Computing
& Networking
CNS Services

Wall-Plate Services

Service Level Objectives

Description of Basic Network Services and Advanced Network Services

Service-Level Objectives:

- Definition of Basic Network Services (BNS)
- Definition of Advanced Network Services (ANS)
- Problem-Resolution Procedures
- Service Level Objectives (SLO) Review Procedures
- Addendums

This document defines the type and nature of various network services provided to the campus by The University of Florida Computing and Networking Services (CNS). Basic Network Services includes adequate connectivity for most of today's high-speed network and computing needs. Basic Network Services also includes network-enabling applications, such as Domain Name Services, that are required for modern networks. Advanced Network Services represent various special services beyond that provided by Basic Network Services. Each Advanced Network Services selection will generate additional installation or recurring charges, and the unit will decide which, if any, Advanced Network Services are needed.

Additional information about the Wall-Plate Project can be found at the CNS web page.

http://www.cns.ufl.edu/wallplate/

Application level services, such as Websphere, Gatorlink, e-mail, etc. are handled by the application support groups and are not addressed in this document. For questions about other support services, contact the UF Computing Help Desk at 392-4357 or the CNS Support Desk at 392-2061.

Health Science Center users should contact HealthNet at 392-7383 or visit the Healthnet web page.

http://www.healthnet.ufl.edu

Services Provided by CNS

Basic Network Services (BNS) – BNS represents the minimum level of network services that is supplied to Wall-Plate customers, as a goal, at any point in time. BNS includes the following:

1. Desktop Connections
2. Server Connections
3. Quality of Service
4. Core Network Support
5. Supported Protocols
6. Supported Equipment
7. Network Malfunction Resolution
8. Network Performance Monitoring
9. Network Upgrades
10. Network Enabling Applications
11. Security Services (programmable filters that meet current Design Standards)
12. Network Address Space Management
13. Client Remote Access VPNs
14. Basic Wireless Services
15. Voice Services
16. Virtual Private Networks (VPNs) and Private WAN links
17. Site to Site VPN Services

Advanced Network Services (ANS) – Certain services not covered as Basic Network Services are available as an Advanced Network Service and arranged on a per request basis.

1. Security Services
2. High Density Wireless Services
3. Video Services (Provided by OIT-AT)
4. Authentication services
5. Firewall Services
6. High Speed Core connections (10G+)
7. Connectivity to HPC Research Network
8. Storage Area Networking
9. Research Waves

Definition of Basic Network Services

Basic Network Services are delivered to the end user via data equipment and campus wiring infrastructure that conform to the current design standards of CNS. The Design Standards represent currently available and cost-effective technologies, and configuration and design guidelines that best address current campus needs. BNS represents the goal for the minimum level of network services that is supplied to Wall-Plate customers, at any point in time.

The following defines Basic Network Service:

1. **Desktop Connections**

    - The current standard for desktop connections in new construction or retrofit projects is switched, 10/100 Mbps, over Unshielded Twisted Pair Category 5E copper cabling (UTP Cat5E). The Wall-Plate project does not support fiber to the desktop.
    - Additional connections that require deployment of an additional switch will be subject to a one-time charge for each additional switch. Locations not funded by the Provost will also incur an additional recurring monthly charge for each additional activated port.
    - New construction, as well as renovated construction standards for wall-plate density, will follow current campus standards.
    - Local administrators and users must not attempt to implement their own network infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. They must not offer alternate methods of access to UF IT resources such as modems and virtual private networks (VPNs). Active electronics that expand the network connectivity beyond that of the wall plate must be approved and managed by CNS for the purpose of providing a secure and reliable network for all users.

2. **Server Connections**

    - Server connections are supplied at switched, fast Ethernet (100 megabits/second) speeds.
    - Special, higher-speed, connections for servers are available at an additional cost.

3. **Quality of Service (QoS)**

    CNS recognizes the additional demands of voice and video over the network. For this reason, CNS will be implementing a basic QoS design to prioritize IP traffic accordingly where required.

4. **Core Network Support**

    - CNS will provide access to the Internet, Florida LambdaRail, National LambdaRail, Internet 2, and the UF Intranet as a component of BNS.
    - The Core Network and campus LANs will evolve as indicated by ongoing traffic engineering studies.

5. **Supported Protocols**

    - Basic Network Service provides support for routing multiple networking protocols. Only the protocols that are specifically listed in the SLO will be supported.

- The campus backbone currently supports the following protocols:
    - Internet Protocol version 4
    - IPv6 (available summer 2008)
- This protocol list will change in the future relative to the needs of the University.
- Limited support may be given to troubleshoot non-routed protocols on campus LANs.

6. Supported Equipment and Infrastructure

- Communications equipment rooms and pathways should meet University standards as defined in the University Telecommunications Standards**.**

    http://net-services.ufl.edu/infrastructure

- During the initial stages of a wall-plate engagement, telecommunication closet network infrastructure and electronics will be brought up to the University standards if possible. Conditions may exist that prevent these standards from being met. These conditions will be evaluated individually for each wall-plate engagement.

7. Network Malfunction Resolution

- Troubleshooting, analysis, repair, and problem resolution of malfunctioning networks, and all types of network maintenance, are provided as a BNS.
- If the problem is determined NOT to be a result of the wall-plate infrastructure, network services will contact the local support personnel to address the issue.
- Disruptive network devices will be disconnected until the end-user can arrange repair of the malfunctioning device in accordance with the University IT Security Policy.

    http://www.it.ufl.edu/policies

- CNS will not troubleshoot any network problem where a user or local administrator has deployed active electronics for the purpose of expanding the network connectivity beyond that of the wall plate.
- CNS will disable or disconnect any LAN segment that has been altered to expand the network connectivity beyond that of the wall plate.
- Support of desktop computers and other end-user network devices is not included in BNS. This is the responsibility of the end-user, the local support personnel, and the University Help Desk.

8. Network Performance Monitoring

- All CNS-managed network devices will be monitored for availability.
- All switch ports on building-point-of-presence switches (BPOPs) will be

monitored for utilization and error statistics.

- All statistical network data will be archived.
- All data will be available to CNS and local personnel via a web-based system currently under development.

9. Network Upgrades

- Performance enhancements to congested networks will be provided when analysis shows that the current subscription level is not providing adequate network services.
- If a unit requests upgrades due to increased requirements (bandwidth, density, or to support special needs), a proposal will be provided for the unit's consideration.
- Periodic upgrades may be applied to keep the network updated.
- Malfunctioning equipment will be immediately replaced or upgraded as appropriate.

10. Network Enabling Applications

BNS includes the provision of essential network services such as Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP), Trivial File Transfer Protocol (TFTP) and Gatorlink authenticated network access.

11. Security Services

- Security will be monitored and enforced in accordance with the UF IT security policies and procedures.

  http://www.it.ufl.edu/policies.

12. Network Address Space Management

CNS will allocate supported protocol address space as needed.

13. Client Remote Access VPNs

- CNS offers a remote access VPN solution to all University Faculty, staff, and students with active Gatorlink accounts.

  http://net-services.ufl.edu/provided_services/vpn

- VPN allows Gatorlink users to remotely access most campus services via a general UF assigned IP address.

14. Wireless Services

Wireless services under BNS provide a wireless signal for simple connectivity and does not provide for high-density wireless usage.

15. Voice Services

Physical infrastructure as well as network electronics that are provided for Basic Network Services will support IP Telephony communications. Power over Ethernet (PoE) and Voice services provided by this infrastructure are available at an added cost.

16. Virtual Private Networks (VPNs) and Private WAN links

Organizations interested in having either a private WAN link or in using specialized VPN services can have these services managed by CNS. Departments wishing to customize the CNS Gatorlink Remote Access VPN so their users get an IP address in a specific range may do so with the Departmental Remote Access VPN service.

http://net-services.ufl.edu/provided_services/vpn

17. Site-to-Site VPN Services

CNS also provides secure site-to-site tunnels using the industry standard IPsec suite of protocols.

http://net-services.ufl.edu/provided_services/vpn

Definition of Advanced Network Services

Certain services not covered as a Basic Network Service are available as an **Advanced Network Service** with an added fee. Charges for Advanced Network Services will be levied on a one-time, recurring, or time and materials basis. Requests for Additional Network Services may require an individual estimate or quote, as each case is different and equipment prices vary.

Examples of Advanced Network Services (ANS) include the following:

1. **Security Services**

   CNS strives to ensure the security of the University of Florida network. Should a unit or department need assistance with the security of their upper layer devices, CNS will provide security services.

2. **High-Density Wireless Services**

   Wireless networking is fast becoming a widely used service. Wireless networking services for high-density wireless use areas are available from CNS with which users can connect to the UF network via wireless connections.

   http://net-services.ufl.edu/provided_services/wireless

3. **Video Services**

   Specialized video services such as multipoint video conferencing are available. In-depth assistance to support basic video conferencing issues such as room setup, design, and renovation are available through Video & Collaboration Services.

   http://www.video.ufl.edu

4. **Authentication services**

   Verification of the end user to the network are paramount to security. Secure ID Challenge Card Systems is a prime example of an authentication service beyond that provided with BNS. CNS can provide these services to the unit or department.

   For electronic door access, contact PPD for assistance.

5. **Firewall services**

   For those units who need a network-based firewall, this service must be provided by CNS. The addition of any firewall must be coordinated with CNS to ensure compatibility with the campus network and adherence to campus security policies.

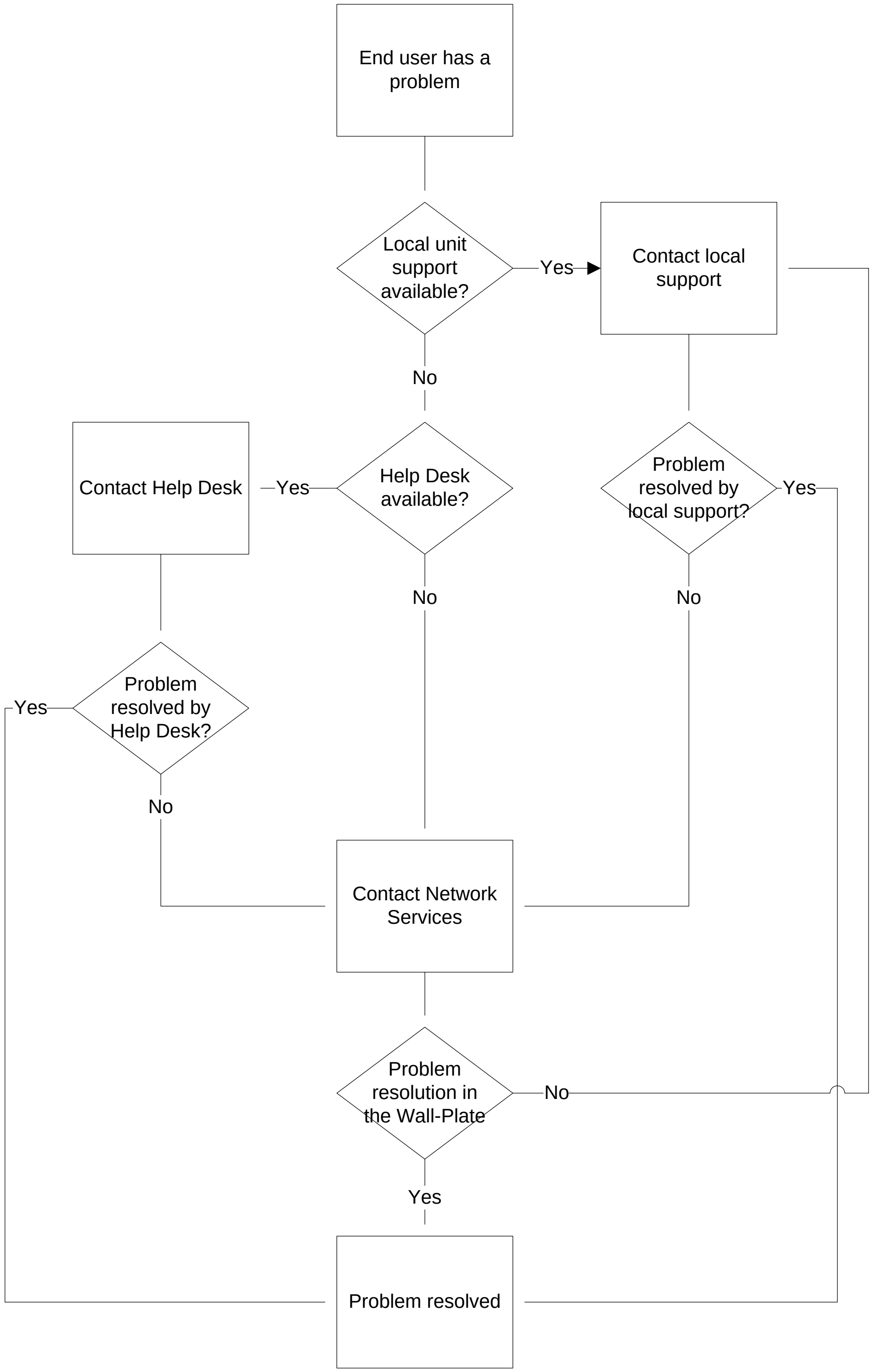
6. **Special Network Connections**
    a. High Speed Core connections (10G+)
    b. Connectivity to Campus Research Network
    c. Storage Area Networking
    d. Research Waves

Problem Resolution Procedures

When a problem is encountered by an end-user in which he/she needs assistance, one of two courses of action will be followed. If the problem occurs during business hours that local unit support is available, the user should contact the local support for assistance. Local support personnel will then contact CNS if the problem is suspected to be behind the wall plate. If local support personnel are not available, the end user should contact the help desk to report the problem. CNS will then work to determine if the problem is within the network. If the problem is within the network, CNS will correct the problem as soon as possible. However, if the problem is determined to NOT be with the network, the problem will be handed off to the local support personnel as soon as they are available. Additional local support during those times that local support is not available can be provided by CNS for an additional fee as an ANS.

The following flowchart summarizes problem resolution procedures:

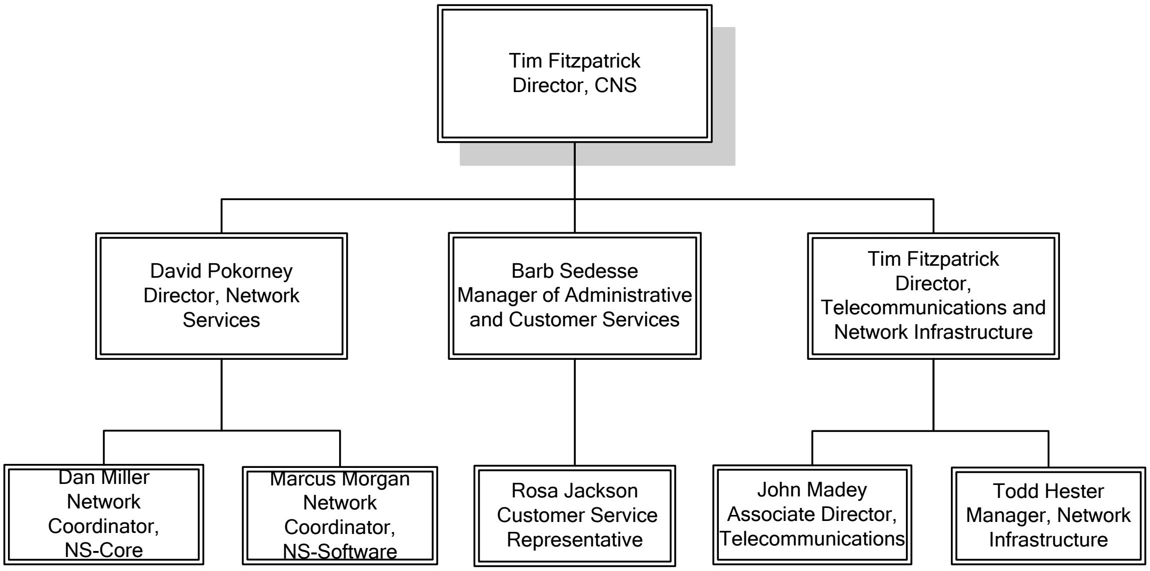
Problem Resolution Flowchart



Service Level Objectives Review Procedures

CNS staff and management are committed to providing the highest quality service possible. Network Services is part of the Office of Information Technology and consists of three main groups: Software Support, Core Networking, and Network Infrastructure. Each group works closely with one another to provide a suite of network services to the UF Campus.

Local support personnel who have problems or issues with the services being provided should notify CNS through proper problem resolution channels. Below is an overview of the structure of CNS:


Tim Fitzpatrick
Director, CNS
David Pokorney
Director, Network Services
Barb Sedesse
Manager of Administrative and Customer Services
Tim Fitzpatrick
Director, Telecommunications and Network Infrastructure
Dan Miller
Network Coordinator, NS-Core
Marcus Morgan
Network Coordinator, NS-Software
Rosa Jackson
Customer Service Representative
John Madey
Associate Director, Telecommunications
Todd Hester
Manager, Network Infrastructure

Addendums

1. Procedure for Requesting Exception to Standards or Policies
2. Switch Exchange Policy
3. Requirements for Connecting to the Wall-Plate Data Network
4. Deploying Departmental Servers in Telecommunication Closets
5. Technical Staff Access to Telecommunication Rooms
6. Network Edge Protection – User Guidelines for Wall-Plate Networks (7-1-08)
7. Draft Addendum: Wall-Plate Firewall Services
8. Draft Addendum: Requirements for Establishing a Non-Wall-Plate Network Zone within a Wall-Plate Building
9. Draft Addendum: Withdrawing from the Wall-Plate Program

1. Procedure for Requesting Exception to Standards or Policies

Local administrators may request exceptions to Wall-Plate policies or standards by submitting a written request to CNS by clicking on “Request Network Service” on the CNS web page at http://www.cns.ufl.edu/

Requests for exceptions to the policy will be evaluated on the following criteria:

- Justification for requesting the exception
- Risk to network stability or security
- Impact or cost to the requesting department, CNS, or the Wall-Plate Project
- Length of time requested for the exception
- Adequate advance notice for proper planning and deployment
- Available resources

Some examples for which exceptions may be granted are the following:

- Creating swing space during construction or renovation projects
- One-time special events
- Waiting for new cable to be installed
- “Tech Bench switch” for IT staff locations
- Pilot, demonstration, or evaluation projects

2. Switch Exchange Policy

Departments that are waiting for the Wall-Plate Project deployment may request to exchange some of their older switches for newer switches from the CNS surplus switch inventory (subject to availability). The following guidelines are required to be eligible for the exchange:

- The Department must make a commitment to join the Wall-Plate Project.
- The exchanged switch must be used to replace an older or less functional deployed switch and will not be used for port count expansion.
- Department agrees to transfer the older switch to CNS in exchange for use of the newer switch.
- The exchanged switch will be reclaimed by CNS when the Wall-Plate project deploys at that location.
- Department agrees to return the exchanged switch to CNS if it is no longer needed or is no longer functional.
- The useable port count of the two exchanged switches should be equivalent.
- The department is responsible for the installation and maintenance of the switch until the Wall-Plate project assumes support for that location.

Requests for exchange should be made thru the CNS “Request Network Service” web page.

http://net-services.ufl.edu/problems.html

3. Requirements for Connecting to the Wall-Plate Data Network

February 13, 2008

The data network has become a critical component of the campus infrastructure, serving almost every aspect of the UF mission. For example: WebCT is used in teaching and learning. High Performance Computing is used in Research. MyUFL systems are used in HR and Finance administration, and Student services. And GatorLink e-mail is used by just about everyone. All ride on the campus data network.

In order to assure that the data network remains robust, reliable, and secure, the Provost's Office has been investing in a multi-year, multi-million dollar project and ongoing program to upgrade and expand the campus data network. Known as the Wall-Plate project, over the past 3 years about ½ of all data ports on campus have been replaced. Over the next 3 years, most of the remaining data ports will be replaced. Similar network upgrades have occurred in Housing and the Health Sciences Center.

Current Wall-Plate program requirements prohibit the use of any device not managed by CNS, which extends the network beyond the Wall-Plate data port. Such devices can cause problems in the network. Examples include: hubs, switches, routers, and wireless access points. Such devices defeat the purpose of having upgraded to a modern, ubiquitous, and standardized data network.

Any unit, choosing to "op-in" to the centrally funded wall-plate program, must remove local network hubs and resolve related wiring problems. Because Wall-Plate data ports are paid for centrally, most units choose to opt-in. Because the cost of fixing any in-building wiring problems must be paid by the local unit, some units may perceive these costs as prohibitive. This is especially true in buildings where substandard wiring and/or hubs have been used for years to avoid the cost of wiring upgrades when new users were added to the network.

Effective July 1, 2008, network monitoring and protection methods will automatically shut down any Wall-Plate port showing symptoms of such devices or similar problematic traffic. Exceptions must be reviewed and approved by CNS. A description of central Wall-Plate services provided by CNS, and local unit requirements for connecting to the Wall-Plate Data Network, are documented at:

http://www.cns.ufl.edu/wallplate/CNS_Wall-Plate_SLO.pdf

4. Deploying Departmental Servers in Telecommunication Closets

Departmental servers shall not be deployed in telecommunications closets. Exceptions may be granted for full size telecommunication rooms (10’x12’ or larger as defined in the University of Florida Telecommunication Standards). Requests for exceptions will be evaluated on the following criteria:

1. The security, support and maintenance of the Wall-Plate infrastructure and electronics must not be jeopardized by the server presence.
2. Cooling capacity of the room is adequate for the anticipated heat load (ambient temperature not to exceed 80°F).
3. Servers shall be rack mounted in a secure enclosure independent of the network infrastructure or electronics.
4. Server rack shall not interfere with access to the network infrastructure and electronics racks.
5. Access to the room shall be limited to authorized personnel.
6. Local server support staff must not attempt to configure, modify or access network infrastructure or electronics.
7. Adequate electrical facilities are available independent of the network electrical services and UPS capacity.

5. Technical Staff Access to Telecommunication Rooms

Local technical staff may request access to Telecommunication rooms. Technical support staff must not attempt to configure, modify or access Wall-Plate network infrastructure or electronics. All port activations and changes shall be submitted via the CNS web page or by calling 392-2061.

6. User Guidelines for Wall-Plate Networks

This document serves as a guideline for end users and administrators who operate hosts in a Wall-Plate Network with Network Edge Protection enabled. This is part of a new CNS network standard which will protect the network from many problems including most network loops, rogue DHCP servers, malfunctioning NICs, and misconfigured or misbehaving hosts. Automated systems will notify local administrators via email when ports in their area are disabled so that they may work with users and CNS to resolve any problems.

What the Users will See

A port that has been disabled will reactivate in 5 minutes. If the cause of the error has been removed, the port will remain active, and if not, it will be disabled again for another 5 minutes, and the cycle will continue. A Wall-Plate port will not display Ethernet link when it’s disabled, but a disabled port on an IP phone will show link up and simply not pass traffic. The IP phone should remain functional even if the network port has been disabled. Some common problem causes are listed below.

Laptops with Wired and Wireless NICs Set to Bridging Mode

A laptop (or desktop) host which has two connections to the network and has bridging enabled in the OS may be disabled. This is most commonly seen with hosts that have active wired and wireless connections. All such hosts should have bridging turned off in their network driver configuration.

Hubs and Switches Connected to Edge Ports

Hubs and Switches connected to edge ports (intended for hosts) may be disabled for several reasons. All network devices that extend the network beyond the wall plate must be approved and managed by CNS.

IP Phones and Moving Hosts

The switches in Cisco IP phones do not communicate link down traps to the Wall-Plate switches they connect to. As a result, a host that is connected to an IP phone and then moved to another Wall-Plate port within 5 minutes will be disabled. This will occur whether the destination port is on an IP phone or wall port. If a host is moved from a wall port to any other network port, there should be no problem since the link down state will cause the Wall-Plate switch to flush the tables. The vendor has been asked to improve IP phone and switch integration.

NICs with Non-Standard 802.1x Enabled

Some Marvel NICs have been found that assert a common MAC address during boot up, and then change their MAC address. These NICs do not follow Ethernet standards; i.e., they have a bug. The port may be disabled if the switch has learned the same MAC address on another port within 5 minutes. The offending MAC address for these NICs will be filtered at the Wall-Plate switch, but there may be others that have not been discovered. The network drivers for all wired NICs should have 802.1x disabled as a precaution until that technology has matured and is supported by Wall-Plate networks.

VMware Hosts and Servers

A VMware server configuration that is copied to create a new server must have its configuration altered to change the MAC address or the address will show up twice. This is a duplicate MAC address, and port security will shut down that port.
VMware servers that have 2 NIC cards connected to 2 Wall-Plate ports for failover will not work with port security. Please inform CNS when you wish to connect a redundant server, and network edge protection will be disabled on those ports.
A VMware host that is running more than 3 virtual machines within 5 minutes would be disabled.

Rogue DHCP Servers

All DHCP servers in Wall-Plate networks must be registered with CNS so that they may be explicitly allowed. The default configuration will filter DHCP packets which will protect local users from rogue DHCP servers. This condition will not reset or cause the port to be disabled.

Notification of Disabled Port

All subnet managers listed as supporting the subnet with a disabled device will receive an email notification with the Wall-Plate port number for any disabled device each hour until the cause of the error is removed. An example of the email notification follows:

Subject: CNS Wall-Plate Network Edge Protection alert, port *xxxx-xx-xxxx date time*

This is an automated notice that Wall-Plate port *xxxx-xx-xxxx* has been automatically disabled at *date time*. A port that has been disabled will reactivate in 5 minutes. If the cause of the error has not been removed, the port will become disabled again, but these automated alerts will only be sent every hour. Please check this link for a list of possible causes and other details:
http://www.cns.ufl.edu/wallplate/wallplate_user_guidelines.pdf

Please open a ticket with CNS if you believe this was a false positive or if you require other assistance to restore service:
https://remedy.cns.ufl.edu/cgi-bin/cnsproblems.cgi

If you have other questions or concerns regarding this matter, please reply to this email as soon as possible.

Thank you,
Network Services
Net-Services@lists.ufl.edu
(352) 392-2061
Home page: http://net-services.ufl.edu

Draft Firewall Addendum for Wall-Plate SLO 12-4-08
****

7. Wall-Plate Firewall Services

Programmable Filters
The Wall-Plate Basic Network Service offers the ability to implement complex customer specified programmable filters to control access to or from workstations or servers. The customer specified filters can be based on source/destination IP networks, host addresses and /or port numbers. Up to three different customer filters can be defined per building. Any of the three customer filters can be applied to a single host or to any number of hosts within the building. There is no additional charge for the Basic Network Service programmable filters. Customers can request programmable filter configuration changes by submitting a Wall-Plate "Service Request" or can report a problem by submitting a "Trouble Ticket" via the CNS web page or by calling CNS.

Advanced Firewall and Security Services
Advanced firewall services are available as an Advanced Network Service with an added fee. The Wall-Plate Advanced Network Service offers additional programmable filters for groups requiring more than three filters per building or that require more in-depth firewall security services. The advanced firewall and security services are deployed via enterprise class firewall hardware such as the Cisco ASA 5500 series of security devices. One or more security devices can be deployed per closet and can provide security services for any number of hosts serviced by that closet. The firewalls are maintained and configured by CNS. Customers can request firewall configuration changes by submitting a Wall-Plate service request or can report a problem by submitting a Trouble Ticket via the CNS web page or by calling CNS.

Initial configuration and installation charges for the Advanced Firewall and Security Services will be levied on a time and materials basis. The customer will also be responsible for the installation and replacement cost of the firewall devices at each five year refresh cycle. The cost for each installation will vary based on the technical requirements of the firewall environment and the amount of time required for configuration and installation. For example a firewall with up to 150 Mbps throughput (ASA 5505), serving up to 8 devices, could cost about $2000 installed, and a firewall with up to 300 Mbps throughput (ASA 5510), serving up to 24 ports, could cost about $5000 installed.

Additional customer initiated configuration changes after initial installation may be billed at $100 per hour. In most cases only major reconfigurations or excessive repetitive change requests will be charged. Charges for infrequent minor changes will be waived.

Draft non-Wall-Plate zone Addendum for Wall-Plate SLO 11-17-08
****

8. Requirements for Establishing a Non-Wall-Plate Network Zone within a Wall-Plate Building

Departments may choose to create locally managed wired network zones within a Wall-Plate building to address any special needs of academic research not achievable within the Wall-Plate program. Additional actions must be taken when implementing a locally managed network within a Wall-Plate building in an effort to maintain the integrity of the Wall-Plate "Port Security" features and to insure overall stability and performance of the greater Wall-Plate network. Departments must comply with the following requirements to implement a locally managed network within the Wall-Plate program:

- Customer shall define the geographical area of the locally managed network.
- Customer shall agree to not use CNS managed horizontal infrastructure or Telecom closets for locally managed network service distribution.
- Customer shall provide a firewall class device to isolate the locally managed network from the Wall-Plate network.
- Customer shall agree not to expand the locally managed network into an area supported by the Wall-Plate Project.
- Locally Managed Network shall comply with UF IT Policies and Standards.
- Customer shall agree to be responsible for resolving all network problems within the locally managed network.

Customer shall define the geographical area of the locally managed network.

1. Customer shall register with CNS all rooms that will be locally managed.
2. Areas of local management must be defined by permanent walls. Rooms cannot be subdivided for partial local management.

Customer shall agree to not use CNS managed horizontal infrastructure or Telecom closets for locally managed network service distribution.

1. CNS will provide one standard Wall-Plate Network Edge Protection configured port for the upstream connection from the customer's locally managed network.
2. No other Wall-Plate ports will be activated within the locally managed network zone except for VoIP service.
    a. VoIP will only be delivered on standard Wall-Plate ports supported by CNS closet and CNS managed horizontal infrastructure.
    b. Ports activated for VoIP will be limited to one MAC address for the phone. The data port on VoIP phone will be deactivated.

Customer shall provide a firewall class device to isolate the locally managed network from the Wall-Plate network.

1. Customer may connect any firewall class device to the single CNS provided Wall-Plate port.
2. CNS will not define or maintain static or dynamic routes on the firewall port.
3. Customer is responsible for troubleshooting any firewall actions that trigger the Wall-Plate Port security features. See Wall-Plate SLO addendum 6 for information on Port Security triggers: http://www.cns.ufl.edu/wallplate/CNS_Wall-Plate_SLO.pdf
4. Customer may implement locally managed network behind locally managed firewall.

Customer shall agree not to expand the locally managed network into an area supported by the Wall-Plate Project.

1. Customer shall notify CNS before changing the locally managed network perimeter.
2. If locally managed network ports are activated in a CNS managed Wall-Plate area the Wall-Plate ports will be deactivated within 24 hours of detection.
3. If an un-registered firewall is found to be attached to a Wall-Plate port the firewall Wall-Plate port will be deactivated within 24 hours of detection.

Locally managed network shall comply with UF IT Policies and Standards.

1. Locally managed networks must be in compliance with UF IT Policies and Standards:
   http://it.ufl.edu/policies/
2. Locally managed firewalls must allow access by the UF security scanner or request an exemption to use internal scanning and reporting.
3. Locally managed networks not in compliance with the UF IT Policies and Standards will be disconnected from the Wall-Plate network.

Customer shall agree to be responsible for resolving all network problems within the locally managed network.

1. CNS will not provide troubleshooting assistance within the locally managed network.
2. CNS will not troubleshoot connectivity problems traversing the locally managed firewall.
3. Customer may disconnect the locally managed firewall and connect a single workstation to the Wall-Plate port to demonstrate connectivity problems.
4. A single workstation connected to a single Wall-Plate port will receive standard Wall-Plate support services.
5. CNS response to a trouble ticket will be to disconnect the locally managed firewall from the Wall-Plate port and connect a CNS laptop to troubleshoot connectivity issues.

A non-Wall-Plate network zone area may rejoin the Wall-Plate program at any time by purchasing port expansion capacity for the number of ports to be reactivated in the Wall-Plate program. See the Wall-Plate FAQ for current port count expansion charges.

Scheduling for the re-integration of a non-Wall-Plate network zone into the Wall-Plate program will vary and depends on the availability of resources at the time.

Draft Wall-Plate exit policy Addendum for Wall-Plate SLO 11-21-08
****

9. Withdrawing from the Wall-Plate Program

A department may withdraw from the Wall-Plate program in entirety at any lifecycle equipment replacement window (approximately every five years). The withdrawal requirements are the same as those outlined in the previous addendum titled “Requirements for Establishing a Non-Wall-Plate Network Zone within a Wall-Plate Building” with the following exceptions:

- The switches that were previously used to support the area occupied by the withdrawing department under Wall-Plate and that are not required for lifecycle trade-in to support remaining Wall-Plate and VoIP services within the building can be transferred to the withdrawing department.
- The horizontal cable and Telecom closets not required by CNS to support the remaining Wall-Plate and VoIP services can be utilized by the non-Wall-Plate network.

A withdrawn non-Wall-Plate department may rejoin the Wall-Plate program at any time by purchasing port expansion capacity for the number of ports to be reactivated in the Wall-Plate program. See the Wall-Plate FAQ for current port count expansion charges. Scheduling for the re-integration of a department into the Wall-Plate program will vary and depends on the availability of resources at the time.