DRAFT Procedures Document to Accompany DRAFT Network Operations Policy

This document is intended to provide specific procedures pertaining to "covered devices", as defined by the Network Operations Policy. Procedures described here shall be approved by the ITEC Advisory Council (IAC). This document should be reviewed at least annually. Any recommended changes to this document must also receive IAC approval before going into effect.

An implementation plan describing how, when, and by whom work is to be done as buildings are migrated to be compliant with the Network Operations Policy is provided as Appendix E.

A glossary of terms and acronyms is provided as Appendix A.

Read Access to Ethernet Switches

ACNS will provide Authorized Personnel access, via console (ssh/telnet) or web interface (http/https), to Ethernet switches in their department. This will allow authorized personnel to monitor traffic patterns, spot traffic anomalies, diagnose throughput problems, etc.

In addition, authorized personnel will have access to:

- Real-time and historical information for various performance metrics (port utilization, errors, etc.) via Cacti (see http://www.cacti.net/), for all campus network devices.
- Read-only access to Nagios for uptime monitoring (http://www.nagios.org/).
- Read-only access to HP ProCurve Manager for switch statistics and troubleshooting.

All performance monitoring applications mentioned in this section will be accessible via the secure gateway (https://secure.colostate.edu/subnetmgrs).

Data Jack Activation

Open network switch ports (i.e. switch ports with no patch cord attached) on ACNS-operated switches are to be configured by default to be on a data VLAN consistent with the unit serviced by that switch. Modules A and B are reserved on ACNS-operated building distribution switches for connectivity to communications rooms and other special-purpose needs. Otherwise, to activate an open data jack, authorized personnel may:

1. Establish connectivity by attaching one end of the patch cord to an open switch port, and the other end to the patch panel port corresponding to the desired location.
    a. Response time is dictated by the authorized personnel doing the patching.
    b. In order to maintain our Systimax cable plant certification, only approved patch cords are to be used for this purpose. Approved patch cords are available on campus from RAMtech, but may also be ordered ahead of time from suppliers such as Anixter.
    c. Patch cords are to be placed neatly in the rack, using existing cable organizers (reference proper cabling procedures in Appendix D).

    d. Patch cords are to be consistent with the color code being used to clearly indicate the type of service being provided (color codes are provided in Appendix B).
    e. Within two business days of performing the work, authorized personnel should access a web page <URL goes here> to document what has been patched (specifying the communications room number, switch, switch port, patch panel port, and building/room number that has been connected).
2. Use the self-service web page <URL goes here> to request ACNS/Telecommunications to patch the connection(s) on your behalf.
    a. An account number must be supplied to cover the cost of patch cords required to perform this work.
    b. Requests for up to six connections at a time may be made with an expected completion time of within one business day from when the request was made.
    c. Requests for greater than six connections at a time may be made with an expected completion time of within two business days from when the request was made
        i. If no available switch ports are available to accommodate either 2.a or 2.b, response time may be increased by up to two business days.
    d. "Emergency" requests, with an expected completion time of within 3 business hours from when the request was made, will be allowed at one such request per unit per month. Emergency requests in excess of one/unit/month will be billed for time and materials.
3. Use the self-service web page <URL goes here> to document that previously patched ports are no longer in use, and may be re-used for new activations.

Port Mirroring

Authorized personnel may request via the self-service web page <URL goes here> the ability to send all traffic to/from a specific switch port in their area to another port (assuming it is in the same switch stack) in order to troubleshoot application problems. Such requests will be honored within 3 business hours from when the request was made.

VLAN Changes

Authorized personnel may request VLAN changes for specific switch ports in their area via the self-service web page <URL goes here>.

a. Requests for up to six VLAN changes at a time may be made with an expected completion time of within one business day from when the request was made
b. Requests for greater than six VLAN changes at a time may be made with an expected completion time of within two business days from when the request was made
c. "Emergency" requests, with an expected completion time of within 3 business hours from when the request was made, will be allowed at one such request per unit per month. Emergency requests in excess of one/unit/month will be billed for time and materials.

Departmental Firewall implementation

Authorized personnel may request assistance implementing a departmental firewall via the self-service web page <URL goes here>. Departmental firewalls will be implemented via Cisco's Firewall Services Module (FWSM) on the core routers to which departmental LANs are attached. ACNS Security staff will work with authorized personnel in the units to migrate existing firewall functionality to the Cisco platform.

Requests to maintain existing firewalls and other network traffic control devices may be submitted to the CIC for consideration, with an expected turn-around time of 10 business days.

Policy Exemptions

Authorized personnel may request certain switches in their environment to be exempt from the Network Operations Policy via the self-service web page <URL goes here>. Such requests will be reviewed by the CIC within 10 business days from the time the request was made. Exceptions will be granted with the following understanding:

- Exempted devices will be attached to devices operated by the ACNS NOC.
- ACNS may disable ports connecting exempted devices at any time it is detected that traffic from such devices are adversely affecting other network devices or services.
- Minimum configuration standards must be met when configuring options such as spanning tree, multicast, VLANs, etc. See Appendix C for specifics regarding these configuration options.
- Moving approved, exempted devices from one switch port to another must be coordinated with the ACNS NOC.

Appendix A - Glossary

ACNS – Academic Computing & Networking Services

Authorized Personnel – IT Staff not part of the ACNS NOC group but who have been delegated authority within their unit to access communications rooms in support of local users.

CIC – Communications Infrastructure Committee, an ad-hoc subcommittee of the ITEC Advisory Council. See http://iac.colostate.edu for more information.

Covered Devices – Network switches, as defined by the Network Operations Policy, in areas where devices supporting Voice over IP, life and safety, access control, electronic surveillance, etc. have been placed into service.

ITEC – Information Technology Executive Council. See http://itec.colostate.edu for more information.

NOC – Network Operations Center, a functional area within ACNS responsible for configuration, installation and management of core campus networking devices.

Appendix B – MDF/IDF Patch Cord Standards

MDF/IDF Patch Cord Standards:

CommScope Systimax patch cords, of equal or greater level as the cable plant in the building, must be used when patching data connections.

The following color standards have been adopted on campus, and must be adhered to:

- **Red, Gray:** Data
- **White:** VoIP*
- **Green:** Security Cameras, CardKey, Meters, EMS, Facilities*
- **Yellow:** Wireless*
- **Violet:** A/V*
- **Orange:** Switch-switch links*
- **Light Blue:** Departmental specific

*If White, Green, Yellow, Violet, or Orange patch cables have been installed, please do not move them for any purpose. If you have questions or concerns about these connections, please call the ACNS NOC at 970.491.5133.

Appendix C – Network Switch Configuration Standards

Spanning-Tree

- 802.1W (RSTP)
- Switch is not set as a root switch nor is the default priority reduced
- No loop or BPDU protect settings on feed port to campus switch. Campus switch port should be configured as a regular data port

LLDP

- LLDP supported and enabled

SNMP

- SNMP v3 support
- SNMP community changed from the default
- Read/write disabled unless necessary

VLANs

- 802.1q support
- No central VLANs are to be configured on exempt switches

Trunking

- LACP

Username/password and switch access

- username/password Changed from the default
- RADIUS authentication support
- SSH support
- https support

Multicast/IGMP

- Enabled for all VLANs and port connecting to campus switch

Naming/labeling

- Switch description defined in switch configuration including Building name, room number

Routing

- Disabled

IPV6

- Supported

Appendix D – Proper Cabling Procedures

- Proper length cables are to be used such that no more than 1 foot of slack and no tension is put on the cables.
- Switches should be divided down the middle with cabling on the left side being routed to the left and cabling to the right, routed to the right.
- No cables should extend down or across the middle of switches or patch panels.
- All cables should be routed through horizontal and vertical organizers. Cables are not to be left freely hanging anywhere in their path.
- Extreme care should be taken to avoid crimping any cabling.
- Extreme care should be taking to avoid disturbing any fiber cabling. (Note: Fiber cabling connected to ACNS operated switches is to be installed/maintained/connected/disconnected by ACNS Telecom/NOC staff only.)

Appendix E – Implementation Plan

Purpose

This document provides guidelines for implementing the Network Operations Policy in campus buildings.

When

As of July 1, 2011, 77% of campus network switches are under the direct operational management of the ACNS Network Operation Center (NOC). The remaining 23% will be migrated to ACNS management by January 1, 2014. Buildings will be systematically prioritized based on the following criteria:

- For the 77% of switches currently under ACNS Operational Control, formalize NOC management by ensuring configuration and management standards have been uniformly applied
- As building connections are upgraded to the dual gigabit standard described in the Network Operations Policy, operational management will be transferred to the ACNS NOC
- As Voice over IP (VoIP) services are installed in a building, operational management will be transferred to the ACNS NOC
- As requests from units are received for ACNS to assume operational management of Ethernet switches, such requests will be honored as quickly as possible
- The remaining 23% will be scheduled in coordination with IT staff in the appropriate units

Progress on the above will be monitored closely by the ACNS NOC and communicated to the IAC on a quarterly basis.

How

Migrating operational control of campus network switches will essentially ensure the application of the ACNS NOC's standards for configuration, monitoring and management to network switches. This activity will be closely coordinated with relevant subnet managers on a building by building basis.

Equipment coming under the control of the ACNS NOC will be reviewed for compliance in areas including, but not limited to, those specified in Appendix C.

By Whom

Planning and implementation of migration of Ethernet switches to ACNS NOC control will take place in collaboration with relevant subnet managers. All work will be managed by the ACNS NOC.