

APPN—A Technology Overview

Systems Network Architecture (SNA) was introduced in 1974. Over the last 25 years, it has been used by most Fortune 1000 companies to support their mission-critical applications. The earliest SNA implementations assumed that the enterprise server running Advanced Communications Function/Virtual Telecommunications Access Method (ACF/VTAM) was the hub of the network, responsible for establishing all sessions and activating and deactivating resources. The design goal of these early subarea SNA networks was reliable delivery of information across low-speed analog lines. Resources were explicitly defined, eliminating the need for broadcast traffic, and header overhead was minimized.

What Is APPN?

Advanced Peer-to-Peer Networking (APPN) is second-generation SNA. It moves SNA from a hierarchical enterprise server-centric environment to a peer-to-peer environment, providing capabilities similar to other LAN protocols, such as dynamic resource definition and route discovery. Given the success of subarea SNA, what were the requirements for a new generation of SNA?

- Unlike other protocols today, legacy SNA was not dynamically routable at Layer 3, requiring static path definitions and loss of session connectivity when network outages occurred.
- The addition of TCP/IP to the enterprise server moved the data center from an SNA-centric environment to a multiprotocol environment, which required a new format of “router” that could support SNA and TCP/IP traffic into the enterprise server.

- The subarea SNA network was not a flat address space. It required that “local” addresses be translated to “network” addresses at the edge of the network.
- A variety of scalable servers no longer required that sessions be managed through ACF/VTAM.
- The requirement to predefine resources and routes was no longer acceptable.
- Session disruption during a network failure was no longer acceptable in global enterprises that required 7x24 availability.

APPN enhances subarea SNA with the following features:

- Two types of APPN nodes are defined. Network nodes (NNs) are SNA routers, responsible for locating resources, selecting paths, and working with the users to set up sessions. End nodes (ENs) are application hosts, end users, or controllers representing multiple users.
- The topology of the network is not predefined. NNs exchange information so that each has an entire picture of the network—all the NNs and links connecting them. Each NN also maintains a local topology—the ENs and links between ENs and NNs.
- Directory services are distributed. Each NN knows about the resources attached to its ENs, plus other network resources that have sessions with its resources. Locations of network resources are determined via broadcast or through a central directory server (CDS).
- SNA class of service (COS) enables paths to be selected to deliver an appropriate service level and messages to be prioritized to ensure that the service level is maintained.

- Using High Performance Routing (HPR), APPN can reroute a session around a failure in the network if an alternate path providing the appropriate level of COS is available.
- Like TCP/IP, flow control, error control, and segmentation are performed end to end, providing an increase in throughput when compared to earlier subarea node-to-node support.

The original APPN architecture was defined so that NNs maintained local and network topology databases. When an EN requests a session setup for a pair of resources, the NN first looks in its directory to see if it knows the location of the destination. If it does, session setup can proceed. If it does not know the location of the destination, the NN sends a broadcast throughout the network to locate the destination. When the destination is found, the NN adds information about the destination to its directory, selects a session path to meet the COS defined in the session setup request, and tells the EN to complete session setup.

When Is APPN Required?

In fact, APPN is never required. Subarea SNA can continue to be supported, even in a multiprotocol environment, either using a separate parallel network for SNA or encapsulating subarea traffic in TCP/IP, using a standard such as data-link switching (DLSw). Today, the trend is to move to an IP infrastructure to support the corporate intranet and Internet strategies of enterprises and position them for future multiservice networks that include voice and video, in addition to data. For this reason, Cisco is seeing more and more enterprises consolidate their SNA and IP networks, rather than maintain parallel networks. GartnerGroup, in a research note published February 1999 and titled "The Last SNA Network?," states: "Enterprises that continue to use SNA networks as their primary access to enterprise server data will spend more money and derive less benefit from their network than those that run a consolidated internetwork based on IP."

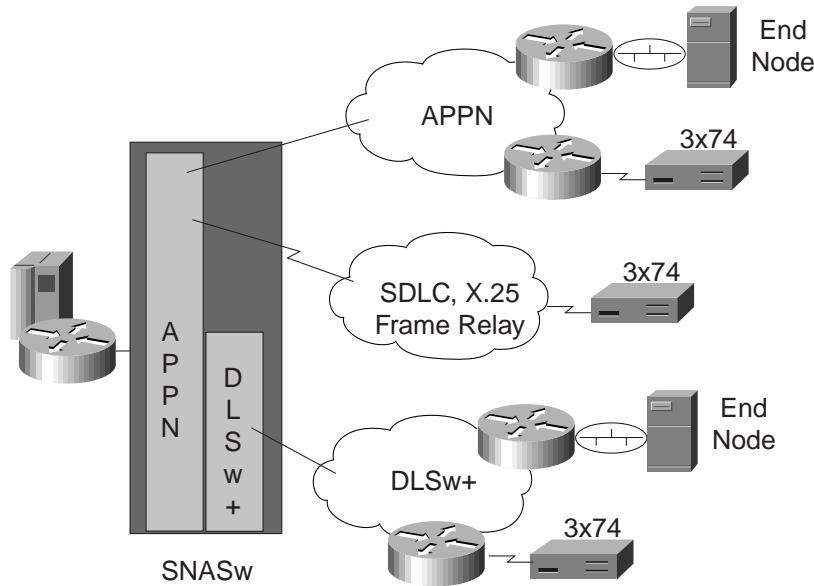
As enterprises move to an IP infrastructure with SNA and IP applications in the data center, front-end processors (FEPs) must be replaced to provide adequate TCP/IP support. Channel-attached multiprotocol routers provide the connectivity, while APPN on the router provides SNA routing between enterprise servers. If multiple servers exist, an SNA routing decision must be made somewhere.

Traditionally, SNA routing decisions were made in the enterprise server or FEP. Cisco APPN support has enabled this functionality in the Cisco routers.

Although APPN can be beneficial in the consolidated infrastructure, it is important to carefully plan and design where APPN is used in the network and data center. As the infrastructure moves to IP, it is not necessary to place APPN routing throughout the network. In fact, a single SNA routing decision is all that is required. In most cases, that decision can occur in the data center, eliminating native SNA routing from the network. Moving that decision to an aggregation point, or regional office, might be beneficial if traffic is consistently routed between multiple data centers. APPN routing at each remote location is not necessary unless branch-to-branch routing is required and the direct links are available to transport the traffic.

As shown in Figure 1, APPN in the data center can support a variety of SNA traffic and can be transported concurrently with TCP/IP directly into the enterprise server over the Channel Interface Processor (CIP) or Channel Port Adapter (CPA). SNA devices can attach directly into the APPN router. APPN ENs can also attach into that router. Finally, DLSw+ can transport both APPN and subarea traffic across the IP network into the APPN router.

Figure 1 Data Center Router Supporting APPN and TCP/IP



How Should APPN Be Integrated into the IP Infrastructure?

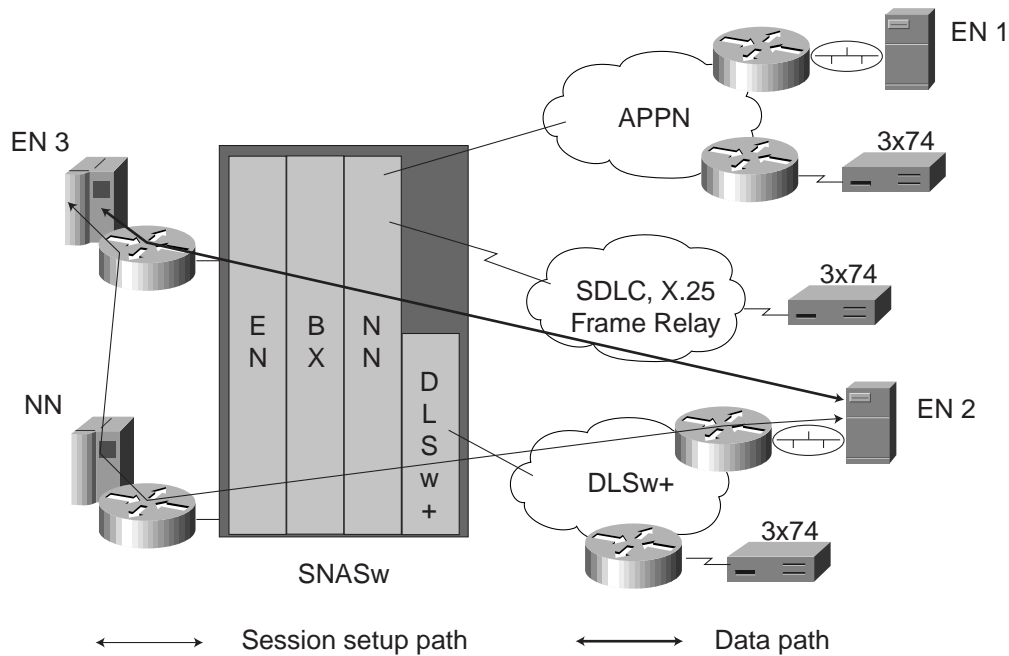
Implementing Cisco SNA Switching Services (SNASw) provides the APPN functionality needed by enterprises today while simplifying network design and configuration.

Minimizing the number of APPN NNs has been a necessity, traditionally, because of scalability issues associated with the original architecture. This is an additional reason why 90 percent of the enterprises implementing APPN today do so in the data center or regional offices only. Because NNs maintain large topology databases and issue broadcasts for topology updates and resource discoveries, the NN has required significant resources in terms of memory and processing. It has also required considerable system definition to customize a

particular network design. The SNASw solution eliminates scalability issues by no longer implementing a full NN, but instead provides Branch Extender (BX) node functionality.

BX is an architectural feature of APPN that appears as an EN to VTAM and a NN to downstream APPN devices. It effectively subdivides the network into manageable subnets. Because NNs exchange topology information only with other NNs, BX effectively eliminates topology exchanges. Discovery traffic is also minimized without full NN support. Figure 2 expands on the network design in Figure 1 and demonstrates the effect of BX.

Figure 2 BX in the Data Center



EN1 and EN2 go to the BX for NN services. The BX passes these requests on to the VTAM NN in the enterprise server. VTAM selects a session path to the application host, EN 3, and BX routes all subsequent data messages on that path without having to go to the NN VTAM.

Cisco recommends to its customers that they move to SNASw for APPN support, implementing BX nodes instead of NNs to provide a more scalable and simpler network design.

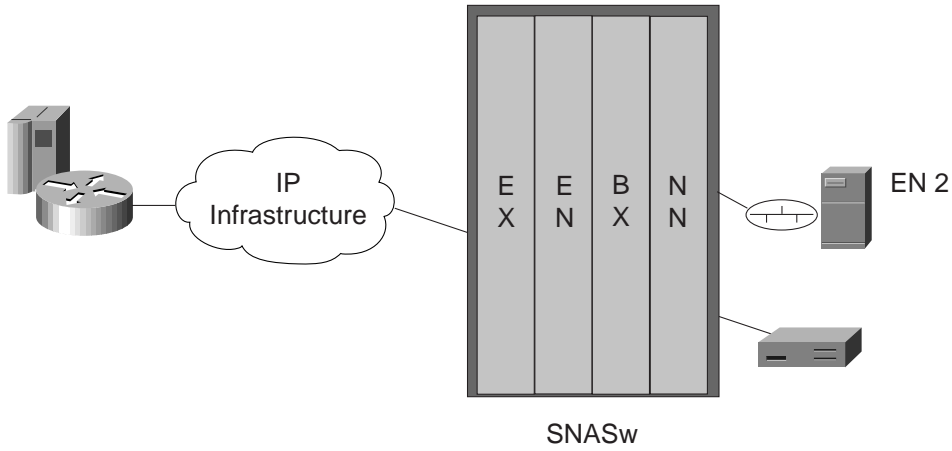
A second feature of SNASw is Enterprise Extender (EX). EX routing at Layer 3 is done using the IP routing infrastructure, while APPN HPR is used to provide reliability. Therefore, end-to-end error control, flow control, and segmentation are performed using HPR's Rapid Transport Protocol (RTP), while each SNA device maintains an IP address and routing is accomplished using one of the IP routing algorithms. EX has been implemented in OS/390

(V2R6 with authorized program analysis report OW36113, or a higher version), which means that the enterprise server can now send IP packets for all traffic—SNA and IP.

EX provides a means to transport SNA data over an IP network. Although DLSw+ also provides this capability, the EX functionality is unique because EX is also supported on the enterprise server. EX therefore, provides the only solution that allows a pure TCP/IP data center while supporting legacy SNA applications and desktops.

Figure 3 demonstrates how EX could be implemented. In this example, an SNASw node is implemented in the branch router to convert the traffic from IP to SNA. Across the WAN, the SNA traffic is routed using IP routing. The end-to-end flow control, error control, and segmentation would be performed between the EX router at the branch and the application server in the data center.

Figure 3 EX Network Design with EX in the Remote Office



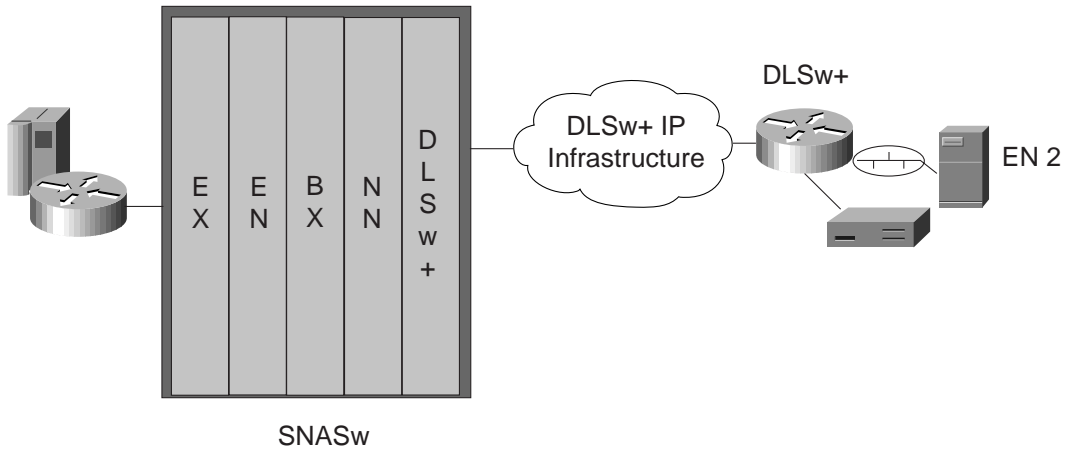
Although this network design does eliminate SNA from the data center and WAN, there are some issues that must be considered when choosing this design:

- Software on the enterprise server must be OS/390 V2R6 with authorized program analysis report OW36113, or a higher version.
- All remote routers must be upgraded to support EX.
- The points of failure are the enterprise server and the remote router supporting EX.

- Failures in the network or in the enterprise server could result in a large number of HPR session switches, including rebuilding of HPR RTP connections or session restarts if the RTP endpoint fails.
- EX can be considered a riskier solution, because large networks that have implemented this design do not yet exist and performance impacts in the enterprise server are not yet fully understood.
- Additional processing requirements in the enterprise server are required to convert from SNA to TCP/IP.

Figure 4 presents a second design using EX and Cisco DLSw+.

Figure 4 EX with DLSw+ Network Design



In this design DLSw+ is maintained across the WAN, while EX is implemented only in SNASw in the data center.

Although it might seem more efficient to run EX all the way to the branch office, there are some issues that are addressed by this design:

- Existing remote DLSw+ routers need not be upgraded to a new level of software.
- The number of HPR RTP connections is minimized.
- DLSw+ is a less risky solution, with more than 500,000 routers implementing DLSw+ today.

On the other hand, DLSw+ introduces an additional point of failure in the data center DLSw+/EX router. Looking at these two options, Cisco recommends that each enterprise examine the issues and choose the best design based on those issues.

Summary

APPN is a powerful technology that provides native SNA routing to enterprise networks. It enables enterprises to upgrade their data centers with routers that support SNA and IP applications on the enterprise server. As enterprises develop new IP applications and move to a corporate IP intranet, the ability to support a consolidated data center is key.

It is important to note, however, that to achieve the benefits of APPN a minimum number of APPN routers are required and a full NN implementation in the data center router is generally unnecessary and undesirable. The goal of an enterprise should be to add sufficient APPN support to provide the needed SNA routing while minimizing the amount of SNA traffic in the network. The Cisco SNASw solution does this with BX, which provides direct routing of data to the correct application host, supports all downstream subarea and APPN devices, and minimizes the scalability and complexity issues associated with a network containing a large number of NNs. The SNASw solution also provides EX, which can be used to more fully integrate APPN into the IP network and data center.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas
Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 1999 Cisco Systems, Inc. All rights reserved. Printed in the USA. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9907R) SPS 8/99