

Recommendations for Wireless Implementation at STScI  
23 January 2002  
- Carol Christian/ Development Technology and Innovation

The wireless project goal was to develop a plan for deploying wireless networking at STScI. The evaluation phase has been completed and the wireless project team (CISD and DTI) has proposed a recommendation for deployment. This document will summarize the report of the team and outline the proposed plan for implementation.

Interviews. DTI surveyed STScI staff to determine what needs existed and how staff envisioned using wireless at STScI. The uses of wireless technology expressed by interviewees include:

- Use during meetings to improve work efficiency
- Provide immediate access to pertinent data while doing collaborative work in another staff member's office
- Provide network connectivity to visitors in many locations throughout Muller
- Provide ability to move equipment within large lab areas without having to move a network connection

Equipment recommendation. The recommended hardware for the wireless access points is the Cisco Aironet 350 series. It implements WEP (wired equivalent privacy) and satisfies requirements for security, area coverage, and health and safety concerns. The security features of the Cisco product include:

- Mutual authentication scheme by use of the extensible authentication protocol (EAP) as implemented in Cisco's LEAP.
- Per user, per session key management with implementation of dynamic WEP
- Integrated network logon

Wireless security. As stated above, the Cisco product is being used as it provides the functionality for as secure a wireless environment as possible. Our overall security plan has three elements:

- Limiting the transmitting power of the access point
- Packet encryption by using WEP keys
- Mutual authentication by use of Cisco's LEAP product

Site survey. A site survey of Muller and Bloomberg buildings was completed to identify locations for wireless access points to provide wireless coverage in both buildings. The site survey did not include the Rotunda office space. The sites were identified for Muller, and will require 20 access points to cover the entire building from the Ground floor to the 4<sup>th</sup> floor. Bloomberg presents security issues in that some areas (4<sup>th</sup> and 6<sup>th</sup> floor) are shared JHU/STScI areas and often accessible by the public. Coverage can be provided for the 3<sup>rd</sup> floor area where physical access is controlled outside normal business hours. It is possible that we can provide some limited wireless for specific locations on other floors in Bloomberg, if they can be installed and contained within access controlled areas.

Deployment. DTI and IDTL have already purchased the recommended hardware to be used as access points; these units were part of the evaluation. These two access points have been installed in N324 (DTI) and Bloomberg 020 (IDTL) with static WEP keys.

Prior to installation and use of access points by additional staff, we will:

- Procure and install RADIUS server software to enable use of dynamic WEP
- Procure client cards and an additional 6 access points through use of ED05 and CISD division M&E funds
- Complete procedures and train CISD staff on installation of client cards and software

The 6 access points to be procured should be installed in locations where they will be most beneficial, or an immediate need is identified. Potential locations might include major meeting rooms such as the Board Room, Cafe-Con, 112, S321, etc. CISD will seek input on where these locations should be. Funding for additional access points is to be determined, but could come from the FY 2003 ED05 or division M&E funds. Before additional access points are procured, we should have 3 months experience with wireless to determine what, if any, problems might exist and make any necessary changes.

Policy: A draft STSci Network Wireless Policy has been completed. This policy follows guidelines required under NASA Policies and Guidelines (NPG) 2810.

Obtaining access: CISD will maintain a supply of client cards to install in individual user's systems. The user's Division would then purchase a card to replenish the CISD supply. Users will be able to request access to the wireless network via a request to cisdsupport. The CISD help desk will have responsibility for installing and configuring client cards.

Requirements for clients:

- PCs – must have available one PCIMA slot
- Macs – Macs must have their firmware upgraded to v2.0 to work with the Cisco Aironet access points and must be running Mac OS 9.x.

Schedule for deployment:

22 January	Deployment of DTI and IDTL access points (completed)
31 January	Decision on location of first 6 access points
15 February	Additional Access Points, client cards, and server software delivered
28 February	Deployment of additional access points and availability for use, assuming 15 Feb delivery
28 February	Convert existing clients from static WEP to dynamic WEP as soon as RADIUS server is installed
TBD	Remove any remaining airports from STSci network