AO 38 UNIVERSITY OF PITTSBURGH POLICY (formerly 10-02-13)

CATEGORY: SUPPORT SERVICES
SECTION: Computing, Information, and Data
SUBJECT: University Network
EFFECTIVE DATE: January 26, 2018 Revised
Page(s): 8

I. SCOPE

This policy establishes the provisions for the installation, maintenance, and operation of the University of Pittsburgh's Network (PittNet).

II. POLICY

Computing Services and Systems Development (CSSD) is responsible for the installation, maintenance, and operation of the University's data communications network. Only networking equipment installed and managed by CSSD is allowed to be connected to the University network.

Device Addresses

Network users may operate only those devices attached to PittNet with addresses that have been authorized by CSSD. Network Addresses (IPv4 and IPv6 addresses) are the property of the University not individual units or persons and CSSD has sole responsibility for assignment of all network addresses. User or departmental assignment on PittNet address space is not permitted without an exception granted by CSSD for a specific application. Any statically allocated IP address assigned to a device that is not in use for 60 days or longer may be reclaimed by CSSD for assignment to another device. This restriction will not apply in those situations where IP addresses are dynamically assigned to devices by CSSD.

Supported Protocols

In order to ensure network reliability, CSSD provides network support only for the IP version 4 and IP version 6 protocols on PittNet. Many transport protocols are supported (e.g., TCP, UDP, ICMP, IPSec, etc.) and both unicast and multicast transports are supported. Units must not attach any device that relies only on an unsupported protocol to a network access point.

Network Operations

Wired

Installation of cabling (including fiber-optic cable) and network access points (ports) is the responsibility of CSSD. University units must not engage in the installation of network cable and/or network infrastructure devices, either on their own or by engaging the services of any third party.

Each network access point (port) is intended to support one and only one device. PittNet ports are RJ-45 10/100/1000baseT connections. Speed and duplex setting may be set to a fixed speed and duplex, or to auto-negotiate as requested by the user.

Network users must acquire, install, operate, configure, and maintain any hardware and software attached to network ports in accordance with current CSSD security standards.

Remote Access is available to end users via VPN connectivity using the Secure Remote Access service. PittNet is connected to the Internet and many public services are available without VPN connectivity, but access to private or secure services may only use VPN connectivity. University units must not configure any modem to support incoming connections other than facsimile

connections, which may be permitted with a device that is granted through the network firewall request process.

CSSD provides alternatives to access IP-restricted services. The installation of any type of device that allows the sharing of a single IP address by multiple devices compromises the operation of the network and must not occur. This includes proxy servers, personal routers, and residential network equipment. It is expected that each end-user device on PittNet will be configured with a single registered IP address from one of University's networks.

Wireless

University students, faculty, staff, and units may purchase the Wi-Fi certified wireless network interface adapters of their choice to connect end user devices to the University's wireless networks, but all wireless network access points or other wireless communications equipment to the/a University of Pittsburgh network must only be installed by CSSD.

University units will be required to remove any wireless network infrastructure equipment (Wi-Fi routers, and bridges) not installed by CSSD.

Wireless network access points will be connected to the University's wired network by means of a specially designated wireless port that is installed specifically for this purpose. University units and individuals may not disconnect a wireless access point from its associated wireless port or interfere with any components of the wireless AP assembly including antennas, antenna cables, or management cables. Wireless ports are specially configured to supply electrical power to the wireless access point and may cause permanent damage to an improperly connected device.

Wireless network installations at University locations consist of the necessary Wi-Fi certified wireless access point devices. The number of access points required will be determined by initial estimates of demand for users and the size of the area to be covered. Additional access points may be installed if the number of users to be served exceeds the practical number of users that can connect to single access point with sufficient bandwidth available to each user. In areas with a high density of users, such as classrooms and lecture halls, additional access points will be installed to satisfy the usage requirements. All wireless access point devices will be installed and maintained by CSSD.

Wireless Usage

Some services can have a negative impact on a wireless network because they generate a high level of activity on the network. Such services can negatively affect your wireless network performance and the network performance of other wireless users. The wireless network is a shared resource, which means the bandwidth available to each user of an access point will decline as high-bandwidth services are used. If a student, faculty member, or staff member has a need for a service that requires high bandwidth, a wired network connection should be used.

The following list provides examples of high bandwidth usage. Please note that this list is not all inclusive.

- Web servers
- Peer-to-peer file sharing servers
- FTP servers
- Multiplayer game servers

NOTE: You cannot use any computer connected to the wireless network as a server of any kind.

An unsecured computer may have problems that will also result in high bandwidth usage, including:

- Infections by worms or viruses
- Compromised systems running FTP, IRC, or other services or malicious spyware programs

Some activities may also use excessive wireless bandwidth. Following are some examples of user activities that consume high amounts of bandwidth:

- Reinstalling an operating system
- Downloading and installing applications
- Performing system backups
- Transferring large files (e.g., images, video, music, databases) to other system

Problems can occur if other devices use the same radio frequency range (2.4 GHz) as the wireless network. Because of the potential for conflicts, it is important for all users to understand which technologies are permitted in our environment and which are not.

In order to provide wireless network service at the highest level of quality, all non-client devices that use the 2.4 GHz range should be removed from service in any University building. Only devices that are part of the Wireless PittNet network will be permitted to use the 2.4 GHz range.

This includes any device that is used as a wireless base station or router, such as the Apple Airport Base Station, or any other wireless router. Cordless phones, cameras, and audio speakers that use the frequency band of 2.4 GHz or 5 GHz should also not be used in areas with wireless coverage.

Network Reliability

In order to ensure the reliable performance of the University's network, CSSD investigates reports of specific wireless devices that are suspected of causing interference and performance problems in the same manner in which CSSD investigates reports of specific devices connected to wired ports that are suspected of causing disruption. Although CSSD will not actively monitor content carried on the University's wireless network radio frequencies when investigating reports of potentially interfering devices, wireless network detection equipment will be used to detect unauthorized wireless network equipment. Units will be required to remove any such equipment found in unit-controlled University space.

Wireless access service is provided on the basis of anticipated utilization data gathered during initial site surveys conducted by CSSD. As the number of users increases, effective wireless network performance may be diminished.

Current industry standards for wireless network service do not provide sufficient throughput to effectively support bandwidth-intensive applications and network services. CSSD prohibits the use of serving-based applications (e.g., file, web, media servers) on Wireless PittNet.

CSSD will address problems encountered in the use of wireless network services according to the following priority list: public access, academic, research, administrative, and staff use.

Security

Access to the University's wireless networks will require all authorized users in all areas to authenticate to the network using his/her assigned University Computer Account username and password combinations through the use of University-provided wireless client software or 802.1x

supplicant. Network access logs are maintained and contain the username, time of access, and duration of use for all users who access the network using wireless connections. This information will be provided to authorized governmental authorities if the University is required to release such information.

Wireless technology deployed at the University of Pittsburgh includes the use of WPA (Wi-Fi Protected Access), which provides improved data encryption through the Temporal Key Integrity Protocol (TKIP) and user authentication through the Extensible Authentication Protocol (EAP). To provide additional security, all University wireless networks will require authentication of end users to the network upon connection of any wireless end-user device using an 802.1x supplicant or provided wireless client software. Each user will be required to authenticate to the network using his or her University Computer Account and password. The University's Central Directory Service is used as the basis for authentication to services, including wireless network access.

The use of WPA and 802.1x for user authentication will provide advanced security levels for the activities of University wireless network users. Now that Temporal Key Integrity Protocol (TKIP) and even Advanced Encryption Standard (AES), can be practically deployed, CSSD will stop supporting older, less secure security methods at some point in the future. Reports have been published demonstrating the weaknesses in the WEP protocol and stating that it should not be used to protect sensitive data, such as identifiable patient information, payroll, and student data. With the use of the newer and more advanced encryption mechanisms and user authentication protocols, these weaknesses are mitigated. Although the security of the wireless network is now as secure as the wired network, the University will prevent wireless access to these kinds of data when such data are stored on protected central services. Units using the wireless network in their areas for day-to-day operations will not be granted exceptions through the CSSD firewalls to gain native access to sensitive information via the Wireless PittNet without the use of a VPN (CSSD Secure VPN Service or IP Sec).

University students, faculty, staff, and units must follow the terms of all applicable University-acceptable use policies, network usage guidelines, and all applicable local, state, and federal regulations when using equipment connected to the University's network whether or not the individual is using wireless or wired network connections. Violations of such guidelines will be reported to the University's computer incident response team and may be forwarded to the appropriate University or governmental authorities.

University students, faculty, staff, and units are reminded that the use of wireless network connections may increase the risk that confidential information can be intercepted by unauthorized or unintended parties and that this risk in inherent in wireless network technology irrespective of security measures that can be implemented by the University. Users should avoid sending or receiving confidential or other sensitive data via wireless connections whenever possible.

CSSD Responsibilities

1. Development and maintenance of the network standard and network guidelines.

2. Installation and maintenance of all equipment supporting wired and wireless network service at the University of Pittsburgh.

3. Investigation and resolution of communication interference problems.

4. Deployment, management, and configuration of network access in public areas, classrooms, and office areas.

5. Development and implementation of network security protocols and practices.

6. Provision of user training on network security issues and acceptable use of network services.

7. Performance and security monitoring for all installed access points and provision of performance statistics to University units upon request.

8. Monitoring of the development of network technologies and evaluation of their potential use within the University's network infrastructure.

9. Responding to problems reported to the Technology Help Desk in accordance with standard procedures and levels of service.

University Network User Responsibilities

1. Adherence to the wired and wireless network standards and related guidelines and policies established by the University of Pittsburgh.

2. Implementation of recommended security software, hardware settings, patches, and protocols on end-user equipment used to access the University's networks.

3. Following all relevant University policies and procedures along with federal, state, and local laws pertaining to the security of sensitive and confidential data when working with such data on the University's networks.

4. Installation of network interface adapters according to published instructions.

5. Assumption of responsibility for support and troubleshooting of problems when using network interface adapters not supported by CSSD.

6. Immediately reporting known misuse or abuse of the network or associated equipment to the Technology Help Desk.

Network Management

Devices attached to PittNet must implement all required security measures to protect data stored within the device. This security cannot be based on access security provided by PittNet. The network device must use a scheme such as unique user identifiers and passwords. Users of the network must not divulge or otherwise use any information obtained through the network via monitoring of the network.

In order to ensure the fair use of network resources by all members of the University community, CSSD must take steps to identify devices that adversely affect PittNet. CSSD will attempt to notify the unit responsible for the offending device to correct the problem. In extreme situations, the network access point to which the offending device is attached may be disconnected until the unit or individual can demonstrate that the problem has been resolved. Upon disconnecting a network port for this reason, CSSD will notify both the individual using the network access point and the unit administrator of the unit in which the network access point is located.

CSSD is responsible for the University's external connectivity to the Internet and Research Networks (I2, NLR). CSSD reserves the right to selectively block any traffic that does or may have a harmful effect on Internet connectivity, enterprise systems that represents a security threat to the University network, or systems that comprise the University network. This applies to all PittNet traffic including internal, outgoing, and incoming.

Units may wish to use network management tools to manage the devices under their control. Units must not use network management tools to discover or attempt to manage network devices under the control of any other unit. The use of network traffic monitoring and analysis devices by anyone other than designated CSSD staff impedes the network operation and must not occur.

Non-University Networks

Network users must abide by the rules set by the governing body of each external network when a University network user is using that external network.

Misrepresentation in Electronic Communication

Network users must not misrepresent or hide their identities in all forms of electronic data communication, both inside and outside of the University.

Definitions

Wireless Access Point

A wireless communications hardware device that creates a central point of wireless connectivity. A wireless access point behaves much like a “hub” in that the total bandwidth is shared among all users for which the device is maintaining an active network connection.

Wireless Port

A network port that has been installed for the purpose of connecting a wireless access point to the University’s wired network. Wireless ports provide both data and power service to the wireless access point and are clearly distinguished from ordinary network ports by an affixed yellow warning label. Because wireless ports carry both data and electrical power, ordinary end-user devices could be severely damaged if they are connected to this type of port.

Wireless client software or built in 802.1x supplicant

CSSD provides client software client that allows for a computer to utilize 802.1x authentication to the wired and wireless networks. Some operating systems have built-in support for 802.1x and can be used for accessing the University’s networks. The University-provided client software will be preconfigured to support the specific setup for Wireless PittNet.

Coverage Area

The geographical area in which an acceptable level of wireless connection service quality is attainable. Coverage areas for similar devices can vary significantly due to the presence of building materials, interference, obstructions, and access point placement.

Interference

Degradation of a wireless communication radio signal caused by electromagnetic radiation from another source including other wireless access points, cellular telephones, microwave ovens, medical and research equipment, and other devices that generate radio signals. Interference can either degrade a wireless transmission or completely eliminate it entirely depending on the strength of the signal generated by the offending device.

Privacy

The condition that is achieved by successfully maintaining the confidentiality of personal, student, employee, and or patient information transmitted over a wireless network.

Security

Security is particularly important in wireless networks because data is transmitted using radio signals that, without implementation of specific data-encryption mechanisms, can easily be intercepted.

Wireless Network Infrastructure

The collection of all wireless access points, antennas, network cabling, power, ports, hardware, and software associated with the deployment of a wireless communication network.

Wired Equivalent Privacy (WEP)

A security protocol for wireless networks defined within the 802.11b standard. WEP is designed to provide the same level of security as that of a wired network. Recent reports indicate that the use of WEP alone is insufficient to ensure privacy unless used in conjunction with other mechanisms for data encryption.

WPA

Short for Wi-Fi Protected Access, a Wi-Fi standard that was designed to improve upon the security features of WEP. This technology features improved data encryption through the Temporal Key Integrity Protocol (TKIP) and user authentication through the Extensible Authentication Protocol (EAP), PEAP – MSChapV2. Wireless PittNet utilizes the WPA protocol.

802.1x

This standard enhances the security of local area networks by providing an authentication framework allowing users to authenticate to a central authority, such as LDAP or Active Directory. In conjunction with 802.11 access technologies, it provides an effective mechanism for controlling access to the wireless local area network.

802.11a

An extension to the 802.11 standard developed by the IEEE for wireless network technology. 802.11a applies to wireless local area networks and supports a maximum connection rate of 54 Mbps throughput in the 5GHz band. This specification is not backwardly compatible with 802.11b/g and requires special wireless adapters.

802.11b

An extension to the 802.11 standard developed by the IEEE for wireless network technology. 802.11b applies to wireless local area networks and supports a maximum connect rate of 11 Mbps with fallback to 5.5, 2, and 1 Mbps in the 2.4GHz ISM band. This standard was ratified in 1999.

802.11g

An extension to the 802.11 standard that allows for a maximum connect rate of 54 Mbps while maintaining compatibility with the 802.11b standard in the 2.4Ghz band This specification is compatible and complimentary to the 802.11b standard.

802.11i

An extension to the 802.11 standard to provide improved security over that which is available under 802.11 extensions. This extension provides for improved encryption methods and for the integration of the IEEE 802.1x authentication protocol, as well as advanced encryption mechanisms such as AES (Advanced Encryption Standard) for an optional, fully compliant implementation of 802.11i

802.11n

Uses multiple transmitter and receiver antennas (MIMO) to allow for increased data throughput and range. This is not a ratified standard as of Dec 2006. Pre-standard hardware is commercially available and not compatible with Wireless PittNet.

Infrastructure Mode

The operating mode for wireless networks in which each end-user device is configured to associate with a wireless network access point through which network services are accessed.

Ad hoc Mode

The operating mode for wireless service in which end-user devices interact with each other in a "peer- to-peer" configuration. Ad hoc mode does not require the use of a wireless network access point.

III. REFERENCE

Policy 10-02-05, Computer Access and Use