Wireless Networking & VPNs

Marconi Invents Radio 1897 & Wireless Telegraphy 1901

So What’s New…

The Application

William J Burkhard
Director, Electronic & Computer Services
149 Hammond Bldg
University Park, PA 16802
Discussion Topics

- History
- Standards
  - Ethernet
  - Wireless Ethernet
- Specifications
- Wireless Networking Topologies
- Issues
- The Virtual Private Network (VPN)
- College of Engineering Implementation
- What Else… 3G & What’s Next?? … 4G
- Summary

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
Wireless History

- Marconi Invents the First Transmitter in 1897 & Wireless Data Communications (Telegraph) in 1907.
- Actress Hedy Lamarr & Composer George Antheil Received a U.S. Patent in 1942 for Developing the First Frequency Hopping Spread Spectrum System that was Quickly Classified.
- In 1981 the U.S. Government Declassified the Lemarr/Antheil “Secret Communications System”.

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
Standards
OR – Where Did 802.11a/b/g Come From

- Protocol Built Around the IEEE 802 Standards Base for Ethernet Data Communications: -- The Physical Media Side
  - 802.3 – Defining the Ethernet Open Standard Interconnection (OSI) Model, Frame Format, Ethernet Addressing, Carrier Sense Multiple Access with Collision Detection (CDMA/CD), and Common Media (10Base2, 10Base5, 10BaseT & 10BaseFL)
  - 802.3u – Fast Ethernet in 1995 Opens up 100Mbps services: 100BaseTX & 100BaseFX
  - 802.3x – In 1995 the IEEE Approved the Standard that Opened up “Full-Duplex” Data Communications
  - 802.3ab – 1000BaseT OR Gigabit Over Copper Established Circa 1997.
  - 802.3z – Ratified in 1999, Set Standards for Gigabit Ethernet Over Fiber: 1000Base–SX, 1000Base–LX & 1000Base–CX
- Other Protocols Not Discussed:
  - Token Bus Standard (802.4), Token Ring (802.5), Ethernet over Type 2 Wiring or Fiber Distributed Data Interface (FDDI)
Relating the OSI Model To the IEEE Standards

OSI Layer

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

IEEE Standard

<table>
<thead>
<tr>
<th>OSI Layer</th>
<th>IEEE Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>PHY – Physical Connectivity</td>
</tr>
<tr>
<td>Data Link</td>
<td>LLC – Link Layer Control, MAC – Media Access Control</td>
</tr>
</tbody>
</table>
| Network | 802.2
| Transport | 802.3, 802.4, 802.5, 802.11
| Session | CS, TR |

802.2
802.3
802.4
802.5
802.11
Wireless Standards

Base Characteristics of 802.11

- Protocol Built Around the IEEE 802 Standards
  Base for Ethernet Data Communications: --
  Wireless Media

  - 802.11 – The Standard was Adopted by the IEEE in Ratified 1997 & Approved in Sept. 1999 – BUT Products were out there much earlier!

    - Specifies Wireless Connectivity Constraints for Fixed, Portable Clients
    - Constrained to a Limited Geographic Coverage Area
    - Defines the Interface Between Wireless Clients & Access Points
    - Deals with Fragmentation of Data Packets, Error Recovery, Mobility Management & Power Conservation
    - Specifies that Transmitted Data Rate Throughput Must be a Minimum 1Mbps.
Wireless Standards

The 802.11__ Family

- **802.11b** – First Deployed Units; Operate @ 2.4GHz; Provide a Maximum of 11Mbps Throughput; Operates Across 11 Channels to Minimize RFI Effects... Only 3 are Usable Because of Channel Overlap... 2.4 GHz Portable Analog Phones Interfered with Early Units Throughput
- **802.11a** – Deployed After 802.11b; Operate @ 5GHz; Provide a Maximum of 54Mbps Throughput; Operates Across 8 Channels That are all Usable... Operates at Shorter Ranges Than 802.11b
- **802.11g** – Provides 54Mbps Maximum Throughput @ 2.4GHz; Operates Across 14 Channels BUT FCC Regulations Limit Use to 11; Only 3 of the Usable Channels do not Overlap.
Wireless Standards
The 802.11__ Family

• **802.11e** – Proposed IEEE Standard to Define QOS Mechanism for Wireless Equipment that Supports Bandwidth Sensitive Applications; e.g., Voice & Video

• **802.11f** – Still in Works at Attempting to Define an Inter-Access Point Protocol to Facilitate Roaming Across Multiple Vendor’s Access Points

• **802.11h** – Attempts to Improve Channel Energy Measurements/Reporting, Channel Coverage in Regulated Domains, Dynamic Channel Selection & Transmit Power Control

• **802.11i** – Specifies Improvement in MAC Level Wired Equivalent Privacy (WEP) Security *(WEP is Generally Considered Insecure)* Algorithm by Removing Security Flaws Through Encryption & Authentication {Advanced Encryption Standard (AES)– 256 bit Encryption} … *Task Group’s Recommends Use of Virtual Private Network Appliance*

• **802.1x** – Currently in the IEEE Task Group; Aimed at Improved Security Through Port Authentication Protocol & Applies Equally to Wired or Wireless; Includes a Supplicant (Client), an Authenticator, & an Authentication Server.

• Together, 802.11i Combined With 802.1x Will Provide The Authentication, Security and Tunneling Performed by the Virtual Private Network (VPN) Appliances Used Today.

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
## Wireless Standards

### Performance Summary

<table>
<thead>
<tr>
<th>Standard</th>
<th>Freq (GHz)</th>
<th>Data Rate</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>5.1–5.2</td>
<td>54 Mbps</td>
<td>Maximum Power in mw: 5.1 Band–40; 5.2 Band–250; &amp; 5.7 Band–800; Non Overlapping Channels–12 FCC mandates that only 8 are useable</td>
</tr>
<tr>
<td></td>
<td>5.2–5.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.7–5.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4–2.485</td>
<td>11 Mbps</td>
<td>Maximum Power in mw: 800 Non Overlapping Channels–3 of 11</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4–2.485</td>
<td>36 or 54 Mbps</td>
<td>Maximum Power in mw: 800 Non Overlapping Channels–3 of 11</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>2.402–2.48</td>
<td>1 Mbps</td>
<td>Maximum Power in mw: 100 Maximum Number of Devices: 26 Maximum Range: 10–100m Frequency Hopping: 79 Hops</td>
</tr>
<tr>
<td>Not 802.11</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Technology Comparisons

<table>
<thead>
<tr>
<th></th>
<th>802.11a</th>
<th>802.11g</th>
<th>802.11b</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
<td>5GHz, Number of Non Overlapping Cells; Better Performance</td>
<td>Crowded 2.4GHz Band; Cell Overlap &amp; Less Throughput</td>
<td>Crowded 2.4GHz Band; Cell Overlap &amp; Less Throughput</td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
<td>8 Usable Channels= 432Mbps</td>
<td>3 Usable Channels= 162Mbps</td>
<td>3 Usable Channels= 33Mbps</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>Shorter Range/ Wavelength &amp; FCC Limit</td>
<td>Greatest Range</td>
<td>Greatest Range</td>
</tr>
<tr>
<td><strong>Interference</strong></td>
<td>Fairly Open 5GHz Band</td>
<td>Crowded 2.4GHz Band; Interference Prone</td>
<td>Crowded 2.4GHz Band; Interference Prone</td>
</tr>
<tr>
<td><strong>Migration</strong></td>
<td>Incompatible with 802.11b/g</td>
<td>Compatible with 802.11b</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Installation Flexibility</strong></td>
<td>Fixed Antenna Only; Restricted by FCC</td>
<td>External Antenna Allowed</td>
<td>External Antenna Allowed</td>
</tr>
</tbody>
</table>

**Advantage**  **Disadvantage**

wjb   November, 2004   Electronic & Computer Services   Embracing the Future Today
Wireless Networking Topologies
Independent Basic Service Set

aka– Ad Hoc Wireless Networks
Wireless Networking Topologies
Independent Basic Service Set

aka—Ad Hoc Wireless Networks
Wireless Networking Topologies
Basic Service Set

High Speed Backbone

Ethernet Switches

Wireless Cells

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
802.11b Wireless Range Profiles

If limit of range is 90 ft, for best rates must be within 22 ft.

Throughput

Range

11 Mbps
5.5 Mbps
2 Mbps
1 Mbps

11 Mbps
5.5 Mbps
2 Mbps
1 Mbps
802.11g Wireless Range Profiles

If limit of range is 90 ft, for best rates must be within 22 ft. 802.11g provides higher data rate over 802.11b
Theoretically, 802.11a should cover ~75% of the area of an 802.11b/g radio.
ISSUES

• Service Requirements: Selective Versus Full Coverage; Indoor/Outdoor Coverage
• Performance Limitations: Range, Attenuation, Penetration, Multipath
• Cost
  ◦ Reduced When Deploying Selective Coverage Plan
  ◦ Increased When Covering Outdoors
• Range Limitations
  ◦ 802.11b/g Range Can Be Extended With External Antennas
• Interference Susceptibility
  ◦ 2.4GHz Portable Phones May Effect Throughput
• Shared Media – More Users…Slower Response
  ◦ Can Be Mitigated by Auto Load Sharing/Load Balancing
• Security–(WEP is Insecure!)
  ◦ Virtual Private Networks (VPNs), Restricted User Base, Authentication
  ◦ 802.11i & 802.1x Will Replace VPNs
The BIGGER Issues!

- Stealing Bandwidth
- Eavesdropping
- Stolen Data
- Modification & Insertion
- Impersonation
- Denial of Service (DoS)
The BIGGER Issues!

- Stealing Bandwidth
- Eavesdropping
- Stolen Data
- Modification & Insertion
- Impersonation
- Denial of Service (DoS)
General Antenna Patterns

Beamwidth

Horizontal Pattern

Beamwidth

Vertical Pattern
Dipole Antenna

Frequency Range 2.4–2.484GHz
Typical Gains... 2.2–5.5 dBi
Nominal Gain... 3dBi
Maximum Power ~ 10 Watts
Short Range: 90–150 ft.

Horizontal
BW=360°

Vertical
BW~60°

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
Omni Directional Antenna

Frequency Range 2.4–2.484GHz
Typical Gains... 4–15dBi
Nominal Gain...6 dBi
Maximum Power ~ 100 Watts
Typical Range: 120–175 ft

Vertical BW~28°

Horizontal BW=360°
Flat Panel Antenna

Frequency Range 2.4–2.484 GHz
Typical Gains... 3–19 dBi
Nominal Gain... 8 dBi
Maximum Input Power ~ 100 Watts
Medium Range: 150–250 ft
Yagi Antenna

Frequency Range 2.4–2.484GHz
Typical Gains… 8–14 dBi
Nominal Gain…12dBi
Maximum Power ~ 100 Watts
High Range: 1-5 miles
Parabolic Antenna

Frequency Range 2.4–2.484GHz
Typical Gains… 20–40 dBi
Nominal Gain… 25 dBi
Maximum Power ~ 100 Watts
Long Range: 10–15 miles
Selected Coverage Plan

8 Units

Electronic & Computer Services

Embracing the Future Today

wjb  November, 2004
Networking Topology

University Backbone

Internet

Router

Open Network vs Secure Network

Switches
Networking Topology

University Backbone

Firewall/VPN

Switches

Router

Internet

Open Network vs Secure Network
**Virtual Private Network (VPN)**

- **Definition:** A private network constructed over a public network that uses data encryption and IP transport or tunneling modes to facilitate secure data communications over the public network and internet.

- **Transport Mode v.s. Tunneling Mode:**

<table>
<thead>
<tr>
<th>Original IP datagram</th>
<th>IP Hdr</th>
<th>Payload</th>
<th>Trailer*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Mode</td>
<td>AH/ESP Hdr</td>
<td>IP Hdr</td>
<td>Payload</td>
</tr>
<tr>
<td>Tunnel Mode</td>
<td>New Hdr</td>
<td>AH/ESP Hdr</td>
<td>IP Hdr</td>
</tr>
</tbody>
</table>

AH– Authentication Header
ESP– Encapsulating Security Protocol * ESP Only
Some Terminology

- Virtual Private Network (VPN): A mechanism for establishing secure point-to-point connectivity between a client and parent network through the insecure internet or wireless computing environment.

- Internet Protocol Security (IPSec): Standards as established by the Internet Engineering Task Force (IETF) that defines a set of security policies that provide for confidentiality, integrity, and authentication.

- Authentication Header (AH): An IPSec protocol providing origin authentication, packet integrity, protection from attacks, and tunneling capability.

- Encapsulating Security Payload (ESP): An IPSec protocol providing a range of services that include encryption, authentication, tunneling, and protection from attacks.

- Key: The Key is a cryptolographic algorithm that produces ciphered text for secure authentications and communications between a source and destination.

- Data Encryption Standard (DES) & Triple DES (3DES): DES–A symmetric key bulk encryption mechanism that uses a 56-bit key. 3DES–Enhances the security of data by applying the encryption algorithm 3 times with different sub keys.
IPSec Data Encryption Process

- IPSec involves a process that takes place between two parties, the Sender & Receiver.
  - The Relationship is Called a “Security Association,” also called Session or Connection.
  - The process culminates with a “Secure Session” between the two parties.

1. Both Sender and Receiver obtain a Key using an IPSec supported technique: manually, statically, or or dynamically.
2. The “Security Association” exists once the Key is established & maintained by the Sender & Receiver.
3. The Sender “hashes” its data using the keyed value. This produces a digital signature that can only be read by the specific receiver.
4. The sender encrypts the data according to the ESP algorithm used: DES or 3DES. This resulting scrambled data is the ciphertext.
5. The sender transmits the secure packet over the network towards its destination.
Putting It All Together

University Backbone

Software VPN Client Resides on User’s Computer

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
Putting It All Together

University Backbone

Firewall/VPN

Software VPN Client
Resides on User’s Computer

Internet

Client on Remote/Laptop Computer
Establishes Communications
Link/Tunnel Over which Secure
Communications may Pass
1. Client Contains Communications Protocols
2. Client Communicates with VPN & Establishes Key
3. Secure Session Opened AND
   • Sender applies Hash Algorithm to Data Packets
   • 3DES ESP Encoding Applied to Data Packet
   • Tunnel Mode Established
4. User Authentication Process Proceeds
5. User Authentication Approved
6. Session Opening Confirmed
7. Secure Communications into Network Begins
VPN – Pros & Cons

- Customer Perspective:
  - Pros:
    - Accessibility Independence
    - Service Provider Independent
    - Guaranteed End-to-End Security
  - Cons:
    - Requires Client Software
    - Possible Initial Configuration Complexity
    - Multiple Configurations
    - Potential for Inconsistent Performance

- Service Provider:
  - Pros:
    - Possibly Other Related Services
    - No Additional Infrastructure
  - Cons:
    - Lack of Control
COE Wireless Network

Electronic & Computer Services

Embracing the Future Today

wjb  November, 2004
4G Embodies all the Concepts of 3G But Goes Beyond & Begins a New Paradigm in Data & Voice Communications
What Else... 4G

- AVNet
  - Digital TV
  - VCR
  - DVD

- PC Net
  - PC
  - VideoPhone
  - Web Pad

- Living Net
  - Refrigerator
  - Air-Conditioner
  - Washing Machine
  - Microwave Oven

3G Handsets
PDA
Internet Connection
Home Server
Grow Rates

Millions of Users

- Laptop/PDA
- Cell Phones
- Internet

2000  2001  2002  2003

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
3G Service Projections

- Simple Voice
- Mobile Internet Access
- Multimedia Messaging Service
- Customized Infotainment

Worldwide Subscriptions (in millions)

02 03 04 05 06 07 08 09 10

wjb  November, 2004  Electronic & Computer Services  Embracing the Future Today
Summary

- Wireless Standards are Built on and are a Subset of the IEEE 802.11 Ethernet Standards
- 802.11a/b/g
  - Radio Output Powers are Regulated by the FCC
  - “a” & “g” Have Identical Throughputs of 54Mbps Max; “b” only has 11Mbps Max
  - Inherently “b” & “g” Have Greater Range & can Have External Gain Added for Extended Range
  - “a” is Less Susceptible to RFI
  - “a” has 8 Usable Non-Overlapping Channels; “b” & “g” Only Have 3
- Other Wireless Standards Address Roaming Across Multiple Vendor APs, Channel Energy Issues, Regulated Domain Requirements, Dynamic Channel Allocation, and Security Issues
- VPNs Provide a Mechanism for Establishing Secure Point-to-Point Encrypted Connectivity Between a Client and Parent Network
- 3G Wireless Aims at Mobile Communications Networks Integrating Multiple Device Technologies into a Seamless Communications Environment
- 4G Wireless Focuses on Integrating Many More Traditional Devices into the Environment
- Almost Exponential Growth to ~1.6 Billion Voice Subscribers Worldwide and Steady Growth to 900 Million Mobile Internet, 600 Million Multimedia Service & 200 Million Customized Infotainment Worldwide Service Subscribers
References

• LG International: http://www.lgicorp.com/