Integrating IBM Mainframes with TCP/IP Networks

Introduction
There are four common approaches for integrating IBM mainframes with TCP/IP networks:

- Configuring a PU on every desktop and using router to encapsulate SNA within TCP/IP.
- Deploying IBM AnyNet™ products on the host and client PCs.
- Running TCP/IP on the host.
- Deploying an SNA gateway to provide support for SNA over TCP/IP networks.

Regardless of the approach, network managers seek to accomplish a number of sometimes conflicting goals when merging SNA with TCP/IP networks, including:

- Supporting a broad range of existing SNA applications.
- Reducing resource requirements on the workstation, local area network (LAN), wide area network (WAN), and host.
- Allowing easy network management.

Now, we will examine the four approaches for merging SNA with TCP/IP, focusing on how each approach satisfies the required goals. A summary of each approach is provided below in Table 1.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PU on every desktop</td>
<td>SNA TCP SNA</td>
<td>Full support</td>
<td>Requires SNA capable routers</td>
<td></td>
</tr>
<tr>
<td>AnyNet</td>
<td>TCP TCP TCP</td>
<td>LU0-3 support requires a separate gateway</td>
<td>Workstations and host perform protocol conversion</td>
<td>Requires dedicated IP client configuration</td>
</tr>
<tr>
<td>TCP/IP on Host</td>
<td>TCP TCP TCP</td>
<td>No LU0 No LU6.2</td>
<td>Host performs protocol convergence</td>
<td>Requires dedicated IP client configuration</td>
</tr>
<tr>
<td>SNA gateway</td>
<td>TCP TCP SNA</td>
<td>Full support</td>
<td>Gateway performs protocol convergence</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Summary of approaches for integrating IBM mainframes with TCP/IP networks.

1. Physical Unit (PU) on Every Desktop Approach
One approach for integrating SNA with TCP/IP is to install a full SNA stack for every desktop and then use Data Link Switching (DLSw) routers at each branch office to encapsulate SNA in TCP/IP, or use RFC 1490-compliant Frame Relay Access Devices (FRADs) to transport SNA in Frame Relay across a WAN. This approach is depicted in
Figure 1. In the example, remote PCs running a 3270 emulator are connected to a Front End Processor (FEP) over a WAN via routers. To these SNA devices, the routers appear to be source routing bridges. The result is no SNA link level traffic on the WAN. Yet, SNA is still required between the SNA nodes and their local routers or FRADs on the LAN.

![Diagram of SNA and TCP/IP connection](image)

**Figure 1: Configuring a PU on every desktop result in a mixed TCP/IP and SNA LAN.**

**SNA Application Support**

The routers encapsulate the full SNA data stream. There are no session type limitations, such as in the case of AnyNet or TCP/IP on the host approaches. Therefore, standard 3270 terminal emulation, 3287 printer emulation, and LU0 and LU6.2 applications can be supported over the WAN.

**Resource Requirements**

This approach requires that each desktop run the data link control (DLC/802.2) protocol for SNA plus TCP/IP for general LAN/WAN access. Therefore, the goal of a simplified TCP/IP-only workstation and LAN is not fully realized.

With MS-DOS® and Windows® workstations, which represent the vast majority of desktops today, the DLC protocol is a terminate-and-stay-resident (TSR) program. The TSR uses up much of the available memory on the PC in terms of real-mode RAM in MS-DOS. Configuring MS-DOS and Windows desktops to run both DLC and TCP/IP can be a challenge.

DLSw routers or RFC 1490-compliant FRADs handle the encapsulation and de-encapsulation of SNA at both ends. The host is unaware of the TCP/IP WAN connection. It sees the client as a PU Type 2.0 or 2.1 device connected via DLC across a traditional SNA network. As such, there is no net effect on host memory or CPU cycles compared to a bridged token ring network running SNA.
Network Management
This approach requires a separate DLSw-equipped router or RFC 1490-compliant FRAD in the remote office and another in the central office.

IBM released DLSw as a feature on its 6611 routers in 1992, and then submitted the DLSw specification to the Internet Engineering Task Force (IETF) as an informal RFC. In 1993, the IETF published RFC 1434. Most router vendors have implemented a mix of capabilities from both the 1434 standard and 6611 capabilities, while few have strictly adhered to the "standard." The most current iteration of DLSw resides in RFC 1795. This newer specification provides solutions for some of the reliability and timing issues of RFC 1434.

Neither RFC 1795 nor RFC 1490 support SNA/MS (SNA Management System) nor SNMP (Simple Network Management Protocol). The SNA data stream is encapsulated in TCP/IP or Frame Relay for most of the transmission between client and host. The routers and FRADs that perform the encapsulation/de-encapsulation are not aware of the SNA data stream or its need to report data to SNA/MS. An SNMP MIB for DLSw has been proposed and will be available as a post-RFC 1795, vendor-implemented solution.

2. AnyNet Approach
When merging SNA with TCP/IP networks, one alternative is IBM's AnyNet, also referred to as Multi Protocol Transport Networking (MPTN). AnyNet allows existing SNA applications written to APPC and CPI-C to communicate over TCP/IP.

AnyNet is essentially a gateway function that moves TCP/IP encapsulation of SNA from the hardware router down to the desktop and up to the mainframe. See Figure 2 for a depiction of the AnyNet approach.

Figure 2: AnyNet does not directly support dependent LU sessions.
SNA Application Support
AnyNet applications supporting APPC and CPI-C are available on most client platforms. However, LU0-3 support requires deployment of a separate AnyNet gateway.

Resource Requirements
No new LAN or WAN hardware is required beyond that used to create the TCP/IP network. However, one needs to employ a specialized TCP/IP pass-through controller, such as an IBM 3172, to forward the TCP/IP traffic to the mainframe.

Both the host and the client perform the encapsulation/de-encapsulation of SNA and TCP/IP frames. Additionally, the host manages each desktop separately as in all direct connect approaches. This consumes expensive CPU cycles on the host.

Network Management
With AnyNet, the network manager must configure static IP addresses for each client PC connecting to the mainframe. Although the clients can access the host using an IP name that is resolved by a DNS server, the host must locate the clients via a fixed IP address. This means the network manager cannot use Dynamic Host Configuration Protocol (DHCP), bootp, or Reverse Address Resolution Protocol (RARP) to assign IP addresses dynamically.

3. TCP/IP on the Host Approach
This approach makes the host look like a UNIX® system. IBM offers TCP/IP suites for MVS™ and VM today that support a number of terminal types and utilities, including TN3270, FTP and LPR/LPD. One of the benefits of TN3270 is that it is available on almost all client platforms, often as a low-cost solution. TN3270 clients are frequently included as part of TCP/IP protocol suites for the MS-DOS and Windows platforms.

Figure 3: The TCP/IP on the host approach lacks LU0 and LU6.2 support.
In a typical TCP/IP on the host scenario, such as that depicted in Figure 3, the client running a TN3270 emulator connects directly to the mainframe via a pass-through controller, such as an IBM 3172. The host then processes the TCP/IP frames received from the client. Additionally, the mainframe may support other TCP/IP-based services, such as FTP file transfer and LPR/LPD printing.

**SNA Application Support**

TN3720 provides LU2 terminal model types 2-5. This provides a base level of support for the majority of legacy mainframe applications. However, the TN3270 standard lacks graphics support, access to the SSCP-LU session, full host AID key functionality, and LU1 or LU3 printer emulation.

For instance, the standard printing solution available with TN3270 is LPR/LPD. This mechanism allows for a host-installed Line Printer Remote (LPR) process to send basic text data to a LAN-based or PC-based program via TCP/IP. The Line Printer Daemon (LPD) then translates the print data to the output accepted by the target printer. Some essentials are lacking in the LPR/LPD solution, such as end-to-end acknowledgment of successful output. Another problem with LPR/LPD is that it does not handle most host formatted data. For instance, it cannot support SCS and other common SNA printer commands.

Even without these 3270 session capabilities, customers and vendors have embraced TN3270. Over time, a number of client vendors offering TN3270 products implemented proprietary work-arounds for the lack of capability in TN3270. One de facto standard supported by some vendors was TN3287, which provides basic LU1 and LU3 printing.

Recently, a new, open standard was proposed to add the required functionality. This standard, called TN3270E, is embodied in RFC 1647. TN3270E overcomes most of the shortcomings of TN3270, including LU1 and LU3 printing. However, even TN3270E does not provide full SNA application support. TN3270E lacks Intelligent Printer Data Stream (IPDS) through Advanced Function Printing (AFP) for emulating IBM 3812 and IBM 3816 postscript printers. Most importantly, TN3270E lacks LU0 and LU6.2 application support.

**Resource Requirements**

Due to the substantial performance costs to the host, vendors have produced a number of methods to off-load some or all of the TCP/IP-to-SNA protocol conversion required to support TCP/IP client programs.

- **IBM 3172 Controller.** The 3172 can be run in pass-through mode or off-load mode. In pass-through mode, the 3172 sends TCP/IP directly to the host channel from the LAN. In off-load mode, the 3172 processes the lower-level TCP/IP stack, reducing the processing requirements on MVS or VM.

- **IBM 3745 with 3746 option.** The 3745 FEP only supports SNA protocols. The IBM 3746 add-on provides the TCP/IP-to-SNA off-load capability of the 3172 while leveraging the capacity of the 3745’s channel attachments. The 3746, like the 3745, is an expensive option. Maintenance costs alone for a 3745 can easily eclipse the costs of a complete channel-attached SNA gateway solution.

- **TCP/IP-to-SNA Gateway.** An SNA gateway can act as a centralized TN3270 server, providing a more complete TCP/IP-to-SNA off-loads than the IBM 3172 controller. Some, like SNA Server, support TN3270E (a new feature available as part of Service Pack 1 for SNA Server 2.11), as well as split-stack TCP/IP clients for LU0 and LU6.2 applications. Others support only the base TN3270 capability.
Network Management
With a TCP/IP on the host approach, just as with AnyNet, the network manager must configure static IP addresses for each client PC connecting to the mainframe. This can present a significant burden on the host and LAN administrators.

4. SNA Gateway Approach
This discussion focuses on SNA gateways that support native TCP/IP connections between client and server. We will refer specifically to Microsoft® SNA Server where needed to provide examples.

![SNA Gateway Diagram](image)

Figure 4: SNA gateways allow for flexibility when integrating TCP/IP networks with IBM mainframes.

SNA Application Support
SNA gateways can be configured to support LU0-LU6.2 applications on most client platforms, such as those depicted in Figure 4, across a TCP/IP LAN and WAN.

SNA gateways can perform multiple functions. They can function as TCP/IP-to-SNA protocol converters, supporting TN3270 emulators and split-stack SNA clients. Additionally, SNA gateways can function as servers for LU6.2 applications, such as high-speed file transfer or host database access. For example, SNA Server can function as an FTP server for TCP/IP clients uploading or downloading files to a mainframe. The mainframe does not have to run TCP/IP because a new feature in Service Pack 1 for SNA Server 2.11 converts the FTP commands to APPC File Transfer Protocol (AFTP) commands. The FTP (TCP/IP) to AFTP (APPC) protocol conversion takes place on the SNA Server (requires IBM APPC Application Suite for MVS or VM).
Resource Requirements
An SNA gateway approach allows the host to be configured only with native SNA. The workstations can be configured only with TCP/IP. The SNA gateway approach allows PU-sharing, reducing the number of PUs required on the host; therefore, the host only needs to poll the SNA gateway. With other host-access models, hundreds of end-user definitions are typically stored in resident memory on the host system and FEP, consuming expensive host resources. By assigning host sessions to individual user accounts on the SNA gateway machine, SNA gateways save memory and CPU cycles on the host system.

Existing routers can be used in connecting clients and central site gateways over a TCP/IP WAN. For examples, see SNA Server's connectivity options depicted in Figure 5.

Network Management
When all host-bound traffic is concentrated through an SNA gateway, the LAN administrator can use the performance monitoring, event logging, and tracing capabilities of the server platform. An individual desktop problem is easy to work around by simply assigning a new LU while the administrator performs debugging at the server without interrupting other users or restarting the server.

Administering and monitoring mainframe access can also be accomplished from an IBM host console when the SNA gateway, such as SNA Server, supports NetView®:

- SNA Server can be configured to provide custom alerts to NetView in addition to informational messages and alerts from any Windows NT™ Server in the domain.
- NetView RunCmd support enables the NetView operator to directly control all functions on the Windows NT Server running SNA Server. The SNA Server RunCmd service extends access to the Windows NT command line to NetView.
Not all organizations are ready to move to a single TCP/IP-only LAN and WAN. For example, many organizations have invested in leased SDLC lines between remote and central sites. SNA Server supports SDLC leased line connections to make use of existing infrastructure where appropriate. It is important that an SNA gateway approach be able to leverage current investments as well as provide for a migration. SNA Server offers three deployment options that support a migration to a TCP/IP-only LAN and WAN.

**Branch-Based Deployment Model** - The branch-based model is the traditional way to deploy SNA gateways. SNA Servers are placed in branches and communicate with the host using native SNA protocols via DLC/802.2, which are tunneled from the branch LAN to the central site LAN by routers using DLSw or RFC 1490. See Figure 6.

**Centralized Deployment Model** - Channel-attached or token ring-attached SNA Servers are placed at the data center and connect to the host using native SNA protocols. The centralized SNA Servers provide split-stack 3270 or TN3270 service for local and remote desktops, which connect to the gateways using TCP/IP. Additionally, client- or server-based LU0 or LU6.2 applications can connect through these gateways from anywhere on the TCP/IP WAN. See Figure 7.
Figure 7: Centralized SNA Servers support local and remote TN3270 emulators, split-stack TCP/IP clients, and server-based applications.

Distributed Deployment Model - Branch-based SNA Servers connect to the host through centralized SNA Servers. The distributed deployment model relies on a capability in Service Pack 1 for SNA Server 2.11 called Distributed Gateway Service, which allows the branch-based SNA Servers to connect to central SNA Servers using native TCP/IP. The centralized SNA Servers connect to the host via direct channel attachment or a local token ring using native SNA protocols. The most significant advantages of distributed deployment over centralized deployment are improved host response times for users in the branch offices and reduced load on the WAN. See Figure 8.
Other advantages of the distributed deployment model include:

- The branch-based SNA Servers can connect to the host via multiple centralized SNA Servers, load-balancing between the central site SNA Servers at connect time. Should a central site SNA Server fail for any reason, the branch-based SNA Servers will automatically establish a new connection through an alternate centralized SNA Server for fault-tolerance.
- As an additional backup, the branch-based SNA Servers can use the traditional SNA WAN, such as dial-up SDLC, to connect to the host should the TCP/IP WAN fail.
- Since the central site SNA Servers provide the equivalent of PU pass-through service for the branch-based SNA Servers, the host operator sees each branch-based SNA Server as a single PU and can manage the branches via standard NetView alerts and RunCmds.

Summary
The SNA gateway approach to integrating mainframes with TCP/IP networks achieves the goals of most network managers, including supporting the complete range of existing SNA applications; reducing the resource requirements on the desktop, network and host; and allowing easy network management. Unlike the PU on every desktop approach, an SNA gateway allows for a TCP/IP only LAN and WAN. Only TCP/IP is required on the desktops to support all SNA protocols. The host is not burdened with the TCP/IP-to-SNA protocol conversion, as in the cases of AnyNet and TCP/IP on the host.

An SNA gateway can support both TN3270 and native SNA clients while offering a more cost-effective off-load than a 3172 or 3746. Finally, the SNA gateway approach ensures greater flexibility in deployment, offering a migration plan from current host-access methods.