Internetworking for the Beginner
Janice R. Kolb and David F. Kolb, SAS Institute Inc., Cary, NC

ABSTRACT
SAS/CONNECT® software is a cooperative processing tool which allows a local SAS® session to utilize files, hardware resources, and SAS software on various remote hardware platforms such as mainframes, mini-computers, workstations and personal computers. You can establish a SAS/CONNECT conversation to multiple SAS sessions on multiple hardware platforms to distribute SAS processing to the most appropriate machine in order to use your computing resources to their best advantage. To be able to use SAS/CONNECT software, all of the different hardware platforms have to be networked together. Internetworking can be defined as "the communication between data processing devices on one network and other possibly dissimilar devices on another network". The purpose of this paper is to cover the general concepts of internetworking and explain some of the current buzzwords such as routers, brouters, bridges, gateways and protocols enabling the user to understand the structure of the network and different communication access methods used by SAS/CONNECT software. This paper will first cover the definition of a network, the hardware components, topology, and types of networks used by SAS/CONNECT software followed by network communication protocols and how SAS/CONNECT software utilizes them via access methods.

HISTORY OF A NETWORK
A network can be defined as a group of computers that can communicate to one another, share peripherals, and access other networks or remote hosts. A LAN or Local Area Network can be defined as a collection of computing resources all located within one geographic area. A WAN or Wide Area Network is a collection of computing resources covering a large geographic area.

Networking started in the late 1960's and early 1970's. During that time period, mainframes defined computer networks. Once companies chose a mainframe, they were committed to that mainframe architecture until that system became obsolete which demanded a complete change in their hardware design. Because of the proprietary nature of the networking architecture, companies rarely considered third-party equipment.

In the mid 1970's, the idea of an "open" system became popular. An "open" system now had to adhere to published standards which drastically reduced dependency on proprietary architecture. During this period, many standards organizations started to appear. They included the International Telegraph and Telephone Consultative Committee (CCITT), which defines standards and makes recommendations for international networking, the International Organization for Standards (ISO), which was formed to define standards for multivendor network communications, and the American National Standards Institute (ANSI) which is the United States member of ISO.

In 1978, the need for internetworking or the communication between two or more networks led to the Open Systems Interconnection (OSI) Reference Model. This model defines seven distinct levels of communications as defined by ISO.

The seven layers of the OSI model are:

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

Physical Layer
The Physical Layer handles the transmission of the bit stream between the workstations or nodes. The functions associated with the physical layer deal with the physical transmission of the data packet such as interfacing with the transmission media; determining the electrical voltage level; half or full duplex; encoding the data signal. The most common form of this layer is the physical cable used for an Ethernet or Token Ring network.

Data Link Layer
The Data Link layer assumes that the Physical layer can contain errors or noise and therefore its function is to maintain a reliable communication link to transmit a frame of data bits to the next node. The data link layer provides a reliable delivery mechanism by inserting source and destination addresses in the data frame and including transmission error control information. A Cycle Redundancy Check (CRC) is usually implemented for error control. Examples are the IBM® Synchronous Data Link Control (SDLC) and CCITT's High Level Data Link control (HDLC). Token Ring and Ethernet networks break this layer into two layers, the Logical Link Layer (LLC) and the Media Access Control (MAC). The logical link layer is a common link to the Network layer and above. It is responsible for getting packets onto the network cable and also manages the flow of the data bit stream into and out of each network node. The MAC layer is unique to the LAN protocol being used. MAC is a method for controlling access to a transmission medium. Two widely used methods of this are Ethernet's CSMA/CD and Token Ring's token passing. Each of these will be discussed later.

Network Layer
The Network layer establishes a route for the transmitted data packet from the source node to the destination node along the network. As well as insuring delivery of the data packets, the network layer keeps track of what is sent, sends control messages to its peer layers in the network about its own status, prioritizes messages, and regulates the receiving rate. This layer also allows the interconnection of other networks.

Transport Layer
The Transport layer provides a reliable transmission of host messages from the Application layer through the network. Its responsibilities are much like the Data Link layer only the Transport layer's region extends from the source to the destination nodes within the subnet while the Data Link's region resides between adjacent nodes. The Transport layer transmits messages by segmenting a message into smaller packets and then reassembling them back into the original message at the destination node. This layer guarantees that the data packets are received in the proper order, it can use parallel paths for fast message delivery, and it can broadcast messages to multiple receivers. This layer is usually software found in the host, intelligent terminals and network processors. It is responsible for mapping user names to network addresses and supports data/message recovery by rerouting the path or saving the data if a network link or node fails.
Session Layer
The Session layer’s function is to establish and terminate a logical connection between the end-user and the application. This requires support functions in the host such as file transfer, data base integrity, system access security and message accounting and billing information. This layer also provides the important function of allowing for reliable session termination even during an abrupt termination. The Session layer usually involves the host’s operating system software along with communications software.

Presentation Layer
The Presentation layer determines the form in which the data are exchanged between two hosts such as the number of lines per screen, the number of characters per line, code conversion, cursor addressing, data encryption, data compression and terminal emulation.

Application Layer
The Application layer deals with the interaction of the user. This layer provides end-user services, such as Application layer file transfers, electronic mail messages, virtual terminal emulation, and remote database access.

The ISO model can be subdivided into two distinct subsets. The first subset consists of the Physical, Data Link, and Network layers. This subset is referred to as the communications subnetwork, the subnet or the carrier portion of the network. The second subset consists of the Session, Presentation, and Application layers. This subset is referred to as the host process or customer portion of the system. The Transport layer acts as a buffer between the communications subnetwork and the host process. If it were to be grouped with either subset it would be with the host process.

DESIGNING A NETWORK
Based on the ISO model, when designing and building a network, there are many different kinds of cabling media and network and internetwork devices to choose from such as cables, repeaters, bridges, routers, brouthers and gateways. There is not an ideal or correct answer as to what hardware is best; it strictly depends on the demands of the network.

Cabling
There are several different types of cabling media that can be used when designing a network such as twisted pair, shielded twisted pair, coax and fiber. Each type of cable has its advantages and disadvantages which will be factors in determining which to use in a specific environment.

Twisted Pair cabling is a common wire used to transmit such things as data, voice, and video. This type of wire should be used in electronically noisy areas. Twisted Pair cable consists of pairs of wires twisted together to reduce interference. For added protection against interference, the pair of wires can be wrapped with an aluminum-backed plastic or a braided metal shield. The shields are grounded to dispense the interference. This is IBM® type 1 cable and is known as Shielded Twisted Pair (STP). This type of cable commonly used in IBM systems. It allows data to travel at 4 Mbps (million bits per second) up to 2000 feet and 16 Mbps up to 1000 feet. Due to the coating, shielded twisted pair is more expensive than unshielded twisted pair.

Unshielded twisted pair (UTP) is an IBM type 3 cable and should be used in conditions where there is low electromagnetic interference. The following is a guideline for minimum distances from the UTP wire to some electromagnetic sources:
- 5 inches from power lines of 2k volts or less
- 12 inches from a fluorescent light or power lines between 2k to 12k volts
- 36 inches from power lines of 5k volts or more
- 40 inches from transformers and motors.

When using UTP, do not assume that you can use existing cabling in a building. In general, an Ethernet network should use at least grade 3 UTP cable and a Token Ring network should use at least grade 4 UTP cable. Most existing UTP cable is probably of a lesser grade and originally used for telephone voice transmission.

Coax cable is made of a solid center conductor with shielding around it. Coax cable allows transmission of high speed data over greater distances than twisted pair. This type of cable was once the standard but has lost that popularity due to the expense, bulkiness, high maintenance and difficulty to troubleshoot. Coax cable is used to connect a CRT terminal to a cluster controller, connect processors together and is a transmission media for LANs. The two types of coax cable are baseband and broadband.

Baseband cable consists of a thin solid center conductor and a braided metal shielding. It is a single channel and allows only one logical transmission at a time. The transmission rate exceeds 10 Mbps over a 600-foot distance.

Broadband cable consists of a thick solid center conductor with a solid heavy metal shielding. This type of wire supports multiple channels and can transmit at rates exceeding 10 Mbps over a 1600-foot distance.

Fiber Optic cable consists of two glass materials with different reflective qualities. The outside layer reflects light while the inside layer lets the light pass easily. A laser light source produces high speed pulses of light which represent 1 and 0 bits that are converted back to electrical signals for use by digital equipment. This type of wire is used for high volume data transmissions such as voice or imaging. The transmission rate can exceed 100 Mbps over 2000 meters between repeaters.

Internetworking Devices
The internetworking devices of a network are repeaters, bridges, routers, brouthers and gateways. A repeater operates at the Physical layer of the ISO model. It is not an intelligent device and offers little in network control, management or diagnostics. A repeater is used to extend the length of the cabling; to add to the number of workstations on the segment; or to convert the type of cable being used to connect LAN segments. Its main function is to regenerate or amplify the electrical signal, or data packet, being passed between the cable segments of a LAN. The amplification of the signal allows the signal to travel over longer distances along the LAN than the cabling normally allows. The Ethernet specifications suggest not transmitting a signal through more than four repeaters since a delay is experienced each time the signal travels through a repeater. The ability to avoid using more than four repeaters are to segment or bridge the traffic or use star wire hubs.

Multiport repeaters can connect several LAN segments together at one time and act much as a hub. A hub is a network device that relays and repeats signals to other devices. The type of repeater can also convert between different types of cable being used to connect LAN segments.

A bridge operates at the Data Link layer of the OSI model. A bridge is used to logically segment networks into subsets based upon network traffic. The subsets or subLANs are connected by the
bridge which is responsible for passing information between them. Each sub-LAN becomes more efficient because it is supporting fewer devices which will reduce the number of data packets and therefore have fewer collisions. Segmenting allows workstations that frequently communicate to be on a common sub-LAN which therefore have fewer collisions. Segmenting allows workstations that frequently communicate to be on a common sub-LAN which reduces unnecessary traffic across the entire LAN. The primary function of a bridge is to transfer data packets between connecting networks based on the destination address. A bridge learns which node addresses are on which sub-LANs by listening to the transmissions from all of the workstations. By learning these addresses, a bridge will “filter” and “forward” data packets. The "filtering" process involves examining the destination address of each data packet and then comparing it to the routing table. The bridge only "forwards" the packet if the destination address of the packet is on a network or segment on the other side of the bridge. If the destination address is on the same side of the bridge as the source, the bridge just ignores the packet and lets it continue around the sub-LAN. Bridges are less expensive than routers or gateways, require less configuration and have greater throughput. Most bridges operate on networks of similar architectures such as Token Ring to Token Ring or Ethernet to Ethernet even if it is not a requirement.

Advanced bridges have the additional ability to perform functions such as address lock-in and lock-out, protocol-based filtering and forwarding and backup routing.

The address lock-in and lock-out feature allows you to configure a bridge to only allow certain information to pass. It allows individual source and destination addresses to be locked in or accepted, or locked out or rejected.

The protocol-based filtering and forwarding feature allows restriction of where different protocols can be accessed across the network. This enables them to be restricted to one LAN or allows the protocol to transmit across multiple LANs.

The backup routing feature allows automatic rerouting over alternate paths if a bridge or data communications link fails.

A router operates at the Network layer of the OSI model. Routers, like bridges, logically separate LANs but they contain a programmability which is not available in a bridge. This programmability allows a router to increase throughput and decrease congestion in complex LANs. These tasks are accomplished by choosing the best routes between the source and destination network. Routers should be used on networks with many alternate paths.

The nature of the Network layer requires routers to do more processing than bridges at the Data Link layer. They take longer to manage the data packet than bridges and are also more complex to operate and install. Routers are more expensive than bridges and some protocols such as DECnet’s LAT and the IBM NETBIOS cannot be directly routed.

A broutr operates at the Data Link and Network layers of the ISO model. They are also known as routing bridges. A broutr is the hybrid of a bridge and a router. They were designed to improve the processing speed of the bridge with the internetworking capabilities of a router. A bridge uses the Data Link layer address of the frame to make filtering and forwarding decisions. A router uses the Network layer address to choose the best outgoing path. A bridge therefore is protocol independent while a router is protocol dependent. A broutr provides the protocol independence of a bridge while using the ability to direct LAN traffic to one or more networks depending on the Network layer protocol being used.

A gateway operates at the host process of the ISO model, the Session layer through the Application layer. It provides much of the same functionality as bridges, routers and brouters, but gateways are capable of translating between protocols. This feature allows networks of different protocols to be linked together.

Topologies

When designing a network, there are different topologies to be considered such as bus, ring or star. Network topology is the logical or physical arrangement of the workstations or nodes on a network in relation to each other.

Bus or Daisy Chain topology is designed to be long and linear. It is used for Ethernet LANS. All workstations share a common cable which is the bus. The advantages of bus topology are that they require less cable and pre-planning and they handle long runs well. The disadvantages are most failures are not isolated to an individual workstation but instead involve all the stations on the bus or segment. Trouble shooting is difficult and time-consuming.

Ring topology is designed to look like a ring and all the workstations and devices are on this ring. It is used for Token Ring or FDDI networks. An advantage of ring topology is that in the case of cable failure, the data packets will automatically bypass the problem station. A disadvantage is it is difficult to manage the cabling.

Star topology is designed with a center hub and all of the workstations individually connected to that hub. This topology is specially designed for Token Ring and Ethernet networks. The advantages are that almost all failures involve only one workstation, trouble shooting is simplified, modifications and changes are easily made, and it provides a centralized wiring scheme for easy cable management. The disadvantages are if the main hub is lost, all of the satellite hubs and interconnections are lost; uses more cable and components; and requires more advanced planning.

The total number of devices including workstations, terminals, servers, printers and other peripherals connecting to the hub and inter-hub connections must be considered when planning a network. For a 16-Mbps Token Ring network, the maximum number of connections per segment is 70. A 4-Mbps Token Ring network can have as many as 260 devices. An Ethernet network can have 100 connections per segment.

Ethernet Network

An Ethernet network is a bus-based network operating at 10 Mbps and uses CSMA/CD (Carrier Sense Multiple Access/Collision Detection) which allows all transmitters and receivers or transceivers to contend equally for bus access. Every packet that is transmitted is received by all transceivers. A transceiver is a device which transmits and receives data on the network for the workstation.

When a transceiver is ready to transmit data, it first listens to the network to see if data are being transmitted by any other transceiver. If the sending transceiver detects other data being transmitted, it waits; otherwise it transmits the data while listening to the network. If the transceiver detects a possible collision with data being transmitted by another transceiver, it retransmits by sending a collision signal back to the attached workstation. The transmitting workstation waits a certain period of time and when the network is clear it attempts to resend the data. This process is repeated until the packet can be transmitted successfully onto the network.

A small delay occurs during the time that the transceiver starts transmitting the data to the time that the other transceivers on the network start receiving the data. During this delay, other transceivers may think that the network is clear and start to transmit data. This is when data collisions occur. The chances of a data collision occurring increase with the amount of network traffic as well as the size of the network.

An Ethernet Network must conform to one of the IEEE (Institute of Electrical and Electronics Engineers) standards which are 10base5, 10base2, 10base7 or 10baseT. 10base5 supports thick Ethernet coax segments up to 1640 feet. Each of these segments can support up to 100 transceivers.
10Base2 supports thin coax segments up to 607 feet. Each of these segments can support up to 30 devices and the transceivers are usually built into the network interface cards (NIC). A NIC card is installed into a network device to provide a direct link to the network. 10BaseT supports twisted pair segments up to 328 feet with only 1 transceiver per segment.

10BaseF (Fiber-optic media) supports up to 3000 feet of fiber optic cable between repeaters.

Token Ring Network

The IBM Token Ring LAN is a ring-based network that can operate at 4 Mbps or 16 Mbps. Since the network forms a closed ring, all of the stations on the ring receive all transmitted messages in sequence rather than all at once like on an Ethernet network. On an idle ring, the token is passed from station to station until the token is acquired by a station that is ready to transmit data. That station then creates a data packet which consists of the data and the addresses of the destinations.

The data packet is then passed to the next station on the ring. If that station is not the destination station for the packet, it puts the packet and token back onto the ring and the packet is forwarded to the next station.

When the data packet reaches the destination station, it copies the message, marks it as “received” and then puts the data packet and token back on the ring. The station which sent the message then looks to see if the message has been marked “received”. If it has, it removes the packet and can then either put the token back out on the ring and make it available for another station, or transmit another message.

If a station receives a bad packet, it knows it was caused by the last station. It transmits a “beacon” onto the ring that lets all of the other stations know about the failure. When the station which corrupted the packet receives the beacon, it removes itself from the network. Regular data transmissions are suspended during the beacon process.

FDDI Network

FDDI (Fiber Distributed Data Interface) networks are a physical ring and also use token passing. They can operate at distances up to 62 miles and operate at 125 MHz with a data rate of 100 Mbps.

FDDI is the protocol used for high-performance workstations, remote host channels, and backbones that link interwork traffic. In an FDDI network, bridges, routers or gateways can serve as links between LANs. An FDDI network will allow packets to be transferred in opposite directions so it can automatically compensate for nodes or link failures.

COMMUNICATION PROTOCOLS

Once the network has been implemented, there are multiple communication protocols that can run on top of the network which can be used by SAS/CONNECT software to connect SAS sessions on multiple hardware platforms. The actual hardware configuration or layout of the network is transparent to SAS/CONNECT software. SAS/CONNECT software interacts with the communication protocol such as APPC, DECnet, HLLAPI, NETBIOS, and TCP/IP that is linking the workstations and hosts together.

APPC is the IBM Advanced Program to Program Communication. APPC is an implementation of the SNA/SDLC LU6.2 protocol which allows distributed processing within an IBM SNA network. This protocol is supported on a Token Ring, Ethernet, SDLC, channel-to-channel and X.25 links.

DECFnet is a Digital Equipment Corporation (DEC) proprietary networking communication protocol. This protocol is supported on an Ethernet and Token Ring connections.

HLLAPI is a High Level Language Application Program Interface to 3270 emulation in the PC DOS and OS/2 environments. PC workstations running HLLAPI and 3270 emulation often use coax cable to connect to a 3174 or 3274 controller in the classic 3270 architecture fashion. Most of the newer emulation programs allow configuration over a network using an SDLG gateway PC to connect to the mainframe or on a network using a 3174 controller to act as the gateway to the host. In these configurations, the 3270 emulation program can share the same LAN as other applications and uses no special 3270 facilities.

NETBIOS (Network Basic Input/Output System) is an operating system interface for applications on workstations attached to a Token Ring or Ethernet network.

TCP/IP (Transmission Control Protocol/Internet Protocol) is a communication protocol that is supported on most hardware platforms. It will allow peer-to-peer connectivity for most Local Area Networks and Wide Area Networks.

TELNET is an application protocol in a TCP/IP environment that allows a workstation to access a remote workstation and appear as if it were a locally attached terminal. TELNET’s underlying protocol is Transmission Control Protocol (TCP)

SAS/CONNECT software uses two methods of communication, either program-to-program or terminal-based. A program-to-program method of communication is designed for the interaction of two processes. This protocol allows for much larger packet sizes. Data are transmitted in binary form and, therefore, do not require the application to perform any character set encoding. Message notification is often done asynchronously. Program-to-program interfaces may require additional third-party software in order to get the support of all of the necessary platforms. This type of communication includes the APPC, DECnet, NETBIOS and TCP access methods.

A terminal-based method of communication such as HLLAPI, TELNET or asynchronous is designed for displaying data on a terminal and thus imposes limitations when used for communication between two processes. This protocol restricts throughput and efficiency because it forces the application to put the data into a “screen image” even though it is not intended for users to read from the screen. The transmission packet sizes are constrained by the size of the screen. The application must typically perform character set encoding in order to write binary data to the screen. Message notification is generally accomplished through polling. Terminal-oriented interfaces, however, are relatively cheap and generally available. This type of communication includes the HLLAPI, TELNET and RASYNC access methods.

ACCESS METHODS

SAS/CONNECT software uses access methods to interface with the communication protocols. The access method is by the SAS system option COMAMID. The following is a list of the available program-to-program access methods along with any additional information which is required for SAS/CONNECT software and the hardware platforms they are available on at the time of this printing. It is important to note that more than one communication protocol can reside on a network. APPC, NETBIOS, TCP/IP and Netware can reside on the same LAN. SAS/CONNECT software can establish concurrent conversations using all of these access methods.
APP C

Until the APPC configuration is properly specified it may be very
difficult to establish connections within an SNA network.
SAS/CONNECT software has tried to simplify the troubleshooting
by returning the operation codes, return codes and sense data of
the APPC error. To determine the APPC error messages, refer
APPC

To the IBM Corporation's Extended Services for OS/2 Programming
Services and Advanced Problem Determination for
Communications (SO4-G-1007), the IBM SNA Formats
(GA27-3136); and SAS Technical Report P-224, SAS/CONNECT
Software: Changes and Enhancements, Release 6.08 for a listing
and explanation of the most common APPC error messages. This
access method is available under the CMS and MVS operating
systems using Release 6.07 of the SAS System and under the
CMS, MVS, and OS/2 using Release 6.08 of the SAS System.

DECnet

In this paper, the term DECnet interface is used to describe the
task-to-task communication interface over a DECnet network. This
access method is available under OpenVMS using Release 6.07 of
the SAS System and under OS/2 and OpenVMS using Release 6.08 of
the SAS System.

NETBIOS

NETBIOS will allow peer-to-peer communications between
machines running under OS/2 2.0 as well as between a local
machine running under Microsoft Windows and a remote machine
running under OS/2. The same vendor software must be used on
both the local and remote machines. This access method is
available under OS/2 and Microsoft Windows using Release 6.08
of the SAS System.

TCP

The TCP access method establishes the host connection using
linemode TELNET until a remote SAS session is instantiated then
TCP/IP communications are used. This access method is available
under MVS, UNIX, and OpenVMS using Release 6.07 of the SAS
System, under CMS, MVS, OS/2, and OpenVMS using Release
6.08 of the SAS System, and under UNIX using Release 6.09 of
the SAS System.

The following is a list of terminal-based access methods along with
any additional information which is required for SAS/CONNECT
software and the hardware platforms they are available on at the
time of this printing.

HLLAPI

High Level Language Application Programming Interface is a
standard 3270 programming interface that uses SNA's LU2 protocol
and is provided by many third-party vendors under OS/2, Microsoft
Windows, and DOS. SAS/CONNECT software first moved to this
standard interface with Release 6.06 of the SAS System under
OS/2. HLLAPI and HLLAPI are sometimes used interchangeably.
This access method is available under PC DOS using Release 6.06
of the SAS System, under OS/2 using Release 6.06 of the SAS
System, under OpenVMS using Release 6.06 of the SAS System.

TELNET

The TELNET access method is used when the local platform is
running a TCP/IP package supported by SAS/CONNECT software
and the remote platform does not have a supported TCP/IP
package or the TCP access method. Note, however, that TCP/IP
software is still required in both the local and remote environments.
This configuration uses the asynchronous message protocol. The
remote SAS System is invoked with the SAS system option
COMAMID set to RASYNC. This access method is available under
UNIX and OpenVMS using Release 6.07 of the SAS System, under
OS/2, Microsoft Windows, and OpenVMS using Release 6.08 of
the SAS System and under UNIX using Release 6.09 of the SAS
System.

RASYNC

RASYNC is a primitive, nonstandard method of communication that
uses phone lines or RS232-type cables as its medium. This is a
relatively slow but inexpensive method of communication that
requires much error checking and recovery overhead on the part of
the application. This access method is available under PC DOS
using Release 6.04 of the SAS System, under OS/2 using Release
6.06 of the SAS System, and under OS/2 using Release 6.08 of
the SAS System.

SUPPORTED COMMUNICATION SOFTWARE

The following is a list of the tested communications products for
which the Institute claims support for the SAS/CONNECT product
at the time of this writing.

Communication Software for OS/2 1.3 (SAS software
Release 6.06)

COMAMID=EHLLAPI

• IBM Corporation's Communication Manager Version 1.2 or 1.3
• DCA's SELECT Version 1.0+

Communication Software for OS/2 2.0 (SAS software
Release 6.08)

COMAMID=APPC

• IBM Corporation's Extended Services Version 1.0 or later.
• Should support any OS/2 2.0 emulation program that supports
the IBM APPC standard.

COMAMID=EHLLAPI

• IBM Corporation's Extended Services Version 1.0
• Should support any emulation program that supports the IBM
EHLLAPI standard.

COMAMID=MNETBIOS

• the Novell Netware Requestor for OS/2 Version 2.0
• Should support any vendor package that supports the Novell
NETBIOS Submit Interface.

COMAMID=NBIOS

• IBM Corporation's Extended Services Version 1.0
• Should support any vendor package that supports the IBM
NETBIOS 3.0 Interface.

COMAMID=TCP

• IBM Corporation's TCP/IP Product Version 1.2.1+
• the Novell LAN Workplace for OS/2 (as local only) Version 3.0

Communication Software for Microsoft Windows 3.1 (SAS
software Release 6.06)

COMAMID=DECNET

• Pathworks for MS-DOS V4.0+
COMAMID=EHLLAPI
- Attachmate’s EXTRA for Microsoft Windows
- the DCA IRMA WorkStation for Windows Version 1.0+
- IBM Corporation’s Personal Communications/3270 Version 2.0+
- Wall Data’s Rumba Version 3.1+

COMAMID=NETBIOS
- IBM Corporation’s LAN Support Program
- the Novell Netware Requestor for DOS
- Should support any vendor that provides a compatible NETBIOS interface on the Microsoft Windows 3.1 and OS/2 2.0 platforms.

COMAMID=TCP
- the Novell LAN Workplace for DOS V4.0+
- the Microsoft LAN Manager V2.1+
- the DEC Pathworks for DOS (TCP/IP) V2.0
- For any product that supports Microsoft’s WinSockAPI, an experimental SAS/CONNECT WinSockAPI module is available from SAS Institute’s Technical Support Division.

Communication Software for MVS (SAS software Release 6.07 and later)
COMAMID=APPC
- VTAM® Version 3 Release 2 or later is required. In order to support SAS/CONNECT software access from another MVS, VM/CMS, or (without a TSO logon) OS/2, MVS/ESA™ Version 4 Release 2 or later, with APPC/MVS configured, is required.

COMAMID=TCP
- IBM MVS TCP/IP Release 2+. IBM MVS TCP/IP V2 Pascal API subroutine module. IBM VS Pascal Release 2 Run-Time Library.

Communication Software for CMS (SAS software Release 6.07 and later)
COMAMID=APPC
- VM/SP Release 6 or later is required to gain APPC/VM support. For communication among more than one VM/SP system, the Transparent Services Access Facility (TSAF) is needed. TSAF provides Interprocessor communication services for up to eight VM/SP systems located within a single TSAF collection. For communication with other systems outside of the TSAF collection that are connected by an SNA network, ACF/VTAM™, Group Control System (GCS), and APPC/VM VTAM Support (AVS) are needed.

COMAMID=TCP
- IBM Corporation’s VM TCP/IP Release 2+

Communication Software for VMS (SAS software Release 6.07 and later)
COMAMID=DECNET
- DECnet must be installed.


American Research Group 1991, *Understanding Local Area Networks* (course notes), Cary, NC.


SAS and SAS/CONNECT are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. IBM, OS/2, VTAM, ACF/VTAM, and MVS/ESA are registered trademarks or trademarks of International Business Machines Corporation. * indicates USA registration.

Other brand and product names are registered trademarks or trademarks of their respective companies.