

Mobile Computing

Unit I

Process Transformation

Business Strategy

Enterprise Architecture

Change Management

IT Strategy

Analytics & Business Intelligence

Social Media

What is mobile computing?

- ❖ Mobile computing is to describe technologies that
 - ❖ enable people to access network services **anyplace, anytime, and anywhere**,
 - ❖ with **portable** and **wireless** computing and communication devices.
- ❖ Aspects of mobility
 - ❖ User mobility
 - ❖ Between different geographical locations
 - ❖ Between different networks
 - ❖ Between different communication devices
 - ❖ Between different applications
 - ❖ Device portability
 - ❖ Between different geographical locations
 - ❖ Between different networks

Mobile Computing vs. Ubiquitous Computing/Pervasive Computing

- **Mobile Computing** is a generic term describing the application of small, portable, and wireless computing and communication devices. This includes devices like laptops with wireless LAN technology, mobile phones, wearable computers and Personal Digital Assistants (PDAs) with Bluetooth or IRDA interfaces, and USB flash drives.
- **Ubiquitous computing** (ubicomp, or sometimes ubiqcomp) integrates computation into the environment, rather than having computers which are distinct objects.
- **Pervasive computing**. Promoters of this idea hope that embedding computation into the environment would enable people to move around and interact with computers more naturally than they currently do.

Challenges

- Disconnection
- Low bandwidth
- High bandwidth variability
- Low power and resources
- Security risks
- Wide variety terminals and devices with different capabilities
- Device attributes
- Fit more functionality into single, smaller device

Future of Mobile Computing

- Use of Artificial Intelligence
- Integrated Circuitry -> Compact Size
- Increases in Computer Processor speeds

Mobile Computing

Mobile Computation

- Mobile agent
- Mobile process

Mobile Communication

- Mobile network
- Mobile service
- Mobile user
- Mobile device

Mobility

has

has

include

Mobility
in physical
space

Mobility
in network
space

Mobility
in information
space

What is Mobile Computing?

□ What is computing?

The capability to automatically carry out certain processing related to service invocations on a remote computer .

□ What is the mobility ?

The capability to change location while communicating to invoke computing service at some remote computers.

□ What is mobile computing?

Ability to compute remotely while on the move. It is possible to access information from anywhere and at anytime.

- A simple definition could be:

Mobile Computing is using a computer (of one kind or another) while on the move

- Another definition could be:

Mobile Computing is when a (work) process is moved from a normal fixed position to a more dynamic position.

- A third definition could be:

Mobile Computing is when a work process is carried out somewhere where it was not previously possible.

- Mobile Computing is an umbrella term used to describe technologies that enable people to access network services anyplace, anytime, and anywhere.

Mobile computing vs Wireless networking

- ❖ Mobile computing is based on wireless networking and helps to invoke computing services on remote servers while on the move.
- ❖ So Wireless networking is an important and necessary ingredient of mobile computing.
- ❖ Mobile computing also requires the applications themselves – their design and development, the hardware at the client and server sides

Classification of Wireless networks

Wireless networks can be classified into basic types

- Infrastructure network -One is extension of wired networks. It uses fixed infrastructure such as base station to provide single hop wireless communication with wired network as shown in figure 2.1.
- ❖ Two-hop cellular communication as shown in figure 3.

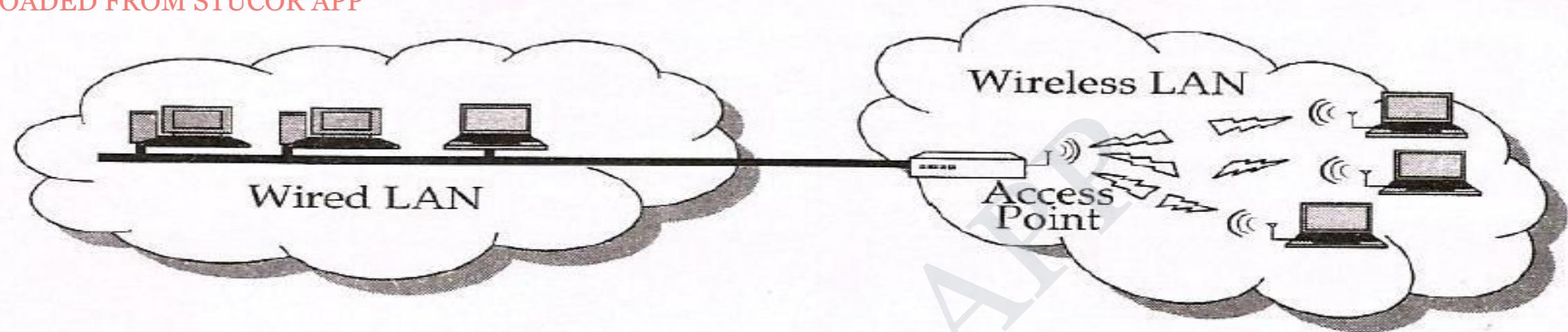


Figure 2.1 Wireless network based on fixed infrastructures.

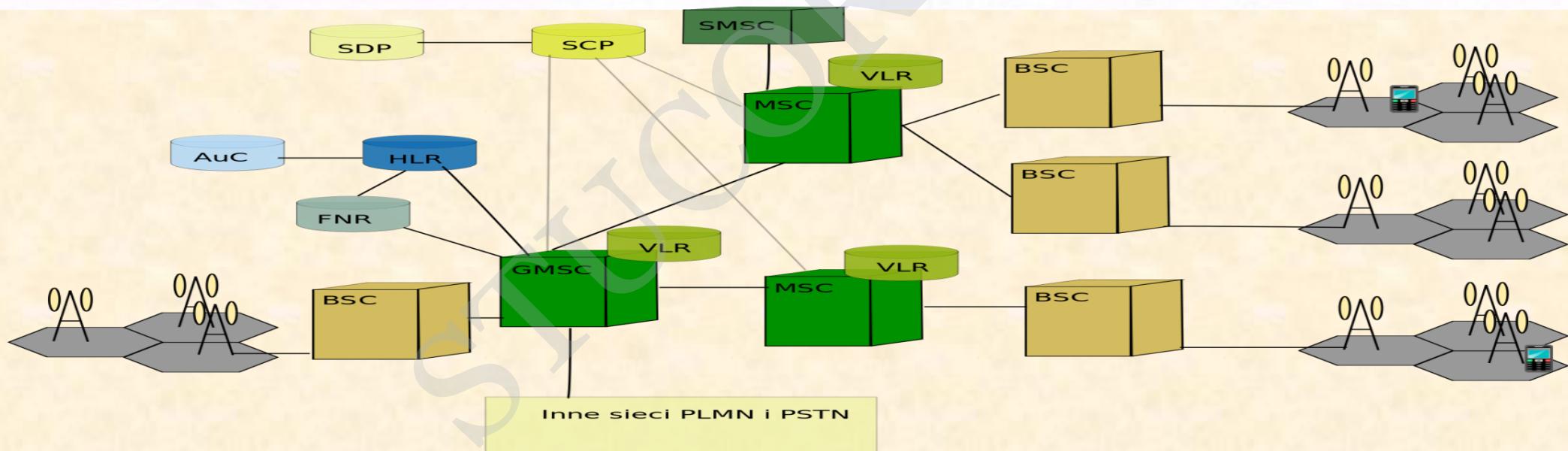


Figure 3- Two-hop cellular communication

- **Ad Hoc network** It does not use any fixed infrastructure and is based on multi-hop wireless communication as shown in figure 2.2

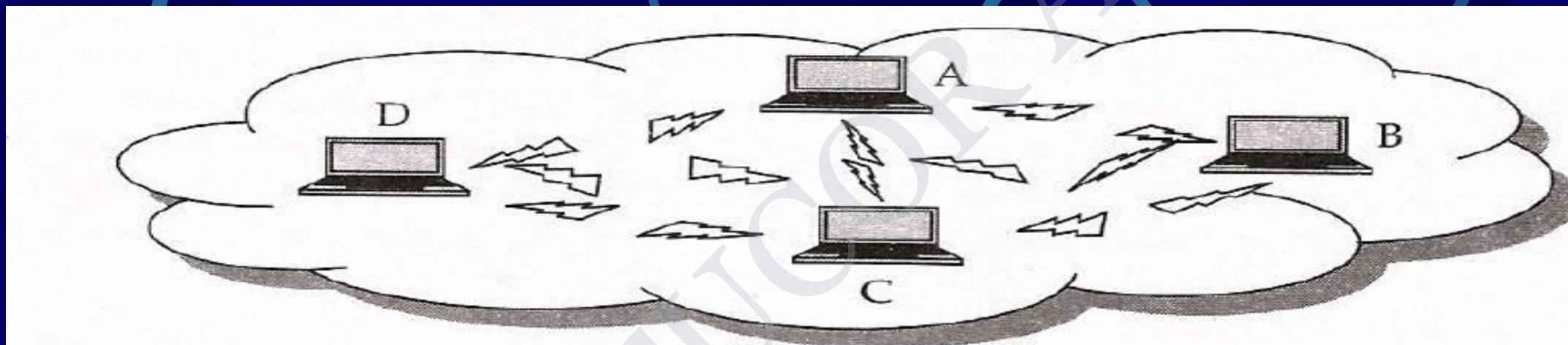


Figure 2.2 Wireless network having no fixed infrastructures.

Applications of Mobile Computing

- Stock Information Collection/Control
- Emergency services
- For Estate Agents
- In courts
- In companies
- Credit Card Verification
- Taxi/Truck Dispatch
- Electronic Mail/Paging

Applications Conti...

- Vehicles
 - transmission of news, road condition, weather, music via DAB
 - personal communication using GSM
 - position via GPS
 - local ad-hoc network with vehicles close-by to prevent accidents, guidance system, redundancy
 - vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance
- Medical
 - Nurses/Doctors in Medical offices are now using Wireless Tablet PCs/WLAN to collect and share patient information.
- Sales
 - Sales representatives are using Tablet PCs with Smart phones for presentation, transmitting/access information among office, hotel, and customer location.
- Emergencies
 - Early transmission of patient data to the hospital, current status, first diagnosis
 - Provide mobile infrastructure in dealing with Natural Disaster (earthquake, hurricane, fire), terrorist attacks, war, ...

Characteristics of Mobile Computing

- **Ubiquity** – The ability of a user to perform computation from anywhere and at anytime.
- **Location awareness** – Many applications require or value additions by location based services.
- **Adaptation**- Ability to adjust to bandwidth fluctuations without inconveniencing the user.

- **Broadcast**- Efficient delivery of data can be made simultaneously to hundreds of mobile users
- **Personalization** – Services in a mobile environment can be easily personalized according to a user's profile.

Structure of Mobile Computing Application

- A mobile computing application is usually structured In terms of the functionalities implemented .
- As shown in the figures 2.3 and 2.4 the three tiers are named presentation tier, application tier and data tier.

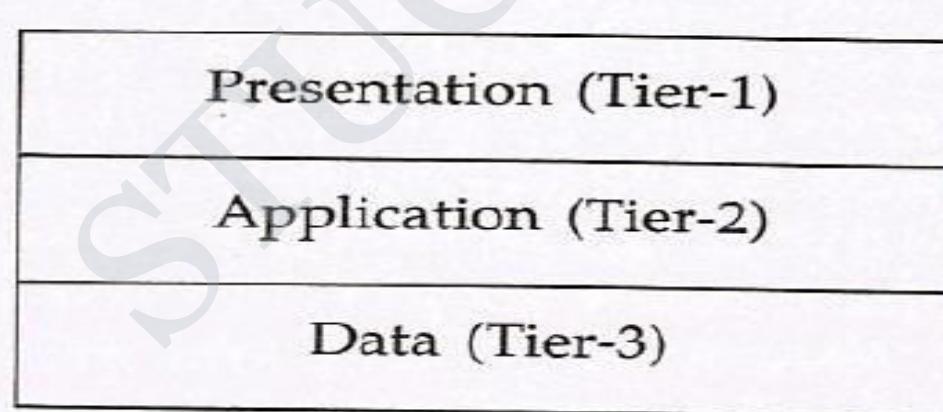


Figure 2.3 *The three tier structure of a mobile computing application.*

Presentation
Tier

Find the
sales
total

Five total
sales

Tier 1

Application
Tier

Find the list of sales
made in last year

Query

Sum of all the sales

Sales 1
Sales 2
Sales 3
Sales 4
Sales 5

Tier 2

Data
Tier



Storage

Tier 3

Figure 2.4 Functionalities provided by each tier structure of a mobile computing application.

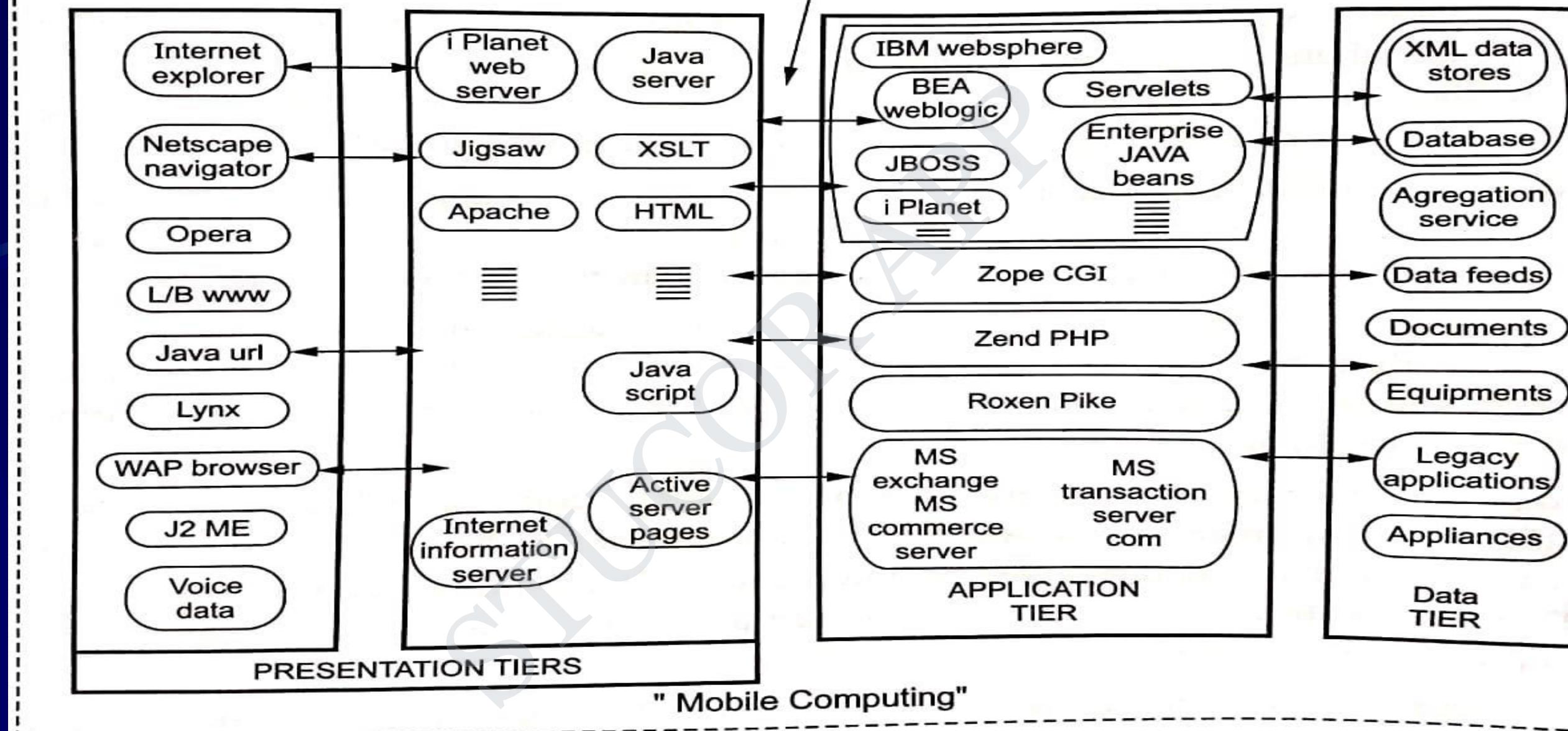


Fig. 1.3.1 Architecture of mobile computing

- **Presentation tier** – The topmost level, concerns the user interface. It facilitates the users to issue requests and to present the results meaningfully. It includes web browsers and client programs.
- **Application tier** – It is responsible for making logical decisions and performing calculations. Implemented using Java, .NET services, cold fusion etc. Implemented on a fixed server.
- **Data tier** – Responsible for data storage, access and manipulation. Implemented on a fixed server.

MEDIA ACCESS CONTROL(MAC)

- A channel-access scheme is also based on a multiple access protocol and control mechanism, also known as media access control (MAC). This protocol deals with issues such as addressing, assigning multiplex channels to different users, and avoiding collisions.

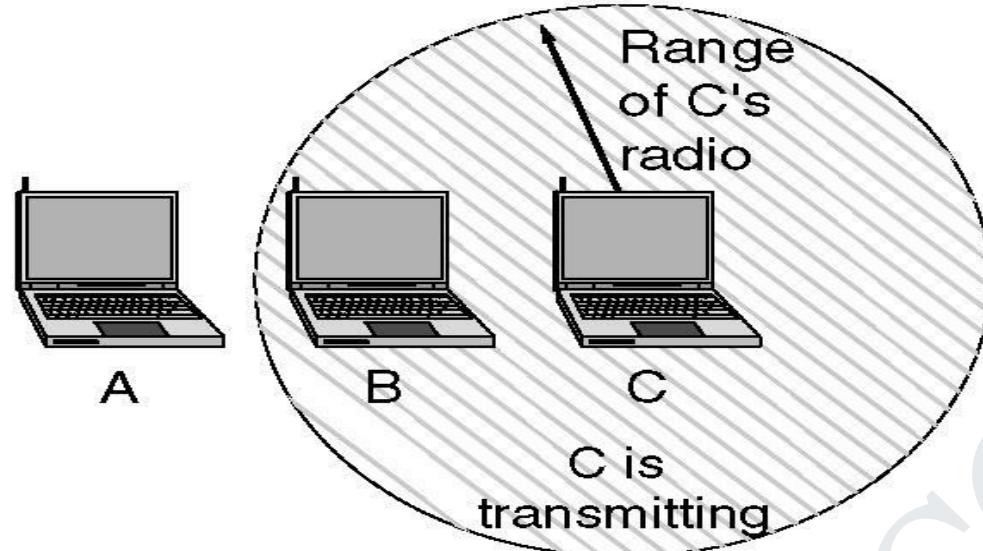
Responsibility and objective of MAC Protocol

- **Responsibility** :Enforce discipline in the access of a shared channel when multiple nodes contend to access that channel.
- **Objective**: Maximization of the utilization of the channel and minimization of average latency of transmission .

The Hidden Terminal Problem

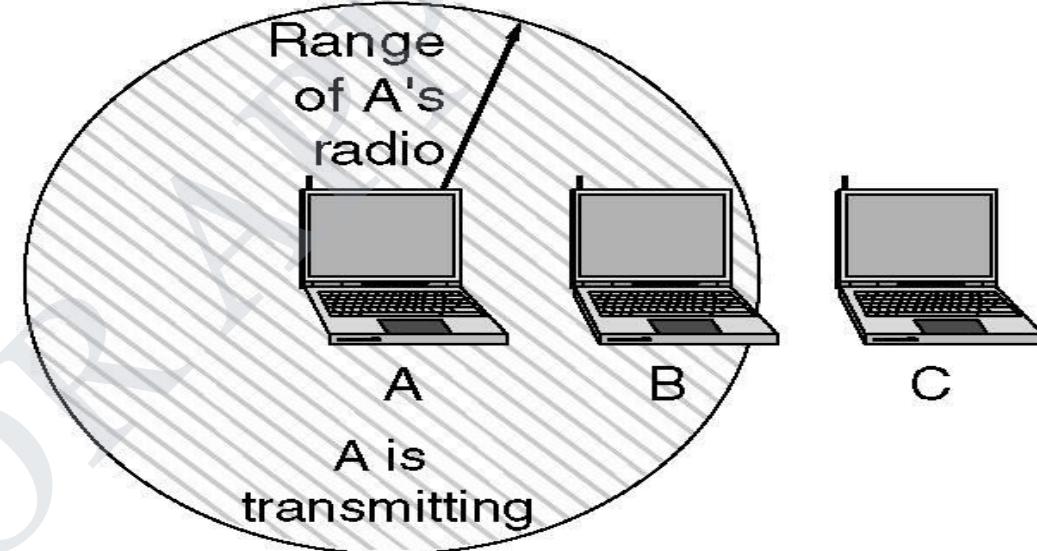
- ❖ Wireless stations have transmission ranges and not all stations are within radio range of each other.
- ❖ Simple CSMA will not work!
- ❖ C transmits to B.
- ❖ If A “*senses*” the channel, it will not hear C’s transmission and falsely conclude that A can begin a transmission to B.
- ❖ Create a very difficult and important arbitration problem that a MAC protocol needs to resolve.

A wants to send to B
but cannot hear that
B is busy



(a)

B wants to send to C
but mistakenly thinks
the transmission will fail



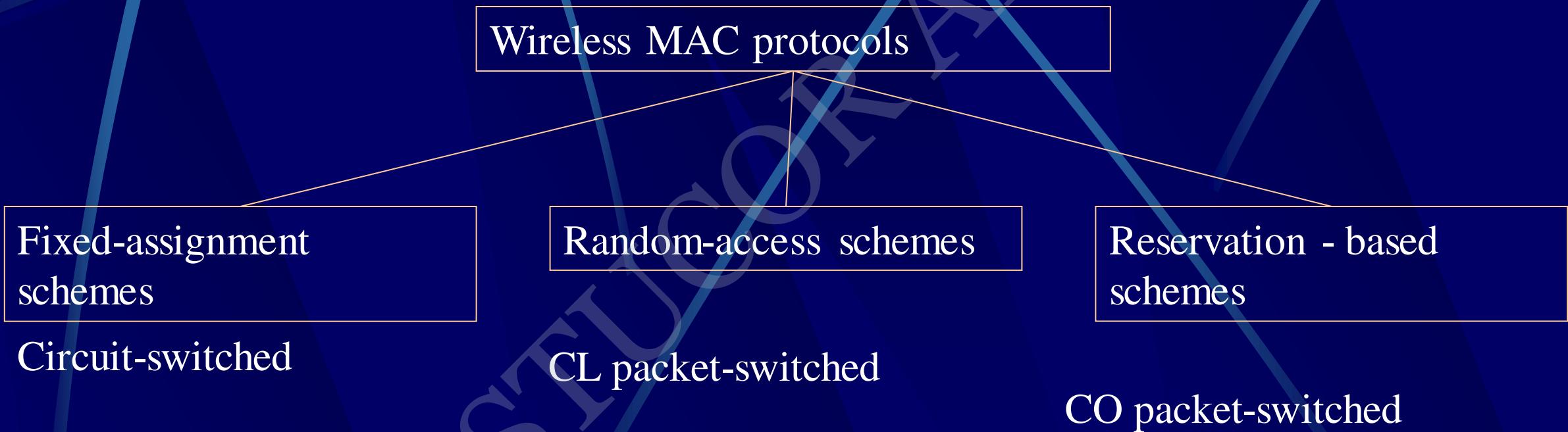
(b)

Figure 4-26.(a)The hidden station problem. (b) The exposed station problem.

The Exposed Station Problem

- ❖ The inverse problem.
- ❖ B wants to send to C and listens to the channel.
- ❖ When B hears A's transmission, B falsely assumes that it cannot send to C.
- ❖ It leads to inefficient spectrum usage as well as unnecessary transmission delays.

Classification of wireless MAC protocols

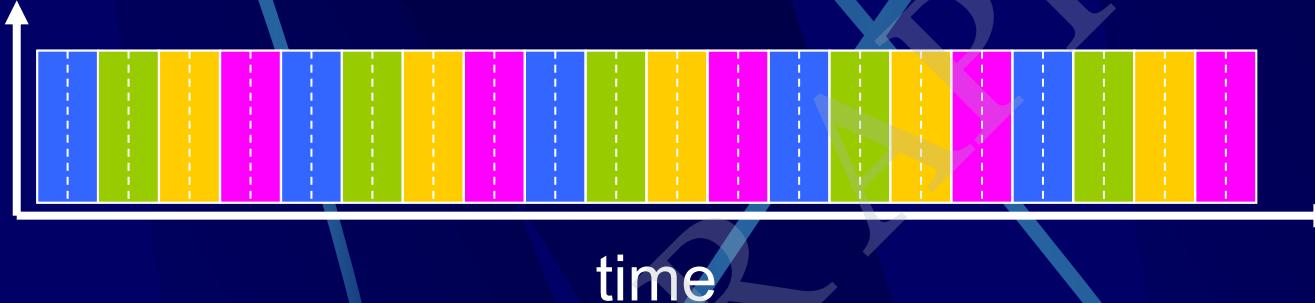


CL – Connection Less. CO – Connection Oriented

Channel Partitioning MAC protocols

TDMA: Time Division Multiple Access

Frequency

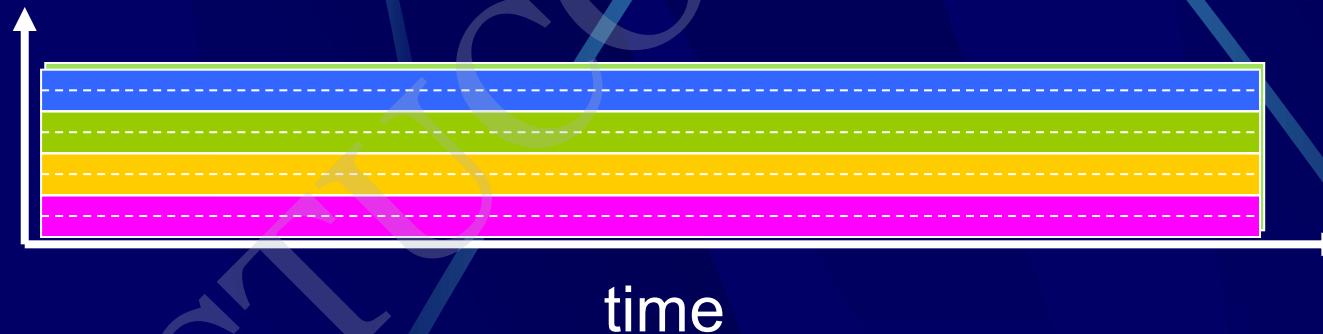


Example:
4 users



FDMA: Frequency Division Multiple Access

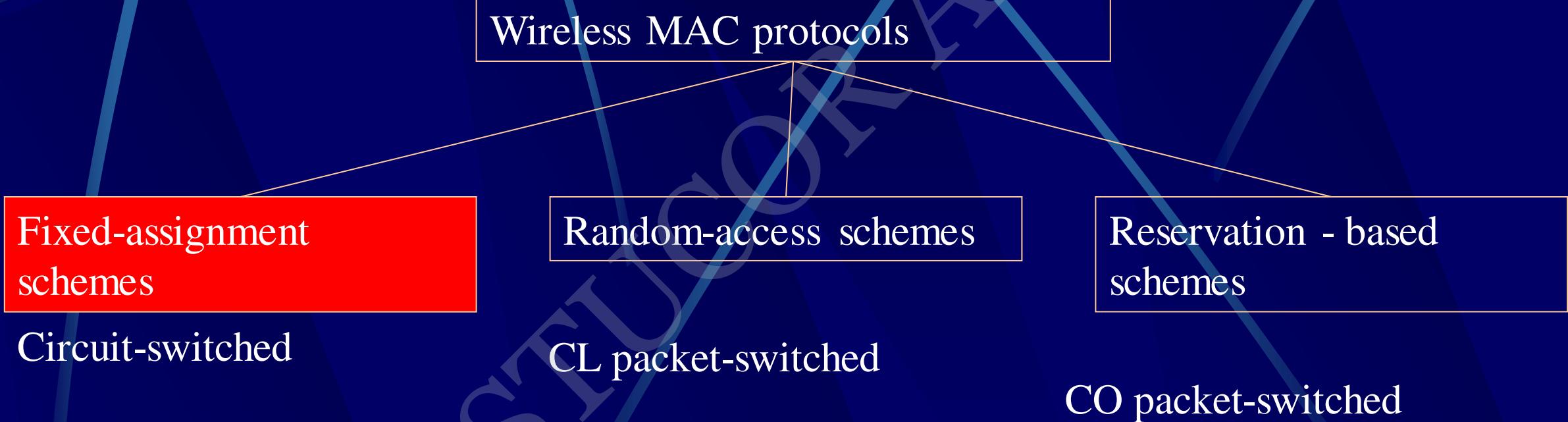
Frequency



CDMA: Code Division Multiple Access

- Same frequency and time but different codes.

Classification of wireless MAC protocols

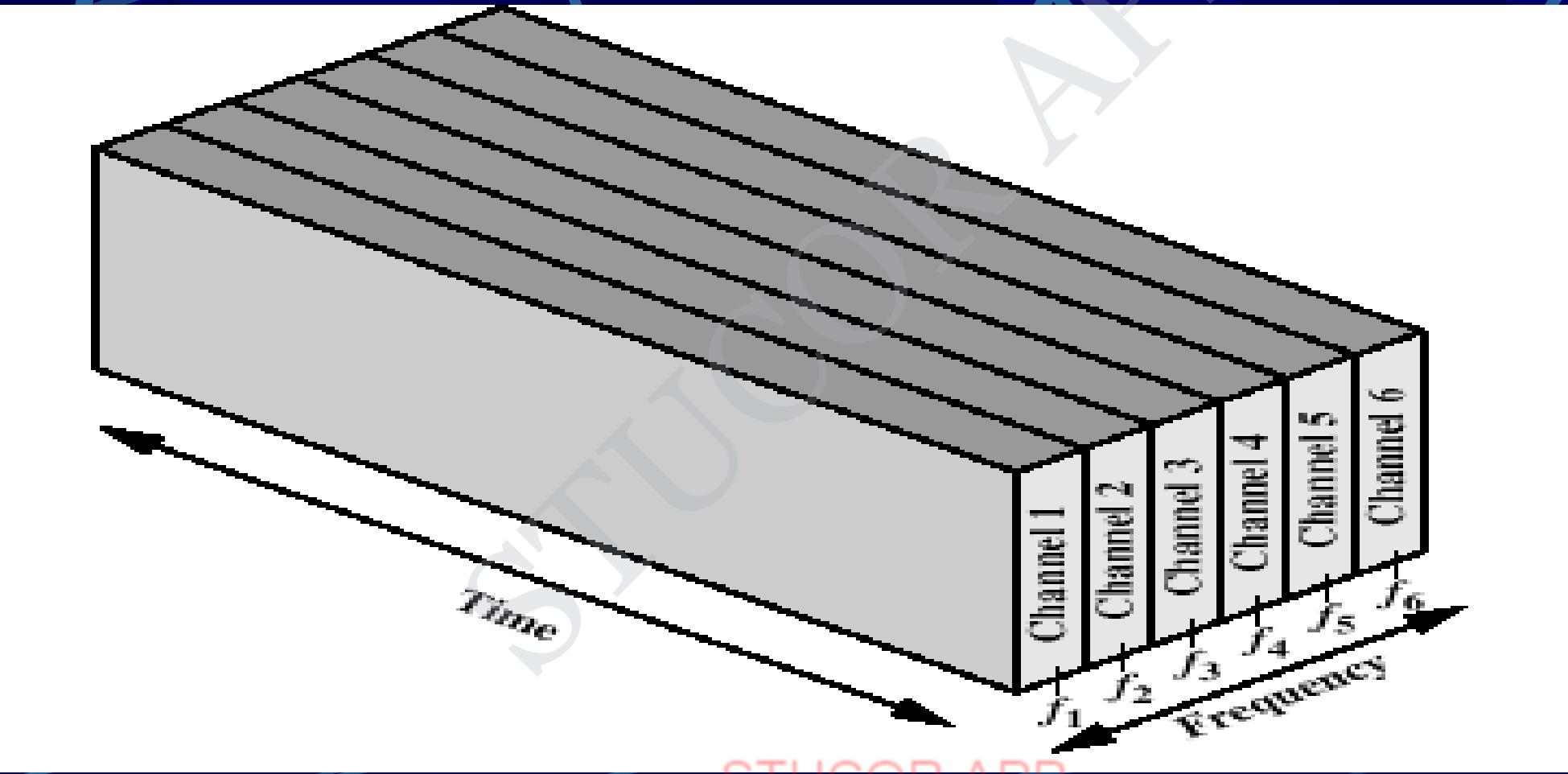


CL – Connection Less. CO – Connection Oriented

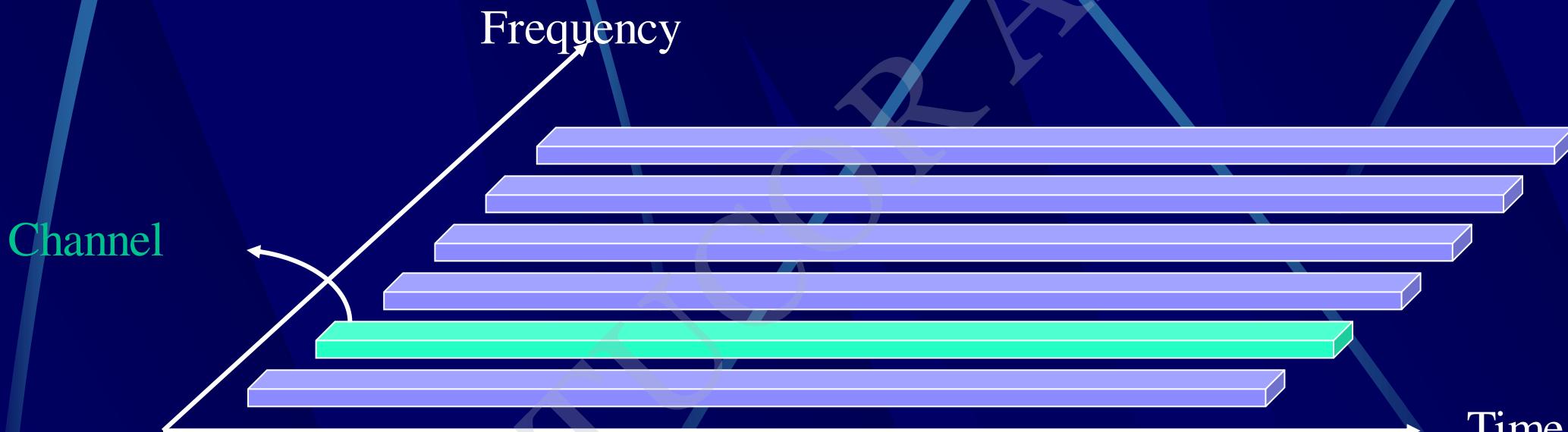
Frequency Division Multiple Access (FDMA)

- ❖ In an FDMA system, each user has its own frequency channel. This implies that relatively narrow filters are needed in each receiver and transmitter.
- ❖ Most duplex FDMA systems must transmit and receive simultaneously. (Frequency Division Duplex, FDD).
- ❖ It does not achieve a high channel utilization.

Frequency Division Multiple Access



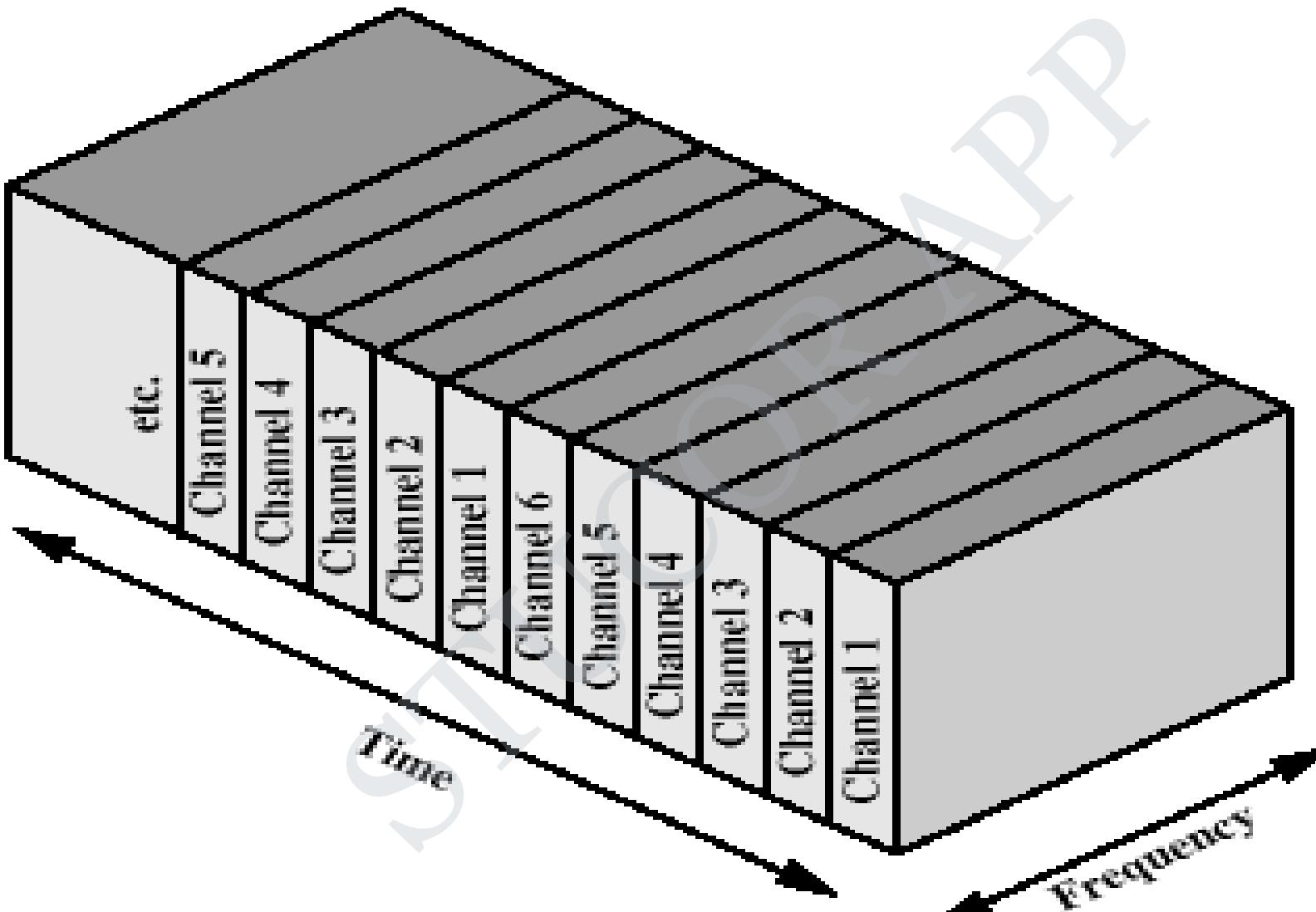
FDMA

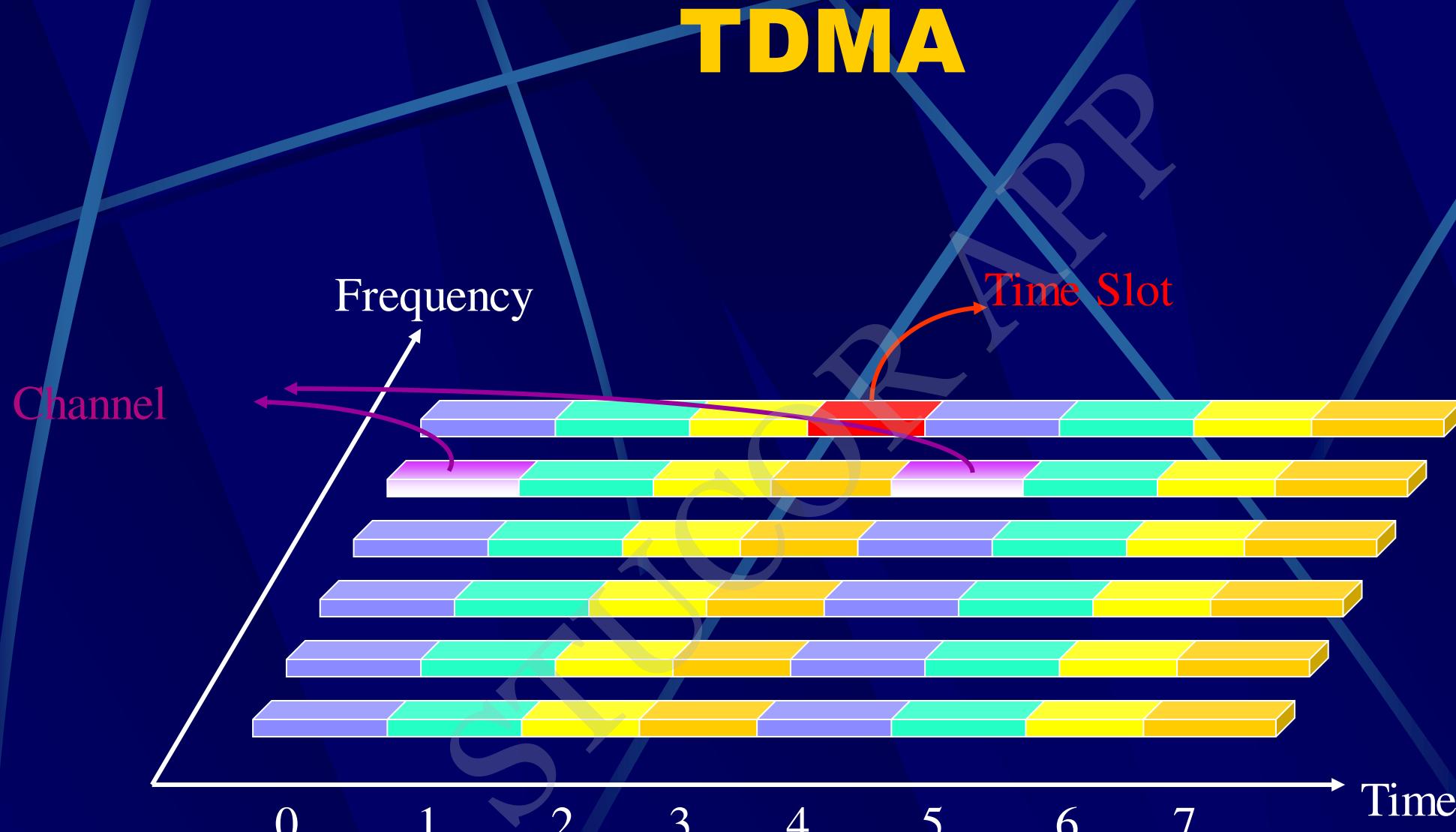


Time Division Multiple Access (TDMA)

- In TDMA, a set of N users share the same radio channel, but each user only uses the channel during predetermined slots.
- A frame consists of N slots, one for each user. Frames are repeated continuously.
- Time slots are allocated to users in a round robin manner .
- Un used time slots go idle, leading to low channel utilization

Time-division multiplexing





Code Division Multiple Access **(CDMA)**

- Multiple users use the same frequency at the same time.
- All the senders send signals simultaneously.
- The signals can be distinguished from each other by frequency spreading code known as the m bit pseudo-noise(PN) sequence.
- Using m bits $2^m - 1$ codes obtained
- Each user will use only one code.

CDMA

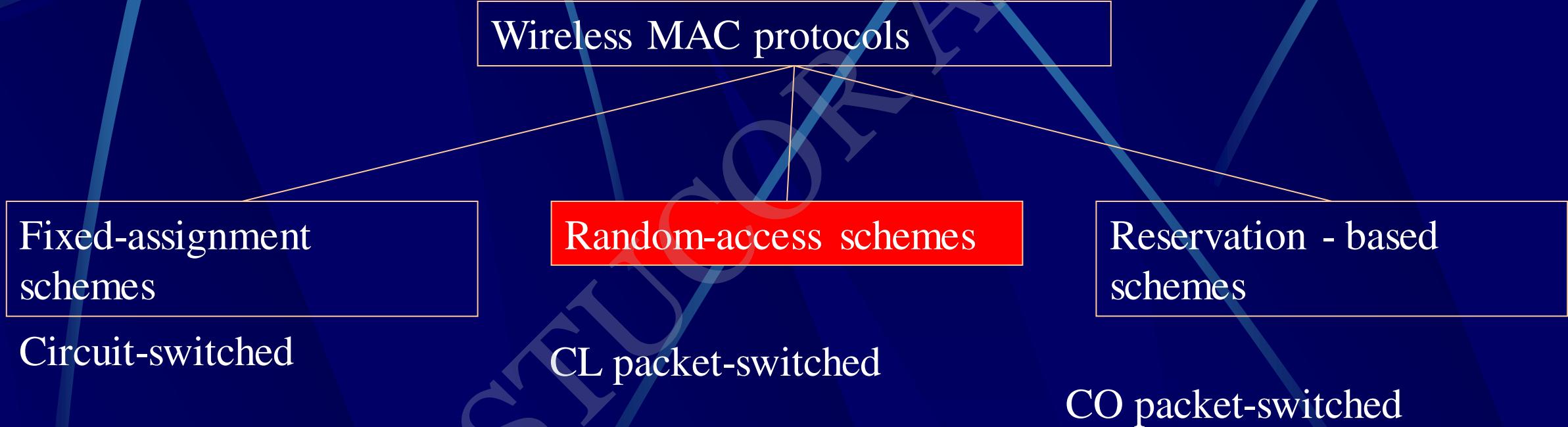
Frequency

Code

Time

Code 1
Code 2
Code 3

Classification of wireless MAC protocols



CL – Connection Less. CO – Connection Oriented

Random access MAC Schemes

- Number of random assignment schemes . A few important.
- ALOHA
- Slotted ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA

- Simplest scheme
- True free-for-all. When a node needs to send, it does so.
- It listens for an amount of time equal to the maximum round trip delay plus a fixed increment.
- If it hears an acknowledgment, fine; otherwise it resends after waiting a random amount of time.
- After several attempts, it gives up.
- Low delay if light load

Slotted ALOHA

- ❖ An improvement over pure ALOHA.
- ❖ Time is divided into equal sized slots in which a packet can be sent. The size of pocket is restricted.
- ❖ Send packet only at the beginning of a slot.
- ❖ Employ beacon signals to mark the beginning of a slot.
- ❖ Does not work well if the number of stations contending to send data is high.
- ❖ In such case CSMA scheme works better.

Carrier Sense Multiple Access CSMA

- ❖ Carrier Sense Multiple Access
 - ❖ sense carrier
 - ❖ if idle, send
 - ❖ wait for ack
 - ❖ If there isn't one, assume there was a collision, retransmit
- ❖ Vulnerable period: one t_{prop}

Extension of CSMA

- ❖ The extension of CSMA are the collision detection CSMA/CD and the collision avoidance CSMA/CA techniques.
- ❖ Why CA and CD?
 - ❖ Difficult to detect collisions in a radio environment – why?
 - ❖ A transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission; need a full duplex radio to listen and transmit on same frequency (not true in FDD systems)
 - ❖ Hidden station problem:
 - ❖ Two mutually far away stations A and C want to send to B.
 - ❖ At A and C, channel appears idle
 - ❖ But collision occurs at B

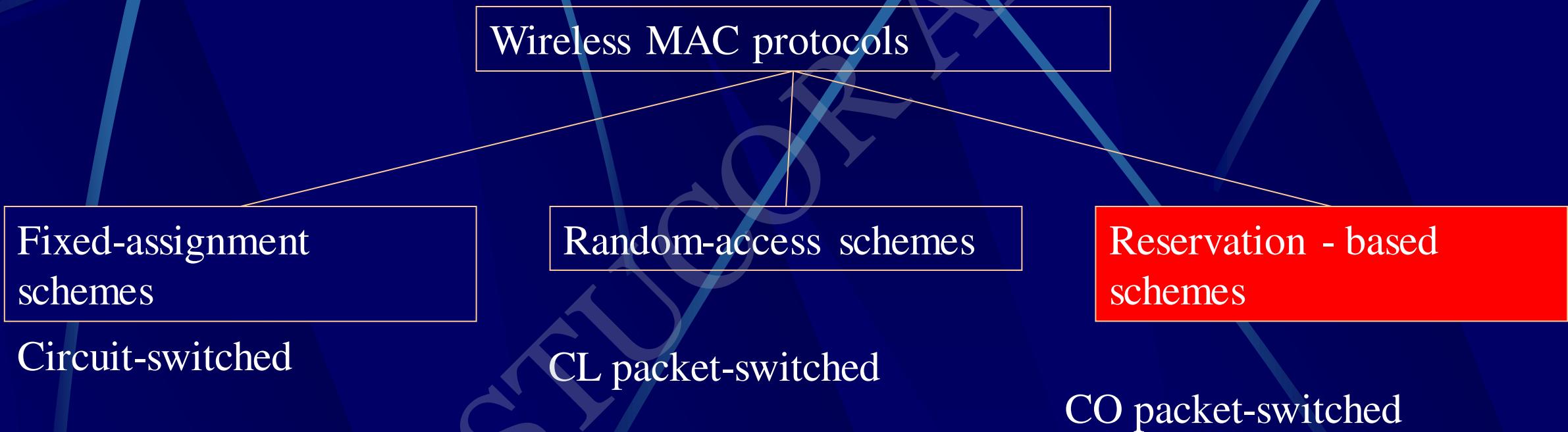
CSMA/CD

- CSMA/CD multi-access control protocol.
 1. Each station listens before it transmits.
 2. If the channel is busy, it waits until the channel goes idle, and then it transmits.
 3. If the channel is idle it transmits immediately. Continue sensing.
 4. If collision is detected, transmit a brief jamming signal, then cease transmission, wait for a random time, and retransmit.
 - collision detection is not by waiting for an ACK

CSMA/CA

- ❖ Prevent collision at the moment they are most likely occur, when bus is released after a packet transmission.
- ❖ During the time a node is transmitting on the channel, several nodes might be wanting to transmit and waiting for it to become free.
- ❖ The moment the transmitting node completes its transmission and would all starts transmitting at the same time.
- ❖ To overcome in the collision avoidance scheme, all nodes are forced to wait for a random time and then sense the medium again before starting their transmission.
- ❖ If the medium is sensed to be busy, further random amount of time and so on.
- ❖ Thus the chance of two nodes starting to transmit at the same time would be greatly reduced.

Classification of wireless MAC protocols



CL – Connection Less. CO – Connection Oriented

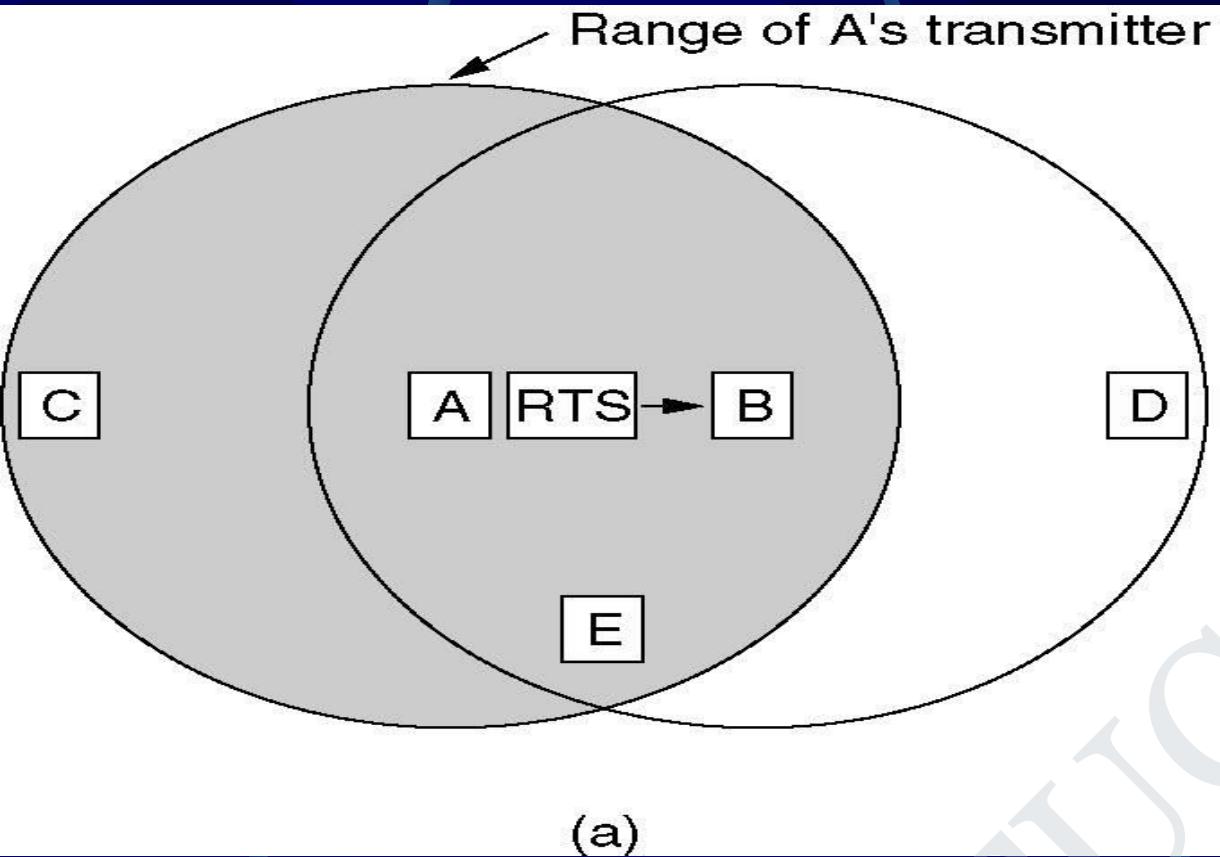
Reservation based schemes

- Basic form of the reservation scheme is RTS/CTS scheme.
- A sender transmits an RTS (Ready to Send) packet to the receiver before the actual data transmission.
- On receiving this the receiver sends CTS (Clear to Send) packet.
- The actual data transfer commences only after that.
- The other nodes sharing the medium sense the CTS packet, they refrain from transmitting until the transmission from the sending node is complete.

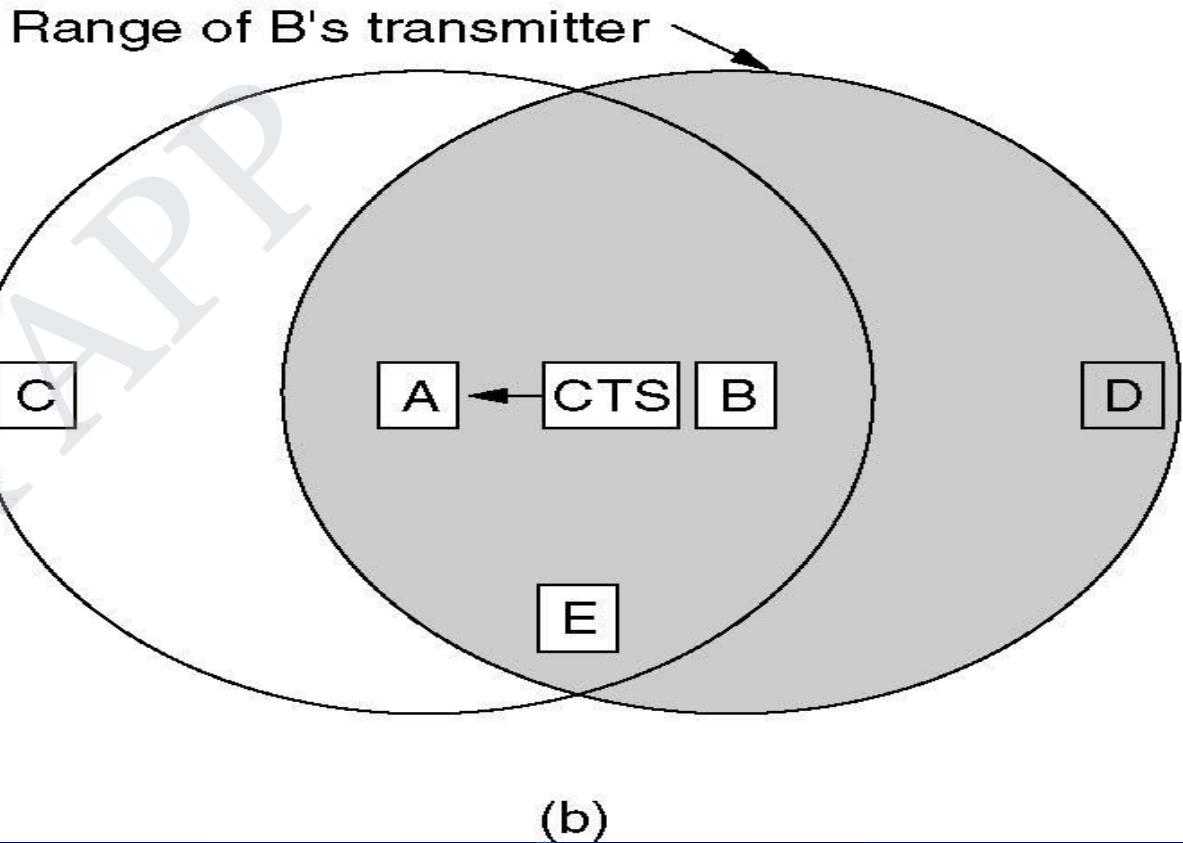
Contention-based protocol

- MACA(Multiple Access Collision Avoidance) Protocol
- MACA solves the hidden/ exposed terminal problems
 - When a node wants to transmit a data packet, it first transmit a **RTS (Request To Send)** frame.
 - The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a **CTS (Clear to Send)** packet.
 - Once the sender receives the CTS packet without any error, it starts transmitting the data packet.
 - If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying.
- The binary exponential back-off mechanism used in MACA might starves flows sometimes. The problem is solved by MACAW.

MACA Protocol



(a)



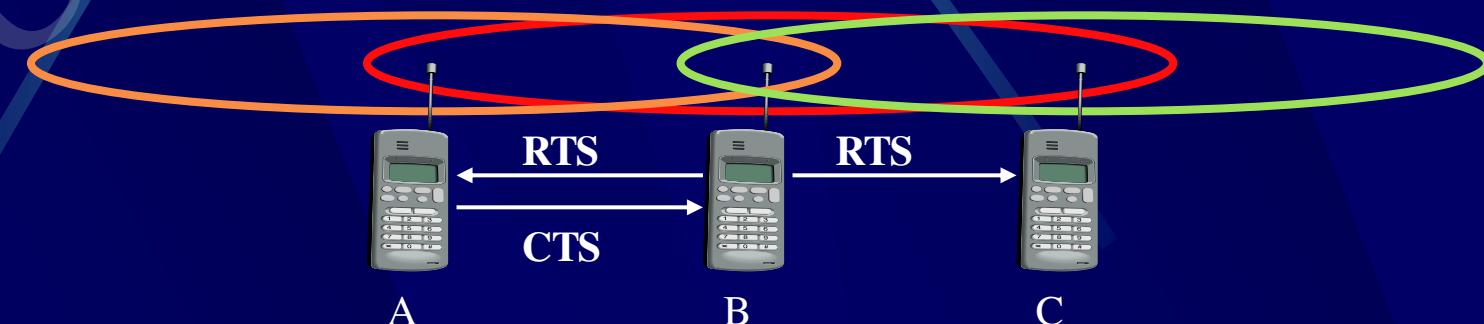
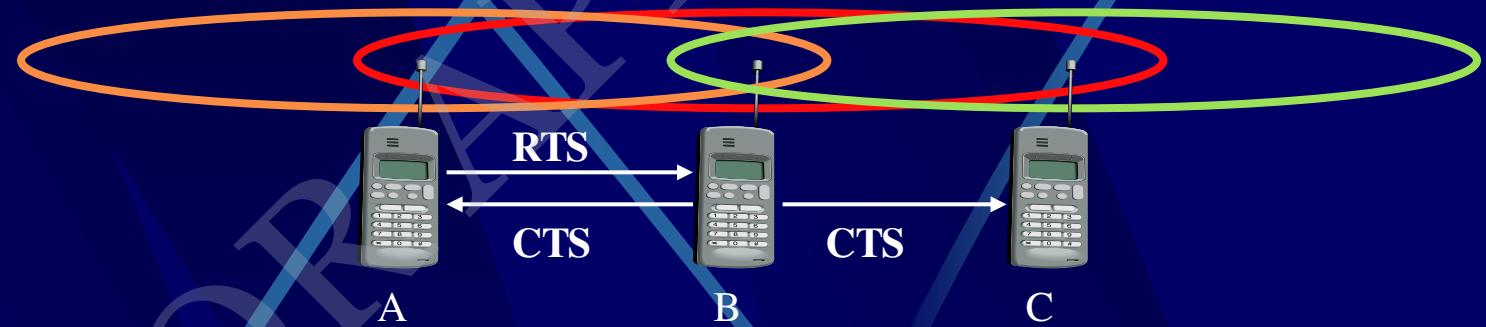
(b)

The MACA protocol.

- A sending an RTS to B.
- B responding with a CTS to A.

MACA examples

- ❖ MACA avoids the problem of hidden terminals
- ❖ A and C want to send to B
- ❖ A sends RTS first
- ❖ C waits after receiving CTS from B
- ❖ MACA avoids the problem of exposed terminals
- ❖ B wants to send to A, C to another terminal
- ❖ now C does not have to wait for it cannot receive CTS from A



References

Book: Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.

Web: http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/vk5/report.html

PPT:

- <http://www.slideshare.net/tapeshchalisgaonkar1/mobile-computing-25723678>
- https://cs.uccs.edu/~chow/pub/master/ycai/mobile_computing_mtu.ppt
- <http://www.slideshare.net/SukumarNayak/snsecurity-architecture-for-mobile-computing-and-iot>

**Thank You
Questions and Comments?**

STUCOR APP

STUCOR APP



UNIT II

MOBILE TELECOMMUNICATION SYSTEM

Introduction to cellular system- GSM – Services & Architecture –Protocol – Connection Establishment –Frequency Allocation – Routing –Mobile Management –Security - GPRS –UMTS –Architecture – Handover - Security

Cellular System

- Cellular Systems for mobile communications implement SDM, Each transmission typically called a base station, Covers a certain area are called cell.
- Cell Radio can vary from tens of meters in building, and hundreds of meter in cities, up to tens of kilometers in the country side.
- Cellular systems implements Space Division Multiplexing Technique (SDM). Each transmitter is called a base station and can cover a fixed area called a cell. This area can vary from few meters to few kilometers.
- Mobile network providers install several thousands of base stations each with a smaller cell instead of using power full transmitters with large cells because

Advantages of cellular systems

Higher capacity

- Smaller the size of the cell more the number of concurrent users i.e. huge cells do not allow for more concurrent users.

Less transmission power

- Huge cells require a greater transmission power than small cells.

Local interference only

- For huge cells there are a number of interfering signals, while for small cells there is limited interference only.

Robustness

- As cellular systems are decentralized, they are more robust against the failure of single components.

Disadvantage cellular systems

Infrastructure needed

- Small cells require a complex infrastructure to connect all base station. The infrastructure required includes switches for call forwarding, location registers etc.

Handover needed

- The mobile station has to perform a handover when changing from one cell to another very frequently.

Frequency planning

- To avoid interference, frequency spectrum should be distributed properly with a very less range of frequency spectrum.

Cellular System Infrastructure

- Early wireless systems had a high-power transmitter, covering the entire service area.
- This required a very huge amount of power and was not suitable for many practical reasons.
- The cellular system replaced a large zone with a number of smaller hexagonal cells with a single BS (base station) covering a fraction of the area.
- Evolution of such a cellular system is shown in the given figures, with all wireless receivers located in a cell being served by a BS.

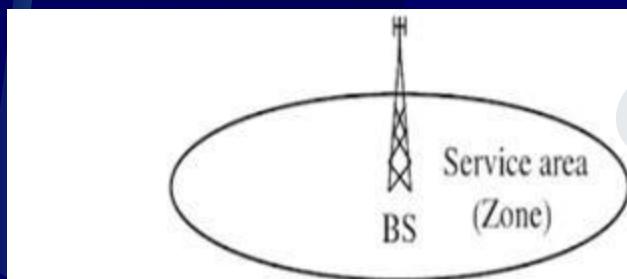


Fig: Early wireless system: large zone

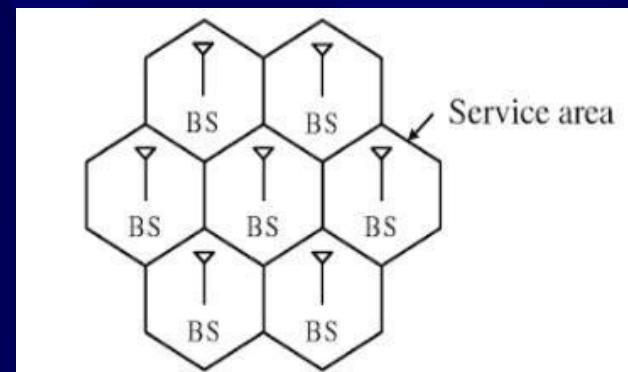
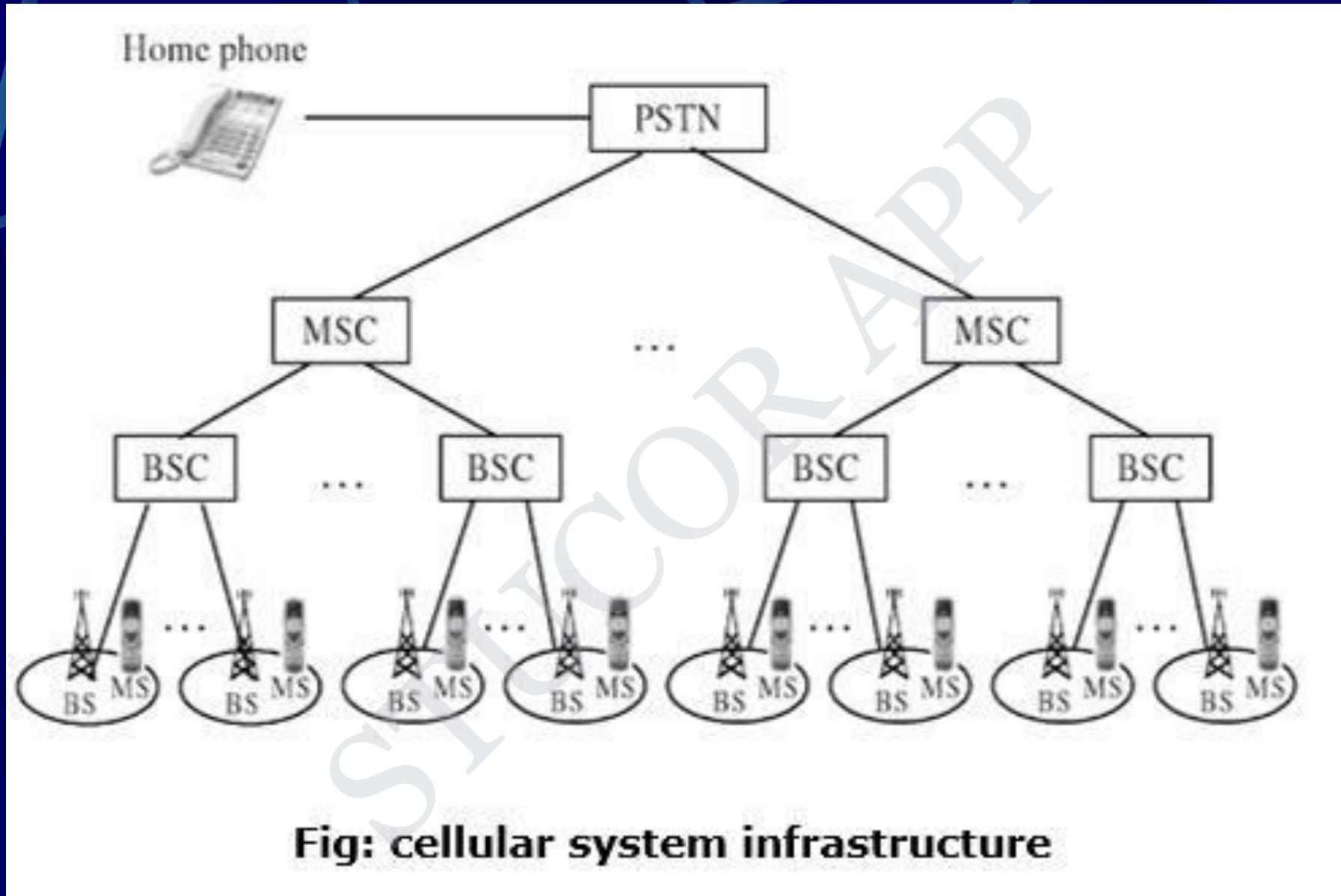


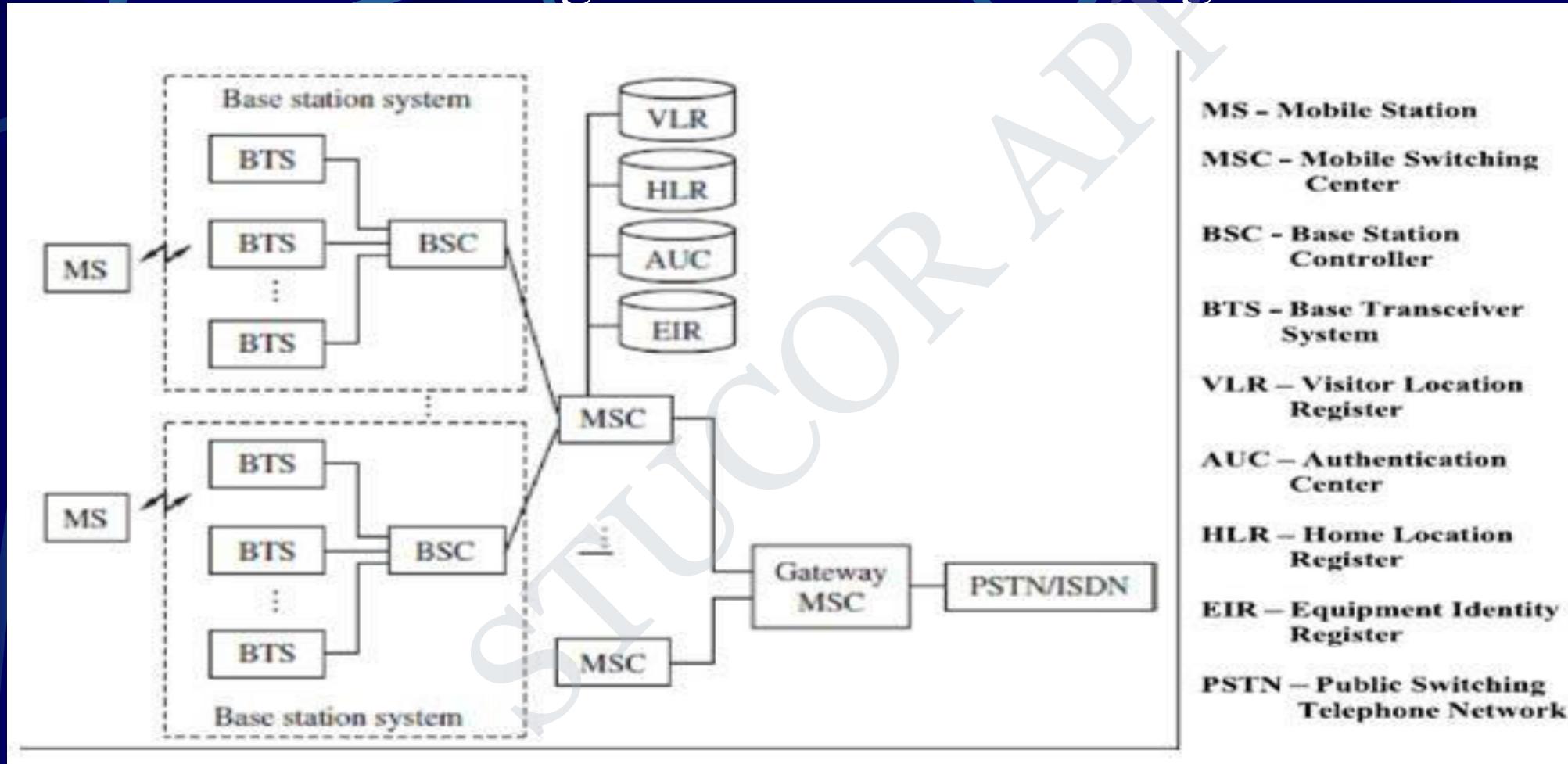
Fig: Cellular system: small zone

- Wireless devices need to be supported for different types of services, the wireless device could be a wireless telephone laptop with wireless card, personal digital assistant (PDA), or web enabled phone. For simplicity, it could be called an MS.
- In a cellular structure, a MS (mobile station) needs to communicate with the BS of the cell where the MS is currently located and the BS acts as a gateway to the rest of the world.
- Therefore, to provide a link, the MS needs to be in the area of one of the cells (and hence a BS) so that mobility of the MS can be supported.

- Several base stations are connected through hard-wires and are controlled by a BS controller (BSC), which in turn is connected to a mobile switching center (MSC).
- Several mobile switching centers are interconnected to a PSTN (public switched telephone network) and the ATM (asynchronous transfer mode) backbone.
- To provide a better perspective of wireless communication technology, simplified system infrastructure for cellular system is shown in the figure:



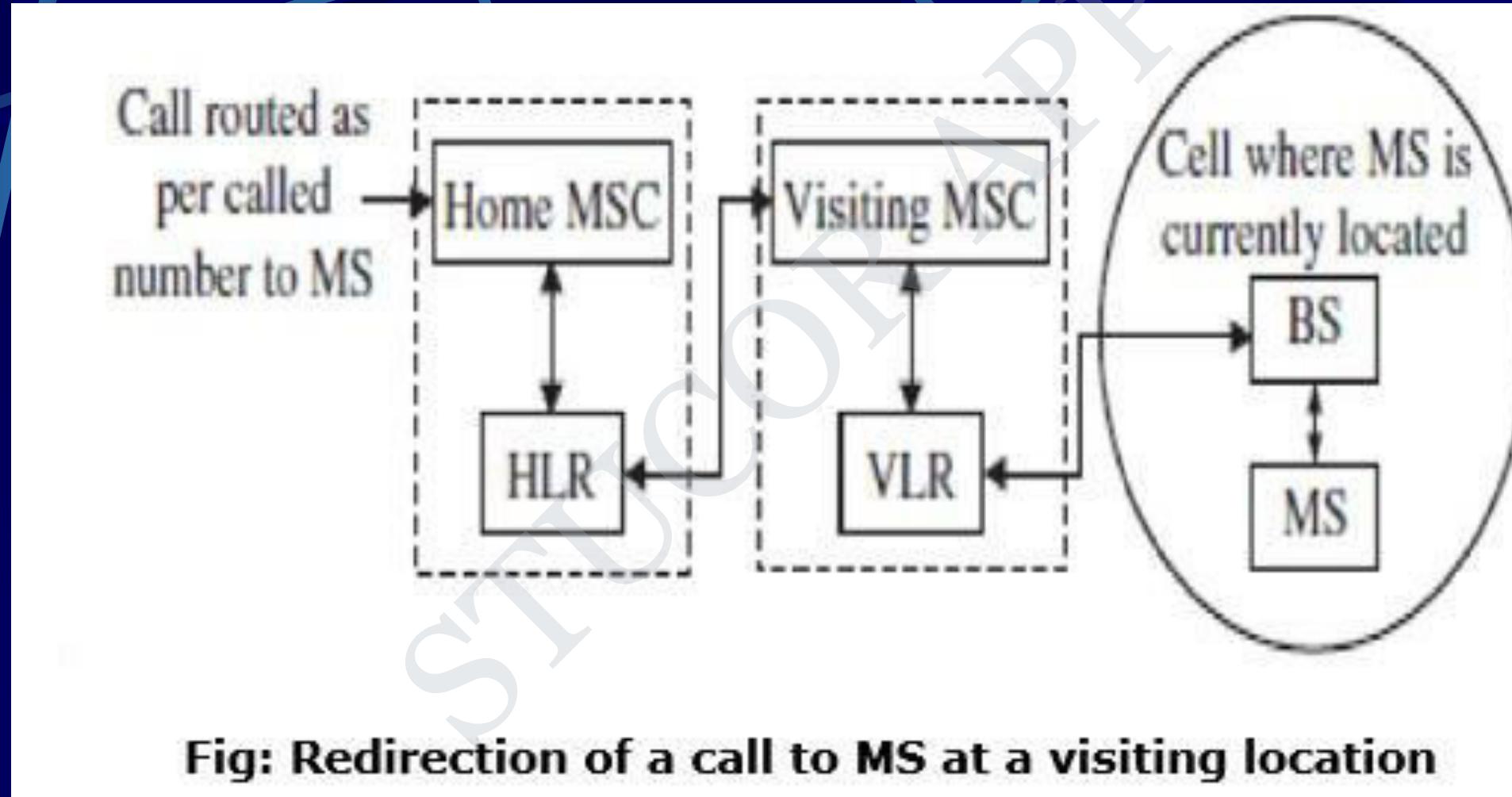
A cellular system requires a fairly complex infrastructure. A generic block diagram is shown in the figure:



- A BS consists of a base transceiver system (BTS) and a BSC. Both tower and antenna are a part of the BTS, while all associated electronics are contained in the BSC.
- The HLR (home location register) and VLR (visitor location register) are two sets of pointers that support mobility and enable the use of the same telephone numbers worldwide.
- The AUC (authentication center) unit provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each cell.

- The EIR (equipment identity register) is a database that information about identity of mobile equipment. Both AUC and EIR can be implemented as individual stand-alone units or as a combined AUC/EIR unit.
- The HLR is located at the MSC where MS is initially registered and is the initial home location for billing and access information.
- In simple words, any incoming call, based on the calling number, is directed to the HLR of the home MS where the MS is registered. The HLR then points to the VLR of the MSC where the MS is currently located.

Bidirectional HLR-VLR pointers help in carrying out various functionalities, as illustrated in the figure:



- The VLR contains information about all MS visiting that particular MSC and hence points to the HLR of the visiting MSs for exchanging related information about the MS.
- Such a pointer allows calls to be routed or rerouted to the MS, wherever it is located.
- In cellular systems, a reverse direction pointer is needed that allows traversal of many control signals back and forth between the HLR and VLR such bidirectional HLR-VLR pointers help in carrying out various functionalities.

GSM – GLOBAL SYSTEM FOR MOBILE COMMUNICATION

STUCOR APP

STUCOR APP

GSM SERVICE

GSM provides three categories of services.

- I. Bearer service
- II. Teleservices
- III. Supplementary services

Bearer Services

- Bearer Services or Data services are used through a GSM phone to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer.
- GSM currently has a data transfer rate of 9.6k.
- New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

Teleservices

The abilities of a Bearer Service are used by a teleservice to transport data. These services are further transited in the following ways:

- ***Voice Calls***

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps

- ***Emergency calls***

where the nearest emergency-service provider is notified by dialing three digits.

•*Short Text Messages*

SMS service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone.

In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

•*Facsimile or Fax:* Using modem fax data is transmitted as digital data over the analog telephone network.

Supplementary services

- Supplementary services are additional services that are provided in addition to teleservices and bearer services.
- These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls

Building Blocks

- AMPS – Advanced Mobile Phone System
- TACS – Total Access Communication System
- NMT – Nordic Mobile Telephone System

Building Blocks

contd.

AMPS – Advanced Mobile Phone System

- analog technology
- used in North and South America and approximately 35 other countries
- operates in the 800 MHz band using FDMA technology

Building Blocks contd.

TACS – Total Access Communication System

- variant of AMPS
- deployed in a number of countries
- primarily in the UK

Building Blocks

contd.

NMT – Nordic Mobile Telephone System

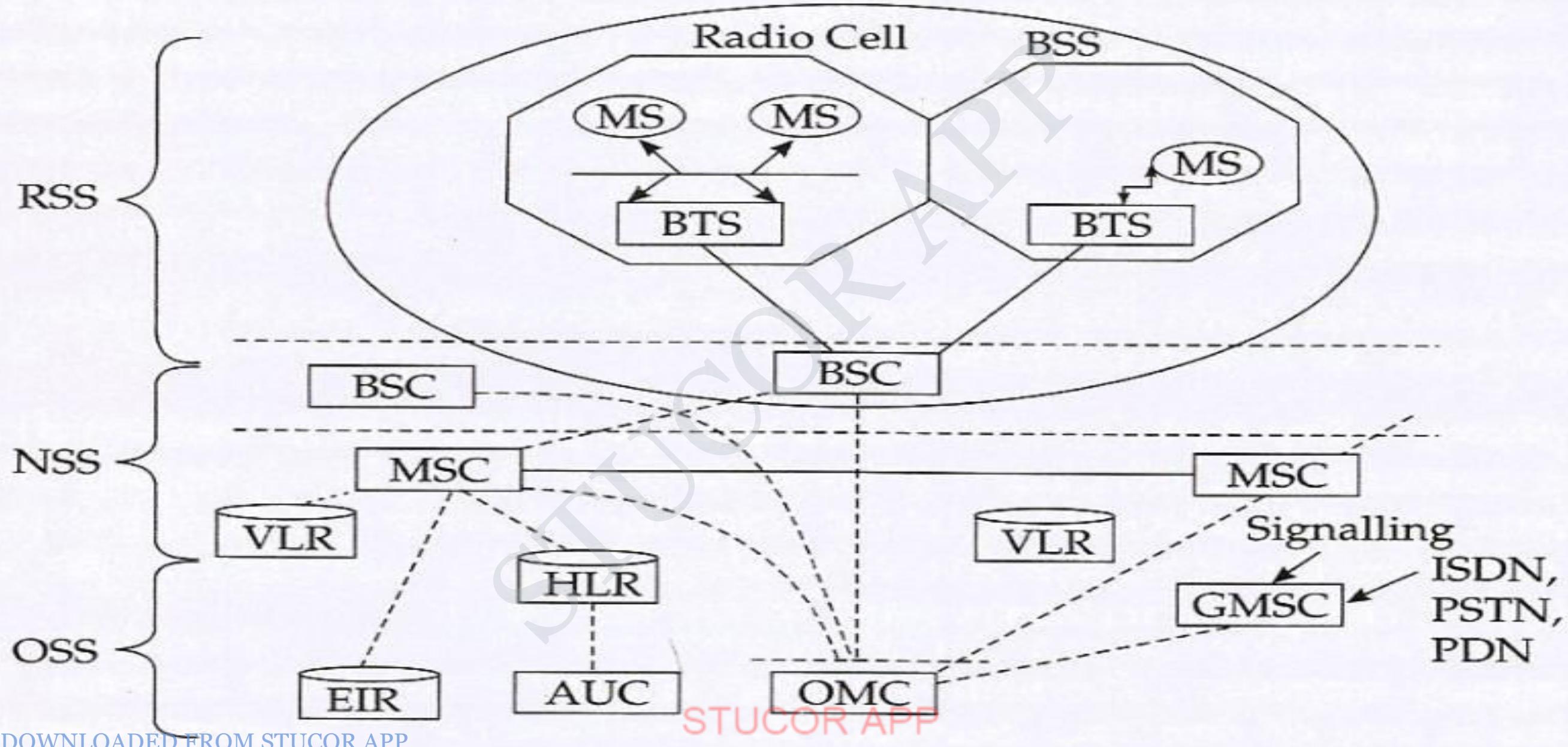
- analog technology
- deployed in the Benelux countries and Russia
- operates in the 450 and 900 MHz band
- first technology to offer international roaming – only within the Nordic countries

System Architecture of GSM

The GSM System architecture consists of three major interconnected subsystems. The three main subsystems are

- I. Radio Subsystem (RSS)
- II. Networking and switching subsystem(NSS)
- III. Operation Subsystem (OSS)

Functional architecture of a GSM system



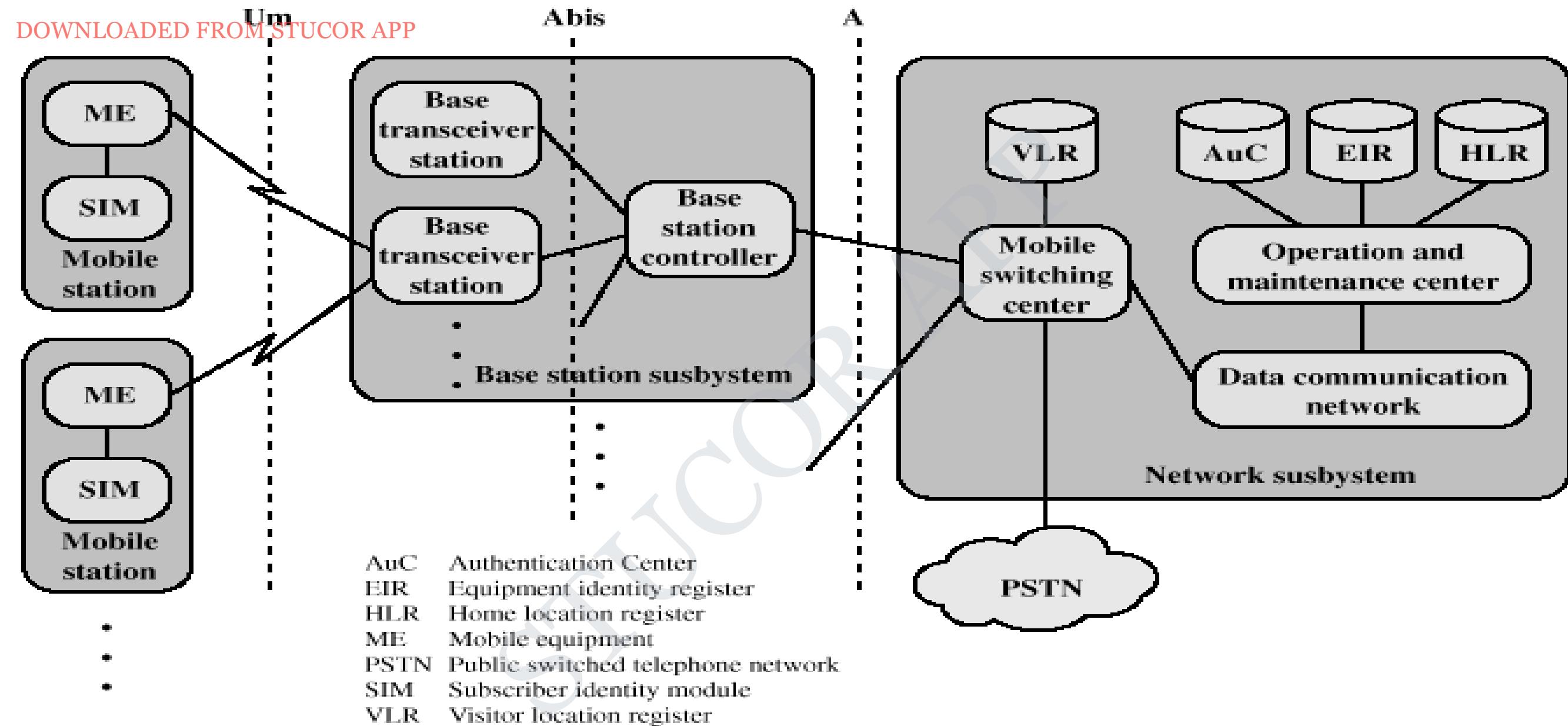
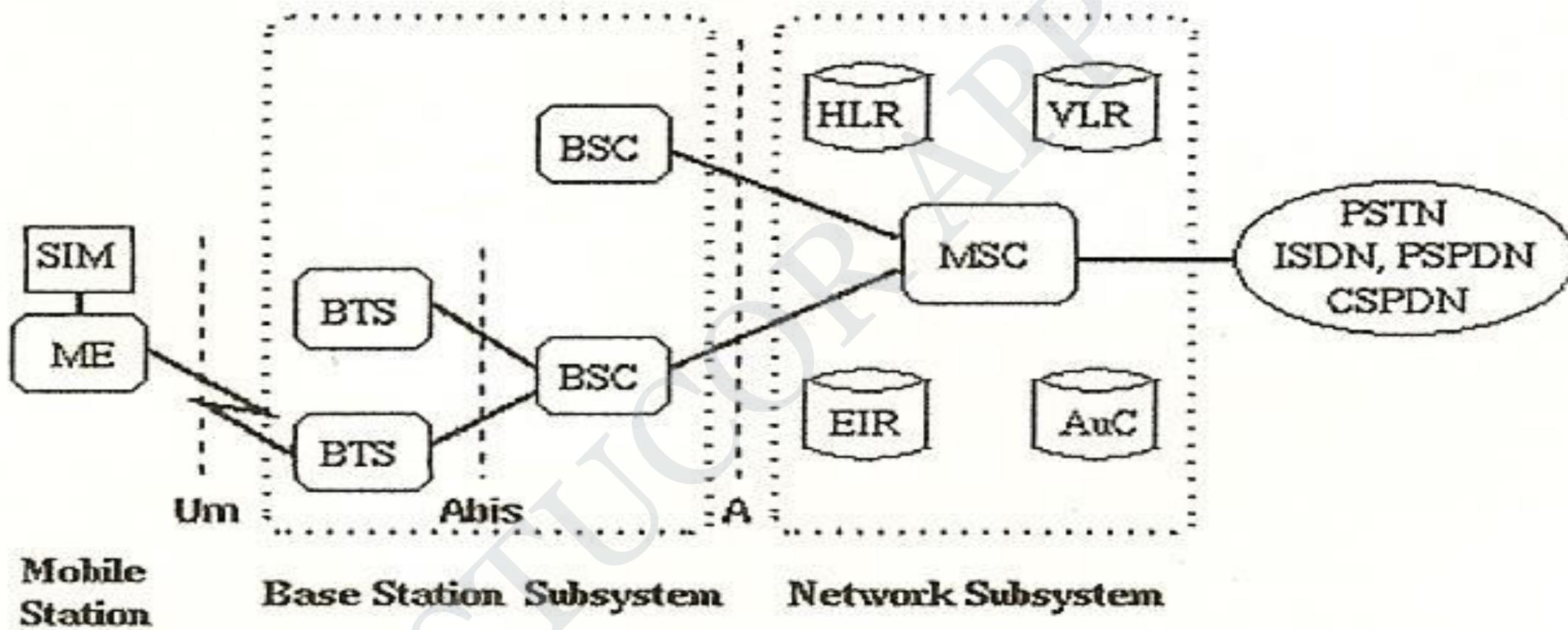


Figure 10.14 Overall GSM Architecture

System Architecture



SIM Subscriber Identity Module

ME Mobile Equipment

BTS Base Transceiver Station

BSC Base Station Controller

HLR Home Location Register

VLR Visitor Location Register

MSC Mobile services Switching Center

EIR Equipment Identity Register

AuC Authentication Center

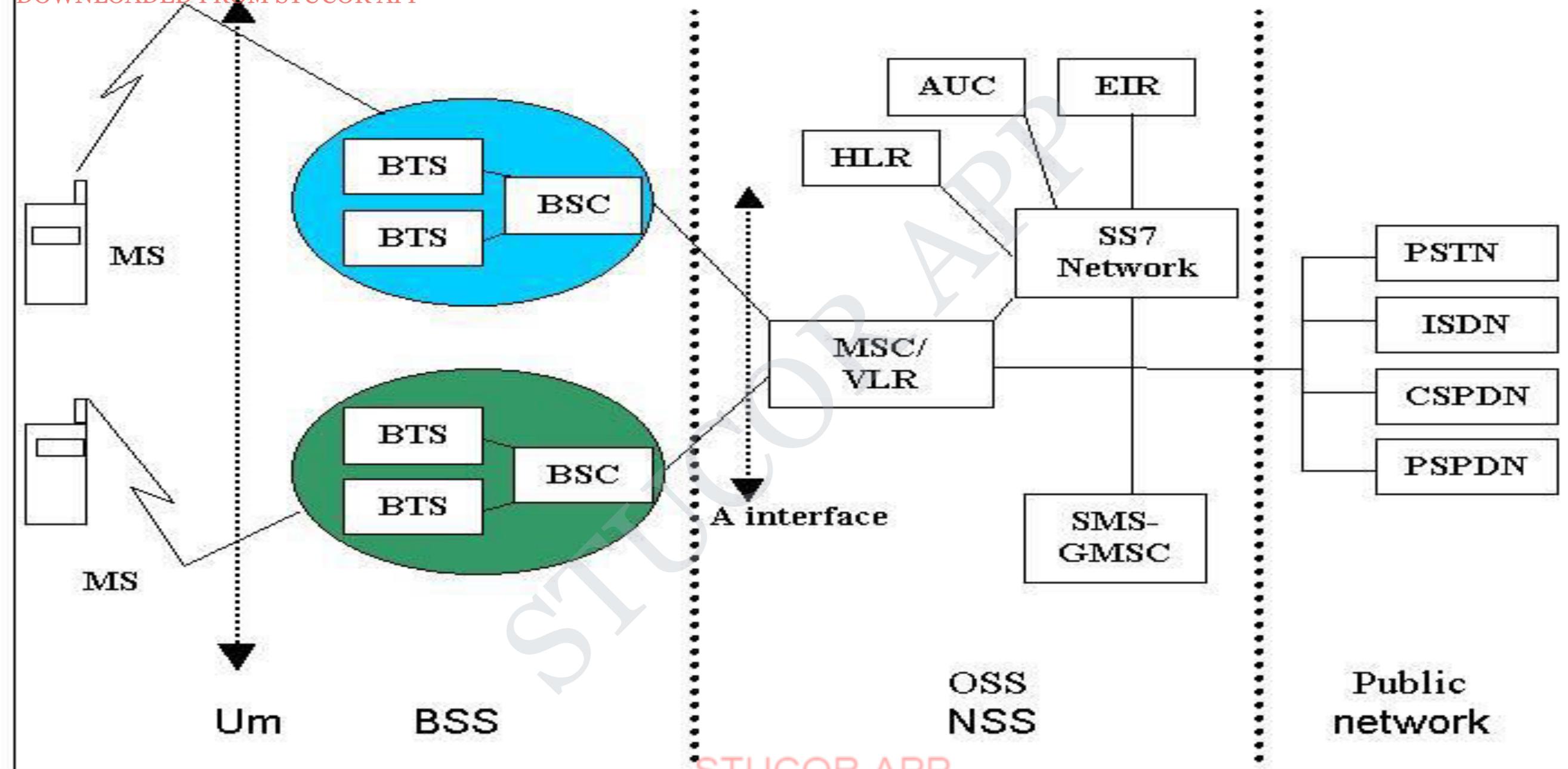
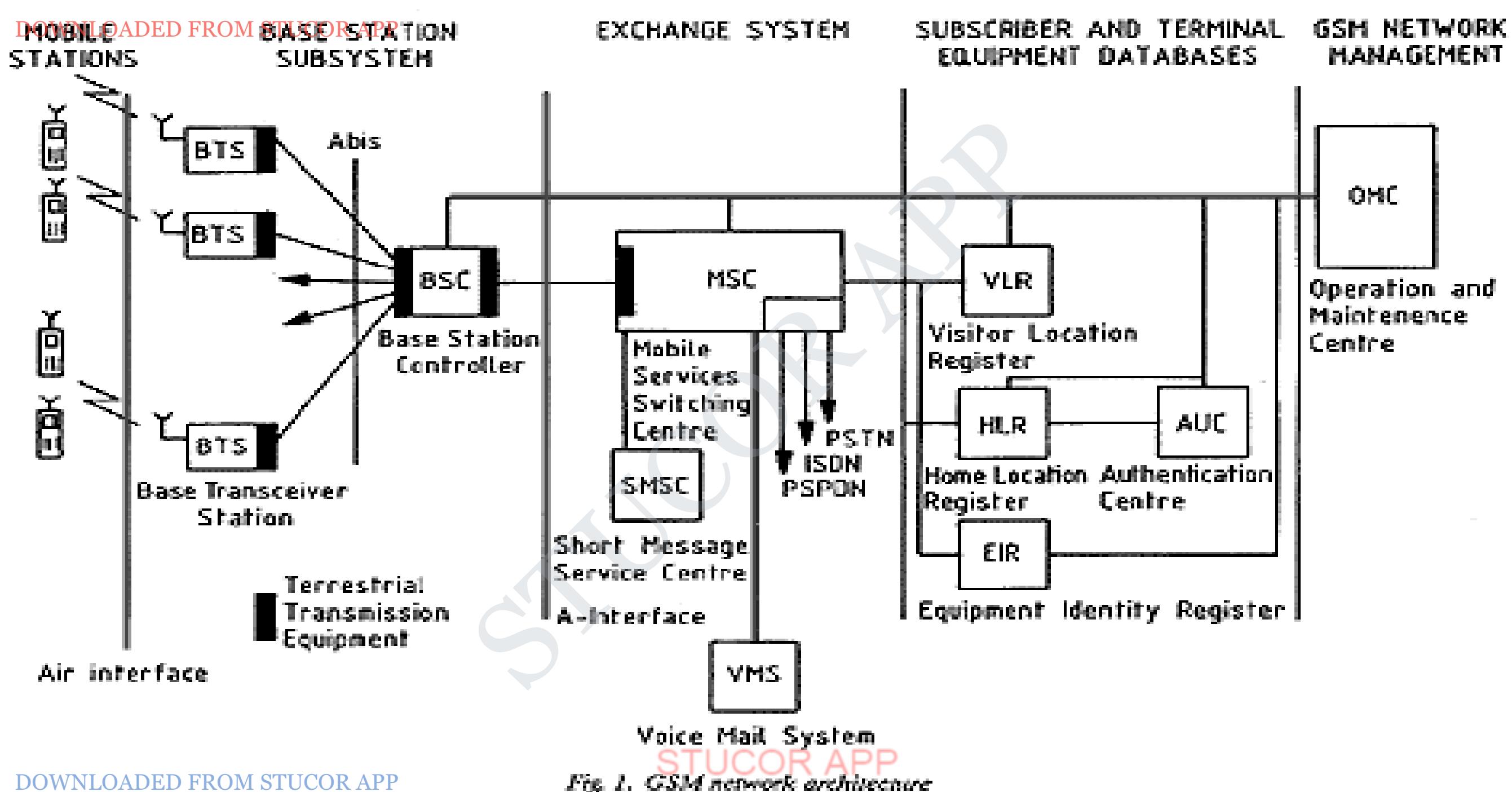


Figure 1: GSM System Architecture.



Radio Subsystem (RSS)

This subsystem comprises all the radio specific entities.

1. Mobile Station (MS)
2. Base Station Subsystem(BSS)

The Mobile Station is made up of two entities:

- I. Mobile Equipment (ME)
- II. Subscriber Identity Module (SIM)

Mobile Equipment

- Produced by many different manufacturers
- Must obtain approval from the standardization body
- Uniquely identified by an IMEI (International Mobile Equipment Identity)

Subscriber Identity Module (SIM)

- Smart card containing the International Mobile Subscriber Identity (IMSI)
- Allows user to send and receive calls and receive other subscribed services
- Encoded network identification details
- Protected by a password or PIN
- Can be moved from phone to phone – contains key information to activate the phone

Base Station Subsystem (BSS)

Base Station Subsystem is composed of two parts that communicate across the standardized Abis interface allowing operation between components made by different suppliers

1. Base Transceiver Station (BTS)
2. Base Station Controller (BSC)

Base Transceiver Station (BTS)

- A BTS comprises all radio equipment such as antenna, signal processors and amplifiers that are necessary for radio transmission.
- It encodes the received signal, modulates it on a carrier wave and feeds the RF signals to the antenna.
- It communicates with both the mobile station and the BSC

Base Station Controller (BSC)

- Manages Resources for BTS
- It assigns frequency and time slot for and MS for call set up
- It manages the handoff from one BTS to another within the BSS.
- BSC multiplexes the radio channel onto the fixed network connection to the Mobile Switching Centre.

Network and Switching Subsystem(NSS)

It is the heart of the GSM system. It connects the wireless networks to the standard public networks. It carries out usage based charging, accounting and also handles roaming.

Mobile Switching Center (MSC)

- Heart of the network
- Switch speech and data connections between:
 - Base Station Controllers
 - Mobile Switching Centers
 - GSM-networks
 - Other external networks
- Three main jobs:
 - 1) connects calls from sender to receiver
 - 2) collects details of the calls made and received
 - 3) supervises operation of the rest of the network components

Home Location Registers (HLR)

- contains administrative information of each subscriber
- IMSI and current location of the mobile

Visitor Location Registers (VLR)

- A temporary database that is updated whenever a new MS enters its area by roaming.
- contains selected administrative information from the HLR
- authenticates the user
- tracks which customers have the phone on and ready to receive a call
- periodically updates the database on which phones are turned on and ready to receive calls

Operation subsystem (OSS)

The operation subsystem contains all the function necessary for network operation and maintenance.

Authentication Center (AUC)

- mainly used for security
- data storage location and functional part of the network
- Ki is the primary element

Equipment Identity Register (EIR)

- Database that is used to track handsets using the IMEI (International Mobile Equipment Identity)
- Made up of three sub-classes: The White List, The Black List and the Gray List
- Optional database

GSM Security

Security in GSM is broadly supported at three levels: Operator level, Customer's level and System level. These three levels help oversee aspects such as correct billing, avoiding fraud, protecting services and ensuring anonymity.

Authentication

- Protect the network against unauthorized use.
- Denying the possibility for intruders to impersonate authorized users.
- GSM network operator verify the identity , making it highly improbable to clone someone's mobile phone identity.
- Authentication can be achieved in a simple way by using a password such as PIN.

Confidentiality

- GSM network protects voice, data and sensitive information against eavesdropping on the radio path.
- It is achieved by using encryption techniques by GSM designers.
- Data on the radio path is encrypted between the ME and BTS against eavesdropping.

Anonymity

- GSM protects against someone tracking the location of a user or identifying calls made to the user by eavesdropping on the radio path.
- It is achieved by allocating Temporary Mobile Subscriber Identity (TMSIs) instead of permanent identities.

Advantages of GSM

- Crisper, cleaner quieter calls
- Security against fraud and eavesdropping
- International roaming capability in over 100 countries
- Improved battery life
- Efficient network design for less expensive system expansion
- Efficient use of spectrum
- Advanced features such as short messaging and caller ID
- A wide variety of handsets and accessories
- High stability mobile fax and data at up to 9600 baud
- Ease of use with over the air activation, and all account information is held in a smart card which can be moved from handset to handset

General Packet Radio Service GPRS

GPRS when integrated with GSM significantly improves and simplifies Internet access.

- GPRS is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications (GSM).
- GPRS was originally standardized by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies.
- It is now maintained by the 3rd Generation Partnership Project (3GPP).
- GPRS usage is typically charged based on volume of data transferred, contrasting with circuit switched data, which is usually billed per minute of connection time.

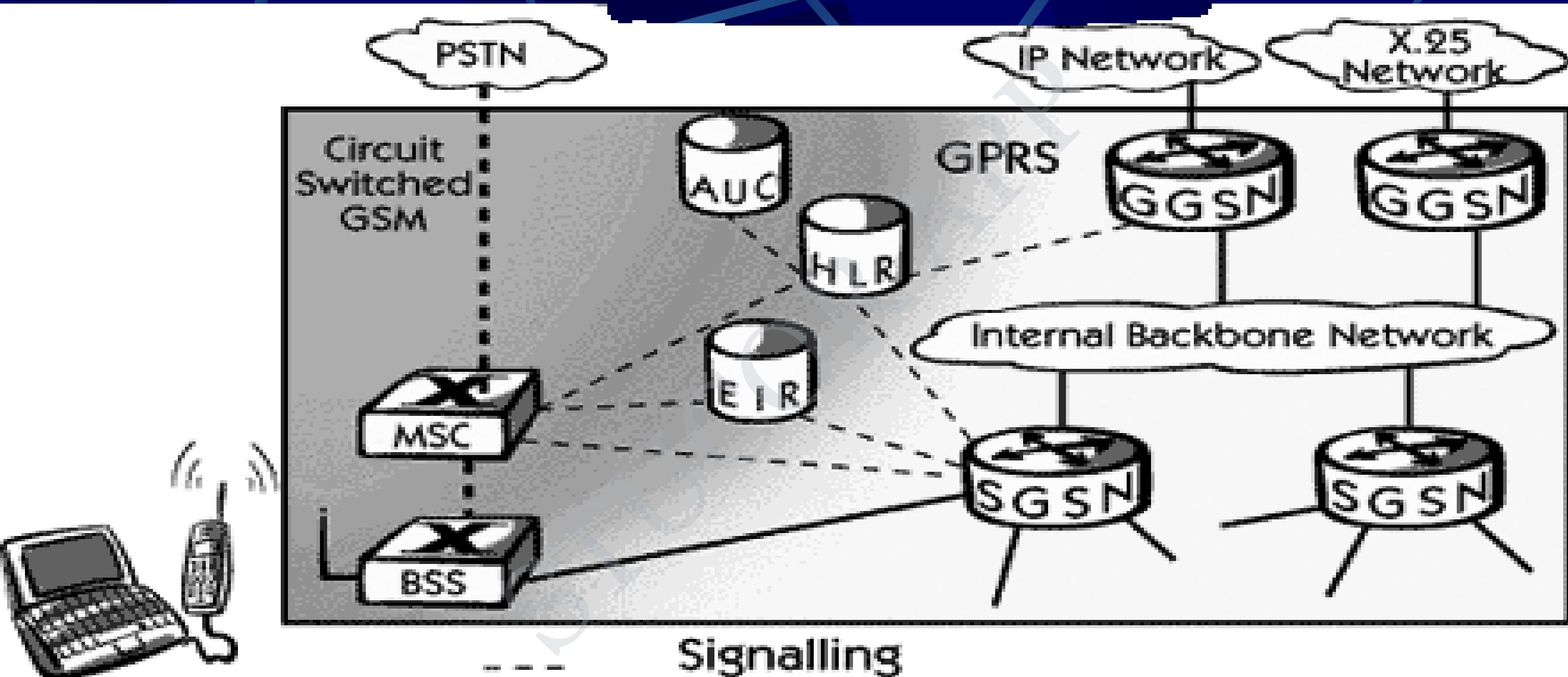
GPRS Services

GPRS offers end-to-end packet-switched data transfer services which can be categorized

- I. Point-to-point (PTP) services
- II. Point-to-Multipoint (PTM) services

- I. Point-to-point (PTP) service is between two users and can either be connectionless or connection-oriented.
- II. Point-to-Multipoint (PTM) services is data transfer from one user to multiple users. The two types of PTM services.
 - I. One is multicast PTM where the data packets are broadcast in a certain area and
 - II. The other is group PTM where the data packets are addressed to a group of users

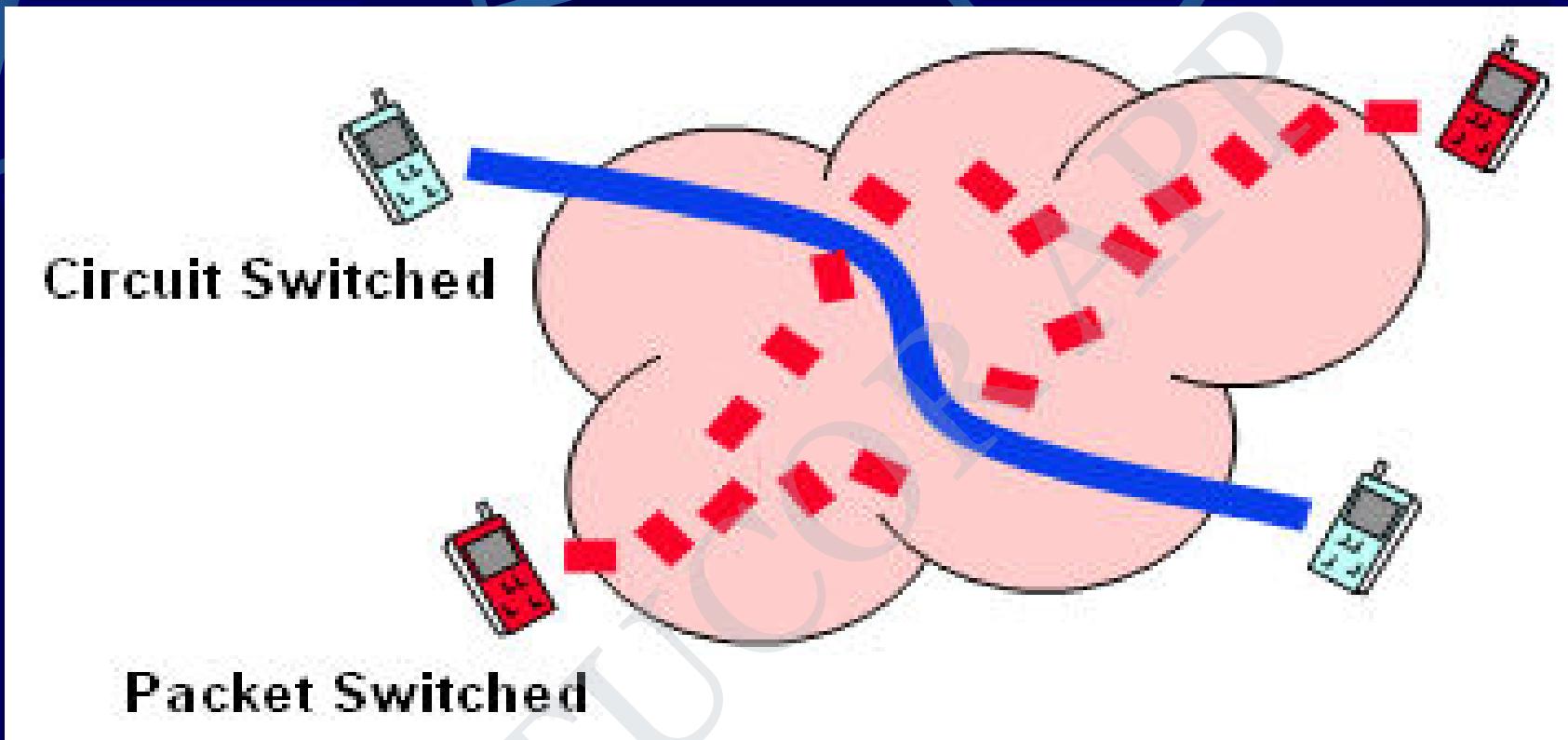
GPRS Architecture

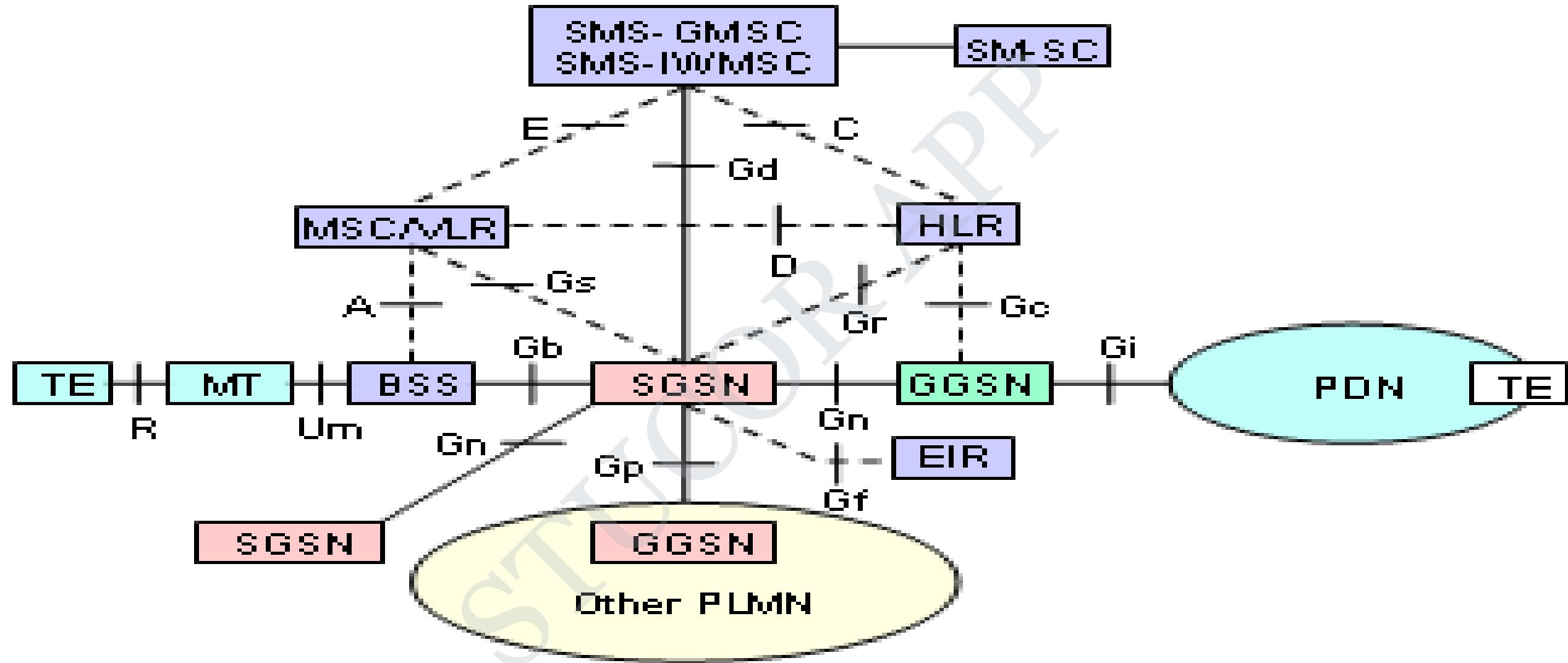


STUCOR APP
Signalling
Circuit Switched GSM
Packet Switched Data and Signalling

Modification or Upgrade Required for GPRS.

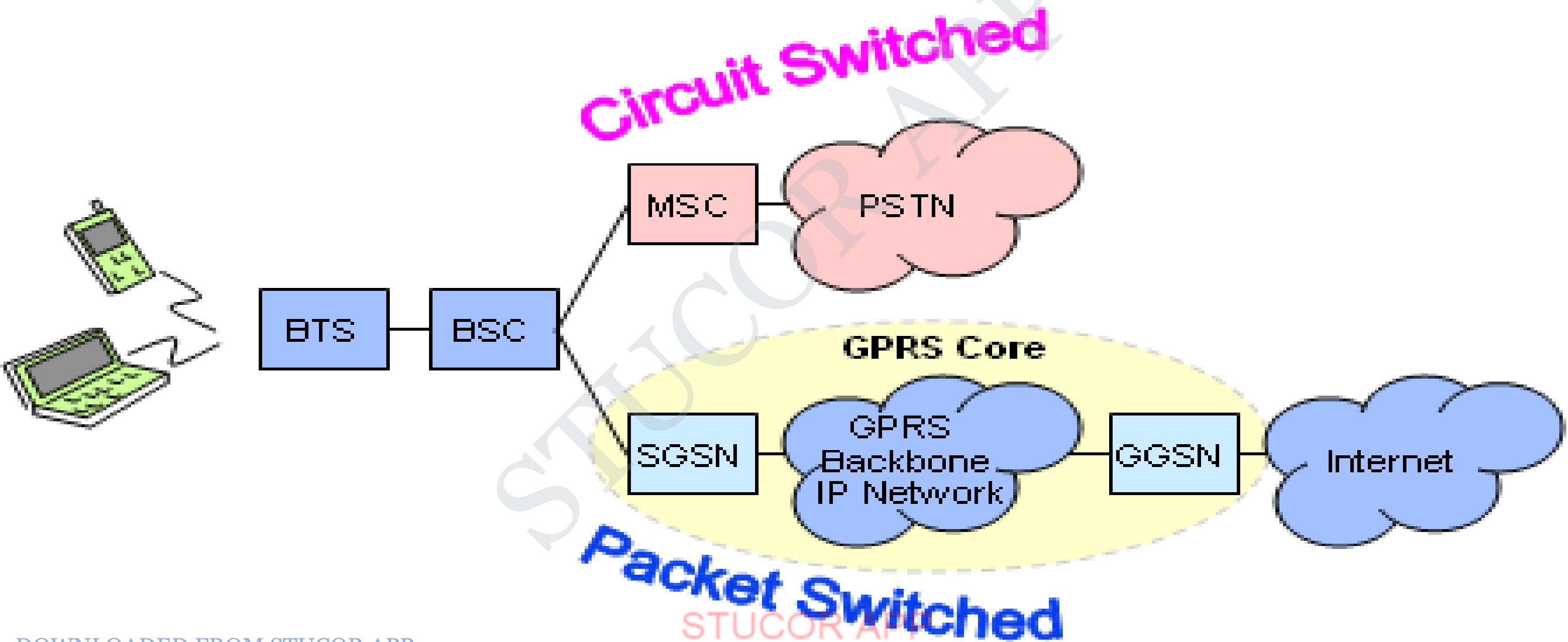
GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing base transceiver site.
BSC	The base station controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.





----- Signalling Interface

— — — Signalling and Data Transfer Interface



Universal Mobile Telephone System (UMTS)

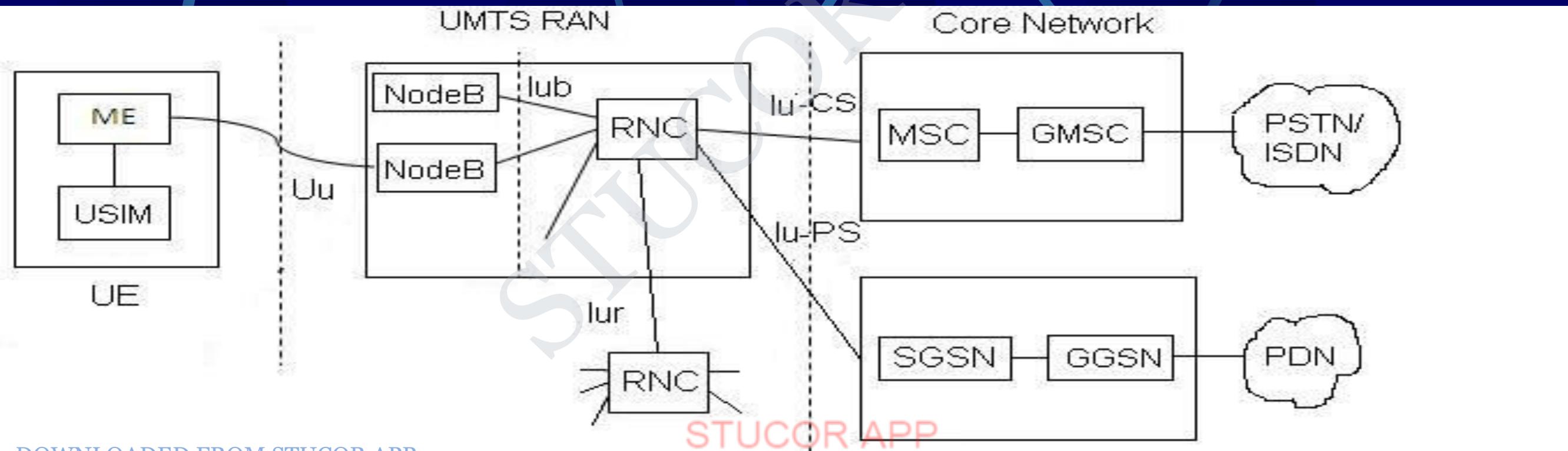
- Reasons for innovations
 - new service requirements
 - availability of new radio bands
- User demands
 - seamless Internet-Intranet access
 - wide range of available services
 - compact, lightweight and affordable terminals
 - simple terminal operation
 - open, understandable pricing structures for the whole spectrum of available services

- The UMTS was developed mainly for countries with GSM networks and it is compatible with GSMAll
- All GSM networks will be upgraded to UMTS
- The UMTS network is different from the 2G networks in the following respects.
 - ❖ ***Higher speech quality***: In addition to speech traffic, it supports advanced data and information service – true multimedia network
 - ❖ ***Higher data rate***: The UMTS support 2 Mbps data rate much higher than 2G
 - ❖ ***Virtual home environment***: A user roaming from his network to other UMTS network will not feel any discontinuity or service difference – giving the feeling of being in the home network. In 2G a user registered to a visitor location and is also charged a roaming overheads.

UMTS Network Architecture

The UMTS network architecture is divided into three main elements

- I. User Equipment (UE),
- II. Radio Network Subsystem(RAN)
- III. Core Network



User Equipment (UE)

- ❖ UE incorporates greater functionality
- ❖ compared to a cell phone.
- ❖ It can be thought of as both a mobile phone used for talking and a data terminal attached to a computer with no voice capability.

Radio Network Subsystem(RAN)

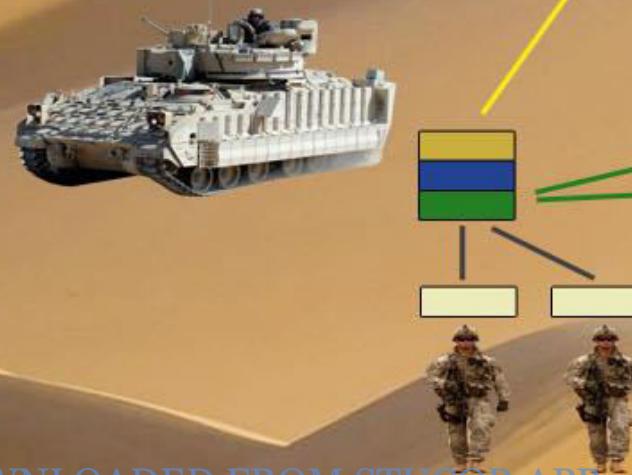
- ❖ The RNS is the equivalent of BSS in GSM.
- ❖ It provides and manages the wireless interface for the overall network.

Core Network

- ❖ The Core network is the equivalent of the GSM Network Switching Subsystem(NSS)

References

- Book: Prasant Kumar Patnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.
- cse.yeditepe.edu.tr/~sbaydere/courses_new/cse402/files/GSM.ppt
- www.harding.edu/white/classes_old/engr475/.../lecture_12_gsm.ppt



IT6601 MOBILE COMPUTING

Unit III



UNIT III MOBILE NETWORKS LAYER

Mobiel IP – DHCP -Ad-Hoc –Proactive Protocol –DSDV -, Reactive Routing Protocols – DSR, AODV, Hybrid Routing –ZRP, Multicast Routing- Vehicular Ad Hoc networks (VANET) – MANET Vs VANET – Security

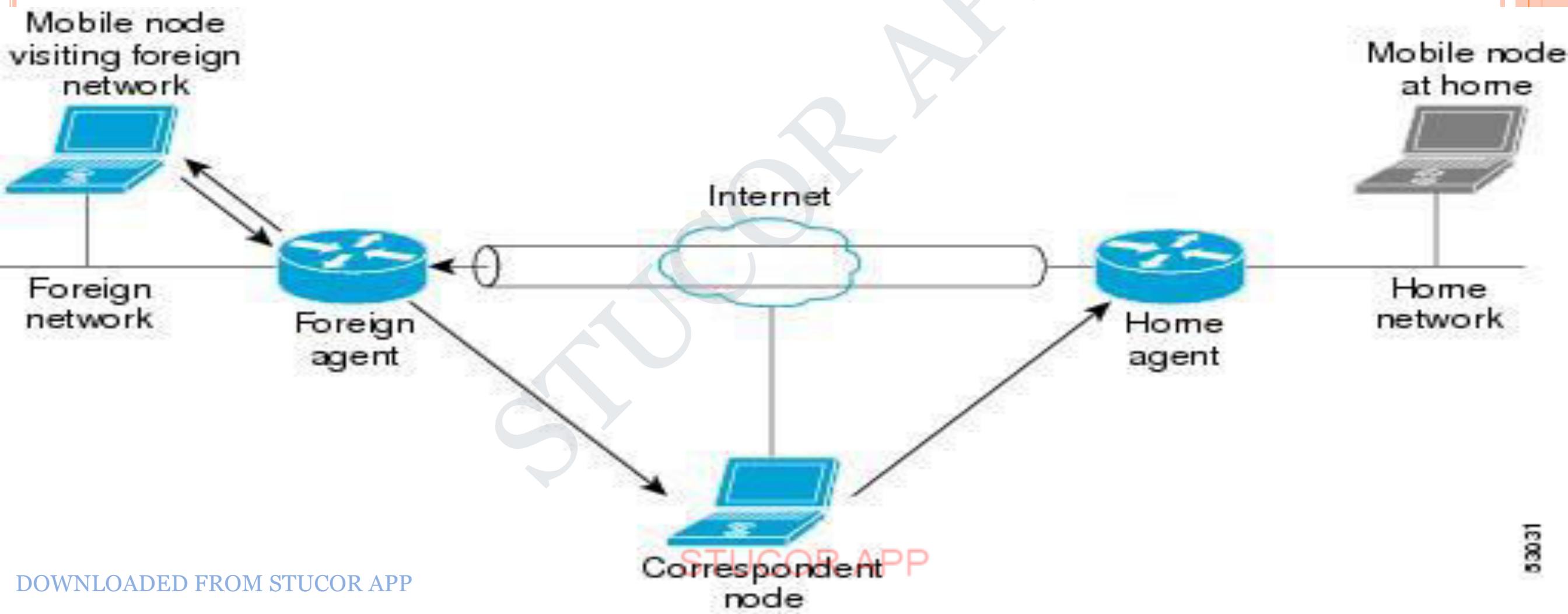
WIRELESS NETWORKS

- **Need:** Access computing and communication services, **on the move**
- Infrastructure-based Networks
 - traditional cellular systems (base station infrastructure)
- Wireless LANs
 - Infrared (IrDA) or radio links (Wavelan)
 - very flexible within the reception area; ad-hoc networks possible
 - low bandwidth compared to wired networks (1-10 Mbit/s)
- Ad hoc Networks
 - useful when infrastructure not available, impractical, or expensive
 - military applications, rescue, home networking

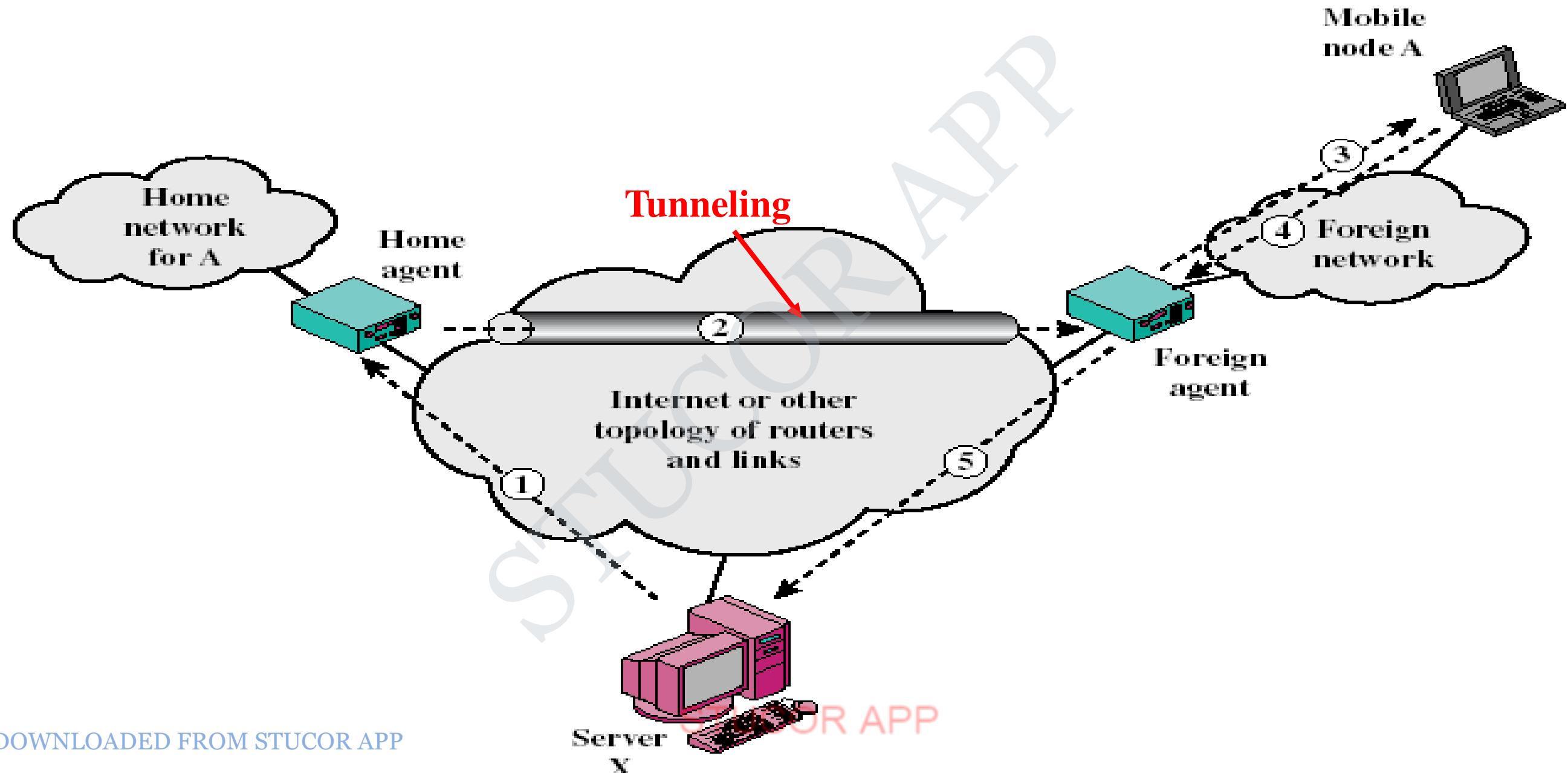


MOBILE IP

- Mobile IP enables an IP node to retain the same IP address and maintain existing communications while traveling from one link to another.



Mobile IP



MOBILE IP COMPONENTS

- ❑ Mobile node (MN)
- ❑ Home agent (HA)
- ❑ Foreign agent (FA)
- ❑ Correspondent Node (CN)

MOBILE NODE (MN)

The Mobile Node is a device such as

- a cell phone,
- personal digital assistant,
- or laptop

whose software enables network roaming capabilities.

HOME AGENT (HA)

- Home Agent is a router on the home network serving as the anchor point for communication with the Mobile Node;
- it tunnels packets from a device on the Internet, called a Correspondent Node, to the roaming Mobile Node.

(A tunnel is established between the Home Agent and a reachable point for the Mobile Node in the foreign network.)

FOREIGN AGENT (FA)

- The Foreign Agent is a router that may function as the point of attachment for the Mobile Node when it roams to a foreign network, delivering packets from the Home Agent to the Mobile Node.

CORRESPONDENT NODE (CN)

- End host to which MN is corresponding (eg. a web server)

The Mobile IP process has three main phases
the following sections.

❖ Agent Discovery

A Mobile Node discovers its Foreign and Home Agents during agent discovery.

❖ Registration

The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.

❖ Tunneling

A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

TWO IP ADDRESSES FOR MOBILE NODE

- Home address:** static
- Care-of address:** topologically significant address

The care-of address is the termination point of the tunnel toward the Mobile Node when it is on a foreign network. The Home Agent maintains an association between the home IP address of the Mobile Node and its care-of address, which is the current location of the Mobile Node on the foreign or visited network

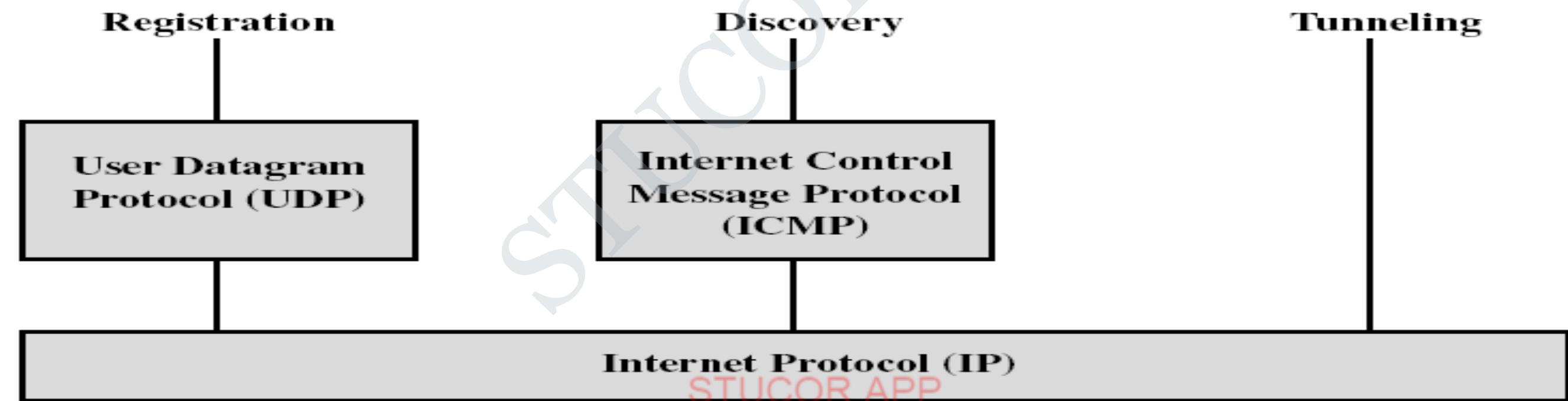
FEATURES OF MOBILE IP

- ❑ Transparency : IP address should not be any effect of mobility on any ongoing communication
- ❑ Compatibility: It should compatible with existing Internet protocols.
- ❑ Security: It should provide users with secure communication over internet.
- ❑ Efficiency : It should neither result in large number of message nor should it incur too much computational overheads
- ❑ Scalability: It should also be scalable to support billions of moving hosts worldwide.

KEY MECHANISM IN MOBILE IP

Three basic mechanisms

1. **Discovering** the care-of address
2. **Registering** the care-of address
3. **Tunneling** to the care-of address

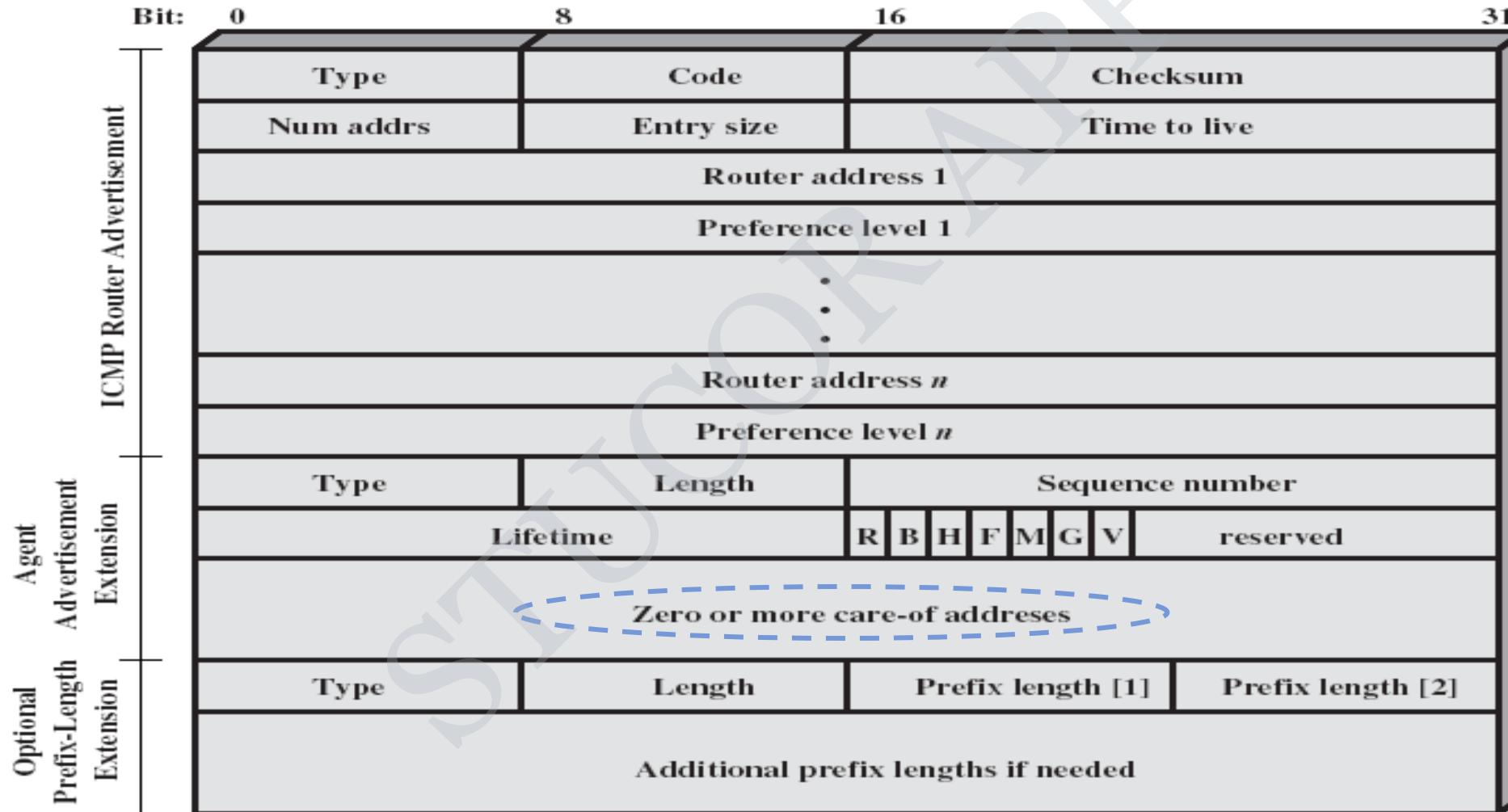


1. Discovery of care-of-address

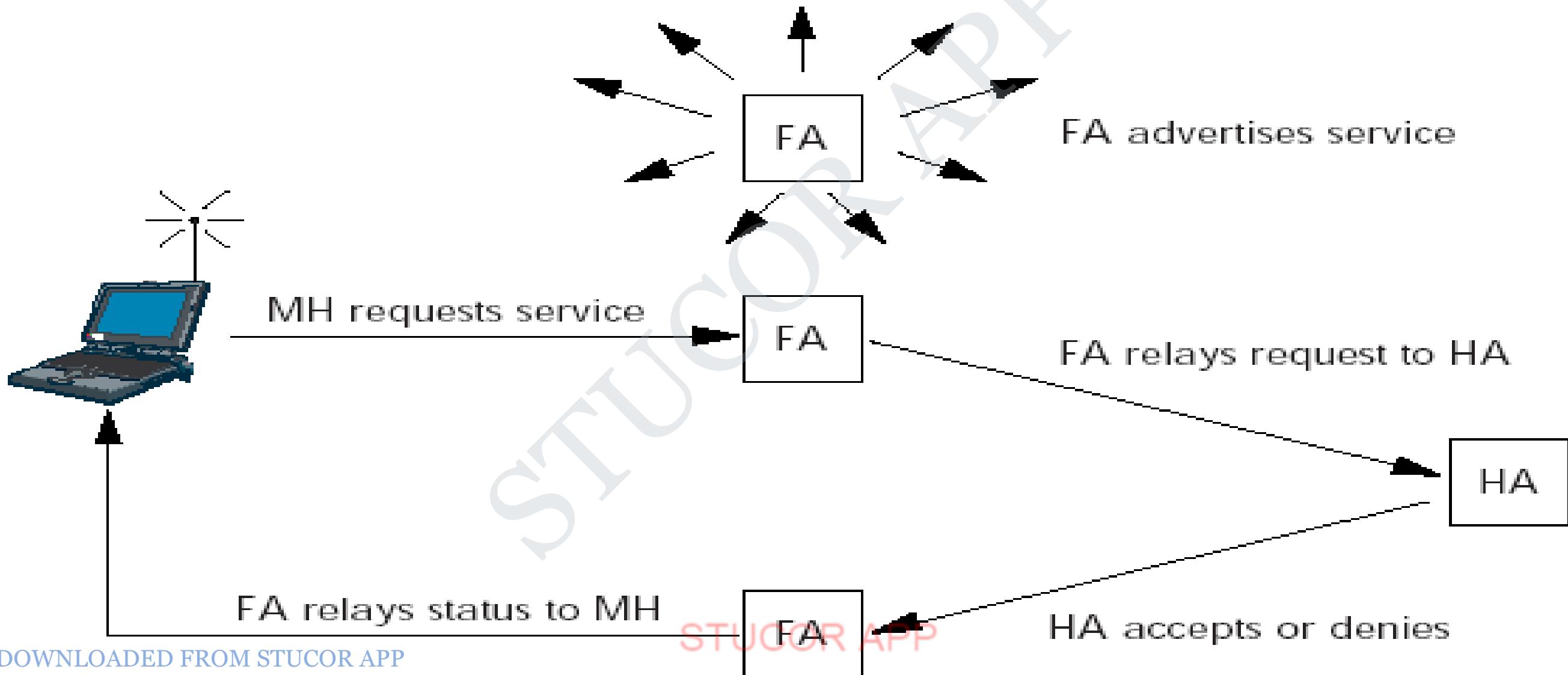
Extension of ICMP Router Advertisement

- Home agents and foreign agents broadcast ***agent advertisements*** at regular intervals
 - Allows for the detection of mobility agents
 - Lists one or more available care-of addresses
 - Informs the mobile node about special features
 - Mobile node selects its care-of address
 - Mobile node checks whether the agent is a home agent or foreign agent
 - Mobile node issues an ICMP router solicitation message

Mobile IP Agent Advertisement Message



Once a mobile node has a care-of address, its home agent must find out about it



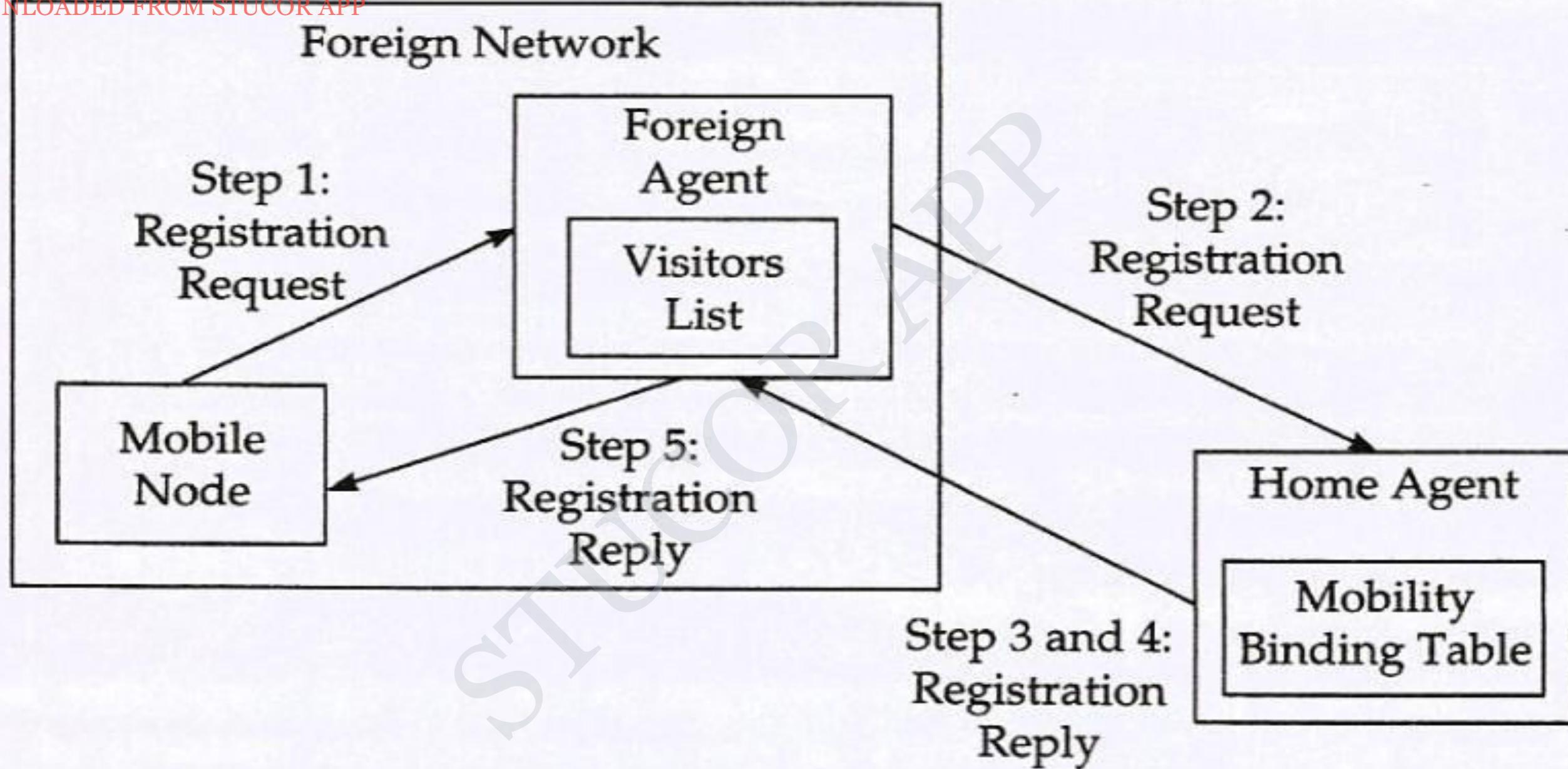


Figure 4.3 Registration process in Mobile IP.

3. Tunneling to the care-of address

Src Dest Proto

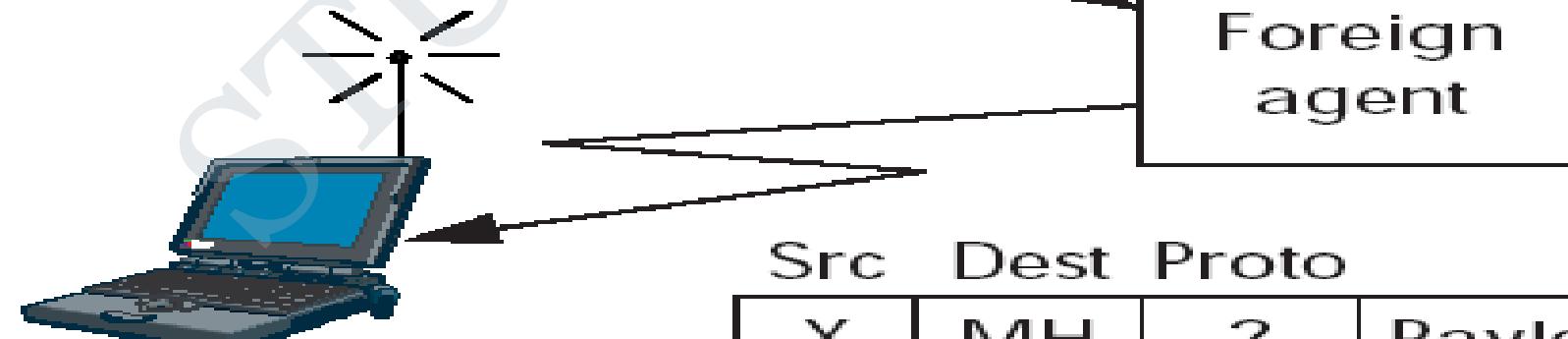
X	MH	?	Payload
---	----	---	---------

Encapsulated diagram

Home agent

Src	Dest	Proto
HA	COM	4 or 55

Src	Dest	Proto
X	MH	?
Payload		

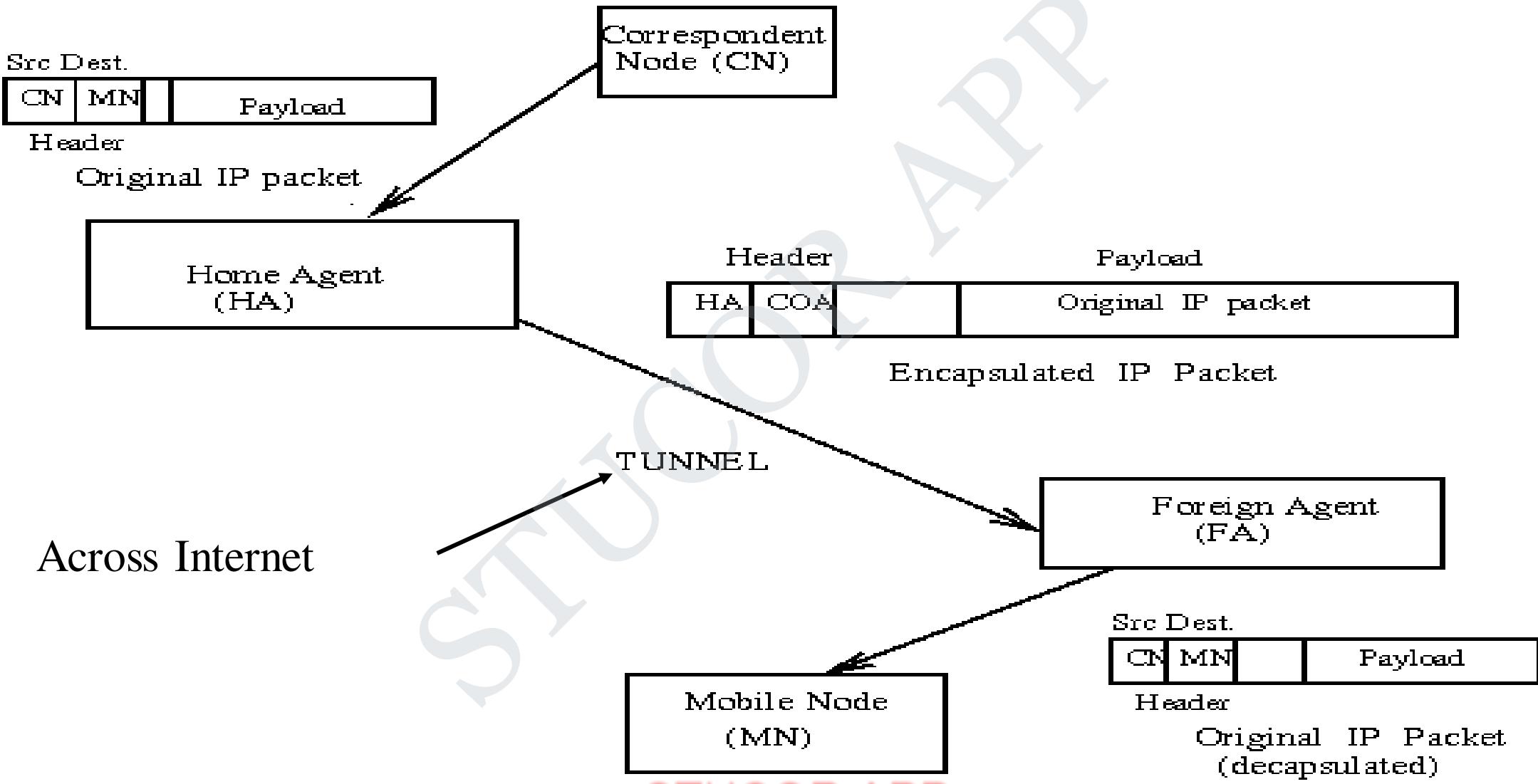


Src Dest Proto

X	MH	?	Payload
---	----	---	---------

STUCOR APP

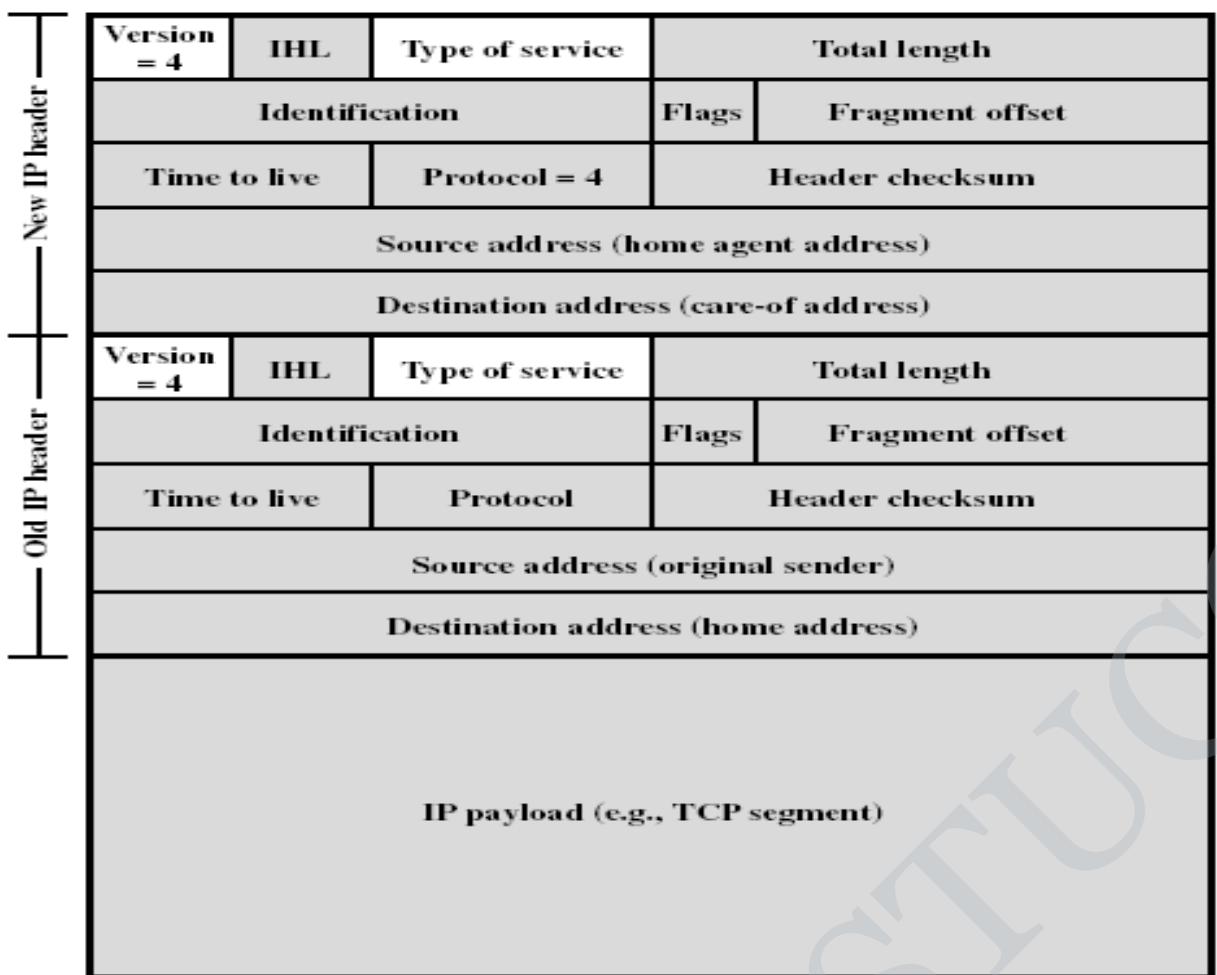
MOBILE IP TUNNELING



Tunneling takes place to forward an IP datagram from home agent to a care-of-address.

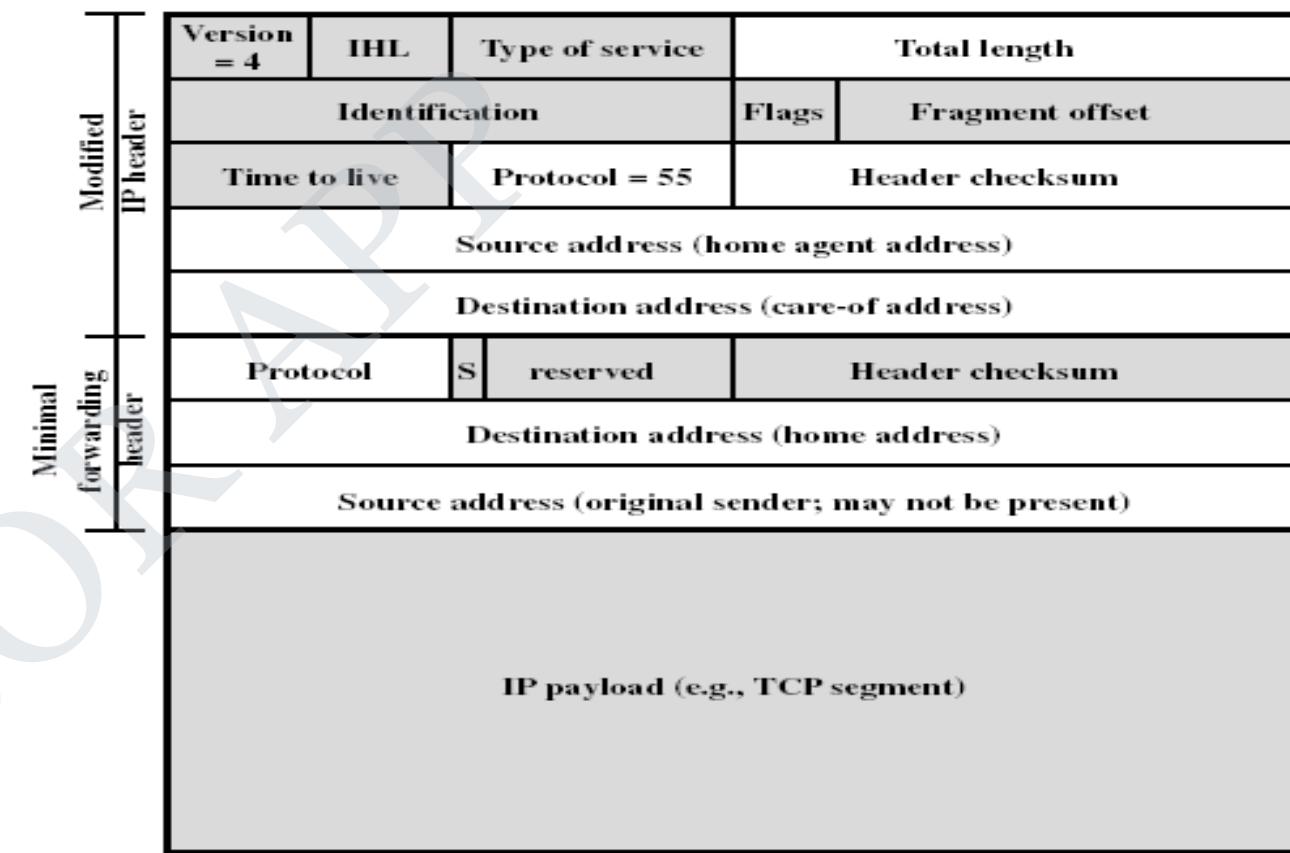
- When a home agent receives a packet addressed to a mobile host , it forwards the packet to the care-of-address using IP-within-IP(encapsulation)
- Using IP-within-IP, the home agent inserts a new IP header in front of the IP header of any datagram.
- Destination address is set to the home agent's address.
- Source address is set to the home agents address.
- After stripping out the first header, IP processes the packet again.

Two Tunneling Methods



Unshaded fields are copied from the inner IP header to the outer IP header.

IP-within-IP Encapsulation



Unshaded fields in the inner IP header are copied from the original IP header.
Unshaded fields in the outer IP header are modified from the original IP header.

Minimal Encapsulation

ROUTE OPTIMIZATION

- ❖ All the data packets to the mobile node go through the home agent.
- ❖ There will be a heavy traffic between HA and CN causing latency to increase.
- ❖ To overcome this problem the following route optimization needs
 - Enable direct notification of the corresponding host
 - Direct tunneling from the corresponding host to the mobile host.
 - Binding cache maintained at the corresponding host

The association of the home address with care-of-address is called binding

CELLULAR WIRELESS

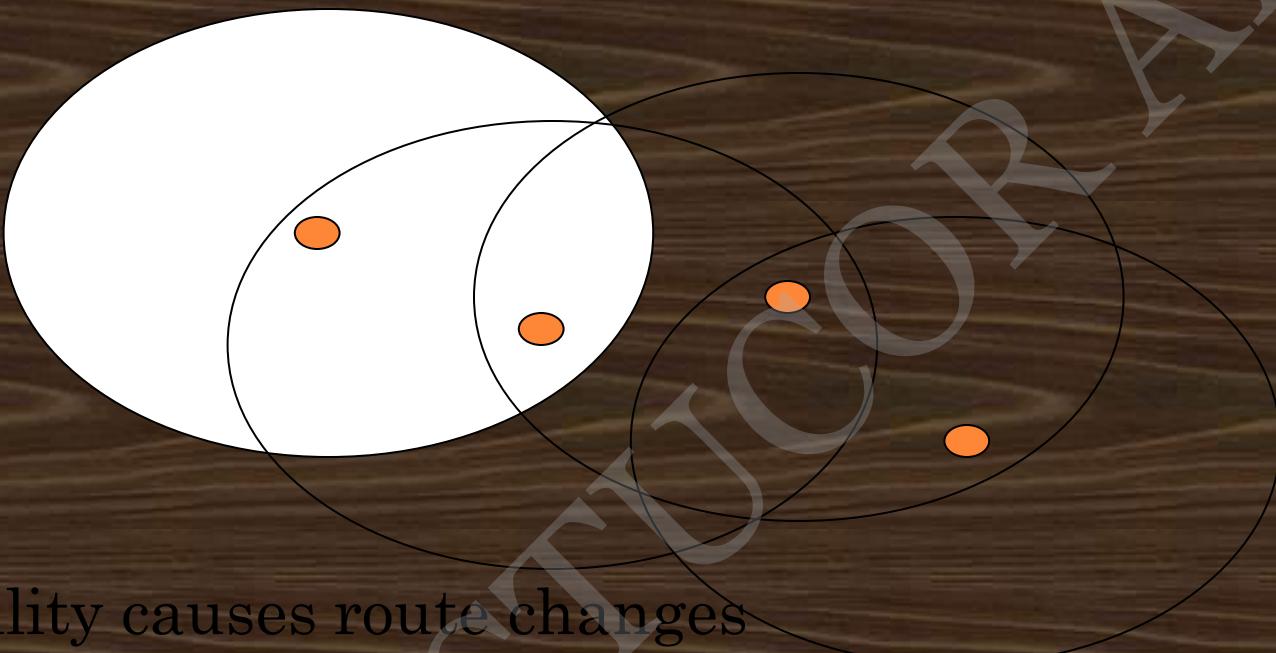
- Single hop wireless connectivity to the wired world
 - Space divided into **cells**
 - A **base station** is responsible to communicate with hosts in its cell
 - Mobile hosts can change cells while communicating
 - **Hand-off** occurs when a mobile host starts communicating via a new base station



STUCOR APP

MULTI-HOP WIRELESS

- May need to traverse multiple links to reach destination



- Mobility causes route changes



MOBILE AD HOC NETWORKS (MANET)

- ❑ Host movement frequent
- ❑ Topology change frequent



- ❑ No cellular infrastructure. Multi-hop wireless links.
- ❑ Data must be routed via intermediate nodes.

WHY AD HOC NETWORKS ?

- Setting up of fixed access points and backbone infrastructure is not always viable
 - Infrastructure may not be present in a disaster area or war zone
 - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)
- Ad hoc networks:
 - Do not need backbone infrastructure support
 - Are easy to deploy
 - Useful when infrastructure is absent, destroyed or impractical



MANY APPLICATIONS

- Personal area networking

- cell phone, laptop, ear phone, wrist watch

- Military environments

- soldiers, tanks, planes

- Civilian environments

- taxi cab network
 - meeting rooms
 - sports stadiums
 - boats, small aircraft

- Emergency operations

- search-and-rescue
 - policing and fire fighting



AD-HOC BASIC CONCEPTS

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires

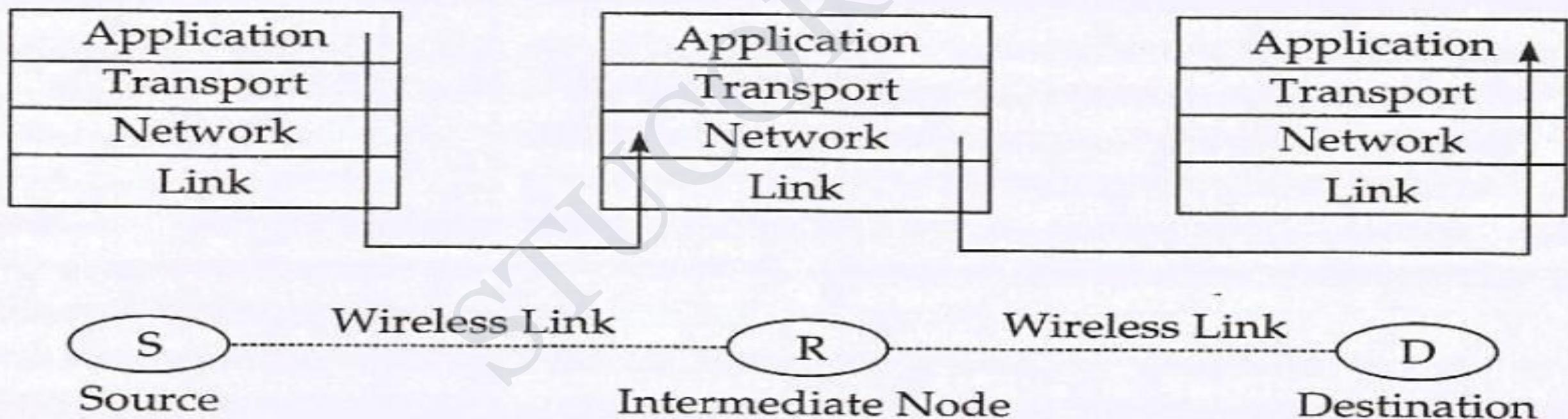


Figure 7.1 A schematic model of a mobile ad hoc network.

CHARACTERISTICS

- I. Lack of fixed infrastructure
- II. Dynamic topologies
- III. Bandwidth constrained, variable capacity links
- IV. Energy constrained operation
- V. Increased vulnerability
- VI. Other characteristics

APPLICATIONS

- ❖ Communication among portable computers
- ❖ Environmental monitoring
- ❖ Military
- ❖ Emergency applications

MANET DESIGN ISSUES

- Network size and node density
- Connectivity
- Network topology
- User traffic
- Operational environment
- Energy constraint

ROUTING

The purpose of routing is to find the best path between the source and the destination for forwarding packets in any store and forward network.

- Packet routing is usually a much more complex task in an ad-hoc compared to infrastructure based networks.
- The main complications arise on account of continual topology changes and limited battery power of the nodes.
- The destination node is not in transmission range of the source node, the route has to be formed with the help of the intervening nodes in the network.

In MANET, the node making up a route may themselves move or shut down due to low battery energy - therefore necessary to find a new route each time a node needs to transmits a message, making routing an expensive and difficult task.

Based on the above discussion,

- Traditional routing protocols would not suitable in an ad hoc network.
- Each node in an ad hoc network needs to have routing capability and also needs to

ESSENTIAL OF TRADITIONAL ROUTING PROTOCOL

- ❖ The two important classes of routing protocols for traditional networks are the link state and the distance vector
- ❖ Both are extremely popular in packet-switched networks.
- ❖ The shortest path is computed according to some specific cost metric such as the no of hops in the route.

APPROACHES TO SHORTEST PATH ROUTING

1. Link State Routing or Link State Protocol (LSP)

- Each node knows the distance to its neighbors
- The distance information (=link state) is broadcast to all nodes in the network
- Each node calculates the routing tables independently

2. Distance Vector Routing

- Each node knows the distance (=cost) to its directly connected neighbors
- A node sends a list to its neighbors with the current distances to all nodes
- If all nodes update their distances, the routing tables eventually converge

LINK STATE ROUTING

- ❖ Each node must
 - discover its neighbors
 - measure the delay (=cost) to its neighbors
 - broadcast a packet with this information to all other nodes
 - compute the shortest paths to every other router
- ❖ The broadcast can be accomplished by flooding
- ❖ The shortest paths can be computer with Dijkstra's algorithm

LINK STATE ROUTING: BASIC PRINCIPLES

1. Each router establishes a relationship (“*adjacency*”) with its neighbors
2. Each router generates *link state advertisements (LSAs)* which are distributed to all routers. The LSA contains
 - The identity of the router originating the message
 - The identities of all neighbors.

LSA = (link id, state of the link, cost, neighbors of the link)
3. Each router maintains a database of all received LSAs (*topological database or link state database*), which describes the network has a graph with weighted edges
4. Each router uses its link state database to run a shortest path algorithm (Dijkstra’s algorithm) to produce the shortest path to each network

A ROUTER IS CONNECTED TO OTHER ROUTERS THROUGH LINKS

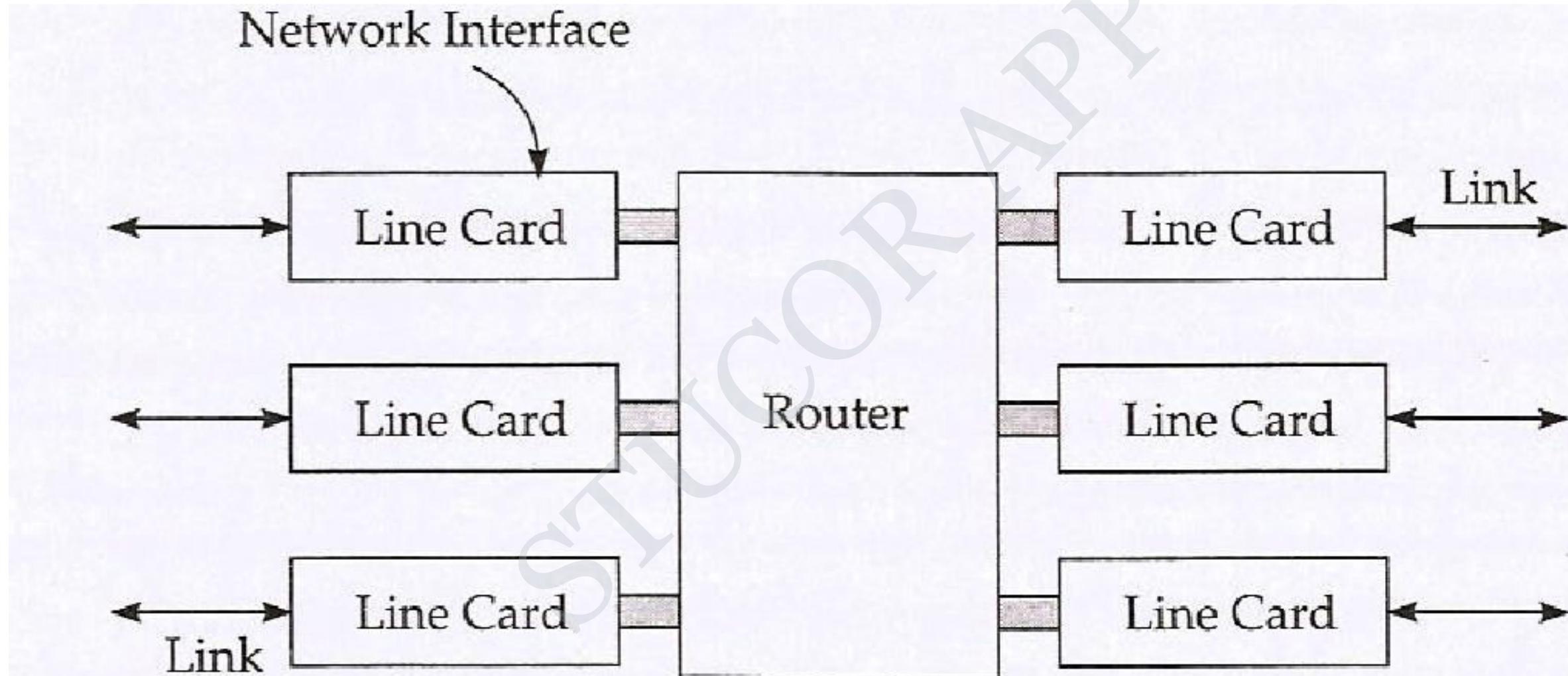


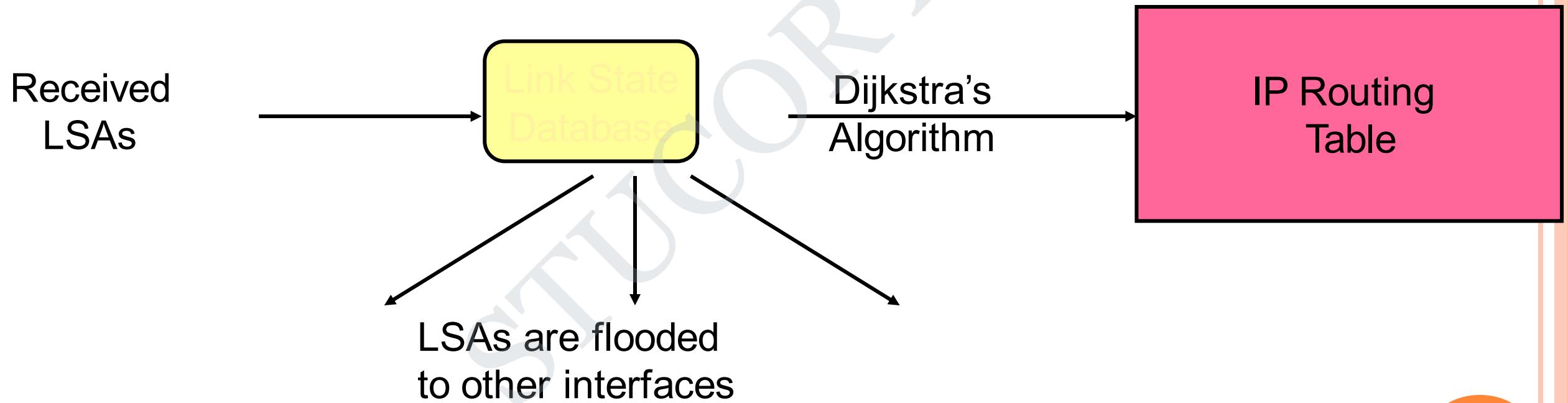
Figure 7.2

STUCOR APP
Schematic diagram of a router.

LINK STATE ROUTING: PROPERTIES

- Each node requires complete topology information.
- Link state information must be flooded to all nodes.
- All routers which are connected to the router added to the tree or in the candidate list.
- The delay in the candidate list to every other router in the tree are compared
- The shortest delay is moved in to the tree and attached to appropriate neighbor router and removed from the candidate list.
- The above steps are repeated till there are no more routers left in the candidate list.
- The network topology has been determined in the form of a shortest path tree a router forms its routing table and uses it to find the best route to

OPERATION OF A LINK STATE ROUTING PROTOCOL



ADVANTAGES AND DISADVANTAGES

Advantages

- Builds a topological map –Full knowledge of the network
- Fast convergence –Floods LSPs immediately
- Event-driven updates –LSP sent when there is a change, only contains information regarding the affected link
- Hierarchical design –Areas can be used to separate routing traffic

Disadvantages

- **Significant demands on memory and processing resources**
- **Requires very strict network design**
- **Requires a knowledgeable network administrator**
- **Initial flooding can impede network performance**

DISTANCE VECTOR(DV) PROTOCOLS

DISTANCE VECTOR

- The term vector means that routes are advertised as vector (distance, direction) Each node maintains two tables:
- Distance is the number of hops between the two nodes and direction is defined in terms of the next hop router to which the packets need to be forwarded.
- The distance vector protocols are based on well known Bellman-Ford algorithm.
- The protocol share everything in the network with neighbors by broadcasting the entire router table
- Router updates its own routing table by examining the received information and in turn informs its own neighbors of the changes, called ‘routing by rumor’
- The router do not have knowledge of the entire path, just know the following vector
 - Direction in which a packet should be forwarded.
 - Its own distance from the destination.

The two popular DV routing protocol are RIP(Routing Information Protocol) and IGRP(Interior Gateway Routing Protocol)

ADVANTAGES AND DISADVANTAGES

Advantages:

- Simple implementation and maintenance
- Low resource requirements (memory, CPU)

Disadvantages:

- Slow convergence (periodic updates)
- Limited scalability
- Routing loops (due to slow convergence)

ROUTING IN MANET VS - TRADITIONAL NETWORKS

The three important ways in which a MANET routing protocol differs from routing of packets in traditional networks.

- ❖ In MANET each node act as a router, whereas ordinary nodes in a traditional wired network do not participate in routing the packets.
- ❖ In MANET the topology is dynamic because of the mobility of the routing, the routing table become obsolete and routing process complicated.
- ❖ In the simple IP based addressing scheme deployed in wired networks, the IP address encapsulated in the subnet structures does not work because of node mobility

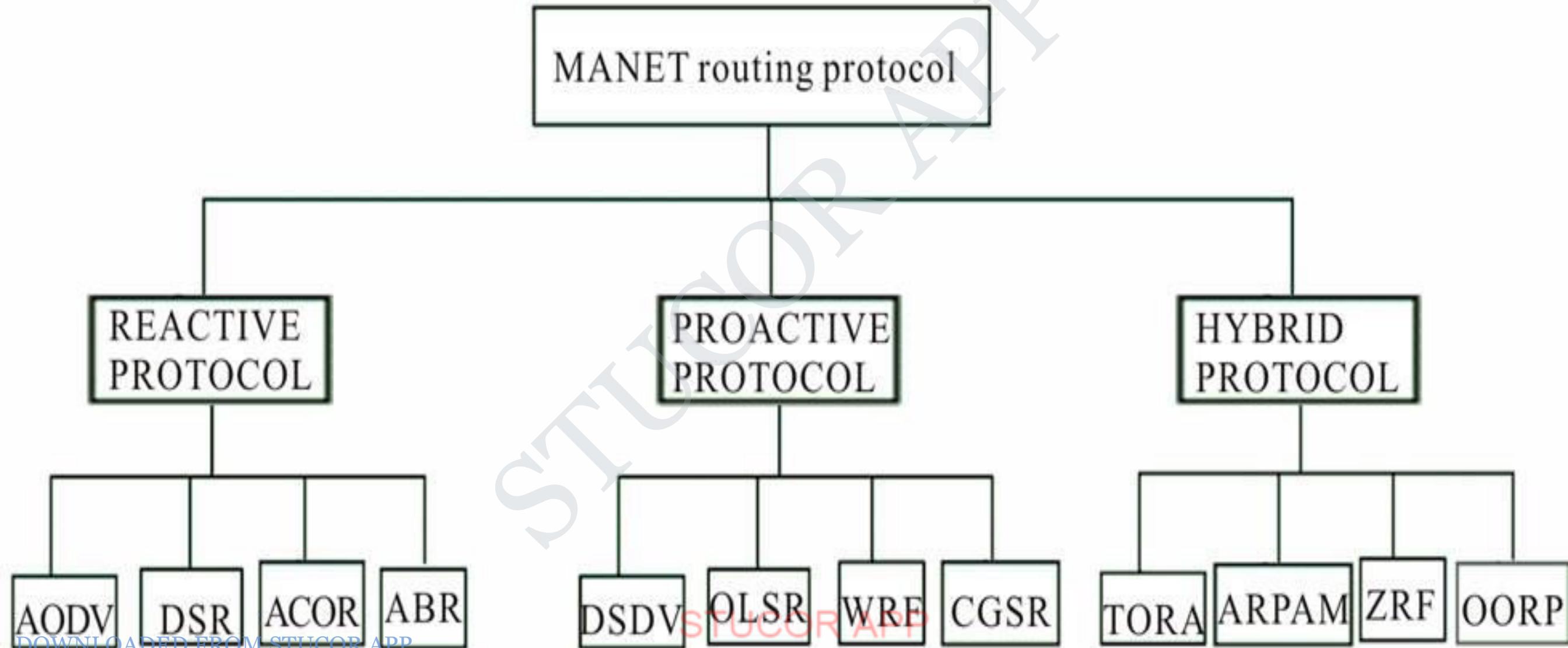
To cope with the above three impermanent differences, MANET need to carryout route discovery and route maintenance.

TYPES OF COMMUNICATIONS

The node initiate the following types of communication.

- ❖ Unicast: The message is sent to a single destination node.
- ❖ Multicast: The message is sent to a selected subset of the network nodes.
- ❖ Broadcast: The message is sent to all node in the network. Since unrestrained broadcast can choke a MANET, applications usually do not use broad cast.

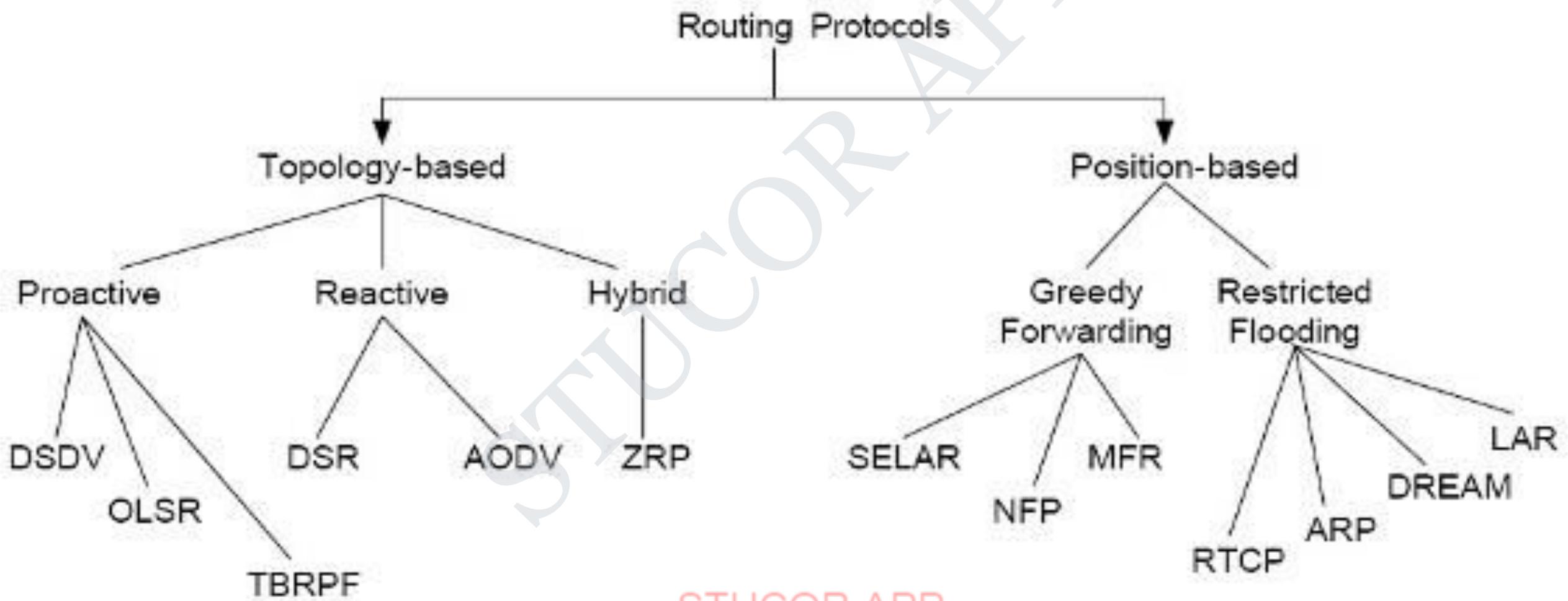
A CLASSIFICATION OF UNICAST ROUTING PROTOCOLS



UNICAST ROUTING PROTOCOLS

- Many protocols have been proposed
- Some specifically invented for MANET
- Others adapted from protocols for wired networks
- No single protocol works well in all environments
 - some attempts made to develop adaptive/hybrid protocols
- Standardization efforts in IETF
 - MANET, Mobile IP working groups
 - <http://www.ietf.org>

POPULAR MANET ROUTING PROTOCOLS



ROUTING PROTOCOLS

❖ **Proactive protocols**

- Traditional distributed shortest-path protocols
- Maintain routes between every host pair at all times
- Based on periodic updates; High routing overhead
- Example: DSDV (destination sequenced distance vector)

❖ **Reactive protocols**

- Determine route if and when needed
- Source initiates route discovery
- Example: DSR (dynamic source routing)

❖ **Hybrid protocols**

- Adaptive; Combination of proactive and reactive
- Example : ZRP (zone routing protocol)



PROTOCOL TRADE-OFFS

- ❑ Proactive protocols
 - Always maintain routes
 - Little or no delay for route determination
 - Consume bandwidth to keep routes up-to-date
 - Maintain routes which may never be used
- ❑ Reactive protocols
 - Lower overhead since routes are determined on demand
 - Significant delay in route determination
 - Employ flooding (global search)
 - Control traffic may be bursty
- ❑ Which approach achieves a better trade-off depends on the traffic and mobility

POPULAR MANET ROUTING PROTOCOL

DESTINATION-SEQUENCED DISTANCE-VECTOR (DSDV) ROUTING PROTOCOL

DSDV is based on the table driven (Proactive) approach to packet routing, it extends the distance vector protocol of wired networks (Bellman-Foard routing algorithm) . Improvement made is the avoidance of routing loops through the use of number sequencing scheme

Important steps in the operation of DSDV

1. Each node maintains information regarding routes to all the known destinations. The routing information updated periodically.
2. This can be considered shortcoming – traffic overhead and maintain routes which they may not use.
 - Full Update or full dump: Send all routing information from own table.
 - Incremental Update: Send only entries that has changed. (Make it fit into one single packet)

Important steps in the operation of DSDV

3. Each router in node in the network collects route information from all its neighbors.
4. After gathering information, the node determines the shortest path to the destination based on the gathered information.
5. Based on the gathered information, a new routing, table is generated
6. The router broadcast this table to its neighbors. On receipt by neighbors, the neighbor nodes re compute their respective routing tables.
7. This process continues till the routing information become stable.
8. DSDV incorporates a sequenced numbering scheme .
9. Each routing advertisement comes with a sequence number
10. Advertise to each neighbor own routing information
 - Destination Address
 - Metric = Number of Hops to Destination

11. Advertise to each neighbor own routing information

- Destination Address
- Metric = Number of Hops to Destination
- Destination Sequence Number

12. Rules to set sequence number information

- On each advertisement increase own destination sequence number (use only even numbers)
- If a node is no more reachable (timeout) increase sequence number of this node by 1 (odd sequence number) and set metric = ∞

13. Update information is compared to own routing table

- Select route with higher destination sequence number (This ensure to use always newest information from destination)
- Select the route with better metric when sequence numbers are equal.

DSDV (Table Entries)

Destination	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr_C
D	B	4	D-312	001200	Ptr_D

- **Sequence number:** originated from destination. Ensures loop freeness.
- **Install Time:** when entry was made (used to delete stale entries from table)
- **Stable Data:** Pointer to a table holding information on how stable a route is. Used to damp fluctuations in network.

DSDV- ADVANTAGES AND DISADVANTAGES

❑ Advantages

- ❑ Simple (almost like Distance Vector)
- ❑ Loop free through destination seq. numbers
- ❑ No latency caused by route discovery

❑ Disadvantages

- ❑ No sleeping nodes
- ❑ Overhead: most routing information never used

DYNAMIC SOURCE ROUTING (DSR) PROTOCOL

- DSR is a source initiated on-demand (or reactive) routing protocol for ad hoc networks.
- It uses source routing, technique in which sender of a packet determines the complete sequence of nodes through which a packet has to travel.
- The sender of the packet then explicitly records this list of all nodes in the packet's header.
- Not exchange the routing table information periodically
- Each mobile node in the protocol maintains a ***routing cache*** – which contains the list of all routes that the node has learnt and maintains a sequence counter called ***request id*** to uniquely identify the last request it had generated.
- DSR works in two phases:
 - I. Route discovery
 - II. Route maintenance

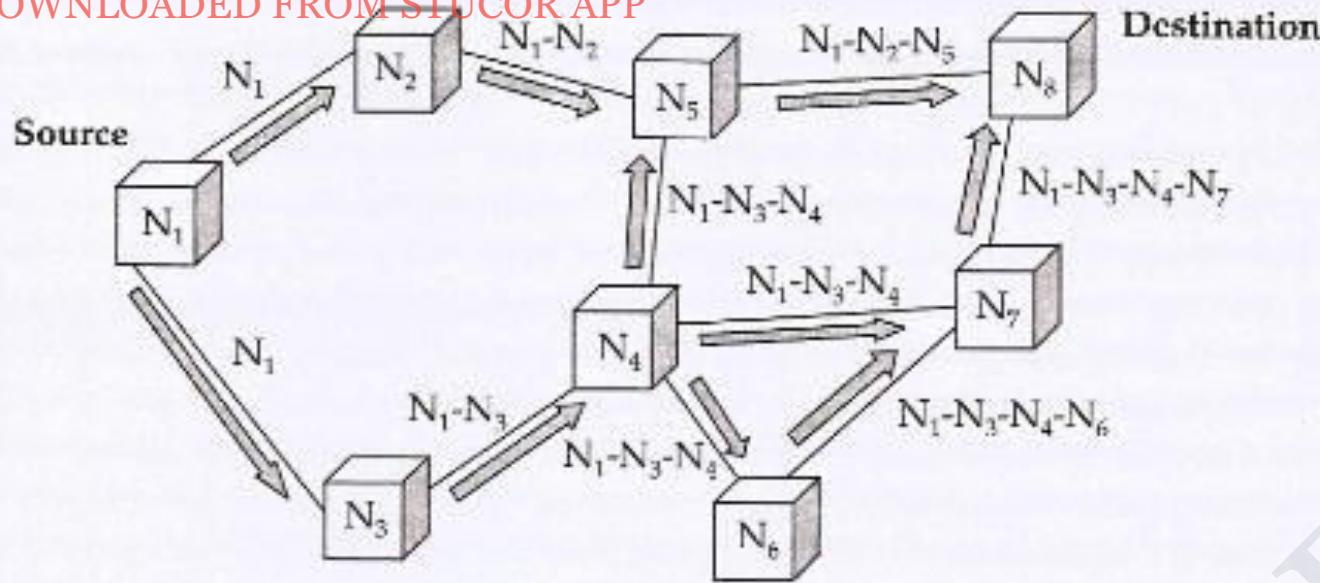


Figure 7.4 An example of the route discovery process in DSR.

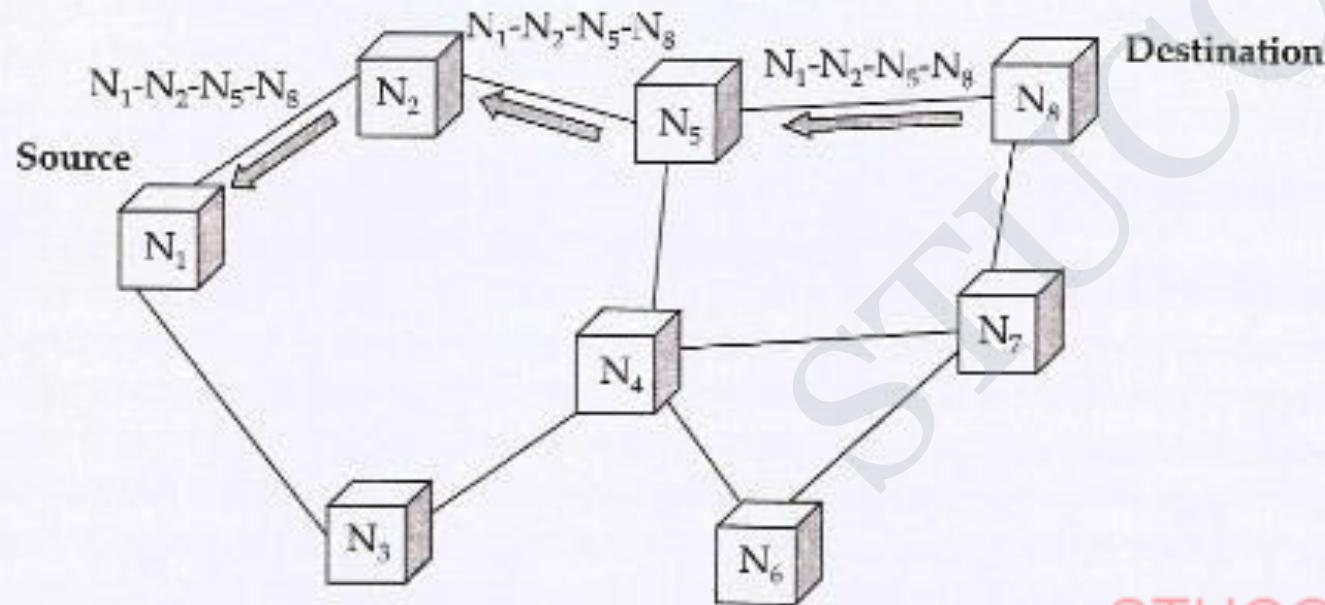


Figure 7.5 An example of the propagation of route reply in DSR.

Route discovery -

- First checks its own routing cache. If there is a valid route, sends put the packet otherwise
- It initiate the route discovery by **route request**
- The route request packet initiates a **route reply** either by the destination node or by an intermediate node that knows a route to the destination.

Route maintenance

- Route maintenance is the process of monitoring the correct operation of a route in use and taking the corrective action when needed.
- As soon as the source receives the RouteError message, it deletes the broken-link-route from its cache.
- If it had another route to the destination, it starts to retransmits the packets using alternative route otherwise it intimates⁵⁹ the route discovery process again.

DYNAMIC SOURCE ROUTING: ADVANTAGES AND DISADVANTAGES

Advantages

- ❖ Routes maintained only between nodes who need to communicate reduces overhead of route maintenance
- ❖ Route caching can further reduce route discovery overhead
- ❖ A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches

Disadvantages

- ❖ Packet header size grows with route length due to source routing
- ❖ Flood of route requests may potentially reach all nodes in the network
- ❖ Potential collisions between route requests propagated by neighboring nodes
 - ❖ insertion of random delays before forwarding RREQ
- ❖ Increased contention if too many route replies come back due to nodes replying using their local cache
 - ❖ Route Reply *Storm* problem
- ❖ Stale caches will lead to increased overhead

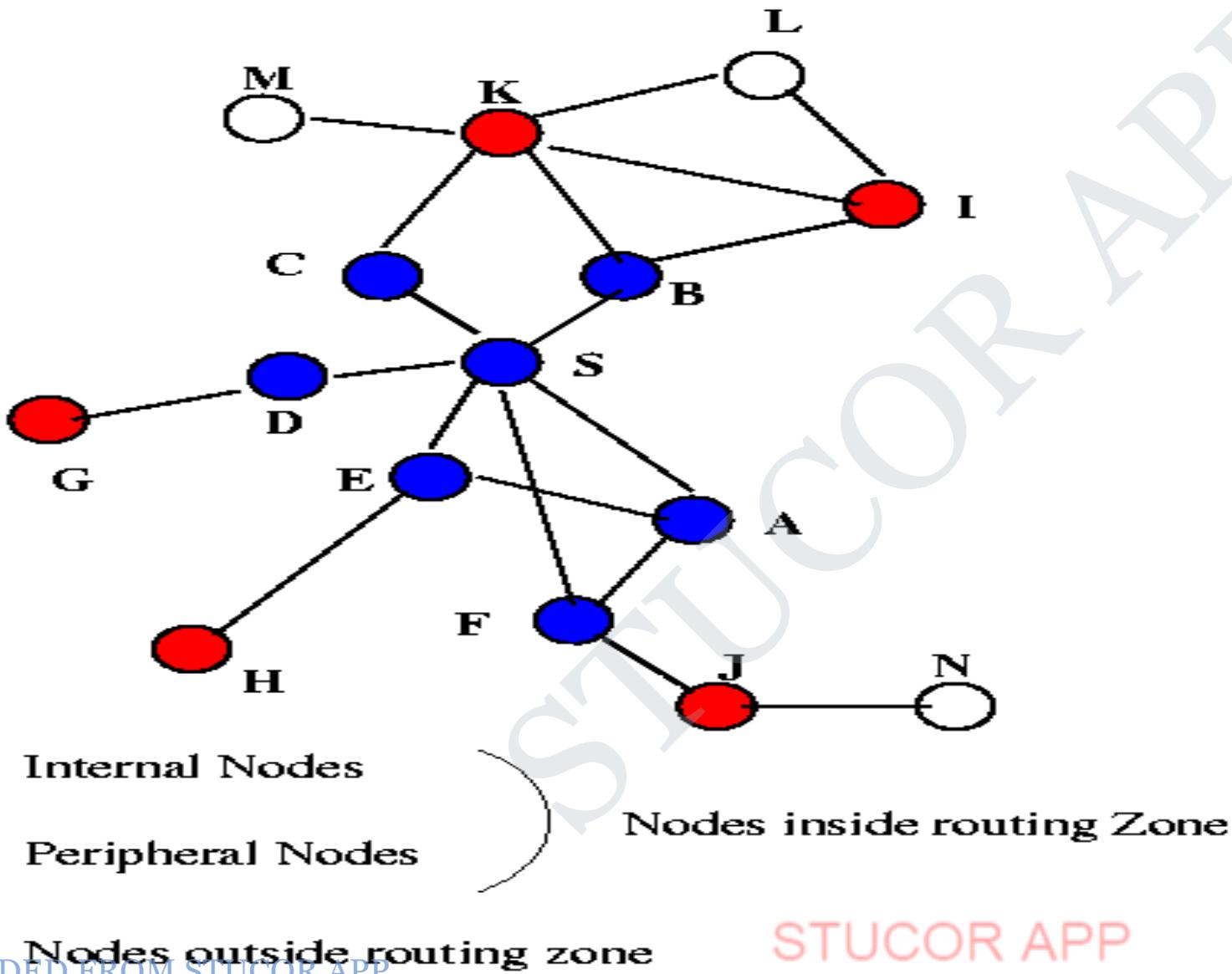
AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

- DSR includes source routes in packet headers
- Resulting large headers can sometimes degrade performance particularly when data contents of a packet are small
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate
- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
 - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP)
- Route Reply travels along the reverse path set-up when Route Request is forwarded

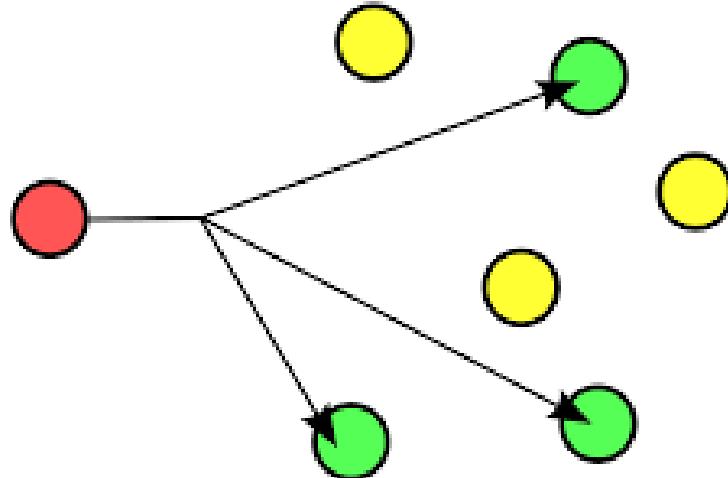
ZONE ROUTING PROTOCOL (ZRP)

- ZRP combines proactive and reactive approaches –hybrid Protocol.
- It incorporates the merits of both on demand and proactive protocols
- All nodes within hop distance at most d from a node X are said to be in the **routing zone** of node X
- All nodes at hop distance exactly d are said to be **peripheral** nodes of node X's routing zone
- **Intra-zone routing:** Proactively maintain routes to all nodes within the source node's own zone.
- **Inter-zone routing:** Use an on-demand protocol (similar to DSR or AODV) to determine routes to outside zone.

ZONE ROUTING PROTOCOL (ZRP)



MULTICAST ROUTING PROTOCOLS FOR MANET



- Multicast is the delivery of a message to a group of destination nodes in a single transmission as shown in figure
- Providing efficient bandwidth, Reducing communication cost, Efficient delivery of data, Supporting dynamic topology Multiple uncast
- Minimizing network load ,Providing basic support for reliable transmission, Designing optimal routes, Providing robustness, efficiency, and adaptability

There are two main categories of multicast routing protocols: Tree-based protocols, and Mesh-based protocols

Tree-based protocols : Establish a single path between any two nodes in the multicast group. Minimum number of copies per packet to be sent in the tree. Bandwidth efficient .

Example Multicast Ad hoc On-Demand Distance Vector (MAODV) routing protocol

Mesh-based protocols : Establish a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility. Drawback – Multiple copies of the same packet are disseminated through the mesh., resulting in reduced packet delivery and increased overhead under highly mobilized conditions.

VEHICULAR AD HOC NETWORKS(VANET)

- VANET is a special type of MANET in which moving automobiles from the nodes of the network
- Vehicle can communicate with other vehicle that are within a range of about 100 to 300 meters – Multi- hop communication.
- Any vehicle that goes out of the signal range in the network excluded from the network.
- A vehicle come in the range of a vehicles of a VANET can come in the range can join the network
- A VANET can offer a significant utility value to a motorist.
- It can help drivers to get information and warnings from a nearby environment via message exchange
- It can help disseminate geographical information to drivers as he continues⁶⁵

DOWNLOADED FROM STUCOR APP

The driver can get road condition ahead or a warning about the application of emergency electronic brake by a vehicle ahead in the lane.

- Drivers may have the opportunity to engage in other leisurely tasks, VoIP with family, watch news and participate in an office video conference etc
- Two vehicles are involved in a collision. The trailing vehicle get advance notification of the collision ahead on the road. The scenario shown in figure.

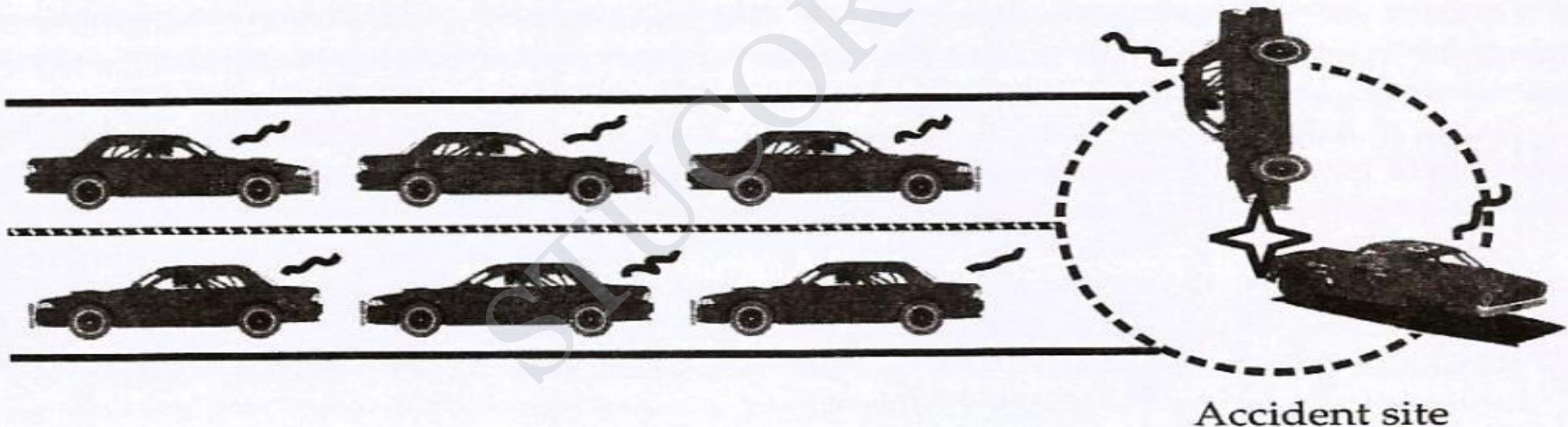


Figure 7.7 STUCOR APP
A VANET use scenario.

MANET VS VANET

MANET

A mobile ad-hoc network (MANET) is a self-configuring infrastructure-less network of mobile devices connected by wireless.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently

Dynamic topologies

- variable capacity links
- Energy constrained operation
- Limited physical security

VANET

Vehicular Ad hoc Network (VANET) is a subclass of mobile Ad Hoc networks (MANETs)

These networks have no fixed infrastructure and instead rely on the vehicles themselves to provide network functionality.

The very high speed of the nodes
Vehicles that are not subjected to the strict energy, space and computing capabilities restrictions
The VANET nodes are not subject to storage and power limitation.
67

SECURITY

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons :

- ❖ Open Medium - Eavesdropping is more easier than in wired network.
- ❖ Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network , thereby allowing any malicious node to join the network without being detected.
- ❖ Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
- ❖ Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system.
- ❖ Lack of Clear Line of Defense –
- ❖ The important characteristics of ad hoc networks that can be exploited to cause security vulnerabilities
 - Lack of physical boundary – difficult to deploy firewalls or monitor the incoming traffic.
 - Low power RF transmission – signal jamming lead to denial of service(DoS) attack
 - Limited computational capabilities- Inability to encrypt messages – spoofing and routing

CHARACTERISTICS OF SECURE AD HOC NETWORKS

A secure ad hoc network should have the following characteristics

- ❖ ***Availability*** – able to survive denial of service(DOS)
- ❖ ***Confidentiality***- Prevent unauthorized users to access confidential information
- ❖ ***Integrity***- no tampering of transmitted messages.
- ❖ ***Authentication*** – Guarantee about the true identity of peer node
- ❖ ***Non-repudiation***- Should ensure that a node having sent a message can not deny it.

References

- Book: Prasant Kumar Patnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.
- http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfmobip.html#wp1010213
- <http://www.hh.se/download/18.70cf2e49129168da015800072015/>
- <https://www.hh.se/download/18.70cf2e49129168da015800088935/Distance+Vector+Routing+Protocol.pdf>

PPT

- <http://www.it.iitb.ernet.in/~sri>
- www.comm.utoronto.ca/~jorg/.../Routing-distancevector-linkstate.ppt
- cone.informatik.uni-freiburg.de/teaching/vorlesung/manet.../DSDV.ppt
- www.drrbpatel.org/lecture/CSE-302-MANET-DSR.ppt
- [ftp://ftp.kemt.fei.tuke.sk/.../MANET/MANET_Presentation.ppt](http://ftp.kemt.fei.tuke.sk/.../MANET/MANET_Presentation.ppt)

OTHER PRESENTATIONS

<http://www.slideshare.net/drgst/presentations>

THANK YOU

Questions and Comments?

MOBILE COMPUTING

Unit IV



STUCOR APP

UNIT IV

MOBILE TRANSPORT LAYER AND APPLICATION LAYER

Mobile TCP – WAP- Architecture – WDP – STLS – WTP- WSP- WAE- WTA
Architecture - WML

Overview of TCP/IP

- TCP/IP protocol suite is a collection of a large number of protocols.
- The four layer of protocols are
 - Application layer
 - Transport layer
 - Internet layer
 - Network layer
- TCP/IP allows any of the standard protocols to be used for network interface

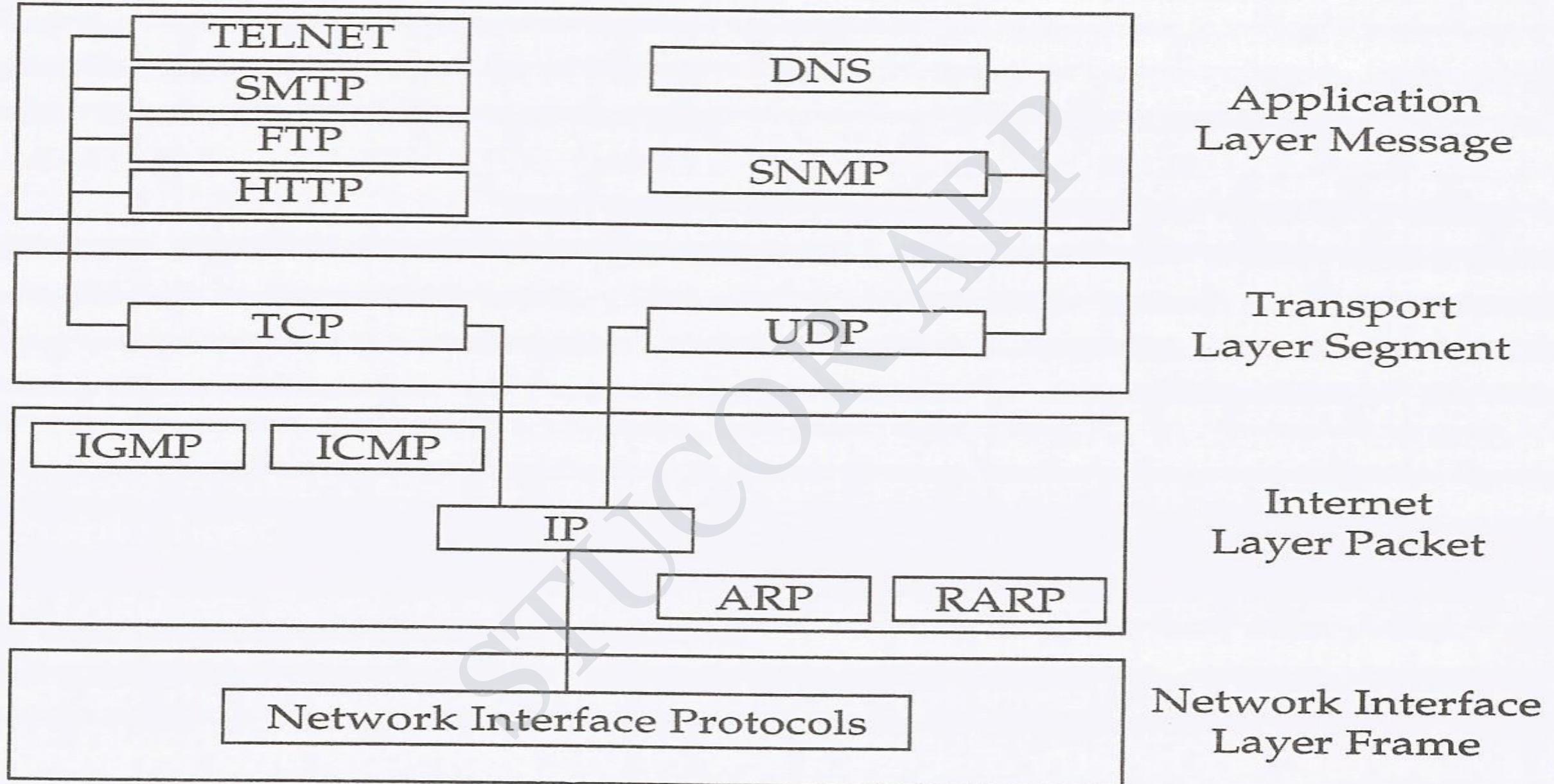


Figure 5.1 *TCP/IP protocol stack.*

Architecture of TCP/IP

TCP/IP protocol consists of four layers. 1. Application layer, 2. Transport layer, 3. Internet layer and 4. Network access layer

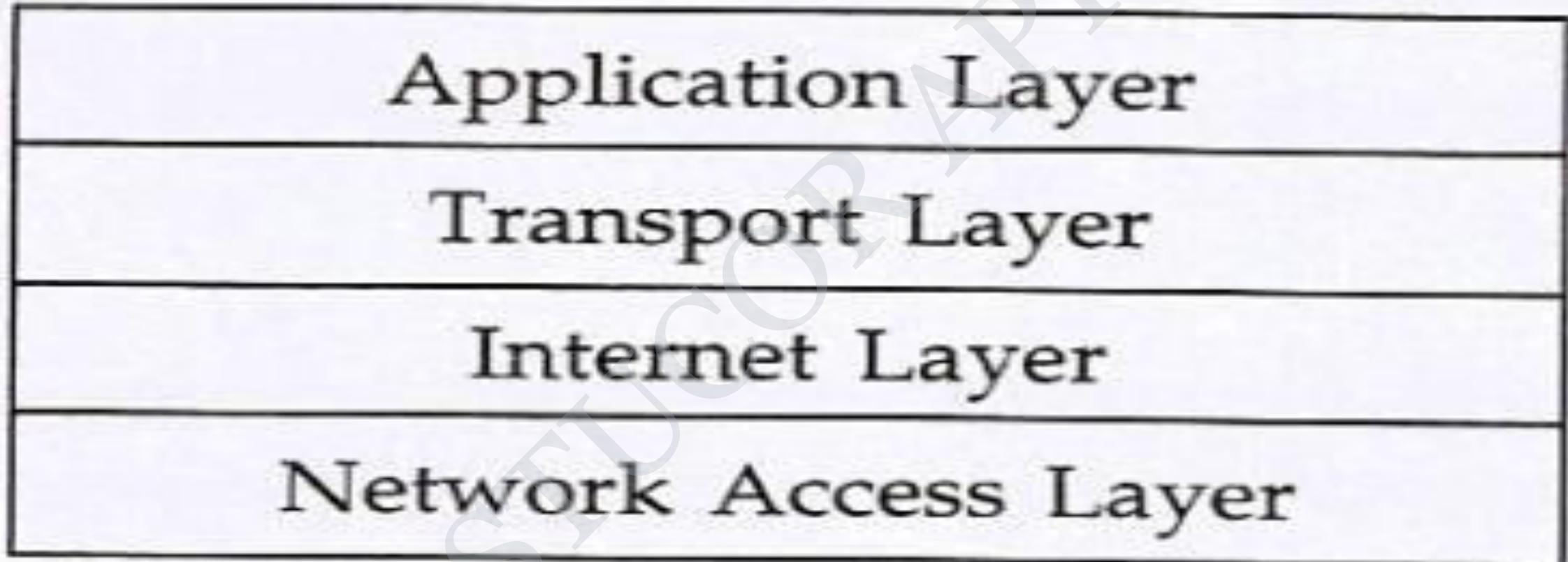


Figure 5.2 *TCP/IP protocol layers.*

1. Application layer:

- ❖ Establish communication with other applications which may be running on separate hosts.
- ❖ Example http,ftp and telnet.

2. Transport layer:

- ❖ The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Provides reliable end-to-end data transfer services.
- ❖ Also referred as host-to-host protocol.
- ❖ The main protocols included at Transport layer are
 - I. TCP (Transmission Control Protocol) and
 - II. UDP (User Datagram Protocol).

3. Internet layer

- ❖ Internet layer pack data into data packets known as IP datagrams,
- ❖ which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.

4. Network access layer

- ❖ The Network Access Layer of the TCP/IP model is associated with the Physical Layer (Layer 1) and the Data Link layer (Layer 2) of the OSI model.
- ❖ The Network Access Layer's function is to move bits (0s and 1s) over the network medium such as coaxial cable, optical fiber, or twisted pair copper wire.
- ❖ The OSI Physical layer is responsible for converting the frame into a stream of bits suitable for the transmission medium and synchronizes signals for the actual transmission.
- ❖ On the destination device, the Physical layer reassembles these signals into a data frame.
- ❖ The OSI Data Link layer is again subdivided into the following two sub layers according to their function:
- ❖ Media Access Control(MAC) Sublayer :— MAC sublayer provides an interface with the network adapter.
- ❖ Logical Link Control(LLC) Sublayer :— LLC sublayer is responsible for error-checking functions for frames delivered also responsible for managing links between communicating devices.

Comparison of TCP/IP and OSI network models

APPLICATION LAYER

PRESENTATION LAYER

SESSION LAYER

TRANSPORT LAYER

NETWORK LAYER

DATALINK LAYER

PHYSICAL LAYER

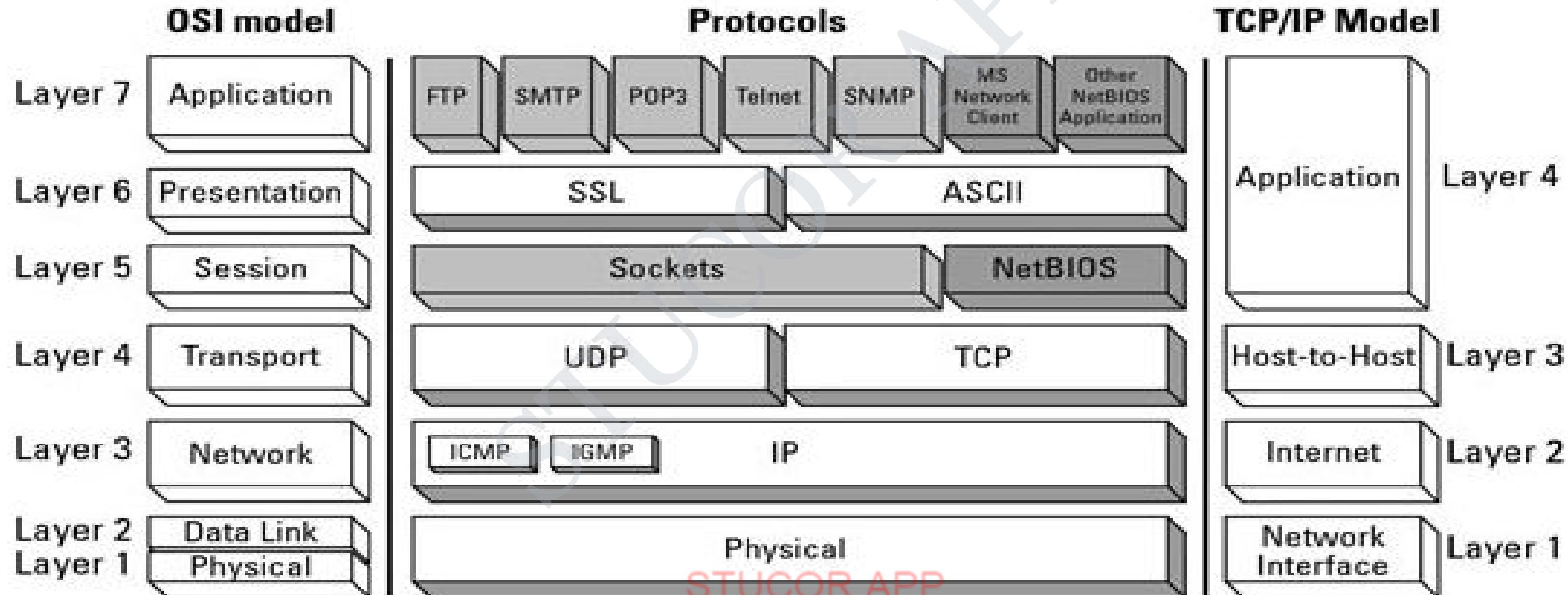
APPLICATION LAYER

TRANSPORT LAYER

INTERNET LAYER

NETWORK ACCESS
LAYER

Comparison of TCP/IP and OSI network models



Adaptation of TCP Window

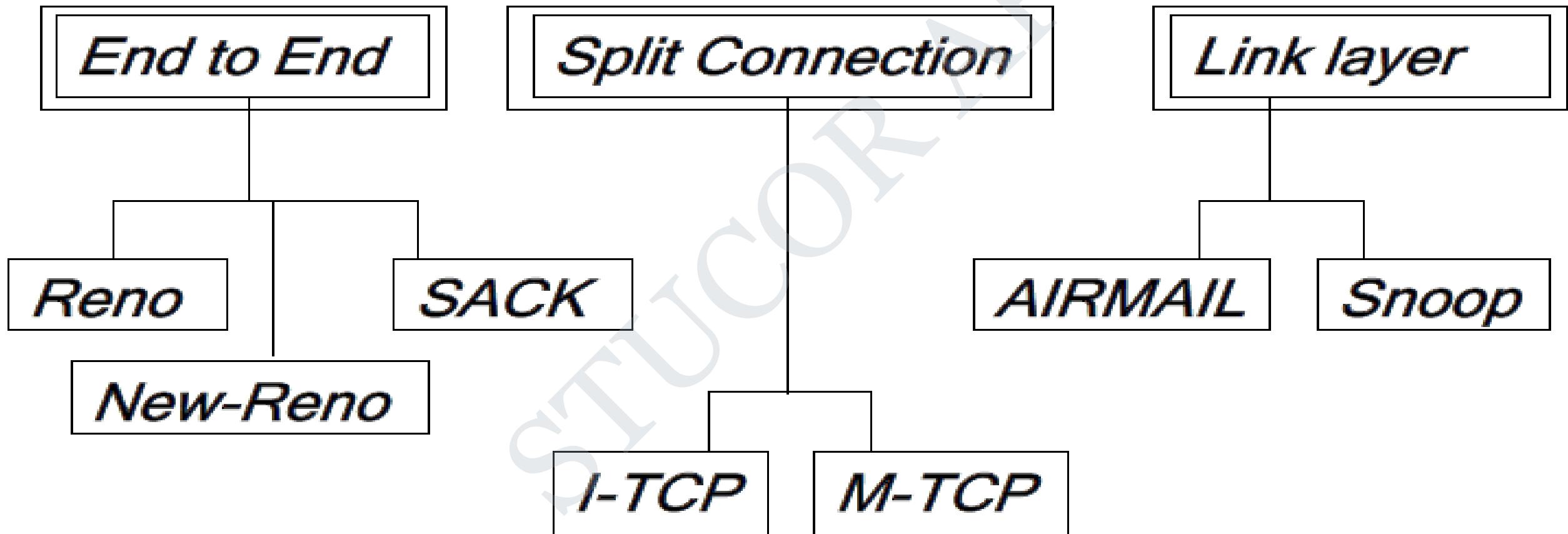
- TCP deploys a flow control technique to control congestion in a network.
- Traffic congestion occurs when the rate at which data is injected by a host into the network exceeds the rate at which data can be delivered to the network.
 - I. Router buffer overflow.
 - II. Receiver buffer overflow
- A flow control technique by TCP helps adapt the rate at sending host end and to prevent overrun at the slow receiver.
- The flow control mechanism by TCP called the sliding window protocol.

Improvements of TCP Performance

Traditional networks

- Transport protocols typically designed for
 - Fixed end-systems
 - Fixed, wired networks
- TCP congestion control
 - Packet loss in fixed networks typically due to (temporary) overload situations
 - Routers discard packets as soon as the buffers are full
 - TCP recognizes congestion only indirectly via missing acknowledgements
 - Retransmissions unwise, they would only contribute to the congestion and make it even worse
 - Slow-start algorithm as reaction

Classification of Schemes



TCP Slow Start

- Sender calculates a congestion window for a receiver
- Start with a congestion window size equal to one segment
- Exponential increase of the congestion window up to the congestion threshold, then linear increase
- Missing acknowledgement causes the reduction of the congestion threshold to one half of the current congestion window
- Congestion window starts again with one segment

Congestion avoidance

- It starts where slow start stops.
- Once congestion window reaches the congestion threshold level, then after that if an acknowledgement is received the window size is increased linearly i.e. the window size doubling is avoided.
- The TCP increases its rate linearly by adding one additional packet to its window at each transmission time. If congestion is detected at any point the TCP reduces its transmission rate to half the previous value. Makes to right transmission rate.
- This scheme is less aggressive than slow start phase.

Fast Retransmit/ Fast Recovery

- TCP sends an acknowledgement only after receiving a packet.
- If a sender receives several acknowledgements for the same packet, this is due to a gap in received packets at the receiver.
- However, the receiver got all packets up to the gap and is actually receiving packets
- Therefore, packet loss is not due to congestion, continue with current congestion window (do not use slow-start)

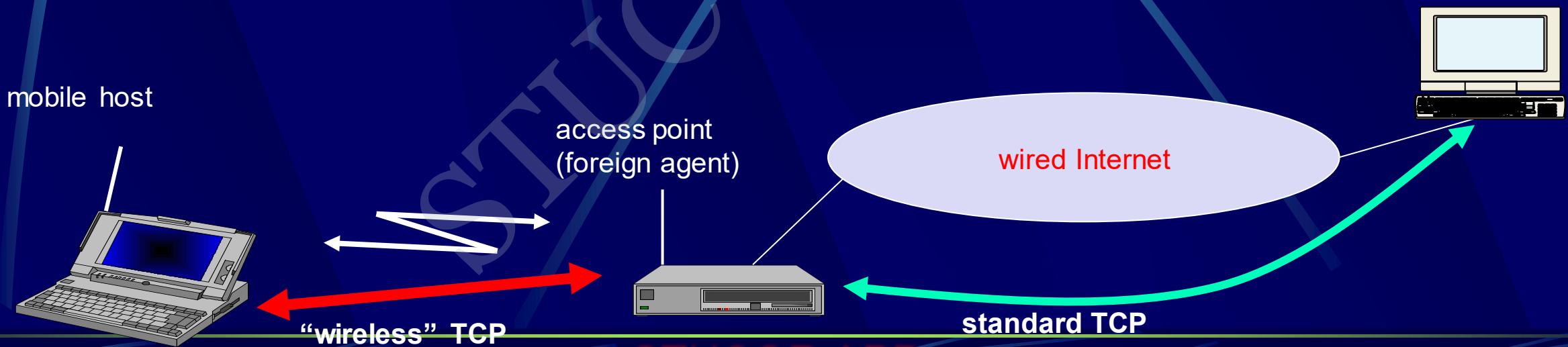
TCP in mobile networks

- TCP assumes congestion if packets are dropped
 - typically wrong in wireless networks, here we often have packet loss due to *transmission errors*
 - furthermore, *mobility* itself can cause packet loss, if e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while there are still packets in transit to the wrong access point and forwarding is not possible
- The performance of an unchanged TCP degrades severely
 - however, TCP cannot be changed fundamentally due to the large base of installation in the fixed network, TCP for mobility has to remain compatible
 - the basic TCP mechanisms keep the whole Internet together

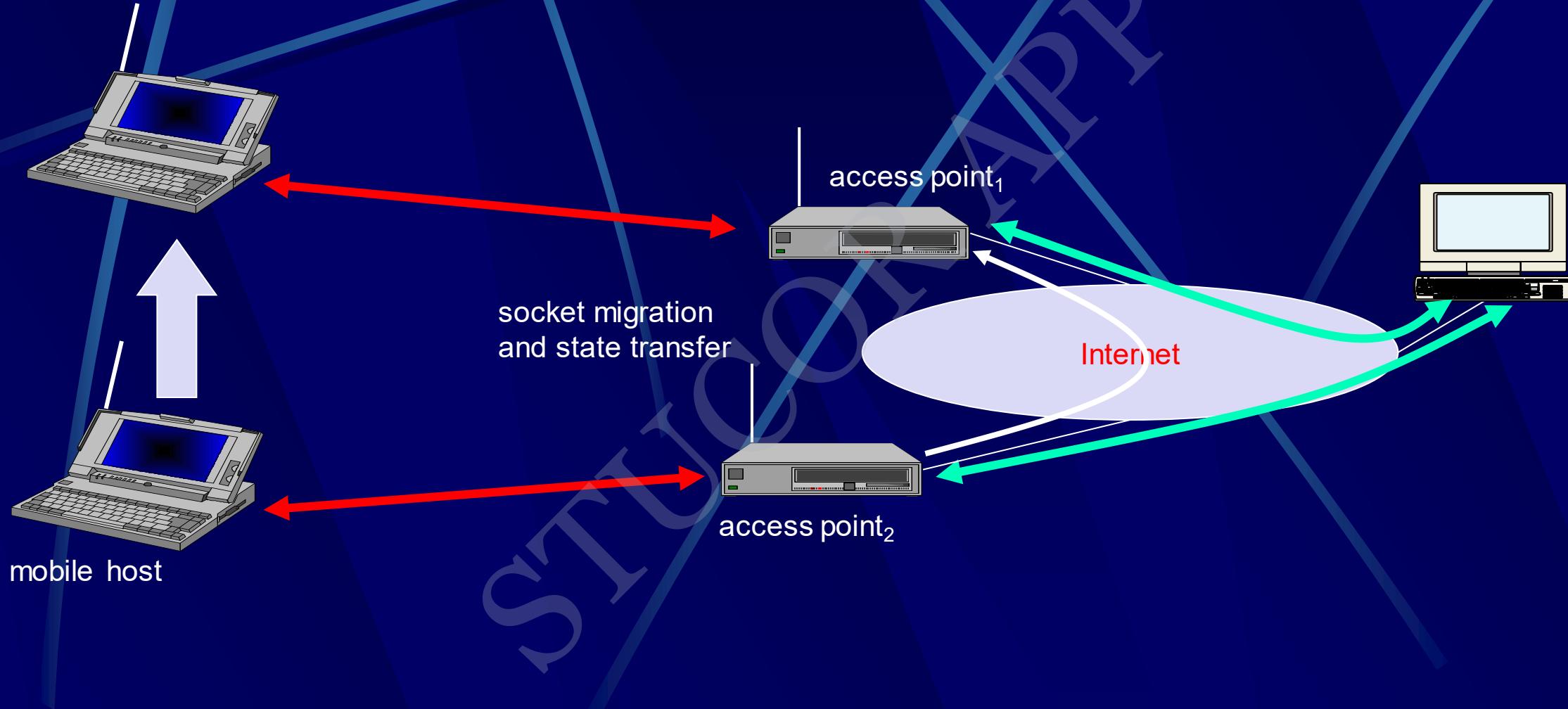
Indirect TCP (I-TCP)

□ Indirect TCP or I-TCP segments the connection

- no changes to the TCP protocol for hosts connected to the wired Internet, millions of computers use (variants of) this protocol
- optimized TCP protocol for mobile hosts
- splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
- hosts in the fixed part of the net do not notice the characteristics of the wireless part



I-TCP socket and state migration



Indirect TCP II

□ Advantages

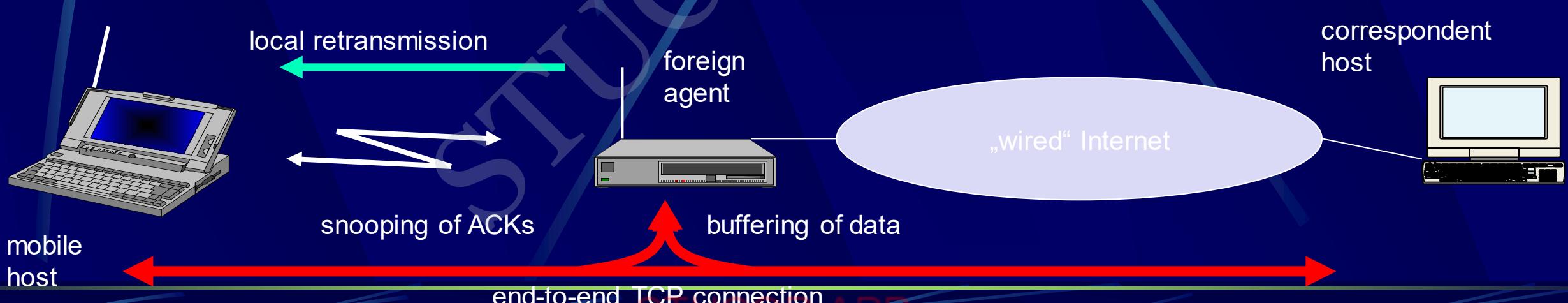
- no changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
- transmission errors on the wireless link do not propagate into the fixed network
- simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
- therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop is known

□ Disadvantages

- loss of end-to-end semantics, an acknowledgement to a sender does not any longer mean that a receiver really got a packet, foreign agents might crash
- higher latency possible due to buffering of data within the foreign agent and forwarding to a new foreign agent

Snooping TCP (S-TCP)

- Transparent extension of TCP within the foreign agent
- buffering of packets sent to the mobile host
- lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called “local” retransmission)
- the foreign agent therefore “snoops” the packet flow and recognizes acknowledgements in both directions, it also filters ACKs
- changes of TCP only within the foreign agent (+min. MH change)



Snooping TCP II

- Data transfer to the mobile host
 - FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
 - fast retransmission possible, transparent for the fixed network
- Data transfer from the mobile host
 - FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
 - MH can now retransmit data with only a very short delay
- Advantages:
 - Maintain end-to-end semantics
 - No change to correspondent node
 - No major state transfer during handover
- Problems
 - Snooping TCP does not isolate the wireless link well
 - May need change to MH to handle NACKs
 - Snooping might be useless depending on encryption schemes

Mobile TCP(M-TCP)

- Special handling of lengthy and/or frequent disconnections
- M-TCP splits as I-TCP does
 - unmodified TCP fixed network to supervisory host (SH)
 - optimized TCP SH to MH
- Supervisory host
 - no caching, no retransmission
 - monitors all packets, if disconnection detected
 - set sender window size to 0
 - sender automatically goes into persistent mode
 - old or new SH reopen the window
- Advantages
 - maintains semantics, supports disconnection, no buffer forwarding
- Disadvantages
 - loss on wireless link propagated into fixed network
 - adapted TCP on wireless link

Mobile TCP(M-TCP)

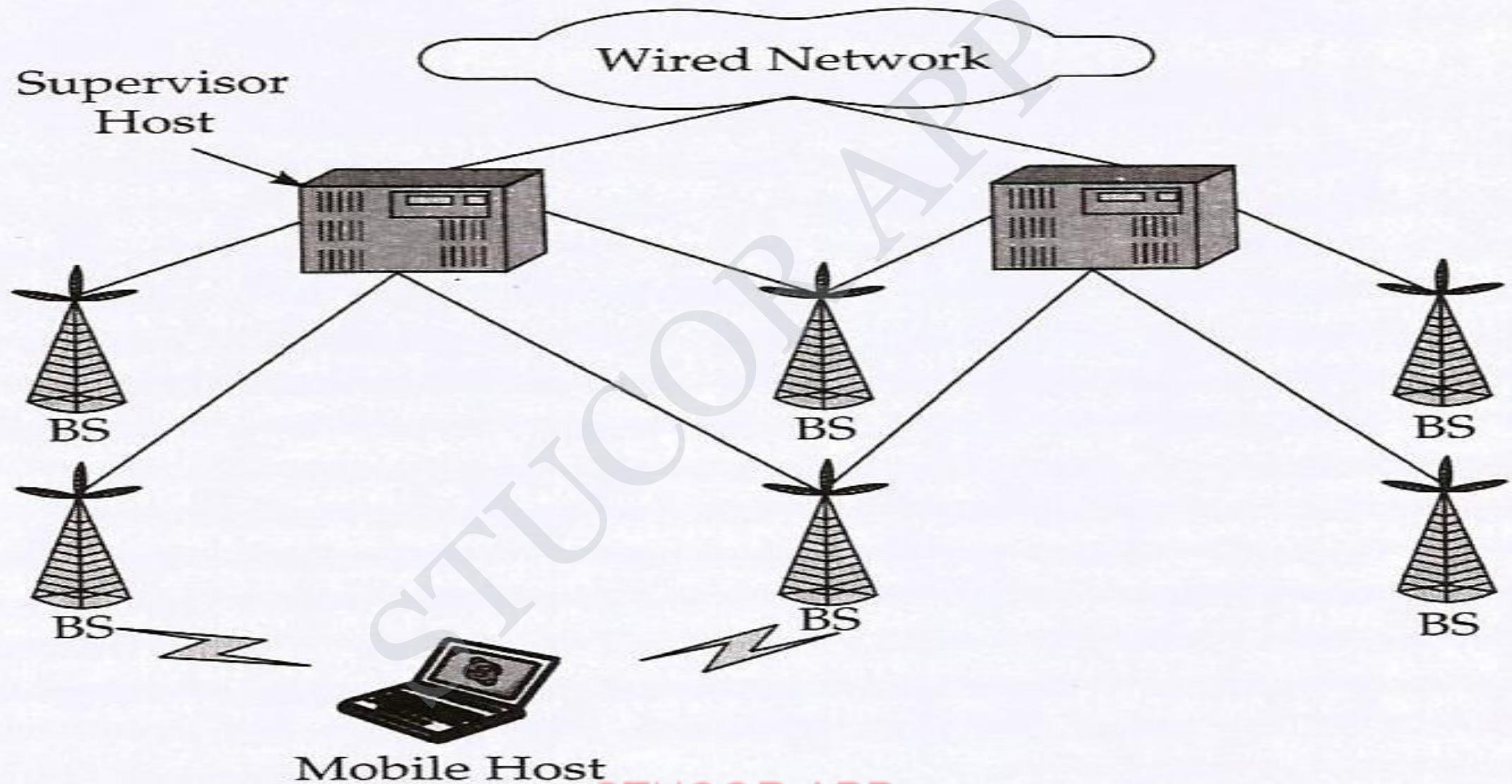


Figure 5.8

A schematic of operation of the M-TCP protocol.

Fast retransmit/fast recovery

- Change of foreign agent often results in packet loss
 - TCP reacts with slow-start although there is no congestion
- Forced fast retransmit
 - as soon as the mobile host has registered with a new foreign agent, the MH sends duplicated acknowledgements on purpose
 - this forces the fast retransmit mode at the communication partners
 - additionally, the TCP on the MH is forced to continue sending with the actual window size and not to go into slow-start after registration
- Advantage
 - simple changes result in significant higher performance
- Disadvantage
 - further mix of IP and TCP (to know when there is a new registration), no transparent approach

Freeze-TCP

- Mobile hosts can be disconnected for a longer time
 - no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or mux. with higher priority traffic
 - TCP disconnects after time-out completely
- TCP freezing
 - MAC layer is often able to detect interruption in advance
 - MAC can inform TCP layer of upcoming loss of connection
 - TCP stops sending, but does not assume a congested link
 - MAC layer signals again if reconnected
- Advantage
 - scheme is independent of data and TCP mechanisms (Ack,SN) => works even with IPsec
- Disadvantage
 - TCP on mobile host has to be changed, mechanism depends on MAC layer

Selective retransmission

- TCP acknowledgements are often cumulative
 - ACK n acknowledges correct and in-sequence receipt of packets up to n
 - if single packets are missing quite often a whole packet sequence beginning at the gap has to be retransmitted (go-back-n), thus wasting bandwidth
- Selective retransmission as one solution
 - RFC2018 allows for acknowledgements of single packets, not only acknowledgements of in-sequence packet streams without gaps
 - sender can now retransmit only the missing packets
- Advantage: much higher efficiency
- Disadvantage
 - more complex software in a receiver, more buffer needed at the receiver

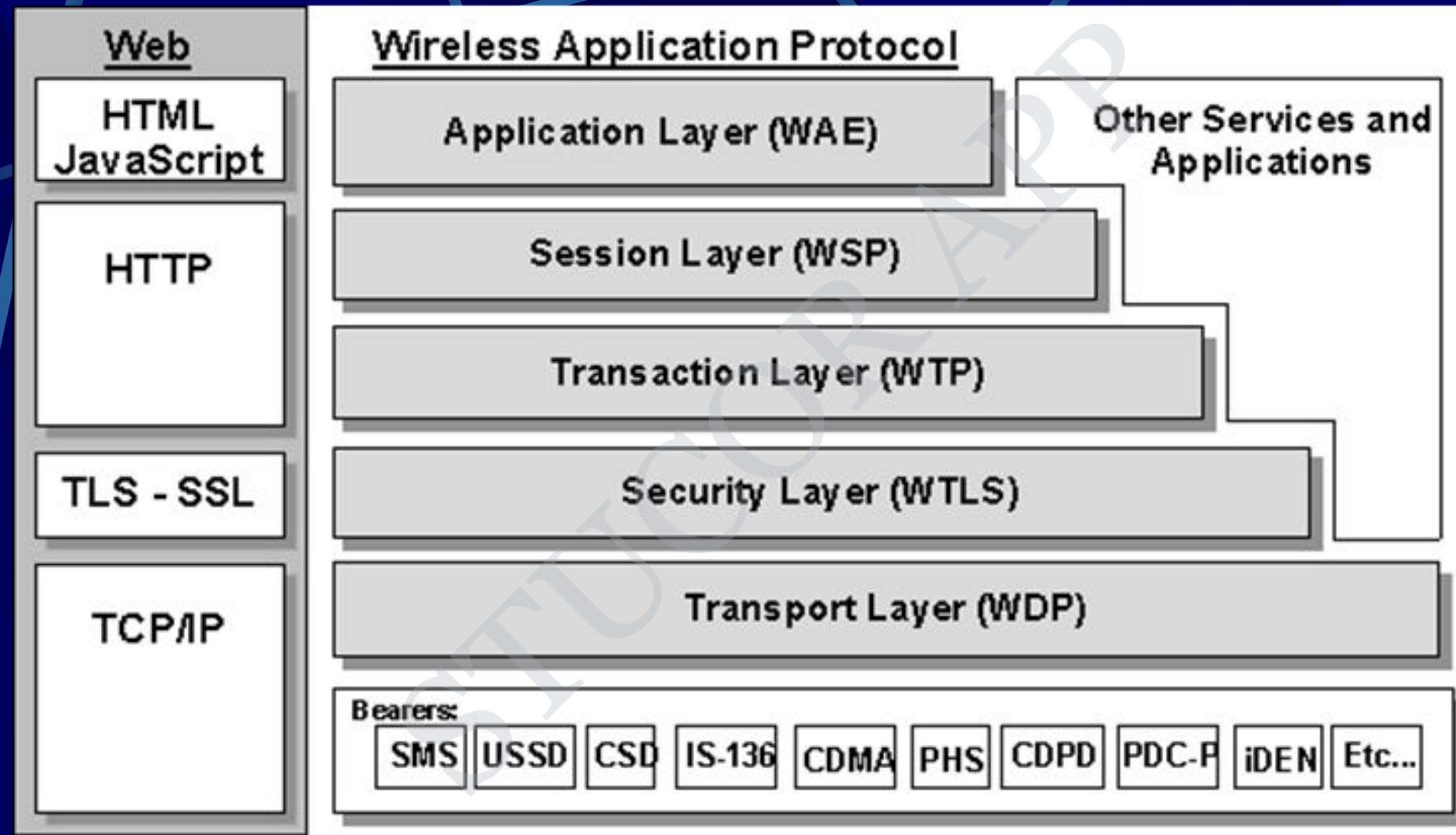
Transaction oriented TCP

- TCP phases
 - connection setup, data transmission, connection release
 - using 3-way-handshake needs 3 packets for setup and release, respectively
 - thus, even short messages need a minimum of 7 packets!
- Transaction oriented TCP
 - RFC1644, T-TCP, describes a TCP version to avoid this overhead
 - connection setup, data transfer and connection release can be combined
 - thus, only 2 or 3 packets are needed
- Advantage
 - efficiency
- Disadvantage
 - requires changed TCP
 - mobility no longer transparent

TABLE 5.2 A Comparative Study of a few Important Protocols for Mobile Applications

<i>TCP approach</i>	<i>Mechanism used</i>	<i>Merits</i>	<i>Demerits</i>
Indirect TCP (I-TCP)	Segments the TCP connection into two	<ul style="list-style-type: none"> • Simple • Isolation of wire and wireless links is possible 	<ul style="list-style-type: none"> • Loss of the TCP semantics • Security problem
Snooping TCP (S-TCP)	Snooping of data and acknowledgements	<ul style="list-style-type: none"> • Transparency • MCA interaction 	<ul style="list-style-type: none"> • Inadequate isolation of the wireless links • Security problem
Mobile TCP (M-TCP)	The segmented TCP connection can choke the sender through window sizes	<ul style="list-style-type: none"> • End-to-end segment is maintained • Handles frequent disconnections 	<ul style="list-style-type: none"> • Poor isolation wireless links • Security Problem
Fast retransmission	It avoids slow-start after any roaming	<ul style="list-style-type: none"> • Simple • More efficient 	<ul style="list-style-type: none"> • Not transparent • Mixed layers
Fast recovery			
Freeze-TCP	It freezes the TCP, later it resumes the TCP after reconnection	<ul style="list-style-type: none"> • Works even when there are long interruptions 	<ul style="list-style-type: none"> • Changes in TCP • MAC dependent

WAP



Layers of WAP Protocol

- **Application Layer**

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WML Script.

Session Layer

- **Wireless Session Protocol (WSP).** Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Security Layer

- Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.
- Transport Layer
- Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.
- Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.
- The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.

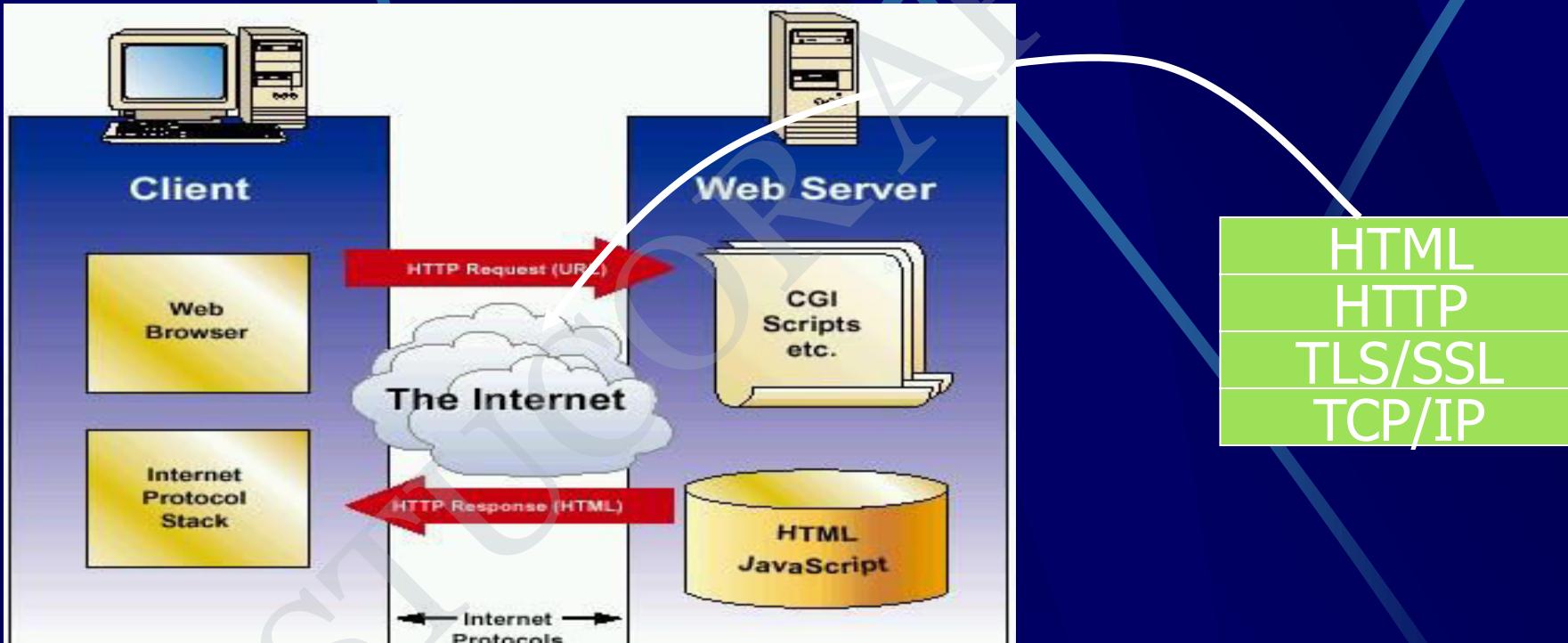
Wireless Application Protocol (WAP)

- Empowers mobile users with wireless devices to easily access and interact with information and services.
- A “standard” created by wireless and Internet companies to enable Internet access from a cellular phone
- wapforum.org:
 - co-founded by Ericsson, Motorola, Nokia, Phone.com
 - 450 members in 2000, comprise of Handset manufacturers, Wireless service providers, ISPs, Software companies in the wireless industry
 - Goals
 - deliver Internet services to mobile devices
 - enable applications to scale across a variety of transport options and device types
 - independence from wireless network standards
 - GSM, CDMA IS-95, TDMA IS-136, 3G systems (UMTS, W-CDMA)

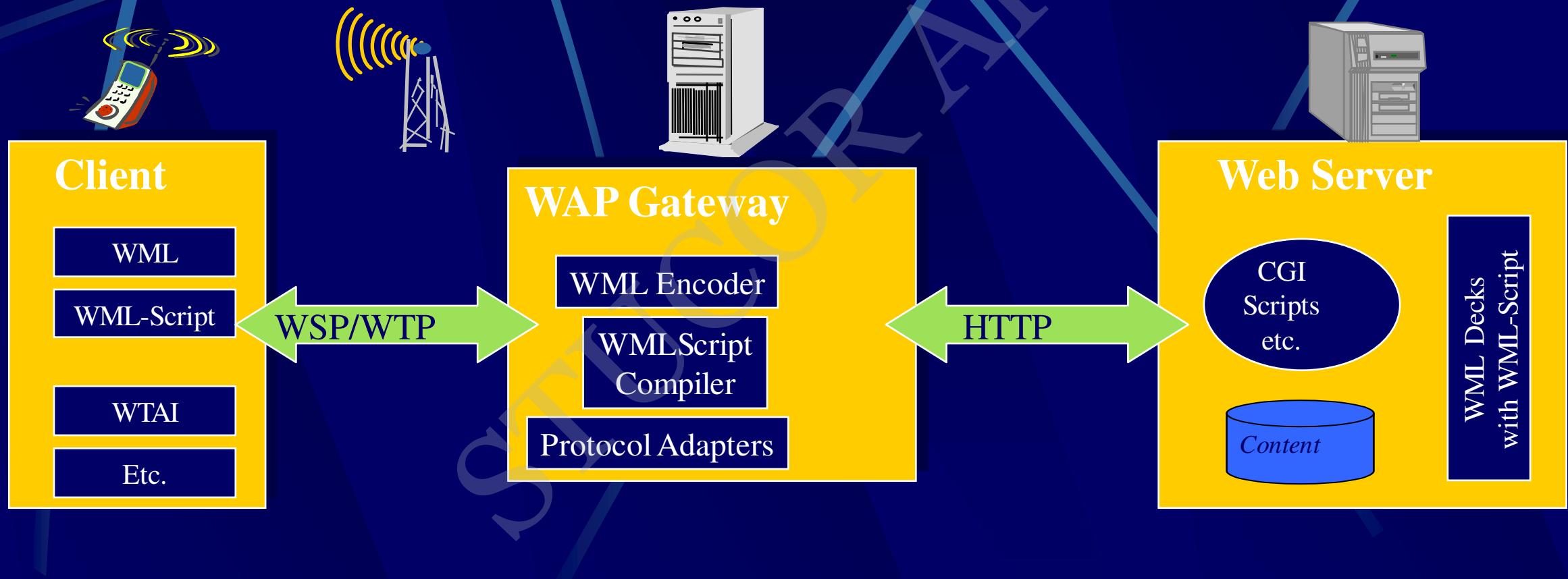
WAP: Main Features

- **Browser**
 - “Micro browser”, similar to existing web browsers
- **Markup language**
 - Similar to HTML, adapted to mobile devices
- **Script language**
 - Similar to Javascript, adapted to mobile devices
- **Gateway**
 - Transition from wireless to wired world
- **Server**
 - “Wap-Origin server”, similar to existing web servers
- **Protocol layers**
 - Transport layer, security layer, session layer etc.
- **Telephony application interface**
 - Access to telephony functions

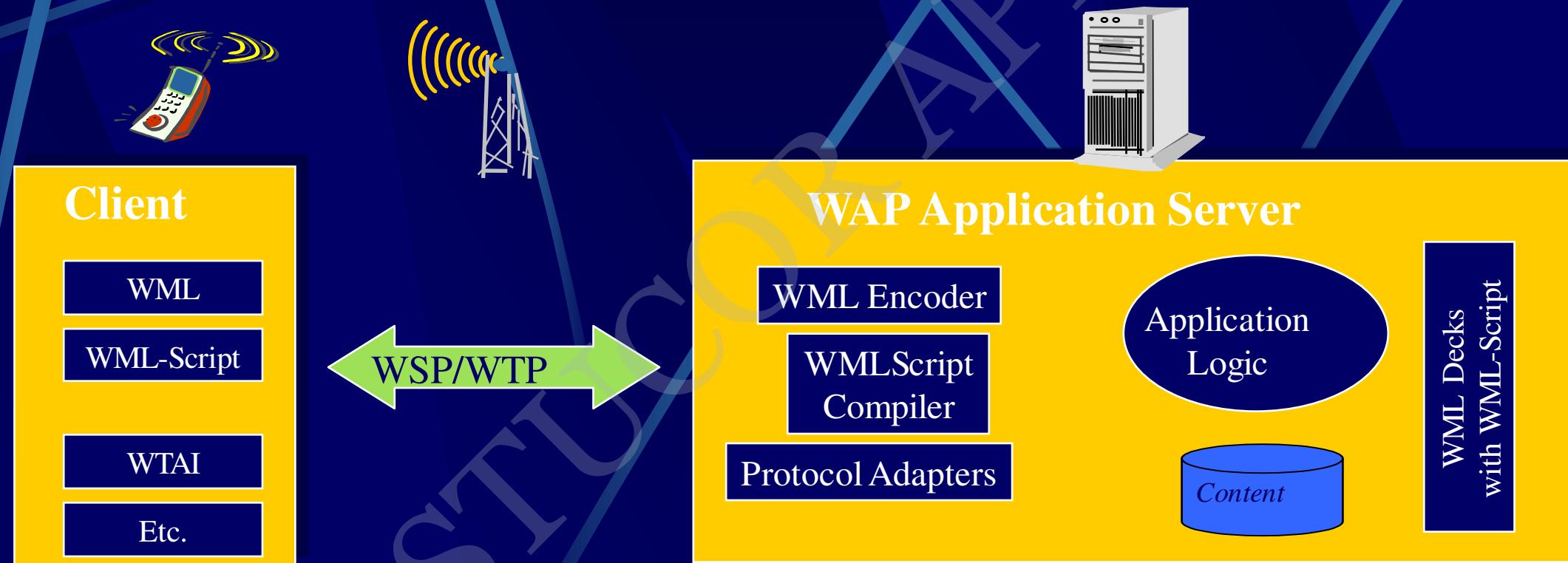
Internet Model



WAP Architecture

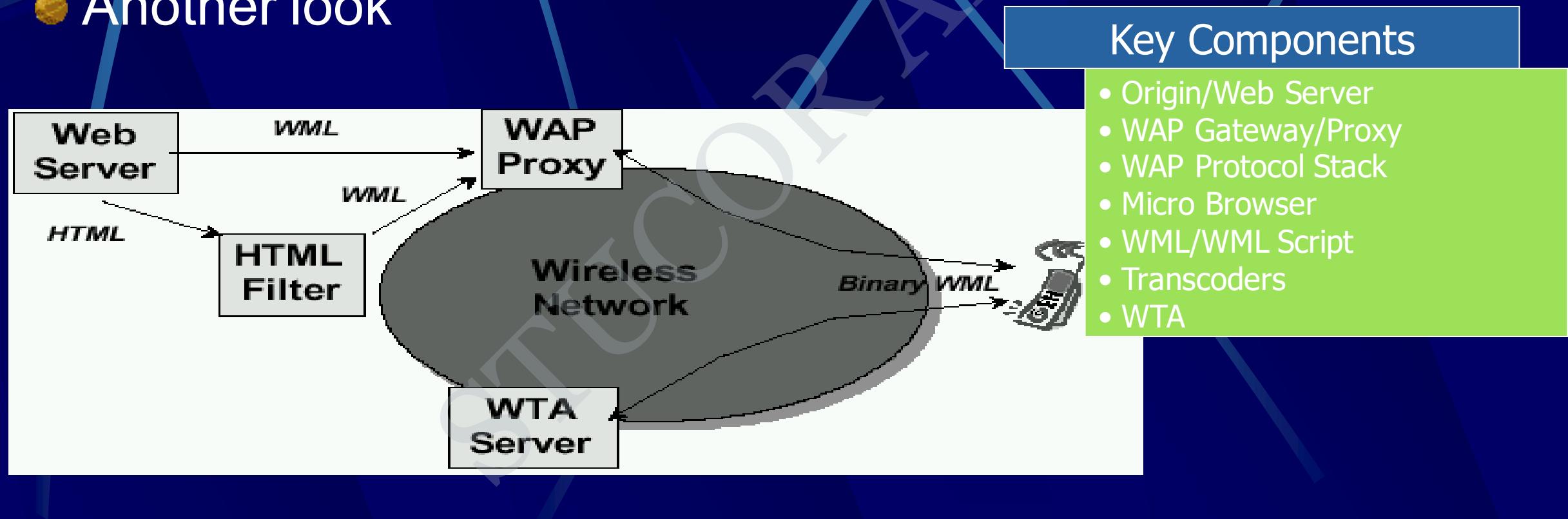


WAP Application Server

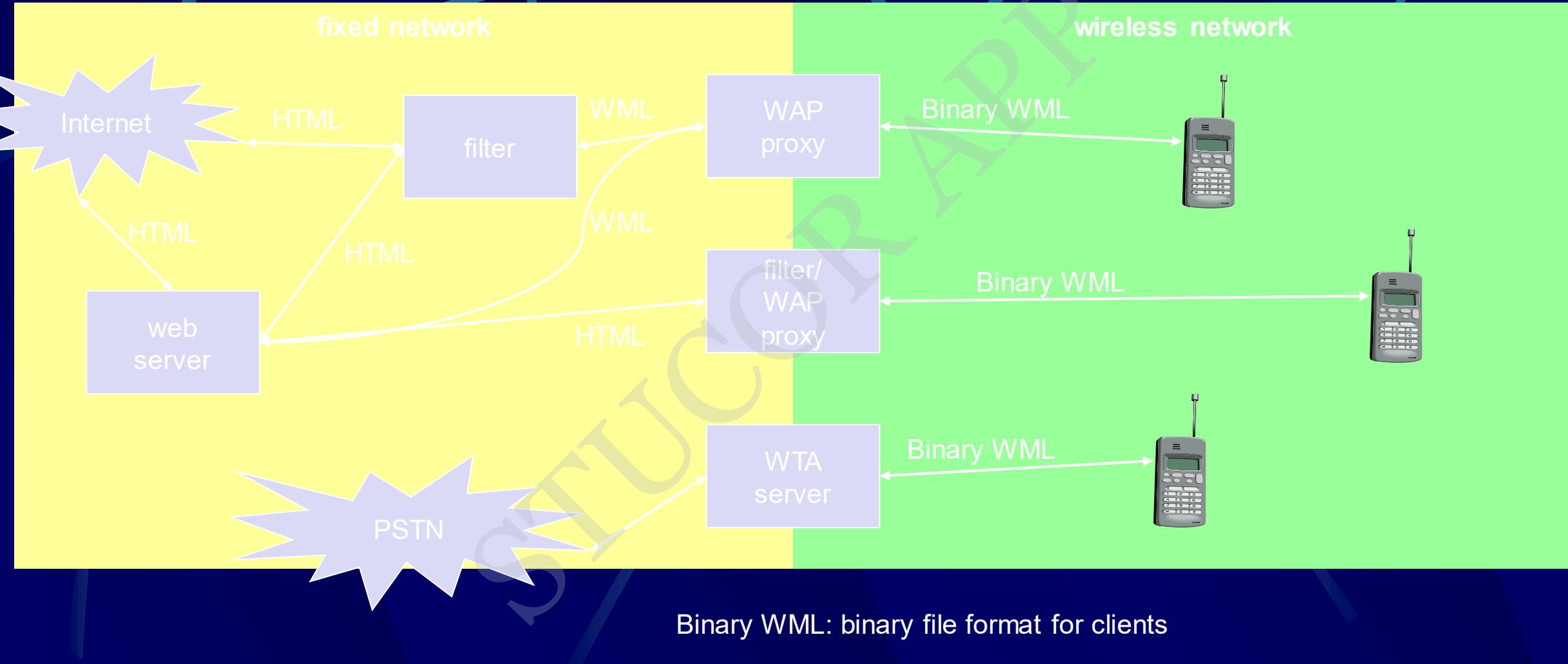


WAP Architecture

- Another look



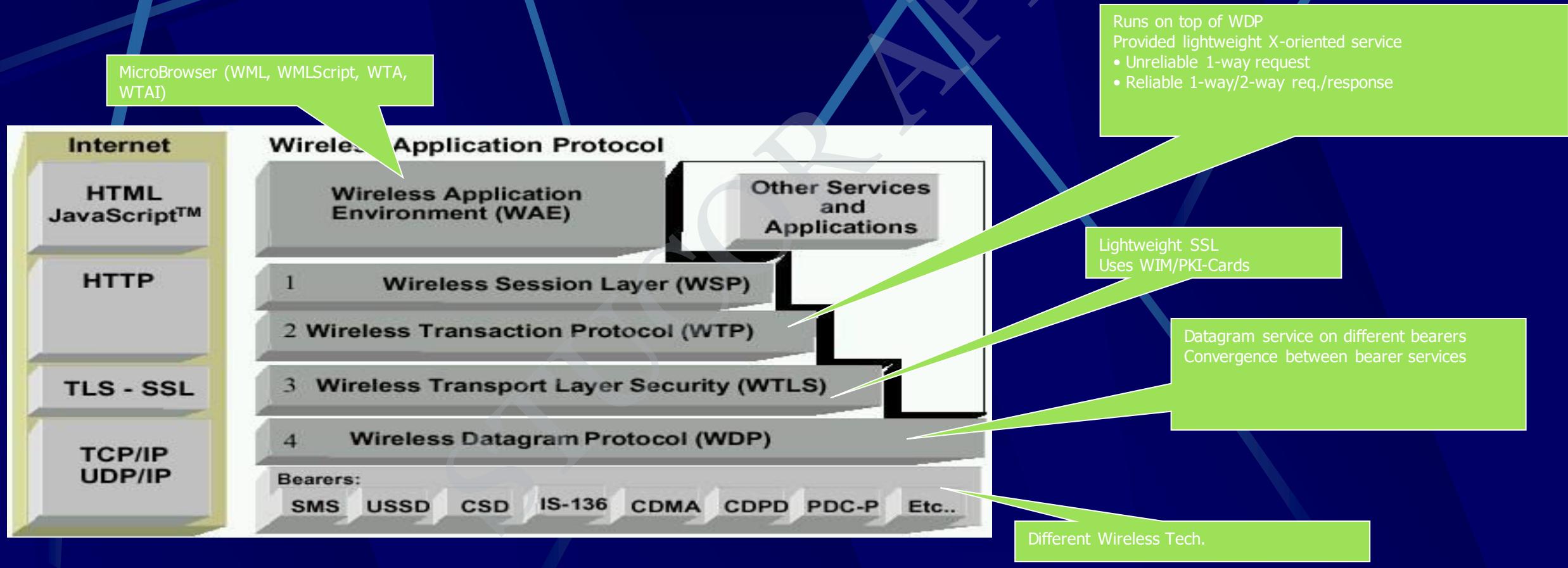
WAP: Network Elements



WAP Specifies

- **Wireless Application Environment**
 - WML Microbrowser
 - WMLScript Virtual Machine
 - WMLScript Standard Library
 - Wireless Telephony Application Interface (WTAI)
 - WAP content types
- **Wireless Protocol Stack**
 - Wireless Session Protocol (WSP)
 - Wireless Transport Layer Security (WTLS)
 - Wireless Transaction Protocol (WTP)
 - Wireless Datagram Protocol (WDP)
 - Wireless network interface definitions

WAP Stack



WAP Stack

- **WAE (Wireless Application Environment):**
 - Architecture: application model, browser, gateway, server
 - WML: XML-Syntax, based on card stacks, variables, ...
 - WTA: telephone services, such as call control, phone book etc.
- **WSP (Wireless Session Protocol):**
 - Provides HTTP 1.1 functionality
 - Supports session management, security, etc.
- **WTP (Wireless Transaction Protocol):**
 - Provides reliable message transfer mechanisms
 - Based on ideas from TCP/RPC
- **WTLS (Wireless Transport Layer Security):**
 - Provides data integrity, privacy, authentication functions
 - Based on ideas from TLS/SSL
- **WDP (Wireless Datagram Protocol):**
 - Provides transport layer functions
 - Based on ideas from UDP

Wireless Application Environment (WAE)

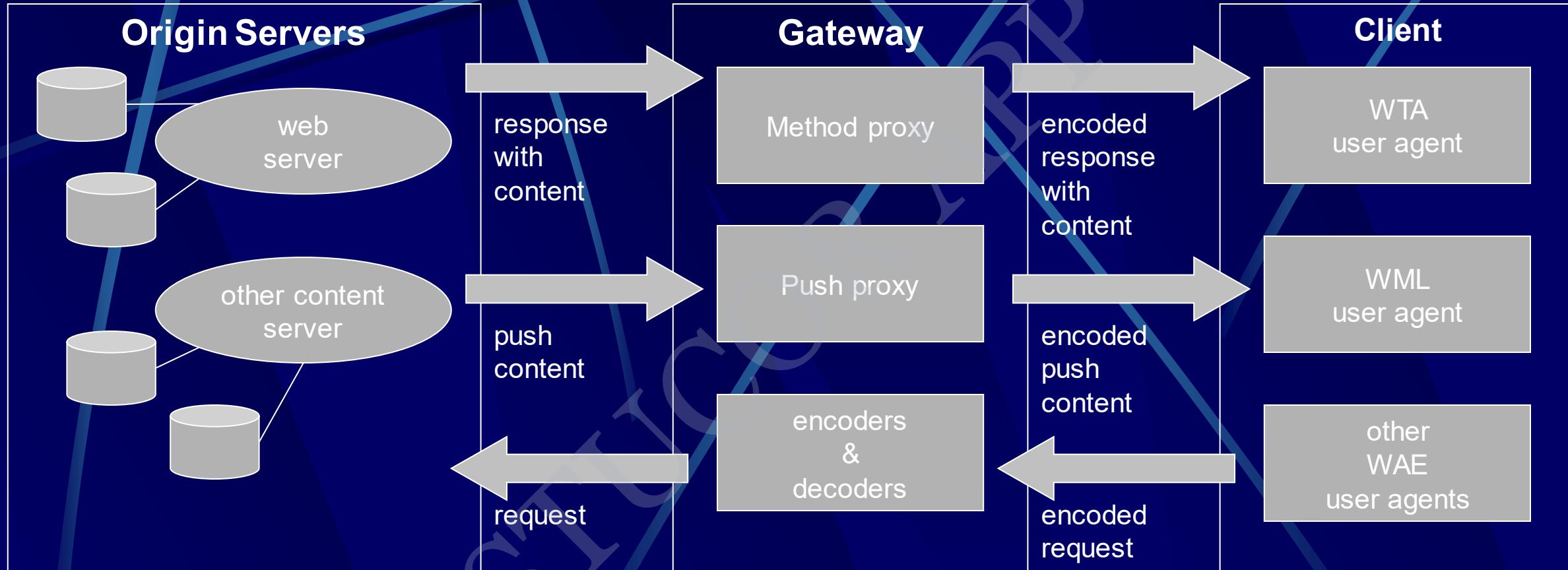
● Goals

- device and network independent application environment
- for low-bandwidth, wireless devices
- considerations of slow links, limited memory, low computing power, small display, simple user interface (compared to desktops)
- integrated Internet/WWW programming model
- high interoperability

WAE Components

- **Architecture**
 - Application model, Microbrowser, Gateway, Server
- **User Agents**
 - WML/WTA/Others
 - content formats: vCard, vCalendar, Wireless Bitmap, WML, ...
- **WML**
 - XML-Syntax, based on card stacks, variables, ...
- **WMLScript**
 - procedural, loops, conditions, ... (similar to JavaScript)
- **WTA**
 - telephone services, such as call control, text messages, phone book, ... (accessible from WML/WMLScript)
- **Proxy (Method/Push)**

WAE: Logical Model



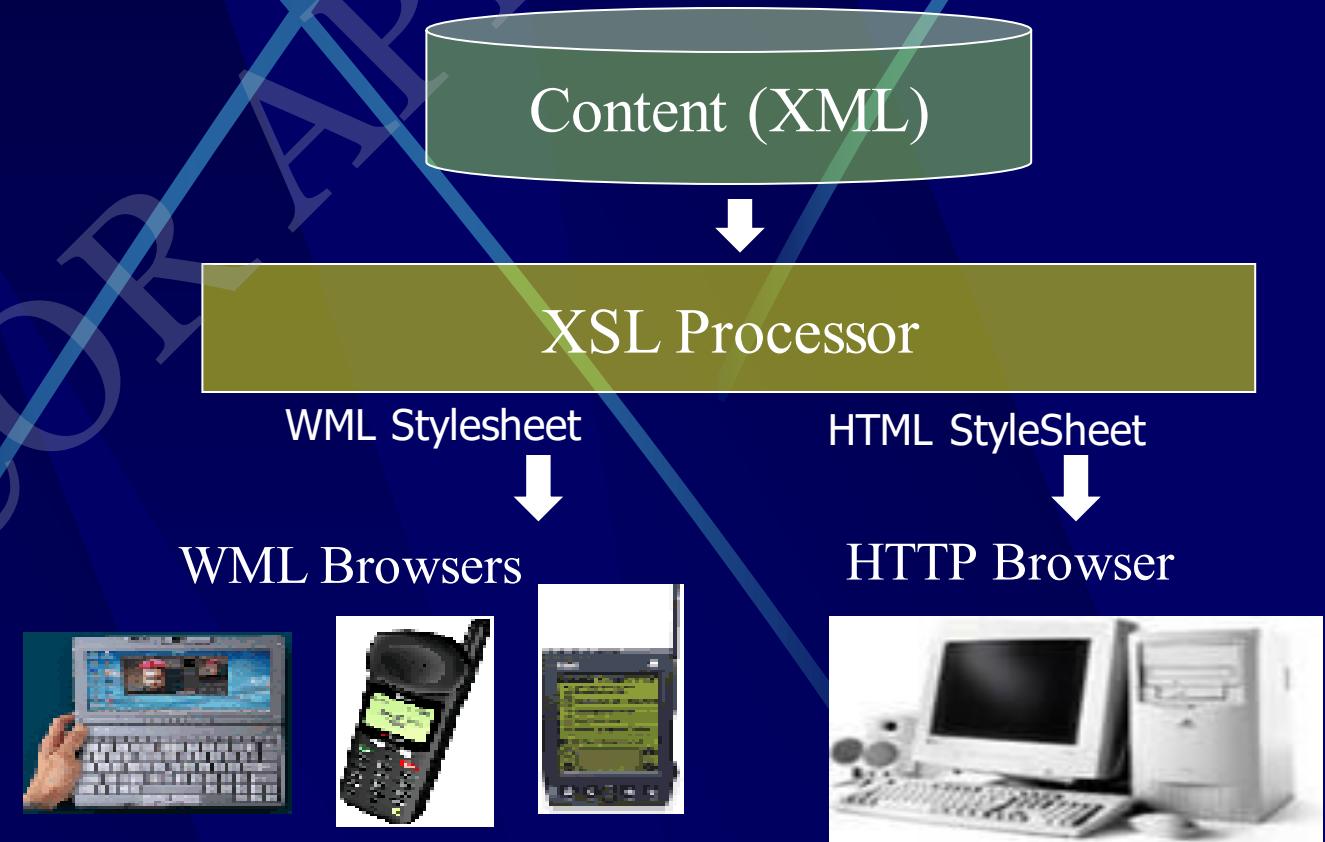
WAP Microbrowser



- Optimized for wireless devices
- Minimal RAM, ROM, Display, CPU and keys
- Provides consistent service UI across devices
- Provides Internet compatibility
- Enables wide array of available content and applications

WML: Wireless Markup Language

- Tag-based browsing language:
 - Screen management (text, images)
 - Data input (text, selection lists, etc.)
 - Hyperlinks & navigation support
- Takes into account limited display, navigation capabilities of devices
- XML-based language
 - describes only intent of interaction in an abstract manner
 - presentation depends upon device capabilities
- Cards and Decks
 - document consists of many cards
 - User interactions are split into cards
 - Explicit navigation between cards
 - cards are grouped to decks
 - deck is similar to HTML page, unit of content transmission
- Events, variables and state mgmt



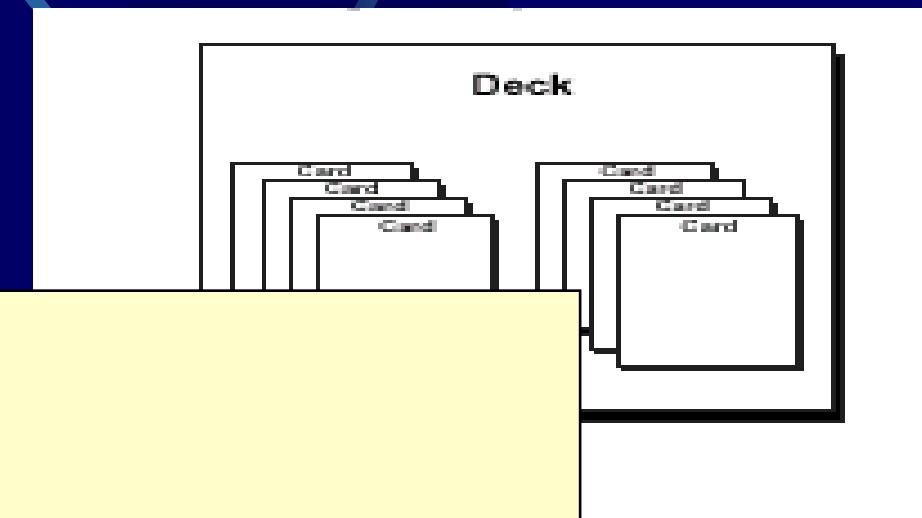
WML

- The basic unit is a **card**. Cards are grouped together into **Decks** Document ~ Deck (unit of transfer)
- All decks must contain
 - Document prologue
 - XML & document type declaration
 - **<WML>** element
 - Must contain one or more cards

WML File Structure

```
<?xml version="1.0"?>
<!DOCTYPE WML PUBLIC "-//WAPFORUM//DTD WML 1.0//EN"
  "http://www.wapforum.org/DTD/wml.xml">

<WML>
  ...
</WML>
```



WML Example

Navigation

Variables

Input Elements

```
<WML>
<CARD>
  <DO TYPE="ACCEPT">
    <GO URL="#eCard" />
  </DO>
  Welcome!
</CARD>
<CARD NAME="eCard">
  <DO TYPE="ACCEPT">
    <GO URL="/submit?N=$ (N) &S=$ (S)" />
  </DO>
  Enter name: <INPUT KEY="N"/>
  Choose speed:
  <SELECT KEY="S">
    <OPTION VALUE="0">Fast</OPTION>
    <OPTION VALUE="1">Slow</OPTION>
  <SELECT>
</CARD>
</WML>
```

Card

Deck

Wireless Telephony Application (WTA)

- Collection of telephony specific extensions
 - designed primarily for network operators
- Example
 - calling a number (WML)
wtai://wp/mc;07216086415
 - calling a number (WMLScript)
WTAPublic.makeCall("07216086415");
- Implementation
 - Extension of basic WAE application model
 - Extensions added to standard WML/WMLScript browser
 - Exposes additional API (WTAI)

WTA Features

- Extension of basic WAE application model
 - network model for interaction
 - client requests to server
 - event signaling: server can push content to the client
 - event handling
 - table indicating how to react on certain events from the network
 - client may now be able to handle unknown events
 - telephony functions
 - some application on the client may access telephony functions
- WTAI includes:
 - Call control
 - Network text messaging
 - Phone book interface
 - Event processing
- Security model: segregation
 - Separate WTA browser
 - Separate WTA port

WTA Example (WML)

Placing an outgoing call with WTAI:

WTAI Call

Input Element

```
<WML>
  <CARD>
    <DO TYPE="ACCEPT">
      <GO URL="wtai:cc/mc;$ (N) "/>
    </DO>
    Enter phone number:
    <INPUT TYPE="TEXT" KEY="N"/>
  </CARD>
</WML>
```

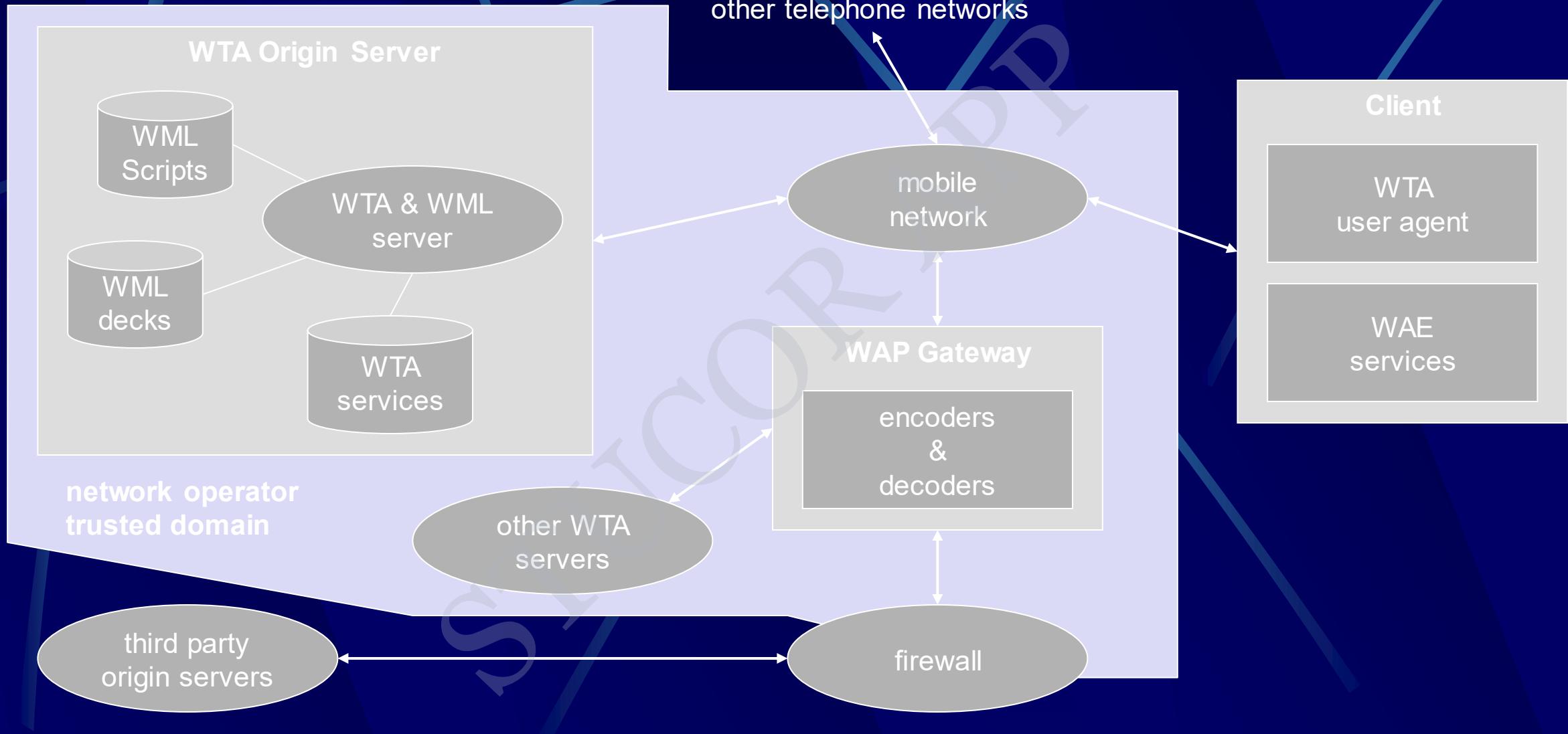
WTA Example (WMLScript)

Placing an outgoing call with WTAI:

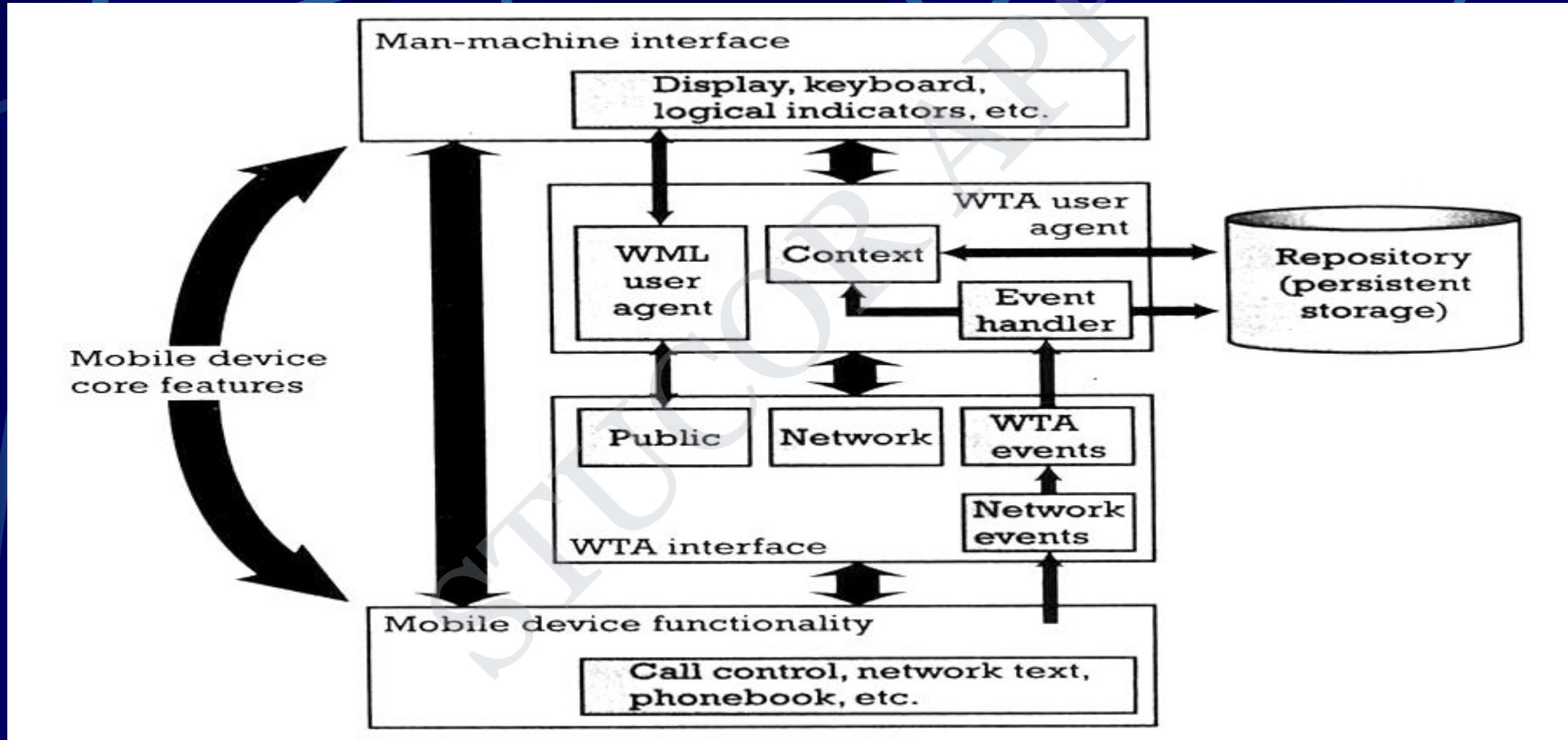
WTAI Call

```
function checkNumber(N) {  
    if (Lang.toInt(N))  
        WTAI.makeCall (N);  
    else  
        Dialog.alert("Bad phone number");  
}
```

WTA Logical Architecture



WTA Framework Components



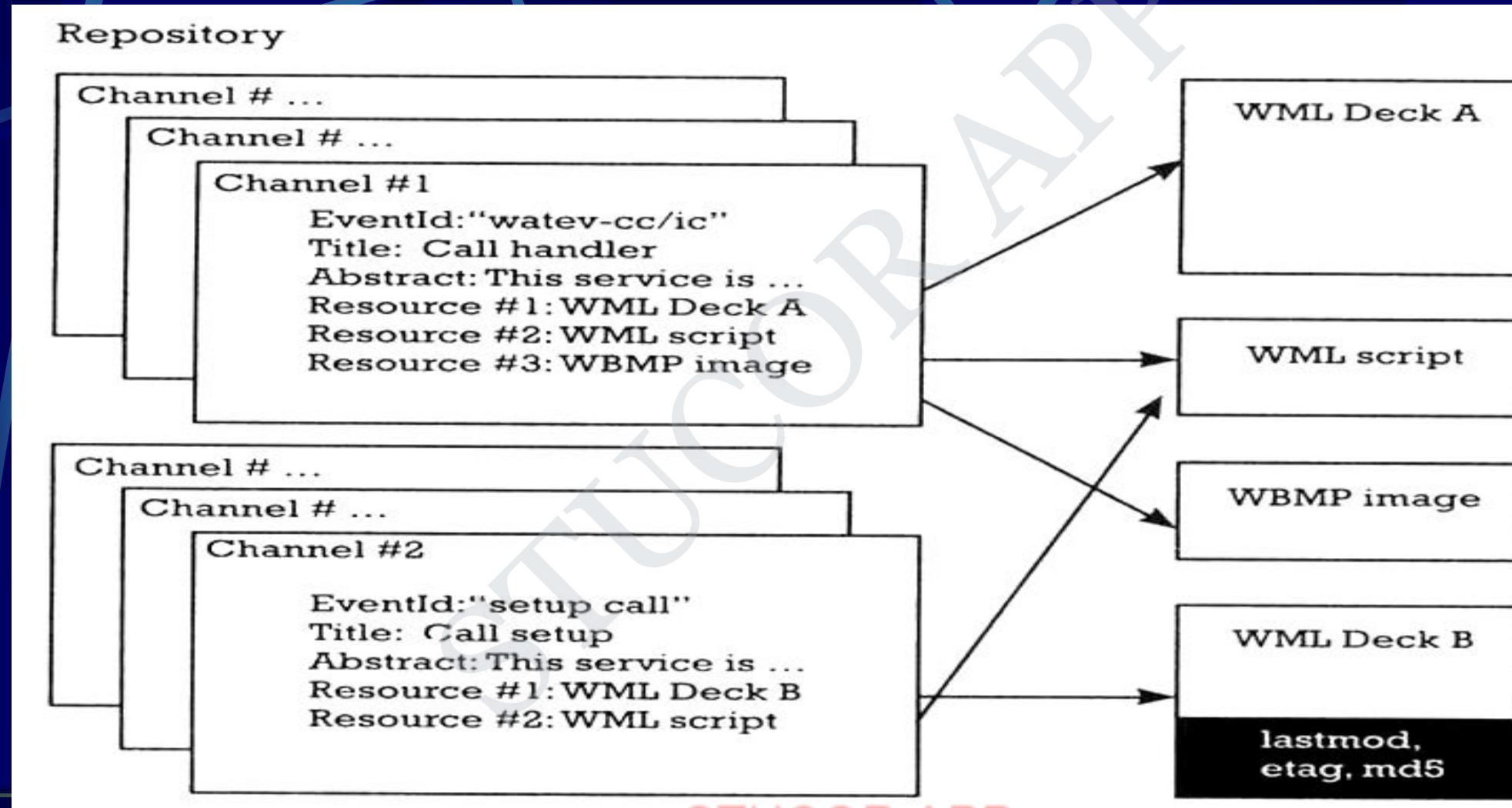
WTA User Agent

- **WTA User Agent**
 - WML User agent with extended functionality
 - can access mobile device's telephony functions through WTAI
 - can store WTA service content persistently in a repository
 - handles events originating in the mobile network
- **WTA User Agent Context**
 - Abstraction of execution space
 - Holds current parameters, navigation history, state of user agent
 - Similar to activation record in a process address space
- Uses connection-mode and connectionless services offered by WSP
- Specific, secure WDP ports on the WAP gateway

WTA Events and Repository

- **WTA Events**
 - Network notifies device of event (such as incoming call)
 - WTA events map to device's native events
 - WTA services are aware of and able to act on these events
 - example: incoming call indication, call cleared, call connected
- **WTA Repository**
 - local store for content related to WTA services (minimize network traffic)
 - **Channels:** define the service
 - content format defining a WTA service stored in repository
 - XML document specifying eventid, title, abstract, and resources that implement a service
 - **Resources:** execution scripts for a service
 - could be WML decks, WML Scripts, WBMP images..
 - downloaded from WTA server and stored in repository before service is referenced
 - Server can also initiate download of a channel

WTA Channels and Resources



WAP: Protocol Stack

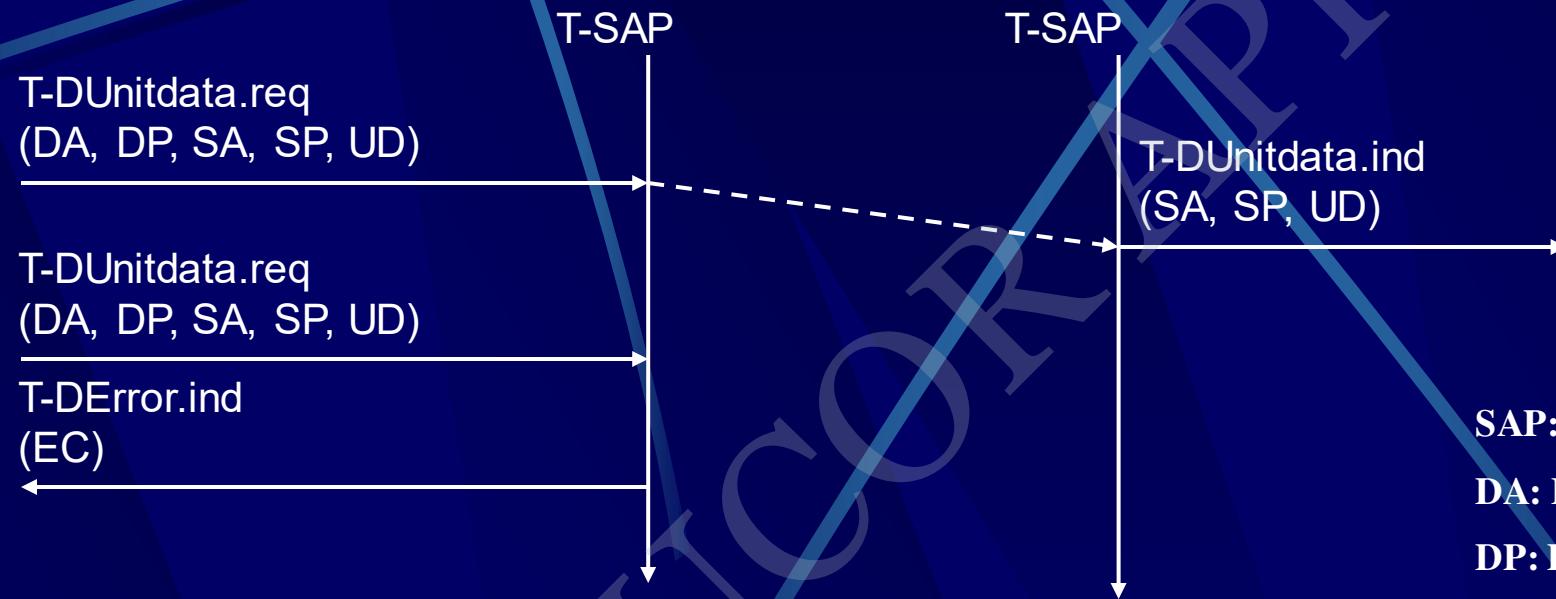


WAE comprises WML (Wireless Markup Language), WML Script, WTAI etc.

WDP: Wireless Datagram Protocol

- Goals
 - create a worldwide interoperable transport system by adapting WDP to the different underlying technologies
 - transmission services, such as SMS in GSM might change, new services can replace the old ones
- WDP
 - Transport layer protocol within the WAP architecture
 - uses the Service Primitive
 - T-UnitData.req .ind
 - uses transport mechanisms of different bearer technologies
 - offers a common interface for higher layer protocols
 - allows for transparent communication despite different technologies
 - addressing uses port numbers
 - WDP over IP is UDP/IP

WDP: Service Primitives



SAP: Service Access Point

DA: Destination Address

DP: Destination Port

SA: Source Address

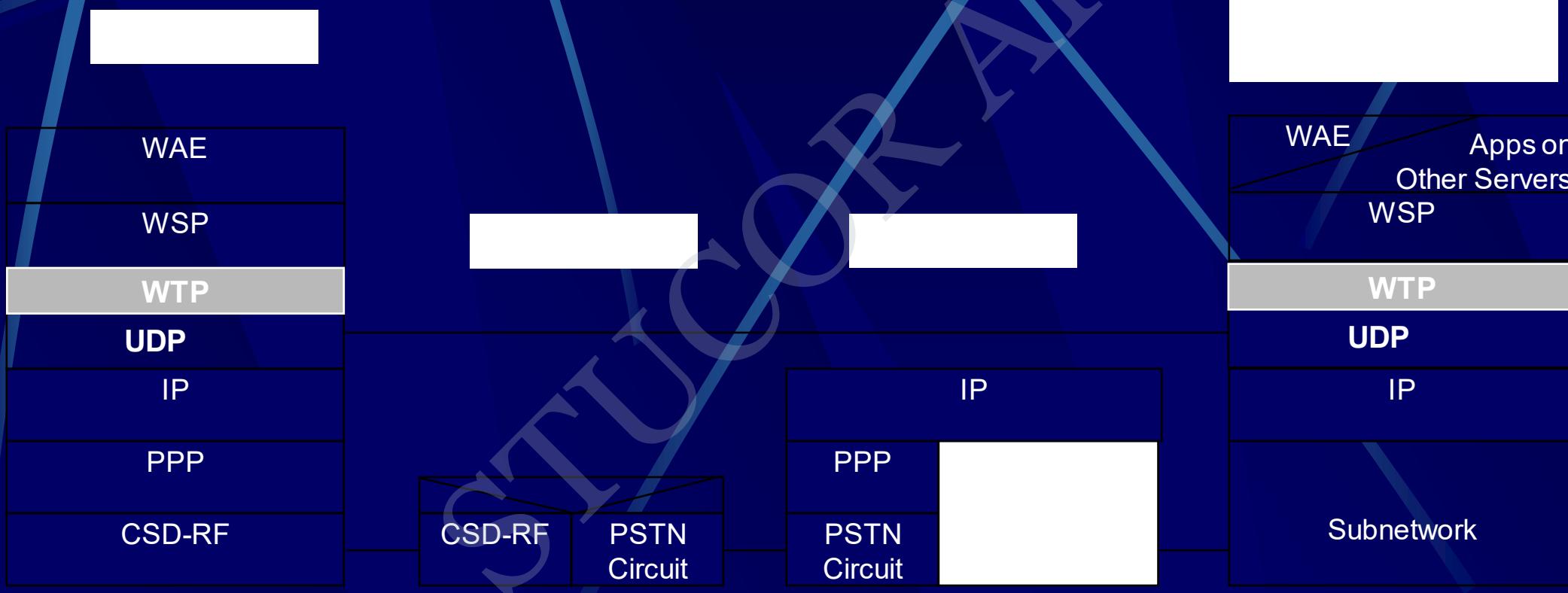
SP: Source Port

UD: User Data

EC: Error Code

Service, Protocol, and Bearer Example

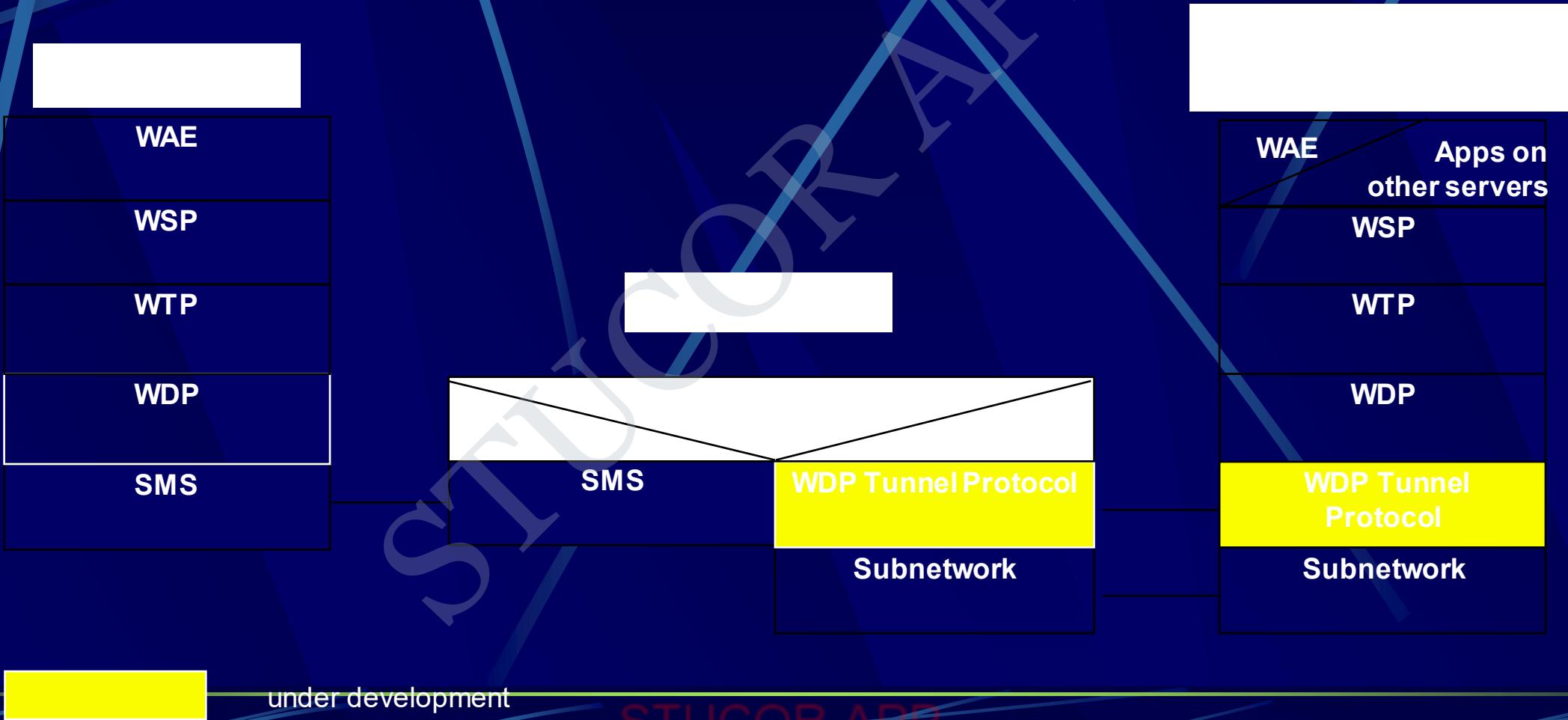
WAP Over GSM Circuit-Switched



RAS - Remote Access Server
IWF - InterWorking Function

Source: WAP Forum

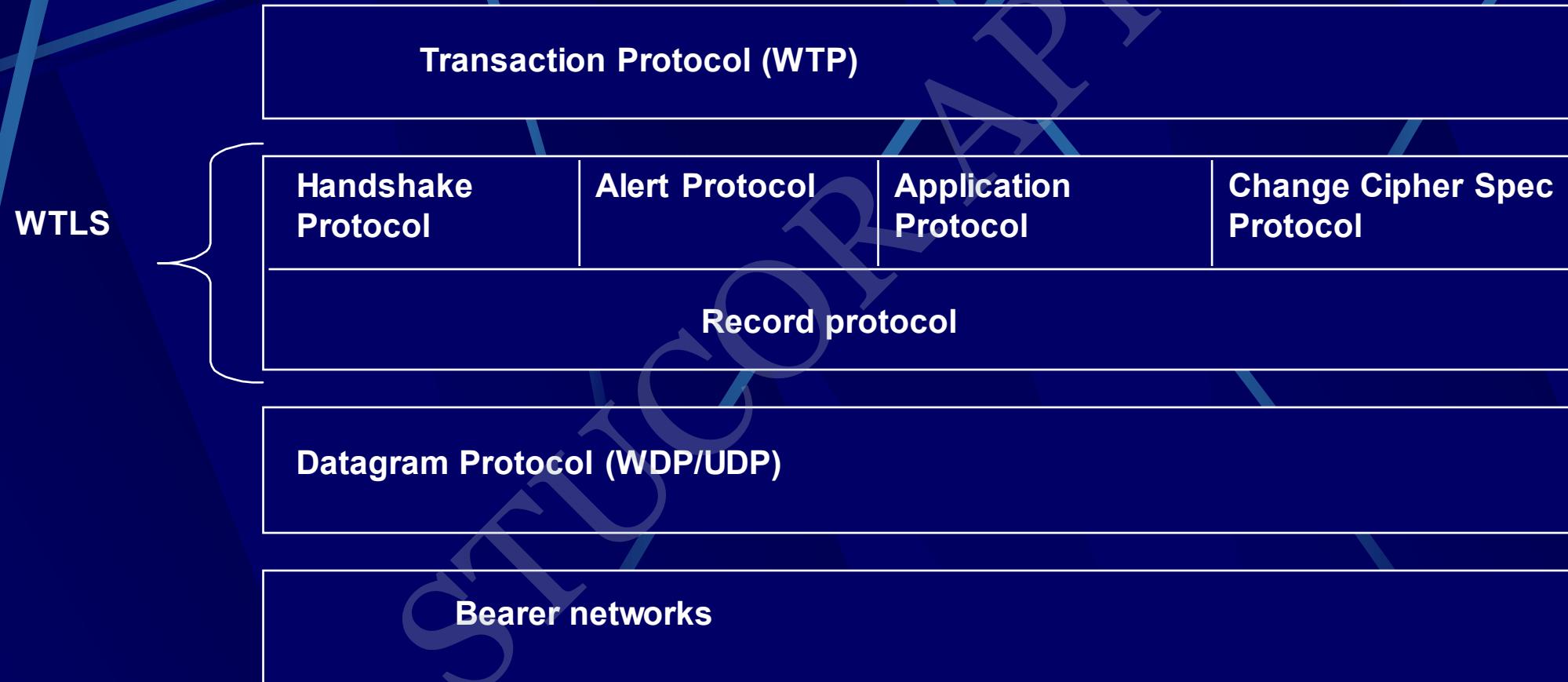
Service, Protocol, and Bearer Example



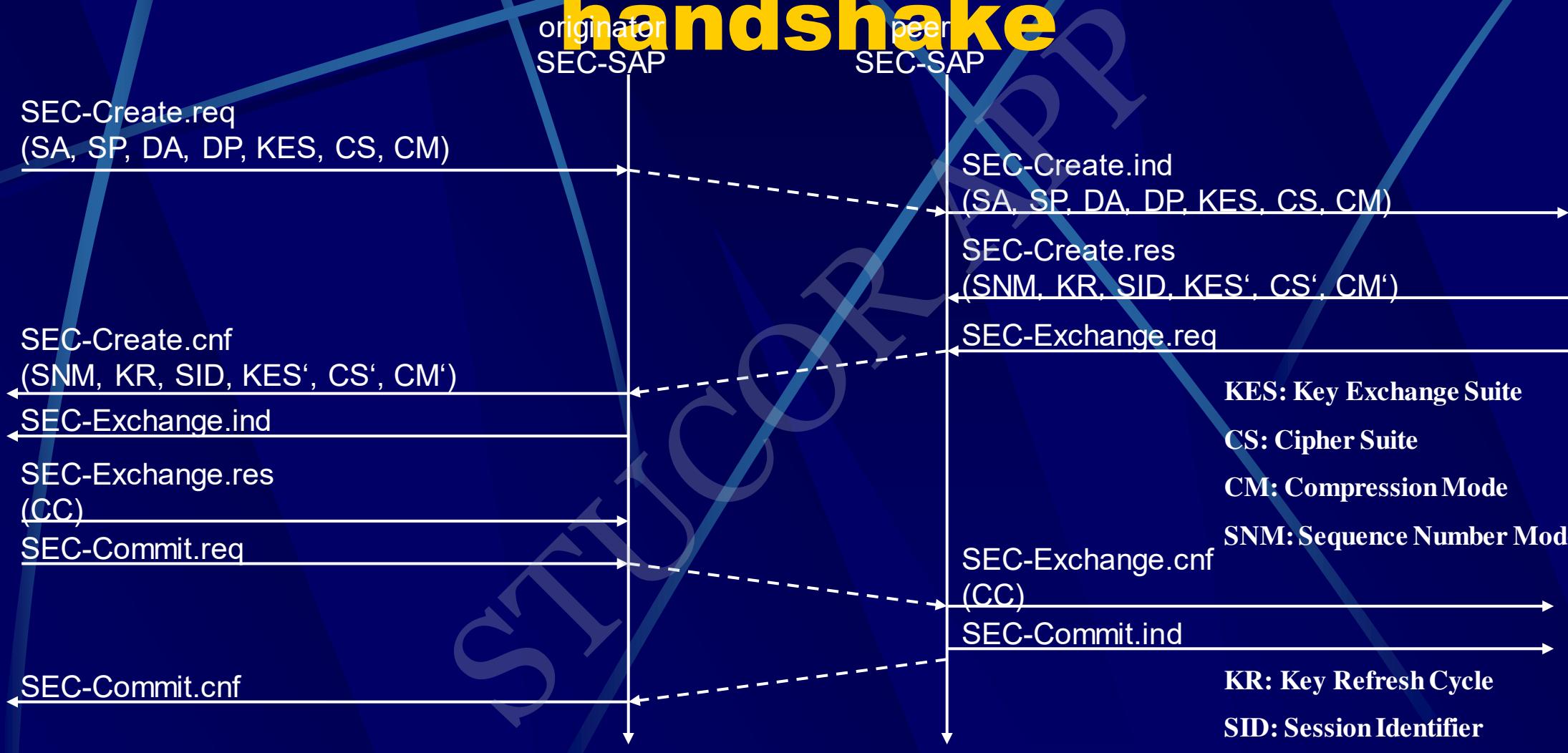
WTLS:Wireless Transport Layer Security

- Goals
 - Provide mechanisms for secure transfer of content, for applications needing privacy, identification, message integrity and non-repudiation
 - Provide support for protection against denial-of-service attacks
- WTLS
 - is based on the TLS/SSL (Transport Layer Security) protocol
 - optimized for low-bandwidth communication channels
 - provides
 - privacy (encryption)
 - data integrity (MACs)
 - authentication (public-key and symmetric)
 - Employs special adapted mechanisms for wireless usage
 - Long lived secure sessions
 - Optimised handshake procedures
 - Provides simple data reliability for operation over datagram bearers

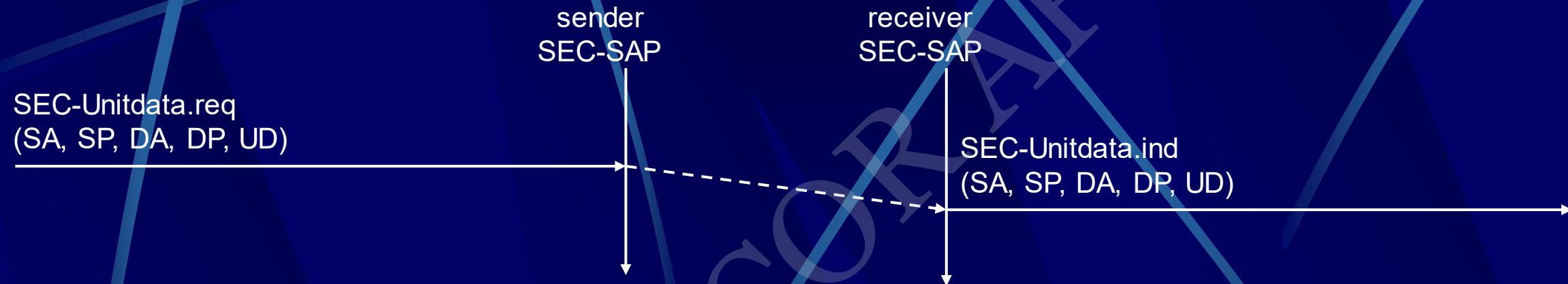
WTLS Internal Architecture



WTLS: Secure session, Full handshake



WTLS: Transferring Datagrams



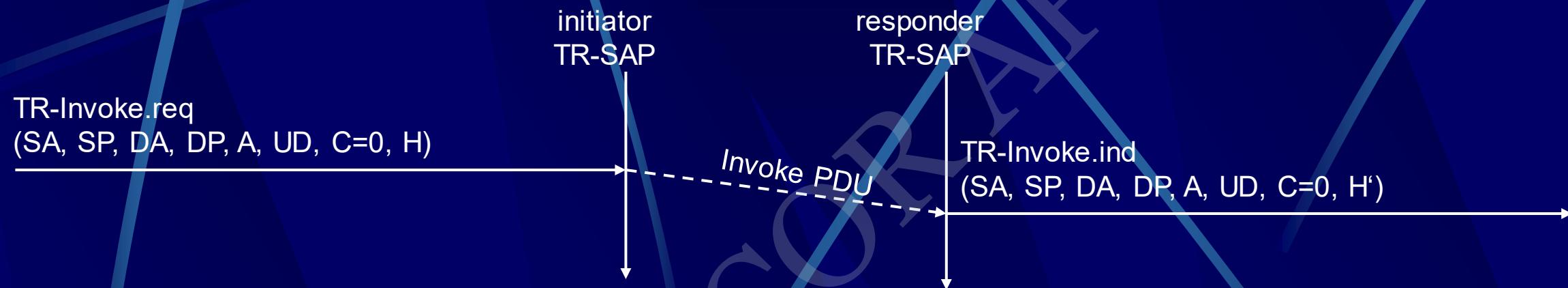
WTP: Wireless Transaction Protocol

- Goals
 - different transaction services that enable applications to select reliability, efficiency levels
 - low memory requirements, suited to simple devices (< 10kbyte)
 - efficiency for wireless transmission
- WTP
 - supports peer-to-peer, client/server and multicast applications
 - efficient for wireless transmission
 - support for different communication scenarios
 - **class 0:** unreliable message transfer
 - unconfirmed Invoke message with no Result message
 - a datagram that can be sent within the context of an existing Session
 - **class 1:** reliable message transfer without result message
 - confirmed Invoke message with no Result message
 - used for data push, where no response from the destination is expected
 - **class 2:** reliable message transfer with exactly one reliable result message
 - confirmed Invoke message with one confirmed Result message
 - a single request produces a single reply

WTP Services and Protocols

- WTP (Transaction)
 - provides reliable data transfer based on request/reply paradigm
 - no explicit connection setup or tear down
 - optimized setup (data carried in first packet of protocol exchange)
 - seeks to reduce 3-way handshake on initial request
 - supports
 - header compression
 - segmentation /re-assembly
 - retransmission of lost packets
 - selective-retransmission
 - port number addressing (UDP ports numbers)
 - flow control
 - message oriented (not stream)
 - supports an Abort function for outstanding requests
 - supports concatenation of PDUs
 - supports User acknowledgement or Stack acknowledgement option
 - acks may be forced from the WTP user (upper layer)
 - default is stack ack

WTP Class 0 Transaction

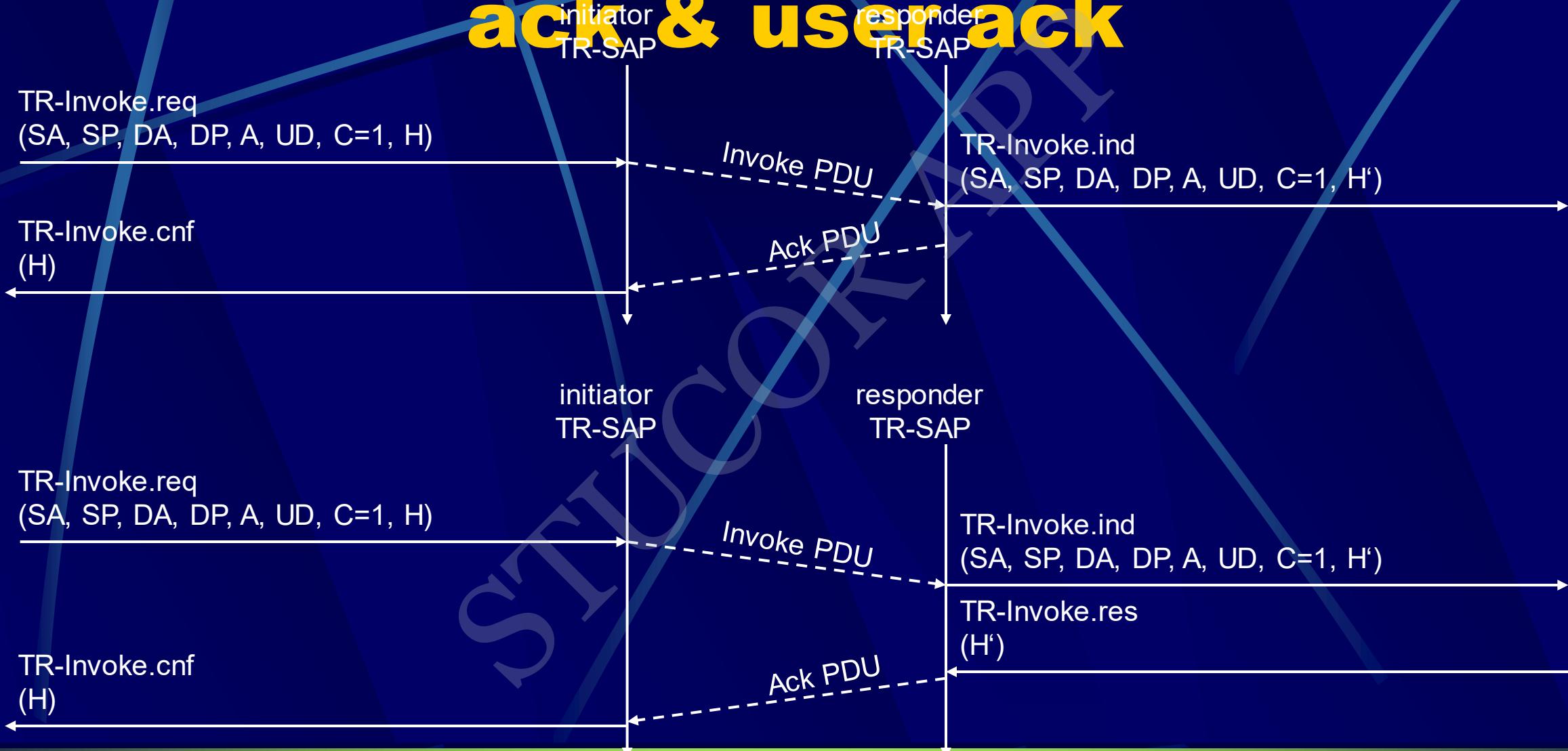


A: Acknowledgement Type
(WTP/User)

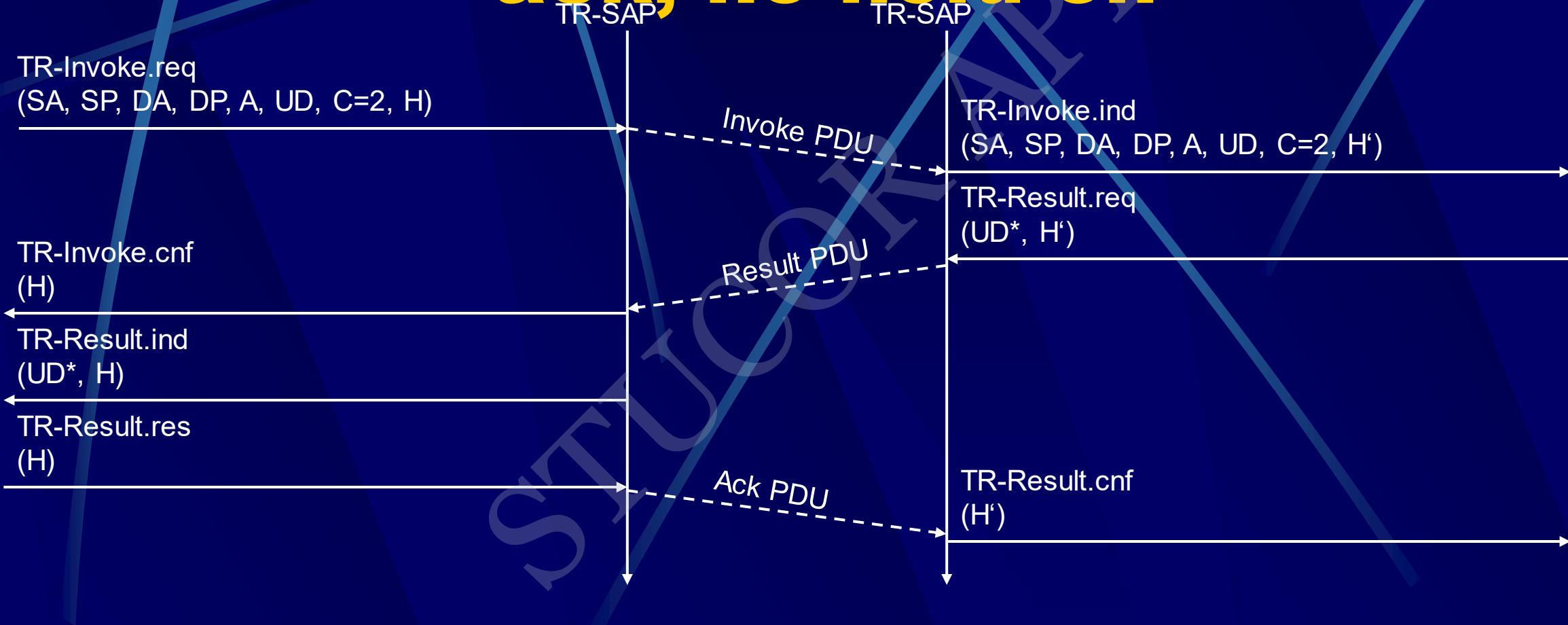
C: Class (0,1,2)

H: Handle (socket alias)

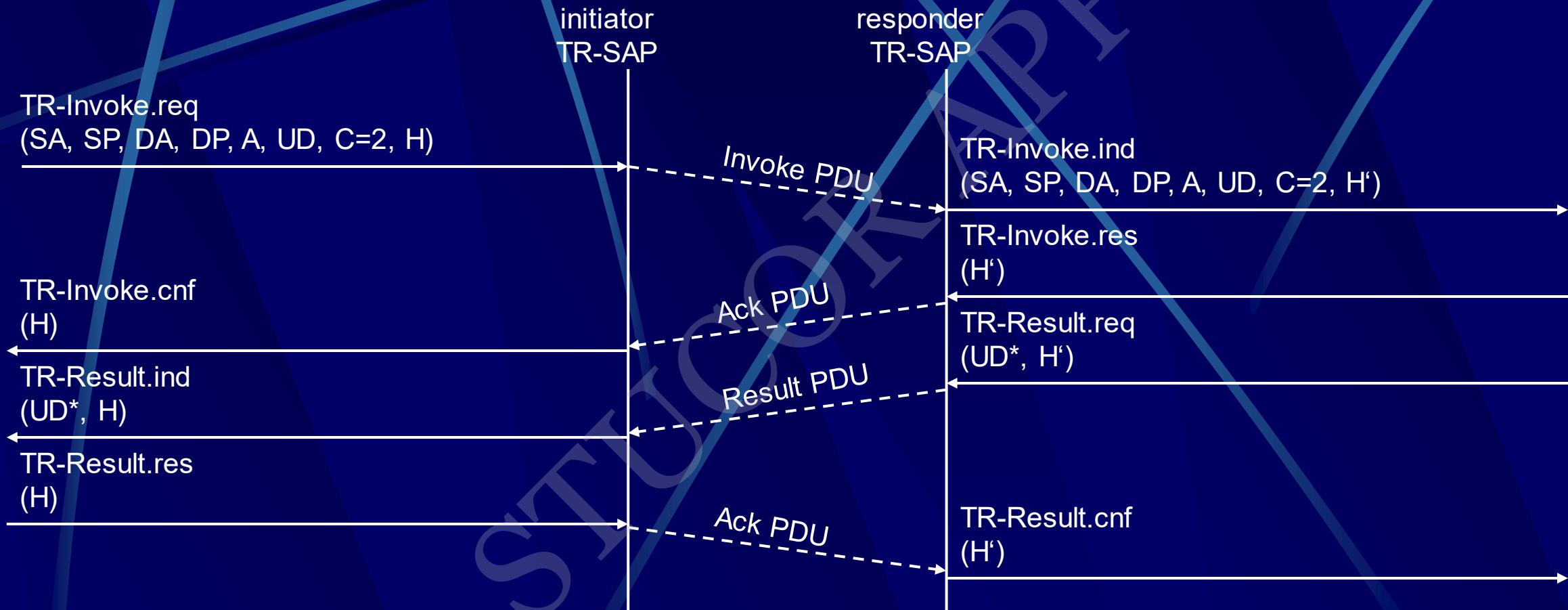
WTP Class 1 Transaction, no user ack & user ack



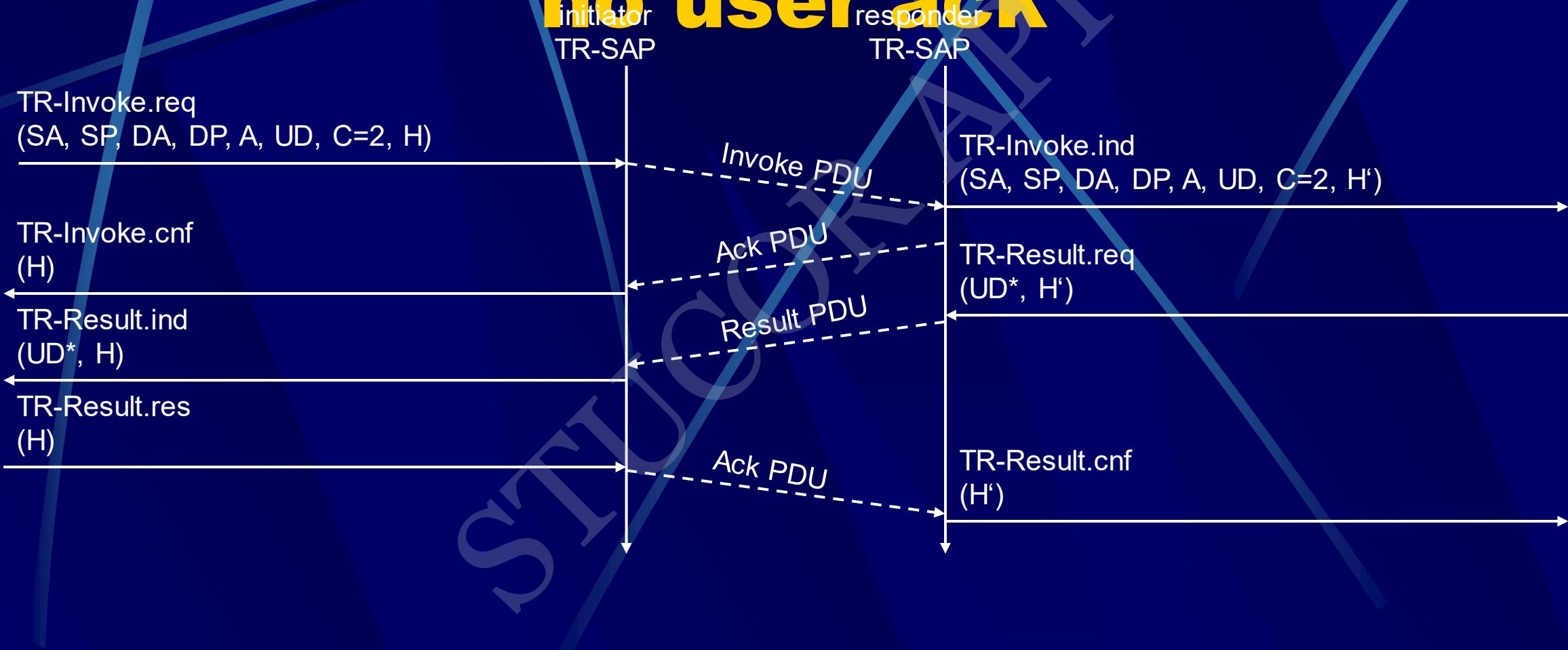
WTP Class 2 Transaction, no user ack, no hold on



WTP Class 2 Transaction, user ack



WTP Class 2 Transaction, hold on, no user ack



WSP - Wireless Session Protocol

- Goals
 - HTTP 1.1 functionality
 - Request/reply, content type negotiation, ...
 - support of client/server transactions, push technology
 - key management, authentication, Internet security services
- WSP Services
 - provides shared state between client and server, optimizes content transfer
 - session management (establish, release, suspend, resume)
 - efficient capability negotiation
 - content encoding
 - push
- WSP/B (Browsing)
 - HTTP/1.1 functionality - but binary encoded
 - exchange of session headers
 - push and pull data transfer

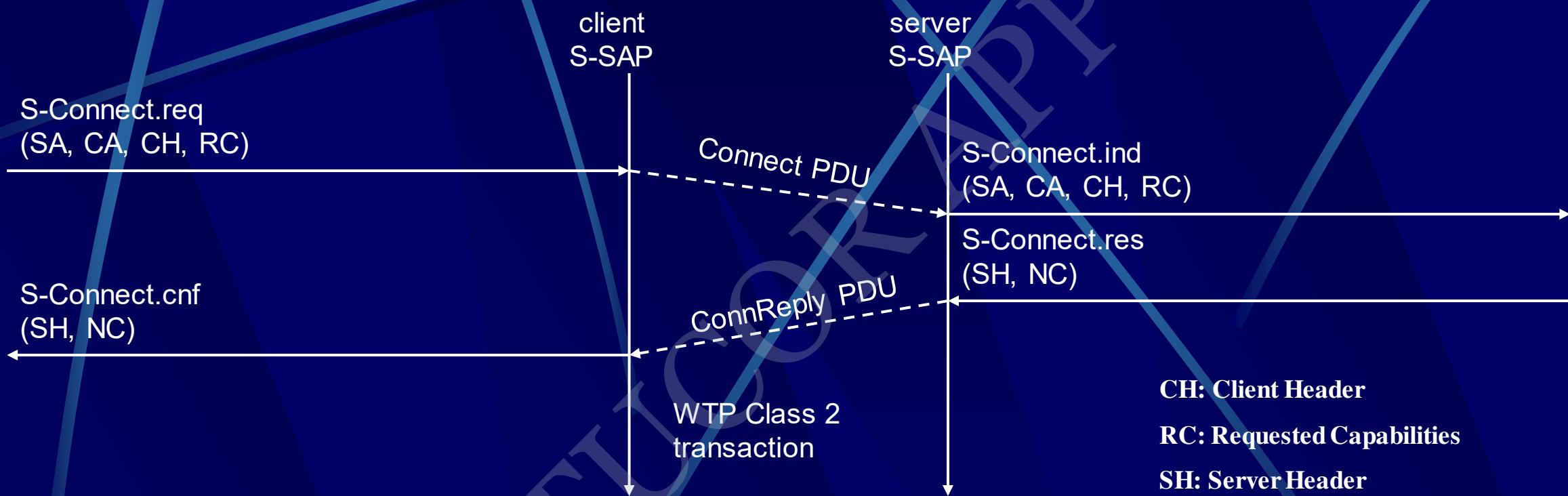
WSP Overview

- **Header Encoding**
 - compact binary encoding of headers, content type identifiers and other well-known textual or structured values
 - reduces the data actually sent over the network
- **Capabilities** (are defined for):
 - message size, client and server
 - protocol options: Confirmed Push Facility, Push Facility, Session Suspend Facility, Acknowledgement headers
 - maximum outstanding requests
 - extended methods
 - header code pages
- **Suspend and Resume**
 - server knows when client can accept a push
 - multi-bearer devices
 - dynamic addressing
 - allows the release of underlying bearer resources

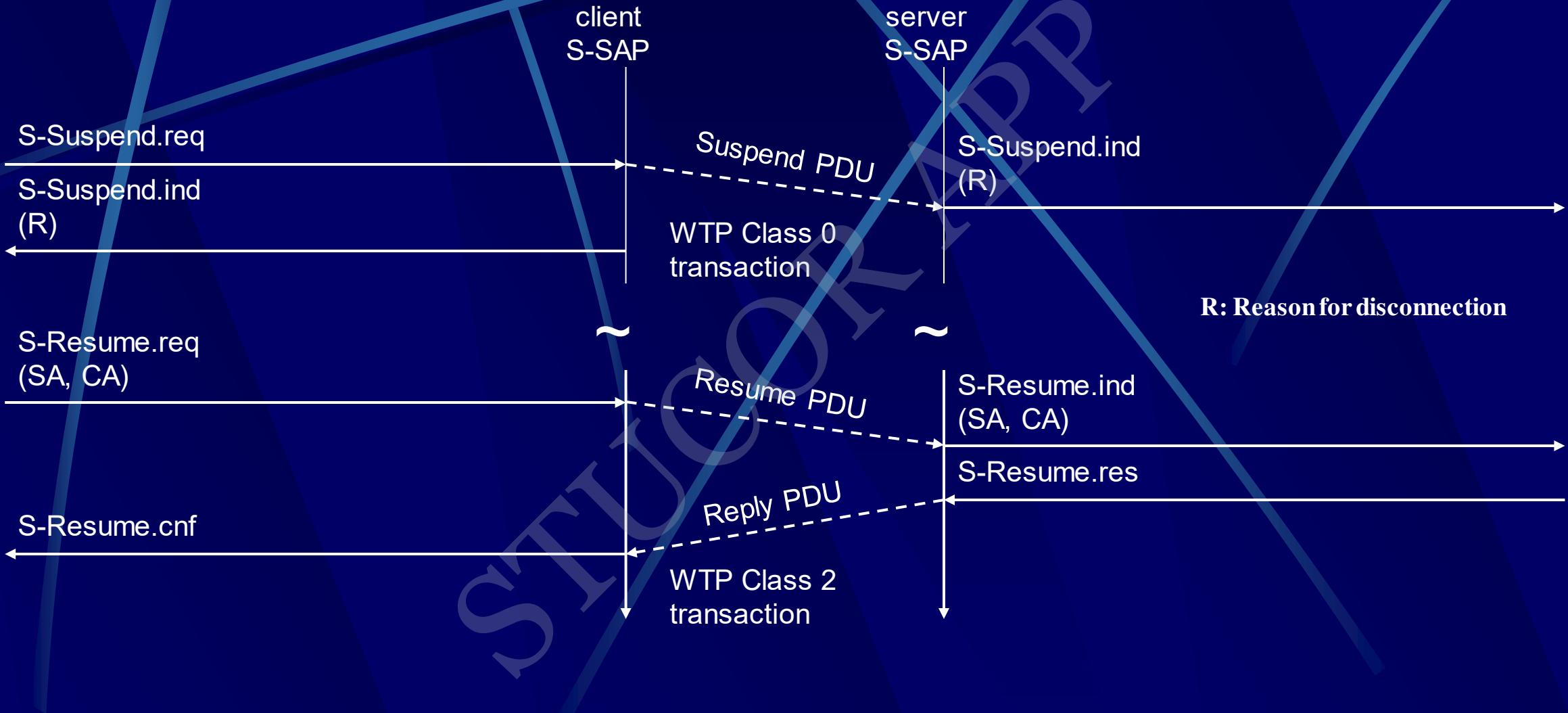
WSP Sessions

- **Session Context and Push**
 - push can take advantage of session headers
 - server knows when client can accept a push
- **Connection-mode**
 - long-lived communication, benefits of the session state, reliability
- **Connectionless-mode**
 - stateless applications, no session creation overhead, no reliability overhead

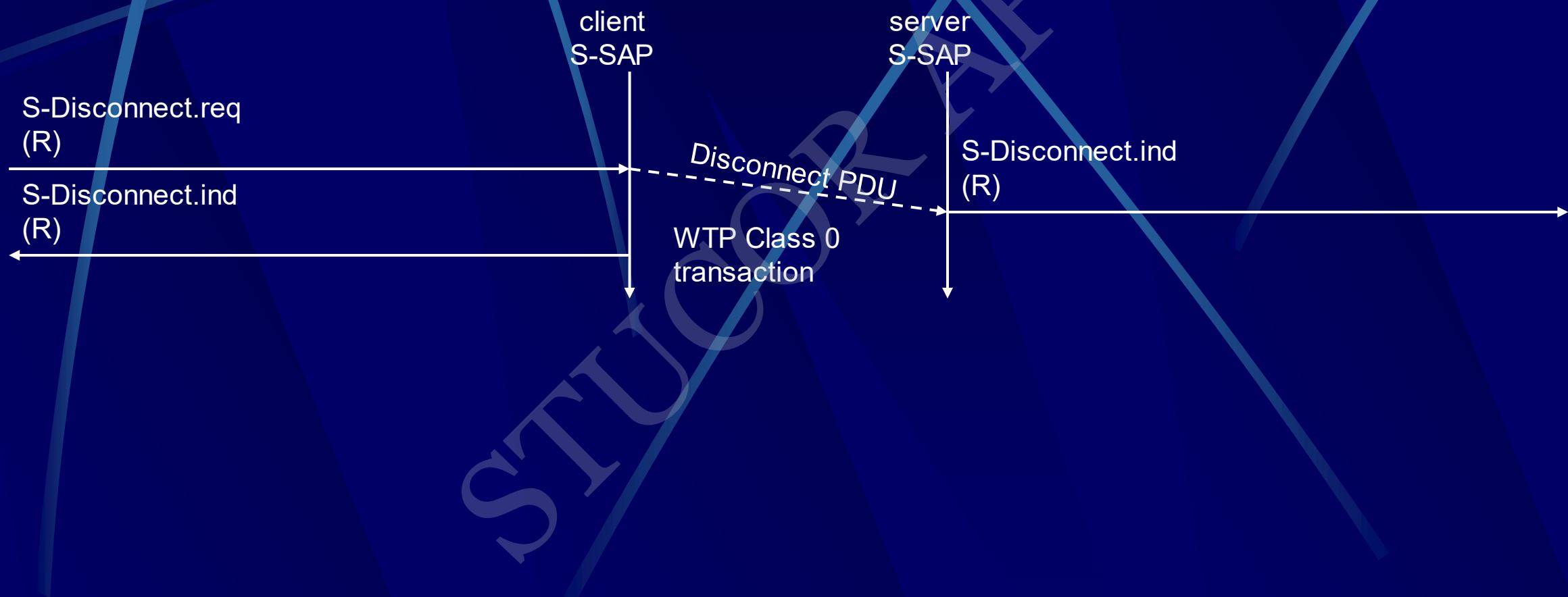
WSP/B session establishment



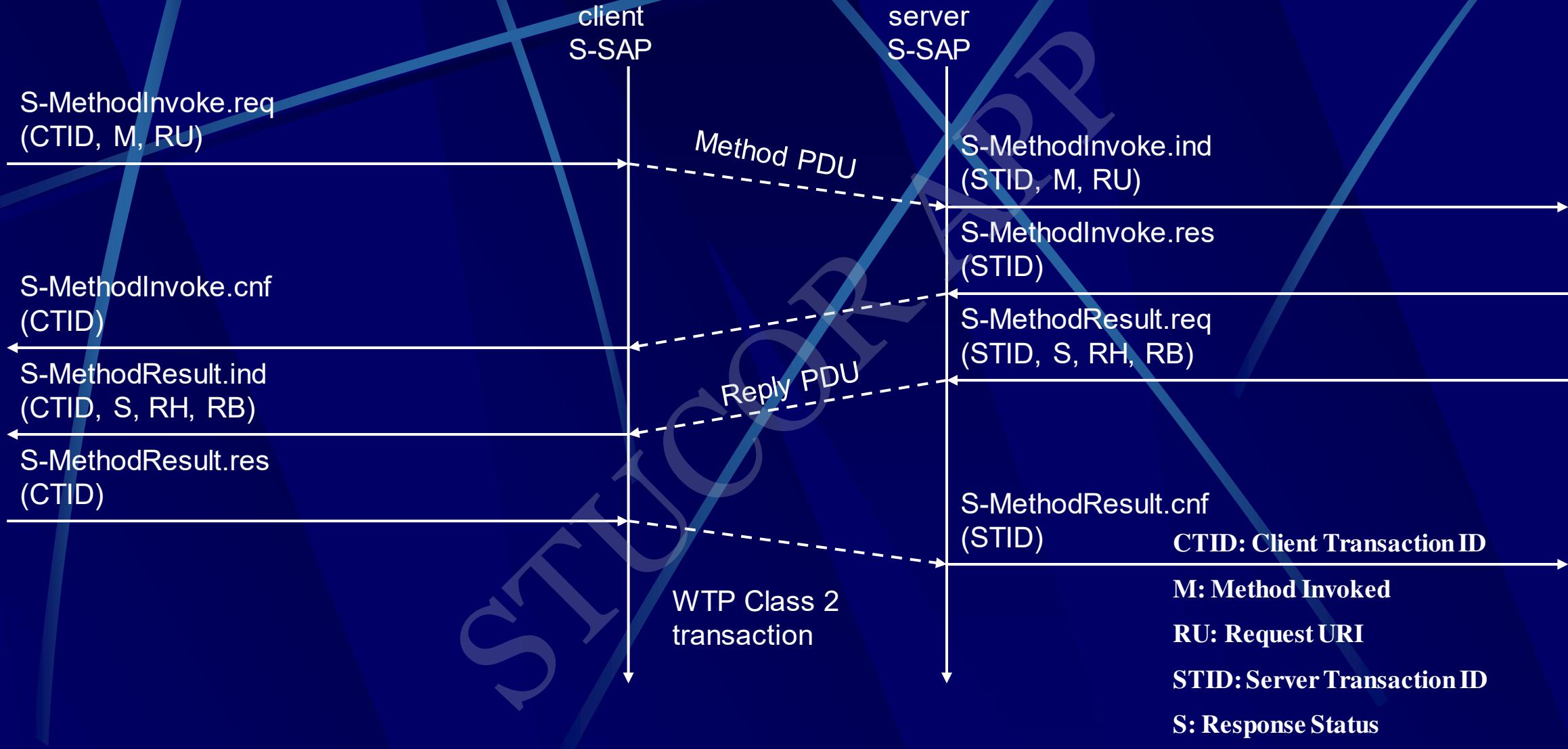
WSP/B session suspend/resume



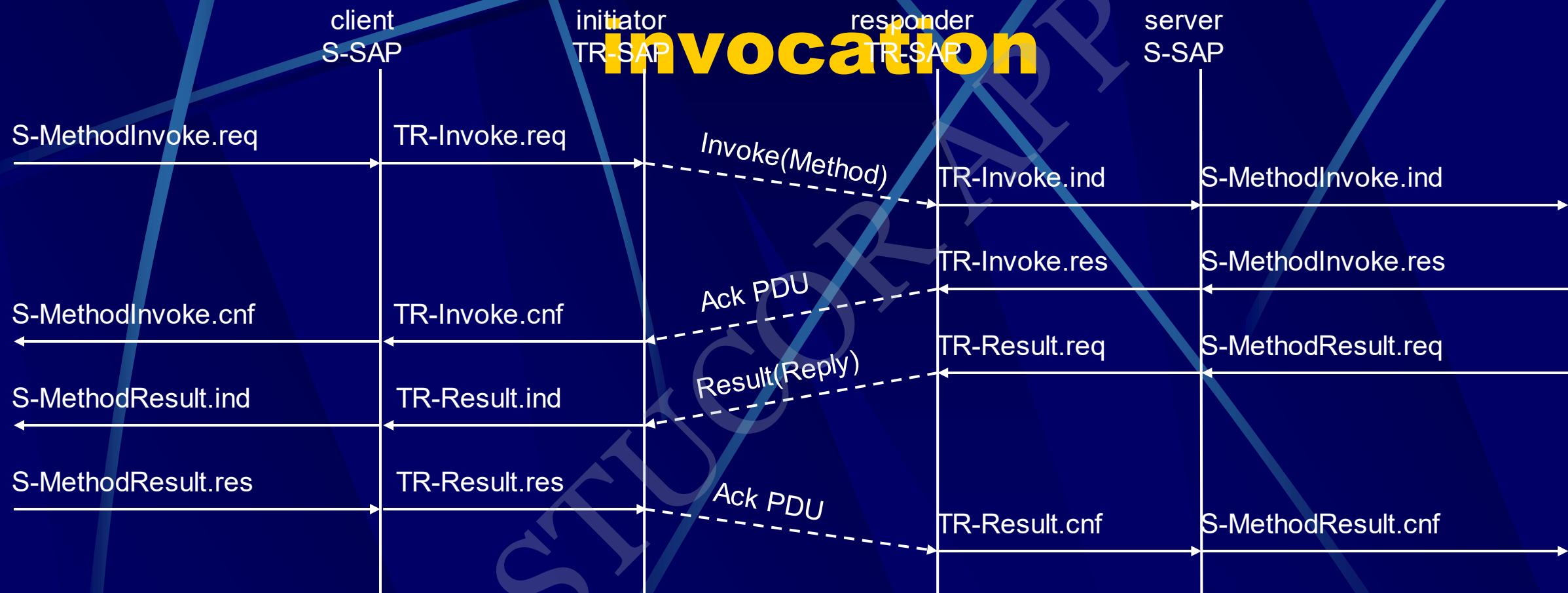
WSP/B session termination



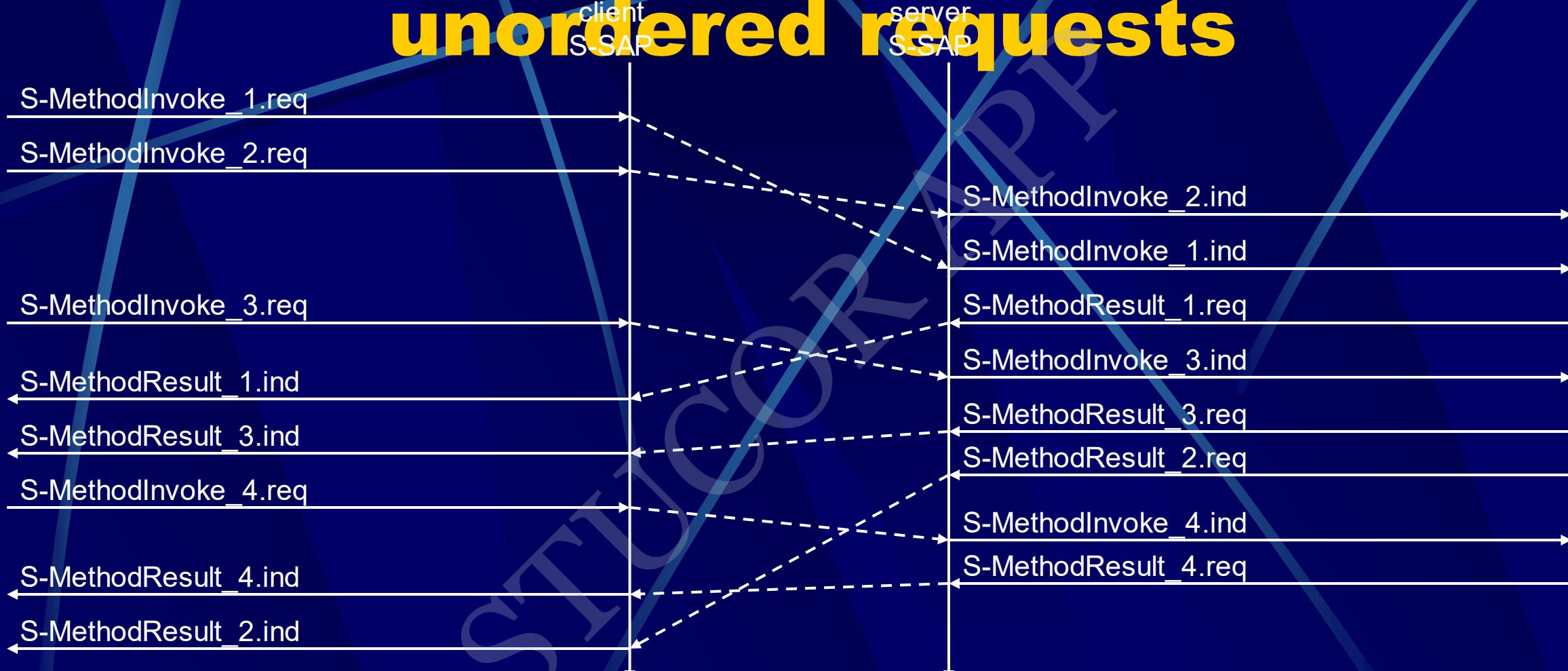
WSP/B method invoke



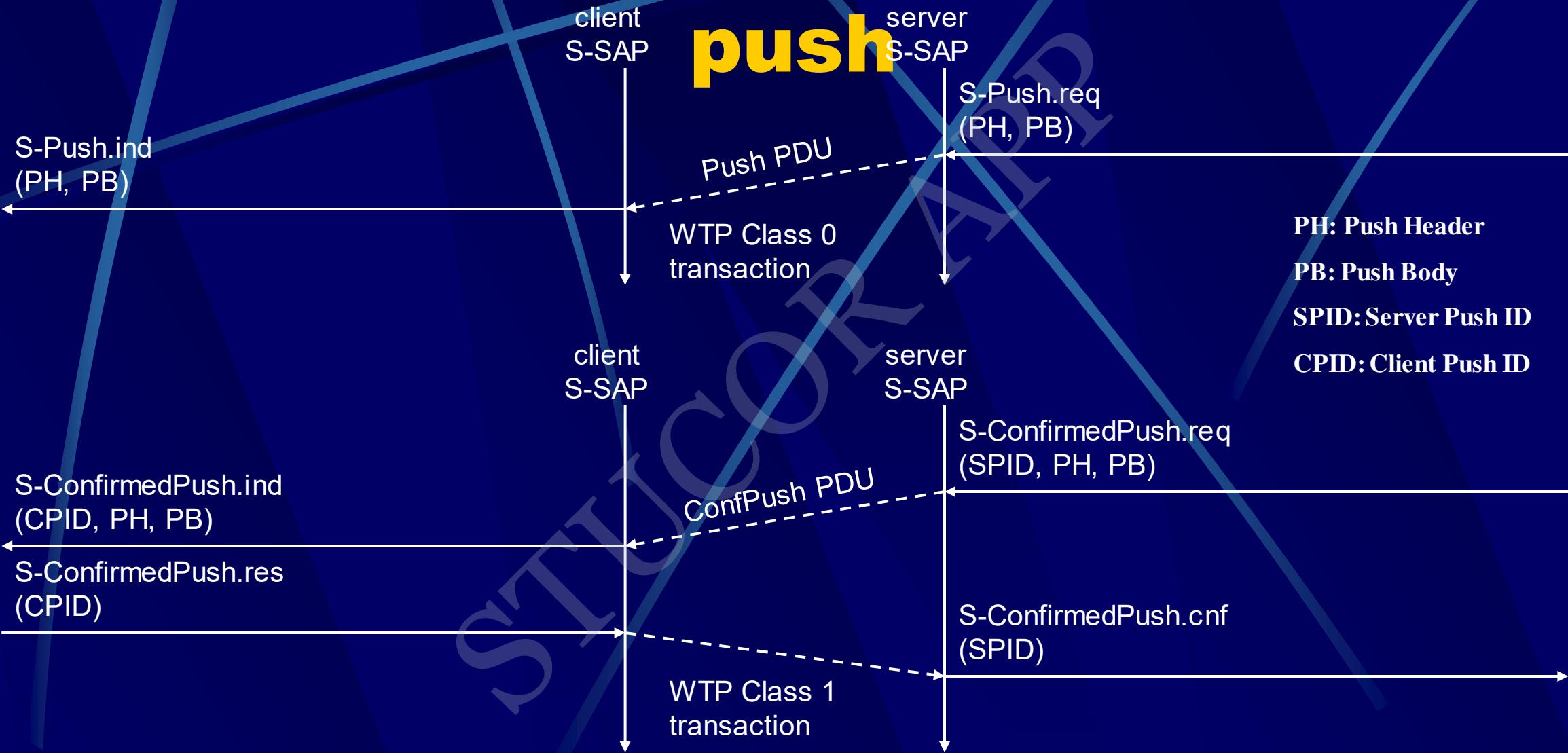
WSP/B over WTP - method invocation



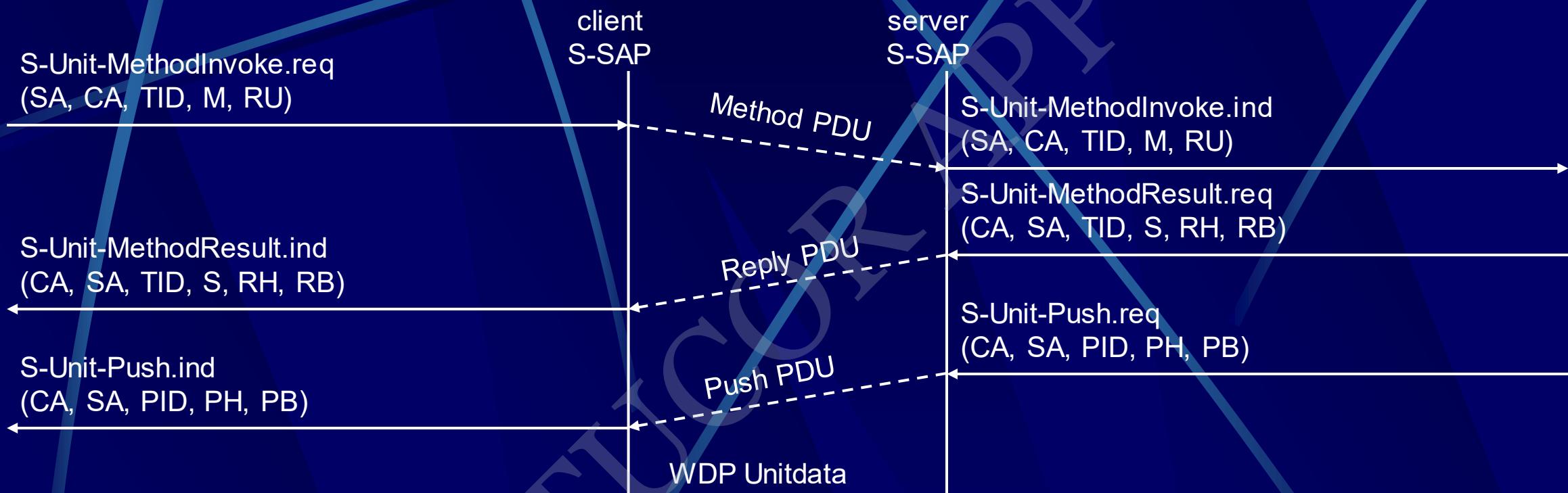
WSP/B over WTP - asynchronous, unordered requests



WSP/B - confirmed/non-confirmed push



WSP/B over WDP



MOBILE COMPUTING

Unit V



STUCOR APP
webOS™



symbian



UNIT V MOBILE PLATFORMS AND APPLICATIONS

Mobile Device Operating Systems – Special Constraints & Requirements – Commercial Mobile Operating Systems – Software Development Kit: iOS, Android, BlackBerry, Windows Phone – M-Commerce – Structure – Pros & Cons – Mobile Payment System – Security Issues.

Mobile Device Operating System Introduction

- Design and capabilities of a Mobile OS (Operating System) is very different than a general purpose OS running on desktop machines:
 - ❖ mobile devices have constraints and restrictions on their physical characteristic such as screen size, memory, processing power and etc.
 - ❖ Scarce availability of battery power
 - ❖ Limited amount of computing and communication capabilities
- Thus, they need different types of operating systems depending on the capabilities they support. e.g. a PDA OS is different from a Smartphone OS.
- Operating System is a piece of software responsible for management of operations, control, coordinate the use of the hardware among the various application programs, and sharing the resources of a device.

Operating System Structure

- A mobile OS is a software platform on top of which other programs called application programs, can run on mobile devices such as PDA, cellular phones, Smartphone and etc.



Mobile Operating System Platforms

□ There are many mobile operating systems. The followings demonstrate the most important ones:

- ❖ Java ME Platform
- ❖ Palm OS
- ❖ Symbian OS
- ❖ Linux OS
- ❖ Windows Mobile OS
- ❖ BlackBerry OS
- ❖ iPhone OS
- ❖ Google Android Platform

Java ME Platform

- ❑ J2ME platform is a set of technologies, specifications and libraries developed for small devices like mobile phones, pagers, and personal organizers.
- ❑ Java ME was designed by Sun Microsystems. It is licensed under GNU General Public License

Special Constraints & Requirements

There are special constraints under which the operating system of a mobile device to operate

- ❖ Limited memory
- ❖ Limited screen size
- ❖ Miniature keyboard
- ❖ Limited processing power
- ❖ Limited battery power
- ❖ Limited and fluctuating of the wireless medium

Special service Requirements

- ❖ Support for specific communication protocols
- ❖ Support for a variety of input mechanism
- ❖ Compliance with open standard
- ❖ Extensive library support

Commercial Mobile Operating System

- Palm OS
- Symbian OS
- Linux OS
- Windows Mobile OS
- BlackBerry OS
- iPhone OS

Android Platform

DOWNLOADED FROM STUCOR APP

STUCOR APP

Palm OS

- ❖ Palm OS is an embedded operating system designed for ease of use with a touch screen-based graphical user interface.
- ❖ It has been implemented on a wide variety of mobile devices such as smart phones, barcode readers, and GPS devices.
- ❖ It is run on Arm architecture-based processors. It is designed as a 32-bit architecture.

Palm OS Features

- The key features of Palm OS are:
 - A single-tasking OS:
 - ❖ Palm OS Garnet (5.x) uses a kernel developed at Palm, but it does not expose tasks or threads to user applications. In fact, it is built with a set of threads that can not be changed at runtime.
 - ❖ Palm OS Cobalt (6.0 or higher) does support multiple threads but does not support creating additional processes by user applications.
 - ❖ Palm OS has a preemptive multitasking kernel that provides basic tasks but it does not expose this feature to user applications .

Palm OS Features (Cont.)

□ Memory Management:

- ❖ The Memory, RAM and ROM, for each Palm resides on a memory module known as card. In other words, each memory card contains RAM, ROM or both. Palms can have no card, one card or multiple cards.

□ Expansion support:

- ❖ This capability not only augments the memory and I/O , but also it facilitates data interchanges with other Palm devices and with other non-Palm devices such as digital cameras, and digital audio players.

□ Handwriting recognition input called Graffiti 2

Palm OS Features (Cont.)

- ❑ HotSync technology for synchronization with PC computers
- ❑ Sound playback and record capabilities
- ❑ TCP/IP network access
- ❑ Support of serial port, USB, Infrared, Bluetooth and Wi-Fi connections
- ❑ Defined standard data format for PIM (Personal Information Management) applications to store calendar, address, task and note entries, accessible by third-party applications
- ❑ Security model:
 - ❑ Device can be locked by password, arbitrary application records can be made private [2]
 - ❑ Palm OS Cobalt include a certificate manager. The Certificate Manager handles X.509 certificates^[3].

Symbian OS

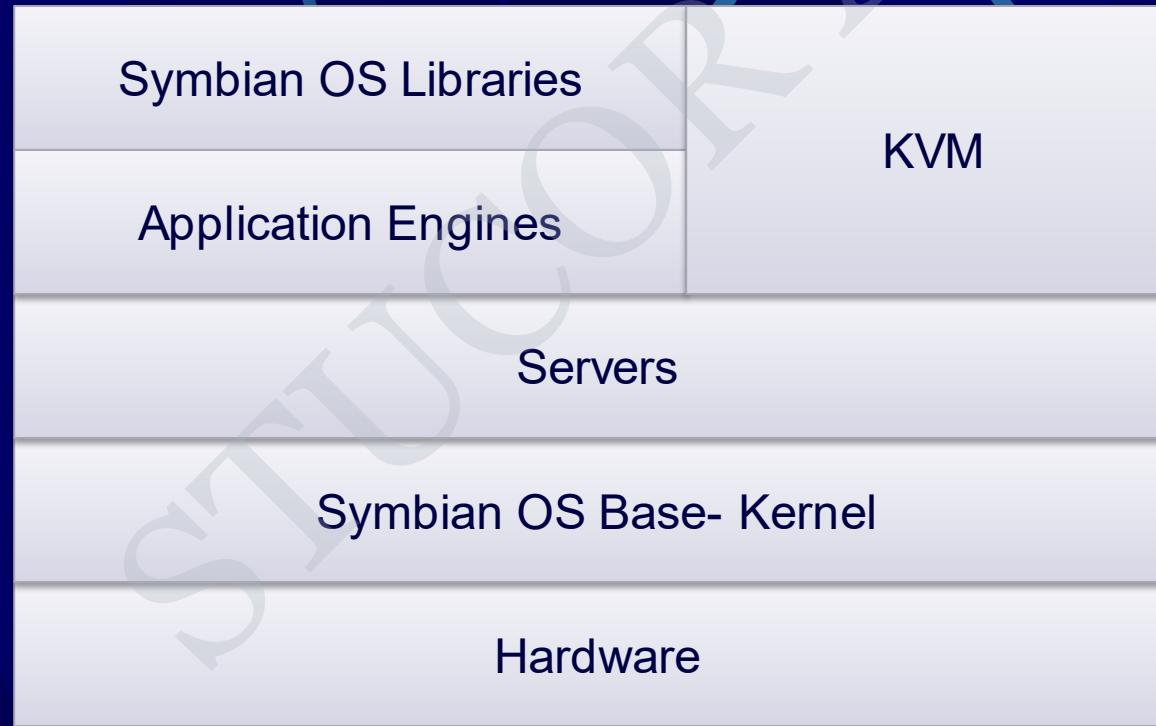
- ❑ Symbian OS is 32 bit, little-endian operating system, running on different flavors of ARM architecture^[4].
- ❑ It is a multitasking operating system and very less dependence on peripherals.
- ❑ Kernel runs in the privileged mode and exports its service to user applications via user libraries.

Symbian OS Structure

- User libraries include networking, communication, I/O interfaces and etc.
- Access to these services and resources is coordinated through a client-server framework.
- Clients use the service APIs exposed by the server to communicate with the server.
- The client-server communication is conducted by the kernel.

Symbian OS Structure (Cont.)

- The following demonstrates the Symbian OS architecture^[1]:



Symbian OS Features

- Real-time: it has a real-time, multithreaded kernel.
- Data Caging : it allows applications to have their own private data partition. This feature allows for applications to guarantee a secure data store. It can be used for e-commerce applications, location aware applications and etc.
- Multimedia: it supports audio, video recording, playback and streaming, and Image conversion.
- Platform Security : Symbian provides a security mechanism against malware. It allows sensitive operations can be accessed by applications which have been certified by a signing authority. In addition, it supports full encryption and certificate management, secure protocols (HTTPS, TLS and SSL) and WIM framework.
- Internationalization support: it supports Unicode standard.
- Fully object-oriented and component- based
- Optimized memory management
- Client- server architecture : described in previous slides, it provides simple and high-efficient inter-process communication. This feature also eases porting of code written for other platforms to Symbian OS.
- A Hardware Abstraction Layer (HAL): This layer provides a consistent interface to hardware and supports device-independency
- Kernel offers hard real-time guarantees to kernel and user mode threads.

Embedded Linux OS

- It is known as Embedded Linux which is used in embedded computer systems such as mobile phones, Personal Digital Assistants, media players and other consumer devices.
- In spite of Linux operating system designed for Servers and desktops, the Embedded Linux is designed for devices which have relatively limited resources such as small size of RAM, storage, screen, limited power and etc. Then, they should have an optimized kernel.
- It is a Real-Time Operating System (RTOS). It meets deadlines and switch context
- It has relatively a small footprint. Today, mobile phones can ship with a small memory. Thus, OS must not seek to occupy a large amount of available storage. It should have a small foot print. Theoretically, they deploy in a footprint of 1MB or less.
- It is open source. It has no cost for licensing.
- Examples: Motorola Mobile phones such as RAZR V8, RAZR V9, A1200 are based on MontaVista Linux.
- ARM and MIPS structures [7]: Embedded CPU architectures like ARM and MIPS offer small instruction sets and special execution modes that shrinks application size and

Windows Mobile OS

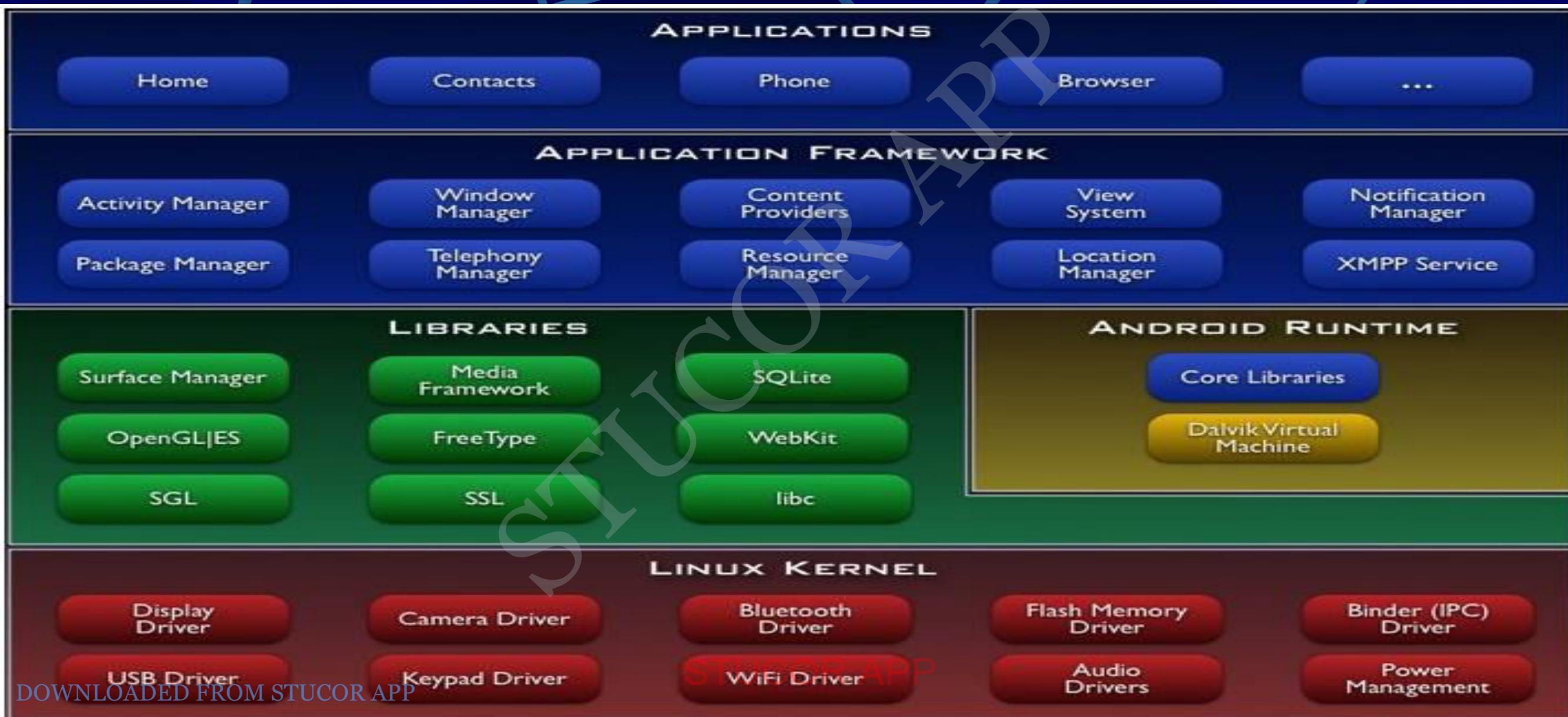
- Windows Mobile is a compact operating system designed for mobile devices and based on Microsoft Win32.
- It is run on Pocket PCs, Smart phones and Portable media centers.
- It provides ultimate interoperability. Users with various requirements are able to manipulate their data.

Google Android Platform

- It is a platform and an operating system for mobile devices based on the Linux operating system.
- It allows developers design applications in a java-like language using Google-developed java libraries.
- It supports a wide variety of connectivity such as GSM, WiFi, 3G, ...
- The Operating system has not been implemented yet (Feb, 2008). Several prototypes have been proposed.

Google Android Platform

Android architecture: <http://code.google.com/android/what-is-android.html>



Google Android Platform

- ❖ As demonstrated in the previous slide, the Android platform contains the following layers:
 - ❖ Linux Kernel: Android relies on Linux for core system services such as security, memory management, process management and etc.
 - ❖ Android Runtime: it provides a set of core libraries which supports most of the functionality in the core libraries of Java. The Android Virtual Machine known as Dalvik VM relies on the linux kernel for some underlying functionality such as threading,...
 - ❖ Libraries: Android includes a set of C/C++ libraries. These libraries are exposed to developers through the Android application framework. They include media libraries, system C libraries, surface manager, 3D libraries, SQLite and etc.
 - ❖ For more details, please visit the following link:
 - ❖ <http://code.google.com/android/what-is-android.html>
 - ❖ Application Framework: it provides an access layer to the framework APIs used by the core applications. It allows components to be used by the developers.

iPhone OS

- ❖ iPhone OS is an operating system run on iPhone and iPod.
- ❖ It is based on Mach Kernel and Drawin core as Mac OS X.
- ❖ The Mac OS X kernel includes the following component:
 - ❖ Mach Kernel
 - ❖ BSD
 - ❖ I/O component
 - ❖ File Systems
 - ❖ Networking components

iPhone OS

- The following is Mac OS X Architecture:



iPhone OS

- ❖ Mac OS X has a preemptive multitasking environment.
- ❖ Preempting is the act of taking the control of operating system from one task and giving it to another task.
- ❖ It supports real-time behavior.
- ❖ In Mac OS X, each application has access to its own 4 GB address space.
- ❖ Not any application can directly modify the memory of the kernel. It has a strong mechanism for memory protection.
- ❖ For more details about kernel architecture, please visit the following link:
 - ❖ <http://developer.apple.com/documentation/Darwin/Conceptual/KernelProgramming/Architecture/Architecture.html>

BlackBerry OS

- ❖ BlackBerry OS has a multitasking environment.
- ❖ It enables heavy use of input devices like trackball, and scroll wheel. It does not support touchpad.
- ❖ It is an event-driven Operating System.
- ❖ Later BlackBerry Smartphone's CPU architecture is based on ARM XScale. The other BlackBerry devices has Intel-based processors.
- ❖ It supports multitasking and multithreading applications.
- ❖ Security: Any application that want to use certain BlackBerry functionality must be digitally signed.

TABLE 9.1 A Comparison of the Features of Three Popular Mobile Operating Systems

<i>Feature</i>	<i>Android</i>	<i>Symbian OS</i>	<i>Windows Phone 7</i>
License	Public, Free, and Open Source	Initially was private, later became public.	Proprietary
Footprint	250 KB	200 KB	300 KB
Change of UI	Possible	No	No
Power management	Yes	Yes	Yes
Kernel	Linux with minor changes	Proprietary	Win CE
True multitasking	Yes	Yes	No
Premptive scheduling	Yes	Yes	Yes
Demand paging	Yes	Yes	Yes
CPU architecture supported	ARM, MIPS, STUCOR APP x86	ARM	ARM

M-Commerce

Involves carrying out any activity related buying and selling of commodities, services or information using the mobile hand held devices.

- ❖ Applications of M-Commerce

M-commerce applications can be broadly categorized into B2C and B2B.



Business-to-Consumer (B2C) Applications

- ❖ Advertising
- ❖ Comparison shopping
- ❖ Information about a product
- ❖ Mobile ticketing
- ❖ Loyalty and payment service
- ❖ Interactive advertisement
- ❖ Catalogue shopping

Business-to-Business (B2B) Applications

- ❖ Ordering and delivery confirmation
- ❖ Stock tracking and control
- ❖ Supply chain management
- ❖ Mobile inventory management

M-Commerce Structure

- ❖ Content provider implements an application by providing two sets of programs: Client-side and Server-Side
- ❖ Client side programs run on the browsers installed on users mobile.
- ❖ Server side programs performs database access and computations, resides on the host computers(Servers)

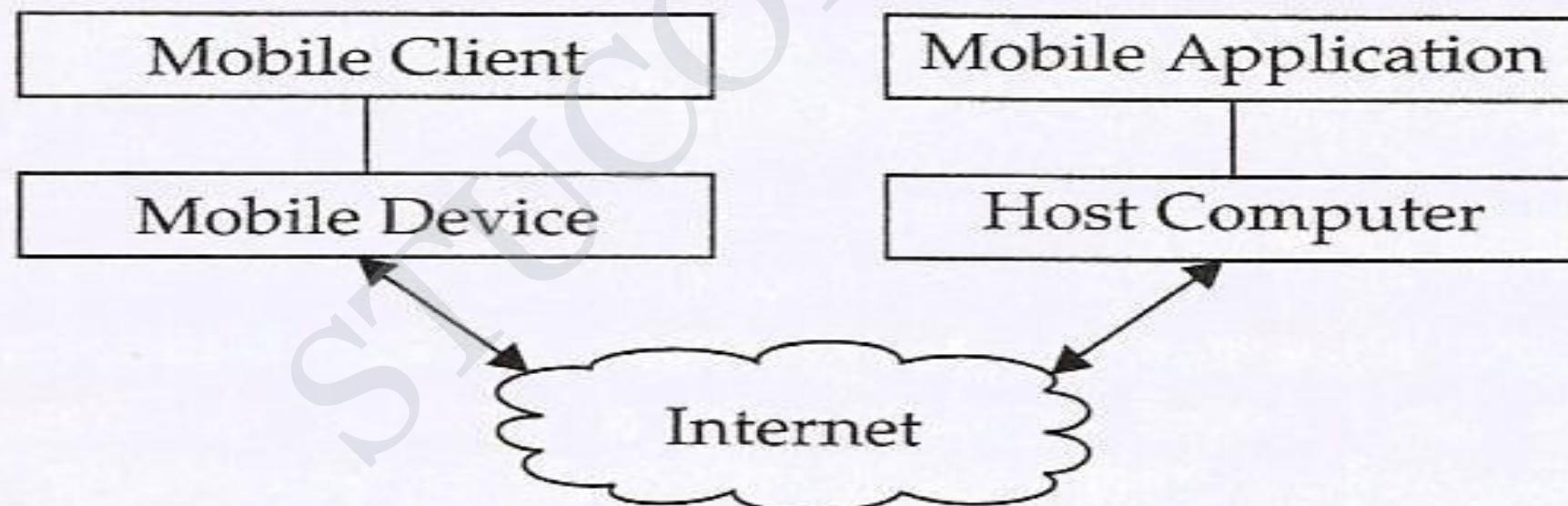


Figure 11.1 Architecture of a mobile commerce framework.

- Hand-held devices interfaced to mobile user, user specify their requests using interface programs,
- which are transmitted to mobile commerce application
- The result obtained from the mobile commerce application are displayed in suitable formats.

Mobile middleware

- The purpose of mobile middleware is to seamlessly and transparently map the internet content to mobile phones
- It also handle encrypting and decrypting communication for secure transaction.

Network

- The request are delivered to the closet wireless access point or base station or wired network such as internet for mobile commerce system

Host computers

- Process and stores all information needed for mobile commerce.
- It consists of three parts web servers, database servers and application program and support software.

M-Commerce Pros & Cons

Advantages

- For business organization: Customer convenience, cost savings and new business opportunities.
- For customer: Any where, any time shopping using light weight device.
- Without physically visiting to store identifying the right product at the lowest price.
- Highly personalized thereby providing an additional level of convenience to customer.

Disadvantages

- Mobile device not offer graphics or processing power of a PC
- The small screens of mobile devices limit the complexity of application.
- Network imposes several types of restriction.

Mobile Payment System

Mobile payment or m-payment defined as any payment instrument where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services.

OR

Mobile payment, also referred to as mobile money, mobile money transfer, and mobile wallet generally refer to payment services operated under financial regulation and performed from or via a mobile device.

Mobile Payment Schemes

Three popular types of M-payment schemes are currently used are

- I. Bank account based
- II. Credit card based
- III. Micropayment

- ❖ In each of these approach, a third party service provider (Bank, Credit card company or telecom company) make payment on the customer's behalf .
- ❖ The service provider may charge small amount as service charge

Bank account based M-payment

- The bank account of the customer is linked to his mobile number.
- When the customer makes an M-payment transaction with vendor, the bank account of the customer is debited and the value is credited to the vendor's account.

Credit card based M-payment

- The Credit card number is linked to mobile number of customer.
- When the customer makes an M-payment transaction with vendor, the credit card is charged and the value is credited to the vendor's account.

Micropayment

- ❖ The Micropayment is for small purchase such as from vending machines.
- ❖ A customer makes a call to the number of a service provider where the per call charge is equal to the cost of the vending item.
- ❖ The micropayment scheme is implemented thorough the cooperation of the mobile phone operator and a third party service provider.

Security Issues

- ❖ M commerce is anticipated to introduced new security and privacy risks.
- ❖ Users of mobile device can be difficult to trace because of roaming of the users.
- ❖ The mobile device go on-line and off-line frequently, thus attacks would be very difficult to trace.
- ❖ Another risk unique to the mobile devices is the risk of loss or theft.
- ❖ A major problem in this regard is lack of authenticate a particular user.

References

- Book: Prasant Kumar Patnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.
- <http://cmer.cis.uoguelph.ca>
- PPT:
- www.cmer.ca/cmer-ak/AcademicKitV1.0/.../OpSys_slides_1.ppt
- www.cmer.ca/cmer-ak/AcademicKitV1.0/.../OpSys_slides_2.ppt

Other presentations

<http://www.slideshare.net/drgst/presentations>