introduction

Key Technology Transitions

1. Device: PC/laptop → mobilephone/tablet
2. Service: Voice → non-voice
3. Bandwidth: Kilo → Mega → Giga
4. Processing power: MHz → GHz
5. Spectrum: Licensed → license-exempt
6. Protocol: Non-IP → all-IP
7. Radio: Single interface → multiple interface

BT: Only PCP can send a beacon(That means every antenna sectors one beacon during beacon time); PCP starts beamforming training in BT by sending training frames; STAs cannot transmit, listening in omni-direction mode **A-BFT**: PCP performs antenna training with its members (STAs). STA transmit training frame At all sectors, **for exhaustive search**, O(B1xB2) training frames are transmitted. For **omni-directional search**, O(B1 + B2). AP listen in omni-direction mode

Beamforming tranining stage: Sector Level Sweep(SLS)粗方向,low data rate->Beam Refinement Protocol(BRP) narrower with high rate. Only SLS end in BT and A-BFT, BRP is optional

AT: PCP polls members and receives non-data responses (STAs can request service periods or SPs to be scheduled during DTT) **DTT**: STA-to-STA exchange happens

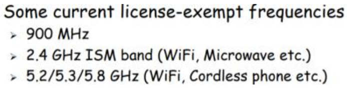
802.11 ad clustering Effective beacon interval for the entire cluster = BI x N (N = # of cluster members)only one S-PCP allocates N SPs(service period) for N beacon transmissions

PHY FUNDAMENTALS

Spatial Frequency Sharing (SFS): Multiple transmissions may be scheduled on the same frequency at the same time if they don't interfere. PCP use learned beamforming pair to determine pair.

Wavelength $\lambda = \mathrm{v}T = \frac{\mathrm{V}}{f}$ (v 一般设为 c = 3 * 10^8m/s)

IEEE 802.11ad Relays (中继器)1. Link Switch Relays (接受然后转发) 2.Link Cooperation Relays(destnation 可能会收到 direct signal and relayed signal)


Some current license-exempt frequencies

- 900 MHz
- 2.4 GHz ISM band (WiFi, Microwave etc.)
- 5.2/5.3/5.8 GHz (WiFi, Cordless phone etc.)

IOT, Bluetooth

Energy = power * time Energy comsumption = tx_power*(data_size/ data_rate) 单位是 Joule IOT network use **16-bit** local addr, **64bits** global addr

WPAN challenges: Battery powered, No infrastructure, dynamic topologies.

Bluetooth(802.15.1-2002) until bluetooth 4.0 first use BLE &blue smart Frequncy Range:2402-2480(79MHz) Frequency hopping:625us/hop

Decibel (dB) Formula(P1 ->P2)

$$dB = 10\log_{10}(P_1/P_2)$$

1. Path loss(trans->receiver)
2. SNR(signal->noise)
3. Signal power(signal-> reference)

Power in dbm && dbw

Piconet (7 active slaves, 255 parked slaves, slave can't talk with each other) **rules**: Master start in even slot only, slave start in odd slot only. Packet only 1, 3, 5 slots long.

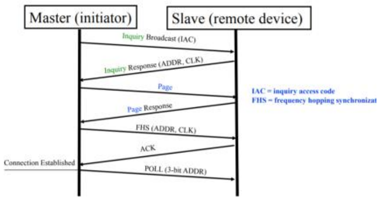
Slave can transmit right after receive a msg from Master. Frequency hopping skip during a packet. Hopping rate = # of hop / duration time

Bluetooth packet format: (packets only 1, 3, 5 slots, dont have other slot, and data rate of bluetooth is 1Mbps) 18b Header is encoded using 1/3 rate FEC resulting in 54b

Access Code	Baseband/Link Control Header	Data Payload
72b	54b	0-2745b

Bluetooth Operational States

Bluetooth Connection Establishment Procedure
Inquiry and Paging Flow Diagram



Standby: Initial state

Inquiry: Master broadcasts an inquiry packet. Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA） So slave can join in piconet.

Page: Master in page state invites a slave device to join the piconet, slave enters page response state and sends page response to the master

Connected:A short 3-bit logical address is assigned for the slave

Energy save state:Hold, Sniff(Low power), park(very low power, wake up) periodically listen to master's beacon.

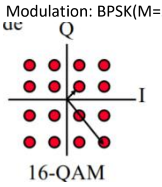
Power in dBm = 10 log (power in milliwatt)

$$\mathrm{dbm} = \mathrm{dbw} + 30$$ (w->mw->uw->nw->pw)

Modulation Rate: = 1/symbol_duration = Baud rate (or symbol rate)

data rate = baud rate x log2(M) (one symbol can carry multiple-bits)

Modulation: BPSK(M=2), QPSK(M= 4), x-QAM(M=x)



16-QAM

A:长度，P:方向(eg, 16QAM -> 3A, 12P)

Nyquist Theorem (noiseless channel) Baud rate < 2 B(log 2 M)

Shannon's Theorem(noisy channel)

Maximum number of bits/sec = B log2 (1+S/N)

Doppler Shift(Freq diff)= v/λ = vf/c

Doppler Spread = 2vf/c = 2 × Doppler shift

Coherence time=1/Doppler spread

(FDD) (Full-Duplex)全双工(TDD)(Half-Duplex)

Bluetooth and WiFi Coexistence(channel 37,38,39 is less interference) 1.Collaborative Strategies: Two networks on the same device (1)Time Division (2)Packet Traffic Arbitration, all packets are on same queue for transmit (3)Notch Filter 2.Non-Collaborative Coexistence Strategies(1)Adaptive Packet Selection(2)Master Delay Policy(3)Adaptive frequency hoping(4) Adaptive Notch Filter

Low Power Wide Area Network 802.11h 900MHz(New wifi standard) && LoRaWAN (New industry-alliance standard)

802.11 ac PHY down clocked by factor **10X** is 802.11h PHY (down 是时间会更长)

802.11 spectrum use in diff country

902-928 MHz (USA)
863-868.6 MHz (Europe)
916.5-927.5 MHz (Japan)
755-787 MHz (China)
917.5-923.5 MHz (Korea)

antenna length = ½ wavelength，If dipole (two rods), each rod is ¼ wavelength

if antennas are spaced >λ/2 apart, multipath signals for different antennas can be uncorrelated

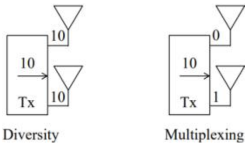
Free Space Path Loss or Propagation (Frii's Law) $P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi d}\right)^2$

d-4 Power Law (2-ray) $P_R = P_T G_T G_R \left(\frac{h_t h_r}{d^2}\right)^2$ (It's valid for distance > $d = \frac{4h_t h_r}{\lambda}$)

802.11 MAC protocol version 0 is designed for a/b/ac/g/n, 36 bytes head

802.11 MAC protocol version 1 is designed for h, head shorter, 10-24 bytes

Note that the received power becomes independent of the frequency



Overall multiplexing gain is limited by degrees of freedom = min(NT, NR)

Beamforming(used when LOS), transmit same signal used multiple antenna

Multiple Access Methods

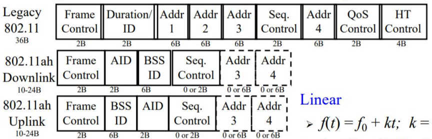
1G->FDMA 2G->TDMA 3G->CDMA 4G->OFDMA(FDMA+TDMA)

Advantage of OFDM: OFDM splits a band in to many orthogonal subcarriers.

1. easy to implement using FFT/IFFT
2. Robustness against frequency selective burst errors
3. Allows pilot subcarriers for channel estimation

Short MAC Header

- MAC Header shortened by 12-26 Bytes:
  - Removed: High throughput control, QoS, Duration field (No virtual carrier sensing)
  - Optional: 3rd address
  - 2-byte AID in place of some 6-byte addresses
  - Frame Control indicates what protocol version is being used
  - Sequence field indicates if 3rd /4th addresses are present



LoRaWAN (bi-direction communication,star of star topologies, low rate)

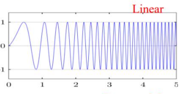
it use chirp spread spectrum(signal is frequency modulated with frequncy increase or decrease

Symbol duration T = B/k
Data rate = 1/T

Chirp Rate

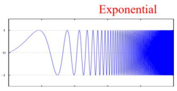
Linear

- $f(t) = f_0 + kt$; k = rate of frequency change (chirp rate)
- $k = (f_1 - f_0)/T$; f_1 = final frequency, T = chirp interval
- Chirp bandwidth = $(f_1 - f_0)$



Exponential

- $f(t) = f_0\, k^{t}$; k = rate of exponential change
- $k = (f_1/f_0)^{1/T}$



Effect of frequency:

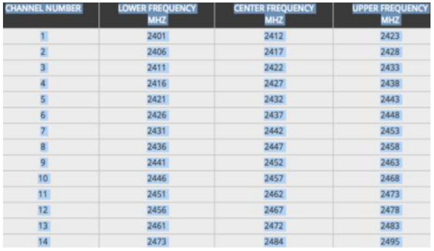
1. Higher Frequencies have higher attenuation, so shorter reach(传播距离短)
2. Higher frequencies need smaller antenna
3. Higher frequencies have more bandwidth and higher data rate
4. Higher frequencies allow more frequency reuse

WLAN LAN (802.11 -1997 first version)

802.11b/g/n 2.4Ghz 802.11a/n/ac 5GHz 802.11ad/ay 60GHz 802.11ah (IoT) 900MHz

Each Wifi channel is always 20Mhz or 22Mhz

2.4GHz channel overlap, as shown below, each channel 22MHz wide (1-6-11)5GHz channel:20Mhz, non-overlap,some used by radar



CHANNEL NUMBER	LOWER FREQUENCY MHZ	CENTER FREQUENCY MHZ	UPPER FREQUENCY MHZ
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

Hidden node problem: solved by 4-ways handshake(CSMA-CA) to

Avoid collision RTS->CTS->DATA->ACK Listen before you talk.

If the medium is busy, the transmitter backs off for a random period.

RTS contain Dest addr && duration of msg, tell other back off

CTS tell other AP wait for that duration

Contention Window (CW) Backoff count (BO)

Network Allocation Vector (NAV) is the waiting time to sense

Inital BO = random(0,CW), BO is backoff time, if unchoiced to transmit, BO -1 在下次争用

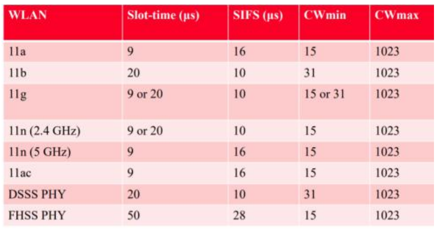
Initial/sucessful transfer, CW = CWmin, after every unsuccessful,CW = min{2CW + 1, CWmax}

Virtual carrier sense (duratio is RTS + SIFS + CTS + SIFS + Frame + SIFS + Ack)

ACK 结束后要等待一个 **DIFS**， 才开始下次争用， 争用时每个都要等待各自的 **BO** 长的时间 最快的能争用到信道使用权， 才开始 **RTS**。若传输过程中失败，**cw** 改变， 然后重新取 **BO** **Backoff** 然后重新传输

chirp modulation: binary 1-(k = k1) 0-(k = -k1)

OOK 1-(Postive k) 0-(no signal)

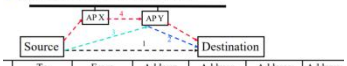


WLAN	Slot-time (μs)	SIFS (μs)	CWmin	CWmax
11a	9	16	15	1023
11b	20	10	31	1023
11g	9 or 20	10	15 or 31	1023
11n (2.4 GHz)	9 or 20	10	15	1023
11n (5 GHz)	9	16	15	1023
11ac	9	16	15	1023
DSSS PHY	20	10	31	1023
FHSS PHY	50	28	15	1023

- PIFS = SIFS + 1 slot time
- DIFS = SIFS + 2 slot times

802.11 Frame Address Fields

- BSS X and BSS Y are connected via a distribution system
- Four possibilities (all stations filter on "Address 1")



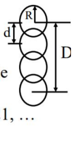
	To Distribution System	From Distribution System	Address 1	Address 2	Address 3	Address 4
1	0	0	Destination Address	Source Address	BSS ID (Y)	-
2	0	1	Destination Address	BSS ID (Y)	Source Address	-
3	1	0	BSS ID (Y)	Source Address	Destination Address	-
4	1	1	BSS ID (Y)	BSS ID (X)	Destination Address	Source Address

Cellular Network

Macro: section of a city, more than 1km

Micro:less than 1km Pico:Busy area 200m Femote:Inside home 10m

- D = minimum distance between centers of cells that use the same band of frequencies (called co-channels)
- R = radius of a cell
- d = distance between centers of adjacent cells (d = R√3)
  - d < 2R due to *overlapping* cells
- N = number of cells in repetitious pattern (Cluster)
  - Reuse factor
  - Each cell in pattern uses unique band of frequencies
- Hexagonal cell pattern, following values of N possible
  - $N = I^2 + J^2 + (I \times J)$, $I, J = 0, 1, 2, 3, \ldots$
- Possible values of N are 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, …
- Reuse Ratio = Distance/Radius = D/R= $\sqrt{3N}$
- D/d = $\sqrt{N}$



Frequency reuse notation

N*S*K

N: # of cell in cluster

S: # of Sectors in a cell.

K: # of Frequencies per cell

LTE(Near 4G, but not 4G)

Normal cyclic prefix:7 symbols/slot

Extended Cyclic prefix:6 symbols/slot

802.11a/b-1999 802.11d-2001 802.11g-2003 802.11e-2005 802.11n-2009 802.11p-2010 802.11ad-2012 802.11ac-2013

802.11 a(OFDM) 20 MHz channel divided into **64** subcarriers. **6** subcarriers at **each side** are used as guards and **4** as pilot,else **48** for data.

Coding rate:1/2,2/3,3/4 data rate:6(BPSK)-54Mbps(64-QAM) symbol length: 3200ns data+800ns guard interval=>1/4000=**0.25Msymbol/s**

Data rate = Data bits/symbol * 0.25M Data bits/symbol = coded rate/symbol * coding rate coded rate/symbol=code rate/subcarrier *48

802.11 g(OFDM) 54Mbps 802.11e-2005 (Enhanced QoS)

802.11n(first to use MIMO contain beamforming/powersave, channel bonding: 40MHz per channel, 108+6 subcarriers, frame aggregation)

Coding rate:5/6 1/3.6symbol/s SIFS=2 µs, instead of 10 µs 20MHz, use 52 replace 48 subcarrier, no pilot

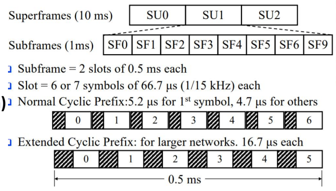
Guard Interval = 4 × **Multi-path delay spread**

802.11 ac(use multi-user MIMO 7Gbps Supports 80 MHz and 80+80 (channel bonding) MHz channels 468+16)

MU-MIMO: Two single-antenna users can act as one multiantenna device

Drawback of channel-bonding: less orthogonal channels are available in the network.difficult for multiple WLANs to operate next to each other without interfering

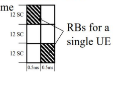
LTE Frame Structure

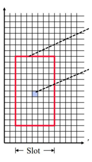


- Subframe = 2 slots of 0.5 ms each
- Slot = 6 or 7 symbols of 66.7 µs (1/15 kHz) each
- Normal Cyclic Prefix:5.2 µs for 1st symbol, 4.7 µs for others
- Extended Cyclic Prefix: for larger networks. 16.7 µs each

Resource Allocation

Time slot: 0.5 ms
6 or 7 OFDM symbols
Subcarriers: 15 kHz
Physical Resource Block (RB): 12 subcarriers (180 kHz) over 1 time slot
Minimum Allocation: 2 RBs per subframe





RB= # of slots * # of subcarriers

each RB has 12 subcarriers, 12 * 15 = 180KHz

WLAN 802.11ad

Advantage: Large spectrum: 7 GHz,Easy Beamforming,Low Interference because reach shorter,Difficult to intecept

Disadvantage:easily blocked, large attenuation,Directional Deafness: Can't hear unless aligned

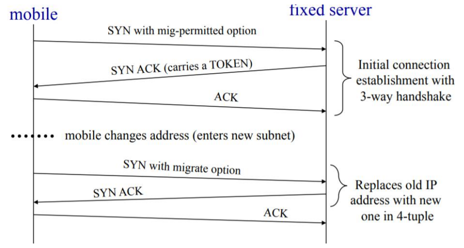
802.11 ad MAC(Beacon Interval) 4 access period:Beacon Time (BT), Associating Beamforming Training (A-BFT), Announcement Time (AT), and Data Transfer Time (DTT)

Mobility Management (Transport Layer)

Traditionally, IP addresses of communicating parties are statically bound to a transport connection,Dynamic binding required to support handoff (method: TCP connection migration)

Migration-permitted option: 3 bytes   Migration option: 19 bytes

- Mobile uses migration-permitted option with SYN during connection establishment and negotiates a TOKEN
- From now on, the connection can be identified by the TOKEN
- When mobile moves to different subnet, it uses migration option and sends a SYN to its peer
- Upon receiving a SYN with migration option, peer replaces old destination IP address with new one in the 4-tuple
  - new IP address is carried in the IP packet header


mobile
fixed server
SYN with mig-permitted option
SYN ACK (carries a TOKEN)
ACK
Initial connection establishment with 3-way handshake
mobile changes address (enters new subnet)
SYN with migrate option
SYN ACK
ACK
Replaces old IP address with new one in 4-tuple

LTE transmission bandwidth

Channel bandwidth [MHz]	1.4	3	5	10	15	20
Transmission bandwidth [MHz]	1.08	2.7	4.5	9	13.5	18
Transmission bandwidth [RB]	6	15	25	50	75	100

1G: Analog Voice. FDMA. 1980s

2G: Digital Voice. TDMA. 1990

2.5G: Voice + Data. 1995.

3G: Voice + High-speed data. All CDMA. 2000   3.5G: Voice + Higher-speed data   3.9G: High-Speed Data. VOIP. OFDMA

4G: Very High-Speed Data. 2013.   5G: Ultra High-Speed Data. 2020.

A particular cellular system has the following characteristics: cluster size =9, uniform cell size, user density=100 users/sq km, allocated frequency spectrum = 900-945 MHz, bit rate required per user = 10 kbps uplink and 10 kbps downlink, and modulation code rate = 2 bps/Hz. Answer the following questions.

(a) Using FDMA/FDD:

1. How much bandwidth is available per cell using FDD?
2. How many users per cell can be supported using FDMA?
3. What is the cell area
4. What is the cell radius assuming circular cells?

(b) If the available spectrum is divided in to 100 channels and TDMA is employed within each channel:

1. What is the bandwidth and data rate per channel?
2. How many time slots are needed in a TDMA frame to support the required number of users?
3. If the TDMA frame is 10ms, how long is each user slot in the frame?
4. How many bits are transmitted in each time slot?

(a) Using FDMA/FDD:

1. How much bandwidth is available per cell using FDD?
   45MHz/9 = 5 MHz/cell
   FDD ⇒ 2.5 MHz/uplink or downlink
2. How many users per cell can be supported using FDMA?
   10 kbps/user = 5 kHz ⇒ 2500/5=500 users per cell
3. What is the cell area?
   100 users/sq km ⇒ 5 Sq km/cell
4. What is the cell radius assuming circular cells?
   $\pi r^2 = 5 \Rightarrow r = \sqrt{5/\pi}$ km = 712 m

(b)

1. What is the bandwidth and data rate per channel?
   2.5 MHz/100 = 25 kHz/Channel = 50 kbps
2. How many time slots are needed in a TDMA frame to support the required number of users?
   10 kbps/user ⇒ 5 users/channel
3. If the TDMA frame is 10ms, how long is each user slot in the frame?
   10 ms/5 = 2ms
4. How many bits are transmitted in each time slot?
   2 ms x 50 kbps = 100 b/slot

(b)中的 channel 划分是对单个 cell 中的 download link/up link 划分

SCTP is third protocol in transport layer, A connection in SCTP is called association

Multistreaming:Single association maintains multiple streams

Multihoming:

- A host may be connected to multiple subnets for reliability reason
- Multiple subnet = multiple IP addresses
- SCTP allows a host to bind multiple IP addresses to a single association
- Must nominate one as primary address
- Primary address is used for all communication
- Other addresses used only if primary address fails

Soft handover(make-before-break)新的连接建立才断开旧的

hard handover(break-before-make) 两个 base 中间没有重叠才没法先 make

SCTP-DAR(solution) allow soft handover

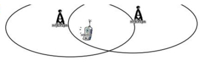
SCTP uses a verification tag (VT) to identify an established association,

VT is similar to the token concept in TCP migration

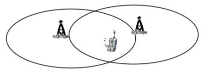
Two new chunk types are proposed

1. 0xC1 ASCONF address conf change chunk
2. 0x80 ASCONF-ACK

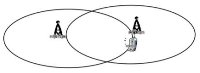
1. Mobile enters overlapping zone, obtains new IP address, and adds new IP address to SCTP association as the secondary address using ASCONF chunk (0xC001)



2. Mobile hands off to new subnet → switch primary address to new address using ASCONF chunk (0xC004)



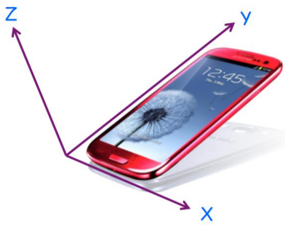
3. Mobile leaves overlapping zone and deletes old IP address using ASCONF chunk (0xC002)



Sensor-aided Wireless Networking

Accelerometers (加速器) can use in screen orientation detect(portrait(竖屏)or landscape 横屏) F = Ma

加速器显示的数值的方向是重力计的除去重力方向剩下的力的方向(mems_sample 测得值)



Low-pass filter (large value for α, say 0.8) to extract gravity from mems reading

Initialize g.x=g.y=g.z=0

$$g.x = \alpha \times g.x + (1-\alpha) \times mems\_sample.x$$
$$g.y = \alpha \times g.y + (1-\alpha) \times mems\_sample.y$$
$$g.z = \alpha \times g.z + (1-\alpha) \times mems\_sample.z$$

$$a.x = mems\_sample.x - g.x$$
$$a.y = mems\_sample.y - g.y$$
$$a.z = mems\_sample.z - g.z$$

$$\vec{F}_{Coriolis} = -2m\vec{\Omega} \times \vec{v} \qquad \Omega = -\frac{F}{2mv}$$

Gyroscope(Gyro)陀螺仪 Gyro drift(陀螺飘移) due to its sensitivity to environmental factors need be adjust constantly to overcome drift   180 度 = pi rad

Magnetometer(磁力计)

- Measure force on a current carrying straight wire
- Tesla T = Newton per ampere meter
- Earth's magnetic force is in the order of micro tesla

$$B = \frac{F}{IL}$$

If we keep the device horizontal to earth's surface (no tilt), the heading can be calculated just from the x and y components of the sensor output (tilt 倾斜)

Magnetic north

If (Mx > 0) ψ = 270 + arctan(My/Mx)

If (Mx < 0) ψ = 90 + arctan(My/Mx)

If (Mx = 0, My > 0) ψ = 0

If (Mx = 0, My < 0) ψ = 180

true north heading (we should loop up D in IGRF database)

if D = x E, then true north heading = magnetic north heading + D, else D = x W, true north heading = magnetic north heading - D

Q8. You are measuring the magnetic field in Sydney, Australia, using your smartphone magnetometer. Which of the following readings indicate that there is likely to be some magnetic perturbation (give your reason)?

(a) Mx=10, My=20, Mz=52.4
(b) Mx=25,My=40, Mz=52

A8. IGRF provides total magnetic field $F = \text{sqrt}(m.x^2+m.y^2+m.z^2)$. F for (a) is 56.98, which is very close to the value (57) reported in IGRF for Sydney. F for (b) is close to 70, which is far from the IGRF value. Therefore, the values in (b) are likely to be due to the presence of magnetic perturbation.

Pros and cons of transport layer mobility

- Pros
  - no triangular routing (low latency)
  - no changes in network infrastructure (e.g. no HA)
  - soft handover possible (with SCTP)
- Cons
  - changes required in transport layer software
  - location privacy not protected

Mobility Management (Network Layer)

Quasi-mobility can't move across subnet boundary within session, Full Mobility can

Mobile IP enabling full mobility in IP networks

Coa (临时地址)，与之相反的是 permanent address(永久地址)

1. Co-located CoA

- mobile needs unique IP address (consumes IP address)
- unique address is obtained using DHCP etc.

2. Foreign agent CoA

- typically FA is a router known by several IP addresses
- mobile uses one of FA IP addresses as CoA
- several mobiles can use the same CoA
- no new IP address is consumed (*DHCP not used!*)
- Mobile connects using its permanent address

Mobility IPv6 (support Bidirectional tunneling mode and Route optimisation mode)

Q1. List some of the features of the IPv6 that makes it relatively (in comparison to IPv4) easier to support the concept of Mobile IP.

A1.

128-bit addresses. Co-located CoA becomes easier to implement. Shortage of IP addresses is not an issue anymore. Auto-configuration of IPv6 addresses (suffixing the MAC to the network prefix) obviates the need for DHCP servers.

Header options. Header options in IPv6 allow carrying both CoA and home address in the IP header satisfying any ingress filters in the foreign network. Route optimization becomes easier.

Q2. What are the benefits of having a foreign agent (FA)?

A2.

Having a FA is particularly useful for IPv4 because many visitors can share the same CoA. The address sharing makes it easier to support Mobile IP even when the foreign network has limited IP addresses available.

With FA, the mobile host does not have to process IP-in-IP encapsulation/decapsulation (tunnel ends at the FA).

Nemo (NEMO is based on MIP)

Onboard router (OR) uses MIP to manage the mobility of the moving subnet

Phase of Mobile IP

1. Agent discovery 2. Registration 3. Data Transfer   (foreign agent coa)

Detail:

If co-located coa, then replace agent discovery by DHCP for colocated CoA

A registration request or reply is sent by UDP, port 434

Data exchange: (CH is 远程主机(remote host), MH is mobile host)

- Step1: CN sends a packet to MN using home address
  - mobility remains transparent to CN
- Step2: HA intercepts it, encapsulates it in another packet with destination address as CoA and retransmits it (tunneling to FA)
- Step3: FA decapsulates, looks up MAC address of MN in registry, and sends the packet in LAN frame to MN
- Step4: MN sends packets directly to CN with source address as home address
  - mobility remains transparent to CH

CH-MH Data Exchange

CoA is co-located

- Step1: CH sends packet to MH using home address
  - mobility remains transparent to CH
- Step2: HA intercepts it, encapsulates it in another packet with destination address as CoA and retransmits it (tunneling to MH), MH decapsulates and delivers to upper layers
- Step3: MH sends packets directly to CH with source address as home address
  - mobility remains transparent to CH

Headers of a Tunneled Packet

Using IP-in-IP Encapsulation

Inner Header: From CN to MN
Outer Header: From HA → FA/CoA

Outer IP Header	Inner IP Header	Transport Layer Header	User Data (if any)
Src Addr = HA Dest Addr =CoA Proto = IP	Src Addr = CN Dest Addr = MN Proto = TCP/UDP		

Reverse tunneling was introduced to enable MIP to work with ingress filtering mechanism.

Disadvantage for MIP?

Jser device requires software upgrade
- Cost
- Admin overhead (MIP requires kernel support)
- Population of mobile device may be dynamic (for a large organisation, it may be difficult to keep track which devices need MIP)
- Security hole: MIP is in the kernel, opening new threats for security for the organisation