

UMB, UMMC, UPI and SOM Enterprise Campus Network Device Naming Policy

Executive Summary

All devices connected to campus networks need to be identified by network administrators for the purpose of notifying responsible parties about such devices when necessary. The following naming convention standard applies to every device that is attached to the campus network, and which has the capability of having a configured network name.

Goal

To provide easy identification of the responsible organization, department and individual for devices connected to the campus network.

Scope

All devices operated by campus organizations, their workforce or their students that connect to campus networks and that have configurable network names are governed by this policy.

Definitions:

Departmental IT Manager – Individual or group responsible for maintaining network devices for an organization and/or department.

General Policy

All devices connected to the campus network must contain at least 6 characters identifying the organization and department of the person responsible for that device.

It is recommended that the 6-character identification be at the beginning of the name.

All device names must use standard host naming conventions set by RFC 952, namely:

- A "name" (Net, Host, Gateway, or Domain name) is a text string up to 24 characters drawn from the alphabet (A-Z), digits (0-9), minus sign (-), and period (.). Note that periods are only allowed when they serve to delimit components of "domain style names". (See [RFC-921](#), "Domain Name System Implementation Schedule", for background). No blank or space characters are permitted as part of a name. No distinction is made between upper and lower case. The first character must be an alpha character. The last character must not be a minus sign or period. A host, which serves as a GATEWAY, should have "-GATEWAY" or "-GW" as part of its name. Hosts, which do not serve as Internet gateways, should not use "-GATEWAY" and "-GW" as part of their names. Single character names or nicknames are not allowed.

Examples:

- A device that is physically connected to the SOM network infrastructure and is operated by the Department of Medicine may have a device with the following identification:
 - SOMMED41966-SERIALNUMBER
- A device that is physically connected to the UMMS network infrastructure and is owned by the Department of Neurology but managed by SOM may have a device name with the following identification:
 - UMMSNEURO-SPECIFICID
- A device owned and managed by CITS will have a device name with the following identification:
 - citsXXXXXX.campus.umaryland.edu, with XXXXXX denoting the specific internal device name or number that corresponds to a specific user.

All servers must have corresponding DNS names.

- The initial host (“A”) DNS record will match the configured network name on the device exactly.
- Any alias (“CNAME”) DNS records may be different name.

Auditing and Monitoring

Campus DHCP and DNS tables will be monitored periodically by their respective owners for compliance with this policy. Policy violations will be reported to the CIO of the appropriate organization.

Communication

All network devices requiring DNS names must be submitted to the local DNS administrator for review. Requests must include the device’s:

- MAC Address
- Network Name
- Location
- Contact Person’s/Group’s name
- Contact Phone number
- Contact Email Address

Effective Date

The rules defined in this document are effective as of April 1, 2004. . All existing workstations must have their network name changed to comply with this policy. There will be a 6-month grace period to update workstation machine names.

Existing servers will be grand fathered and will not require name changes. As new servers are installed they must comply with this policy..

Violations

Failure to properly configure new or redeployed workstations is a violation of this policy.

It is the responsibility of each departmental IT manager to make sure that they are keeping their departmental systems in compliance with the above stated policy. Failure to do so constitutes a violation of policy.

Enforcement

Violations in policy could result in progressive disciplinary action dealt with through normal disciplinary processes within each organization.

Any computer found not to be in compliance will be disconnected from the network until it is properly configured.

Revisions

As the nature of technology continues to change and improve, this policy will be reviewed and revised to address those changes.