INTRODUCTION

Customer Case Study: KPMG
Eric Peter, KPMG IT Manager
KPMG Luxembourg Overview

• 3 Buildings – in total 200 Antennas
• 750 users

Business Challenge

• Mobility
• Voice capable
• Guest control

Solution Provided

• Centralized Management Solution: Cisco Unified Wireless System
• Security: Encryption, LWAPP tunneling...
• Solution fully redundant

AGENDA

→ The Goal of WiFi in the Enterprise

1) Concepts of a Centralized Solution
   • Before / Today
   • Dynamic Control

2) Voice over Wireless (WVoIP)
   • Dynamic Transmit Power Control
   • Coverage Issues
   • Security and Optimization

3) Specific Case of Guest Access
   • On-Demand Access
   • The Anchor Model

4) Connectivity Security
   • Security Method Summary
   • MFP and IDS Shunning

5) Air Protection
   • Rogue Detection
   • Containment
   • Localization

→ Case Study
   • KPMG
   • Customer References
The Goal of WiFi in the Enterprise

- Access anywhere and anytime = MOBILITY
- Providing a secured wireless connection to the corporate network’s services, and a controlled connection for guests!

AGENDA:
Part 1

Concepts of a Centralized Solution

Wednesday, October 24, 2007
A Single Unified WLAN System

Services:
- WLAN service delivery
- Real-time RF management
- Encryption/authentication
- Intrusion protection (IPS)
- Location tracking
- Capacity Management
- Seamless mobility
- Guest Access
- Dynamic Control

Channel Assignment can only be DYNAMIC because ...

Channel layout should also be considered in 3-dimensions.
Radio Resource Management (Auto-RF)
Real-Time RF Management

- The RF domain is an ever changing environment
  - Users are mobile
  - Interference prone

- The controller has a system level view of the RF domain and adjusts individual access points to optimize coverage and network availability

Benefits

- An optimized RF environment allows for superior application performance and higher network availability
- Complete RF management without specialized RF skills
- No RF recalibration required – decreased support costs

Client Roaming & Dynamic Load Balancing

- Dynamic client load balancing
- Solving performance & capacity problems in high density areas
  - e.g. conference rooms, cafeteria…
- Infrastructure and clients (via CCX) determine optimal load balancing

Benefits

- Preserves application and network performance
- Guarantees bandwidth and lower latency for network sensitive applications (e.g. voice over IP)
- Decreased support costs; increased user satisfaction
Business-Class Reliability for Mission Critical Mobility

Maximized system availability
- Controller redundancy
- Access point failover

System level management automates failover to guarantee availability

- No single point of failure
- Automated network failover decreases support and downtime costs
- Wireless network reliability on par with wired

AGENDA:
Part 2
VoW (Voice over Wireless)

Wednesday, October 24, 2007
DTPC helps for Voice!

- Wireless phones support 1, 5, 20, 50, 100 mW transmit power.
- If advertising a non-supported rate, the phone will roll up to next transmit power.
  - Prevents one-way audio
  - Otherwise RF traffic is only heard in one direction!

100mW 5mW

This is also why it is important to respect some coverage rules:

- The RADIUS of the Cell Should Be: -67 dBm
- The phone should see at any place:
  - 2 AP with a minimal RSSI=35
  - and Channel Utilization (CU) must be < 45

COVERAGE: Strategic Areas
Security and Optimization for Voice

→ Authentication
  • WPA2
  • WPA
  • WPA-PSK
  • CCKM
  • EAP-FAST
  • LEAP

→ Encryption
  • AES
  • TKIP/MIC
  • WEP (40/128 bits)

→ Infrastructure
  • Image Authentication
  • Device Authentication
  • Encrypted Files
  • Signaling Authentication
  • Signaling Encryption (TLS)
  • Media Encryption (SRTP)

→ Mode Selection
  • Auto-sensing, a preferred over b/g
  • Auto-sensing, b/g preferred over a
  • Fixed 802.11a
  • Fixed 802.11b/g
  • Received Signal Strength Indication (RSSI) – Default

All the blocks for a Complete Solution

Authentication/Encryption
Nokia Device Management
Call Manager Registration
AGENDA:
Part 3

The Specific Case of Guest Access

Web Authentication Feature

- Efficient control of “on-demand” access for guest services
- Soon (with WCS v4.2), will be also possible for wired access!
**Guest Access Securisation 1/2: Routing to FW**

- For zero configuration on guest’s PC, we use Open Authentication.
- Traffic is limited to a specific VLAN that can only discuss with the firewall.
- Traffic can be played on your internal network...
- Specific additional routing and switching configuration required!

**Guest Access Securisation 2/2: Anchor Model**

- **Benefits of virtual anchor:**
  - Ports on the firewall:
    - UDP 16666 for tunnel control traffic
    - IP Protocol 97 for user data traffic
    - NO NAT CONFIGURED ON THE FIREWALL (The tunnel cannot support it)
Summary Traffic Flow

- Basic Open access for Guest (No config required on PC!)
- Web authentication with “On-Demand” username/password creation for a limited period of time
- Tunneling of the Guest’s traffic directly to External Zones (like DMZ)
- Direct Routing to Internet WITHOUT USING YOUR LAN GATEWAYS!

AGENDA:
Part 4
Connectivity Security

Wednesday, October 24, 2007
## Security Method Summary

### Encryption

<table>
<thead>
<tr>
<th>Method</th>
<th>SOHO (no authentication server)</th>
<th>Enterprise (802.1x based)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCMP (AES)</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>TKIP</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>CKIP</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Dynamic WEP</td>
<td>☒ (WEP)</td>
<td>☒ (WEP)</td>
</tr>
<tr>
<td>Static WEP</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Open</td>
<td>☒</td>
<td>☒</td>
</tr>
</tbody>
</table>

### Authentication

- **None or SSID**
- **MAC**
- **Shared key**
- **PSK**
- **LEAP or EAP-FAST**
- **Other EAP types**

## CCX (Cisco Compatible Extensions)

### CCX v1
- 802.1x authentication
- EAP-TLS and LEAP
- Cisco pre-standard TKIP
- Client rogue reporting

### CCX v2
- WPA compliance
- Fast roaming with CCKM
- PEAP

### CCX v3
- WPA2 compliance
- EAP-FAST
- CCKM with EAP-FAST
- AES encryption

### CCX v4
- CCKM with EAP-TLS, PEAP
- WIDS
- MBSSID
MFP: Management Frame Protection
The only real protection against MiM attacks

→ Problem:
• there’s no “physical security” for wireless and management frames are not authenticated, encrypted, or signed.

→ Solution:
• Insert a signature (Message Integrity Code/ MIC) into the management frames:
  – AP beacons
  – Probe requests/responses
  – Associations/re-associations
  – Dissociations
  – Authentications/de-authentications
  – Action management frames

• Specifics of MFP “MIC”:
  – MFP Information Element adds timestamp, sequence number
  – MIC key to management frames
  – MFP employs HMAC-SHA1 hash algorithm to calculate MIC key

→ Initially it has been deployed as a proprietary security mechanism to validate infrastructure equipments
→ Today it is extended to client adapters via CCX version 5 !

IDS and Client “Shunning”

1. Malicious traffic
2. Wired IDS 4200 series IDS Sensor
3. Deep Packet Inspection
4. LWAPP Encapsulated

1. Client to AP/Controller
2. Controller to IDS
3. Client Block event at sensor, retrieved by controller

Cisco Controller

1. Poll
2. Shun
3. Controller to IDS
4. Disassociation
BE PROTECTED AGAINST UNDESIRED WIFI?

→ “NO WIFI IN MY HOUSE” Policy ??? Is it realistic ???

   NO !

   Simply because WiFi uses free licensing frequencies.
   Your neighbor is allowed to send you waves !

→ SO THE BEST PROTECTION AGAINST WiFi IS...

WiFi
Rogue Access-Point Detection

Alarms can be assigned for tracking.

A Rogue's state can be:
Unknown - Alert
Known - Internal
Unknown - External

Annotation area to track resolution

RF Fingerprinting places rogue on map to 10 meter resolution

Real-Time Cartography Reporting
Tracking over Time

Customer Case Study: KPMG

Wednesday, October 24, 2007
Overview of KPMG Design

Main Campus
- LWAPP local
- VLAN-abc
- DHCP Assignment
- WiSM

Up to 300 AP managed!

Backup Campus
- LWAPP local
- VLAN-def
- DHCP Assignment
- WiSM

Load Sharing & Complete Redundancy of 300 AP!

Branch Office
- LWAPP local
- VLAN-xyz
- DHCP Assignment
- WiSM

Guest / visitors' access with Web Authentication
Corporate employees' access with strong policies
Corporate voice access with strong policies & high quality

Practical References in Luxembourg

uni.lu
UNIVERSITÉ DU LUXEMBOURG

Cargolux

Husky
Keeping our customers in the lead

CEGEDEL
End, but …

Questions ???