



Wireless Access & Security

April 7, 2008

GROUNDFORCE™ IT

www.GroundForceIT.com ■ tel: 804.553.2456

- Welcome
- Wireless & Network Terminology
- Access Point Considerations
 - What Band?
 - How many?
 - Where?
 - Channels & Antennas
 - Controller Based Architecture
 - Site Survey & Access Point Placement
- Security Concerns & Solutions
 - Encryption
 - Authentication
 - VLANs & Guest Access
- Network Infrastructure
 - Basic Architecture
 - Using VLANs to separate, secure, & track traffic
- Conclusions
- Q & A

GroundForce IT Services Include:

- Infrastructure design, implementation, and support
- Server Virtualization and Consolidation
- Virtual Private Networking/Remote Access
- Security Audits and Assessments
- Desktop hardware and peripheral support
- Hardware and Software Procurement



802.11 – Wireless standard first defined in 1997 by the IEEE. Maximum of 2Mb transfer

A – The same core protocol as the original standard, operates in 5Ghz band with a maximum raw data rate of 54 Mb. Has a lower range than the 2.4Ghz bands, but has 7x the number of discreet channels

B – Based on the original standard with increased throughput to 11Mb. Unlike A, B operates in the 2.4Ghz space giving it only 3 discreet channels, but with greater range

G – An extension of the 802.11b amendment that offers greater throughput of up to 54Mb. Fully compatible with 802.11b

N – Emerging amendment that extends both 802.11a & g to allow for operation in both the 5Ghz space for density and the 2.4Ghz space for range. Also allows for up to 248Mb of throughput with the use of multipathing of traffic (MIMO). Not expected to be finalized until late 2008

Access Point – The piece that connects wireless clients to the rest of the network. APs are wireless equivalent of a wired hub

OSI Model – 7 layer model that standardizes communication between networked hosts. For the purposes of today's discussion we will be working with layers 2 (Data-link) & 3 (Network)

Power over Ethernet (PoE) – IEEE standard that Allows for the transmission of power over a standard Ethernet connection. There are 2 "standards": 802.3af and Inline Power

RADIUS – Remote Authentication Dial-In User Service. A old service that we use to authenticate users to a central directory or server.

SSID – Service Set Identifier. Essentially the name of a wireless network.

Wireless Controller – An appliance or server that manages multiple access points as a single entity. Often these allow for a set of advanced features not available with independent APs

WEP – Wired Equivalency Privacy – Not really. This was the first standardized attempt to secure wireless traffic. WEP still works, and is supported by almost all devices. However, WEP has several well publicized vulnerabilities and is no longer considered “secure”

WPA – Wi-Fi Protected Access. Designed to replace WEP. Offers stonger security and better authentication.

VLAN – Virtual LAN. Used by routers and switches to allow the segmentation of a physical network into multiple logical networks using one set of networking equipment

What 802.11 band do I use? How many APs do I need? Where do I put these things?

Depends on the number of concurrent users, range, obstacles, AP density, and the type of antennas your installation calls for

- **Concurrent users**
 - Most APs will accommodate ~ 20 connections. Wireless bandwidth is shared, so the more users/ AP the slower data moves.
- **Signal range – With all of these**
 - 802.11 A – ~100 ft. Indoors / ~300 ft. Outdoors
 - 802.11 B – ~120 ft. Indoors / ~ 350 ft. Outdoors
 - 802.11 G – ~120 ft. Indoors / ~ 350 ft. Outdoors
 - 802.11 N – ~200 ft. Indoors / ~ 600 ft. Outdoors
- **Obstacles & building layout**
 - Range and throughput decrease as the number of obstacles increases. 2.4Ghz bands have better penetrating capability and can easily penetrate most non-metallic obstacles. 5Ghz bands can penetrate most interior walls but is generally stopped by denser exterior walls
- **Access Point density**
 - 5Ghz – Where 5Ghz does not provide the indoor range of the 2.4Ghz bands it has more discreet channels (21), allowing for more access points to be in close proximity to each other without interference
 - 2.4Ghz – The 2.4Ghz band in North America has 11 channels, but because of narrow differences in the channels there are only 3 discreet channels. Placing more than 3 b/g APs in close proximity can cause interference resulting dropped connections and low throughput
 - 802.11 N – 802.11n melds the best of both bands by using both. This allows for best of both worlds devices and flexible deployments
- **Antenna types**
 - Omni-directional – Broadcast signal in all directions with equal strength. These are the standard antenna on most all devices
 - Uni-directional – Broadcast the signal in one direction for a strong coverage area with little interference to neighboring coverage areas
 - Yagi's – Very specialized antennas generally used for wireless bridging. They are uni-directional and broadcast over long distances

Using a Controller Based Architecture

- Access points become “config-less”. The Wireless Controller handles all of the work of the wireless network, effectively making the APs remote antennas of the Controller
- Some controller based architectures offer advanced features such as device tracking, guest access and provisioning, and time and bandwidth limits.
- Some controllers even allow for roaming at both Layer 2 and Layer 3, which means less time between AP changes – No more drops as you walk through a building
- Controller architectures are vendor specific. Generally any client will do but the APs and controller must be from the same vendor, some even go so far as to require vendor specific routers and switches.

Answer all of your questions with a wireless site survey

We recommend getting a wireless site survey done prior to deploying any wireless solution. A wireless survey can save money and lots of aggravation by providing a shopping list of access points and accessories, as well as specific placement and configuration plans. Some of the most common issues associated with large wireless deployments stem from poor AP placement or “flooding” and area with too much signal, both resulting in low or poor signal.

Authentication

- Pre-Shared Key
 - Simple password or hexadecimal key that must be given to each user/ device that accesses the wireless network
 - The key is the same for all devices on each SSID
 - If the key changes it must be redistributed to each user/ device and manually input
 - Pre-Shared keys are fine for small workgroups and for guest access networks, but lack the security required for larger internal deployments
 - Both WEP and WPA allow for the use of a pre-shared key
- RADIUS
 - Users and devices authenticate against a central user directory
 - Can be tied to an existing directory service such as Active Directory or Open Directory
 - The user's/ device's account and password serve as credentials to access the network, everyone has unique credentials. Changing a user's password affects only that user
 - Can be used to dynamically assign SSID/ VLAN based on the user's directory group membership
 - Only WPA is designed for use with RADIUS authentication, some vendors allow for a proprietary WEP deployment that uses RADIUS

Encryption

- **WEP - Wired Equivalent Privacy**
 - The original specification for allowing data privacy and integrity.
 - First introduced in 1999
 - WEP uses either a 64 or 128 bit key to provide data integrity and encryption
 - WEP has 2 forms of Authentication, Open and Shared
 - Open Authentication is misleading. Open actually means none, any device can associate with the AP
 - Shared Authentication uses a shared key that users must enter to access the wireless network
 - In 2001 several groups published papers outlining weaknesses in WEP. Today WEP 128 encryption can be broken with widely available software in minutes.
 - All devices share the same key
- **TKIP - Temporal Key Integrity Protocol**
 - TKIP is an extension of WEP that resolves the identified problems in WEP
 - Each device has a unique key that is recalculated on each new connection to an AP, or on a scheduled basis
 - Developed for use with WPA
 - Has no known vulnerabilities. Cracking a TKIP encrypted packet would take from months to years
- **AES - Advanced Encryption Standard**
 - Most secure encryption standard
 - Uses a unique key that is recalculated on each new connection to an AP, or on a scheduled basis
 - Used for WPA2
 - Has no known vulnerabilities. Cracking AES encrypted packet is reported to be impossible
 - WPA2 specific wireless hardware is recommended

Basic Infrastructure

- Integrate wireless into the existing network
- Use existing switches and IP network to support wireless clients
- Speed limitations of wireless can affect the wired network
- All wireless traffic is broadcast, this can expose sensitive data to the world
- No opportunity for guest access or for securing different traffic streams

Advanced Infrastructure

- In most cases existing switches need to be replaced with new equipment
 - Layer 3 capable switches allow for the routing of traffic with out the need for traditional routers, and compose the distribution layer of the network
 - Less expensive layer 2 switches and access points that support VLANs are used for the access layer of the network
- VLANs allow for separation of traffic based on security, source, type, and location
 - Separate Servers, Students, Faculty, management, and wireless traffic
 - Separate buildings, halls, and classrooms
 - Separate voice and data traffic
 - Access lists can be used to limit traffic between VLANs without a firewall
 - Eases management and identification of client devices
- Guest Access
 - Allow access to the internet through your network to visitors with out exposing your internal network
 - Use a controller based architecture
 - A “locked down” VLAN
 - Controllers have added security & customization features, like a sign-on page and time/bandwidth limiting
 - A “locked down” VLAN can achieve an acceptable level of security with out the “creature comforts”

List Pricing Information:

Aironet 1130AG Access Point (MSRP - \$699):

- A lightweight version
- An autonomous version that can be field-upgraded to lightweight operation
- A single-band 802.11g version for use in regulatory domains that do not allow 802.11a/5 GHz operation

Cisco 4402 Wireless LAN Controller (MSRP - \$9995 – \$19,995):

- Configurations that support up to 12, 25, and 50 lightweight access points.
- Two Gigabit Ethernet Ports
- One expansion slot

Cisco 4404 Wireless LAN Controller (MSRP - \$34,995):

- Configurations that support up to 100 lightweight access points.
- Four Gigabit Ethernet Ports
- Two expansion slots

Cisco Catalyst 3750 –25WS (MSRP - \$20,500 - \$25,500):

- Integrated Wireless LAN Controller functionality for WLAN security, mobility and ease of use with support for up to 25 or 50 access points per switch and 100 per stack
- 24 Ethernet 10/100/1000 ports with Power over Ethernet and 2 small form-factor pluggable (SFP) transceiver-based Gigabit Ethernet ports
- Innovative stacking technology

Q&A

Presentation Deck can be found at:

events.GroundForceIT.com