Options in IPV4

IPV4 OPTIONS

The header of the IP datagram is made of two parts: a fixed part and a variable part.

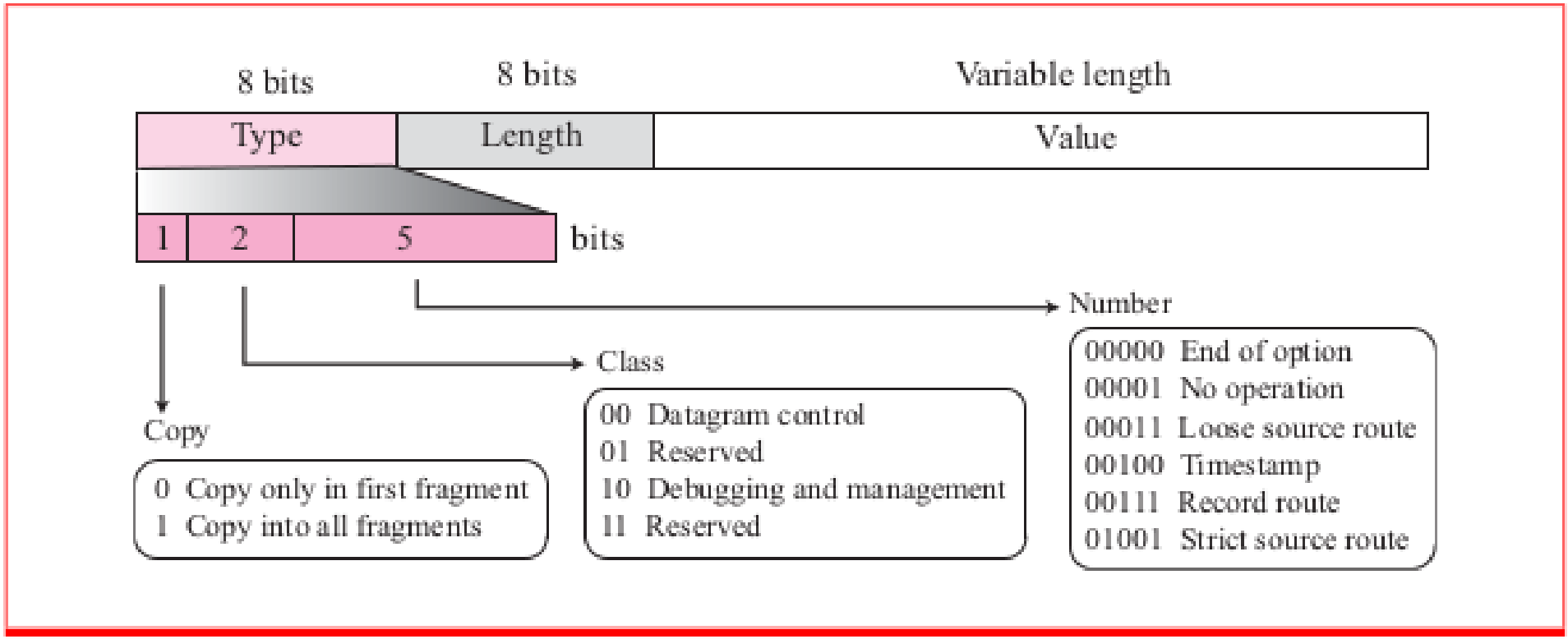
The fixed part is 20 bytes . The variable part comprises the options, which can be a maximum of 40 bytes.

Options, as the name implies, are not required for a datagram.

They can be used for network testing and debugging.

Format

Figure 22-1 *Option format*



Type

The type field is 8 bits long and contains three subfields: copy, class, and number.

Copy. This 1-bit subfield controls the presence of the option in fragmentation.

When its value is 0, it means that the option must be copied only to the first fragment. If its value is 1, it means the option must be copied to all fragments.

Type

- Class. This 2-bit subfield defines the general purpose of the option. When its value is 00, it means that the option is used for datagram control. When its value is 10, it means that the option is used for debugging and management. The other two possible values (01 and 11) have not yet been defined.

Type

- Number. This 5-bit subfield defines the type of option. Although 5 bits can define up to 32 different types, currently only 6 types are in use.

Other Fields

Length

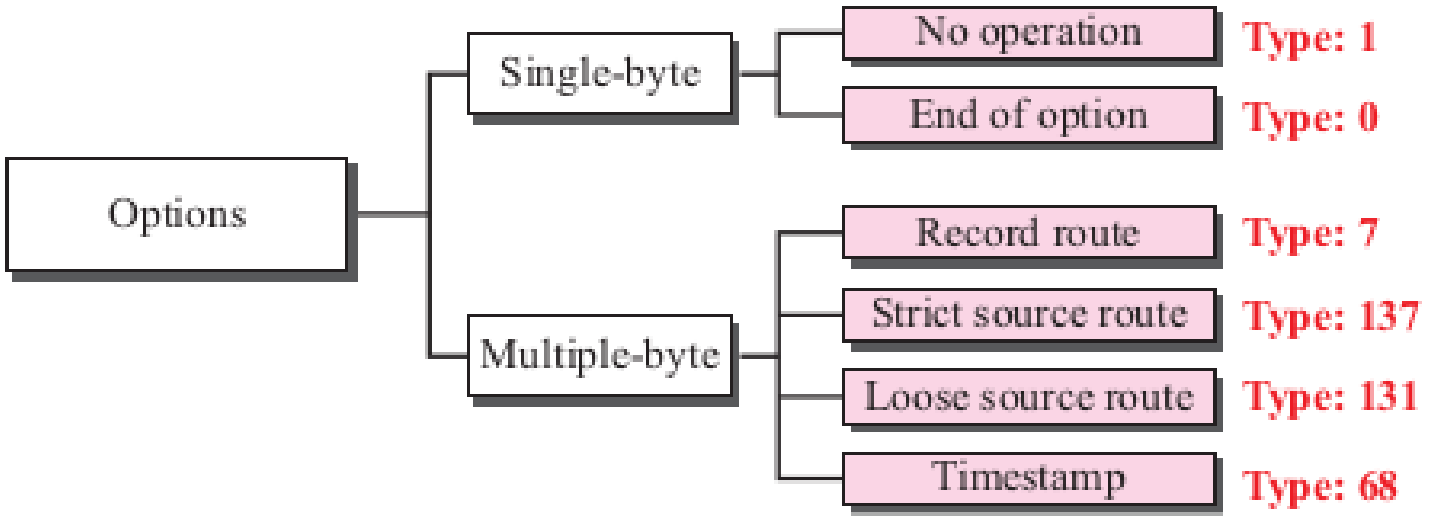
The length field defines the total length of the option including the type field and the length field itself. This field is not present in all of the option types.

Value

The value field contains the data that specific options require. Like the length field, this field is also not present in all option types.

Option Types

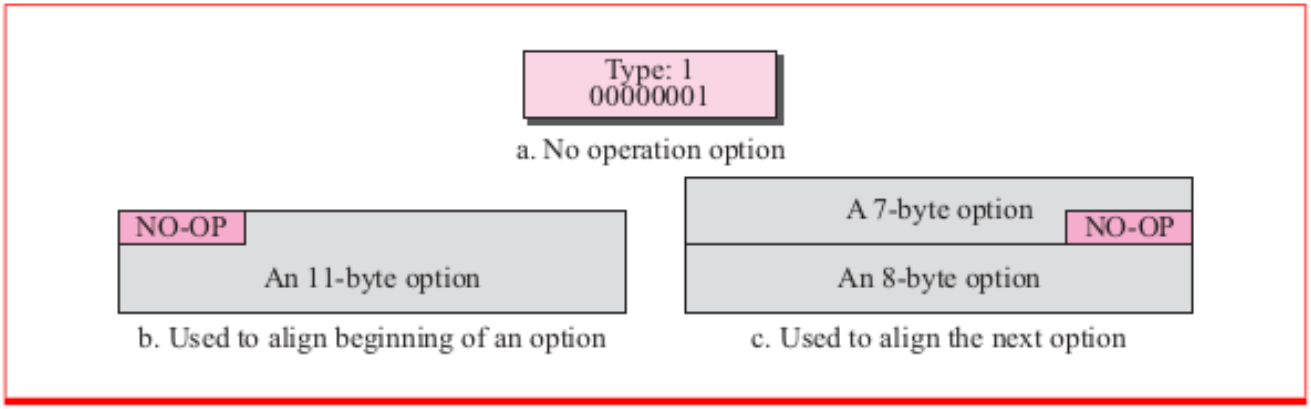
Figure 22-2 *Categories of options*



Single Byte Options do not require the length or the data fields.

No-Operation Option

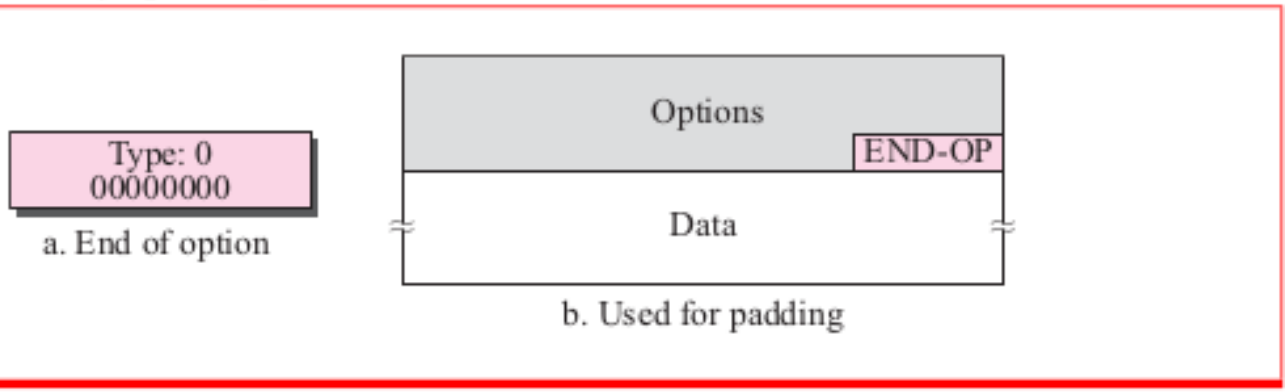
Figure 22-3 *No operation option*



A no-operation option is a 1-byte option used as a filler between options. For example, it can be used to align the next option on a 16-bit or 32-bit boundary

End-of-Option Option

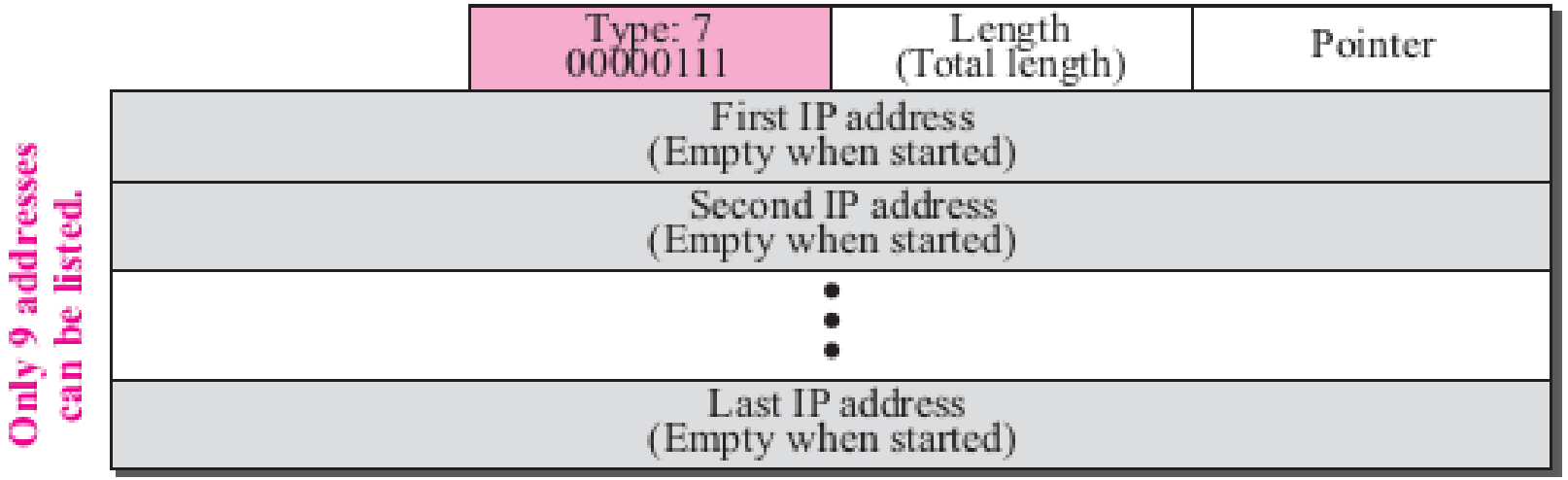
Figure 22-4 *End-of-option option*



An end-of-option option is also a 1-byte option used for padding at the end of the option field. It, however, can only be used as the last option. Only one end-of-option option can be used. After this option, the receiver looks for the payload data.

Record-Route Option

Figure 22-5 *Record-route option*



Record-Route Option

A record-route option is used to record the Internet routers that handle the datagram.

It can list up to nine router IP addresses since the maximum size of the header is 60 bytes

The source creates placeholder fields in the option to be filled by the visited routers.

The pointer field is an offset integer field containing the byte number of the first empty entry.

In other words,it points to the first available entry.

Record-Route Option

The source creates empty fields for the IP addresses in the data field of the option.

When the datagram leaves the source, all of the fields are empty. The pointer field has a value of 4, pointing to the first empty field.

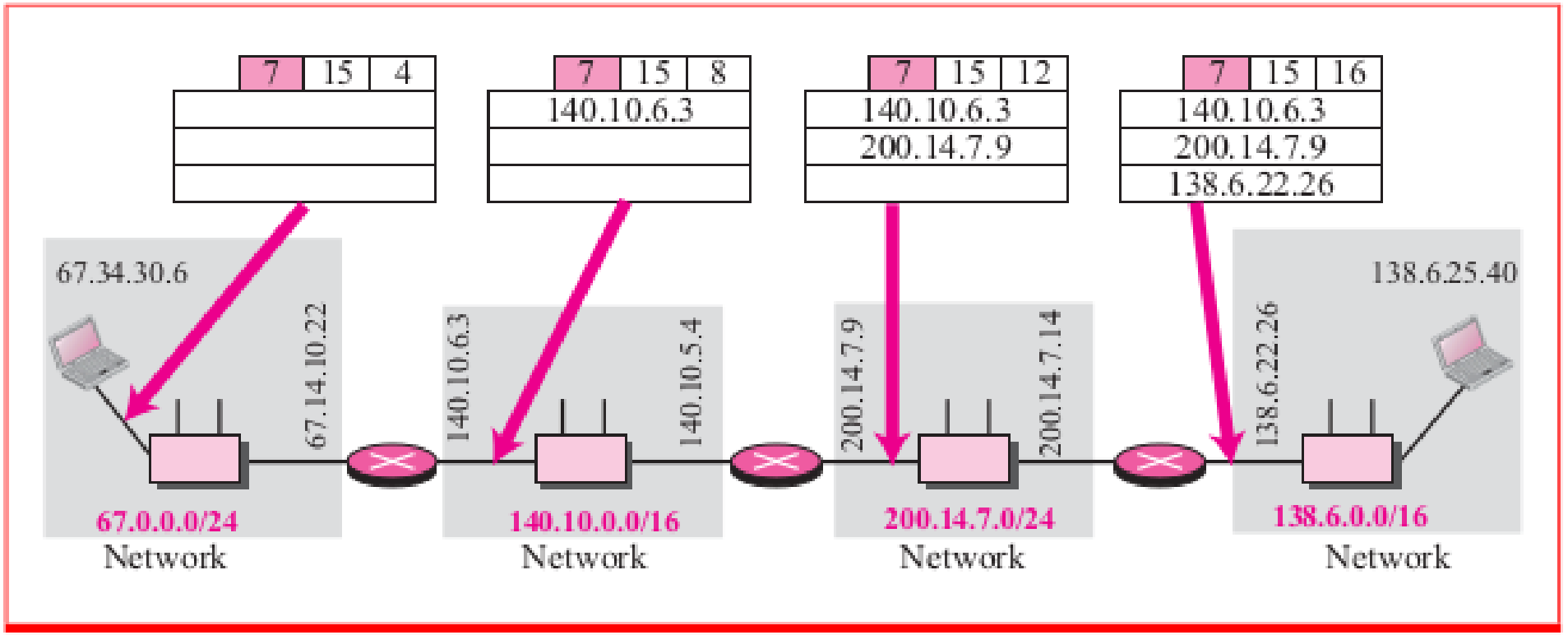
When the datagram is traveling, each router that processes the datagram compares the value of the pointer with the value of the length.

If the value of the pointer is greater than the value of the length, the option is full and no changes are made.

However, if the value of the pointer is not greater than the value of the length, the router inserts its outgoing IP address in the next empty field

Record-Route Option

Figure 22-6 *Record-route concept*



Strict-Source-Route Option

A strict-source-route option is used by the source to predetermine a route for the datagram as it travels through the Internet.

Dictation of a route by the source can be useful for several purposes.

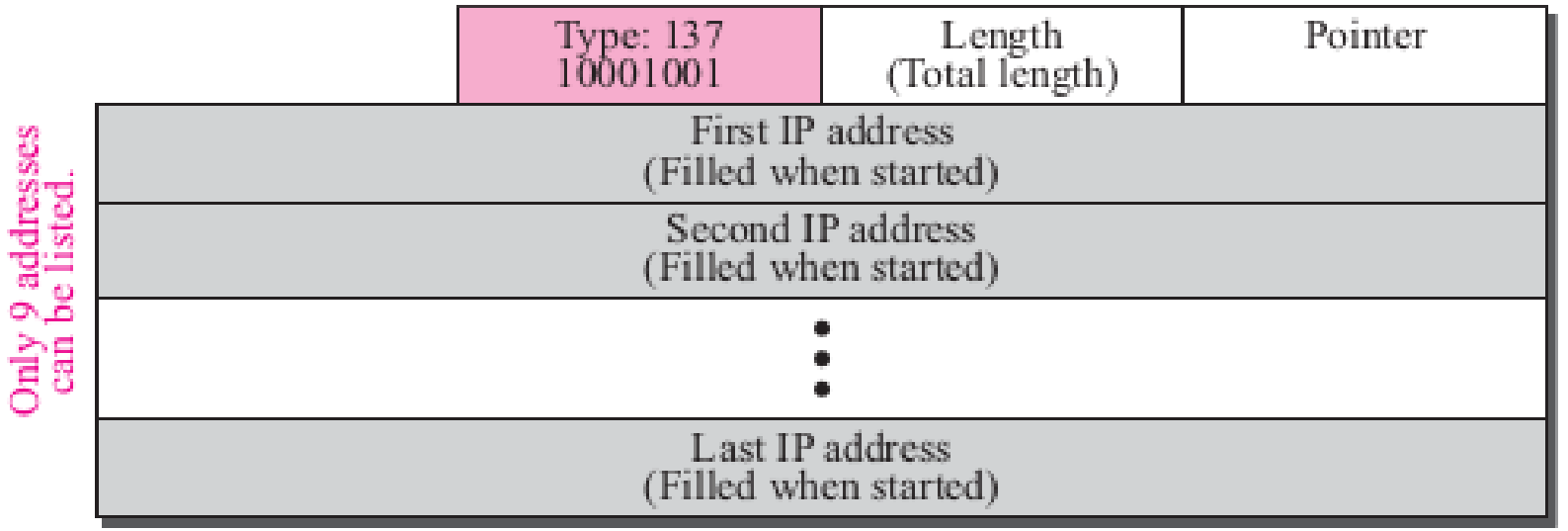
The sender can choose a route with a specific type of service, such as minimum delay or maximum throughput.

If a datagram specifies a strict source route, all of the routers defined in the option must be visited by the datagram.

A router must not be visited if its IP address is not listed in the datagram. If the datagram visits a router that is not on the list, the datagram is discarded and an error message is issued.

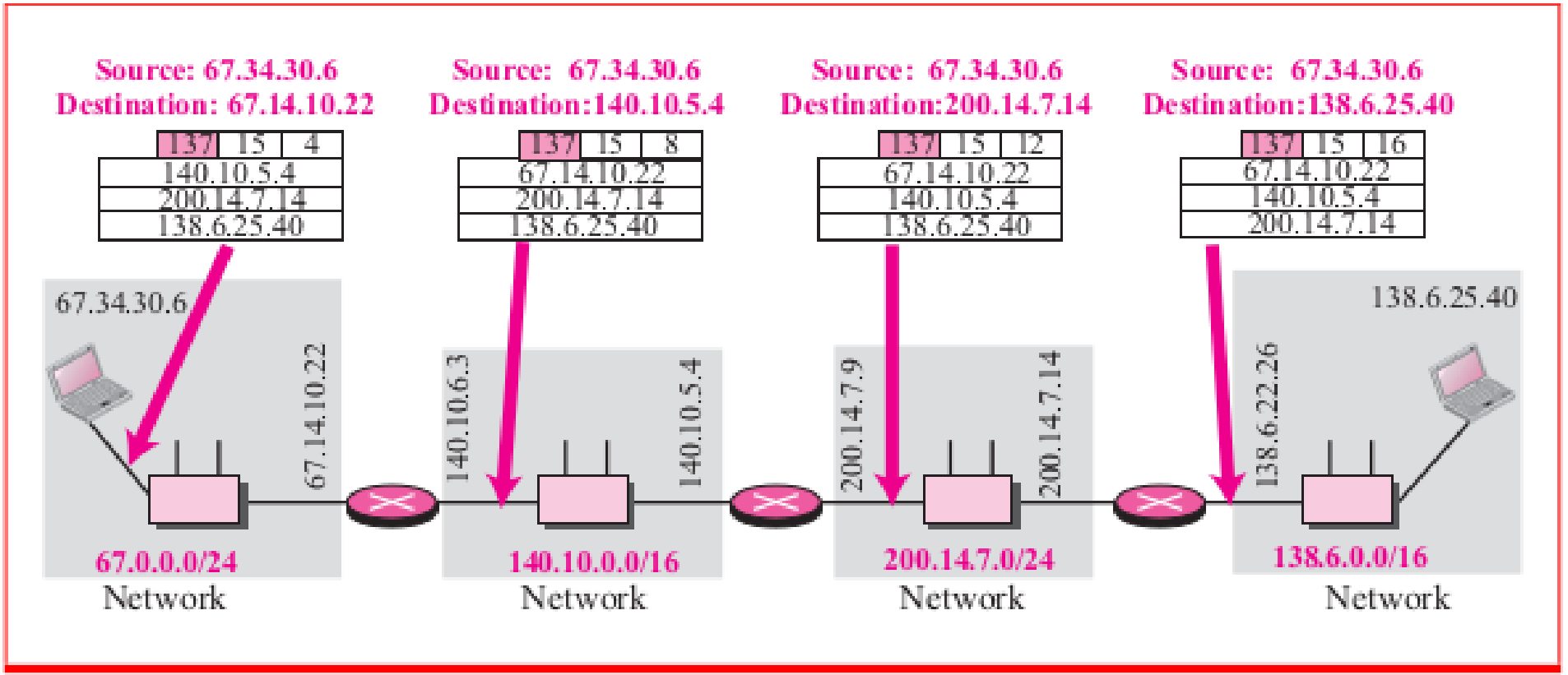
Strict-Source-Route Option

Figure 22-7 *Strict-source-route option*



Strict-Source-Route Option

Figure 22-8 *Strict-source-route concept*



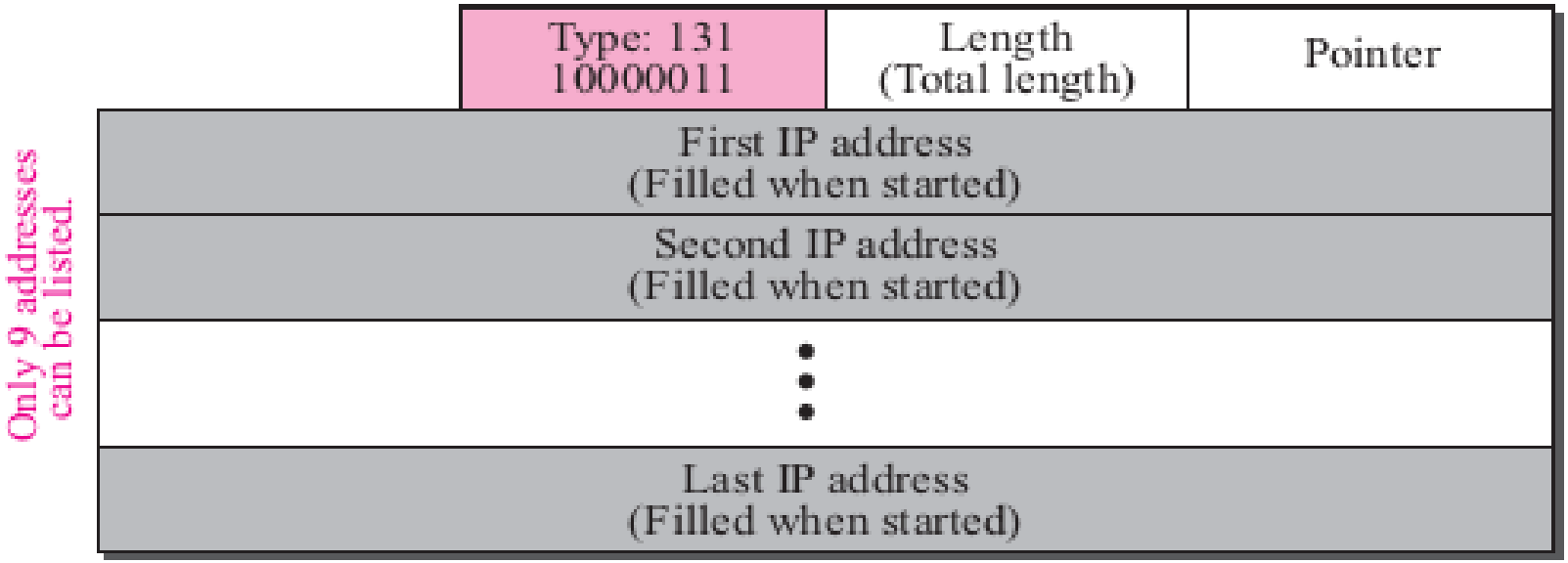
Loose-Source-Route Option

A loose-source-route option is similar to the strict source route, but it is more relaxed.

Each router in the list must be visited, but the datagram can visit other routers as well.

Loose-Source-Route Option

Figure 22-9 *Loose-source-route option*



Timestamp

A timestamp option is used to record the time of datagram processing by a router.

The time is expressed in milliseconds from midnight, Universal Time.

Knowing the time a datagram is processed can help users and managers track the behaviour of the routers in the Internet.

Security of IPv4 Datagrams

- **Packet Sniffing**
- **Packet Modification**
- **IP Spoofing**
- **IPSec**
  - Algorithms and Keys
  - Packet Encryption
  - Data Integrity
  - Origin Authentication

Packet Sniffing

An intruder may intercept an IP packet and make a copy of it.

Packet sniffing is a passive attack, in which the attacker does not change the contents of the packet.

This type of attack is very difficult to detect because the sender and the receiver may never know that the packet has been copied.

Although packet sniffing cannot be stopped, encryption of the packet can make the attacker's effort useless.

The attacker may still sniff the packet, but the content is not detectable.

Packet Modification

The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.

The receiver believes that the packet is coming from the original sender.

This type of attack can be detected using a data integrity mechanism.

IP Spoofing

An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer.

An attacker can send an IP packet to a bank pretending that it is coming from one of the customers.

This type of attack can be prevented using an origin authentication mechanism

IPSec

The IP packets today can be protected from the previously mentioned attacks using a protocol called IPSec (IP Security).

IPSec provides the following four services:

- Algorithms and Keys
- Packet Encryption
- Data Integrity
- Origin Authentication