

Migration Scenarios

This chapter shows the basic configuration of several of the most common networks. The chapter covers network design and explains why and when to use a particular network design. It briefly describes how to migrate from, or coexist with, a FEP for each of the sample networks. In some cases, before and after pictures of the network and step-by-step configuration instructions are included.

This chapter includes the following scenarios:

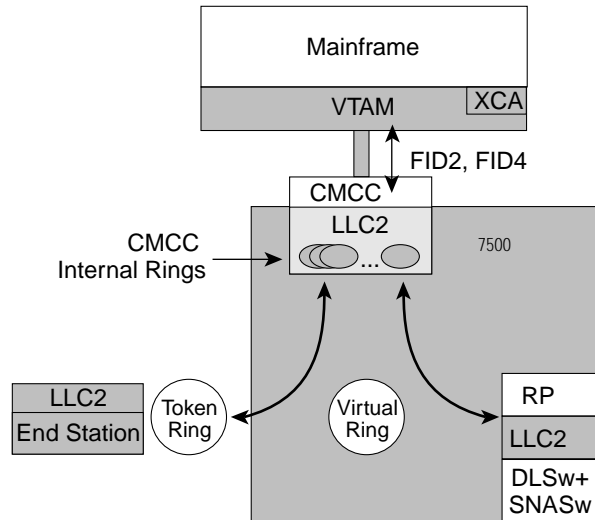
- Scenario 1—Replacing a FEP with a single CMCC on a single host
- Scenario 2—Replacing a FEP with a redundant CMCC on a single host
- Scenario 3—Replacing a FEP with a single CMCC on multiple hosts
- Scenario 4—Combining SNASw with DLSw+
- Scenario 5—Migrating to SNASw only
- Scenario 6—Migrating to TCP/IP across CLAW
- Scenario 7—Migrating to TCP/IP across CMPC+

To use the scenarios, you must include the VTAM definitions and configure your routers, which are discussed in the following sections.

Using SNA Communication over CSNA

SNA nodes communicate with the CMCC using LLC2, a connection-oriented data-link protocol for LANs. An LLC2 stack on the CMCC card communicates with either the adjacent SNA device (over a physical Token Ring) or to DLSw+ or SNASw running in the channel-attached router, as illustrated in Figure 6-1.

Figure 6-1 Communication between CSNA in the CMCC and SNA Nodes



The CMCC running CSNA can support multiple internal LAN interfaces, each appearing as a LAN port to the VTAM. Although VTAM supports a maximum of 18 LAN ports, only a single LAN port is required. CSNA also supports up to 256 open LLC2 service access points (SAPs) per LAN port.

Using VTAM Definitions

The CMCC running CSNA is not an SNA-addressable node, because it has no PU or LU appearance. CSNA is defined to the host control program (MVS or VM) as a channel-to-channel machine (an IBM 3088). CSNA provides VTAM with a physical connection to the LAN through a subchannel.

To enable VTAM communication over the CMCC to SNA devices, you must configure an XCA major node and a switched major node to VTAM. The XCA major node allows VTAM to communicate with the CMCC, and the switched major node definition allows SNA devices to communicate with VTAM over the CMCC.

XCA Major Node Definition

Define an XCA major node for each connection (port) between the VTAM and a CSNA. A single XCA major node can support up to 4096 LLC2 connections, although better results are achieved with 3000 or fewer LLC2 connections per XCA major node. If more LLC2 connections are needed, define additional XCA major nodes as well. You can configure multiple XCA major nodes for availability, with each node pointing to a different CMCC.

The CSNA feature is defined to the host control program (MVS or VM) as being a channel-to-channel adapter (CTCA) or machine; for example, an IBM 3088. VTAM identifies the CSNA gateway through a combination of the following:

- ADAPNO—Adapter number
- CUADD—Subchannel address
- SAPADDR—SAP address

The following configuration provides an example:

```
XCANAME VBUILD TYPE=XCA ** EXTERNAL COMMUNICATION ADAPT**
PORTNAME PORT ADAPNO=?, ** RELATIVE ADAPTER NUMBER ** X
      CUADDR=???, ** CHANNEL UNIT ADDRESS ** X
      MEDIUM=RING, ** LAN TYPE ** X
      SAPADDR=4 ** SERVICE ACCESS POINT ADDRESS **
GRPNAME GROUP ANSWER=ON, ** PU DIAL INTO VTAM CAPABILITY ** X
      AUTOGEN=(5,L,P), ** AUTO GENERATE LINES AND PUS ** X
      CALL=INOUT, ** IN/OUT CALLING CAPABILITY ** X
      DIAL=YES, ** SWITCHED CONNECTION ** X
      ISTATUS=ACTIVE ** INITIAL ACTIVATION STATUS **
```

Switched Major Node Definition

Configure one or more switched major nodes. Within a switched major node definition, configure every SNA PU that will access VTAM through the CMCC. For each PU, configure its associated LUs. Many networks today already include SNA devices defined in a switched major node. For example, if the devices attach to a FEP over Token Ring, the devices are defined as part of a switched major node. In this case, the only change is to add the XCA major node.

The following configuration provides an example:

```
SWMSNAME VBUILD          TYPE=SWNET,          **      X
                          MAXGRP=14,          **      X
                          MAXNO=64           **
PUNAME PU                ADDR=01,            **      X
                          PUTYPE=2           **      X
                          IDBLK=???,         **      X
                          IDNUM=???,         **      X
                          ISTATUS=ACTIVE     **      X
LUNAME1 LU               LOCADDR=02
LUNAME2 LU               LOCADDR=03
LUNAME3 LU               LOCADDR=04
LUNAME4 LU               LOCADDR=05
LUNAME5 LU               LOCADDR=06
```

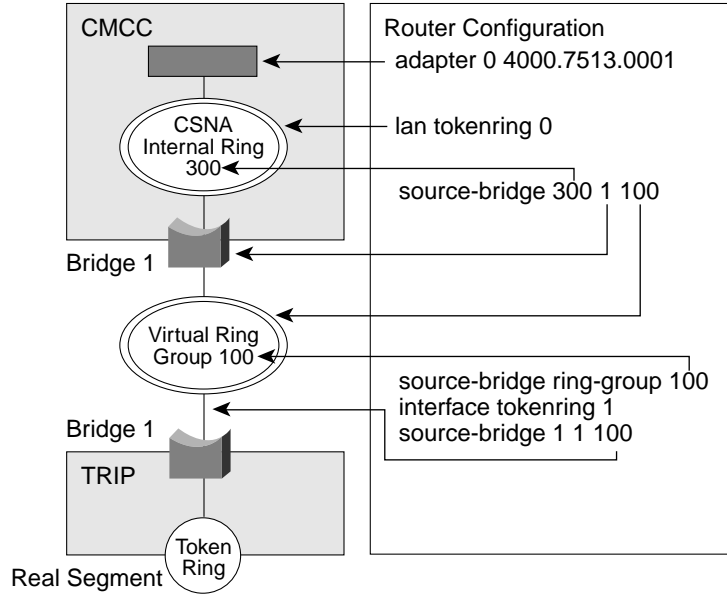
Configuring Routers

You must configure the router to:

- Bridge the traffic from a physical LAN or a router component (DLSw+, SRB, SR/TLB, and so on) onto the router virtual ring
- Bridge the data from the router virtual ring to one of the CMCC internal rings, or connect a data-link user (APPN or DSPU) to one of the CMCC internal rings
- Connect the CMCC to VTAM

Figure 6-2 shows the major configuration parameters of CMCC and Token Ring interfaces and how they are logically combined using the source-bridge definition. The CMCC ring is referred to as an internal ring. The Route Switch Processor (RSP) ring is referred to as a virtual ring.

Figure 6-2 Using Virtual Rings to Provide Connectivity

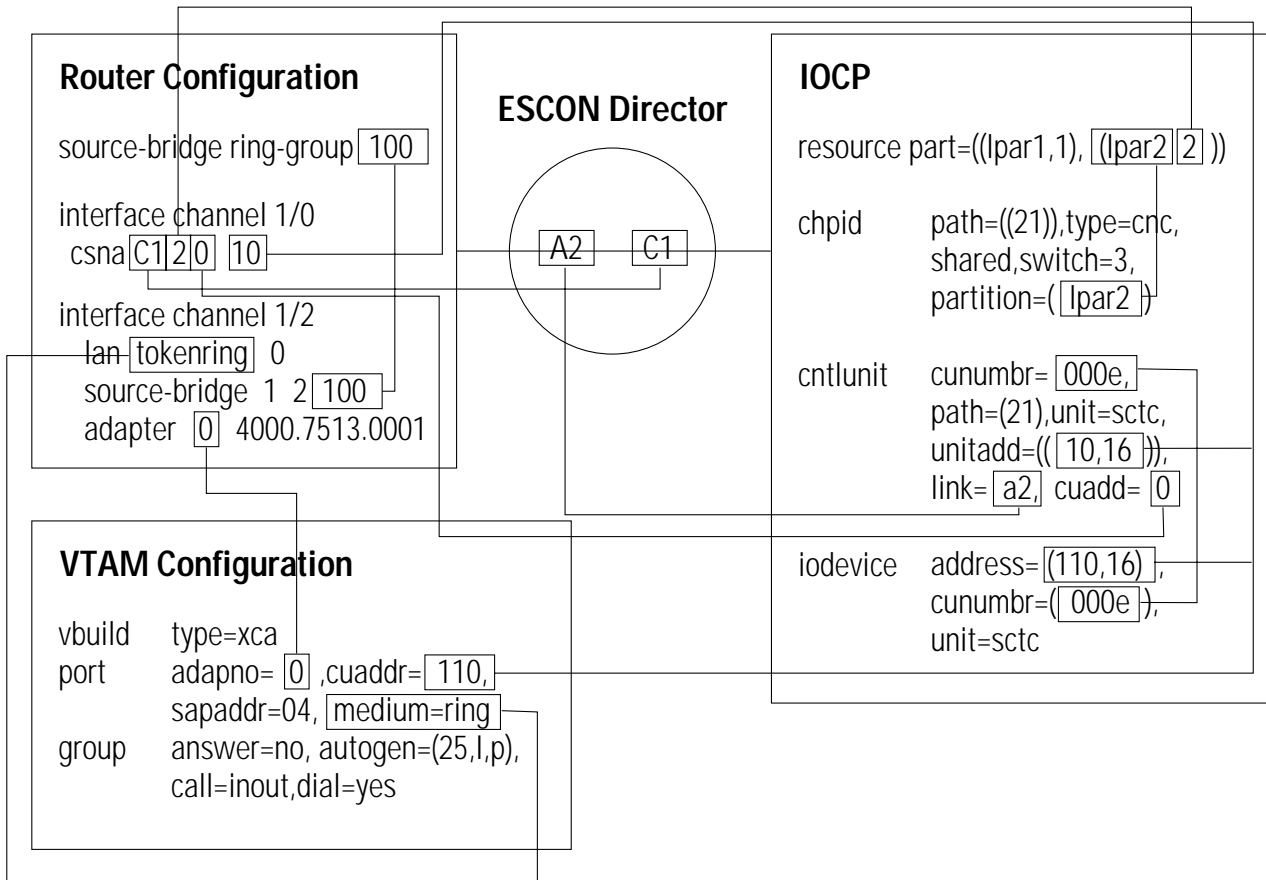


Configure an adapter on the CMCC to associate with the XCA major node definition. For each adapter you configure, CSNA creates an internal Token Ring. A virtual bridge connects the CSNA internal ring to a virtual ring group in the router. The Token Ring Interface Processor (TRIP) is also configured to connect to the same virtual ring group as the CMCC.

Understanding Configuration Relationships in the ESCON Environment

Figure 6-3 shows the relationship among router configuration, VTAM parameters, and MVS IOCP generation commands when the CMCC connects via an ESCON Director.

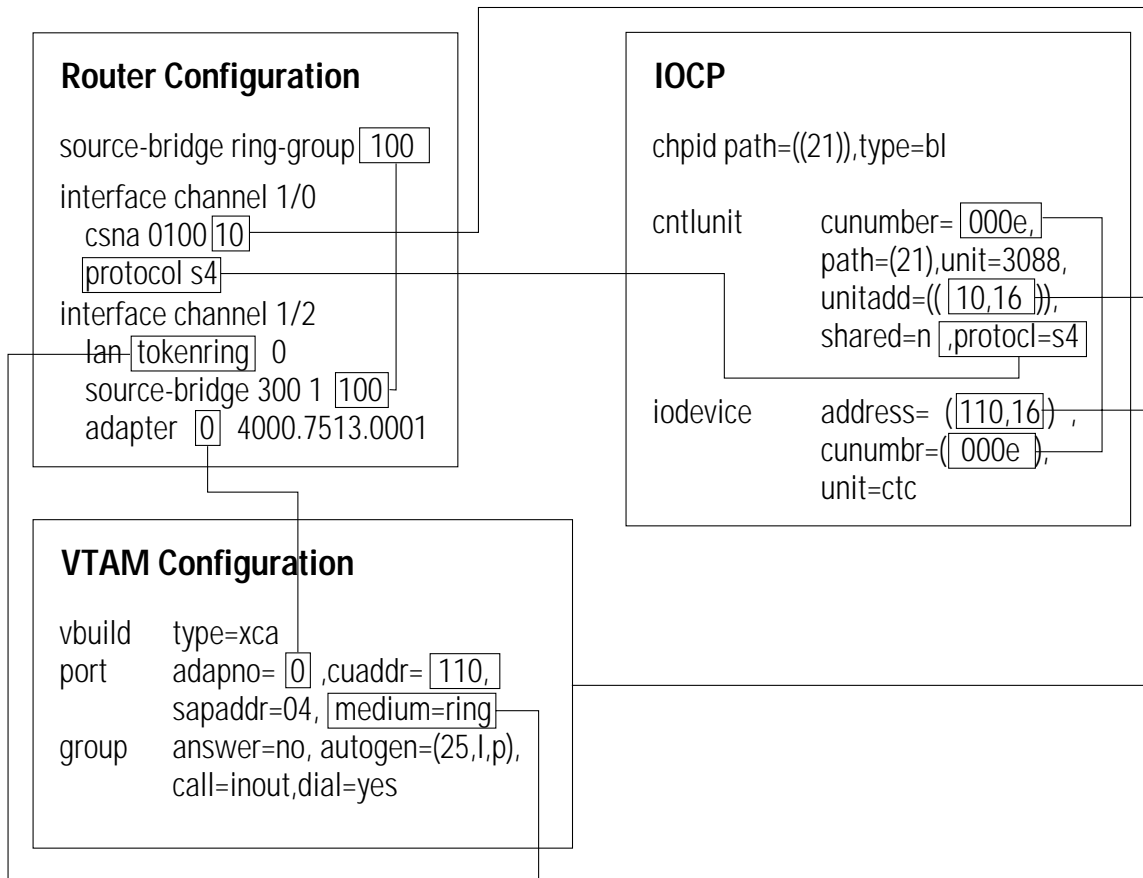
Figure 6-3 Configuration Relationship in an ESCON Environment



Understanding Configuration Relationships in the Bus and Tag Environment

Figure 6-4 shows the relationship among router configuration, VTAM parameters, and MVS IOCP generation commands when the CMCC connects via bus and tag.

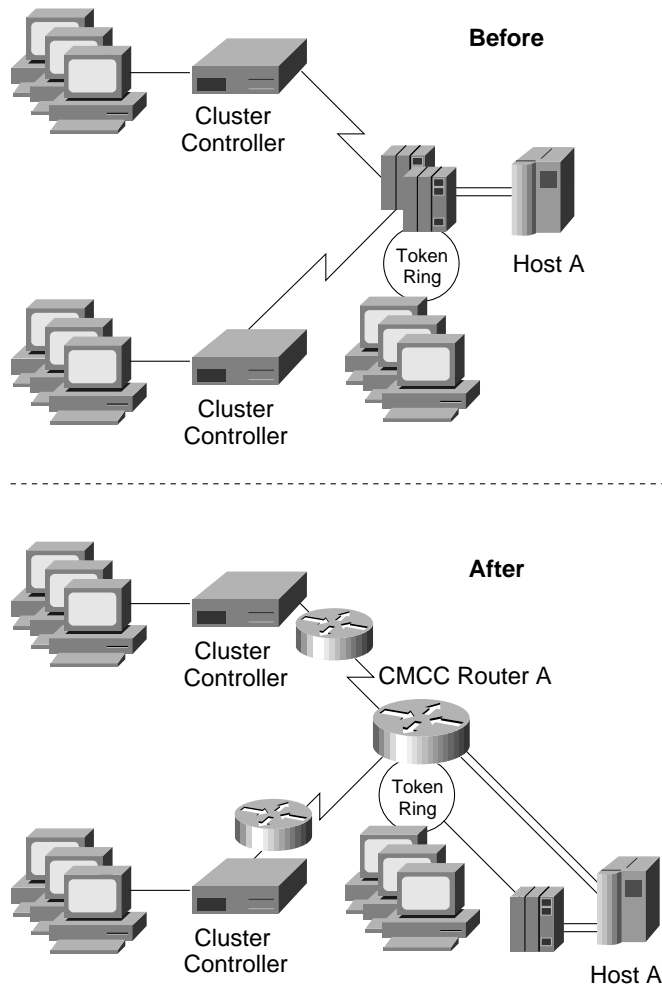
Figure 6-4 Configuration Relationship in a Bus and Tag Environment



Scenario 1—Replacing a FEP with a Single CMCC on a Single Host

The first scenario describes a network that replaces a FEP with a CMCC. As shown in Figure 6-5, a single mainframe exists in this network. Historically, IBM SNA networks were built using the IBM FEP, and remote terminals were connected via SDLC links. In the Before scenario, a second FEP was in place only for backup. In the After scenario, one FEP is replaced with a channel-attached router with a CMCC. Both the CMCC and the remaining FEP have the same MAC address. Eventually, the second FEP also will be replaced, but for now it provides SNI connectivity to a supplier and functions as a backup to the CMCC. DLSw+ is used to transport SNA traffic from remote sites to the central site. When data reaches the headquarters site, DLSw+ sends the traffic to the CMCC, which is the first to respond to explorers. In the event the CMCC is not available, the FEP is used automatically.

Figure 6-5 Single CMCC to Single Host



Reasons for Change

The FEP was at capacity and the company preferred to use its IS dollars on technology that would carry the company into the future while addressing today's requirement. In addition, the Cisco channel-attached router replacing the leased FEP would pay for itself in 18 months—with savings coming from lease costs and monthly NCP licensing costs. Migrating from an SDLC/FEP network to a LAN/channel-attached router network simplified SNA system configuration significantly and reduced the downtime for planned outages. Finally, this infrastructure enabled the customer to use TCP mainframe applications in the near future.

Design Choices

This customer opted to combine SNA functionality (DLSw+) and WAN connections in the CMCC router because the network was very small (25 sites). The design provided a very safe fallback to the FEP, but at the same time enabled SRB dynamics and configuration simplicity.

XCA Major Node Configuration

```
XCANODE    VBUILD    TYPE=XCA
PRTNODE    PORT      ADAPNO=0 , CUADDR=770 , SAPADDR=04 , MEDIUM=RING , TIMER=30
*
GRPNODE    GROUP     ANSWER=ON,           X
                        AUTOGEN=(100,L,P),          X
                        CALL=INOUT,                 X
                        DIAL=YES,                    X
                        ISTATUS=ACTIVE
```

Router Configuration

```
!
source-bridge ring-group 100
!
interface tokenring 1/0
- no ip address
- no ip route-cache
- ring-speed 16
- source-bridge 200 1 100
!
interface Channell/0
- no ip address
- csna 0100 70
!
interface Channell/2
- no ip address
- no keepalive
- lan TokenRing 0
- source-bridge 300 1 100
- adapter 0 4000.7000.0001
!
end
```

Implementation Overview

The first step is to implement DLsw+ from the remote site to the central site and to change the FEP access from SDLC to Token Ring. As part of this step, configure the VTAM switched major nodes. Next, perform the following steps to enable the CMCC in this configuration:

- Step 1. Perform IOCP generations to configure the channel definitions, as shown in Figure 6-5.
- Step 2. Configure the VTAM XCA major node.
- Step 3. Configure the attached router with the CMCC definitions and bridge traffic from the internal ring group to the CMCC virtual ring.
- Step 4. Vary the channel online (Vary E00,ONLINE).
- Step 5. Confirm the CMCC is online (Display U,,E00,1).
- Step 6. Activate the VTAM XCA (Vary NET,ACT,ID=name_of_member).

Scenario 2—Replacing a FEP with a Redundant CMCC on a Single Host

Initially this site had an IBM 3745-410 running in twin-standby mode to provide better network resiliency. In this case there is one active NCP while the second one is in standby mode. The second NCP takes over only if the first NCP has problems. This allows quick recovery from storage-related failures and from a CCU hardware check. Note that the idle CCU is inactive unless a failure is detected. With the inclusion of duplicate Token Ring addressing, this design provides another level of network redundancy.

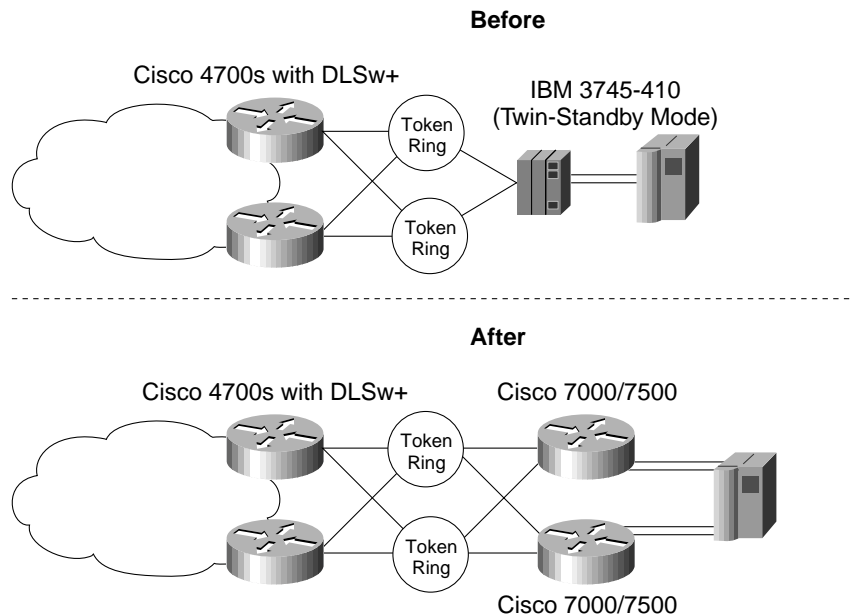
Optionally, the IBM 3745-410 could be configured in twin-backup mode, where each CCU controls approximately half the network. It is the equivalent of having two IBM 210s running at half capacity. If there is a failure in one CCU, the other takes over, just as in the first example. However, only half the resources are impacted, resulting in a faster recovery.

Regardless of the current configuration, the use of CSNA on two Cisco 7500 Series routers with one or more CMCC cards can provide better load sharing and redundancy features, as described in the Designing for High Availability section.

The After scenario is designed without a single point of failure in the network. The redundant CMCC to a single host scenario is often used when the end systems cannot afford the downtime of a failure. For many companies that require online access to provide 24-by-7 customer support, the loss of host access for even a short period can incur a significant loss in both income and credibility. It is important for these networks to implement a solution that avoids or minimizes the amount of downtime due to network problems. Also, for these companies the redundancy option provides the necessary network configuration to perform maintenance or configuration changes with minimal impact on the end-system users.

Providing redundancy to the single CMCC to single host solution is quite straightforward. In Figure 6-6, two Cisco 7500 Series routers, each with a CMCC, are deployed in place of the IBM 3745-410. In this example both CMCCs have the same virtual MAC address. When one router is unavailable, the SNA end system automatically finds the backup router using standard SRB protocols. Note that in both the Before and the After networks, the loss of a channel-attached gateway is disruptive.

Figure 6-6 Redundant CMCCs to Single Host



Reasons for Change

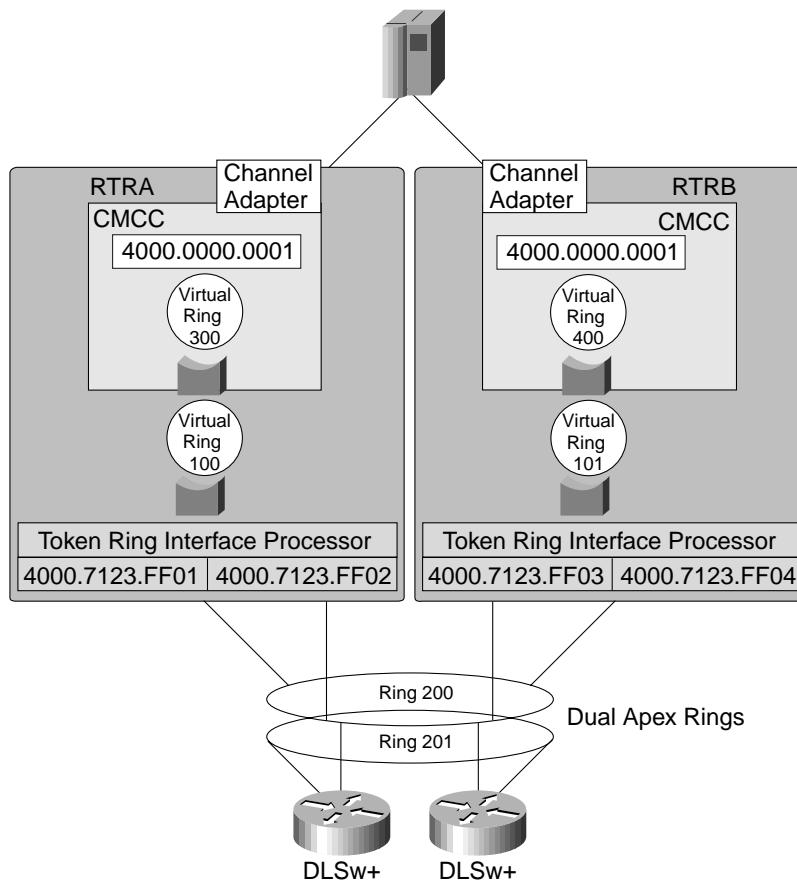
The IBM 3745-410 did not have the capacity to support the entire network if one of the processors was down. During outages, the entire network slowed down. To address this problem with more FEPs was not cost-effective. In addition, this enterprise was considering migrating to FDDI, which the IBM 3745 does not support. With the Cisco channel-attached routers, the company could migrate its campus to FDDI, ATM, or Gigabit Ethernet in the future.

Design Choices

In this network they opted to separate DLSw+ from the channel-attached router, thus minimizing both scheduled and unscheduled outages in their network. Also, they already had DLSw+ installed in these routers before they installed the CMCCs, which simplified migration. Finally, as their DLSw+ routers (Cisco 3600s) reach capacity, it would be less costly to add a Cisco 3600 Series router than a Cisco 7500 Series router with a CMCC. Either of the channel-attached routers could handle their entire capacity today, and if the network were to grow, they would have sufficient slots in their Cisco 7500 Series routers to add CMCCs.

The network uses load balancing across central site DLSw+ routers and duplicate Token Rings to ensure there is no single point of failure, as shown in Figure 6-7.

Figure 6-7 Dual Routers with Duplicate MACs



Router Configuration

This configuration uses the same MAC address on internal Token Ring LANs of two different routers:

```
RTRA
!
source-bridge ring-group 100
int tok 0/0
source-bridge 200 1 100
int tok 0/1
source-bridge 201 2 100
!
interface Channell/0
- no ip address
- csna 0100 70
!
lan TokenRing 0
- source-bridge 300 1 100
- adapter 0 4000.0000.0001
!

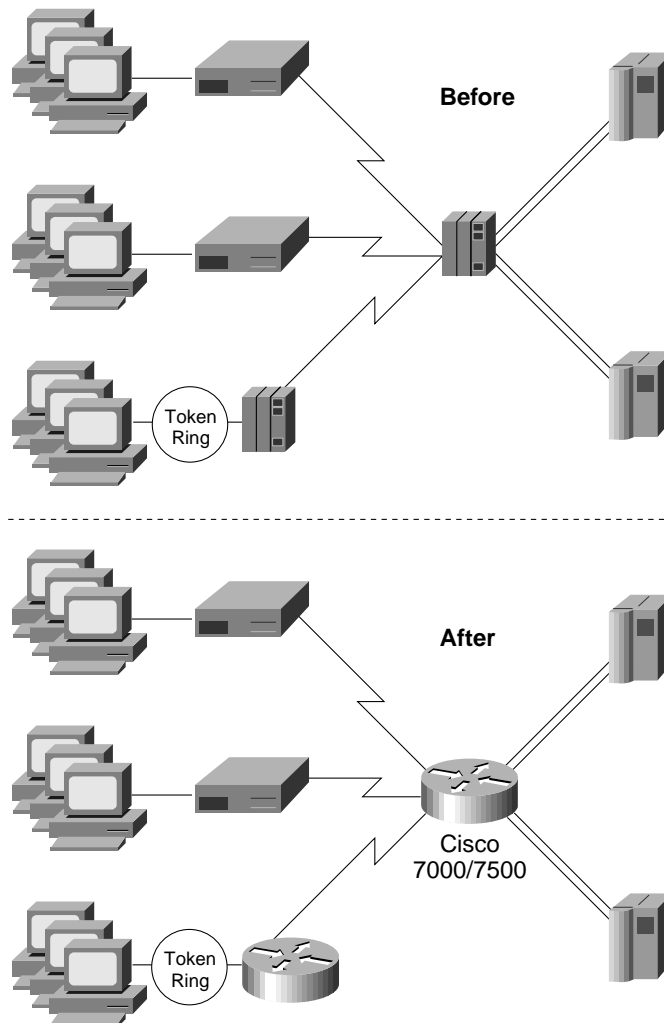
RTRB
!
source-bridge ring-group 101
int tok 0/0
source-bridge 200 1 101
int tok 0/1
source-bridge 201 2 101
!
interface Channell/0
- no ip address
- csna 0100 80
!
lan TokenRing 0
- source-bridge 400 1 101
- adapter 0 4000.0000.0001
!
```

Scenario 3—Replacing a FEP with a Single CMCC on Multiple Hosts

This scenario reflects a legacy SNA network with several remote sites connected via SDLC links to cluster controllers. Also, a high-speed line was connected to a remote IBM 3745 at a site that demanded high-speed connection back to the mainframe, but had more remote users than a cluster controller could support. This enterprise also had a separate multiprotocol network running in parallel.

At the data center, there are two VTAM's. One is used primarily for production and the other for testing. There is little, if any, cross-domain routing. Figure 6-8 shows the Before and After networks.

Figure 6-8 Replacing a Single FEP with a Channel-Attached Router



Reasons for Change

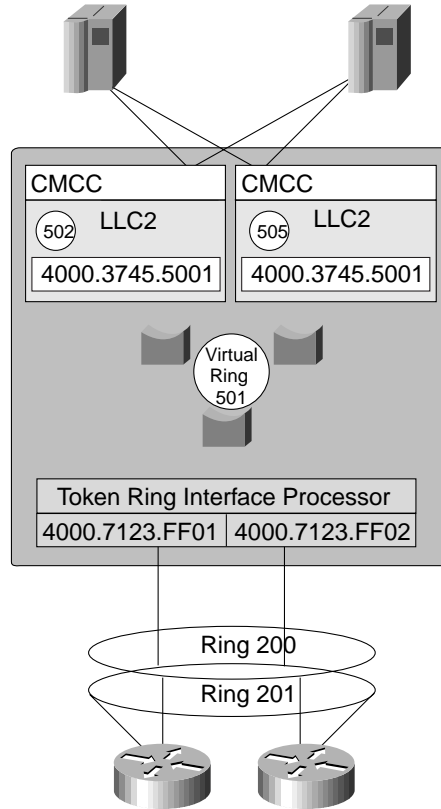
The primary reasons for change were to minimize costs and increase throughput and flexibility. The remote IBM 3745 was replaced with a lower-cost Cisco 4500 Series router to eliminate recurring NCP and maintenance charges, consolidate multiprotocol and SNA WAN traffic, and simplify network configuration. The central site FEP was replaced with a channel-attached router to increase channel throughput and to enable TCP/IP on the mainframe in the future.

Design Choices

This enterprise chose not to implement APPN despite having multiple mainframes. The reason is that all SNA sessions were in the same domain. The VTAM in the second mainframe was used just for testing and backup. They decided against implementing two channel-attached routers for redundancy, but did use two CMCCs in a single channel-attached router. This created higher availability than they had previously and provided an option

to separate CMCC functionality across multiple CMCCs in the future. They plan eventually to add TN3270 Server capability to the CMCC to allow access to VTAM applications from Web-based clients. They also anticipate a need for TCP/IP on the mainframe. Figure 6-9 shows the logical configuration.

Figure 6-9 Dual CIPs in a Single Router



Scenario 4—Combining SNASw with DLSw+

In this case study, the enterprise wants to leverage its Parallel Sysplex complex and achieve the high availability it affords. The customer is migrating to Gigabit Ethernet in the data center and the applications are being rewritten to run TCP/IP natively. However, it will be several years before that migration is complete, and in the interim, the customer wants the high availability and design simplicity afforded by having an all-IP data center.

Reasons for Change

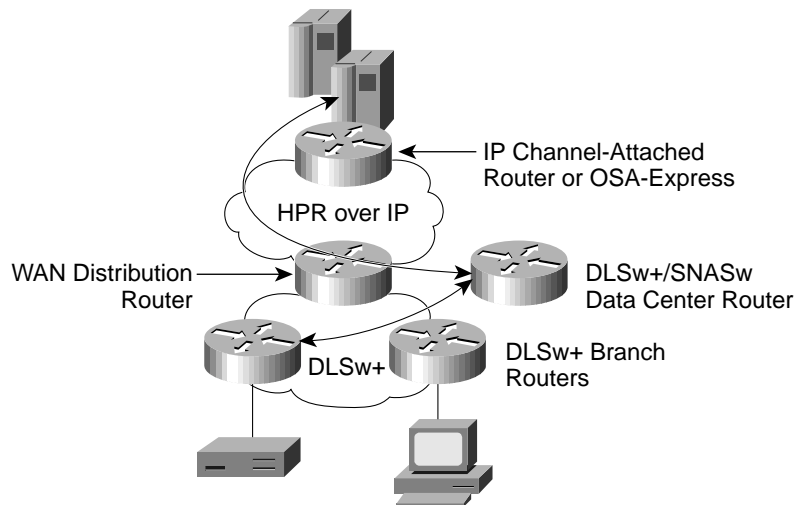
This enterprise already uses DLSw+ to transport SNA traffic over an IP backbone. The customer chose not to make an additional investment in SNASw for the branch because the DLSw+ network has been very stable, and if outages occur, they affect only a small portion of the network (by design) and are recovered automatically. However, the customer wants to ensure that a CMCC or channel outage (which today would bring down almost the entire network) can be handled transparently. Hence, the customer is adding SNASw to the SNA routers. The SNA routers use DLSw+ to transport SNA traffic to and from the branch routers and use HPR over IP to transport SNA traffic to and from VTAM. By using HPR over IP directly to VTAM, the customer eliminates any

potential looping problems that can occur in a bridged Ethernet environment. In addition, should a channel failure occur, IP immediately reroutes traffic and SNA sessions are not impacted. Finally, this design positions the customer to use a Gigabit Ethernet OSA-Express for SNA traffic.

Design Choices

This enterprise chose to keep the SNA data center router separate from the WAN distribution router to simplify change management and maximize availability. Two CIPs (one primary and one backup) run IP to handle all the SNA traffic, and six Cisco 7200 Series routers run DLSw+ (to handle a 1000-branch network), including one DLSw+ router used only for backup. Figure 6-10 shows the basic components of this design.

Figure 6-10 Combined SNASw and DLSw+ Design



DLSw+/SNASw Data Center Router Configuration

The following configuration is for the SNASw router named Coppito:

```
sh run
Building configuration...
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname COPPITO
!
ip subnet-zero
ip ftp source-interface TokenRing1/0
ip ftp username cse
ip ftp password csecse
no ip domain-lookup
ip host redclay2 172.18.125.3
!
lane client flush
cns event-service server
!
source-bridge ring-group 400
dlsw local-peer peer-id 10.10.10.99
dlsw remote-peer 0 tcp 10.10.10.1
!
interface FastEthernet0/0
 no ip address
 shutdown
 half-duplex
!
interface TokenRing1/0
 ip address 10.17.1.67 255.255.255.0
 ring-speed 16
!
interface TokenRing1/1
 no ip address
 shutdown
 ring-speed 16
!
interface TokenRing1/2
 no ip address
 shutdown
 ring-speed 16
!
interface TokenRing1/3
 no ip address
 ring-speed 16
 source-bridge 100 1 400
!
interface FastEthernet3/0
 no ip address
 shutdown
 half-duplex
!
interface Ethernet5/0
 ip address 10.10.10.99 255.255.255.0
!
```

```

interface E
thernet5/1
  no ip address
  shutdown
!
interface Ethernet5/2
  no ip address
  shutdown
!
interface Ethernet5/3
  no ip address
  shutdown
!
interface Ethernet5/4
  no ip address
  shutdown
!
interface Ethernet5/5
  no ip address
  shutdown
!
interface Ethernet5/6
  no ip address
  shutdown
!
interface Ethernet5/7
  no ip address
  shutdown
!
snasw pdlog exception file ftp://172.18.125.3/snaswpd1.log
snasw dlctrace file ftp://172.18.125.3/dlctrace1.log
snasw cpname NETA.COPPITO
snasw dlns NETA.MVSD
snasw port HPRIP TokenRing1/3 vname NETA.EEJEB
snasw port DOWNST vdlc 400 mac 4000.eeee.0000 sap 0x08 conntype nohpr
snasw link TOMVSD port HPRIP ip-dest 172.18.51.1
!
ip classless
ip route 172.18.125.3 255.255.255.255 10.17.1.1
no ip http server
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
line vty 0 4
!
end

```

IP Channel-Attached Router Configuration

```
CISCO.NETMD.VTAMLST(XCAEEJEB)
```

```
-----  
EEXCAJ VBUILD TYPE=XCA  
EETGJ PORT MEDIUM=HPRIP, X  
VNNAME=EEJEB, X  
VNGROUP=EEGRPJ, X  
LIVTIME=15, X  
SRQTIME=15, X  
SRQRETRY=9, X  
SAPADDR=04  
*  
EEGRPJ GROUP ANSWER=ON, X  
AUTOGEN=(64,L,P), X  
CALL=INOUT, X  
DIAL=YES, X  
DYNPU=YES, X  
DYNPUPFX=$E, X  
ISTATUS=ACTIVE
```

```
CISCO.NETMD.VTAMLST(EETGJEB)
```

```
-----  
EETGJEBV VBUILD TYPE=TRL  
EETGJEB TRLE LNCTL=MPC,MAXBFRU=16, X  
  
READ=(4F92), X  
  
WRITE=(4F93)
```

```
-----  
PROFILE.TCPIP
```

```
DEVICE IUTSAMEH MPCPTP AUTORESTART  
LINK samehlnk MPCPTP IUTSAMEH  
;  
DEVICE EETGJEB MPCPTP  
LINK EELINK2 MPCPTP EETGJEB  
;  
DEVICE VIPADEV2 VIRT 0  
LINK VIPALNK2 VIRT 0 VIPADEV2  
;  
HOME  
172.18.1.43 EELINK2 ; This corresponds to the host-ip-addr for the CIPRouter tg  
command  
172.18.1.41 VIPALNK2 ; This corresponds to the ip-dest specified in the SNASW router  
link command  
GATEWAY  
172.18 = EELINK2 4468 0.0.255.248 0.0.1.40  
172.18 172.18.1.42 EELINK2 4468 0.0.255.0 0.0.49.0  
;  
START IUTSAMEH  
START EETGJEB
```

```
-----  
VIEW CISCO.NETMD.VTAMLST(SNASWCP) - 01.02 Columns 00001 00072  
***** ***** Top of Data *****  
==MSG> -Warning- The UNDO command is not available until you change  
==MSG> your edit profile using the command RECOVERY ON.
```

```

000001 *          SNASWITCH CONTROL POINT
000002          VBUILD TYPE=SWNET
000003 *
000004 R7507PU  PU      ADDR=01,ANS=CONTINUE,DISCNT=NO,          X
000005          PUTYPE=2, ISTATUS=ACTIVE,          X
000006          NETID=NETA, CPCP=YES, CONNTYPE=APPN, CPNAME=SNASW, HPR=YES
000007
***** ***** Bottom of Data *****

```

```

-----
VIEW          CISCO.NETMD.VTAMLST(SNASWPUS) - 01.02          Columns 00001 00072
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG>          your edit profile using the command RECOVERY ON.
000001 *          SNASWITCH DOWNSTREAM PU
000002          VBUILD TYPE=SWNET
000003 *
000004 DSPU02  PU      ADDR=01,ANS=CONTINUE,DISCNT=NO,          X
000005          PUTYPE=2, ISTATUS=ACTIVE,          X
000006          DLOGMOD=D4C32782, MODETAB=ISTINCLM, USSTAB=USSTCPMF,  X
000007          IDBLK=022, IDNUM=01002          X
000008 DSPU02LU LU    LOCADDR=02
***** ***** Bottom of Data *****

```

Scenario 5—Migrating to SNASw only

In this case study, the enterprise demands the highest availability for its SNA applications.

Reasons for Change

The customer has invested a great deal in developing SNA LU 6.2 applications over the years and wants to continue to leverage that investment. The customer has been running separate networks for SNA and IP and has decided to consolidate using SNASw with HPR over IP. The network is already at the latest operating system level and is running APPN in VTAM.

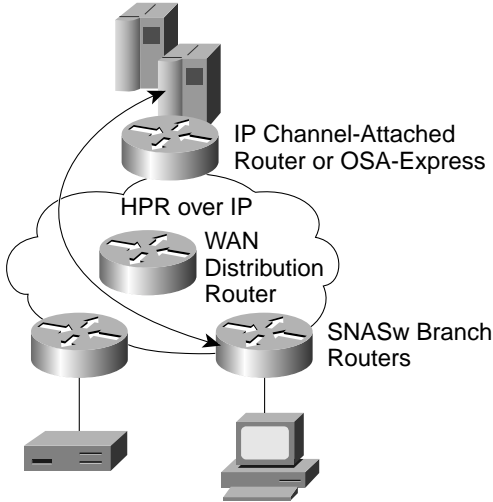
The OSA-Express Gigabit Ethernet card is for TCP/IP environments only. This card supports SNA traffic when SNA is encapsulated in IP using the EE support in OS/390 Version 2, Release 7 or higher.

Design Choices

The customer has 200 regional offices that will run SNASw. From the branch into the S/390, the SNA traffic is transported in IP. Hence, there is no need for SNA routers in the data center. The customer leverages the Cisco IOS QoS features to ensure that the interactive SNA and Telnet traffic take precedence over SNA batch and FTP traffic. Figure 6-11 shows this design.



Figure 6-11 SNASw Design



SNASw Branch Router Configuration

```
Current configuration:
!
version 12.0

hostname SNASW
!
boot system flash slot0:rsp-a3jsv-mz.120-5.XN
enable password lab
!

ip subnet-zero

!
source-bridge ring-group 100
!
interface Ethernet0/0/0
 ip address 172.18.49.37 255.255.255.128
 no ip directed-broadcast
 no ip route-cache distributed
!
interface TokenRing2/0/2
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 ring-speed 16
 source-bridge 200 1 100
 source-bridge spanning

interface Virtual-TokenRing2

description this interface is used to connect in the downstream PU

mac-address 4000.eeee.0000
 no ip address
 no ip directed-broadcast
 ring-speed 16
 source-bridge 222 1 100
 source-bridge spanning

snasw cpname NETA hostname
snasw port HPRIP hpr-ip Ethernet0/0/0 vname NETMD.EEJEB
snasw port VTOK2 Virtual-TokenRing2 vname NETMD.EEJEB
snasw link HPRMVSD port HPRIP ip-dest 172.18.1.41

router eigrp 109
 network 172.18.0.0
 no auto-summary
!

ip classless

line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end

SNASW#
```

IP Channel-Attached Router Configuration

```
Current configuration:
!
version 12.0

hostname CIPRouter
!
enable password lab
!
microcode CIP flash slot0:cip216-30
microcode reload
ip subnet-zero

source-bridge ring-group 80

interface Ethernet0/0
 ip address 172.18.49.17 255.255.255.128
 no ip directed-broadcast
 no ip mroute-cache

interface Channell1/0
 no ip address
 no ip directed-broadcast
 no keepalive
!
interface Channell1/1
 no ip address
 no ip directed-broadcast
 no keepalive
 cmpc E160 92 EETGJEB READ
 cmpc E160 93 EETGJEB WRITE
!
interface Channell1/2
 ip address 172.18.1.42 255.255.255.248
 no ip directed-broadcast
 no ip mroute-cache
 no keepalive
 lan TokenRing 0
 source-bridge 70 1 80
 adapter 0 4000.dddd.aaaa
 tg EETGJEB ip 172.18.1.43 172.18.1.42

router eigrp 109
 network 172.18.0.0
 no auto-summary
!
ip classless
ip route 172.18.1.41 255.255.255.255 172.18.1.43

!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0
 exec-timeout 0 0
 password lab
 login
 length 75
```

```
width 114
line vty 1 4
  exec-timeout 0 0
  password lab
  login
!
end

CIPRouter#
```

Host Definitions

```
CISCO.NETMD.VTAMLST(XCAEEJEB)
```

```
-----  
EEXCAJ VBUILD TYPE=XCA  
EETGJ PORT MEDIUM=HPRIP, X  
VNNAME=EEJEB, X  
VNGROUP=EEGRPJ, X  
LIVTIME=15, X  
SRQTIME=15, X  
SRQRETRY=9, X  
SAPADDR=04  
*  
EEGRPJ GROUP ANSWER=ON, X  
AUTOGEN=(64,L,P), X  
CALL=INOUT, X  
DIAL=YES, X  
DYNPU=YES, X  
DYNPUPFX=$E, X  
ISTATUS=ACTIVE
```

```
CISCO.NETMD.VTAMLST(EETGJEB)
```

```
-----  
EETGJEBV VBUILD TYPE=TRL  
EETGJEB TRLE LNCTL=MPC,MAXBFRU=16, X  
  
READ=(4F92), X  
  
WRITE=(4F93)
```

```
PROFILE.TCPIP  
DEVICE IUTSAMEH MPCPTP AUTORESTART  
LINK samehlnk MPCPTP IUTSAMEH  
;  
DEVICE EETGJEB MPCPTP  
LINK EELINK2 MPCPTP EETGJEB  
;  
DEVICE VIPADEV2 VIRT 0  
LINK VIPALNK2 VIRT 0 VIPADEV2  
;  
HOME  
172.18.1.43 EELINK2 ; This corresponds to the host-ip-addr for the CIPRouter tg  
command  
172.18.1.41 VIPALNK2 ; This corresponds to the ip-dest specified in the SNASW router  
link command  
GATEWAY  
172.18 = EELINK2 4468 0.0.255.248 0.0.1.40  
172.18 172.18.1.42 EELINK2 4468 0.0.255.0 0.0.49.0  
;  
START IUTSAMEH  
START EETGJEB
```

```
VIEW CISCO.NETMD.VTAMLST(SNASWCP) - 01.02 Columns 00001 00072  
***** ***** Top of Data *****  
==MSG> -Warning- The UNDO command is not available until you change  
==MSG> your edit profile using the command RECOVERY ON.  
000001 * SNASWITCH CONTROL POINT  
000002 VBUILD TYPE=SWNET
```

```

000003 *
000004 R7507PU  PU      ADDR=01,ANS=CONTINUE,DISCNT=NO,          X
000005          PUTYPE=2, ISTATUS=ACTIVE,                          X
000006          NETID=NETA,CPCP=YES,CONNTYPE=APPN,CPNAME=SNASW,HPR=YES
000007
***** ***** Bottom of Data *****

VIEW          CISCO.NETMD.VTAMLST(SNASWPUS) - 01.02          Columns 00001 00072
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG>          your edit profile using the command RECOVERY ON.
000001 *          SNASWITCH DOWNSTREAM PU
000002          VBUILD TYPE=SWNET
000003 *
000004 DSPU02  PU      ADDR=01,ANS=CONTINUE,DISCNT=          X
000005          PUTYPE=2, ISTATUS=ACTIVE,                          X
000006          DLOGMOD=D4C32782,MODETAB=ISTINCLM,USSTAB=USSTCPMF, X
000007          IDBLK=022,IDNUM=01002                              X
000008 DSPU02LU LU      LOCADDR=02
***** ***** Bottom of Data *****

```

Scenario 6—Migrating to TCP/IP across CLAW

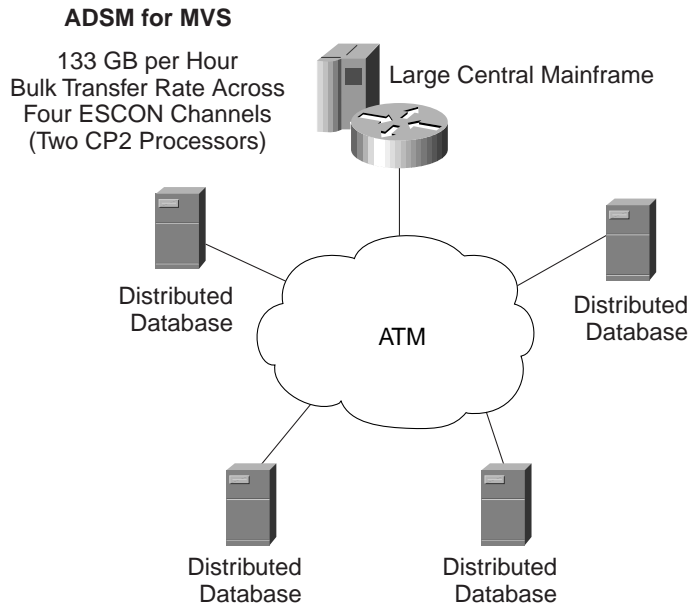
In this scenario, a customer wants to increase the reliability and robustness of the network by migrating to TCP/IP.

Reasons for Change

Many companies implement a client/server environment by using the database applications available on distributed UNIX or Windows NT servers. Companies also leverage the centralized nature of mainframes to back up this distributed data. IBM's backup product, Tivoli Storage Manager, previously known as ADSTAR Distributed Storage Manager (ADSM), is used to store large amounts of data from distributed platforms to a central mainframe resource (either direct access storage device [DASD] or tape).

Figure 6-12 shows the schematic for this scenario, in which four Sun servers are used for distributed database applications. Each night, the servers use Tivoli Storage Manager to transfer 250 GB data to the centralized mainframe for backup during a three-hour window.

Figure 6-12 Bulk Data Transfer from Distributed UNIX Servers to Central Mainframe



Testing of a CIP in IP Datagram mode determined that a single CIP processor can transfer 18.4 MBps across two ESCON channels. Therefore, two CIP processors can transfer 36.8 MBps. In one hour, the data center router can transfer 133 GB per hour:

$$36.8 \text{ MB per second} \times 60 \text{ seconds per minute} \times 60 \text{ minutes per hour} = 133 \text{ GB per hour}$$

Therefore, a Cisco 7507 with two CIP cards with dual ESCON interfaces (four ESCON channels) and two Asynchronous Transfer Mode (ATM) interface processors is capable of transferring 133 GB per hour. To determine the amount of time required to transfer the 250 GB of data in the bulk data transfer application example:

$$250 \text{ GB} / 133 \text{ GB per hour} = 1.88 \text{ hours, or } 112 \text{ minutes}$$

As these calculations demonstrate, the Cisco data center router can support the required data transfer rate.

Design Choices

The customer considered several factors before choosing the appropriate components to implement this solution. Although speed and cost were certainly important, the overriding concerns were robustness and reliability. For these reasons, the customer chose CLAW as the channel protocol, because it has been implemented in thousands of data centers and been in widespread use for more than five years.

If your OS/390 host environment supports the use of the Gigabit Ethernet OSA-Express, you should consider the use of OSA-Express with the Tivoli Storage Manager. This solution is optimized to provide very high throughput for bulk data transfer using Large Format Ethernet Frames (also known as Jumbo Frames) and can achieve data transfer rates approaching Gigabit Ethernet speed.

Router Configuration

For configuration examples, see www.cisco.com/warp/public/650/8.html.

Scenario 7—Migrating to TCP/IP across CMPC+

This scenario describes a customer who wants to redesign the OS/390-based data center. This customer wants to migrate from SNA to pure IP using CMPC+.

Reasons for Change

The network architecture group needed to redesign its OS/390-based data center to be the core of a fully enabled e-business and multiservice environment. They had been using CMCC technology for several years to connect both TCP/IP and SNA clients to the S/390s using CLAW channel protocol for the IP traffic and using CSNA for the SNA traffic.

The customer carefully considered and decided that the requirement for successfully moving forward was the ability to control QoS across all applications, from traditional SNA through voice over IP. The customer realized that achieving acceptable QoS would be impossible without removing the protocols that depend on OSI Layer 2 mechanisms for flow control, and that moving to a purely IP transport-based solution would be the best way to optimize positioning for the future.

Design Choices

To reach the goal of building an IP-based backbone network, the customer needed to find a way to transport significant amounts of SNA traffic without depending on the traditional Layer 2-based protocols. EE, which transports SNA data directly over IP, provided the answer. Because this group had extensive experience with CMCC technology, the decision was then largely a matter of deciding which of the IP-capable channel protocols to choose. They decided that CMPC+ provided the best balance of performance for the resulting mix of interactive, batch, and streaming traffic.

Router Configuration

For configuration examples, see www.cisco.com/warp/public/650/8.html.

CMPC+ with TCP/IP Stack Example

This example demonstrates the TCP/IP link for CMPC+ between a host and a Cisco router with a CMCC adapter. The following configuration is for the CIP in the Cisco 7500 Series router:

```
hostname ipclust1
!
microcode CIP flash slot0:cip27-0
microcode reload
!
interface Channel0/1
no ip address
no keepalive
cmpc 0170 00 TG00 READ
cmpc 0170 01 TG00 WRITE
!
interface Channel0/2
ip address 80.12.165.1 255.255.255.0
no ip redirects
no ip directed-broadcast
ip route-cache same-interface
no ip mroute-cache
load-interval 30
no keepalive

tg TG00      ip 80.12.165.2 80.12.165.1
```

In this configuration, the CMPC+ configuration is for the TCP/IP stack on the host. The host IP address of 80.12.165.2 in the transmission group statement corresponds to the IP address for the TCP/IP stack in the TCP/IP profile on the host. The IP address for the CIP is 80.12.165.2.

TCP/IP Profile

The following example shows the TCP/IP profile on the host:

```

ARPAGE 5
telnetparms timemark 600 port 23 dbcstransform endtelnetparms
ASSORTEDPARMS NOFWD ENDASSORTEDPARMS
;
DEVICE mpc4b00 MPCPTP
LINK MPCPLNK2 MPCPTP mpc4b00
;
AUTOLOG
  OEFTPE3
ENDAUTOLOG
INCLUDE TODD.MPCP.TCPIP.PROFILES(PORTS)
HOME
  80.12.165.2 MPCPLNK2
GATEWAY
; NETWORK      FIRST      DRIVER      PACKET      SUBNet mask      subnet value
;              HOP              SIZE
  80.12.165.1  =      mpcplnk2 4468host
DEFAULTNET 80.12.165.1 mpcplnk244680
BEGINVTAM
  ; Define logon mode tables to be the defaults shipped with the latest
  ; level of VTAM
  3278-3-E NSX32703 ; 32 line screen - default of NSX32702 is 24 line screen
  3279-3-E NSX32703 ; 32 line screen - default of NSX32702 is 24 line screen
  3278-4-E NSX32704 ; 48 line screen - default of NSX32702 is 24 line screen
  3279-4-E NSX32704 ; 48 line screen - default of NSX32702 is 24 line screen
  3278-5-E NSX32705 ; 132 column screen - default of NSX32702 is 80 columns
  3279-5-E NSX32705 ; 132 column screen - default of NSX32702 is 80 columns
  ; Define the LUs to be used for general users
  DEFAULTAPPL ECHOMVSE
; DEFAULTAPPL ECHOMVSE 10.10.1.188
; DEFAULTAPPL NETTMVSE
  DEFAULTTLUS
    TCPE0000..TCPE9999
  ENDDFAULTLUS
  ALLOWAPPL * ; Allow all applications that have not been previously
              ; specified to be accessed
ENDVTAM
DATASETPREFIX TODD.MPCP
start mpc4b00

```

In this TCP/IP profile, the DEVICE specifies the VTAM TRLE mpc4b00 and LINK specifies the link name (MPCPLNK2) associated with the IP address (80.12.165.2) for that link. The host IP address 80.12.165.2 that is specified for the transmission group in the router configuration must be identical to the IP address specified for the transmission group in the router configuration.

TRL Major Node Example

The following configuration shows the TRL major node example:

```
TRL4B00 VBUILD TYPE=TRL
MPC4B00 TRLE LNCTL=MPC,MAXBFRU=16,X
          READ=(4B00),X
          WRITE=(4B01)
```

In this TRL major node example, the parameter MPC4B00 must be identical to the LINK parameter in the TCP/IP profile.