

DATA NETWORK PROCEDURES

Each user of computing resources is not allowed to add, modify, reconfigure, or extend any component of the University network, including, but not limited to:

- switches
- routers
- hubs
- wireless access points
- domain name servers (with the exception of caching DNS servers)
- DHCP servers
- firewalls.

Users of computing resources are required to pay network access charges for each node requested per month. Sharing of service is strictly prohibited. More specifically, only one client device can be connected to any single port provided by the Division of University Networking & Infrastructure (UNI). As well, no ports for which a designated device has not been identified should be activated; essentially open ports should not be available. Exceptions for devices (i.e. clusters, virtual machines, or standing temporary facilities) should be submitted, in writing, to the Network Operations Center (NOC) at noc@lsu.edu.

Each user of computing resources is allocated a single network port, and only 2 MAC addresses are allowed on any single port on the University network. Installing additional unnecessary connections on the University network increases the risk of a security incident, strains University resources, and may degrade services. Requests for additional ports on the University network should be submitted, in writing, to the NOC at noc@lsu.edu.

All devices connected to the LSU network are required to be continuously updated with the latest system and anti-virus updates. Should a device begin to cause problems on the LSU network due to a threat and/or vulnerability, ITS will attempt to contact the system administrator to remove the device from the network. However, if contact cannot be made in a timely manner, the port connecting the device to the network will be deactivated until it is determined the device has been cleaned. In order to protect University data and systems, as well as protect threatened systems external to the University, the IT Security and Policy Office may place limits or restrictions on technology services provided on or from any computing resources, and may unilaterally direct that a specific computing resource be isolated from University, campus or external networks.

Please consult [LSU System Permanent Memoranda 36](#).

Also consult:

- [PS-107 – Use of Computing Resources](#)
- [PS-06.20 Security of Data](#)
- [PS-114 Security of Computing Resources](#).

Users of computing resources are not allowed to install, remove, reroute, or otherwise modify network cabling without the express permission of Information Technology Services (ITS) in conjunction with the

Office of Facility Services. For additional information, please refer to [PS-84 – Custody of Facilities and Premises](#).

Ownership and control of IP networks and addresses resides with UNI. Use of Private addresses (RFC 1918) is also controlled by UNI and routed within the LSU IGP (inter-gateway protocol). Unauthorized use of private addresses by any LSU entity without the express consent of UNI is forbidden. Final decision on any rules pertaining to IP addresses, DNS, or DHCP is the responsibility of UNI.

Questions or comments regarding the procedures outlined above should be submitted, in writing, to noc@lsu.edu.