Cisco Unified Mobility
Wireless Network

Greg Gordon
Cisco’s Wireless Technology Vision

**Wireless Connectivity**
- Best in class range and throughput
- Simple to deploy and manage
- Enterprise-class Security
- Capital Efficiency

**Centralized WLAN Systems**
- Centralized Management and Control
- Layer 2/3 Mobility
- Wireless IDS/IPS
- Hierarchical approach for scalability
- Location aware, voice support

**Wired+Wireless Integration**
- Integrated and Unified Security (AAA, Firewall, IDS/IPS, etc)
- Exploding number of Wi-Fi Clients (dual-mode PCS Phones, Video PDAs)
- Higher-capacity, higher-density WLANs (Pico Cells)
- Unified wired+wireless support for applications (Voice/Video, Location, AAA)
- Extending networking outdoors (mesh, outdoor AP, etc.)
- Enterprise scalability and reliability
A Unified WLAN System

Cisco:
- WLAN service delivery
- Real-time RF management
- Encryption/authentication
- Intrusion protection
- Location tracking
- Capacity Management
- Seamless mobility
- Guest Access
- Centralized management
- Dynamic Control
LWAPP Overview

- LWAPP is the protocol between an LWAPP AP and its controller
- The LWAPP Model is referred to as split MAC, with the Controller managing some MAC functions and the AP others
- Part of the split MAC is a layer 2 tunnel between AP and Controller
- This tunnel is one of the functions of LWAPP
- LWAPP Comes in two versions Layer 2, and Layer 3
- Layer 2 LWAPP Encapsulates the traffic into Ethernet Frames
- Layer 3 LWAPP Encapsulates LWAPP Frames in UDP
LWAPP is now Changing into CAPWAP

What is CAPWAP?

- CAPWAP (Control and Provisioning of Wireless Access Points) is a Tunnel protocol between AC and WTP a.k.a Controller and AP
- CAPWAP is based in initial draft of LWAPP
- CAPWAP is in IETF (version 10) draft pending approval

Just Like LWAPP, CAPWAP …
- WLC uses AP-Manager Interface(s) to manage APs
- APs discover WLC’s management address
- APs Join WLC and form CAPWAP tunnel using WLC’s AP manager interface
Cisco Unified Wireless Solution

Security

Rogue APs—Employees create opening to enterprise network unknowingly

DoD Policy

Guest Access

Performance

- RRM Dashboard
- RF Monitoring
- Spectrum Expert
- Client reporting

Products
Cisco Unified Wireless Network

Security Features
Cisco Unified Wireless Security Solution

Fine-grained Mapping and Authentication
Location services enable precise mapping of clients and threats, allowing fine-grained authentication and quick removal.

Wired IDS Integration
Unified wired and wireless IDS ensures malicious wireless clients are disconnected from the network.

Wireless Endpoint Compliance
Cisco NAC prevents wireless endpoints from introducing viruses, spyware, malware, etc.

Wireless IDS/IPS
Comprehensive wireless threat identification and over-the-air prevention.

Offsite Endpoint Protection
Cisco Secure Agent detects and prevents offsite wireless threats such as ad hoc networks.
Automated Wireless Security Vulnerability Assessment

- Provides network-wide security health summary
- Proactively monitors entire wireless network
  - WLCs, APs and management interfaces
- Identifies vulnerabilities in:
  - Encryption
  - User/network auth
  - Threat mitigation
  - Management
- Reduces configuration errors by recommending optimal security settings
- Increases awareness of potential security issues

### Security Summary

**Security Index: 17.76**

<table>
<thead>
<tr>
<th>Top Security Issues</th>
<th>View All</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFP Client Protection set to Optional for WLAN. (42)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface set to management for WLAN. (30)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No enabled IDS Sensor configured for a Controller. (28)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No WLAN Key Management methods set (only settable when Authentication Method is WPA+WPA2). (26)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection Type set to None for a Controller. (24)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Rogue APs and Adhoc Rogues

<table>
<thead>
<tr>
<th></th>
<th>Last 24 Hours</th>
<th>Total Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Rogue APs</td>
<td>Alert 994, 806</td>
<td>Alert 899, 899</td>
</tr>
<tr>
<td>Unclassified Rogue APs</td>
<td>Alert 167</td>
<td>Alert 425, 462</td>
</tr>
<tr>
<td>Friendly Rogue APs</td>
<td>Alert 6</td>
<td>Alert 7, 2</td>
</tr>
</tbody>
</table>

#### Threats And Attacks

<table>
<thead>
<tr>
<th></th>
<th>Last 24 Hours</th>
<th>Total Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFP Attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invalid MAC</td>
<td>Alert 14</td>
<td>Alert 75, 82</td>
</tr>
<tr>
<td>Invalid Sequence Number</td>
<td>Alert 36</td>
<td>Alert 45, 48</td>
</tr>
<tr>
<td>SPF</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Re-Designed “At-a-Glance” WCS Security Dashboard

- Graphically-oriented “at-a-glance” security posture and state
- Dynamically generates view of only current alarms
- Click to drill down to any level of reported event
- Single view for wireless security events
  - MFP alarms and errors
  - Grouping by attack types
- Reduces time required by administrator to determine status and respond to alarms
wIPS Integrated Attack Encyclopedia

- Available for each alarm
- Accessible from the wIPS Profile page or by clicking ‘Help’ on each attack alarm
Forensics

- User configurable per attack
- Captured the first time the attack is detected
- A .cap capture of packets
  Opened by Wireshark, Omnipeek, etc.
- Stored on the MSE
  Can be requested by WCS on-demand
NAC Out-of-Band Support

- No longer requires all WLAN traffic to route through the NAC Appliance
- Can be used upon authentication for posture assessment and remediation
- Will poll devices to determine policy and configuration status
- Offers flexibility in design
- Lowers capital expense, especially for branch office deployments
Benefits of Unification

Optimizing Wireless Performance
Enterprise-Class Reliability for Mission Critical Mobility

- Maximized system availability
  - Controller redundancy
  - Access point failover
- System level management automates failover to guarantee availability

**Benefits**
- No single point of failure
- Automated network failover decreases support and downtime costs
- Wireless network reliability on par with wired
Radio Resource Management
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
Radio Resource Management
Enterprise-Class Network Performance

- Dynamic client load balancing
- Solving performance & capacity problems in high density areas
  e.g. conference rooms, cafeteria...
- Clients and infrastructure 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
Cisco WCS RRM Dashboard

- New graphical interface in Cisco WCS for RRM
- Features
  - APs with most channel changes
  - APs running at maximum power
  - APs with coverage hole events
  - Top channel change reasons
  - RRM related configuration mismatches across all controllers in RF Group
- Benefits
  - Simplified troubleshooting of RRM-related events
# RRM Dashboard

## RRM Statistics (Last 24 Hours)

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
<th>Statistics</th>
<th>Last 24 Hrs</th>
<th>Last 7 Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of RF Groups</td>
<td>2</td>
<td>Total Channel Changes</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>AP’s at max. power (a/n)</td>
<td>22.41% (13 out of 58)</td>
<td>Total Coverage Holes</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>AP’s at max. power (b/g/n)</td>
<td>39.66% (23 out of 58)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Configuration Mismatches</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Channel Change Reason (a/b/g/n)

- **Last 24 Hours**
  - Signal: 50%
  - Interference: 30%
  - Noise: 10%
  - Load: 5%
  - Radar: 0%
  - Other: 5%

- **Last 7 Days**
  - Signal: 60%
  - Interference: 20%
  - Noise: 10%
  - Load: 5%
  - Radar: 0%
  - Other: 5%

---

**Quick Snapshot of the Network, and the reasons behind a certain event, such as, channel changes**
Green Initiative

- Improved power management of Cisco Aironet access points to support the Cisco Green initiative.
  
  Cisco access points can be turned on or off periodically at scheduled intervals to save power.

- **Benefit:**
  
  Reduce power costs by turning access points on or off periodically at scheduled intervals.

  Manage network security or restrict WLAN usage.
Detailed Client Report

- New report added called “Detailed Client Report”
- Customizable report fields
- Client statistics (MAC, AP associated, Tx/Rx throughout, RSSI, CCX, SNR, etc)
- Generate report based on variety of criteria such as floor area, controllers, access point, and SSID

**Benefit:**

Easily gather, track and report on key information about client devices on the network
Cisco WCS Monitoring of Cisco Spectrum Expert Sensor(s)

- Monitor Cisco Spectrum Expert sensor(s) in Cisco WCS
  - Snapshot of a given sensor
  - Summarized view of all sensors
- Cisco WCS screens & menu options
  - Detected interferer types with severity
  - Impacted channels
  - Affected access points and clients
  - Non-Wi-Fi interference trap
- Search capabilities
  - Interferer types
  - Interference properties
- Find interferers
  - Map sensor with effective range
  - Approximate location of interferers
Cisco Unified Wireless Network

Guest Access
The Challenge of the “Guest” User

- Guest traffic should be segregated from the internal network
- Limited internal network access must be extended to guest securely
- “Guest network” must be cost-effective and non-disruptive
- Must not require guest desktop software or configuration
Path Isolation
WLAN Controller Deployments with EoIP Tunnel

- Use of EoIP tunnels to logically segment and transport the guest traffic between edge and anchor controllers
- Other traffic (employee for example) still locally bridged at the edge controller on the corresponding VLAN
- No need to define the guest VLANs on the switches connected to the edge controllers
- Original guest’s Ethernet frame maintained across LWAPP and EoIP tunnels
- Redundant EoIP tunnels to the Anchor WLC
- 2106 model can’t terminate EoIP connections (no anchor role)
Cisco Unified Wireless Network

Product Portfolio
Proven Platform for Mobile Access

Indoor Access Points
- 1131AG
- 1142AGN

Indoor Rugged Access Points
- 1240AG
- 1250AGN

Outdoor Access Points/Bridges
- 1522
- 1310G
- 1410A
- MAR3200

Mobility Platform

Features
- Industry’s best AP range & throughput
- Enterprise class security
- Many configuration options
- Simultaneous air monitoring and traffic delivery

Benefits
- Zero touch management
- No dedicated air monitors
- Supports all deployment scenarios (indoor and outdoor)
- From secure coverage to advanced services
Delivering Network Unification

**Intelligent Access**
- Catalyst 3750G Integrated WLAN Controller

**Distribution**
- 4400 Wireless LAN Controller

**Network Core**
- Wireless Integrated Services Module (WISM)

---

**Cisco Unified Wireless Network**
- **Scalability**
- **Ease of Deployment**
- **Flexibility**
- **Lower TCO**
- **High Availability**
- **Investment Protection**

---

**Branch Office**
- Wireless LAN Controller for ISR Series Routers
- 2106 Wireless LAN Controller

**Remote Office**
- Hybrid Remote Edge Access Points (H-REAP)
Cisco Wireless Controller Family

- Cisco 3750 50 APs
- Cisco 3750 25 APs
- Cisco 4402-50 50 APs
- Cisco 4402-25 25 APs
- Cisco 4404 100 APs
- Cisco WiSM 300 APs

Deployment Size:

- 1-2 APs
- >=2-6 APs
- >=12 APs
- >=25 APs
- >=50 APs
- >=100 APs
- <300 APs
Cisco Wireless Control System (WCS)

World-Class Network Management

Features
- Planning, configuration, monitoring, location, IDS, and troubleshooting
- Hierarchical maps
- Intuitive GUI and templates
- Policy based networking (QoS, security, RRM, etc.)

Benefits
- Lower OPEX and CAPEX
- Better visibility and control of the air space
- Consolidate functionality into a single management system
Location Tracking Services

- 1st integrated location solution
- Real-time location services
  - Asset tracking
  - Rogue AP and device location
  - E911 services
- Advanced RF fingerprinting for greater accuracy
- Simultaneous real-time tracking 17,000+ devices
- API Third Party Applications
- RF capacity management
- Intuitive management GUI

Cisco 3300 Series Mobility Services Engine
Cisco Mobility Services Engine
Scalable, Multi-Function Services Platform

3300 Series Mobility Services Engine

**Common Framework for Multiple Services**
- Wireless IPS, Context-Aware Location, Mobile Intelligent Roaming

**Powerful Security Analysis & Archiving**
- Analyzes traffic for anomalous behavior
- Performs event analysis and correlation
- Stores events and forensics

**Abstraction Layer with CAPWAP/NMSP**
- Allows Transport and Applications to evolve independently

**Services and Applications Platform**
- Unified API enabling Enterprise 3.0 applications
## Voice over WLAN
Requires end-to-end intelligence

<table>
<thead>
<tr>
<th>VoWLAN Clients</th>
<th>Voice Ready WLAN Infrastructure</th>
<th>Unified Wired/Wireless LAN Infrastructure</th>
<th>Cisco CallManager &amp; Mobility Applications</th>
</tr>
</thead>
</table>

### Today
- Comprehensive on campus solution
- Dedicated clients, soft phones
- CCX enables QoS, Fast Secure Roaming
- IEEE 802.11b easy to use wireless IP phone
- Pixel display provides intuitive access to features and applications

### Future!
- Mobility on / off campus
- Dual 802.11 and cellular phone
- Partners: Nokia, RIM
- Additional voice clients
WCS Location/VoWLAN Service Planning

- Location readiness
  Assess location accuracy for existing deployments

- Location/VoWLAN planning mode
  Suggests AP density and placement based on data, voice, or location services

- Location inspector
  Post deployment and calibration tool for location quality verification

- Accuracy improvements
  Smoothing, additional antennas, faster calibration, enhanced algorithms—minimum variance estimation
Meet DoD Policy
8100.2 WLAN Policy FIPS 140-2 Requirement

- "Encryption for unclassified data in transit via WLAN-enabled devices, services, and technologies must be implemented **end-to-end over an assured channel** and be validated under the NIST CMVP as meeting requirements per FIPS 140-2 at a minimum overall Level 1"
Pre 802.11i Wireless Deployments

- WLAN stations w/ VPN clients
- WLAN
- OPEN AP
- Firewall router
- Encrypted traffic
- DMZ
- VPN Concentrator
- Security Border w/VPN
- Firewall
- DHCP/DNS Servers
- AAA/Cred Servers
- Application Servers
- Clear-text traffic
FIPS 140-2 / 802.11i end-to-end Security

- APs authenticate into DoD network with X.509 certs as CC trusted network devices
- APs enforce 802.1X port access control & terminate FIPS 140-2 encryption/decryption services at the edge of the DoD security border
- Controller/APs establish FIPS 140-2 validated assured control channel
- Controller centrally manages 802.1x state machine providing secure mobility
Over 20 Wireless Product FIPS 140-2

FIPS Certificate # 693 - Cisco WLAN Controllers 4402-12; 4402-25; 4402-50 and 4404-100
FIPS Certificate # 695 - Cisco Aironet (LWAPP) LAP1242, LAP1131, LAP1232, LAP1231
FIPS Certificate # 701 - Cisco Aironet (IOS) AP1242, AP1131, AP1232 & BR1310
FIPS Certificate # 729 - Cisco WiSM w/Catalyst 6506, 6506-E, 6509, 6509-E Switches
FIPS Certificate # 948 - Cisco Secure ACS FIPS Module
FIPS Certificate # 955 - Cisco WLAN Controllers 4402-12; 4402-25; 4402-50 and 4404-100
FIPS Certificate # 957 - Cisco WiSM w/Catalyst 6506, 6506-E, 6509, 6509-E Switches
FIPS Certificate # 958 - Cisco Catalyst 3750G-25/50 WLAN Controller
FIPS Certificate # 913 - Cisco Aironet (LWAPP) LAP1242, LAP1131
FIPS Certificate # 1016 - Cisco Secure SSC FIPS Module

In Process

Cisco Unified Wireless 5.2 FIPS Release + 15 Devices!
Cisco Wireless DoD Certifications

- Common Criteria - 10 Wireless Products in Process
  - Submitted with DoD approved NIAP lab for DoD WLAN Protection Profile conformance

Cisco Wireless DoD Approvals

- U.S. Army IAAPL – 5 products approved today / 10 more submitted in 2009
- U.S. Navy NMCI ATO – Cisco Wireless 802.11i end-to-end solution approved – FIPS client, APs, Controllers, ACS, Location, etc
- DoD 8100.2 WLAN Policy Compliance
- DISA Wireless STIG Compliance
5.2 FIPS Release:

802.11n FIPS APs
802.11n FIPS APs - AP1142 / AP1252

- **Cisco Aironet 1140 Series**
  - Carpeted Indoor Environments
  - Easy to Deploy-Sleek design with integrated antennas
  - 802.11n performance with efficient 802.3af power

- **Cisco Aironet 1250 Series**
  - Rugged Indoor Environments
  - Versatile RF coverage with external antennas
  - Modular flexible platform
  - Flexible power options for optimal RF coverage
802.11n is Ready for Primetime!

- 350+ Wi-Fi certified devices
- Cisco has shipped over 150K AP 1250s
- Intel has shipped over 17M Intel 11n clients
- Market projections show 11n will rapidly overtake 802.11a/b/g
15 Minute Break
What is 802.11n?
Evolution to MIMO Technology

Single Input Single Output (SISO)  Multiple Input Multiple Output (MIMO)
MIMO Overview

Maximal Ratio Combining
• Performed by receiver
• Combines multiple received signals
• Increases receive sensitivity
• Works with non-MIMO and MIMO clients

Transmit beam forming (ClientLink)
• Performed by transmitter
• Ensures signal received in phase
• Increases receive sensitivity
• Works with non-MIMO and MIMO clients

Spatial Multiplexing
• Transmitter and receiver participate
• Multiple antennas txmt concurrently on same channel
• Increases bandwidth
• Requires MIMO client
## Technical Elements of 802.11n

<table>
<thead>
<tr>
<th>MIMO</th>
<th>40Mhz Channels</th>
<th>Packet Aggregation</th>
<th>Backward Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Aspects of 802.11n

MIMO (Multiple Input, Multiple Output)

Performed by Transmitter (Talk Better)
Ensures Signal Received in Phase
Increases Receive Sensitivity
Works with non-MIMO and MIMO Clients

Beam Forming
Maximal Ratio Combining
Spatial Multiplexing
Existing 802.11n Solutions
Beam Strength Not Directed to Client

802.11a/g Client Connection Not Optimized, Creates Coverage Hole
Existing 802.11n Solutions
Beam Strength Not Directed to Client

802.11a/g Client Connection Not Optimized, Creates Coverage Hole
M-Drive with ClientLink
Cisco Innovation: Beam Forming Intelligence

Intelligent Beam Forming Directs Signal to Improve Performance and Coverage for 802.11a/g Devices
M-Drive with ClientLink
Cisco Innovation: Beam Forming Intelligence

Intelligent Beam Forming Directs Signal to Improve Performance and Coverage for 802.11a/g Devices
Benefit #1: Higher throughput per 11a/g device

Up to 65% Increase in Throughput

Throughput vs. Distance

Test: 802.11a/g device with 802.11n network
Source: Miercom
Benefit #2: Higher system capacity

Up to 27% Improvement in Channel Capacity

- Faster data transmission, less retries = more efficient use of RF channel.
- Faster 11a/g transactions opens airtime for 11n devices, providing them improved experience

Test: 802.11a/g device measured at 16 antenna orientations w/ 802.11n network
Source: Miercom
Aspects of 802.11n

40Mhz Channels | Packet Aggregation | Backward Compatibility

MIMO (Multiple Input, Multiple Output)

- With MMRC
  - Multiple Signals Sent out
  - One Signal Chosen

- MIMO AP

- Performance

- Performed by Receiver (Hear Better)
- Combines Multiple Received Signals
- Increases Receive Sensitivity
- Works with non-MIMO and MIMO Clients

Beam Forming | Maximal Ratio Combining | Spatial Multiplexing
Aspects of 802.11n

MIMO (Multiple Input, Multiple Output)

Information Is Split and Transmitted on Multiple Streams

MIMO AP

- stream 1
- stream 2

Transmitter and Receiver Participate
Concurrent Transmission on Same Channel
Increases Bandwidth
Requires MIMO Client

Beam Forming
Maximal Ratio Combining
Spatial Multiplexing
Aspects of 802.11n

40Mhz Channels

Moving from 2 to 4 Lanes

40-MHz = 2 aggregated 20-MHz channels—takes advantage of the reserved channel space through bonding to gain more than double the data rate of 2 20-MHz channels
Aspects of 802.11n

Packet Aggregation

Carpooling Is More Efficient Than Driving Alone

Without Packet Aggregation

<table>
<thead>
<tr>
<th>802.11n Overhead</th>
<th>Data Unit Packet</th>
<th>802.11n Overhead</th>
<th>Data Unit Packet</th>
<th>802.11n Overhead</th>
<th>Data Unit Packet</th>
</tr>
</thead>
</table>

With Packet Aggregation

<table>
<thead>
<tr>
<th>802.11n Overhead</th>
<th>Data Unit Packet</th>
<th>Data Unit Packet</th>
<th>Data Unit Packet</th>
</tr>
</thead>
</table>
Aspects of 802.11n

- MIMO
- 40Mhz Channels
- Packet Aggregation
- Backward Compatibility

Backward Compatibility

2.4GHz

5GHz

11n Operates in Both Frequencies

802.11ABG Clients Interoperate with 11n AND Experience Performance Improvements
Effective use of 5 GHz
Effective Frequency Use—5GHz and 2.4GHz
Create a 5GHz Strategy

- 5GHz Recommended for 802.11n
  More available spectrum—greater number of channels
  Benefits from 40MHz channels, although 20MHz still works well
  Many 11n devices only support 40MHz in 5GHz, although Cisco supports 40MHz in both 2.4GHz and 5GHz

- 2.4GHz still benefits from MIMO and packet aggregation
  Ideal for legacy apps (handhelds, scanners, med. applications)
**5GHz Dynamic Frequency Selection**

When Radar Is Present

APs Shift Channels—
Results in Lower Available Channels and Loss of UNII-2 and UNII-2 ext Bands

<table>
<thead>
<tr>
<th>Available 40MHz Channels</th>
<th>No DFS Support</th>
<th>DFS Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>11</td>
</tr>
</tbody>
</table>

← 5 GHz Frequency →
DFS and Available Bandwidth

- Full DFS support is required for complete use of channels in 5GHz
- Limited DFS support directly impacts available bandwidth
- Limited bandwidth restricts application support and negates investment in 11n

<table>
<thead>
<tr>
<th>Available Channels per Region</th>
<th>Theoretical</th>
<th>Cisco</th>
<th>Meru/Aruba</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11n 5GHz 20MHz</td>
<td>24</td>
<td>21</td>
<td>8</td>
</tr>
<tr>
<td>11n 5GHz 40MHz</td>
<td>11</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Europe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11n 5GHz 20MHz</td>
<td>19</td>
<td>19</td>
<td>4</td>
</tr>
<tr>
<td>11n 5GHz 40MHz</td>
<td>9</td>
<td>9</td>
<td>2</td>
</tr>
</tbody>
</table>