The following document provides details about the operation and configuration parameters for Penn State Wireless 2.0 and Visitor Wireless. It is intended for Penn State network administrators who are considering a new wireless assist LAN or are looking for information about how the services work. The document is divided into seven sections:

1. Concept of Operation
2. LAN Diagrams
3. VLAN Information
4. Network Security
5. Hardware Requirements
6. Administrative Requirements
7. Configuring a New Wireless Assist LAN

1. Concept of Operation

Penn State Wireless 2.0 provides two SSIDs on a single wireless LAN infrastructure. The "psu" SSID uses WPA2-Enterprise (AKA 802.11i) for authentication and encryption, while the "psuwirelesssetup" SSID is an open SSID used for client configuration and provides no access to the internet. Both SSIDs must be broadcast in order to minimize problems with client connections.

To segregate client traffic on the two SSIDs from each other as well as from management/RADIUS traffic, the wireless access point must tag each client's traffic with an appropriate VLAN based on the SSID to which that client is associated. Customarily, client traffic associated with the "psu" SSID is tagged with VLAN 991, and "psuwirelesssetup" client traffic is tagged with 993, but the need to isolate growing wireless networks means other VLANs may need to be used. Confirm the VLANs configured for your wireless assist connection with the TNS staff assigned with the delivery of wireless LAN interface.

Network management& RADIUS traffic must also be on its own VLAN. If the TNS wireless LAN interface will provide the wireless LAN hardware addresses, the customer must provide TNS with the subnet to be used & TNS will provide each customer with their own VLAN tag for that traffic. Customers whose wireless LAN hardware addresses are provided via some other network interface must provide their own VLAN tag. In that case the switch port connected to the TNS wireless LAN interface should not be a member of the management VLAN.

Each University Park hub site will have at least one TNS provided aggregation switch. All clients connected to the same SSID on a LAN connected to the same aggregation switch will share the same subnet. This architecture will mitigate the problem of wireless clients roaming between LANs with different subnets; however, due to rare instances at UP where adjacent buildings have fiber routed to different hub sites, the problem may not be totally eliminated. If you become aware of a situation where clients within a building roam between WLANs on different subnets, please contact the TNS NOC so that steps may be taken to eliminate the problem.

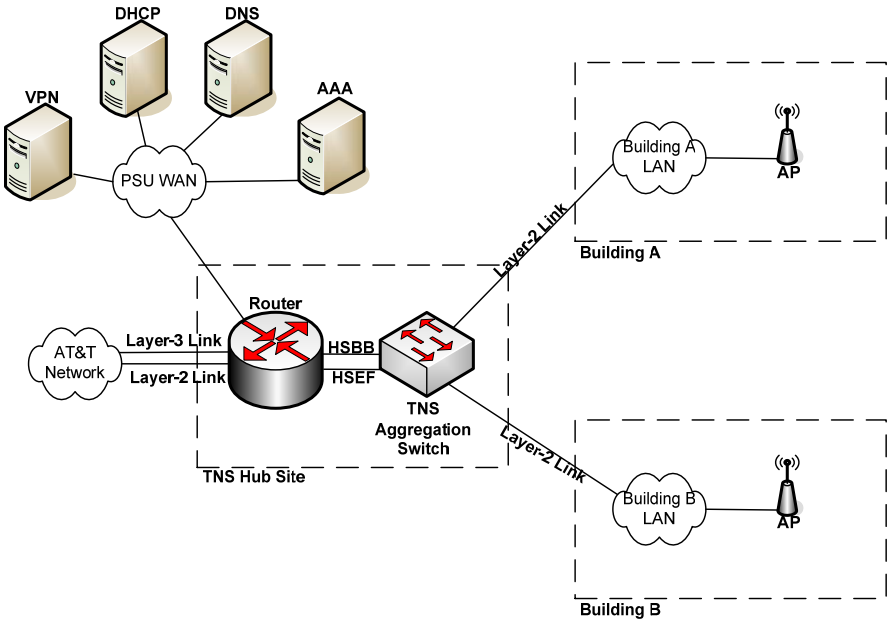
In addition to Penn State Wireless 2.0, the TNS wireless aggregation switches are capable of distributing Visitor wireless. When customers opt to include visitor wireless, the wireless LAN

must be able to support an additional VLAN/SSID pair. The SSID for Visitor wireless is "attwifi" and the VLAN tag is 360. This SSID must be broadcast.

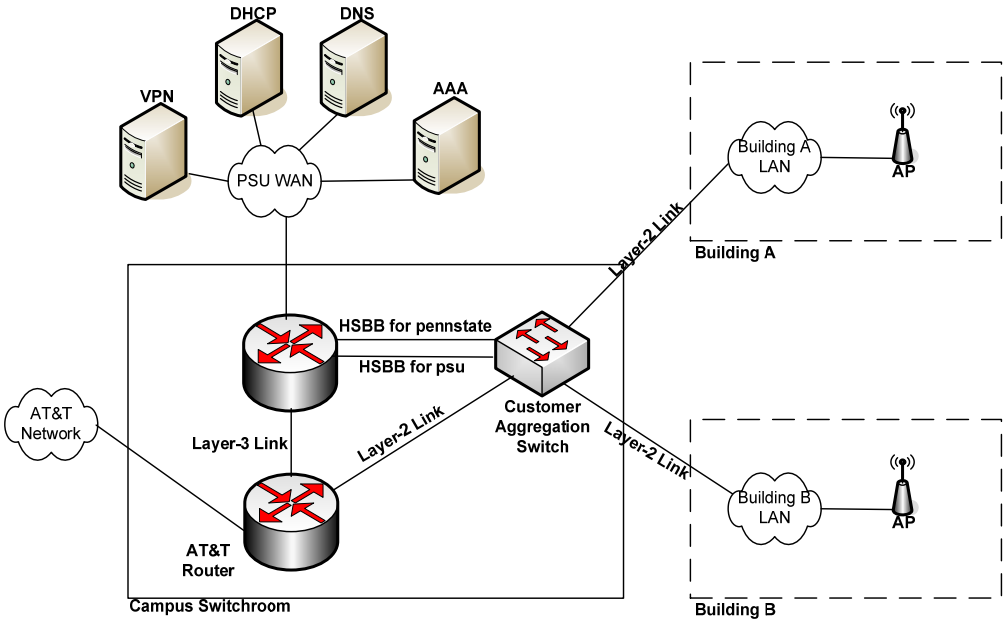
Finally, Wireless Assist LAN administrators are free to provide additional SSIDs on the same wireless LAN hardware provided those SSIDs comply with Penn State policies and client traffic does not use the TNS wireless LAN interface.

To further assist in understanding Penn State wireless 2.0, the following three diagrams show the physical architecture and logical architecture of the network.

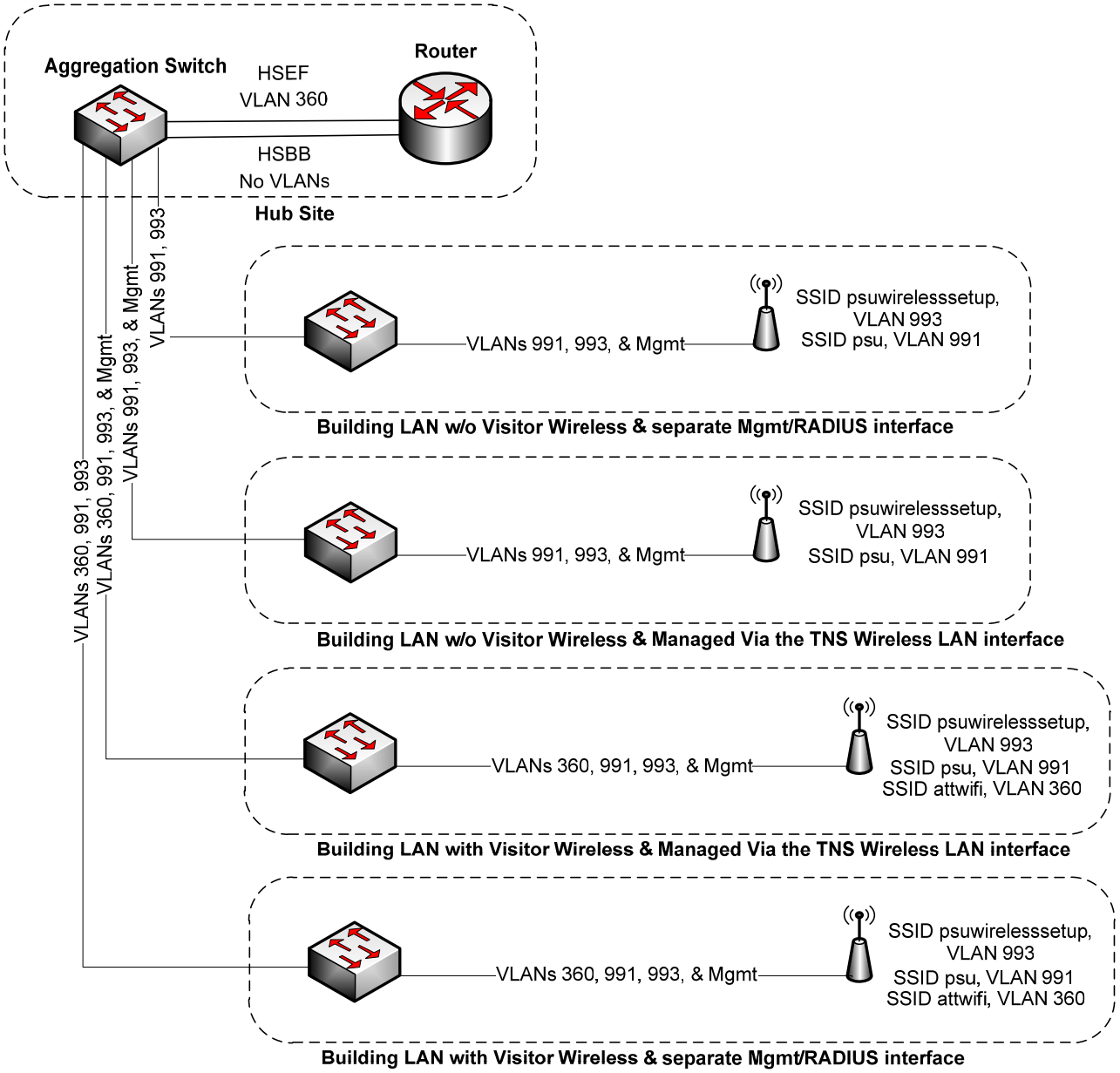
2. LAN Diagrams



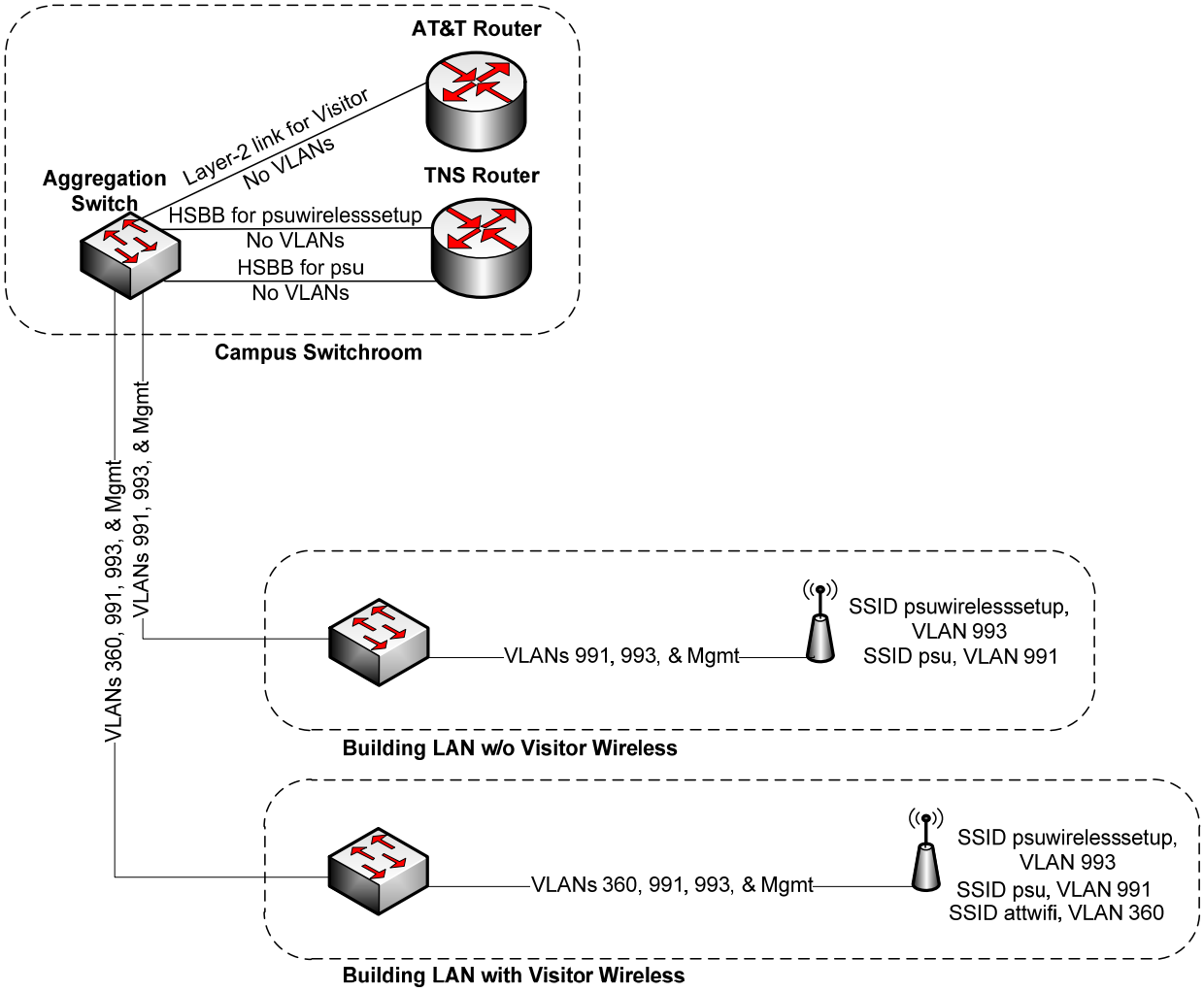
UP Wireless 2.0 Physical LAN Diagram



Non-UP Wireless 2.0 Physical LAN Diagram



UP Wireless 2.0 VLAN Diagram



Non-UP Wireless 2.0 VLAN Diagram

3. VLAN Information

The following section describes the functions and requirements of the various VLANs associated with wireless 2.0 and visitor wireless. Some installations will not require all four VLAN types. The VLAN tags provided are the tags used by TNS for each VLAN. Customers may use other VLAN tags within their networks, so long as the interface to any TNS maintained equipment is as specified.

“psu” client VLAN (commonly 991)

- VLAN for wireless clients connected to “psu” SSID
- One subnet for all wireless clients connected to the “psu” SSID for all interfaces on the same aggregation switch.
- Clients must connect using 802.1X (EAP-TTLS-PAP)
- Once connected, ACLs are consistent with accountable LANs
- Connected clients receive an internet-resolvable IP address

- Requires measures to ensure the client MAC address to IP address relationship is known at all times.

“psuwirelesssetup” client VLAN (Commonly 993)

- VLAN for wireless clients connected to “psuwirelesssetup” SSID
- One subnet for all wireless clients connected to the “psuwirelesssetup” SSID for all interfaces on the same aggregation switch.
- Connected clients can access only DHCP, DNS, & work.psu.edu
- Connected clients receive a non-internet-resolvable IP address
- Clients not configured to use the "psu" SSID can connect to the "psuwirelesssetup" SSID and use a web browser to go to http://wireless.psu.edu/, where they will find instructions and software needed to connect to "psu".

“attwifi” client VLAN (360)

- VLAN for wireless clients connected to “attwifi” SSID
- Participation in Visitor wireless is optional
- Subnet and routing provided by AT&T.
- One VLAN per campus location

Management VLAN

- VLAN for LAN equipment management and RADIUS authentication traffic.
- Customers may use other interfaces for this traffic.
- Each customer using the TNS wireless LAN interface for LAN management will have their own management VLAN tag and subnet. The VLAN tag will be assigned by TNS prior to installation.
- VLAN must not be available from AP wireless interfaces.

4. Network Security

It is vital for network security that the wireless security mechanisms as well as the VLAN membership for all network interfaces be properly configured. Improper wireless security configuration could allow unauthenticated clients to connect to the “psu” SSID. Additionally, improper VLAN configurations could allow clients associated to the “psuwirelesssetup” or “attwifi” SSID, which do not require authentication, to access the unrestricted IP addresses on the “psu” client VLAN. As such, it is critical that your wireless LAN configuration be thoroughly tested for proper functionality prior to deploying or converting your wireless assist LAN.

One additional requirement for responsible network administration is the ability to identify which network client was using which IP address at a given time. This is not necessary for the "psuwirelesssetup" (which does not have access to the internet) or "attwifi" (for which AT&T is responsible). For clients connected to the “psu” SSID, the access point provides the required encryption, but there is no single component capable of logging the user to IP address relationship. For clients that connect to and use the “psu” SSID in the conventional manner, the combined logs of the RADIUS authentication server and the DHCP server can be used to determine that relationship. However, should a client at any time choose to self-assign an IP

address, this system of logs by itself is no longer effective. In order to ensure a know MAC to IP relationship, it is necessary for one or more devices on the wireless LAN to participate in this process. The means of accomplishing this function fall into two main categories: logging and enforcement.

In logging, a device on the wireless LAN is responsible for keeping time-stamped logs of all changes in the MAC address to IP address relationship for all devices in the "psu" client VLAN. This is usually accomplished by monitoring and logging all ARP traffic in that VLAN. To reduce the size of the log file it may be useful to parse the full log such that only new and changed relationships are retained. This logging could be accomplished by way of a reliable server with an interface on the "psu" client VLAN which can monitor and log ARP traffic, or by a network component which can send information about address changes to a log server located elsewhere. Done correctly, the combined RADIUS, DHCP, and ARP logs can be used to identify a network client by their IP address.

Enforcement involves one or more network components which monitor DHCP traffic and deny the use of the network to clients which do not receive and use an IP address assigned by the appropriate DHCP server. This feature, sometimes referred to as "DHCP snooping", is available on some access points, wireless LAN controllers, and LAN switches. With a properly enforced DHCP assigned IP address, the combined RADIUS and DHCP logs are all that is needed to identify a network client by their IP address.

5. Hardware Requirements

Wireless LAN hardware must be capable of all the following in order to support Penn State Wireless 2.0:

- Support for 802.11g, typically achieved through an 802.11n AP with support for 802.11g enabled. 802.11n coverage in both 2.4GHz and 5GHz is recommended. In order to maximize performance, it is also advisable to disable support for 802.11b data rates.
- Support WPA2- Enterprise (802.11i)
- Support at least (2) VLANs and be able to associate an SSID to a VLAN without direction from the AAA infrastructure. Support for additional VLANs may be needed for Visitor Wireless or a private SSID
- Support radius accounting and be capable of sending start and stop records.
- Capable of broadcasting at least two SSIDs ("psuwirelesssetup" & "psu"), and use a unique BSSID for each SSID.
- Capable of broadcasting a third SSID if Visitor Wireless is desired.
- Capable of enforcing or logging the relationship between MAC address and IP address for all clients associated with the "psu" SSID.
- For administrators wishing to provide additional SSIDs using 802.1X, be capable of directing authentication and accounting traffic on each SSID to a different radius server.

6. Administrative Requirements

The University Auditors require that all Penn State wireless LAN's be registered with ITS. It is also necessary for ITS to know the full extent of the "psuwirelesssetup" and "psu" network

coverage in order to provide client support. Additionally, the contract with AT&T for visitor wireless requires that we notify them of which buildings contain Visitor Wireless coverage. You can satisfy all of these needs by visiting http://wireless.psu.edu/wireless.html, clicking the "Register my wireless network" link, and registering all your wireless networks.

7. Configuring a New Wireless Assist LAN

- If the wireless LAN will be managed via the TNS wireless LAN interface, provide TNS with the subnet to be used and a list of IP addresses for acceptable managing host devices. TNS will assign the maintenance VLAN tag.
- Coordinate the Radius shared secret and network access server (APs or wireless controller) IP addresses with AIT.
- Configure the APs
    - Configure IP addresses
    - Configure the client VLANs, & the management VLAN assigned by TNS (if applicable).
    - Configure the "psu" SSID
        - Open Network (broadcast SSID)
        - Unique beacon per SSID
        - Associate with the correct VLAN
        - Use WPA2-Enterprise (AKA, 802.1X with AES or 802.11i)
        - Direct Radius authentication and accounting to radius1.aset.psu.edu on ports 1812 & 1813, respectively.
    - Configure the "psuwirelesssetup" SSID
        - Open Network (broadcast SSID)
        - Unique beacon per SSID
        - Associate with the correct VLAN
        - No Security
    - Configure the "attwifi" SSID (Visitor wireless only)
        - Open Network (broadcast SSID)
        - Unique beacon per SSID
        - Associate with VLAN 360
        - No Security
- At UP locations, configure VLANs on the TNS wireless LAN interface port to the correct clients VLANs & the management VLAN assigned by TNS (if applicable)
- At non-UP locations, configure the uplink ports of the aggregation switch as untagged members of the appropriate VLANs.
- Configure VLANs on the AP switch ports to the correct client VLANs & the management VLAN.