

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>