UTnet Guide to Subnet Policy

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

Document version 2.0

1. Introduction

This guide describes UTnet policy for departmental subnets and their connection to the UTnet backbone network system. The packet switches required for access to the backbone network system are also described.

2. Subnet Policy

The University of Texas at Austin campus internet (UTnet) is managed by the Computation Center. The primary goal of UTnet management is to provide reliable network services and equal access to all users of the network system. To that end, the Computation Center has formulated policies for subnet access to the UTnet backbone.

The word ‘‘subnet’’ refers to both the intra-building physical network connected to the backbone network system, and the individual TCP/IP subnet number assigned to a given department. To be more precise, the physical network segment is a sub-network of the backbone system. The subnet address of this physical sub-network is the IP number assigned to a given sub-network. When new hosts are attached to a physical sub-network of the UTnet system, host addresses are assigned so as to include the IP subnet number of the department utilizing that particular physical network segment. This makes it possible for network managers to locate a problem physical network through analysis of packet traces containing logical IP subnet addresses.

A given intra-building physical network may support hosts belonging to multiple departments, and therefore will have host addresses with multiple IP subnet numbers attached to it. These multiple subnet addresses may be used as pseudo subnets, or they may be used as true subnets by the hosts for routing purposes, depending on whether or not a subnet gateway is in place between the intra-building network and the backbone system. The difference between such subnets is explained in further detail in the **UTnet Guide To TCP/IP Host Configuration.**

If the number of hosts on a given intra-building network supporting multiple departments becomes too large, a subnet gateway can be used to form separate physical segments, typically one per department. These segments would then support only hosts from a given department with a given IP subnet address. At that point there would be a one-to-one correlation between the IP subnet address and the physical sub-network wire in use by the hosts with that subnet address.

Subnet addresses are assigned on a per-physical-network-segment basis only. In other words, a large department spread across several buildings may not use one subnet address for every network segment the department employs. Subnet addresses are important for network troubleshooting purposes, and must be bounded by a given physical segment to maintain their utility in troubleshooting network problems.

2.1. Point of Presence

Providing reliable network services to the entire campus requires that a packet switch be located at the boundary point between the backbone network system and the intra-building network(s). This point is called the UTnet point of presence (POP). The packet switch provides for:

- Isolation of the campus backbone from damaged packets, collision, jabber (overlong) packets, and other intra-network media failures.
- Isolation of the campus backbone from failures due to high level protocol problems originating in the intra-network system. Failures may be caused by broadcast storms, or any high rate of packets sent due to misconfigured or failing software. Failures requiring isolation may also be due to misbehaving applications that affect network services elsewhere on the UTnet system.

A packet switch automatically provides isolation from low level physical media failures. Higher level protocol interactions that are causing problems require that the Computation Center staff take action to determine the failure mode, locate the source of the packets causing the failure, and isolate the source if the operator of the machine cannot be located.

Currently there are two packet switches authorized for use on UTnet. They are the DEC LAN Bridge 100 (LB100) product, and the cisco Systems Gateway Server (gateway) product. Both packet switches perform the point of presence function, and both switches are operated by the Computation Center.

3. Operations Policy

The Computation Center has the following policy with regard to the operation of the packet switches in use on UTnet.

3.1. LAN Bridge 100

The LB100 packet switch is operated by the Computation Center staff. The software and configuration of the LB100 is entirely under the control of Computation Center staff. Upgrades to LB100 software and address filters in LB100s on campus can only be accomplished by Computation Center staff. In the special case of network debugging the Computation Center staff may elect to allow local network administrators to modify LB100 bridge address filters as necessary.

In the event of network service disruption the Computation Center will attempt to find the designated subnet manager for the subnet in question. It is the responsibility of the subnet manager to keep the Computation Center advised of current contact information. If no contact can be made in a reasonable time, or if the problem persists in disrupting network service, the Computation Center reserves the right to interrupt backbone access until the problem can be resolved. This is done to preserve backbone services for all other users on campus.

3.2. cisco Systems Gateway Server

Once a subnet system achieves a given level of packet traffic and/or host population, it is advantageous to divide the intra-building network into multiple ‘‘true’’ subnets. This is done with a subnet gateway. Subnet gateways are considerably more complex to install and operate than a LAN Bridge 100 packet switch. On the other hand, they provide superior isolation from broadcast packets, and allow multiple media attachments and more sophisticated network load management.

The gateway is operated by the Computation Center (CC) staff.

(1) The CC staff provides the latest gateway software and manages the boot file for the gateway’s operation.

(2) The configuration files and password protection are provided.

(3) The gateway is included as part of the internal system (IS) routing system in use on campus.

In event of network service disruption, the CC staff will proceed as described above for the LAN Bridge 100 packet switch. If multiple physical subnets are provided inside the building, the subnet gateway may make it possible to shut off service to the failing subnet alone, without disrupting the rest of the networks in the building.

3.3. Private Gateways

In the event that a department or other entity wishes to operate their own gateway, the Computation Center policy is as follows.

(1) The Computation Center must retain a packet switch point of presence that is entirely under the control of the Center. This requirement is made to preserve backbone services no matter what may happen to the private gateway. At a minimum, there will be a LAN Bridge 100 between the backbone system and the private gateway.

(2) The private gateway must be able to meet the routing requirements of the UTnet system. CC staff will advise any group wishing to attach a private gateway of the requirements.

(3) The CC staff will not manage gateway software, configuration files or passwords for the private gateway.

(4) CC staff will establish UTnet and wide area routing mechanisms for the private gateway, but will not being responsible for the operation of same. The private gateway will be dealt with as a separate network entity, and a routing path will be initially established by CC staff.

(5) It is expected that debugging routing problems, configuration problems, or any other operational difficulty with the private gateway will be the responsibility of the entity that owns and operates the gateway. The proper operation of the network system will be maintained up to the LB 100 by the Computation Center. CC staff will be available to troubleshoot private gateway problems only as time permits.

(6) Access to the private gateway via SNMP mechanisms must be provided to allow CC staff to examine routing tables in the gateway. This is required since the routing tables are part of the backbone system network services, and may need to be examined during the analysis of a backbone service disruption.

3.4. Subnet Allocation

Every department that wishes to attach hosts to a given network segment on the UTnet system is assigned an IP subnet address by the UT Network Information Center. The netmask scheme chosen for the UTnet system allows 254 subnets to be assigned before another institution-wide Class B network number must be acquired. Subnet numbers are therefore a limited resource for UTnet, but are not as yet in short supply.

Departments that wish to have more subnet numbers than they are assigned, whether to accommodate a large number of hosts or for some other reason, need to make special application to the UT NIC. In this application, the department should specify the requirements that make it necessary to acquire extra subnets. This information is collected by the UT NIC to document that subnets are allocated fairly and as required for smooth network operations.