



Wireless Infrastructure Request for Proposal (RFP)

November 2011

Mansfield Public Schools
<http://mansfieldct.gov/mboe>

Regional School District 19
<http://www.eosmith.org>

Town of Mansfield
<http://www.mansfieldct.gov>

SUBMISSION DEADLINE:

Friday, December 9, 2011 at 1:00pm

SUBMISSION CONTACTS:

Jaime Russell and Jan Poland

WirelessRFP@eosmith.org

Proposals will be accepted in electronic format only.

Purpose

Regional School District 19 (Region 19), the Mansfield Public Schools (Mansfield Schools), and the Town of Mansfield (Town) are seeking to purchase hardware for a managed wireless infrastructure. Our entities may optionally also purchase services to assist with the installation.

Background

Region 19, the Mansfield Schools, and the Town are three separate entities with their own distinct leadership structures, missions, and budgets, but they also share a common wide area network infrastructure and joint Finance and Information Technology Departments. Appendix A at the end of this document provides additional background on our current infrastructure.

In 2007, our entities purchased a Hewlett Packard ProCurve Access Control Server Appliance to support both internal (trusted) and public (untrusted) wireless access. This solution allowed each of the three entities to gradually deploy wireless access points through their respective budgets. Our organizations' needs have now surpassed the capabilities of this initial solution and we are looking to implement a new system for managing wireless access.

Vendor Submission Requirements

Vendors that wish to be considered will need to meet the following response requirements:

- Submissions will be accepted in electronic format only to WirelessRFP@eosmith.org and must be submitted prior to Friday, December 9, 2011 at 1:00pm.
- The submission should provide the following information:
 - The vendor's name and website address, the name of the individual that is coordinating the vendor's submission, and the e-mail address, phone number, and postal address for the aforementioned individual.
 - General information about the vendor. The intent is to familiarize our entities with the vendor's background such as the number of employees, annual revenue, the types of clients served by the vendor, and the types of services and technologies provided by the vendor.
 - Descriptions of two previous examples where the vendor supplied a wireless infrastructure solution to clients. The descriptions should speak to the client's size and needs, the vendor's role in providing the solution, the technologies used, and the end result of the deployment. Preferably the description will mention the clients' names, but if not, it should at least describe the type of client (i.e. relative size and nature of the school/government/business entity).
 - A draft proposal of an overview wireless infrastructure solution that generally speaks to the nine items listed below. The proposal does not need to be a final document and is intended to provide a summary overview of a potential solution. For example, the proposal does not need to speak to the number of wireless access points required. Vendor(s) that are selected as finalist(s) will be interviewed either in person or via telephone and can elaborate on these items. If the vendor already has copies of existing reference pdf sheets for hardware, those can be included in the submission, but are not required.
 1. The vendor's relative involvement in the selection, design, installation, and ongoing support of the wireless solution.
 2. The method(s) for differentiating between users on mobile equipment owned by our entities (trusted users) and users on publicly owned equipment (untrusted users).
 3. The design of the initial welcome interface and access presented to public users on untrusted devices.
 4. The approach to maintaining wireless coverage. Some examples could include 802.11n compatible access points, wireless mesh technologies, and logging of use levels per access point.
 5. The management interface and capabilities available to Information Technology support staff for ongoing maintenance of existing access points and users as well as setup of additional access points.
 6. The safeguards in the design of the system to support reliability such as redundancies, alerting/reporting, system data backups, security, and the ability to handle growth over time in access points and users.
 7. The specific support process in the event of failures or ongoing hardware management questions. This should speak to options for purchased access to warranties, access to software patches/upgrades, and the availability of

support mechanism such as a knowledgebase support website, email support, telephone support, and if needed onsite support.

8. The flexibility (if any) for differentiating between access points given the different buildings that could use this solution. Some examples could include the ability to group access points/users per building in the management interface, presenting unique public welcome pages per entity, and differentiating routes to the Internet for public users depending on the connecting access point (our entities have different connections to the Internet with differentiated filtering).
9. The flexibility (if any) to use a variety of access point models and antennas. This could be to address special coverage needs (such as outdoor antennas or high user concentration locations), or to provide lower cost access points to rooms with less robust access needs, or to use existing third party access points already owned by the entities.

Summary

We intend to “short-list” vendors responding to this RFP and to interview one or more vendors either in person or via telephone to make a final selection. We reserve the right to reject any or all submissions, to extend the submission deadline, and to select a vendor in a manner that meets our needs. We do not expressly state or imply any obligation to reimburse the responding vendors for any expenses in preparing submissions in response to this request. Our three entities are equal employment opportunity employers. Please address any questions related to this RFP to the contact information listed at the beginning of this document.

Appendix A: Description of Current In-Place Infrastructure

The Region 19 – Mansfield Schools – Town of Mansfield Wide Area Network (WAN) includes twelve school and municipal buildings interconnected by gigabit fiber-optic cable. Hewlett Packard ProCurve switches provide a managed environment with IP subnets and vlans. Some network services are provided in common among all three entities and some services are handled by individual portions of the network. Region 19 operates its own Microsoft Windows Server Active Directory structure and the Mansfield Schools and the Town of Mansfield share a mutual Microsoft Windows Server Active Directory structure.

Presently, a Hewlett Packard 740wl Access Control Server Appliance and accompanying Access Controller Module manage the wireless infrastructure. Hewlett Packard 802.11b/g compatible access points feed all wireless connection requests within an isolated vlan back to the central appliance which determines if it is a trusted (entity owned) or untrusted (public owned) wireless device. Untrusted devices remain within the isolated vlan and can only access the Internet via the controller and a CISCO firewall appliance and are initially presented a welcome page with our acceptable use policy. Trusted devices are placed into designated vlans depending on which entity owns the device thereby providing internal access similar to a wired device. Additionally, trusted devices connect to the wireless access points using an encrypted connection.

Nine of our twelve fiber-optic connected buildings participate in this common wireless infrastructure. This allows students, staff, and the public to connect to wireless in nine of the twelve buildings in a common manner. One of the twelve buildings (Public Library) requires a unique entry page and unfiltered Internet access and our control appliance is not capable of providing this need, so the Library uses a separate solution. An additional four buildings connect to the WAN through either cable or DSL modems via VPN appliances and the control appliance is not able to see the access points through the VPN connection so they operate a separate wireless access solution.

Information Technology staff connect to the control appliance through a remotely accessible interface that provides certain limited management capabilities for assigning entity owned equipment to the appropriate categories, restricting certain port access for public users, saving system backups, and minimal troubleshooting and logging.

The present infrastructure includes ninety (90) wireless access points. Each access point must be initially configured on both the access point itself and on the central controller. The majority of these access points cover indoor locations; however there are a number of outdoor antennas as well covering common areas used by students, staff, and the public. Trusted and untrusted users connect using a variety of mobile devices such as laptops, tablets, and handhelds.