

Standard ID:	AC-Wireless-001
Title:	Wireless 802.11 Architecture Standard
Domain:	Architecture
Discipline:	Network
Revision Date:	11/25/2013
Revision no.:	6
Original date:	7/1/2001

I. Authority, Applicability and Purpose

- A. **Authority:** Title 29, Chapter 90C provides broad statutory authority to the Department of Technology and Information (DTI) to implement statewide and inter-organization technology solutions, policies, standards, and guidelines for the State of Delaware's technology infrastructure. "Technology" means computing and telecommunications systems, their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information or data electronically. Technology includes systems and equipment associated with e-government and Internet initiatives.
- B. **Applicability:** This applies to all State of Delaware communications and computing resources. DTI is an Executive Branch Organization and has no authority over the customers in Legislative and Judicial Branches, School Districts, and other Federal and Local Government entities that use these resources. However, all users must agree to abide by all policies and standards promulgated by DTI as a condition of funding and continued use of these resources.
- C. **Purpose:** The purpose of this standard is to ensure that all access points are secure before attaching to the existing network. The main considerations should be classification of use, intended user, and network security.

II. Scope

- A. **Audience:** Project Leaders, Application Developers, Systems Administrators, Network Administrators, IT Security Personnel, Computer Auditors, and their managers and application development contractors for the State are the intended audience. IT personnel are the only intended users of this document.
- B. **Applicability:** This standard will cover all systems installed or in use by the State and will include installations owned by the State and housed by third-party contractors.
- C. **Environments:** Any device that uses 802.11 to connect to data or voice networks.

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.

III. Process

- A. **Adoption:** DTI adopted these standards through the Technology and Architecture Standards Committee (TASC). They are applicable to all Information Technology use throughout the State of Delaware.
- B. **Revision:** Technology is constantly changing. It is the intent of TASC to review each standard yearly. Your Information Resource Manager (IRM) will channel your suggestions and comments to TASC.
- C. **Contractors:** DTI requires all contractors or other third parties to comply with these standards when proposing technology solutions to other State entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a non-rated component, contact TASC at dti_tasc@state.de.us.
- D. **Implementation responsibility:** DTI and/or the organization's technical staff will implement this standard during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.
- E. **Enforcement:** DTI will enforce this standard during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. This standard may also be enforced by others during the course of their normal business activities, including audits and design reviews.
- F. **Contact us:** Please direct any questions or comments to dti_tasc@state.de.us.

IV. Definitions/Declarations

- A. **Definitions:**
 - 1. **Wireless Systems Architecture:** The design of IT solutions into isolated and independent platforms so that interoperability, security, scalability, and change are accomplished. The architecture of a complex system is analogous to the infrastructure of a highly evolved social system or biological organism. The absence of an architecture may nonetheless result in something we all identify as architecture. It is a trivial matter to make a design that can accommodate some change that was explicitly expected by the designer. However, how do we design to accommodate unexpected change? This is the central technological challenge of system architecture. System architecture is expensive, but probably not as expensive as its absence. Today we have the capacity to build successful architectures, but often not the will.
 - 2. **Systems Administrator:** The person responsible for running and maintaining a computer system especially a mainframe, minicomputer, or local area network. System administrators (sometimes called network administrators) issue login names, maintain security, fix failures, and advise management about hardware and software purchases.
 - 3. **IEEE:** The **Institute of Electrical and Electronics Engineers** or **IEEE** (pronounced as eye-*triple-e*) is an international non-profit, professional organization for the advancement of technology related to electricity. To learn more about this organization, click on the link to their web site <http://www.ieee.org>.

4. **IEEE 802.11:** A set of standards for [wireless local area network](#) (WLAN) computer communication, developed by the [IEEE](#) LAN/MAN Standards Committee ([IEEE 802](#)) in the 5 GHz and 2.4 GHz public spectrum bands. Although the terms 802.11 and [Wi-Fi](#) are often used interchangeably, the [Wi-Fi Alliance](#) uses the term Wi-Fi to define a slightly different set of overlapping standards.

5. **802.11 Family:**

Protocol	Release Date	Op. Frequency	Throughput (Type)	Data Rate (Max)	Range (Radius Indoor) Depends, # and type of walls	Range (Radius Outdoor) Loss includes one wall
Legacy	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s	~20 Meters	~100 Meters
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	~38 Meters	~140 Meters
802.11n	2009	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s	~70 Meters	~250 Meters

6. **WEP (Wired Equivalent Privacy):** An optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy confidentiality.

7. **WPA (Wi-Fi Protected Access):** Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products enabled with WEP (i.e., as a software upgrade to existing hardware). The WPA technology includes two improvements over WEP:

- 1) **Improved Data Encryption** - WPA offers improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature, which ensures that the keys haven't been tampered with.

- 2) **User Authentication** - WPA employs a more secure user authentication process over WEP. WPA enhances user authentication through the use of the extensible authentication protocol (EAP). EAP is a more secure public-key encryption system that limits access to the network to only those network users that are authorized. WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. .
8. **WPA2 (Wi-Fi Protected Access 2):** Follow-on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the IEEE 802.11i standard, WPA2 provides government-grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm and 802.1x-based authentication [adapted from Wi-Fi.org]. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.
9. **PEAP --** Pronounced "peep" and short for **Protected Extensible Authentication Protocol**: Protocol developed jointly by Microsoft, RSA Security and Cisco for transmitting authentication data (including passwords) over 802.11 wireless networks. PEAP authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The tunnel protects the subsequent user authentication exchange. PEAP and EAP-TTLS makes it possible to authenticate wireless LAN clients without requiring them to have certificates.
10. **RADIUS (Remote Authentication Dial-In User Service):** RADIUS Centralized User Authentication is provided between the wireless client and the RADIUS server, in conjunction with the IEEE 802.1x standard-based network log-in. Any RADIUS supporting AES, EAP-MD5, EAP-TLS, EAP-TTLS can be implemented in conjunction with 802.1x to provide a secure authentication solution for wireless clients.
11. **AAA (Authentication, Authorization and Accounting):** A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.
- 1) **Authentication** is the process of identifying an individual, usually based on a username and password. Authentication is based on the idea that each individual user will have unique information that sets him or her apart from other users.
 - 2) **Authorization** is the process of granting or denying a user access to network resources once the user has been authenticated through the username and password. The amount of information and the amount of services the user has access to depend on the user's authorization level.
 - 3) **Accounting** is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent in the network, services accessed while there, and amount of data transferred during the session.

AAA services often require a server that is dedicated to providing the three services listed directly above. RADIUS is an example of an AAA service.

- 12. AES (Advanced Encryption Standard):** A Federal Information Processing Standard (FIPS), specifically, [FIPS Publication 197](#), that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information. National Institute of Standards and Technology (NIST) anticipates that the AES will be widely used on a voluntary basis by organizations, institutions, and individuals outside of the U.S. Government - and outside of the United States - in some cases.
- 13. EAP (Extensible Authentication Protocol):** EAP is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

In wireless communications using EAP, a user requests connection to a WLAN through an Access Point (AP), which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication.

- 14. EAP-TTLS (Tunneled Transport Layer Security):** An EAP protocol that extends TLS, is widely supported across platforms, and offers very good security. The client does not need to be authenticated via a CA-signed PKI certificate to the server, but only the server to the client. This greatly simplifies the setup procedure since a certificate does not need to be installed on every client.

After the server is securely authenticated to the client via its CA certificate, the server can then use the established secure connection (tunnel) to authenticate the client. It can use an existing and widely deployed authentication protocol and infrastructure, incorporating legacy password mechanisms and authentication databases, while the secure tunnel provides protection from eavesdropping and man-in-the-middle attack. Note that the user's name is never transmitted in unencrypted clear text, thus improving privacy. EAP-TTLS is being considered by the IETF (Internet Engineering Task Force) as a new standard.

- 15. PSK Pre-Shared Key:** A secret that was previously shared between the two parties using a secure channel before it needs to be used. Such systems almost always use symmetric key cryptographic algorithms. The characteristics of this secret or key are determined by the system that uses it. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems (e.g., in Wi-Fi encryption such as WEP or WPA). Since one weak point of the crypto system is the encryption algorithm's key, the strength of the key is important. Since the strength of a key is in part dependent on its length, it is important to choose a key that is secure.
- 16. TKIP Temporal Key Integrity Protocol:** Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm. Adding an integrity-checking feature ensures that the keys haven't been tampered with.
- 17. IEEE 802.1x: Port-Based Network Access Control**
- 802.1x is a standard for authenticating wireless clients onto wireless 802.11 networks. It is a key feature in Microsoft's Windows XP operating system. Control needs to be implemented in conjunction with a centralized RADIUS authentication server supporting AES, EAP-MD5, or EAP-TLS. Authentication is central, rather than at each access point.

18. MS-CHAP-V2: Challenge Handshake Authentication Protocol, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value (or nonce), ID, and secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum, and compares the result with the value received from the peer. If the values match, the peer is authenticated.

By transmitting only the hash, the secret can't be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks.

19. ACL Access Control List: A set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it. The ACL is a list of each object and user access privileges; i.e., read, write, or execute.

20. VoIP Voice over Internet Protocol: A category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions of the public switched telephone network (PSTN). The network must be setup on separate VLAN with a firewall equivalent to restrict access only to the call manager, phone appliance, or PBX.

21. QoS Quality of Service: Capability of a network to provide better service to selected network traffic over various technologies such as Ethernet, 802.1 networks, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority service including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail. Fundamentally, QoS enables you to provide better service to certain flows. This is done by either raising the priority of a flow or limiting the priority of another flow when configuring wireless controllers.

22. End-to-End QoS Levels:

Service levels refer to the actual end-to-end QoS capabilities, meaning the capability of a network to deliver service needed by specific network traffic from end to end. The services differ in their level of *QoS strictness*, which describes how tightly the service can be bound by specific bandwidth, delay, jitter, and loss characteristics.

- a) **Best-effort service (Silver data)** - Also known as lack of QoS, best-effort service is basic connectivity with no guarantees. This is best characterized by FIFO queues, which have no differentiation between flows.
- b) **Differentiated service (Gold video)** - Some traffic is treated better than the rest (faster handling, more average bandwidth, and lower average loss rate). This is a statistical preference, not a hard-and-fast guarantee.
- c) **Guaranteed service (Platinum voice)** - This is an absolute reservation of network resources for specific traffic.

- 23. PBX:** Private branch exchange. Like any PBX, it allows a number of attached telephones to make calls to one another, and to connect to other telephone services including the public switched telephone network (PSTN).
- 24. AP (Access Point):** Hardware device that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.
- 25. WAN Wide Area Network:** Used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations.
- 26. WLAN Wireless LAN Controller:** Responsible for system-wide wireless LAN functions, such as security policies, intrusion prevention, RF management, and mobility. They work in conjunction with access points to support business-critical wireless applications.
- 27. Public NET:** Primary use is to provide for State owned public access terminals to access Internet facing State services. Wireless network devices are authenticated to the wireless network. Examples, Public access terminals at Public Archives for research or Department of Labor for job searches.
- 28. State NET:** Primary function of the State's Enterprise Wireless Network offering. A closed Network intended for State Employee access to computing resources located on the State Network. Access can be limited to resources within a user's home VRF. The client must be able to authenticate and be fully encrypted before network connectivity can be established.
- 29. Guest NET:** Part of State's Enterprise Wireless Network offering. An open network intended to provide Internet services to the public while visiting a state facility. This network requires no authentication but does require acceptance of end user agreement prior to having access. This network is isolated from State Networks.
- 30. Environment Classifications:**
- a) **Production:** This environment is the State of Delaware's live Transaction Processing environment; as such, this environment must be guarded and protected from corruption. Whatever is done must be auditable and controlled by application systems that have been approved by business managers.
- 31. DR/BCP Criticality Classifications:**
- a) **Critical (1)** – Loss of this business function threatens the ability for the state to operate. Loss of business function disrupts the security and well being of the state. Related business processes are generally defined as affecting statewide public safety or public health.
 - b) **Significant (2)** – Loss of this business function significantly reduces the effectiveness of the states operations. Loss of business function has a negative citizen impact and affects the financial well being of the State. Related business processes are generally defined as affecting statewide financials or state's economic base.
 - c) **Moderate (3)** – Loss of business function affects multiple State Organizations and their ability to operate. Loss of business function has a negative citizen impact and impacts a State Organization's mission critical business function. Related business processes are generally defined as mission critical at the department level.

- d) **Limited (4)** – Loss of business function is limited to only the person or State Organization using the application. Loss of this business function has little or no effect on the State's ability to carry out business. Related business processes are business critical to the division or business unit.
- e) **Minimal (5)** – Loss of business function does not have a direct impact on a State Organization's ability to do business.

DR/BCP Criticality	Business Continuity
Minimal, Limited	Stand alone access points.
Moderate	Centralized wireless LAN controller with multiple access points.
Significant, Critical	Provide redundancy by using multiple wireless LAN controllers to handle fail over of access points due to failure of hardware, causing network interruption.

B. Declarations

StateNet must be used where the requirement is to support State Employees access to state computing resources.

Guestnet must be used where the requirement is to provide Internet access for visitors at state facilities.

All other Wireless implementations must:

- Be approved by DTI;
- Be accurately documented and maintained on site;
- Be flexible, allowing for changes in technology, risk, and law;
- Provide security and privacy;
- Perform required functionality to maintain business continuity and enable recovery in the event of a disaster based on the classification availability (normal business, business critical or enterprise critical). Update your organization's Disaster Recovery/Business Continuity Plans and ensure that a wireless section is included if necessary;
- Comply with the [Enterprise Standards and Policies](#) and notably with the [Delaware Information Security Policy](#).

V. Definition of Ratings

Individual components within a Standard will be rated in one of the following categories. COMPONENT RATING	USAGE NOTES
<ul style="list-style-type: none"> • STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and can be expected to enjoy a useful life of 5+ years from the Effective Date. 	<p>These components can be used without explicit DTI approval for both new projects and enhancement of existing systems.</p> <p><i>(1) Note the useful life concern for the “Acceptable” rating.</i></p>
<ul style="list-style-type: none"> • ACCEPTABLE – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is stable, but has a useful life ⁽¹⁾ of less than 5 years from the Effective Date. 	
<ul style="list-style-type: none"> • EMERGING – DTI considers the component to be a likely candidate for future classification as STANDARD or ACCEPTABLE within the state pending further investigation. 	<p>These components must be explicitly approved by DTI for all projects. They must not be used for minor enhancement and system maintenance without explicit DTI approval.</p>
<ul style="list-style-type: none"> • DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete. 	
<ul style="list-style-type: none"> • LIMITED SUPPORT – DTI has limited or no internal support capability for the component; or has no arrangement for vendor support for the product. Users must arrange for adequate overall support of the component through their own efforts. 	
<ul style="list-style-type: none"> • NOT SUPPORTED BY DTI – DTI offers no internal support and has no arrangement for vendor support. Users must arrange for all support of the component through their own efforts. 	<p>No waiver requests for new solutions with this component rating will be considered.</p>
<ul style="list-style-type: none"> • DISCONTINUE – For reasons of overall risk, product support, high TCO, or other issues, the use of this technology is discouraged. All current instances of this technology should have a plan developed for its retirement. DTI expects to work aggressively with the users of such technologies to devise a collaborative plan. 	
<ul style="list-style-type: none"> • DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered. 	<p>No waiver requests for new solutions with this component rating will be considered.</p>

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.

- A. **Applicability of Ratings:** The ratings and usage notes are intended to encourage technology decisions to move toward components that enjoy the full support of DTI. However, acknowledging that mass replacement of lower rated components is not feasible, DTI will allow continued maintenance, enhancement, and possibly limited new development using these components. In making such determinations, DTI may require that the requestor demonstrate that they have adequate support arrangements in place.
- B. **Missing Components:** No conclusions should be inferred if a specific component is not listed. Instead, contact TASC to obtain further information.

VI. Component Assessments

A. Scope:

This document specifically addresses the 802.11a and 802.11g radio standards. The 802.11a standard is a 54mbps WLAN solution that operates in the UNI, 5.2 GHz, and the UNII, 5.8 GHz, radio bands. The 802.11g standard is a 54mpbs WLAN solution that operates in the ISM 2.4 GHz radio band, operates on the same channels as 802.11b, and is also backward compatible with 802.11b technology. Both 802.11a and 802.11g use the Orthogonal Frequency Division Multiplexing (OFDM) modulation technology. More information on the 802.11a, 802.11g, and OFDM technologies can be found at <http://www.ieee.org>.

Wireless LAN technology based on the 802.11b standard was not designed to run some of the more complex security algorithms found in the 802.11i standard, especially the Advanced Encryption Standard (AES). **802.11b equipment is no longer permitted in the State's network.** Only the 802.11a/g/n standards have the capability to run AES and are currently approved by DTI.

The IEEE has spent years developing a centralized security standard known as 802.11i that addresses and resolves the flaws in the originally deployed security solution of WEP. The 802.11i standard and how it is to be deployed using 802.11a/g/n wireless technology are addressed in this document. It is not practical or appropriate to use only physical means to control access to a wireless network as it is with a wired network due to extreme lack of security capabilities. The wireless signal is pervasive in spaces where the service is provided, and it is not physically obvious who is using the system. In addition to the wireless signal's ability to penetrate walls, floors, and buildings, this gives it a high degree of exposure, which requires more substantial security mechanisms.

State Organizations participating in the State Enterprise Wireless LAN solution, (StateNet and or GuestNet) they must coordinate with DTI before making purchases. State Organizations wanting wireless solutions beyond those to support user must consult and receive DTI approval.

B. Security:

Currently, most wireless products lack effective scalable security mechanisms in out-of-the-box solutions. However, by taking the appropriate steps and precautions, the implementation of WLANs can be configured to operate using multiple levels of security. Authentication, authorization, encryption, and spectrum management are the issues.

- a) **Authentication:** Authentication is one of the most stable and reliable means of providing security as long as the user name and password are user specific, and not shared throughout an entire group. 802.11 client authentication is to be performed via the 802.1x standard.

StateNet utilizes 802.1x standard via RADIUS.

- b) **Authorization:** Most access points include a feature known as an “Access Control List” or (ACL) that permits a network administrator or WLAN administrator to manage their wireless access points. Access control lists are now being used that require a username/password in order to gain access to a wireless network. An ACL can be maintained through either an access point or a RADIUS server. When performing maintenance, or installing a WLAN; configuration of the wireless access point should be performed through a secure means; e.g., https, SSH, or a similar protocol.

StateNet Access Points are managed through centralized controllers and are not directly accessible for the local networks.—Authorization through means of a username/password access control is required on all wireless solutions. Management of an access point must be done either through https, SSH or another secure protocol.

- c) **Encryption:** It is extremely important that an 802.11 network be encrypted to ensure all data being transmitted is secure. The AES algorithm should be deployed as defined in the 802.11i standard.

StateNet wireless utilizes 128-bit AES encryption. All wireless solutions except the State’s GuestNet are required to use encryption, 128-bit AES or stronger.

- d) **Spectrum Use:** The spectrum use will have to be regulated in order to prevent conflicts. The 2.4GHz spectrum should be reserved for wireless LAN use. DTI recommends use of channels 1, 6 and 11 to ensure non-overlapping channels. 802.11a technology that runs in the 5.2/5.8GHz spectrum has eight non-overlapping channels, so more wireless devices can operate in this frequency. But the same considerations as mentioned for the 2.4GHz solution should also be taken into account for the 5.2/5.8GHz technologies, since interference is still a possibility.
- e) **Violations:** DTI performs random scans of the State’s network on a daily basis. During these scans, it is possible to detect the presence of wireless networks. If an organization is found with a rogue wireless access point, or if they are not abiding with all of the standards in this document, then the organization or local IRM or network administrator will be notified of their site’s violation and requested to either take the access point offline or make the appropriate changes to be in compliance with the State’s standards. An organization will have 24 hours to bring their network into compliance. If this does not occur, the organization faces the possibility of being removed from the State’s network until they are in compliance.

VII. Conclusion

Wireless LAN technologies have matured to the point where it is now practical and secure to consider the technology as an extension of an organization's network. Wireless LANs are not intended to be installed to replace existing cabled networks, but are designed to operate as an extension of the wired network and enable features; i.e., the ability to roam and provide network presence in areas where cable may not be an appropriate solution.

State NET	Intended Use	Access	Minimum Level of Security
<p>State Enterprise Service.</p> <p>Submit request to DTI for approval. Can only be installed by DTI.</p>	<p>Primarily intended to allow the State employees access to computing resources located on the State Network. Can be used as a production platform. Employee Access can be limited to resources within a user's home VRF. The client must be able to authenticate and be fully encrypted before network connectivity can be established.</p>	<p>Allows only State employees access to the State network.</p> <p>Provides users access to resources within their assigned VRF.</p>	<p>Fully encrypted, 128-bit AES encryption, and 802.1x RADIUS authentication. MS-CHAP-V2, PEAP Certificate and user authentication require to connect to the Network.</p>
Public NET	Intended Use	Access	Level of Security
<p>Submit request to DTI for approval. Can only be installed by DTI.</p>	<p>Primarily intended to allow the public to access Delaware Internet sites for the purpose of completing documents required by the State such as registrations, permits, licenses, etc. The wireless network is accessible only to the public while they are in the State building. Can be used as a production platform.</p>	<p>Internet access only. Must not be able to access the State network.</p>	<p>The client must use some means of encryption between the client and the access point to ensure security/integrity of data. The minimum level of security must be 128-bit AES or stronger. WPA or WPA2 using PSK for data encryption must be used at all times.</p>
GuestNet	Intended Use	Access	Level of Security
<p>State Enterprise Service</p> <p>Submit request to DTI for approval. Can only be installed by DTI.</p>	<p>An open Network intended to provide Internet services to the public while visiting a state facility. This network requires no authentication but does require acceptance of an end user agreement prior to having access. This network is isolated from the State Networks.</p>	<p>Internet access only. Only outbound services supported.</p>	<p>Open access, no encryption. Access only requires acceptance of the End User Agreement.</p> <p>Service is firewalled and proxy isolated from the Internet.</p>

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.

Protocol	Rating	Comments
802.11a	Acceptable	Less area coverage per Access Point
802.11b	Disallow	Does not support AES; therefore is no longer allowed.
802.11g	Acceptable	Good area coverage per Access Point
802.11n	Standard	Best network throughput
802.11ac	Emerging	

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.