Wireless Network Installations (ISSP-008)

I - Introduction

Wireless connectivity presents unique challenges in designing, securing, and managing networks. It has the potential to offer ubiquitous connectivity and great ease of mobility, but if deployed in a haphazard manner, loss of connectivity and mobility is assured.

It is extremely easy to simply plug a wireless access point or router into the wired network and within a few seconds be surfing the Internet. Because of this, it's tempting for individuals to go down to their favorite computer store, pick up an access point, and drop it in their office so they can use their laptop without wires. These unplanned installations cause several problems. They interfere with other installed access points and may even prevent connectivity.

They also thwart the security mechanisms USF is implementing to reduce our liability in the event of illegal activities originating from our network. Unauthenticated wireless access points, even if just placed in someone's office for their own use, provide connectivity to surrounding offices and outside of the building. Drive-by-hacking, where individuals sit in the parking lots of companies and capture wireless traffic or access that company's network has become a common event. The risks from these attacks must be controlled and proper authentication of access points is one method of doing this.

This document covers some general wireless network installation guidelines that **must be** followed to ensure USF's campus-wide wireless offerings are compatible, provide mobility between locations, and prevent unauthorized access.

Please read this documentation carefully. Any unauthorized wireless router found on our network will have its connection turned off immediately.

II - Prohibited Equipment

Wireless routers are prohibited on USF's network. To understand the reasoning behind this, we must first discuss the difference between a wireless router and access point.

What is a wireless router?

Wireless routers are the kind of products you'd find used in a wireless network for your home. They are sometimes called a wireless DSL or cable router. Some familiar brands are Linksys, Netgear, Belkin, and D-Link. The router attaches to the wired network (typically your DSL/cable modem) via an Ethernet connection and obtains a single IP address from the network that it uses to communicate with the Internet. It then provides private IP's to its clients and translates between these private IPs and the one external IP as traffic passes through the router. This makes it appear to computers on the Internet that all computers behind the router are just one machine.

In an environment where you want to authenticate each user, wireless routers make it impossible to distinguish the individual users since they all have the same address. Although it is possible to configure these routers to only allow certain wireless clients to connect, in an environment with

tens to hundreds of routers providing wireless coverage over larger areas, the administrative overhead of configuring each router to allow each new client is unfeasible.

Mobility (roaming) between wireless routers is not possible. Since each router is responsible for handing out IP addresses to its clients, when you move from router-to-router, not only does your assigned IP change, but the IP seen by the world (the IP of the router you're connected to) changes as well. For example, if you have a shared drive mapped from a server and you roam from one wireless router to the next (i.e.: your wireless NIC decides that another router in your area now has a better signal strength), your IP changes and you WILL LOSE CONNECTIVITY to that shared drive. The same loss of connectivity occurs if you're using any other network application (web, streaming media, etc).

What is an access point?

Wireless access points operate differently than routers. Their sole job is to transmit data between the wired and wireless network without altering the data (or changing any IPs). They are transparent to the network.

Because of this, authentication of individual users is now possible since each user is completely visible to the network. Each user is assigned an individual IP address and assignment of those IP's can be controlled centrally. By centrally controlling what IP a client is assigned, policies can be placed on unregistered clients restricting what they can access. Central management of the client registrations doesn't require any configuration on the access points.

Mobility between access points is easy. Your assigned IP address does not change when roaming from access point to access point. So, whatever network applications you are running will still be able to communicate.

For these security and mobility reasons, wireless routers are not permitted on USF's network. Any wireless router found on our network will have its connection turned off immediately. The **Data Network Management (DNM) group** is attempting to provide a common authentication methodology that will be used on all of USF's open access (wired and wireless) networks. For this to be successful, we must only deploy equipment that makes this central authentication possible. We are also actively deploying wireless networks for classroom and outside access. Our deployments are compatible with the current authentication system and any wireless router placed on the network will cause not only our own networks to fail, but will cause users of that wireless router to lose connectivity.

III - Notification of New Wireless Installations

The DNM is not trying to discourage departments and users from purchasing wireless access points. In fact, purchasing is encouraged. In the absence of central funding to provide campus-wide wireless, the more equipment users and departments purchase individually, the better coverage we will have.

Any new installations must be coordinated with USF's Data Network Management group
(See contact info below)

We will gladly assist in the installation of any access point. The DNM will place and configure the access points so that they do not interfere with other access points already deployed. We will make sure that the new access points are put on the appropriate network so that authentication is required before a client can use our network. If the access point supports the necessary network management protocols, we will even monitor it for reachability and graph the number of clients

using the access point over time. If the access point fails for some reason, we'll be notified immediately and will work to bring it back online.

Also, by contacting us, each new access point will be placed on the same network as all of the other access points on campus. This will allow mobility between access points. Someone walking through a building, or walking between buildings will be completely able to roam from access point to access point without losing connectivity.

All of these services are freely available with only a phone call or email to our group informing us of a new access point installation.

Any unknown wireless access point found on USF's network will have its wired connectivity removed until the owner can be contacted and the access point is properly secured.

IV - Summary

Wireless routers are not allowed on USF's network. Wireless access points are welcome, but their installation must be coordinated with USF Data Network Management to ensure that proper configuration and security guidelines are followed.

We are attempting to provide a consistent campus-wide network for both wired and wireless clients. By coordinating this initiative, we all benefit from increased network access, mobility and security.

Contact Info:	The easiest way to contact the DNM group for new wireless installations is to send an email to wireless@net.usf.edu.