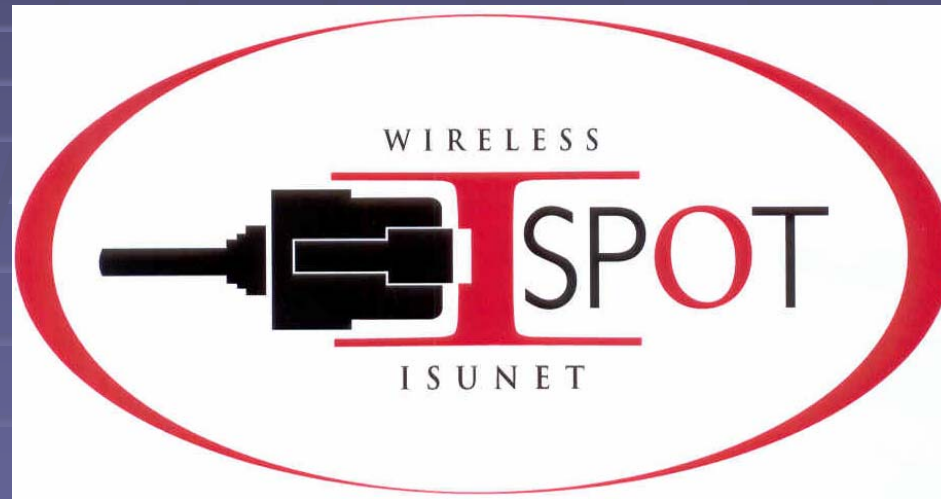


A Technical Overview of wireless ISUnet



Fall 2004

contents



- introduction
- connectivity to wireless ISUnet
- iSpot coverage areas
- roaming between wireless ISUnet and other networks
- the future of wireless ISUnet

introduction to wireless ISUnet

introduction

- why was wireless ISUnet introduced?
 - designed to provide access to campus or Internet based services for a mobile computing device such as laptop, notebook, tablet computers, PDAs *, etc

* not supported by Helpdesk



introduction

- what were some of the guiding principles?
 - service needs to be available to all faculty, staff, students, and emeritus but exclude non-University users
 - data needs to be encrypted to prevent eavesdropping and it should not be possible to decipher the keys used for encryption
 - the implementation needs to be standards based as much as possible to support the ubiquitous use of the technology throughout campus

introduction

- are there any restrictions?
 - desktops are not supported to keep the number of devices concurrently competing for shared bandwidth in a given coverage area as low as possible
 - systems that are found to be using wireless coverage areas in a pattern that is inconsistent with the mobile computing initiative may be denied access to the network

introduction

- what are the issues?
 - range of frequencies used by specific wireless technologies are managed by the FCC to prevent conflict between applications as it relates to licensed - vs- unlicensed spectrum
 - actual throughput of a wireless device is dictated by power levels, range, and degrees of interference (and it is shared media)
 - constant infusion of new wireless technologies makes interoperability of features difficult
 - market uncertainties regarding security solutions

introduction

- IEEE 802.11 working groups
 - standards body that defines implementation guidelines for wireless LANs (including 11b, 11g, 11a, and WEP)
- WiFi
 - consortium of vendors that defines rules for the interoperability of 11b (and theoretically 11b, 11a) technologies
- WPA (WiFi Protected Access)
 - consortium of vendors that defines rules for the interoperability of 802.1x (EAP), TKIP, and MIC

connectivity to wireless ISUnet

connectivity

- access technologies
 - spectrum
 - defines the range of frequencies
 - modulation
 - defines rules for how bit patterns are mapped to transmitted frequency
 - access method
 - wireless LAN technology is shared media
 - CSMA/CA

connectivity

- IEEE 802.11b (WiFi)
 - 11Mb/s @ 2.48Ghz (unlicensed spectrum) using DSSS modulation
 - actual shared throughput around 6Mb/s (shared)
 - 11 channels (only 3 are non-overlapping)
 - available on all wireless coverage areas on wireless ISUnet

connectivity

- IEEE 802.11g
 - up to 54Mb/s @ 2.48Ghz (unlicensed spectrum) using OFDM modulation
 - can support the concurrent association of either 11b or 11g clients
 - actual shared throughput for 11g clients when only 11g clients are associated as high as 24Mb/s
 - actual shared throughput for 11g clients when both 11g and 11b clients are associated drops to 8Mb/s
 - actual shared throughput for 11b clients always 6Mb/s
 - 11 channels (just like 11b)
 - deployed in nearly all existing coverage areas during spring 2004 (will be available in all coverage areas during fall 2004)

connectivity

- IEEE 802.11a
 - UNI I, II, III
 - available in select areas (UNI I only)
 - 54Mb/s @ 5Ghz (unlicensed spectrum) using OFDM modulation
 - substantially smaller coverage areas than 11b or 11g
 - actual shared throughput around 24Mb/s
 - 24 non-overlapping channels
 - major power issues

connectivity

- interference
 - unlicensed spectrum means many applications competing for same channel assignments
 - sources include non-ISU wireless coverage areas adjacent to campus, rogue devices, wireless appliances, and so on
 - commercially available products to flood unlicensed RF spectrum for DoS (no defense)

connectivity

- rogues
 - for DSSS and OFDM modulation, channel assignments are fixed (unauthorized wireless devices can easily create interference for these coverage areas)
 - unprotected wireless devices create backdoor points of entry into the network exposing the inside of the network to unknown threats
 - these devices will be located through devices that scan frequencies as well as network based devices
 - requirement by State Auditor General to identify and remove these threats to prevent the exposure of sensitive data
 - once a rogue is found, it will be immediately removed from the network and the department will be assessed a \$100 policy violation fee

connectivity

- security model
 - authentication
 - is the user authorized to access wireless ISUnet?
 - encryption
 - prevents data transmitted through the air from being deciphered by something other than the intended receiver
 - key management
 - used to make sure that the key used to encrypt data between client and base station cannot be derived

connectivity

- dynamic WEP
 - 802.1x (using an EAP type of LEAP)
 - AAA currently based upon AD authentication
 - RC-4 encryption
 - keys are expired at 5 minute intervals
 - current security implementation on wireless ISUnet

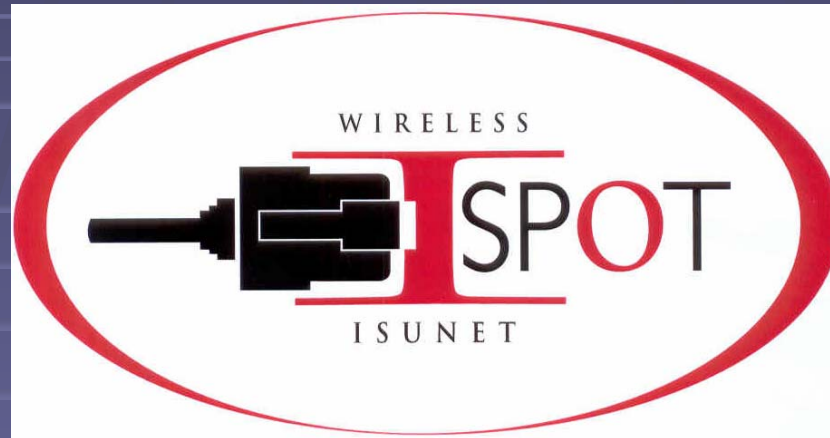
security

- WPA-EAP
 - 802.1x (using an EAP type of EAP-FAST)
 - AAA based upon LDAP authentication (to increase flexibility of service offerings)
 - RC-4 encryption
 - TKIP (per packet key morphing)
 - MIC (to prevent session hijacking)
 - coexistence issues with dynamic WEP (using LEAP)
 - support for both security models on wireless ISUnet during fall 2004

security

- why not support the native Microsoft zero config?
 - EAP-TLS requires the use of client side certificates (imagine maintaining certificates for a large number of mobile devices)
 - MS-PEAP is based upon mschap (ie: AD) while the rest of the world uses GTC (requiring all clients be able to interface to AD)

iSpot



iSpot




- coverage areas
 - where is wireless ISUnet service available
 - iSpot logo was designed to allow users of wireless ISUnet service be able to quickly and easily locate coverage areas

ATTENTION:



THIS BUILDING CONTAINS INTERNET HOT SPOTS

Hot Spots allow students, faculty and staff to connect a personal computer to ISUnet from many public areas throughout the campus. You can surf the web, check e-mail or even use the

 portal while you are mobile.

New Hot Spots are being added all the time so be sure to check the mobile computing web site for more information on where and how you can get connected.

WWW.ILSTU.EDU/MOBILE

iSpot

- coverage area list

- <http://www.ilstu.edu/helpdesk/howto/getconnected/win/mobile.shtml#wireless>

University Computer Help Desk - Mobile Computing - Microsoft Internet Explorer

[Printable Version](#)

Access Point Location	Wireless Coverage Area	Radio Type
Milner 6th floor NW	northwest, west and west-central areas of 6th floor	802.11b/g
Milner 6th floor SW	southwest, west and west-central areas of 6th floor	802.11b/g
Milner 5th floor East	central and east areas of 4th and 5th floors	802.11b/g
Milner 5th floor West	central and west areas of 4th and 5th floors	802.11b/g
Milner 5th floor NW	northwest, west and west-central areas of 4th and 5th floors	802.11b/g
Milner 3rd floor NE	northeast and north areas 2nd, 3rd, and 4th floors	802.11b/g
Milner 3rd floor SE	southeast and south areas of 2nd, 3rd, and 4th floors	802.11b/g
Milner 3rd floor East	central and east areas of 2nd, 3rd, and 4th floors	802.11b/g
Milner 3rd floor NW	northwest, west and west-central areas of 2nd, 3rd, and 4th floors	802.11b/g
Milner 3rd floor SW	southwest, west and west-central areas of 2nd, 3rd and 4th floors	802.11b/g
Milner 1st floor South	south, southeast and south-central areas of 1st and 2nd floors	802.11b/g
Milner 1st floor West	central and west areas of 1st and 2nd floors	802.11b/g

iSpot

- roaming within a building
 - same address space throughout building so DHCP lease is valid anywhere there is coverage
 - authentication is done behind the scenes as a client passes from one coverage area to the next

iSpot

- roaming between buildings
 - different address spaces between buildings
 - adjacent coverage areas between buildings will not support subnet roaming
 - future implementation

**roaming between wireless
ISUnet and other networks**

roaming

- static WEP
 - no authentication (consumer)
 - static shared key
 - which can be derived if an attacker is given enough time (better than no defense at all)
 - 40 or 128 bit keys (cannot mix in the same coverage area)

roaming

- WPA-PSK
 - no directory based authentication like WPA-EAP (consumer)
 - PSK (PreShared Key) like WEP key
 - still use TKIP and MIC (PSK is starting vector)
 - more secure than static WEP because it currently cannot be derived

roaming

- SSID
 - identifies name of wireless network
 - can be used by client to manage security profiles that are specific to each network
 - ex: SSID=isunet, use dynamic WEP with LEAP; SSID=(name of your home network), use static WEP or WPA-PSK
 - home users should ALWAYS use some form of wireless security even if it is only static WEP

roaming

- VPN
 - remember that home users still need to use the campus VPN client to access restricted resources on ISUnet from foreign wireless networks regardless of the security model used

the future of wireless ISUnet

future

- coverage areas
 - continue to grow public spaces but expect more requests from departments for private spaces
 - expect major growth in classroom spaces
 - there are no plans to cover the entire campus (growth will be dictated by demand)
 - expect to increase from 60 to 100+ coverage areas by fall 2005
 - expect to introduce more 11a coverage areas throughout campus
 - expect to introduce on quad (no date established yet)

future

- security
 - expect that dynamic WEP will be replaced by WPA-EAP in our environment as early as fall 2005
 - expect that EAP-FAST will eventually replace LEAP using WPA-EAP
 - expect the need for Aegis may disappear as more manufacturers write their own security supplicants
 - planned registration system that will allow users to download security supplicant and network security suite developed by Helpdesk (as described by Conditions of Access policies)
 - very limited guest privileges

future

- subnet roaming
 - mobile IP proxy has too many limitations
 - expect split tunnel approach from base stations to backbone based device that allows a client that has been served an IP address in one building to continue to use this address in another without loss of connection

future

- 802.11i
 - 802.1x (supports all EAP types)
 - support for TKIP and MIC
 - replaces RC-4 encryption with AES (most legacy wireless clients and base stations cannot support this algorithm because it is processor intense)

future

- 802.11e
 - QoS implementation for wireless to provide higher priority for streaming audio or video

future

- 802.11h
 - provides the means for 11a clients to hop to other channels in the event of interference
 - power management techniques to control transmit power on clients to reduce the noise these clients inject into adjacent coverage areas

conclusion

conclusion

- alphabet soup
 - WEP
 - LEAP
 - WPA
 - EAP-FAST
 - TKIP
 - MIC
 - AES

conclusion

- sources
 - <http://www.tnss.ilstu.edu/>
 - <http://www.ilstu.edu/mobile>
- presenter
 - Scott Genung, Manager of Networking Systems
- questions?