

BROOKHAVEN NATIONAL LABORATORY

SBMS Interim Procedure

Interim Procedure Number: 2004- 003

Revision: 0

Title: Deployment and Management of 802.11 and Related Wireless Standards

Point of Contact: Kathleen P. Hauser

Management System: Information Resource Management System

Effective Date: September 20, 2004

Expiration Date: November 30, 2004

Approved by (Line Management, Management System Steward): Kathleen P. Hauser, Thomas Schlagel

Approved by (Deputy Director, Operations): Michael Bebon

Applicability: All Employees, Guests, System Administrators, and Management

General

The purpose of the wireless policy and related standards and guidelines is to assure that Brookhaven National Laboratory's (BNL's) employees, guests, and contractors have access to a reliable, robust, and integrated wireless network, and to increase the security of the campus wireless network to the extent possible.

This document describes how wireless technologies are to be deployed, administered, and supported at BNL. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Cyber Security are approved for connectivity to BNL's networks.

This procedure addresses wireless access points (APs) connected to Brookhaven's network.

Note: Wireless access points and client systems (desktop, laptop, handheld-, portable-, or other computing devices) are prohibited in Limited Areas.

Campus and Visitor Wireless Zones

Wireless APs, by default, will reside on BNL's *Visitor Wireless Zone*. Cyber Security will review, case-by-case, all wireless APs that must reside on the BNL *Campus Wireless Zone* because of operational needs.

All wireless APs connected to the Brookhaven network must be registered through the Cyber Security Management Information System (CSMIS) before installation.

APs will be scanned for vulnerabilities to assess the needed base level of security relevant to the network.

Wireless subnets will be isolated by a firewall from the rest of the BNL network to restrict access to network resources and allow logging. All well-known exploits will be blocked with firewall rules.

Client systems accessing the BNL Visitor Wireless Zone must have antivirus software and up-to-date patches.

Campus Wireless Zone

Client systems accessing the BNL Campus Wireless Zone must follow all the same guidelines for access to the network as for the wired Local Area Network (LAN) including, but not restricted to, network registration, antivirus software, up-to-date patches, and strong passwords that comply with the [BNL Password Policy](#).

Approved Technology

To ensure that technical coordination is in place to provide the best possible wireless network for the Laboratory, the Information Technology Division will centrally manage the procurement, installation, operations, and maintenance of wireless APs.

All new wireless access points must use Brookhaven-approved vendor products and security configurations. To retain legacy wireless APs on the BNL Wireless Campus Zone, users must apply for an exception to this policy via the CSMIS at <http://intranet.bnl.gov/itd/reg/waprequest.asp>.

Campus and Visitor Wireless Zones - All wireless APs shall support controlled remote management; SNMPv3 will be used when available, and SSL for web-based management. Wireless APs shall be managed from the wired-LAN only. Wireless routers are not permitted on the network. Wireless APs shall not run Network Address Translation/Port Address Translation. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. Clients requiring the Dynamic Host Configuration Protocol (DHCP) service must use the normal DHCP server for BNL's networks.

Authentication

Visitor Wireless Zone - While the Wireless Visitor Zone will, by default, be unencrypted, individual departments may request their own encrypted enclave on it after being approved by the CSMIS.

Wireless Campus Zone - To comply with this policy, wireless implementations must maintain point-to-point hardware encryption with state-of-the-art technology (at least 128 bits). All systems must support and employ strong user authentication, authorization, and accounting that checks against an external database, such as the TACACS/ RADIUS server.

Setting the Service Set Identifier (SSID)

The SSID shall not contain any identifying information about the organization, such as the employee's name or product identifier.

Exceptions

The Cyber Security Office may grant specific exceptions to this policy to address needs that are not adequately provided for by the Campus and Visitor Wireless Networks, or for other reasons that Cyber Security deems appropriate. Requests for exceptions must be detailed and documented via the CSMIS and must justify the waiver. The Cyber Security Office makes all decisions about exceptions to the wireless policy.

Responsibilities of Requestor

The following steps must be taken to apply for approval to have a wireless AP installed:

- Contact the Help Desk at itdhelp@bnl.gov or at ext. 5522. The Help Desk first will determine if a wireless AP already is located in the physical area where the requestor is asking for it to be installed. If so, the Help Desk then will assist the requestor in getting connected to it. If there is no wireless AP, the Help Desk will respond by routing a service call to the ITD Network Services.
 - If the request is to locate an AP in the range of an existing AP within an encrypted enclave, and the requestor is not a member of the group, the requestor may not be allowed to use it. At this point, the Help Desk will fulfill the request for the AP.

- The Network Services then will contact requestor to review the request. If it is to install the wireless AP in BNL Campus Wireless Zone, the requestor must apply for a waiver through the CSMIS at <http://intranet.bnl.gov/itd/reg/waprequest.asp>,
- Once approval is received, Network Services (ITD/WAP Administrator) will register and install the wireless AP.

Responsibilities of the ITD WAP System Administrator

The Administrator will undertake the following tasks:

- Change the Wireless AP default SSID; examine and change all other default parameters.
- Manage the 128-bit access keys.
- Ensure that wireless APs are properly registered at <http://intranet.bnl.gov/itd/reg/wapreg.asp>
- Ensure that exceptions are processed and approved before installation.
- Ensure all wireless APs comply with stated policies.

Responsibility of Chief of Cyber Security

- Review and approve waivers for exception to the policy.
- Conduct regular “compliance checks” on all wireless APs on the Campus network.
- Conduct periodic penetration tests and audits on all wireless APs.
- Carry out periodic sweeps of the Laboratory network to locate unregistered rogue access points.
- Disconnect these access points from the network until they are properly approved, and also any access point used for irresponsible, inappropriate or illegal activity based upon the [BNL Personal User Agreement](#).

Questions about requirements within this document can be directed to the ITD Help Desk (itdhelp@bnl.gov or Ext. 5522), to Cyber Security Operations (security@bnl.gov) or to the Cyber Security Office (Ext. 2223).

Definitions

BNL Network - BNL's Network includes the backbone network and all Local Area Networks at the Laboratory funded by BNL, the DOE, or collaborators.

Client Systems (hardware/software) - The equipment and software that is installed in a desktop, laptop, handheld-, portable-, or other computing device.

Campus Wireless Zone – The zone that accommodates wireless devices in the internal Campus Zone. It allows users to connect directly to the internal BNL network without using VPN access.

Media Access Control (MAC) - This is a unique hardware identifier for each individual device or device interface on a network.

Network Address Translation (NAT) – This is a mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating them into globally routable address space. It is also known as a Network Address Translator.

Port Address Translation (PAT) – The function of PAT is similar to that of NAT, but here data from different IP addresses are altered so that they can share the same source IP address. To ensure that the data is still distinguishable (and the replies can be routed back correctly), the source port is varied in some defined way. Again, if NAT means Translation rather than Translator, omit “a” in front of NAT and PAT.

SSID – A Service Set Identifier is a name that identifies a wireless network. All devices on a specific wireless network must know its SSID.

User Authentication - A method verifying that the user of a wireless system is a legitimate user, independent of the computer or operating system being employed.

Visitor Wireless Zone – A zone that allows persons using laptop computers equipped with wireless network cards to connect to the Visitor Network without needing to physically attach to the network, and with the capability to access the internal BNL Campus Zone via a VPN. Public access points are generally located in areas accessible to all people, and are usable by all members of the Brookhaven community.

Wireless Access Point - Any piece of equipment that allows wireless communication using transmitters and receivers. These devices act as hubs and allow communications to the campus network.

Wired Equivalent Privacy – This is a system used to encrypt and decrypt data signals transmitted between Wireless LAN devices.