pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Wireless LAN Technology

ITP Number	***Effective Date***
ITP-NET001	11/13/2012
Category	***Supersedes***
Network Infrastructure	
Contact	***Scheduled Review***
ra-itcentral@pa.gov	December 2015

1. **Purpose.** The purpose of this Information Technology Policy (ITP) is to establish enterprise-wide standards for Wireless Local Area Network (LAN) Technology and their secure usage in a production environment. The objectives for uniform implementation of Wireless LANs and assurance of information security are to protect confidentiality of information, to safeguard the integrity of information, to establish common equipment platforms, and to ensure appropriate access to information.

2. **Scope.** This ITP applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP to ensure they design and implement wireless LANs that facilitate enterprise-wide interoperability and standardization.

3. **Definitions.**

Access Point (AP): WLAN transmitter/receiver that acts as a connection between wireless clients and wired networks.

Client: Wireless device that accesses the WLAN; can be a computer, PDA, or other hand-held device with a wireless connection.

Controller: Network device which controls the access points within a wireless network.

GHz: The GHz, or Gigahertz, is a unit of either electromagnetic or alternating current wave frequency equal to one billion hertz. The GHz is most commonly used to determine the frequency of ultra-high frequency (UHF) and microwave electromagnetic signals. GHz is also used in some computers to reflect microprocessor clock speed.

Guest Wireless: A wireless implementation where the agency uses OA's wireless controller for access to the Internet only.

IEEE (Institute of Electrical and Electronics Engineers): The IEEE is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. Through its members, the IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace and consumer electronics, among others.

Lobby Ambassador: Individual capable of creating guest wireless accounts.

Local Area Network: A Local Area Network (LAN) is a network that connects computers, printers and perhaps other devices within a department, building or house.

Mbps: Millions of bits per second, or Megabits per Second (Mbps), is the measurement of bandwidth on a telecommunication medium. Bandwidth is also sometimes measured in Kbps (kilobits per second), or Gbps (billions of bits per second).

RF (Radio Frequency): Radio Frequency (RF) refers to alternating current that if put into an antenna, would produce an electromagnetic field suitable for wireless broadcasting and/or communications. The frequencies cover a large portion of the electromagnetic radiation spectrum, varying from 9 kHz, the lowest allocated wireless frequency, to several thousand GHz. When an RF current is placed into an antenna, it creates an electromagnetic field that broadcasts through space. All RF fields have wavelengths inversely proportional to their frequency.

Secure Wireless: A wireless implementation where the agency uses its own wireless controller for access to the internal Commonwealth network as well as the Internet.

SSID (Service Set Identifier): Identifies and specifies which 802.11 network is being joined.

WEP (Wired Equivalent Privacy): An inferior security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b that was designed to provide a WLAN with a moderate level of security.

WPA (Wired Privacy Access): A security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i, that is designed to provide a WLAN with a level of

security and privacy comparable to what is usually expected of a wired LAN.

WPA2 (Wi-Fi Protected Access version 2): A security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i, WPA2 uses AES (Advanced Encryption Standard), meaning it can now meet the government's FIPS (Federal Information Processing Standard) 140-2 security requirements.

4. Objective. This ITP provides minimum requirements applicable to the design, installation and operations of Wireless Local Area Network (WLAN) equipment and systems for use in the Commonwealth of Pennsylvania (CoPA) enterprise network. The standards specified in this guide have applicability across all current standard technology and are to be used for all WLAN Technology implementation.

5. Policy. All new wireless LAN technology implementations are required to comply with the standards and operational guidelines set forth in sections 6 and 7 of this ITP.

6. Standards.

Current

These technologies meet the requirements of the current architecture and are recommended for use.

Technology	Platforms	Technology Classification
Network 802.11g	Any	Current
Network 802.11i	Any	Current
Network 802.11n	Any	Current
Network 802.11ac	Any	Current

Contain

These technologies no longer meet the requirements of the current architecture and are not recommended for use. They are no longer being deployed, and are to be phased out over time. No date has been set for their discontinuance.

Technology	Platforms	Technology Classification

Retire

These technologies are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as a lack of vendor support.

Technology	Platforms	Technology Classification

Network 802.11a	Any	Retired
Network 802.11b	Any	Retired
Network - Unapproved or undocumented	Any	Retired
All other non-WPA2	Any	Retired

Emerging / Research

Emerging technologies have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request. Research Technologies are less widely accepted and time will determine if they become a current standard.

Technology	Platforms	Technology Classification

7. Operational Requirements

Operational Requirements provides the minimum requirements applicable to the design, installation and operations of Wireless Local Area Network (WLAN) equipment and systems for use in the Commonwealth of Pennsylvania (CWOPA) enterprise network. The requirements specified have applicability across all current standard technology and are to be used for all WLAN Technology implementation.

The list below provides a brief description of the content and purpose of the sections follow:

WLAN Technology Overview: This section provides a high-level overview of acceptable WLAN Technology for use on the CoPA network.

Engagement Process: This section provides the user with the methods and process for approval to implement a WLAN infrastructure in the CoPA Enterprise environment.

Equipment Standards and Specifications: This section provides direction regarding minimum specifications and features that are to be included when purchasing WLAN equipment for use in the CoPA Enterprise network.

Network and System Design: This section provides the site survey requirements necessary to comply with ITP-NET001 *Wireless LAN Technology*.

Installation: This section provides the vendor and IT professionals with guidance on implementing a secure WLAN installation.

Operations: This section provides guidelines on the continuing use of WLAN technology in the CoPA Enterprise Network.

WLAN Technology Overview

Purpose

The purpose of this section is to provide a high-level overview of the 802.11 series of standards for WLAN Technology to be followed for use on the CWOPA network.

Overview

802.11 refers to a family of specifications developed by the IEEE for WLAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several specifications in the 802.11 family:

- **802.11:** Supports bandwidth up to 2 Mbps and signals at 2.4 GHz.
- **802.11a:** Supports bandwidth up to 54 Mbps and signals at 5 GHz.
- **802.11b:** Supports bandwidth up to 11 Mbps and signals at 2.4 GHz.
- **802.11e:** Also known as IEEE 802.11e-2005, defines a set of Quality of Service enhancements for Wireless LAN applications.
- **802.11g:** Supports bandwidth up to 54 Mbps and signals at 5 GHz. 802.11g is backwards compatible with 802.11b.
- **802.11i:** Defines security mechanisms, specifically WPA2, for wireless networks.
- **802.11n:** Supports bandwidth up to 600 Mbps and can signal at 2.4 GHz or 5 GHz. 802.11n is backward compatible with 802.11g.
- **802.11mb:** Also known as 802.11-2012, combines 10 minor 802.11 amendments (k, r, y, n, w, p, z, v, u and s).
- **802.11ac:** Supports bandwidth up to 6.9 Gbps and signals at 5 GHz.

The 802.11 standards are the basis of this ITP. The various standards provide guidance for design and implementation of the security features that are needed in order to deploy a successful WLAN in the agency. Since the standards were ratified, most vendors now have product items that meet most, if not all, of the latest requirements for securing a WLAN in the enterprise, and work with both open source

and proprietary operating systems.

Engagement Process

Purpose

The purpose of this section is to provide the methods and process for approval to implement a WLAN infrastructure in the CWOPA Enterprise environment.

General

Step One:

Agencies having a business need to implement a WLAN segment are to submit a SERP request. This document will clearly state the installation requirements, equipment locations, and configurations. The SERP design will be reviewed by the Office of Administration, Office for Information Technology, Bureau of Infrastructure and Operations (OA/OIT/BIO).

Step Two:

If OA/OIT/BIO has given approval to move forward with this project, the next step is to complete a site survey. The complexity of the site survey can vary with the scope of the project.

Network and System Design

Purpose

This section provides the agency IT professional with an overview of the equipment needed, placement in the network, and the configuration specifics to make a secure WLAN connection on the network.

General

Key issues to consider:

Deploying a WLAN includes determining Radio Frequency (RF) coverage from a single access point (AP), ensuring sufficient capacity to support the user population and accounting for RF signal-loss factors.

Many APs will automatically decrease their data rates as the RF signal degrades because a lower-frequency signal is more likely to get through when there is interference. Additionally, one user associated at minimal Mbps will slow the entire group, since the AP will take longer to communicate with that user, taking bandwidth away from all other connected users.

To avoid degrading the performance for all users associated to an AP, consider setting minimum association rates that force users to associate with a new AP once their throughput falls below the minimum rate. By designing smaller cells with higher throughput, an enterprise-quality experience can be created.

The number of users and their applications are major drivers of bandwidth requirements. The network architect is to account for the number of users within the cell diameter of the AP. In a large office or where user density is high, smaller cells are to be designed to achieve a higher data rate, since walls and other objects will not naturally create the cells by attenuating or blocking the RF signal. With smaller cells, you will need to re-use frequencies more often and thus ensure that the channels do not overlap.

Because of several factors, actual throughput on a wireless system is much lower than the technology's specified data rate. For instance, with even a one-way transmission on a 54-Mbps system, the best possible throughput is approximately 30 Mbps.

A major difference between designing for wired and WLANs is the impact of objects on RF signals. Walls, doors, windows, and other fixed objects in the building will absorb RF signals, causing signal loss. The building construction also has an impact: Concrete absorbs more signal than wood.

Agency Responsibilities:

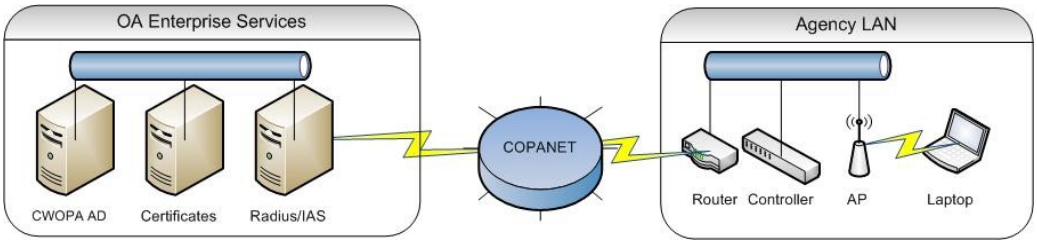
- Equipment – Agency is to purchase the WLAN devices (APs, secure controller and client cards.)
- Client wireless workstation is to reside within the Commonwealth of Pennsylvania active directory forest (CWOPA) domain or be a member of a resource domain that has a trust/relationship with CWOPA in order to receive the necessary security certificate.
- Authentication standardization – Agencies are to utilize Active Directory and Certificate Services provided by Office of Administration/Office for Information Technology, Bureau of Infrastructure and Operations (OA/OIT/BIO) Enterprise Certificate Authority to provision certificates.
- Naming Conventions – Devices are to follow the standardized naming convention of XXYYYY - XX is the two-letter agency code, and YYYY is the specific device name determined by the agency.
- For guest wireless, agencies send the MAC address of each AP to OA for authentication.
- For guest wireless, agencies will submit the name of an individual to OA who will be responsible for creating guest wireless accounts as the “Lobby Ambassador”.
    - The Lobby Ambassador is responsible for the creation, auditing and removal (as necessary) of user accounts.
    - Accounts should be time specific to the length required.
    - There are to be no shared/generic account user IDs and passwords. Each Guest Wireless user should have a unique user ID and password. This is required for accountability of usage.

Enterprise Responsibilities:

- Security/access control – OA/OIT/BIO will assign certificates through group policy.
- Configuration – OA/OIT/BIO can provide AP setup and configuration assistance as needed to enable Wireless Fidelity (WiFi), and client configuration.
- Certificate – Provided via auto enrollment to enable Extensible Authentication Protocol (EAP)-Protected EAP (PEAP) authentication.
- For guest wireless, OA/OIT/BIO will enter the AP’s MAC address into the guest wireless controller for authentication.
- For guest wireless, OA/OIT/BIO will enter the name of the agency individual who will be responsible for creating guest wireless accounts into the Network Control System.

Equipment Requirements:

- Computer accounts for wireless client devices are to reside within the CWOPA domain. This is necessary for the proper operation and distribution of security certificates required for secure network access.
- Wireless devices are to be IPv6 capable.



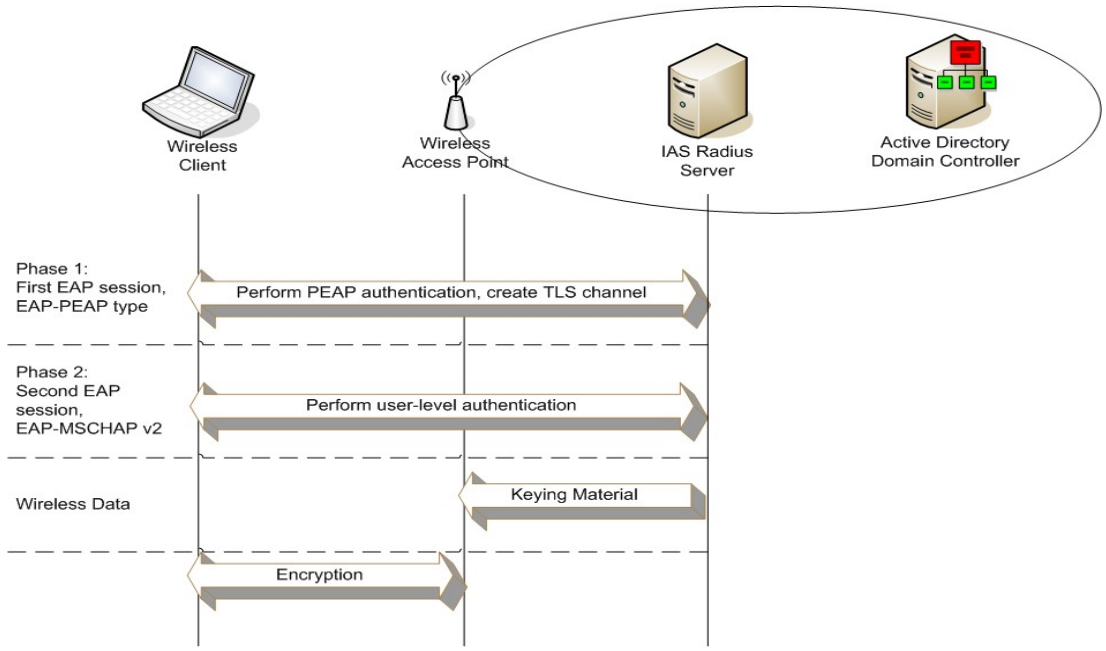
Encryption Standards and Specifications

The OA Exchange group will provide agencies with a centralized RADIUS and certificates-based solution leveraging the Windows platform that will also support group policy in the Active Directory structure now being used to authenticate CoPA users.

Each wireless laptop will receive a certificate issued by the Enterprise Certificate Authority via auto-enrollment at an enterprise level. The OA LAN Management group will add the user to a wireless certification group. The next time the user logs in, the certificate is automatically downloaded to their PC. Additional wireless settings can be configured through group policy at the agency level.

Authentication Process and Specifications

The process of authentication requires a user log-on to the network the same way if the user was sitting at a desktop machine in his/her office.



The process for authenticating using EAP-PEAP is designed to allow users to connect to their enterprise resources based on their CWOPA account information. In this design the wireless user can have secure access to the network from any location with a properly installed and configured WLAN connection.

Installation

Purpose

This section provides guidance on the installation of WLANs.

General

The OA/OIT/BIO Network Operations/Security will coordinate WLANs connecting to the enterprise network. This is required to secure the enterprise.

OA/OIT/BIO will maintain documentation of the WLAN site survey and installation plan. This is a standard industry best practice and will ensure that agencies located in the same physical location do not interfere with each other's wireless network.

Any conflict between wireless devices will be resolved, with assistance from

OA/OIT/BIO, to maximize general access.

Equipment is to be installed in a manner that minimizes interference with other RF activities. Security of data within and between agencies could be compromised, including, but not limited to, Health Insurance Portability and Accountability Act (HIPAA), Criminal History Record Information Act (CHRIA), Internal Revenue Service (IRS), and privacy information.

Equipment is to meet Wi-Fi Alliance certification standards and comply with FCC regulations.

Due to major security risks, clients' PC Cards will not be configured to act as an access point (ad hoc mode). Group policy will be needed to ensure compliance with the no ad-hoc rule.

Installation Plan

The installation plan is a timeline of the project showing the process of equipment installs, configurations, and testing.

Information to be included in installation plan:

- Network configuration document for your secure wireless implementation, including a network diagram that shows the firewalls, switches, IPs, protocols, MSEs, WCS, Controllers, APS, etc.
- A copy of the site survey that was conducted on this network (see below).
- Types of users who will be accessing this network and how will they be accessing it (laptops, tablets, smart phones, etc.).
- Written procedures for access control, user management, auditing, and rogue AP detection.
- Current ability to detect and block hacking attempts on the network.

- Identify the type of data that will be traversing the wireless network. If the agency intends on passing sensitive data across the agency managed Wireless network, additional regulatory compliance requirements may be in scope. If PII, HIPAA, CJIS, or any other sensitive type data transverses this network, a review of more stringent wireless controls may be in scope for a wireless security assessment. As such,

additional controls above and beyond those listed in the NIST-800-97, pages 8-3 to 8-19 wireless controls may be required.

Site Survey

Agencies planning to use this technology are to initiate a site survey and coordinate with OA/OIT/BIO to complete a project plan. Wireless equipment is to be placed in locations, and set to frequencies, that coordinate reasonably with other wireless mechanisms. Appropriate arrangements may include: base stations in protected closets, specialized antennae to provide required coverage of surrounding areas, and transmitter levels adjusted to avoid interference in high- density areas. Service interruptions, security issues, and data compromise could occur if not followed.

Any equipment not complying with this policy is prohibited.

Operations

Purpose

This section provides requirements applicable to the continuing use of WLAN networking in the CWOPA Enterprise Network.

General

Wireless services are subject to the same rules and policies that govern other communications services in the Commonwealth. Commonwealth standards are to be followed to guarantee network integrity and security.

Abuse, interference or disruption of authorized communications or unauthorized interception of WLAN traffic, by use of sniffers or intrusion programs is prohibited. Authorized agency security staff is permitted to utilize these products and devices to continue to audit and monitor their agency networks. It will be necessary for the agency staff to notify OA/OIT/BIO of these tests prior to the event, as a precaution and advisory.

Recommended configuration - Do not suppress Service Set Identifier (SSID)

The SSID (also known as a wireless network name) is by default included in the Beacon frames sent by wireless access points. Configuring the wireless access points to suppress the advertising of the SSID information element in Beacon frames does prevent the casual wireless client from discovering the wireless network. However, SSID suppression does not prevent the most unsophisticated hacker from capturing other types of wireless management frames sent by the wireless AP and determining the SSID.

If SSID suppression is desired, WLAN AutoConfig service will connect to the first preferred wireless network that is advertising its SSID, even though it is lower in the preferred networks list than a wireless network that is present but is not advertising its SSID. This behavior can produce confusing results when a Windows- based wireless client using Wireless Auto Configuration is introduced into a wireless environment in which some wireless networks are advertising their SSID and some are not.

Auditing

Agencies have the responsibility to ensure they are themselves compliant with not just our ITP's but also any regulatory requirements pertaining to whatever data flows over their managed wireless networks. Any agency implementing their own secure wireless network will need to perform an assessment on the wireless network to show it has been set up correctly and in compliance with our ITP's and NIST 800-97, pages 8-3 to 8-19. The results should be sent to Office of Administration, Office for Information Technology, Enterprise Information Security Office (EISO).

EISO may perform follow up spot checks on approved agency managed wireless networks on an add-needed basis.

8. Related ITPs/Other References

NIST 800-97 – Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

9. Authority

Executive Order 2011-05, Enterprise Information Technology Governance

10. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov. Questions regarding this publication are to be directed to ra-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	04/22/2005	Creation of ITP
Revision	11/24/2008	Update to leverage the Enterprise Certificate of Authority
Revision	10/25/2010	Move 802.11n to current
Revision	12/20/2010	ITP refresh
Revision	08/01/2012	ITP refresh

Revision	12/30/2014	Added policy to limit the number of simultaneous connections using the same user name to COPA_GUEST wireless network (Agency Responsibilities) Removed “draft” from 802.11ac standard specification (Wireless LAN Technology Overview) and moved 802.11ac from research to current. Updated the WiFi Alliance logo Removed “Windows XP Wireless Auto Configuration” language, replaced with “WLAN AutoConfig service” in Section 7 (Recommended configuration - Do not suppress Service Set Identifier (SSID)) General formatting