TCP/IP-(18MCA45E)
UNIT-V
'Simple Network Management Protocols'

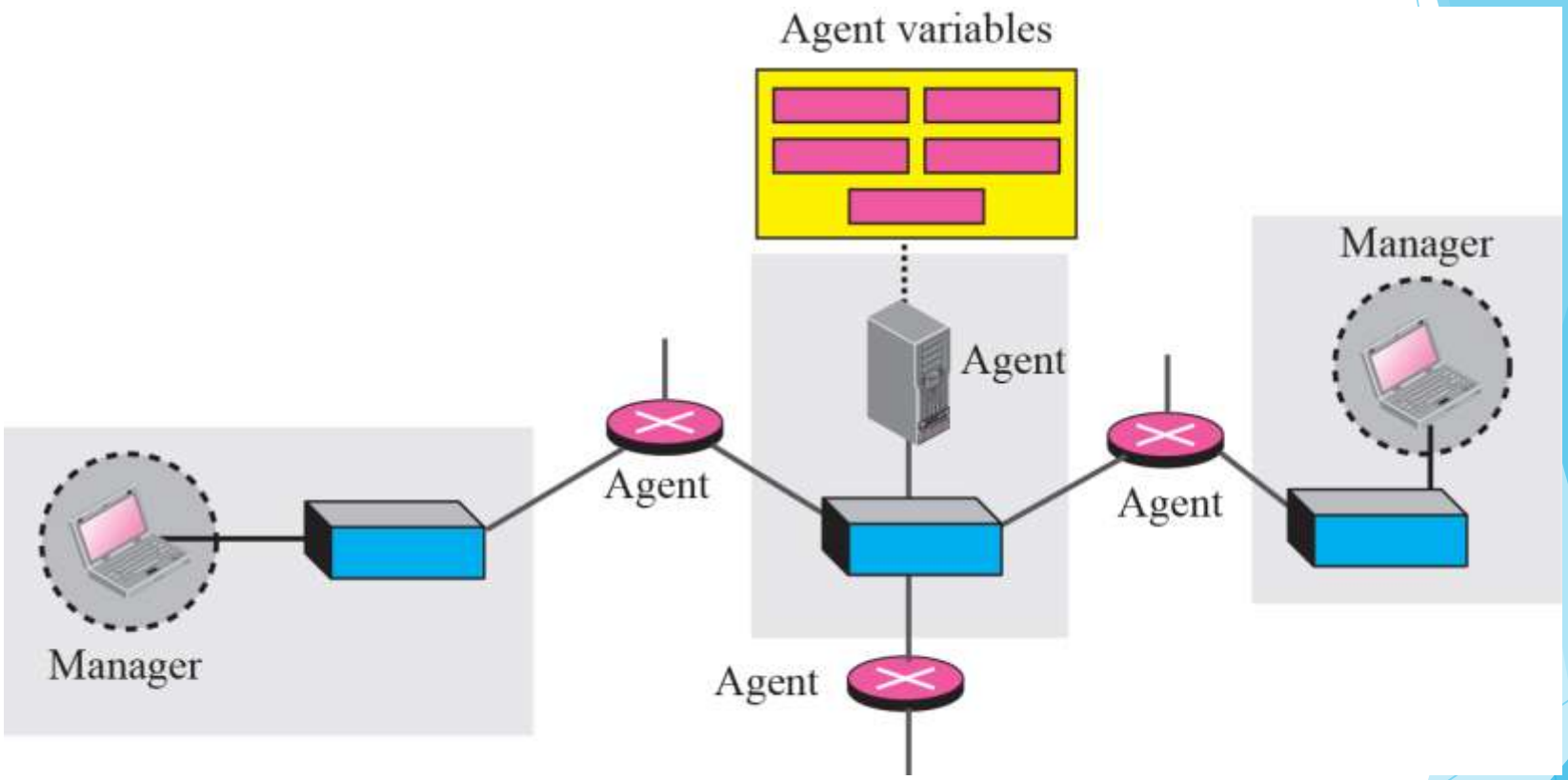
FACULTY:

Dr. R. A. Roseline, M.Sc., M.Phil., Ph.D.,
Associate Professor and Head,
Post Graduate and Research Department of Computer Applications,
Government Arts College (Autonomous),
Coimbatore – 641 018.

CONCEPT

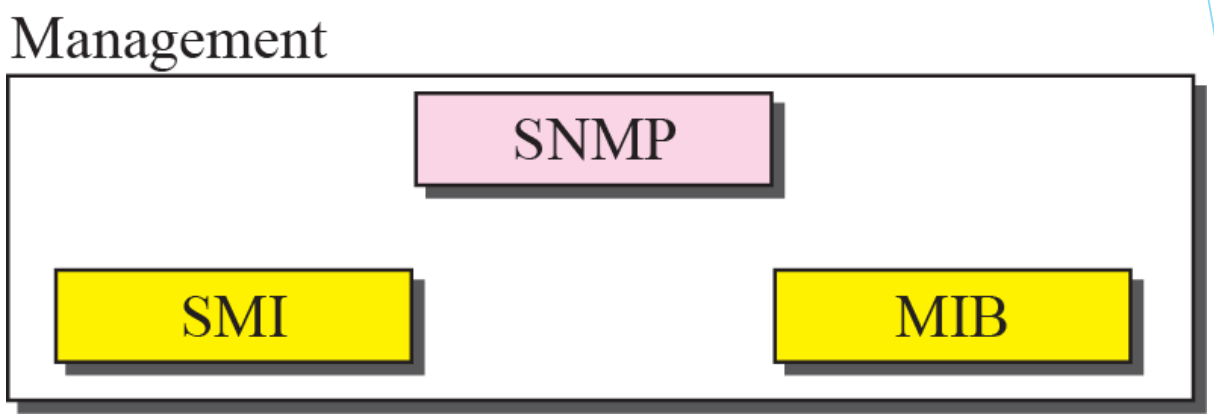
SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers or servers (see Figure 24.1).

SNMP concept



MANAGEMENT COMPONENTS

To do management tasks, SNMP uses two other protocols: Structure of Management Information (SMI) and Management Information Base (MIB). In other words, management on the Internet is done through the cooperation of three protocols: SNMP, SMI, and MIB, as shown in Figure 24.2.


Management
SNMP
SMI
MIB

Note

SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status of objects (values of variables) in SNMP packets.

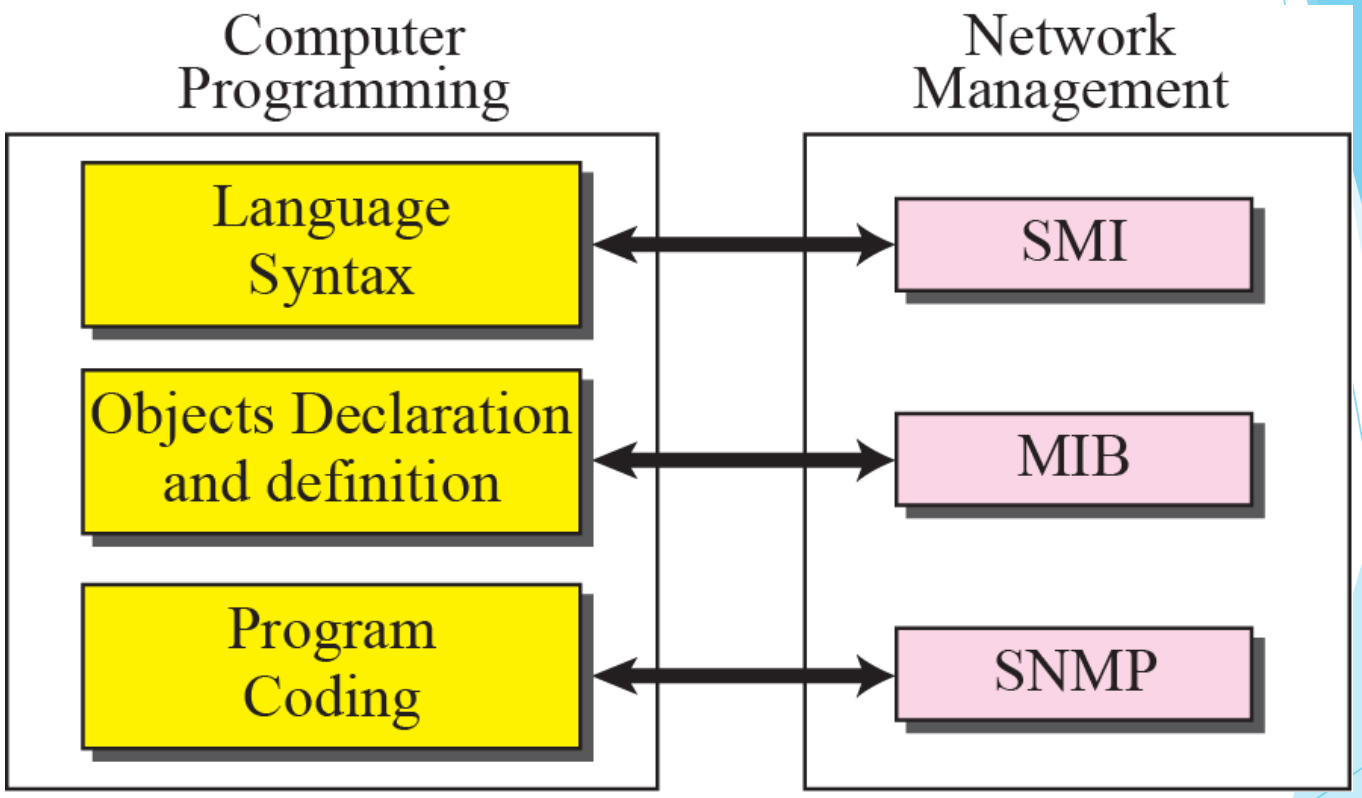
Note

SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.

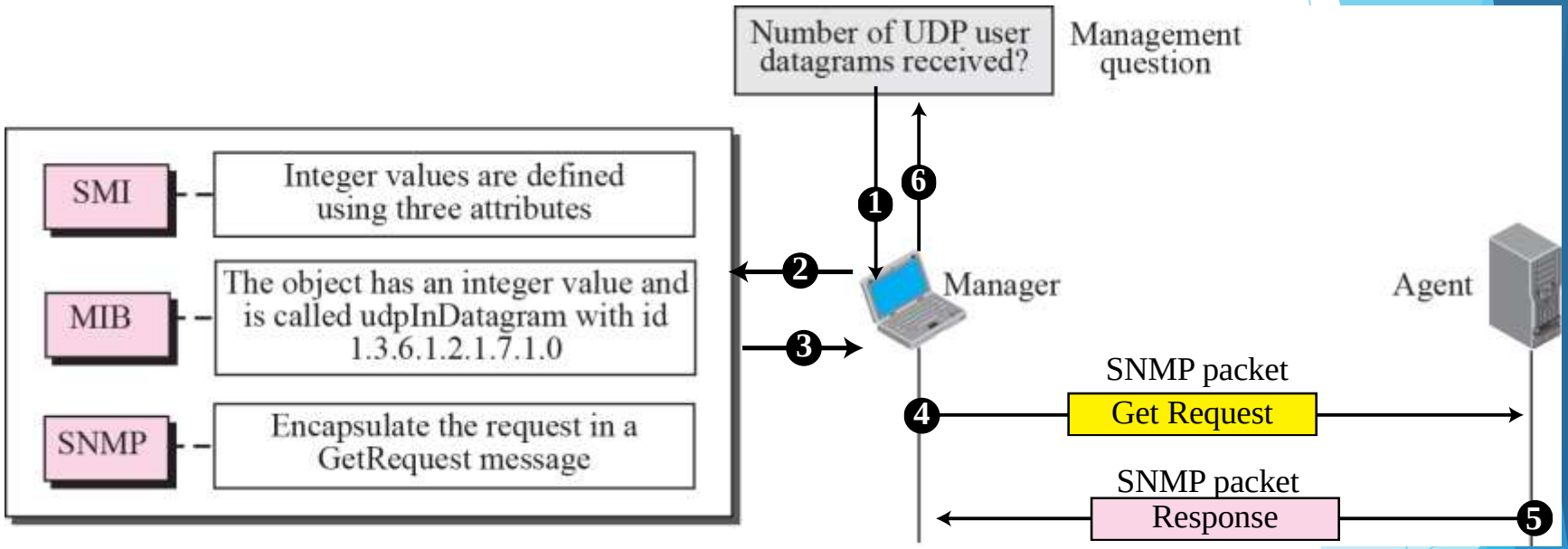
Note

MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.

Comparing computer programming and network management



Management overview



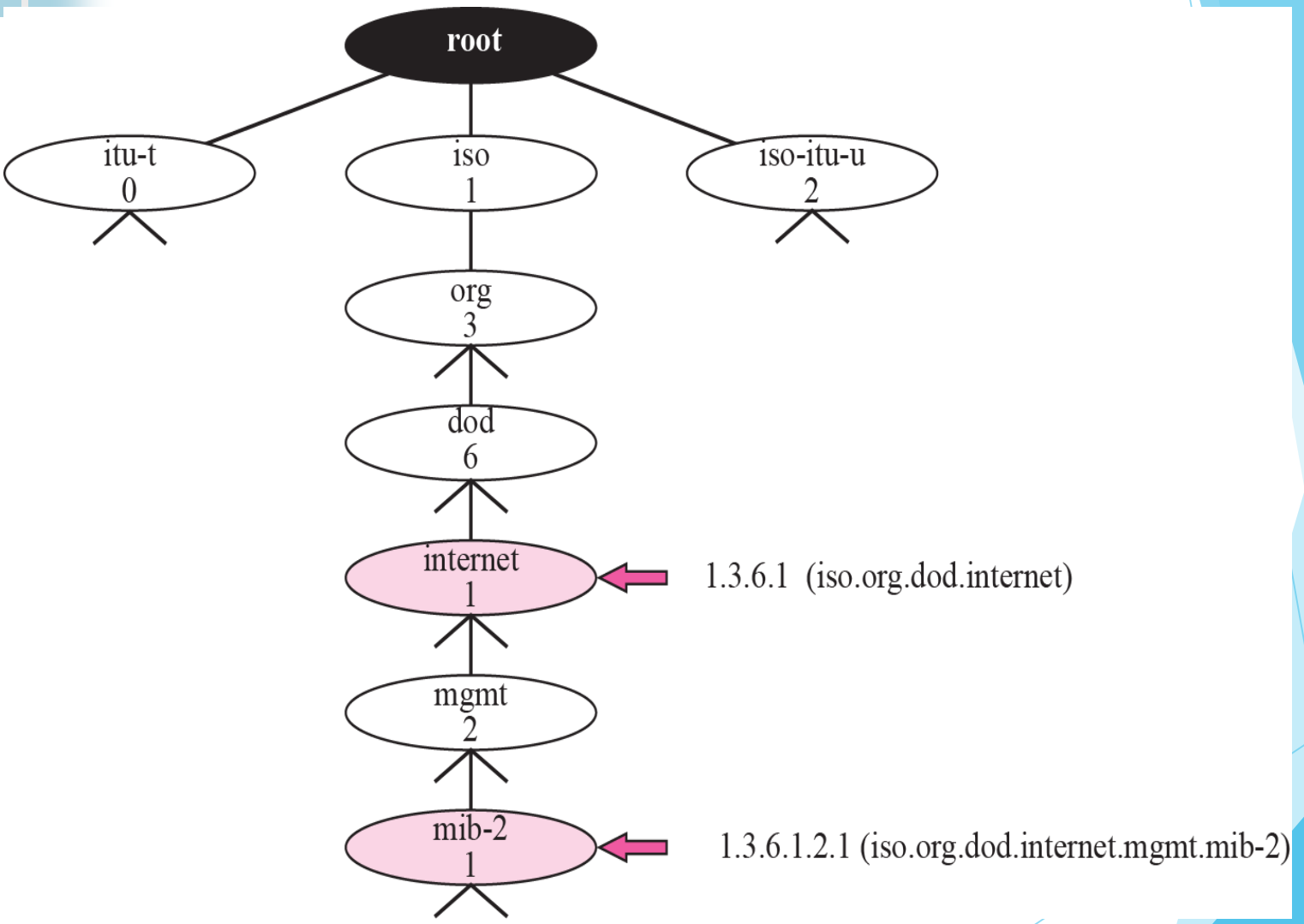
SMI

The Structure of Management Information is a component for network management. Its functions are:

1. To name objects.
2. To define the type of data that can be stored in an object.
3. To show how to encode data for transmission over the network.

SMI is a guideline for SNMP. It emphasizes three attributes to handle an object: name, data type, and encoding method.

Object identifier



Note

All objects managed by SNMP are given an object identifier. The object identifier always starts with 1.3.6.1.2.1.

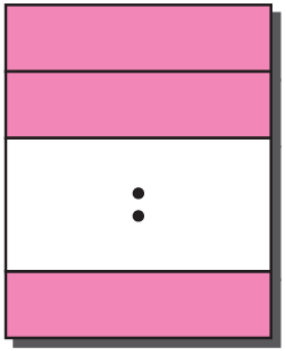
Table 24.1 *Data Types*

Type	*Size*	*Description*
INTEGER	4 bytes	An integer with a value between -2^{31} and $2^{31}-1$
Integer32	4 bytes	Same as INTEGER
Unsigned32	4 bytes	Unsigned with a value between 0 and $2^{32}-1$
OCTET STRING	Variable	Byte-string up to 65,535 bytes long
OBJECT IDENTIFIER	Variable	An object identifier
IPAddress	4 bytes	An IP address made of four integers
Counter32	4 bytes	An integer whose value can be incremented from zero to 2^{32}; when it reaches its maximum value it wraps back to zero
Counter64	8 bytes	64-bit counter
Gauge32	4 bytes	Same as Counter32, but when it reaches its maximum value, it does not wrap; it remains there until it is reset
TimeTicks	4 bytes	A counting value that records time in 1/100ths of a second
BITS		A string of bits
Opaque	Variable	Uninterpreted string

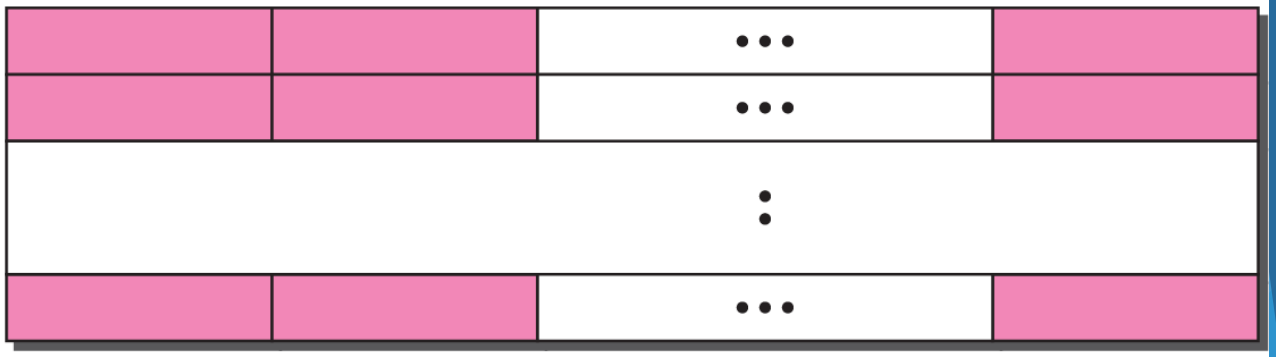
Conceptual data types

a. Simple variable

c. Sequence



b. Sequence of (simple variables)



d. Sequence of (sequences)

Encoding format

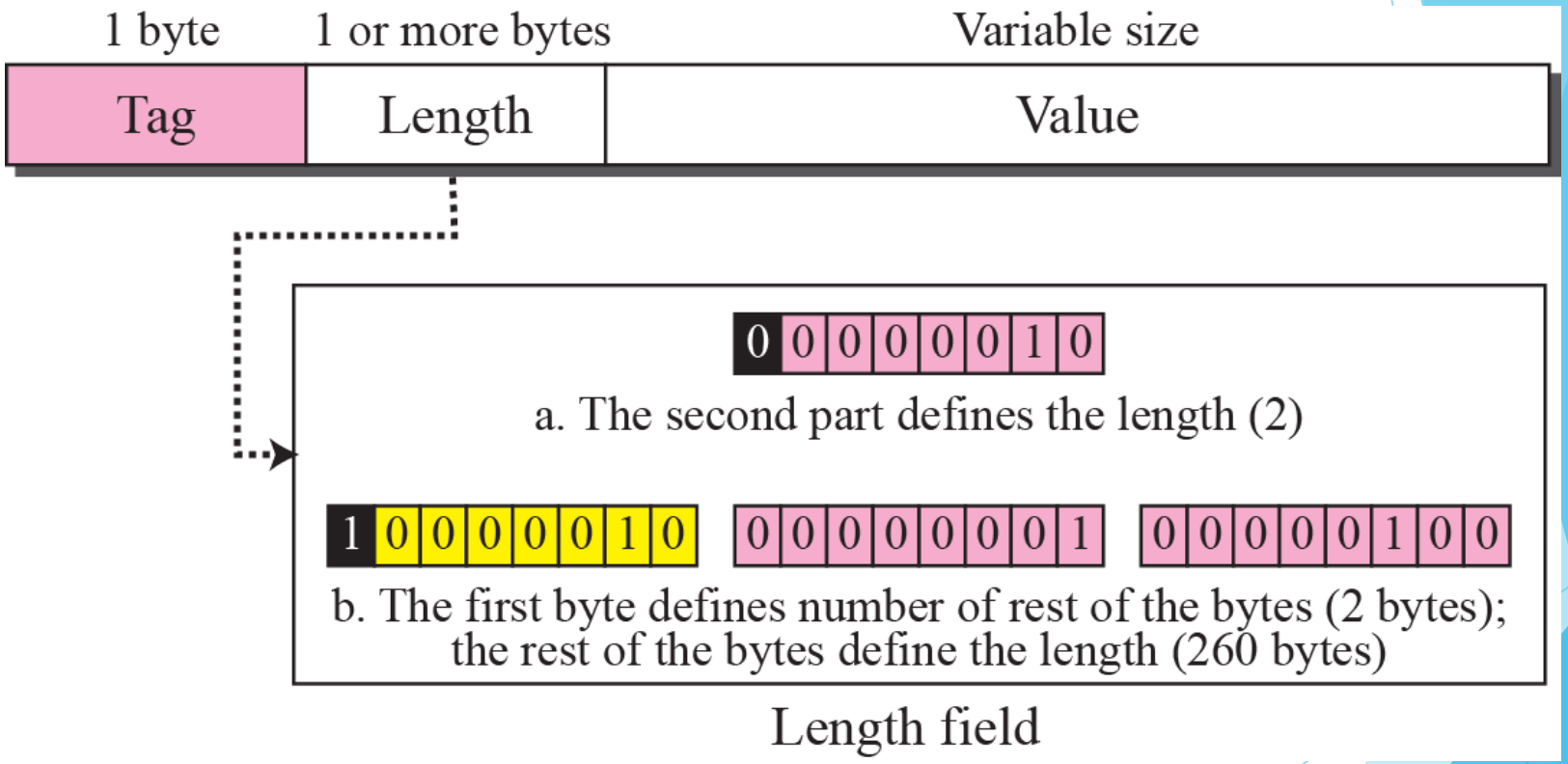


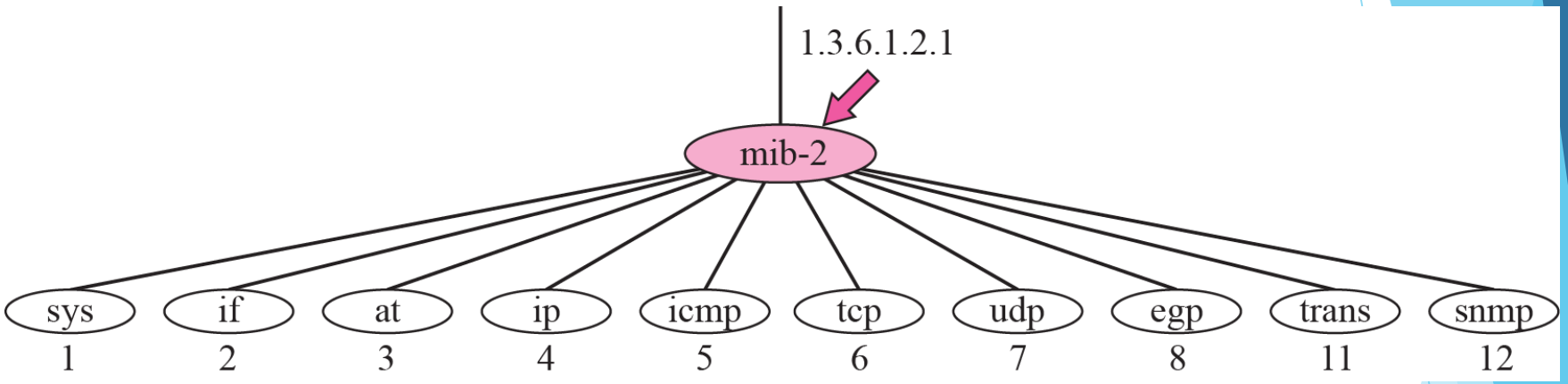
Table 24.2 *Codes for Data Types*

Data Type	*Tag (Binary)*	*Tag (Hex)*
INTEGER	**00000010**	**02**
OCTET STRING	**00000100**	**04**
OBJECT IDENTIFIER	**00000110**	**06**
NULL	**00000101**	**05**
Sequence, sequence of	**00110000**	**30**
IPAddress	**01000000**	**40**
Counter	**01000001**	**41**
Gauge	**01000010**	**42**
TimeTicks	**01000011**	**43**
Opaque	**01000100**	**44**

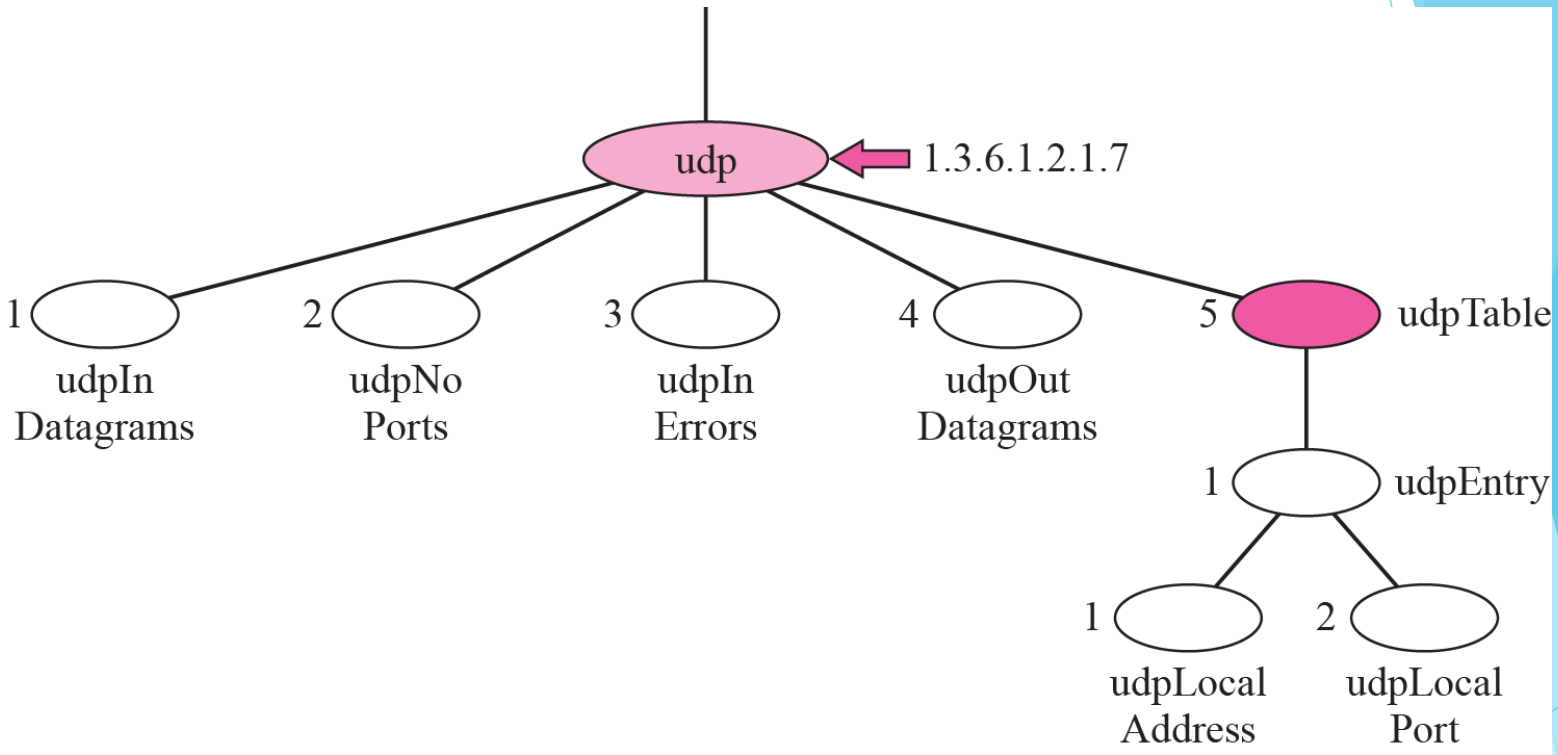
MIB

The Management Information Base, version 2 (MIB2) is the second component used in network management. Each agent has its own MIB2, which is a collection of all the objects that the manager can manage. The objects in MIB2 are categorized under 10 different groups: system, interface, address translation, ip, icmp, tcp, udp, egp, transmission, and snmp. These groups are under the mib-2 object in the object identifier tree (see Figure 24.12). Each group has defined variables and/or tables.

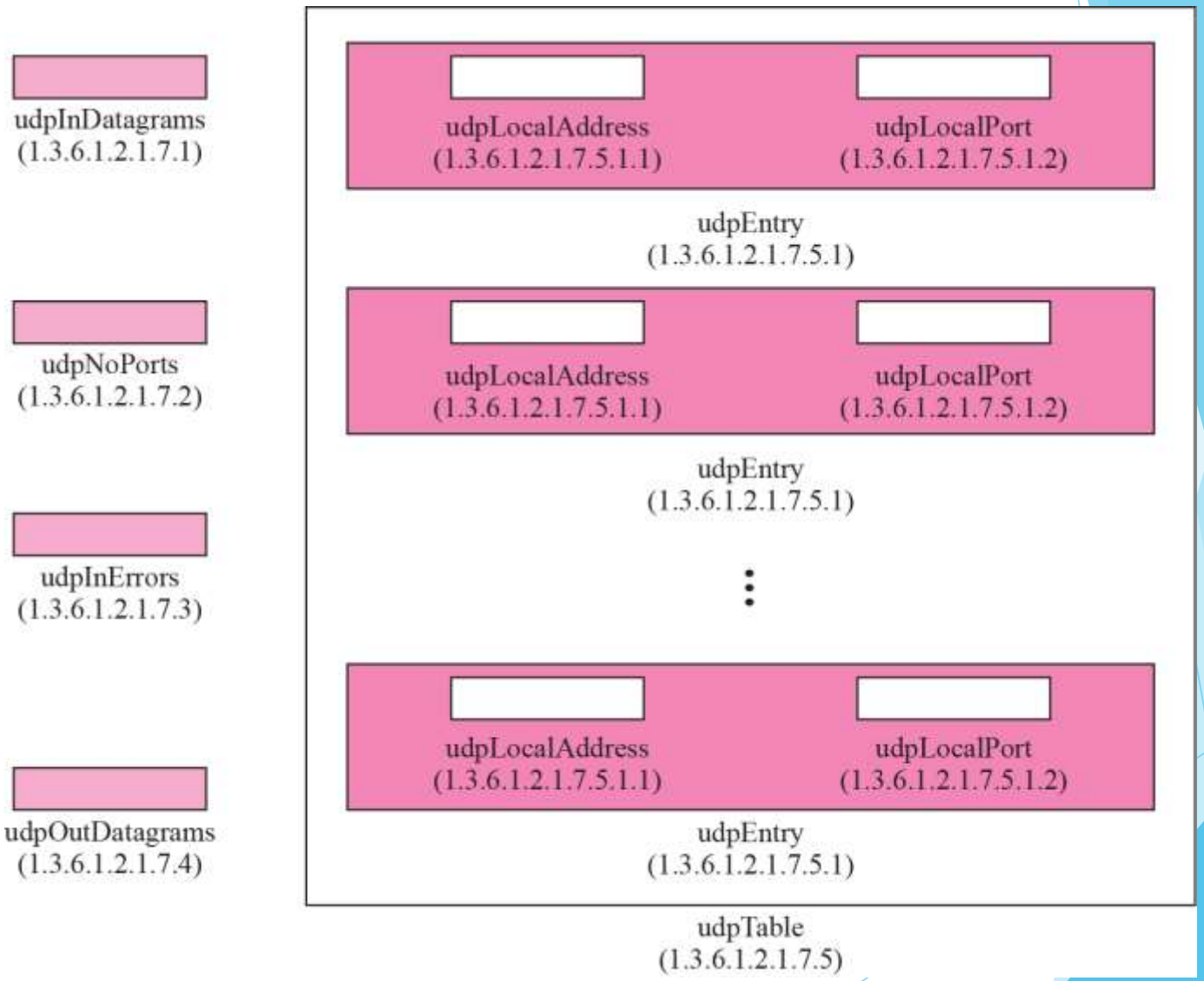
mib-2


1.3.6.1.2.1
mib-2
sys
1
if
2
at
3
ip
4
icmp
5
tcp
6
udp
7
egp
8
trans
11
snmp
12

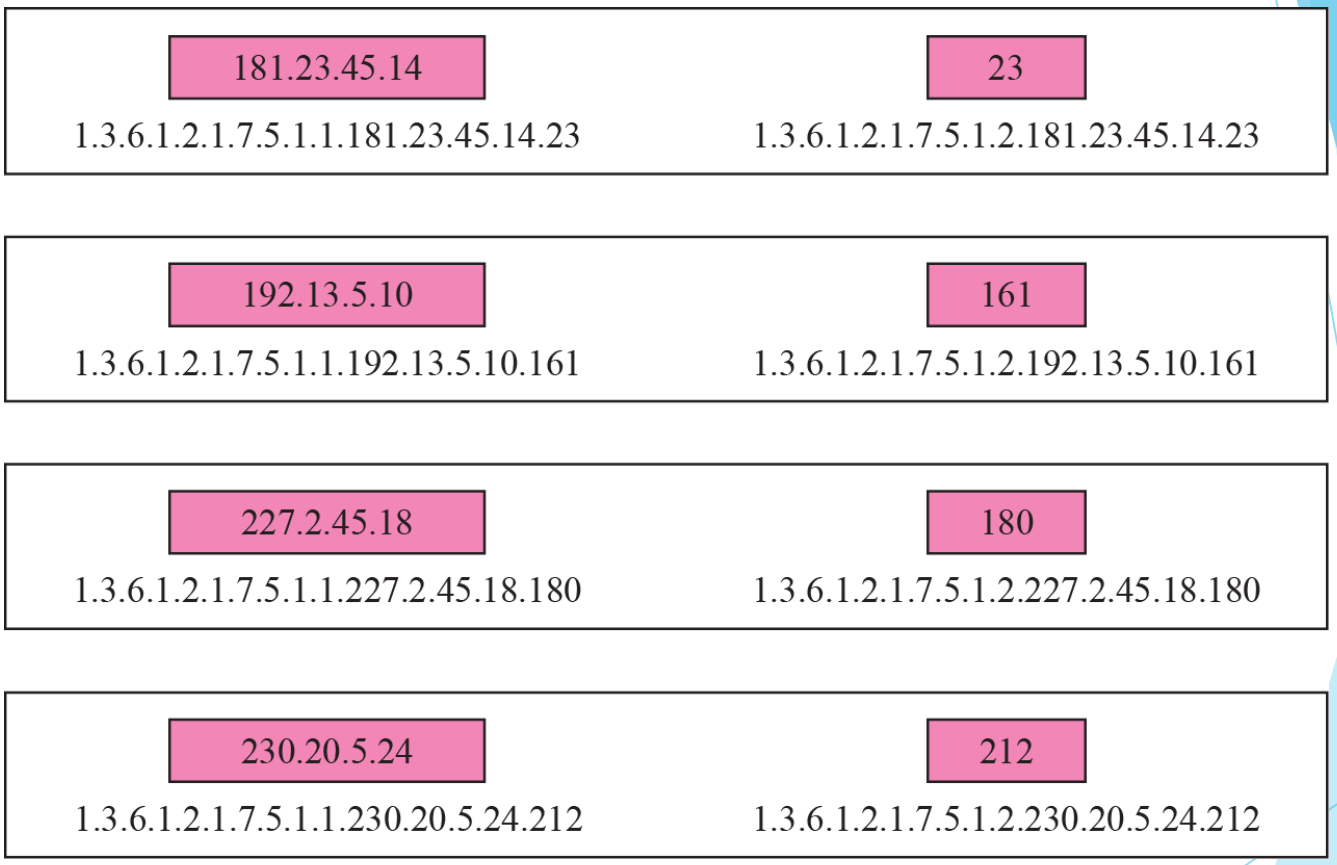
udp group


udp
1.3.6.1.2.1.7
1
udpIn
Datagrams
2
udpNo
Ports
3
udpIn
Errors
4
udpOut
Datagrams
5
udpTable
1
udpEntry
1
udpLocal
Address
2
udpLocal
Port

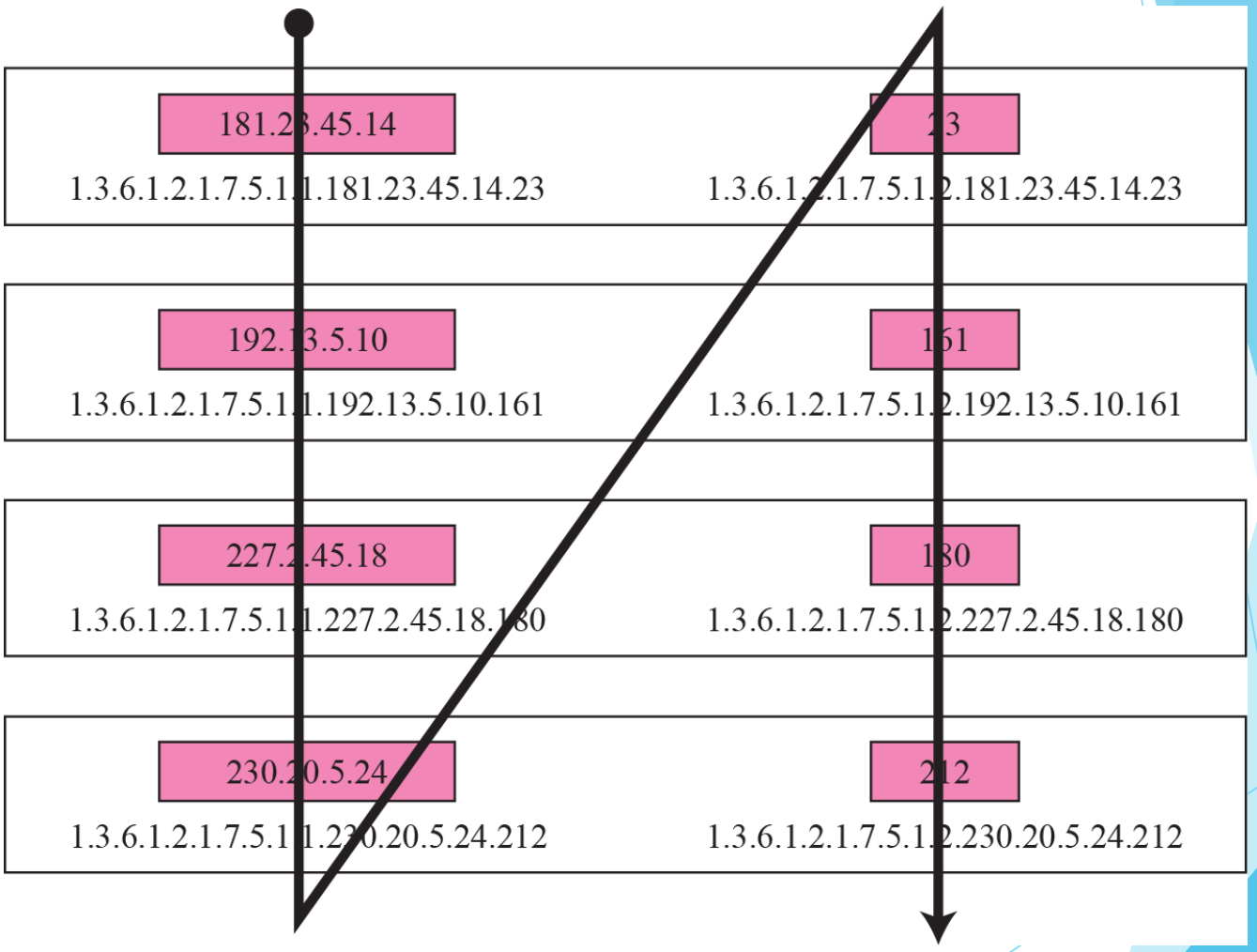
udp variables and tables



Indexes for udpTable



Lexicographic ordering

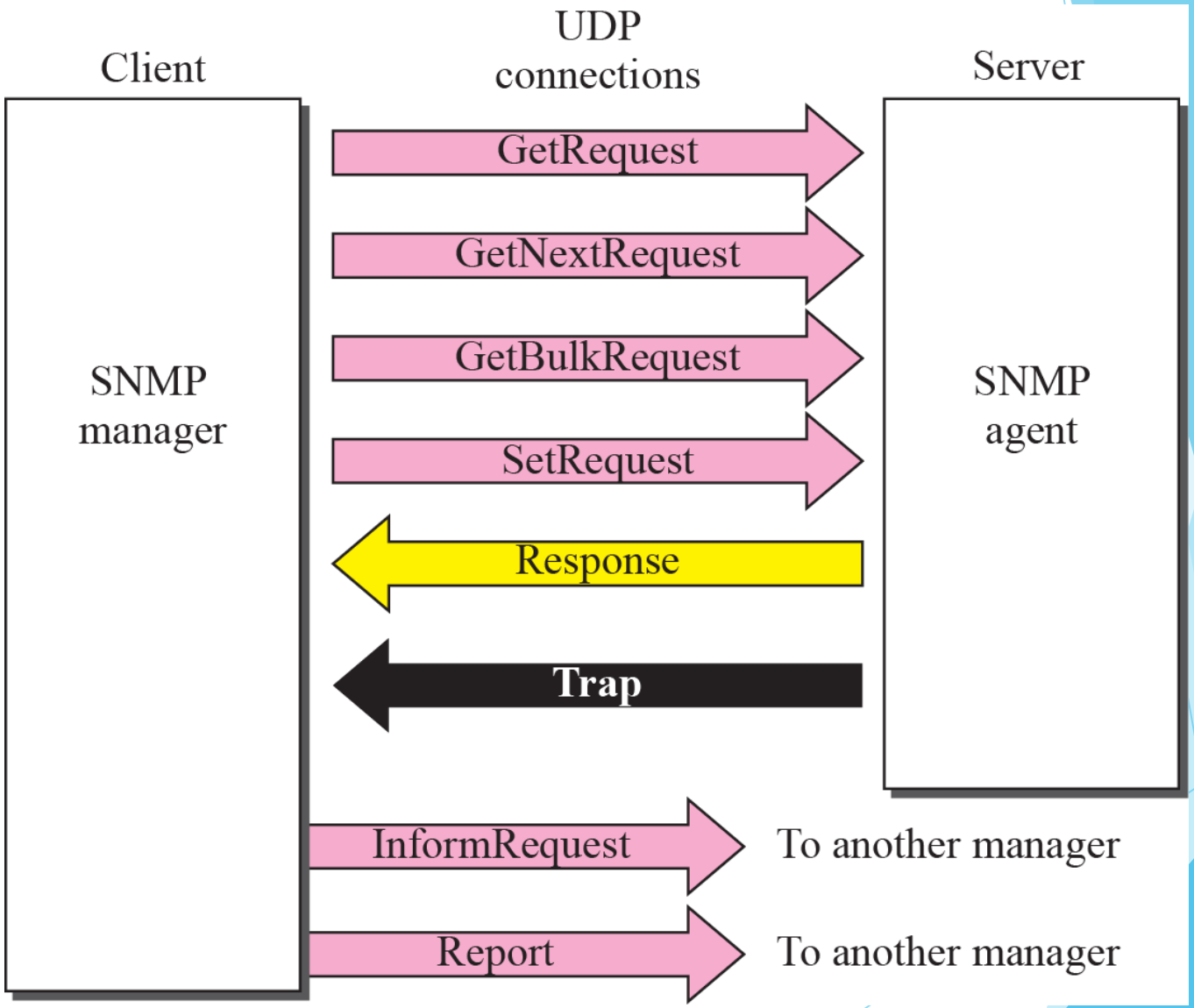


SNMP

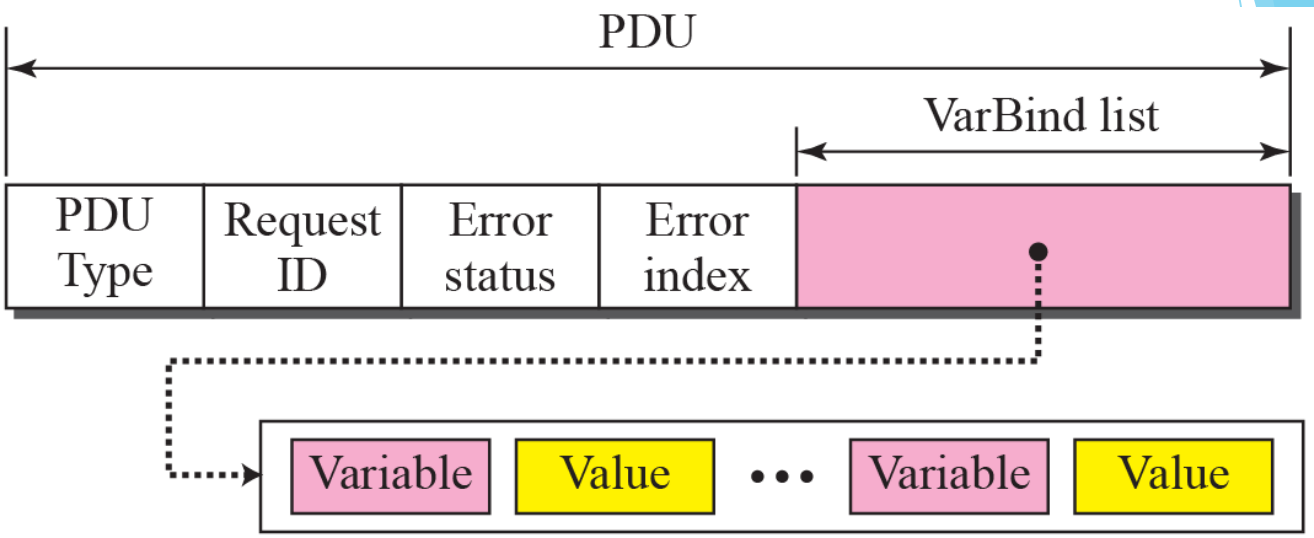
SNMP uses both SMI and MIB in Internet network management. It is an application program that allows:

1. A manager to retrieve the value of an object defined in an agent.
2. A manager to store a value in an object defined in an agent.
3. An agent to send an alarm message about an abnormal situation to the manager.

SNMP PDUs


Client
UDP connections
Server
SNMP manager
SNMP agent
GetRequest
GetNextRequest
GetBulkRequest
SetRequest
Response
Trap
InformRequest
To another manager
Report
To another manager

SNMP PDU format



Differences:

1. Error status and error index values are zeros for all request messages except GetBulkRequest.
2. Error status field is replaced by non-repeater field and error index field is replaced by max-repetitions field in GetBulkRequest.

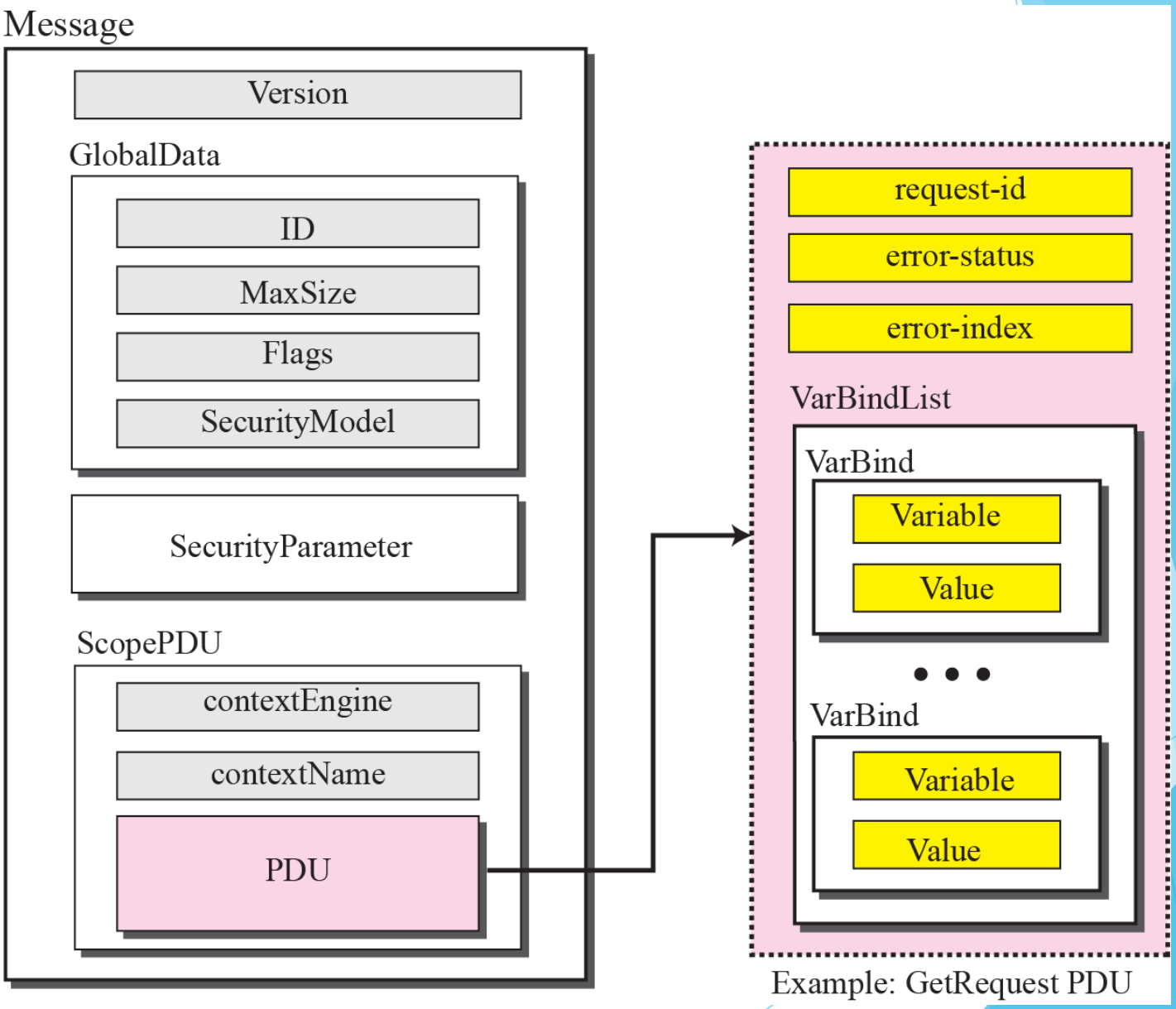
Table 24.3 *PDU Types*

Type	*Tag (Binary)*	*Tag (Hex)*
GetRequest	**10100000**	**A0**
GetNextRequest	**10100001**	**A1**
Response	**10100010**	**A2**
SetRequest	**10100011**	**A3**
GetBulkRequest	**10100101**	**A5**
InformRequest	**10100110**	**A6**
Trap (SNMPv2)	**10100111**	**A7**
Report	**10101000**	**A8**

Table 24.4 *Types of Errors*

Status	*Name*	*Meaning*
0	noError	No error
1	tooBig	Response too big to fit in one message
2	noSuchName	Variable does not exist
3	badValue	The value to be stored is invalid
4	readOnly	The value cannot be modified
5	genErr	Other errors

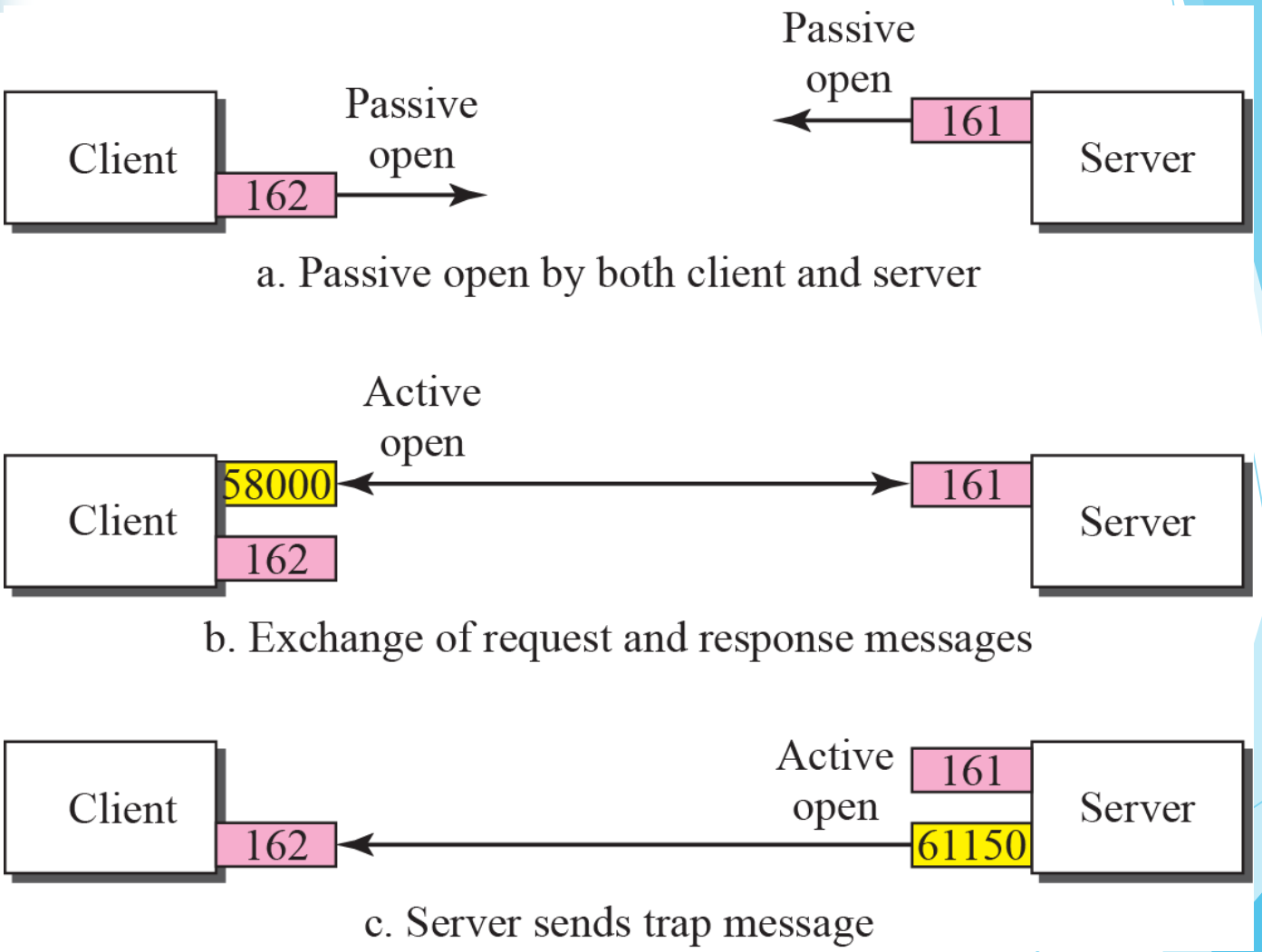
SNMP message



UDP PORTS

SNMP uses the services of UDP on two well-known ports, 161 and 162. The well-known port 161 is used by the server (agent), and the well-known port 162 is used by the client (manager).

Port numbers for SNMP



SECURITY

SNMPv3 has added two new features to the previous version: security and remote administration. SNMPv3 allows a manager to choose one or more levels of security when accessing an agent. Different aspects of security can be configured by the manager to allow message authentication, confidentiality, and integrity.

SNMPv3 also allows remote configuration of security aspects without requiring the administrator to actually be at the place where the device is located.

IP Over ATM

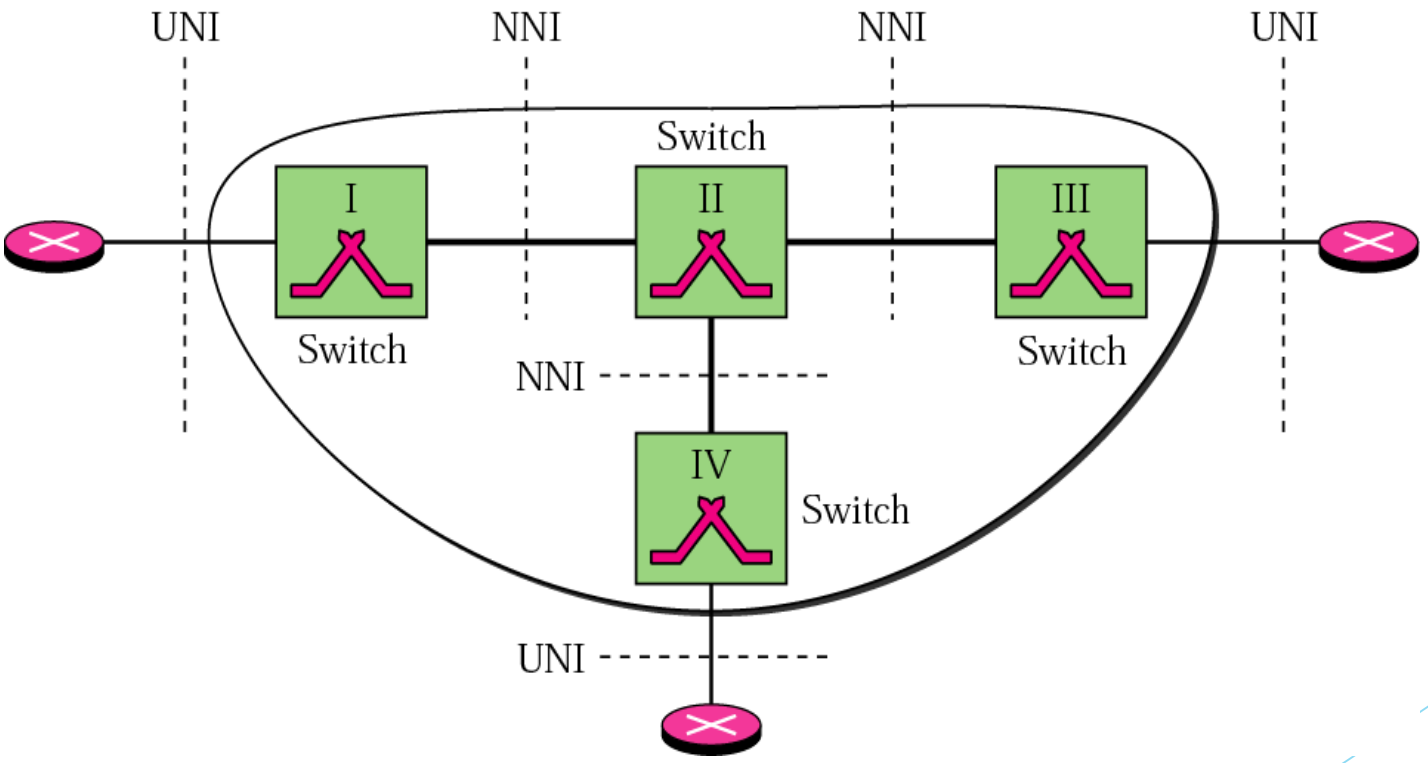
ATM WANS

We review some features of the ATM WAN needed to understand IP over ATM. The only AAL used by the Internet is AAL5, sometimes called the simple and efficient adaptation layer (SEAL).

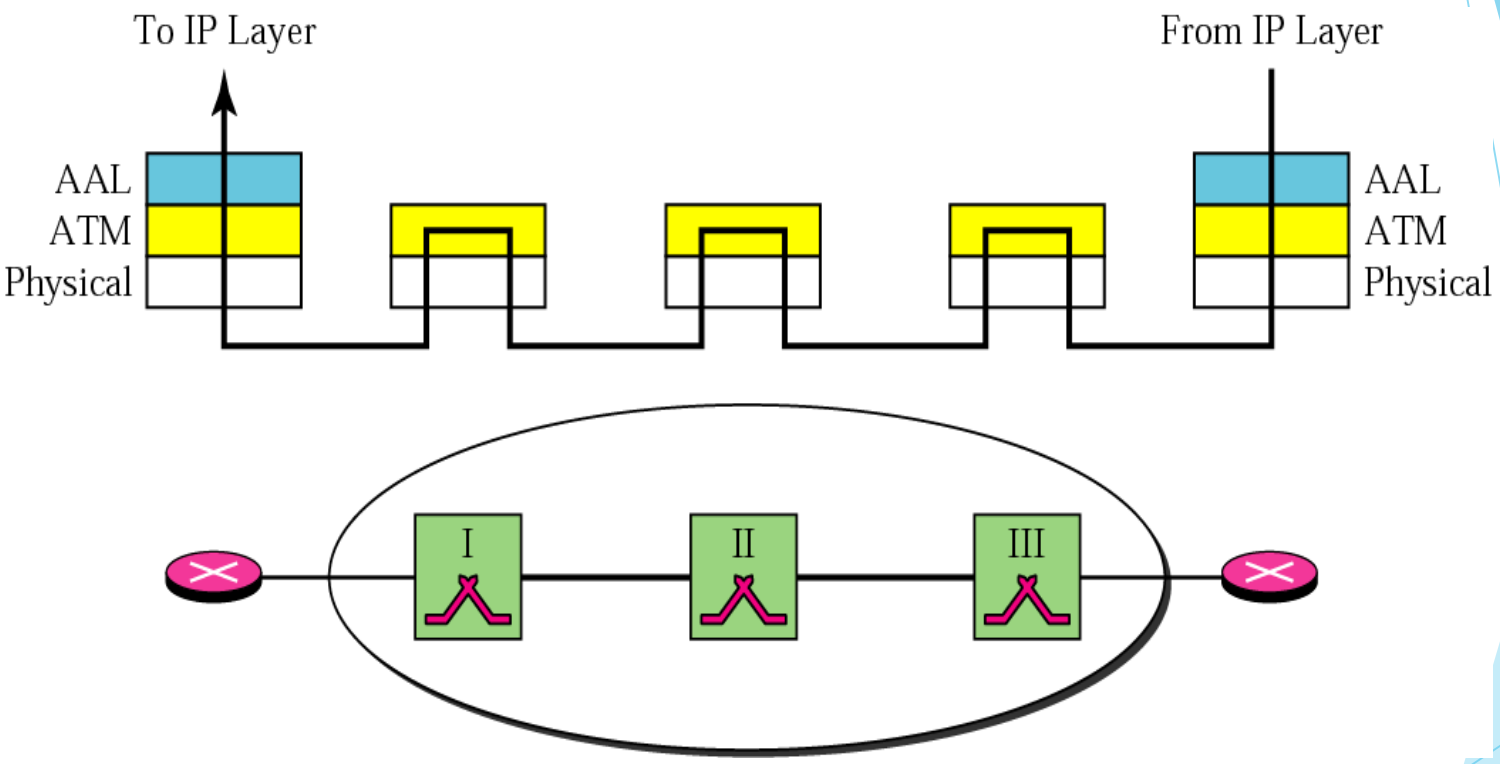
The topics discussed in this section include:

- ***Layers***

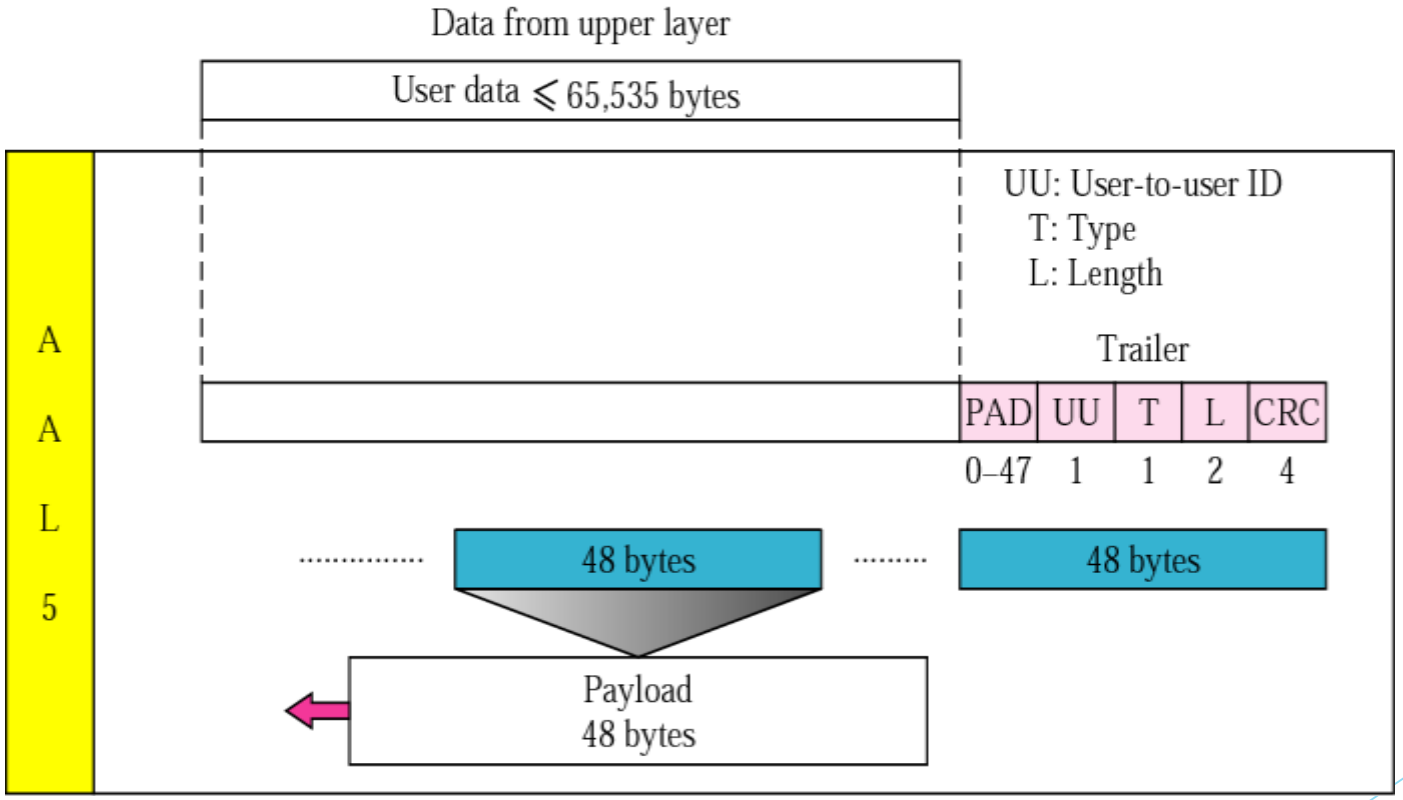
An ATM WAN in the Internet



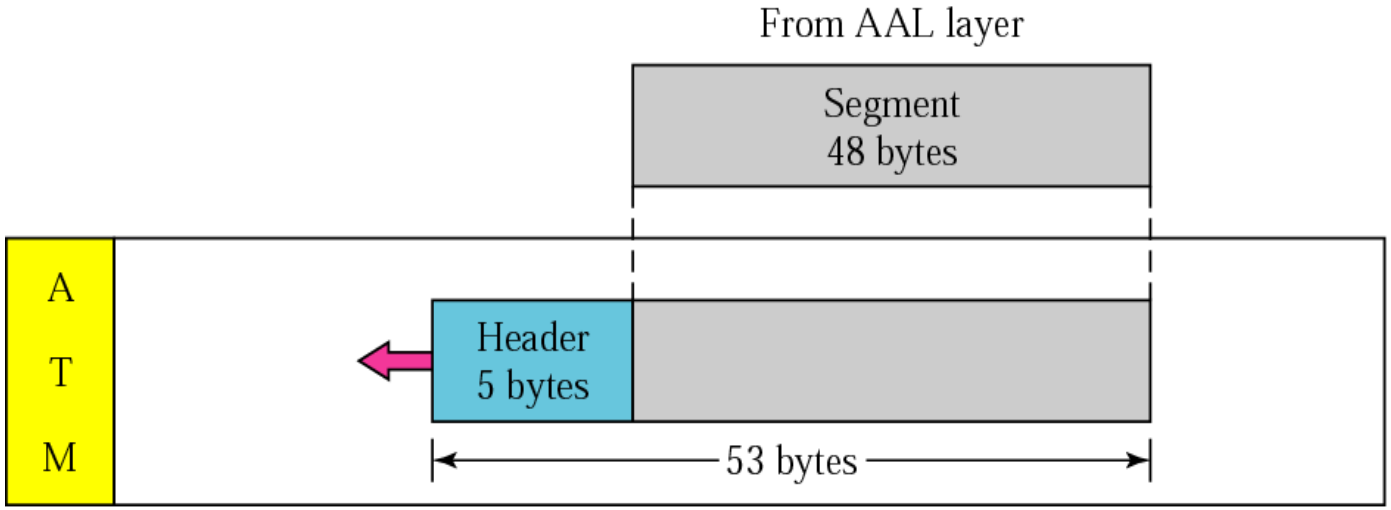
ATM layers in routers and switches



AAL5

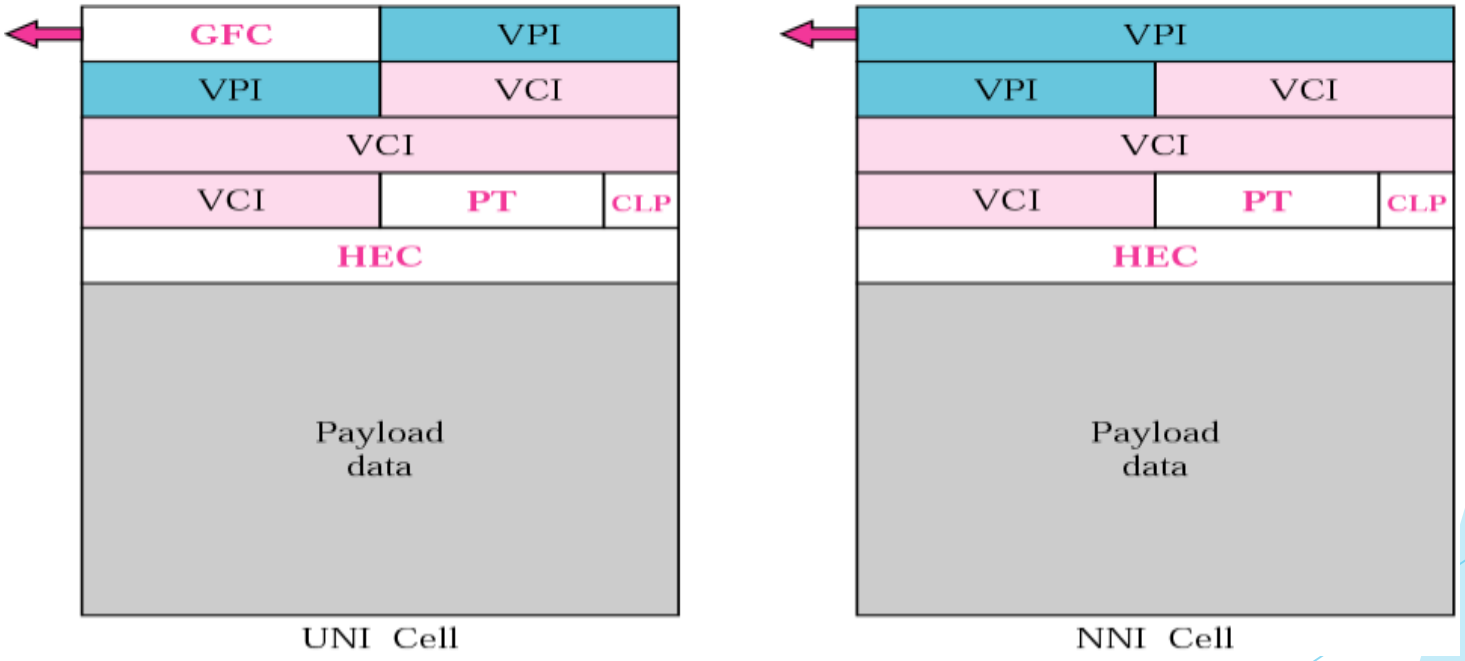

Data from upper layer
User data ⩽ 65,535 bytes
UU: User-to-user ID
T: Type
L: Length
Trailer
PAD
UU
T
L
CRC
0–47
1
1
2
4
AAL5
48 bytes
48 bytes
Payload
48 bytes

ATM layer



ATM headers

GFC: Generic flow control
VPI: Virtual path identifier
VCI: Virtual channel identifier
PT: Payload type
CLP: Cell loss priority
HEC: Header error control



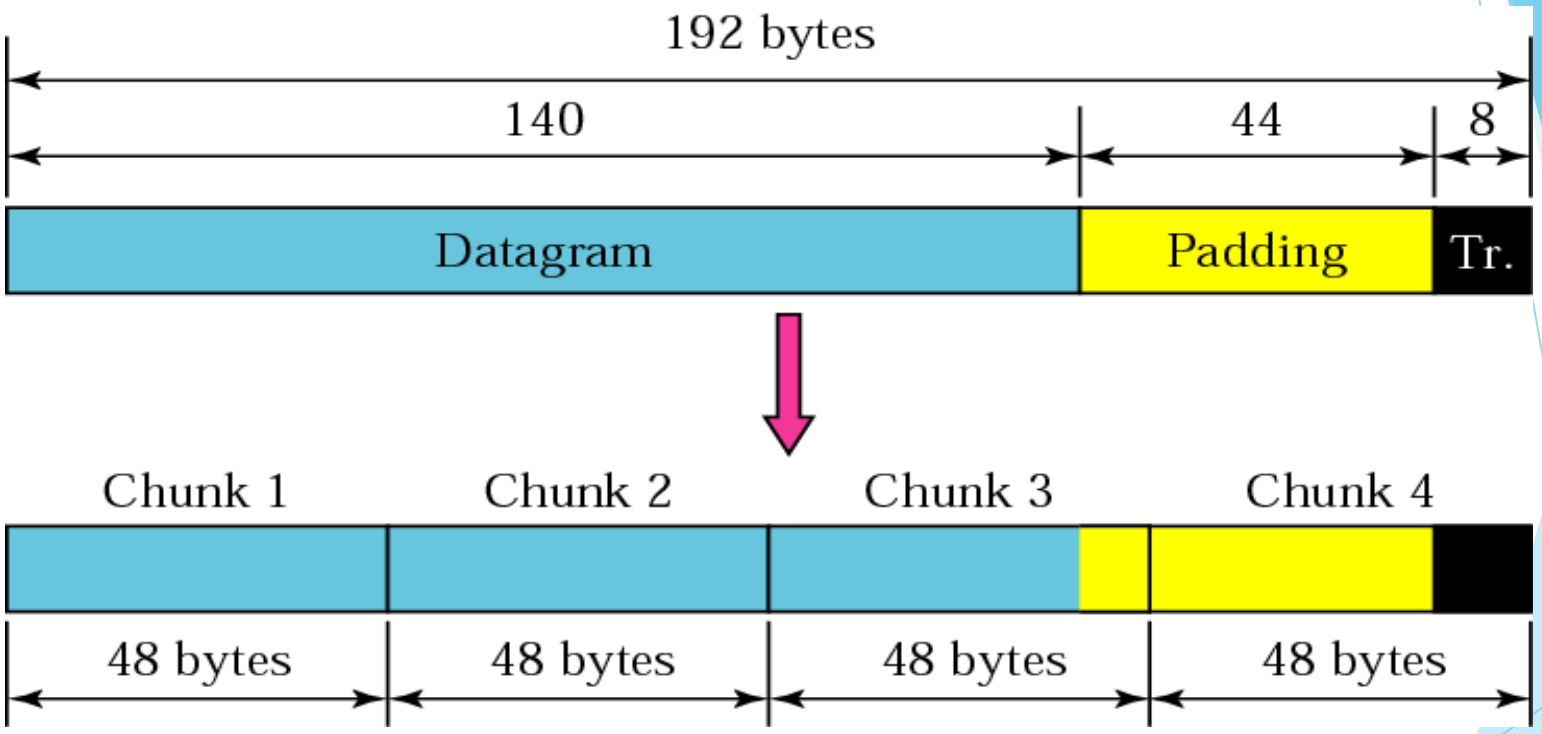
CARRYING A DATAGRAM IN CELLS

We show how an example of a datagram encapsulated in four cells and transmitted through an ATM network.

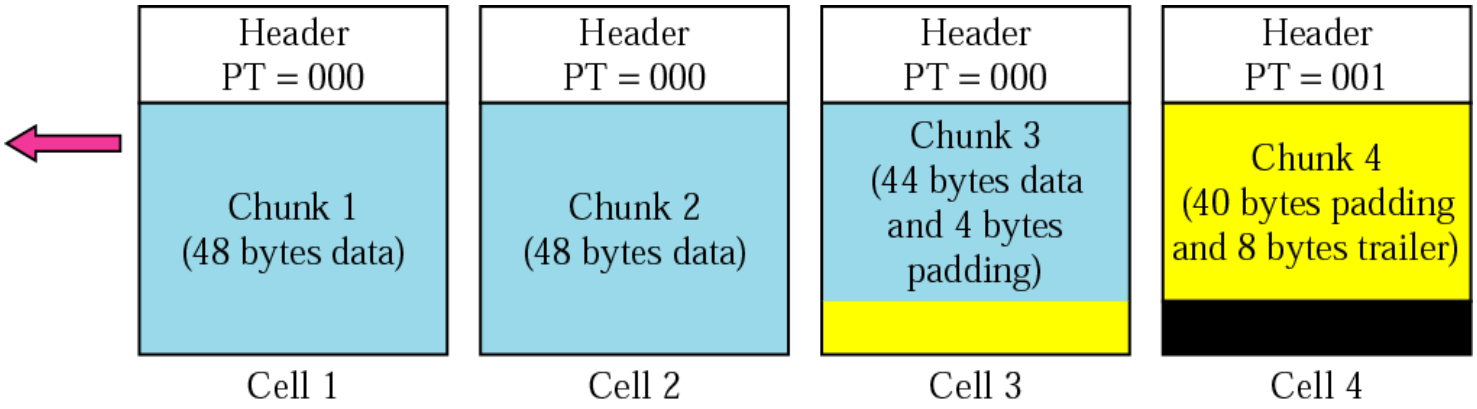
The topics discussed in this section include:

Why Use AAL5?

Fragmentation



ATM cells


Header
PT = 000
Chunk 1
(48 bytes data)
Cell 1
Header
PT = 000
Chunk 2
(48 bytes data)
Cell 2
Header
PT = 000
Chunk 3
(44 bytes data
and 4 bytes
padding)
Cell 3
Header
PT = 001
Chunk 4
(40 bytes padding
and 8 bytes trailer)
Cell 4

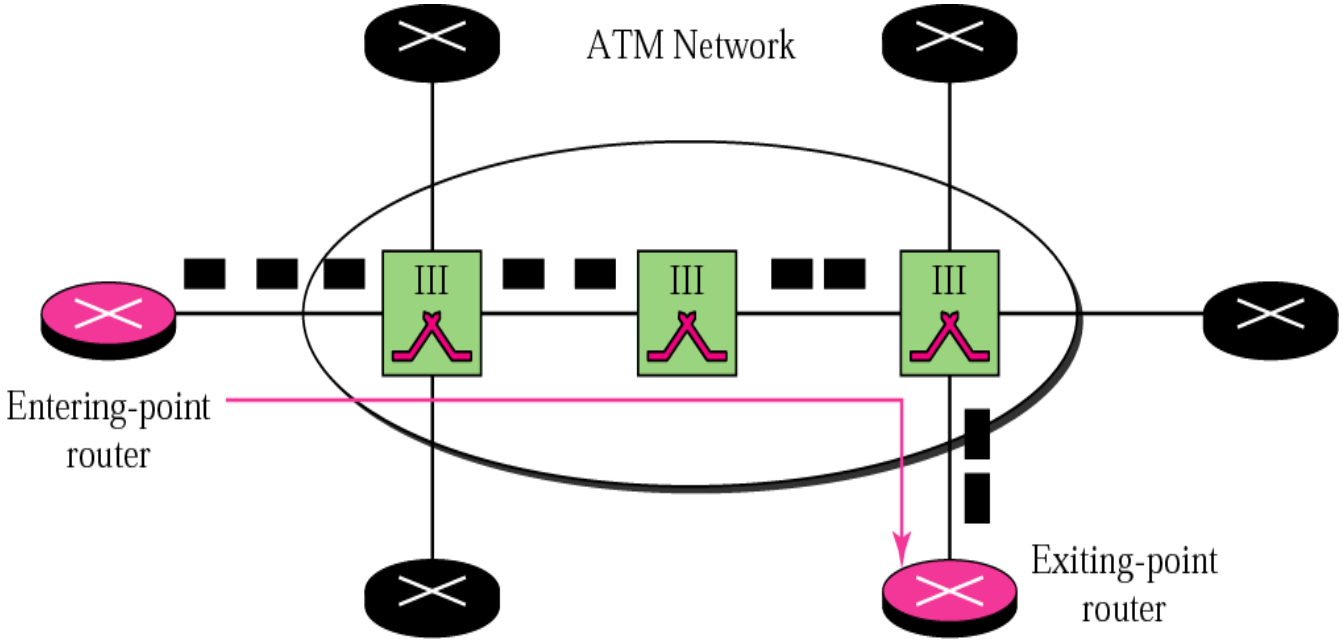
ROUTING THE CELLS

The ATM network creates a route between two routers. We call these routers entering-point and exiting-point routers.

The topics discussed in this section include:

Addresses
Address Binding

Entering-point and exiting-point routers



ATMARP

ATMARP finds (maps) the physical address of the exiting-point router given the IP address of the exiting-point router. No broadcasting is involved.

The topics discussed in this section include:

Packet Format
ATMARP Operation

ATMARP packet

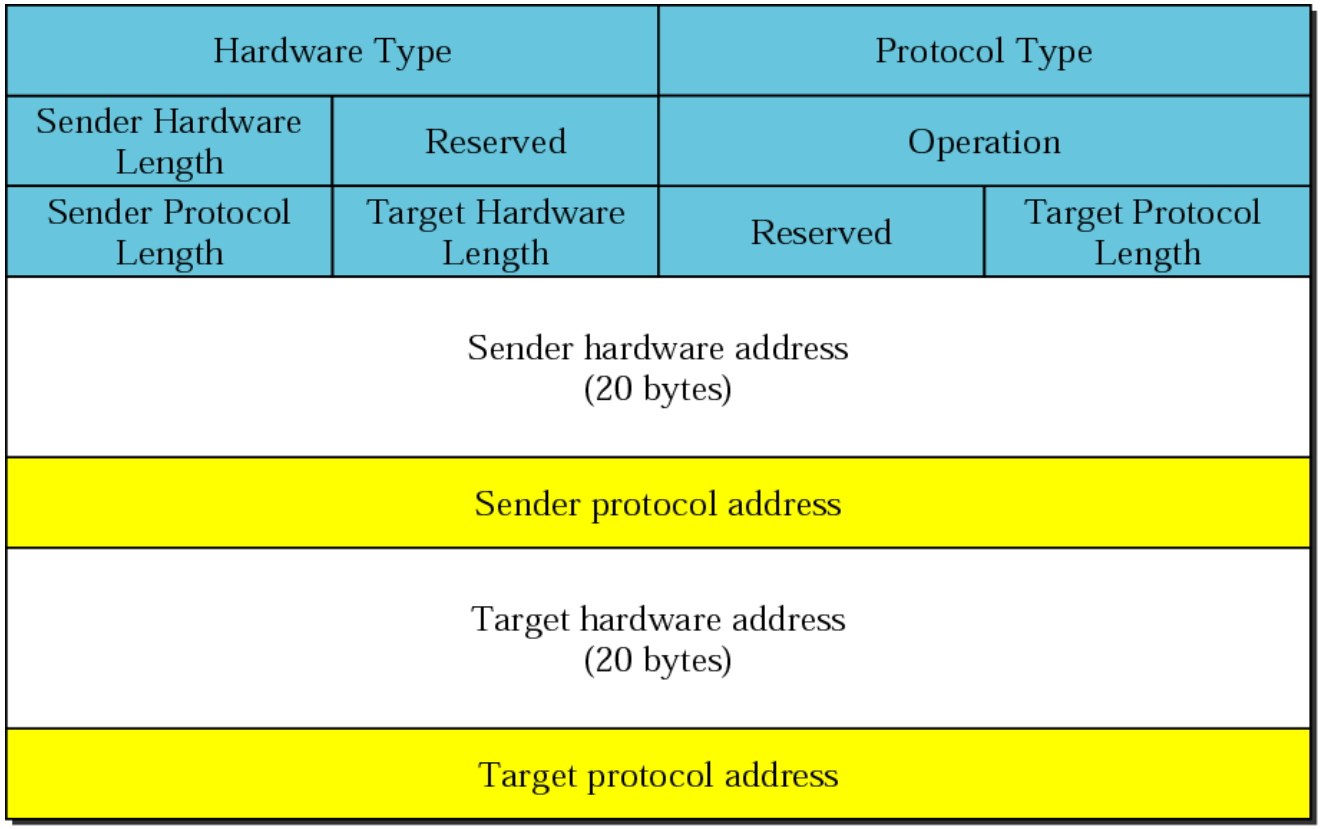
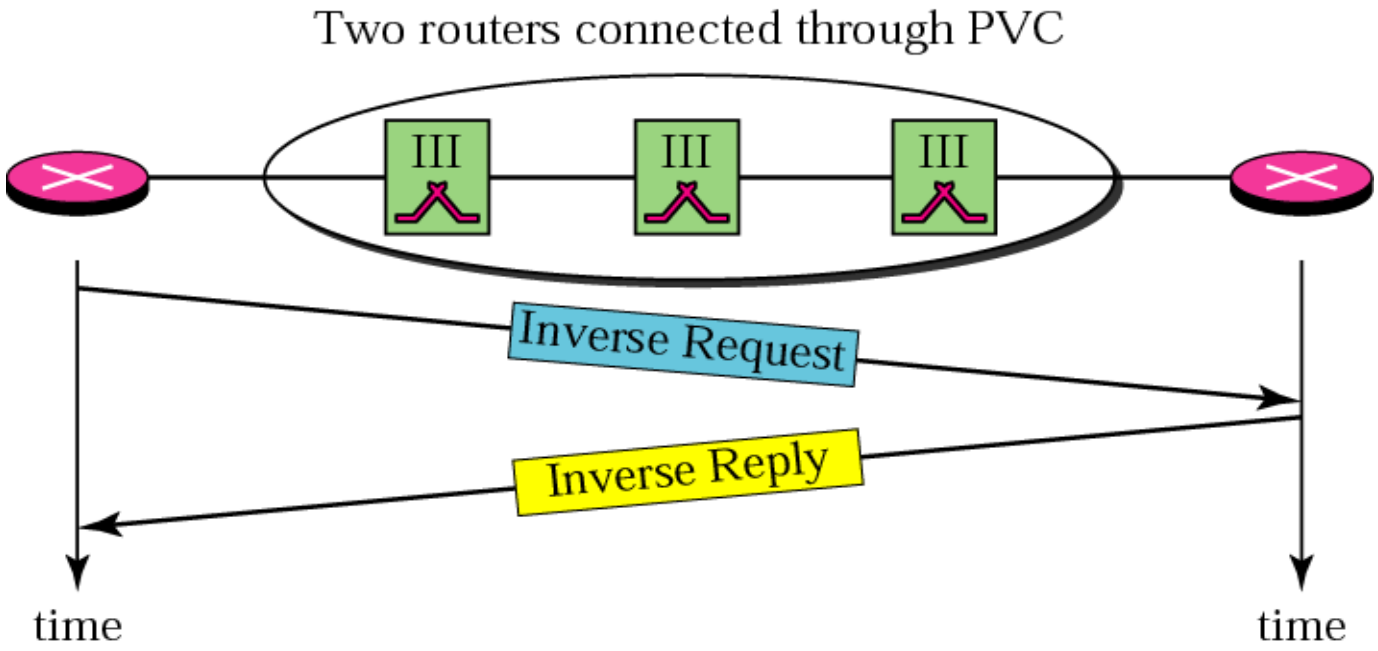


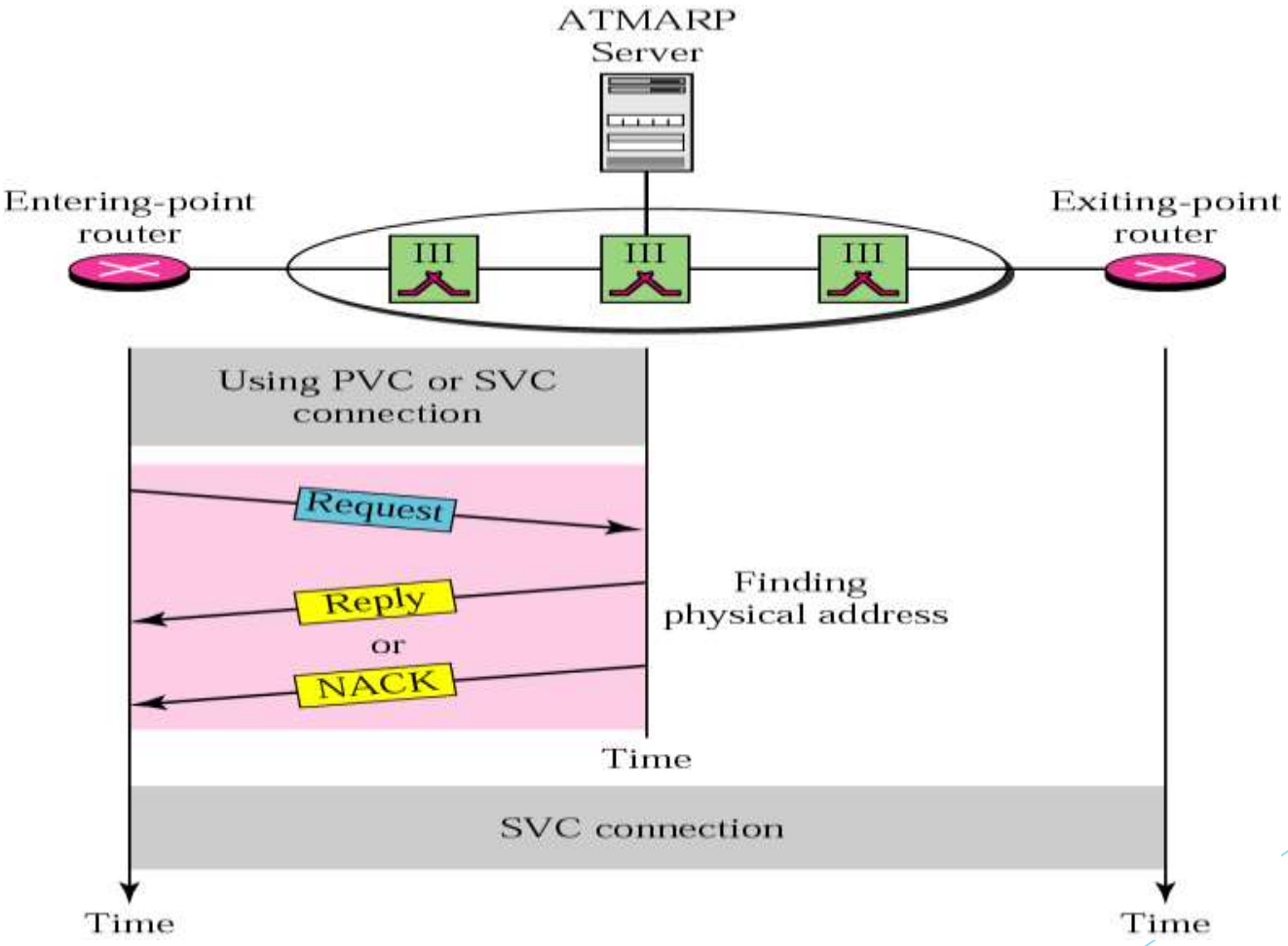
Table 23.1 OPER field

Message	*OPER value*
Request	1
Reply	2
Inverse Request	8
Inverse Reply	9
NACK	10

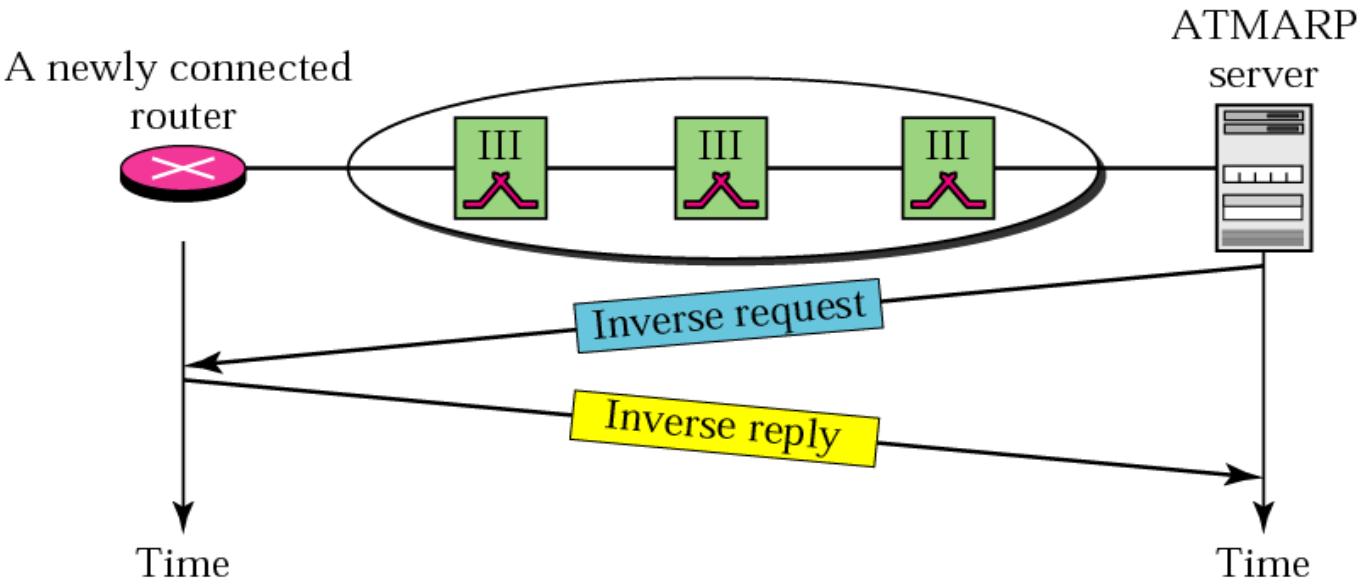
Binding with PVC



Binding with ATMARP



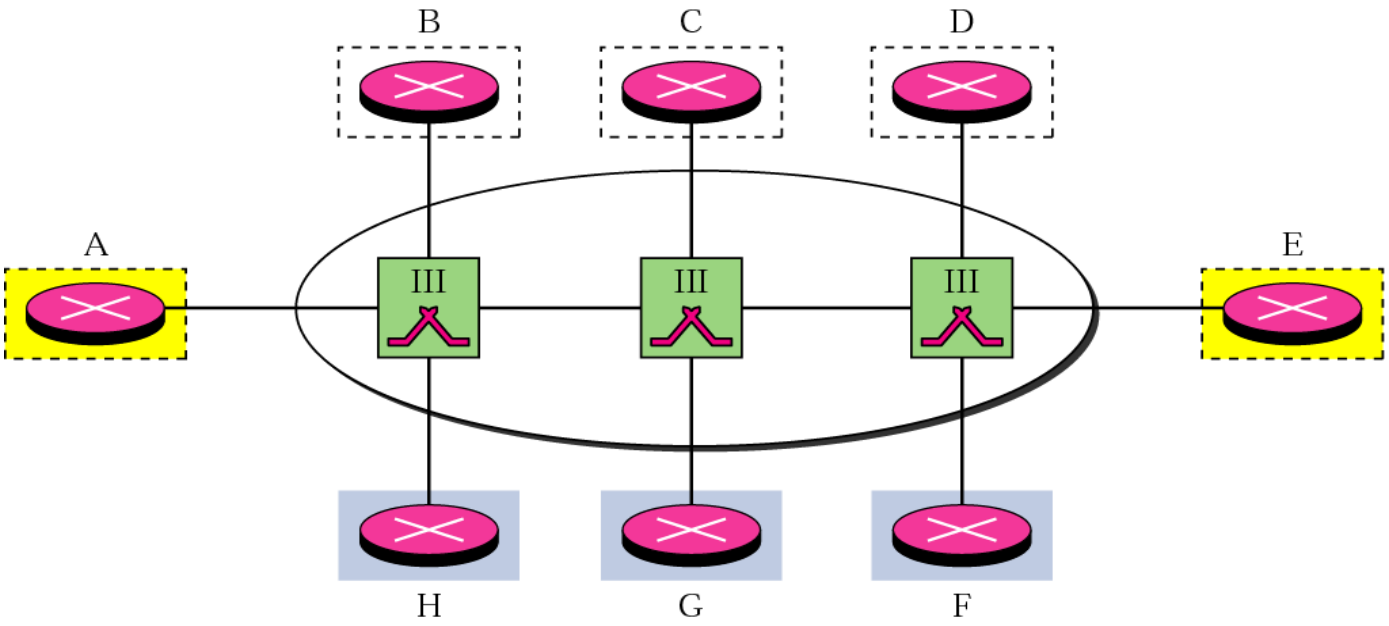
Building a table



LOGICAL IP SUBNET (LIS)

An ATM network can be divided into logical (not physical) subnetworks. This facilitates the operation of ATMARP and other protocols (such as IGMP) that need to simulate broadcasting on an ATM network.

LIS



MOBILE IP

ADDRESSING

Addressing

- **Addressing**
  - The main problem that must be solved in mobile communication using the IP protocol
- The original IP address was based on the assumption that a host is stationary
  - Routers use the hierarchical structure of an IP address to route an IP datagram
  - The address is valid only when it is attached to the network
    - If the network changes, the address is no longer valid

Mobile Hosts

- When a host moves from one network to another
  - The IP addressing structure needs to be modified
- Possible solutions
  - Changing the address
  - Two addresses

Changing the Address

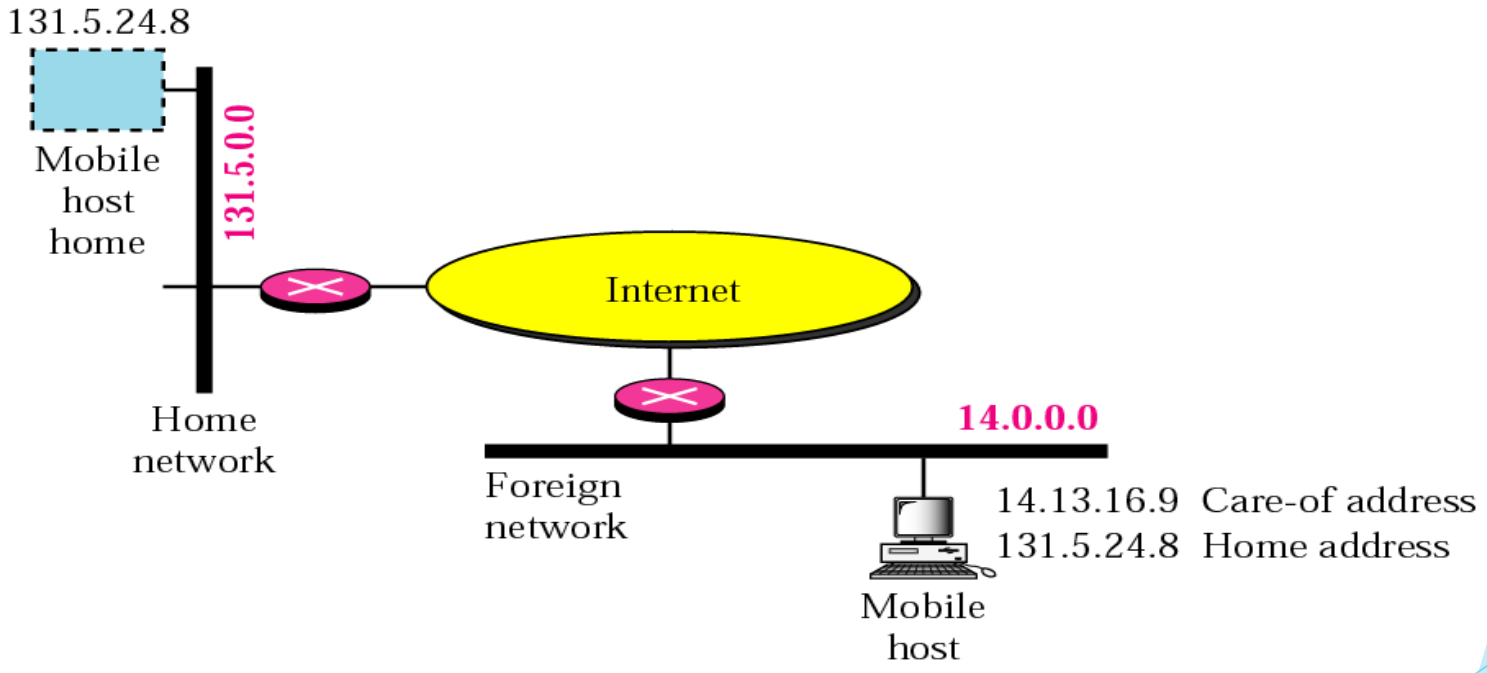
- The most host changes its address as it goes to the new network
  - For example, DHCP protocol
- Drawbacks
  - The configuration files would need to be changed
  - Each time the computer moves from one network to another, it must be rebooted
  - The DNS tables need to be revised so that every other host in the Internet is aware of the change
  - If the host roams from one network to another *during a transmission*, the data exchange will be interrupted
    - Since the port and IP addresses of the client and the server must remain constant for the duration of the connection

Two Addresses

- The host has
  - Its original address, called the *home address*
    - Permanent and associate the host to its *home network*
  - A temporary address, called the *care-of address*
    - Temporary
    - When a host moves from one network to another, the care-of address changes
    - Associate the host with the *foreign network*
    - A mobile host receives its care-of address during the agent discovery and registration phase

Figure 27-1

Host address and Care-of Address



AGENTS

Agents

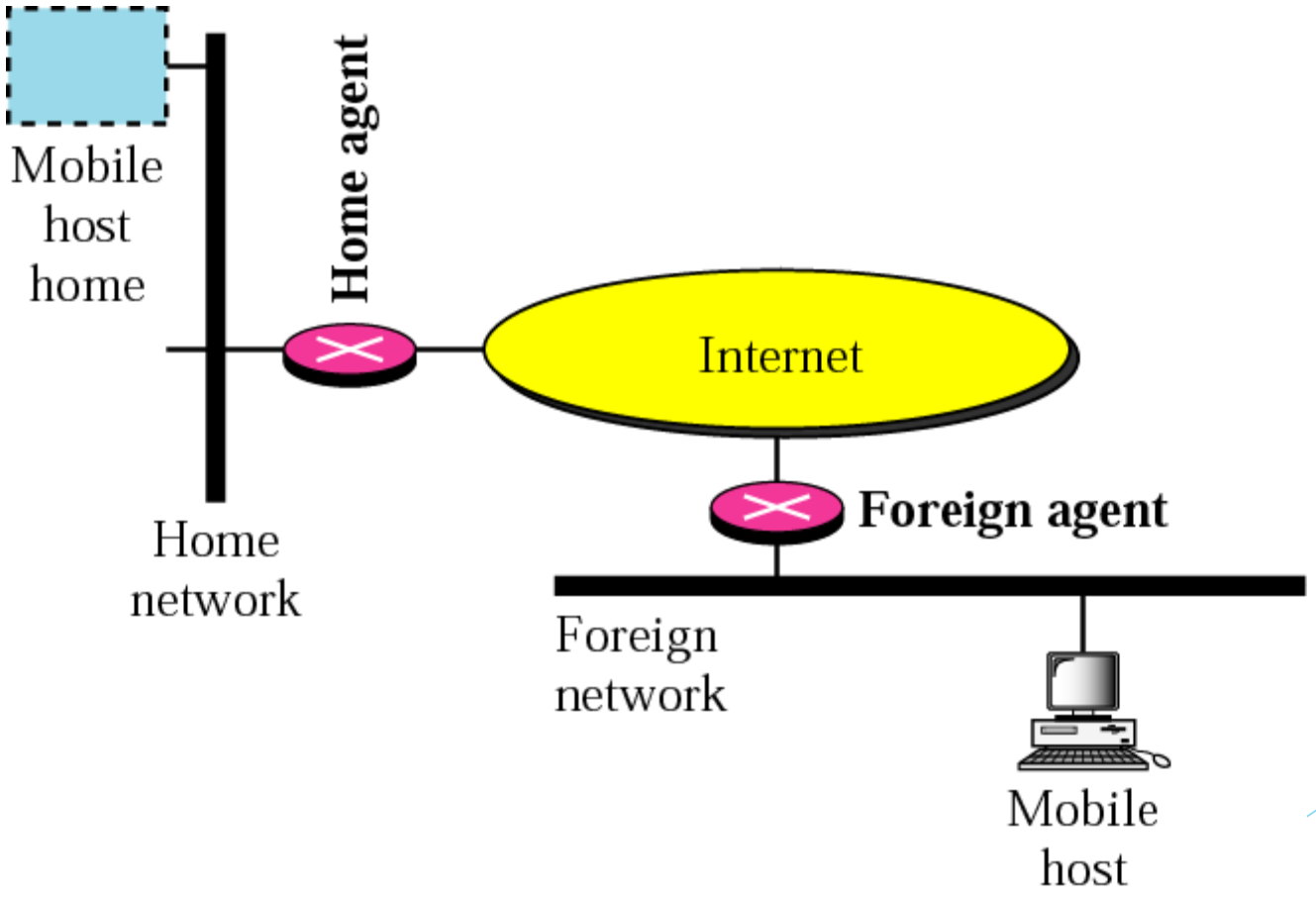
- To support Mobile IP, there are two agents
  - *Home agent* and *foreign agent*
- Home agent
  - Usually a router attached to the home network of the mobile host
  - Acts on behalf of the mobile host when a remote host sends a packet to the mobile host
    - The home agent then sends it to the foreign agent

Agents

- Foreign Agent
  - Usually a router attached to the foreign network
  - Receive and delivers packets sent by the home agent to the mobile host
- A mobile host can also act as a foreign agent
  - The care-of address is called a *colocated care-of address*
  - Advantages:
    - The mobile host can move to any network without worrying about the availability of a foreign agent
  - Disadvantages
    - The mobile host needs extra software to act as its own foreign agent

Figure 27-2

Home Agent and Foreign Agent



THREE PHASES

Three Phases

- To communicate with a remote host, a mobile host goes through three phases
  - ***Agent discovery***
    - Involve the mobile host, the foreign agent, and the home agent
  - ***Registration***
    - Involve the mobile host and two agents
  - ***Data transfer***
    - All four entities are involved

Figure 27-3

Remote Host and Mobile Host Communication:

AGENT DISCOVERY

Agent Discovery

- Consist of two subphases
  - A mobile host must discover a *home agent* before it leaves its home network
  - A mobile host must also discover a *foreign agent* after it has moved to a foreign network
    - Discover the *care-of address* and the *foreign agent's address*
- The discovery involves two types of messages
  - *Advertisement* and *solicitation*

Agent Advertisement

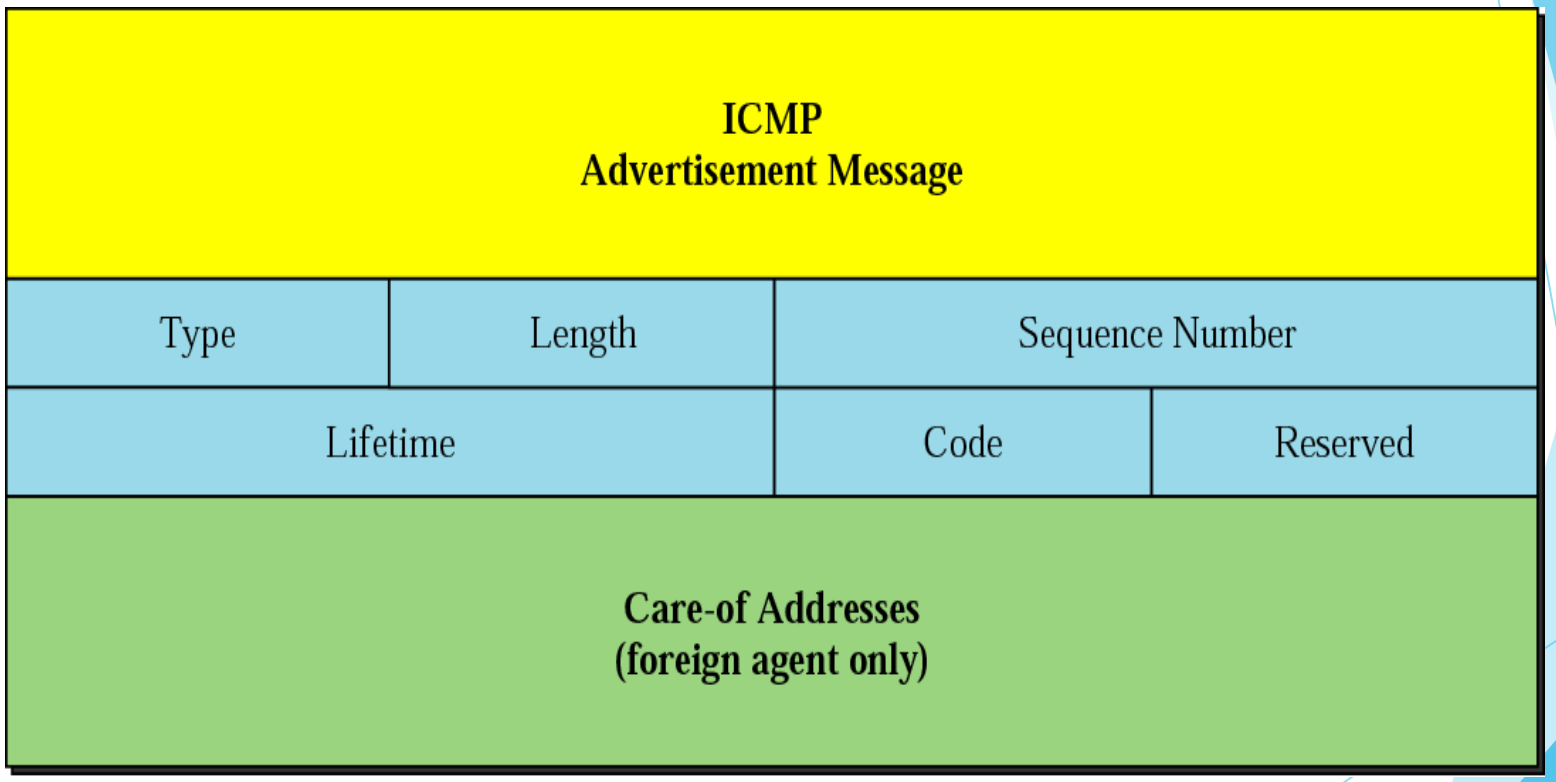
- When a router advertises its presence on a network using an *ICMP router advertisement*
  - It can append an *agent advertisement* to the packet if it acts as an agent
- Thus, an agent advertisement is piggybacked to the router advertisement packet

Packet Format of Agent Advertisement

- **Type:** set to 16
- **Length:**8-bit
  - Define the total length of the extension message
- **Sequence Number:** 16-bit
  - Hold the message number
- **Lift time:** 16-bit
  - Define the number of seconds that the agent will accept the request
- **Code:** 8-bit
  - See the Table 27.1
- **Care-of-Address:** a list of addresses available for uses as care of address. This field is used only by a foreign agent
  - The mobile host can choose one of these addresses.
  - The selection of this care-of address is announced in the *registration request message*

Figure 27-4

Agent Advertisement



Code Bits

Bit	Meaning
0	Registration required. No co-located care-of address
1	Agent is busy and does not accept registration at this moment
2	Agent acts as a home agent
3	Agent acts as a foreign agent
4	Agent uses minimal encapsulation
5	Agent uses generic routing encapsulation (GRE)
6	Agent supports header compression
7	Unused (0)

Agent Solicitation

- When a mobile host has moved to a new network and has not received agent advertisements
  - It can initiate *an agent solicitation*
- Also, *agent solicitation* is piggybacked to the *ICMP solicitation message*

REGISTRATION

Registration

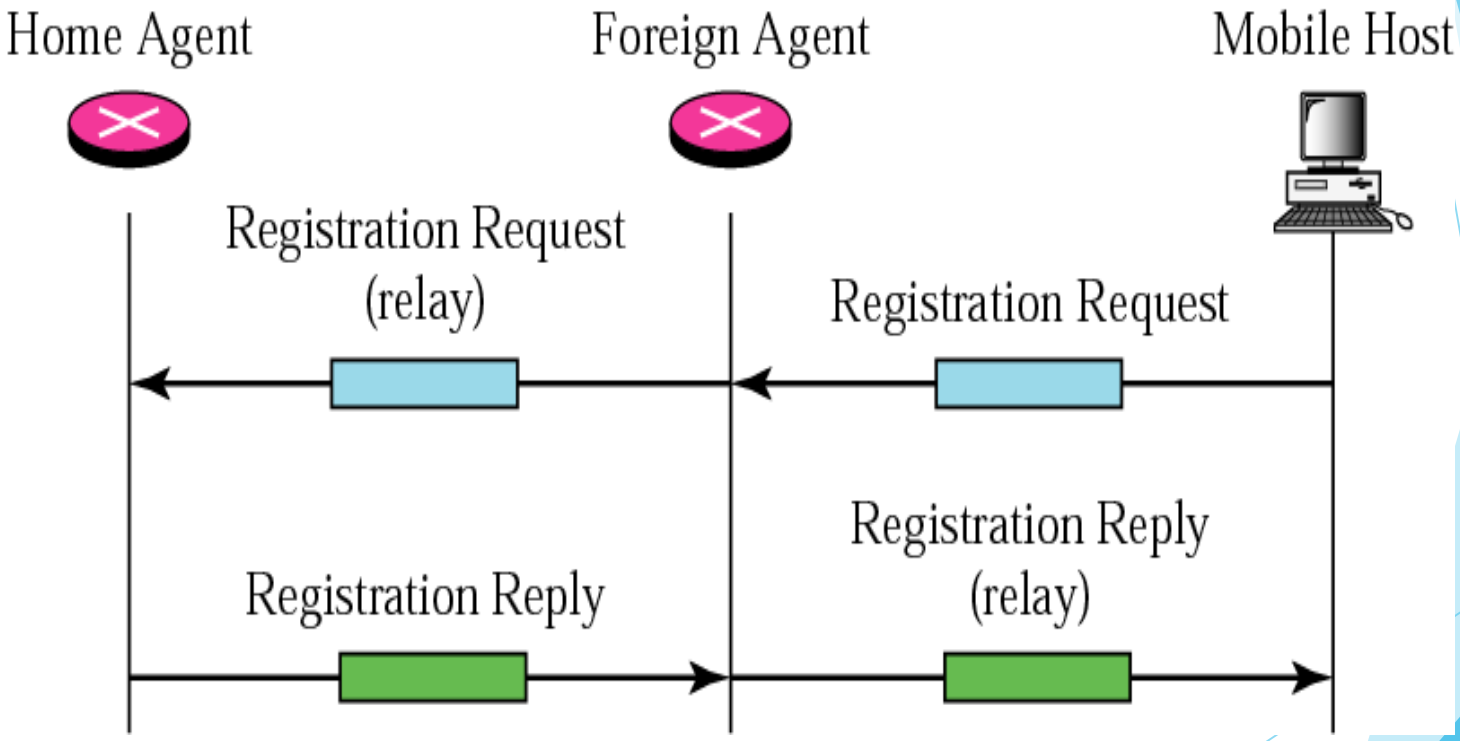
- After a mobile host has moved to a foreign network and discovered the foreign agent, it must register
- Four aspects of registration
  - The mobile host must register itself with the foreign agent
  - The mobile host must register itself with its home agent
    - This is done normally by the foreign agent on behalf of the mobile host
  - The mobile host must renew registration if it has expired
  - The mobile host must deregistration when it returns home

Request and Reply

- Registration request and registration reply
  - To register with the *foreign agent* and the *home agent*

Figure 27-5

Registration Request and Reply



Registration Request

- Sent from the mobile host to the foreign agent
  - To register its *care-of address*
  - To announce its *home address* and *home agent address*
- The foreign will then relay the request to the home agent
  - Home agent now knows the address of the foreign agent
    - Since the relay packet's source address is the foreign agent's IP address

Registration Request Format

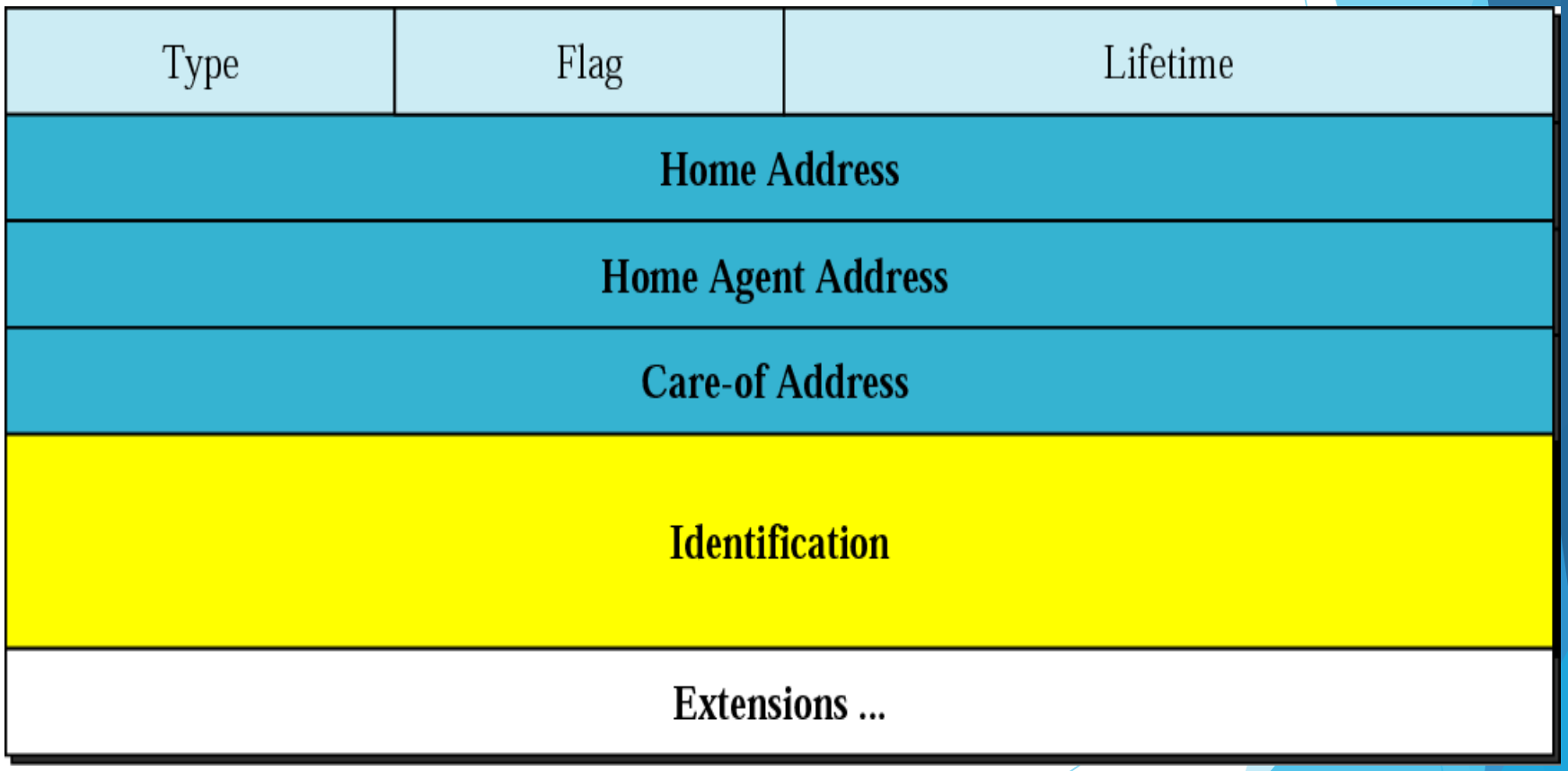
- **Type:** 8-bit
  - Define the type of the message
- **Flag:** 8-bit
  - Define forwarding information.
  - The value of each bit can be set or unset. See next slide
- **Lifetime:** 16-bit
  - Define the number of seconds the registration is valid
  - If a string of 0s: the request message is deregistration
  - If a string of 1s: the lifetime is infinite

Registration Request Flag Field Bits

Bit	Meaning
0	Mobile host requests that home agent retain its prior care-of address
1	Mobile host request that home agent tunnel any broadcast message
2	Mobile host is using co-located care-of address
3	Mobile host requests that home agent use minimal encapsulation
4	Mobile host requests generic routing encapsulation (GRE)
5	Mobile host requests header compression
6-7	Reserved bits

Figure 27-6

Registration Request Format



Registration Request Format (Cont.)

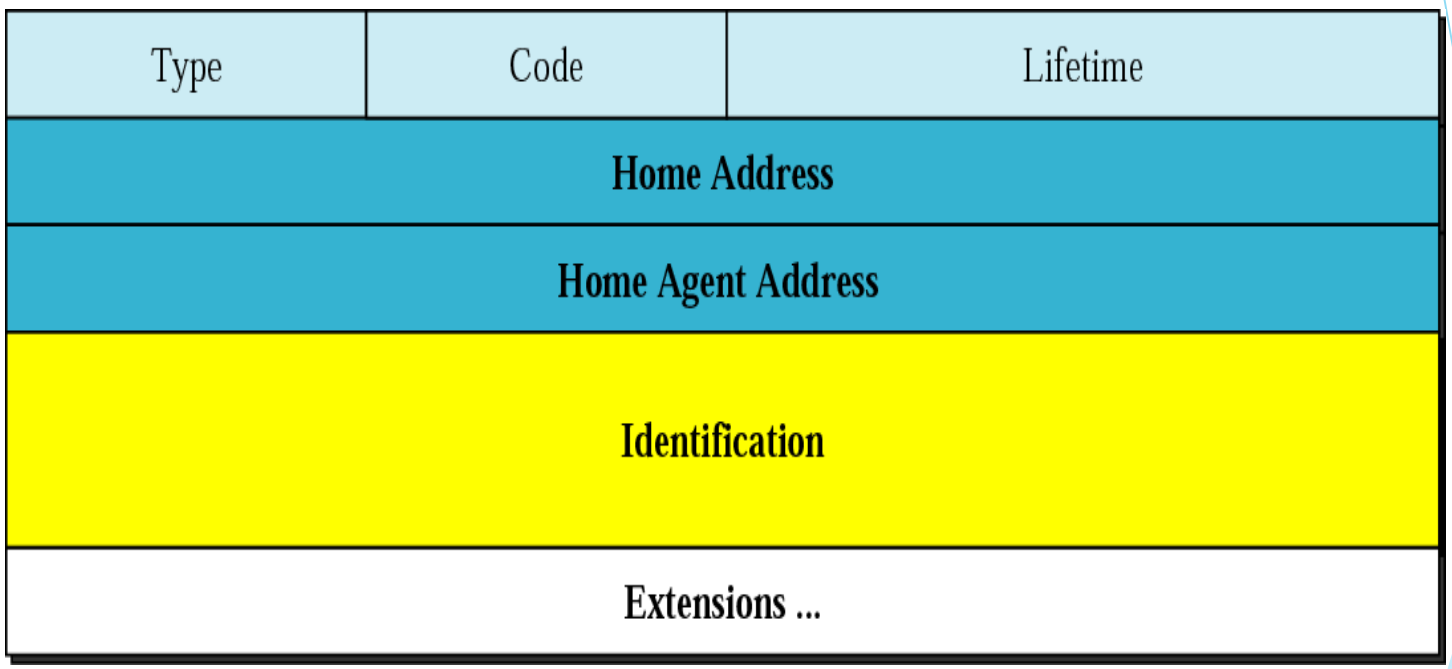
- **Home address:** 32-bit
  - Contain the permanent address of the mobile host
- **Home agent address:** 32-bit
  - Contain the address of the home agent
- **Care-of address:** 32-bit
  - Contain the temporary address of the mobile host
- **Identification:** 64-bit
  - Inserted into the request by the mobile host and repeated in the reply message
  - Used to match a request with a reply
- **Extension:**
  - Variable length extensions are used for authentication

Registration Reply

- Sent from the home agent to the foreign agent and then relayed to the mobile host
- Used to confirms or denies the registration request
- Format: similar to those of the registration request
  - **Code field** replaces the flag field
    - Show the result of the registration request (acceptance or denial)

Figure 27-7

Registration Reply Format



Encapsulation

- Registration message are encapsulated in a UDP user datagram
  - An agent uses the well-known port 434
  - A mobile host uses a temporary port

Note

A registration request or reply is sent by UDP using the well-known port 434.

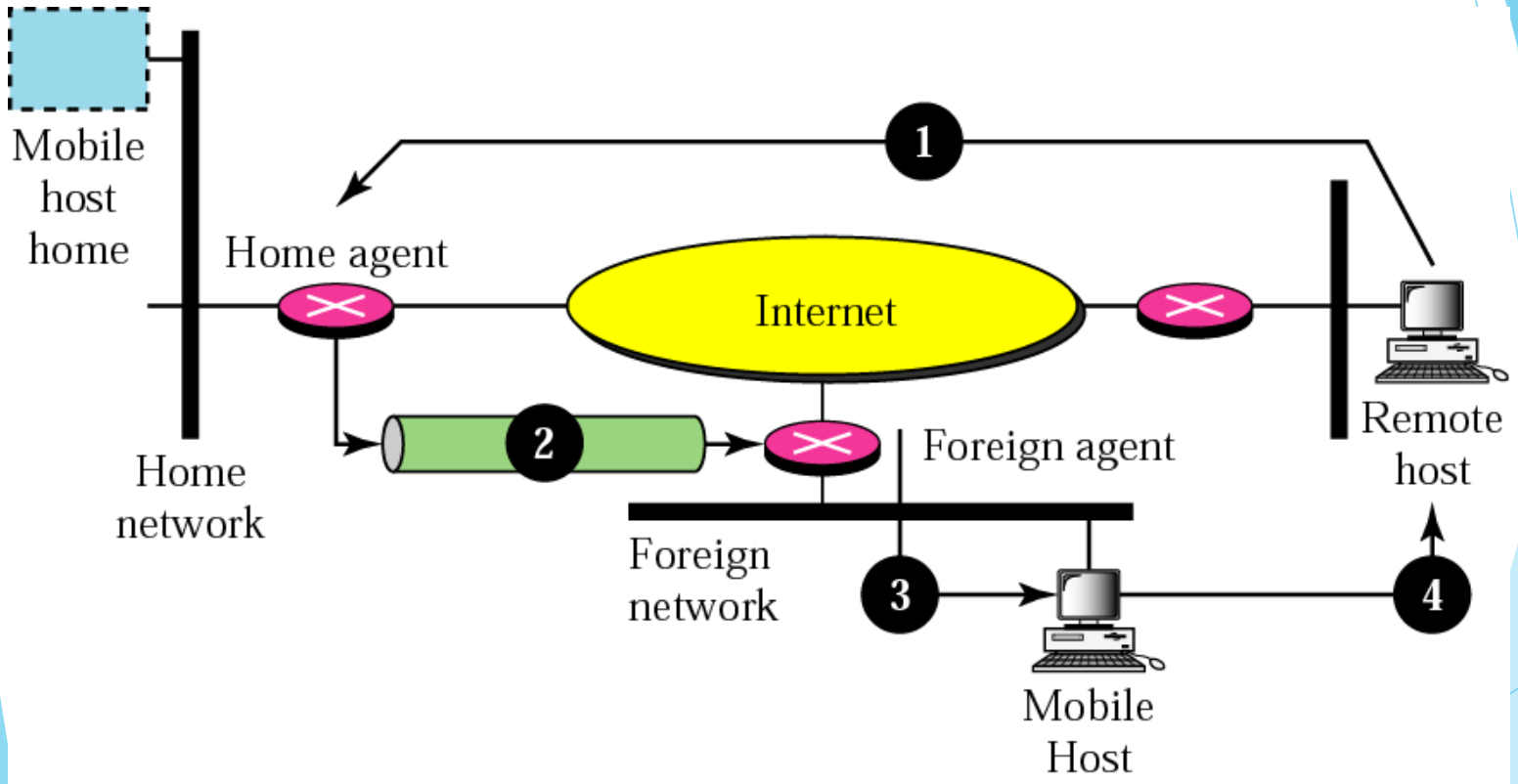
DATA TRANSFER

Data Transfer

- After agent discovery and registration, a mobile host can communicate with a remote host
  - From remote host to home agent
  - From home agent to foreign agent
  - From foreign agent to mobile host
  - From mobile host to remote host

Figure 27-8

Data Transfer



From Remote Host to Home Agent

- A remote host sends a packet to a mobile host
  - Source address: the address of the remote host
  - Destination address: the home address of the mobile host
- The packet is intercepted by the home agent, which pretends it is the mobile host
  - Using the proxy ARP

From Home Agent to Foreign Agent

- After receiving the packet, the home agent sends the packet to the foreign agent
  - Using the tunneling concept
  - The home agent encapsulates the whole IP packet inside another IP packet
    - Source address: the home agent's address
    - Destination address: the foreign agent's address

From Foreign Agent to Mobile Host

- When the foreign agent receives the packet
  - It removes the packet header added by tunneling
  - Then change the home address of the mobile host to its care-of address
  - Then send the packet to the mobile host

From Mobile Host to Remote Host

- When a mobile host wants to send a packet to a remote host
  - It sends as it does normally
  - Source address: the mobile host's home address
  - Destination address: the remote host's address

Transparency

- The remote host is unaware of any movement by the mobile host
  - To send packet
    - Destination address: the home address of the mobile host
  - To receive packet
    - Source address: the home address of the mobile host
- Thus, the movement is totally transparent

Note

The movement of the mobile host is transparent to the rest of the Internet.

INEFFICIENCY IN MOBILE IP

Inefficiency in Mobile IP

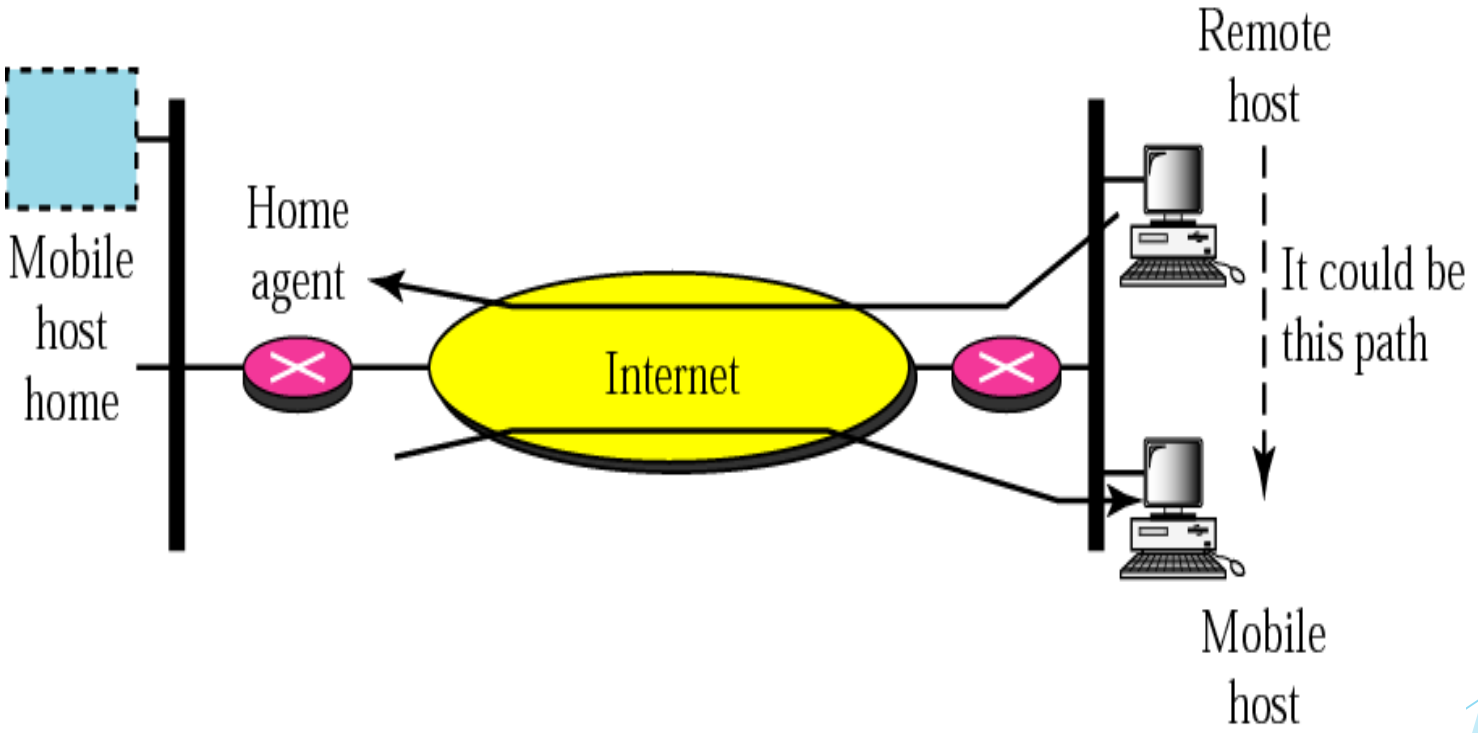
- Communication involving mobile IP can be inefficient
  - *Double crossing*: or *2X*
  - *Triangle routing*: *dog-leg routing*

Double Crossing

- Occurs when a *remote host* communicates with a *mobile host* that has moved to *the same network as the remote host*
- When the mobile host sends a packet to the remote host
  - There is no efficiency; the communication is local
- When the remote host sends a packet to the mobile host
  - The packet crosses the Internet twice

Figure 27-9

Double Crossing

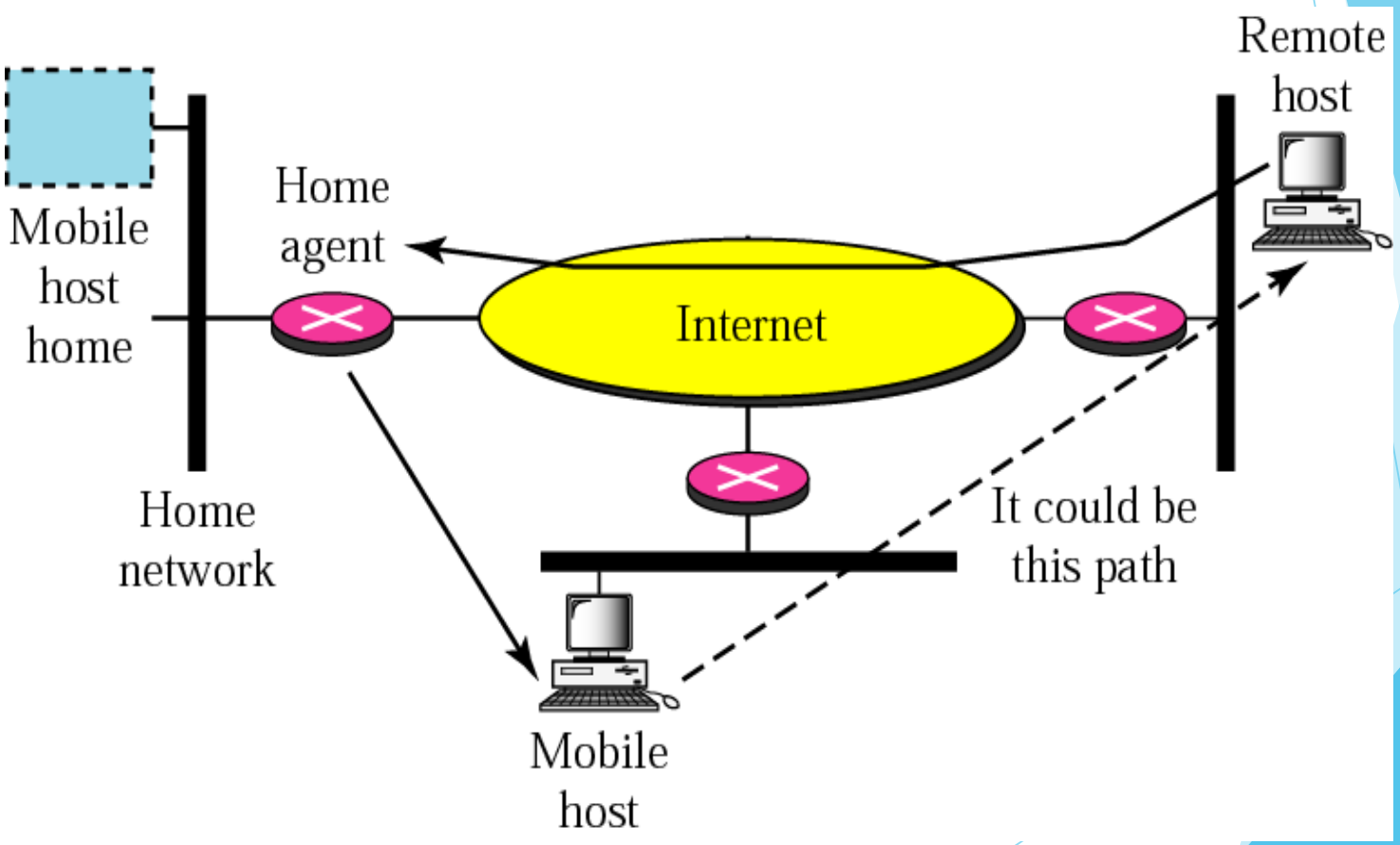


Triangle Routing

- Occurs when the *remote host* communicates with a *mobile host* that is not attached to the same network as the mobile host
- When the mobile host sends a packet to the remote host
  - There is no efficiency
- When the remote host sends a packet to the mobile host
  - The packet goes from the remote host to the home agent and then to the mobile host
  - The packet travels *the two sides of a triangle*

Figure 27-10

Triangle Routing



Solution

- The remote host must know the mobile host's care-of address
  - Send packet using the mobile host's care-of address
  - The home agent can tell the remote host about this information by *the update binding packet*
- However, when the mobile host moves, its care-of address may be changed
  - The home agent needs to send a *warning packet* to the remote host to inform it

virtual private network

- A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.
- Encryption is a common, although not an inherent, part of a VPN connection

Thank you

The Content in this Material are from the Textbooks and Reference books given in the Syllabus