



Wireless LAN



SWITCH Module 8

Agenda

- **WiFi Introduction**
- **WLAN Devices**
- **WLAN Security**
- **Autonomous vs. Lightweight AP**

Introduction

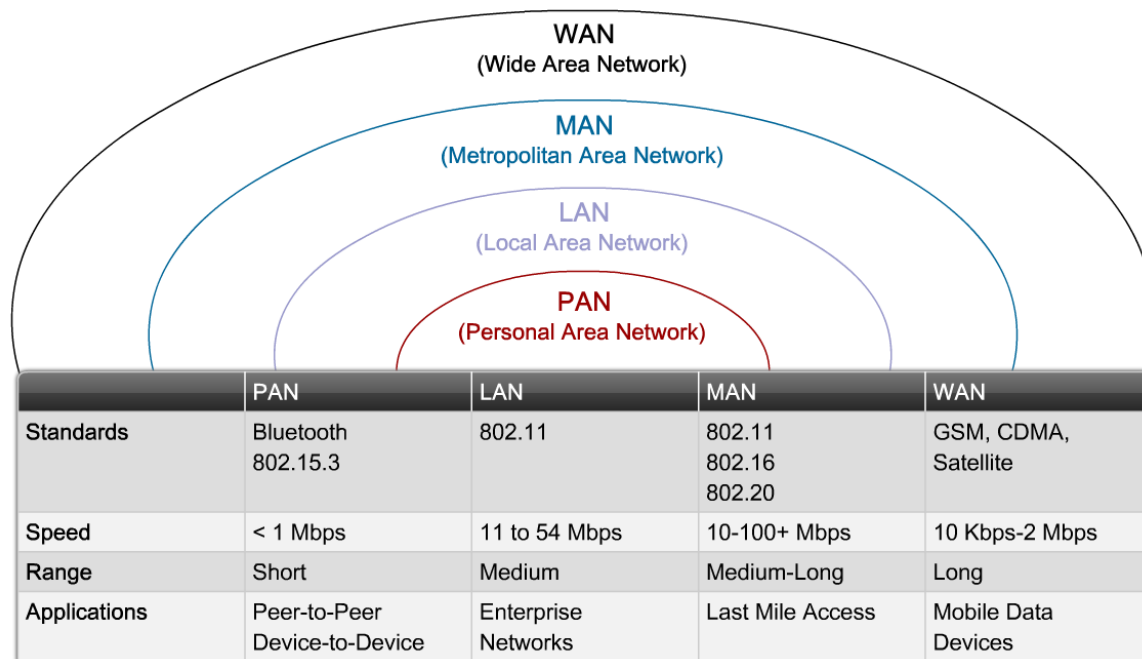


Wireless LAN

- WLAN uses EM waves as medium for high-speed data transfers
 - Radio waves
 - Light
- Advantages
 - Widespread coverage
 - Mobility
 - Ability to cope with large distances and relatively rolling ground

WLAN as Technology ①

- Wireless LANs (WLANs) are subpart of wireless communication technologies that provide traditional LAN services
 - Excluding Bluetooth, GSM and others
- The most used are nowadays IEEE 802.11 standards



WLAN as Technology ②

- WLANs are not a replacement for “wired” LANs
 - Transfer speed is still a lower by order of magnitude
 - LAN is acting as a “glue” when interconnecting multiple WLANs
 - WLANs have some inherent disadvantages which don’t exist or are solved in LANs
- *It is preferable to consider WLANs as extension of ordinary LANs and consequently deploy WLANs in this sense*

LAN vs. WLAN

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

Basic Terms ①

▪ Channel Coding

- Transformation of data to symbols more suitable for transfer across target technology

▪ Bandwidth

- Frequency range available for WLAN
 - 2.4 GHz – it is from 2.412 to 2.484 GHz
 - 5 GHz – it is from 5.150 to 5.825 GHz

▪ Carrier signal

- Information (data content) is expressed by altering this signal (its frequency, amplitude, phase)

Basic Terms ②

▪ Modulation

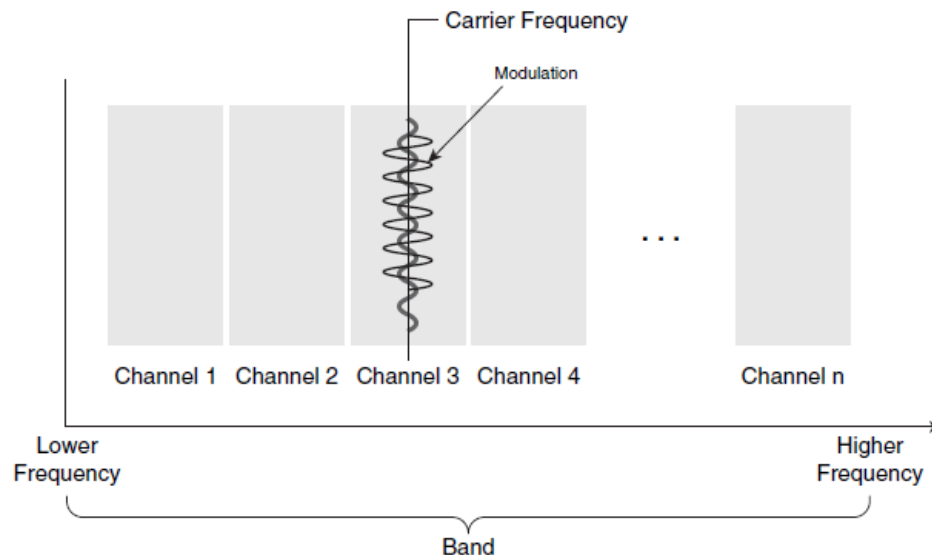
- Change of signal characteristic which express transferred symbol
- Three types: **amplitude**, **phase** and **frequency modulation**

▪ Channel

- Interval of usable frequencies for signal modulation

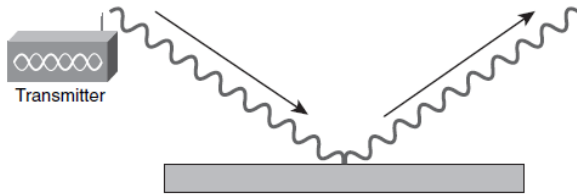
▪ Frequency scheme

- The way, how transmitter control frequency range in target channel

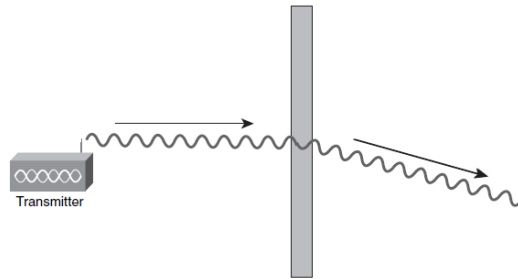


Radio Wave in Environment

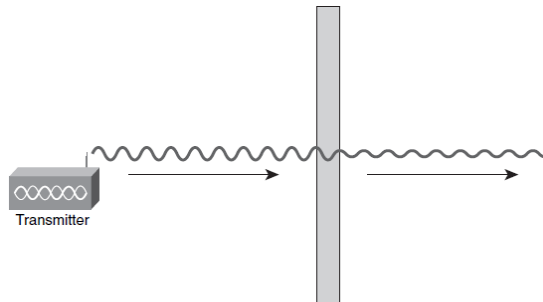
- Reflection



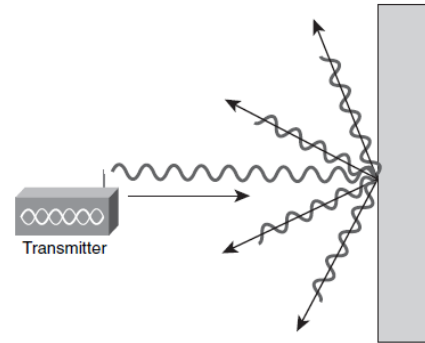
- Refraction



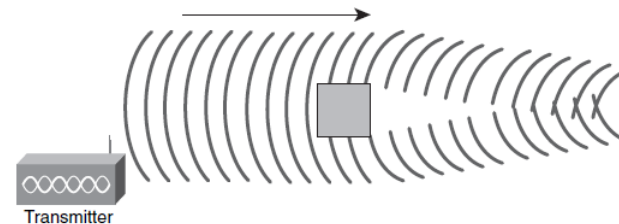
- Absorbption



- Scattering



- Diffraction



WLAN Networks

- Current WLANs use unlicensed 2.4 GHz and 5 GHz band
 - Sometimes is 2.4 GHz band referred as **ISM** (Industrial, Science, Medical)
 - Niekedy sa tieto pásma, zvlášť 2,4GHz označujú ako ISM (Industrial, Science and Medical)
- WLAN devices occupy in this band some frequency ranges (spread spectrum)
 - It is resistant against interference
 - **Direct Sequence Spread Spectrum (DSSS)**
 - Pseudonoise PN sequence known by transmitter and also receiver
 - **Orthogonal Frequency Division Multiplex (OFDM)**
 - FDM with subcarriers

WLAN Standards

- Main standardizer is [Institute of Electrical and Electronics Engineers](#)



- IEEE standards relevant to WLAN:
 - 802.11a – 54 Mbps, 5 GHz
 - 802.11b – 11 Mbps, 2.4 GHz
 - 802.11g – 54 Mbps, 2.4 GHz
 - [802.11n](#) – 600 Mbps, 2.4 GHz a 5GHz
 - 802.11e – QoS
 - 802.11i – Securing WLAN

IEEE 802.11a

- Formerly not so known standard, nowadays it is common but not dominant
- **Speed**
 - Theoretical maximum transfer speed is 54 Mbps
 - Fallback speeds: 48 - 36 - 24 - 18 - 12 - 9 - 6 Mbps
 - Realistic transfer speed is cca 25 Mbps
 - Uses 5 GHz frequency band
- **Channels**
 - 5 MHz gaps between two consecutive channels
 - Channel is 20 MHz wide and divided into 64 subchannels
 - Each subchannel is 312.5 kHz wide, 4 subchannels are pilots, 12 subchannels are unused
- Smaller signal range
- Incompatible with IEEE 802.11b

IEEE 802.11b

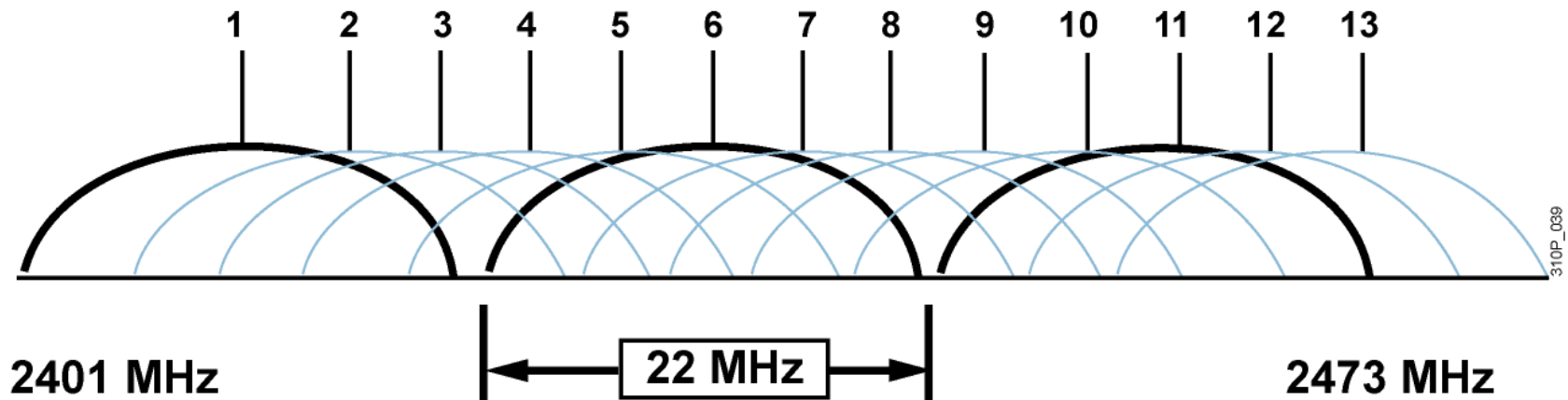
- Originally very popular and widely deployed standard, nowadays it becomes obsolete
- Fair price of 802.11b devices started WLAN boom
- **Speed**
 - Theoretical maximum transfer speed is 11 Mbps
 - Fallback speeds: 5.5 - 2 - 1 Mbps
 - Realistic transfer speed is cca 5 Mbps
 - Uses 2.4 GHz frequency band
- **Channel**
 - Channel is 22 MHz wide
- Uses DSSS, DBPSK, DQPSK
- Larger signal range

Channel Occupation on 2.4 GHz

Channel Identifier	Channel Center Frequency	Channel Frequency Range [MHz]	Regulatory Domain		
			Americas	Europe, Middle East, and Asia	Japan
1	2412 MHz	2401 – 2423	X	X	X
2	2417 MHz	2406 – 2428	X	X	X
3	2422 MHz	2411 – 2433	X	X	X
4	2427 MHz	2416 – 2438	X	X	X
5	2432 MHz	2421 – 2443	X	X	X
6	2437 MHz	2426 – 2448	X	X	X
7	2442 MHz	2431 – 2453	X	X	X
8	2447 MHz	2436 – 2458	X	X	X
9	2452 MHz	2441 – 2463	X	X	X
10	2457 MHz	2446 – 2468	X	X	X
11	2462 MHz	2451 – 2473	X	X	X
12	2467 MHz	2466 – 2478		X	X
13	2472 MHz	2471 – 2483		X	X
14	2484 MHz	2473 – 2495			X

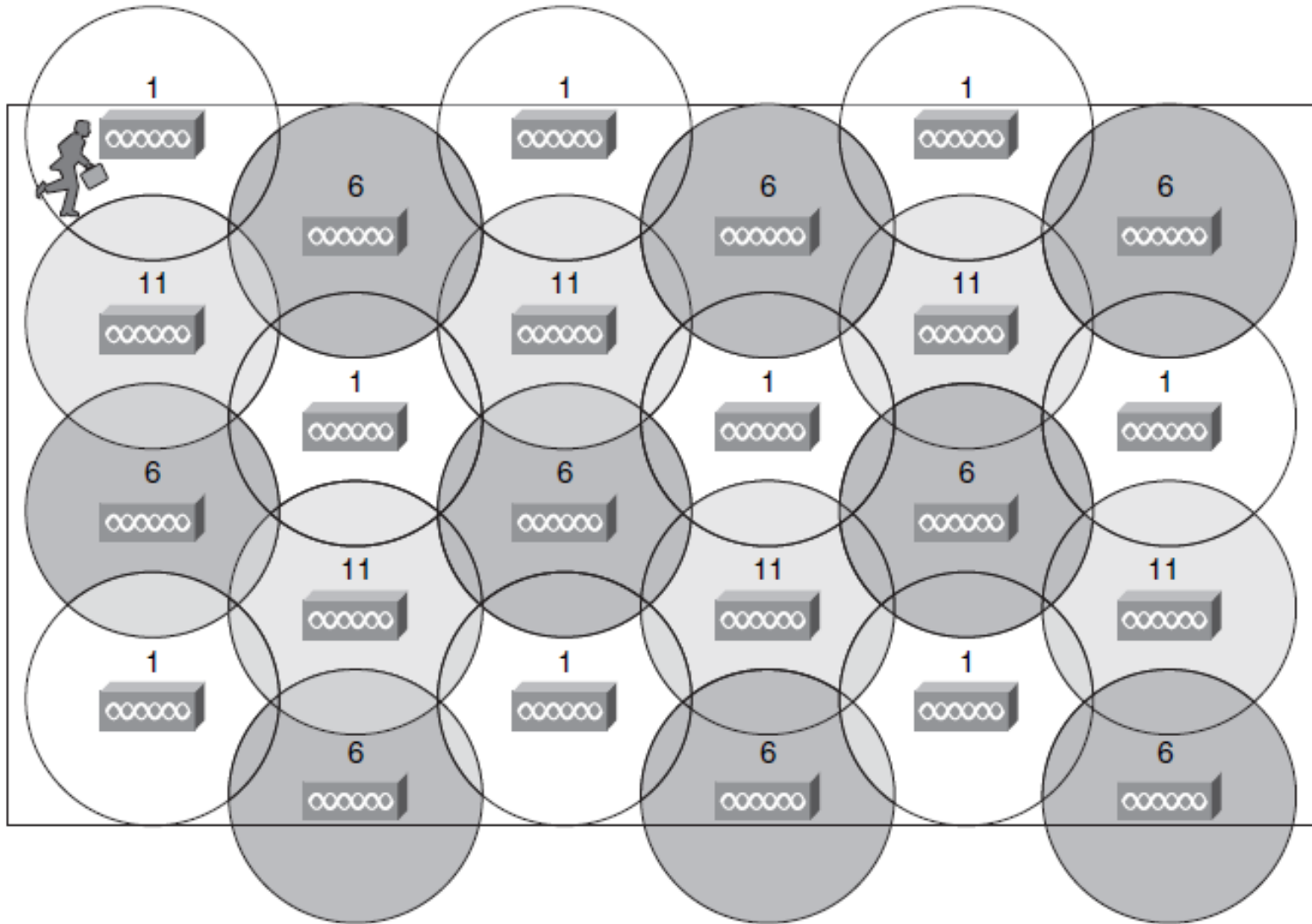
IEEE 802.11b Channel Overlapping

802.11 b/g 2.4-GHz Channels

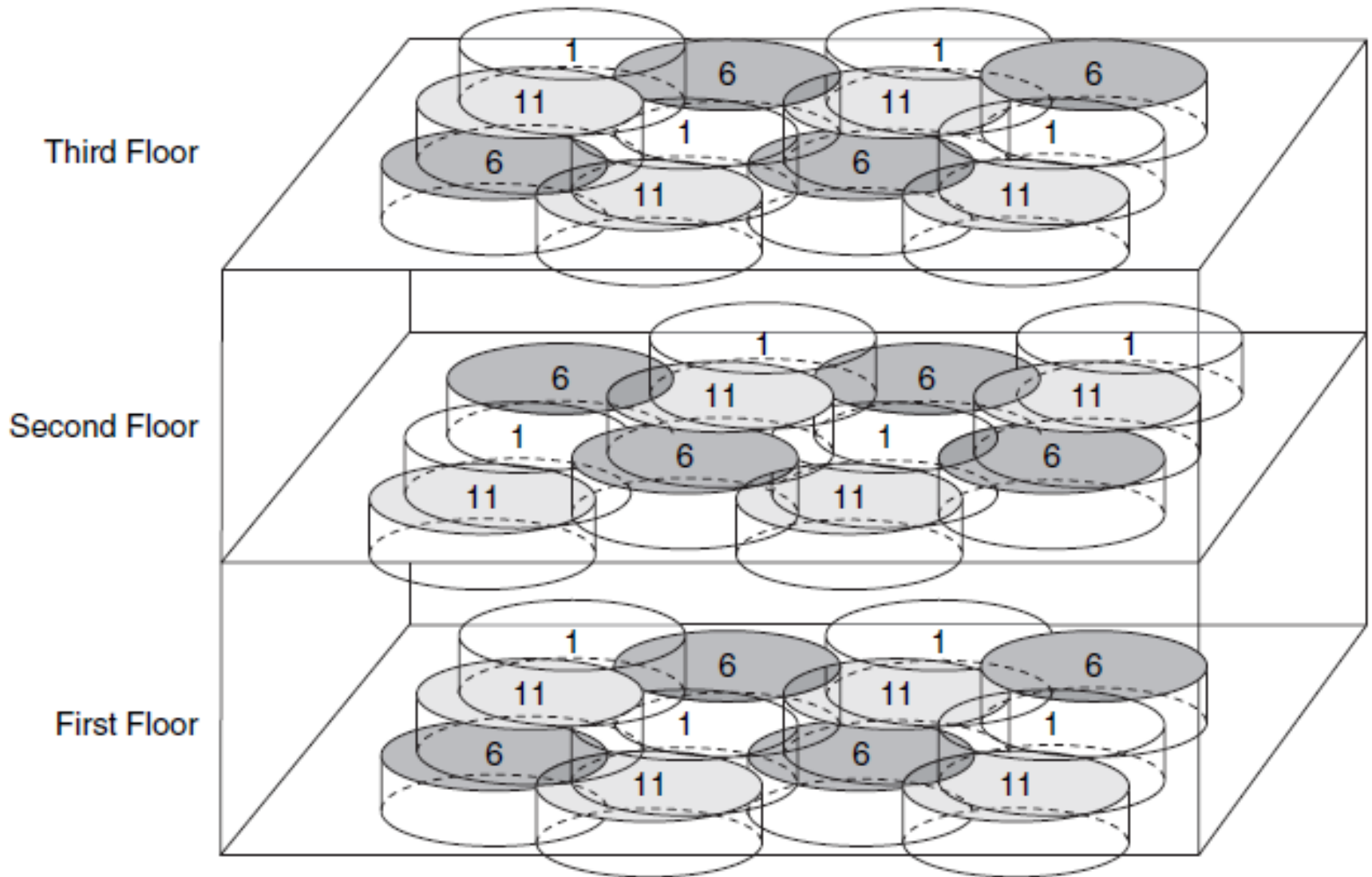


- Channels 1, 6 and 11 are three most close not overlapping channels
- Using channels with spacing lesser than 5 could lead to signal interference
- Same area could be share only by 3 access points

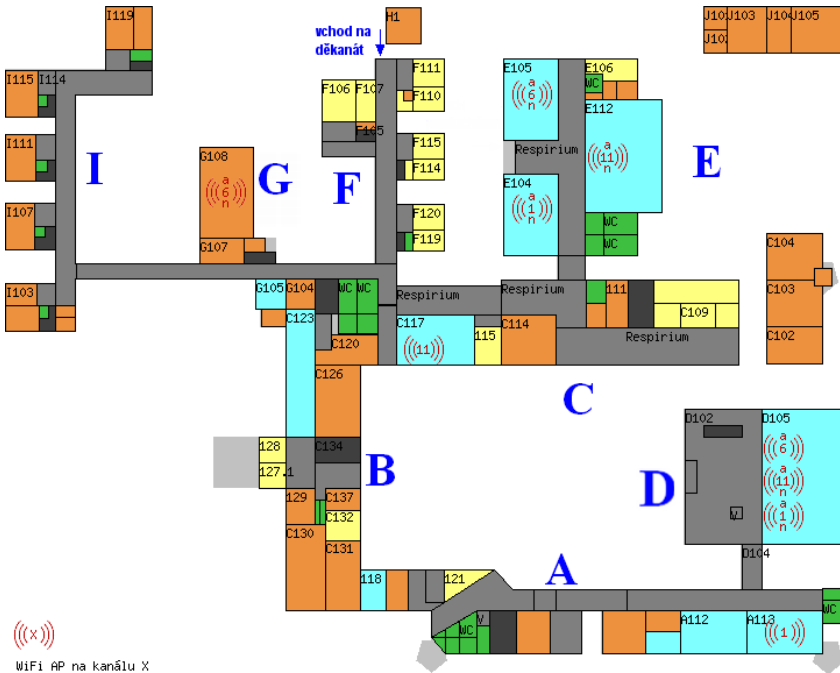
Frequency Plan – Planar



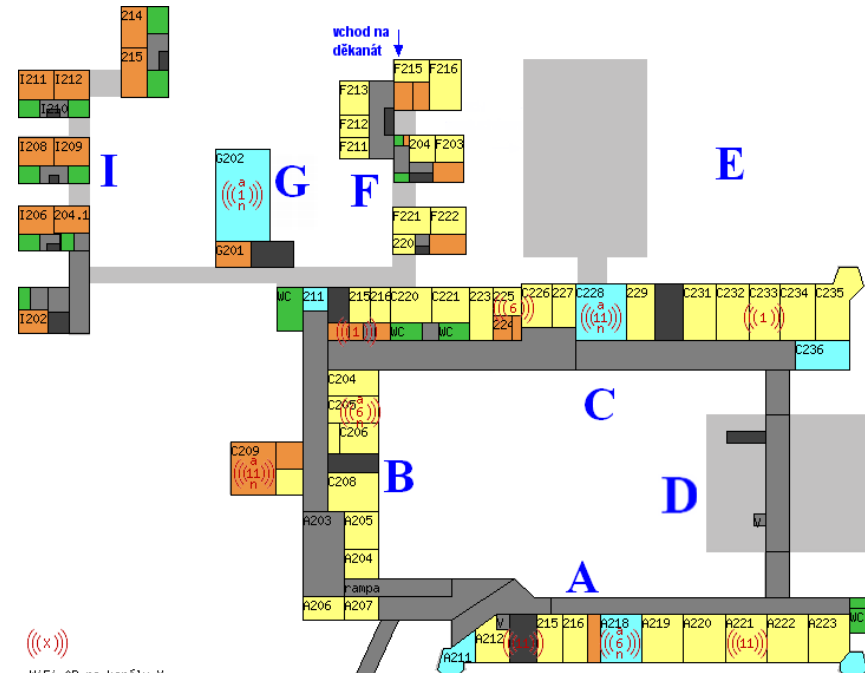
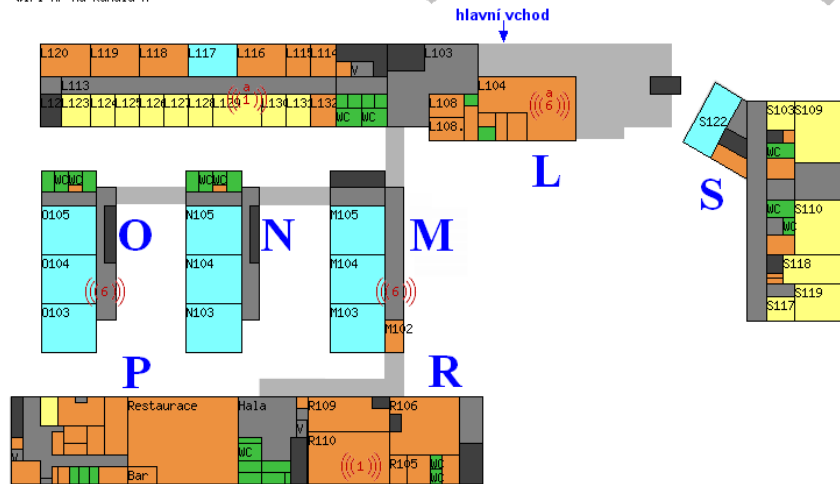
Frequency Plan – Spatial



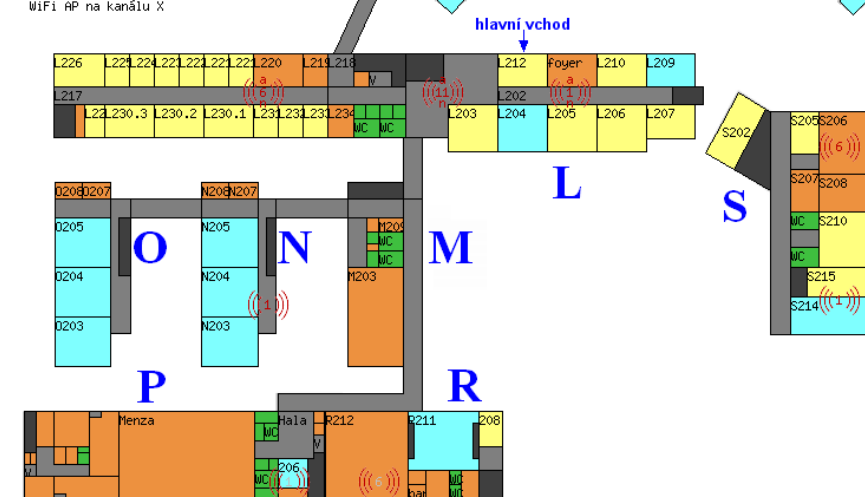
Frequency Plan – Example



WiFi AP na kanálu X



WiFi AP na kanálu X



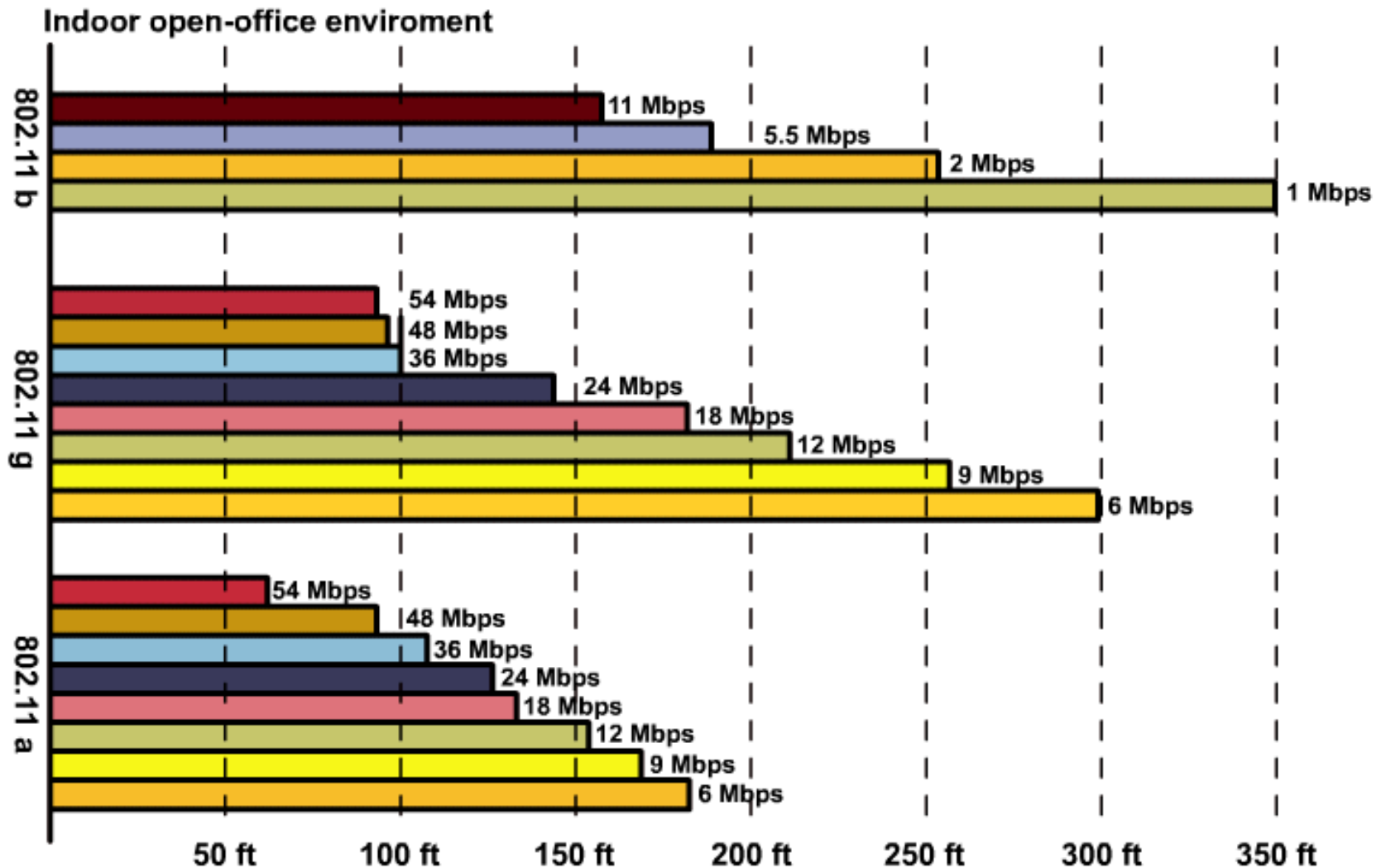
IEEE 802.11g

- Currently most popular WLAN standard
- Backwards compatible with 802.11b
- **Speed**
 - Theoretical maximum transfer speed is 54 Mbps
 - Fallback speeds: 48 - 36 - 24 - 18 - 12 - 9 - 6 Mbps and then back to 802.11b
 - Realistic transfer speed is cca 27 Mbps
 - Uses 2.4 GHz frequency band
- **Channel** properties are same as in 802.11b
- Uses OFDM
- In network could coexist either 802.11b and 802.11g devices
 - Each one will communicate with own separate speed
 - Overall data transfer efficiency will be degraded a little bit comparing to not mixed environment

IEEE 802.11n

- Significant speed boost of WLAN data transfers
- Properties
 - Backward compatibility with previous standards
 - Uses multiple antennas for transmission and receiving – **Multiple Input Multiple Output (MIMO)**
 - Uses 2.4GHz and 5 Ghz frequency band
 - Theoretical maximum transfer speed is 600 Mbps when using 40 MHz wide channel and 4 discrete antennas

Range Comparison



WiFi Alliance

- WLAN implementations could differ even thou standard specifying it is exact
 - Interoperability problems
- Group of WLAN devices manufacturers had founded WECA which was later renamed to **WiFi Alliance**
 - <http://www.wi-fi.org/>
- The goal of alliance is guarantee and certify interoperability of WLAN products using following logo:



Cisco Compatible Extensions ①

- Cisco established own organization for extending its WLAN products
- Cisco also founded own certification program called CCX
 - Verifies compatibility of third party devices with WLAN Cisco stuff



<http://www.cisco.com/go/ciscocompatible/wireless>

Cisco Compatible Extensions ②

CCX Version	Features Covered
CCXv1	Basic 802.11 and Wi-Fi compatibility 802.1X authentication for LEAP Multiple SSID use
CCXv2	WPA 802.1X authentication for PEAP Fast roaming with CCKM RF scanning for WLAN site survey and interference monitoring
CCXv3	WPA2, including AES encryption 802.1X authentication for EAP-FAST Wi-Fi Multimedia (WMM) as part of the 802.11e QoS standard
CCXv4	Cisco Network Admission Control (NAC) Call admission control for Voice over IP (VoIP) Reporting VoIP metrics Enhanced roaming 802.11 location tag functionality (radio frequency identification [RFID])

WLAN Architecture



Wireless Client

- Host endpoint of WLAN
- Connectivity is established via specialized wireless NIC
- Variety of wireless NIC with many bus types



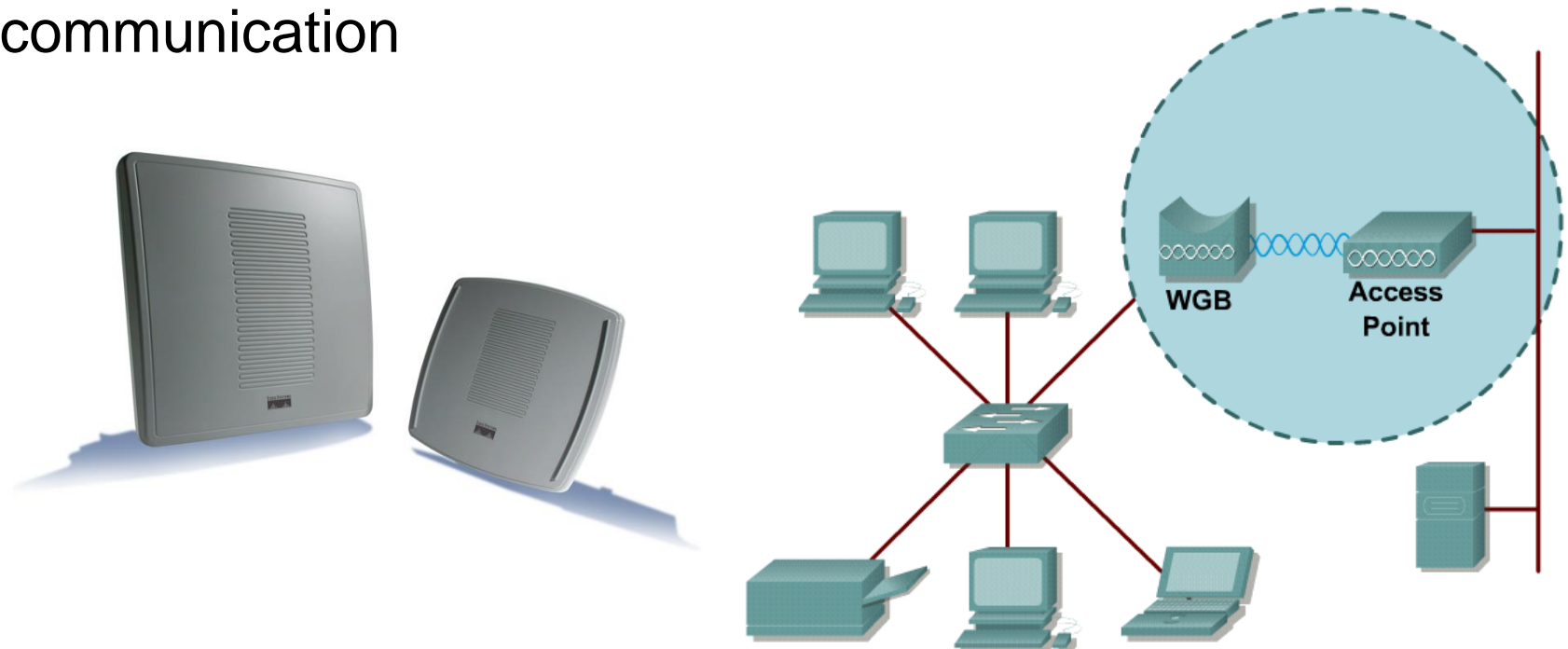
Access Point (AP)

- Ensure communication of WLAN clients between each other and interconnects WLAN with LAN
- By a design it could be also part of other network device such as router
- Variety types for indoor/outdoor usage
- **Cell** = area covered by AP WLAN signal



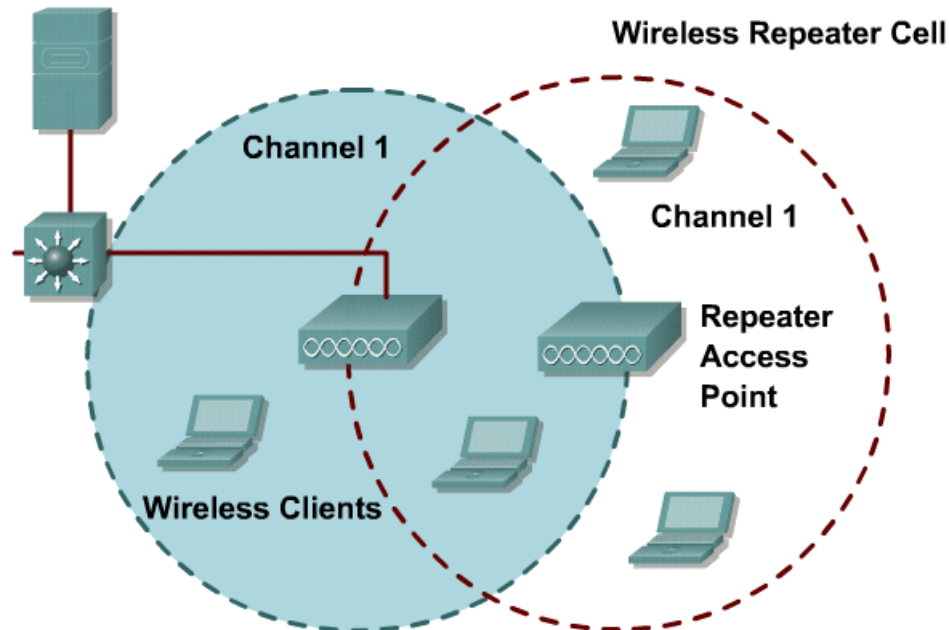
Wireless Bridge

- a.k.a Workgroup Bridge (WGB)
- Provide interconnection of two separate LANs via wireless
- Point-to-Point or Point-to-Multipoint
- Bridges commonly use altered protocols for more efficient communication



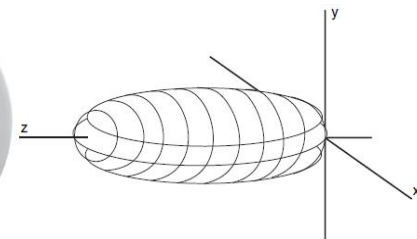
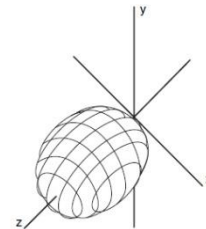
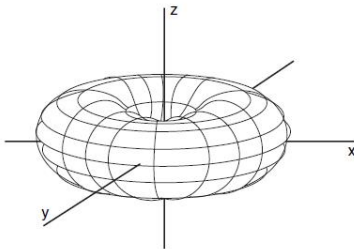
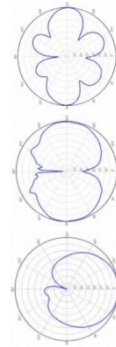
Repeater

- Increases cell range by wider signal coverage
- Using of repeater drastically decreases effective transmission speeds
- Whenever we want to use repeater overlapping between repeater and AP cell should be at least 50% - **catchment area**



Antennas ①

- They could be differ by connector type, cable, signal gain, direction and other factors
- Cisco devices uses RP-TNC connector (2.4/5 GHz)
- Antenna types according to direction:
 - **Omnidirectional** (gain 2 dBi)
 - **Dipole** (gain 6-8 dBi)
 - **Directional** (gain 22 dBi)



Antennas ②

- **dB_i** (isotropic)

- the forward gain of an antenna compared with the hypothetical isotropic antenna, which uniformly distributes energy in all directions
- $G_{dB_i} = 10 \cdot \log(P/P_0)$

- **dB_d** (dipole)

- the forward gain of an antenna compared with a half-wave dipole antenna
- 0 dB_d = 2.15 dB

Antennas ③

- *Why antennas have sizes which they have?*
- $f = 2.4\text{GHz}$
- $c = 300\,000\text{ km/s}$
- $\lambda = c / f = 0.125\text{ m} = \underline{12.5\text{ cm}}$

WLAN Topologies ①

- **Independent Basic Service Set (IBSS)**

- Network formed only by WLAN clients without any AP
- a.k.a. Ad-Hoc network/mode

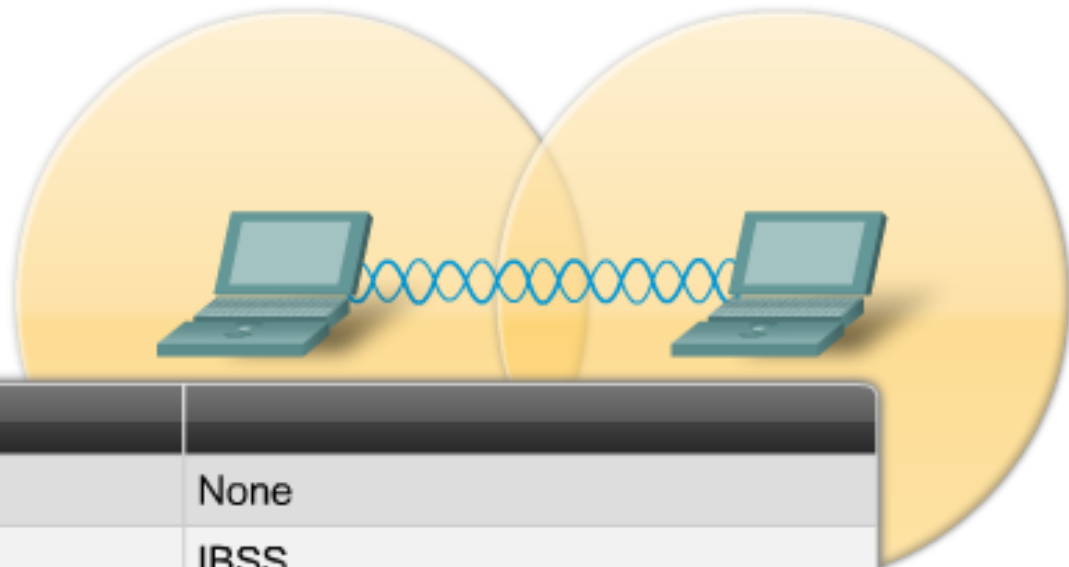
- **Basic Service Set (BSS)**

- Network consists of WLAN clients and also APs
- a.k.a. Infrastructural (Infra-BSS) network/mode

- **Extended Service Set (ESS)**

- WLAN network consisting of multiple interconnected BSS
- a.k.a. Infrastructural network/mode

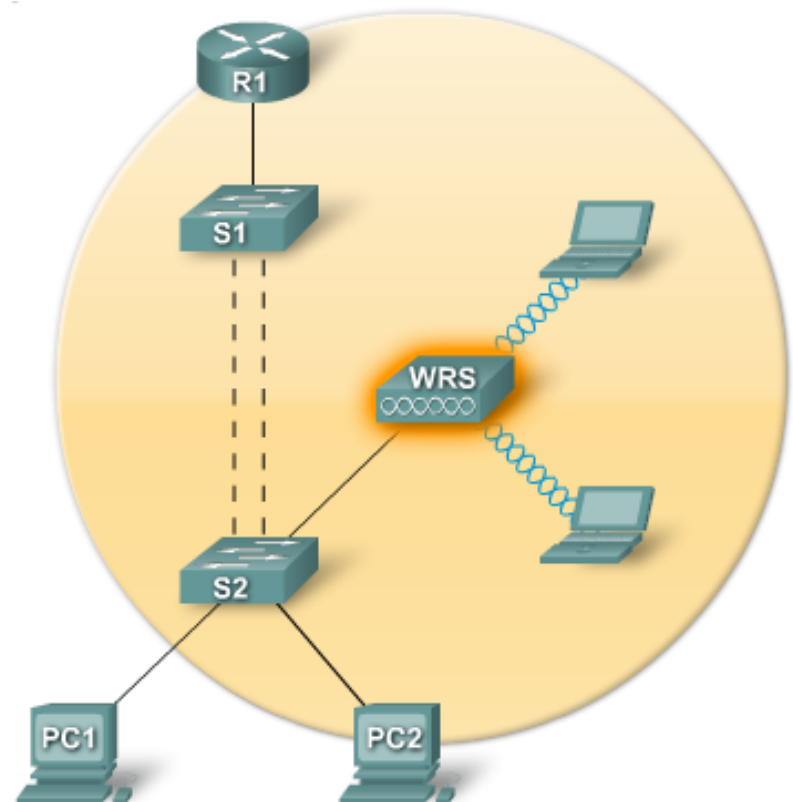
WLAN Topologies – IBSS (Ad-Hoc)



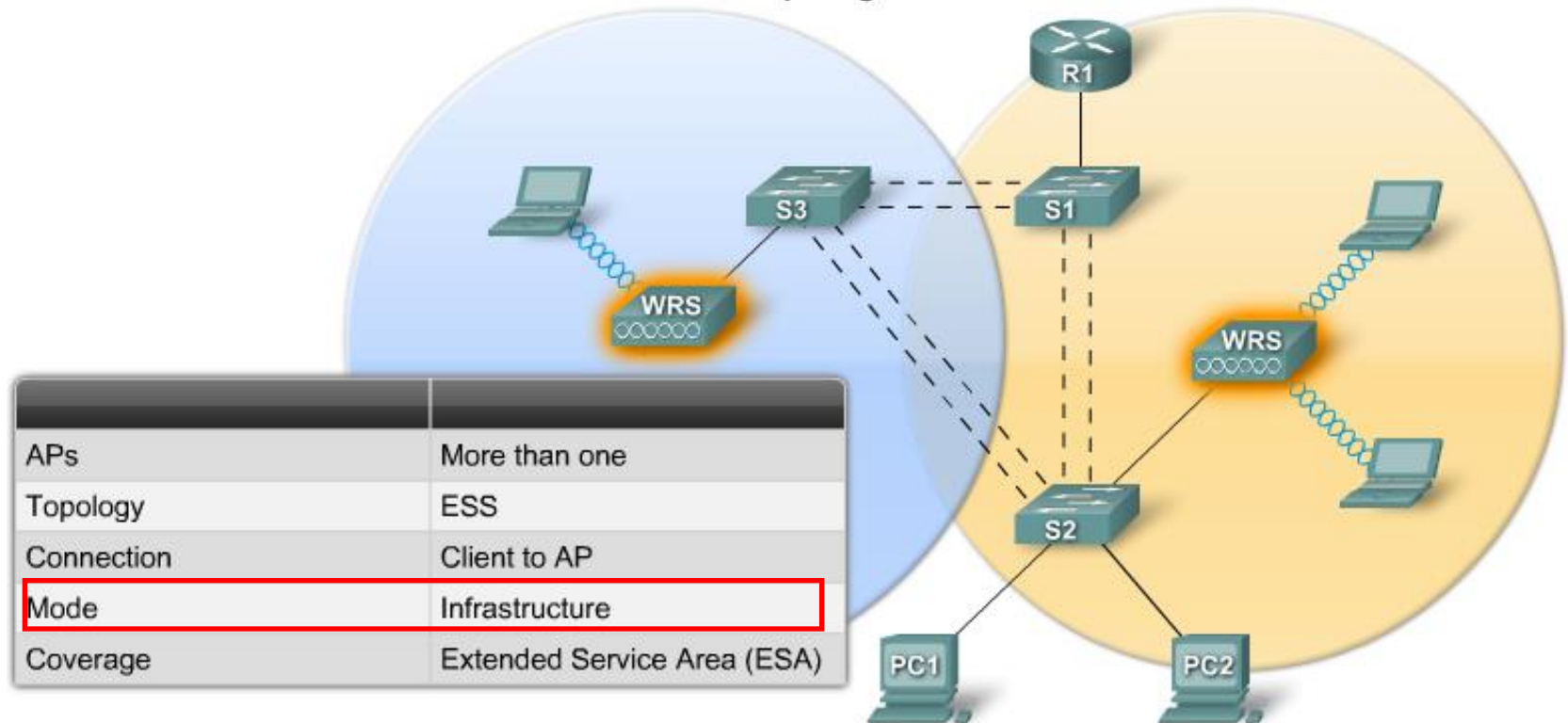
APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

WLAN Topologies – BSS

APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)



WLAN Topologies – ESS

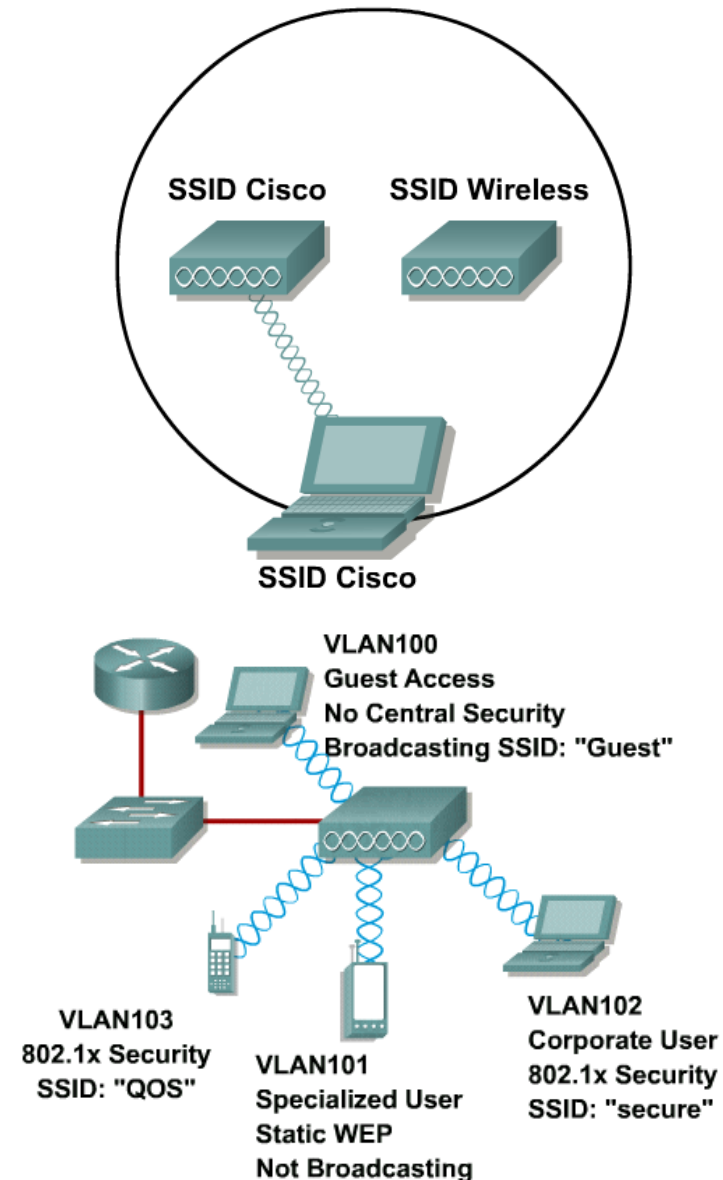


WLAN Topologies ②

- *In one area could operate multiple BSS or ESS. How to distinguish them?*
 - **Service Set ID (SSID)** resp. Extended SSID (ESSID) is unique identifier of WLAN in concrete area
 - SSID is basic parameter used by WLAN client when accessing WLAN
- *But how to overcome problem when client could be associated with different APs in the realm of one ESS?*
 - **Base Service Set ID (BSSID)** is unique identified of concrete AP
 - BSSID has form of MAC address

SSID

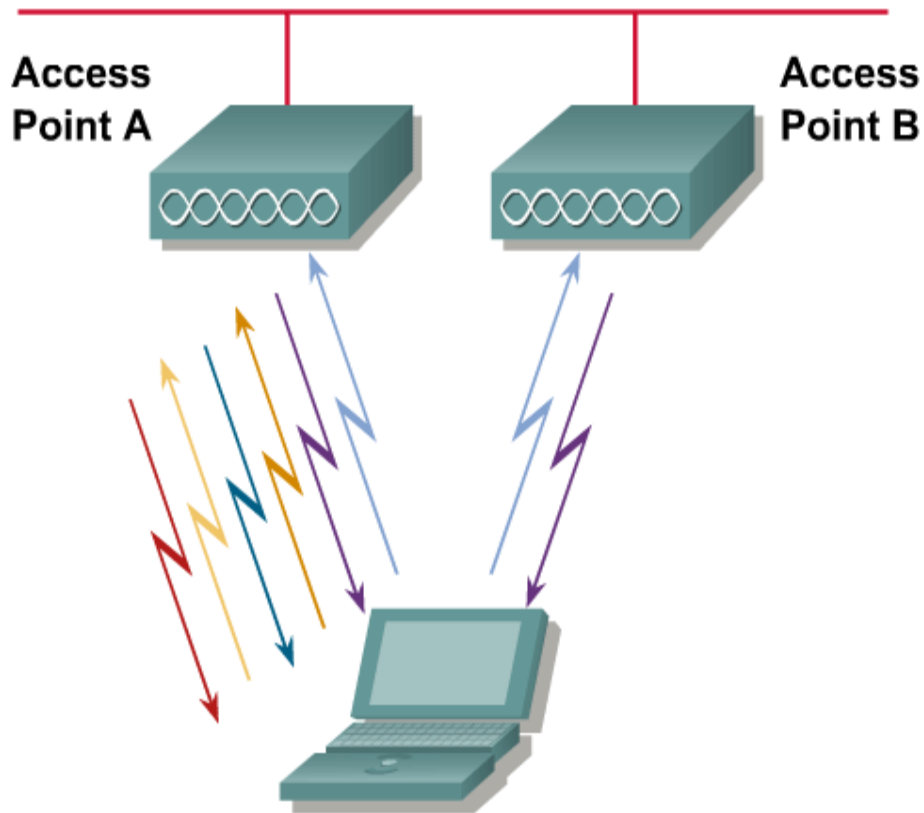
- SSID has text form – name of the network
- It is used to logically separate WLANs
- It must **match exactly** between the client and the access point – client must know SSID
- AP announces its SSID in so called **beacon frames**
 - SSID could be also hidden
- One AP could advertise multiple SSIDs
 - Each SSID has its own VLAN
 - AP uses 802.1Q and trunking to mark and separate SSID/VLAN pairs



WLAN Client Access

- WLAN client must have
 - Required SSID
 - Compatible data speed
 - Right authentication information
- Client association with network has three stages:
 1. Unauthenticated, Unassociated
 - Initial state
 2. Authenticated, Unassociated
 - Client provided right authentication information to network but it's not yet associated with any AP
 3. Authenticated, Associated
 - Client is associated to concrete AP and has full connectivity

Client Association Steps



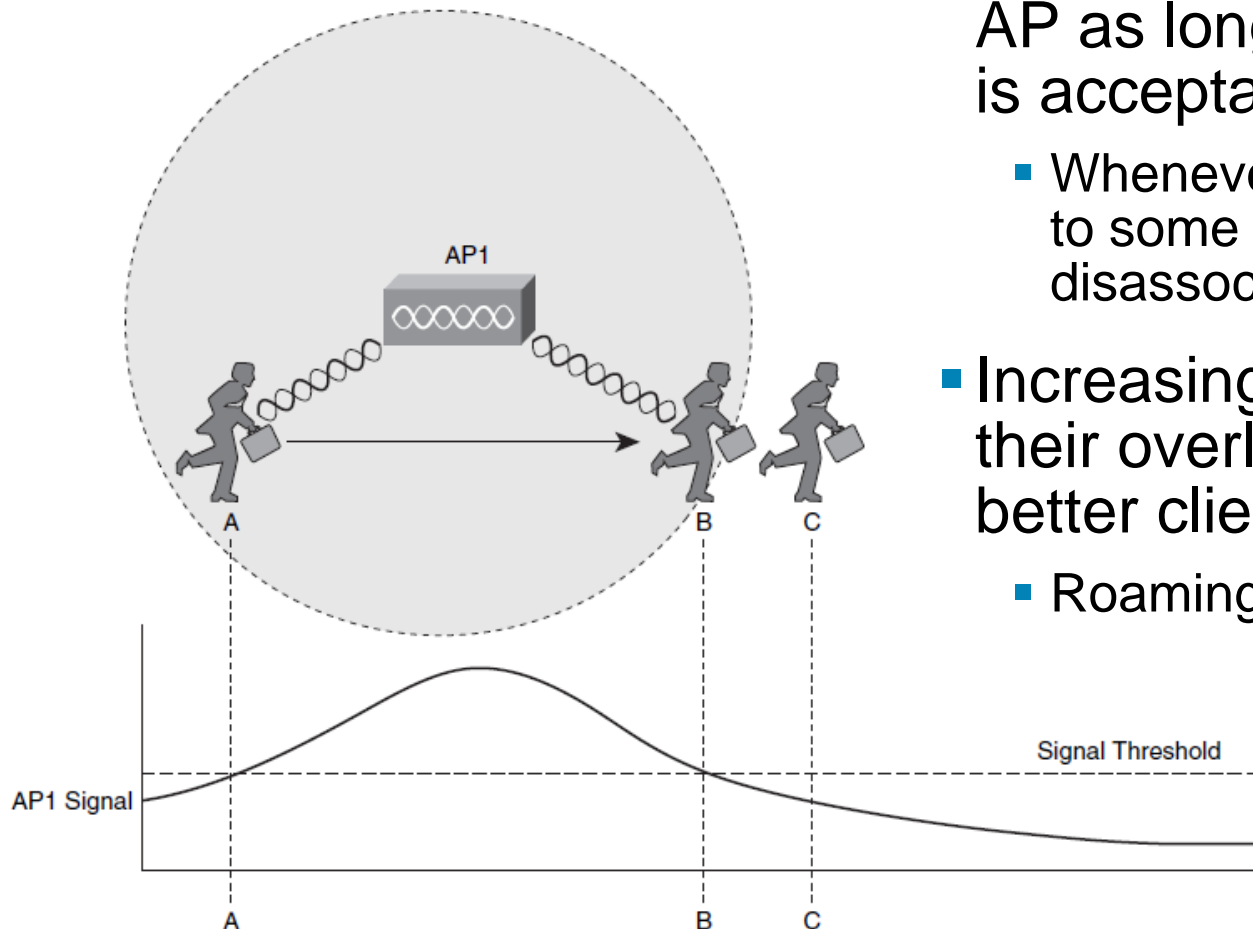
Initial Connection to an Access Point

Steps:

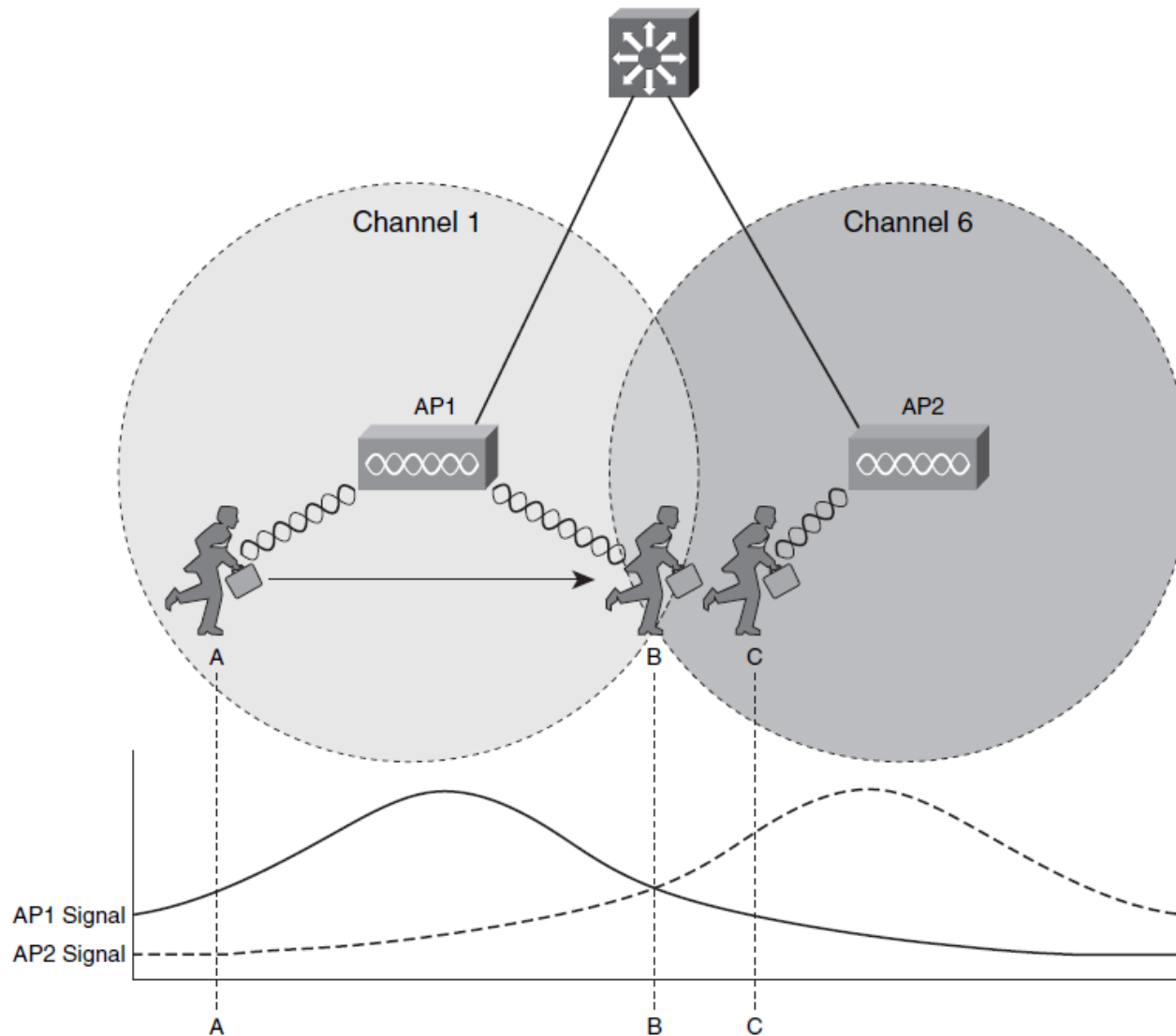
1. Client sends probe request
 2. AP sends probe response
 3. Client chooses among all responses and pick the best AP. Then client initiates association with target AP by authenticating itself
 4. AP accepts authentication
 5. Client sends association request to target AP
 6. AP accepts association and adds client MAC to association table
1. *U-U*
2. *A-U*
3. *A-A*

AP Association

- Client remains associated with AP as long as signal strength is acceptable
 - Whenever signal strength drops to some threshold client become disassociated
- Increasing number of cells and their overlapping supports better client mobility
 - Roaming of client between cells



AP Roaming



- **Roaming** = transfer of client association between APs
 - Directed by client
 - AP assists only in proprietary roaming solutions
- **Roaming criteria**
 - Signal quality, strength, lost, errors during transmission, interferences, etc.
- **Searching for AP**
 - Active: channel range scan by sending probes
 - Passive: waiting for beacon frames

Basic Communication Properties ①

- **Half-duplex**

- Communication happened on one channel
- Only device could transmit at the moment, other devices could receive

- **Shared medium**

- All devices in the one cell share same channel

- **Undirect proportion between speed and distance from AP**

- Speed of each device is affected by distance from AP, quality of medium and channel interferences

- **Different speeds on same channel**

- Devices with slower speed hold others back and decreases overall network speed

- **ACK Transfer**

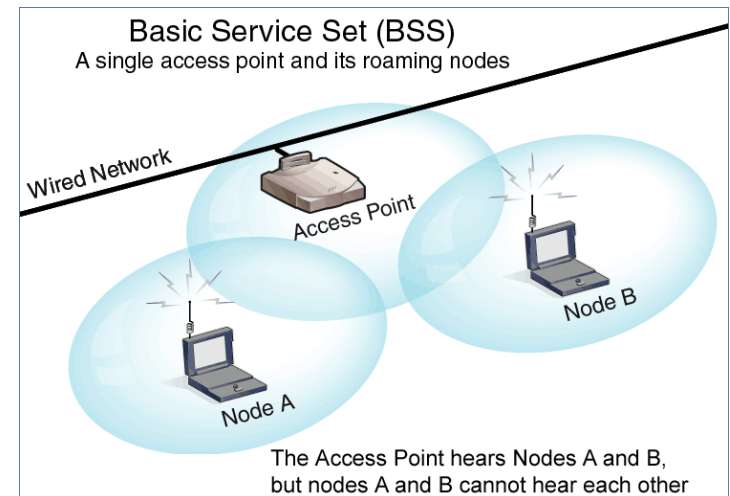
- Devices cannot transmit and receive at the same time – same frequency for transmitting and/or receiving
- Hence, receiver must acknowledge every received frame

Basic Communication Properties ②

- Wireless bridges usually don't allow client association with them
- Pair of wireless bridges associate themselves reciprocally
- APs and wireless bridges are L2 devices behaving similarly as switches
- WLAN creates typically one broadcast domain – one IP range block
- Some advanced APs could operate with multiple SSID where every SSID belongs to different 802.1Q VLAN

WLAN Communication Principles

- WLAN clients must “hear each other” but (with exception to IBSS) data are transferred among them only through AP
- “Hearing each other” is design requirement based on used method how to access shared medium
 - **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
 - It could happened that two clients are so distant to each other that they don't hear each other BUT they both “hear” same AP
 - This so called **hidden node problem** is solved with RTS/CTS mechanism



CSMA/CA

- In CSMA/CA there exist two scenarios:

1. **No client is transmitting**

- After last transmitted period there must follow period of radio silence – so called **DCF Interframe Space (DIFS)**
- IF somebody start to transmit during DIFS THEN client delays its own transmission
- ELSE after DIFS times out THEN client starts transmitting and waits for acknowledgement

2. **Other client is transmitting**

- Client has to wait for = time until ongoing trasnmission ends + random amount of time
- *But how could client guess for how long it should wait?*
 - EITHER all stations hear each other
 - OR RTS/CTS mechanism is used where RTS/CTS messages also contain prediction of transmission time

IEEE 802.11 RTS/CTS

- Add-on to CSMA/CA (not its replacement)
- **Request To Send (RTS)**
 - Control frame where station informs receiver that it wants to send data and signalize about possible amount of time for this data transfer
- **Clear To Send (CTS)**
 - Control frame where receiver acknowledges receiving of RTS message and signalize its own prediction of time required for transfer
- This message exchange instructs all stations in the proximity of transmitter and receiver to hold on communication and keep DIFS

WLAN Frames

▪ Management frames

- Used for WLAN announcing and managing client association
- Includes:
 - Beacons announced by AP with WLAN and its parameters
 - Association, reassociation and disassociation of clients
 - Authentication of clients

▪ Control frames

- Used for first stage of AP-Client association and other controlling issues
- Includes:
 - Probe request (from client) and probe responses (from AP)
 - RTS and CTS messages

▪ Data frames

- Generally all frames carrying any data

Security in WLANs



Security in WLANs

- WLAN security considers following issues:
 - Users and network authentication
 - Data transfer confidentiality
 - Protection against unauthorized extensions to network infrastructure
 - Active network devices protection
- By design WLAN is similarly unsecured as LAN without further configuration
- Wireless character network often make tracing of attacks a much more difficult task and it discourage deploying of WLANs

User Authentication ①

- IEEE 802.11b contains only simple support for user authentication
- Two types of authentication:
 - **Open System**
 - No authentication at all, resp. client request and is automatically granted access to network
 - **Shared Key**
 - AP sends towards a client challenge, client deciphers it with password and sends it back to AP. IF AP is able to decipher with the same password clients response THEN AP considers user to be authenticated
 - Uses static WEP key
 - Password used for authentication is also used for data transfer confidentiality
 - *This procedure has considerable cryptographic issues, hence it's not recommend it to use Shared Key authentication anymore*

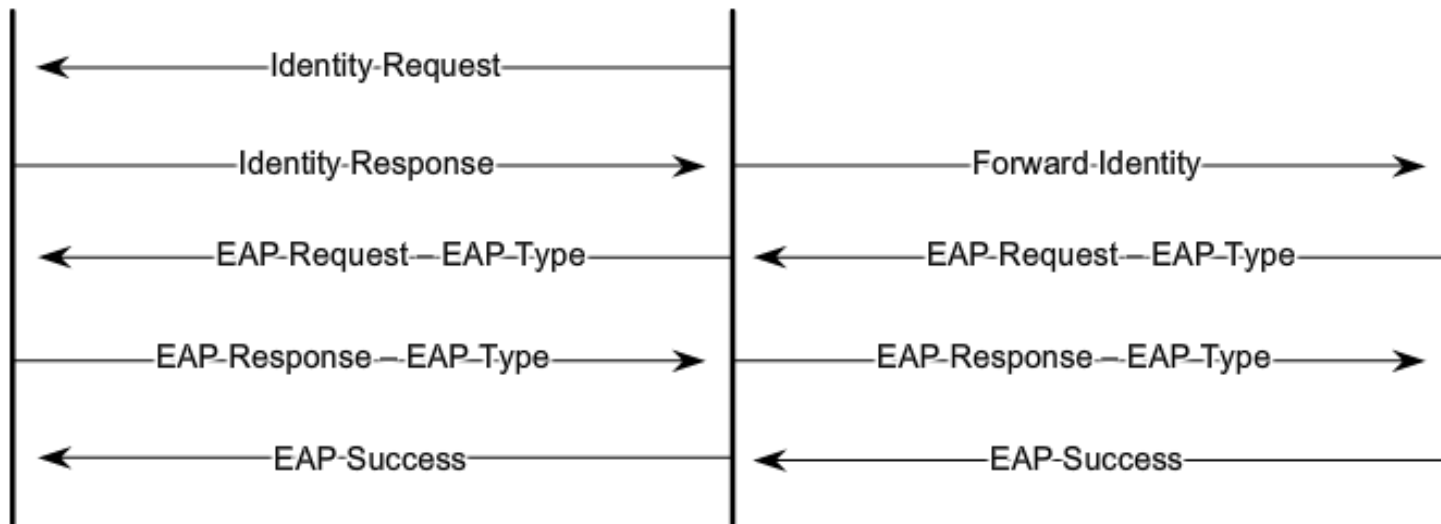
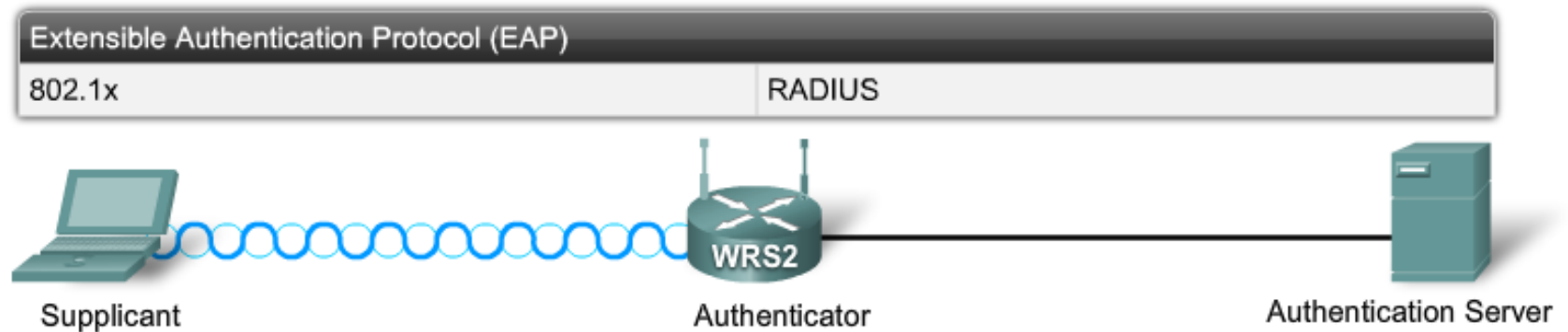
User Authentication ②

- Using Shared Key authentication only threatens overall network security
 - Whenever attacker sniffs initial AP-client authentication messages then the attacker is capable to get password with proper password quickly
 - <http://www.youtube.com/watch?v=uZ5nwjnZVoc>
- This problem is solved by newer authentication mechanisms based on EAP and RADIUS protocols
- Standard IEEE 802.11i covers currently the most deployed security mechanism in WiFi networks – **WPA2**

EAP ①

- **Extensible Authentication Protocol (EAP)**, [RFC 3748](#)
 - Generic protocol (framework) for variety of authentication messages exchange between client (**supplicant**) and point requiring authentication (**authenticator**)
 - It provides basic format of data structures that could be used for any kind of authentication – not an implementation
 - Advantage is that authenticator doesn't have to understand concrete authentication type – it just bridges dialog between supplicant and authentication server
- [RFC 4017](#): “EAP Method Requirements for Wireless LANs”
 - Covers EAP for WiFi environment

EAP ②



EAP – Nowadays Used Variants ①

- Various EAP methods use different credentials for authentication
- **LEAP (Lightweight EAP)**
 - Cisco implementation of challenge-response protocol
 - Username/Password based authentication
- **PEAP (Protected EAP)**
 - Two-phase authentication scheme
 - It requires certificate on server side
 - In the first phase is built secure TLS connection between supplicant and authentication server (verified by TLS certificate)
 - In the second phase user is additionally authenticated

EAP – Nowadays Used Variants ②

- **EAP-TLS (EAP-Transport Layer Security)**

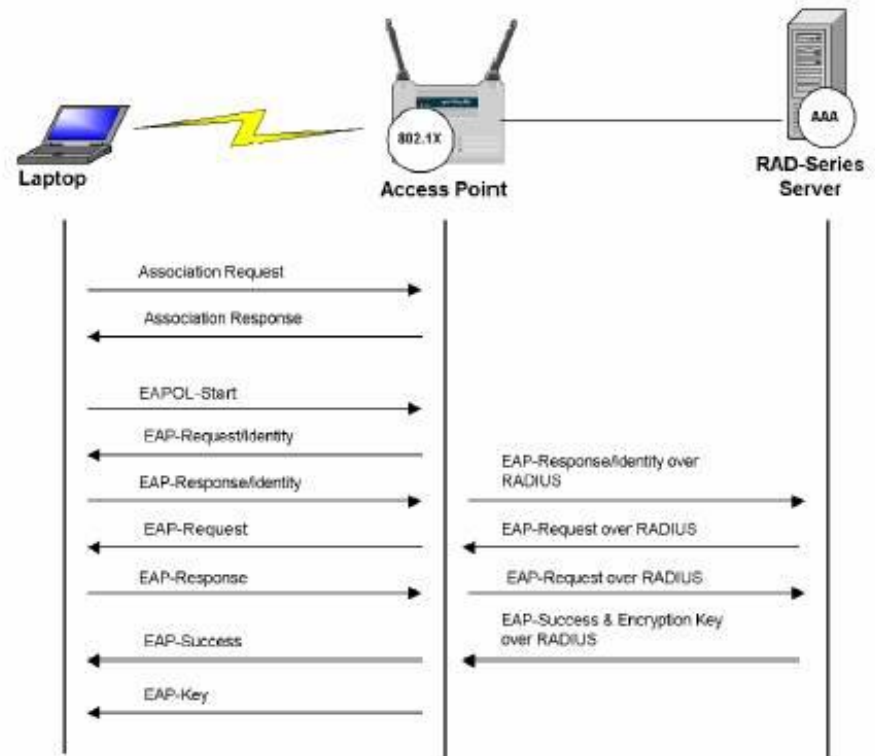
- Mutual authentication of both client and server
 - It requires two certificates – one on clients and one on servers side
 - Secure TLS connection is build between them and both are authenticated and verified based on their certificates
- For multi-vendor environment is suitable to use PEAP or EAP-TLS
- There are plenty of others mostly unused EAP variants
 - EAP-MD5, EAP-PSK, EAP-TTLS, EAP-IKEv2, EAP-FAST, EAP-SIM, EAP-AKA, EAP-AKA', EAP-GTC, EAP-EKE

RADIUS ①

- Open standard specified in IETF [RFC 2865](#)
- Uses TCP/UDP on ports 1812 and 1813
- Provides AAA services between **Network Access Server** (client) and **RADIUS server**
- It allows to client to pass additional configuration information to server in form of attribute-value pairs

RADIUS ②

- EAP messages from client (supplicant) are **encapsulated into RADIUS messages** on AP (authenticator) and are sent to RADIUS server
- Whenever RADIUS server needs additional information then it sends RADIUS message wrapped around EAP messages to AP and following that AP pass it to client



Network Authentication

- Network authentication is needed similarly as user authentication – *Why?*
 - Because it's more than easy to target area put AP with strong signal and same SSID and then lure and associate all possible clients – **Rogue AP**
- For network authentication are suitable EAP methods where server authenticate itself by certificate (PEAP, EAP-TLS, EAP-TTLS, etc.)
- *Unfortunately weak spot of whole process are ordinary users habits ☹*
 - *Typically they completely ignore warning about wrong server certificate and just mindlessly click OK*

Data Confidentiality

- It is necessary to realize that...
 - ...we can not detect passive sniffing of radio transmission
 - ...radio signal can not be easily bounded
 - ...we have to focus on data confidentiality – IF traffic is sniffed THEN attacker should not be able to read it or use it
- Solution is to encrypt all traffic
- First attempt to solve this problem is IEEE 802.11b/g cipher implementation called WEP

WEP

- **Wired Equivalent Privacy (WEP)**

- Symmetric cipher using RC4 algorithm
 - Standard formerly used only WEP 64 (40-bitový key + 24 bit IV vector) but usual implementation WEP 128 uses 104-bit long keys
 - Proprietary implementations have even longer keys
 - Key is static and it same as key for optional authentication
- WEP proofs itself vulnerable for variety of attacks which practically lead to disappearance of this security implementation

WPA

- Replacement for WEP is...
- **WiFi Protected Access (WPA)**
 - Encryption is done by **RC4 algorithm** with 128-bit long basic key and 48-bit long IV vector
 - Key is dynamically changed by **Temporary Key Integrity Protocol (TKIP)**
 - Hence each frame is ciphered with different WPA key derivate from basic key
 - Frame could also carry control checksum which is also encrypted (**MIC – Michael algorithm**)

WPA2

- Successor of WPA is...
- **WiFi Protected Access 2 (WPA2)**
 - Standardized in IEEE 802.11i
 - Uses **Advanced Encryption Standard (AES)** or so called Rijndael encryption algorithm
 - Instead of TKIP it uses **CCMP** for key management
 - Currently there are no effectively working attacks against WPA2
 - Unfortunately because of difference in encryption algorithm deploying of WPA2 is usually connected with changing WLAN infrastructure – devices with performance are needed

Unauthorized Extension to Network Infrastructure

- Attacker could...
 - ...associate itself with our AP even out of the intended signal coverage (outside of the building)
 - ...install its own Rogue AP
- Users could also connect their own WiFi APs or routers to the company network and let it operate with some default (and usually obscure and unsecured) settings
- Solution is not trivial and consists of many safeguard factors
 - List of allowed clients MAC addresses
 - Authentication
 - APs capable of preventive scans to monitor unauthorized APs

Methods for controlling wireless LAN access:

1. SSID broadcasts from access points are off
2. MAC Address filtering is enabled
3. WPA2 Security implemented

CAUTION: Neither items 1 or 2 are considered valid security measures

Active Network Devices Protection

- Administrative access and interfaces should be secured
 - APs are manageable devices and hence could be remotely configured
- *How rare are active network devices with default manufacturers username and password?*
- It is mandatory to at least...
 - ...change access passwords and privileges
 - ...use limited IP range of source addresses for access whenever it's possible
- *No matter how well device is used there's no security benefit when it lacks appropriate configuration!*

Recommended WiFi Security Settings

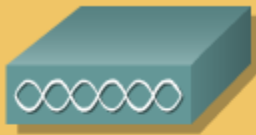
1. Enable data encryption
 - The best is to use WPA2 or at least WPA
 - But using of WEP is at any rate better than to have open unsecured network
2. Change default usernames, passwords and access privileges
 - Those usernames and relevant passwords are well-known and could be easily abused by attackers
3. Change default network name (SSID)
 - Default names only point out to vaguely secured WLAN networks
 - Don't use too evident SSID names (e.g. XYZCompany-Store)
4. Disable printers and file sharing in case you don't need them
 - You block exploitation of relevant information in case that attacker successfully break into and access the network resources
5. Choose place for AP appropriately – signal should cover only allowed area
 - Sector antennas are good choice and place them into the corner of room
 - Some APs allow to change power of emitting signal hence set them appropriately that access could be possible only from secure distance
6. Place firewall between WLAN and LAN where only necessary services should be allowed (web, mail, etc.)
 - Only safe services could be exploited in the case of successful attack

Autonomous and Lightweight Access Points

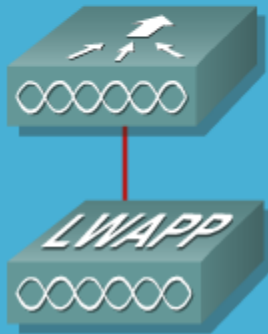


Cisco WLAN Implementations

- Cisco offers two types of WLAN solutions:



- Distributed
 - Autonomous AP
 - Wireless LAN Solution Engine (WLSE)

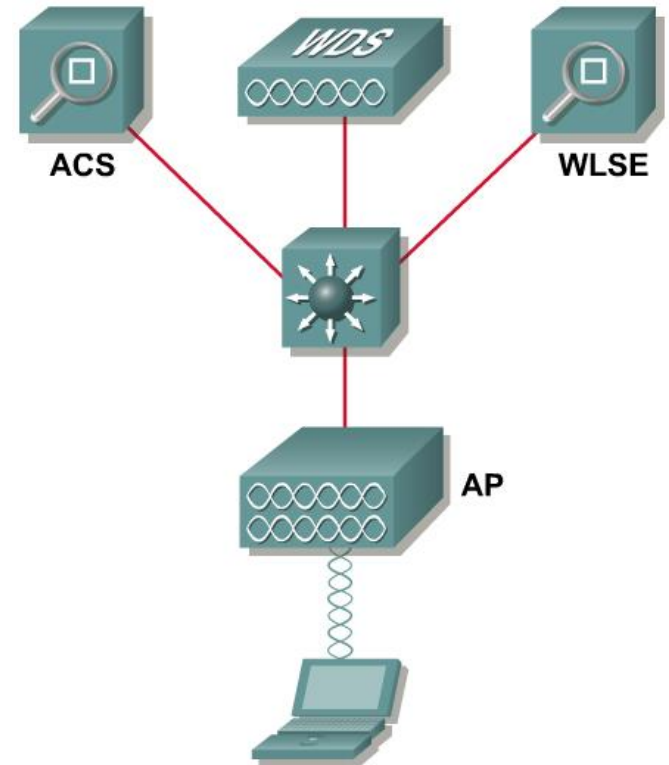


- Centralized (Cisco Unified Wireless)
 - Lightweight AP
 - Wireless LAN Controller (WLC)

- But all approaches require PoE or external power source

Components of Distributed Solution

- **Autonomous AP**
- **Wireless Domain Services (WDS)**
 - Optional
- **Wireless LAN Solution Engine (WLSE)**
 - Management
 - Optional
- **Access Control Server (ACS)**
 - Optional

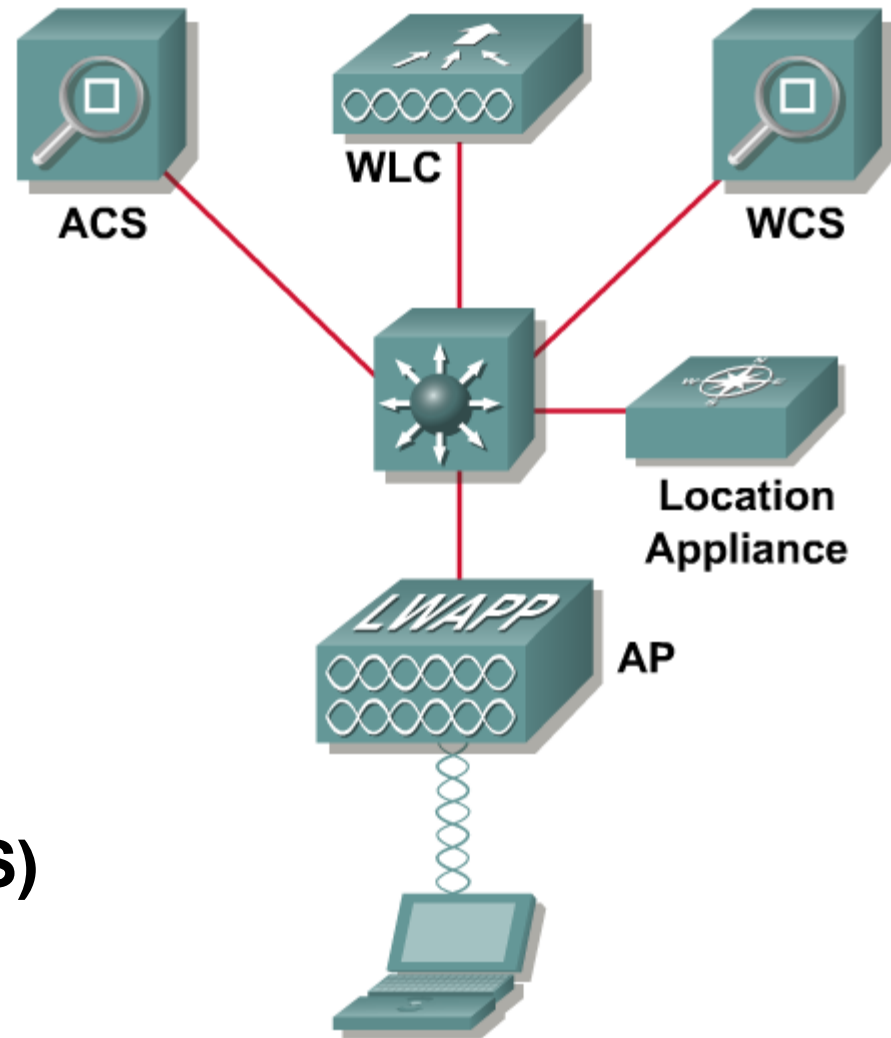


Centralized Solution

- *Idea is as follows*
 - Remove some logic from AP and pass it to some centralized point in the network and this point would provide (share) it to lightweight APs
 - Among those responsibilities are RF management, association and roaming, security and authentication, QoS
 - APs would act only as forwarded antennas which pass all traffic to central point – they remain only 802.11 real-time operations and cyphering
- This innovative idea was invented by Airespace company in year 2002 and later it was bought by Cisco in the 2005
- Solution based on this principles has two base components
 - Lightweight APs
 - Controllers

Components of Centralized Solution

- **Lightweight Aps (LAP)**
- **Wireless LAN controller (WLC)**
 - Mandatory
- **Wireless Control System (WCS)**
 - Optional
 - Manager of multiple WLCs
- **Location appliance**
 - Optional
- **Access Control Server (ACS)**
 - Optional



Operation of Centralized Solution

- Zero configuration of **Lightweight AP (LAP)**
 - All settings are acquired through DHCP server and subsequent communication with WLC
 - Setup of the new LAP is just about installing it on the wall and plugging in network cable
- Controller has all necessary settings for all available LWAPs belonging to its management domain
 - Any change to WLAN settings is done on this central point
 - Central point is aware about whole LAP infrastructure and could revise its operation
 - Controller is point where WLAN frames are fully processed

WLC Functionalities

- **Dynamic management and allocation of channel**
 - WLC defines which channel would LAP use
- **Optimization of transfer performance**
 - WLC sets each LAP transfer performance according to signal coverage and quality
- **Self-Healing**
 - IF one LAPs shuts down THEN signal coverage of other LAPs is increased to overcome problem
- **Flexible roaming**
- **Dynamic load-balance**
 - Client association is distributed among LAPs according to their load
- **RF monitoring**
- **Security management**
 - WLC could enforce client a politic where configuration parameters must be acquired through DHCP server

WLC Platforms

Model	Interfaces	Attributes
2006	4 10/100TX	Handles up to 6 LAPs
4402	2 GigE	Handles up to 12, 25, or 50 LAPs
4404	4 GigE	Handles up to 100 LAPs
WiSM	4 GigE bundled in an EtherChannel for each controller	Catalyst 6500 module with two WLC 4404s; handles up to 300 LAPs (150 per 4404 controller); up to 5 WiSMs in a single chassis
WLC module for ISR routers	Can be integrated in 2800, 3700, and 3800 routers	Handles up to 6 LAPs
Catalyst 3750G integrated WLC	N/A (integrated in 24-port 10/100/1000TX switch)	Handles up to 25 LAPs per switch, up to 100 LAPs per switch stack

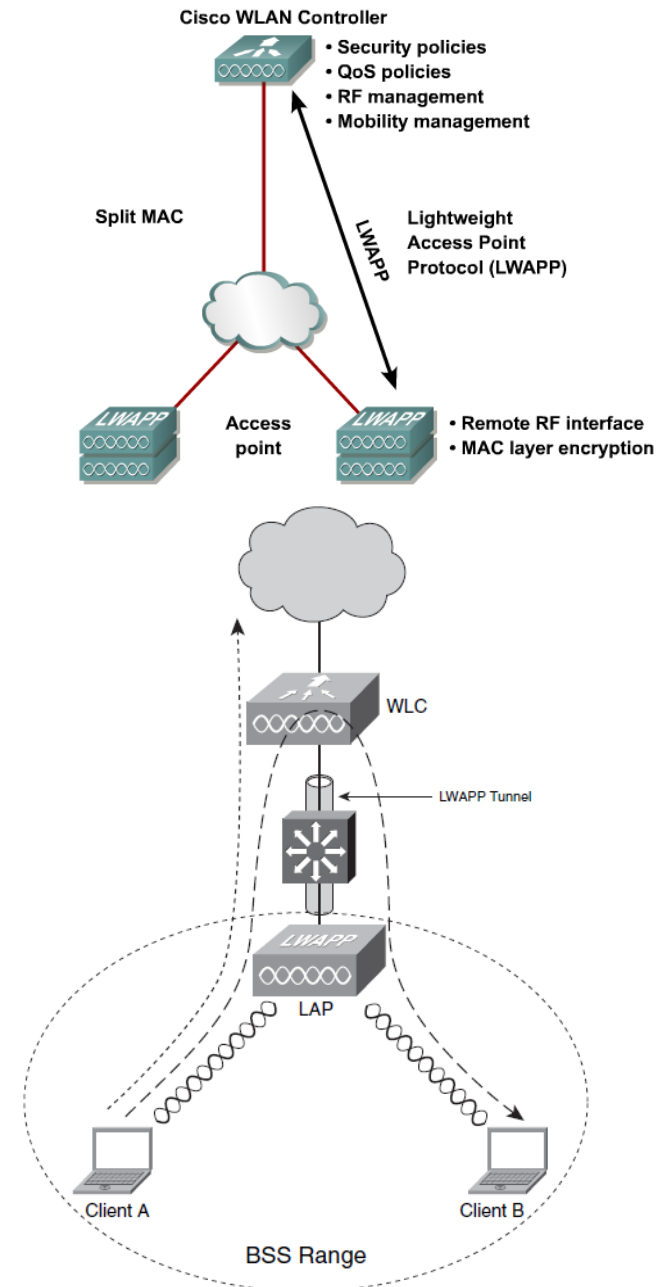
LAP Functionality

Booting up LAP

1. LAP gets all necessary configuration via DHCP (including own IP address, IP address of WLC, etc.) – **L3 LWAPP mode**
2. LAP sends join request to first WLC in the list
 - IF join reply is not received THEN LAP tries another WLC
3. WLC ensures that LAP uses right firmware
 - IF not THEN new firmware is uploaded to LAP
4. WLC and LAP create two LWAPP tunnels – one for management, one for data transfers

Wireless data transfer

1. LAP receives wireless frame from client
2. LAP encapsulates frame into LWAPP and sends it via UDP to WLC for further processing
3. WLC decapsulate frame from UDP/LWAPP segment and process it as ordinary AP
 - Same thing works vice versa in opposite direction

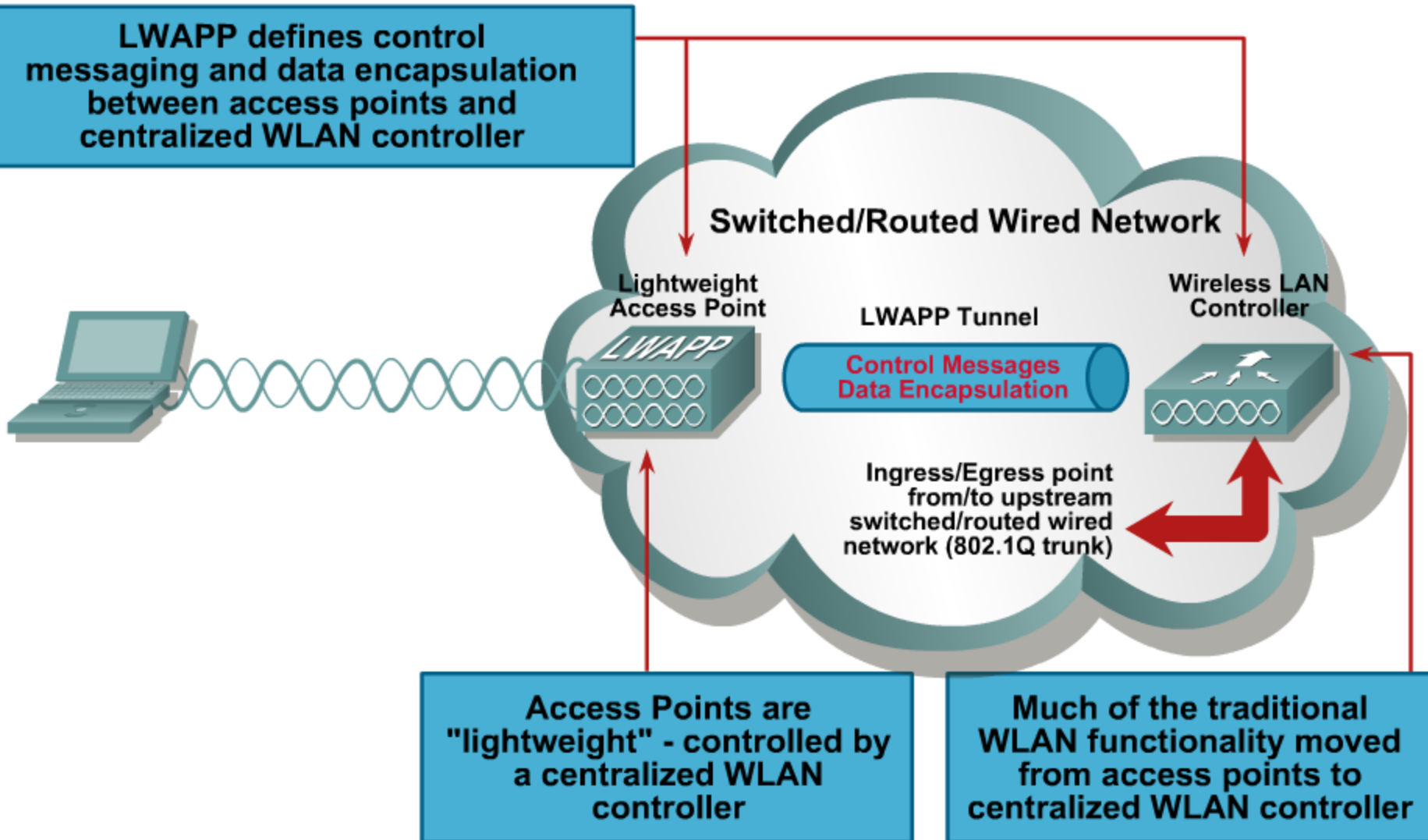


LWAPP ①

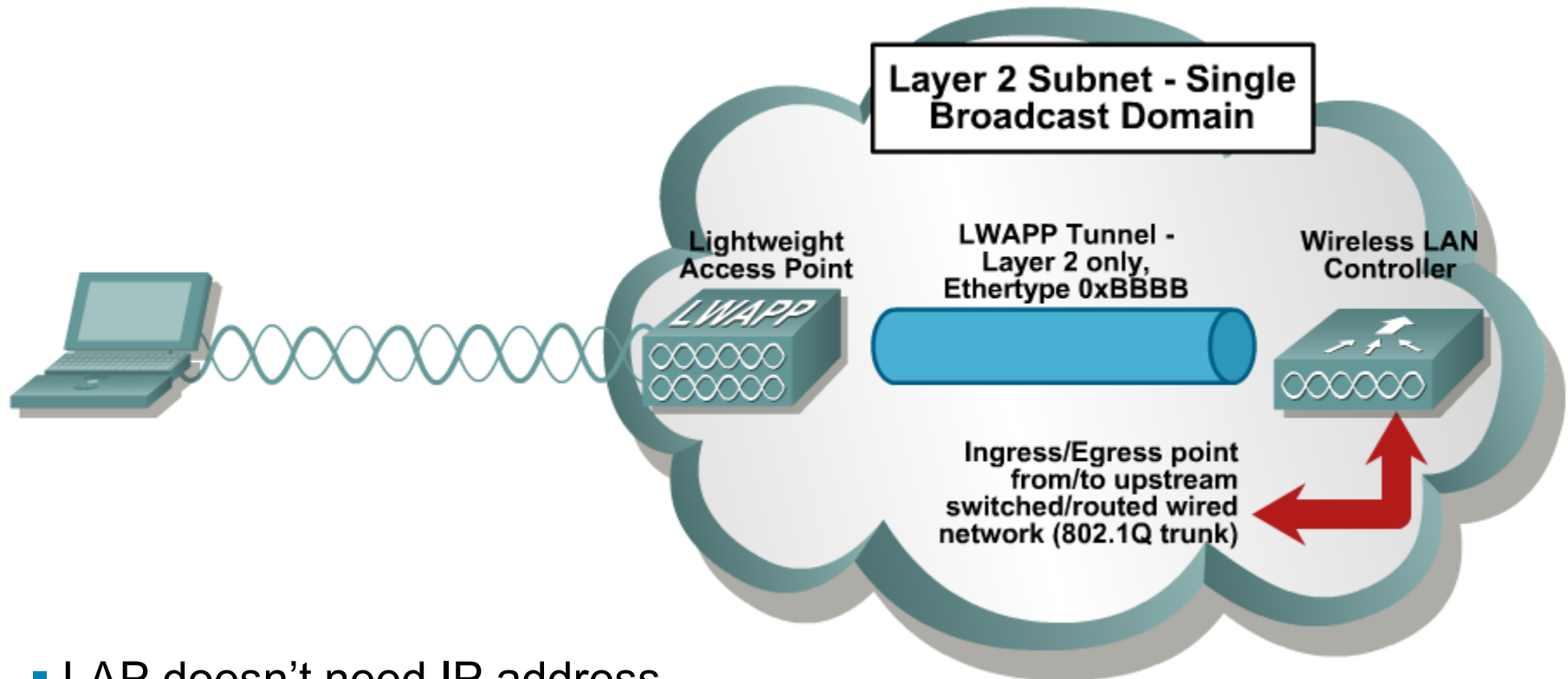
- **Lightweight Access Point Protocol a.k.a LWAPP**
- LAP and WLC communicate via LWAPP
 - Although LWAPP is proprietary protocol, it is described in [RFC 5412](#)
 - LWAPP is predecessor for open standard CAPWAP in [RFC 5415](#)
- LWAPP has two message types
 - **Control**: used for supervising of LAP by WLC, they are cyphered with AES
 - **Data**: inside is encapsulated ordinary wireless client communication, confidentiality is optional (WEP, WPA or WPA2)
- LAP provides only real-time functions where WLC provides all other functions

LWAPP ②

LWAPP defines control messaging and data encapsulation between access points and centralized WLAN controller

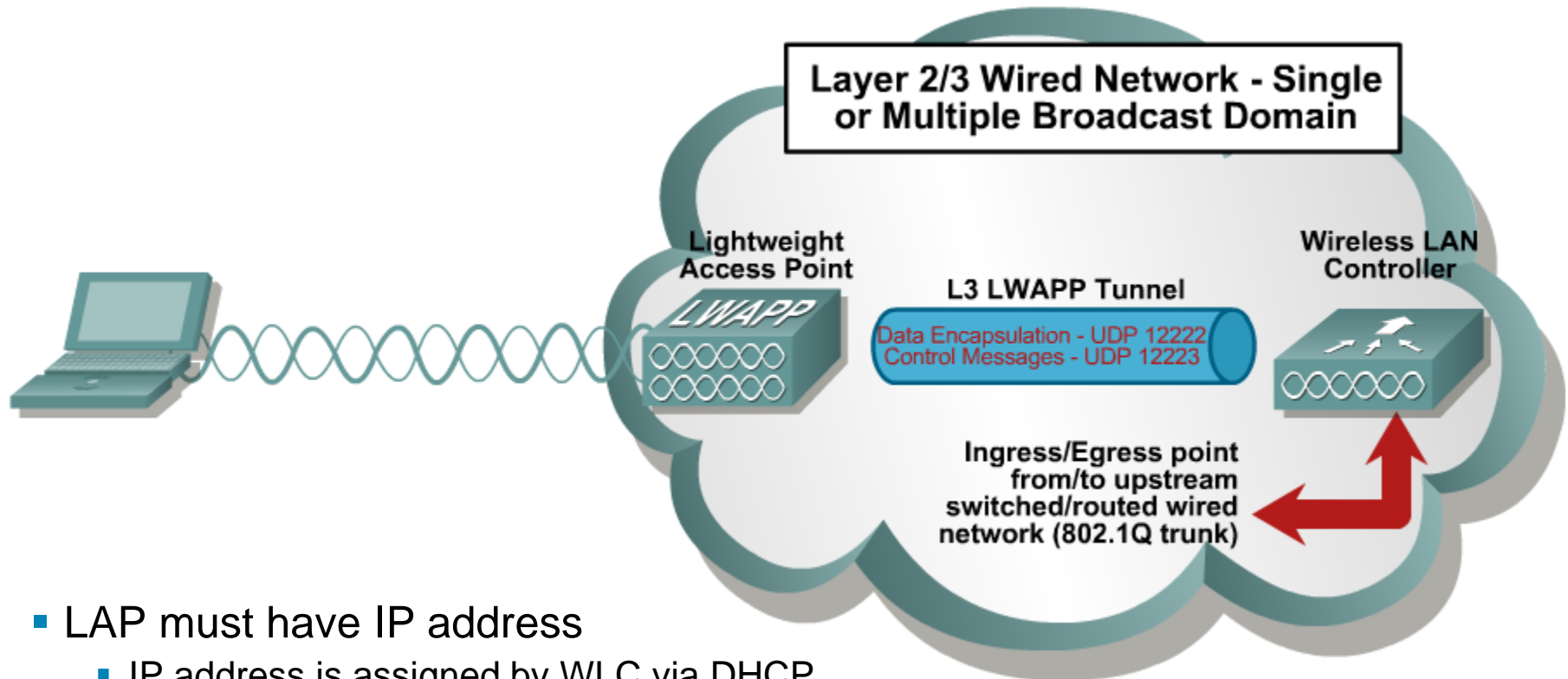


Layer-2 LWAPP



- LAP doesn't need IP address
- WLC must be present in any IP subnetwork where LAPs are present
 - Ethernet frame directly wraps around LWAPP segment
- L2 LWAPP was first attempt in centralized solution, but nowadays it's not implemented or supported anymore

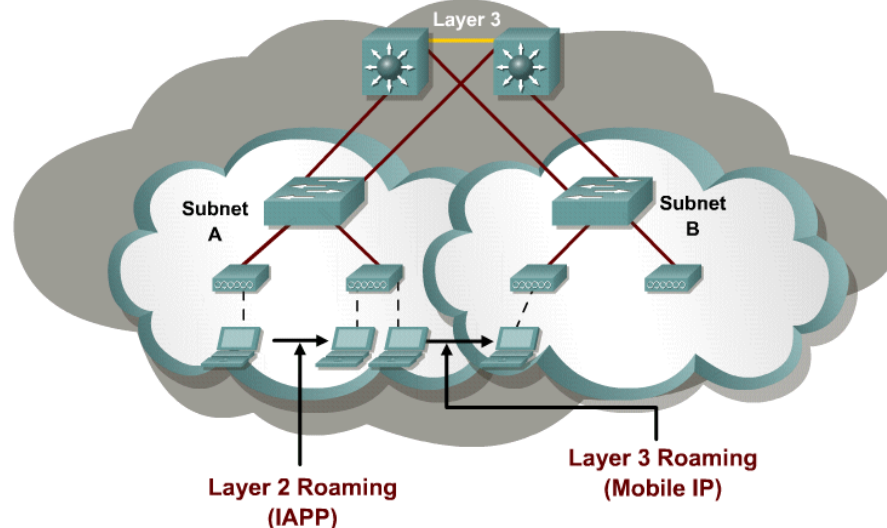
Layer-3 LWAPP













- LAP must have IP address
 - IP address is assigned by WLC via DHCP
- LAP could communicate with WLC independently on its IP subnetwork location
 - LWAPP is usually encapsulated into UDP/IP packets on port 12222 (for data messages) and 12223 (for control messages)
- L3 LWAPP is more flexible than L2 LWAPP

Roaming

- LWAPP allows roaming very easily
 - For users infrastructure between LAP and WLC seems hidden
 - Data traffic is tunneled onto WLC
 - Wherever user resides in network, to WLC tunneled data leaves from this point with IP address of WLC
- According to on which layer roaming occurs there exist two types
 - Layer2 roaming: Inter Access Point Protocol
 - Layer3 roaming: Mobile IP, creates tunnel between Foreign Agent (local router) and Home Agent (user natively belongs to this router when accessing network)



Comparison of Solutions

Distributed Solution	 Wireless clients 	Centralized Solution
Autonomous AP	 Access points 	Lightweight AP
Wireless Domain Services (WDS)	 Control 	WLAN controller
WLAN Solution Engine (WLSE)	 WLAN management 	WLAN Control System (WCS)
PoE switches, routers	 Network infrastructure 	PoE switches, routers
DHCP, DNS, AAA	Network services	DHCP, DNS, AAA

WLC Interfaces

■ Management

- Static IP interface for in-band management of WLC (HTTPS, SSH)

■ AP Manager

- Interface with static IP which all LAP connect to – endpoint for LWAPP tunnel

■ Virtual

- Unique IP address per mobility group used for communication between the access point and the controller for mobility, DHCP relay, Web authentication, and IP Security (IPSec)

■ Service port

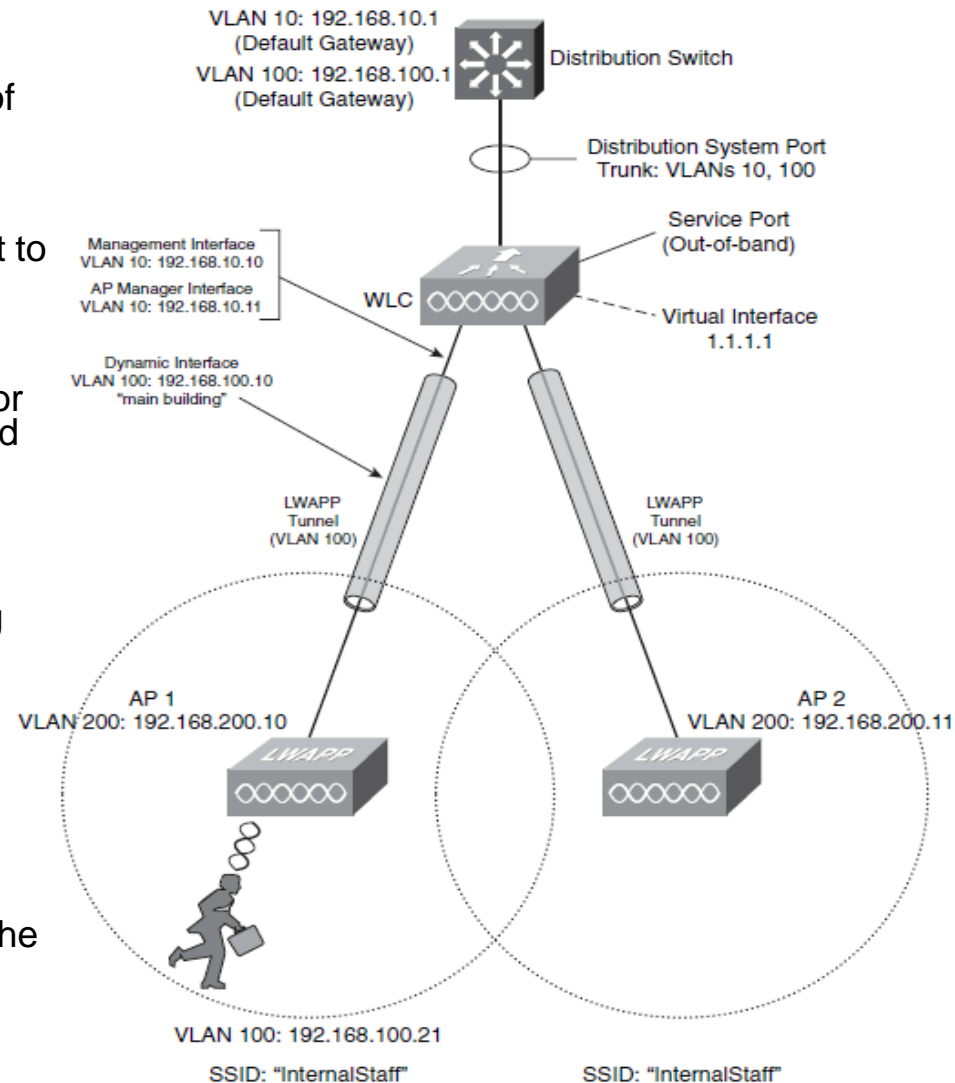
- Used for out-of-band management, including initial setup of the WLAN controller

■ Distribution system port

- Uplink trunk interface to distribution switch

■ Per-SSID Interface

- Carries the data traffic into different VLANs.
- One user interface is configured per VLAN, the SSIDs are mapped to the VLANs



DHCP Server Configuration for LWAPP

```
Switch(config)# ip dhcp pool lap-pool
Switch(dhcp-config)# network 192.168.10.0 255.255.255.0
Switch(dhcp-config)# default-router 192.168.10.1
Switch(dhcp-config)# dns-server 192.168.100.100

! Format of option 43 for Cisco LAP 1000 and 1500 series:
Switch(dhcp-config)# option 43 ascii "192.168.1,10,192.168.1.11,192.168.1.12"

! Format of option 43 for other Cisco LAP:
Switch(dhcp-config)# option 43 hex f10cc0a8010ac0a8010bc0a8010c
```

- Legend:
 - **f1**: type of record
 - **0c**: length of data part in B (three 4 B long IP = 12 B)
 - **c0a8010a**: IP address 192.168.1.10
 - **c0a8010b**: IP address 192.168.1.11
 - **c0a8010c**: IP address 192.168.1.12

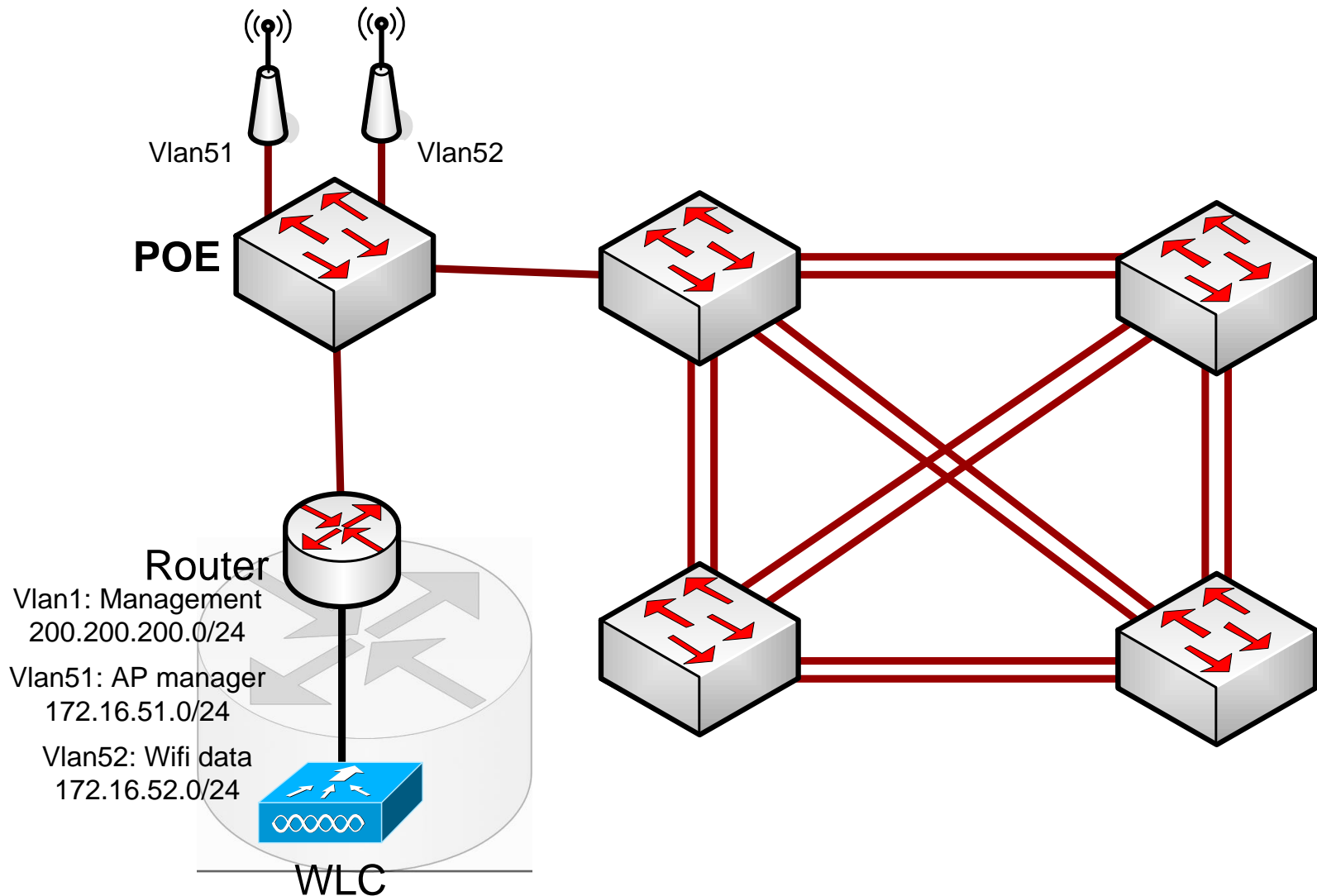
Resetting WLC Configuration

```
(Cisco Controller) > clear config
Are you sure you want to clear the configuration? (y/n) y

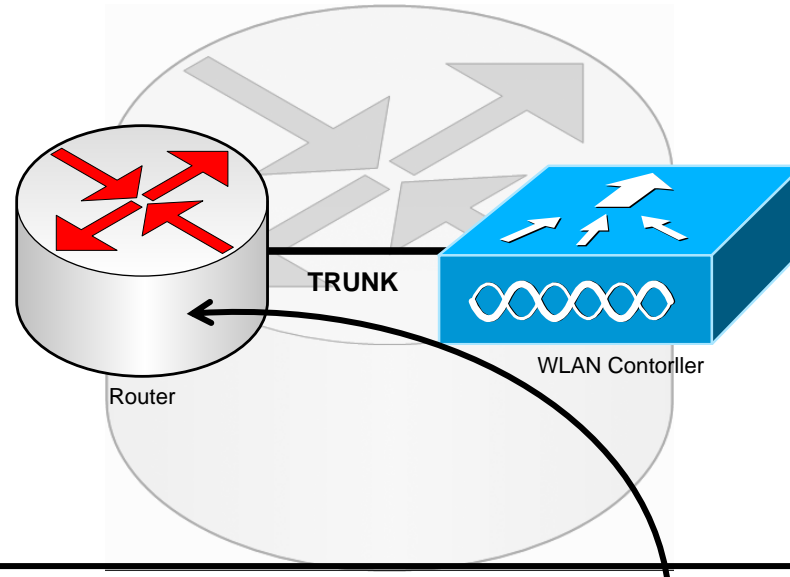
Configuration Cleared!
(Cisco Controller) >
(Cisco Controller) > clear ap-config
Incorrect input! Use 'clear ap-config <Cisco AP>'

(Cisco Controller) > reset system
```

Scenario Topology



Configuring NM-WLC



```
wlc(config)# ntp master
wlc(config)# int wlan-controller 1/0
wlc(config-if)# ip address 200.200.200.1 255.255.255.0
wlc(config-if)# no shutdown
wlc(config-if)# ^Z
```

```
wlc# service-module wlan-controller 1/0 session
Trying 200.200.200.1, 2066 ... Open
```

```
User:admin
Password:*****
(Cisco Controller) >
```

Configuring Router ①

```
wlc(config)# int wlan 1/0
wlc(config-if)# ip add 200.200.200.1 255.255.255.0
wlc(config-if)# int wlan 1/0.51
wlc(config-subif)# description AP manager interface
wlc(config-subif)# encapsulation dot1Q 51
```

If the interface doesn't support baby giant frames maximum mtu of the interface has to be reduced by 4 bytes on both sides of the connection to properly transmit or receive large packets. Please refer to documentation on configuring IEEE 802.1Q vLANs.

```
wlc(config-subif)# ip add 172.16.51.1 255.255.255.0

wlc(config-subif)# int wlan 1/0.52
wlc(config-subif)# description WiFi LAN interface
wlc(config-subif)# encapsulation dot1Q 52
wlc(config-subif)# ip add 172.16.52.1 255.255.255.0
wlc(config-subif)# no shut
```


Configuring Router ②

```
wlc(config)# int fa 0/0
wlc(config-if)# no shut
wlc(config-if)# int fa 0/0.1
wlc(config-if)# encapsulation dot1q 1 native
wlc(config-if)# ip address ...

wlc(config)# ip dhcp pool 51
wlc(dhcp-config)# network 172.16.51.0 /24
wlc(dhcp-config)# default-router 172.16.51.1

wlc(config)# ip dhcp pool 52
wlc(dhcp-config)# network 172.16.52.0 /24
wlc(dhcp-config)# default-router 172.16.52.1
```

Configuring WLC ①

```
wlc# service-module wlan-controller 1/0 session
Trying 200.200.200.1, 2066 ... Open

Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****

Management Interface IP Address: 200.200.200.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 200.200.200.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1]:
Management Interface DHCP Server IP Address: 200.200.200.1

AP Manager Interface IP Address: 172.16.51.2
AP Manager Interface Netmask: 255.255.255.0
AP Manager Interface Default Router: 172.16.51.1
AP Manager Interface VLAN Identifier (0 = untagged): 51
AP Manager Interface Port Num [1]:
AP Manager Interface DHCP Server (200.200.200.1): 172.16.51.1

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: netlab

Network Name (SSID): netlab
Allow Static IP Addresses [YES][no]:
```

Configuring WLC ②

```
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code (enter 'help' for a list of countries) [US]: CZ
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]:
Enter the NTP server's IP address: 172.16.51.1
Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset. [yes][NO]:
yes
Configuration saved!
Resetting system with new configuration...
```

Configuring WLC ③

```
Initializing memory. Please wait. 256 MB SDRAM detected
BIOS Version: SM 02.00
BIOS Build date: 09/17/02
System Now Booting ...
```

```
Booting from disk..., please wait.
```

```
Cisco Bootloader Loading stage2...
```

```
Cisco Bootloader (Version 3.2.171.6)
```

```

      .o88b. d8888888b .d8888. .o88b. .d88b.
d8P  Y8  `88'  88'  YP d8P  Y8  .8P  Y8.
8P      88    `8bo.  8P      88    88
8b      88      `Y8b. 8b      88    88
Y8b d8  .88.  db  8D Y8b d8 `8b d8'
`Y88P' Y888888P `8888Y' `Y88P' `Y88P'
```

```
Booting Primary Image...
Press <ESC> now for additional boot options...
Detecting hardware . . . .
```

```
Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.
```

```
Cisco AireOS Version 3.2.171.6
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
Starting ARP Services: ok
Starting Trap Manager: ok
Starting Network Interface Management Services: ok
Starting System Services: ok
```

Configuring WLC ③

```
Starting Crypto Accelerator: Not Present
Starting Fast Path Hardware Acceleration: ok
Starting Switching Services: ok
Starting QoS Services: ok
Starting FIPS Features: Not enabled
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting LWAPP: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
Starting AireWave Director: ok
Starting Network Time Services: ok
Starting Broadcast Services: ok
Starting Logging Services: ok
Starting DHCP Server: ok
Starting IDS Signature Manager: ok
Starting RFID Tag Tracking: ok
Starting RBCP: ok
Starting Management Services:
  Web Server: ok
  CLI: ok
  Secure Web: ok
```

(Cisco Controller)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration to factory defaults)

User:

Configuring WLC ⑤

! Enable telnet management

```
(Cisco Controller ) > config network telnet enable
```

! Enable web management

```
(Cisco Controller ) > config network webmode enable
```

GUI Setup ①

Cisco - Mozilla Firefox

http://200.200.200.2/screens/frameset.html

Google

Cisco

CISCO SYSTEMS

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor

Summary

Statistics

Controller
Ports

Wireless

Rogue APs
Known Rogue APs
Rogue Clients
Adhoc Rogues
802.11a Radios
802.11b/g Radios
Clients
RADIUS Servers

Summary

Controller Summary

Management IP Address	200.200.200.2
Software Version	3.2.171.6
System Name	Cisco_ea:22:c0
Up Time	0 days, 0 hours, 18 minutes
System Time	Fri Aug 28 12:41:18 2009
802.11a Network State	Enabled
802.11b/g Network State	Enabled

Access Point Summary

	Total	Up	Down	
802.11a Radios	2	2	0	Detail
802.11b/g Radios	2	2	0	Detail
All APs	2	2	0	Detail

Client Summary

Current Clients	2	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs	25	Detail
Active Rogue Clients	4	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

WLAN	# of Clients by SSID	
netlab	0	Detail

Most Recent Traps

Rogue AP : 00:0e:8e:7a:d6:38 detected on Base Radio

Rogue AP : 00:0e:8e:7a:d6:38 detected on Base Radio

Rogue AP : 00:4f:63:80:9d:a3 detected on Base Radio I

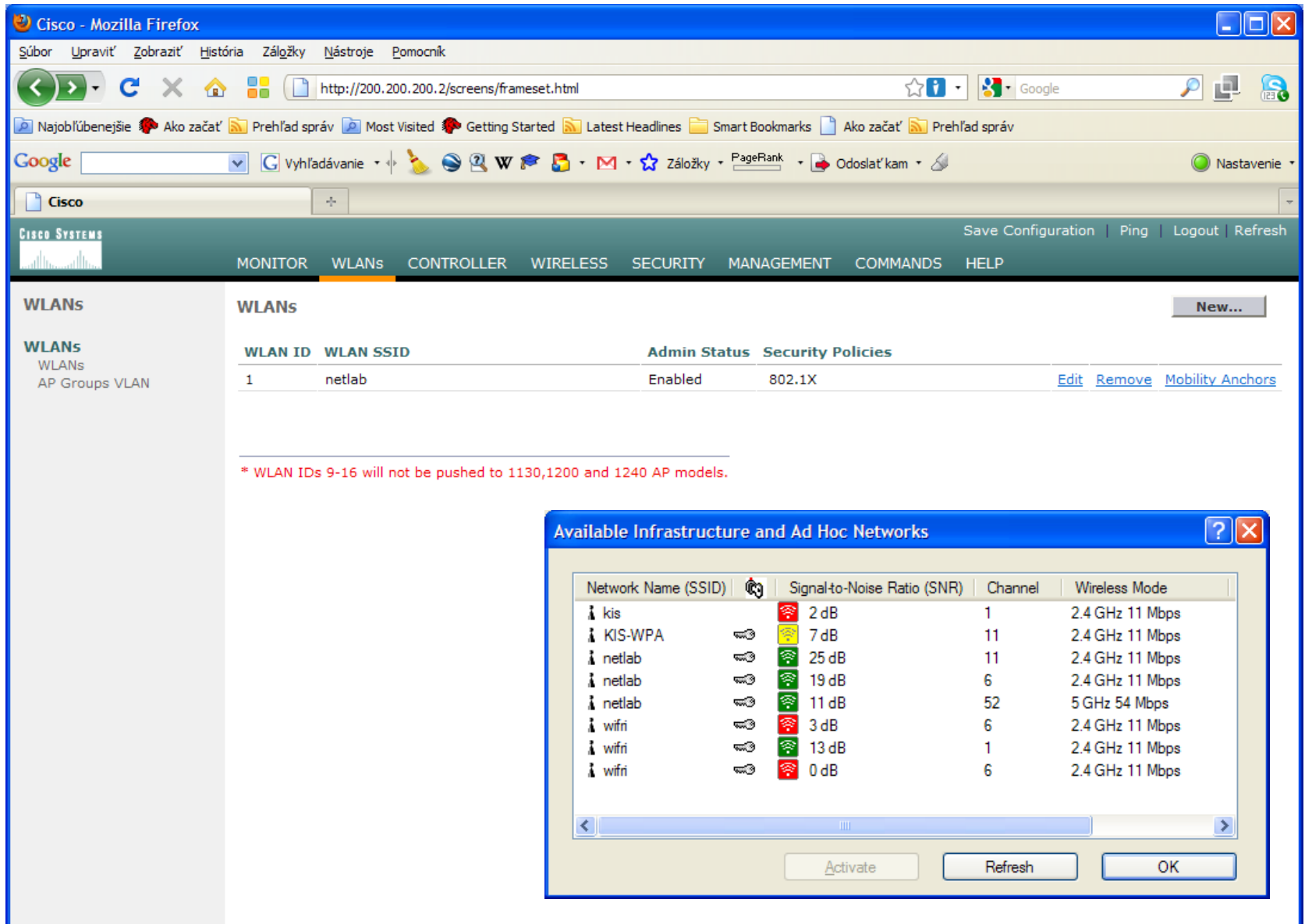
Rogue AP : 00:4f:63:80:9d:a3 detected on Base Radio I

Rogue AP : 00:60:b3:22:71:14 detected on Base Radio

[View All](#)

This page refreshes every 30 seconds.

GUI Setup ②



The screenshot shows the Cisco Wireless LAN Controller (WLC) GUI accessed via a Mozilla Firefox browser. The address bar shows the URL `http://200.200.200.2/screens/frameset.html`. The main navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The 'WLANs' tab is active, displaying a table of configured WLANs.

WLAN ID	WLAN SSID	Admin Status	Security Policies	
1	netlab	Enabled	802.1X	Edit Remove Mobility Anchors

Below the table, a note states: * WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

The 'Available Infrastructure and Ad Hoc Networks' modal window is open, showing a list of detected networks:

Network Name (SSID)	Signal-to-Noise Ratio (SNR)	Channel	Wireless Mode
kis	2 dB	1	2.4 GHz 11 Mbps
KIS-WPA	7 dB	11	2.4 GHz 11 Mbps
netlab	25 dB	11	2.4 GHz 11 Mbps
netlab	19 dB	6	2.4 GHz 11 Mbps
netlab	11 dB	52	5 GHz 54 Mbps
wifri	3 dB	6	2.4 GHz 11 Mbps
wifri	13 dB	1	2.4 GHz 11 Mbps
wifri	0 dB	6	2.4 GHz 11 Mbps

The modal window includes 'Activate', 'Refresh', and 'OK' buttons at the bottom.

GUI Setup ③

Cisco - Mozilla Firefox

http://200.200.200.2/screens/frameset.html

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | **CONTROLLER** | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

Controller

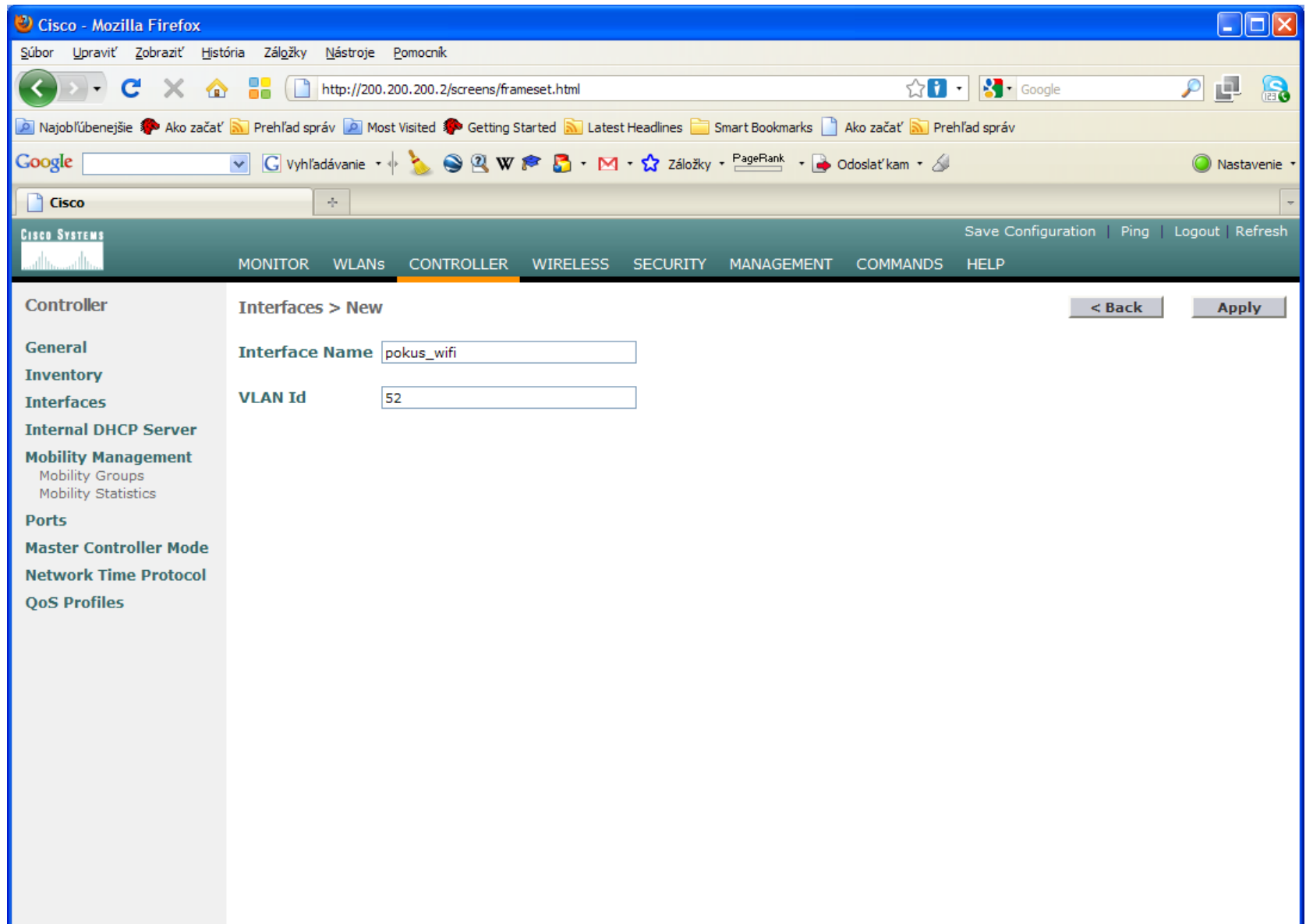
- General
- Inventory
- Interfaces**
- Internal DHCP Server
- Mobility Management
 - Mobility Groups
 - Mobility Statistics
- Ports
- Master Controller Mode
- Network Time Protocol
- QoS Profiles

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
ap-manager	51	172.16.51.2	Static Edit
management	untagged	200.200.200.2	Static Edit
virtual	N/A	1.1.1.1	Static Edit

New...

GUI Setup ④



GUI Setup ⑤

The screenshot shows a web browser window titled "Cisco - Mozilla Firefox" displaying the Cisco Systems GUI. The address bar shows the URL `http://200.200.200.2/screens/frameset.html`. The browser's menu bar includes "Súbor", "Upraviť", "Zobraziť", "História", "Záložky", "Nástroje", and "Pomocník". The toolbar contains various icons for navigation and search. The main content area is titled "Cisco SYSTEMS" and features a navigation menu with options: "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", and "HELP". The "CONTROLLER" tab is selected, and the "Interfaces > Edit" page is displayed. The left sidebar contains a list of configuration categories: "General", "Inventory", "Interfaces", "Internal DHCP Server", "Mobility Management", "Ports", "Master Controller Mode", "Network Time Protocol", and "QoS Profiles". The "Interfaces > Edit" page has a "< Back" button and an "Apply" button. The page is divided into several sections: "General Information" (Interface Name: pokus_wifi), "Interface Address" (VLAN Identifier: 52, IP Address: 172.16.52.2, Netmask: 255.255.255.0, Gateway: 172.16.52.1), "Physical Information" (Port Number: 1), "DHCP Information" (Primary DHCP Server: 172.16.52.1, Secondary DHCP Server: 0.0.0.0), and "Access Control List" (ACL Name: none). A red note at the bottom states: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

Cisco - Mozilla Firefox

Súbor Upraviť Zobraziť História Záložky Nástroje Pomocník

`http://200.200.200.2/screens/frameset.html`

Najobľúbenejšie Ako začať Prehľad správ Most Visited Getting Started Latest Headlines Smart Bookmarks Ako začať Prehľad správ

Google Vyhľadávanie Záložky PageRank Odoslať kam Nastavenie

Cisco

CISCO SYSTEMS

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

General

Inventory

Interfaces

Internal DHCP Server

Mobility Management

Mobility Groups

Mobility Statistics

Ports

Master Controller Mode

Network Time Protocol

QoS Profiles

Interfaces > Edit

< Back Apply

General Information

Interface Name pokus_wifi

Interface Address

VLAN Identifier 52

IP Address 172.16.52.2

Netmask 255.255.255.0

Gateway 172.16.52.1

Physical Information

Port Number 1

DHCP Information

Primary DHCP Server 172.16.52.1

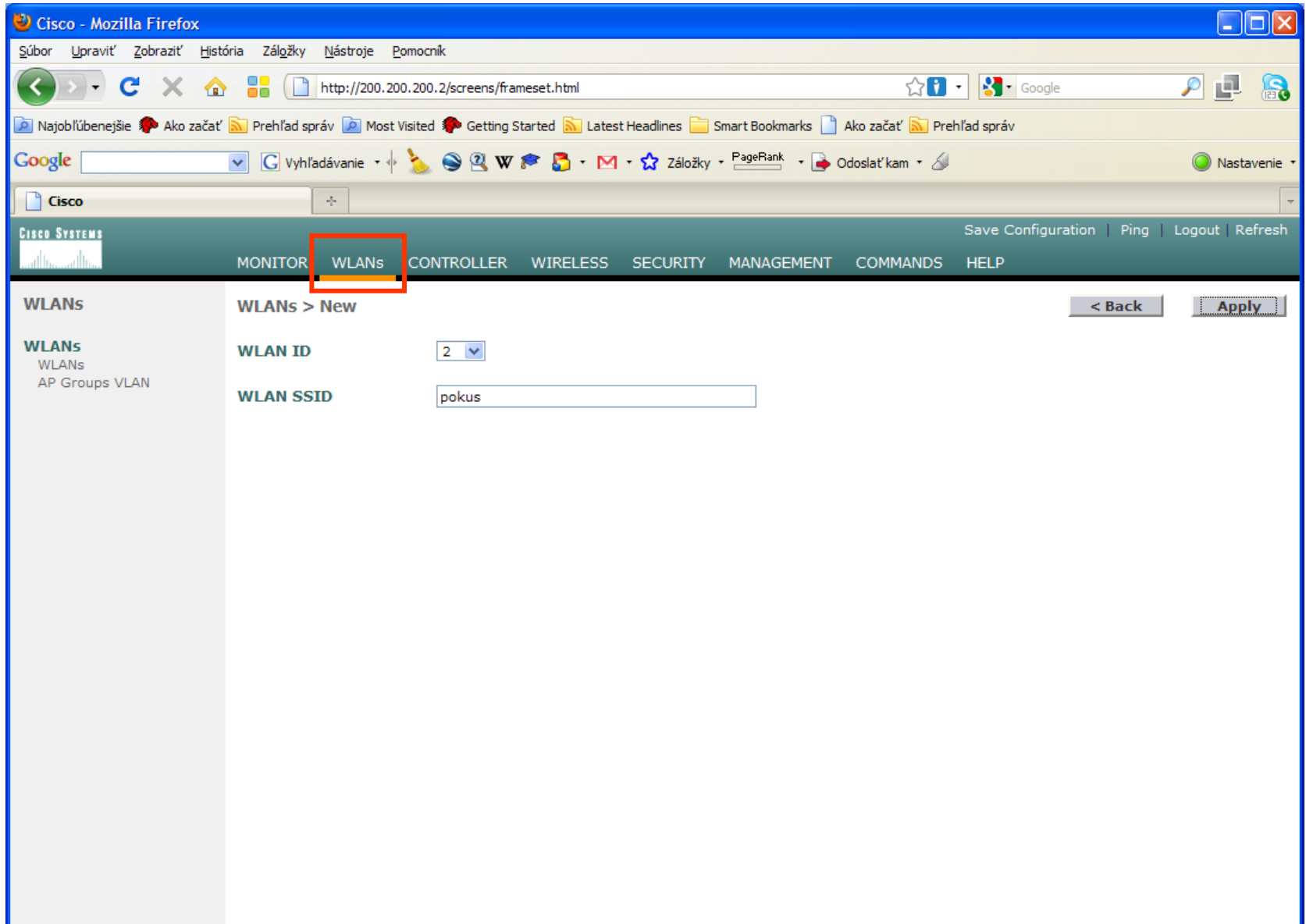
Secondary DHCP Server 0.0.0.0

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

GUI Setup ⑥



GUI Setup ⑦

Cisco - Mozilla Firefox

http://200.200.200.2/screens/frameset.html

Save Configuration | Ping | Logout | Refresh

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

WLANs
WLANs
AP Groups VLAN

WLANs > Edit

WLAN ID 2

WLAN SSID pokus

General Policies

Radio Policy All

Admin Status ☒ Enabled

Session Timeout (secs) 1800

Quality of Service (QoS) Silver (best effort)

WMM Policy Disabled

7920 Phone Support ☐ Client CAC Limit ☐ AP CAC Limit

Broadcast SSID ☒ Enabled

Allow AAA Override ☐ Enabled

Client Exclusion ☒ Enabled ** 60
Timeout Value (secs)

DHCP Server ☐ Override

DHCP Addr. Assignment ☐ Required

Interface Name management
management
pokus_wifi

Radius Servers

Authentication Servers

Accounting Servers

Server 1 none

Server 1 none

Security Policies

Layer 2 Security 802.1X
☐ MAC Filtering

Layer 3 Security None
☐ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

GUI Setup ⑧

Cisco - Mozilla Firefox

Súbor Upraviť Zobraziť História Záložky Nástroje Pomocník

http://200.200.200.2/screens/frameset.html

Najobľúbenejšie Ako začať Prehľad správ Most Visited Getting Started Latest Headlines Smart Bookmarks Ako začať Prehľad správ

Google Vyhľadanie Záložky PageRank Odoslať kam Nastavenie

Cisco

Prajete si, aby si Firefox zapamätal heslo pre používateľa "admin" na serveri http://200.200.200.2? Zapamätať Pre tento server nikdy Teraz nie

CISCO SYSTEMS Save Configuration | Ping | Logout | Refresh

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs [New...](#)

WLAN ID	WLAN SSID	Admin Status	Security Policies	
1	netlab	Disabled	802.1X	Edit Remove Mobility Anchors
2	pokus	Enabled	WPA2 (802.1X)	Edit Remove Mobility Anchors

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

Cisco Solution



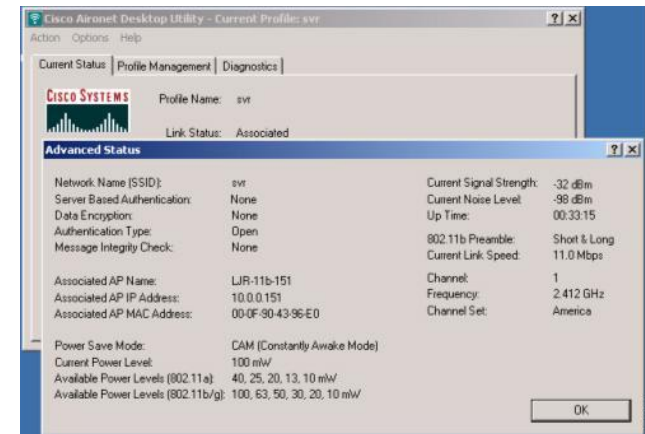
Access Points

- CISCO Aironet 521 AP
- CISCO Aironet 1130AG AP
- CISCO Aironet 1140 AP
- CISCO Aironet 1230AG AP
- CISCO Aironet 1240AG AP
- CISCO Aironet 1300/1400 AP
- CISCO Aironet 1500 AP
- CISCO Aironet Power Injector



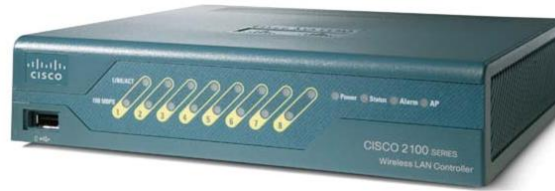
Client Side

- CISCO Aironet 350 WLAN Adapters
- Utilities:
 - ADU = Aironet Desktop Utility
 - ACM = Aironet Client Monitor
 - ACAU = Aironet Client Administration Utility
- CISCO 7921G IP Phone



WLAN Controllers

- CISCO Aironet WLC 2100 Series



- CISCO Aironet WLC 4400 Series



- CISCO Aironet WLC 5500 Series



- CISCO NM-AIR-WLC*



Unified Wireless Network



*Cisco
Self-Defending
Network*



 **Cisco**
Compatible



Unified Advanced Services

Unified built-in support of leading-edge applications not an afterthought. Cisco Wireless Location Appliance, Cisco WCS, SDN, NAC, Wi-Fi phones, and RF firewalls.

World-Class Network Management

World Class NMS that visualizes and helps secure your air space, WCS.

Network Unification

Seamless network infrastructure across a range of platforms. Cisco 4400 and 2000 Wireless LAN Controllers. Future Cisco Catalyst 6500 Series WiSM, ISR, and 3750 integration.

Mobility Platform

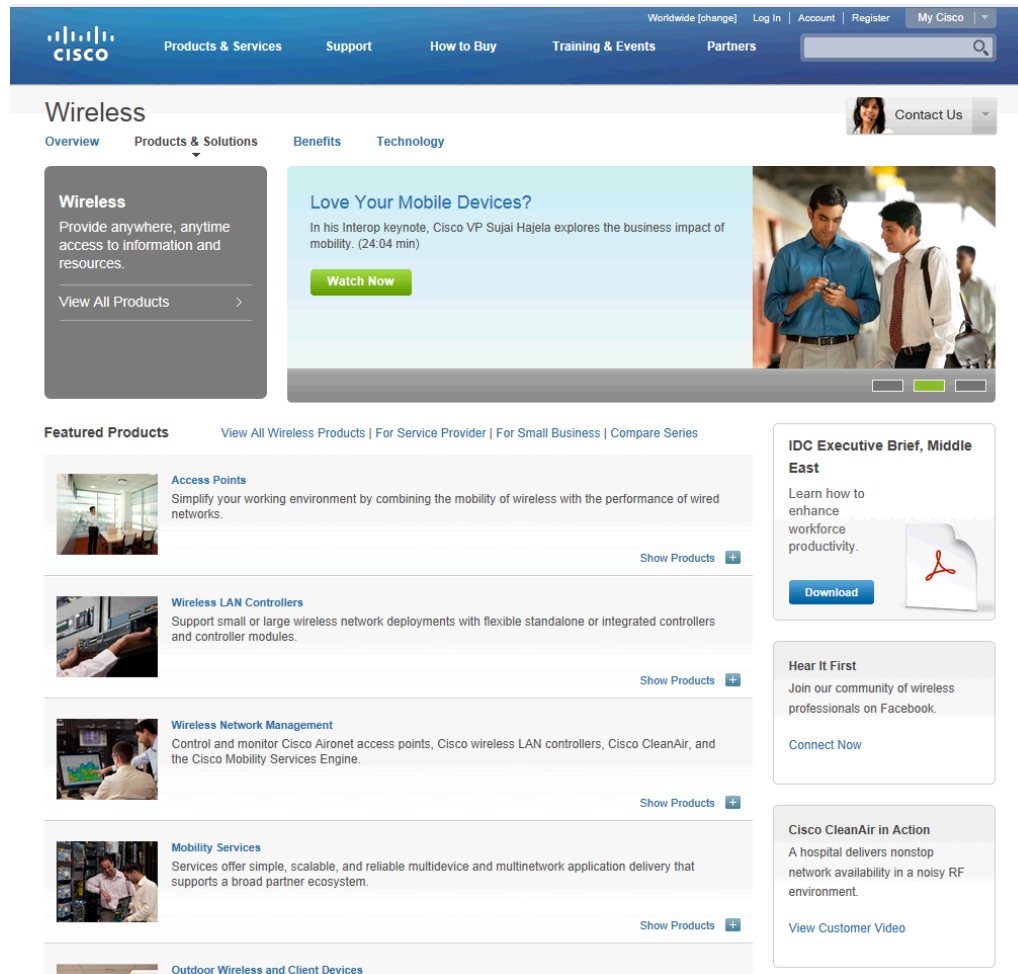
APs dynamically configured and managed through LWAPP. Cisco Aironet Access Points: 1500, 1300, 1240AG, 1230AG, 1130AG, and 1000. Bridges: 1400 and 1300.

Client Devices

Secure clients that work out of the box. Cisco Compatible client devices & Cisco Aironet clients.

Where to go next?

- <http://www.cisco.com/en/US/products/hw/wireless/>



The screenshot displays the Cisco Wireless product page. The top navigation bar includes links for Products & Services, Support, How to Buy, Training & Events, and Partners, along with a search bar and user account options. The main content area is titled 'Wireless' and features a sidebar with a 'Wireless' overview section and a 'View All Products' link. The main content area includes a 'Love Your Mobile Devices?' video player and a 'Featured Products' section with four categories: Access Points, Wireless LAN Controllers, Wireless Network Management, and Mobility Services. Each category has a brief description and a 'Show Products' link. On the right side, there are three additional sections: 'IDC Executive Brief, Middle East', 'Hear It First', and 'Cisco CleanAir in Action', each with a 'Download' or 'View Customer Video' link.

Wireless
Provide anywhere, anytime access to information and resources.
[View All Products](#)

Love Your Mobile Devices?
In his Interop keynote, Cisco VP Sujai Hajela explores the business impact of mobility. (24:04 min)
[Watch Now](#)

Featured Products
[View All Wireless Products](#) | [For Service Provider](#) | [For Small Business](#) | [Compare Series](#)

Access Points
Simplify your working environment by combining the mobility of wireless with the performance of wired networks.
[Show Products](#)

Wireless LAN Controllers
Support small or large wireless network deployments with flexible standalone or integrated controllers and controller modules.
[Show Products](#)

Wireless Network Management
Control and monitor Cisco Aironet access points, Cisco wireless LAN controllers, Cisco CleanAir, and the Cisco Mobility Services Engine.
[Show Products](#)

Mobility Services
Services offer simple, scalable, and reliable multidevice and multinet application delivery that supports a broad partner ecosystem.
[Show Products](#)

Outdoor Wireless and Client Devices

IDC Executive Brief, Middle East
Learn how to enhance workforce productivity.
[Download](#)

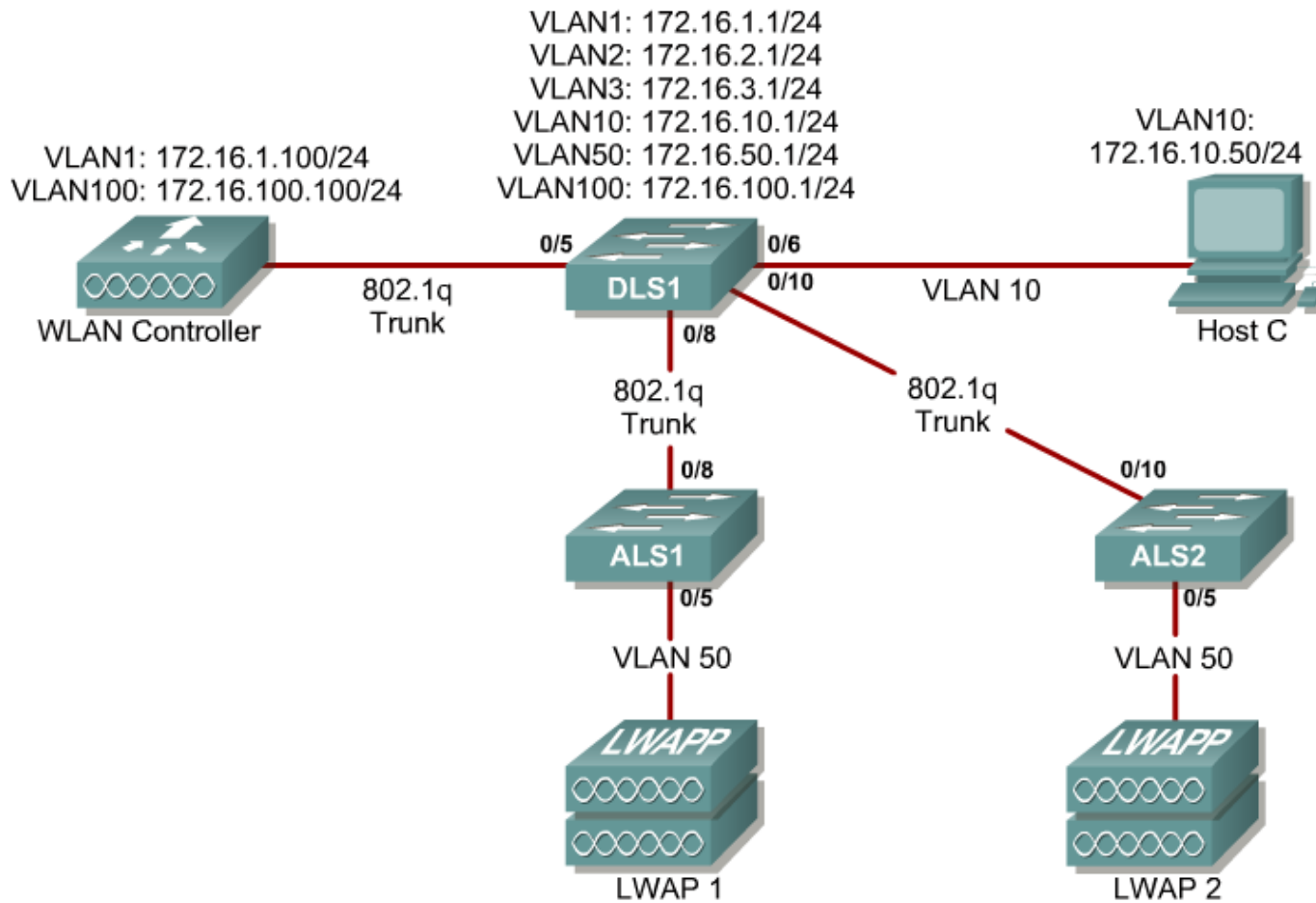
Hear It First
Join our community of wireless professionals on Facebook.
[Connect Now](#)

Cisco CleanAir in Action
A hospital delivers nonstop network availability in a noisy RF environment.
[View Customer Video](#)

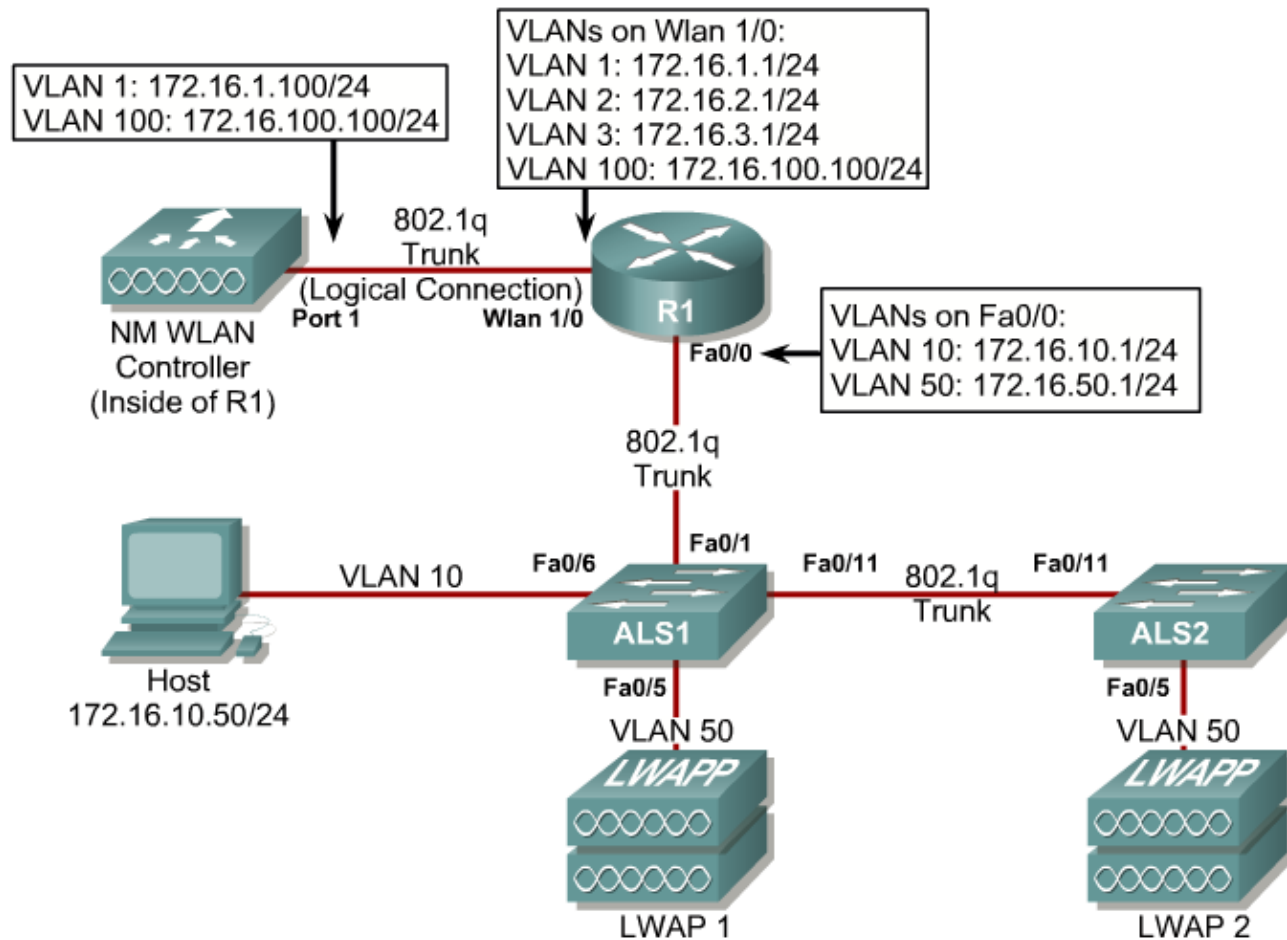
Labs



Variant 1



Variant 2





Slides adapted by [Vladimír Veselý](#) partially from official course materials
but the most of credit goes to CCIE#23527 Ing. Peter Palúch, Ph.D.

The last update: 2013-08-02