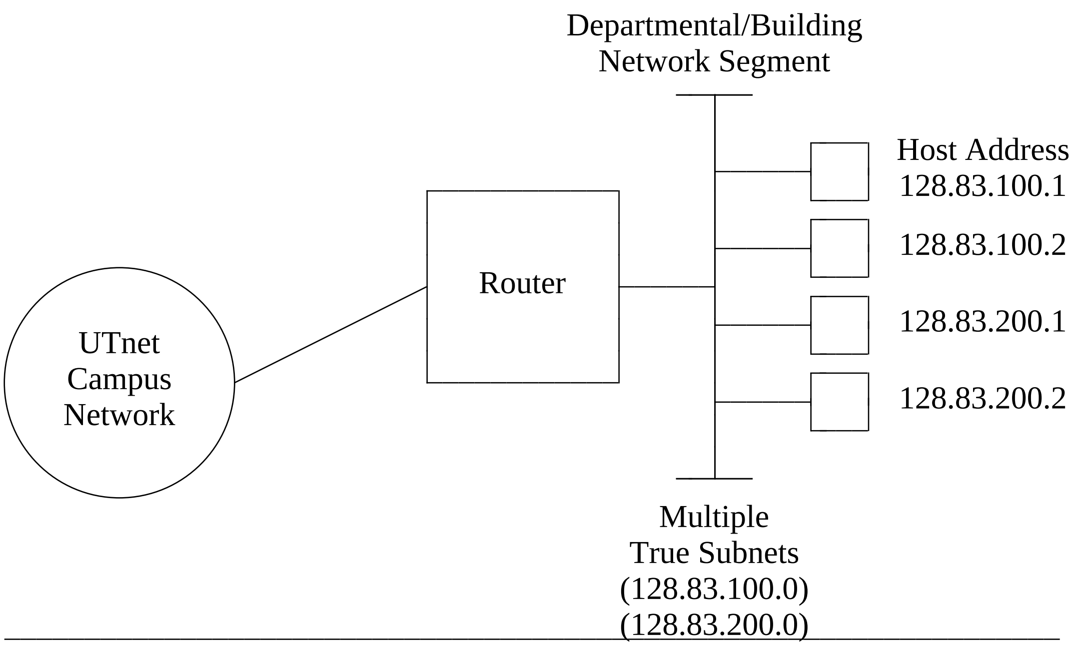

Figure 2. Router and True Subnets

Figure 2 shows a router installed in place of the bridge.

The fact that we can simply plug in a router and the hosts are suddenly functioning with true subnets demonstrates the advantage of having assigned the pseudo-subnets when bridging was in use. The bridges didn't need the pseudo-subnet addresses in order to operate, but since the evolution to routers had been anticipated, pseudo-subnet addresses were assigned. Once a router is installed, they become real subnets for the purposes of routing, and no change need be made in the host addresses for this to take effect.

2.2.3. Routers and Multiple Building Segments

Another advantage of routers is that they allow the building network to be separated into separate network segments, each given a single subnet address. This allows the departments to isolate clusters of hosts from one another, so that as the host population within a building grows, the network traffic can be split among several network segments. This causes a drop in network traffic on each segment, with a corresponding improvement in network reliability and manageability.

This evolution requires routers with multiple network interfaces. Most of the routers now being installed on campus do not currently support multiple interfaces. Nonetheless, once host populations within buildings become large enough, routers with multiple interfaces can be purchased and installed as shown in Figure 3.

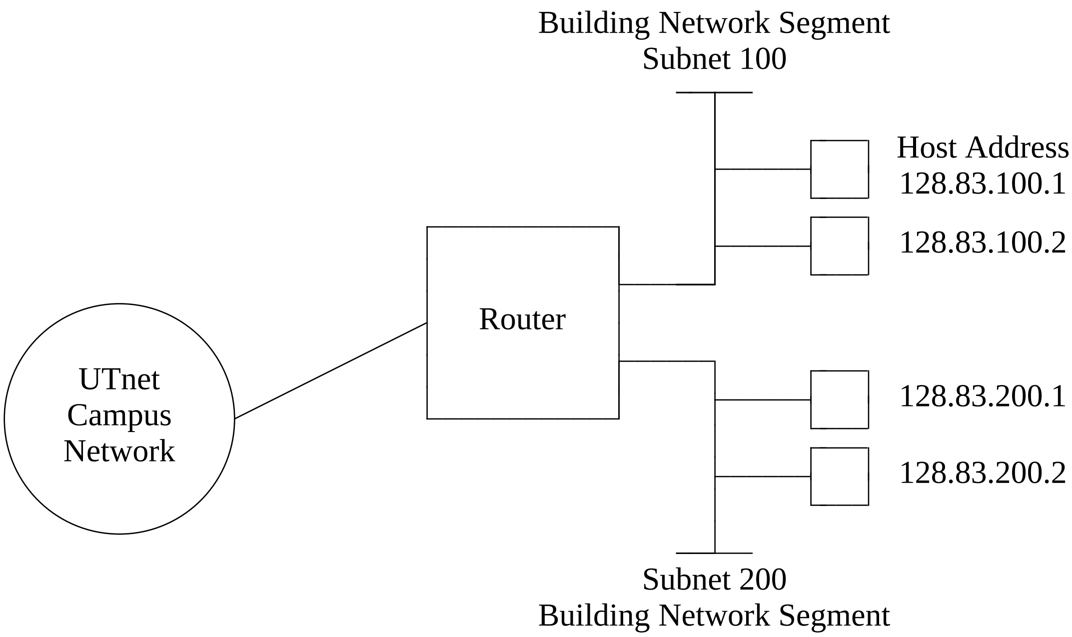

Figure 3. Router and Multiple Network Segments

2.3. Routed Protocols and Non-Routed Protocols

The UTnet routers are configured to route TCP/IP protocols and DECnet protocols. That means that all network services based on these protocols will work as before. The UTnet router is also configured to support DEC Local Area Terminal (LAT) services, so that any terminals using DEC's LAT protocols will continue to function as before.

Any other protocols that are currently being used on the departmental/building network will continue to work *within* the building, but these packets will not be passed onto the backbone by the router.

2.4. Router Installations and Host ARP Tables

Upon installation of a router, nothing need be changed in the host systems attached to the network. After a router is installed, the host configurations can stay the same, or they can be changed slightly to exploit the capabilities of the router. There are several changes that *should not* be made to hosts on network segments that support multiple subnets. These changes are described in the *UTnet Guide to TCP/IP Host Configuration.*

When a router is first installed, there may be some temporary problems with host communications. These problems are caused by incorrect ARP table entries.

2.4.1. ARP Table Entries Will Be Temporarily Incorrect

Every TCP/IP-based host computer keeps an ARP table of address mappings between Ethernet addresses and IP addresses. Once a router is installed some of the ARP table entries in the departmental hosts will be incorrect. ARP tables in hosts on the rest of the campus network system that have been communicating with the hosts on the newly routed network will be incorrect as well. This is due to the fact that the router is now answering ARP requests for TCP/IP communications.

Every time a departmental host wishes to communicate with another host via TCP/IP protocols, it will make an ARP (Address Resolution Protocol) request to initiate communications. The results of the ARP request are automatically cached in an ARP table that is maintained by the TCP/IP software in each host involved in TCP/IP communications. The operation of ARP and IP addresses in general is described in more detail in the document *UTnet Guide to Internet Protocol Addresses and Routing.*

ARP table entries are made automatically, and the table is maintained in the host's memory. ARP tables disappear when a host is shut off or rebooted and are recreated dynamically by the host's routing software. Some systems allow you to examine an ARP table, and on some systems you can do some limited manipulation of the table entries; but in general the creation and maintenance of the ARP table is completely automatic.

Once the router is installed, ARP table entries for hosts that are not attached to the department's network will have to change for communications to proceed. To allow ARP tables to change, most implementations age out the entries. ARP tables entries can age out in 5 minutes, 20 minutes, an hour, or never, depending on the implementation.

Most ARP table entries can be expected to have aged out in an hour. Once that happens, then the host can resume communications without any future problems. But if there are persistent problems communicating with a given host on campus after the subnet router is installed, that host may need to be rebooted to refresh the ARP cache. The problem with incorrect ARP table entries only happens once, when a router is first installed. Once the incorrect ARP table entries are purged, the problem will not recur.

2.4.2. Routers and Proxy ARP

The incorrect ARP entries are due to the fact that the router is now involved in mediating network communications for TCP/IP-based hosts. After a router installation, network routing will function for departmental hosts by way of what's known as the ‘‘proxy ARP’’ mechanism.

Proxy ARP is a method by which routers answer ARPs in proxy for the actual device whose address is in the ARP request. Any host on UTnet that wishes to reach hosts on the newly routed departmental subnets need only ARP for them as usual, and the router will answer the ARP in proxy for the hosts on the departmental subnets to which it is attached. This also works in the opposite direction for hosts on the departmental networks that send out an ARP for hosts located on the UTnet system on the ‘‘campus side’’ of the newly installed router.

In other words, once the old ARP table entries that were active at the time of the router installation have aged out, the ARP mechanism will work just as it did before with no need for any special setup on the hosts. However, unlike the LAN Bridge, the router now plays an active part in establishing low-level communications between hosts separated by the router. This active role in answering ARP broadcasts explains how the router is able to block the flow of Ethernet broadcasts (such as ARP packets) from the backbone to the departmental network and vice versa, yet still allow networking to proceed automatically.

Blocking Ethernet broadcasts eliminates the broadcast storms and harmful host interactions that can occur through the broadcast mechanism. Isolating the departmental network from traffic overloads due to broadcast storms and from misconfigured hosts sending incorrect packets to the broadcast address is the major job of a network router. This is why a router is also called a ‘‘firewall’’ in network jargon.

After a router is installed, the ARP activity is automatic. Since the router operates as fast as the LAN Bridge, the user will not notice any change in the response time of the network. Also, just like the LAN Bridge, the router has no effect on communications between hosts located within the same department and attached to the same network cable.

2.5. Access to Further Information

The UTnet documents cited above are available via anonymous FTP from host **emx.utexas.edu,** in the **pub/netinfo/utnet** directory. The filenames of the documents cited are:

1. **The UTnet Guide to TCP/IP Host Configuration.**

   Available as tcpip-config.txt, an ASCII file and as tcpip-config.ps, a PostScript file suitable for printing on an Apple LaserWriter or equivalent.

2. **UTnet Guide to Internet Protocol (IP) Addresses and Routing.**

   Available as ipaddrs.txt, an ASCII text file and as ipaddrs.ps, a PostScript file suitable for printing on an Apple LaserWriter or equivalent. The text file version is missing several figures that are found in the PostScript version.

The next document is found in the **pub/netinfo/docs** directory.

3. **Network Manager’s Reading List: TCP/IP, UNIX, and Ethernet**

   Available as network-reading-list.txt, an ASCII text file, and as network-reading-list.ps, a PostScript file suitable for printing on an Apple LaserWriter or equivalent.