ELECTIVE –II - TCP/IP(18MIT35E)

UNIT-V: Simple Network Management Protocols: (SNMP) – Concept – Management Components – SMI – MIB – SNMP – Messages – UDP Ports – Security. IP over ATM: ATM Wans – Carrying Datagram in cells – Routing the cells – Atmarp – Logical IP Subnet (LIS). Mobile IP: Addressing – Agents – Three Pahses – Agent Discovery – Registration – Data Transfer – Inefficiency in Mobile IP – Virtual Private Networks (VPN).

Text Book :

1.Behrouz A. Forouzan, “TCP/IP Protocol Suite”, Tata Mcgraw-Hill Publishing Company, Second edition.

Reference Books:

1.W. Richard Stevens, “TCP/IP Illustrated: The Protocols”, Vol.1, Pearson Education.

2. Comer , ” Inter networking with TCP/IP : Principles ,protocols & Architecture”,Vol.1,fourth Edition, Pearson Education.

Prepared by

Dr.M.Soranamageswari

5.1 Simple Network Management Protocols

- The **Simple Network Management Protocol (SNMP) is a framework** for managing devices in an internet using the TCP/IP protocol suite.
- It provides a set of fundamental operations for monitoring and maintaining an internet.
- **OBJECTIVES :**
- ❑ To discuss SNMP as a framework for managing devices in an internet using the TCP/IP protocol suite.
- ❑ To define a manager as a host that runs SNMP client and any agents as a router or host that runs a server program.
- ❑ Discuss SMI and MIB, which are used by SNMP.

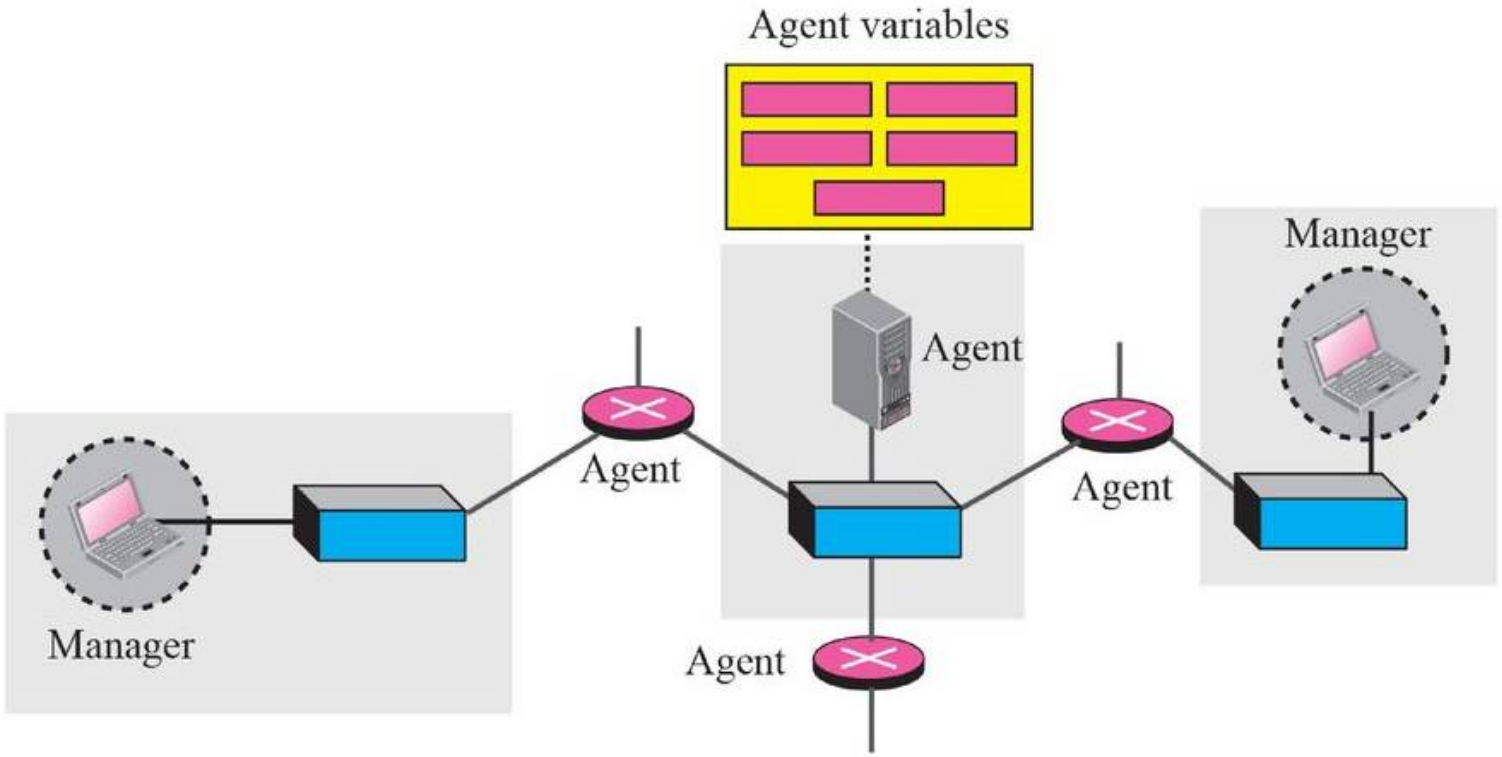
Cont…

- ❑ To show how SMI names objects, defines the type of data, and encodes data.
- ❑ To show how data types are defined using ASN.1.
- ❑ To show how SMI uses BER to encode data.
- ❑ To show the functionality of SNMP using three methods.
- ❑ To discuss the format of SNMP messages.
- ❑ To show how SNMP uses two different ports of UDP.
- ❑ To show how SNMPv3 has enhanced security features over previous versions.

5.2 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 is an application-level protocol in which a few manager stations control a set of agents.
- The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.
- In other words, SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology.
- It can be used in a heterogeneous internet made of different LANs and WANs connected by routers made by different manufacturers.

Figure : *SNMP concept*



Managers and Agents

- A management station, called a **manager, is a host that runs the SNMP client program.**
- A managed station, called an **agent, is a router (or a host) that runs the SNMP server** program.
- Management is achieved through simple interaction between a manager and an agent.
- The agent keeps performance information in a database. The manager has access to the values in the database.

Cont…

- For example, a router can store in appropriate variables
- the number of packets received and forwarded.

- The manager can fetch and compare the values of these two variables to see if the router is congested or not.

- Agents can also contribute to the management process.

- The server program running on the agent can check the environment and, if it notices something unusual, it can send a warning message (called a **trap) to the manager.**

Cont…

- In other words, management with SNMP is based on three basic ideas:

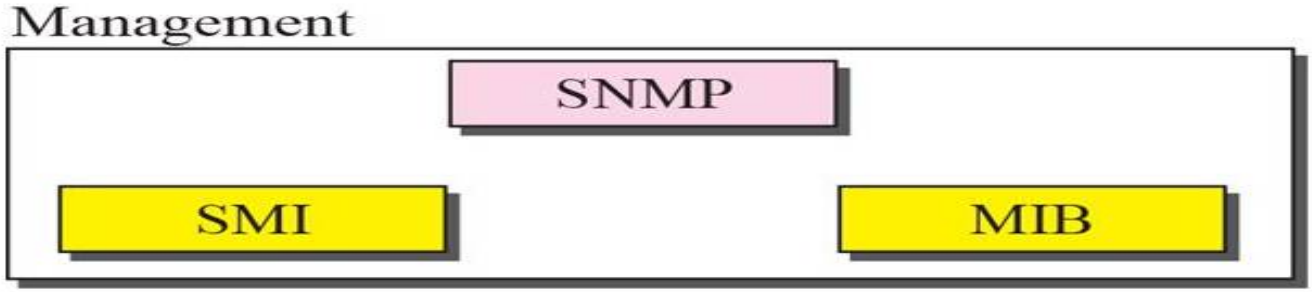
- **1. A manager checks an agent by requesting information that reflects the behavior of the agent.**

- **2. A manager forces an agent to perform a task by resetting values in the agent database.**

- **3. An agent contributes to the management process by warning the manager of an unusual situation.**

5.3 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



Role of SNMP

- SNMP has some very specific roles in network management.
- It defines the format of the packet to be sent from a manager to an agent and vice versa.
- It also interprets the result and creates statistics (often with the help of other management software).
- The packets exchanged contain the object (variable) names and their status (values).
- SNMP is responsible for reading and changing these values.

Role of SMI

- To use SNMP, we need rules. We need rules for naming objects.
- This is particularly important because the objects in SNMP form a hierarchical structure (an object may have a parent object and some child objects).
- Part of a name can be inherited from the parent.
- We also need rules to define the type of the objects.
- We need these universal rules because we do not know the architecture of the computers that send, receive, or store these values.
- The sender may be a powerful computer in which an integer is stored as 8-byte data.

Cont…

- The receiver may be a small computer that stores an integer as 4-byte data.
- SMI is a protocol that defines these rules. However, we must understand that SMI only defines the rules.
- It does not define how many objects are managed in an entity or which object uses which type.
- SMI is a collection of general rules to name objects and to list their types.
- The association of an object with the type is not done by SMI.

Role of MIB

- We hope it is clear that we need another protocol.
- For each entity to be managed, this protocol must define the number of objects, name them according to the rules defined by SMI, and associate a type to each named object.
- This protocol is MIB. MIB creates a set of objects defined for each entity similar to a database (mostly meta data in a database, names and types without values).

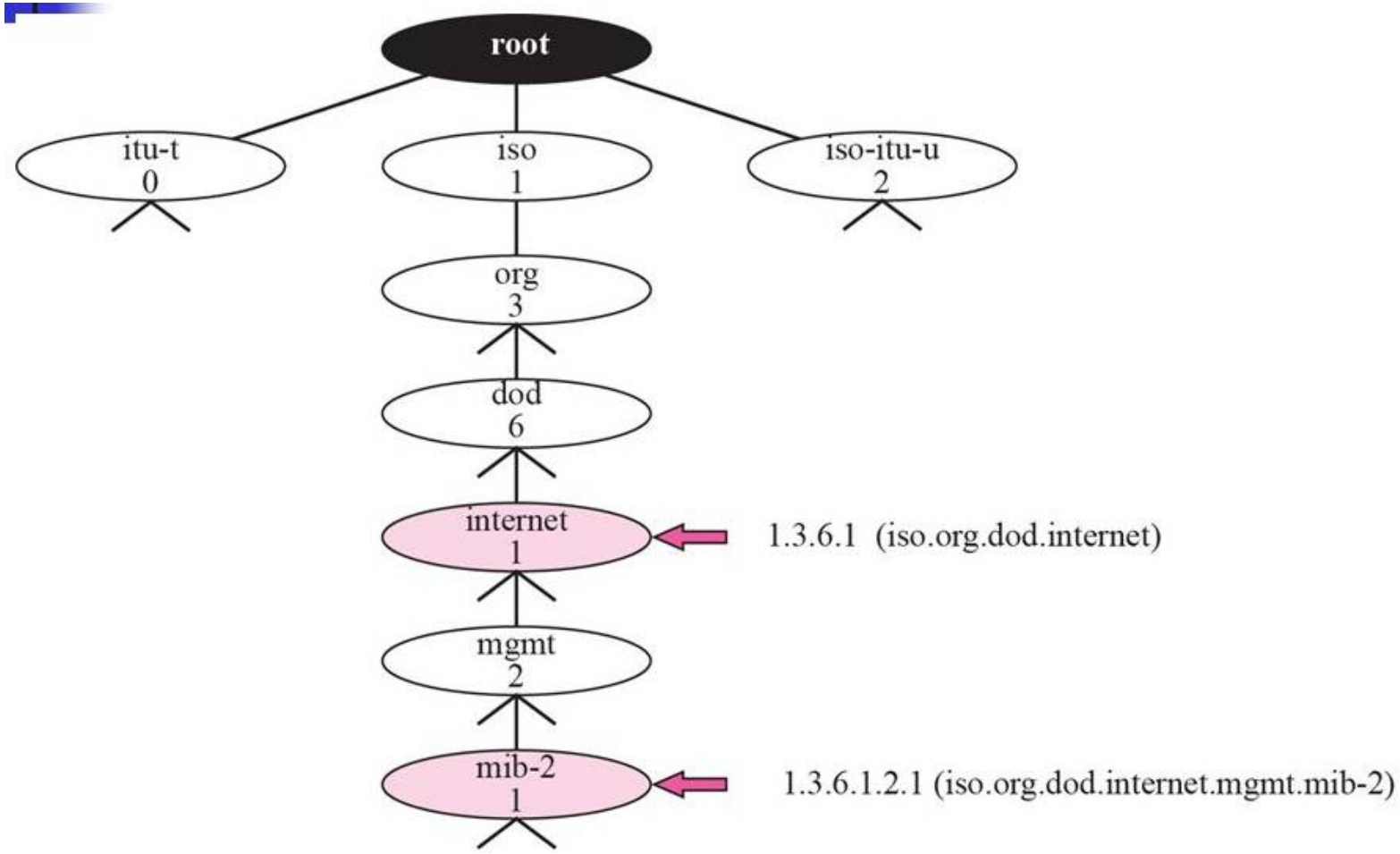
5.4 SMI

- The **Structure of Management Information, version 2 (SMIv2)** 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.

Name

- SMI requires that each managed object (such as a router, a variable in a router, a value, etc.) have a unique name.
- To name objects globally, SMI uses an **object identifier,**
- which is a hierarchical identifier based on a tree structure (see Figure 24.5).
- The tree structure starts with an unnamed root. Each object can be defined using a sequence of integers separated by dots.
- The tree structure can also define an object using a sequence of textual names separated by dots.
- The integer-dot representation is used in SNMP.

Figure :*Object identifier*



Cont…

- The name-dot notation is used by people. For example, the following shows the same object in two different notations:

- **iso.org.dod.internet.mgmt.mib-2 ↔ 1.3.6.1.2.1**

- **Type**

- The second attribute of an object is the type of data stored in it. To define the data type, SMI uses fundamental **Abstract Syntax Notation 1 (ASN.1) definitions and** adds some new definitions.
- In other words, SMI is both a subset and a superset of ASN.1.

Simple Type

- The **simple data types are atomic data types. Some of them are taken directly from** ASN.1; some are added by SMI.
- The most important ones are given in Table 24.1.
- The first five are from ASN.1; the next seven are defined by SMI.

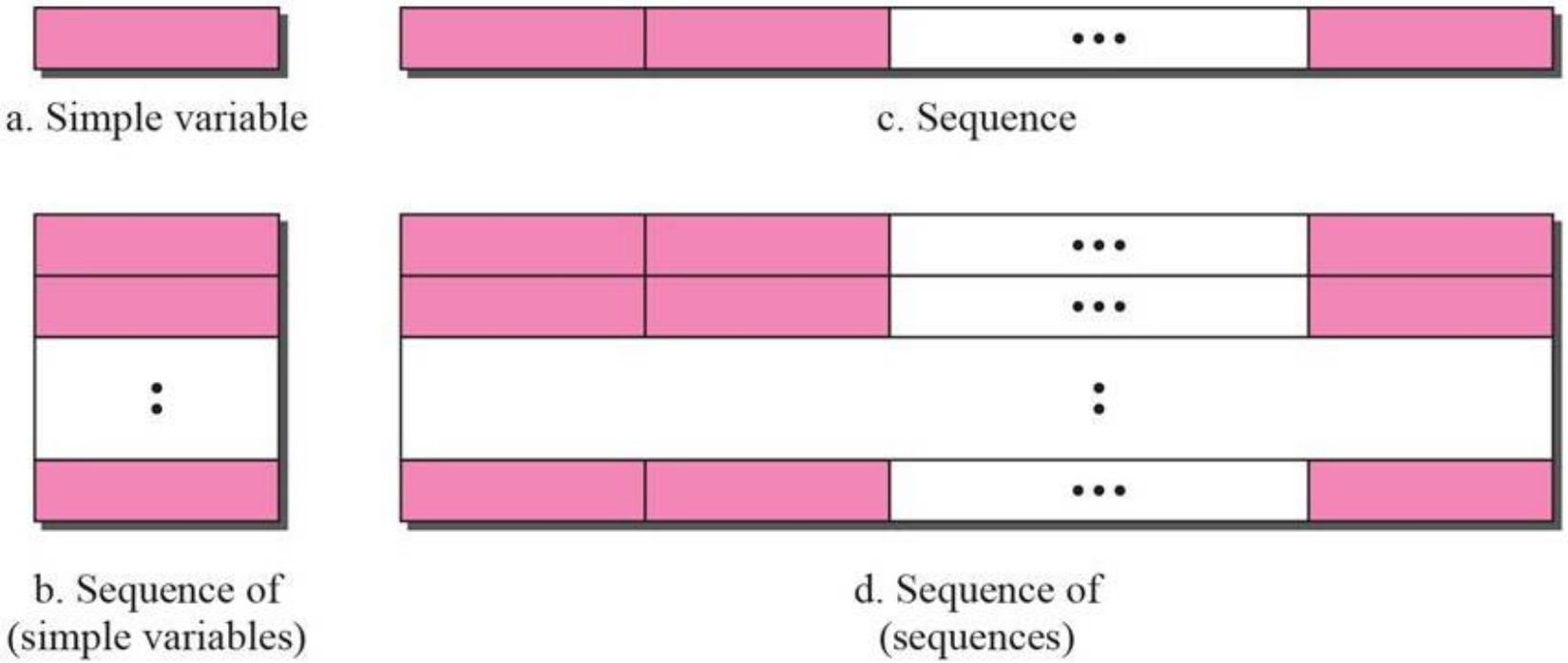
Table 24.1 *Data Types*

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

Structured Type

- **SMI defines two structured data types:**
- ❑ **Sequence.** A sequence data type is a combination of simple data types, not necessarily of the same type. It is analogous to the concept of a struct or a record used in
- programming languages such as C.
- ❑ **Sequence of:** A sequence of data type is a combination of simple data types all of the same type or a combination of sequence data types all of the same type.
- It is analogous to the concept of an *array used in programming languages such* as C.
- Figure 24.6 shows a conceptual view of data types.

Figure : *Conceptual data types*



Encoding Method

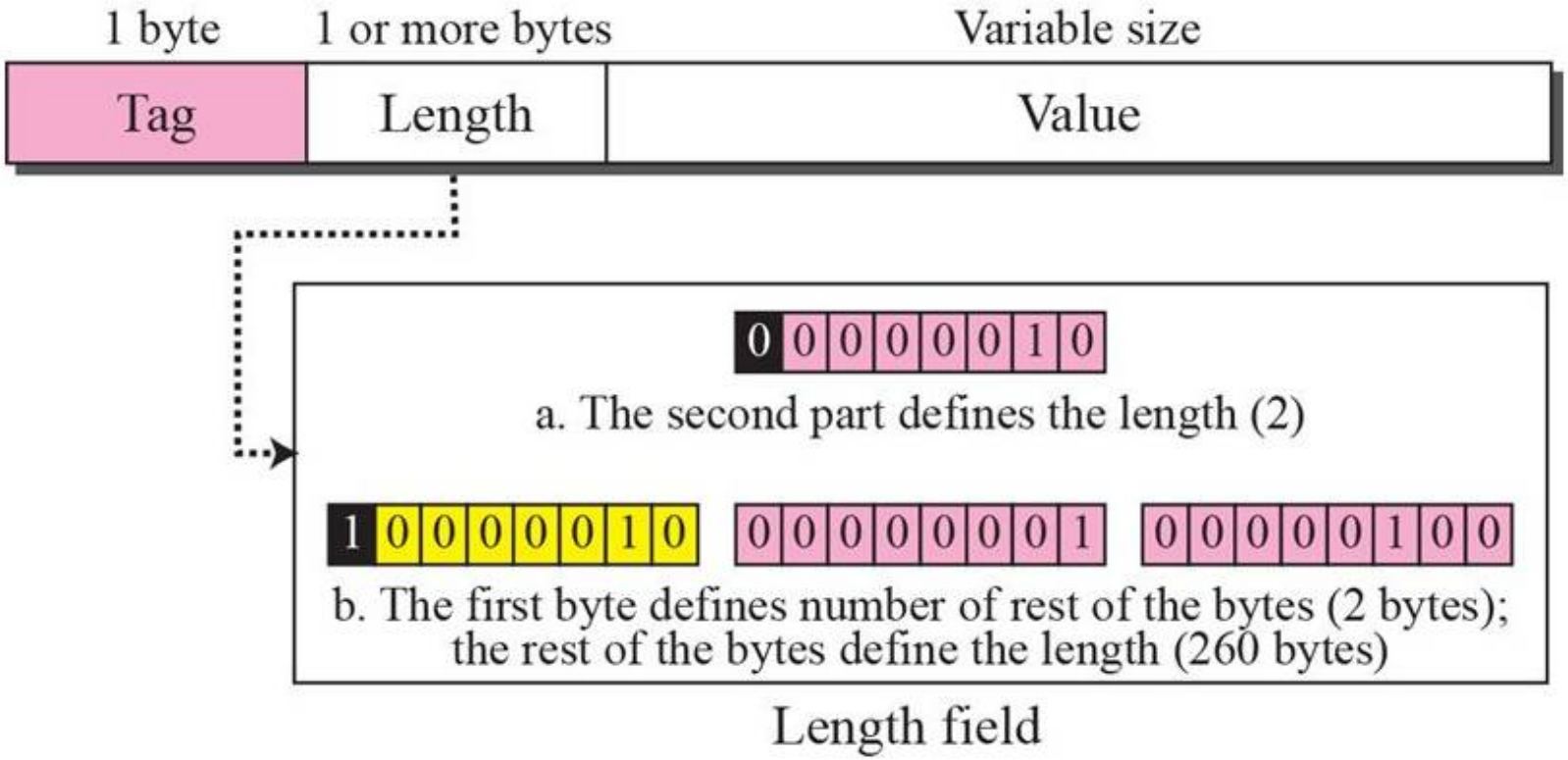
- SMI uses another standard, **Basic Encoding Rules (BER),** to encode data to be transmitted over the network.

- BER specifies that each piece of data be encoded in triplet
- format: tag, length, and value, as illustrated in Figure 24.7.

- The tag is a 1-byte field that defines the type of data. Table 24.2 shows the data types we use in this chapter and their tags in binary and hexadecimal numbers.

- The length field is 1 or more bytes. If it is 1 byte, the most significant bit must be 0.

Figure :*Encoding format*



Cont…

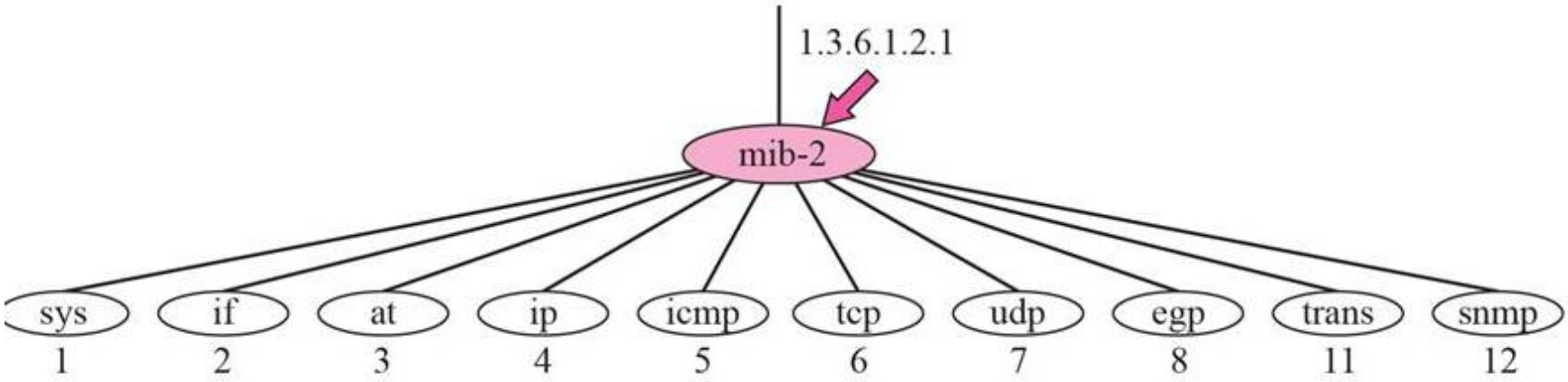
- The other 7 bits define the length of the data. If it is more than 1 byte, the most significant bit of the first byte must be 1.

- The other 7 bits of the first byte define the number of bytes needed to define the length.
- The value field codes the value of the data according to the rules defined in BER.

5.5 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.

Figure : 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

Cont…

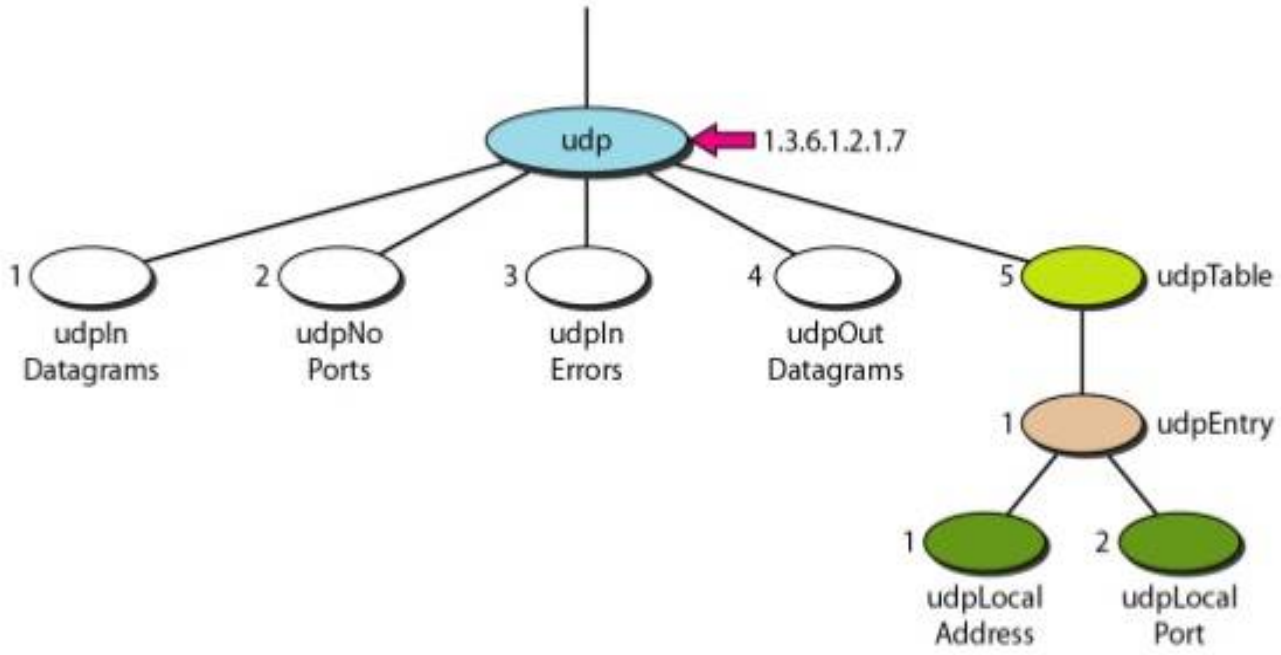
- **The following is a brief description of some of the objects:**

- ❑ **sys :** This object **(system)** defines general information about the node (system), such as the name, location, and lifetime.
- ❑ **if :**This object **(interface)** defines information about all of the interfaces of the node including interface number, physical address, and IP address.
- ❑ **at :**This object **(address translation)** defines the information about the ARP table.
- ❑ **ip :** This object defines information related to IP, such as the routing table and the IP address.

Cont…

- ❑ **icmp :** This object defines information related to ICMP, such as the number of packets sent and received and total errors created.
- ❑ **tcp :** This object defines general information related to TCP, such as the connection table, time-out value, number of ports, and number of packets sent and received.
- ❑ **udp :** This object defines general information related to UDP, such as the number of ports and number of packets sent and received.
- ❑ **snmp :** This object defines general information related to SNMP itself.

Figure :UDP *group*

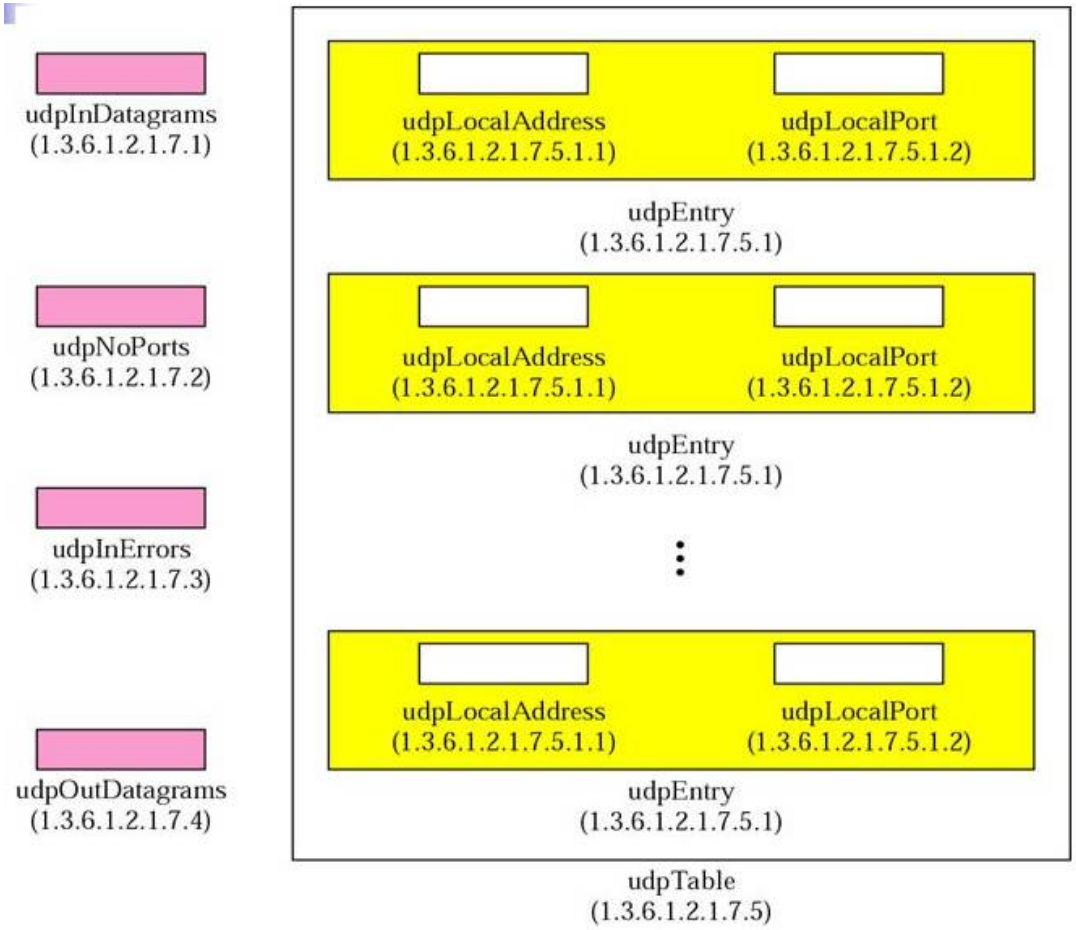


Simple Variables

- To access any of the simple variables, we use the id of the group (1.3.6.1.2.1.7) followed by the id of the variable.
- The following shows how to access each variable.

- **udpInDatagrams → 1.3.6.1.2.1.7.1**
- **udpNoPorts → 1.3.6.1.2.1.7.2**
- **udpInErrors → 1.3.6.1.2.1.7.3**
- **udpOutDatagrams → 1.3.6.1.2.1.7.4**

Figure : *UDP variables and tables*



Cont…

- These two variables are at the leaf of the tree. Although we can access their instances, we need to define which instance.
- At any moment, the table can have several values for each local address/local port pair.
- To access a specific instance (row) of the table, we add the index to the above ids. In MIB, the indexes of arrays are not integers (like most programming languages).
- The indexes are based on the value of one or more fields in the entries. In our example, the udpTable is indexed based on
- both the local address and the local port number.
- For example, Figure 24.15 shows a table with four rows and values for each field.

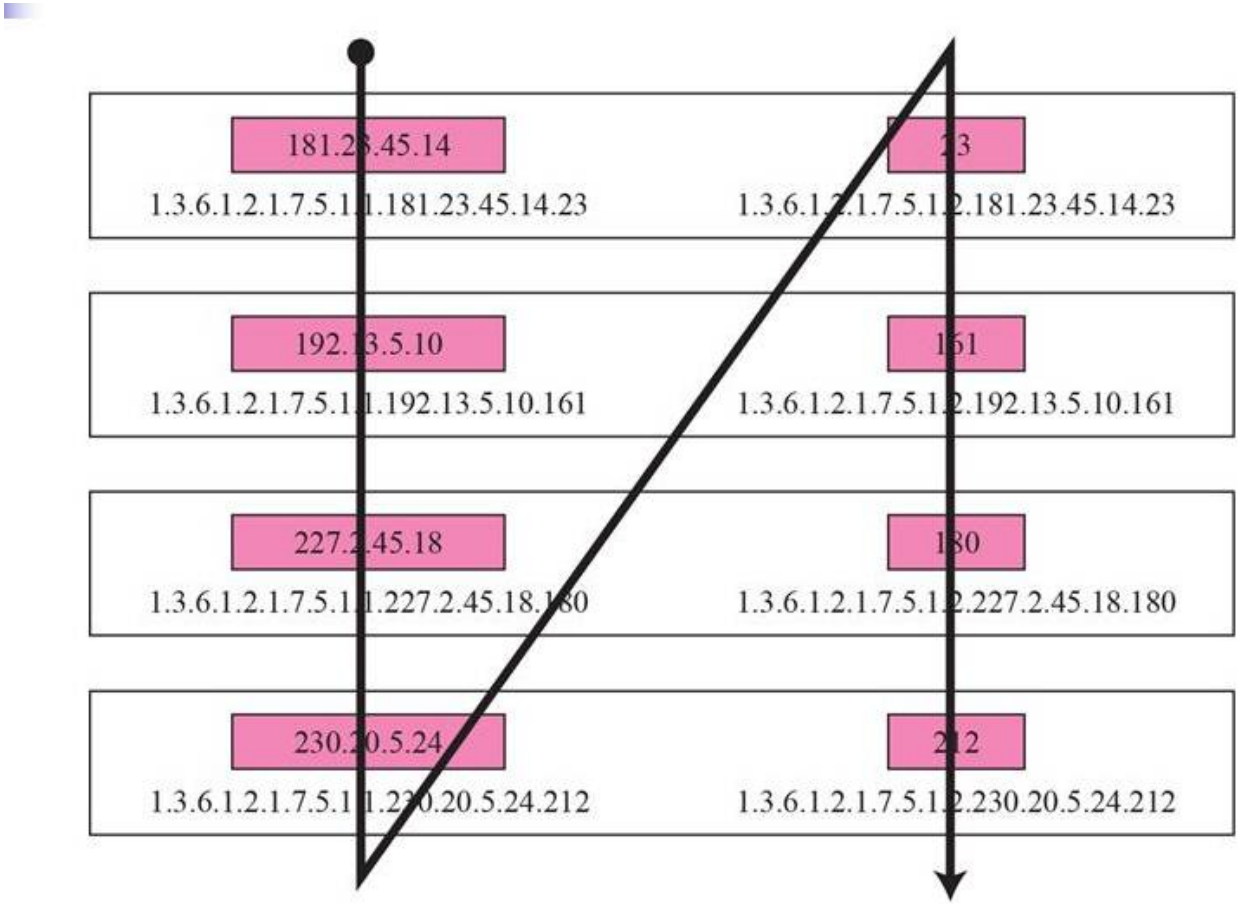
Lexicographic Ordering

- One interesting point about the MIB variables is that the object identifiers (including the instance identifiers) follow in lexicographic order.

- Tables are ordered according to column-row rules, which means one should go column by column.

- In each column, one should go from the top to the bottom, as shown in Figure 24.16.

Figure : *Lexicographic ordering*



5.6 SNMP

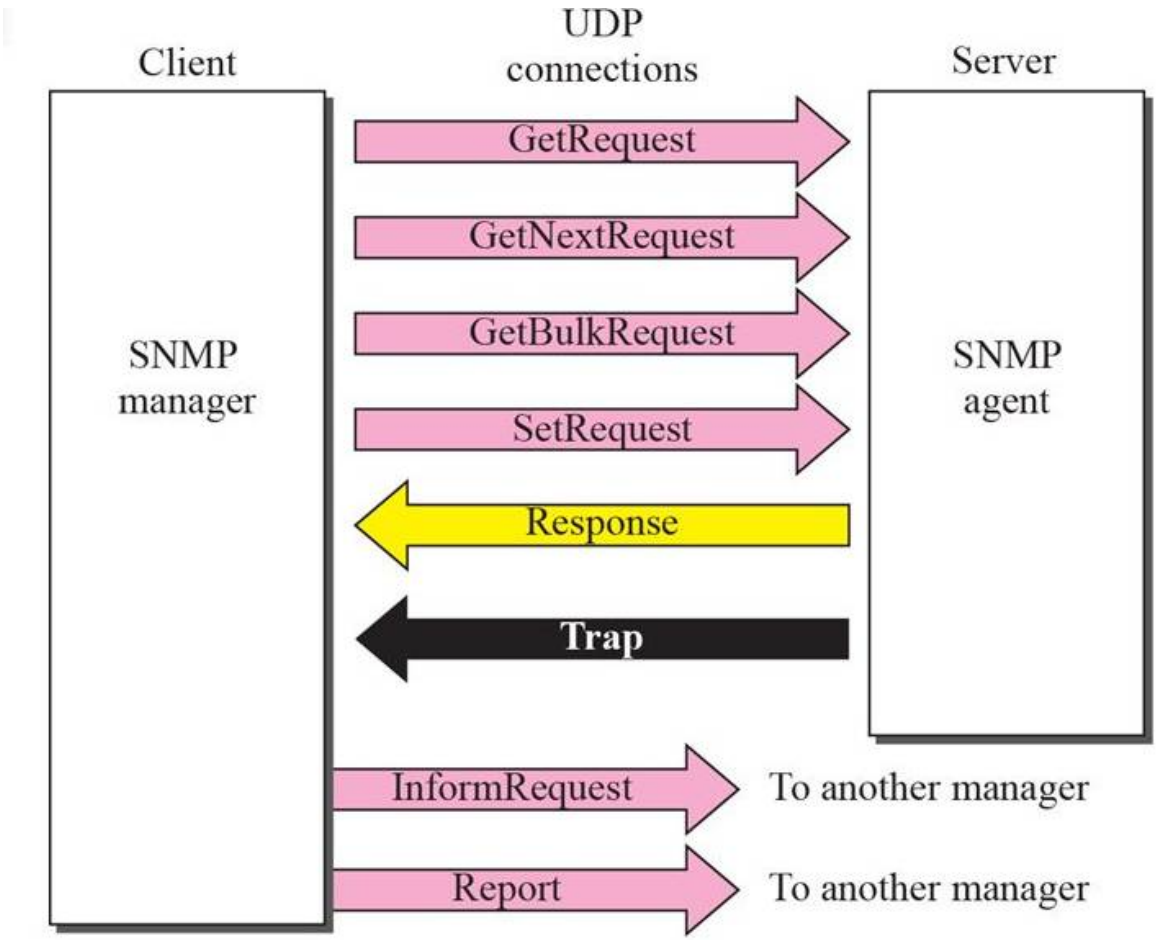
- SNMP uses both SMI and MIB in Internet network management.

- 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.**

Cont…

- **PDUs**
- SNMPv3 defines eight types of protocol data units (or PDUs): GetRequest, GetNext- Request, GetBulkRequest, SetRequest, Response, Trap, InformRequest, and Report (see Figure 24.17).
- ***GetRequest***
- The GetRequest PDU is sent from the manager (client) to the agent (server) to retrieve the value of a variable or a set of variables.
- ***GetNextRequest***
- The GetNextRequest PDU is sent from the manager to the agent to retrieve the value of a variable. The retrieved value is the value of the object following the defined ObjectId in the PDU.

Figure : SNMP PDUs



Cont…

- ***GetBulkRequest***
- The GetBulkRequest PDU is sent from the manager to the agent to retrieve a large amount of data. It can be used instead of multiple GetRequest and GetNextRequest PDUs.
- ***SetRequest***
- The SetRequest PDU is sent from the manager to the agent to set (store) a value in a variable.
- ***Response***
- The Response PDU is sent from an agent to a manager in response to GetRequest or GetNextRequest. It contains the value(s) of the variable(s) requested by the manager.

Cont…

- **Trap**
- The Trap (also called SNMPv2 Trap to distinguish it from SNMPv1 Trap) PDU is sent from the agent to the manager to report an event.
- **InformRequest**
- The InformRequest PDU is sent from one manager to another remote manager to get the value of some variables from agents under the control of the remote manager. The remote manager responds with a Response PDU.
- **Report**
- The Report PDU is designed to report some types of errors between managers. It is not yet in use.

Format

- The format for the eight SNMP PDUs is shown in Figure 24.18.
- The GetBulkRequest PDU differs from the others in two areas as shown in the figure.

- The fields are listed below:

- ❑ **PDU type.** This field defines the type of the PDU (see Table 24.3) .
- ❑ **Request ID.** This field is a sequence number used by the manager in a request PDU and repeated by the agent in a response. It is used to match a request to a response.

Table : *Types of Errors*

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

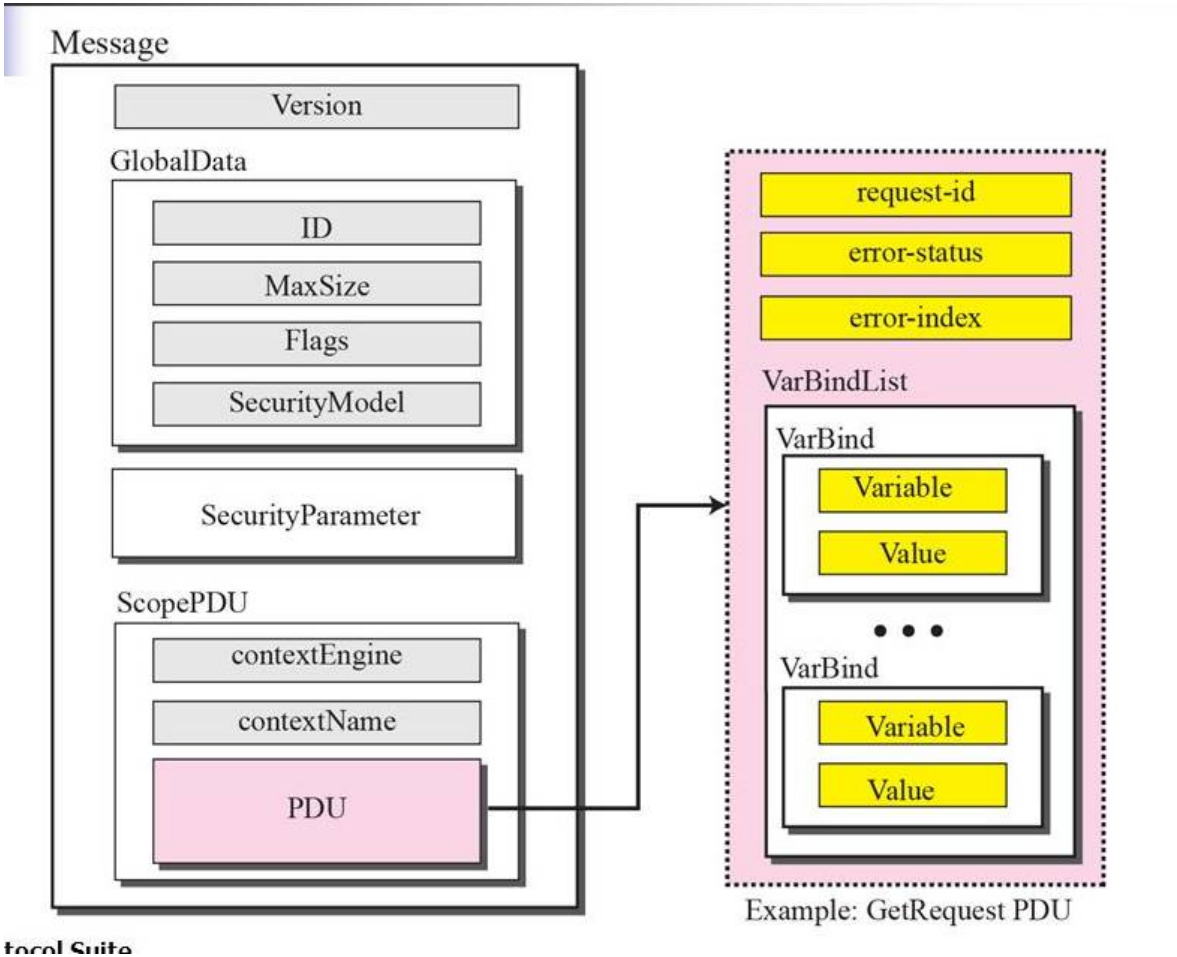
Cont…

- ❑ **Max-repetition.** This field is also used only in GetBulkRequest and replaces the error index field, which is empty in request PDUs.
- ❑ **VarBind list.** This is a set of variables with the corresponding values the manager wants to retrieve or set. The values are null in GetRequest and GetNextRequest.
- In a Trap PDU, it shows the variables and values related to a specific PDU.

5.7 Messages

- SNMP does not send only a PDU, it embeds the PDU in a message.
- A message in SNMPv3 is a sequence made of four elements: Version, GlobalData, SecurityParameters, and ScopePDU (which includes the encoded PDU) as shown in Figure 24.19.
- The first and the third elements are simple data types; the second and the fourth are sequences.

Figure :*SNMP message*



Cont…

- **Version**
- The Version field is an INTEGER data type that defines the version. The current version is 3.
- **GlobalData**
- The GlobalData field is a sequence with four elements of simple data type: ID, Max- Size, Flags, and SecurityModel.
- **Security Parameter**
- This element is a sequence that can be very complex, depending on the type of security provision used in version 3.
- **ScopePDU**
- The last element contains two simple data type and the actual PDU. We have shown only one example of GetRequest PDU.

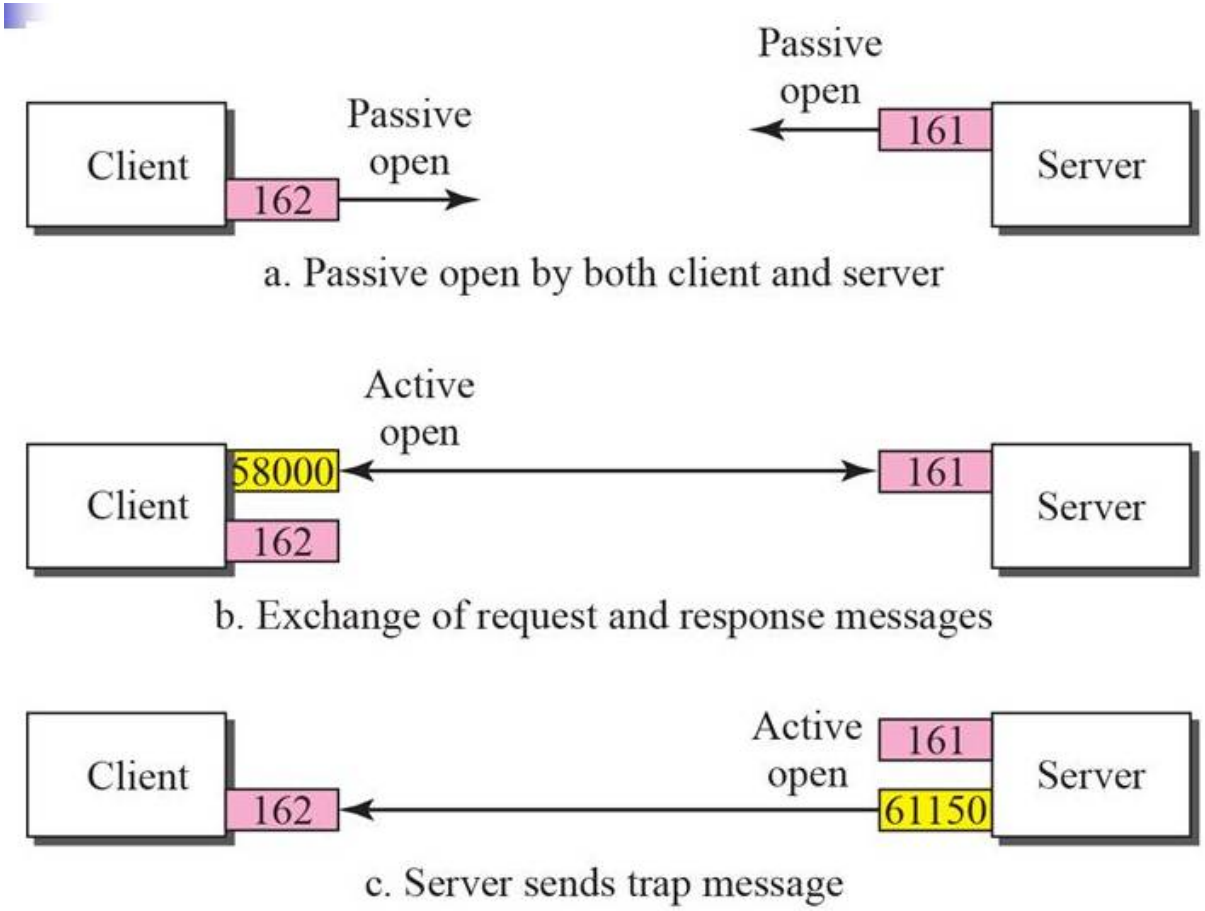
5.8 UDP PORTS

- SNMP uses the services of UDP on two well-known ports, 161 and 162.
- The wellknown port 161 is used by the server (agent), and the well-known port 162 is used by the client (manager).
- The agent (server) issues a passive open on port 161. It then waits for a connection from a manager (client).
- A manager (client) issues an active open using an ephemeral port.
- The request messages are sent from the client to the server using the ephemeral port as the source port and the well-known port 161 as the destination port.

Cont…

- The response messages are sent from the server to the client using the well-known port 161 as the source port and the ephemeral port as the destination port.
- The manager (client) issues a passive open on port 162.
- It then waits for a connection from an agent (server).
- Whenever it has a Trap message to send, an agent (server) issues an active open, using an ephemeral port.
- This connection is only one-way, from the server to the client (see Figure 24.22).

Figure : *Port numbers for SNMP*



Cont…

- The client-server mechanism in SNMP is different from other protocols.
- Here both the client and the server use well-known ports.
- In addition, both thserver are running infinitely.
- The reason is that request messages are initiated by a manager (client), but Trap messages are initiated by an agent (server).

5.9 SECURITY

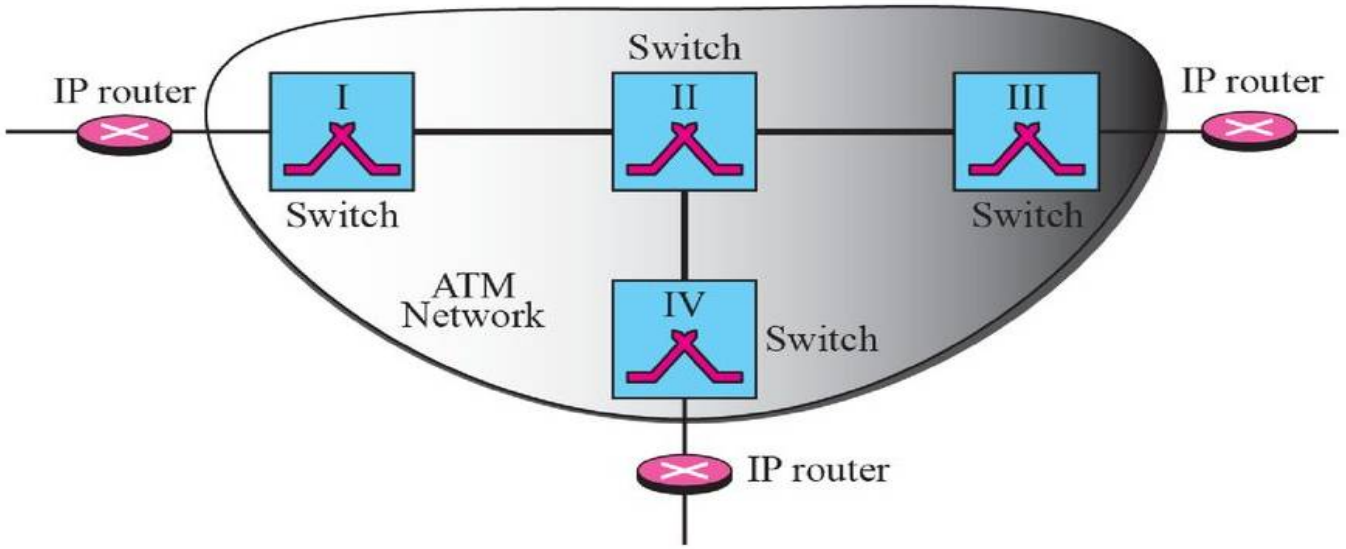
- SNMPv3 has added two new features to the previous version:
- security and remote administration.
- SNMPv3 allows a manager to choose one or more levels of security.
- when accessing an agent. Different aspects of security can be configured by the manager to allow message authentication, confidentiality,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

5.10 IP over ATM

- In the previous sections, we assumed that the underlying networks over which the IP datagrams are moving are either LANs or point-to-point WANs.
- In this section, we want to see how an IP datagram is moving through a switched WAN such as an ATM.
- We will see that there are similarities as well as differences.
- The IP packet is encapsulated in cells (not just one).
- An ATM network has its own definition for the physical address of a device.
- Binding between an IP address and a physical address is attained through a protocol called ATMARP

5.11 ATM WANs

- ATM, a cell-switched network, can be a highway for an IP datagram.
- Figure shows how an ATM network can be used in the Internet.



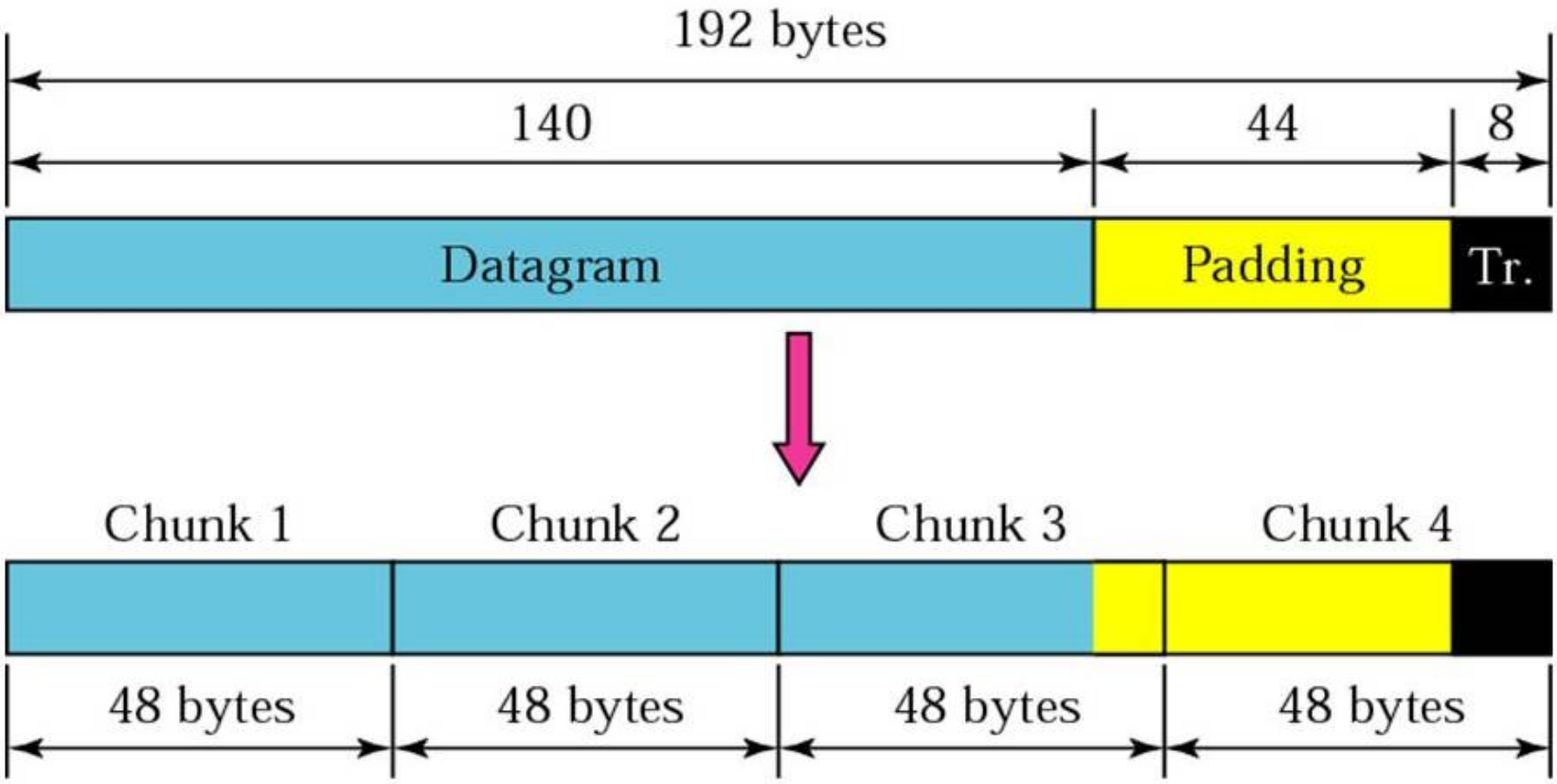
AAL Layer

- The only AAL used by the Internet is AAL5. It is sometimes called the **simple and efficient adaptation layer (SEAL).**
- AAL5 assumes that all cells created from one IP datagram belong to a single message.
- AAL5 therefore provides no addressing, sequencing, or other header information.
- Instead, only padding and a four-field trailer are added to the IP packet.
- AAL5 accepts an IP packet of no more than 65,536 bytes and adds an 8-byte trailer as well as any padding required to ensure that the position of the trailer falls.
- Where the receiving equipment expects it (at the last 8 bytes of the last cell).
- Once the padding and trailer are in place, AAL5 passes the message in 48-byte segments to the ATM layer.

5.12 Carrying Datagram in cells

- As an example, let us show how a datagram of 140 bytes is encapsulated in four cells and transmitted through an ATM network.
- Before encapsulation an 8 byte trailer is added to the datagram.
- However, the size of the packet is now 148.
- Which is not divisible by 48.
- We must add 44 bytes of pudding, which makes the total length 192 bytes .
- The packet is then divided into four chunks of 48 bytes each as shown in figure 23.6

Figure : Fragmentation



Cont…

- At the ATM layer, each chunk of data is encapsulated into a cell as shown in figure .
- Note that the last cell carries no data .
- Also note that the value of the PT field in the last cell is 001 to show that this is the last cell

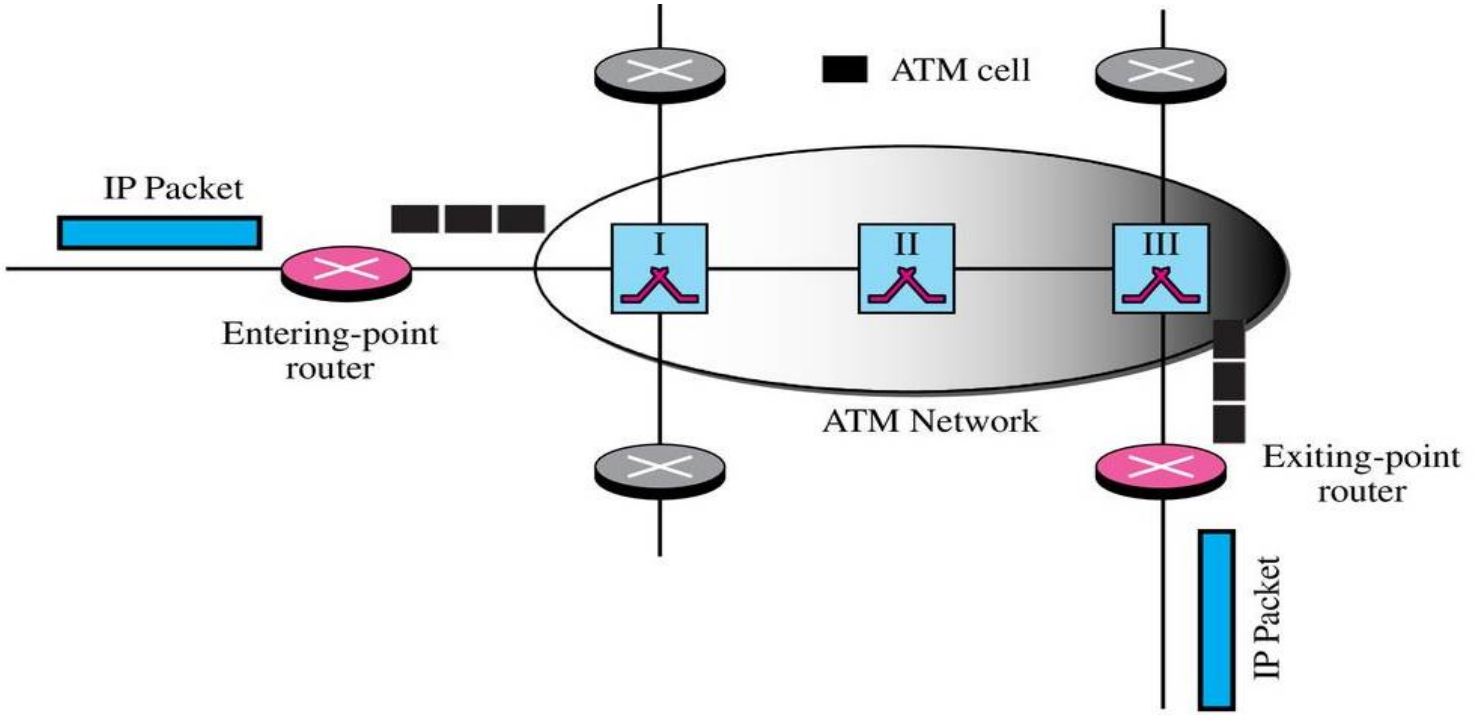
5.13 Routing the Cells

- The ATM network creates a route between two routers.
- We call these routers entering point and exiting-point routers.
- The cells start from the entering-point router and end at the exiting-point router as shown in Figure 7.27.

- **Addresses**

- Routing the cells from one specific entering-point router to one specific exiting-point router requires three types of addressing.
- IP addresses, physical addresses, and virtual circuit identifiers.

Figure : Entering-point and exiting-point routers



Cont…

- IP Addresses Each router connected to the ATM network has an IP address.
- Later we will see that the addresses may or may not have the same prefix.
- The IP address defines the router at the IP layer.
- It does not have anything to do with the ATM network.
- Physical Addresses Each router (or any other device) connected to the ATM network has also a physical address.
- The physical address is associated with the ATM network and does not have anything to do with the Internet.

Cont…

- The ATM Forum defines 20-byte addresses for ATM networks.
- Each address must be unique in a network and is defined by the network administrator.
- The physical addresses in an ATM network play the same role as the MAC addresses in a LAN.
- The physical addresses are used during connection establishment.

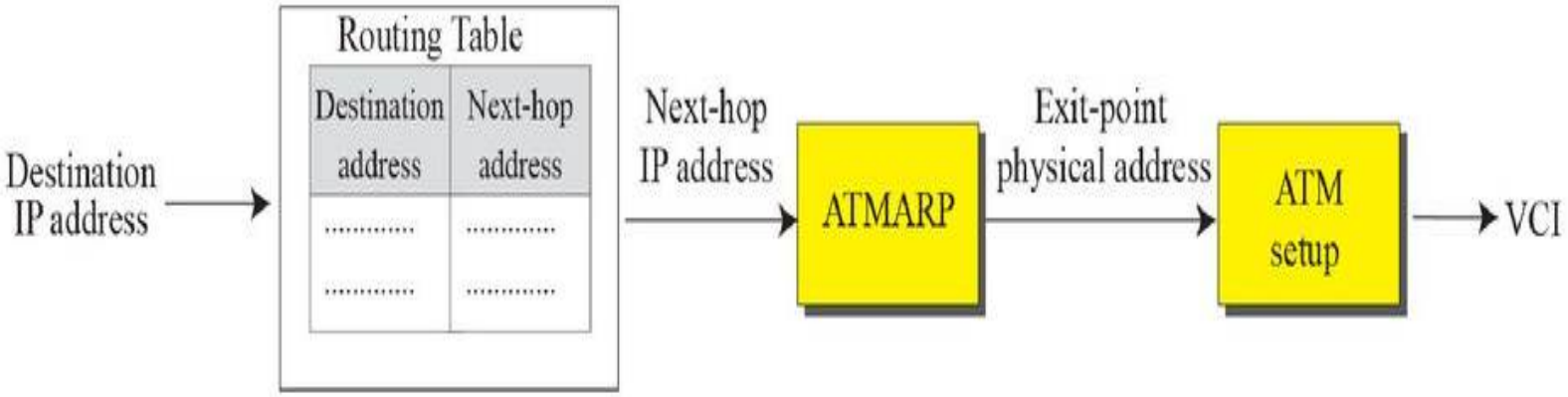
Cont…

- Virtual Circuit Identifiers The switches inside the ATM network route the cells based on the virtual circuit identifiers (VPIs and VCIs).
- The virtual circuit identifiers are used during data transfer.

Address Binding

- An ATM network needs virtual circuit identifiers to route the cells.
- The IP datagram contains only source and destination IP addresses. Virtual circuit identifiers must be determined from the destination IP address.
- Figure shows how this is done.

Figure : *Address binding in IP over ATM*



Cont…

- These are the steps:

- 1. The entering-point router receives an IP datagram. It uses the destination address and its routing table to find the IP address of the next router, the exiting-point router.
- 2. The entering-point router uses the services of a protocol called ATMARP to find the physical address of the exiting-point router.
- 3. The virtual circuit identifiers are bound to the physical addresses .

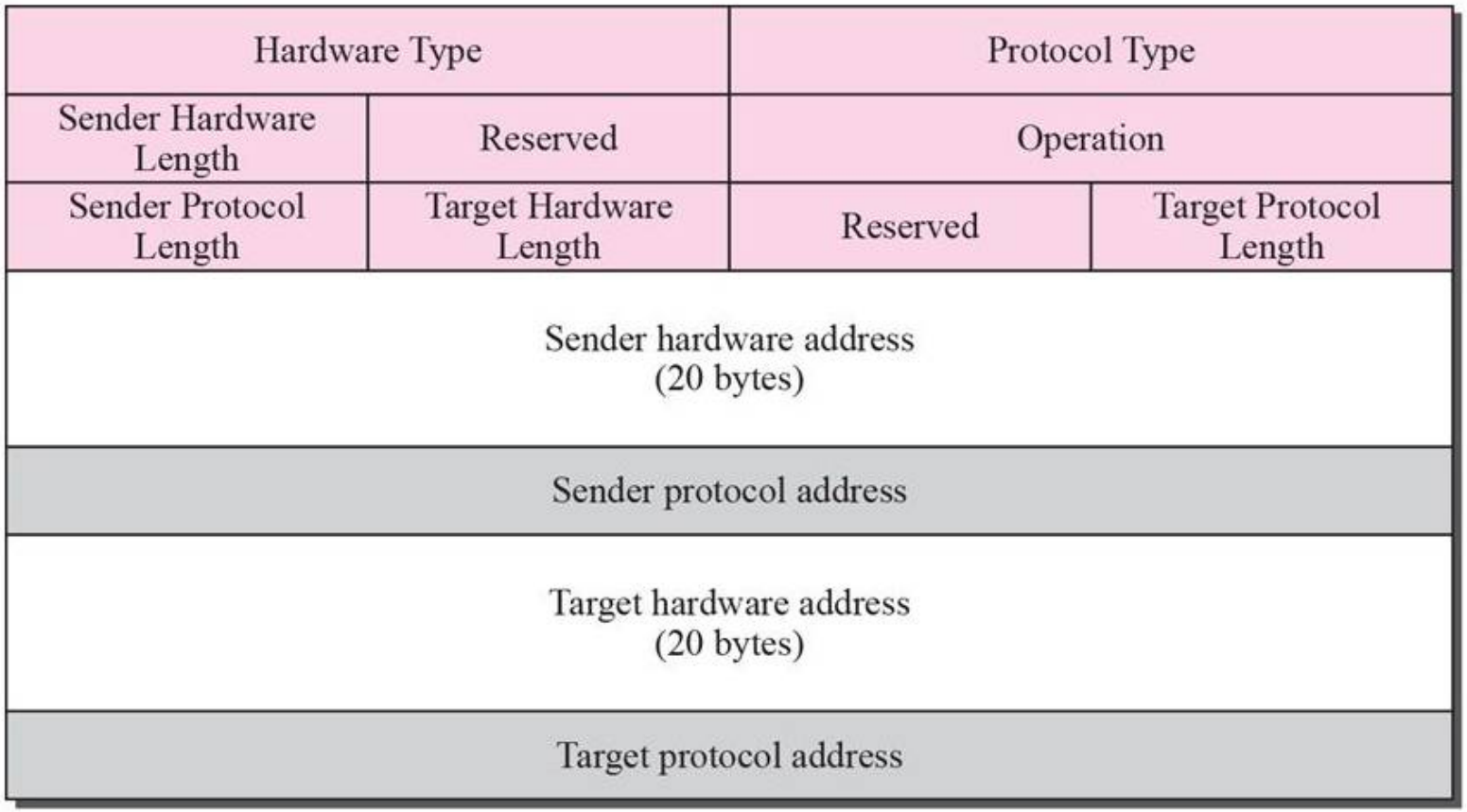
5.14 ATMARP

- When IP packet are moving through an ATM WAN, a mechanism protocol is needed to find (map) the physical address of the exiting-point router in the ATM WAN given the IP address of the router.
- This is the same task performed by ARP on a LAN.
- However, there is a difference between a LAN and an ATM network.
- A LAN is a broadcast network (at the data link layer); ARP uses the broadcasting capability of a LAN to send (broadcast) an ARP request.
- An ATM network is not a broadcast network; another solution is needed to handle the task.

Packet Format

- The format of an **ATMARP packet, which is similar to the ARP packet, is shown in** Figure 8.8.
- The fields are as follows:
- ❑ **Hardware type (HTYPE).** The 16-bit HTYPE field defines the type of the physical network. Its value is 001316 for an ATM network.
- ❑ **Protocol type (PTYPE).** The 16-bit PTYPE field defines the type of the protocol. For IPv4 protocol the value is 080016.
- ❑ **Sender hardware length (SHLEN).** The 8-bit SHLEN field defines the length of the sender's physical address in bytes. For an ATM network the value is 20. Note

Figure :*ATMARP packet*



Cont…

- ❑ **Operation (OPER).** The 16-bit OPER field defines the type of the packet. Five packet types are defined as shown in Table 8.1.
- ❑ **Sender protocol length (SPLEN).** The 8-bit SPLEN field defines the length of the address in bytes. For IPv4 the value is 4 bytes.
- ❑ **Target hardware length (TLEN).** The 8-bit TLEN field defines the length of the receiver's physical address in bytes. For an ATM network the value is 20.
- ❑ **Target protocol length (TPLEN).** The 8-bit TPLEN field defines the length of the address in bytes. For IPv4 the value is 4 bytes.

Table :*OPER field*

Table 8.1 *OPER field*

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

ATMARP Operation

ATMARP Operation

- There are two methods to connect two routers on an ATM network. through a permanent virtual circuit (PVC) or through a switched virtual circuit (SVC).
- The operation of ATMARP depends on the connection method.

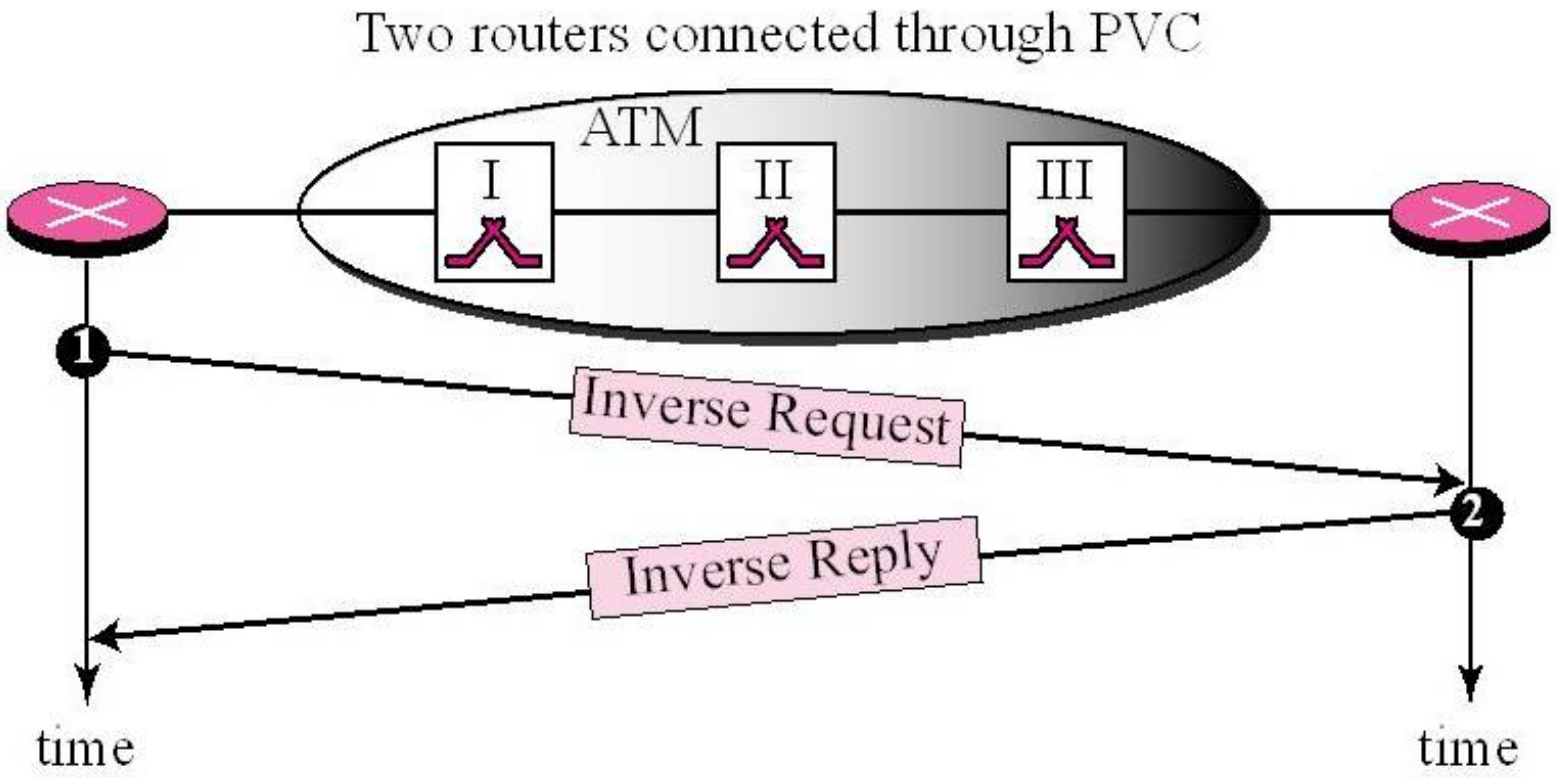
PVC Connection

- A permanent virtual circuit (PVC) connection is established between two end points by the network provider.
- The VPIs and VCIs are defined for the permanent connections and the values are entered in a table for each switch.

Cont…

- If a permanent virtual circuit is established between two routers, there is no need for an ATMARP server.
- However, the routers must be able to bind a physical address to an IP address.
- The **inverse request message and inverse reply message can be used** for the binding.
- When a PVC is established for a router, the router sends an inverse request message.
- The router at the other end of the connection receives the message (which contains the physical and IP address of the sender) and sends back an inverse reply message (which contains its own physical and IP address).

Figure : *Binding with PVC*



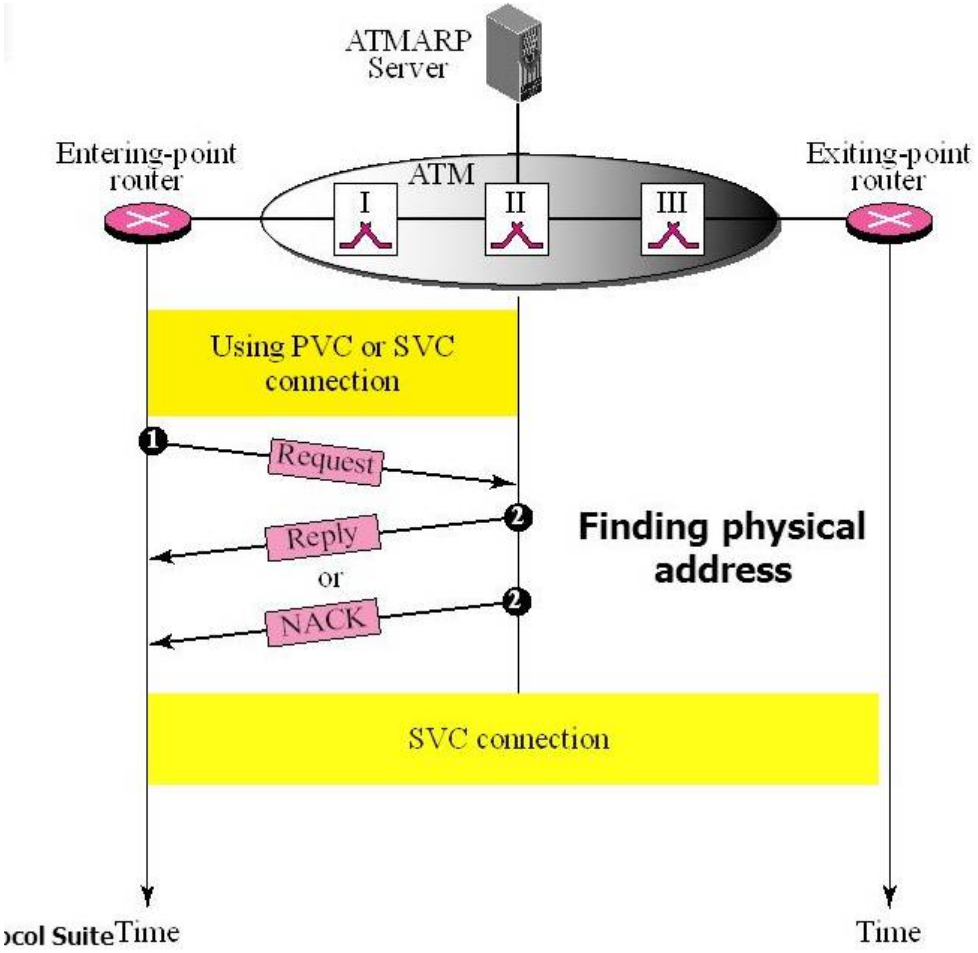
SVC Connection

- In a switched virtual circuit (SVC) connection, each time a router wants to make a connection with another router (or any computer), a new virtual circuit must be established.
- However, the virtual circuit can be created only if the entering-point router knows the physical address of the exiting-point router (ATM does not recognize IP addresses).
- To map the IP addresses to physical addresses, each router runs a client ATMARP program, but only one computer runs an ATMARP server program.
- To understand the difference between ARP and ATMARP, remember that ARP operates on a LAN.

Cont…

- which is a broadcast network.
- An ARP client can broadcast an ARP request message and each router on the network will receive it, only the target router will respond.
- ATM is a nonbroadcast network, an ATMARP request cannot reach all routers connected to the network.
- **The process of establishing a virtual connection requires three steps:**
- **connecting to the server,**
- **receiving the physical address, and**
- **establishing the connection.**
- Figure 8.10 shows the steps.

Figure : *Binding with ATMARP*



5.15 Logical IP Subnet (LIS)

- Before we leave the subject of IP over ATM, we need to discuss a concept called **logical IP subnet (LIS).**
- For the same reason that a large LAN can be divided into several subnets, 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.

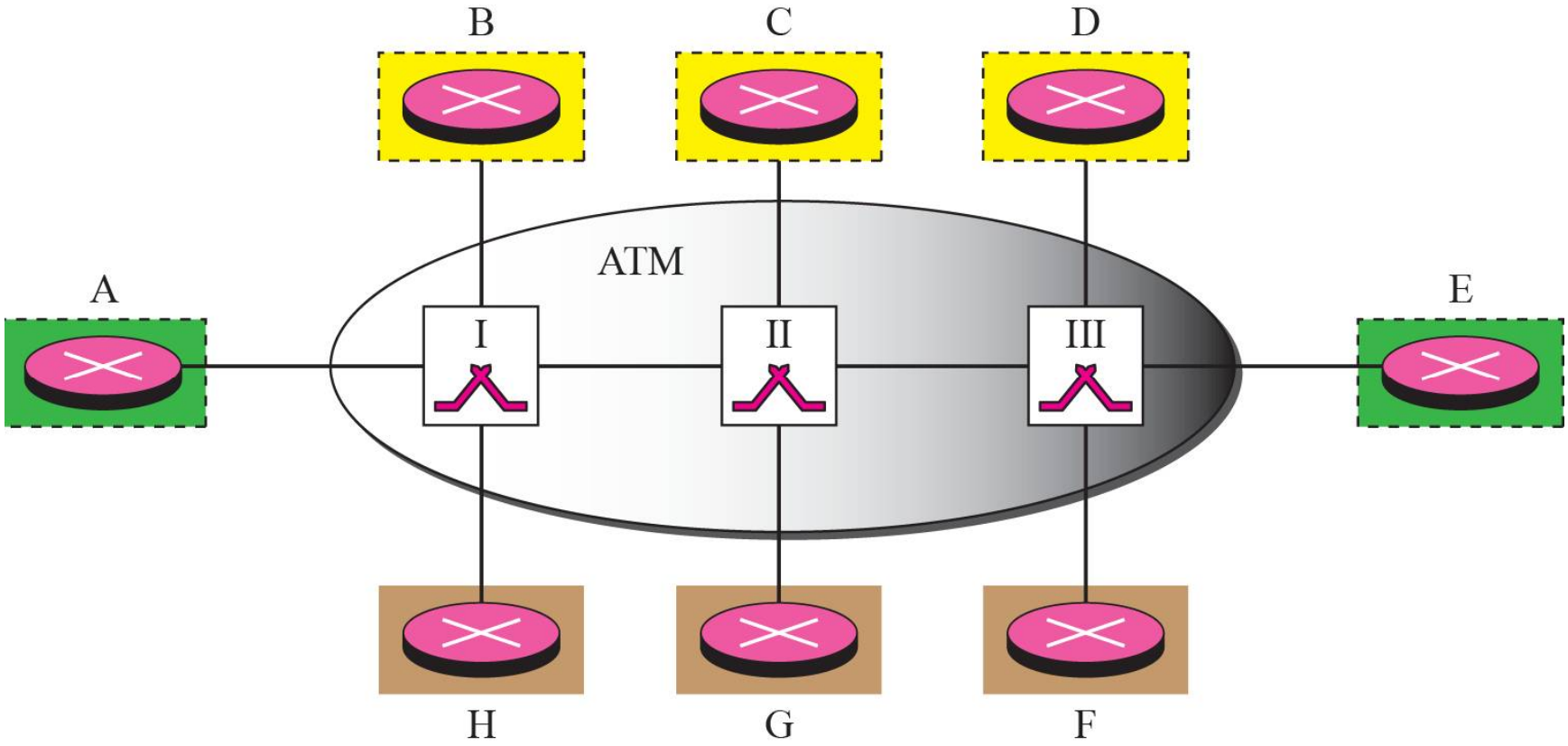
Cont…

- Routers connected to an ATM network can belong to one or more logical subnets, as shown in Figure 8.12. In the figure, routers B, C, and D belong to one logical subnet (shown by broken-line boxes); routers F, G, and H belong to another logical subnet (shown by shaded boxes).
- Routers A and E belong to both logical subnets.
- A router can communicate and send IP packets directly to a router in the same subnet.
- However, if it needs to send a packet to a router that belongs to another subnet, the packet must first go to a router that belongs to both subnets.

Cont…

- For example, router B can send a packet directly to routers C and D. But a packet from B to F must first pass through A or E.
- Note that routers belonging to the same logical subnet share the same prefix and subnet mask.
- The prefix for routers in different subnets is different.
- To use ATMARP, there must be a different ATMARP server in each subnet.
- For example, in the above figure, we need two ATMARP servers, one for each subnet.

Figure :*LIS*



5.16 Addressing

- The main problem that must be solved in providing mobile communication using the IP protocol is addressing.
- **A) Stationary Hosts**
- The original IP addressing was based on the assumption that a host is stationary, attached to one specific network.
- A router uses an IP address to route an IP datagram.
- An IP address has two parts: a prefix and a suffix.
- The prefix associates a host to a network.
- For example, the IP address 10.3.4.24/8 defines a host attached to the network 10.0.0.0/8.

Cont…

- This implies that a host in the Internet does not have an address that it can carry with itself from one place to another.
- The address is valid only when the host is attached to the network.
- If the network changes, the address is no longer valid.
- Routers use this association to route a packet; they use the prefix to deliver the packet to the network to which the host is attached.
- This scheme works perfectly with **stationary hosts.**

Cont…

- **B) Mobile Hosts**
- When a host moves from one network to another, the IP addressing structure needs to be modified.
- Several solutions have been proposed.
- ***Changing the Address***
- One simple solution is to let the mobile host change its address as it goes to the new network.
- The host can use DHCP (see Chapter 18) to obtain a new address to associate it with the new network. This approach has several drawbacks.
- First, the configuration files would need to be changed.
- Second, each time the computer moves from one network to another.

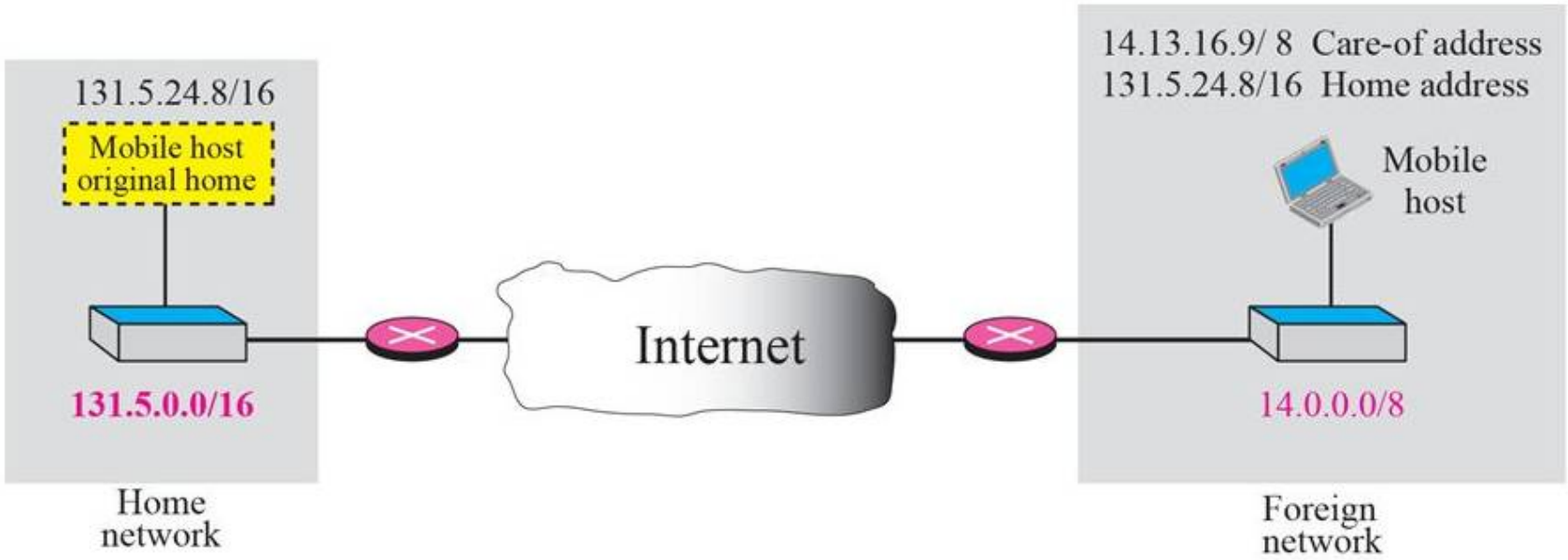
Cont…

Two Addresses

- The approach that is more feasible is the use of two addresses.
- **The host has its original address, called the home address, and a temporary address, called the care-of address.**

- The home address is permanent; it associates the host to its home network, the network that is the permanent home of the host.
- The care-of address is temporary.
- When a host moves from one network to another, the care-of address changes; it is associated with the foreign network, the network to which the host moves.
- Figure 10.1 shows the concept.

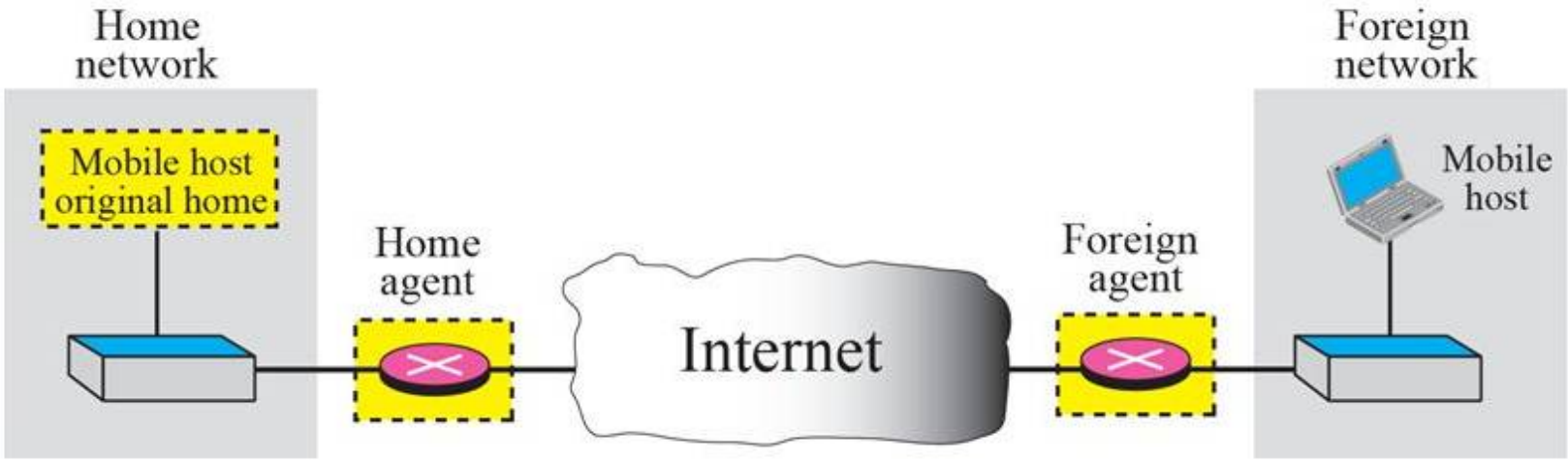
Figure : *Home address and care-of address*



5.17 Agents

- To make the change of address transparent to the rest of the Internet requires a home agent and a foreign agent.
- Figure 10.2 shows the position of a home agent relative to the home network and a foreign agent relative to the foreign network.
- **A) Home Agent**
- The home agent is usually a router attached to the home network of the mobile host.
- The home agent acts on behalf of the mobile host when a remote host sends a packet to the mobile host.
- The home agent receives the packet and sends it to the foreign agent.

Figure : *Home agent and foreign agent*



Cont…

- **B) Foreign Agent**
- The foreign agent is usually a router attached to the foreign network.
- The foreign agent receives and delivers packets sent by the home agent to the mobile host.
- The mobile host can also act as a foreign agent. In other words, the mobile host and the foreign agent can be the same.
- However, to do this, a mobile host must be able to receive a care-of address by itself, which can be done through the use of DHCP.

Cont…

- In addition, the mobile host needs the necessary software to allow it to communicate with the home agent and to have two addresses:
- its home address and its care-of address.
- This dual addressing must be transparent to the application programs.
- When the mobile host acts as a foreign agent, the care-of address is called a **colocated care-of address.**
- The advantage of using a colocated care-of address is that the mobile host can move to any network without worrying about the availability of a foreign agent.
- The disadvantage is that the mobile host needs extra software to act as its own foreign agent.

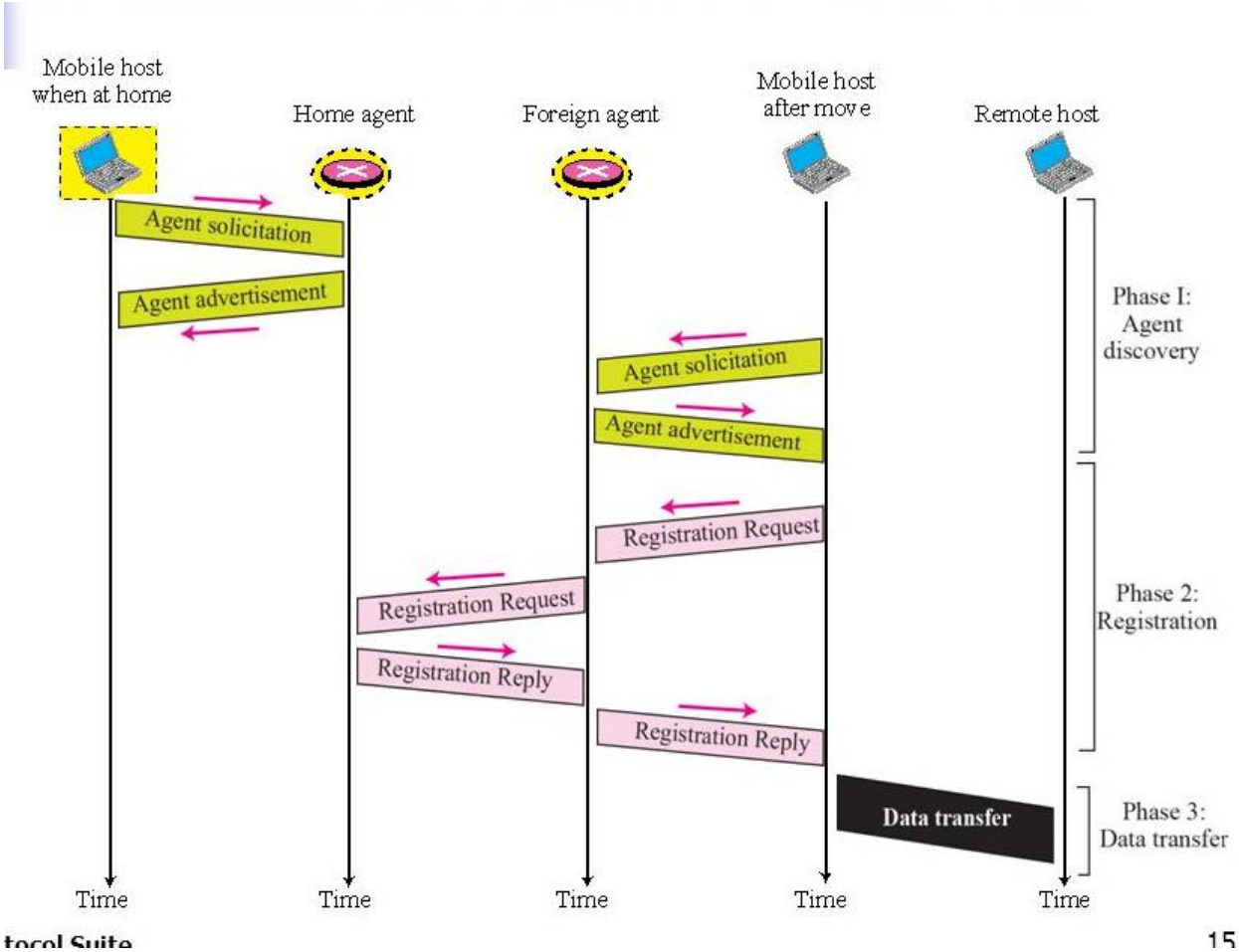
5.18 Three Phases

- **To communicate with a remote host, a mobile host goes through three phases:**
- **A) Agent discovery,**
- **B) Registration, and**
- **C) Data transfer, as shown in Figure 10.3.**
- The first phase, agent discovery, involves the mobile host, the foreign agent, and the home agent.
- The second phase, registration, also involves the mobile host and the two agents.
- Finally, in the third phase, the remote host is also involved. We discuss each phase separately.

5.19 Agent Discovery

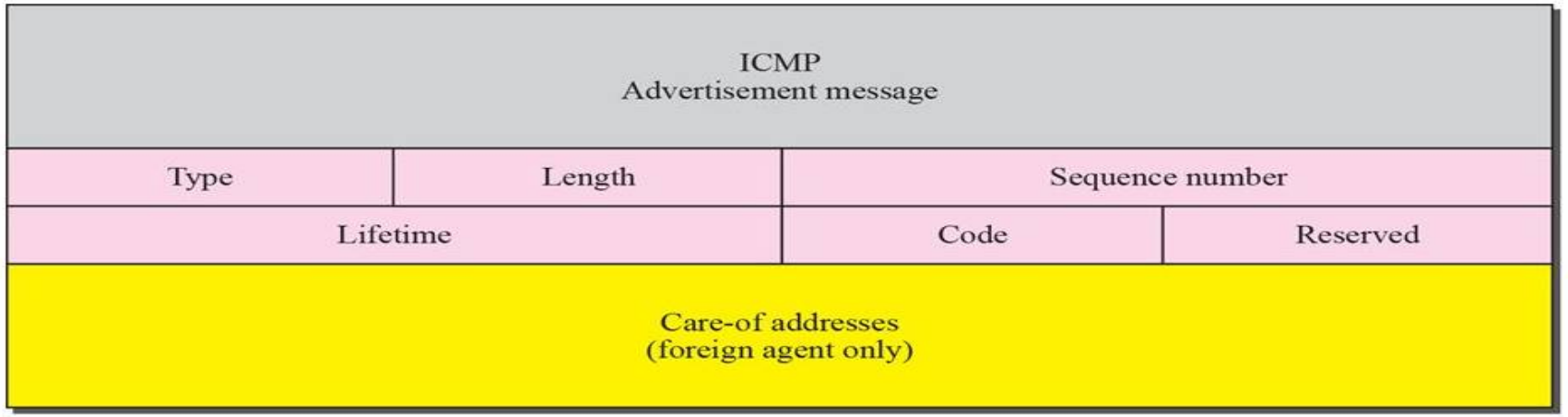
- The first phase in mobile communication, **agent discovery, consists of two subphases.**
- A mobile host must discover (learn the address of) a home agent before it leaves its home network.
- A mobile host must also discover a foreign agent after it has moved to a foreign network.
- This discovery consists of learning the care-of address as well as the foreign agent's address.
- The discovery involves two types of messages: advertisement and solicitation.

Figure : *Remote host and mobile host communication*



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.
- Figure shows how an agent advertisement is piggy backed to the router advertisement packet.



5.20 Registration

- The second phase in mobile communication is registration. After a mobile host has moved to a foreign network and discovered the foreign agent, it must register.

- **There are four aspects of registration:**
- 1. The mobile host must register itself with the foreign agent.
- 2. The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.
- 3. The mobile host must renew registration if it has expired.
- 4. The mobile host must cancel its registration (deregistration) when it returns home.

Request and Reply :

- To register with the foreign agent and the home agent, the mobile host uses a registration request and a registration reply as shown in Figure 10.3.

Registration Request : A registration request is sent from the mobile host to the foreign agent to register its care-of address and also to announce its home address and home agent address.

- The foreign agent, after receiving and registering the request, relays the message to the home agent.
- Note that the home agent now knows the address of the foreign agent because the IP packet that is used for relaying has the IP address of the foreign agent as the source address. Figure 10.5 shows the format of the registration request.

Figure 10.5 *Registration request format*

The field descriptions are as follows:

- ❑ **Type.** The 8-bit type field defines the type of the message. For a request message the value of this field is 1.
- ❑ **Flag.** The 8-bit flag field defines forwarding information. The value of each bit can be set or unset. The meaning of each bit is given in Table 10.2.
- ❑ **Lifetime.** This field defines the number of seconds the registration is valid. If the field is a string of 0s, the request message is asking for deregistration. If the field is a string of 1s, the lifetime is infinite.
- ❑ **Home address.** This field contains the permanent (first) address of the mobile host.

Table : *Registration request flag field bits*

Table 10.2 *Registration request flag field bits*

Bit	*Meaning*
0	Mobile host requests that home agent retain its prior care-of address.
1	Mobile host requests that home agent tunnel any broadcast message.
2	Mobile host is using colocated 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.

Cont…

- ❑ **Home agent address.** This field contains the address of the home agent.
- ❑ **Care-of address.** This field is the temporary (second) address of the mobile host.
- ❑ **Identification.** This field contains a 64-bit number that is inserted into the request by the mobile host and repeated in the reply message. It matches a request with a reply.
- ❑ **Extensions.** Variable length extensions are used for authentication. They allow a home agent to authenticate the mobile agent.

Registration Reply

- A registration reply is sent from the home agent to the foreign agent and then relayed to the mobile host.
- The reply confirms or denies the registration request.
- Figure shows the format of the registration reply.

Encapsulation

- Registration messages are encapsulated in a UDP user datagram.
- An agent uses the well-known port 434; a mobile host uses an ephemeral port.

Figure : *Registration reply format*

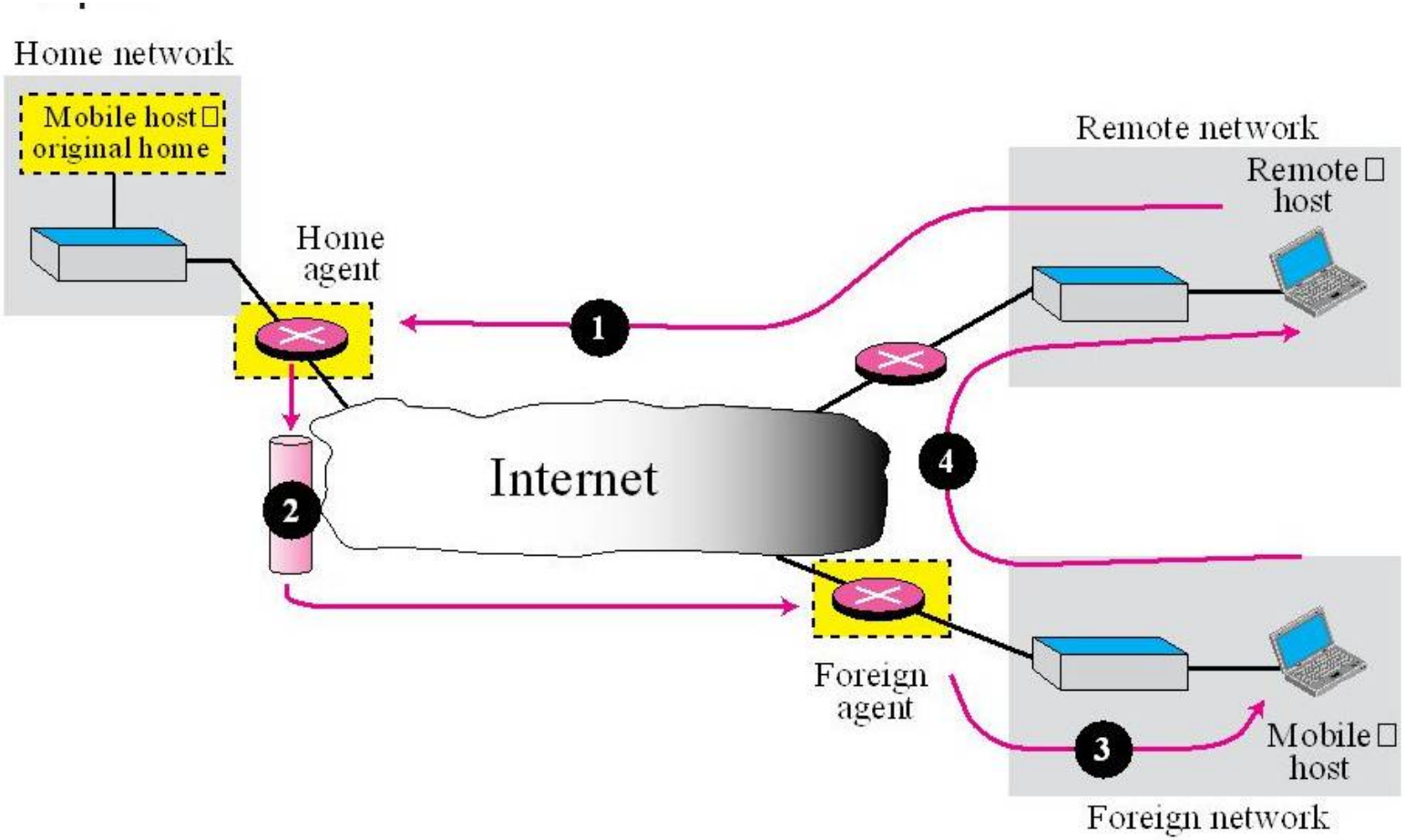
5.21 Data Transfer

- After agent discovery and registration, a mobile host can communicate with a remote host. Figure 10.7 shows the idea.

From Remote Host to Home Agent

- When a remote host wants to send a packet to the mobile host, it uses its address as the source address and the home address of the mobile host as the destination address.
- In other words, the remote host sends a packet as though the mobile host is at its home network.
- The packet, however, is intercepted by the home agent, which pretends it is

Figure : *Data transfer*



Cont…

- ***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 using its address as the source and the foreign agent's address as the destination.
- Path 2 of Figure 10.7 shows this step.
- ***From Foreign Agent to Mobile Host***
- When the foreign agent receives the packet, it removes the original packet.
- However, since the destination address is the home address of the mobile host, the foreign agent consults a registry table to find the care-of address of the mobile host.
- Path 3 of Figure 10.7 shows this step.

Cont…

- ***From Mobile Host to Remote Host***
- When a mobile host wants to send a packet to a remote host (for example, a response to the packet it has received), it sends as it does normally.
- The mobile host prepares a packet with its home address as the source, and the address of the remote host as the destination. Although the packet comes from the foreign network, it has the home address of the mobile host.
- Path 4 of Figure 10.7 shows this step.
- ***Transparency***
- In this data transfer process, the remote host is unaware of any movement by the mobile host.
- The remote host sends packets using the home address of the mobile host as the destination address; it receives packets that have the home address of the mobile host as

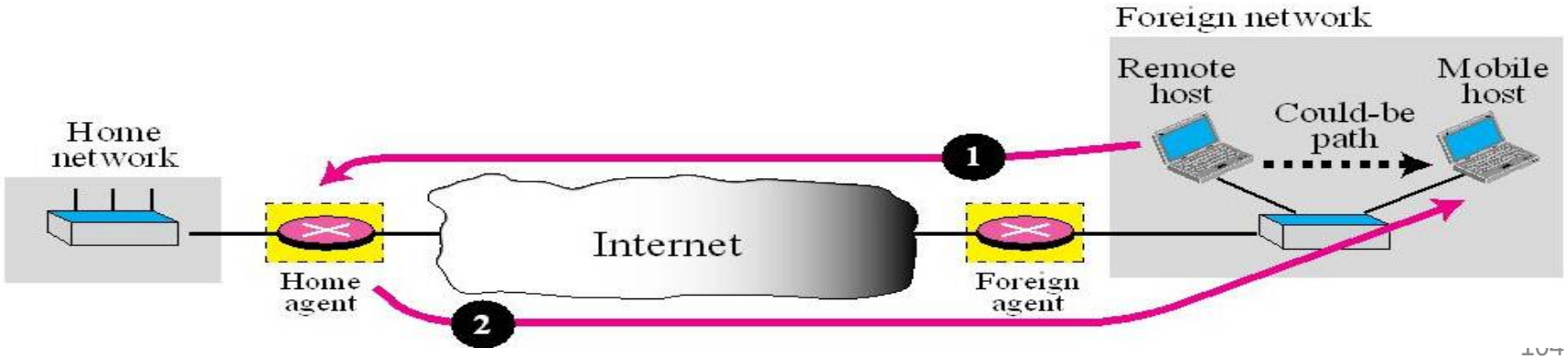
5.22 Inefficiency in Mobile IP

- Communication involving mobile IP can be inefficient.
- The inefficiency can be severe or moderate.
- The severe case is called double crossing or 2X.
- The moderate case is called triangle routing or dog-leg routing.

- **a) Double Crossing :**
- Double crossing occurs when a remote host communicates with a mobile host that has moved to the same network (or site) as the remote host (see Figure 10.8).

Cont…

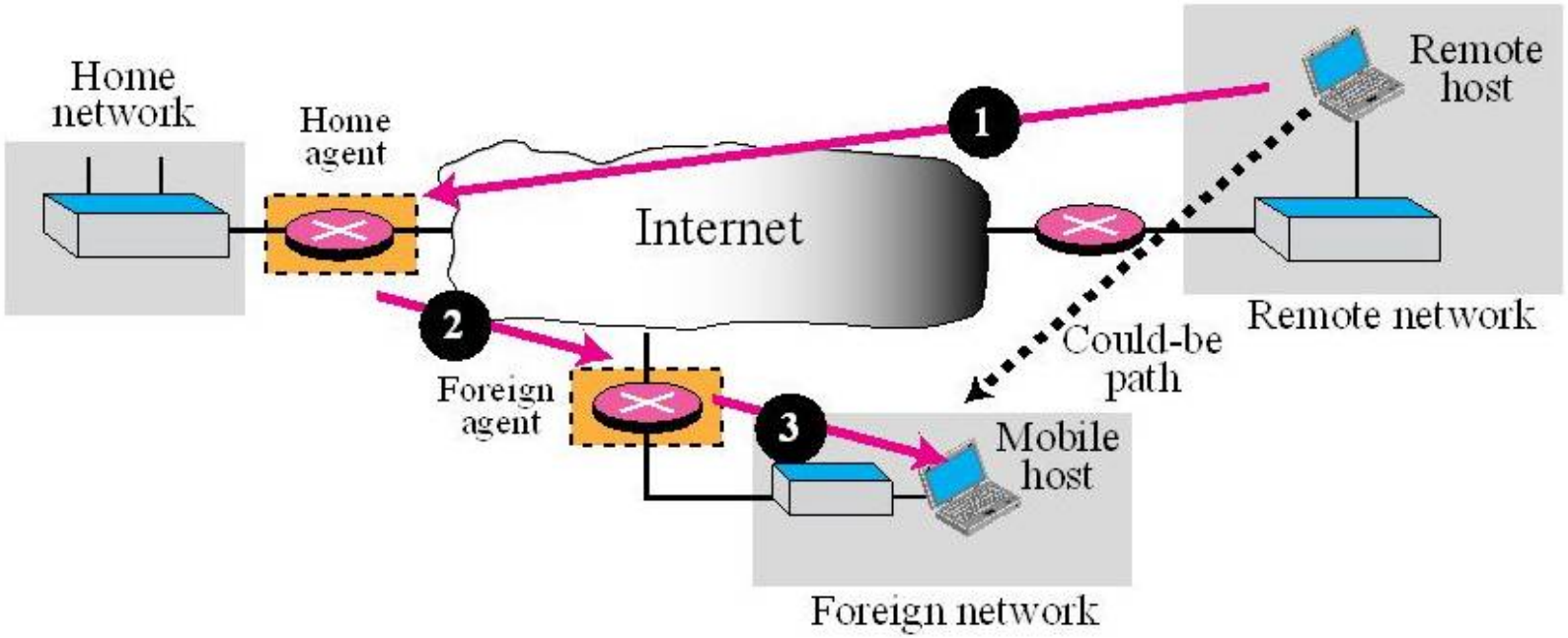
- When the mobile host sends a packet to the remote host, there is no inefficiency; the communication is local.
- However, when the remote host sends a packet to the mobile host, the packet crosses thInternet twice.
- Since a computer usually communicates with other local computers (principle of locality), the inefficiency from double crossing is significant.



b) Triangle Routing

- Triangle routing, the less severe case, occurs when the remote host communicates with a mobile host that is not attached to the same network (or site) as the mobile host.
- When the mobile host sends a packet to the remote host, there is no inefficiency.
- However, 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, instead of just one side (see Figure 10.9).

Figure 10.9 *Triangle routing*



c) Solution

- One solution to inefficiency is for the remote host to bind the care-of address to the home address of a mobile host.
- For example, when a home agent receives the first packet for a mobile host, it forwards the packet to the foreign agent; it could also send an update binding packet to the remote host so that future packets to this host could be sent to the care-of address.
- The remote host can keep this information in a cache.
- The problem with this strategy is that the cache entry becomes outdated once the mobile host moves.
- In this case the home agent needs to send a warning packet to the remote host to inform it of the change.

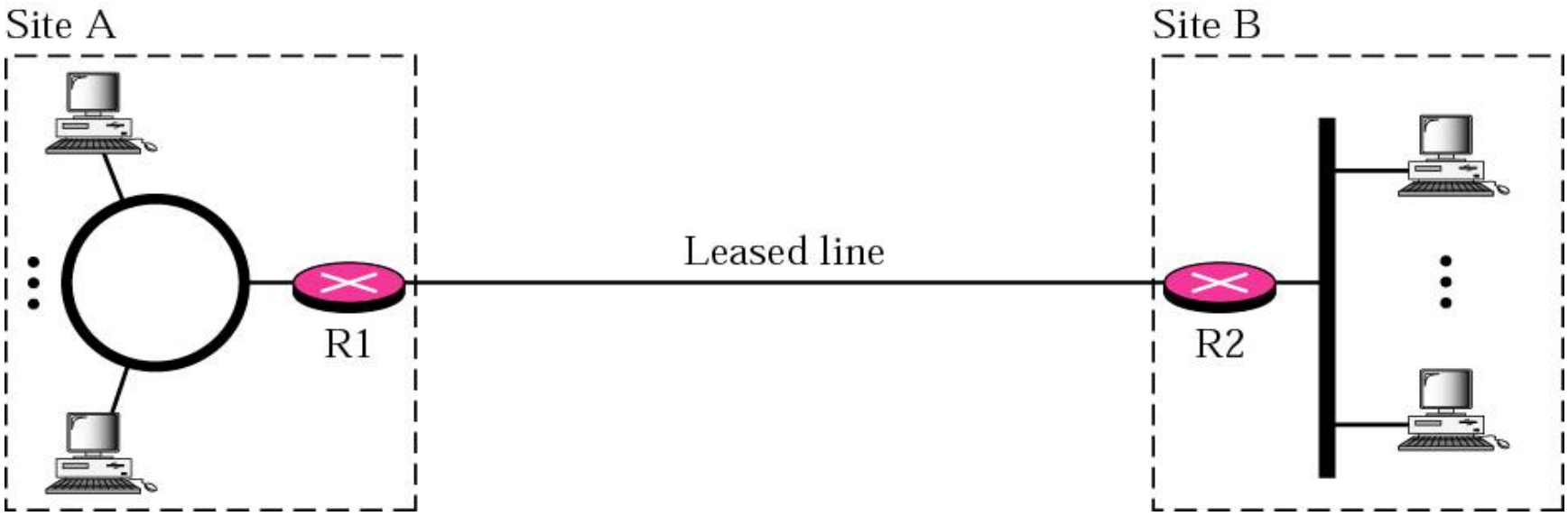
5.23 Virtual Private Networks (VPN).

- **Virtual Private Networks (VPN)** is a technology that is gaining popularity among large organizations that use the global internet for both intra and inter organization communication, but require privacy in their intra organization communication.
- A) Achieving Privacy
- B) VPN Technology
- **This achieving privacy can use three strategies,**
- **Private network**
- **Hybrid network**
- **Virtual private network**

Private network :

- An organization that needs privacy when routing information inside the organization can use a private network .
- A small organization with one single site can use an isolated LAN.
- People inside the organization can send data to one another that today remain inside the organization with several sites can create a private internet.
- The LAN different sites can be connected to each other using router and leased lines.
- The LANs are connected to each other using router and one leased line.

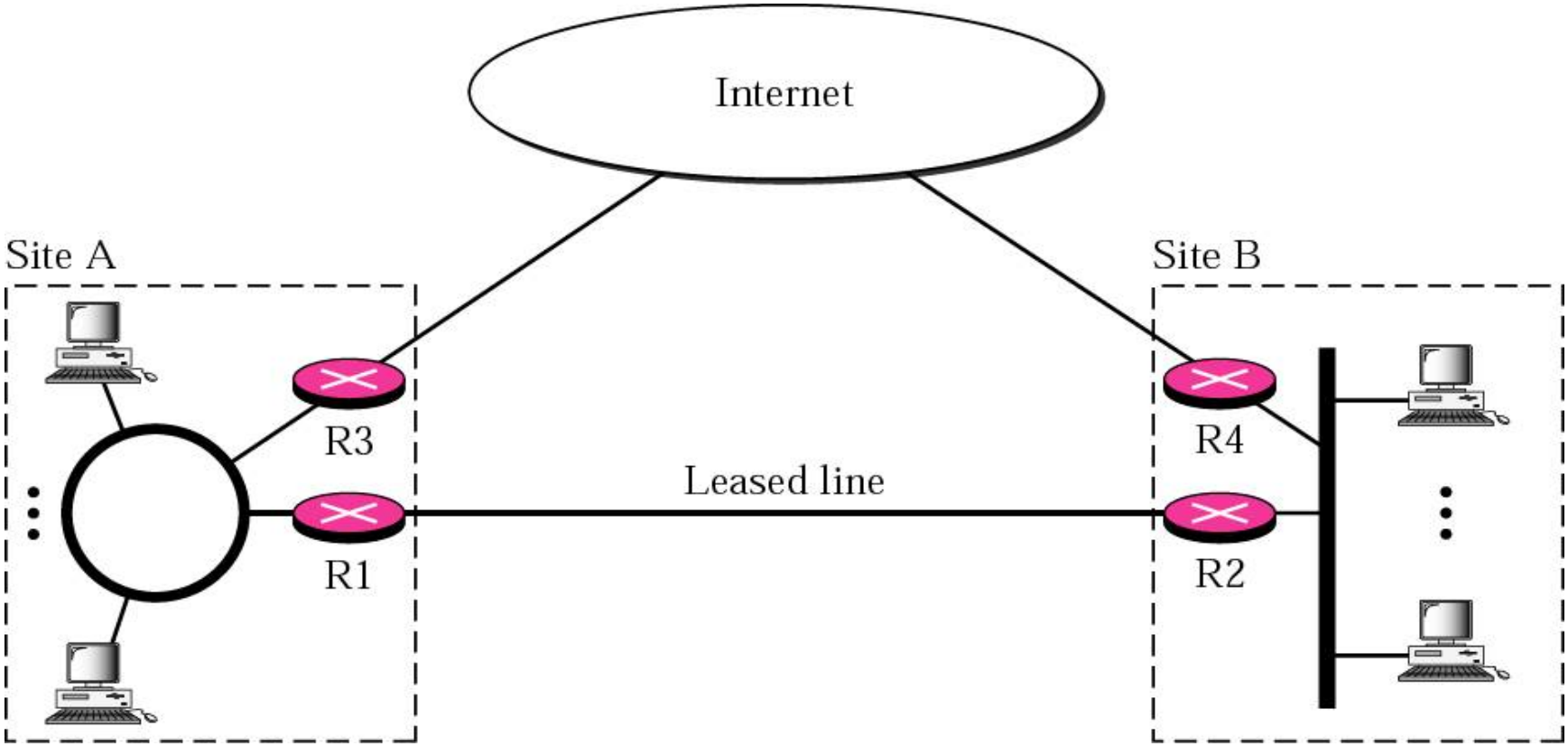
Figure : Private network



Hybrid network

- Today , most organization need to have privacy in intraorganization data exchange.
- But at the same time, they need to be connected to the global internet for data exchange with other organization.
- One solution is the use of hybrid network.
- A hybrid network allows an organization to have its own private internet and at the same time, access the global internet.
- Figure shows an example of this situation.

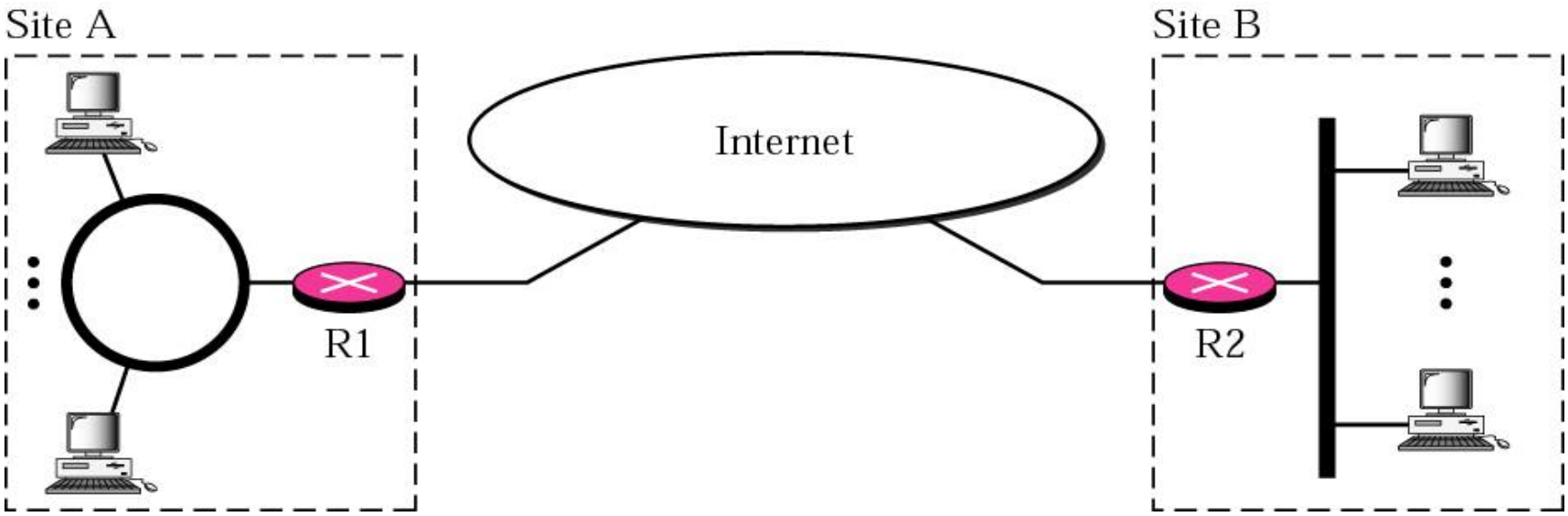
Figure : Hybrid network



Virtual private network

- Both private and hybrid network have a major drawback: Cost and private wide area network are expensive.
- To connect several sites an organization needs several leased lines.
- Which can lead to a high monthly cost.
- One solution is to use the global internet for both private and public communication.
- A technology **called virtual private network**

Figure: Virtual private network



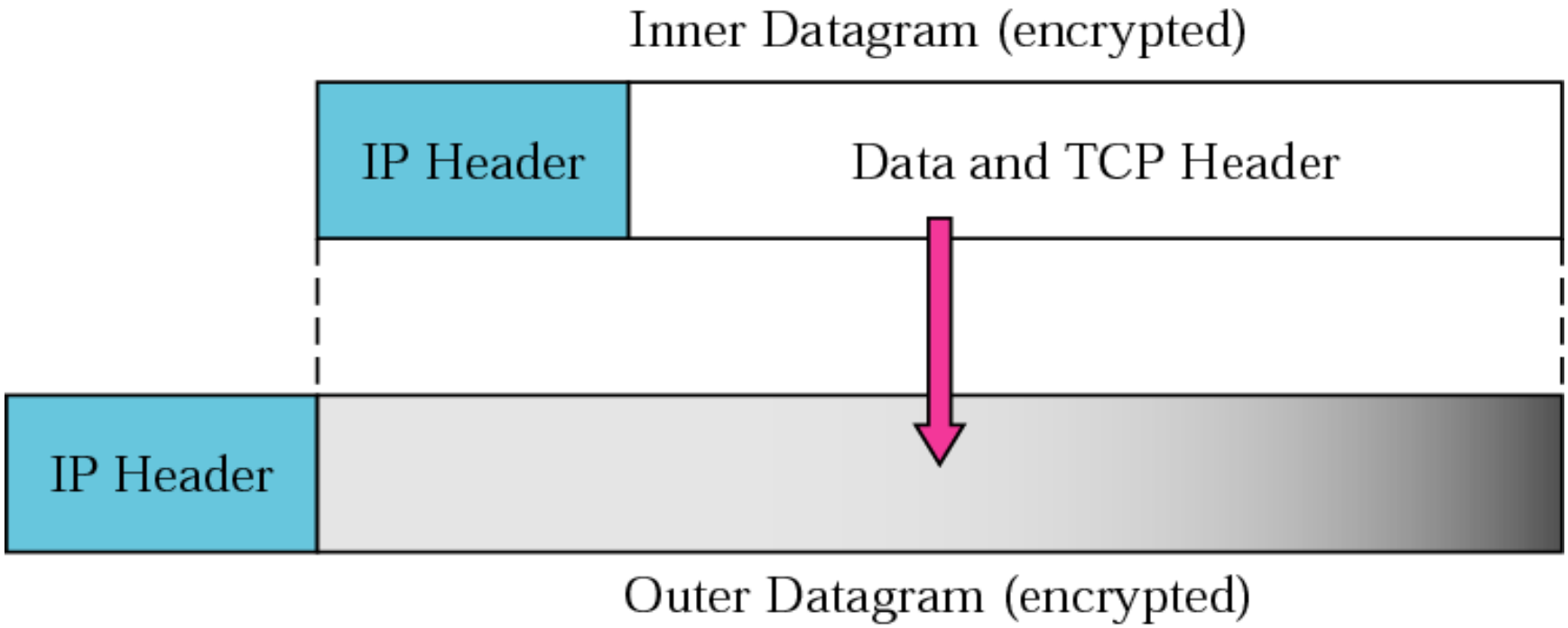
B) VPN technology

- VPN technology uses two techniques to guarantee privacy for an organization.
- **IP sec**
- **Tunneling**

Tunneling :

- To guarantee privacy for an organization.
- VPN specifies that each IP datagram destined for private use in the organization must be encapsulated in another datagram as shown in figure

Figure : Tunneling



Cont…

- This is called as tunneling because the original datagram is hidden inside the outer datagram after existing R1 **figure (addressing in a VPN).**
- Invisible untill is reaches R2.
- It appears that the original datagram has gone through a tunnel spanning R1 and R2.

Figure : Addressing in a VPN