コンピュータセキュリティ 14−18
(2001. 7. 25)

情報ネットワークにおける情報セキュリティに関するいくつかの課題と解決法

副題： 企業向けＩＰ網ＯＢＮの情報セキュリティ

古川久夫† 宮口庄司‡

†（財）流通システム開発センター・OBN 情報センター
〒107-0052 港区赤坂 7-1-16, 日本生命赤坂第 2 ビル 9F, Tel 03-5414-8510
furukawa@obn.dsri-dcc.or.jp http://www.obn.dsri-dcc.or.jp

‡ 芝浦工業大学・工学部・情報工学科
〒330-8570 大宮市深作, labomiya@xa2.so-net.ne.jp

あらまし

ＯＢＮは、インタネットと分離した閉域ＩＰ網であり、企業内のLAN 間通信サービス（イントラ）と、異企業間 LAN 間通信サービス（エクストラ）とを提供する。ＯＢＮは、ＯＢＮ網の内部と外部とを分離するエッジノードを有し、網内部において内部アドレスが、網外部において外部アドレスがそれぞれ用いられる。このアドレス分離は、網の内部を攻撃するＤｏＳ対策として有効である。通信会社は、企業ユーザの端末アドレスをエッジノードの一つに登録し、ユーザへの課金や、マルチキャスト通信サービスにおけるＤｏＳ対策をとれる。

キーワード 情報ネットワーク 情報セキュリティ カプセル

Some problems related to information security in information networks and their solutions

Subtitle: Information security in the business-oriented IP network "OBN"

Hisao Furukawa† Shoji Miyaguchi ‡

† OBN Information Center, The Distribution Systems Research Institute
Nihon-seimei-akasaka-building2, 9F, 7-1-16, Akasaka, Minato-ku, Japan, zip :107-0052
Tel +81-3-5414-8510, E-mail furukawa@obn.dsri-dcc.or.jp,
http://www.obn.dsri-dcc.or.jp

‡ Shibaura Institute of Technology Fukasaku, Ohmiya, Japan, zip : 330-8570

Abstract OBN is configured as a closed IP network separate from the Internet; it offers IP communication services between LANs within the same company (i.e. intra-nets) and can provide IP communication services between LANs owned by different enterprises(i.e. extra-nets). OBN uses edge nodes to isolate each OBN network. External and internal addresses are used for communication outside and inside the network, respectively. Address separation is effective in countering DoS(Denial of Service) attacks inside the network. Communication companies may register terminal addresses of enterprise users with one edge node; this makes it easy to charge users and, furthermore, to develop DoS countermeasures in multicast communication services.

key words information network information security capsule

1. Introduction

The authors have been promoting the business-oriented IP network OBN (Open Business Network) (see document 1,2). The Distribution Systems Research Institute developed the specifications of OBN, and promulgated them to the main communication companies in Japan. These carriers now offer commercial OBN services in Japan (Note-1). One general rule is that it must be possible to connect one OSPN (OBN service provider network) to another OSPN operated by different communication company.

OBN is configured as a closed IP network that offers IP communication services between LANs of the same company (i.e. intra-nets) and IP communication services between LANs owned by different enterprises (i.e. extra-nets). Users can form their own closed IP network using OBN.

The most important point when considering OBN architecture is how to realize communications between LANs; this problem is resolved by encapsulation. IP encapsulation methods are also effective in suppressing DoS (Denial of Service) attacks.

2. IP encapsulation and DoS countermeasures

2.1 IP encapsulation

2.1.1 IP communications between LANs

To resolve the problem of handling LAN private addresses, encapsulation is used. IP packets sent from a source terminal in a LAN reach OBN. An edge node of OBN encapsulates them into internal packets whose IP headers include the internal addresses appropriate for the network. Since different internal addresses are carried in the internal packet headers, overlap can be avoided. Each internal packet is transmitted across the OBN until it reaches the suitable edge node at which point the internal header is deleted (de-encapsulation), and recovered IP packets (traditional style) are transferred to the destination terminal (Fig.1).

Consider the case that the source's external IP address is "EA1", the destination's external IP address is "EA2" (set in traditional IP packet), while the source's internal address is "IA1". This internal address is associated with a logical terminal at the end of a communication line. It is clear that the combination of three addresses, "IA1","EA2" and "EA1" can guide the packet to destination. We set the combination of four addresses, IA1","EA2","EA1","IA2" as the record in the edge node, as shown in record-1 in Fig.2.

Encapsulation can also utilize the masking techniques used in typical IP routers. Here,"IA1","EA2","EA1"are the same as described above. First, select the record that holds "IA1" (this case record-2 in Fig.2), and then check if the result of a logical AND operation between "EA2"and "MSK2" equals "EA2n", and finally check if the result of a logical AND operation between "EA1"and "MSK1" equals "EA1n"; when all checks are satisfied, the destination internal address "IA2" can be used.

2.1.2 Virtual dedicated line IP communication

The OBN offers a virtual dedicated line communication function where only internal address "IA1" is used to decide the destination (internal) address "IA2"(record-3 of Fig.2). The two addresses "IA1"and "IA2"are the same as described above. In this case, addresses "EA1"and "EA2" in the external packet are not referred to. A key point is that an IP network can be configured by edge nodes that hold records identifying the association between internal addresses "IA1" and "IA2"(record-3 of Fig.2); this yields virtual dedicated line IP communication network (Fig.3).

2.1.3 Communication record and closed IP network

The records shown in Fig.2 can be called communication records. An edge node registers the combination of users' external addresses in the form of records 1,2,4 or 5 of figure 2 (record 4 and 5 described later). Reecord-3 is used to set the combination of internal addresses for virtual dedicated line communication between particular users. Accordingly, the edge node rejects those users who attempt to send IP packets to a user who is not registered with the edge node, which enhances information security.

In short, OBN can form a particular closed IP network according to user's needs by making a set of communication records as described above.

2.1.4 Encapsulation techniques

Record-4 of Fig.2. shows an example in which source external address"EA1" can be omitted, and record-5 shows that external address"EA1" can be omitted as a variant of record-2. Fig.4 shows an example in which the internal packet does not include source internal address. MPLS and MAPOS(one of WDM frame) have only destination address, not source address. External packet and internal packet are not limited to the layer three (i.e. IP packet). For example, MAC frame(layer 2) can be adopted as the external packet. MPLS frame(layer may be 2.5) or WDM frame(layer 2) can be adopted as the internal packet.

These techniques can be selected in a future extension of OBN.

2.2 IP encapsulation as DoS countermeasure

As external packets are encapsulated to yield internal packets, address trace in the OBN cannot be carried out. If an external packet has OBN internal address in its header, this internal address is never used inside the OBN. We believe that DoS attacks against servers etc. in the OBN are impossible.

2.3 Terminal address registration

An edge node registers addresses of user terminals as shown "m" in Fig.1. The registration area may memory or a file. For record-1 and record-2 in Fig.2, both "EA1" and "EA1n" can be used for address registration. When an external IP packet that does not include registered source address, it is discarded at the OBN's edge node Therefore, address registration is very effective as a countermeasure to DoS.

Furthermore, we think that terminal address registration is useful to charge packets or users who sent the packets, i.e. only when an address is registered packets are accepted to pass through the edge node which guarantees charging. In addition, an internal address "IA1" (in record-1 to record-5 in Fig.2) can be used to charge the appropriate communication line.

3. Effective applications of closed IP networks

3.1 Authorization communication system for credit cards

(1) A unique authorization communication system for credit card verification in Japan is a type of center and terminal system. The network includes several host computers to identify customers belonging to companies offering credit card services (see: Fig.5. and Note-2). This system is weak against tapping due to the basic transmission procedure; signaling information can be analyzed easily.

(2) Countermeasures:

One solution appears to be the Internet (Fig.6), but there are several problems. The Internet is weak against DoS and communication companies accept no responsibility for Internet operation. The OBN solves all these problems. Fig.7 shows a recent system placed in service in the autumn of 2000.

3.2 IP telecommunication network for a bank

(1)Banks most often use dedicated lines(Fig.8). While secure, such systems are expensive, and many banks want to replace them with cheaper IP communication lines. Internet is weak to DoS and no responsible operation (Fig.9). OBN provides the extremely useful combination of excellent security and low cost.

3.3 Business-oriented IP network

OBN can form closed IP networks, as described at 2.1.3 that can be accessed by, for example, only banks, card companies and contracted companies (see: Fig.10). In addition, OBN will be effective as the IP communication environment that supports ASP service (Fig.11).

Figure 12 shows the business model in which a settlement service company supports an electronic mall on the Internet. The company lies between the mall and banks.

3.4 Multicast

(1) Problems with multicast:

The authors think there are two big problems.

Problem 1: How to charge receivers for multicast data?

Problem 2: If someone sends spam from a multicast source point or from close to the point, the IP network can be easily overwhelmed by the flood of IP packets.

(2) Measures:

Each terminal address is registered with one edge node of the IP network, shown as "m" in Fig.13. Terminal address registration will make multicast charging and the prevention of spamming easier to realize.

4. Application examples of encapsulation

We believe that the encapsulation techniques can be applied to various kinds of communication fields.

4.1 Characteristic:

Basic idea is to establish internal addresses and external addresses, and differentiates them at edge nodes.

Encapsulation is not limited to IP encapsulation, MPLS frames or WDM frames (MAPOS) can be adopted. In addition, classification of a packet entering a network is not limited; for example, even an external MAC frames are accepted. There are two forms of encapsulation, one is to watch address area of inputting packets, other case not to see address area of input packets.

In addition, the rights include edge nodes (equipment) and encapsulation methods other than a communications network or network system. These techniques are accepted as constituting technical property in many countries.

4.2 Examples

(1) Connection service between ISP networks (Fig.14)

A big common carrier can provide interconnect smaller ISP networks. The addresses used in the ISP networks are independent of each other, so encapsulation is necessary to avoid address collision.

(2) A communications network between LANs (see:Fig.15)

An IP network can connect LANs far from each other. An Ethernet frame (MAC frame) sent from a LAN reaches an edge node and is IP encapsulated to become an internal IP packet. It is forwarded through the IP network, and arrives at the destination edge node where reverse encapsulation recovers the original MAC frame. The MAC frame is sent to the destination LAN. MPLS or WDM frames can also be used. Source internal address can be omitted if it is not necessary (in case of MPLS/MAPOS frames for example).

(3) Encapsulation equipment with destination addresses (Fig.16)

It is the equipment which is usable as an edge node of communication between above LAN. The Internet may be used as a communications network.

(4) Home server with encapsulation function (Fig.17)

Home servers can offer IP encapsulation to establish home LANs. The home server checks the addresses of IP packets and encapsulation them using different internal addresses: different servers can be identified by different addresses. Server-1 in Fig.17 has external address "B1" and Internal address Y1.

5. Conclusion

We have discussed the major information security technologies and related communication technologies made possible by the IP network OBN. The idea of the address separation offered by OBN is effective as a countermeasure to DoS (Denial of Service) attacks against entities within the network.

Communication companies may register terminal addresses of enterprise users with an edge node. This makes it easy to charge users, and well handle multicast communication services.

OBN is allowed as a Type 1 telecommunication business in Japan (the same as telephone business on PSTN), and is being used by many enterprises. CALS of Defense Agency of Japan uses OBN to make its own particular closed IP network.

We are considering an IP telephone system based on the No.7 common channel signaling system(see: References 3 and 4).

Acknowledgement:

We would like to thank Mr. Sakai, the Executive Director of the Distribution Systems Research Institute, for the policy of promoting OBN.

References:

(1)Furukawa, Miyaguchi, "Discussion 4 on Extension of Business-oriented IP Network (OBN)", Technical report of IEICE TM99-21 (1999-07) (in Japanese)

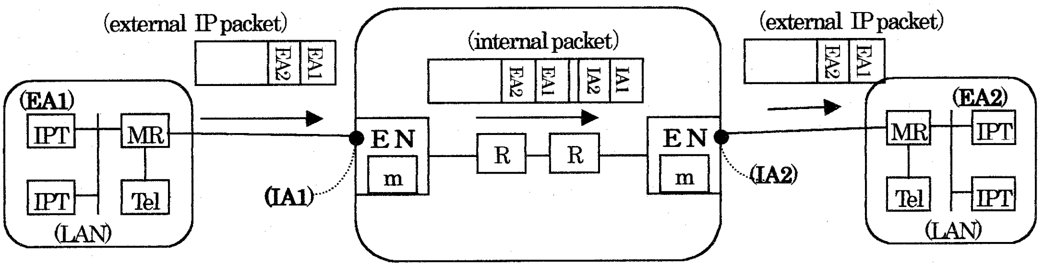
(2) OBN,http://www.obn.dsri-dcc.or.jp

(3)Furukawa, Miyaguchi, "How to introduce Common Channel Signaling system to IP network (Discussion-1)", Technical report of IEICE. IN2004 (2001-5) (in Japanese)

(4)Furukawa, Miyaguchi, "How to introduce Common Channel Signaling system to IP network (Discussion-2)", Technical report of IEICE. IN2019 (2001-6) (in Japanese)

Note-1: Three common carriers, NTT-COM, NTT-PC, and JT are currently providing OBN service (July 2001). OBN service began in January 1997 and consisted of IP communication service (intra-nets); it was expanded to IP communication between different companies(extra-nets) in 1999.

Note-2: The Distribution Systems Research Institute issued basic design of specifications of authorization communication system for credit cards in the 1980's. One of division of NTT implemented the system and has begun commercial services.



MR: Media router(in future), EN: Edge Node EA / IA: External / Internal address

m: registration of terminal address

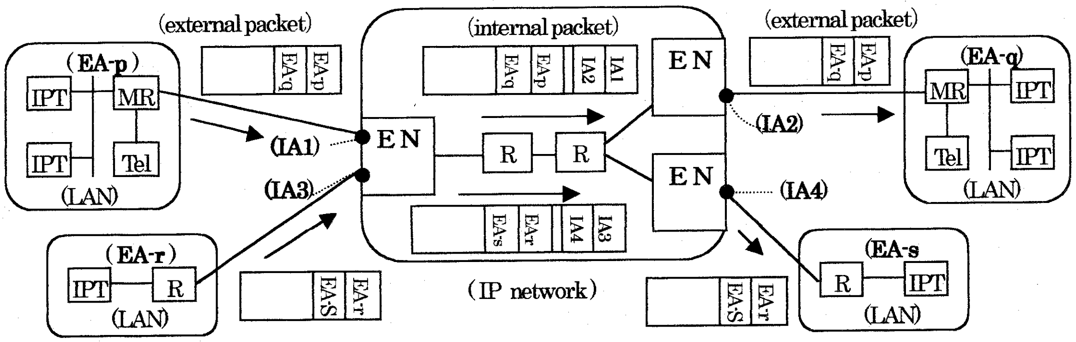
(Case: address area of packet observed)

Fig.1 Internal packet including sender address(IA1 in Fig.) and receiver address(IA2)

Record-1 :	IA1	EA2	EA1	IA2		
Record-2 :	IA1	MSK2	EA2n	MSK1	EA1n	IA2
Record-3 :	IA1	IA2				
Record-4 :	IA1	EA2	IA2			
Record-5 :	IA1	MSK2	EA2n	IA2		

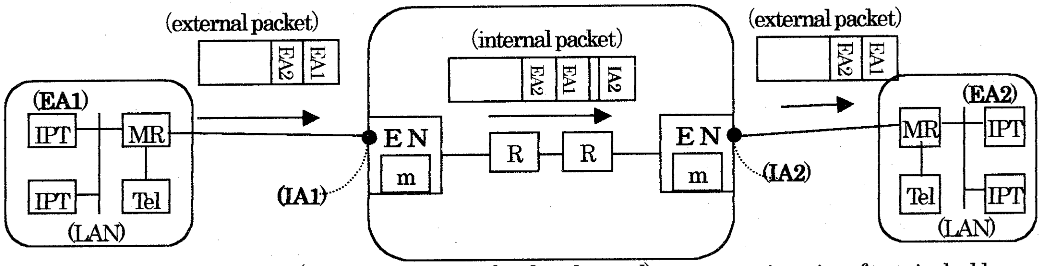
1:sender, 2:receiver,
IA:Internal Address
EA:External Address
MSK:Mask

Fig.2 Various types of communication records (to be set in edge node)



(Case: address area of packet not observed)

Fig.3 An IP communication network formed by combining virtual dedicated lines



(Case: address area of packet observed) m: registration of terminal addresses

Fig.4 Internal packet including destination internal address (not source internal address)

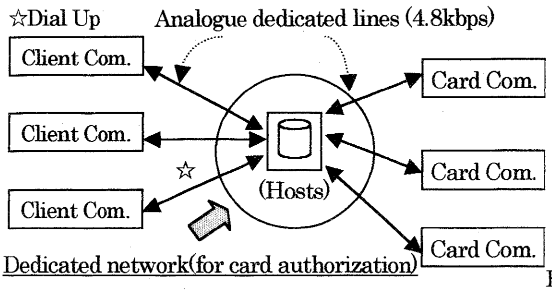
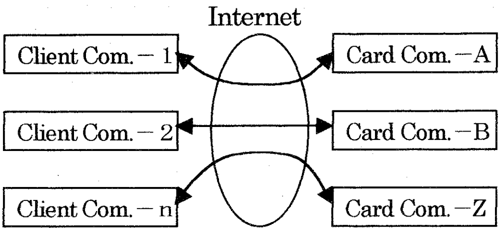


Fig.5 An authorization communication system



Responsibility for network obstacles? weak to DoS ?

Fig.6 Card authorization through Internet

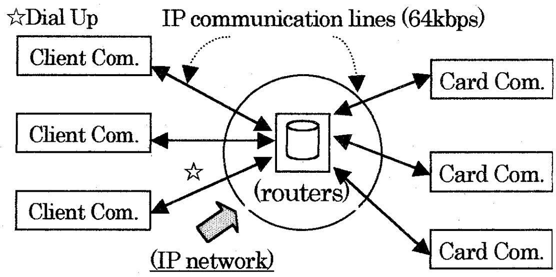


Fig.7 New authorization communication system

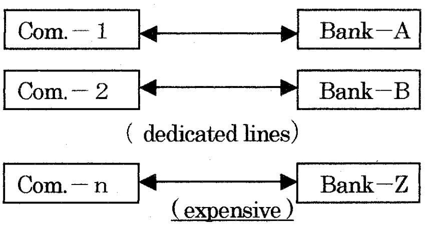
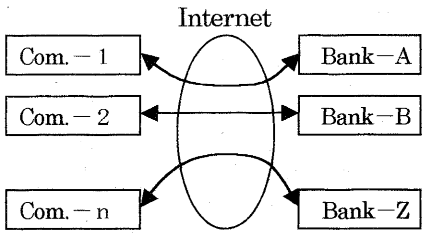


Fig.8 Communication through dedicated lines



Responsibility for communication troubles ?

Weak to Dos

Fig.9 Communications between Companies and Banks

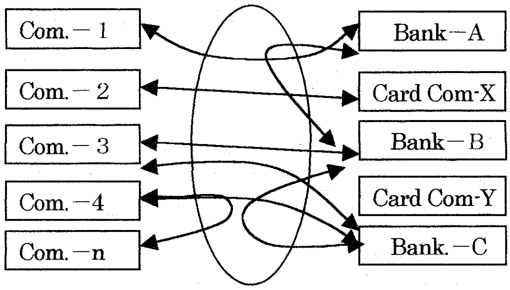
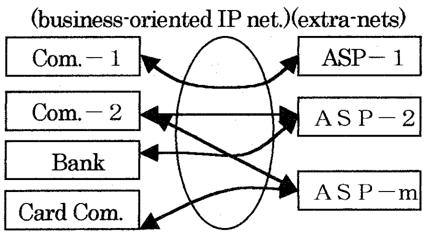
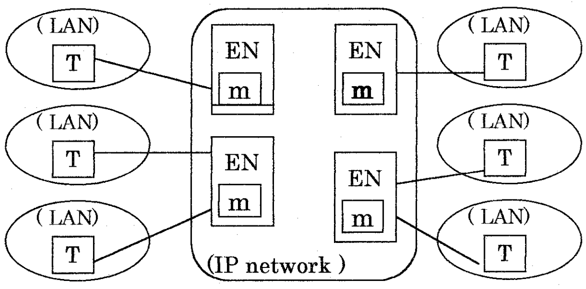


Fig.10 Business-oriented IP network (extra-nets)



ASP including bank and card campany

Fig.11 Secure com. environment for ASPs



T:terminal, EN:edge node, m: address registration

Fig.13 Multicast with registration of terminal address

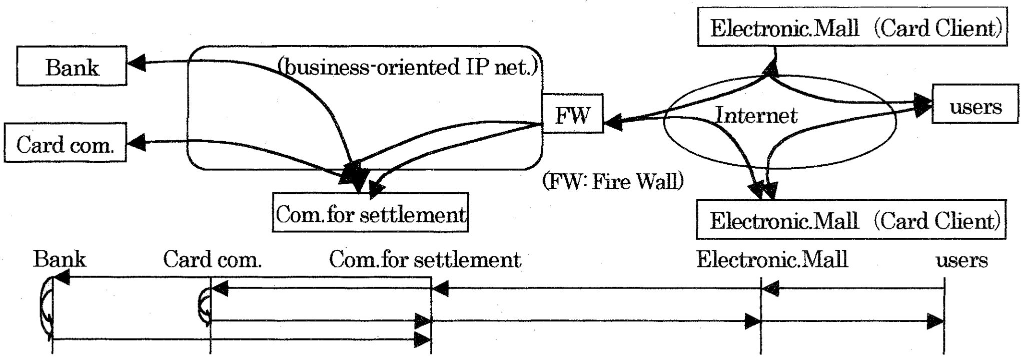
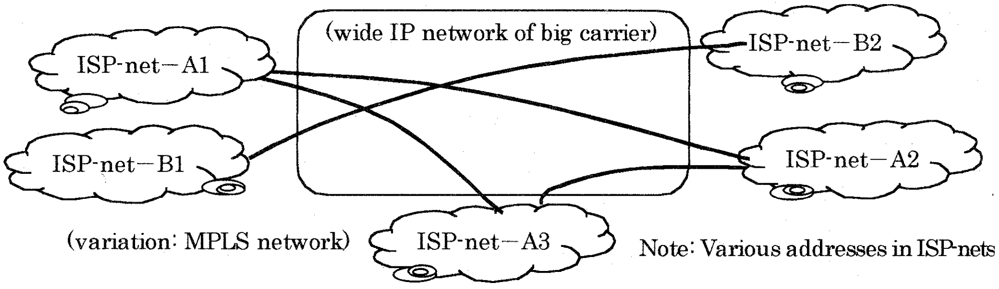
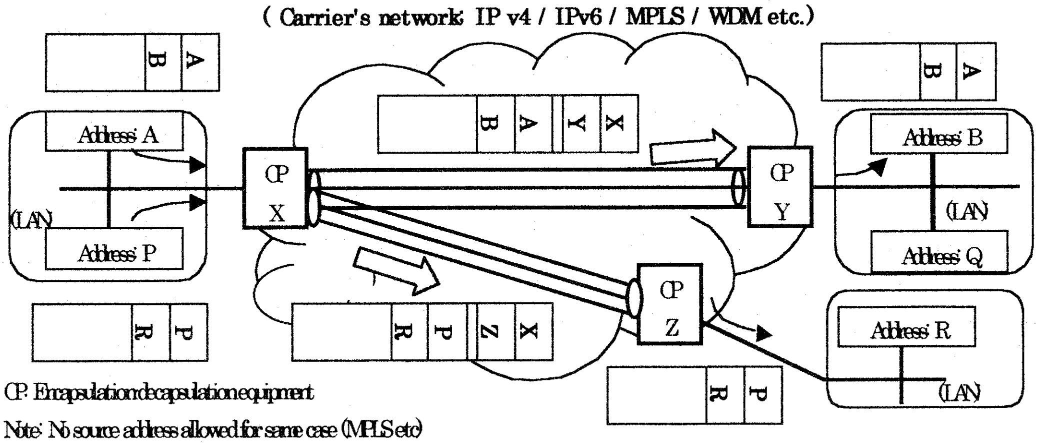


Fig.12 An electronic settlement for Internet Mall through business-oriented IP network


(wide IP network of big carrier)
ISP-net－A1
ISP-net－B2
ISP-net－B1
ISP-net－A2
(variation: MPLS network)
ISP-net－A3
Note: Various addresses in ISP-nets

(Case-1: address area of packet observed, Case-2: address area of packet not observed)

Fig.14 Connection service between ISP nets using encapsulation technique(input: IPpacket/MAC frame)

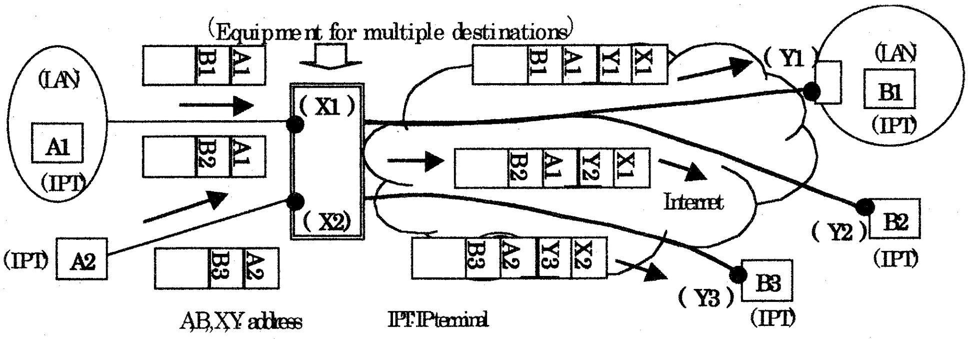


CP: Encapsulation/decapsulation equipment

Note: No source address allowed for same case (MPLS etc)

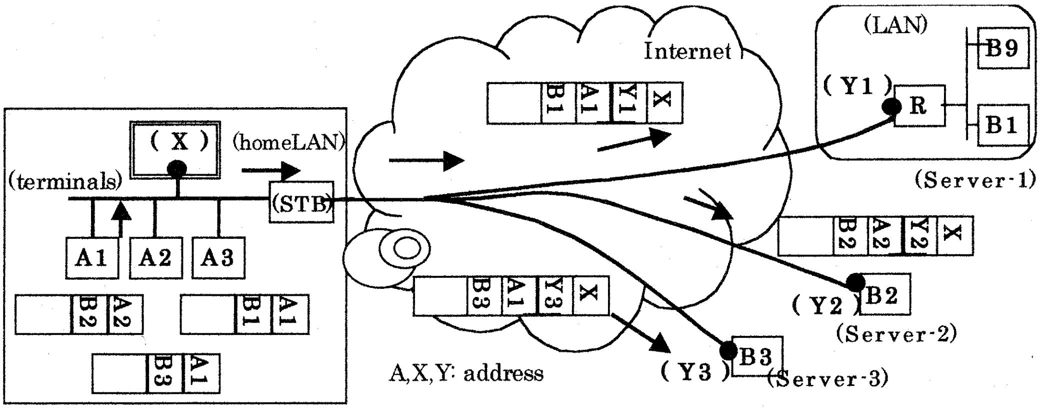
(Case-1: address area of packet observed, Case-2: address area of packet not observed)

Fig.15 Network using encapsulation technique where input packets are Ethernet frame (MAC frame)



(Case: address area of packet observed)

Fig.16 Equipment for multiple destinations and its communication environment



(Case: address area of packet observed)

Fig.17 Home Server with encapsulation for multiple destinations