

Request for Proposals (RFP) for Wireless Infrastructure Solution



Diocese of Camden

**1845 Haddon Ave
Camden, NJ 08103**

PROPOSAL DUE DATE: 12/8/2008

Table of Contents

Organizational Overview	3
Purpose of the RFP	3
Questions About The RFP	4
Proposal Submission	4
Required Deliverables	5
Evaluation of Proposals	6
Reference Summary	6
Functional Requirements	7
Terms & Conditions	11

Organizational Overview

The Diocese of Camden operates four nursing homes for which we are seeking a wireless infrastructure solution. The addresses of each location are outlined below:

Bishop McCarthy Residence
1045 E. Chestnut Ave
Vineland, NJ 08360

Mater Dei Nursing Home
176 Route 40
Newfield, NJ 08344

Our Lady's Residence
1100 Clematis Ave.
Pleasantville, NJ 08232

St. Mary's Catholic Home and The Manor at St. Mary's
220 St. Mary Drive
Cherry Hill, NJ 08003

Purpose of the RFP

The Information Technology Department of the Diocese of Camden is requesting proposals for a wireless infrastructure solution to be installed in 4 locations throughout southern New Jersey. The objective is to select a vendor partner who has demonstrated industry leadership utilizing a centralized management approach and will continue to grow with the technology needs of the Diocese.

It is anticipated that the implementation will occur in several phases over a period of time as yet to be determined. Furthermore, the initial site implementation will also be accomplished in a phased manner. Thus, producing a proof of concept approach on a very small level and expanding outward to the entire operation.

Questions About the RFP

Prospective vendors with questions regarding the contents of this request or the procedures by which proposals will be received and evaluated should contact Ron Pilla, Network Services Manager at ron.pilla@camdendiocese.org. All questions must be submitted in writing.

All questions should be submitted no later than **12/1/2008**

Proposal Submission

Please review this RFP carefully before responding to ensure that you understand fully all procedural, system and contractual requirements.

Each RFP response should be presented so that it can be readily reviewed (an index is desirable). Submit an original and two (2) copies to the Diocese of Camden along with an electronic mail copy of the final RFP response in either Microsoft Word or PDF format to:

Ron Pilla
Diocese of Camden
IT Department
1845 Haddon Avenue
Camden, NJ 08103

Email: ron.pilla@camdendiocese.org

Required Deliverables

Proposal responses should include the following sections:

1. Title Page including vendor name, address and contact information for the vendor representative.
2. Table of Contents
3. A brief overview of your proposed solution describing the overall functionality of your product including the overall architecture of the proposed solution.
4. Corporate Background
5. Client References as described in this document.
6. Technical Requirements:
 - a. Outline hardware and software requirements both minimum and recommended for each location.
 - b. Include minimum network requirements.
7. Responses to Functional Requirements as described in this document.
8. Implementation Plan
9. Training Plan
10. Support Services - Describe how your organization provides support and maintenance services to your customers.
11. Pricing as outlined below. Fill in the table below (or provide a similar table) giving all costs (e.g. license fees, implementation, training, maintenance and documentation). List any add-ons and their related costs.

ITEM DESCRIPTION	COST
Installation / Implementation Fees (per location)	
Annual Support Fees (per location)	

Annual License Fees (per location)	
Initial Training	
Project Management	
ADD-ONS:	
<i>Outline add-ons required to address functional requirements</i>	
<i>Outline optional add-ons available to enhance system functionality</i>	

Evaluation of Proposals

The following are the criteria by which the Diocese will evaluate the proposed solutions:

1. Degree to which the solution fits the Diocese's functional requirements without requiring modification.
2. Service and support provided by the vendor.
3. Reputation, capacity, financial stability of the vendor.
4. Successful history of vendor in similar environments.
5. Cost of the system including purchase costs, maintenance and support costs, and implementation costs.

Reference Summary

Provide three references of similar installations of wireless installations where centralized management is necessary for multiple sites.

For each reference site provide general information including potential installation timeframes, versions and detailed hardware schedules. For each reference site, provide contact information including name, address, phone number and title.

Functional Requirements

General

- Please give a short descriptive summary of your proposed solution. Identify the number of similar installations that your company has achieved and how many similar installations your company currently supports.
- Describe the process of implementing your solution.
- What do you provide in terms of support and training during implementation?
- Explain the maintenance of your product.

- How do you disseminate updates?
- What are the costs of updates and what support do you provide?

Technical

The following listing of technical requirements have been determined to be mandatory to meet functional, operational, and Security needs, both short and long term. Responding vendors shall address each item with: Fully Comply, Partially Comply, or Does Not Comply. Vendors must provide detailed explanation for Partial and Do Not comply responses.

General

- Must be a centralized architecture with “thin” Access Point and centralized switches and management.
- Must be dual port radio Access points.
- Must be WiFi Alliance Certified.
- Solution must be self-contained, integrated, overlay solution, not requiring upgrades or enhancements to existing routers and switches.

Access Points (AP's)

- Must support 802.11 a/b/g and 802.11n.
- Must be Plenum rated with applicable certifications.
- Must support auto-sensing 10/100/1000 on the network port.
- Must support local power adapters.
- Must support options for dual-band single-radio APs which can perform RF scanning on both bands while serving WLAN clients on one.
- Must support 802.3af standard, power over Ethernet, for dual-radio operation at full power of the radios – and 2 spatial streams for the 802.11n capable APs.
- Must offer optional mounting kits for ceiling and/or wall mounting.
- AP's must provide integral facility for security lockdown.
- AP's must support out-of-the box, auto configuration across layer-2 and layer-3 networks without having to enter configuration information into the AP.
- AP's must not hold “hard configured” internal network information or certificates.
- AP's must support minimum of 8 SSID's and BSSID's.
- AP's must be capable of multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, real-time non-disruptive packet capture, RF monitoring with no physical “touch” and no additional cost.
- Must provide versions of AP's that support internal and external antennae.
- Vendor must provide a broad family of external antennae that vendor will certify to meet FCC standards and will fully support.

AP to Switch/Controller Communications

- Must use industry standard tunneling protocol(s).
- Control path between the AP and the controller can be encrypted with standards based protocols.
- Data path between the wireless user and the controller must be encrypted if wireless encryption is in use.
- Must be upgradeable to emerging CAPWAP standard (as currently drafted) with no Hardware (AP touch) upgrades or additional costs.
- Must support secure connection over “untrusted” network transport. E.g. IPSEC/VPN.

AP Management

- Must update firmware and software on all AP's automatically.
- Must support discovery protocol from AP's to find and sync with controller, that works over routed and switched subnets and that does not require reconfiguration or features on routers or switches.
- All AP configuration and service delivery information must be centrally managed and maintained via the switch/controller.

RF Management

- Must automatically set and adjust individual AP power and channel setting to maximize performance around other AP's, interference (both 802.11 and non-802.11) and coverage holes.
- Must support dynamic load balancing based on user defined thresholds for associations and active users. Load balancing must not require any client specific configurations or software.
- System must support these functions in real time and without the need to perform any network baselines, manually administered measurements and must be based on real RF information versus models in management systems.
- RF Management features must be voice-aware and provide the capability to pause channel scanning if an active voice-call(s) is detected.

Intrusion Detection/Prevention

- Must provide for Rogue detection and containment.
- Must provide accurate method of classifying real Rogues (on network) versus interfering neighbor networks whether Rogues have encryption or not and without client software or upgrades to current network.
- Must provide for Ad-hoc network detection and containment.
- Must provide for detection of wireless bridges.
- Must provide protection for Man-In-The-Middle and Honey-Pot attacks.
- Must provide protection for denial of service attacks.
- Must provide protection for MAC address spoofing.
- Must provide user-definable rate threshold detection and protection.

- Must provide detection of network scanning tools.
- Must provide for data/packet CRC and sequence error detection and prevention.
- Must provide on-the-fly, update-able, user specified signatures.

Authentication & Encryption

- Must support the following: MAC, 802.1x, WPA2, WEP, TKIP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC
- Must provide Web-Based Authentication (e.g. WebAuth/Captive Portal) that:
 - o Must be integrated into the controller/switch.
 - o Must provide user name and password authentication.
 - o Must provide option for simple logging of user name for entry.
 - o Must provide tool to allow non-IT staff to create temporary guest ID's and passwords to automatically age out.
 - o Must provide ability to customize the pre-authentication network access rights beyond DHCP response (e.g. to allow PC's and MACs to finish network scripts and network boot ups).
 - o Must provide API's for scripted control of these features from external system.
 - o Must support airtime based bandwidth contract for the guest SSID to preserve channel access for employee SSID.
 - o Must support packet rate based bandwidth contract for individual guest users for increased control of guest traffic usage.
 - o Must support blacklisting of guest devices in case of specified number of failed authentication attempts for increased security.
 - o Must support blacklisting of guest devices in case of firewall rule violations for increased security.
 - o Must support 802.1x based guest access with local database and integrated RADIUS termination for increased security.
 - o Must support time-of-day / duration based access per guest user of increased control and security.
 - o Must support secure tunneling via IPsec / GRE to a DMZ WLAN controller or L3 switch for ease of deployment.
- Must support Centralized Encryption/De-encryption (e.g. on switch/controller, in data center) and optionally distributed Encryption/De-encryption (e.g. on AP's) without the need for specialized hardware and must support mixed mode operations from a single switch/controller.

Access Control

- Must support security enforcement for wireless users through the use of role based stateful firewall, which will integrate directly with the roles defined within the already installed authentication servers.
- System must provide dynamic, stateful (as defined by ICSA) access rights into the network once authenticated, based on source, destination, and/or ports.

- Stateful access “service” must be ICSA certified to meet firewall standards for security adherence and enforcement.
- Violation of Access policies must provide for automatic blacklisting of users and/or devices where users/devices are no longer permitted to associate to AP’s and must provide for automatic capture of data for audit and analysis.
- Rules for access rights must support any combination of time, location, user identity, device identity, and extended attributes from the authentication database.

Quality of Service

- Must be WMM-certified.
- Must support both upstream and downstream packet tagging between AP and controller/switch.
- Must support per user, per device, and per application/TCP-port prioritization.
- Must support bandwidth contracts per SSID and/or per user.
- Must support advanced Voice QoS services that:
 - o Prioritize voice streams over data for mixed mode devices (e.g. traffic-based vs. SSID-based prioritization).
 - o Can notify applicable AP’s of active voice calls to pause off-channel RF and Rogue/IDS scanning.
 - o Can reserve bandwidth capacity for a user defined number of phone calls per AP.
 - o System must support or be upgradeable to support 802.11e standard without hardware or incremental software purchases.
- Must support Call Admission Control (CAC) capabilities (e.g. ability to limit the number of voice calls on an AP and actively move voice clients to a less-utilized AP by stateful monitoring signaling streams).
- Must support Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), VOCERA, Spectralink Voice Protocol (SVP) VoWLAN protocols.
- Must support multiple, battery-saving features.

Network Services

- Must support internal routing to the system.
- System must support switching and spanning tree between SSID’s, ports and segments.
- Must support NAT and DHCP.
- Must support GRE and IPSEC tunnels between controllers and other GRE/IPSEC termination devices.
- Must be capable of separating IP addressing from SSID from location.
- Must be able to work with Network Access Control software.

Mobility

- Must support L2/L3 Roaming capabilities with no special client-side software required.

Management

- Controller/switch must provide a complete command line interface to control and manage all aspects of the system.
- System must support SNMP V3.
- Systems must support SSH.
- System changes must be real-time configurable, not requiring reboots or re-compilation to affect changes.
- Vendor must provide complete Browser-based system for total solution management including: site planning, configuration, monitoring, troubleshooting, and reporting.
- System must support single, unified management view to multiple controllers/switches and access points.
- Management system must provide single screen view of overall network, user, and security status and “posture”.
- Must support administrative rights partitioning - different admins have different rights.
- Configuration and policy changes must be applied globally to all systems and AP’s from a single entry point.
- System must provide for accurate, real-time location tracking of devices and users including rogue AP’s and security violators.
- System must provide visual RF maps of actual coverage and data rates without the requiring baselines of network signals and/or material modeling of facilities.
- Solution must not require external management systems.

Solution

- Must support chassis, box and N+1 redundancy with under 20 seconds failover time.
- Newly installed controllers must be synchronized automatically with the already existing controller(s), without requiring a separate network management server.
- The same software, configurations and functionality must be supported across all platforms in the product family proposed.
- System must support a software-only upgrade 802.11abg to 802.11n.

Terms and Conditions

General Requirements

The diocese reserves the right to reject any and all proposals received as a result of this request for proposal, or negotiate separately with any source whatsoever in any manner necessary to serve the best interest of the diocese.

The contents of the proposal of the successful vendor(s) may become contractual obligation, if a contract ensues. Final contractual obligations will be determined through contract negotiation between the Diocese of Camden and the selected vendor.

Non-response

In the event you do not desire to respond, please submit a "NO BID" letter indicating your organization will not be submitting a response.

Pricing

Vendors must affirm that the purchase price of the system will be valid for a minimum of 90 days from the date the proposal is submitted.

Cost of RFP Preparation

The Diocese of Camden will not pay any costs incurred in RFP preparation, presentation, demonstration or negotiation, and does not commit to procure or contract for any services. All costs of RFP preparation shall be borne by the vendor.

Confidential and Proprietary Information

All materials received in response to this RFP may be made available to the public. If any part of a vendor's proposal is proprietary or confidential, the vendor must so identify and so state. The Diocese reserves the right to retain all RFP's submitted, whether or not the RFP was selected or judged to be responsive.