University of
Waterloo Research Institute

The Interconnection of Local Area Networks with Public Data Networks

July 1983

sponsored by
Department of Communications
under
Department of Supply and Services
Contract No. 23SU.36100-1-0167

DOC CONTRACTOR REPORT

DEPARTMENT OF COMMUNICATIONS - OTTAWA - CANADA

COMMUNICATIONS SYSTEMS RESEARCH AND DEVELOPMENT

TITLE: THE INTERCONNECTION OF LOCAL AREA NETWORKS WITH PUBLIC DATA NETWORKS

AUTHOR(S): VIC DICICCIO
ERIC MANNING

ISSUED BY CONTRACTOR AS REPORT NO: FINAL

CONTRACTOR: UNIVERSITY OF WATERLOO
INSTITUTE FOR COMPUTER RESEARCH
COMPUTER COMMUNICATIONS NETWORKS GROUP

DEPARTMENT OF SUPPLY AND SERVICES CONTRACT NO: 23SU.36100-1-0167

DOC SCIENTIFIC AUTHORITY: B.H. HO

CLASSIFICATION: UNCLASSIFIED

DATE: July 1983

THE INTERCONNECTION OF LOCAL AREA NETWORKS AND PUBLIC DATA NETWORKS

EXECUTIVE SUMMARY

As Local Area Networks (LANs) begin to proliferate, there will be increasing pressure to interconnect them with public packet-switched data networks (PDNs) such as Datapac and Infoswitch. Such interconnection will allow LAN users much less expensive and more convenient access to the internationally interconnnected PDN networks than if the LAN users subscribed to a PDN as individual users. Also, PDNs will form a long haul transport network among LAN users on remotely located LANs.

The interconnection of private LANs to PDNs will require gateway nodes to provide a means for the transmission of data while satisfying the protocol requirements of both networks. A successful gateway design must achieve an appropriate trade-off among the following principles:

a) The amount of change required to existing networks for the provision of interconnection must be minimized.

b) The impact on intranet traffic by provisions introduced to permit internetworking should be minimized.

c) the internetwork services provided (datagrams, X.29 terminal handling, etc.) should be chosen to be similar to those services which LAN and PDN users use for

intranet traffic.

d) Users who do not wish to use internetwork services should not have to implement any new or changed protocols because of changes introduced in the network to facilitate internetworking.

e) The design should comply with CCITT Recommendations wherever possible and sensible.

f) The design should adopt the Open System Interconnection model as described in CCITT Draft Recommendation X.200 - Reference Model of Open Systems Interconnection for CCITT Applications - in planning protocol architectures.

An internetwork strategy requires the specification of three factors which together characterize the design of the gateway: the internetwork service level, the level of interconnection of the gateway and the level of service of the gateway. The internetwork service level is the type of service (eg. unreliable datagrams, reliable datagrams or virtual circuits) available to users on interconnected networks. The level of interconnection of the gateway specifies whether the gateway connects to each network as a network switching node (node level interconnection) or as a host (host level interconnection). Node level interconnection is impractical; we suggest only host level interconnection. The level of service specifies the type of service used in each individual network to transmit data among internetwork users. The level of service may be different or of a lower level than the internetwork service level if an end-to-end protocol is implemented at the source and destination network nodes, so that the end-to-end protocol provides the desired internetwork service level.

Three approaches were devised for the interconnection of LANs with PDNs. These are: the stepwise approach using a transforming gateway; the endpoint approach based on the use of a common, internet, end-to-end protocol in the source and destination hosts; and the provision of internet service by a stepwise series of internetwork protocol entities using encapsulation/extraction.

The first approach provides internetwork service by employing a transforming gateway which maps a service in one net into the most similar service offered in the other net. For example, a gateway could transform the unreliable datagram service on an LAN, such as Ethernet, into the X.25 datagram service available on a PDN. This is accomplished by translating between functions of the network access protocols as much as possible. Functions of one network access protocol which have no analogue in the access protocol of the other net must be terminated; that is, the gateway must act as the reciprocating protocol entity for that function.

This first approach has an important advantage over the other two approaches. Because the gateway transforms services already available on the two networks to provide the internetwork service, the internetwork service appears to a host to be as similar as possible to the intranetwork service. Therefore, the users need to implement none or only a minimum number of new protocol functions to use the internetwork service.

If an internetwork strategy which requires the hosts to implement an internetwork protocol entity is chosen, problems with stop-start mode DTEs may ensue. Since a terminal cannot implement a protocol unless it is intelligent, the Packet Assembler-Disassemblers (or PADs, such as the Datapac NIMs) would be required to implement the new internetwork protocol. This may be very difficult, since the PADs have already been developed and are in service.

The third interconnection strategy, based on an internet protocol entity between levels 3 and 4, deviates from the Open Systems Interconnection Reference Model. The internet entity recognizes internetwork addresses, performs internetwork routing, fragments and reassembles packets and generally encapsulates data in the network level protocol format of the networks to which it is attached. These functions are not normally provided either by level 3 or level 4.

In summary, the stepwise and transforming gateway approach offers a number of advantages over other strategies and is a first choice.

Although the interconnection strategies described in this report were developed initially for bus LANs (in fact, bus LANs are used as examples in the diagrams), the functions which must be provided by the gateway are identical if ring LANs or most types of star LANs are substituted. Similarly, the results also apply to these types of LANs.

PABXs which offer features for the digital transmission of data do not require gateway translations of the types described in this report. The PABX can provide the subscriber with a switched digital circuit directly to an X.25 Front End or a transceiver on the target LAN. Hence, PABXs should be simple to interconnect with PDNs and other LANs. Other advantages of PABXs include: they are designed to interconnect with the telephone system; they may use existing wiring; they not only provide data service but also telephone service; and they are reliable, flexible and expandable. Therefore, PABXs will be a very significant type of LAN.

Internetwork addressing and routing were examined in detail. CCITT Recommendation X.121 is a numbering plan which provides an address scheme for internationally interconnected PDNs, but it is inadequate to provide addressing for the thousands, or hundreds of thousands, of LANs which may be attached to PDNs in the future.

Two addressing schemes which do provide for private LANs have been suggested recently. These are the IEEE 802 HILI Subcommittee "X.122" proposal, and the March 1, 1982

Canadian CCITT Proposal for Private/Public Network Interworking. Both of these plans exhibit some operational impracticalities related to internetwork routing which are explained in Section 5.

We have proposed an Extended, 26-digit, X.121 addressing plan, which overcomes all of the disadvantages of the other techniques. The host level gateway to each private LAN is assigned a normal, 14-digit, X.121 international address. Each host on that LAN has its own international address comprised of the gateway address with a 48-bit (or less) suffix. This suffix can be the host's intranetwork address on the LAN.

Extended, 26-digit X.121 permits easy international routing. PDNs and X.75 STEs can perform routing based on the first 14 digits of the address, just as they do now. For hosts on PDNs, the address could be truncated to a normal 14-digit X.121 address, or the extra digits could be used to identify a particular process, computer port, or Service Access Point on the host. Furthermore, this extended X.121 scheme accommodates the long 48-bit intranet addresses which are used by Ethernet and which are under discussion in the IEEE 802 Local Area Networking Committee.

TABLE OF CONTENTS

THE INTERCONNECTION OF LOCAL AREA NETWORKS
AND PUBLIC DATA NETWORKS

1. INTRODUCTION

Office communications systems in the automated office of the future will be based on Local Area Networks (LANs). These will connect terminals and workstations with each other and with computers offering specialized services such as bulk file storage, program execution requiring very large amounts of memory, and particular data bases. The LANs will be privately owned and will provide intra and inter office communications over distances up to a few kilometres.

As LANs begin to proliferate, there will be immediate pressure to interconnect them with the public "long haul" packet switched data networks (PDNs) such as Datapac and Infoswitch. There are three motivations for the interconnection of LANs and PDNs.

1. There is almost certainly a cost reduction achievable by connecting an entire LAN to the PDN at a single interface, rather than individually connecting each terminal, workstation and computer which requires access to the PDN.

2. The terminals, workstations and computers connected to the LAN can interwork with subscribers on the PDN to obtain specialized computer services. Furthermore, if the PDN has international interconnections

with other national PDNs, then international interworking is possible.

3. A terminal, workstation or computer on an LAN may interwork with a terminal, workstation or computer on another LAN over the PDN. This is certainly of interest to corporations with offices in several cities.

   Viewed another way, LANs are certain to become an additional and pervasive Local Distribution Facility for public data networks, easily surpassing dial-up PAD access in importance.

At each interconnection point between a local network and a public data network, a specialized computer node referred to as a gateway will be required. Its function is to satisfy the protocol requirements of both networks while providing a means for the transmission of data between the two networks.

If two networks connected by a gateway use very similar protocols and offer similar services to the user (e.g. datagrams, fast select, virual calls, etc.), then the gateway's functions are quite simple and it must only translate between the few differences which exist. Also, the users would perceive very little difference between the services offered on their own net and the internetwork services. The gateway would be very unobtrusive.

However, a gateway which interconnects two dissimilar networks must terminate elements of the protocol in either network which cannot be transformed or translated into elements in the other network in a meaningful fashion [DICI79]. Of the data services available to the user on his network only a subset may be available for internetwork use over this terminating gateway.

Since about 1976, there has been a great deal of research into gateways for the interconnection of PDNs. This work led to the specification of X.75, the CCITT interface standard for the interconnection of PDNs. Initially, network adminstrations experimented with non-standardized host level gateways (typically based on a single minicomputer), however, these are now being replaced by X.75 gateways [UNSOY81]. This study will draw heavily on the insights into gateway design gained by interconnecting PDNs.

Initially, the interconnection of LANs with PDNs will be accomplished in a very ad hoc manner, using gateway boxes supplied by the individual LAN manufacturers. These gateway boxes will provide translations between the protocols used on the LANs and the access protocol of the PDN (which is X.25 in almost all cases). It is certain that the LAN vendors will adopt various means for solving gateway problems such as subscriber addressing, flow control and higher level protocol issues. Most of these solutions will require manual user operations, that is, the interworking of a user apparatus on the LAN with one on the PDN will not happen automatically in a manner transparent to both users. If these interconnections evolve without a broad agreement on interconnection principles, the result will be a large number of subscribers who can interwork but must use various vendors' gateways, each of which requires a different style or format of user intervention.

This unfortunate and ultimately unworkable scenario can be prevented if some guidelines, and perhaps a special interface for the interconnection of private LANs to PDNs, are developed.

Although outside the scope of this study, it is worth noting that private networks other than local area networks (for example, public networks for weather information and corporate networks supporting applications such as order entry, airline reservations and electronic funds transfer) will seek interconnection with PDNs to achieve interworking with subscribers on PDNs, LANs and other private networks. Hopefully some of the techniques developed in this study for LANs can be applied or adapted to other private network interconnections.

2. A SUMMARY OF LOCAL AREA NETWORK ARCHITECTURES AND PROTOCOLS

Local area network topologies include the star, ring and bus. Each is described briefly below. Data communications capabilities of PABXs, which are a star topology network, are also discussed.

2.1 Star Local Area Networks

In a star network, each user apparatus (terminal, workstation or computer) is individually connected to a central node which performs switching of data or circuits among the subscribers. It is impossible to make general assumptions about the protocols used with this architecture, since the central node may be a simple as a character-at-a-time data switch with in-band or out-of-band addressing. The gateway to a PDN should appear as a special purpose "user apparatus" (in this case, a computer) connected to the central node like the other user equipment. A user who wishes to interwork will first be required to enter into a dialogue with the gateway to provide the destination subscriber address and any parameters for protocol translation.

Examples of local networks organized as stars include the Gandalf PACX network, the Hubnet network (developed by the Computer Systems Research Group at the University of Toronto) and the Fibernet II star - configured Ethernet developed at Xerox PARC. The use of PABX networks for data communications is discussed in the next section.

The Gandalf PACX network provides low speed circuit-switched connections through a central switch (Computer Exchange). The users are classified into two groups: "connection originators" which are generally users at terminals and "connection destinations" which are usually computer ports. Since an originator cannot call another originator, the network is really only useful for terminal to computer communications purposes. It uses inexpensive digital baseband signalling boxes at each station.

Hubnet is a high data rate (approximately 50 Mbps) network based on a central switch (the "hub") which when idle, senses incoming data then broadcasts it to all users while simultaneously blocking all other users with data to send. Fibre optics cables are used to interconnect microprocessor based subscriber interface units to the hub. Hubs may be organized in a hierarchical structure to support larger user populations and to provide multiplexing to reduce the amount of fibre required. However, only a single user may transmit on the network at any time.

The Xerox Fibernet II network [RAWSO82] is somewhat similar to Hubnet. It consists of an active repeater to which up to 25 transceivers are connected by duplex optical cables. If the net is idle when a transceiver transmits, the central repeater retransmits the optical signal to all transceivers. If two transceivers transmit simulataneously, the central repeater detects the collision and sends a special "collision signal" (2.5 MHz optical signal) to the transceivers.

The Fibernet II transceivers satisfy the Ethernet specifications at the transceiver cable interface to the station. (The station is typically connected to the transceiver by a special Ethernet interface board in the station's computer or intelligent terminal.)

Fibernet repeaters contain a back-plane which is actually an Ethernet. Repeaters may be bussed together using their back-plane Ethernets to create a network of up to 5 repeaters with a total of 125 transceivers.

In general, star networks tend to require more cable than bus topologies. Also, an additional user must be wired back to the central node; he cannot be serviced by installing a tap on a line which already passes his equipment. However, the user station equipment for network access can usually be made simpler than that of a bus or ring net, because the scheduling of network resources (i.e. deciding who transmits when) is performed at the central node instead of being distributed throughout the user sites. Some star network architectures do not offer all users equal opportunity at frequent intervals to transmit data, that is, they do not exhibit the property of fairness. Nevertheless, star networks will probably seize most of the market for LANs, largely because of the popularity of the use of PABXs for data communications.

2.2 Data Communications on PABXs

PBXs have historically performed, for voice, exactly those functions which we require LANs to perform for data. They permit direct connection of users' apparatus on a single premise without having to go through a common carrier public network. Also, they act as a concentrator to connect on-premise users' apparatus to the common carriers' public networks for both incoming and outgoing calls.

Recently, electronic PABXs which use digital transmission between the telephone and the PABX switch have been introduced. Switch manufacturers are also providing data services to the user which support data transmission among stations on the PABX, or from a station on the PABX to either an attached LAN or one of the public data network services.

The provision of data services on PABXs, when considered in combination with their flexibility, expandability and reliability, will make the PABX a very significant contender in the LAN market. PABXs can use existing wiring; they do not require the installation of new fibre or coaxial cable. Also, most installations which require an LAN also need telephone service. The PABX can fulfill both of these requirements.

The manufacturers who offer PABXs with data communications capabilities include AEL Microtel (on the GTD 1000), Mitel (SX 2000), Northern Telecom (SL-1 and SL-100), Plessy (K2), Anaconda Ericsson (MD 100) and Rolm (VLCBX). Typically, an electronic telephone set, containing a codec, is connected to the switch by 4 or 6 wires. The telephone set is the user's terminus for both voice and data transmission, which can usually be handled simultaneously. Most manufacturers currently provide asynchronous data transmission at speeds up to 19.2 Kbps and synchronous transmission at speeds up to 56 Kbps. Electrical interfaces such as RS-232-C and RS-449 are standard, and some manufacturers, including Mitel and Northern Telecom, offer connections using the X.25 network access protocol.

PABXs offer switched digital circuits to the subscriber. This simplifies the interconnection of PABXs with other LANs or with PDNs because a transforming gateway is not required; the PABX only needs to implement the access protocol of the attached network. The PABX subscriber should be able to give a PABX local number which would set up a data circuit directly to an X.25 Front End, or an LAN transceiver. The user may then proceed as if he was directly attached to the target network. Therefore, PABXs are well suited to interconnection; the interconnection strategies described in this report are not necessary and are not applicable to PABXs.

The PABX manufacturers will soon go beyond digital data switching to providing messaging systems (both data and voice) and even the transmission of slow scan, specially encoded video among subscribers.

The data communications speed available to a single subscriber on a PABX is not as high as is achievable on star LANs such as Hubnet, or on ring or bus LANs. Also, the circuit set-up time through a PABX may not be as fast as the delivery time of a frame or packet on the other types of networks. The speed issue may be of importance for communications among larger computers, or applications involving digitized video. Fast circuit set-up time and features such as broadcast to all stations are important in distributed processing systems. Therefore, for some applications, the data communications services provided on a PABX may not be as suitable as other types of LANs. However, for most current data communications needs, especially in offices, the data communication on PABXs appear ideal.

It is interesting to speculate on the suitability of PABX data services for networks of high performance computer workstations such as the Xerox Star or the Waterloo Port Workstation. Further experimentation with larger networks of such workstations installed in real user environments is needed to answer that question.

One of the advantages of PABXs is their typically high reliability. Telephone users are generally much less tolerant of downtime than computer users. Also, in some sense, the cost of data networking on a PABX is an incremental cost on top of the cost of a telephone system (which is virtually essential). For example, data networking may be introduced in an organization through the installation of a new PABX without requiring any new cabling. For these reasons data services on PABXs may dominate the local area network market.

2.3 Common Medium Networks: Ring Local Area Networks

In a ring network, each subscriber apparatus is connected to a node, and the nodes are connected by unidirectional links to form a closed ring. Each node receives messages or packets on its incoming link, checks their address fields to determine whether they are directed to that particular node and, if not, merely retransmits them on the outgoing link. The delay at each node may be as low as one to a few bit times.

Various control strategies have been developed to determine which node may transmit at any given time. These include out-of-band control signalling and three in-band techniques: control tokens, message slots, as used in the Cambridge ring [WILKE79], and register insertion, as used in the Distributed Loop Computer network (DLCN) at Ohio State [REAME].

Because of the ring architecture and well-defined transmission control strategies, it is possible to build rings with very low error rates. Therefore, they may not have as severe a requirement for error control, flow control and message sequencing between nodes as do buses and conventional packet switched networks. However, an OSI level 2 protocol between nodes on the ring would ensure reliable data transmission. (A level 2 protocol for use over both control token rings and contention buses is currently under study by the IEEE 802 committees [IEEE81].) Furthermore, some aspects of protocols in the higher levels, levels 3 through 7, will probably be required if the ring is to support a wide range of applications successfully. It is reasonable to perform most of the higher level protocol functions in the user equipment rather than in the node.

2.4 Common Medium Networks: Bus Local Area Networks

In a bus network, each subscriber apparatus interfaces with a network node as in the ring architecture, but each node contains a transceiver which broadcasts the data on a bi-directional transmission medium such as coaxial cable. Logically, the transmission medium connects the nodes in a linear series fashion, although they may actually be connected by an arbitrary unrooted tree of cable as long as a broadcast by any node can reach all other nodes.

In most bus networks, no provision is made for passing transmission control among the nodes in a well defined way. That is, there is no means to perform global scheduling of the access to the transmission medium by the transceivers.

Instead, a contention type of local scheduling strategy is adopted, such as Carrier Sense Multiple Access with Collision Detection (CSMA-CD), which is as used in Ethernet [METCA76] and the SYTEK network [SYTEK81]. CSMA-CD networks operate in the following way:

Each node is equipped with a full duplex transceiver. If a node has a packet to transmit, it first waits for the bus to become idle, and then transmits. However, due to the propagation delay of the cable, it cannot always know whether another node has already commenced transmission. Hence, as the node transmits the packet, it continuously compares the received data to the data being transmitted. If they are identical, the node continues to transmit. If they are not identical, then another node has also been transmitting and a data collision has occured. Each node ceases transmission upon detection of the collision and waits a random period of time before restarting the transmission. There are various schemes for determining the wait time, each of which attempts to minimize the chance of re-collision and thus maximize the throughput.

Mark and Todd have developed and implemented a Distributed Scheduling Multiple Access (DSMA) technique for a bus local net called WELNET [MARK80, TODD80]. Unlike CSMA-CD, which relies on locally derived scheduling information to control each station's contention for the bus, DSMA provides complete scheduling information to each transceiver on the network. In WELNET, a ring which is separate from the data bus is used to pass tokens to reserve slots on the bus for data transmission. As a result, the bus is totally conflict free and exhibits a delay-throughput performance very close to a perfect scheduling system. In effect, Welnet uses a token-passing ring for control purposes and a bus for user data.

2.5 A Comparison of Rings and Contention Bus Networks

Saltzer and Clark, in their paper entitled "Why a Ring?" [SALTZ81] point out two basic design distinctions between rings and buses:

1. access control by contention (in contention buses) versus tokens or slots (in rings), and

2. communication of data by broadcast (contention buses) versus point-to-point (in rings). (However rings can provide a broadcast <u>service</u> to their subscribers.)

Saltzer and Clark describe three advantages and three disadvantages of rings vis-a-vis contention buses:

1. Most contention buses have a significant analog component (the bus transceiver - media access unit) while ring repeater nodes can be designed to be completely digital.
2. Contention buses must have at most only one ground point on the coax shield to avoid transients. Since

the cable must be divided into sections for troubleshooting, Ethernet has chosen to have no ground point. This has created a safety hazard and has impeded safety certification.

3. Since it uses repeaters, a ring can be configured to span longer distances than a contention bus, because on a bus the propogation delay between the two most widely spaced stations limits the length.

4. Saltzer and Clark assert that, because a fibre optics tap has not been developed, contention bus systems cannot make use of fibre-optical cable. In fact, fibre optics taps have been developed, however, these tap couplers cannot couple light into the bus fibre in both directions simultaneously. Therefore, two bus fibres are used to provide bidirectional communications; one fibre for each direction. A fibre bus may be arranged in one of two ways: either each station transmits and listens in one direction on one fibre and in the other direction on the other fibre or all stations transmit upstream to a "head end" repeater on one fibre and listen to the repeater's output on the other fibre. The Canadian Department of National Defence, in cooperation with Sperry Univac and Canstar Communications, has designed a network of the former type [JOHNS82]. Bell Telephone laboratories is experimenting with buses of the latter type

[ALBAN82].

Albanese, Revett and Davis did encounter some limitations in current fibre optic technology while designing the DND fibre bus. They could not replicate their current triaxial cable network with 64 taps; because of fibre optic technology limitations they had to reconfigure their network to 32 taps. Also, to obtain high performance asymmetric tap couplers they found it necessary to evaluate special developmental fibres.

5. The contention bus has few or no active components whose failure can disrupt the net.
6. The contention bus physical medium is easier to install than a loop topology.

2.6 Issues in the Choice of an LAN

The selection of an LAN is a multi-dimensional decision, which clearly involves a detailed knowledge of the requirements for communications in the environment in which the LAN is to be installed. An LAN characteristic such as distance may be a pivotal issue for network comparison for one application, and yet in another scenario the requirements for a network may be totally insensitive to the maximum distances different networks can support. This section merely discusses some properties of LANs which are focal points for network planning; the list of properties is not exclusive and the authors have not made a comparison of the available LANs.

Cost

For bus and ring LANs, the cost of the transceiver or repeater at each station is typically in the range of $1000 to $5000. Added to this is the cost of the transmission medium used (coax, twisted pair or fibre). Baseband networks should be less expensive than broadband nets, since many of the latter incorporate a frequency agile modem in the transceiver.

The development of VLSI chips (or small chip sets) for LAN transceivers will cause a great reduction in cost. The IEEE 802 local net standards activities should soon culminate in the introduction of standard chips.

The cost per user of star networks varies considerably depending on the cost and capacity of the central switch. On a Gandalf PACX system, the per user cost is about $300 for the digital signalling box and the central switch. (The cost of the circuit from the user to the central switch is additional.) Most PABX systems are probably on the order of $1000 per user.

Different networks have different incremental costs related to growth, especially if the network has components shared by several users. When a shared component is saturated, the next growth increment may be very expensive.

Distance

The maximum total length for baseband bus LANs is on the order of 1 km. Broadband bus LANs can frequently support longer distances; they are usually rated in db loss, rather than distance, since they are likely to include CATV bidirectional amplifiers spaced throughout the network to regenerate the signals. Maximum distances may be in the range of 2 to 40 km, although long distances introduce performance problems if CSMA-CD is used, because of the long period required to sense collisions and their increased likelihood. The longer broadband LANs usually operate at lower signalling rates, which reduces the importance of propagation delay (network length) vis-a-vis transmission time for a packet.

As a rough rule of thumb, a single baseband bus LAN can be used in a building, while a single broadband bus LAN can be used for small group of buildings such as a campus or industrial park.

Ring LANs are sensitive to the distance between each pair of adjacent stations, however, additional repeaters can be introduced on interstation links to provide signal regeneration. The delay of data propagation may be the determining factor for the maximum length allowable for each link.

The maximum distance allowable between the central switch and users of star LANs is determined by the drivers used at the user stations and central switch, and can vary considerably. Many PABXs can support distances of a few to several kilometers.

Throughput

Bus LANs are based on the dynamic allocation of transmission capacity according to a multiple access technique such as CSMA-CD or DSMA. Most bus LANs have a raw data transmission rate (data signalling rate) of 1 to 10 Mbps. However, if the bus uses a contention multiple access technique, such as CSMA-CD, the data collisions, and the time required for their resolution, waste significant fractions of network capacity. Unfortunately, the likelihood of collisions increases proportionally to the amount of data load offered to the network. Therefore, contention buses work best at light loads.

At heavier loads, methods which resolve contention without wasting time (i.e. conflict-free systems) provide a greater throughput. These include DSMA (used in Waterloo WELNET), BRAM (Broadcast Recognizing Access Method, used at the University of Minnesota) and Hubnet.

Ring networks can usually support very high data rates, since the data transmission is from repeater to repeater in a simple point-to-point fashion. The experimental Cambridge Ring, described by Wilkes, runs at 10 Mbps. Because access to transmission is controlled by conflict free techniques on rings (tokens, slots or register insertion), there is no bandwidth wasted in collisions. Therefore, rings can support throughputs close to their maximum capacities, minus some protocol overhead.

Most PABXs provide data rates of 19.2 Kbps asynchronous and 56 Kbps synchronous. These rates are supported by various forms of circuit switching, therefore, the full data capacity of the circuit is available to the user.

Interfaces to User Equipment

Many bus LANs offer transceivers which interface with the user equipment via RS-232-C or RS-422 terminal interfaces. (Of course, computer terminal ports can also be connected to these.) Other bus LANs offer transceivers which can attach directly to a computer bus to perform Direct Memory Access (DMA) transfers. Greater flexibility results if both interfaces are available for a given LAN; this can be achieved perhaps through the use of transceivers from different manufacturers with different interfaces to user equipment. However, to combine transceivers from different manufacturers, it is necessary that they are designed for a standard bus network using a standard medium access protocol and a standard level 2 link protocol (if one is used). This requirement emphasizes the importance of LAN standards such as the DEC-Intel-Xerox Ethernet and IEEE 802, to ensure the flexibility of system configuration which is made possible only by the compatibility of equipment from several vendors.

Ring LANs attach directly to individual vendors' computer equipment, therefore a ring which is sold to interconnect IBM Series 1 computers cannot be used to interconnect Prime computers.

PABXs, and most other star networks, provide user interfaces of the terminal variety, such as RS-232-C and RS-422. Some PABXs are providing X.25 interfaces. Many of the non-PABX star networks are compatible with X.21.

Expandability

All LANs permit incremental growth up to the maximum number of users for which the network was designed. If the planner envisions exceeding the network's capacity, it may be important to choose a network which can be easily bridged to a clone of itself using interconnection hardware provided by the vendor. For example, does the manufacturer of a particular bus LAN offer gateways or bridges to easily allow the interconnection of multiple segments of the network?

Other Features

The selection of a particular LAN may be determined by the need for non-data services which are more easily provided by one LAN than another. For example, broadband bus LAN systems also permit the transmission of video, unlike baseband bus LANs.

3. PRINCIPLES FOR NETWORK INTERCONNECTION

Several alternative strategies exist for the interconnection of local area networks to public data networks. Two obvious criteria which can be used to choose among them are the performance and the cost of the interconnection - the gateway. However, there are other less quantitative principles or ideals which can be used to compare the relative merits of various interconnection strategies, and can be used as goals for the development of new interconnection techniques.

Unfortunately, some of these principles conflict with each other when they are applied to practical systems. That does not detract from their usefulness, however; it is important for a gateway designer to appreciate the negative consequences which result from basic decisions on interconnection architecture and protocol.

A successful interconnection strategy must achieve an appropriate trade-off among the following principles.

1. The amount of change required to existing networks for the provision of interconnection should be minimized. Interconnection strategies which require extensive changes in network protocols or architecture will be both costly and slow to gain acceptance. Furthermore, it may be very difficult to coordinate the efforts of more than one network administration so that the new

features introduced for internetworking are identical.

2. One effect of any changes made in network access protocols to support internetworking is a usual decrease in the efficiency of intranet traffic. This impact on intranet traffic should be minimized so that users who do not interwork are not unduly penalized by the features introduced to support those who do [TANEN81].

3. The internetwork services provided, for users who wish to interwork, may include datagrams, virtual circuits, X.29 terminal handling, file transfer services, etc. It is desirable to choose internetwork services which are similar to those which are routinely used by LAN and PDN users for intranetwork traffic. For example, if User A, on a local area net which provides only unreliable datagram service wishes to interwork with User B on an X.25-based data network, those users are least inconvenienced if User A sends and receives datagrams to communicate with User B, and User B obtains a virtual circuit to communicate with user A. These seemingly incompatible requirements can be met by performing a translation between the virtual call and datagrams at the gateway.

It would be very difficult for User A if this principle was violated and he was forced to use virtual calls as the internetwork service, since he would have to implement X.25 for internetwork use only. It may be easier for User B to adapt to a datagram internetwork service, although it will require a change in User B's host software.

4. Users who wish to use internetwork services may have to implement new protocols or change the existing network access protocol in their hosts. However, users who do not use internetwork services should not have to implement any new or changed protocols because of changes introduced in the network to facilitate internetworking.

5. It is desirable to comply with CCITT Recommendations, wherever it is possible and sensible to do so, in the planning for network interconnection. Also, the architecture of the Open System Interconnection model should be adopted in planning gateway and interconnection protocols.

The principles listed above tend to preserve the status quo and protect users from experiencing unnecessary change due to the introduction of internetworking. However, if a large fraction of the current users of intranet services are eager to use internetwork services, and if the network administration has determined that it is in its best interests to implement major changes, then the principles described above may be relaxed.

4. STRATEGIES FOR THE PROVISION OF INTERNETWORK SERVICES OVER INTERCONNECTED NETWORKS

The choice of a gateway architecture cannot be made independently of the services to be provided to internetwork users and the protocol requirements which a particular gateway design may impose on the users' hosts. In this section, three different interconnection strategies are presented and compared. These three strategies are actually generic types which span the range of useful network interconnections and can be used to classify specific gateways.

An internetworking strategy requires the specification of the following three determining factors: the internetwork service level, the level of interconnection of the gateway and the level of service of the gateway.

4.1 Internetwork Service

The internetwork service is, more precisely, the type of internetwork service which is available to users on interconnected networks. This service may be, for example, unreliable datagrams, reliable datagrams, or virtual circuits. In order to comply with the third principle for interconnection presented in Section 3, it is desirable from the users' viewpoint if the internetwork service is the same as one of the intranetwork services. If not, the user must make a distinction between protocols or procedures used for internetwork communications from those used for intranetwork communication.

4.2 Level of Interconnection

The level of interconnection of the gateway has been called the local net interface level by Sunshine [SUNSH77]. It specifies whether the gateway connects to each network as a network switching node (node level interconnection) or as a host (host level interconnection).

If node level interconnection is chosen, from each network's viewpoint the gateway appears to be a network node. The two networks are "extended" into each other at the subnetwork level, and the gateway must translate between the two networKs' internal internode protocol (unless, of course, the two networks use the same internal internode protocol, which is unlikely in the case of a PDN and an LACN).

An interconnection strategy based on node level interconnection is impractical for the interconnectiion of an LACN to a PDN, for a number of reasons. First, it may not be possible for a gateway to appear to be a switching node on all local area nets. What is required, for example, to connect a gateway as a switching node on a star architecture LAN based on an augmented PABX? Secondly, a node level interconnection gateway would require reprogramming whenever the PDN network administration decided to modify their internal switch-to-switch protocol. In fact, one can imagine changes in the PDN internode protocol which might make the translation between the two networks' internode protocols impossible, so that the gateway would have to be disconnected and the availability of internetwork service to those LAN users would be discontinued. Thirdly, significant addressing changes would be required in each network's internode protocol to permit the signalling and recognition of internet addresses. This is a breach of the first principle for network interconnection presented in section 3.

In summary, it is not sensible for a PDN to offer its own internal internode protocol as an interface for the interconnection of private networks. Therefore, no strategies based on node level interconnection will be discussed in this study.

In host level interconnections, the gateway attaches to each network as a host, and appears to the network as a source and/or destination of network services (such as datagrams or virtual calls).

4.3 Level of Service

The level of service, as defined by Sunshine [SUNSH77], specifies the type of service used in each individual network to transmit data among internetwork users. The level of service may be different or of a lower level than the internetwork service level if an end-to-end protocol is implemented at the source and destination network nodes, so that the end-to-end protocol provides the desired internetwork service level.

An example is shown in figure 4.1. The level of service used in the individual networks and thus by the gateways is unreliable datagrams in the local area networks and X.25 datagrams in the PDN, although the end-to-end protocol entities supply functions such as sequencing of packets, duplicate packet detection, error correction and call establishment and clearing. In this case, the users have virtual circuit internetwork service which has been provided in an <u>endpoint</u> fashion.

An example of the <u>stepwise</u> provision of virtual circuit internetwork service using a virtual circuit level of service at the gateways is shown in figure 4.2. Internetwork virtual circuit service is provided to user hosts A and B by the concatenation of virtual circuit segments using the virtual circuit service available in each of the three networks.

4.4 Strategy 1: Stepwise with Translating/Terminating Gateway

One approach to the provision of internetwork services relies on a concatenation of similar services in each network to provide the internetwork service, as discussed above. Of course, the internetwork service level which results will be the same as the level of service used in the individual networks, by definition.

In most cases, the services available in LANs and PDNs which are to be interconnected using this stepwise approach

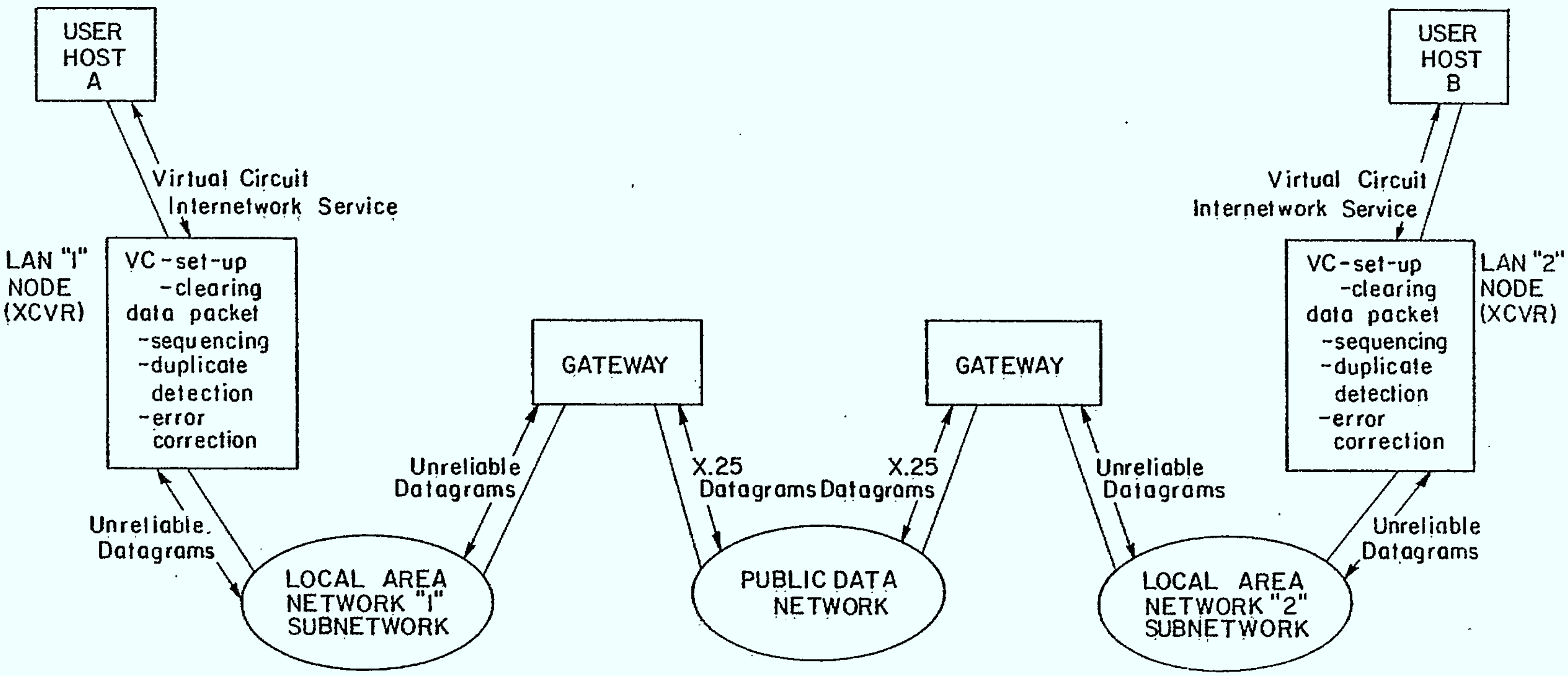


FIGURE 4.1 Virtual Circuit Internetwork Service Provided by the Endpoint Approach based on a Datagram Service Level

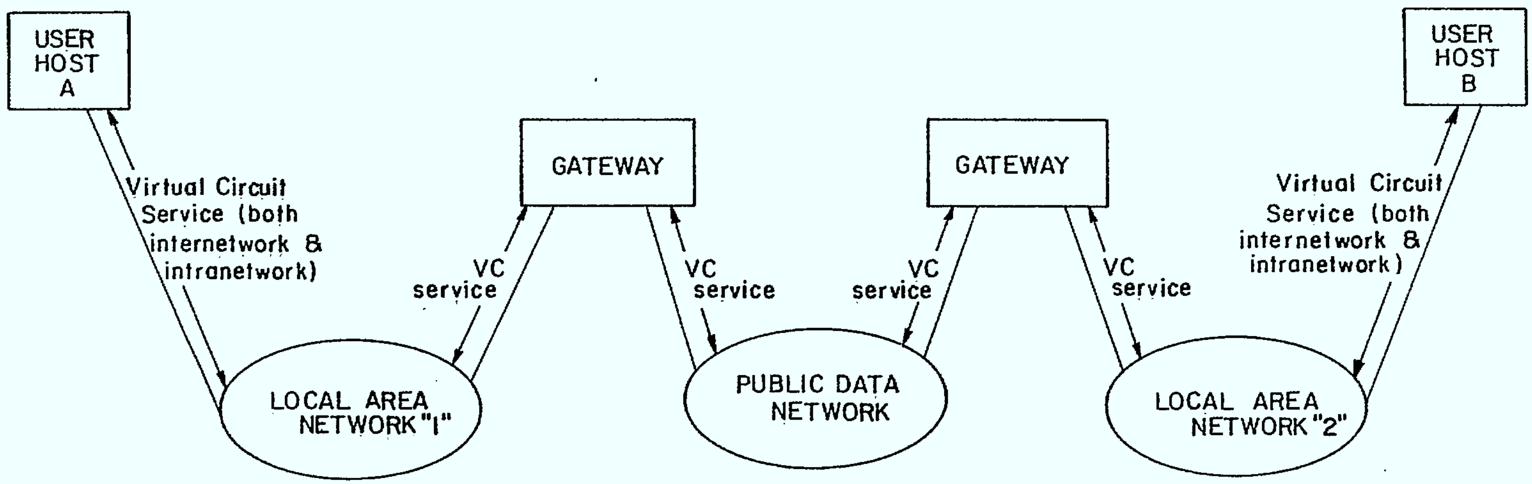


FIGURE 4.2 Virtual Circuit Internetwork Service Provided by the Stepwise Approach based on a Virtual Circuit Service Level

are similar but not identical. For example, an LAN may support virtual calls, but may use a simpler (and perhaps, more restrictive) access protocol than X.25. Similarly, LANs and PDNs may vary in the quality of datagram service which each provides, and the length of data packet which each may support. The gateway acts as a converter in such cases, by transforming the service available in one network into the service available on the other and vice versa. Some portions of a service may be passed transparently, by the gateway, between the two networks. Other functions of a network access protocol on one network may be translated, at the gateway, into different but equivalent, functions of the access protocol for the other network. Still other functions may be terminated at the gateway if they have no meaning or corresponding equivalent partners in the other network.

If the services being transformed at the gateway make a fortuitous match, then the gateway is transparent to most of the functions of the network access protocol and translates the rest; no functions are terminated at the gateway. This tends to produce an internetwork service which appears, to the users, to be identical or very similar to their intranetwork services.

The CCITT strategy for the interconnection of PDNs using the X.75 interface is based on the stepwise provision of virtual circuit service [CCITT80, DICIC79]. Virtual circuit segments in each network are connected by VC segments between the X.75 gateway halves (STEs or IDSEs) to form a concatenation of VC segments between the source and destination DTEs, as shown in figure 4.3. Any variations in individual networks' virtual call services or access protocols are translated or terminated at the gateway in the conversion between the network's own protocols and X.75. The intent is that, <u>if</u> the network designers have carefully implemented X.25 and have matched their virtual call service exactly to the individual functions of X.25, the VC service should map very easily into X.75.

If the services being transformed at a gateway are significantly different (for example, X.25 virtual calls in Datapac and Ethernet unreliable datagrams on an LAN), then the gateway must <u>terminate</u> functions of the network access protocol. The internetwork service which results may be based on the subset of functions which both networks have in common. Therefore, the internetwork service is simpler and more primitive than the intranetwork service normally used on one or both sides of the gateway.

For example, the interconnection of an LAN which offers unreliable datagram service, such as Tornet [LOUCK82], to a PDN which offers X.25 datagram service [FOLTS80], is shown in figure 4.4. The datagram service on the PDN is quite robust, including stepwise flow control, delivery confirmation or non-delivery indication or datagram rejected packets

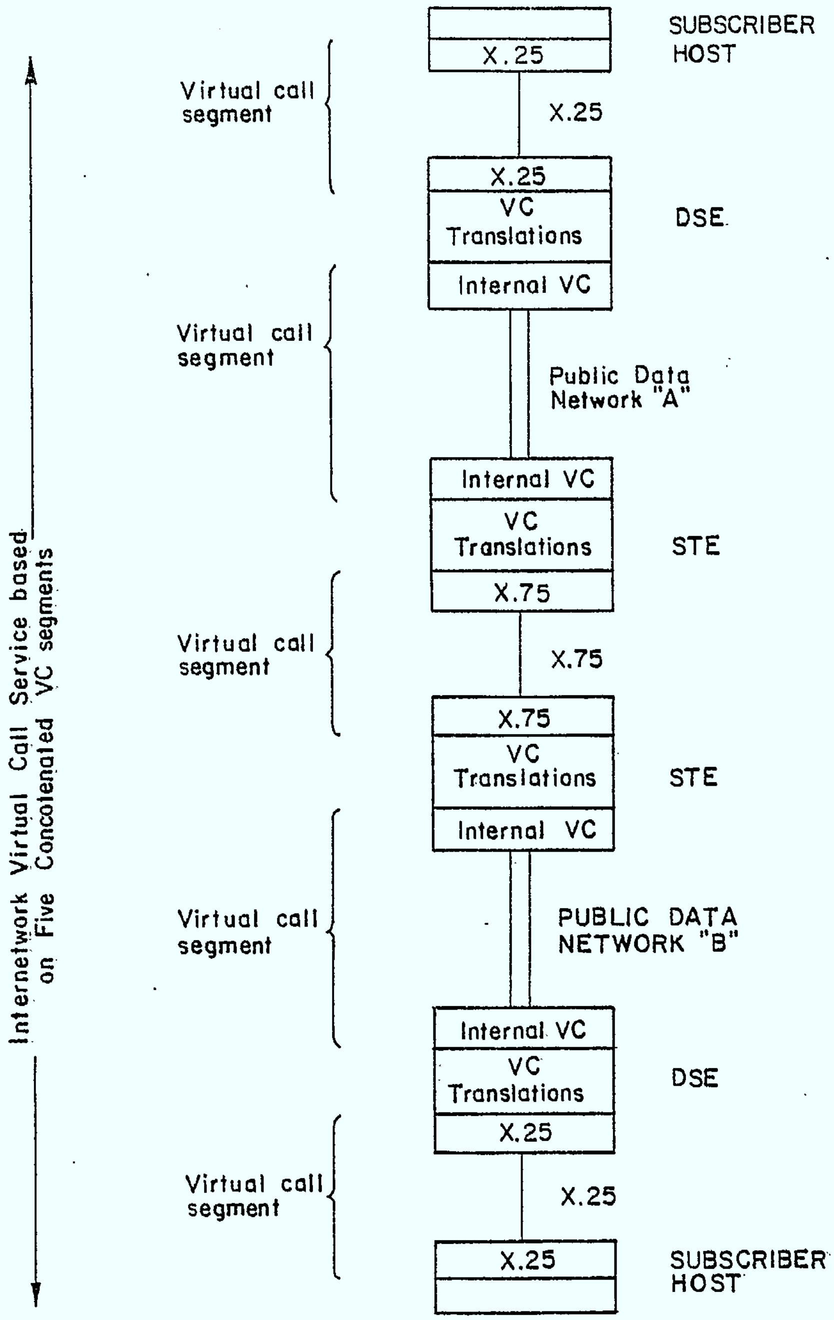


FIGURE 4.3 The CCITT Strategy for the Interconnection of Public Data Networks based on the Concatenation of Virtual Circuit Segments

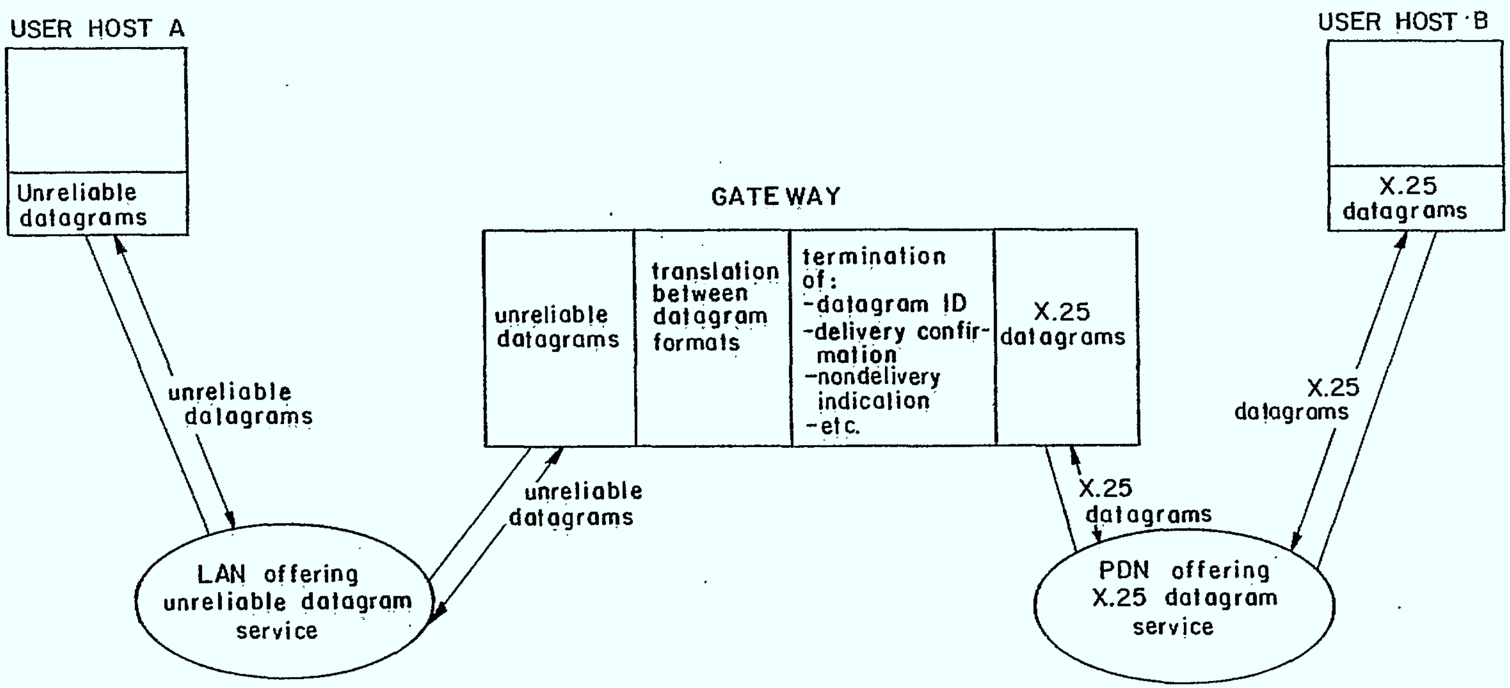


FIGURE 4.4 Use of the Stepwise Approach and Transforming Gateway to Provide Internetwork Datagram Service

from the network, reset and restart capabilities, and a two byte datagram identification field which the subscriber can specify. (Please see Appendix B for a more complete description of the X.25 datagram.) However, none of these features is available on the LAN and there are no equivalent functions on the LAN into which they may be translated. Therefore, they must be terminated at the gateway, if the stepwise approach is used, and the PDN user will observe a degradation in service when communicating with an LAN user as compared to communicating with another PDN user.

4.5 Strategy 2: The Endpoint Approach

In the endpoint approach, a level of service which is common to all of the networks, is used to carry data among hosts on the interconnected networks. The hosts must implement a standard end-to-end protocol, at the transport level, which provides the desired level of internetwork service by performing functions such as multiplexing, error recovery and flow control.

An example of the provision of virtual circuit internetwork service, through the use of datagrams in each network and an end-to-end virtual circuit protocol in the source and destination LAN transceivers, is shown in figure 4.1.

Another example of the provision of internetwork service, based on the endpoint approach, is shown in figure

4.5. With the assumption that X.75 can be extended to include datagram service in a fashion identical to X.25 this example can be used. Assume both User Host A and B contain several applications processes which require reliable inter-process message communications. (Message-switching among processes is the basis for many distributed operating systems, such as Shoshin and Waterloo Port, which are currently under development at Waterloo [MANN81].) Using the endpoint approach, the messages are sent through the interconnected networks in datagrams, and end-to-end protocols which are carefully tailored to the application are implemented in each user host.

4.6 Strategy 3: Stepwise Series of Encapsulatations/Extractions

If the networks to be interconnected do not have the ability to recognize internetwork addresses and use them for routing, then probably the simplest means for providing internetwork service is to use each network solely for the provision of basic data transport among gateways. Each host and gateway must implement an internetwork protocol layer (or sub-layer) above the Network layer but below the Transport layer. This internetwork protocol is based on the use of a specified internetwork service between internetwork protocol layers, on a stepwise basis, as they are encountered between the source and destination users. Each internetwork protocol entity is responsible for encapsulating the

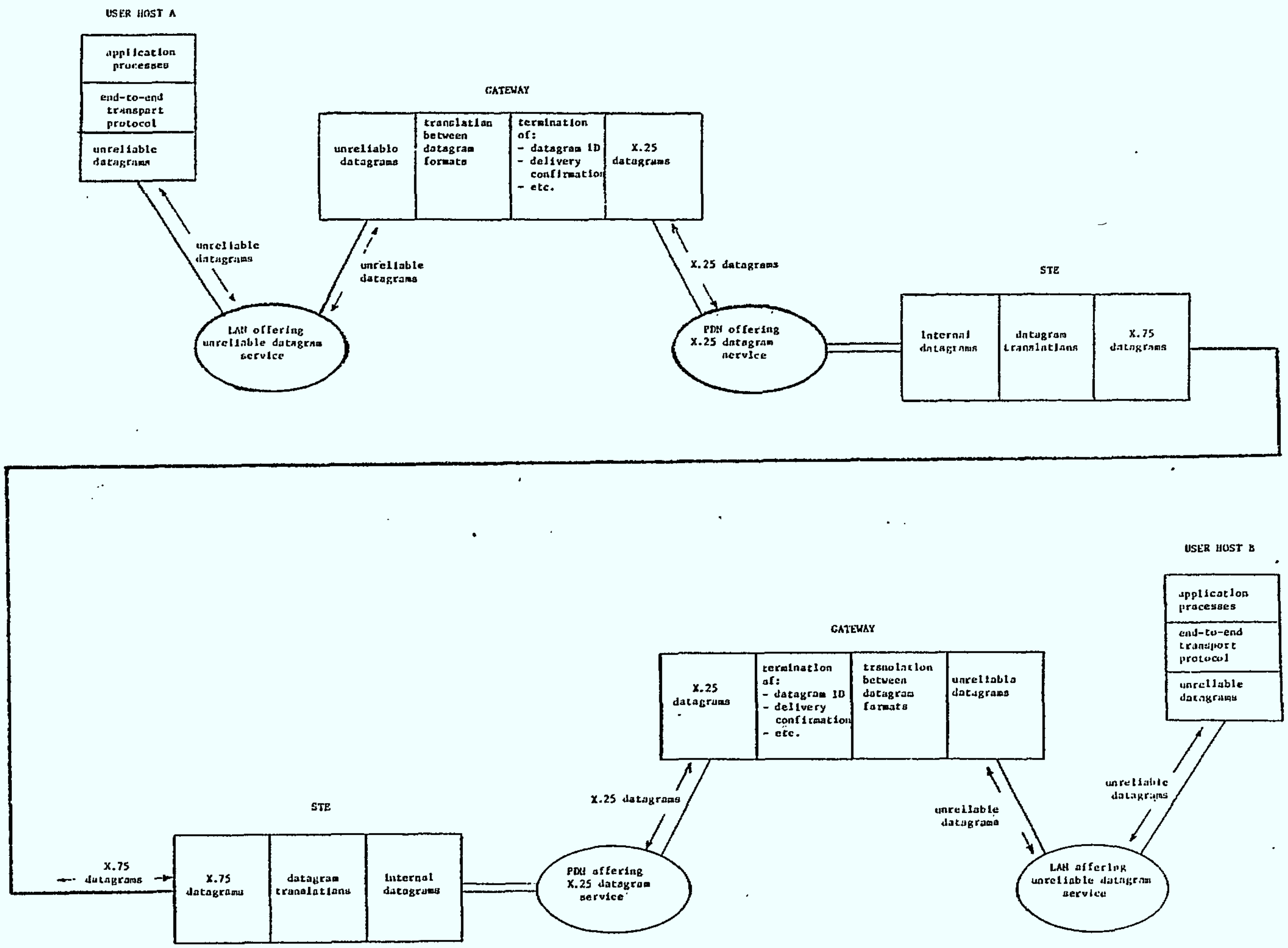


FIGURE 4.5 Use of the Endpoint Approach

data packets of the internetwork service in whatever packet format is necessary to transmit the data to the next internetwork protocol entity, where the data is extracted and then encapsulated in the packet format required for the next network.

Figure 4.6 shows a simple example of this type of interconnection in which a datagram internetwork service is used in conjunction with an end-to-end transport protocol implemented in the hosts. The internetwork datagram service protocol entities are also responsible for routing the datagrams to the gateway and hosts if the networks cannot recognize internetwork addresses.

The ARPA internetwork system, which includes satellite, packet radio and local area networks, has adopted a stepwise series of encapsulations and extractions of datagrams to provide internetwork datagram service. This approach permits a variety of networks, which differ in performance and access protocol, to be interconnected without requiring any changes to the individual networks.

One weakness of this approach is that it does not strictly conform to the Open Systems Interconnection Reference Model. This violation is caused by the internetwork protocol layer (or sublayer) which is implemented between the Network and Transport layers in all hosts and gateways.

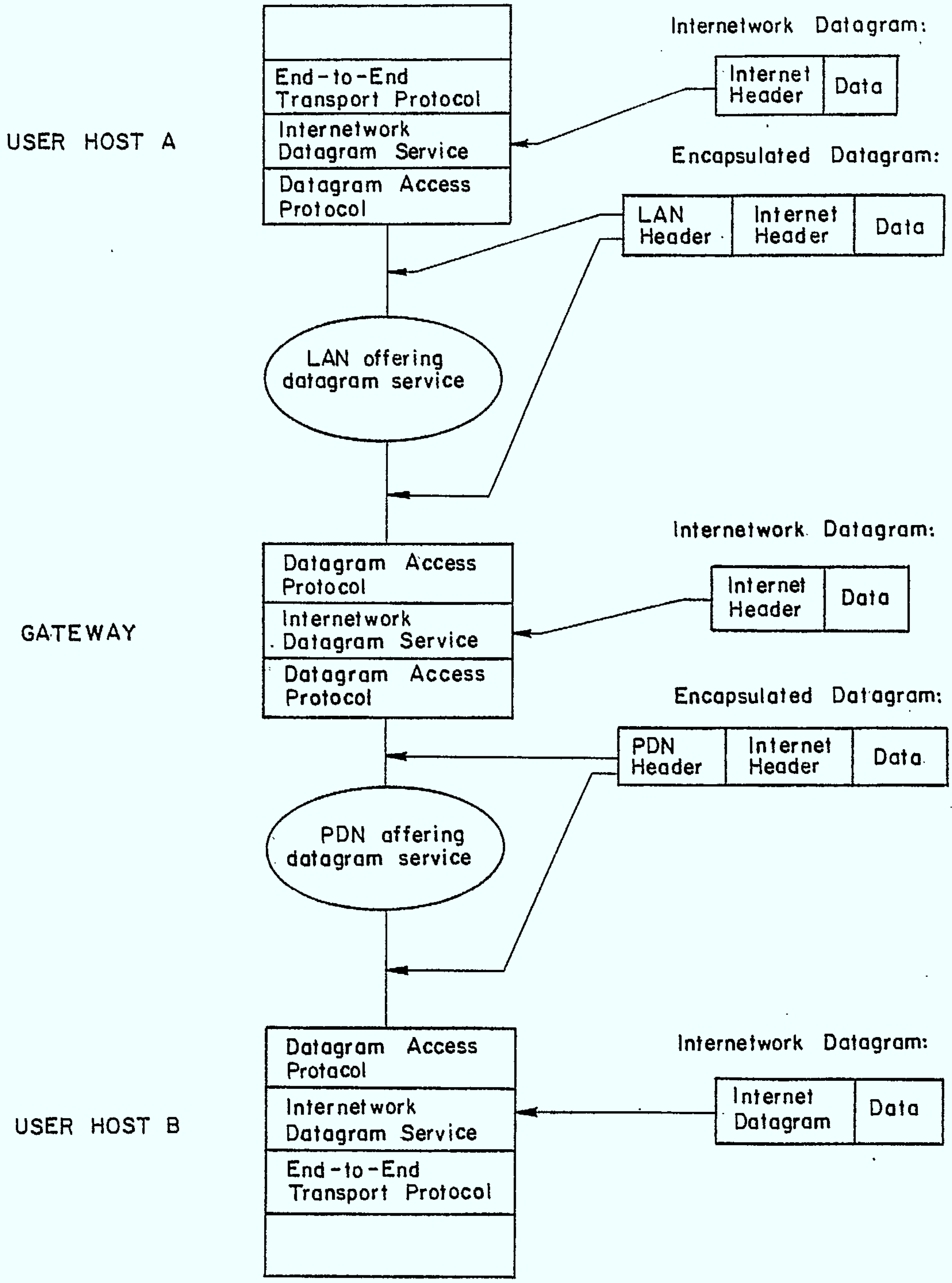


FIGURE 4.6 The Provision of Internetwork Datagram Service based on a Stepwise Series of Encapsulations and Extractions

4.7 Internetwork Functions

In many discussions of network interconnections, the functions required for the reliable transport of data are frequently confused with the functions actually required for internetworking. An exact knowledge of this distinction will simplify the discussion of gateway implementations in the remainder of this study.

The transport functions typically required for internetwork services include error control and flow control. The resequencing of data packets to correct disorder resulting from multiple paths is also a data transport function which is often confused with internetwork functions.

There are only three internetworking protocol functions which may be required at a gateway: the ability to recognize and handle internetwork addresses, internetwork routing, and the fragmentation and reassembly of data packets to accommodate individual networks' maximum data length restrictions.

4.8 A Comparison of the Three Internetworking Strategies

Table 4.1 provides a comparison among the three internetworking approaches as they are used to provide the interconnection of a private LAN with a public data network.

TABLE 4.1

CRITERION/APPROACH	Stepwise with Translations and Terminations	Endpoint	Stepwise Series of Encapsulations and Extractions
Degree of change for existing networks	low	high if specified level of service is unavailable	none
Degree of similarity of internet service to intranet service	high if all nets offer similar services	high	high
Do hosts require the implementation of a special new protocol layer for inter-networking?	no	yes (or no if the end-to-end transport protocol is also used for intra-network service)	yes
Must each network perform inter-network routing?	yes	yes	no
Reliable recovery from failure along route?	no	yes	no
Degree of compliance with CCITT strategy	very high	workable	low

5. ADDRESSING ISSUES

On a network, the address of a host, subscriber, terminal or process, is a unique number corresponding to each destination, which the network can use to route packets to that destination. However, subscriber equipment can be moved, and since on many LANs the subscriber's address is determined by his physical location, a subscriber's address may change every time he moves offices. This is not desirable, therefore the concept of a name (or host name or host number) has emerged.

A name is an alphanumeric string which can be used to uniquely identify a subscriber. It is used, rather than the address, for two reasons: it may be easier to remember and it does not change when the address changes. A name could also be used to identify generic servers, such as all the hosts on a particular net which offer Fortran compiler service or Telidon database service. Usually, when the use of names is contemplated on a network, the network designer includes a name server host as part of the network equipment, so that users can obtain the network addresses which correspond to particular names [DALAL81, LOUCK82].

In order to ensure the uniqueness of user addresses in a system of interconnected networks, the network administrators must agree to use a common address format. There are two fundamental techniques for internetwork addressing: the use of a single flat address space and the use of a hierarchical address format.

The assignment of single level flat addresses is a difficult problem, since it requires the cooperation of both public and private network administrators to ensure that an address is not duplicated. Routing based on a flat address is an even greater concern; either each routing entity must know the route for every possible address in the address space, which implies an impossibly large routing table, or the routing entity must obtain that routing information from a directory server.

Hierarchical addressing is based on a multiple level format. A very common example is the telephone network numbering plan, which consists of a country code followed by an area code followed by a central office number and then a subscriber number.

An important property of the hierarchy is that each field is specific to the preceeding field; therefore, for every possible entry in the first field, all possible entries can be used in the second field, and so on. This provides a high degree of autonomy concerning the assignment of address in each network, and reduces the potential for duplication. Hierarchical addressing simplifies routing. Networks and gateways need not obtain routing information from a directory as with flat addresses, since the hierarchical address may have a country field and then a network-within-country field on which the gateways can route.

5.1 Ethernet 48-bit Host Numbers

Ethernet researchers [DALAL81] have proposed that each item of office automation equipment, which is likely to be used on local area networks, should be given a "built in" 48-bit host number by the manufacturer. These host numbers are to be drawn from a flat addressing space.

Ethernets will use the 48-bit host numbers as subscriber addresses. However, in general, the 48-bit numbers are actually host names, and all non-Ethernet networks will need to consult directories to obtain the network number and subscriber address which corresponds to a given host name. (Ethernets must also consult the directory for information needed for internetwork routing.)

5.2 Recommendation X.121

CCITT Recommendation X.121 is an international numbering plan for PDN subscribers based on hierarchical address. The composition of the international data number for a subscriber is shown in figure 5.1. The address begins with a 3-digit Data country code, followed by a 1-digit network Digit, which together comprise the Data network Identification Code (or DNIC). This is followed by the Network Terminal Number, which may contain up to ten digits (Datapac uses eight).

Internetwork routing is performed at the gateways on the basis of the DNIC alone. Only the destination network

14 DIGIT X.121 NUMBERING PLAN FOR PDNs

X INDICATES ANY DIGIT FROM 0 TO 9 (4 BITS)

Z INDICATES ANY DIGIT FROM 2 TO 7 (4 BITS)

COMPOSITION OF THE INTERNATIONAL DATA NUMBER

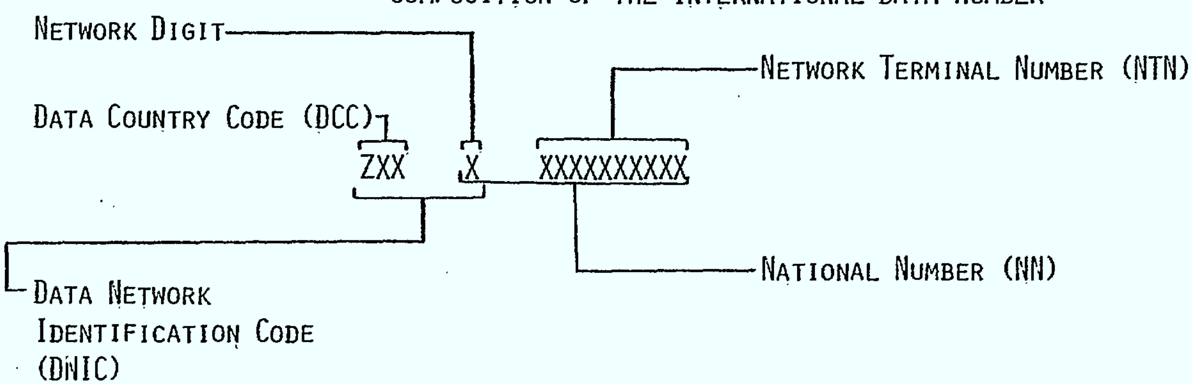


FIGURE 5.1 The format of an X.121 PDN subscriber address

requires the Network Terminal Number to make routing decisions to the destination subscriber.

5.3 The LAN Internet Addressing Problem

Unfortunately, the current X.121 standard cannot be used to provide international addresses for LAN hosts and terminals, without some modifications or extensions. It is not practical to use the Network Digit to differentiate among LANs, as is done with PDNs, for two reasons. First, there are potentially far, far too many LANs to be described by one digit, unless many more country codes are assigned to each country. One solution is to expand the Network Digit to a multi-digit Network Code, however, this is not viable because of the second problem. If local nets are allocated individual Network Digits, then they will have individual DNICs. Since international gateways route on the basis of DNICS, every international gateway would have to contain information for routing to every LAN as well as every PDN in the world. This requirement would nullify much of the advantage of hierarchical addressing over flat addressing.

Any solution to the LAN internet subscriber addressing problem must give consideration to the following objectives:

1. permit the use of X.121 for PDN subscribers without change;
2. provide internetwork addresses which can be used by any PDN or LAN user to access the addressee (This means that every user can be identified by an address which

can be used by any other user to send data to him, with the possible exception of users on his own net who may be required to use an abbreviated address.);

3. permit the use of individual address structures on LANs, since these are not standardized now and there are good technical reasons for them to be different;
4. permit the administration of addresses on each LAN to be performed independently; and
5. be compatible with an address plan for ISDNs, to be determined in the future.

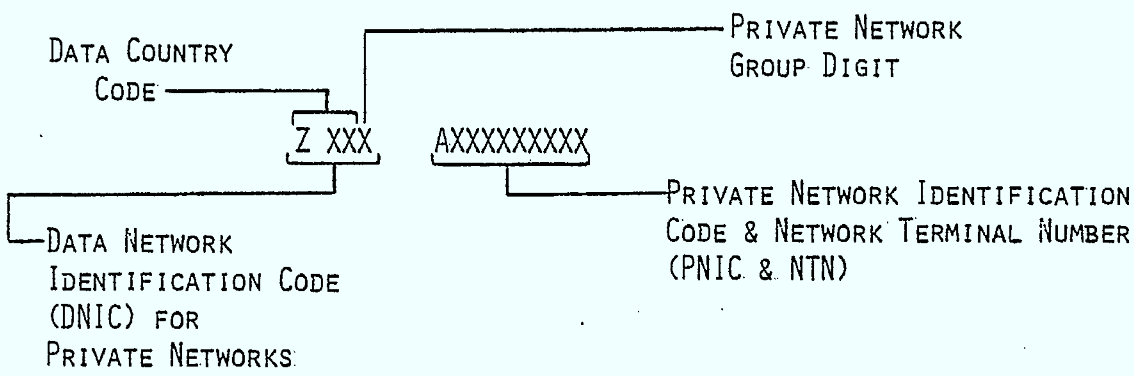
The following sections describe proposed LAN internetwork addressing schemes.

5.4 X.122

One technique which has been proposed for internet subscriber addressing on LANs and other private networks is X.122 [HILI82]. One DNIC per country is assigned to denote all the private networks within that country. The remaining 10 digits of that DNIC, which in X.121 are the Network Terminal Number, are split up in X.122 into a Private Network Identification Code (PNIC) and a Network Terminal Number on the private network. The private network administration may choose any length of NTN from 4 to 8 digits, as shown in figure 5.2. This determines the length of the PNIC; it is 10 digits minus the length of the NTN. The first digit of the PNIC indicates its length, so if an 8-digit NTN is used, only one digit remains to differentiate among private

14 DIGIT X.122 NUMBERING PLAN FOR PRIVATE NETWORKS

X INDICATES ANY DIGIT FROM 0 TO 9
Z INDICATES ANY DIGIT FROM 2 TO 7
A INDICATES ANY DIGIT FROM 2 TO 6



PNIC	+	NTN:	No. of Nets Per PNIC:	No. of Addresses Per Net:
2X	+	XXXXXXXX	10	100,000,000
3XX	+	XXXXXXX	100	10,000,000
4XXX	+	XXXXXX	1000	1,000,000
5XXXX	+	XXXXX	10000	100,000
6XXXXX	+	XXXX	100000	10,000

Figure 5.2 The Proposed X.122 Addressing Scheme

networks. However, up to 100,000 private networks which use 4-digit NTNs may be accommodated. Of course, these limitations may be overcome by using more than one DNIC per country for LAN and private network addresses.

There are three problems with X.122:

1. An X.122 address indicates the country of the subscriber, but not the PDN to which his LAN is connected. If a country has two or more PDNs which are not interconnected, then a gateway in another country cannot determine which PDN to route data to, based on the X.122 address. Canada has two PDNs, Datapac and Infoswitch, and they are not interconnected.
   Furthermore, even if the multiple PDNs in a country are interconnected, the use of X.122 would require each PDN to be able to route on the basis of the PNIC, for all the private networks in that country. This requirement violates the principle that the provision of interconnection should require a minimum of change in existing networks.
2. When long NTN numbers are required, X.122 allows only a small number of private networks per DNIC.
3. Many LANs use hexadecimal digits for NTNs. X.121 and X.122 are based on decimal digits.

5.5 Canadian CCITT Proposal for Private/Public Network Interworking

This proposal, dated March 1, 1982, was circulated for the Special Rapporteur Meeting in Melbourne (see Appendix C). It suggests a technique for routing calls through concatenations of PDNs and LANs using a series of address encapsulations and extractions. The addresses are based on X.121 for the PDNs, and non-standardized LAN addresses subject to a maximum length constraint. LAN/PDN gateways encountered enroute, between the source and destination subscribers, are called "relay points".

The technique is best explained diagramatically. In figure 5.3(a), the source DTE, user A, on a PDN wishes to send data to LAN user B through a subscriber level gateway. G is the gateway address on the PDN and G' is its address on the LAN. In the PDN, G is specified as the destination for A's data, and user B is its <u>forward relay point</u>.

The forward relay point address is carried in the facilities field of the CALL REQUEST packet. At the gateway, the addresses are modified so that B becomes the destination address, G' becomes the originating address, and A is the <u>backward relay point</u>.

Figure 5.3(b) depicts a more complicated case in which two users on different LANs wish to interwork over a pair of concatenated PDNs. Because the PDNs are interconnected

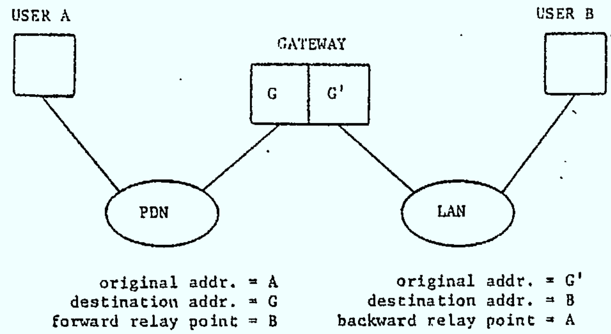


FIGURE 5.3 (a)

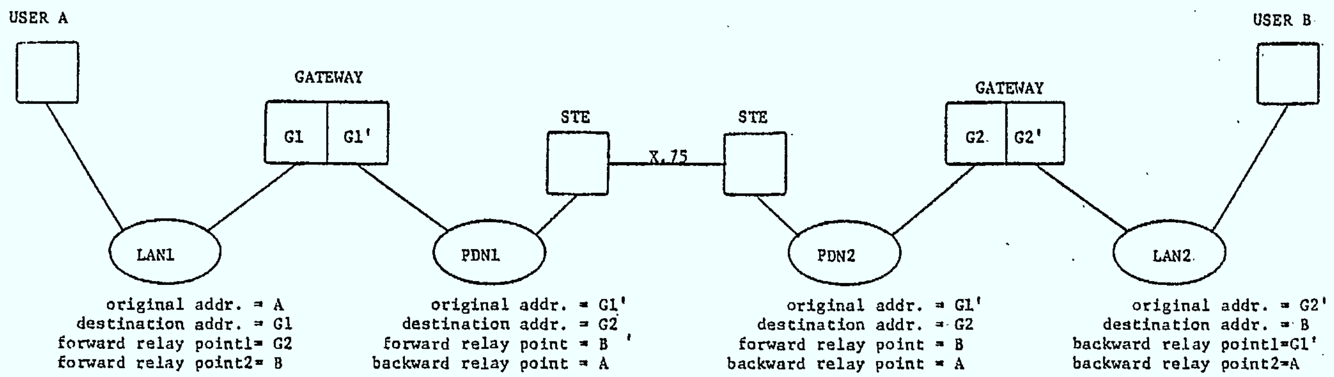


FIGURE 5.3 (b)

through a translation type X.75 gateway and use X.121 addressing, there is no need for an address extraction/encapsulation at the gateway between the PDNs.

The advantage of this technique is that it can be adopted easily by the PDNs because it uses the X.121 addresses for the PDN segments of the data transmission. However, it forces destination users to make distinctions between PDN source users and LAN source users when interpreting the relay point information. Also, the source users are required to identify many gateways on the route, especially if one user is on a LAN which connects to a PDN through another LAN.

This technique makes the assumption that the LAN actually can transmit a relatively large amount of address information in its internode protocol packets. Instead, it may be necessary to store the intermediate relay point addresses at the gateway, and only the source user address would be sent to the destination user.

5.6 Extended 26-Digit X.121

Figure 5.4 presents our proposal for the extension of the X.121 numbering plan from 14 to up to 26 digits. This modified plan specifies international, internetwork addresses for PDN, LAN and other private network users in a common format, which can be used easily on letterhead, or in a printed directory, to identify a destination user. The

PROPOSED EXTENDED 26 DIGIT X.121 NUMBERING PLAN
FOR PDN AND PRIVATE NETWORK USE

X INDICATES ANY DIGIT FROM 0 TO 9 (4 BITS)
Z INDICATES ANY DIGIT FROM 2 TO 7 (4 BITS)
Y INDICATES ANY DIGIT FROM 0 TO F (4 BITS)

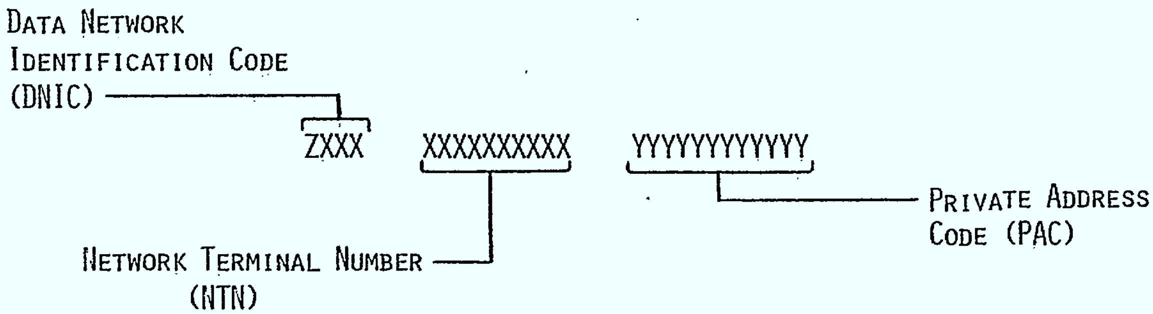


FIGURE 5.4 Extended 26 digit X.121

first 14 digits (or fewer, depending on the length of the NTN) are used to indicate a PDN DTE address of either a PDN subscriber, or a gateway to a private network. The last twelve hexadecimal digits (or fewer, at the discretion of the private network administration) contain the private network address of the destination user. These digits might even be used as a sub-address by a PDN DTE, to indicate a particular process, application, service access point, or computer port.

Twelve hexadecimal digits are enough to accommodate both the 48-bit Ethernet host numbers, and the 16 or 48-bit addresses proposed by IEEE 802 [HILI82]. These are the longest LAN addresses which have been proposed. Dalal [DALAL81] states that 48 bits will permit the unique identification of each unit of office automation equipment for the forseeable future.

Since the PDNs do not have to examine the last 12-digit field to perform routing, this extension of X.121 does not require a modification of existing PDN networks beyond the need to transmit the extra digits across the X.25 interface and through the PDN subnetwork. There are already length fields for both the source DTE and destination DTE addresses included in the X.25 packets. The complexity of modifying the PDN to accept these longer addresses depends on the software capabilities of the existing PDN switches.

One possible objection to this proposal is that it does not take into account the case of an LAN user whose LAN connects to a PDN through another LAN. This would be handled neatly in the Canadian CCITT contribution technique by specifying the gateway between the two LANs as a relay point. However, we believe that this routing and addressing problem is a matter to be solved by the LANs, and any special routing information which the LANs need should be encoded in the distination user's twelve digit address. In almost all cases the source user is interested in specifying an address for the destination, and does not want to have to explicitly specify the entire route.

It is important that the impact of ISDN addressing on this proposal for Extended X.121 be studied, so that the Extended X.121 is not adopted without taking interworking with ISDNs into account, in the same way that X.121 was adopted while ignoring the LAN inteconnection issue.

6 GATEWAY FUNCTIONS FOR STRATEGY 1

This section describes the layered protocol architecture and functions required at the gateway to provide internetwork services in a stepwise manner with a transforming gateway between LAN users and PDN DTEs.

There is a compelling argument in favour of this interconnection strategy over the other two: both the endpoint approach, and the stepwise series of incapsulations/extractions, require that host users implement new protocols, solely for internetworking purposes. However, the goal of the stepwise approach, with the transforming gateway, is to provide an internetwork service which is as close as possible to the intranetwork service.

This section considers four combinations of LAN services and user equipment. These are:

1. host on an LAN using unreliable datagram service,
2. host on an LAN using reliable datagram service,
3. host on an LAN using virtual call service, and
4. terminal on an LAN using virtual call service.

Three combinations of user equipment and PDN services are considered. These are:

1. host using X.25 datagrams,
2. host using virtual call service, and
3. terminal using virtual call service.

The following subsections present the gateway functions required to provide translations between all of the combinations of user equipment and services which may interwork.

6.1 LAN Host Using Unreliable Datagrams Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

Figure 6.1 depicts the gateway translations and protocol architecture required for a host on an LAN using unreliable datagrams to interwork with a host on a PDN using X.25 datagrams or X.25 virtual call service.

The LAN host is connected to a transceiver (XCVR) which transmits and receives datagrams over the LAN medium. Unreliable datagram service means that the transceivers do not perform sequencing and complete error recovery. (This is true for Ethernet.) Therefore, it is assumed that the LAN hosts would normally use an end-to-end protocol to ensure reliable transmission. However, this may be omitted.

The gateway shown in figure 6.1 is actually a special LAN transceiver which connects to the PDN using X.25 (host level interconnection). The gateway attaches to the LAN medium and supports the unreliable datagram transmission protocol, just like any other transceiver. It also terminates the LAN end-to-end protocol, which creates a stream of sequenced, reliable datagrams. The internetwork address is somehow extracted from these datagrams, so that X.25 packets can be formed using an appropriate addressing strategy (for example, Extended 26-digit X.121 - see Section

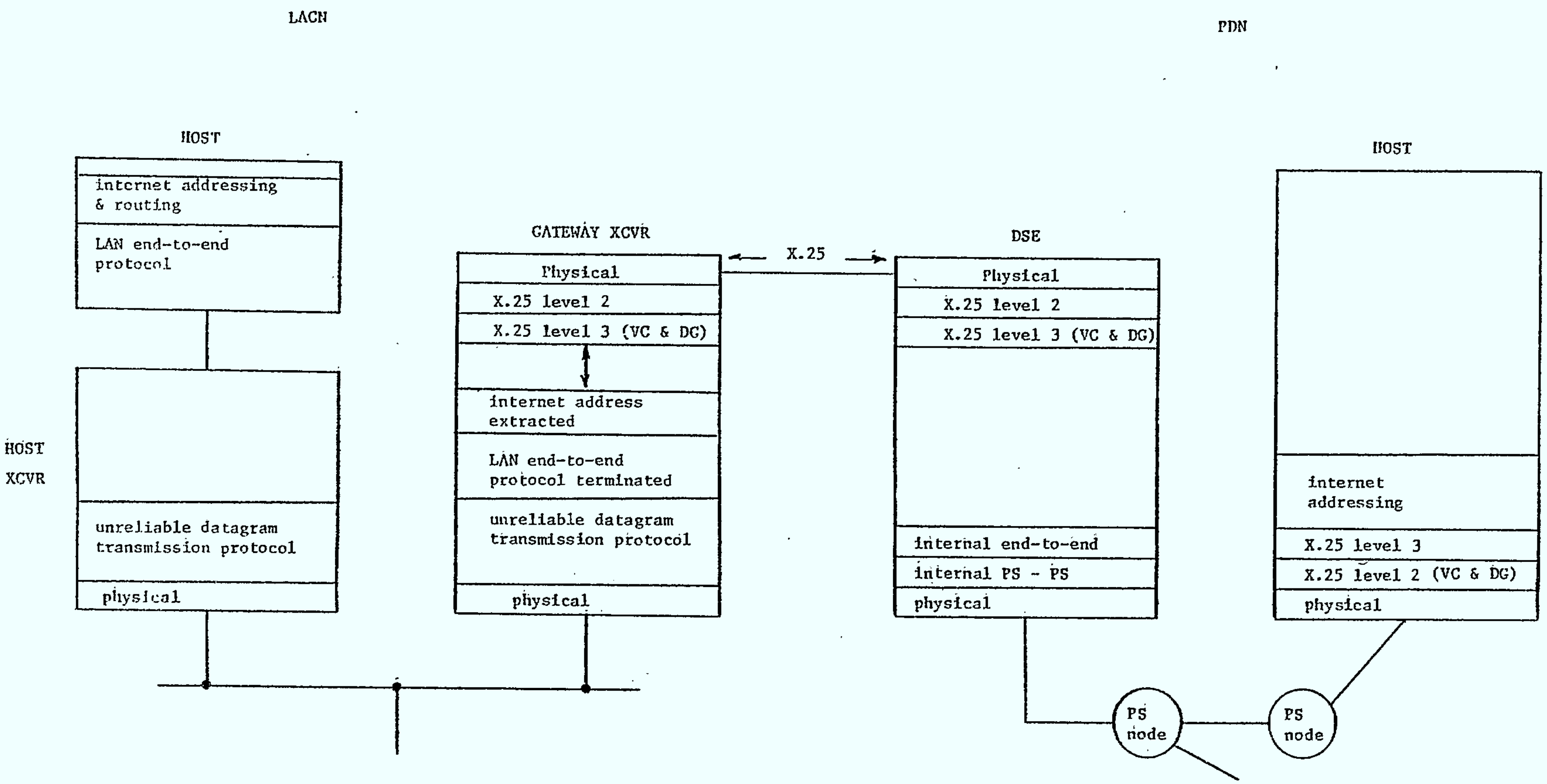


FIGURE 6.1 LAN Host Interworking with PDN Host Using Unreliable Datagram Service on the LAN and X.25 VC or Datagram Service on the PDN

5.6). These X.25 packets are then transmitted to a PDN DSE for transmission to the PDN host.

6.2 LAN Host Using Unreliable Datagrams Interworking with PDN Terminal Using A Virtual Call

This case is identical to Section 6.1 except that the PDN user is a terminal rather than a host. (By terminal, we mean a start-stop mode DTE.) The terminal connects to a Packet Assembler-Disassembler (PAD) containing packetization parameters which can be set by the terminal user using X.28, or by a remote host using the X.29 protocol. Therefore, the PAD is "expecting" to communicate with the LAN user via the PAD portion of X.29.

However, the LAN host must have an LAN terminal handling protocol, which it uses to communicate with transceivers for terminals on its own net. It violates one of our basic principles of network interconnection to require the LAN user to implement the host portion of X.29 if it is different from the LAN terminal handling protocol used for intranet traffic. Therefore, the gateway must translate the LAN terminal handling protocol to the host portion of X.29. This is done at a level above the internetwork address extraction.

6.3 LAN Host using Reliable Datagrams Interworking with PDN Host using X.25 Datagrams or Virtual Calls

This case, shown in figure 6.3, is identical to the

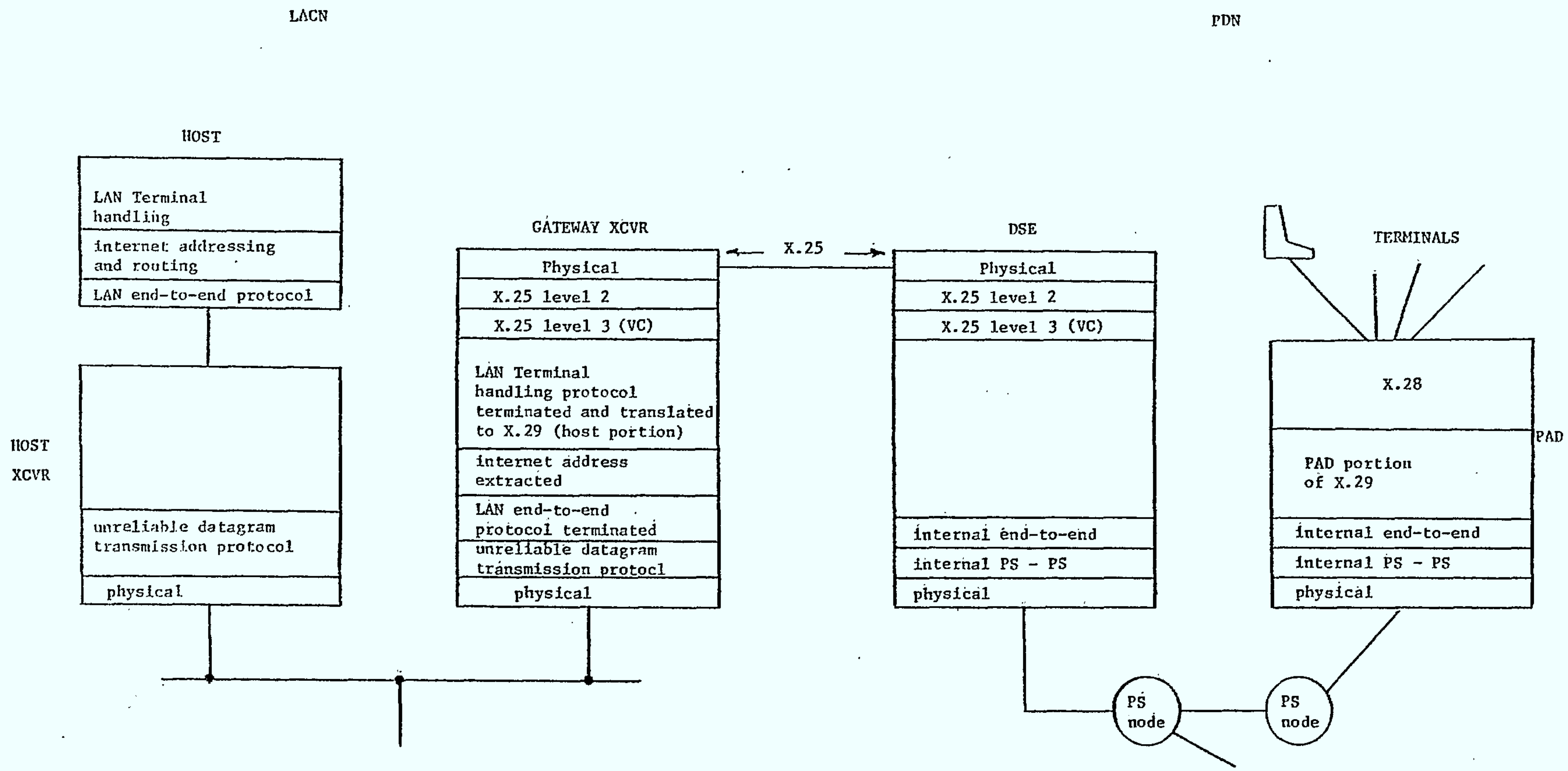


FIGURE 6.2 LAN Host Interworking with PDN Terminals Using Unreliable Datagram Service on the LAN and X.25 VC Service on the PDN

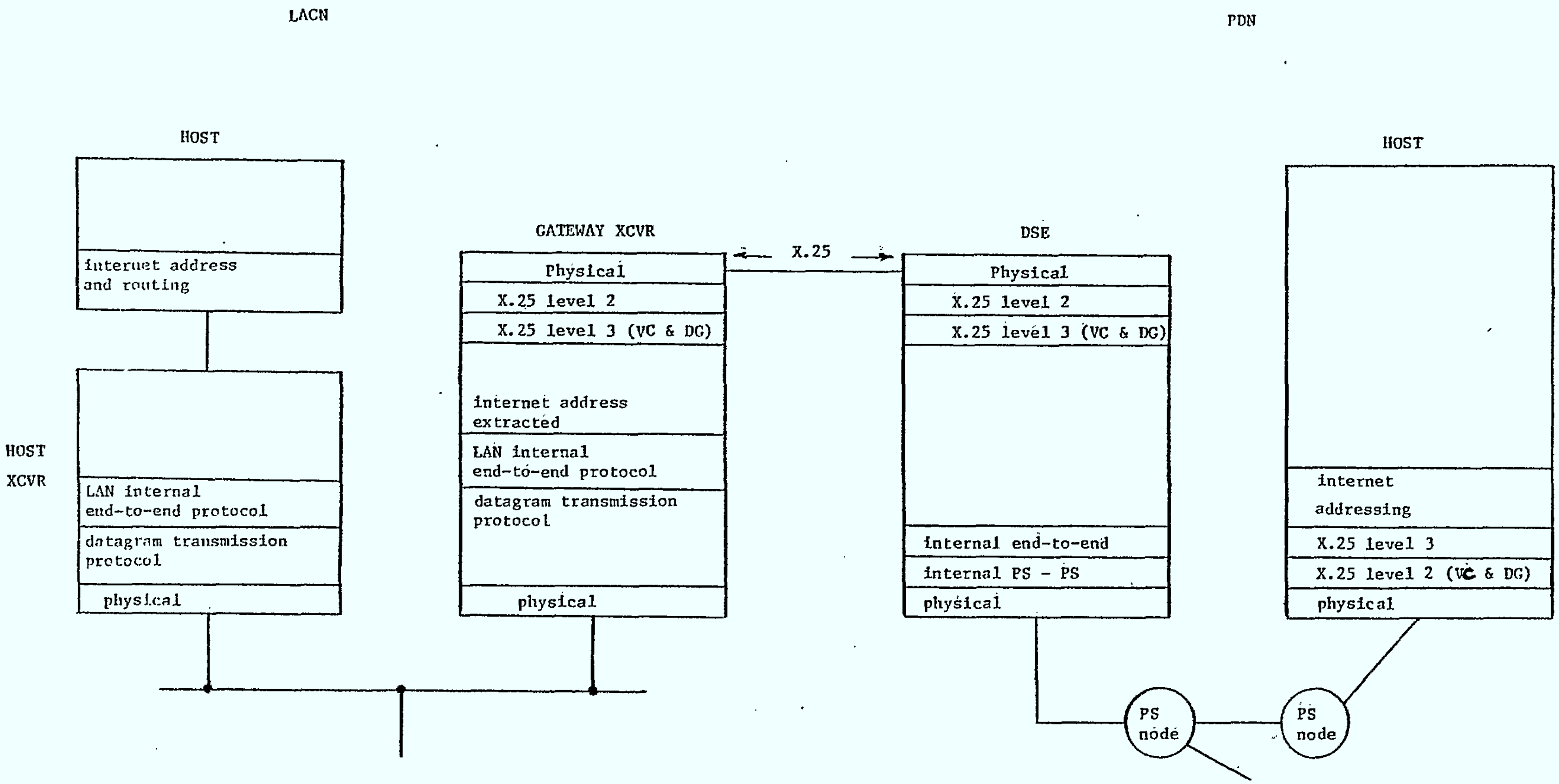


FIGURE 6.3 LAN Host Interworking with a PDN Host Using Reliable Datagram Service on the LAN and X.25 VC or Datagram Service on the PDN

case in Section 6.1 except that the LAN offers reliable datagram service. The LAN host no longer implements a LAN end-to-end protocol, since this is contained in the transceivers. It must be terminated at the gateway where packets are extracted for insertion into the PDN using X.25.

6.4 LAN Host using Reliable Datagrams Interworking with PDN Terminal using a Virtual Call

This case, shown in figure 6.4, is similar to the case in Section 6.2 except that the LAN offers reliable datagram service. Therefore, the LAN transceiver, rather than the LAN host, implements an LAN end-to-end protocol layer.

6.5 LAN Host Using Virtual Call Service Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

In figure 6.5, a LAN host which uses virtual circuit (VC) service on the LAN is shown. The VC service has an access protocol, and is supported by the use of an LAN internal end-to-end protocol among transceivers. This latter protocol is transformed by the gateway into the X.25 access protocol for the PDN.

6.6 LAN Host Using Virtual Call Service Interworking with PDN Terminal Using a Virtual Call

This case, shown in figure 6.6, is similar to Section 6.5 except that the gateway must translate terminal handling protocols to accommodate the PDN terminal.

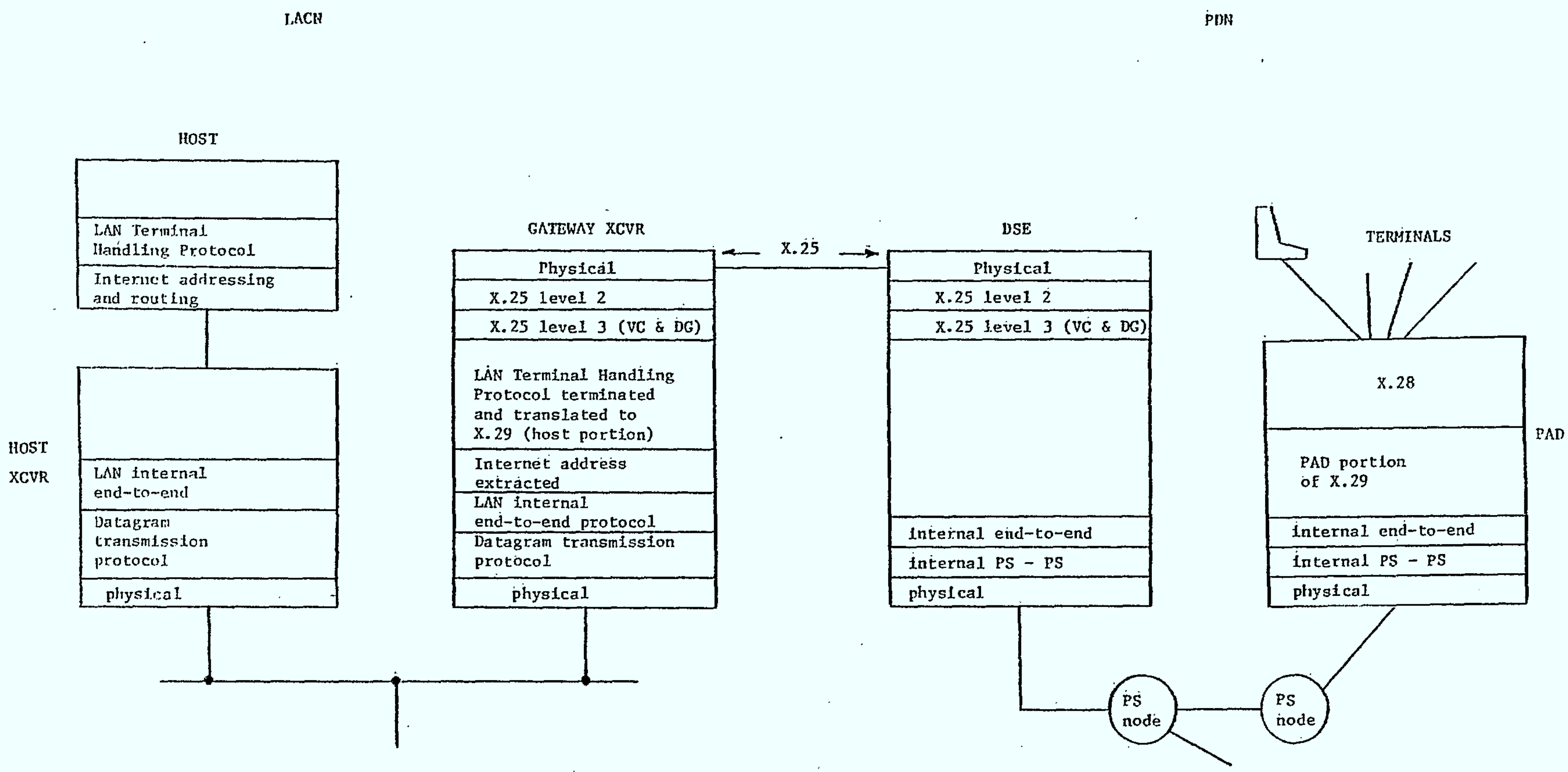


FIGURE 6.4 LAN Host Interworking with a PDN Terminal Using Reliable Datagram Service on the LAN and X.25 VC Service on the PDN

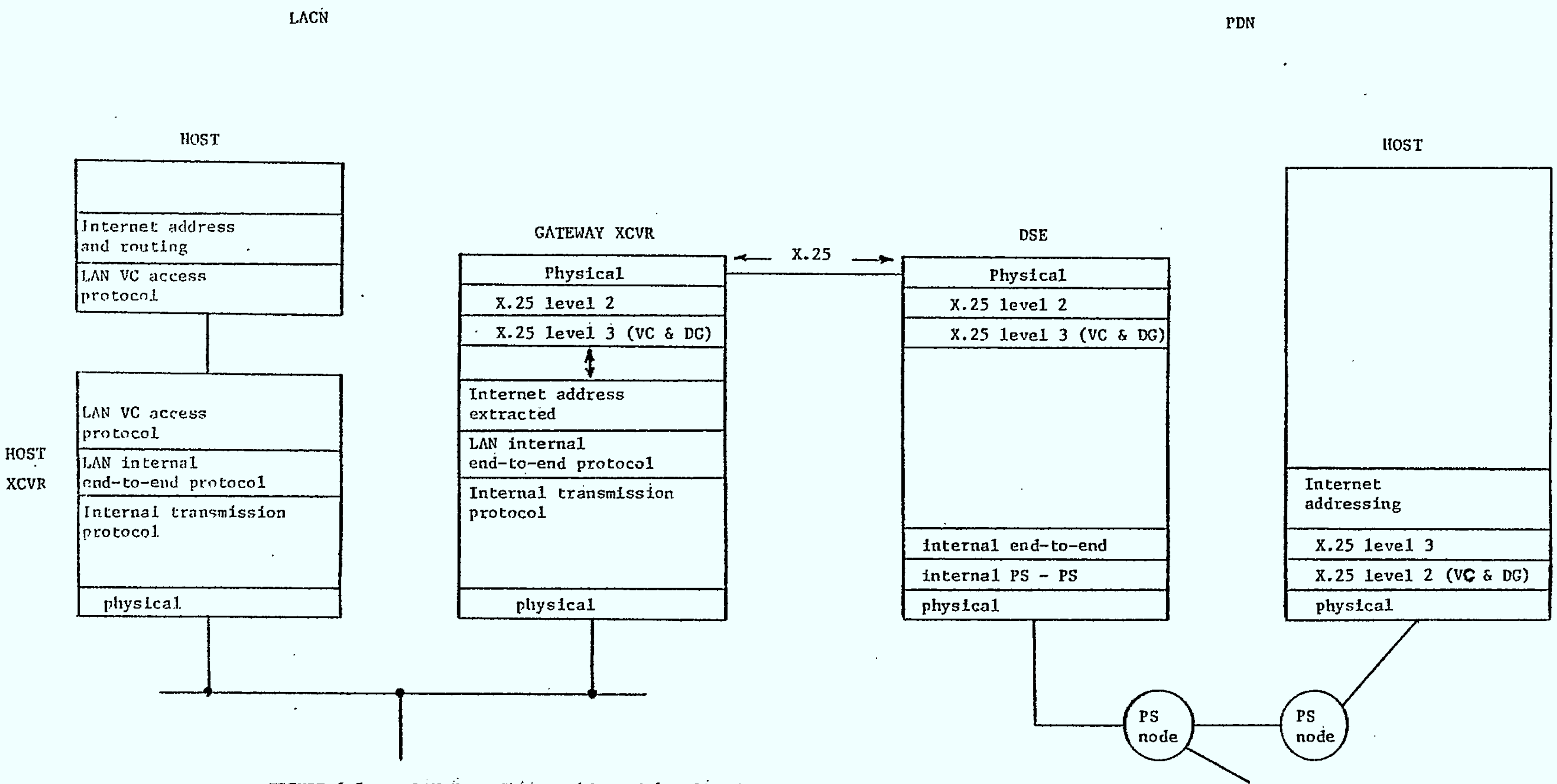


FIGURE 6.5 LAN Host Interworking with a PDN Host Using VC Service on the LAN and X.25 VC or X.25 Datagram Service on the PDN

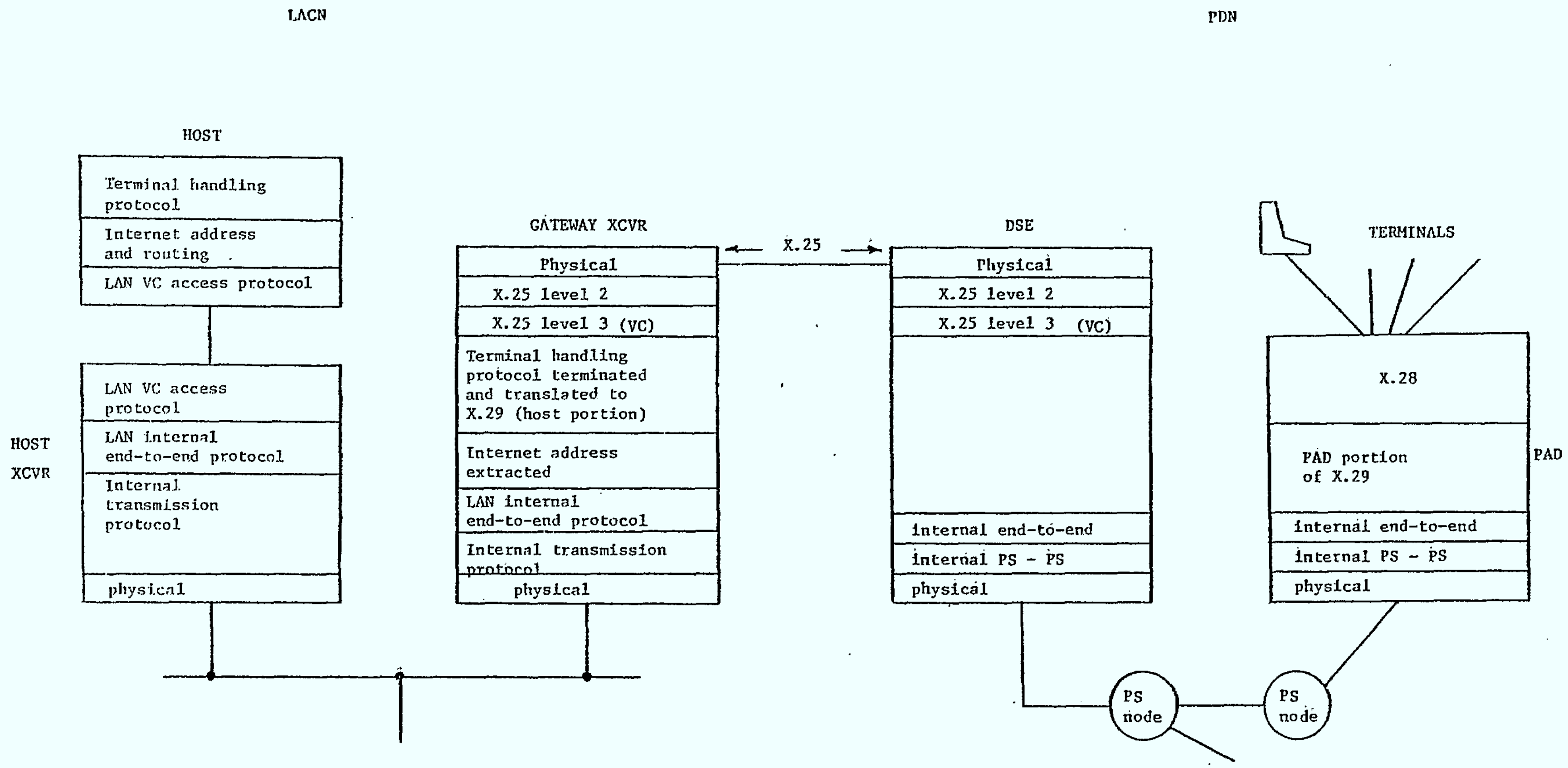


FIGURE 6.6 LAN Host Interworking with a PDN Terminal Using VC Service on the LAN and X.25 VC Service on the PDN

6.7 LAN Terminal Using a Virtual Call Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

In this case, depicted in figure 6.7, a terminal on the LAN is connected to an LAN transceiver which can perform PAD and terminal handling functions. It must also provide virtual circuit service, since the use of datagrams by a dumb terminal is nonsensical.

The PDN host, with which the LAN terminal is interworking, uses the host portion of X.29 to communicate with terminals on the PDN. Since it is highly desirable to use the same protocol to interwork with terminals on the LAN, the gateway must transform the LAN terminal handling protocol (PAD portion) into the PAD portion of X.29.

6.8 LAN Terminal using a Virtual Call Interworking with PDN Terminal using a Virtual Call

An LAN terminal is shown interworking with a PDN terminal in figure 6.8. The gateway transceiver must translate the terminal handling protocol from each terminal's handling protocol for the other network.

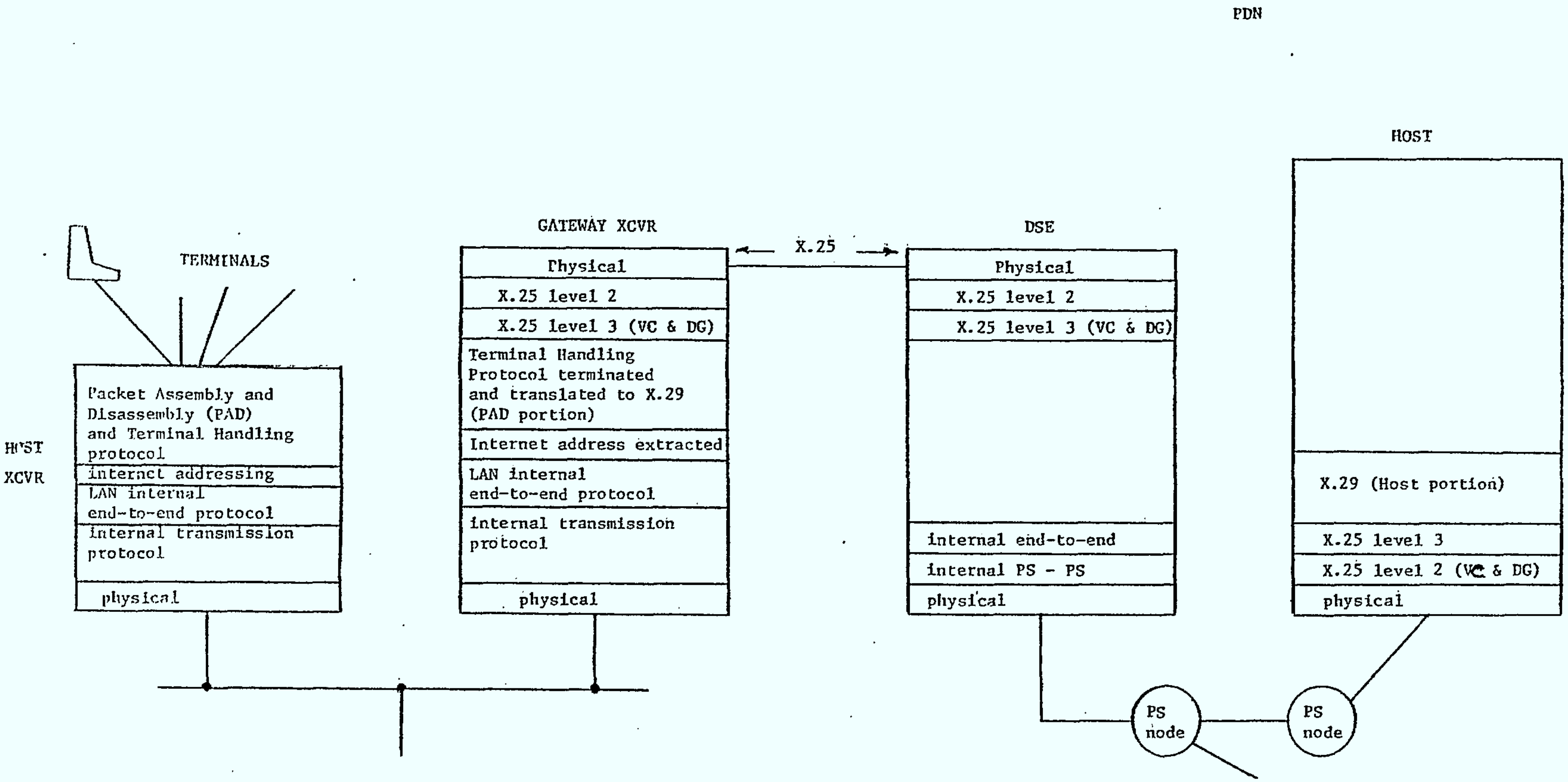


FIGURE 6.7 LAN Terminal Interworking with a PDN Host Using VC Service on the LAN and X.25 VC or X.25 Datagram Service on the PDN

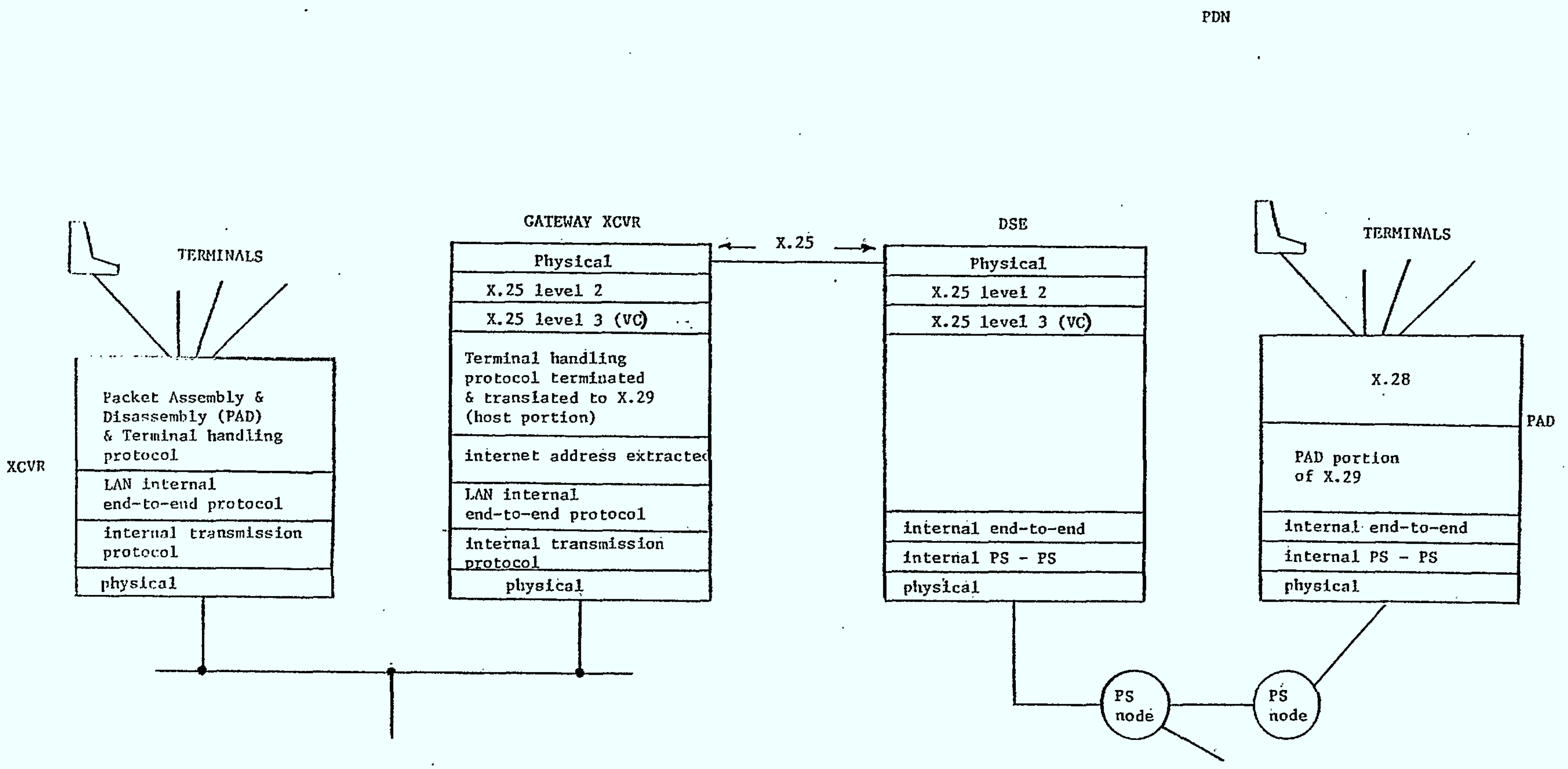


FIGURE 6.8 An LAN Terminal Interworking with a PDN Terminal, Using VC Service on the LAN and X.25 VC Service on the PDN

7. GATEWAY FUNCTIONS FOR STRATEGY 2

This section describes the layered protocol architecture and functions required at the gateway to provide internetwork services in an endpoint manner using a common end-to-end protocol and whatever services are available in the networks being interconnected.

This section considers four combinations of LAN services and user equipment. These are:

1. host on an LAN using unreliable datagram service,
2. host on an LAN using reliable datagram service,
3. host on an LAN using virtual call service, and
4. terminal on an LAN using virtual call service.

Two combinations of user equipment and PDN services are considered. These are:

1. host using X.25 datagrams, and
2. host using X.25 virtual calls.

A terminal on a PDN cannot be considered using this approach since the PDN PAD protocols (X.28 and X.29) would have to be redefined to include an end-to-end internetwork protocol.

The following subsections present the gateway functions required to provide internetwork service between all of the above combinations of user equipment and services which may interwork.

7.1 LAN Host Using Unreliable Datagrams Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

Figure 7.1 depicts an LAN host on an LAN which offers unreliable datagram service interworking with a host on an X.25 PDN. It is assumed that the LAN host uses an end-to-end transport protocol for intranet traffic to ensure reliable data transmission. However, for internetworking, the LAN host must circumvent this LAN transport protocol and use the same end-to-end internetwork protocol as the PDN host uses. Therefore, the host is required to implement an additional protocol for internetworking which is not used for intranetworking.

The gateway transceiver must extract internet addresses and form appropriately addressed packets for use in each network. The LAN datagrams are transformed into X.25 datagrams or X.25 virtual call packets, and then sent to the PDN DSE via a host level gateway connection.

7.2 LAN Host Using Reliable Datagrams Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

The case depicted in figure 7.2 is similar to Section 7.1 except that the LAN provides reliable datagram service rather than unreliable datagrams. Therefore, the LAN host does not require an LAN end-to-end transport protocol entity to ensure reliable data transmission.

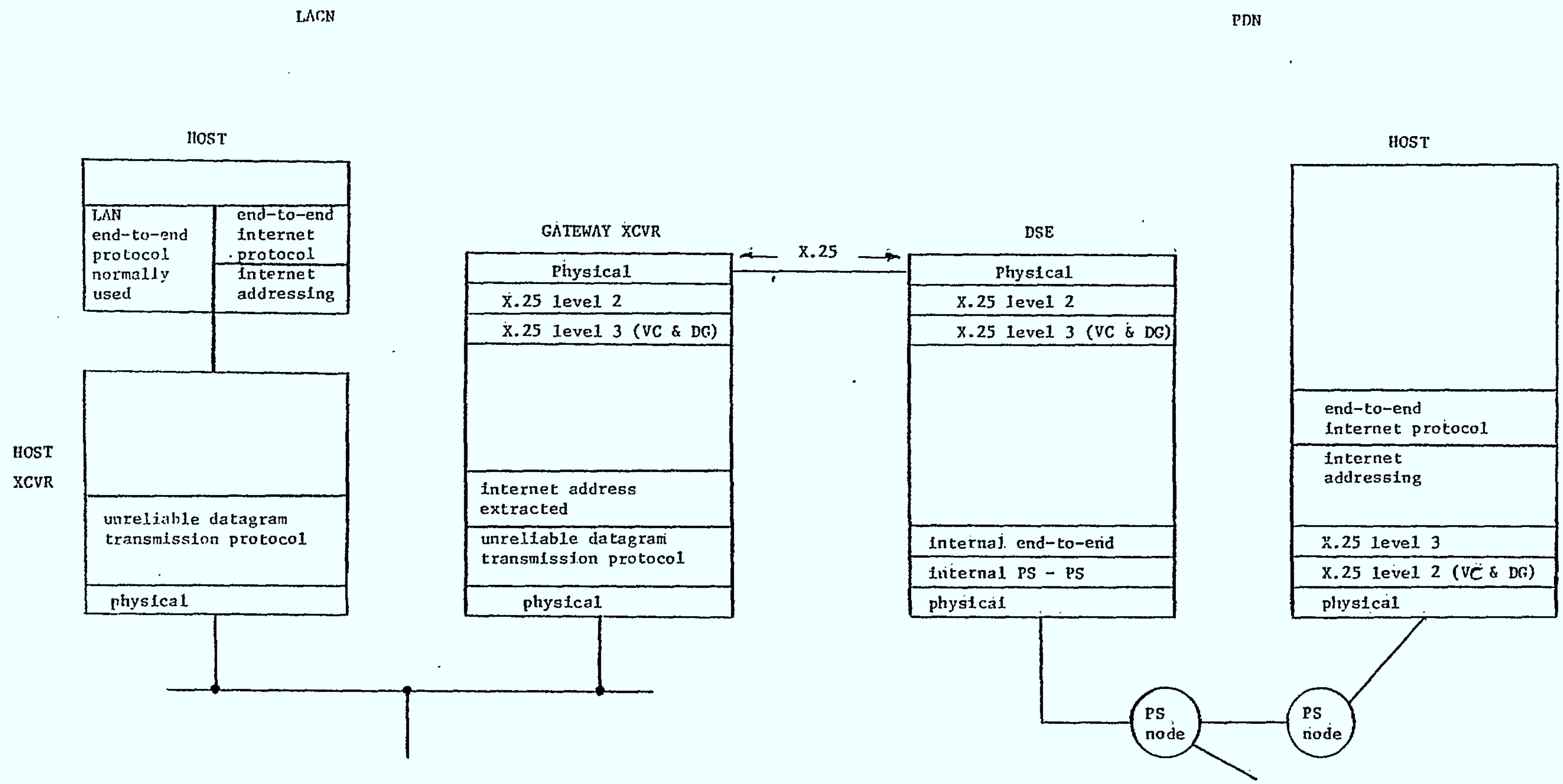


FIGURE 7.1 LAN Host Interworking with PDN Host Using Unreliable Datagram Service on the LAN and X.25 VC or Datagram Service on the PDN, and an End-to-End Internetwork Protocol

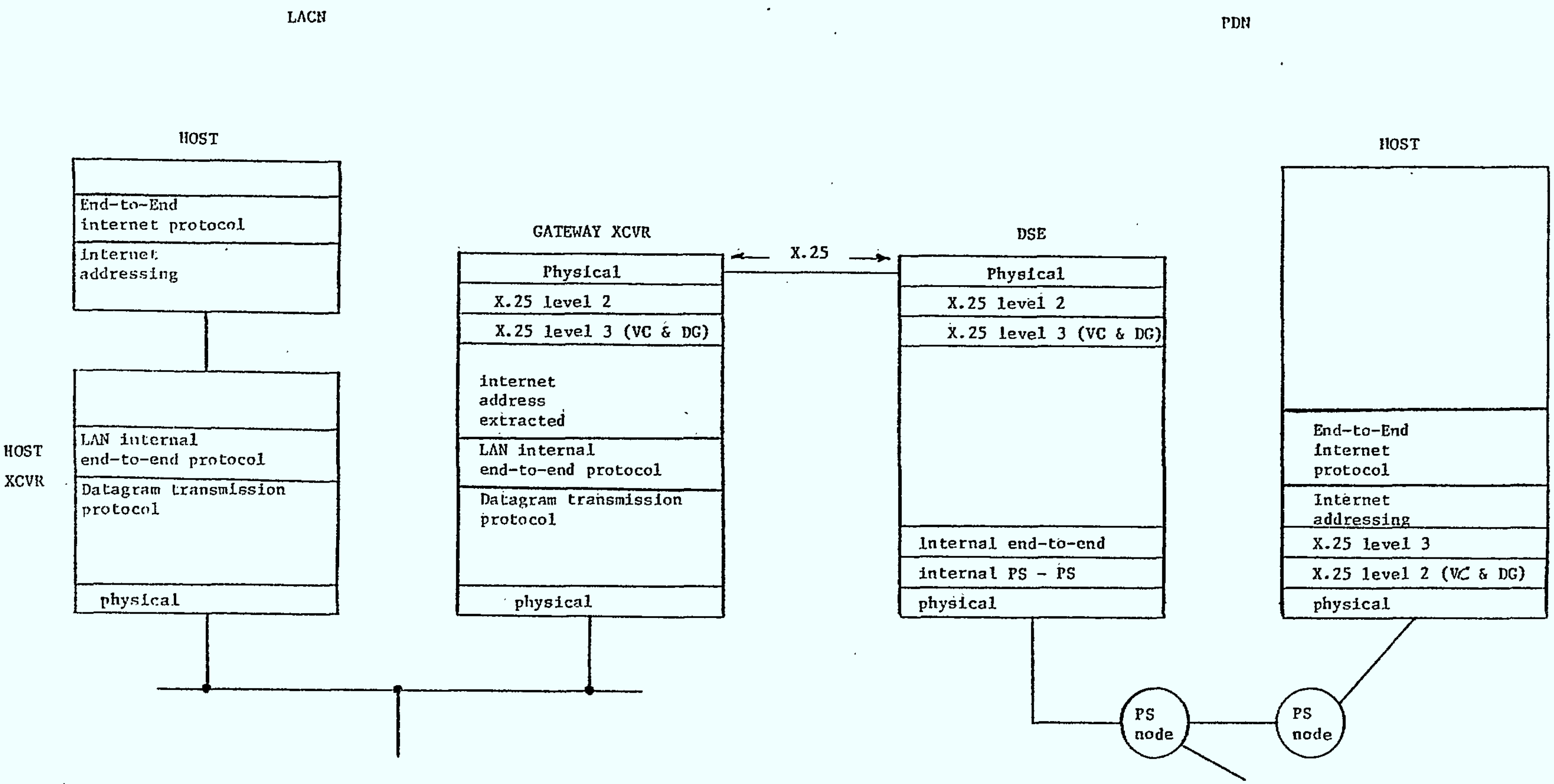


FIGURE 7.2 LAN Host Interworking with PDN Host Using Reliable Datagram Service on the LAN and X.25 VC or Datagram Service on the PDN, and an End-to-End Internetwork Protocol

7.3 LAN Host Using Virtual Call Service Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

Figure 7.3 shows an LAN host interworking with a PDN host using virtual call service on both networks. The virtual call service on the LAN requires the use of an "end-to-end" protocol in the transceivers to provide sequencing and error control. The gateway transceiver performs internet addressing functions and transforms the VC service of each net into the VC service of the other. Because this transformation may not be perfect, the hosts use and end-to-end internet protocol to ensure reliable data transmission.

7.4 LAN Terminal Using Virtual Call Service Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

Figure 7.4 depicts a terminal on an LAN interworking with a host on a PDN. The LAN must offer virtual circuit service for dumb terminals, even for intranet traffic, since it makes no sense for terminal users to type datagrams. The transceiver to which the terminal is connected must provide Packet Assembly-Disassembly (PAD) functions, and must implement the end-to-end internetwork protocol and internet addressing. The transceiver also contains the LAN VC internal protocol. Because the protocol layers for this transceiver are so complex, the level for some of the protocol entities is given in the figure.

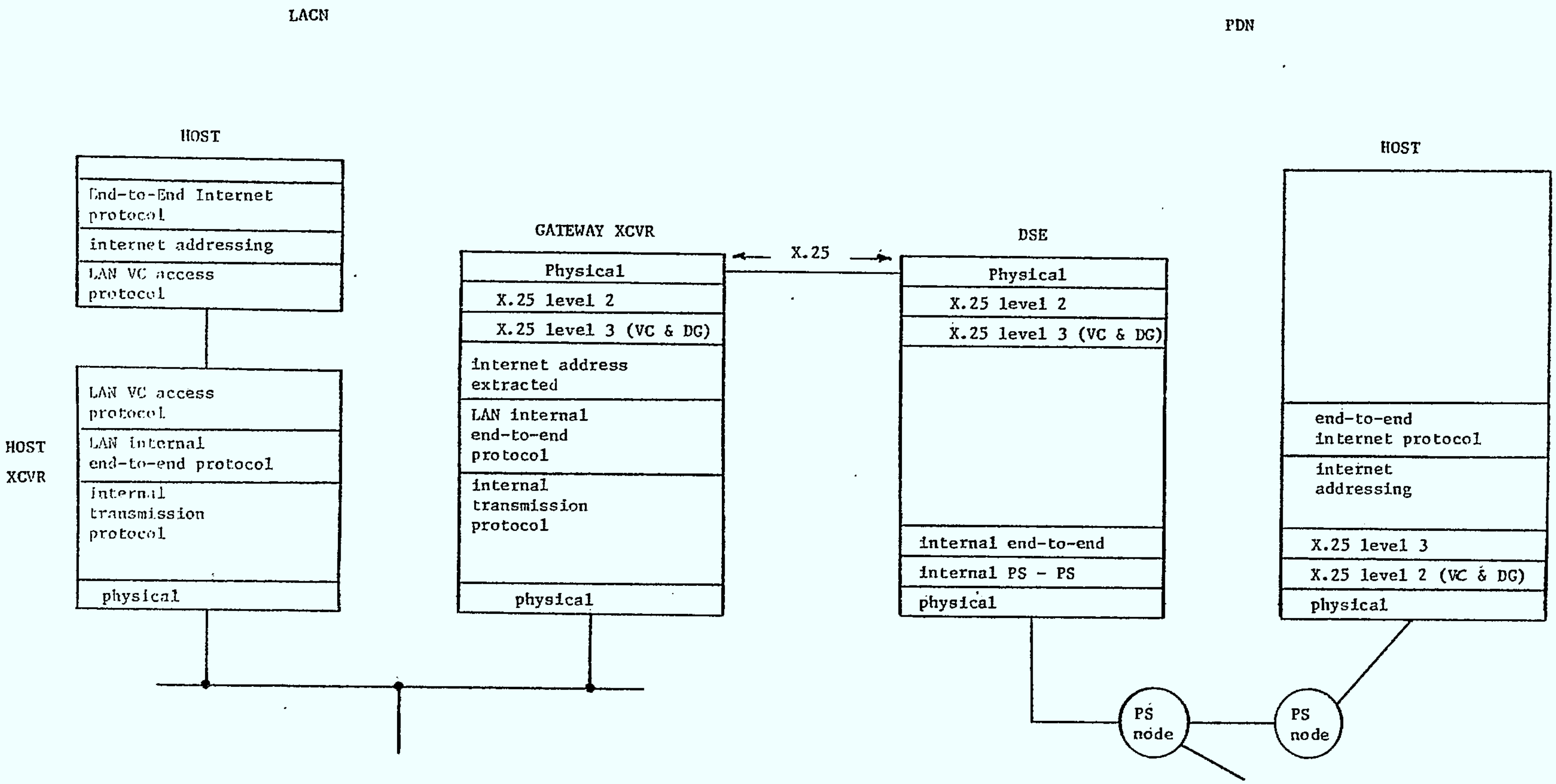


FIGURE 7.3 LAN Host Interworking with PDN Host Using VC Service on the LAN and X.25 VC or X.25 Datagram Service on the PDN, and an End-to-End Internetwork Protocol

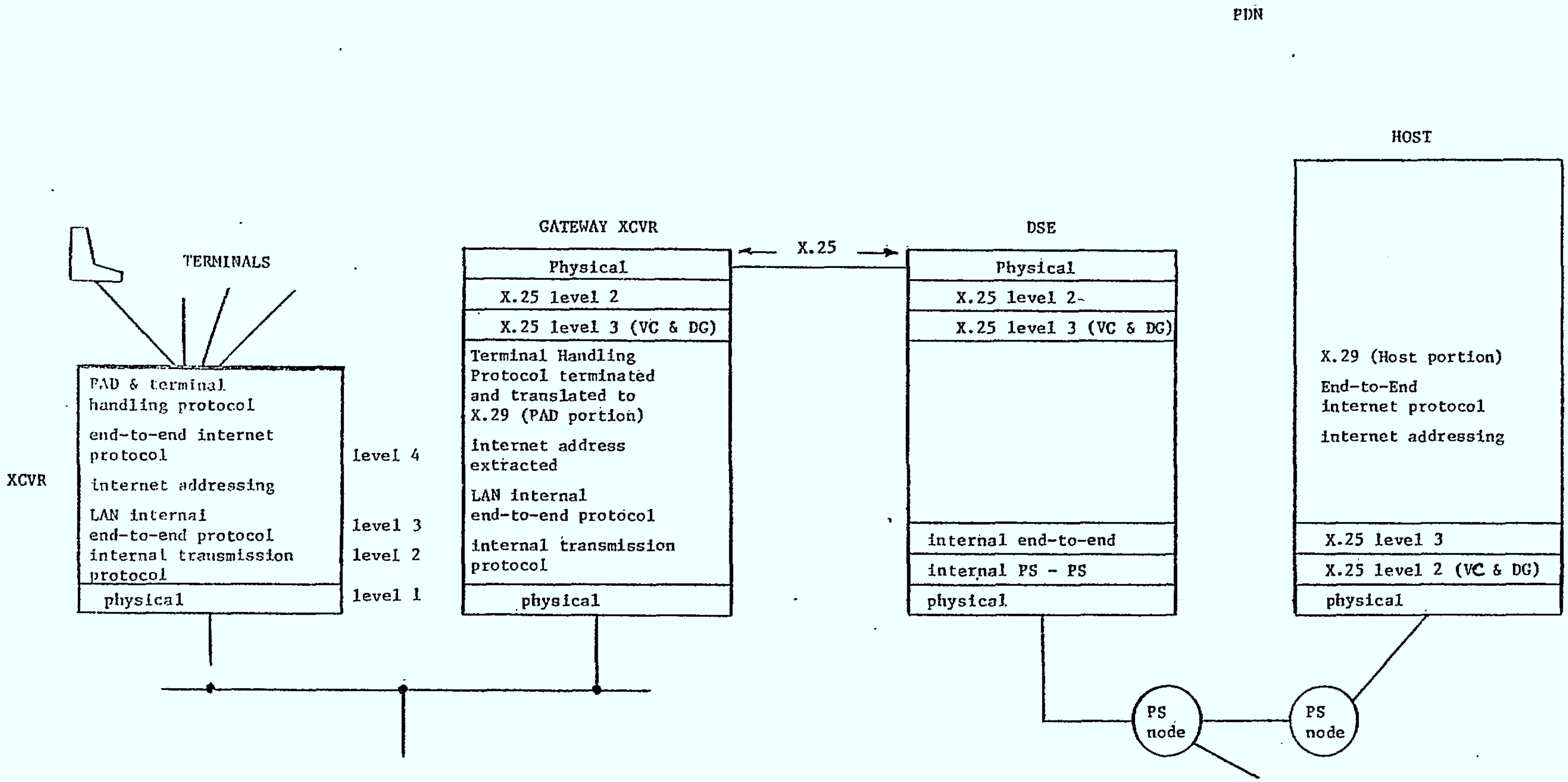


FIGURE 7.4 LAN Terminal Interworking With PDN Host Using VC Service on the LAN and X.25 VC or X.25 Datagram Service on the PDN, and an End-to-End Internet Protocol

The remote PDN host uses the end-to-end internet protocol and internet addressing. The PDN host would use the host portion of X.29 for an intranetwork virtual call with a terminal, so it is reasonable to use this same X.29 protocol entity for internetworking with terminals. Therefore, the gateway transceiver must perform all the functions described in Section 7.3 and it must transform the terminal handling procedures used on the LAN into the PAD portion of X.29 to accommodate the PDN host.

8. GATEWAY FUNCTIONS FOR STRATEGY 3

This section describes the layered protocol architecture and functions required at the gateway to provide internetwork services in a stepwise manner using a common internet protocol above each network's particular services.

This section considers four combinations of LAN services and user equipment. These are:

1. host on an LAN using unreliable datagram service,
2. host on an LAN using reliable datagram service,
3. host on an LAN using virtual call service, and
4. terminal on an LAN using virtual call service.

Two combinations of user equipment and PDN services are considered. These are:

1. host using X.25 datagrams, and
2. host using X.25 virtual calls.

The following subsections present the gateway functions required to provide internetwork service between all of the above combinations of user equipment and services which may interwork.

8.1 LAN Host Using Unreliable Datagrams Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

In figure 8.1, the encapsulation/extraction approach is used to provide internetwork service, on a stepwise basis, between a host on the LAN and a host on the PDN. Internet

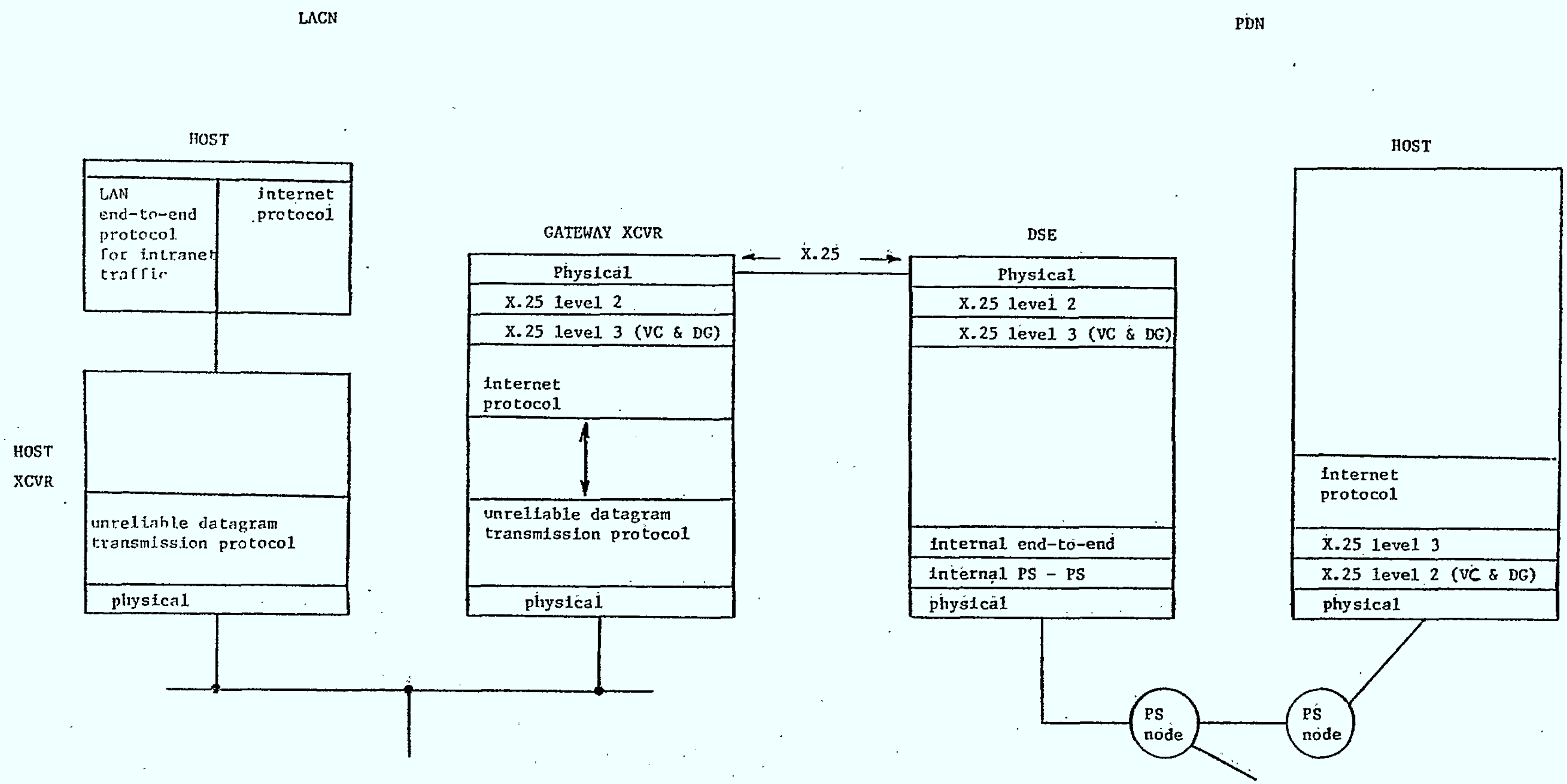


FIGURE 8.1 LAN Host Interworking with a PDN Host Using Unreliable Datagram Service on the LAN and X.25 VC or X.25 Datagram Service on the PDN and An Encapsulation/Extraction Internet Protocol

protocol entities are required at the gateway and in the hosts. These internet protocol entities provide the desired level of internetwork service for which they were designed among themselves, but use the unreliable datagram service for transmission in the PDN and use X.25 datagrams or virtual calls for transmission in the PDN.

The internet protocol includes the internet addressing and routing functions.

The LAN host must implement two protocols: an LAN end-to-end protocol for intranet traffic and the internet protocol.

8.2 LAN Host Using Reliable Datagrams Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

This case is identical to Section 8.1, except that the LAN offers reliable datagram service through the use of an LAN internal "end-to-end" protocol in the transceivers. The LAN host does not require an end-to-end protocol for intranet traffic.

8.3 LAN Host Using Virtual Call Service Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

This example is similar to Section 8.1, except that the internet protocol entities use VC service for data transmission in the LAN instead of datagram service.

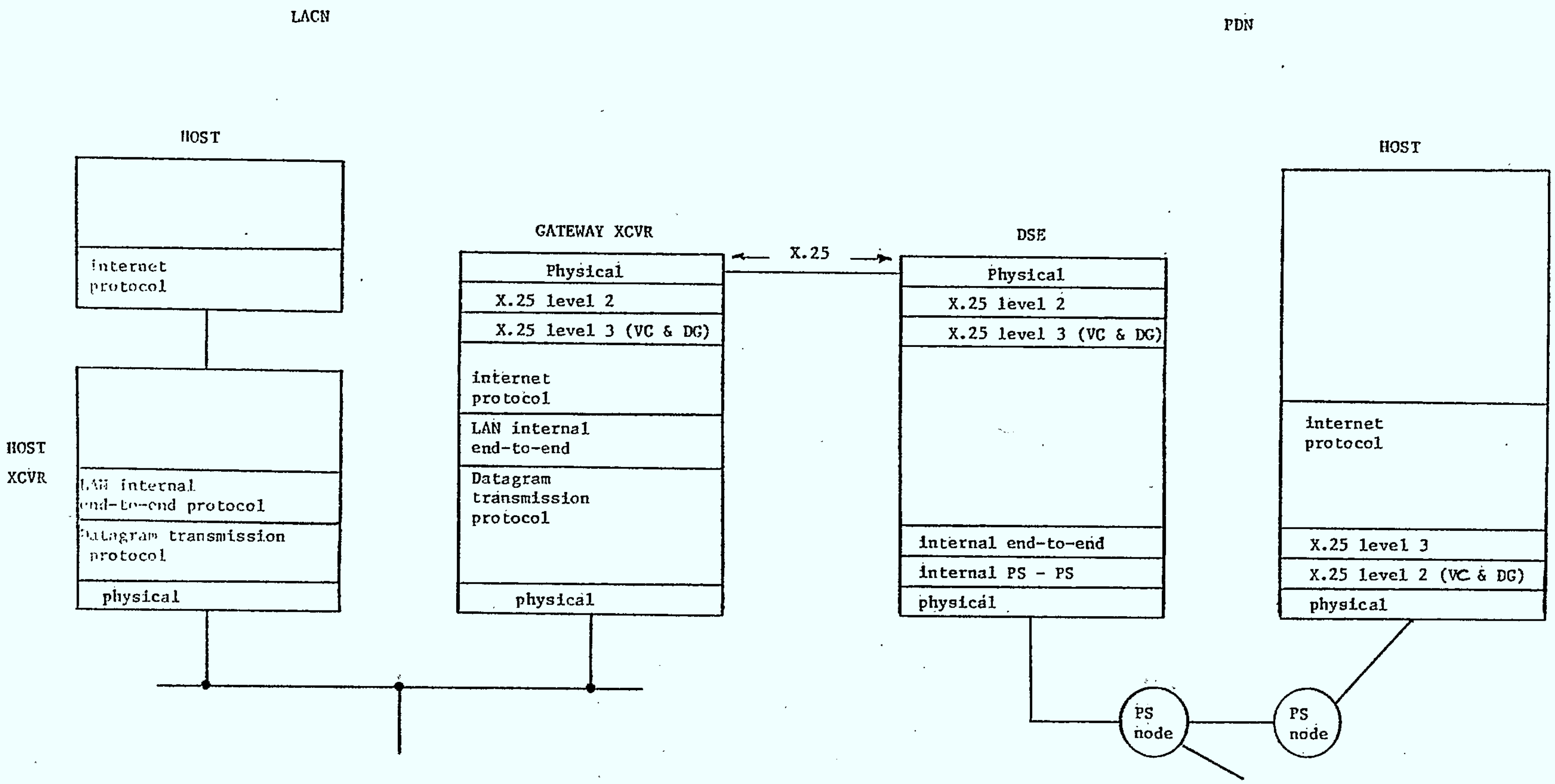


FIGURE 8.2 LAN Host Interworking with PDN Host Using Reliable Datagram Service on the LAN and X.25 VC or X.25 Datagram Service on the PDN and an Encapsulation/Extraction Internet Protocol

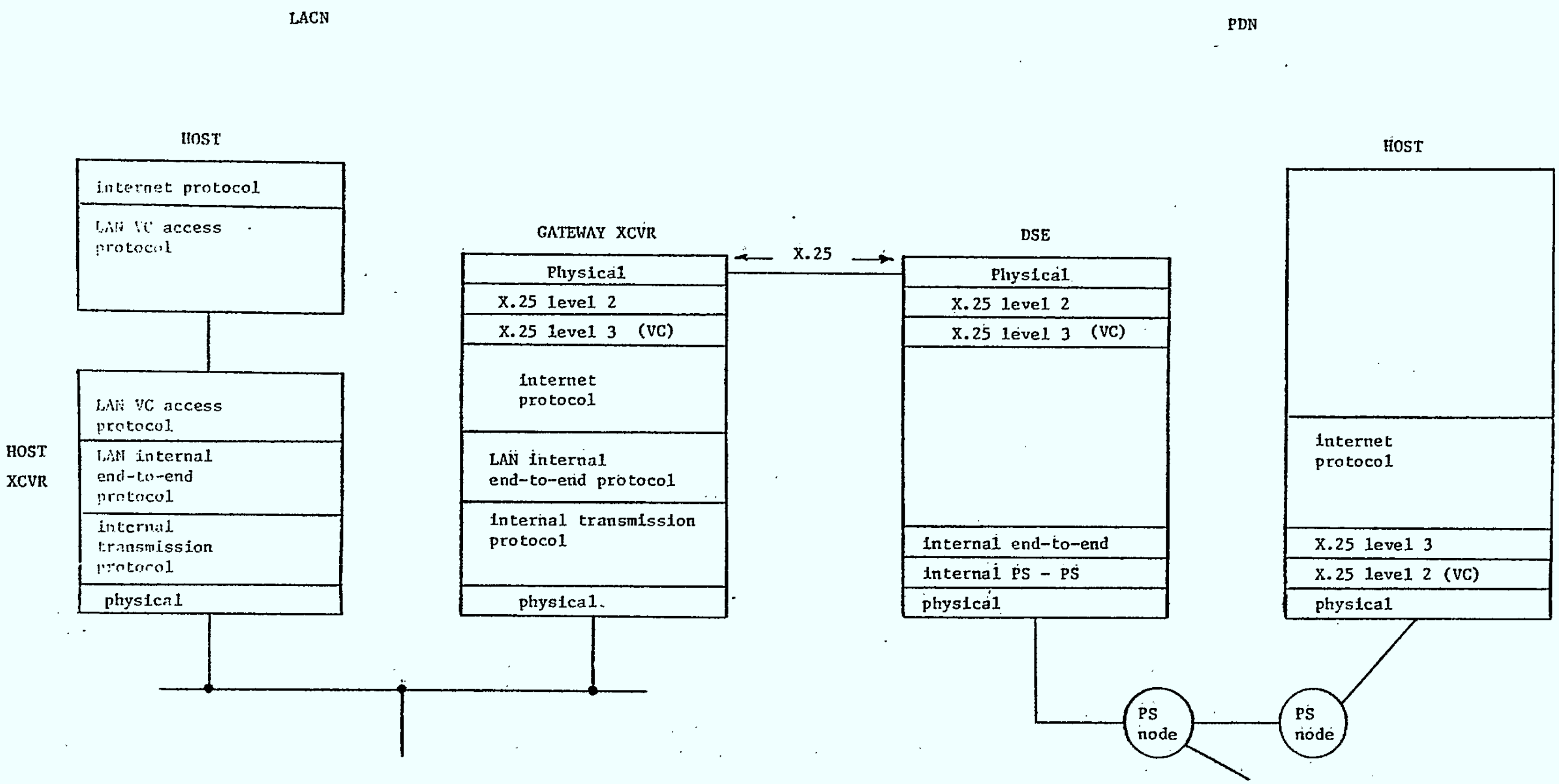


FIGURE 8.3 LAN Host Interworking With a PDN Host Using VC Service on the LAN and X.25 VC Service on the PDN, and an Encapsulation/Extraction Internet Protocol

8.4 LAN Terminal Using Virtual Call Service Interworking with PDN Host Using X.25 Datagrams or Virtual Calls

In this example, shown in figure 8.4, the gateway must transform the terminal handling protocols for the two networks, as discussed in Section 7.4. The internet protocol is transparent to the terminal handling protocols, because the terminal handling protocols are at a level above the internet protocol. To the internet protocol they appear to be data.

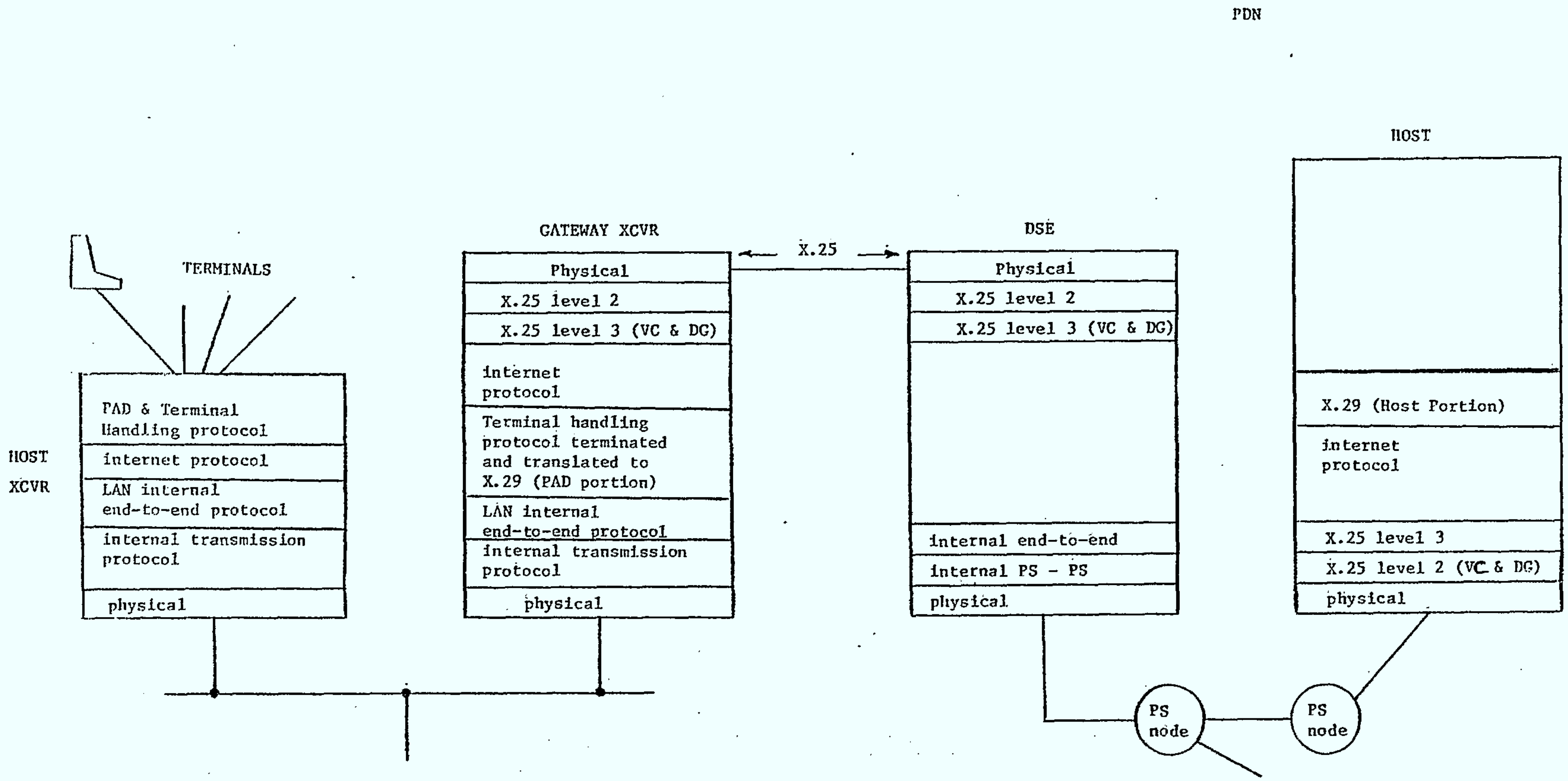


FIGURE 8.4 LAN Terminal Interworking with PDN Host Using VC Service on the LAN and X.25 VC or X.25 Datagram Service on the PDN and an Encapsulation/Extraction Internet Protocol

9. CONCLUSIONS AND RECOMMENDATIONS

This study has identified three types of approaches for the interconnection of Local Area Networks (LANs), excluding data services on PABXs, with Public Data Networks (PDNs). All of these approaches involve the use of a special gateway transceiver on the LAN which connects to the PDN via a host network access connection (eg. X.25). (PABXs do not require a special gateway transceiver because they act effectively as a dedicated data channel when connecting a user to a PDN.) The three approaches are:

a) stepwise provision of internetwork service with translations and protocol terminations at the gateway (eg. concatenated series of virtual calls);

b) endpoint provision of internetwork service based on a common level of service in both networks with an end-to-end protocol in the subscriber hosts; and

c) provision of internetwork service based on a stepwise series of encapsulations and extractions of internet packets by internet protocol entities residing in hosts and gateways. The internet protocol entities use whatever service is available in each network.

The protocol architectures and functions which the gateway must perform for each of the three approaches are described in Sections 6, 7 and 8, respectively. Although these sections use bus LANs to diagrammatically describe the details of the three interconnection strategies, the functions which must be provided by the gateway apply if the LAN is a bus, ring, or non-PABX star. A gateway designer would make use of this information by determining whether his LAN service best matches unreliable datagram, reliable datagram or virtual call service. He must then choose an interconnection strategy corresponding to one of sections 6, 7 or 8.

The last two strategies require that hosts and terminal PADs (Packet Assembler-Disassemblers) implement new protocol entities specifically for internetworking. This is a strong disadvantage, especially for PDN PADs, such as the Datapac NIM, which are already implemented and in service. Therefore, if a gateway designer wishes the internetwork service users to include terminal users on the PDN, we tentatively recommend that the use of a gateway which performs protocol translations and terminations (ie., the "transforming" gateway) should always be the first choice for the interconnection of LANs with PDNs. A firm recommendation must await a careful study of <u>all</u> costs and performances of <u>all</u> alternatives, which is unfortunately beyond the scope of this study. A more detailed description of the relative merits of the three interconnection strategies is given in Section 4.

The transforming gateway attaches to the Public Data Network as a subscriber, using the X.25 network access protocol. The gateway must terminate any LAN end-to-end protocols, virtual circuit protocols or reliable datagram protocols and extract a data bit stream (or packet stream) and an Internet Address for the destination DTE. If a host on the LAN is interworking with a PDN terminal, the gateway must translate the LAN terminal handling protocol (if there is one) to the host version of X.29. Similarly, if a terminal on the LAN interworks with a host on the PDN, the gateway must be conditioned to handle host X.29 packets from the PDN host and react similarly to a PDN Packet Assembler - Disassembler (PAD).

The third interconnection strategy, based on an inter-net protocol entity between levels 3 and 4, deviates from the Open Systems Interconnection Reference Model. The internet entity recognizes internetwork addresses, performs internetwork routing, fragments and reassembles packets and generally encapsulates data in the network level protocol format of the networks to which it is attached. These functions are not normally provided either by level 3 or level 4.

The endpoint approach to interconnection involves using a common transport protocol in all hosts and PADs which wish to interwork to provide a common internetwork transport service. While this is not, in principle, a deviation from the Open Systems Interconnection Reference Model, and although no unusual features are required in a Transport protocol for use on LANs, it is necessary to design an OSI Transport protocol carefully so that it interfaces correctly with the network level protocols on LANs, which are only now beginning to be designed.

Once a gateway designer has classified the LAN service and chosen the interconnection strategy he wishes to use, the gateway functions which he must implement are described in the appropriate subsection in Sections 6, 7 and 8.

PABXs which offer features for the digital transmission of data do not require gateway translations of the types described in this report. The PABX can provide the subscriber with a switched digital circuit directly to an X.25 Front End or a transceiver on the target LAN. Hence, PABXs should be simple to interconnect with PDNs and other LANs. Other advantages of PABXs include: they are designed to interconnect with the telephone system; they may use existing wiring; they not only provide data service but also telephone service; and they are reliable, flexible and expandable. Therefore, PABXs will be a very significant type of LAN.

Internetwork addressing and routing problems have been solved for international interconnection of PDNs by the adoption of the X.121 Numbering Plan. However, the X.121 designers did not allow for the potential attachment of thousands, or hundreds of thousands, of private networks to the PDNs. After examining the alternatives, we have devised and recommended a new numbering plan based on extending X.121 to 26 digits of length. This plan accommodates the use of the existing X.121 addresses for PDN subscribers, and also permits the use of 48 bit LAN addresses as proposed by Xerox for Ethernet and by the IEEE 802 Local Area Network Committee.

The extended 26-digit X.121 address we have proposed consists of up to 14 digits of X.121 address used to indicate a PDN address for a gateway to a private network (such as a LAN), followed by up to 12 hexadecimal digits which contain the private network address of the user on the LAN. Although this addressing system seems extremely simplistic, it is completely compatible with the current X.121 addressing system. Therefore, the Public Data Networks need not be changed to accommodate addressing for LAN interconnection. Furthermore, the extended 26-digit X.121 address overcomes problems such as international routing dilemmas which affect both the proposed X.122 and the Canadian CCITT Proposal for Private/Public Network Interworking.

We recommend that the impact of ISDN addressing requirements on this, or any, addressing proposal for the interconnection of private networks with public networks be studied before it is adopted. The danger is that extended 26-digit X.121 may be adopted without taking interworking with ISDNs into account, in the same way that X.121 was adopted while ignoring the prospect of LAN interconnection.

REFERENCES

[ALBAN82] A. Albanese and B.L. Kasper, "Bidirectional Lightwave Bus," Conference Record of the IEEE Global Telecommunications Conference, Miami, November 1982, pp. 872-874, vol. 2.

[CCITT80] CCITT Revised Recommendation X.75, "Terminal and Transit Control Procedures and Data Tranfer System on International Circuits between Packet Switched Data Networks," amended and approved by Study Group VII, February, 1980.

[DALAL81] Y. K. Dalal and R. S. Printis, "48-bit Absolute Internet and Ethernet Host Numbers," Proc. Seventh Data Comm. symp., pp. 240-245, Oct. 1981.

[DICIC79] V. F. DiCiccio, C. A. Sunshine, J. A. Field and E. G. Manning, "Alternatives for the Interconnection of Public Packet Switching Data Networks," Sixth Data Communications Symposium, Pacific Grove CA, 1979, pp 120-125.

[FOLTS80] H. C. Folts, "X.25 Transaction-Oriented Features-- Datagram and Fast Select," IEEE Trans. on Commun., Vol. Com - 28, no. 4, April 1980.

[HILI82] IEEE Project 802 High Level Committee, "Addressing and Local Networks," March 5, 1982.

[IEEE81] IEEE 802 committee "IEEE 802 Local Network Standard, Draft B," October 1981.

[JOHNS82] D.C. Johnson, P.W. Rivett and W.W. Davis, "Designing a Shipboard Bus with Biconical Taper Couplets," Proceedings of the Sixth International Fiber Optics and Communications Exposition, Los Angeles, September 1982, pp. 139-144.

[LOUCK82] Wayne Loucks, a seminar on Tornet presented at the University of Waterloo, Mar. 22, 1982.

[MANN81] Eric G. Manning, J. W. Wong, P. A. D. Powell, S. R. Radia, H. Tokuda, "Shoshin -- A Testbed for Distributed Software", Int. Conf. on Comm., June 1981.

[MARK80] J. W. Mark, "Distributed Scheduling Conflict-Free Multiple Access for Local Area Communication Networks," IEEE Transactions on Communications, December 1980.

[METCA76] R. M. Metcalfe and D. R. Boggs, "Ethernet-Distributed Packet Switching for Local Computer Networks," Communications of the ACM, July 1976, pp. 395-404.

[POST80] J. B. Postel, C. A. Sunshine, D. Cohen, "The ARPA Internet Protocol," Report of the Information Sciences Institute, Univ. of Southern California, Feb. 1980.

[RAWSO82] E.G. Rawson, R.V. Schmidt, R.E. Norton, M.D. Bailey, L.C. Stewart, and H.G. Murray, "Fibernet II: An Active Star-configured Fibre-optic Local Computer Network with Data Collision Sensing," Technical Digest of Topical Meeting on Optical Fiber Communication, Phoenix, April 1982.

[REAME] C. C. Reames and M. T. Liu, "Design and Simulation of the Distributed Loop Computer Network".

[SALTZ81] J. H. Saltzer and D. Clark, "Why a Ring?," Proceedings of the Seventh Data Communications Symposium, Mexico City, October 1981, pp. 211-217.

[SUNSH77] C. A. Sunshine, "Interconnection of Computer Networks," Computer Networks, vol. 1, pp. 175-195, Jan. 1977.

[SYTEK81] SYTEK Inc., "LocalNet System 20 Model 200 Packet Communications Unit Reference Manual, August 1981.

[TANEN81] A.S. Tanenbaum, "Computer Networks," Prentice Hall, 1981.

[TODD80] T. D. Todd and J. W. Mark, "Waterloo Experimental Local Network (WELNET) Physical Level Design."

[UNGER81] Ungerman-Bass, Inc., "Net/One Concepts and Facilities," 1981.

[UNSOY81] M. S. Unsoy and T. Shanahan, "X.75 Interworking of Datapac and Telenet," Seventh Data Communications Symposium, Mexico City, 1981, pp.232-239.

[WAIN81] P. F. Wainwright, "Internetworking Issues: Local Network Protocols," IEEE 802 HILI Subcommittee, October 1981.

[WILKE79] M. V. Wilkes and D. J. Wheeler, "The Cambridge Digital Communication Ring," Proceedings of the LACN Symposium, Boston, 1979, pp. 47-61.

[XEROX81] XEROX, Intel, DEC, "The Ethernet; A Local Area Network; Data Link Layer and Physical Layer Specifications," Version 1.0, Sept 1980.

APPENDIX A: A Summary of the Specifications of Various Local Area Networks

CAMBRIDGE RING

1. NAME: CAMBRIDGE DIGITAL COMMUNICATIONS RING

2. BASEBAND/BROADBAND: Baseband (uses two balanced channels between each pair of repeaters - a transition on one or the other channel signals at zero bit; a transition on both channels, signals a one bit)

3. TOPOLOGY OF COMM'NS PATH: ring with repeaters at each station

4. MEDIA: two twisted pairs or fibre optics between each pair of repeaters. Each twisted pair is a channel, therefore there are two channels between each pair of repeaters.

5. ACCESS CONTROL: -A fixed number of packets circulate the ring serially head to tail. Each packet has a full/empty indicator bit. An empty packet may be filled by a station and marked full.
   -Use of a source Select Register allows reception of a packet from all or any particular source.

6. SCHEDULING INFORMATION: global scheduling information

7. TRANSMISSION SPEED: 10 Mbps

8. LENGTH: 200 metre station separation for twisted pair; longer on fibre

9. MAX. STATION SEPARATION X BIT RATE PRODUCT: 2 Mbkm/s for twisted pair

10. EXTENSION CAPABILITIES: unknown

11. VARIABLE LENGTH PACKETS?: no
    MAX. LENGTH DATA FIELD: 2 bytes

12. RESOLUTION OF COLLISONS: no collisions

13. ADDRESS CAPACITY: 1 byte address

14. ERROR CONTROL OVER NET: 1 parity bit per packet; recovery from error at higher level

15. INTERFACE WITH HOSTS: Access boxes have been tailor-made to interface the hosts with the repeaters. These may operate in word-at-a-time or DMA mode.

16. PERFORMANCE: -low error rate
    -1 1/2 bit delay at each station

-approximate maximum effective data rate for each station
-is 4/(n+2) Mbps where n is the number of packets circulating the ring

17. SOURCE FOR INFORMATION: M. V. Wilkes and D. J. Wheeler, "The Cambridge Data Communication Ring," Proceedings of the LACN Symposium, May 1979, Boston. [WILK 79]

18. MISC NOTES: -power for each repeater is transmitted over the ring (50 VDC).
-2 bits allow 4 possible responses from the destination to the source station:

00	Destination Busy
01	Packet Accepted
10	Destination Deaf
11	Destination Absent

ETHERNET (XEROX PARC)

1. NAME: Ethernet (Xerox PARC) (Experimental Ethernet)

2. BASEBAND/BROADBAND: Baseband Transmission

3. TOPOLOGY OF COMM'NS PATH: Bus - unrooted tree

4. MEDIA: coax cable with CATV taps and connectors (optical fibre and twisted pair possible)

5. ACCESS CONTROL: CSMA-CD with binary exponential backoff

6. SCHEDULING INFORMATION: local scheduling information (CSMA-CD)

7. TRANSMISSION SPEED: 3 Mbps

8. LENGTH: 1 km.

9. MAX. STATION SEPARATION X BIT RATE PRODUCT: 3 Mbkm/s

10. EXTENSION CAPABILITIES:
    - packet repeaters between segments
    - traffic filters between segments
    - packet gateways between subnets

11. VARIABLE LENGTH PACKETS?: Yes
    MAX LENGTH DATA FIELD: approx 4000 bytes

12. RESOLUTION OF COLLISIONS: binary exponential back-off (wait a random interval with mean 2x previous interval's mean)

13. ADDRESS CAPACITY: max 256 stations

14. ERROR CONTROL OVER NET: CRC signalled (higher level protocol such as EFTP may be built into controllers to include ack, end, endreply, abort and data packet types)

15. INTERFACE WITH HOSTS: unknown/underdevelopment

16. PERFORMANCE: Efficiency is fraction of time the net is carrying good packets

    - if only one station has traffic, efficiency = 1 for all pkt lengths

    - if 10 stations have traffic:

	Packet Length (bits)			
	4096	1024	512	48
Efficiency	.9818	.9310	.8709	.3874

17. SOURCE FOR INFO: [METCA76]

ETHERNET (DEC, Intel, Xerox)

1. NAME: Ethernet (DEC, Intel, Xerox)

2. BASEBAND/BROADBAND: Baseband signalling (Manchester encoded)

3. TOPOLOGY OF COMM'NS PATH: bus - unrooted tree

4. MEDIA: coax cable

5. ACCESS CONTROL: CSMA-CD with binary exponential back-off

6. SCHEDULING INFORMATION: local scheduling information (CSMA-CD)

7. TRANSMISSION SPEED: 10 Mbps

8. LENGTH: 2.5 km.

9. MAX. STATION SEPARATION X BIT RATE PRODUCT: 25 Mbps

10. EXTENSION CAPABILITIES: repeaters and remote repeaters for connecting segments

11. VARIABLE LENGTH PACKETS?: YES

12. RESOLUTION OF COLLISIONS: Binary exponential back-off

13. ADDRESS CAPACITY: max 1024 stations

14. ERROR CONTROL OVER NET: CRC but no request for retransmission; erros are reported upwards from data link layer (level 2)

15. INTERFACE WITH HOSTS: datagram transmission and reception

16. PERFORMANCE: unknown

17. SOURCE FOR INFO: [XEROX81]

NET/ONE

1. NAME: Net/One by Ungermann-Bass, Inc.

2. BASEBAND/BROADBAND: Baseband

3. TOPOLOGY OF COMM'NS PATH: bus

4. MEDIA: coax cable (with adaptation to fibre optics in future)

5. ACCESS CONTROL: CSMA-CD

6. SCHEDULING INFORMATION: local information only (CSMA-CD)

7. TRANSMISSION SPEEDS: 4 Mbps

8. LENGTH: 1.2 km (longer with amplified repeaters)

9. MAX. STATION SEPARATION X BIT RATE PRODUCT: 4.8 km bits/sec

10. EXTENSION CAPABILITIES: segments may be joined by amplifiers or by gateway half nodes over a high speed based line.

11. VARIABLE LENGTH PACKETS?: unknown
    MAX. LENGTH DATA FIELD: unknown

12. RESOLUTION OF COLLISONS: back-off for a "variable randomized" time

13. ADDRESS CAPACITY: STATION CAPACITY is 250 STNS per 1.2 km segment

14. ERROR CONTROL OVER NET: CRC sent and packet discarded if received incorrectly

15. INTERFACE WITH HOSTS: Network Interface Unit can provide datagram or Virtual Circuit service (permanent or switched). Asynchronous or synchronous serial or parallel DMA connections to the subscriber are available.

16. PERFORMANCE: unknown

17. SOURCE FOR INFORMATION: Net/One Concepts and Facilities [UNGER81].

SYTEK LOCALNET 20

1. NAME: LocalNet System 20 Model 200 (SYTEK, Inc.)

2. BASEBAND/BROADBAND: Broadband (RF modulated)
   120 300 KHz channels

3. TOPOLOGY OF COMM'NS PATH: bus-rooted tree

4. MEDIA: coax cable - CATV system with bidirectional amplifiers and repeater (head end frequency translator) at root

5. ACCESS CONTROL: CSMA-CD

6. SCHEDULING INFORMATION: local scheduling information (CSMA-CD)

7. TRANSMISSION SPEED: 128 Kbps/channel

8. LENGTH: unknown

9. MAX. STATION SEPARATION X BIT RATE PRODUCT: unknown

10. EXTENSION CAPABILITIES: TBridges transfer packets among the individual channels

11. VARIABLE LENGTH PACKETS?: variable
    MAX. LENGTH DATA FIELD: unknown

12. RESOLUTION OF COLLISIONS: exponential back-off

13. ADDRESS CAPACITY: max. 8 terminals/station
    max. 200 terminals/channel
    max. 24,000 active terminals on network

14. ERROR CONTROL OVER NET: Yes - modified HDLC error and flow control

15. INTERFACE WITH HOSTS: similar to X.28 - subset

16. PERFORMANCE: unknown for total net
    max. throughput per station is approx. 20 Kbps

17. SOURCE FOR INFORMATION: [SYTEK81]

18. OTHER REMARKS: 70-106 MHz upstream channels (120)
    226-262 MHz downstream channels (120)

WELNET

1. NAME: WELNET (Waterloo Experimental Local Network)

2. BASEBAND/BROADBAND: Baseband signalling - Manchester encoding

3. TOPOLOGY OF COMM'NS PATH: main data channel - bus - unrooted tree

   scheduling aux channel - ring

4. MEDIA: two coax cables

5. ACCESS CONTROL: DSMA (Distributed Scheduling Multiple Access)

6. SCHEDULING INFORMATION: complete scheduling information

7. TRANSMISSION SPEED: 1 Mbps now, but can be increased

8. LENGTH: nominally 1 km.

9. MAX. STATION SEPARATION X BIT RATE PRODUCT: approx. 1 Mbkm/s

10. EXTENSION CAPABILITIES: not yet designed

11. VARIABLE LENGTH PACKETS?: variable length packets
    MAX LENGTH DATA FIELD: unknown

12. RESOLUTION OF COLLISIONS: no collisions occur

13. ADDRESS CAPACITY: 48 bits of station address with potential for up to 256 service access points each

14. ERROR CONTROL OVER NET: uses IEEE 802 LLC Type II (Logical Link Control Protocol - similar to HDLC) including flow control, sequencing, rejects, CRC

15. INTERFACE WITH HOSTS: simplified level 3 somewhat like L3 of X.25 - supports multiple virtual calls

16. PERFORMANCE: mean delay differs from perfect scheduling only by a small constant delay due to scheduling

17. SOURCE FOR INFO: [TODD80, MARK80]

WANGNET

1. NAME: WANGNET (Wang Laboratories, Inc.)

2. BASEBAND/BROADBAND: Broadband

3. TOPOLOGY OF COMM'NS PATH: bus; 2 trees; one for upstream data and one for downstream

4. MEDIA: commercial CATV cable and hardware such as unidirectional amplifiers and four-way multitaps

5. ACCESS CONTROL:

WANGBAND:	CSMA-CD
INTERCONNECT BAND:	Dedicated Channels and Circuit Switching
UTILITY BAND:	Broadcast Video and Environmental Sensors

6. SCHEDULING INFORMATION: WANGBAND: Local
   INTERCONNECT BAND (Dedicated circuits): Polling

7. TRANSMISSION SPEED: WANG BAND: 12 Mbps
   INTERCONNECT BAND: RS 449 Devices - 64 kbps
   RS 232 Devices - 9600 bps

8. LENGTH: nominally 2 miles

9. MAX. STATION SEPARATION X BIT RATE PRODUCT: 38.4 Mbkm/sec

10. EXTENSION CAPABILITIES: connects with leased-lines, "switched line networks", satellite links, microwave links and other WangNets via "gateways".

11. VARIABLE LENGTH PACKETS?:
    MAX. LENGTH DATA FIELD:

12. RESOLUTION OF COLLISIONS: exponential binary back-off

13. ADDRESS CAPACITY: 65,535 user devices

14. ERROR CONTROL OVER NET:

15. INTERFACE WITH HOSTS: WANG BAND provides virtual circuit capability
    but can only be used by WANG computer

16. PERFORMANCE: unknown

17. FREQUENCY ALLOCATIONS:

BAND	FREQ	USE
Interconnect	10-12 MHz	32 RS-232 dedicated channels
Interconnect	12-22 MHz	16 RS-449 dedicated channels
	22-48 MHz	Reserved
Interconnect	48-82 MHz	256 RS-232 circuit switched channels (using one Wang Data Switch) dynamically allocated
	82-174 MHz	Reserved
Utility	174-216 MHz	seven 6 MHz standard CATV video channels - (channel 7-13)
Wang	217-251 MHz	CSMA-CD network

18. SOURCE OF INFORMATION: "WANGNET", Wang Laboratories, Inc., Lowell, Mass., 1981.

HUBNET

1. NAME: Hubnet (developed at University of Toronto)

2. BASEBAND/BROADBAND: baseband

3. TOPOLOGY OF COMM'NS PATH: star (hierarchical star is possible)

4. MEDIA: fibre optics

5. ACCESS CONTROL: FCFS (First Come First Served)
   -entire net can transmit only one subscribers data at a time.

6. SCHEDULING INFORMATION: local information for performing carrier sensing

7. TRANSMISSION SPEED: 50 Mbps

8. LENGTH:

9. MAX. STATION SEPARATION X BIT RATE PRODUCT:

10. EXTENSION CAPABILITIES:

11. VARIABLE LENGTH PACKETS?:
    MAX. LENGTH DATA FIELD:

12. RESOLUTION OF COLLISONS: "Collisions" do not actually occur. The hub switches select one subscriber's data for retransmission and the others retry after a preset wait interval.

13. ADDRESS CAPACITY:

14. ERROR CONTROL OVER NET:

15. INTERFACE WITH HOSTS:

16. PERFORMANCE:

17. SOURCE FOR INFORMATION:

18. MISC NOTES:

TORNET

1. NAME: TORNET (University of Toronto)

2. BASEBAND/BROADBAND: baseband

3. TOPOLOGY OF COMM'NS PATH: hierarchical ring

4. MEDIA: twisted pair

5. ACCESS CONTROL: partial insertion slotted ring (compromise between Cambridge ring and register insertion)

6. SCHEDULING INFORMATION: global - no collisions because of slots

7. TRANSMISSION SPEED: 1 Mbps currently but 10 Mbps possible

8. LENGTH: limited by RS-442

9. MAX. STATION SEPARATION X BIT RATE PRODUCT:

10. EXTENSION CAPABILITIES: Tornets may be interconnected by a Tornet, leased lines or a PDN. (X.25 interface currently under development)

11. VARIABLE LENGTH PACKETS?: Yes
MAX. LENGTH DATA FIELD: 1, 2 or 129 data bytes

12. RESOLUTION OF COLLISONS: no collisions

13. ADDRESS CAPACITY: 8 bits although a name server is planned

14. ERROR CONTROL OVER NET: parity now and CRC on long packets in future. Control bit set by destination when parity doesn't check.

15. INTERFACE WITH HOSTS: RS-232 now
DMA in future

16. PERFORMANCE: not known

17. MISC.: source removes data after it has gone around the ring past the destination. Destination sets 2 response bits:

0 0 - not seen by dest.

0 1 - unused

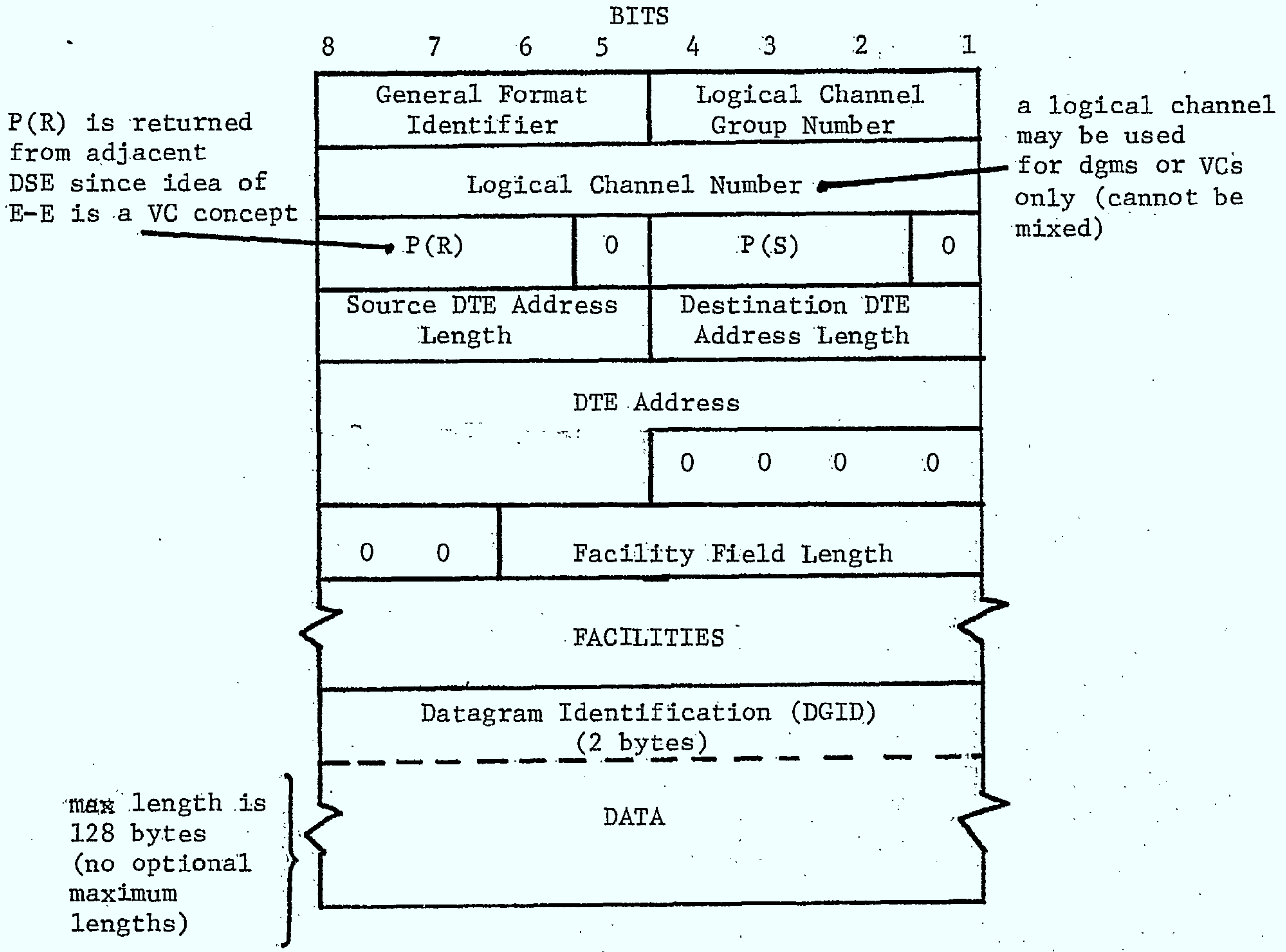
1 0 - rec'd O.K.

1 1 - dest. rejected (full buffers
selective receive)

18. SOURCE FOR INFORMATION: [LOUCK82]

APPENDIX B: X.25 Datagram Packet Format

DATAGRAM PKT FORMAT:



Signals Returned by Network (in DATAGRAM SERVICE SIGNAL SPECIAL PACKET)

DATAGRAM REJECTED ⟶ datagram rejected or discarded by the network

NONDELIVERY INDICATION ⟶ datagram rejected or discarded by the network

DELIVERY CONFIRMATION ⟶ optional by subscription or by faculty request

These refer to the datagram by the DGID

Additional Packets Used in Datagram Service

- Flow Control
- Reset
- Restart
- Diagnostic

APPENDIX C: The Canadian CCITT Contribution entitled "Alternative Proposal for Private/Public Network Interworking"

INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE (CCITT) | CAN COM VII-51

PERIOD: 1981-1984 | ORIGINAL: ENGLISH
QUESTION: 4&41/VII | DATE: 1982-03-01

For Special Rapporteur meeting in Melbourne, March 1982.

SOURCE: CANADA

TITLE: Alternate Proposal for Private/Public Network Interworking

1.0 INTRODUCTION

At the Kyoto meeting, Canada submitted a document (D43), in response to COM VII-37, which suggested that alternative methods be considered for addressing to interwork between public and private data networks Having considered the subject, and also considering the proposals for concatenation of networks in the Reference Model (Q27), this submission proposes a method which requires no alteration to existing numbering plans. The proposal is for the definition of additional facilities for conveyance of extended addresses. The major functionality will reside in the gateway/relay point and not affect network operation.

2.0 PROPOSAL

2.1 Objectives

A workable solution to interworking between public and private data networks should meet the following criteria:

- -allow for varying address structures in private networks.
- -allow routing to be independent of network addressing schemes.
- -allow for varying levels of intelligence in both public and private data networks.
- -maintain compatibility with the PDN numbering plan defined by Recommendation X.121.
- -permit shared X.121 address space and/or sub-addressing schemes.
- -be compatible with the Network Layer of the Reference Model.
- -no practical limits on the number of private networks.
- -apply equally to PDNs based on Rec. X.21 and Rec. X.25.
- -allow multiple connected networks.

2.2 Method

For very practical reasons all networks which interwork do so through some form of gateway or relay point. Given this situation and noting that several Administrations have already suggested methods for handling extended addresses (e.g. by means of a separator character in Rec. X.21 or via the facility fields in Rec. X.25) we propose an expansion of this technique.

The calling DTE would provide the required address(es) in the call request in a form such that:

a) the calling address contains the originating address and the called address contains the destination address as seen by the network currently handling the call request.

b) address extensions would be included (in sequence) by relay point.

c) address extensions would be marked to indicate: 1) next relay point and 2) forward or backward chain.

As an example, for a Rec. X.25 network a D type facility could be defined which would include the following:

```
 D type facility code
+facility length (<=62)
+relay point addr. length and flags (<=?)
+relay point addr. digits
        .
        .
+called DTE addr. length and flags (<=?)
+called DTE addr. digits
```

Note 1: A maximum length for addresses needs to be selected. Obviously if the destination address is 61 digits there would be no room for a relay point address. Some maximum must be selected.

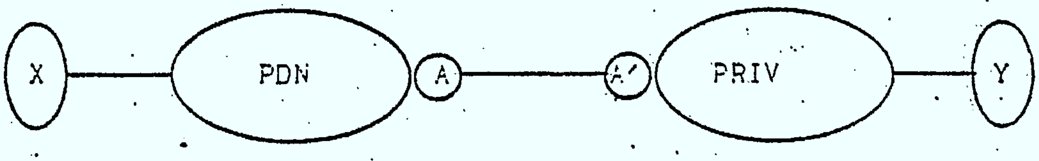
Note 2: Some rules regarding conventions to govern the placement of relay point addresses and usages of these fields need to be formatted.

2.3 Examples

Note: In the following figures the legend is:

- OA=Originating address as seen by the network
- DA=Destination address as seen by the network
- FRP=Forward relay point(s) in sequence
- BRP=Backward relay point(s) in sequence

2.3.1 DTE on a PDN calling a DTE on a private network.

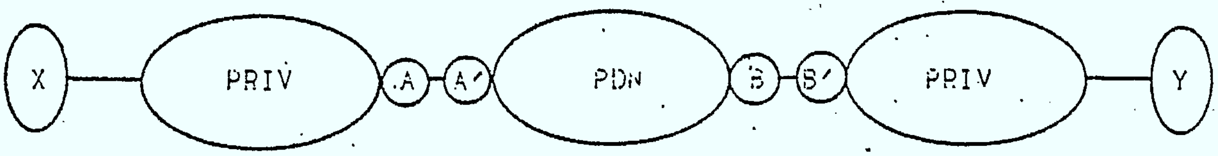


Address		
	OA=X	OA=A′
	DA=A	DA=Y
	FRP=Y	BRP=X

2.3.2 DTE on a private network calling a DTE on a PDN.

This is the same as 2.3.1 only the position of PRIV and PDN are reversed.

2.3.3 DTEs on private networks interconnected by a PDN.



Address			
	OA=X	OA=A′	OA=B′
	DA=A	DA=B	DA=Y
	FRP1=B	FRP=Y	BRP1=A′
	FRP2=Y	BRP=X	BRP2=X

Note 1: In Fig. 2.3.1 X and A are Rec. X.121 addresses.
In Fig. 2.3.3 A′ and B are Rec. X.121 addresses.

Note 2: Shared addressing space and/or sub-addressing schemes would work as well as disjoint addressing schemes.

Note 3: Whether the PDN is a single PDN or concatenated PDNs does not influence the figures as only a single Rec. X.121 address is required.

Note 4: The concept used for gateways/relay points is of a recognized address on each network (e.g. A and A') with some interface between them.

3.0 Further Study Points

The following items require further study;

- exact format of extension address fields.
- maximum relay point address length.
- non numeric coding of relay point addresses (i.e. a 4 digit field permits 0 to 9 and A to F).
- rules of operation for relay points.
- flags to indicate 'next' relay point and forward or backward chain direction.

4.0 Conclusions

This proposal offers many advantages, the following being among the more important ones;

- very flexible.
- no impact on existing numbering plans.
- no impact on internal routing methods of existing or future networks.
- allows for billing/accounting.
- user problems may be alleviated by intelligence in networks.

In effect all that is required is to standardize the method of carrying the extended address facility. All of the management of these addresses takes place in the gateway/relay point such that the network sees a Call Request of a type it is prepared to handle. (i.e., The originating and destination address fields will have the addresses appropriate to the network type)