DOCID: 3929121

Approved for release by NSA on 12-01-2011, Transparency Case# 63852

The PLATFORM Network Evolution (U)

STATUTORILY EXEMPT

This paper, written in 1989, describes the PLATFORM wide area network (WAN) evolution. A brief history describing how PLATFORM arrived at its current, problematic state will be followed by a discussion of the adaptive strategies that are being implemented on PLATFORM today, and finally the future directions of PLATFORM. Items addressed will include descriptions of the present and future PLATFORM networks, hardware and software changes required (protocols, gateways, IMPs (Interface Message Processor)), and the driving forces behind the changes.

I. INTRODUCTION

The National Security Agency has consistently been in the forefront of leading technological advances. One area of technology that has had a tremendous impact on the Agency's mission is computer networking. In the mid-1970s, PLATFORM became NSA's wide area network (WAN), and for several years PLATFORM improved efficiency throughout the Agency. But as Agency elements increasingly took advantage of PLATFORM's resources, problems developed, and it became apparent that the original network design had become outdated.

Over the years, the Agency's continual expansion has hindered the timely implementation of new technological developments. When NSA acquires state-of-the-art advances, implementing these advances without breaking anything is an art in itself. Much planning and replanning are required. PLATFORM is the object of such planning in the form of the PLATFORM Network II Upgrade. New hardware and software will be installed on PLATFORM with minimal service interruption as a major goal.

The purpose of this paper is to present the fundamental technological aspects of the PLATFORM network – past, present, and future. A background discussion will reveal the source and nature of PLATFORM's problems followed by architectural descriptions of the PLATFORM networks I and II. Some basic internetworking concepts and their application to the PLATFORM Network II Upgrade will also be discussed.

In addition to the PLATFORM WAN, other networking developments have surfaced in the Agency as part of the User Interface System (UIS) architecture. (UIS addresses the connectivity issues encountered by placing a workstation on the desk of every NSA analyst.) As a result, local area networks (LAN) such as ASHLAND and CLOVER have entered the Agency networking picture. This paper is about the PLATFORM network evolution; thus, the superset formed by PLATFORM with other Agency networks is beyond the scope of this paper.

~~FOR OFFICIAL USE ONLY~~

II. BACKGROUND

A. History of PLATFORM

In September 1969, the first packet switching computer was connected to a Sigma 7 computer at UCLA, and the Advanced Research Projects Agency Network (ARPANET) was born [9]. This blessed event by the Defense Advanced Research Projects Agency (DARPA) was perpetuated by a variety of universities, industries, and government research facilities across the United States. By the mid-1970s, ARPANET computers were communicating around the world.

In 1974, Bolt, Beranek, and Newman, Inc. (BBN) released the final report for an NSA network study [10]. Of particular interest in this document were the NSA PLATFORM network's original requirements, which included

1. an initial configuration consisting of four different host computers, expanding to an eventual size of about twenty-five host complexes with from one to five hosts per complex (i. e., a maximum of 125 hosts),
2. collocation of all network hosts in the NSA building complex, and
3. use of the ARPANET protocols and Network Control Programs.

Some other requirements concerned reliability, security, synchronous and asynchronous terminals, and traffic needs. Although all of the requirements appeared valid at the time, most of them would cause problems in the future [10].

B. Problems with PLATFORM

It took over a decade, but PLATFORM began to feel confined by its original requirements. Degrading performance, growth limits, and the expense of NSA-unique hardware and software became major problems. The following network design limitations had surfaced [1]:

1. ADDRESSING – Using a virtual host addressing (VHA) scheme simplified address table management. Since logical addresses were mapped to physical ones, a host could move physically yet retain its one-up VHA number. However, software implementations stored this address in an 8-bit entity, thus allowing for a maximum of only 255 hosts. (There is no host 0.) When PLATFORM reached this limit in 1987, a major software upgrade was necessary on all PLATFORM hosts to handle VHAs greater than 255. With the arrival of LANs, the address issue became more complicated.

2. NETWORK GROWTH – With the ever-growing network and an "everyone knows everyone" philosophy, performance and network management were fast becoming a nightmare.
3. PRIORITY HANDLING – PLATFORM had none since it used a fairness algorithm (i.e., everyone gets a turn).
4. ROUTING ALGORITHMS – Since PLATFORM's original concern was minimizing delay, it became apparent later that reliability and throughput were also important considerations for certain applications. Current algorithms were outdated.
5. BANDWIDTH DISPARITIES – Since uniform bandwidths were originally assumed, varying bandwidths across the subnet caused thrashing.
6. NONSTANDARD HARDWARE/SOFTWARE – The 1822 hardware interface and the NCP/1822 protocols that were required to hook into PLATFORM were not off-the-shelf products.

The last problem could not really be avoided although perhaps better anticipated. A need for standards was recognized before 1980, but NSA has been slow to move toward the standards that the Defense Data Network (DDN) and ARPANET have been operating under since 1983 [4]. Although NSA is undoubtedly a huge and complex entity, the "we are special" philosophy has created a very expensive collection of nonstandard hardware and software products that continue to be costly to create and maintain.

III. CURRENT PLATFORM TECHNOLOGY

A. *PLATFORM Network I Architecture*

PLATFORM Network I (PN-I) has existed for over a decade as a system of heterogeneous hosts connected to a packet switching network (subnet). Based on the ARPANET technology of the time, each host is connected to an Interface Message Processor (IMP) that is part of the subnet. A message from a host is sent to its IMP, which disassembles the message into packets. These packets are then sent through the subnet of IMPs to the IMP of the destination host where the packets are reassembled before delivery to the host [2]. (See fig. 1.)

Hardware Configuration

The multitude of hardware used in PN-I is inevitable because of the size and diversity of NSA applications. Users choose hardware technology based on needs, and there is no universal network from a single hardware technology that satisfies all uses [12]. The major original hardware components of PN-I are broken down as follows [2]:

DOCID: 3929121

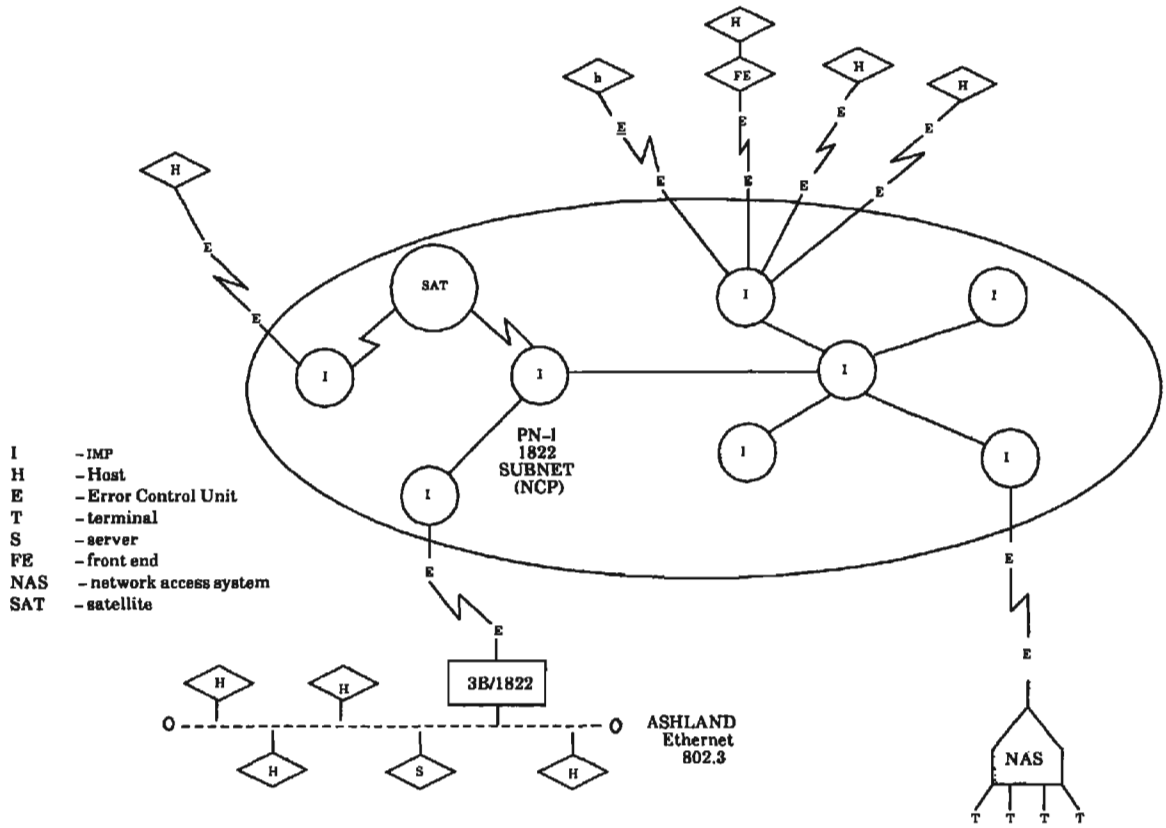


Fig. 1. PLATFORM Network I

1. HOSTS – Probably just about every major vendor has hardware on PLATFORM (IBM, DEC, Honeywell, CDC, etc.). Of course, each type of host had to provide hardware and software interfaces to operate on PLATFORM, an astronomical effort and expense.

2. IMPS – Currently all PN-I IMPs are C/30E members of the BBN C/30 family of packet switched nodes (PSN).

3. FRONT ENDS – These are PDP 11/35 systems that implement the network access protocols so that hosts that do not implement these protocols may connect to an IMP through a front end (FE).

4. NETWORK ACCESS SYSTEM (NAS) – These systems are PDP 11/34 systems that provide FE protocols as well as user-level protocols so that terminals may access PN-I systems through a NAS.

5. ERROR CONTROL UNITS (ECU) – These boxes are used in pairs when a host and its IMP are more than thirty feet apart. Their function is self-explanatory.

6. NETWORK MONITORING AND MANAGEMENT COMPUTER (NMC) – these PDP 11/70 systems collect status and statistical information from the IMPs for network management purposes [13].

7. PLATFORM SERVERS – With the arrival of the Agency Standard Host (ASH) came ASHLAND, a collection of collocated AT&T 3B20 and 3B15 UNIX System V computers interconnected by Ethernet and HYPERchannel. PN-I had reached the maximum host limit of 255. The introduction of PLATFORM servers (AT&T 3B20s) allowed hosts on the Ethernet to access PLATFORM through a server host. The only host requiring a VHA was the server itself. A more detailed discussion of servers will follow.

Software Configuration

PN-I has a set of software guidelines called protocols, which are implemented in IMPs, FEs, NASs, and/or hosts. Again, based on the ARPANET of the time, these protocols are divided into four layers [3].

1. IMP-to-IMP – This protocol governs communication among IMPs.

2. IMP-to-HOST – This protocol specifies the physical and logical message transfer between a host and its local IMP and is defined in BBN Report No. 1822 (hence the protocol name: 1822). It is not sufficient, however, to specify communications between dissimilar hosts, thus the need for layer (3).

3. HOST-to-HOST – The functions of this protocol are to establish communications paths and to provide a means for hosts to allocate buffer space and deliver interrupts. The Network Control Program (NCP) is the implementation of layers (2) and (3) on PLATFORM. The Initial Connection Protocol (ICP) is sometimes

referred to as a separate layer; however, ICP just uses NCP to establish a pair of connections to allow a process on one host to communicate with a process on another host. NCP provides the undercarriage for all higher-level protocol implementations [11].

4. User Level – The PN-I application protocols [2] are as follows:

   telnet – a network virtual terminal capability

   cftp – controller file transfer protocol; also a remote execution capability

   rlp – resource location protocol; allows software on one system to poll a family of computers to determine the availability of a resource (e.g., cftp or M204)

   dcp – direct connection protocol; for short message transfers

   fe – defines communication between a host and the front-end processor handling its network access

   nap – network access protocol; allows a host to be connected through an NAS as if it were a terminal.

Note that there is no separate mail protocol. CFTP included mail functionality by defining a file class "ma," although few systems ever implemented this. UNIX systems provided this functionality through their implementation of ARPANET FTP, not to be confused with the PN-I file transfer protocol (CFTP).

B. PLATFORM Network II Architecture

PLATFORM Network II (PN-II) is modeled after the Defense Data Network in an attempt to take advantage of DDNs internetwork advances and more economical standard products. PN-II is NSA's major effort to overcome the PN-I limitations, yet it is only the beginning of an ongoing effort to prepare for the future. The major conceptual difference between PN-I and PN-II is that ideally PN-II will have no directly connected hosts (pragmatically, there are a few exceptions). Just like PN-I, PN-II has a subnet of IMPs, but hosts access PN-II from LANs via gateways. (See fig. 2.)

Hardware Configuration

1. HOSTS – Any host directly accessing PN-II must use the DoD standard suite of protocols and thus any hardware interface that will facilitate that.
2. IMPS – The C/30X is the C/30 family member that uses the DoD standard X.25 network access protocols. To aid the PN-I and PN-II merger, a C/30 Hybrid IMP that talks both X.25 and 1822 will be introduced. C/300 IMPs will be deployed when higher speeds are required.

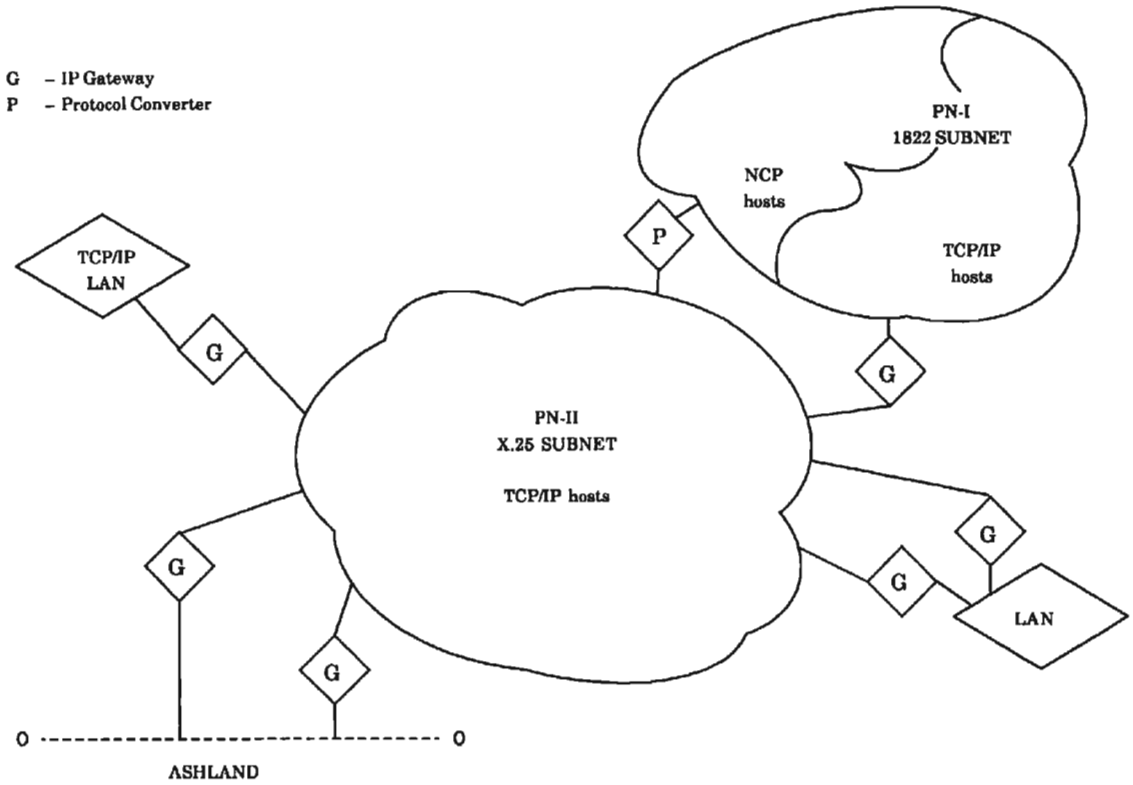


Fig. 2. PLATFORM Network II

~~FOR OFFICIAL USE ONLY~~

3. NMC – Initially, PN-II will be a completely separate network from PN-I and thus will require its own monitoring system.

4. PLATFORM Servers/Protocol Translators – Currently the ASHLAND server hosts on PN-I are providing services in addition to the sharing of a VHA among several hosts. These AT&T 3B20s are also gateways, more specifically, protocol translators. A protocol translator allows a PN-I host talking NCP to communicate with a PN-II host talking TCP/IP (Transmission Control Protocol/Internet Protocol). The introduction of SACRUM protocol translators (AT&T 3B15s) will eventually allow servers to go away.

5. IP GATEWAYS – These boxes will allow hosts on various types of LANs (HYPERchannel, Ethernet, PROnet, etc.) to communicate with other hosts that access PN-II. Evaluation of available gateways will determine the hardware chosen [11].

Software Configuration

PN-II has adopted the DoD standard suite of protocols. The layers of protocols are similar to those of PN-I. Among the big advantages of converting to these "new" protocols (released in 1981) are the introduction of an internetworking layer and a line of commercially available products. The PN-II network layers are as follows [8]:

1. NETWORK ACCESS – The PN-II X.25 protocol defines the communication between a host or gateway and an IMP of the subnet. The protocol is based on the CCITT X.25 Recommendation (1980), which defines layers 1–3 of the OSI network model. Adhering to the X.25 standard allows communication not only between hosts using different vendor-supplied X.25 implementations, but also between hosts where one is using the X.25 interface and another is using the 1822 interface. However, interoperability requires that both hosts use standard higher-level protocols [3].

2. INTERNET – The Internet Protocol (IP) allows data to be routed among multiple networks.

3. HOST-to-HOST – The Transmission Control Protocol (TCP) provides a reliable data transport service across networks and internets.

4. APPLICATIONS - The PN-II application protocols are as follows:

   telnet – a network virtual terminal capability

   ftp – a file transfer capability that is not compatible with cftp

   cftp – controller file transfer protocol; an NSA specific protocol whose future is presently being argued

   smtp – simple mail transfer protocol; the Berkeley UNIX program "sendmail" is a popular implementation

NSA is currently using its own mail protocol based on the old ARPANET ftp protocol. Although similar to smtp, it is not compatible. PN-II systems are capable of using smtp among themselves; however, exchanging mail with PN-I systems requires use of the Agency-specific software.

IV. NETWORK TECHNOLOGY

A. ARPANET as model for PLATFORM (past and future)

In the beginning there was ARPANET, a mechanism that allowed communication between heterogeneous computers. NSA adopted the hardware and software as a basis for its own PLATFORM network. The Agency made the following additions to the ARPANET NCP [11]:

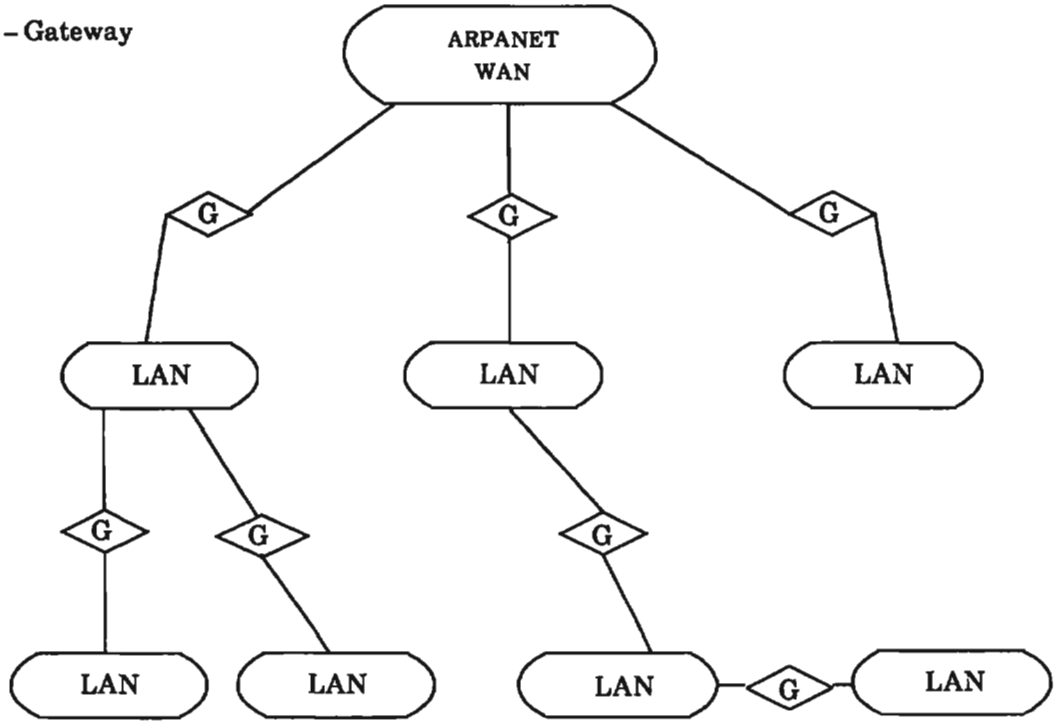
1. a pipelining connection service
2. two security commands
3. a data classification field in the packet header
4. a close code field to provide a reason for closing a connection

NSA then developed and implemented its own protocols on a variety of computer systems. In the meantime, DARPA began to research the next DoD requirement – the interconnection of multiple packet switched networks. As ARPANET grew, DARPA realized that interconnecting several WANs would improve efficiency over using one large network. This effort resulted in "an architecture and set of protocols to accomplish this robust system of interconnected networks [6]." (See fig. 3.)

PN-II is NSA's adoption of this effort. It is important to remember that the current ARPANET internet system "is constantly evolving with new functions and new protocols being developed to meet the everchanging military requirements [6]." NSA has learned the importance of working with government standards organizations (e.g., GOSIP – Government Open Systems Interconnection Profile) to produce standards that satisfy NSA requirements as well. NSA by definition is security conscious and has imposed security requirements on PLATFORM. For example, HAC (host access codes) and SAC (service access codes) allow a system to protect itself from unwanted network access. However, these implementations are Agency specific. With the publicity of viruses, the wide-open access of the DARPA Internet Model was made obvious along with the importance of imposing more security requirements on standards.

NSA will (and should) continue to take advantage of the ARPANET model as well as participate in any standards and protocol development. The International Organization of Standards (ISO) standards effort will be playing a key role in a future ARPANET iteration.

G – Gateway



PSN – Packet Switched Network (WAN or LAN)

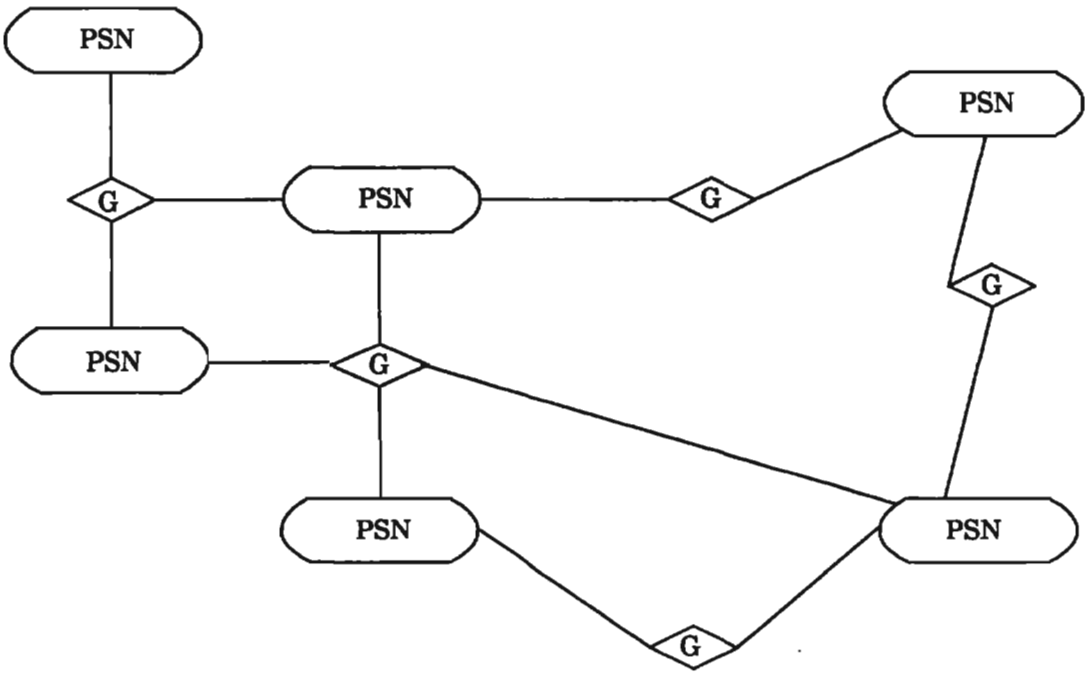


Fig. 3. ARPANET Models

B. Network Interoperability

The major goal in the PN-II effort is interoperability among heterogeneous networks. The Internet Protocol (IP) is the key to providing gateways between these different networks. IP centers on the Internet Address, an addressing scheme that is independent of addresses used in the individual networks forming the internet. In addition to this routing function, IP also performs fragmentation and reassembly of packets if necessary because of maximum packet size constraints on a particular network. IP allows a host to be insulated from any routing concerns. A host just delivers a message to its local network, and IP handles delivery to the destination host [6].

Heterogeneous networks are interconnected via gateways. A gateway may be an actual processor connected between two networks, or it may be additional software implemented in existing processors in one or both nets [7]. Two major gateway tasks are (1) interfacing to local nets and (2) performing IP functions including global addressing, error and flow control, access control, fragmentation and reassembly, and accounting. Gateways provide internet service via IP, which must be implemented in host computers engaged in internet communication as well as gateways [5].

A simplistic view of IP gateway operation follows. An IP packet is wrapped in the local network header. The gateway strips the header to extract the IP packet. The internet address of the destination is used to route the packet to another gateway or to the final destination host. But first the IP packet is reembedded for transmission through the next local network. Local networks are totally unaware when they are carrying internet traffic [7].

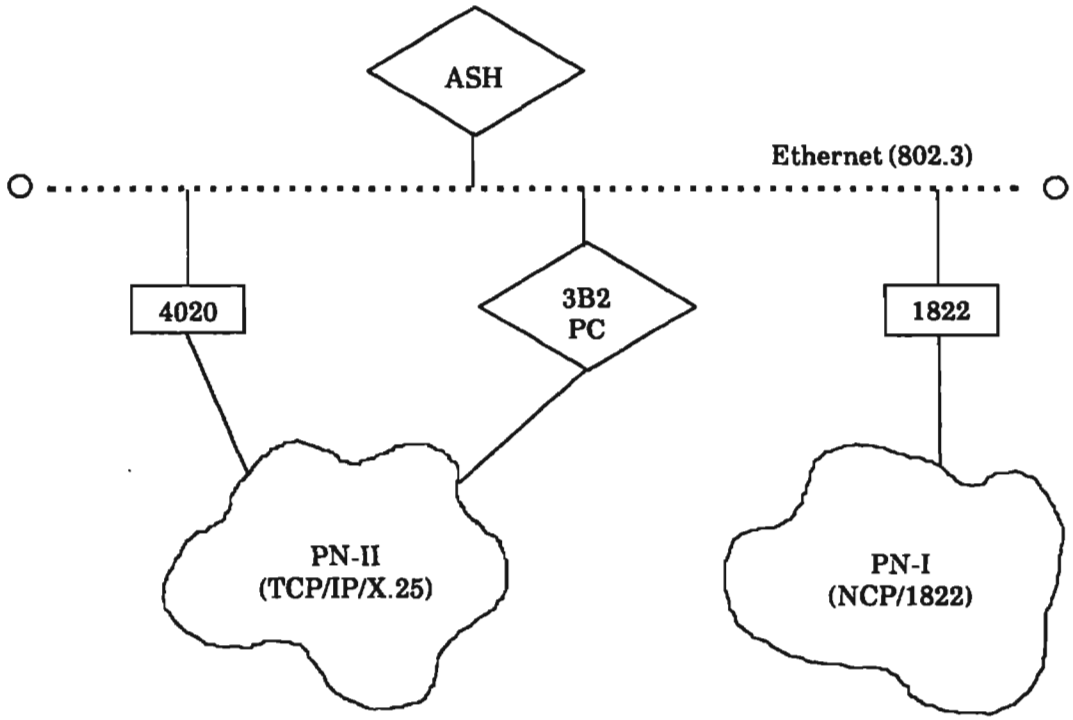
PN-I does not use IP, and thus does not have the key to internetworking. A second type of gateway implemented at the applications layer allows PN-I systems to communicate with other networks. This requires protocols (NCP and TCP/IP) to be translated. These gateways or protocols converters exist on PN-I as PLATFORM server hosts. They allow systems using TCP/IP/802.3 protocols on the ASHLAND Ethernet LAN to talk to systems using NCP/1822 protocols on PN-I. (The network access protocols for Ethernet and PN-I are 802.3 and 1822, respectively.)

The server itself performs the NCP and TCP/IP translation; however, another gateway (the 3B/1822 box) allows the server talking 802.3 on the Ethernet to talk 1822 to the PN-I local IMP.

Similarly, an ASH on an Ethernet can now talk to PN-II by going through an ACC4020 gateway, which provides the 802.3/X.25 interface and performs limited IP routing. Another prototype has an ASH on an Ethernet talking to PN-II by going through an AT&T 3B2 system with both an 802.3 and X.25 interface and server software. The 3B2 software implements more sophisticated IP routing than that of the ACC4020 box. Since the ASHes and PN-II both use IP, application-level protocol conversion is not necessary. However, the 3B2 also has the protocol conversion capability if changes in architecture

require this (i.e., a 3B/1822 is added to the Ethernet to allow the 3B2 to become a gateway between PN-I and PN-II). (See fig. 4.)

PC – Protocol Converter
1822 – 802.3/1822 gateway
4020 – 802.3/X.25 gateway



PATHS:
1. ASH → Ethernet → 3B2/PC (for TCP/IP to NCP translation) → 1822 → PN-I host
2. ASH → Ethernet → 4020 → PN-II host
3. ASH → Ethernet → 3B2/PC (for IP routing only) → PN-II host

Fig. 4. Possible PN-I/PN-II Configuration

The main point of the previous discussion is that there are different kinds of gateways, and there are choices to be made about the deployment of gateways in PN-II. Choice of gateways will depend on choice of LANs and other architectural issues. Also, for reasons of reliability and efficiency, multiple gateways may be desirable to avoid single points of failure and bottlenecking.

Another PN-II goal is to create as little disruption as possible to the current network. The gateway method for interconnecting networks makes minimal demands on individual

networks and allows interoperability among networks that have significantly different protocols and performance [5].

V. PLATFORM NETWORK II UPGRADE

A. Introduction

The evolution of PLATFORM yielded a unique enormous network whose efficiency waned with its growth. Although enhancements and other modifications were applied over the last thirteen years, it became apparent that the original PLATFORM design was outdated. When over 300 systems needed access to the WAN, and there was no way for PLATFORM to accommodate them, taking another direction was necessary. "NSA-unique software was at the heart of the technical limitations highlighting the need to upgrade the network in the direction of DoD standards [1]."

The migration to PN-II should produce the following benefits:

1. solve many of the aforementioned current PLATFORM problems,
2. reduce the number of anticipated problems, and
3. allow for simpler and less expensive solutions to future problems (through the use of off-the-shelf products) [1].

B. The PN-II Upgrade Plan

The Agency has developed a comprehensive plan [1] to further the PLATFORM evolution. The plan not only satisfies NSA's current requirements, but allows for the inevitable changes of the future. NSA is now in Phase 2 of a five-phase plan. In the discussion of the plan that follows, all dates are approximate.

Phase 1: August 1988–October 1988

A TCP/IP/X.25 network (PN-II) has been built totally separate from the existing NCP/1822 network (PN-I). The two networks are closed, i.e., there is no communication between them, and each network has its own Network Monitoring System. Since few PN-II hosts can afford not to communicate with any PN-I hosts, this phase should be short.

Any directly connected PN-II host must use the TCP/IP/X.25 standard protocols and is "encouraged" to implement the standard application layer protocols (FTP, TELNET, etc.) as well. Of course, using the recommended protocols opens more doors of communication, and encourages the use of more economical off-the-shelf products.

Phase 2: October 1988–May 1989

This phase will add interoperability between PN-I and PN-II. Since all PN-II hosts use TCP/IP, PN-I hosts can communicate with PN-II hosts only if they

1. also use TCP.
   TCP/IP also runs over the 1822 protocol. A PN-I host running TCP/IP/1822 can communicate with a PN-II host running TCP/IP/X.25 with the aid of a Hybrid IMP that allows 1822 and X.25 hosts to interoperate. However, the use of Hybrid IMPs is not scheduled until Phase 3; thus, a server host can perform the 1822/X.25 gateway function (just like the 3B2 prototype previously discussed).
2. use a protocol translator.
   The protocol translator will perform the necessary translation from NCP to TCP/IP as well as provide the 1822/X.25 interface. (See fig. 4.)

Phase 3: May 1989–May 1991

This phase will merge PN-I and PN-II into a single wide area network through the Hybrid IMP. Not only does the Hybrid IMP provide the 1822/X.25 interface, but it also uses the old and new IMP-to-IMP (subnet) trunking protocols. The C/30 IMP uses the MII trunking protocol while the C/300 high-speed IMP uses the newer MSYNC trunking protocol. Eventually, PN-II will use all MSYNC since mixing the MII and MSYNC (although possible) makes deployment and maintenance more difficult.

The main reason for merging the two distinct networks is to better use the limited NSA resources. The ARPANET model allows for the multiple WANs, which may be in PLATFORM's future as well. The objectives for Phase 3 are as follows:

1. have one WAN with one Network Monitoring system
2. have a subnet using just MSYNC trunking protocol
3. use as much standard commercially available software as possible
4. provide four levels of host-accessible precedence (in subnet) by November 1989
5. provide for remaining NCP hosts to talk to TCP/IP hosts.

In Phase 3, objectives (3) and (4) apply to the IMP software. PN-I is currently running IMP software that was modified to handle NSA-unique requirements such as VHAs. Although the software is a BBN product, NSA changes have made updates very difficult, and NSA is several versions behind. PN-II will eventually run the latest BBN release (which provides precedence levels), and every attempt will be made to avoid changing it.

Objective (5) will still be satisfied by the SACRUM protocol translators.

Phase 4: June 1989–?

The first IP-wide area gateway will be introduced to PN-II by approximately June 1989. Any new PN-II subscriber will be a LAN, and the existing directly connected hosts will begin migrating to LANs. This phase will continue until there are no directly connected hosts on PN-II except those that have been granted waivers from complying with the 'T' Internet architecture. The introduction of LANs to a WAN is long overdue, as we have seen with the dwindling available communications resources on PN-I.

The IP gateways will be able to provide 1822, X.25, 802.3 (Ethernet), HYPERchannel, and PRONET (LAN/PN-II) interfaces.

Phase 5: no limits

The PN-II topology will be constantly reevaluated while the other four phases are being completed. This phase means we have learned to plan for the future. The original December 1986 PN-II topology design has already exhibited flaws that need to be handled, but the flexible design supports the upgrade process.

Adhering to the PN-II Upgrade Plan depends mainly on the following:

1. deployment of WAN IP gateways and LANs, and
2. ability of hosts to transition from NCP to TCP/IP.

Ideally, all hosts should use TCP/IP. For some systems (e.g., SUN workstations), this is just a matter of purchasing off-the-shelf software. However, for other systems (e.g., PDP 11/70 UNIX systems), the solution is more complex. Some possible solutions follow:

1. replace PDPs with ASHes – eventually, users will find PDP network performance unsatisfactory once they have been exposed to ASHes using TCP/IP (as opposed to NCP). In the long run, it is probably more economical to throw away the PDPs than to dedicate Agency resources to keep them usable.
2. put TCP/IP on PDPs – Most PDPs have been pushed to their kernel and buffer space limits. Adding the extra burden of TCP/IP is not feasible for most PDPs.
3. use FEs that handle TCP/IP for PDPs – These FEs have recently become feasible. Potential problems are performance and any problems that come with using new hardware and/or software.
4. find a way to put PDPs on LANs – Using (3) may facilitate this, or perhaps create small PN-I clones where each PDP LAN would consist of an IMP, the maximum number of PDPs it could service minus a port for a gateway (protocol converter).

This is just a small sample of the problems being faced in the upgrade process. NSA has a big investment in existing hardware and software, and smart decisions must be made concerning the conversion of the hardware and software to conform to PN-II standards.

VI. CONCLUSION

The PLATFORM network has come a long way from its initial four-system configuration almost fifteen years ago. Although considered state-of-the-art at the time, PLATFORM's progress has slowed over the years mainly because of its magnitude and its Agency-unique enhancements. To escape this dilemma, NSA has made a commitment in the form of the PLATFORM Network II upgrade to overcome the limitations of PLATFORM by adhering to the set of DoD standard protocols. The main benefits to be gained from this endeavor are internetworking and economical products. "Although off-the-shelf solutions will [probably] never meet all of the Agency's needs, the capability to use appropriate available technology would allow the Agency to concentrate its limited resources on the future...[9]."

The DoD policy on standards is as follows [9]:

1. if international standards are commercially available and support military requirements, they should be adopted immediately to obtain the maximum economic and interoperability benefits, and
2. if sufficient standards do not exist, DoD will develop its own standards until national or international standards become available.

NSA has realized the importance of participating in the external standards effort. Although the current DoD suite of protocols is being implemented on a wide scale, the International Organization for Standards efforts will be playing a major role in the future of NSA networking.

Another big commitment by NSA is to plan for the future. NSA will be constantly reevaluating the present and future PLATFORM architectures. The PN-II upgrade will create a more flexible networking environment that will facilitate smoother and easier transitions of PLATFORM.

BIBLIOGRAPHY

[1] "Upgrade Plan for the PLATFORM Network." T412, NSA, 28 October 1988.

[2] "Introduction to PLATFORM." NSA Doc. S-216, 705, 1 October 1985.

[3] "PLATFORM X.25 Protocol." Report Nos. 5476, 5500, 5760, 5900, BBN, Inc. for Defense Communications Agency, NSA Doc. S-216,730, 1 November 1986.

[4] "The TCP/IP Primer." Vers. 2.2, WINS, AT&T Technologies, December 1985.

[5] Postel, Jon, Carl A. Sunshine, and Danny Cohn. "The ARPA Internet Protocol." *Computer Networks*, Vol. 5, Number 4, July 1981.

[6] Lerner, Dr. Barry M., Dr. Robert Cole, Dr. Jon Postel, and Dr. David Mills. "The DARPA Internet Protocol," April 1984.

[7] Sunshine, Carl A. "Interconnection of Computer Networks." *Computer Networks*, Vol. 1, 1977.

[8] Stallings, William. *Data and Computer Communications*, 2nd edition. Macmillan Publishing Company, 1988.

[9] "PLATFORM II Network Handbook." NETWORK Project Management Office, NSA Doc. S-216,731, September 1987.

[10] Wolf, Eric W., Eric S. Elsam, and O. Robert Hess. "NSA Network Study Final Report." BBN, Inc. Report 2864, 30 August 1974.

DOCID: 3929121

[11] "Host/Host Protocol for the PLATFORM Network." NSA Doc. S-216,710, 1 August 1978.

[12] Comer, Douglas. *Internetworking With TCP/IP – Principals, Protocols and Architecture*. Prentice-Hall, 1988.