Advanced Lecture on Internet Applications

10. RTP, Time & Clock Synchronization, Authentication, Accounting, RADIUS

Masataka Ohta

mohta@necom830.hpcl.titech.ac.jp

ftp://ftp.hpcl.titech.ac.jp/appli10e.ppt

Networks

- Physical Distribution Networks
  - postal service, parcel services, convenience stores
- Information Communication Networks
  - Publishing Network (Book, News Paper, CD, Movie)
  - Financial Network
  - Phone Network
  - Broadcast Network
  - the Internet

Internet Disintermediate ICN

- Price Destruction of ICN
  - Publishing, financial, phone and broadcast networks will disappear
  - IC cost of the society decreased
    - ISP business itself is not profitable
- Publishing, financial, phone and broadcast services will:
  - remain, but, on the Internet
  - social activities increase

Publishing Network

- Mass Distribution of Same Information
- Delay of the Distribution may be Tolerated
- Protected by Copyright Act
- The First Victim of the Internet
  - Collapsing

Financial Network

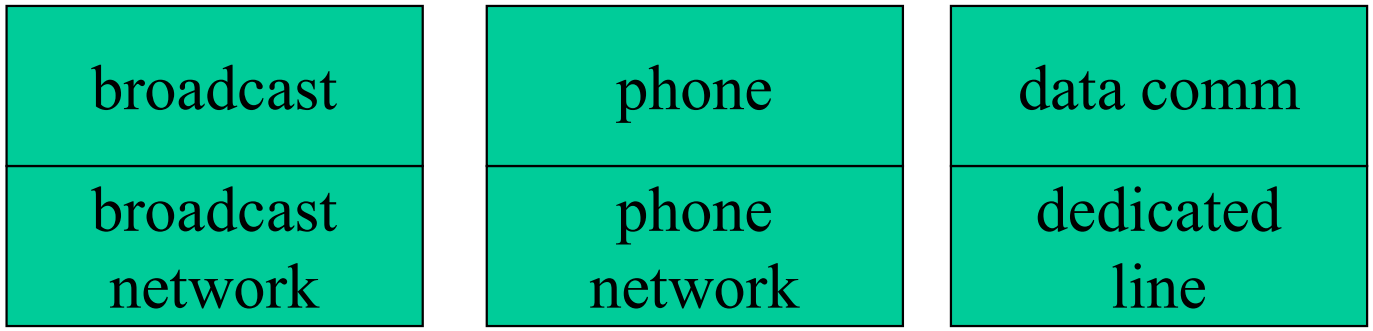
- Manage Transfer of Money
- Partly, Phisical Distribution Network, but, today, mostly ICN
- Security!!!
  - Not that there is no accident
  - Who will pay the loss on accidents

Phone Network

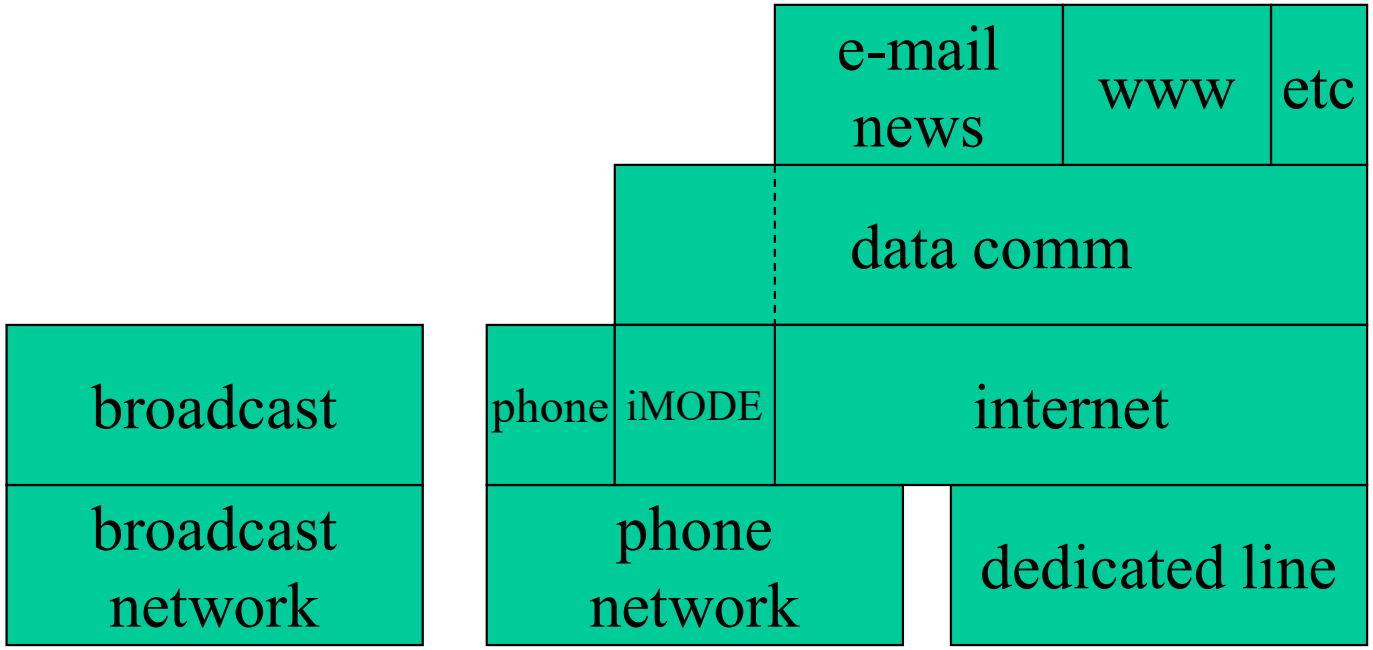
- Network for Realtime Voice Transfer
  - Allocate bandwidth for voice transfer
  - Minimize (guarantee) delay for voice transfer
- Dedicated line service may be Offerred
  - but, primary service is voice transfer
- Slow and Expensive
- Was Protected as National Company
  - Leberated by Telecommunication Business Act

Broadcast Network

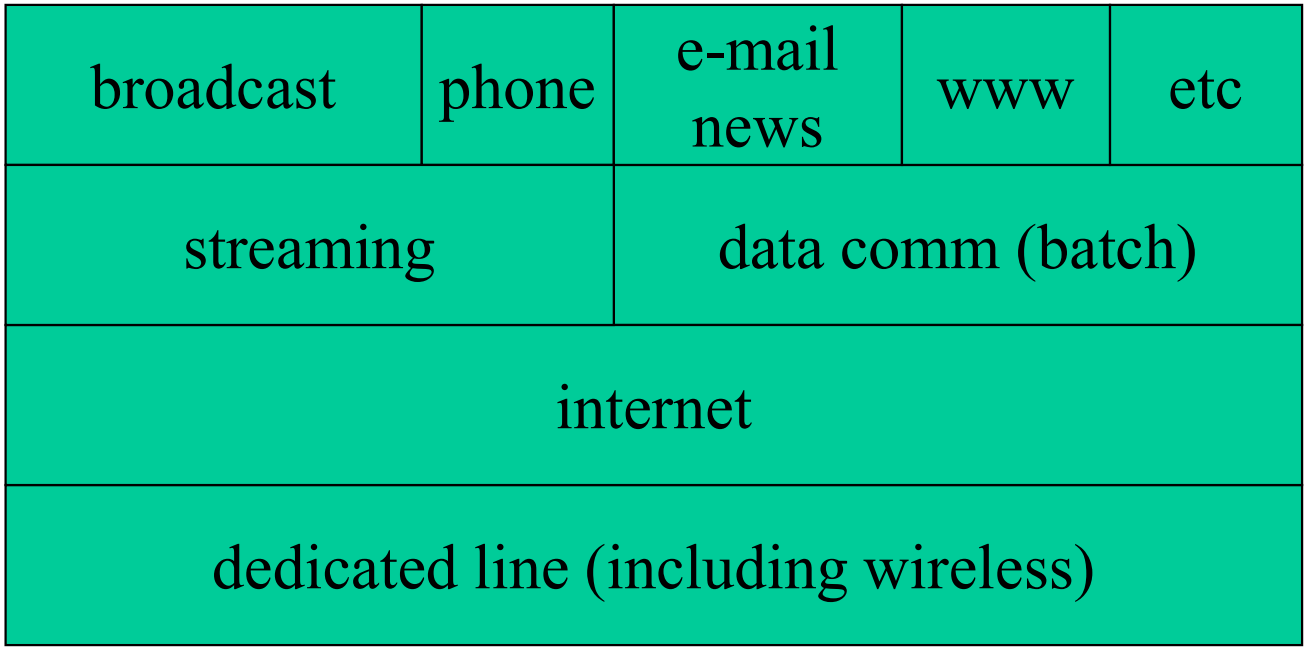
- Network to Transfer Voice/Image to Many in Realtime
  - Allocate bandwidth for the transfer
  - Minimize delay
- Wide Area One to Many Communication over Radio Waves
  - Broadcast/Multicast
- Protected by Broadcast Act



networks before the Internet



networks with the Internet



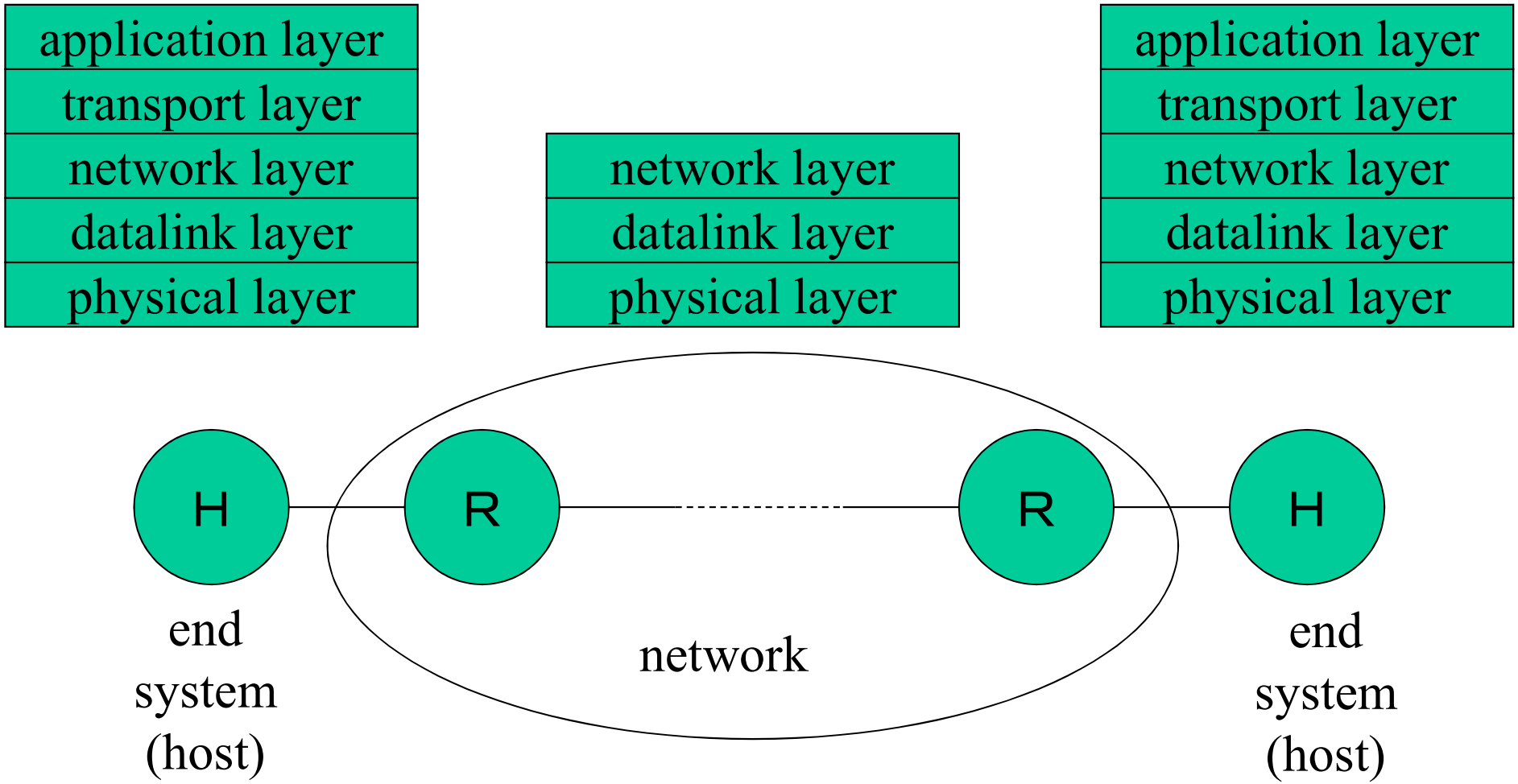
network in the future

How Can Stream Media Transported by the Internet?

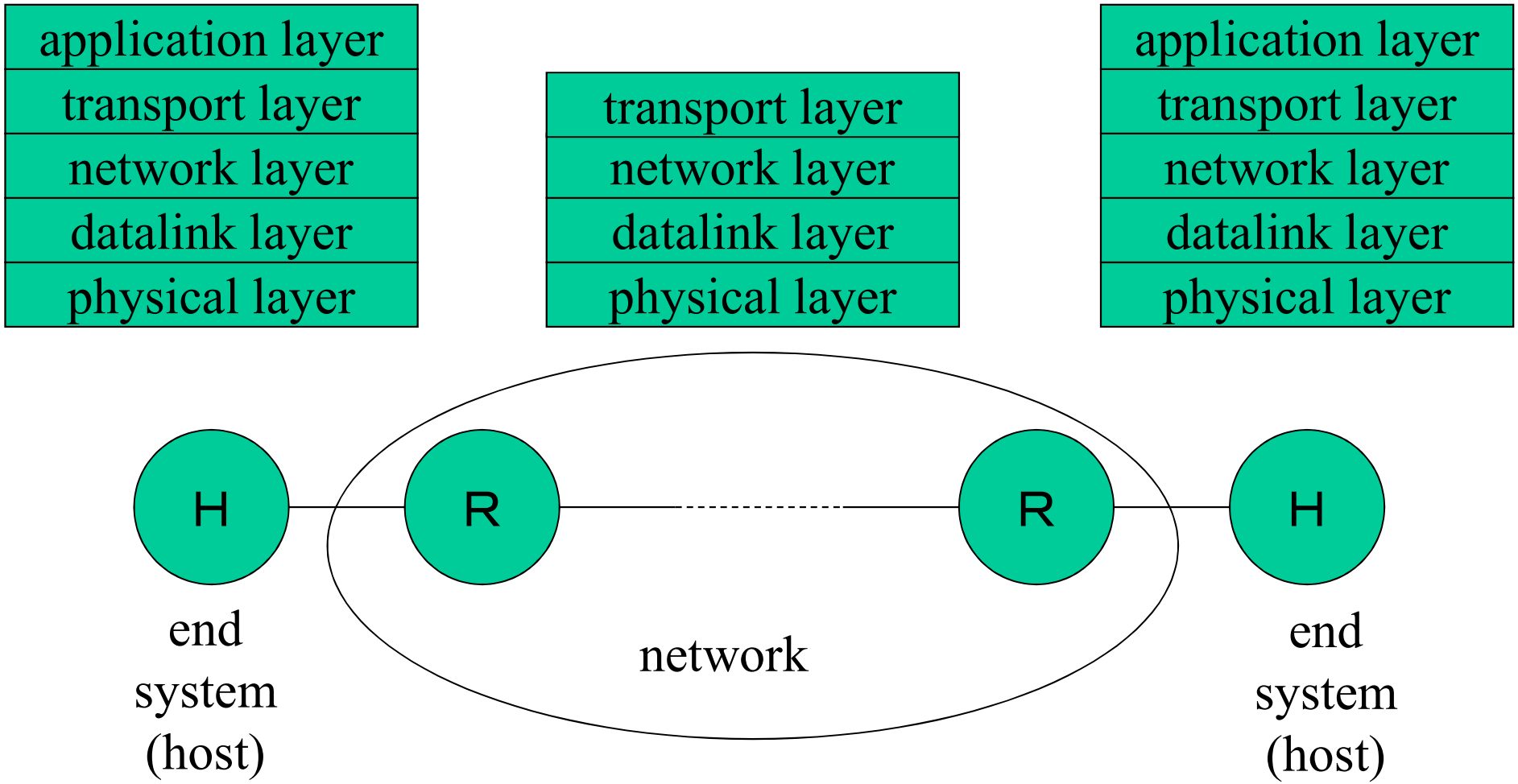
- new IP? (IPv5)
  - not necessary
- QoS guarantee makes streaming comfortable
  - requiring infrastructure modifications
- clock synchronization between ends
  - to prevent buffer overflow/underflow
  - without common clock, can not combine multiple streams

Examples of QoS

- phone
  - BW: 64kbps, delay < 0.1s
- CD play
  - BW: 1.5Mbps, delay < 1s
- TV broadcast
  - BW: 6Mbps, delay < 1s



best effort internet



internet with QoS guarantee

Delay and Jitter

- jitter=(maximum delay)-(minimum delay)
- buffering for jitter*2 necessary at receiver for smooth play
  - no buffer underflow if maximum delay occurs just after minimum delay
  - no buffer overflow if minimum delay occurs just after maximum delay
- clock of sender and receiver must be synchronized

Buffering and Clock Difference

- if sender clock is slower than receiver clock
  - in the long run, receiver buffer will underflow
- if sender clock is faster than receiver clock
  - in the long run, receiver buffer will overflow

How to Synchronize Clock

- provide same clock to all the equipment
  - common with phone/broadcast network
  - impossible with Ethernet
  - IEEE 1394?
  - GPS?

Adjust Playing Speed

- clock speed may be different
  - playing speed should be adjusted
    - more than clock speed difference
- with buffering for jitter*2
  - if buffer is less than half full, slow down playing
  - if buffer is more than half full, speed up playing
- if high precision (crystal) clock is used
  - speed change not noticeable even with sound

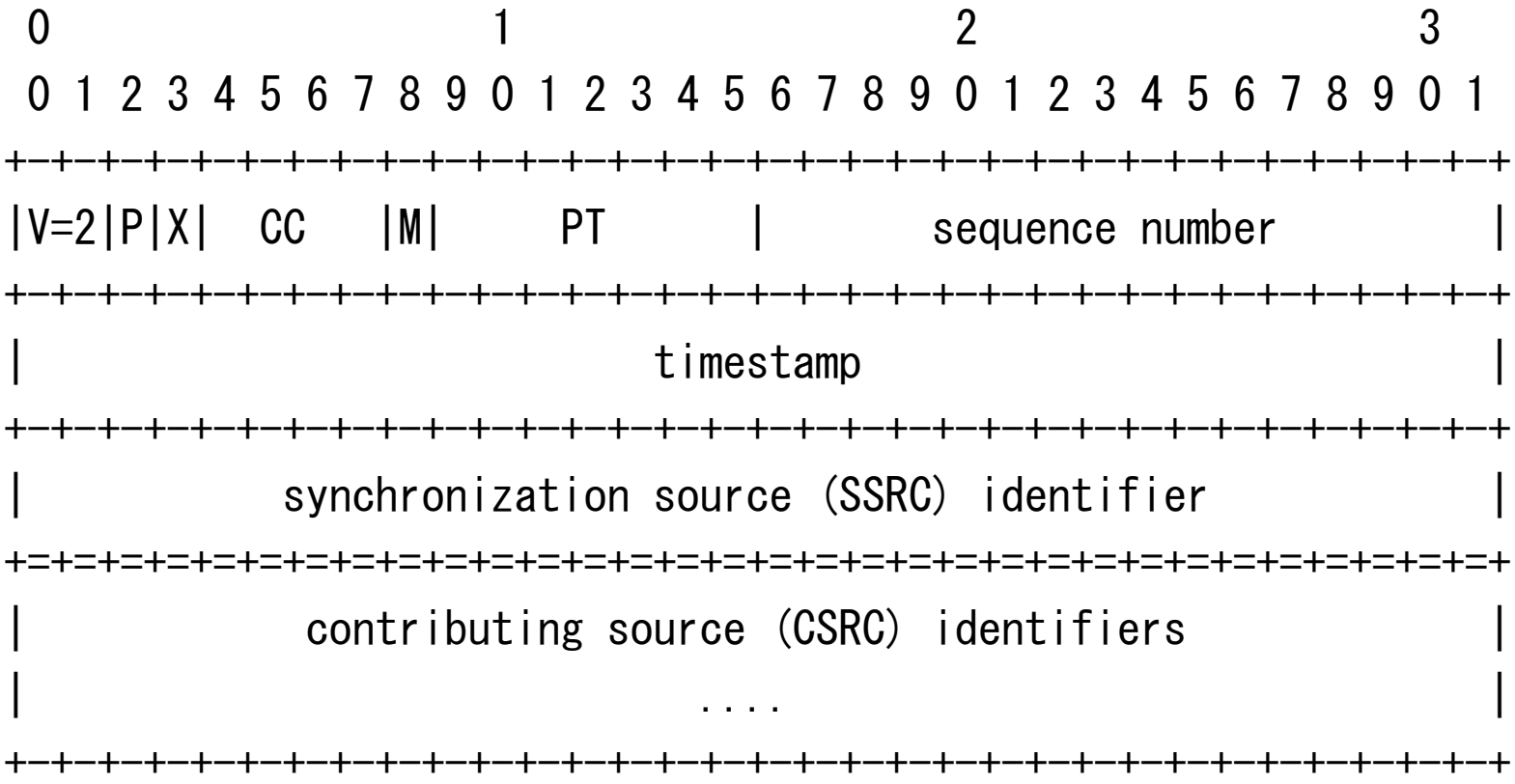
Jitter Causes Delay

- total delay = (propagation delay) + (buffering delay)
- buffering delay at receiver = 2*jitter

RTP (Real-Time Transport Protocol, rfc1889)

- transport/application protocol to synchronize terminals
  - can not reduce delay/jitter within network
  - identify media by PT (payload type)
    - support various media (rfc1890 etc.)
  - restore order by sequence number
  - clock synchronization by time stamp

RTP Header (1)


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|V=2|P|X| CC |M| PT | sequence number |
| timestamp |
| synchronization source (SSRC) identifier |
| contributing source (CSRC) identifiers |
| .... |

RTP Header (2)

- v
  - version (2)
- p
  - padding
- x
  - extension header exists
- CC (CSRC Count)
  - the number of CSRC

RTP Header (3)

- M
  - marker
- PT
  - payload type
  - specify encoding format, speed, etc.
- sequence number
  - sequentially assigned to each packet
  - initial value is random

RTP Header (4)

- time stamp
  - unit different payload by payload
  - initial value is random
- SSRC (Synchronization Source)
  - ID (not IP address) of synchronization source
  - time stamp with same SSRC can be compared
- CSRC (Contributing Source)
  - ID of contents source (speaker)

RTP and E2E Principle

- RTP assumes various application GWs
  - translator
    - convert media
  - mixer
    - mix multiple media (voice?), necessary for conference
  - no room for E2E principle
- clock synchronization is E2E
  - no global clock of the internet

Time Synchronization

- absolute time is not meaningful (not a QM observable but a parameter(?))
  - special relativistic theory means
    - space-time region outside of light cone may considered to be at the same time
      - in networking, space-time region outside of information cone may considered to be at the same time
- NTP (Network Time Protocol, rfc5905)
- RTP may also be used
- GPS is a lot more popular

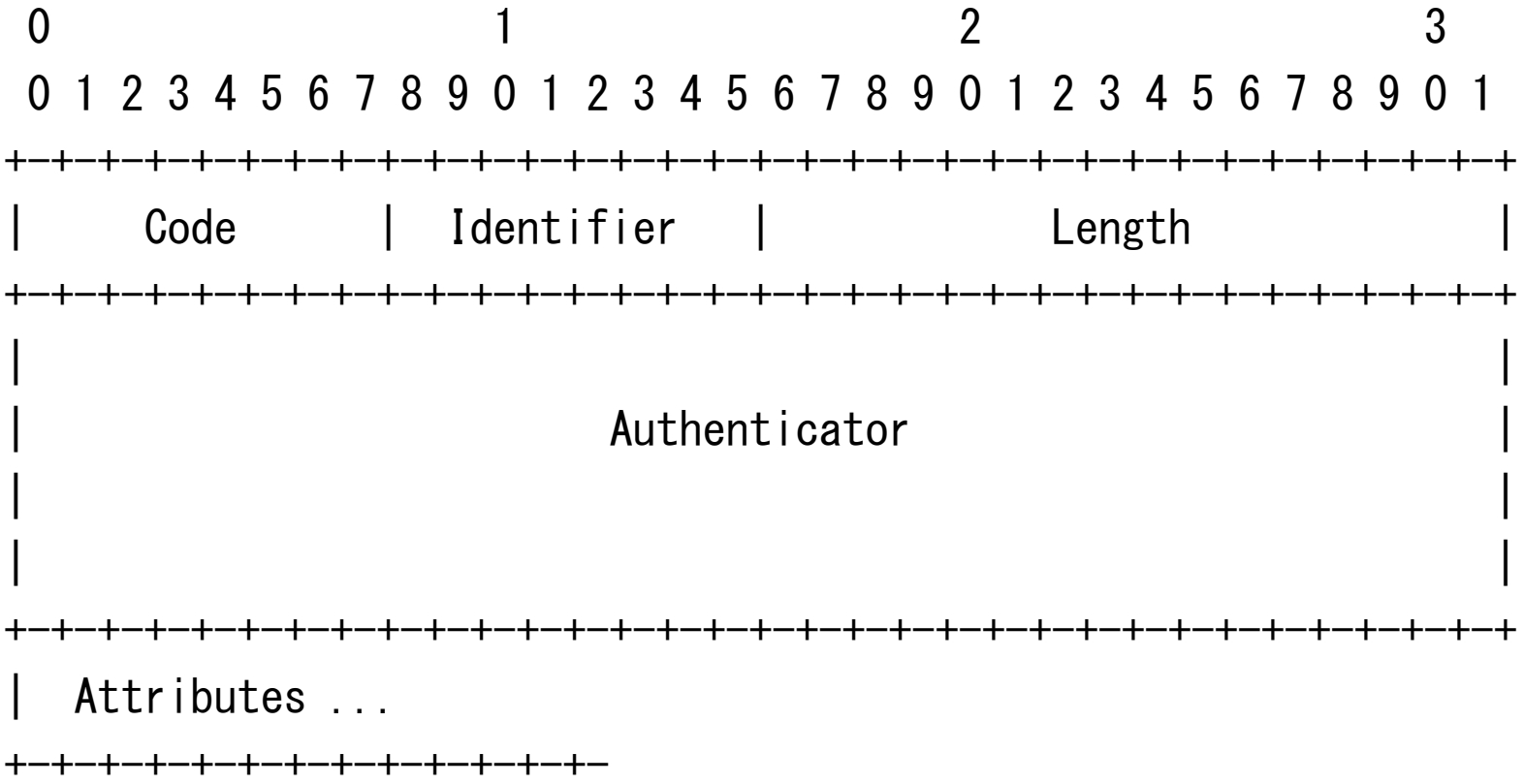
AAA (Authentication, Authorization, Accounting)

- user
  - authentication
    - secure identification
  - authorization
    - permit proper right
  - accounting
    - usage based charging
    - became essentially important as internet was commercialized

Radius (Remote Authentication Dial In User Service, rfc2138, rfc2139)

- protocol for large scale dial-up ISP, originally
- based on UDP (light weight)
- dial-up modems are clients
- central management of clients by radius server
  - authentication between server and client
    - password from user through client to server is encrypted
- perform AAA (Authentication, Authorization, Accounting (rfc2139))

Packet Format of RADIUS (1)

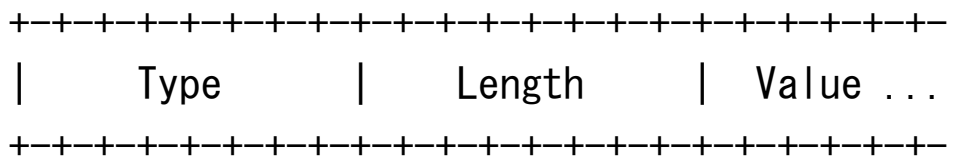


Packet Format of RADIUS (2)

- Code
  - 1 Access-Request
  - 2 Access-Accept
  - 3 Access-Reject
  - 4 Accounting-Request
  - 5 Accounting-Response
  - 11 Access-Challenge
  - 12 Status-Server (experimental)
  - 13 Status-Client (experimental)
  - 255 Reserved

Packet Format of RADIUS (3)

- Identifier
  - match request and reply
- Length
- Authenticator
  - 16B hash on packet contents and password
- Attributes (in TLV format)



Examples of Attributes

- 1 User-Name
- 2 User-Password
- 3 CHAP-Password
- 4 NAS-IP-Address
- 5 NAS-Port

Extensions to RADIUS

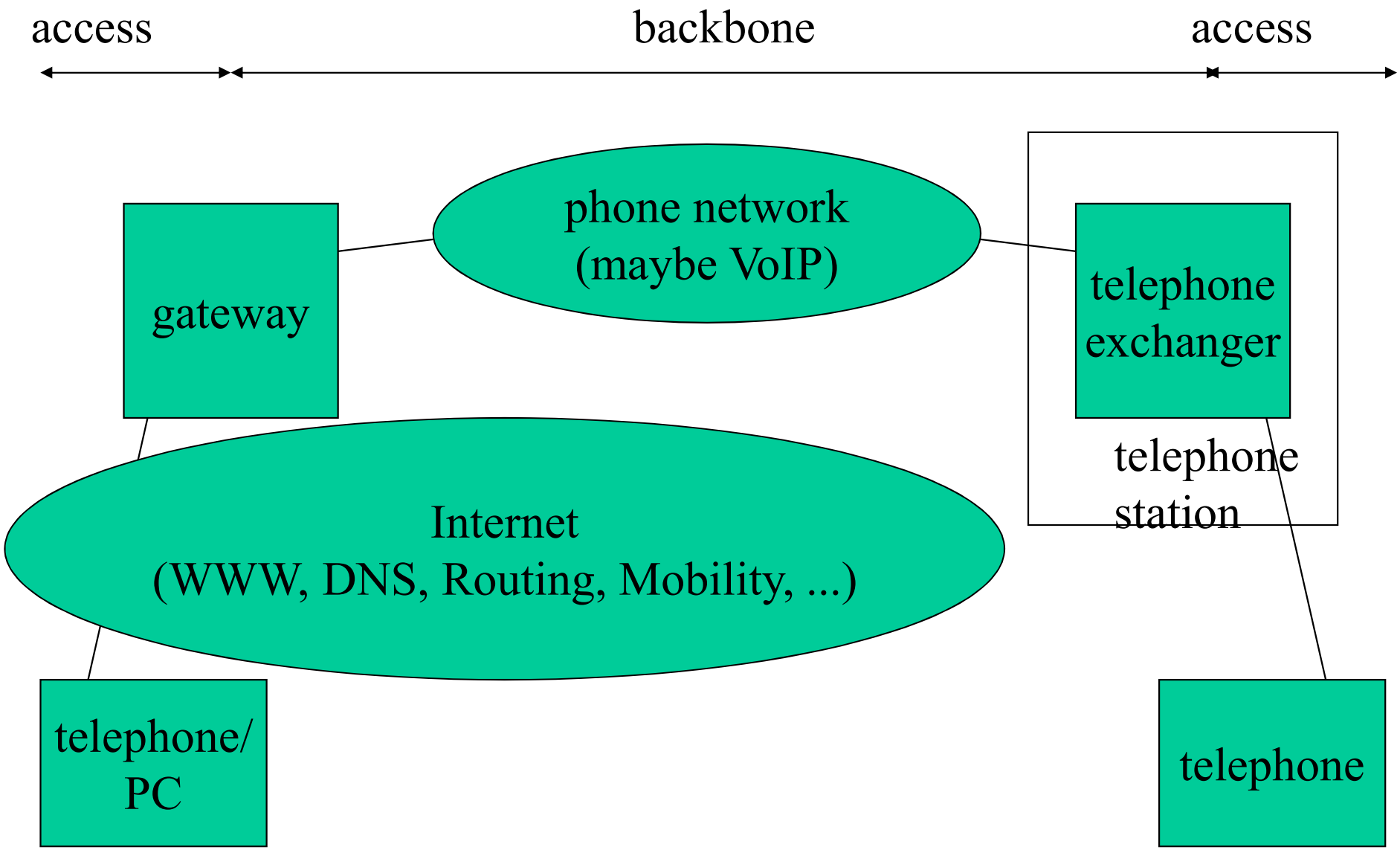
- RADIUS use TLV format
  - easy to extend
    - type may be unique only between servers and clients in an ISP
      - many ISPs have their own extensions
- may be extended for internet phone
  - access phone network through internet
    - dial-up is to access internet through phone network
- may be extended for wifi internet

Service (Business?) Model for the Internet Era

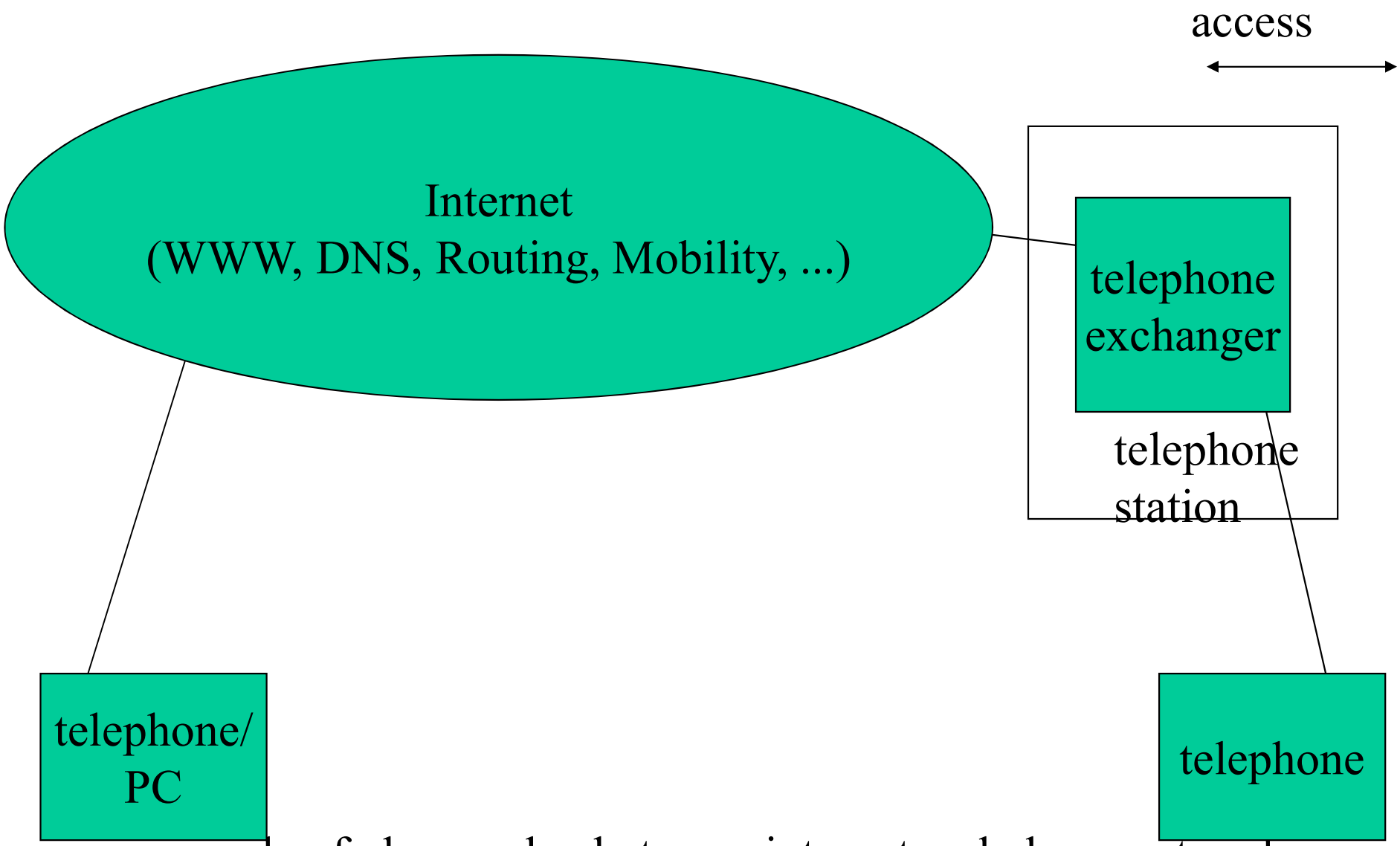
- within internet
  - communicate peer to peer
  - network do nothing, scarcely no ISP operations
    - no room for regulation or business
    - a lot of terminals can be purchased
- gateway between internet and phone network
  - should be profitable (as long as phone network alive)
- abandone immobile phone network?

Phone Relay Service between Internet and Phone Network

- provide relay gateways appropriately
  - maybe at all local stations
  - maybe at Tokyo, Osaka and USA
- free within internet (except for fixed ISP fee)
- usage based charge in phone network



example of phone relay between internet and phone network



example of phone relay between internet and phone network
place gateways at all local stations

Relay Service Model between Internet and Phone Network

- phone network -> internet
  - user in internet side may register (flat rate?)
    - telephone # necessary (maybe free)
- internet -> phone network
  - usage based charge within phone network
    - some security necessary (like calling card)
- phone network -> internet -> phone network
  - not very different from long distance carrier

NOTASIP Project

- a project for internet phone
  - funded by TAO (agency of MPT)
- no inventions, no complications
  - recognize terminals by URLs
  - manage connection to PSTN by RADIUS
    - security of calling card (4 digit PIN) is enough
  - analog telephone device should be usable as is
  - routing and mobility should depend on internet

Wireless Internet

- needs wired Internet infrastructure
  - by densely installed optical fiber
    - FCC once claimed wireless only is enough, but,
  - high speed inexpensive radio stations attached to wired high speed inexpensive flat rated internet
    - inexpensive flat rated wireless internet
  - if stations are dense enough
    - high speed inexpensive flat rated wireless internet

Technical Problems of the Wireless Internet

- wireless can be used by general public
  - authentication
    - good that anyone can use the internet anytime/anywhere
    - no good if users are not identified
      - crime investigation
      - charge money
  - encryption
    - basically should be end to end
    - good for old protocols with plain text password

Security of Dial-up Internet over Phone Network

- connection through phone network
  - moderately secure
    - can use logging by phone network for crime investigations etc.
- established call can not be interrupted
  - initial authentication is enough
    - e.g. with PPP by password

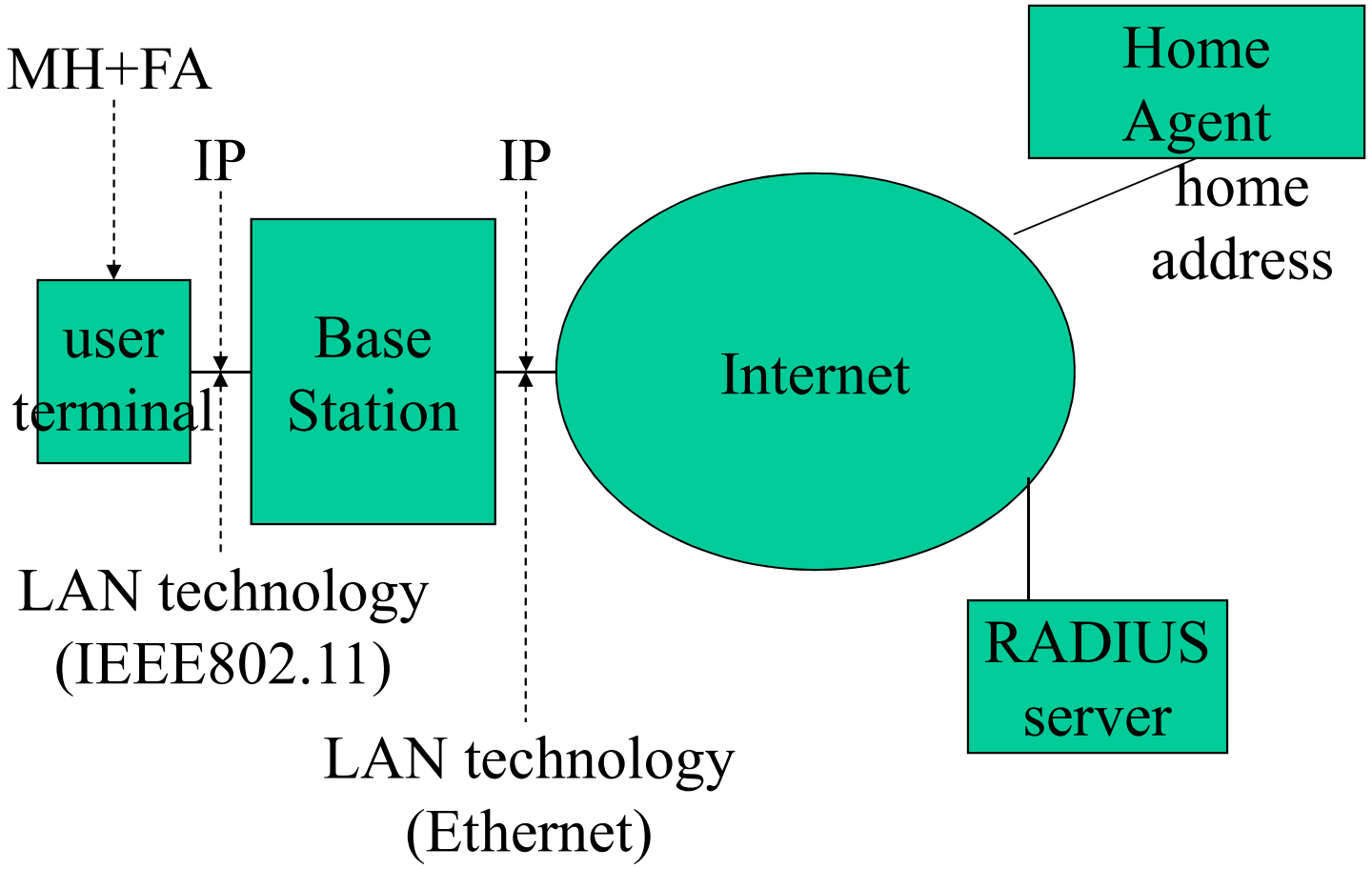
Security of Dial-up (?) Internet over Wireless Network

- connection through Wifi
  - by itself, no security at all
    - user identification and logging by PPP for crime investigations etc.?
- established conneciton can be interrupted
  - initial authentication is not enough
    - identify packets by IP and MAC address?
      - anyone can forge packets
  - packet-wise authentication necessary
    - session key is shared upon connection set up

Security of Wireless Internet

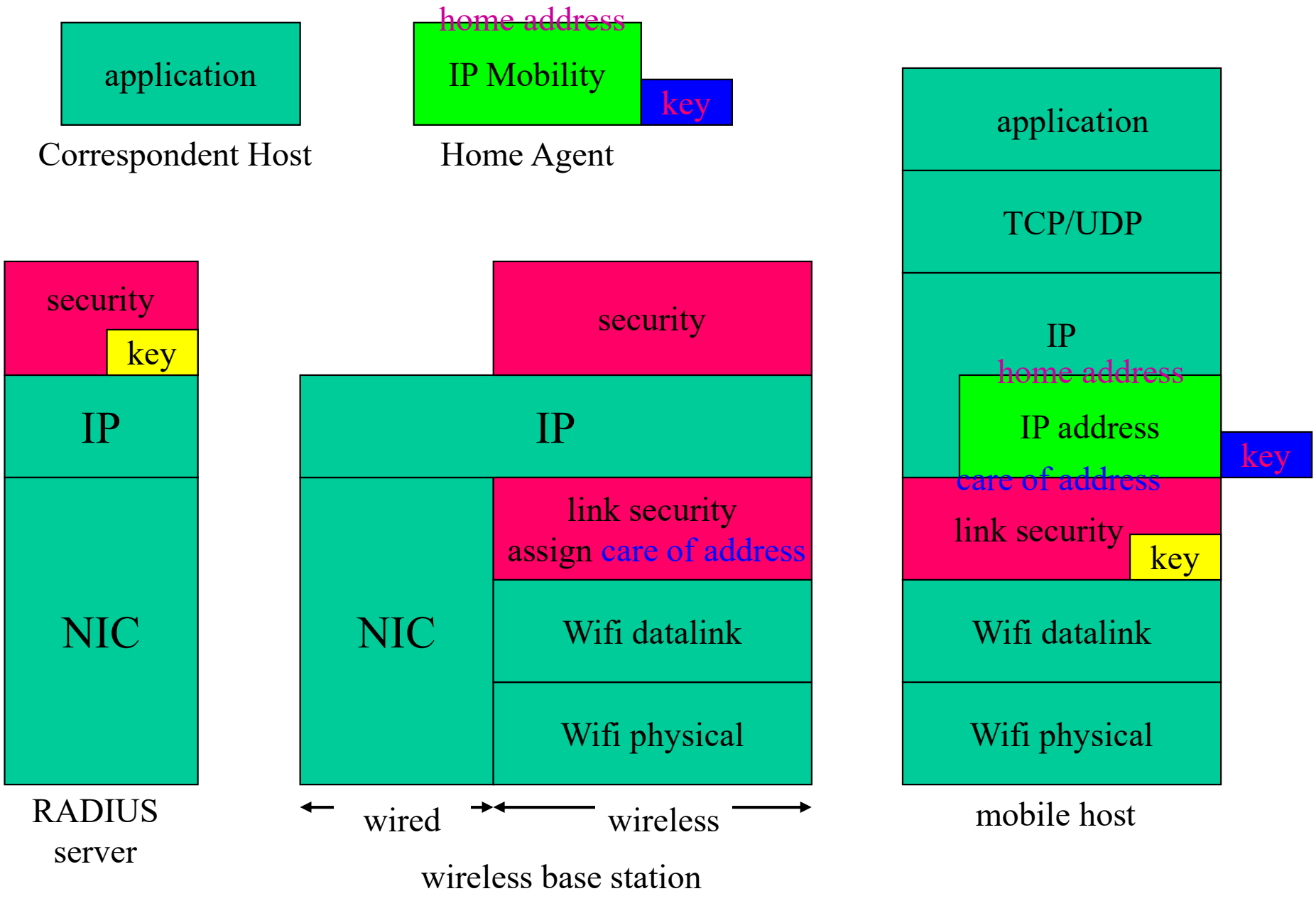
- RADIUS server maintain user keys
- user terminal generate session key, encrypt with user key and send to wireless BS
- BS ask RADIUS server decryption of session key
- session key may be used for authentication and encryption between user terminal and BS

Proper Mobile Internet



Components of Mobile Internet Service

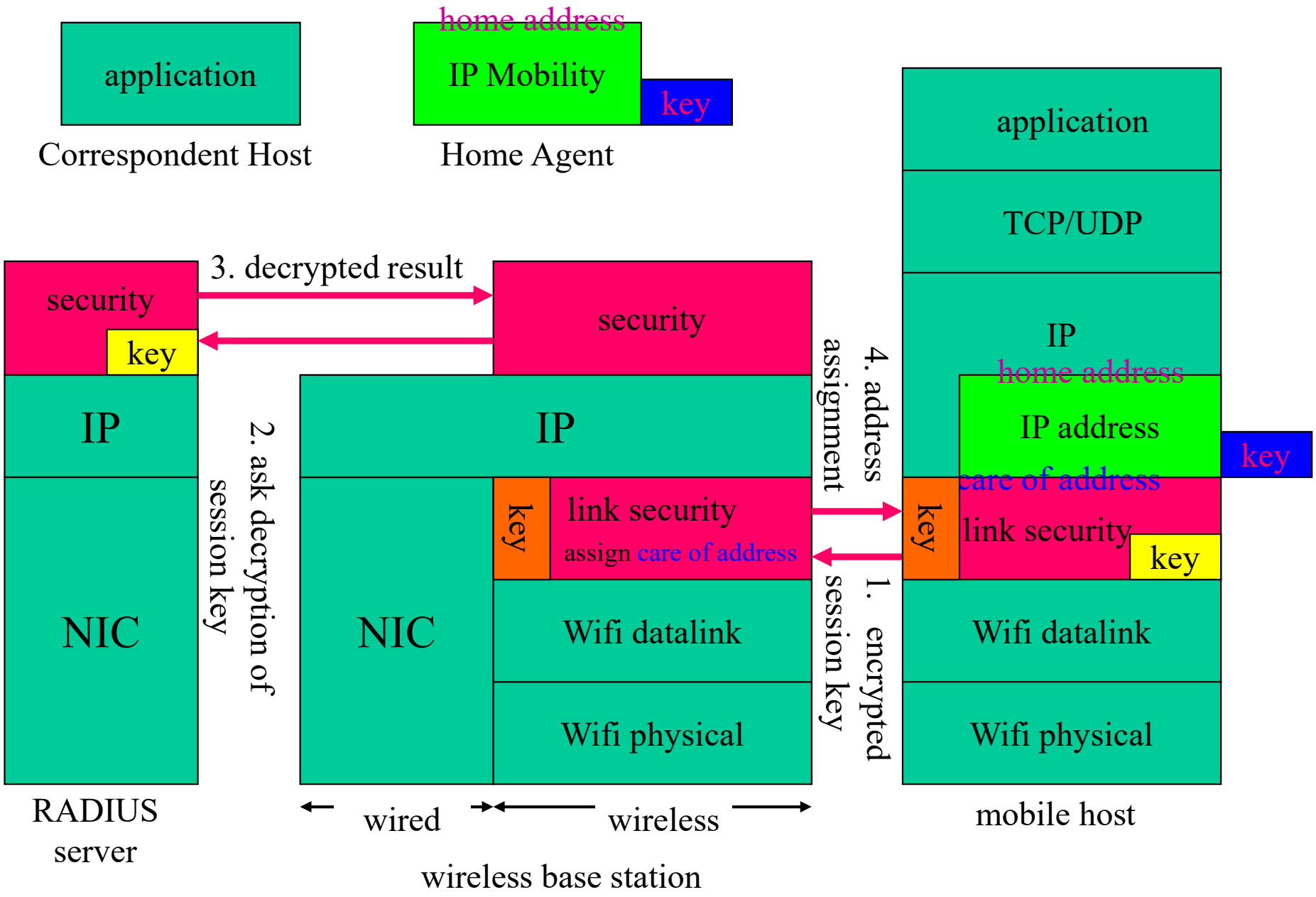
- mobile host (wireless)
  - mobile terminal moving around and between BSes
- BS
  - a router with wireless interface
- RADIUS server
  - manage user key for wireless datalink
- Home Agent
  - forward packets to home address to mobile host



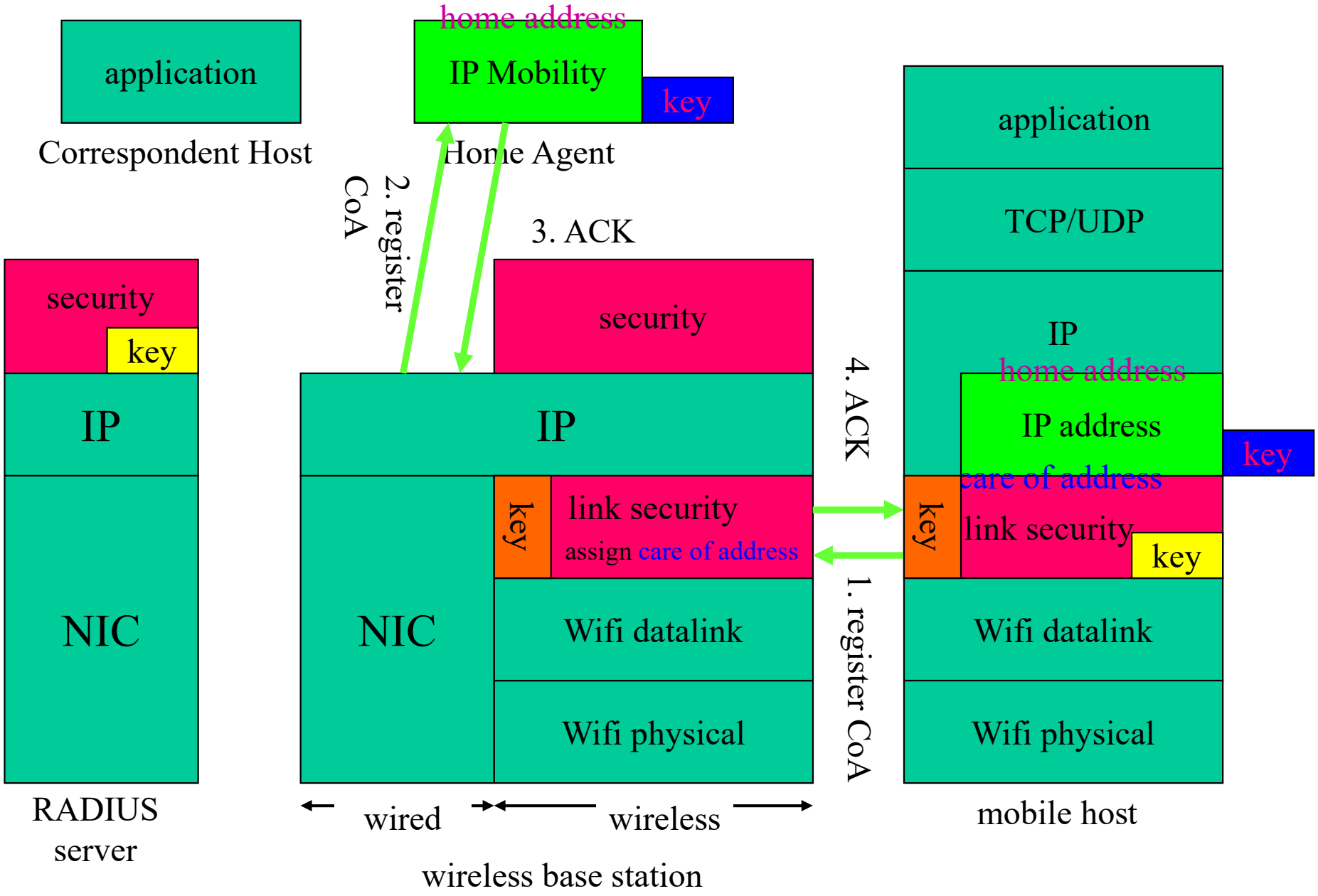
Components for Mobile Internet Service

Authentication, Session Key Sharing and Address Assigenment for Mobile Internet Service

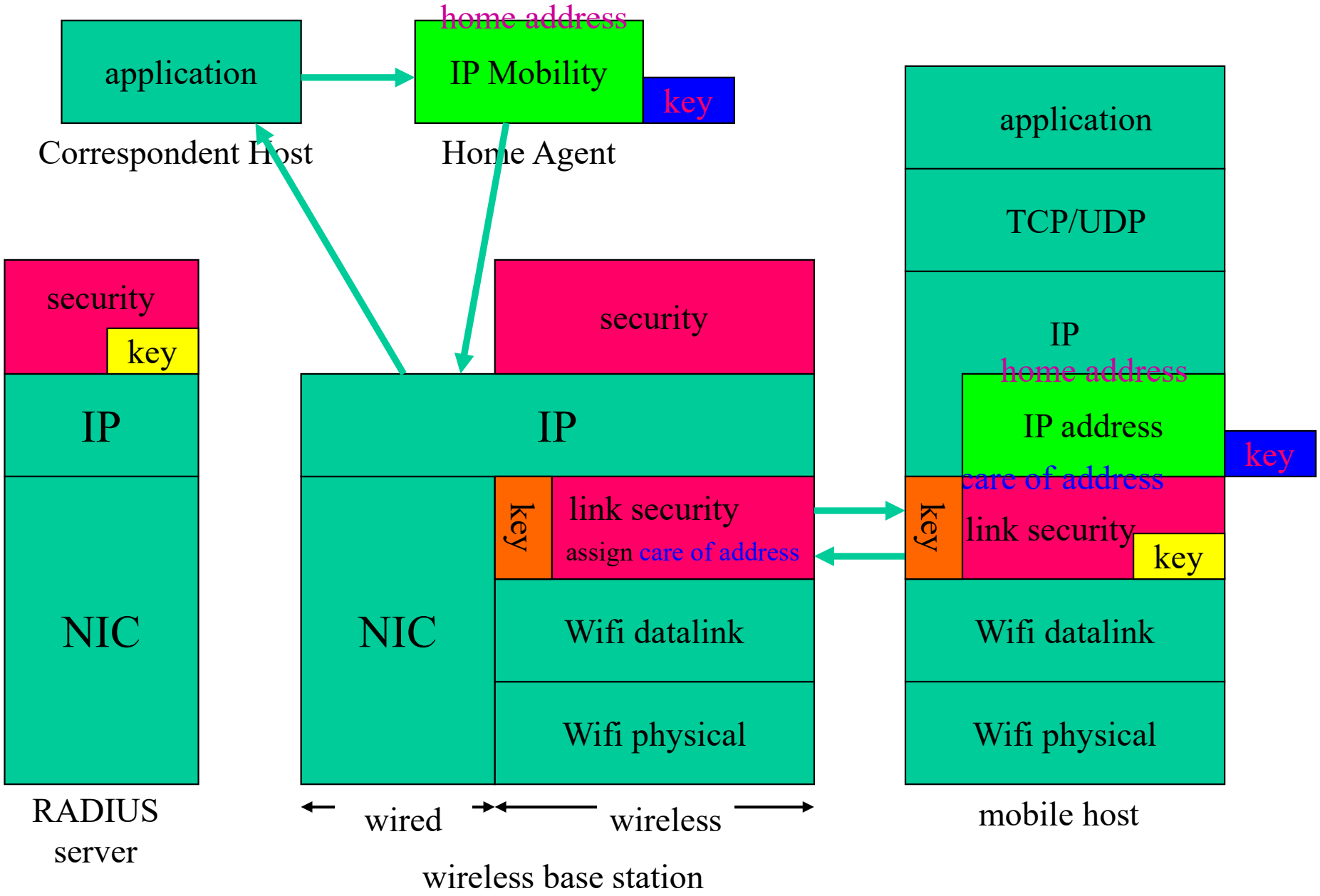
- mobile host generate session key
- encrypt by user key and send to BS
- BS ask RADIUS server decryption
- mobile host and RADIUS server share session key
- BS assign mobile host (care of) address



initial stage of mobile internet service (authentication, share session key, assign address)



second stage of mobile internet service (register location to HA)



final stage of mobile internet service (communicate with correspondent host)

Wrap Up

- internet-wide clock synchronization unnecessary
  - can adjust play speed by buffer
  - time can be synchronized to somewhere
- (extended) RADIUS is useful for various authentication