INTRODUCTION

The UF data network is a shared resource that connects users to network services and each other. All users of the network depend on the reliability (constancy of service), quality (acceptable speed and accuracy of performance) and security (protection from unauthorized access to privileges and services, as well as, protection from denial of legitimate access) of the network. When the network is compromised on one of these items, it will frequently affect more than one user and may well affect users at extreme ends of the network. Users of the network implicitly agree to cooperate with other users in an effort to provide reliable, high quality, and secure network operation for all. The network managers are the people who provide the technical expertise to fulfill this agreement. The purpose of this statement is to describe the distributed organization of the data network management and the role of the network managers. The operational details will come at a later time in coordination with the various campus network support organizations.

Overview of Distribution Network Management

The data network is arranged hierarchically. The hierarchy is based on the connectivity. The lowest level consists of the individual users, while the highest level makes connections across the entire campus, leading to the campus Internet connection. Likewise, management of the data network is arranged hierarchically, corresponding to the various subnets of the physical network. In rough analogy, this hierarchy has the appearance of federal, state, county, and city government domains. The “domain” of a manager is simply all machines and devices on the network which are maintained by that manager. Unlike the government analogy, the hierarchy is not based on authority over the operations of the lower domains, it is based on the responsibility of delivering services and connectivity to the lower domains.

Each user has a local area network manager (LAN manager.) This LAN manager is usually in the same department or unit as the user, though in some cases the LAN manager will be at the next higher budgetary unit, for example, at the college level. In some colleges there are network managers who assist the LAN managers in the identification and resolution of problems. Top level management is handled by the UFNet support team with some off loading of network management, notably IBM Token Ring, to the Northeast Regional Data Center.

The responsibilities of the LAN managers are
1. To be personally knowledgeable of the local area network and its operation and to maintain the documents which describe the network. The network documentation includes description of equipment within the domain, services, locations, and other network identifiers. These documents are operationally specific to the support organizations.

2. To be the first point of contact with the users of the local area network. The users should know their LAN manager and the services supported by the LAN manager. The LAN manager needs to know the users and their support needs.

3. To be the first point of contact with the next manager up in the managerial hierarchy.

Each domain will have a proxy who will perform functions 2 and 3 when the LAN manager is unavailable. More generally, the responsibilities of any network manager are the same as those of a LAN manager suitably applied to their domain. A network manager is sanctioned by the unit which employs her/him. Ultimate responsibility for evaluation of the performance of a network managers rests with that unit. A network manager and his/her supervisor understand the cooperative nature of network management and agree to participate as part of a campus-wide management team.

Maintenance

Reliability depends on a regular schedule of hardware and software maintenance and upgrades. Routine maintenance is done in commonly acknowledged periodic windows. Major maintenance may be performed outside of these windows with adequate warning to the affected network managers and users. Maintenance is to be performed in a way which minimizes the impact on the network both in terms of down time and performance.

Troubleshooting

Serious problems that affect network performance require identification and resolution. Network managers in the affected domains will assume ownership of the problem and they will work cooperatively as a team. Their common goal is to isolate the source of the problem and repair it as quickly as possible. Occasionally, perceived network performance problems involve physical limitations of the network and the resolution will not be as timely as the complainant would like. In as much as a problem may affect disparate segments of the network, it may be necessary to disconnect the source of the problem in an effort to protect other users. Network managers are empowered to do this. Always disconnection is to be viewed as an extreme measure, to be made as close to the problem source as possible and after communication with the affected users and managers (if possible.)

Security

The definition of "authorized access" to computers, networks, and services at the University of Florida is itself a large issue. The granting of access to University computing privileges is generally made by the owner of the privilege. Resulting abuse
or unintended access to the privilege is often erroneously regarded as a local problem. This simple view is dramatically complicated when access in one part of the network is used to compromise security in another part of the network. As in the case of troubleshooting, network managers along with computing system administrators work as a team in the identification and removal of security problems. In some cases disabling the privilege may not be feasible and physically disconnecting the machine or subnet from the network may be necessary. As in the case of troubleshooting procedures this is to be viewed as an extreme measure made in communication with the affected users and managers (if possible.)