

Advanced Internet Technology II: Internet Operation

-Wireless Network Operation-



Masafumi OE

NAOJ

<masa@fumi.org>

Overview

- Learn technologies to develop a wireless network.
 - Summary of IEEE802.11 specification
- Design a wireless network.
 - Hints for successful operation.
- Introduce case studies
 - I learned through wireless network operation at IETF54 and 59.



Technologies for wireless network

Current state of wireless usage

- Everything connects with wireless!



Wireless network printer
HP PSC2710



Network Media player
Buffalo PC-P3LWG

- Notebook computer
- Personal Digital Assistant (PDA)
- Printer
- Media player
- Handheld gaming system
etc.

have built-in wireless device.



Handheld Gaming system
Nintendo DS

Background of this trend

- Why is wireless installed in any equipment?
 - This reason as follows.
 - Decrease price of wireless devices by mass production.
 - At 1997,
 - PC-card type wireless NIC was \$10000/unit.
 - It have no interoperability with other maker's wireless products.
 - Now
 - wireless PC-card based on 802.11b/g is only \$30.
 - It is able to install wireless device to consumer gaming machines due to low priced wireless chipset.
 - Nintendo DS is \$150, PSP by Sony is \$200.



Background of this trend(2)

- Miniaturization of wireless devices.
 - Wireless functions packaged to one chip IC.
 - (Not including RF unit)
 - It becomes easy to develop built-in wireless devices.
 - Various size (type) of NIC released.

SD card type
 IEEE802.11b wireless NIC
 By SanDISK



ONLY
 2.4cm

Background of this trend(3)

- System technology for mobility by manufacturers
 - “Intel Centrino mobile technology”.
 - It is a mobile platform configured from of Pentium M, Intel 855 chipset and Intel Pro/wireless network connection.
 - Wireless built-in notebook PC was popularized.



Background of this trend(4)

- Enrich Hotspot service at public areas.
 - ISP provides Hotspot service, that is wireless connectivity service at public areas.
 - In Japan, many ISP provide hotspot services at airports, railway stations, STARBACKS, McDonalds, etc.
 - Lufthansa provide in-flight internet service “FlyNet” by Connection by Boeing.
- >we can make full use of wireless devices at public area.



Hotspot service providers in Japan

Background of this trend(5)

- Wireless release us from a tangled wire world.
 - In a house, there are a variety of network capable equipment, such as PC, printer, broadband routers, etc.
- > Wireless is able to easy layout of network devices.
- It is not restricted by the length of the cable.
- > Wire instillation is required to take a lot of time and money to equip.

Background of this trend(6)

- Interoperability are certified by WiFi.
 - WiFi CERTIFIED LOGO means the device passed conformance tests for interoperability with IEEE standard.



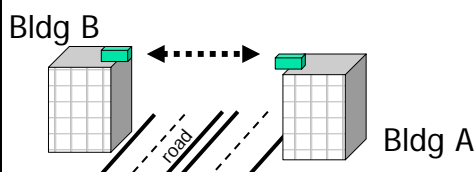
→ This device interoperable with 802.11b device.

WiFi Certified Logo.

Technology overview of wirelsss

Many wireless device released

- Wireless device classify types of media.
 - IR (Infrared light)/Laser type
 - Its are using for high-speed wireless link between bldg.
 - Canobeam · Terabeem · Airfiber etc
 - Link speed is up to 1Gbps.



Many wireless device released(2)



Netwave Airsurfer

- Microwave (Frequency is over 300Mhz-band)
 - Vender specific protocol based.
 - Netwave by Zircom Inc/Netwave-wireless.
 - It is not open standard system.
 - No interoperability for other wireless product.
 - Enclosed system.
 - IEEE 802.11 family protocols.
 - Its are slenderized by IEEE 802.11 WG.
 - Open standard protocol.

In this lecture, I focus on IEEE802.11b/g/a protocols.

Before WiFi(802.11b/a/g) age.

- There was no interoperability with other products before 802.11b appeared.
 - The first product of 802.11b appeared in 2000.
- Wireless system was equal "Product enclosed system."
 - No interoperability with other products.
 - If you want to connect manufacture A's wireless access point, use manufacture A's wireless NIC.
 - When you connect B's AP, you buy B's NIC.
 - In Japan, we were required the radio license for using the wireless system by government.
 - And also we had to use wireless system on the restricted area was permitted by the license.

History of standardization

- IEEE 802.11 commission is working for standardization of wireless network.
- IEEE approved 802.11 at '97
 - Has IR and 2.4GHz-band (microwave) as link carrier.
 - On 2.4GHz-band, 802.11 has two types of spectrum spread method.
 - FH-SS, Frequency Hopping - Spectrum Spread.
 - Fault tolerance is high, transmission rate is slow.
 - DS-SS, Direct Sequence - Spectrum Spread.
 - Fault tolerance is low, transmission rate is fast.
 - has 1Mbps mode and 2Mbps mode as link speed.
- 802.11 based products released, however, did not popularize.

802.11b was appeared.

- IEEE approved 802.11b at '99
- It is extension of 802.11 DS-SS mode.
 - Added 5.5Mbps and 11Mbps as link speed.
 - 11b has the function of dynamically changing link speed to 1, 2, 5.5 and 11Mbps.
 - The speed is depending on a radio signal condition.
 - 11b use 2.4GHz ISM band.
 - ISM: Industry Science Medical band can be used without the radio license.
 - Regulation for ISM-band MAY be different in each country.

802.11b products released

- Manufacturers develop wireless chipsets.
 - Lucent/Intersil/Aironet/3Com etc.
- First product released at '00.

About IEEE802.11a(1)

- IEEE approved 802.11a at 1999, too.
 - Product released at '01.
 - Manufactures released after successful of 802.11b.
- 802.11a use 5GHz-band
 - 11a use more high frequency than 11b.
 - 5GHz-band may have some effect by rain and snow.
- Link speed is 54Mbps.
 - 802.11a use OFDM (Orthogonal Frequency Division Multiplexing) as modulation.
 - OFDM is able to use a radio bandwidth in efficiently than DSSS in 802.11b.
 - Merit of OFDM is strong in phasing and the multipass.

About IEEE802.11a(2)

- Usage limitation of 802.11a is different each country.
 - In Japan, Permitted frequency from 5.15GHz to 5.25GHz without a license and also indoor use only.
 - Because 802.11a interferes in weather observation system, AMEDAS, that use 5GHz-band.
 - In US, permitted 5.15 ~ 5.25GHz, 5.25 ~ 5.35GHz and 5.725 ~ 5.825GHz-band.
 - US has three times of radio band range than Japan.☺
- Country localized products fit each country's law.
 - Japan localized 11a card can't associate with US localized access point.

About IEEE802.11g (1)

- First product was released at '03.
 - Manufacturers release products while IEEE is finalizing specification of 802.11g from draft.
- 11g uses same frequency band as 11b.
 - 2.4Ghz-band.
- Link speed is up to 54Mbps.
 - 11g use OFDM / PBCC(=Packet Binary Convolution Code) / OFDM-CCK as modulation.

About IEEE802.11g (2)

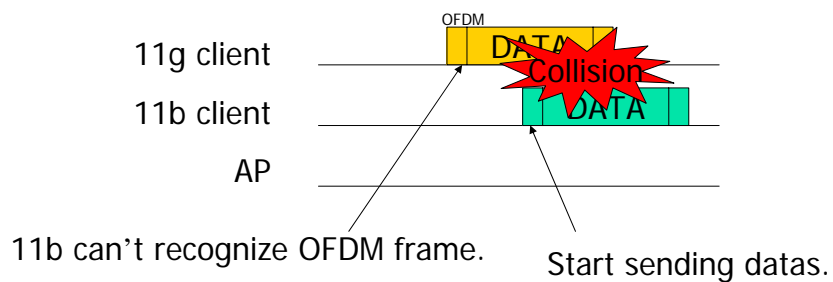
- 802.11b/g combo chipset released
 - It is adopted for a lot of consumer products.
 - Decrease the price of chipset.



Atheros
11b/g combo chip

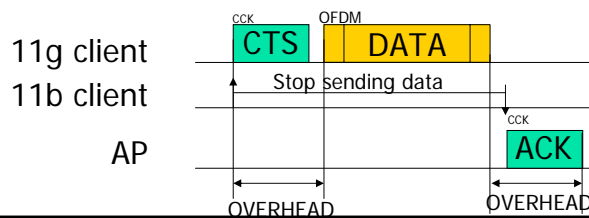
Compatibility with 11b(1)

- 11b and 11g use same 2.4GHz-band with different modulation architecture.
 - 11b can't recognize 11g's OFDM frame.



Compatibility with 11b(2)

- 11g use OFDM-CCK modulation to avoid framing collisions between 11b and 11g.
- OFDM-CCK is send CTS (Clear to send) frame with CCK modulation before OFDM modulation and ACK frame after send.
 - 802.11b clients recognize CTS frame and stop to send data until receiving ACK.
- The performance decreases when both of 11g client and 11b client exist in same area because OFDM-CCK has more overhead than OFDM.

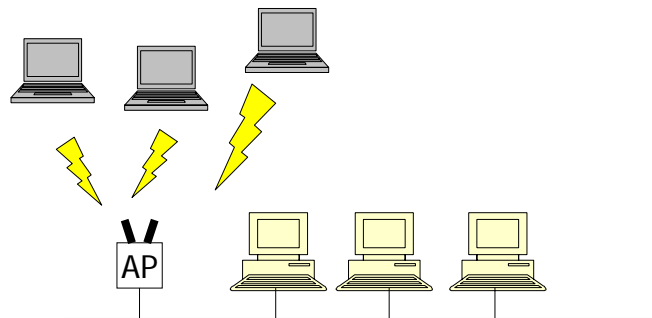


Three operation mode

- IEEE802.11 has three operation mode.
 - Infrastructure mode
 - ad-hoc mode
 - WDS:Wireless Distribution System mode.

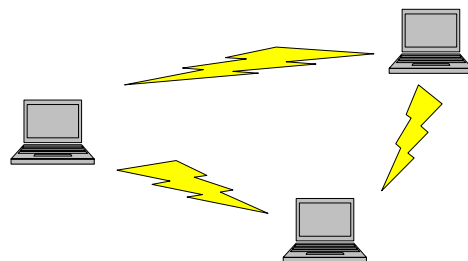
Infrastructure mode

- Node associate with AP as client.
- Client communicate via access point(AP).
- AP works as bridge.
- This mode is usually used in wireless network.



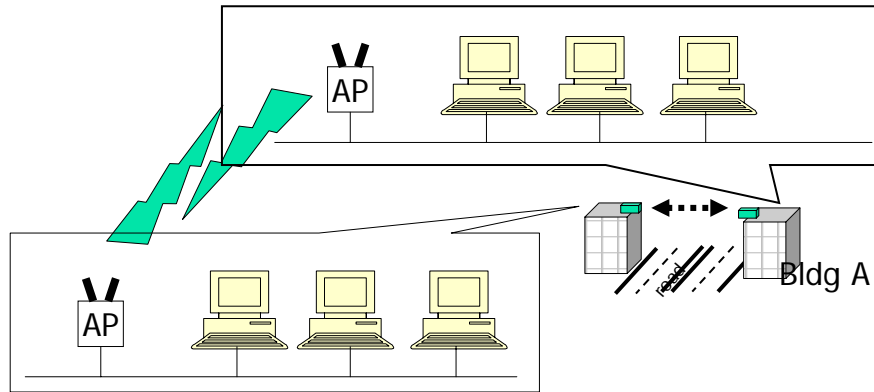
Ad-hoc mode

- A node commutates other node without AP.
- No AP is required



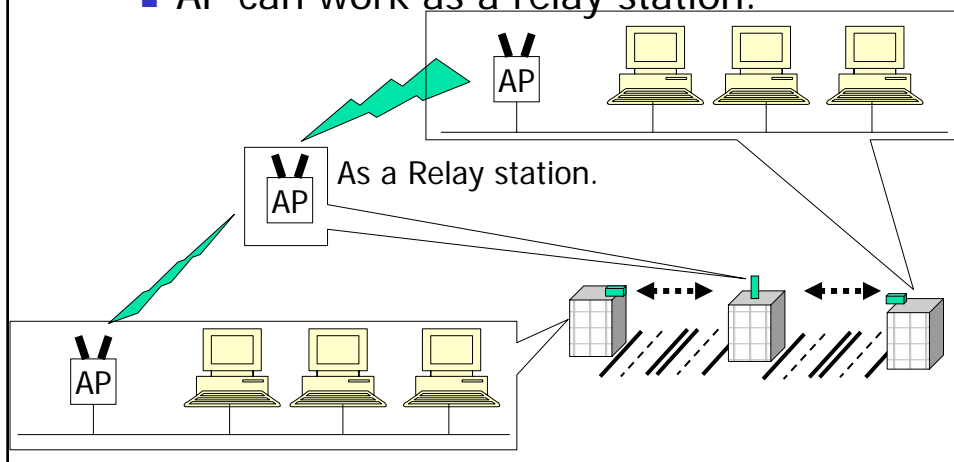
WDS mode(1)

- Connects between LAN and LAN via AP.



WDS mode(2)

- AP can work as a relay station.



Wireless Interoperability

- WECA (Wireless Ethernet Compatibility Alliance) appeared.
 - WECA established to popularize wireless technologies at 1999.
 - Founded by Lucent, Intersil, Aironet (Cisco) .
 - Authorizes interoperability of 802.11 device.
 - It is called "Wi-Fi Certified".
 - Defines specification for interoperability.
 - Wi-Fi System Interoperability Test Plan
 - tests wireless device to interoperable with IEEE 802.11 specification.



Certified Logo

The effects of WiFi(1)

- Make competitive markets.
 - We are able to choice products based on Wi-Fi
 - It is similar to wired NIC markets.
 - Developing of product is sharply contested
 - Product price is going down from \$150 at '99 to \$30 at '04.

The effects of WiFi(2)

- Various of NIC type are released.
 - PC-card type for notebook.
 - CF (Compact Flash) type for PDA/notebook
 - SD/IO type for PDA
 - MiniPCI type for notebook



PC-card type



CF type



MiniPCI type

It is used as built-in wireless device on notebook type.

The effects of WiFi(3)

- The manufacturer develops a good one after another product.
 - Power saving wireless card.
 - More less impact for a battery life on notebook computers.
 - Multi-band wireless card.
 - 802.11a, 11b and 11g combo card released.
- “Enclosed wireless systems” has been to an End.
 - Wireless LAN become open system by WiFi.

Security technology for wireless(1)

- WEP: Wired Equivalent Privacy
 - Encrypts a data link with a shared key.
 - WEP based on RC4 algorithm.
 - Private key length is 128bit and 64bit.
 - 128bit key is recommended.
 - The key should be changed at periodic intervals.
 - *The risk for leaking the key is proportional to the number of users.*

Security technology for wireless(2)

- Operate an authentication system for users.
 - ID/Password authentication on the WEB.
 - MAC address authentication.
 - Permitted user's MAC address is registered. to RADIUS server or to AP's local database..
- Separate wireless network from secured network.
 - Operate wireless network with different security policy.
 - Make access control from wireless network to wire network.

Security technology for wireless(3)

- Operate IEEE802.11i.
 - 802.11i is configured an authentication function and a encryption function.
 - The encryption function on 802.11i is called WPA (WiFi protected access). WPA has more strongly encryption than WEP.
 - The authentication function is based on IEEE802.11x.
- Operating 802.11i takes cost though it is very safe.

Wireless network Design

Design points

- Wireless network design is quite different from a wire network design.
- Understand characteristics of wireless.
 - Cover range of Access Point.
 - Interference with between channels.

How to design a wireless LAN

- Fix policy from purposes, requirement of a wireless network.
 - Who use the wireless network?
 - How long is life of the wireless network?
 - What is security level?
 - etc.
- The design of the wireless network is different according to the operation purpose.
 - Operation wireless network on campus.
 - Operation wireless network on enterprise.
 - Operation temporary network on a conference.

The sense of policy balance is important.

Understanding "Trade-off."

- Operate wireless network with high security level.
 - It is possible to construct it with 802.11i/WPA etc.
 - We can enjoy a safe network.
- BUT
- Management side needs an account work of each user.
- And require to support user side.
 - Assistant settings, distributing account, etc.
- User side is required to install security future capable OS.
 - Linux/FreeBSD/NetBSD support 802.11i?
 - Guys can enjoy the high security wireless network?
 - Only a part of OS supports new security technologies, such as WPA, 802.11i(11x).
- In the compensation for safety, the operation cost is large.

Security level and operation costs(1)

- Operate wireless network with WEP
 - We can prevent to tapping of wireless network from unauthorized user.
 - Need to provide WEP key and parameters information to authorized users.

Security level and operation costs(2)

- Operate 802.11i/WPA on wireless network for high security.
 - It's good for a enterprise network.
 - A leakage of information and unlawful computer access are prevented on a enterprise.
 - It is easy to install this security feature in a enterprise network because users and a variety of clients are limited.

Security level and operation costs(3)

- WEP or 11x are not good for a temporary network on conference.
 - When the distributing information is required to operate secure wireless network,
 - a human cost is also required.
 - We have to care to various OS.
 - Participants use various OS.
 - Can we correspond to the trouble at participant's clients?
 - The workload of the help desk is very large.
 - It might be impossible!
 - When the distributing information is required by a wireless network, a human cost is also required.

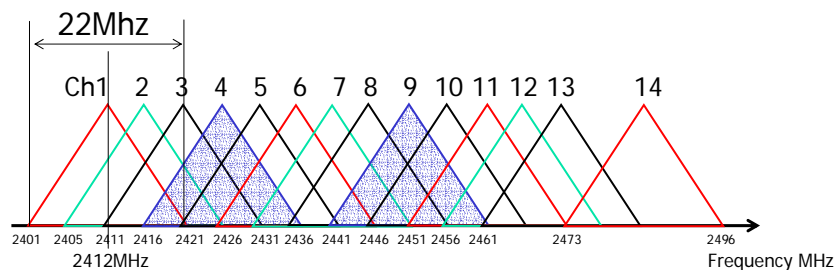
Security level and operation costs(4)

We have to design a wireless network with thinking profits of both user side and manager side.

There is a right design in the right design.

802.11b Channel allocation

- Channel configuration of 802.11b is
 - 2.412GHz(1ch)- 2.484GHz(14ch)
 - The interval of the channel is 5MHz.
 - Bandwidth per channel is about 22MHz.



802.11b Channel allocation(2)

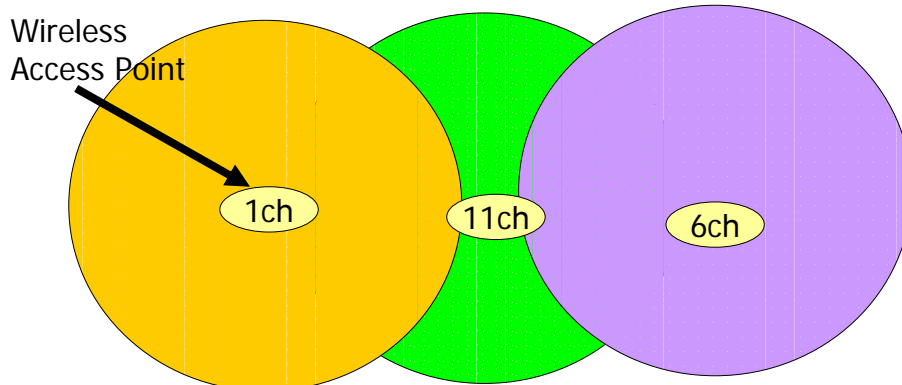
- Combination of channels without interference is limited.
 - The spacing of the channel frequency should be larger than 22MHz.
 - Example for channel combination.
 - Channel 1(2.412GHz) - 6(2.437GHz) - 11(2.462GHz) - 14(2.484GHz)
 - *)channel 14 is only use in Japan.
- Location of access point is decided to avoid overlapping of combination of channels.

Example on next slide.



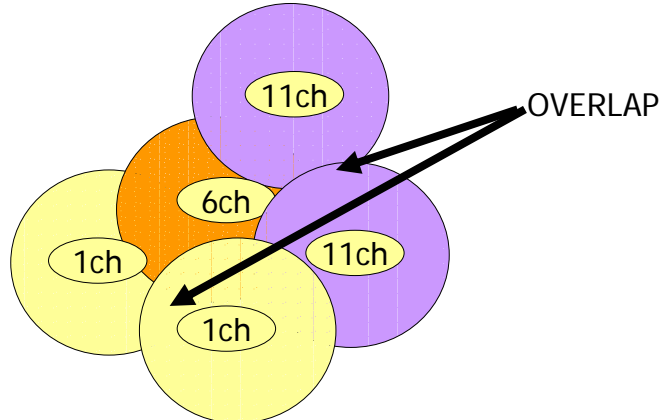
Example-1

- Decide each position of access point to avoid overlapping.



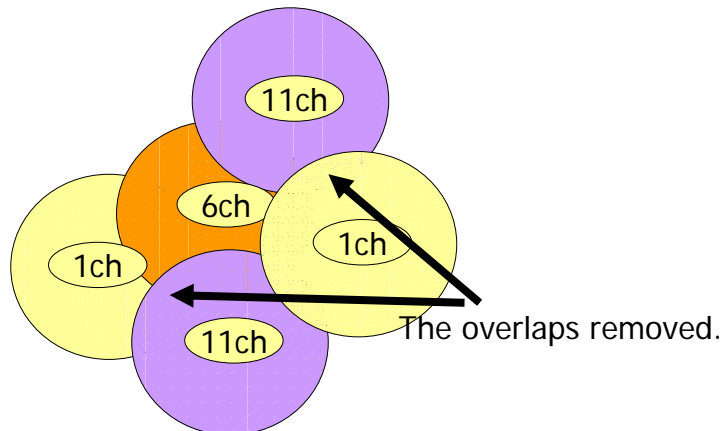
Example-2: Overlap (BEFORE)

- It is Overlapped!



Example-2: Overlap (AFTER)

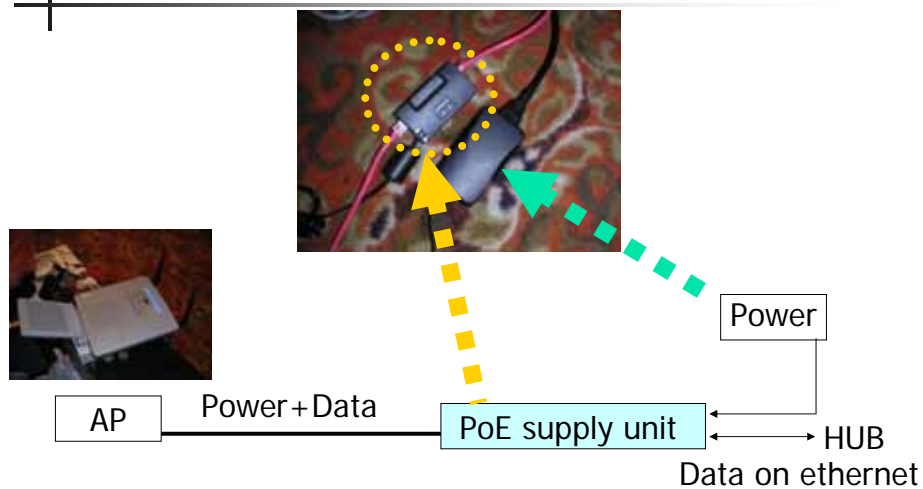
- Swap the position of access points.



Techniques for setting up APs

- Use PoE, Power over Ethernet, to supply power to AP.
 - PoE specifications are existed.
 - IEEE 802.3af
 - Cisco In-Line Power (Cisco original)
 - Use PoE adapter or PoS capable Ethernet switching to supply.
 - Such as Cisco Catalyst series, Foundry, etc..

Cisco inline power Adapter



Benefit for AP with PoE

- The cable wiring for a power supply is unnecessary.
 - PoE decreases the restriction of AP's location at the installation site.
 - Decrease installation cost.

Class of access point(1)

- AP for consumer usages
 - Retail price is about \$100.
 - Management functions are poor.
 - Most AP supports WEB interface only.
 - The performance of access point is low.
 - Maximum capacity of client under AP is about 30 clients.



Class of access point(1)

- AP for enterprise/campus usages
 - Retail price is about \$1000.
 - Cisco aironet 1220 including 11a/b/g interfaces.
 - AP has high performance CPU and tuned software.
 - Maximum capacity of client is up to 120 clients.
 - AP has SNMP/WEB/CLI management i/f.
 - Wireless LAN switch system
 - Able to manage entire of wireless APs on wireless switch.
 - It is convenient in a large-scale wireless network.
 - Wireless switch system manufacture is Aruba/Meru/AeroSwitch etc..

Estimation for number of wireless clients

- AP has the maximum capacity of users.
 - The capacity is depending on the performance of access point.
 - "AP A" is for consumer use can handle 20 users per AP.
 - "AP B" is for enterprise use can handle 120+ users per AP.
- Estimate maximum number of users.
 - 11b can use three channels per room to avoid interference.
 - If you construct wireless network with "AP A",
 - Maximum capacity is 60 users.
 - If you construct wireless network with "AP B",
 - Maximum capacity is 360 users.
 - POINT: A model of AP is selected expecting the number of users.

Example

- A plenary session at IETF meeting, the number of users is up to 500+.
 - If you choose "AP B", You have a lot of troubles@.

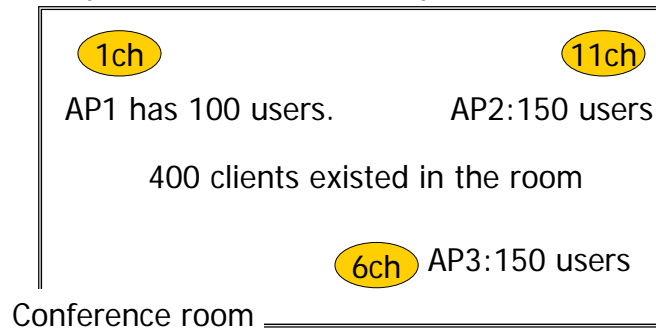
Case study

Threat of AP overload condition

- When the number of clients under AP exceeds the limitation of the base station,
 - The following troubles will occur.
 - New associating clients are rejected by AP.
 - Can't manage the AP.
 - Connection to CLI/WEB is refused.
 - reboot
 - Halt, need to restart in manually.
 - Crash with damaged configuration files.
 - need to re-setup access point.
- (Its are based on my experience.)
No one knows what happens.

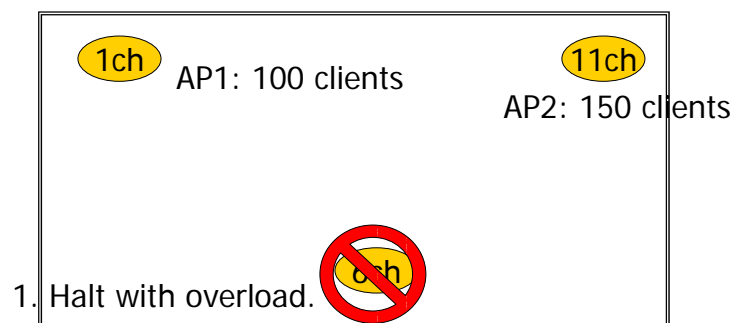
Case study: Chain of failure

- At IETF54 Yokohama conference room.
 - Operate three access point in the room.



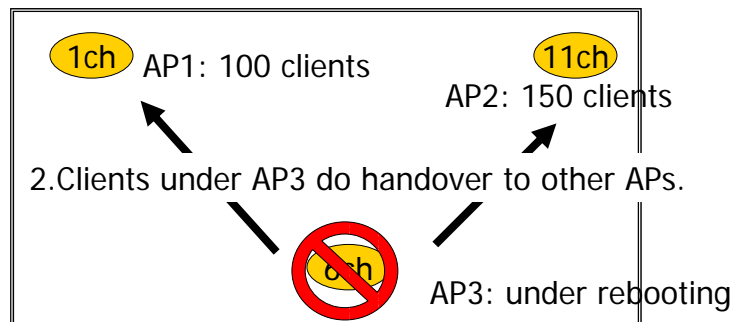
Case study from IETF54

- AP3 was halted due to overload.



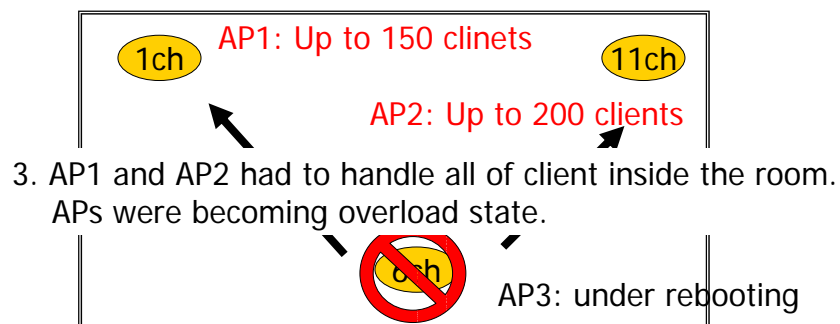
Case study from IETF54

- Clients under AP3 lost signal from AP3, then search and associate with other APs.



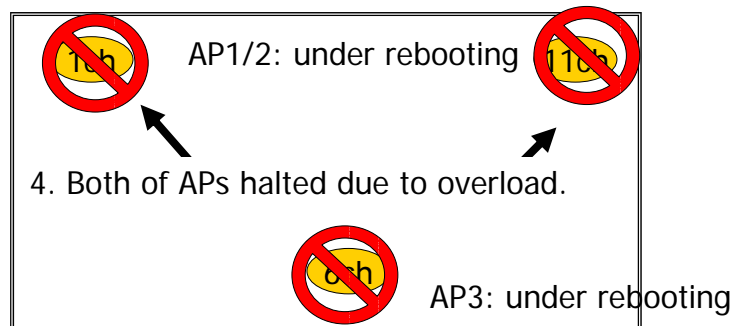
Case study from IETF54

- AP1 and AP2 should handle the clients under AP3.



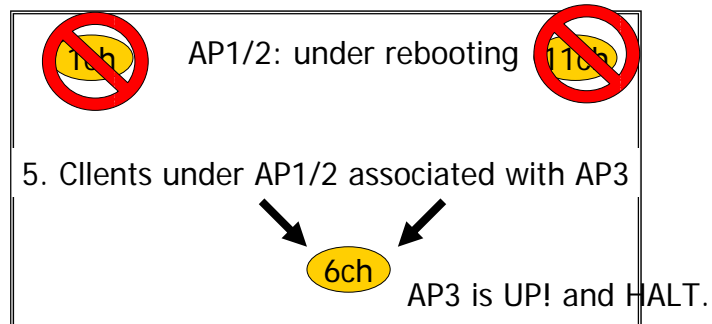
Case study from IETF54

- Also, AP1 and AP2 halted due to overload.



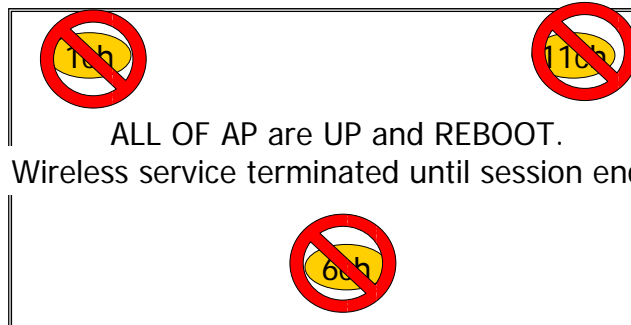
Case study from IETF54

- AP3 was up but halted again due to associate all of client inside the room.



Case study from IETF54

- Wireless service had been terminated until the end of session.



Case study from IETF54

- How to protect from this situation?
 - Set association limit of clients per AP.
 - Some products support for association limit.
 - "Max-association [association limit]" command for cisco Aironet/IOS.
 - We used Orinoco AP1000 and Cisco Aironet at IETF54(2001).
 - Both of them didn't support limitation function.

Case study: Worm infected nodes.

- Blaster worm generate many network traffic.
 - It use ICMP Echo-request and reply to search active nodes.
 - Many nodes infected Blaster worm connected to wireless network.
 - Some user didn't understand infection.
 - Some user infected on wireless network due to forget applying security patches.
- Infected nodes consume wireless resource.
 - Throughput of Wireless is going down.
 - The load of AP is going up.

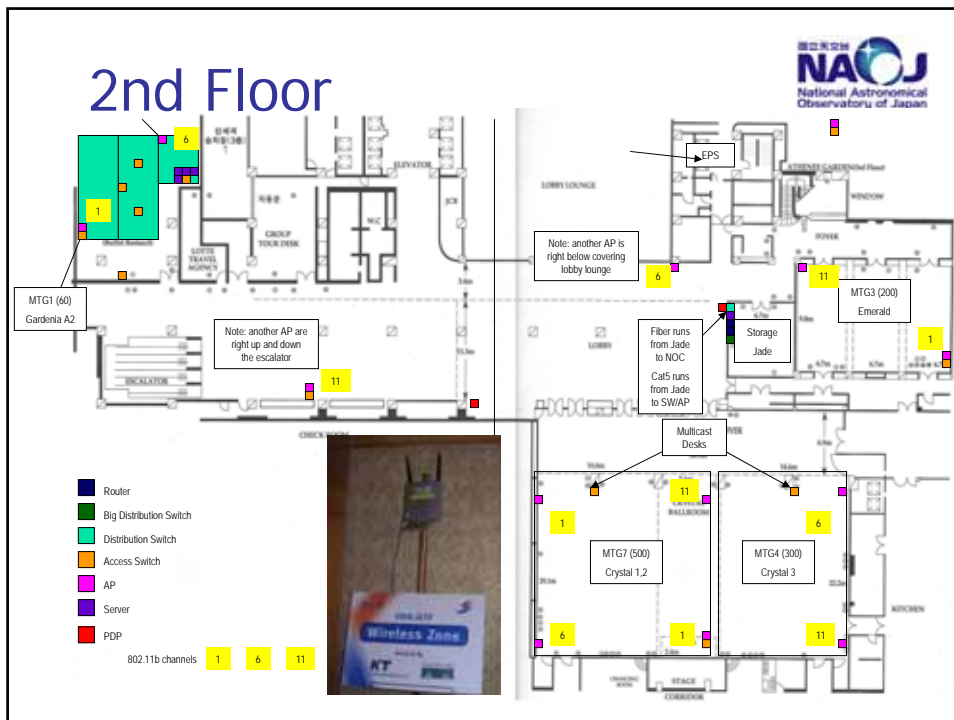
Case study: unofficial DHCP server

- Client with enabled DHCP server function was existed.
 - Ex) At home, a user enable enable Internet Connection Sharing(ICS) service on the notebook to share a connectivity to the Internet.
 - >ICS enable, DHCP Server service start, too.
 - The notebook connect to the wireless network, then, it start to provide un-official DHCP server service.
- Other clients is confused, because two or more DHCP server exists on same network.

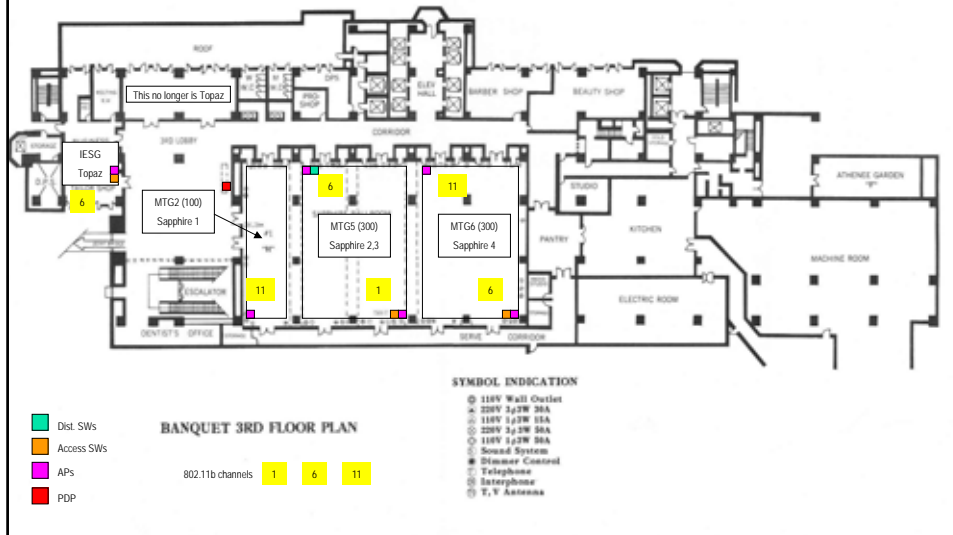
Disassociate illegal clients from network immediately.

Case study: IETF59

- IETF59(Seoul) held 2004.03 at Lotte Hotel Seoul.
- Provided wireless service to three floors.
- Total number of AP was 32.
 - I used Cisco Aironet 1220 with PoE



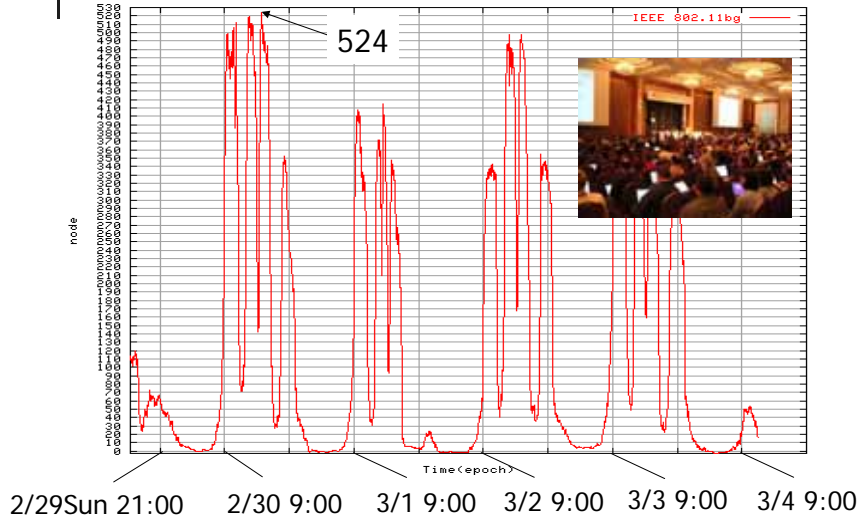
3rd Floor



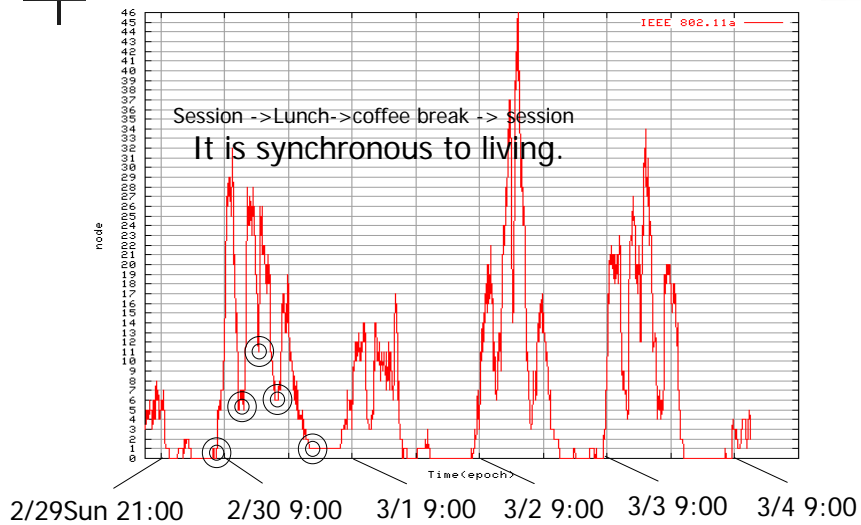
Operate a monitoring system

- I developed and operated the wireless monitoring system.
- This system can monitor all of AP status.
 - Record association number of clients, associating client's MAC address, load average, etc.
- This system has a function to disassociate a client from entire of wireless network.
 - Illegal clients such as worm infected, un-official dhcp server, RA server and etc are forced out.

Result: Number of 802.11b users



Result: Number of 802.11a users



Results

- Total unique client was 1297.
- Peek of 11b clients was 524.
Recorded at 2004/3/1 15:51:21
- Peek of 11a clients was 46

Results

- 10 nodes were shut out from the wireless network.
 - Number of wire-wireless bridging enabled node is 5.
 - Worm infected node : 3
 - RA enabled node : 1
 - DHCP enabled node : 1

It was success in wireless operation.

The End

Any questions?
-> masa@fumi.org