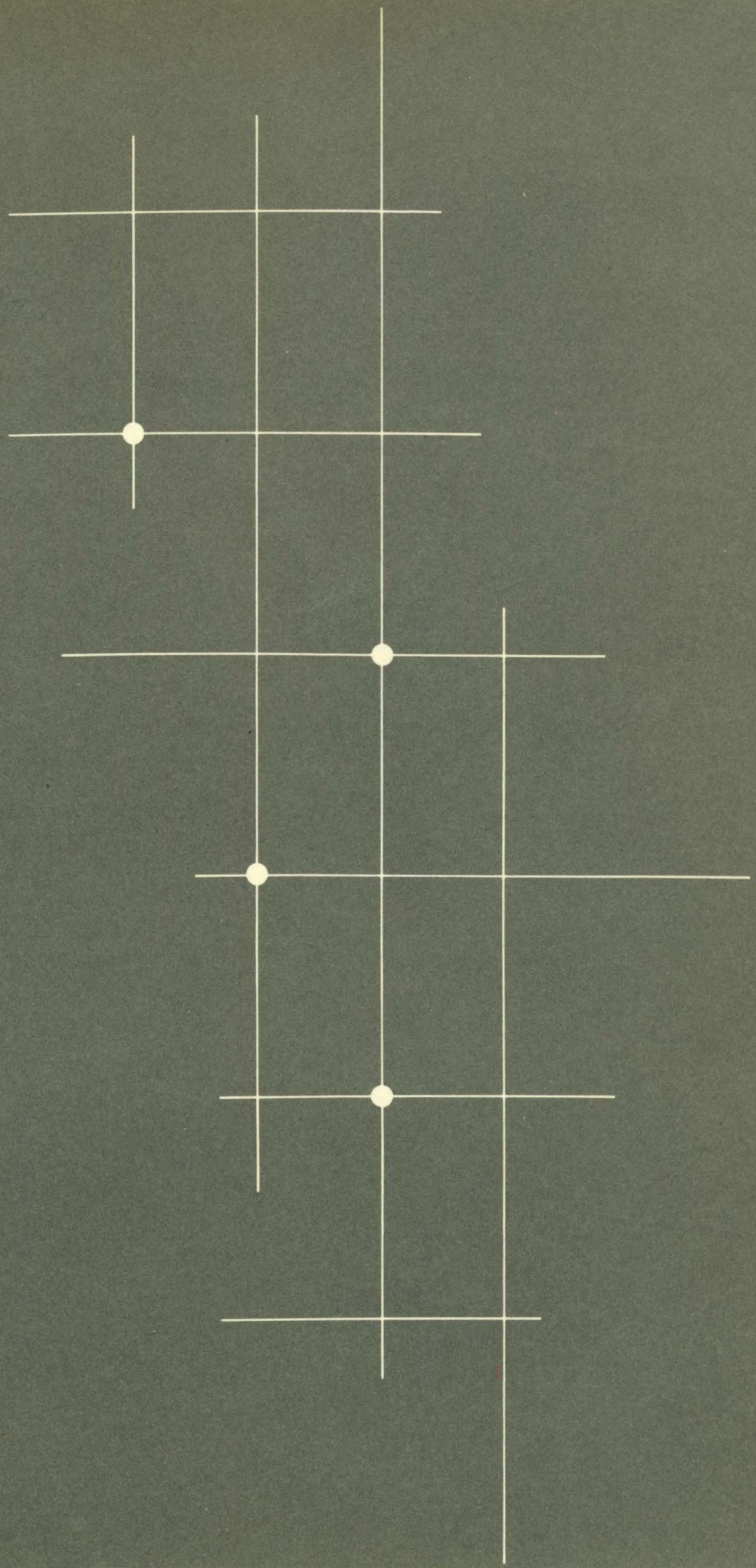
Systems Network Architecture



Format and Protocol Reference Manual: SNA Network Interconnection

IBM

SC30-3339-0

Systems Network Architecture

Format and Protocol Reference Manual: SNA Network Interconnection

FIRST EDITION (MARCH 1985)

Changes are continually made to the information in IBM systems publications. Before using this publication in connection with the operation of IBM systems, consult your IBM representative to find out which editions are applicable and current.

It is possible that this material may contain references to, or information about, IBM products (machines and programs) or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products or services in your country.

Publications are not stocked at the address given below; requests for IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for reader's comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Advanced Networking Architecture, Department E95, P.O. Box 12195, Research Triangle Park, North Carolina 27709, U.S.A. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation whatever. You may, of course, continue to use the information you supply.

PREFACE

This book is a supplement to SNA Format and Protocol Reference Manual: Architecture Logic (SC30-3112). It describes SNA network interconnection, also called gateway services.

The body of the book gives an overview of gateway services, defining terms, showing examples of interconnected network configurations, describing SSCP session services in support of network interconnection, and showing the role played by the gateway function component within an SNA node.

Appendix E gives request-response unit (RU) formats used for SNA network interconnection. This appendix contains a subset of the RUs shown in the SNA Reference Summary (GA27-3136), namely the RUs mentioned in this book.

Appendix G includes sense data used for SNA network interconnection.

Appendix N describes the notation used in the book.

Abbreviations commonly used in the text are listed on foldout pages at the back of the book (Appendix T) for easy reference.

For an introduction to the design concepts of SNA network interconnection, see "Interconnecting SNA Networks," IBM Systems Journal, Vol. 22., No. 4., pp. 344-366, 1983 (which can be ordered through IBM branch offices using IBM Order No. G321-5199).

CONTENTS

LIST OF ILLUSTRATIONS

CHAPTER 1. SNA NETWORK INTERCONNECTION

INTRODUCTION

SNA network interconnection (SNI) allows independent networks to support cross-network end-user communication without giving up their autonomy. Each interconnected network has its own independent name space and address space, and is referred to as a subnetwork of a larger, multiple-address-space SNA network.

This book describes the cooperation required among SNA components in order to achieve SNA network interconnection, also known as gateway services.

Multiple networks may be interconnected serially, or with parallel gateways between a given pair of networks, or with several networks interconnected through the same gateway. These configurations are described in this book.

A major goal of SNI is to achieve network interconnection without any changes to components that are not specifically gateway capable. For example, from the point of view of an LU, the procedures for initiating, terminating, and using a session are the same whether the partner LU is in the same subnetwork or a different subnetwork. The following components are gateway capable, and are described in this book.

- The gateway SSCP—an SSCP with the special data base and facilities required to participate in cross-network session initiation and termination. This book assumes some familiarity with the SSCP session services functions as described in SNA Format and Protocol Reference Manual: Architecture Logic.
- The gateway function component—a component in a node on a subnetwork boundary that accepts message units from one subnetwork and transmits them to the appropriate destination in another subnetwork.
- The gateway PU—the PU in the same node as a gateway function component; the gateway PU receives RUs from a gateway SSCP concerning cross-network sessions.

  The gateway function component and the gateway PU are referred to collectively as the gateway node.

Another goal of SNI is to allow interconnected networks to be configured, defined, and managed independently. Gateway nodes and gateway SSCPs allow different networks to mask their physical and logical configurations from each other, primarily by offering the following services, which are described in this book:

- Address aliasing, allowing duplicate addresses and different subarea/element splits in the interconnected networks
- Name aliasing, allowing duplicate network names in interconnected networks
- Routing of session services RUs between SSCPs in different subnetworks of the composite network, minimizing the data about one subnetwork that is kept by SSCPs in other subnetworks. Thus, a configuration change in one subnetwork does not require changes in the routing tables or directory entries of all SSCPs in the interconnected subnetworks.

TERMS AND CONCEPTS

CROSS-NETWORK SESSION

A cross-network session crosses one or more subnetwork boundaries. It connects two LUs in different subnetworks or a gateway SSCP in one subnetwork to an SSCP in another subnetwork, where the second SSCP may or may not be a gateway SSCP.

DEFINITION OF GATEWAY

A gateway consists of the SNA components that participate in name transformation, network address transformation, and SSCP rerouting in order to allow the interconnection of two or more networks with independent name and address spaces. A gateway includes one gateway node and at least one gateway SSCP.

Several gateway SSCPs may support a single gateway node, i.e., send the gateway node PU RNAA and SETCV requests related to cross-network sessions. The maximum number of gateway SSCPs that may support a particular gateway node is less than or equal to the share limit for the gateway PU, since non-gateway SSCPs may also share control of a gateway PU.

For a single LU-LU session, a maximum of three gateway SSCPs per gateway can partition responsibility for name transformation and gateway node support. See "Gateway SSCP Functions" on page 1-30 for the rules governing the allocation of responsibilities among gateway SSCPs.

Although physically located in a single subnetwork, a gateway SSCP may participate in gateways spanning boundaries between different sets of subnetworks. The architecture does not determine the exact number and physical locations of gateway SSCPs involved in a gateway supporting an LU-LU session. However, different gateway configurations may affect the number of cross-network SSCP-SSCP sessions required and the information required in the tables of the different gateway SSCPs. "Configurations" on page 1-3 discusses some of these considerations.

NETWORK IDENTIFIERS

A network identifier uniquely identifies a subnetwork within a set of two or more interconnected subnetworks. A network identifier serves two purposes:

- The network identifier identifies the address space associated with an address in RUs exchanged by gateway components.
- The network identifier identifies the name space associated with an SSCP name, LU name, class of service (COS) name, or mode name.

A network-ID-qualified name or address is always unique in the entire set of interconnected subnetworks.

VIRTUAL ROUTES

A cross-network session has a virtual route in each subnetwork through which its session traffic travels. These routes are disjoint. A gateway function component transfers session traffic between the two virtual routes terminating in its node, as described in "Gateway Function Component" on page 1-13.

LU ROLES IN SESSION INITIATION

The LUs that participate in session initiation are classified according to the following roles that they play. See SNA Format and Protocol Reference Manual: Architecture Logic for more information about these roles.

- The initiating LU (ILU) is the one that sends the INIT-SELF or INIT-OTHER RU.
- The terminating LU (TLU) is the one that sends the TERM-SELF or TERM-OTHER RU.
- The primary LU (PLU) is the one that sends the BIND RU.
- The secondary LU (SLU) is the one that receives the BIND RU.
- The origin LU (OLU) is the LU whose SSCP originates a CDINIT RU or CDTERM RU. It is either the primary or the secondary LU. For session initiation, this LU is either the ILU (if it sent INIT-SELF) or the LU named second in the INIT-OTHER (in which case, it may or may not be the ILU). Similarly, for session termination, this LU is either the TLU (if it sent TERM-SELF) or the LU named second in the TERM-OTHER (in which case, it may or may not be the TLU).
- The destination LU (DLU) is the one named in the TERM-SELF RU or named first in the TERM-OTHER RU. It is either the primary LU or the secondary LU.

CONFIGURATIONS

This section shows different configurations of interconnected subnetworks, first in terms of gateways, and then in terms of the gateway components comprising the gateways.

NETWORK CONFIGURATIONS

Multiple subnetworks can be interconnected both serially and in parallel. This section shows some of the basic configurations that can be combined to create a wide variety of multiple-network configurations. Different configurations have different performance, reliability, and cost characteristics.

In the simplest case, two subnetworks are interconnected using a single gateway, as shown in Figure 1-1.

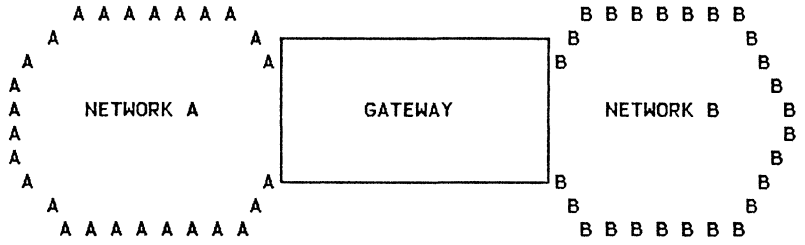


Figure 1-1. One Gateway Connecting Two Networks

Two subnetworks can also be interconnected using multiple, parallel gateways, as shown in Figure 1-2.

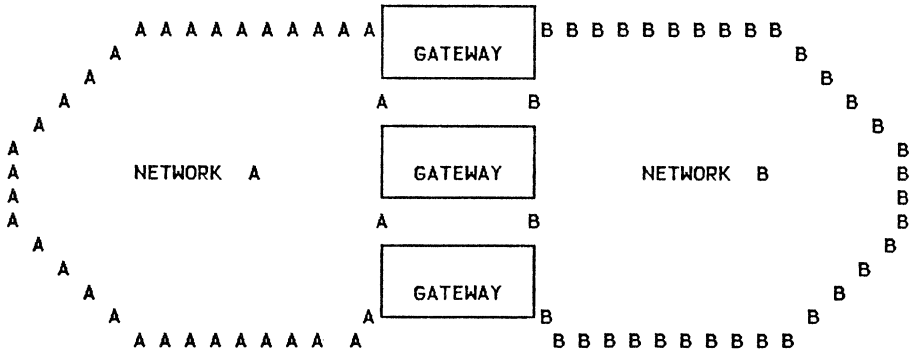


Figure 1-2. Parallel Gateways Connecting Two Networks

Three or more subnetworks can also be interconnected using one or more gateways. Figure 1-3 shows three subnetworks interconnected using a single gateway.

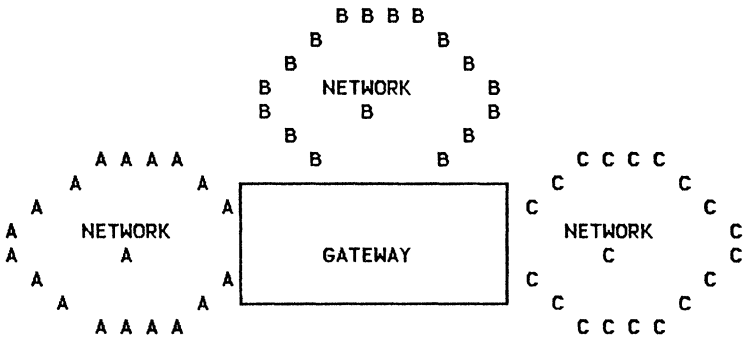


Figure 1-3. One Gateway Connecting Three Networks

Multiple subnetworks can be interconnected by tandem gateways, as shown in Figure 1-4. Thus two networks may access one another via one or more intermediate subnetworks. In the figure, LUs in subnetworks A and C can have sessions through subnetwork B.

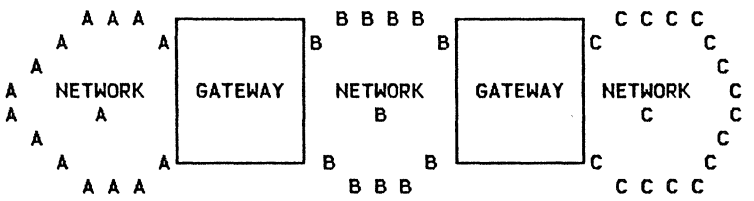


Figure 1-4. Tandem Gateways Connecting Three Networks

CONFIGURATIONS OF GATEWAY COMPONENTS

The figures in this section show the gateway components that participate in the gateway configurations shown above. They also show the sessions involved in the initiation of a single cross-network LU-LU session.

Figure 1-5 shows the minimum set of gateway components involved in the simple one-gateway configuration illustrated in Figure 1-1 on page 1-3.

This configuration requires only one of the subnetworks to contain a gateway SSCP. Every SSCP in subnetwork B that participates in cross-network session initiation must have a session with the gateway SSCP in subnetwork A. From the point of view of the SSCPs in subnetwork B, all LUs in subnetwork A appear to be in the domain of the gateway SSCP; they also appear to be in the subarea of the gateway node.

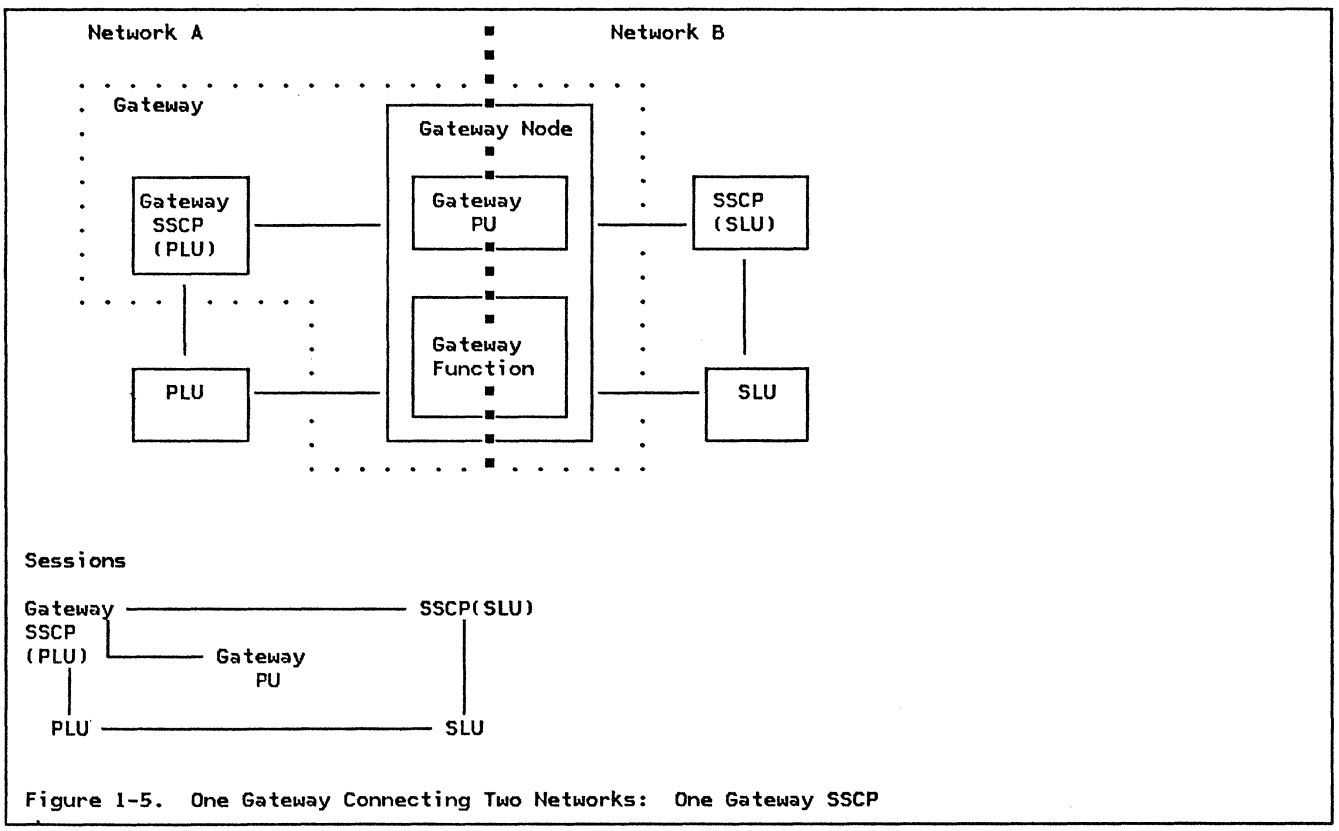


Figure 1-5. One Gateway Connecting Two Networks: One Gateway SSCP

Figure 1-6 shows a slightly more complex example of the simple one-gateway configuration, with a second gateway SSCP added in the second subnetwork. It offers the benefits of simplified cross-network forwarding of RUs by SSCPs: only one SSCP-SSCP cross-network session is required. In addition, name aliasing functions (see "Name Aliasing and Transformation" on page 1-19) may be coordinated so that the required tables can be partitioned between the two gateway SSCPs.

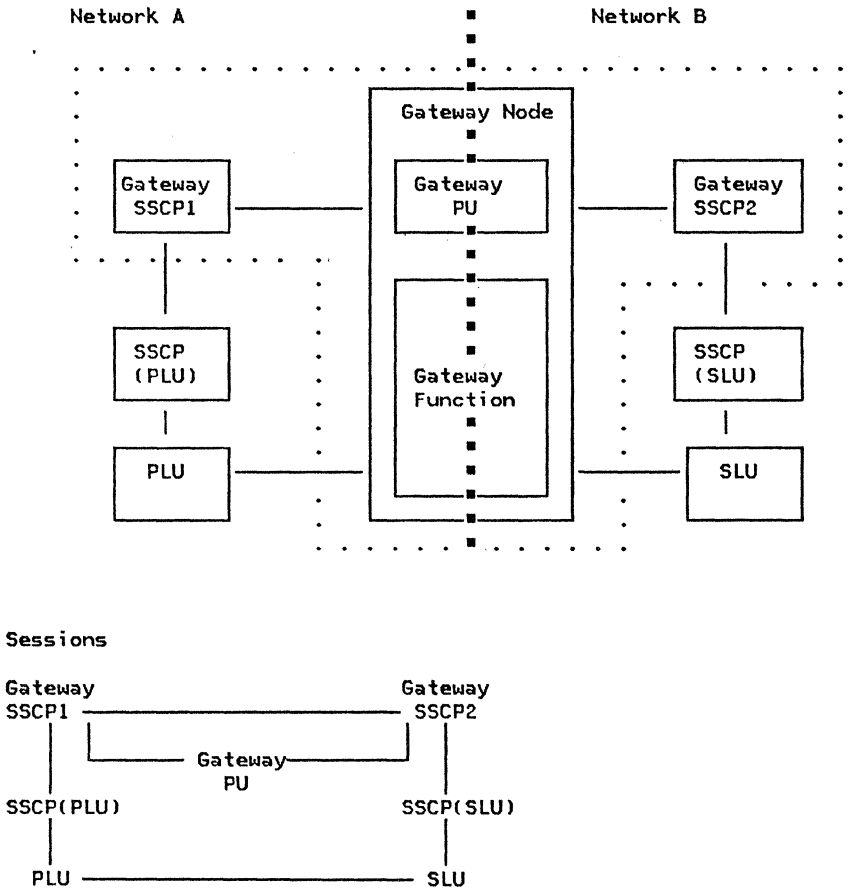
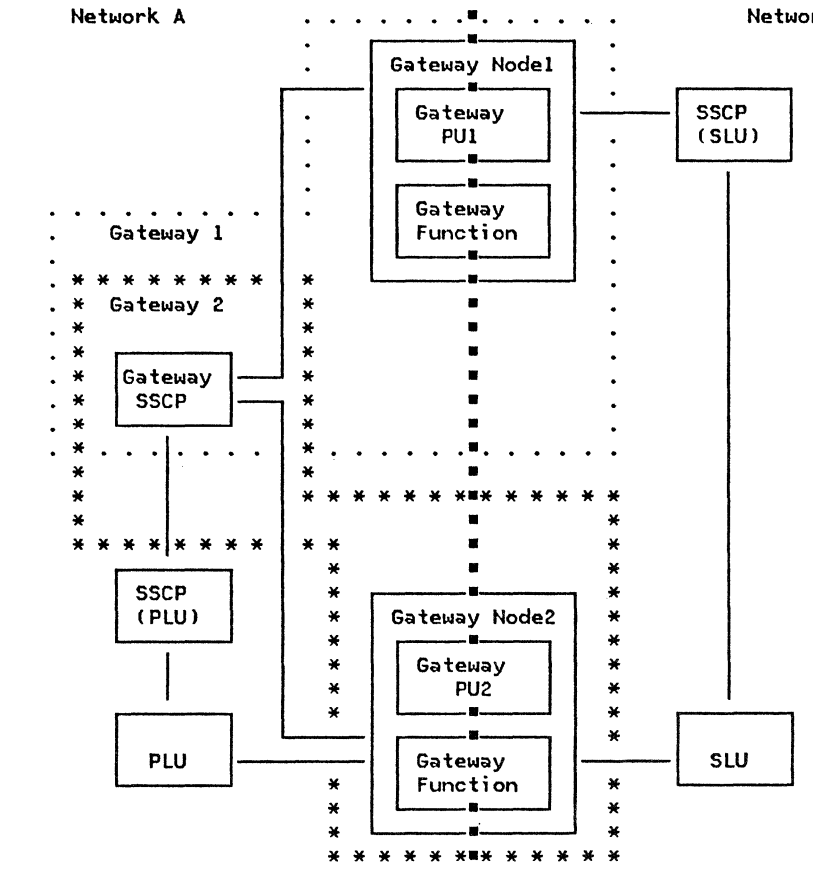


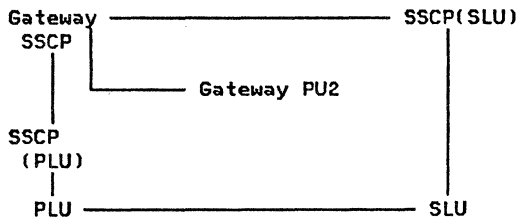
Figure 1-6. One Gateway Connecting Two Networks: Two Gateway SSCPs

Figure 1-7 shows an example of the parallel-gateway configuration shown in Figure 1-2 on page 1-3, in which the same gateway SSCP belongs to both gateways. The cross-network LU-LU session is not constrained to pass through the same gateway node as the cross-network SSCP-SSCP session involved in its initiation. In the figure, the cross-network SSCP-SSCP session crosses the subnetwork boundary through gateway 1, while the LU-LU session crosses it through gateway 2.

Providing parallel gateways increases the number of cross-network sessions that may be established and provides a backup path for cross-network sessions if one of the gateway nodes becomes inoperative.



Sessions



Note: Gateway PU1 is not shown in the session diagram because it does not participate in the setup of the LU-LU session.

Figure 1-7. Parallel Gateways Connecting Two Networks: One Gateway SSCP

Figure 1-8 shows a set of gateway components constituting the configuration illustrated in Figure 1-3 on page 1-4. Only one subnetwork is required to have a gateway SSCP. In this example, all three subnetworks have their own gateway SSCPs, which share gateway node support responsibilities for a given session.

Typically, no more than two gateway SSCPs in a given gateway are involved in any given session. However, a third gateway SSCP is allowed to serve as an intermediary between two entirely independent networks. For example, one network may provide several different networks with access to services provided by each other. Each network contracts with the single network, which controls the establishment of cross-network sessions between any pair of networks.

Three is the maximum number of gateway SSCPs per gateway that may be involved in the initiation of a particular session.

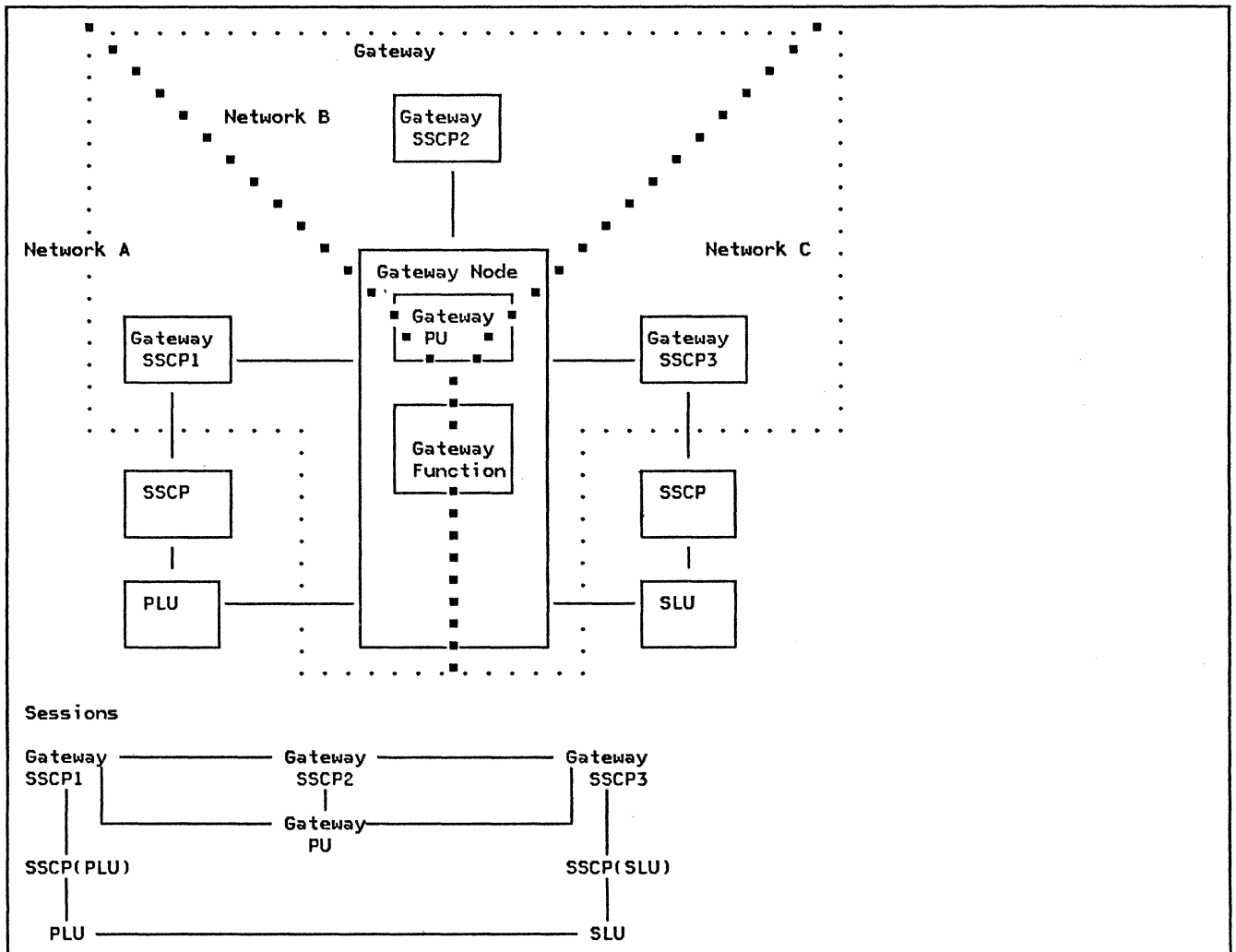


Figure 1-8. One Gateway Connecting Three Networks: Three Gateway SSCPs

A gateway SSCP may be involved in tandem gateways connecting three subnetworks. Figure 1-9 and Figure 1-10 on page 1-10 show two examples of the tandem gateway configuration shown in Figure 1-4 on page 1-4.

In Figure 1-9, the only gateway SSCP is in the intermediate subnetwork. This gateway SSCP is involved in two gateways that connect different subnetworks; it supports both gateway nodes involved in the session.

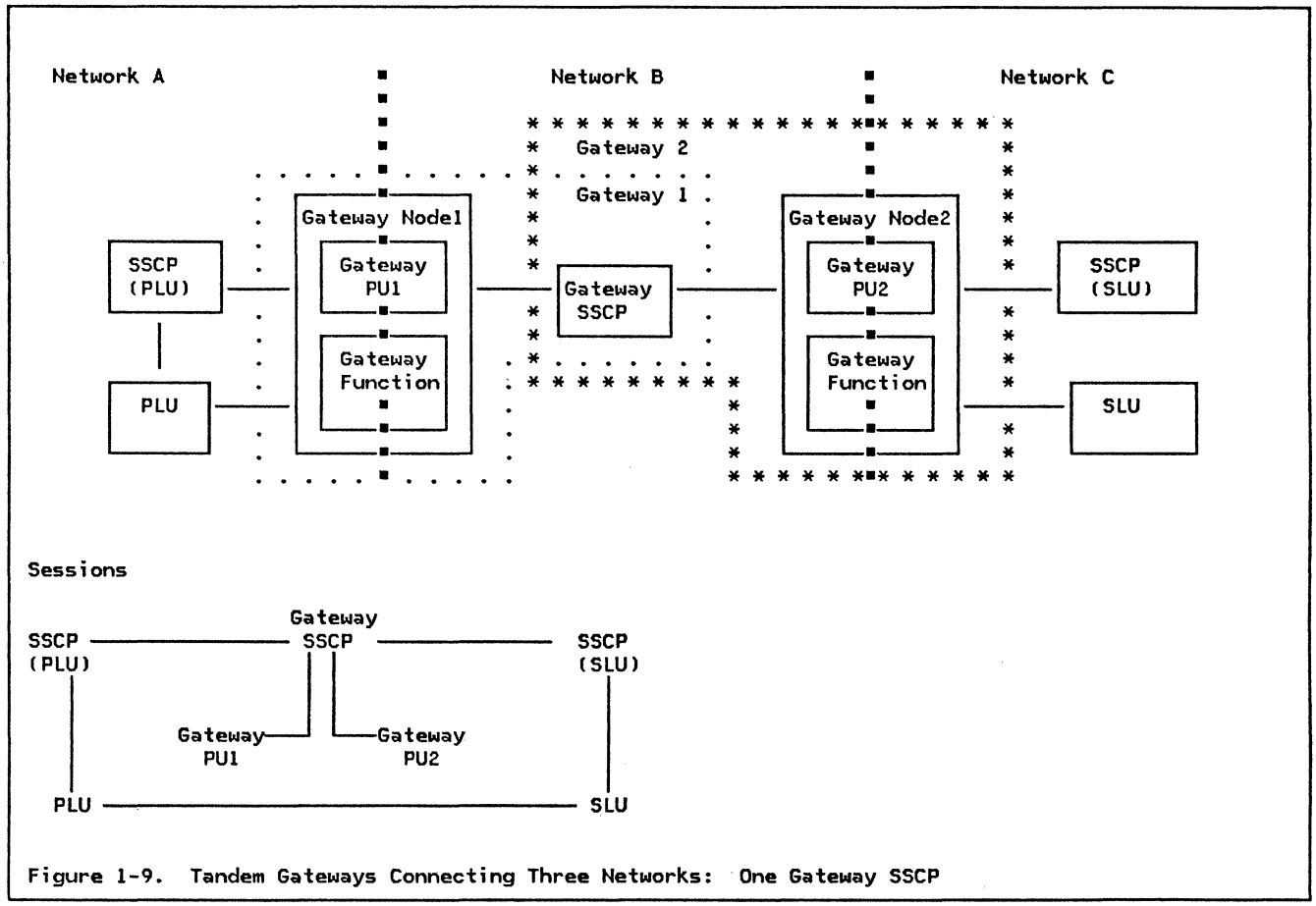


Figure 1-9. Tandem Gateways Connecting Three Networks: One Gateway SSCP

In Figure 1-10, the intermediate subnetwork B has no LUs or gateway SSCPs; it consists entirely of links between the two gateway nodes. This configuration provides the maximum isolation between subnetworks A and C, since neither gateway SSCP has a session with the gateway node on the subnetwork boundary of the other.

In an active gateway, the gateway PU has an active session with at least one gateway SSCP in one of the subnetworks connected in the gateway. Hence, this figure illustrates the greatest separation possible between two gateway SSCPs that share a session: two gateway nodes between them.

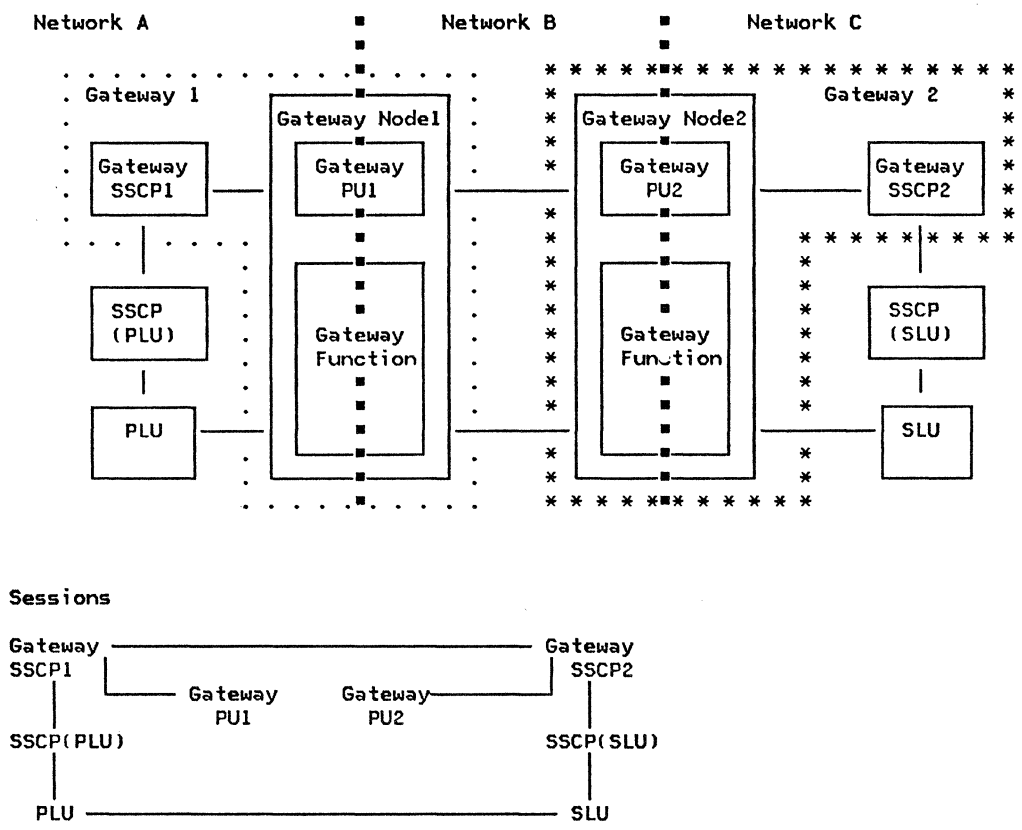


Figure 1-10. Tandem Gateways Connecting Three Networks: Two Gateway SSCPs

GATEWAY-CAPABLE COMPONENTS

GATEWAY SSCP

A gateway SSCP is an SSCP that is able to support gateway PUs, to reroute session services RUs between SSCPs in separate subnetworks, and to make the appropriate name and address transformations within these requests, as described in "Address Aliasing and Transformation" on page 1-16 and "Name Aliasing and Transformation" on page 1-19.

An SSCP that is able to be a gateway SSCP may or may not participate in a gateway for a particular LU-LU session. If so, it reroutes session services RUs across subnetwork boundaries and participates in the control of gateway nodes involved in the session. If not, it behaves as if it were a non-gateway SSCP, sending session services RUs to another gateway SSCP in its subnetwork for rerouting.

A gateway SSCP belonging to multiple parallel gateways may select the gateway node to be used by a particular LU-LU session to cross a subnetwork boundary, since the LU-LU session is not constrained to use the same gateway node as the SSCP-SSCP session.

To a non-gateway SSCP, all LUs in other networks appear to be in the domain of an SSCP session partner (a gateway SSCP), which appears to be in the same subnetwork, whether or not the connecting session is a cross-network session.

Summary of Cross-Network Session Services

Session initiation and termination for an LU-LU session are mediated by one or more SSCPs. If the two LUs are in the same domain, only one SSCP is involved. If the two LUs are in different domains, two SSCPs are involved, exchanging cross-domain session services RUs. For cross-network LU-LU sessions, two or more SSCPs are involved, including at least one gateway SSCP. If multiple SSCPs are involved, they appear to an LU as a single, composite SSCP. For example, a composite SSCP includes the SSCP of the OLU, the SSCP of the DLU, and all the gateway SSCPs that route session services RUs between them (see "SSCP Rerouting" on page 1-23).

Figure 1-11 illustrates this principle. If the OLU and the DLU belong to the same domain, steps 2, 4, 8, and 9 are unnecessary. This figure is a simplification of the flows shown in Figure 1-32 on page 1-37 and Figure 1-34 on page 1-39, deleting responses and showing only flows between SSCPS and other SSCPs or LUs.

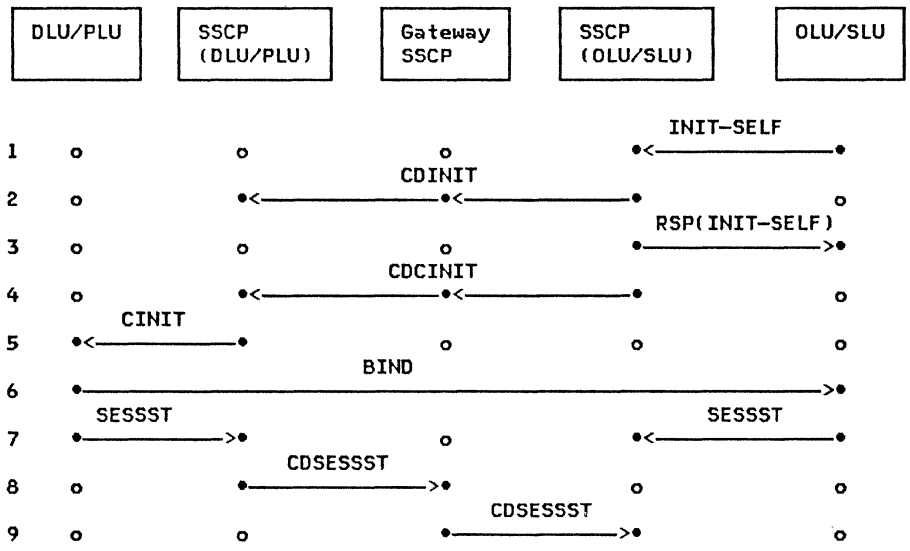


Figure 1-11. Cross-Network LU-LU Session Activation with Multiple SSCPs: A response is not shown if it immediately follows the corresponding request.

Predesignated Gateway SSCP

It is an installation option to predesignate one gateway SSCP to have sole responsibility for control of the gateway node. The functions of the predesignated gateway SSCP are described in "Gateway SSCP Functions" on page 1-30.

For example, gateway SSCP2 in subnetwork B in Figure 1-8 on page 1-8 may be predesignated because the installation requires it to have sole control of the gateway node.

An SSCP notifies its session partner gateway SSCPs in the CDINIT request or response that it is predesignated to control a common gateway node.

Only one gateway SSCP in a gateway may be predesignated. If three gateway SSCPs serve a single session, only the middle one in the session setup path (see "SSCP Rerouting" on page 1-23) may be predesignated.

GATEWAY NODE

A gateway node interconnects two or more subnetworks. It has the following characteristics:

- It contains two or more subarea path controls, each associated with a particular subnetwork. Each subarea path control can perform normal intermediate routing within its subnetwork.
- It contains a gateway function component that interconnects pairs of subarea path controls for cross-network sessions.
- The gateway PU has a network address in each interconnected subnetwork.
- The gateway PU can process gateway RNAA and SETCV RUs from a gateway SSCP.

Native Network

Although the PU in a gateway node may have SSCP-PU sessions with SSCPs in more than one subnetwork, only the SSCPs in one subnetwork can control the subsidiary resources of the PU, such as links and LUs. This subnetwork is called the native network of the gateway node. For example, only the SSCPs in the native network can have SSCP-LU sessions with the LUs in the gateway node or with the LUs in peripheral nodes attached to the gateway node.

Gateway PU

A gateway PU is distinguished by its ability to handle the gateway-related information in the RUs shown in Figure 1-12 on page 1-13. The figure shows the complete set of RUs required to establish the SSCP-PU session and to conduct gateway-related activities. These are the only RUs that may be exchanged by a gateway PU and a gateway SSCP that is not in its native network.

The following notes explain the gateway-related information carried in, or implied by each RU in the figure, where the notes correspond to the numbers in the figure. See Appendix E for the complete format of each RU.

1. The SSCP-PU Session Capability control vector (X'0B') on ACTPU informs the gateway PU of the gateway capability of the SSCP. In RSP(ACTPU), the PU indicates in control vector X'0B' whether it has the same gateway capabilities.
2. Pending-active or pending-reset cross-network LU-LU sessions that are being activated in cooperation with the sender of DACTPU will be reset by the gateway node.
3. To support cross-network route status reporting and testing, the gateway PU sends ROUTE-INOP and ER-TESTED and receives ROUTE-TEST for routes in any subnetwork connected by the gateway node. These three RUs include the network identifier for the referenced route. The gateway PU reports all inoperative routes (via ROUTE-INOPs) to the SSCPs that have requested such reporting in ACTPU control vector X'0B', whether or not they are gateway SSCPs.
4. A gateway SSCP and a gateway PU exchange RNAA and SETCV to set up the address transform for a cross-network session, as described in "Address Assignment Protocols" on page 1-17. A gateway SSCP also uses SETCV to send the gateway PU the LU name transform, as well as VR identifier lists used to request virtual routes in specified subnetworks.
5. A gateway SSCP sends NOTIFY(X'05') to inform the gateway PU that a session setup error condition has been detected, e.g., because the DLU is not available. As a result, the gateway node can free the resources allocated during the RNAA-SETCV sequence.
6. The gateway PU sends NOTIFY(X'05') to each gateway SSCP that has participated in the setup procedures for a session when it detects session activation or deactivation or has detected a session failure resulting from an inoperative route.
7. The gateway PU sends REQACTCDRM to a gateway SSCP after it receives an ACTCDRM request for which it has no established address transform. REQACTCDRM signals the gateway SSCP to initiate the cross-network SSCP-SSCP session with the sender of the unsuccessful ACTCDRM. For more information, see Figure 1-30 on page 1-35 and Figure 1-31 on page 1-36.

Two other RUs processed by PUs have been modified for SNA network interconnection: CONTACTED includes a network identifier for the contacted station. In NC_ER_TEST_REPLY, the ER Configuration control vector (X'1F') includes a network identifier.

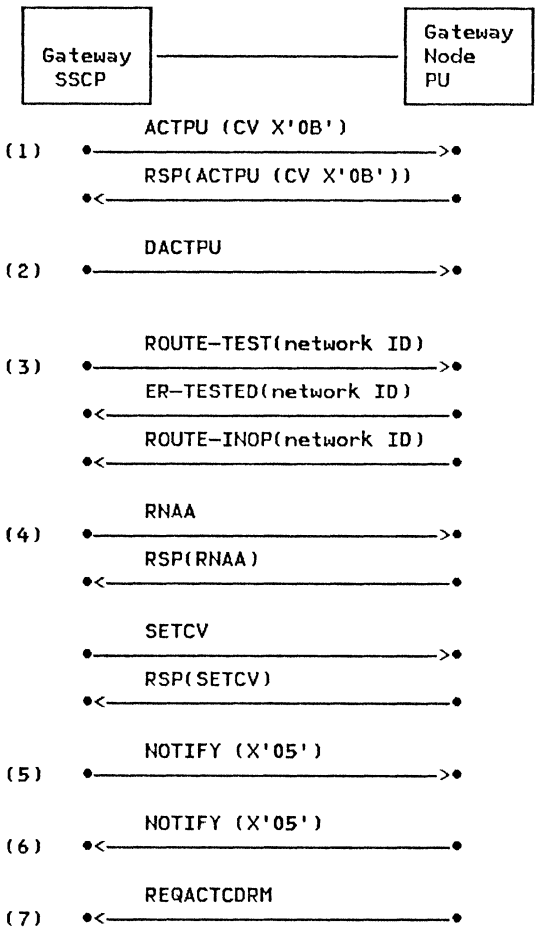


Figure 1-12. RUs Flowing between Gateway PUs and Gateway SSCPs

Gateway Function Component

Figure 1-13 on page 1-14 shows similarities between gateway function components and boundary function components (not otherwise described in detail in this book). Both include session connectors (SC) that interconnect pairs of path controls. A session connector transfers message units from one path control to another, allowing two NAUs to communicate even though they are represented in separate address spaces. As far as the two NAUs are concerned, a session connected through boundary function or gateway function is like any other session; the NAUs are not aware of the session connector interconnecting them.

As far as the two path controls are concerned, the session connector appears to be a half-session. The two path controls are associated with different address spaces, and thus know the session connector by different address pairs.

Thus, a boundary function session connector transfers message units between a subarea path control and a peripheral path control. The session connector has an address in a subarea address space and one in a peripheral address space. Boundary function allows SSCPs and LUs in a subarea routing network to communicate with LUs and PUs in peripheral nodes.

Similarly, a gateway function session connector transfers message units between independent subarea path controls. The session connector has two different subarea address pairs belonging to the two different subarea address spaces associated with the two subarea path controls. Gateway function allows SSCPs and LUs in one subnetwork to communicate with SSCPs and LUs in another subnetwork.

Figure 1-13 on page 1-14 also shows the session types supported by both boundary function and gateway function. Through boundary function, an SSCP can communicate with both LUs and PUs, while an LU can communicate with other LUs. Through gateway function, an SSCP can communicate only with other SSCPs, and an LU can communicate only with other LUs. Cross-network SSCP-LU or SSCP-PU sessions do not exist.

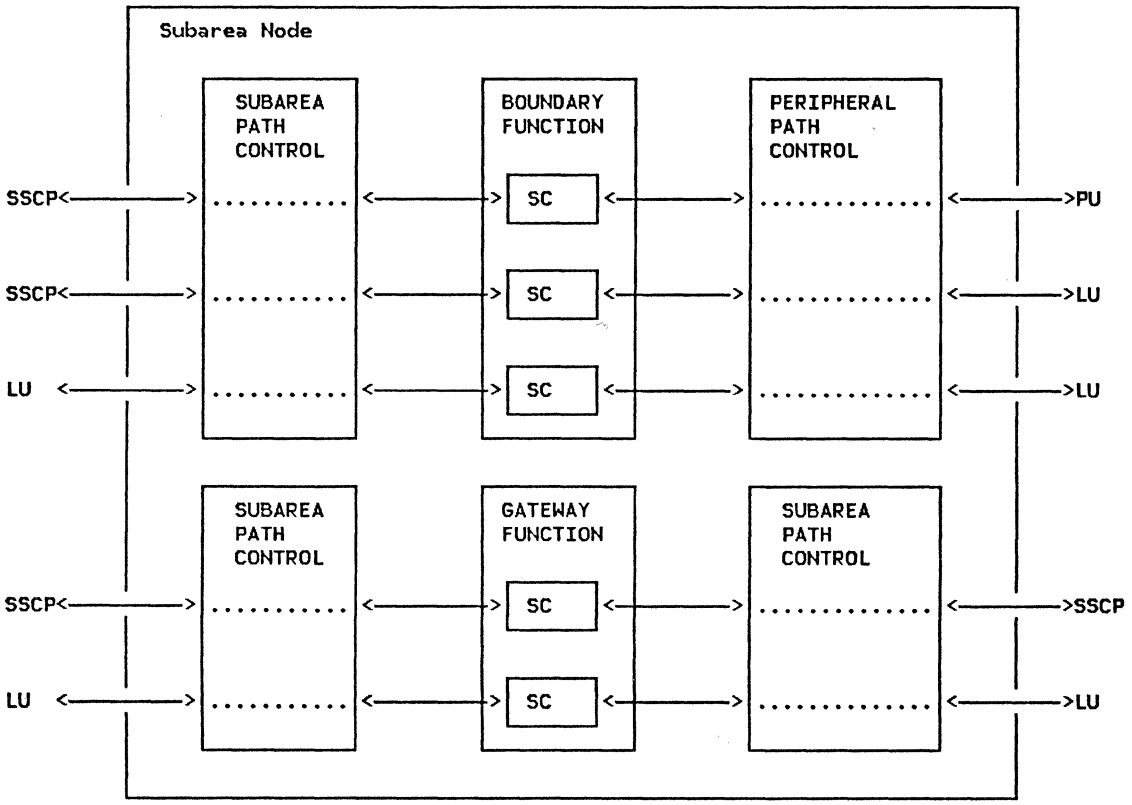


Figure 1-13. Gateway Function Compared to Boundary Function: One session connector (SC) exists for each session connected through a boundary function or gateway function.

Flow between Boundary Function and Gateway Function in the Same Node

In Figure 1-14, network A is the native network of the gateway node. All the peripheral nodes attached to it belong in this network.

Session traffic flowing from an LU in the peripheral node to an LU in network B follows the path described below through the gateway node:

- The peripheral path control delivers it to boundary function.
- Boundary function delivers it to the subarea path control for network A.
- This subarea path control delivers it to gateway function.
- Gateway function delivers it to the subarea path control for network B, which forwards it to the destination LU.

Session traffic flowing in the opposite direction takes the reverse path.

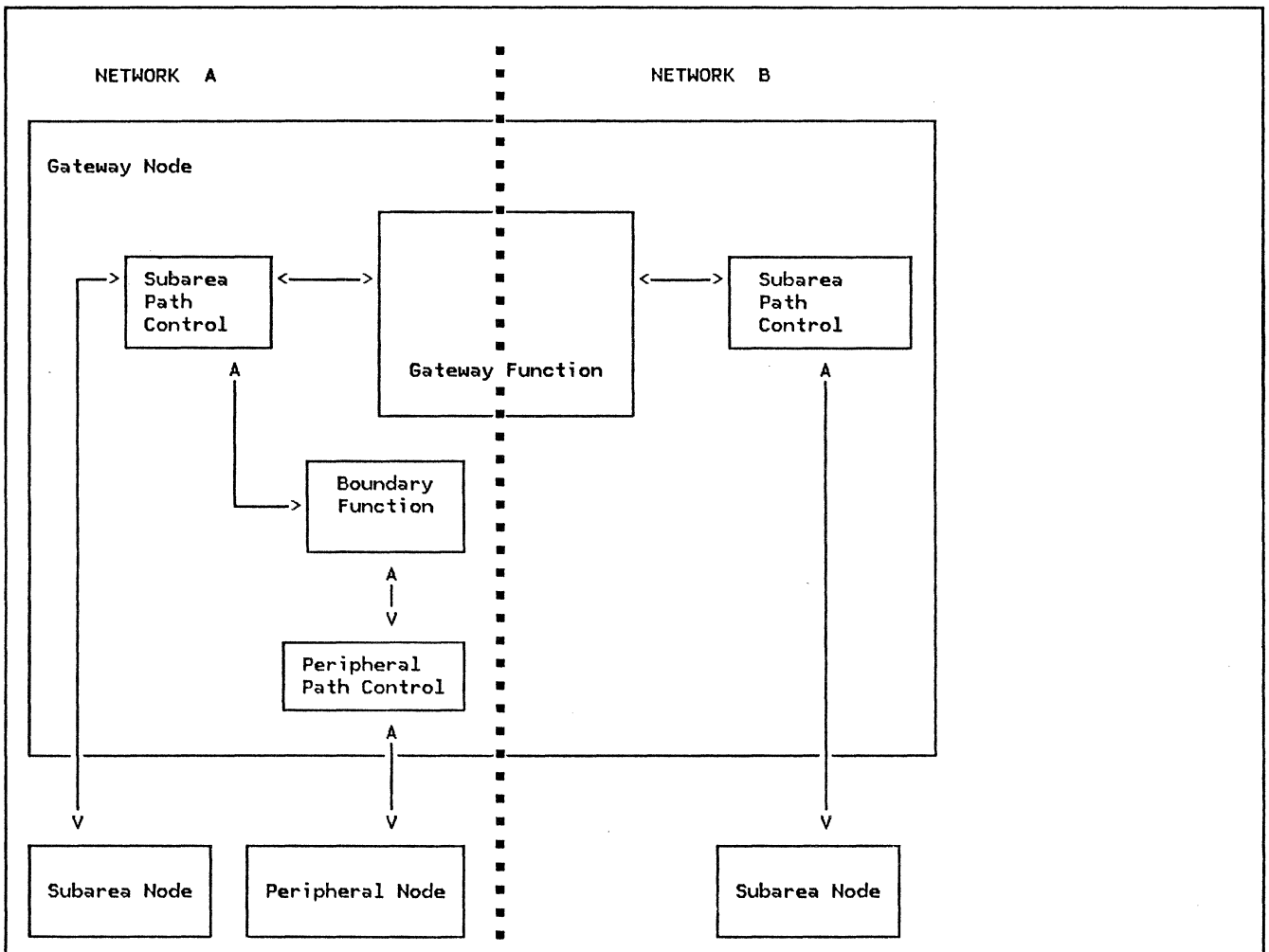


Figure 1-14. Flow between Gateway Function and Boundary Function

Structure of a Gateway Function Component

As shown in more detail in Figure 1-15, a gateway function component consists of one session connector for each cross-network session whose session traffic passes through that gateway node and a session manager.

The session manager manages cross-network session-activation and -deactivation protocols for the gateway node. It receives session-activation and -deactivation requests and responses from one subarea path control and retransmits them via another subarea path control; it also creates and destroys the associated session connectors. The session manager is comparable to the network services component (LNS) in the LU.

Each session connector interconnects two subarea path controls for a particular cross-network session. It receives session traffic from one subarea path control and retransmits it via the other. To the subarea path controls, the session connector appears to be a half-session. Each subarea path control associates the session connector with an address pair in its address space.

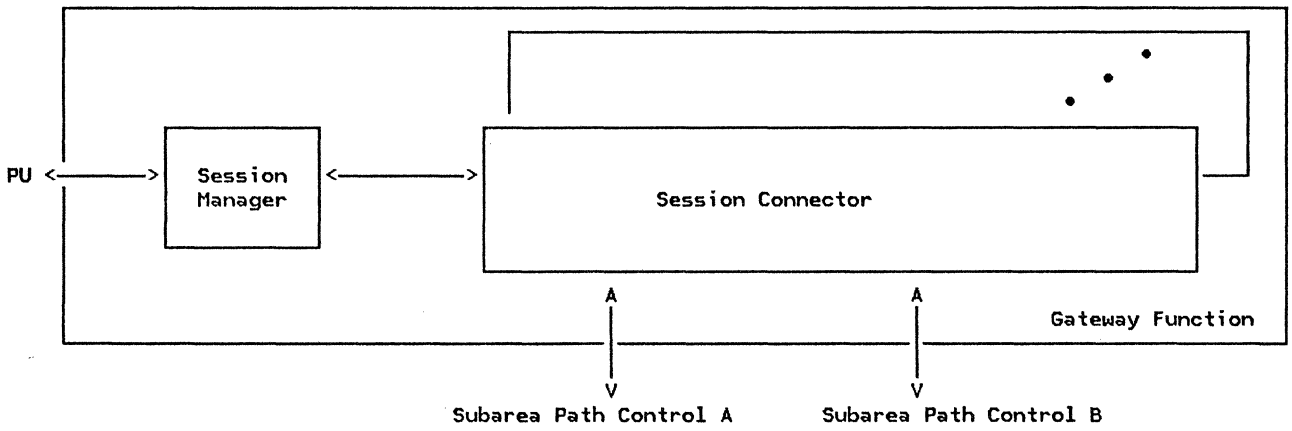


Figure 1-15. Structure of a Gateway Function Component

ADDRESS ALIASING AND TRANSFORMATION

To establish uniqueness of an address among interconnected subnetworks, the address is qualified by the network identifier. In the RUs they exchange, gateway SSCPs and gateway PUs use network-ID-qualified addresses to be unambiguous. However, path control and other NAUs within a subnetwork are not aware of other subnetworks and do not use network-ID-qualified addresses. The purpose of address aliasing is to avoid address ambiguities without requiring the general use of network-ID-qualified addresses.

Address aliasing provides an alias network address within one subnetwork address space to represent a NAU residing within another subnetwork. The alias address and its counterpart in the other address space may have different subarea/element splits.

ADDRESS ASSIGNMENT ALGORITHM

Alias addresses used for either SSCP-SSCP or LU-LU sessions may be either system-defined or dynamically assigned during session initiation. If an alias address is system-defined, it is always used for sessions with a particular NAU in another network.

Each gateway node has a pool of addresses from which it can assign alias addresses. Except for the constraints defined in SNA Format and Protocol Reference Manual: Architecture Logic, the address assignment algorithm is implementation defined.

The primary purpose of the address assignment protocols is to provide each gateway node along a session path with two address pairs for the cross-network session. As session traffic flows through the gateway node, the gateway node transforms the address fields in the transmission header (TH) from values meaningful in one subnetwork to values meaningful in the other.

For a cross-network session, an SSCP or LU in one subnetwork is represented by an alias address in each other subnetwork through which the session traffic flows. Thus, a minimum of two alias addresses are assigned for each session. As shown in Figure 1-16, the address pair in each subnetwork contains the alias address of the SSCP or LU in the other subnetwork and the real address of the local SSCP or LU (i.e., the one used for routing within its own subnetwork). If the subnetwork is an intermediate network, such as network B in Figure 1-10 on page 1-10, both addresses associated with the session are alias addresses.

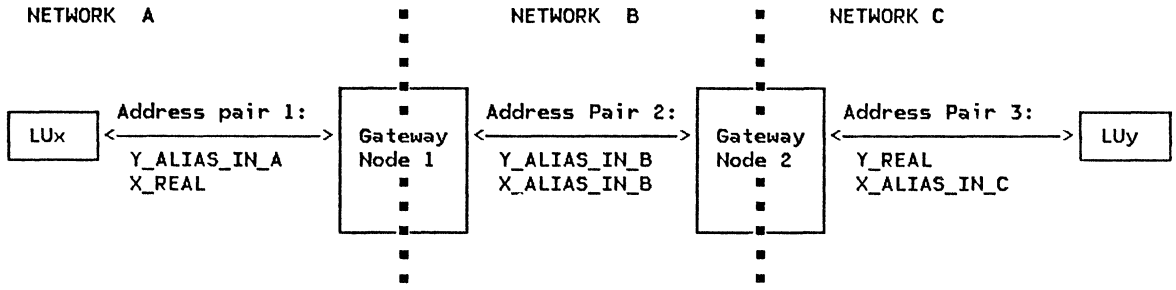


Figure 1-16. Address Transformation: Gateway node 1 transforms TH address pair 1 to TH address pair 2, and vice versa. Gateway node 2 does the same for TH address pair 2 and TH address pair 3.

During session initiation, a gateway SSCP sends an RNAA request to the gateway PU to cause both alias addresses to be assigned. The RNAA carries the real address of the origin LU or SSCP, along with the network-ID-qualified real names of both session partners. The gateway node assigns two alias addresses to the session, and returns them in the RNAA response. It may use the NAU names during the assignment, e.g., to determine whether it has a system-defined address associated with a DLU. The gateway node acquires the real address of the destination LU or SSCP from a SETCV RU sent by a gateway SSCP later in the session initiation sequence, as shown in Figure 1-29 on page 1-34 and Figure 1-32 on page 1-37. For SSCP-SSCP sessions, this address is system-defined in the gateway SSCP. For LU-LU sessions, the address is acquired from the SSCP of the DLU by further exchange of session services RUs. These protocols are illustrated in Figure 1-17 on page 1-18.

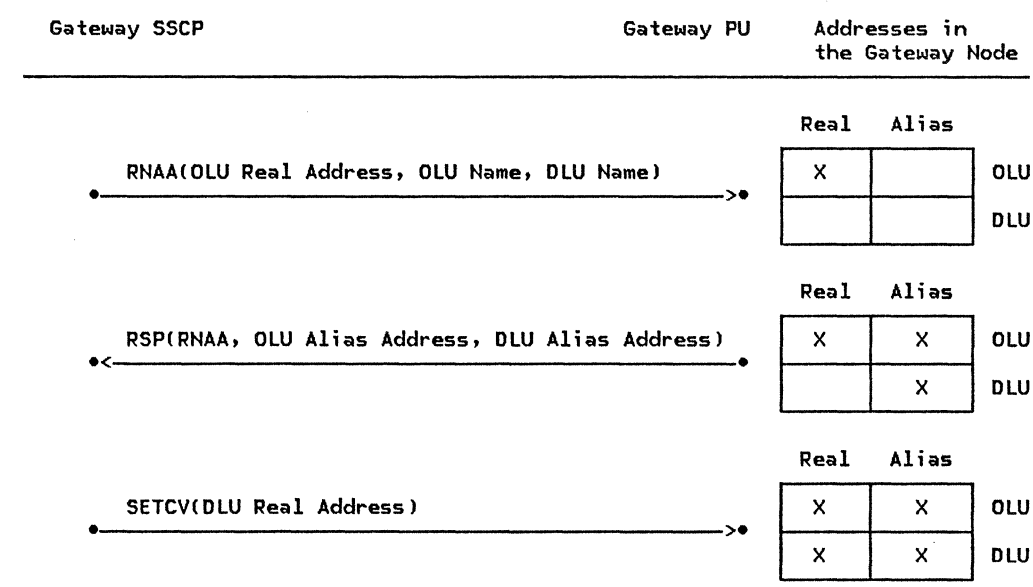


Figure 1-17. Gateway Node Acquisition of an Address Transform

For intermediate subnetworks, addresses may be aliases, even though they appear to be real addresses to particular gateway nodes. For example, in Figure 1-16 on page 1-17, X_ALIAS_IN_B appears to gateway node 2 as the real address of X, even though it is an alias address assigned by gateway node 1.

SYSTEM-DEFINITION CONSIDERATIONS

Each SSCP has a system-defined address for each SSCP with which it can have a session. Thus each gateway SSCP has a network-ID-qualified address for each SSCP with which it can have a cross-network session, and each non-gateway SSCP has an alias address for each gateway SSCP with which it can have a cross-network session.

ADDRESS TRANSFORM RELEASE

An address transform is released by a gateway PU when the session associated with it terminates, or when a gateway SSCP sends a NOTIFY(X'05') instructing the gateway PU to release the session resources.

A dynamically assigned alias address is released when the last address transform using it is released.

ADDRESS TRANSFORMATION PERFORMED BY A GATEWAY SSCP

Before sending a session services RU to another SSCP, a gateway SSCP transforms the addresses appearing in the RU if necessary, so that they are network-ID-qualified addresses, if the partner SSCP is a gateway SSCP, or real or alias addresses meaningful in the destination subnetwork, if the partner SSCP is not a gateway SSCP.

ADDRESS TRANSFORMATION PERFORMED BY A GATEWAY NODE

The gateway node transforms the addresses in the transmission header of each message unit crossing a subnetwork boundary according to the address transform previously established by the exchange of RNAA and SETCV RUs.

NAME ALIASING AND TRANSFORMATION

Each subnetwork has an independent name space, which includes names for the following objects:

- Real names for SSCPs in the local subnetwork
- Real names for LUs in the local subnetwork
- Alias names for LUs in other subnetworks
- Class-of-service (COS) names
- Mode names

The transformation of alias LU names at subnetwork boundaries prevents name ambiguities, while still allowing each subnetwork to have an independent name space. LU names appearing in RUs are transformed between real names and alias names as required, so that the names belong to the name space recognized by the receiver of the RU. Name aliasing allows subnetworks to be interconnected without concern for duplicate use of LU names.

Each alias name is installation assigned. To avoid name conflicts, it should not be the same as any other name in its name space. Since name spaces are independent, there is no coordination of name assignment between connected subnetworks.

Mode names and class of service (COS) names are also transformed by gateway SSCPs as RUs cross subnetwork boundaries.

Figure 1-18 shows the data used by a gateway SSCP to transform names. Name transformations are discussed further below.

1	Netid-A.alias-LU-name	———>	Netid-B.real-LU-name (See Note 2.)
2	Netid-A.real-LU-name and Netid-B	———>	Netid-B.alias-LU-name
3	Netid-A.mode-name and Netid-B	———>	Netid-B.mode-name
4	Netid-A.COS-name and Netid-B	———>	Netid-B.COS-name

Figure 1-18. Data Used for Name Transformation:

Notes:

1. Netid-x.name represents a network-ID-qualified name. This figure shows the information required for the transformation; the information may not appear in exactly this form in the RUs that trigger the transformation.
2. The transformation from alias to real LU name may optionally yield the name of the SSCP of the LU, which can then be used for SSCP rerouting (see Figure 1-24 on page 1-26).

SSCP names that appear in RUs crossing subnetwork boundaries are always network-ID-qualified. As a result, no problem is associated with using duplicate SSCP names in different subnetworks.

Name aliases, if required, are predefined within gateway SSCPs. If an alias name is not provided, it is assumed to be the same as the real name.

LU NAME TRANSFORMATION

LU names appearing in RUs on SSCP-SSCP flows are transformed by gateway SSCPs into their counterparts in the destination subnetwork.

If a gateway SSCP is the only gateway SSCP between the SSCP of the origin LU and the SSCP of the destination LU (see "SSCP Rerouting" on page 1-23), it transforms an alias LU name to a real LU name and a real LU name to an alias LU name.

Otherwise, one of the gateway SSCPs in the first gateway transforms any alias LU names in the RU to network-ID-qualified real names. Any gateway SSCP along the path may transform the real names to alias names recognized in the destination subnetwork. Information used for LU name transformation is shown in lines 1 and 2 of Figure 1-18 on page 1-19.

If the first gateway has more than one gateway SSCP, network-ID-qualified names are not required until a gateway SSCP sends RNAA to the gateway node. This allows knowledge of network-ID-qualified names to be limited to one gateway SSCP in a gateway.

At least one gateway along a tandem gateway path is able to map from real to alias names on behalf of the destination subnetwork. For example, the OLU real name in CDINIT is transformed to an alias name at or before the destination subnetwork's gateway.

Intermediate subnetworks through which session services RUs may flow do not need alias LU names. All session services RUs flowing through intermediate subnetworks are transmitted between gateway SSCPs and use network-ID-qualified LU names. Thus, LU name aliasing is done for the origin subnetwork and the destination subnetwork and for none between.

Figure 1-19 on page 1-21 shows a CDINIT LU-name aliasing example with three networks in tandem. LUa in network A is initiating a session with LUc in network C. However, the name LUc is already used in network A. Consequently, LUc in network C is known in network A as LUx. SSCPa defines LUx to be in the domain of gateway SSCP1.

Gateway SSCP1 in the first gateway recognizes LUa to be the real name of the OLU in network A. Gateway SSCP1 determines that LUx is not in its own domain and transforms the alias name LUx to the network-ID-qualified real name C.LUc before sending the RU to gateway SSCP2. The real name of C.LUc belongs to network C's name space and so does not need further transformation. The name A.LUa requires transformation to a name meaningful in network C's name space. The CDINIT RU format allows this transformation to be done at any gateway SSCP along the session setup path (including gateway SSCP1 in this example). Gateway SSCP2 (the last gateway SSCP) checks that the transformation has been done. In this example, the name A.LUa is transformed to LUz by gateway SSCP2.

The above example illustrates that knowledge of an alias-to-real transform can be confined to a gateway immediately adjacent to the subnetwork in which the alias is required. Thus, gateway SSCP1 does not know the alias name used in network C for LUa.

The example also shows that subnetwork B (the intermediate subnetwork) does not need an alias name for either A.LUa or C.LUc.

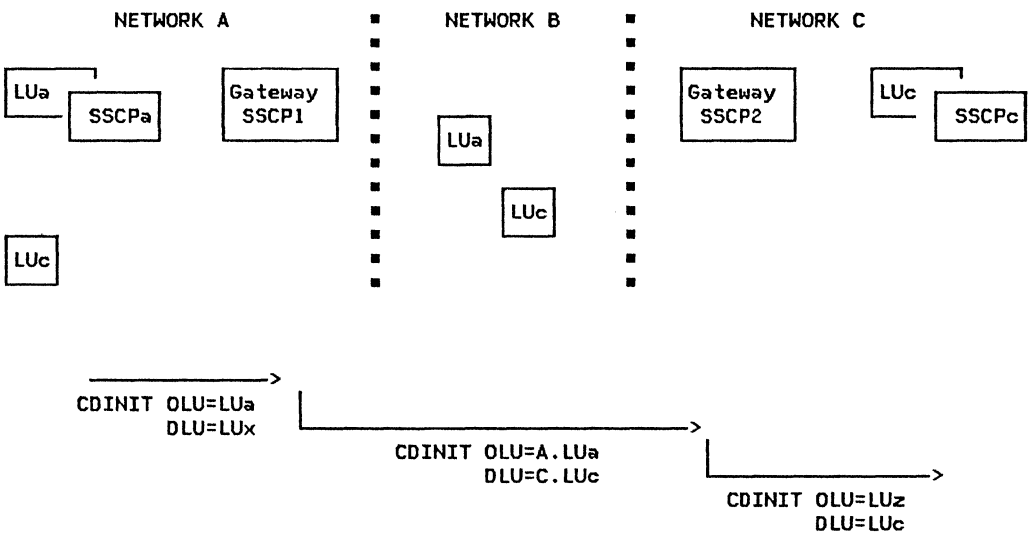


Figure 1-19. LU Name Transformation on a Three-Network CDINIT Flow: LUx and LUz are alias names, to avoid confusion between the names of local LUs and other-network LUs. In the intermediate network, network-ID-qualified names are used to avoid confusion with the names of local LUs. The real name, A.LUa, is transformed to an alias, LUz, before the CDINIT is delivered.

Names in BIND RUs are transformed by the gateway node. A gateway SSCP sends a SETCV request to inform the gateway node of the name transform to be used.

MODE NAME TRANSFORMATION

A mode name represents a set of session parameters requested by an LU. Since different subnetworks need not use the same mode name for the same set of session parameters, gateway SSCPs transform the mode name specified in the source subnetwork to the one used for the same set of parameters in the destination subnetwork.

Any gateway SSCP in the session setup path (see "SSCP Rerouting" on page 1-23) that has the required information may transform the mode name. This information is shown in line 3 of Figure 1-18 on page 1-19.

The mode name is transformed from the one used in the source subnetwork only to the one used in the destination subnetwork; since intermediate subnetworks do not use the mode name, it is not transformed into a mode name in their name spaces.

CLASS OF SERVICE (COS) NAME TRANSFORMATION

A class of service (COS) name represents characteristics of the virtual route connecting two NAUs. Since different subnetworks may use different COS names to represent the same route characteristics and since the session requires a route in each subnetwork, a COS name is required in the name space of each subnetwork traversed by the LU-LU session. Data used for COS name transformation is shown in line 4 of Figure 1-18 on page 1-19.

A COS name appears may or may not appear in a CDINIT request. If a COS name does appear, it is transformed to a COS name meaningful in the subnetwork of the DLU by the gateway SSCP that transformed the DLU name.

A CDINIT response contains one or two COS names:

- Between two gateway SSCPs in different gateways, a single COS name is included. This COS name belongs to the name space of the subnetwork on the OLU side of the sender's gateway and the DLU side of the receiver's gateway.

- Between two gateway SSCPs in the same gateway, two COS names may be included. One is the COS name in the subnetwork on the DLU side of the gateway and the other is the COS name in the subnetwork on the OLU side. The OLU-side COS name may be provided by any gateway SSCP in the gateway, but it is not required to be known until the the last gateway SSCP in the gateway.

These rules are illustrated in Figure 1-20. The middle gateway SSCP in the first gateway transforms the COS name to one meaningful in network C. No COS name is required for network B, since the LU-LU session will not pass through that network.

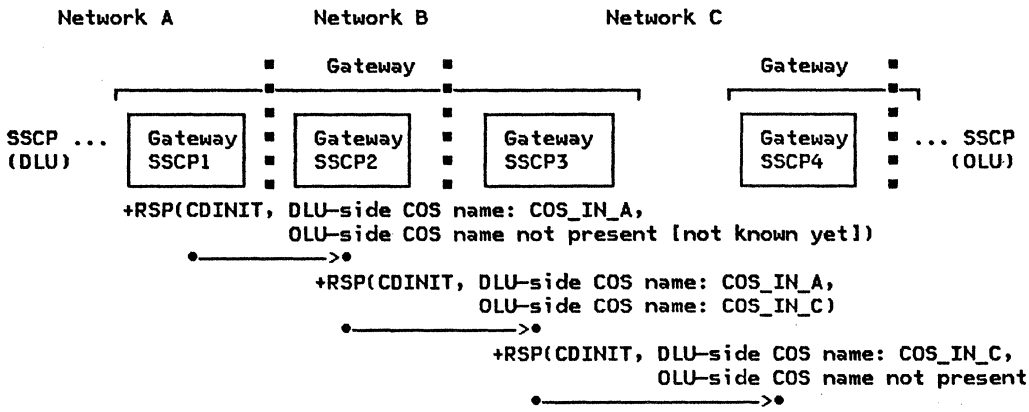


Figure 1-20. Class of Service Names in RSP(CDINIT): DLU-side and OLU-side are defined with respect to the SSCP that receives the RU.

Before it forwards a BIND request, each gateway node uses a list of virtual routes for the subnetwork on the SLU side in order to have a virtual route assigned to the session. A gateway SSCP in the gateway resolves the COS name in the subnetwork on the SLU side to a VR identifier list, and sends the list to the gateway node in control vector X'1B' on a SETCV request. Since either the OLU-side COS name or the DLU-side COS name can be the SLU-side COS name, the gateway SSCP requires both.

Figure 1-21 on page 1-23 summarizes the transformation done for names and addresses. Alias addresses are required in intermediate subnetworks, while alias LU names are not.

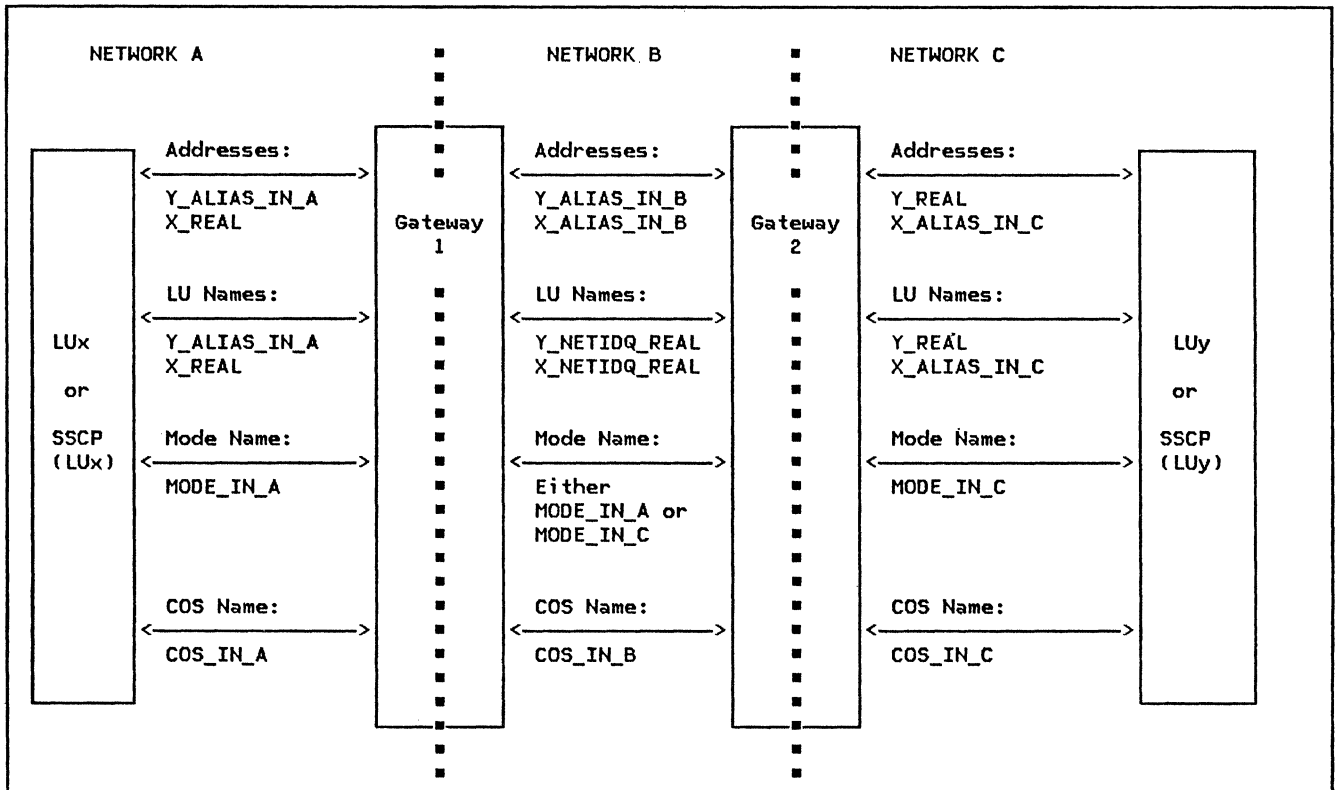


Figure 1-21. Aliasing and Transformation Summary: NETIDQ stands for network-ID-qualified.

SSCP REROUTING AND GATEWAY NODE SELECTION

SSCP REROUTING

As shown in the figures in "Configurations" on page 1-3, the SSCPs involved in session services for a cross-network LU-LU session may be separated by one or more gateway SSCPs. In order for the two SSCPs with primary responsibility for session services for the session (e.g., the SSCPs of the OLU and DLU) to exchange RUs, a path is established between them that may have more than one leg. Each leg of the path is an SSCP-SSCP session, where at least one of the session partners is a gateway SSCP. The process of forwarding RUs along the path by the intermediate gateway SSCPs is called SSCP rerouting, and the path is called the session setup path. In complex configurations, such as tandem gateways, the rerouting may involve a path with several gateway SSCPs in the middle.

A session setup path is established for the life of an LU-LU session during the flow of a CDINIT request. As part of their CDINIT processing, the gateway SSCPs remember the successful path so that they can use it for all subsequent session services RUs concerning that session. As described in "LU-LU Session Awareness Maintained by Gateway Components" on page 1-28 , the path is destroyed when awareness of the session is destroyed in each SSCP along the path. The session setup path is established independently for each session between a particular pair of LUs, and therefore may involve different intermediate gateway SSCPs for different sessions.

Figure 1-22 shows the RUs that follow the path established by CDINIT, the RUs that cause the path to be destroyed, and other RUs besides CDINIT that can cause a path to be established.

RUs that determine their own path	RUs that follow another RU's path		
	Only follow path	Follow and destroy path	Follow and destroy path, with RSP sent immediately by each gateway SSCP
CDINIT (I, I|Q, Q) (Note 1)	+RSP(CDINIT) CDINIT(DQ) CDCINIT +RSP(CDCINIT) CDSESSST RSP(CDSESSST) CDTERM (not Cleanup) +RSP(CDTERM, not Cleanup)	-RSP(CDINIT) -RSP(CDCINIT)	CDSESSEND (Note 2) CDTERM(Cleanup) CDSESSSF CDSESSTF
DSRLST (SA X'02') (Note)		RSP(DSRLST)	
NOTIFY(X'06')		RSP(NOTIFY(X'06'))	
NOTIFY(X'08')		RSP(NOTIFY(X'08'))	

Figure 1-22. Session Services RUs and Path Determination:

Notes:

1. The following abbreviations are used in the table:
   - I: Initiate only
   - I|Q: Initiate or queue
   - Q: Queue only
   - DQ: Dequeue
   - SA: Search argument
2. CDSESSEND, in conjunction with NOTIFY and SESSEND, is used to synchronize SSCPs and gateway nodes with respect to session termination. CDSESSEND does not really follow the CDINIT path, since it may be generated or discarded in the middle of the path.

Figure 1-23 illustrates SSCP rerouting through a four-network configuration in which the gateway nodes are not explicitly shown. A CDINIT request for a session between LU1 and LU2 could follow any of several paths through the set of gateway SSCPs.

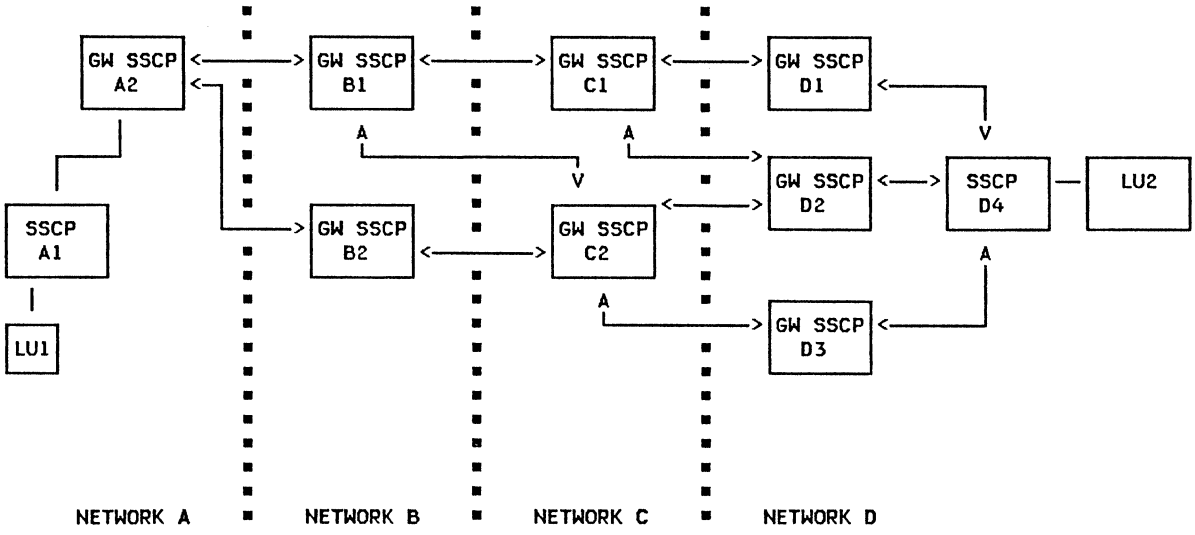


Figure 1-23. Potential Paths for SSCP Rerouting

When a gateway SSCP receives an RU for which a path must be sought, it performs a search using the data shown in Figure 1-24 on page 1-26. The search may produce the LU's SSCP or a list of adjacent gateway SSCPs that can forward the RU one step closer to the LU's SSCP. An adjacent SSCP is an SSCP with which the searching SSCP may have a session. The LU's SSCP may or may not be a gateway SSCP. If the search returns a list of adjacent SSCPs, the gateway SSCP uses a trial-and-error technique to select the next leg of the session setup path.

Trial-and-error rerouting has two goals:

- Path-determining RUs may be automatically rerouted around failed nodes and links.
- Gateway SSCPs need not keep a detailed record of potential end-to-end paths to the SSCP of an LU. Instead, they know only the next gateway SSCP on a particular path.

When a path is being sought, a gateway SSCP progresses through the list of adjacent SSCPs in order, sending the RU to the next SSCP on the list. If it receives a negative response with sense data indicating a rerouting problem, such as resource unknown, it tries the next SSCP on the list. When the list is exhausted without success, it returns a negative response with sense data indicating inability to reroute.

A procedure correlation identifier (PCID) is carried in all session services RUs and is used by a gateway SSCP as a key to determine the next SSCP on a previously established path. For a description of PCIDs, how they are derived, and why a gateway SSCP may have two for a particular session, see "Procedure Correlation Identifier (PCID) Processing" on page 1-27.

User-defined adjacent gateway SSCP lists may cause a routing loop, where a path-determining RU may return to a gateway SSCP that it has already traversed. The SSCP Identifier control vector (X'17') on NOTIFY(X'08') and a Resource Identifier control vector (X'19) on all other path-determining RUs contain a "maximum visits" field. If multiple Resource Identifier control vectors are present, the one representing the DLU is used. The maximum visits field is initialized by the first gateway SSCP and decremented by each subsequent gateway SSCP on the path. The initial value is installation dependent. If this field is decremented to 0 before reaching the target SSCP, it is assumed that a loop in the rerouting path has been detected, and a negative response is sent.

GATEWAY NODE SELECTION

As CDINIT flows from the SSCP(OLU) to the SSCP(DLU), the first gateway SSCP that sends it across each subnetwork boundary or receives it from a non-gateway SSCP across a subnetwork boundary selects the gateway node to be used by the LU-LU session to cross that boundary. Alternate gateways are available only if the gateway SSCP belongs to multiple parallel gateways that cross that boundary.

After selecting an adjacent SSCP to route to, a gateway SSCP selects a gateway node for the LU-LU session from the list of potential gateway nodes associated with the selected SSCP, as shown in Figure 1-24. If the selected SSCP is also a gateway SSCP and in the same gateway, the sending gateway SSCP specifies the gateway node in the Session Initiation control vector (X'14') on the CDINIT request. The receiving gateway SSCP negatively responds to the CDINIT if

- It is required to support the gateway node and does not have an SSCP-PU session with the PU of the gateway node, or
- It is responsible for sending the RNAA RU to that PU and the RNAA fails.

The gateway node specification is retained in the control vector until the last gateway SSCP in the gateway is ready to forward the CDINIT to an SSCP that is not in the gateway.

CROSS-NETWORK DIRECTORY

As shown in Figure 1-24, a gateway SSCP may use a system-defined cross-network directory in order to perform its rerouting and gateway node selection functions. The directory yields a list of adjacent SSCPs to which session-initiation requests concerning a given LU can be routed.

The granularity of the search is implementation dependent. Gateway SSCPs may always route the same way to the same target network, in which case, only the network identifier is needed. If a gateway SSCP routes differently to different SSCPs in a particular network, the SSCP name is also needed. A gateway SSCP may even route differently to target SSCPs depending on the referenced LU, in which case the LU name is needed.

If LU name and SSCP name are both provided, the search first looks for an entry under LU name; if none exists, it looks for an entry under SSCP name; if none exists, it looks for a general entry for that network identifier.

For each adjacent SSCP in an another subnetwork, the directory includes a list of potential gateway nodes that the LU-LU session may use to cross the subnetwork boundary, in order to allow the gateway SSCP to select the gateway node for the LU-LU session.

The cross-network directory described here is an architectural abstraction; the structure is not required of implementations.

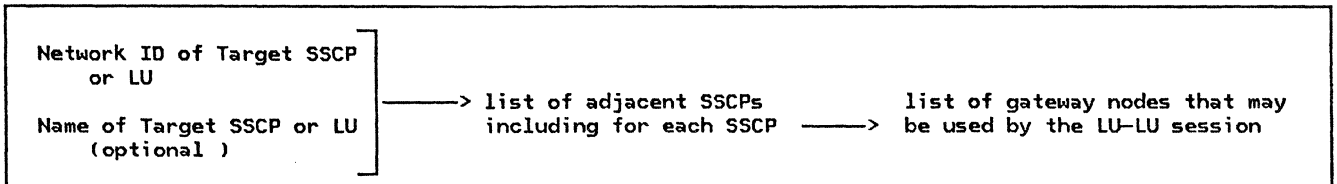


Figure 1-24. Data Determining SSCP Rerouting and Gateway Node Selection for LU-LU Sessions

CONTROL VECTORS CONTAINING GATEWAY RELATED INFORMATION

The following control vectors contain gateway-related information. They are appended to session services RUs sent between current-level SSCPs, i.e., SSCPs that can receive a format 3 CDINIT, as specified in the CDRM (X'06) control vector, whether or not they are serving as gateway SSCPs.

- Resource Identifier control vector (X'19')

  The Resource Identifier control vectors on an RU provide the next gateway SSCP with the information it needs to perform SSCP rerouting and gateway node selection.

Between gateway SSCPs in the first gateway encountered in the session setup path, an LU name in a Resource Identifier control vector may be an alias name, rather than the network-ID-qualified name normally required; in this case, the control vector indicates that the information is tentative. The real names are provided before the RU exits the first gateway. See "LU Name Transformation" on page 1-19 for more information.

Different RUs carry different sets of Resource Identifier control vectors:

- In CDINIT and RSP(CDINIT), one each for the OLU and the DLU
- In NOTIFY(X'06'), i.e., NOTIFY carrying the Cross-Gateway Resource Requested vector, one each for the requesting and requested LUs and one for the session partner of the requested LU
- In NOTIFY(X'08'), i.e., NOTIFY carrying the Cross-Gateway Resource Available vector, one for the DLU
- In DSRLST, one for the LU referenced by the DSRLST

- NAU Address control vector (X'1A'), appearing in CDINIT and RSP(CDINIT).

  The NAU Address control vector carries the real address of the OLU to the SSCP(DLU) or the real address of the DLU to the SSCP(OLU). The network identifier for the address appears in the associated Resource Identifier control vector.

- Session Initiation control vector (X'14') appearing in CDINIT and RSP(CDINIT).

  The Session Initiation control vector carries the class of service (COS) names and the transformed mode name. Between multiple gateway SSCPs in the same gateway, it also specifies the gateway node to be used by the LU-LU session to cross the subnetwork boundary, as described in "Gateway Node Selection" on page 1-26 in more detail. The gateway node name is not sent between gateway SSCPs in different gateways.

- SSCP Identifier control vector (X'17'), appearing in NOTIFY (X'08') only.

  The SSCP Identifier control vector provides the next gateway SSCP with additional information to perform SSCP rerouting.

PROCEDURE CORRELATION IDENTIFIER (PCID) PROCESSING

A procedure correlation identifier (PCID) is a session instance identifier used by two SSCPs to identify a particular session. Each session services RU contains a PCID field that is used by gateway SSCPs as a key to the SSCP rerouting data established for a session setup path, as shown in Figure 1-25 on page 1-28.

A procedure correlation identifier is unique within a particular subnetwork. A cross-network session has a PCID for each subnetwork that it traverses. As a result, each SSCP in the session setup path may associate either one or two PCIDs with a session. Gateway SSCPs that send the CDINIT request across a subnetwork boundary and are in the middle of the session setup path have two PCIDs per session, one each for communicating with the adjacent SSCPs in both directions.

Before a gateway SSCP sends a CDINIT RU (or other RU that determines its own path, as shown in Figure 1-22 on page 1-24) across a subnetwork boundary, it generates a new PCID to replace the one in the RU. If the RU is sent to an SSCP in the same subnetwork, the gateway SSCP sends it without changing the PCID value.

The gateway SSCP saves SSCP rerouting data for the session, as shown in Figure 1-25 on page 1-28, so that it can route subsequent RUs along the same path. The session data includes the PCID transform, if one has been established.

As subsequent requests and responses follow the session setup path, a gateway SSCP uses the PCID in the RU as a key to find the session data that identifies the next SSCP to receive the RU. If the session data contains two PCID values, the gateway SSCP transforms the PCID value before forwarding the RU.

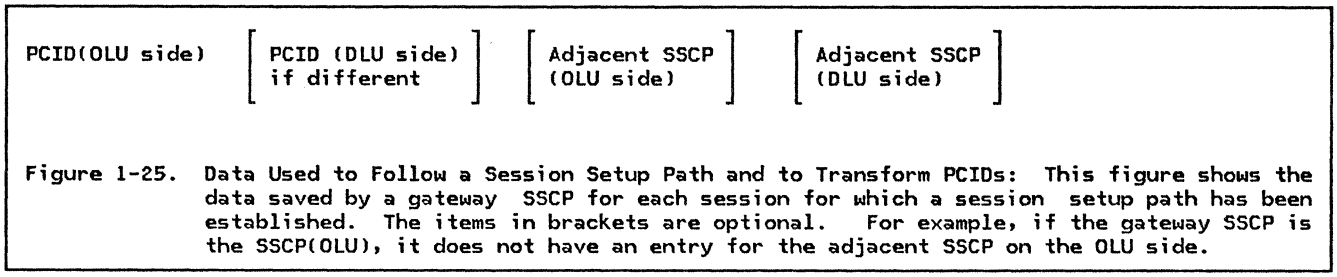


Figure 1-25. Data Used to Follow a Session Setup Path and to Transform PCIDs: This figure shows the data saved by a gateway SSCP for each session for which a session setup path has been established. The items in brackets are optional. For example, if the gateway SSCP is the SSCP(OLU), it does not have an entry for the adjacent SSCP on the OLU side.

LU-LU SESSION AWARENESS MAINTAINED BY GATEWAY COMPONENTS

All of the components involved in cross-network session initiation maintain appropriate session awareness, that is, a record of the existence of the LU-LU sessions that are active or in the process of being activated or deactivated. The session awareness described here is maintained for session services and operator awareness displays, as opposed to any permanent session records that might be kept for problem determination. The components that maintain LU-LU session awareness include:

- PLU
- SLU or boundary function representing the SLU
- SSCP(PLU)
- SSCP(SLU)
- All gateway SSCPs on the session setup path
- All gateway nodes that handle traffic between the two LUs

Maintenance of session awareness for the PLU, SLU, and non-gateway SSCPs is not changed for gateway services.

Figure 1-26 on page 1-29 shows the events that cause changes in LU-LU session awareness in gateway nodes and gateway SSCPs. This table shows only the events that cause changes in awareness, e.g., receipt of a particular RU; it does not show the RUs sent by these components when the events occur.

Awareness Changes	Events for SSCPs on Setup Path (including gateway SSCPs)	Events for Gateway Nodes
Adding Session Awareness	Sends or receives CDINIT	RNAA
Recognizing Session Activation	Sends or receives +RSP(CDSESSST)	+RSP(BIND)
Destroying Session Awareness for the following reasons:		
• BIND failure	BINDF (for SSCP(PLU)) CDSESSSF (for all others) (See note 4.)	NOTIFY(X'05') or -RSP(BIND)
• Normal session deactivation	(See Note 1.)	+RSP(UNBIND)
• UNBIND failure	UNBINDF (for SSCP(PLU)) CDSESSTF (for all others) (See note 4.)	NOTIFY(X'05') or -RSP(UNBIND)
• Cleanup termination	Sends or receives CDTERM(cleanup) (See note 4.)	NOTIFY(X'05')
• Forced termination before session active	Sends or receives CDTERM(not cleanup) when session not active (See note 4.)	NOTIFY(X'05')
• LU-LU route inoperative	(See Note 1.)	• Detects LU-LU route inoperative
• SSCP-gateway PU session outage for pending-active session only (See Note 2.)	Sends DACTPU or detects route inoperative for SSCP-PU session to gateway node	Receives DACTPU or detects route inoperative for SSCP-PU session to a gateway SSCP participating in the gateway (See Note 3.)

Figure 1-26. Events Causing Changes in LU-LU Session Awareness: An RU name by itself represents the event "Receives this RU." If either of two events may occur, the one that occurs first causes the change in session awareness.

Notes:

1. For further events causing changes in SSCP session awareness, see Figure 1-27 on page 1-30.
2. A session is pending-active between the time session awareness is added for it (row 1 in the table) and its activation is recognized (row 2).
3. A gateway node recognizes the gateway SSCPs participating in the gateway because they send it RNAA or SETCV for the session.
4. Before a gateway SSCP can destroy its own session awareness, one of the following must occur for each gateway node that it controls:
   - It has already received NOTIFY(X'05') from the gateway node.
   - It sends NOTIFY(X'05') to the gateway node.
   - The route connecting it to the gateway node is inoperative.

Figure 1-27 shows the rules governing destruction of session awareness in all gateway SSCPs on the session setup path when the session terminates normally or because a route becomes inoperative. Events from both rows 2 and 3 occur before a gateway SSCP destroys its awareness of a particular session. An event from row 1 is required only if the gateway SSCP is also the SSCP of the PLU or the SSCP of the SLU.

Which of two adjacent SSCPs in the session setup path sends CDSESSEND depends on timing considerations governing which one first receives CDSESSEND from the next SSCP in the session setup path or first gains direct knowledge of the session termination from its LU (if it is the SSCP of the PLU or SLU) and knows that all its gateway nodes have destroyed their session awareness, as described above. An example of the application of these rules is shown in "Deactivation of Cross-Network LU-LU Sessions" on page 1-41.

Events Affecting Different SSCPs	Normal Notification	Route Loss Notification
Direct notification by an LU: SSCP(PLU) or SSCP(SLU)	Receives SESSEND	Detects route inoperative for SSCP–LU session
Direct notification by a gateway node: any gateway SSCP on session setup path	Receives NOTIFY(X'05') or Sends NOTIFY (X'05')	Detects route inoperative for SSCP–PU session (to gateway node)
Knowledge that each neighbor SSCP is directly aware of session deactivation: any SSCP on session setup path	Sends RSP(CDSESSEND) or Receives RSP(CDSESSEND)	Detects route inoperative for SSCP–SSCP session (failure between SSCP and gateway) or Receives DACTCDRM (failure in adjacent subnetwork) or Receives CDTERM (cleanup) (failure further down session setup path)

Figure 1-27. Release of an SSCP's LU-LU Session Awareness: "Normal notification" means that an SSCP learns directly from a session partner about the session deactivation. "Route loss notification" means that the route connecting an SSCP to its session partner is inoperative, so that the SSCP cannot learn of any changes in session status from that session partner. It may also mean that a failure has occurred further down the session setup path, so that the SSCP cannot learn of the session status from either the SSCP(PLU) or SSCP(SLU).

GATEWAY SERVICES FUNCTIONS

GATEWAY SSCP FUNCTIONS

Gateway SSCPs perform the following gateway-related functions in addition to their other SSCP functions:

- Activating cross-network SSCP-SSCP sessions
- Rerouting session services RUs received from one SSCP to the next SSCP on the session-setup path
- Supporting testing of routes and route status reporting for routes in other subnetworks
- Session services to support cross-network LU-LU sessions, including the steps listed below. If a gateway contains a single gateway SSCP, it fulfills the roles of the gateway SSCPs on both the OLU and DLU sides of the gateway. If a gateway contains multiple gateway SSCPs,

the list shows which one performs the particular function. Unless otherwise noted, these functions are performed for every gateway in the session setup path.

- Selecting the gateway node to be used to cross the subnetwork boundary—done by the first gateway SSCP that sends a CDINIT across a subnetwork boundary in each gateway
- Transforming alias DLU name to real DLU name in session services RUs—done by any gateway SSCP in the first gateway
- Transforming real OLU name to alias OLU name—done by any gateway SSCP along the session setup path
- Transforming mode names appearing in session services RUs—done by any gateway SSCP along the session setup path
- Transforming COS names appearing in CDINIT requests—done by the gateway SSCP along the session setup path that transformed the DLU alias name to the network-ID-qualified DLU name
- Transforming COS names appearing in CDINIT responses—done by one gateway SSCP in each gateway
- Sending RNAA and SETCV to the gateway node to request resources for a session and to set up the address transform—done by predesignated gateway SSCP or gateway SSCP on the DLU side
- Resolving the COS name to a VR identifier list and sending the list to the gateway node in a SETCV—done by predesignated gateway SSCP or the gateway SSCP on the OLU side
- Sending SETCV with the LU name transform—done by predesignated gateway SSCP or gateway SSCP on the OLU side
- Sending SETCV to the gateway node to indicate its own participation in the session set-up—done by any gateway SSCP that has not otherwise sent SETCV or RNAA to the gateway node
- Generating a new PCID to insert in CDINIT, DSRLST, NOTIFY(X'06'), or NOTIFY(X'08')—done by every gateway SSCP on the path that sends the RU across a subnetwork boundary
- Transforming PCIDs—done by every gateway SSCP that sends a CDINIT request across a subnetwork boundary
- Maintaining session awareness and an associated rerouting path until session termination events occur (see "LU-LU Session Awareness Maintained by Gateway Components" on page 1-28)—done by every gateway SSCP
- Cleaning up affected pending-active or pending-reset cross-network LU-LU sessions before deactivating its session with another SSCP—done by every gateway SSCP

GATEWAY NODE FUNCTIONS

This section outlines the functions performed by the gateway PU and the two components of a gateway function component.

Gateway PU Functions

Gateway-related RUs reach the gateway node over an SSCP-PU session. The gateway PU passes these RUs to the gateway function session manager for processing, and forwards responses and other RUs from the gateway function session manager to the gateway SSCP.

On receipt of a gateway-related RNAA request, the gateway PU assigns two alias addresses for the session before passing the request on to the gateway function session manager.

Gateway Function Session Manager Functions

The gateway function session manager manages the creation and destruction of session connectors. This function involves:

- Reserving resources for a session connector on receipt of an RNAA request from the gateway PU and associating these resources with the addresses in the RNAA
- Forwarding session-activation and -deactivation requests and responses received from one subnetwork to a NAU in another subnetwork, with the following transformations:
  - Addresses in the transmission header are transformed according to the address transform received in earlier RNAA and SETCV requests.
  - Names appearing in BIND requests and responses are transformed according to the name transform received in a SETCV request.
- Activating a virtual route in the subnetwork on the secondary-NAU side of the gateway node, using a virtual route identifier list received in an earlier SETCV request
- Freeing resources reserved for session connectors when requested by the PU
- Sending REQACTCDRM to an SSCP when necessary for SSCP-SSCP session activation as described in "Activation of Cross-Network SSCP-SSCP Sessions" on page 1-34
- Creating and initializing the session connector and connecting it to the associated path controls. The address transform associated with the session connector contains two address pairs; the session manager gives one address pair to one path control and one to the other.
- Keeping track of the gateway SSCPs involved with a particular session connector, i.e., the ones that sent RNAA or SETCV concerning that session; removing SSCPs from the list when they send DACTPU or when the route for the SSCP-PU session becomes inoperative
- Sending NOTIFY(X'05') to the SSCPs involved with a session connector (see above) when LU-LU sessions are started or ended
- Recognizing when session connectors should be destroyed, including all session-outage notification (SON) conditions (for example, session connectors for pending-active sessions are destroyed when an SSCP-PU session between the gateway PU and a participating gateway SSCP is lost)
- Disconnecting the session connector from both path controls and destroying it
- Sending a session-deactivation request to a NAU in one subnetwork if the virtual route to its session partner in another subnetwork is lost
- Deactivating a session if a gateway SSCP sends a NOTIFY(X'05') requesting that the session resources be released
- Resolving ACTCDRM contention and SSCP-SSCP session override for cross-network sessions. See SNA Format and Protocol Reference Manual: Architecture Logic for a description of these functions.
- Maintaining LU-LU session awareness until session termination events occur (see "LU-LU Session Awareness Maintained by Gateway Components" on page 1-28)

Gateway Function Session Connector Functions

A gateway function session connector receives message units from one path control and sends them via the other. It forwards message units in the order it receives them; it does not change the order based on the expedited flow indicator. It may also collect accounting data, if required, in an implementation- and installation-defined fashion.

SUMMARY OF GATEWAY FUNCTIONS RELATED TO LU-LU SESSIONS

Figure 1-28 shows the allocation between gateway SSCPs and gateway nodes of major functions with respect to cross-network LU-LU sessions.

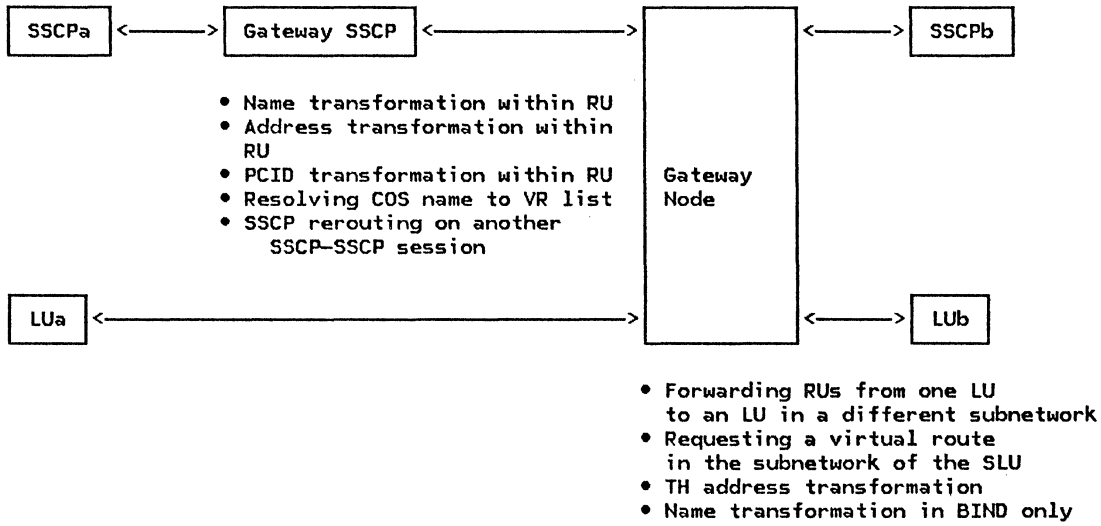


Figure 1-28. Location of Major Gateway Functions with Respect to LU-LU Sessions

The figures below show the exchange of message units among components involved in cross-network sessions.

See Appendix N for an explanation of the notation used in the flows.

ACTIVATION OF CROSS-NETWORK SSCP-SSCP SESSIONS

The following three figures show the activation of cross-network SSCP-SSCP sessions in different configurations.

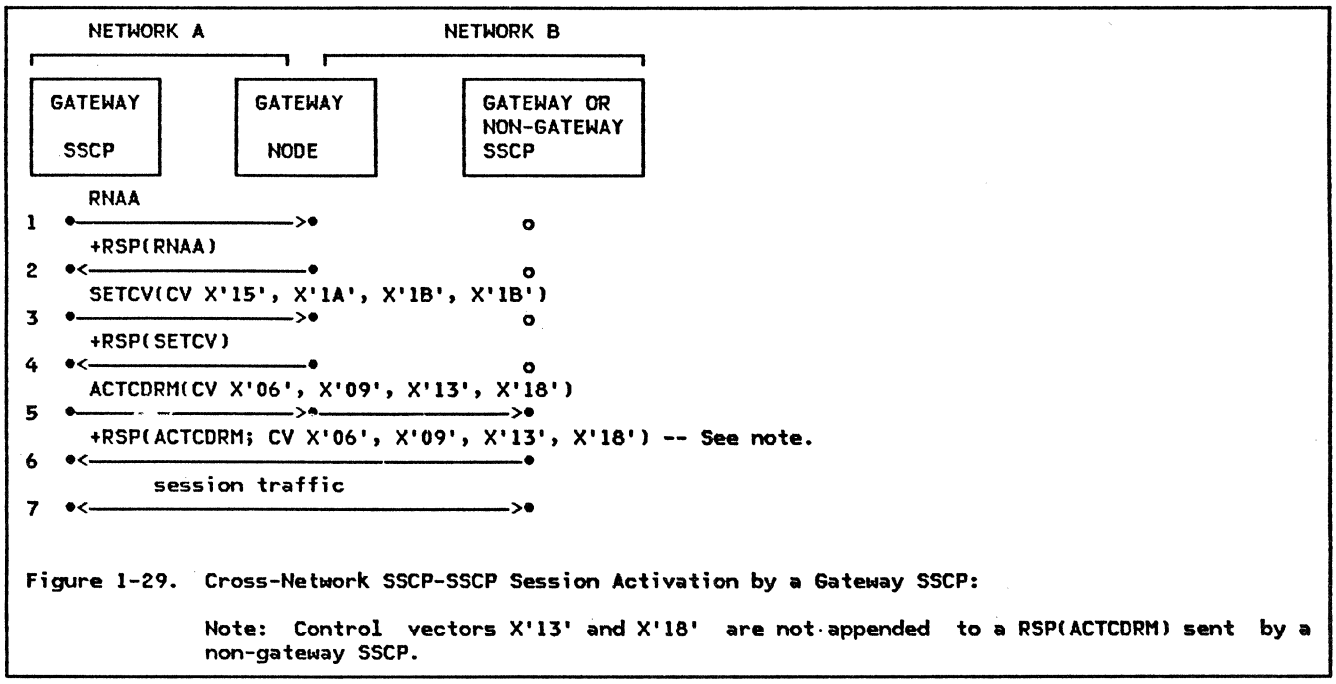


Figure 1-29. Cross-Network SSCP-SSCP Session Activation by a Gateway SSCP:

Note: Control vectors X'13' and X'18' are not appended to a RSP(ACTCDRM) sent by a non-gateway SSCP.

In Figure 1-29, the SSCP initiating the session is a gateway SSCP, which sends RNAA (1) and SETCV (3) to the gateway node in order to set up the address transform for the session before it sends ACTCDRM (5).

Before sending ACTCDRM, the gateway SSCP acquires a virtual route in its own network. The gateway node acquires a virtual route in the second network before forwarding the ACTCDRM (5). Although the SETCV carries two virtual route lists (control vector X'1B'), one for each subnetwork, only the route list corresponding to the second subnetwork is used. The purpose of sending two lists is to allow the ACTCDRM to come from either SSCP; the gateway node is prepared to acquire a route in either network.

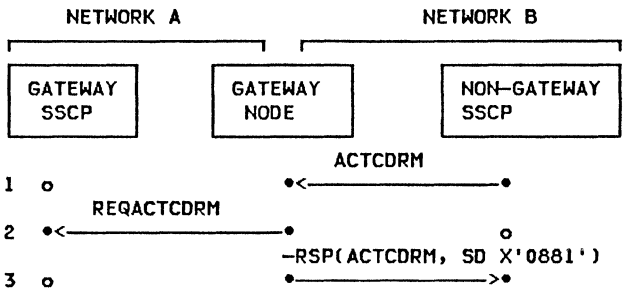


Figure 1-30. Cross-Network SSCP-SSCP Session Activation by a Non-Gateway SSCP: See Figure 1-29 for the steps that follow step 3.

In Figure 1-30, the SSCP initiating the session is not part of the gateway, and therefore does not send the preliminary RNAA and SETCV requests required to prepare the gateway node for the cross-network session. It sends an ACTCDRM request to the gateway node (1), which responds negatively (3). The gateway node matches the alias address in the ACTCDRM request with a gateway SSCP name, and then determines if it has an active session with that SSCP. If so, it sends the gateway SSCP a REQACTCDRM request (2), informing it that an SSCP in another network desires a session with it. The gateway SSCP then initiates the session in the normal manner, as shown in Figure 1-29 on page 1-34.

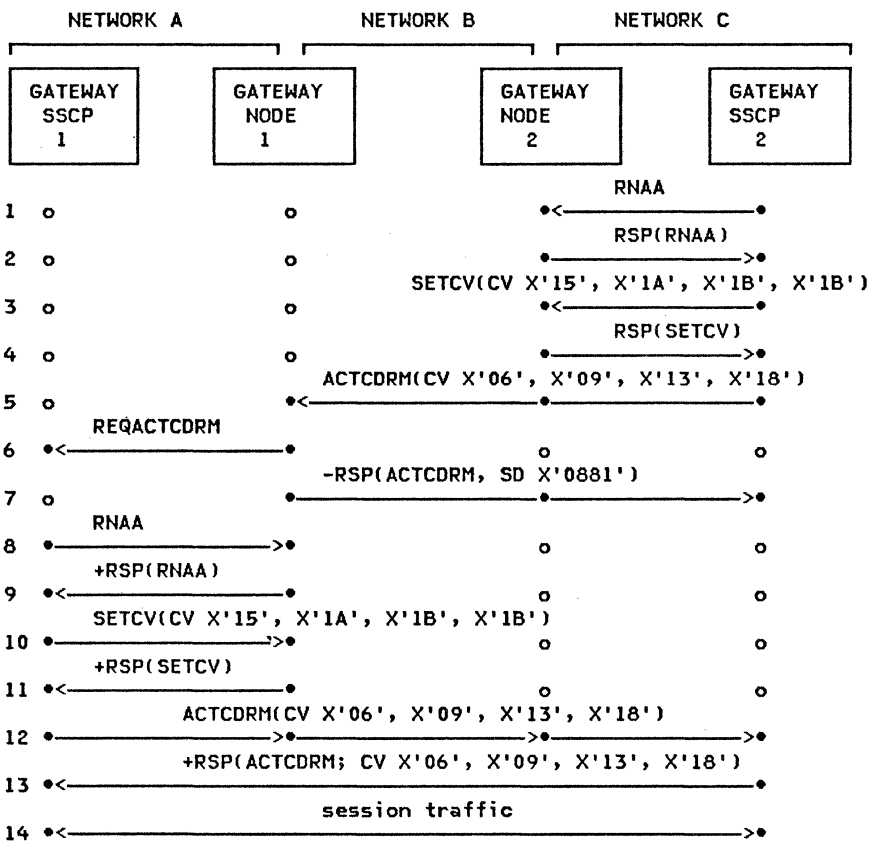


Figure 1-31. Cross-Network SSCP-SSCP Session Activation, Maximum Separation

Figure 1-31 shows the activation of a session between two gateway SSCPs with two gateway nodes between them (see Figure 1-10 on page 1-10). Gateway SSCP 2 sets up the address transform for the SSCP-SSCP session with its neighboring gateway node by sending RNAA and SETCV (1, 3). It then acquires a virtual route in network C and sends the ACTCDRM request (5). Gateway node 2 acquires a virtual route in network B and forwards the ACTCDRM to gateway node 1, being unable to distinguish it from the target SSCP itself (5). Since gateway node 1 does not have a complete address transform for the session, it negatively responds to the ACTCDRM (7) and sends REQACTCDRM to the target gateway SSCP (6) in exactly the manner illustrated in Figure 1-30 on page 1-35.

When gateway node 2 receives the negative response to ACTCDRM (7), it can tell from the sense code that the other gateway SSCP will be initiating the session. Therefore, it retains the address transform set up earlier in anticipation of an ACTCDRM request from the gateway SSCP in subnetwork A. It releases the virtual route in network B that it acquired earlier (5). Gateway SSCP 2 releases the virtual route in network C when it receives the negative response.

The session activation then proceeds, with the gateway SSCP in subnetwork A sending RNAA and SETCV (8, 10) to gateway node 1 and acquiring the virtual route in network A (12), gateway node 1 acquiring the virtual route in network B (12), and gateway node 2 acquiring the virtual route in network C (12).

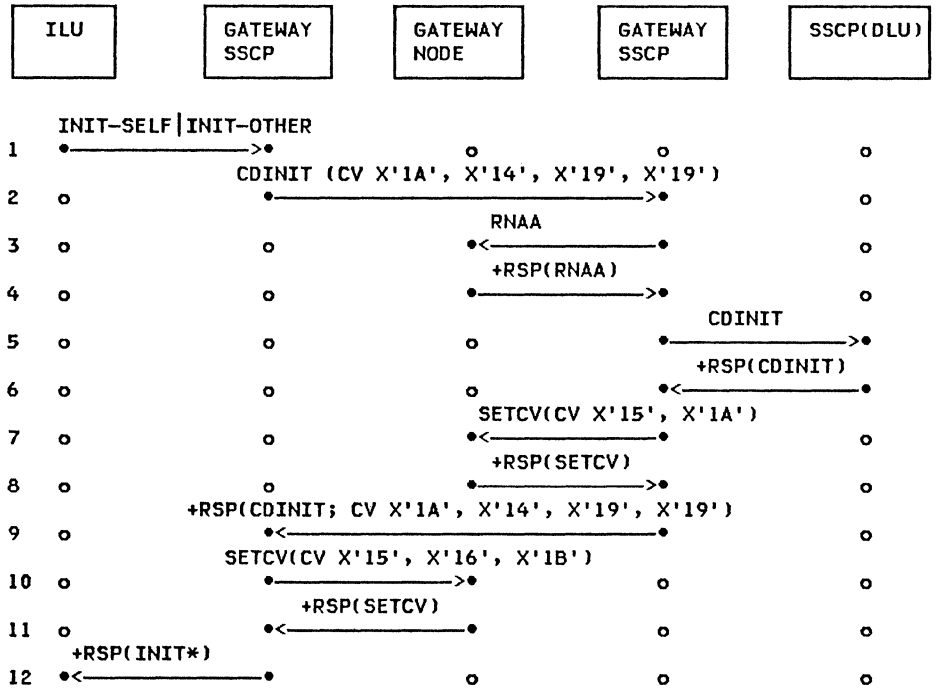


Figure 1-32. LU-LU Session Initiation: This sequence is not affected by the PLU/SLU polarity of the LU-LU session. It is followed by the LU-LU session setup sequence (see Figure 1-34 on page 1-39), which does depend on the PLU/SLU polarity.

LU-LU SESSION INITIATION

The initiating LU (ILU) sends the SSCP in its domain an INIT-SELF or INIT-OTHER request (1). It receives a response from its SSCP (12) after its SSCP receives the CDINIT response (9).

In Figure 1-32, the SSCP of the ILU is also the SSCP of the OLU.

The SSCP of the ILU sends a CDINIT request to the SSCP of the DLU (2, 5). The session setup path is established as this RU flows from the SSCP of the OLU to the SSCP of the DLU. Between gateway SSCPs, this request and its response are required to carry gateway control vectors, as described in "Control Vectors Containing Gateway Related Information" on page 1-26.

The gateway SSCP on the DLU side of each gateway sends an RNAA request to the gateway node, requesting it to assign alias addresses for the LU-LU session (3). The gateway node returns the alias addresses (4).

The CDINIT response contains the real address of the DLU (6, 9). The gateway SSCP on the DLU side conveys this address to the gateway node in the X'1A' control vector of the SETCV request (7).

The gateway SSCP on the OLU side of a gateway resolves the COS name for the SLU side of the gateway to a VR identifier list, and sends the list (control vector X'1B'), along with the LU name transform (control vector X'16') to the gateway node in a SETCV request (10).

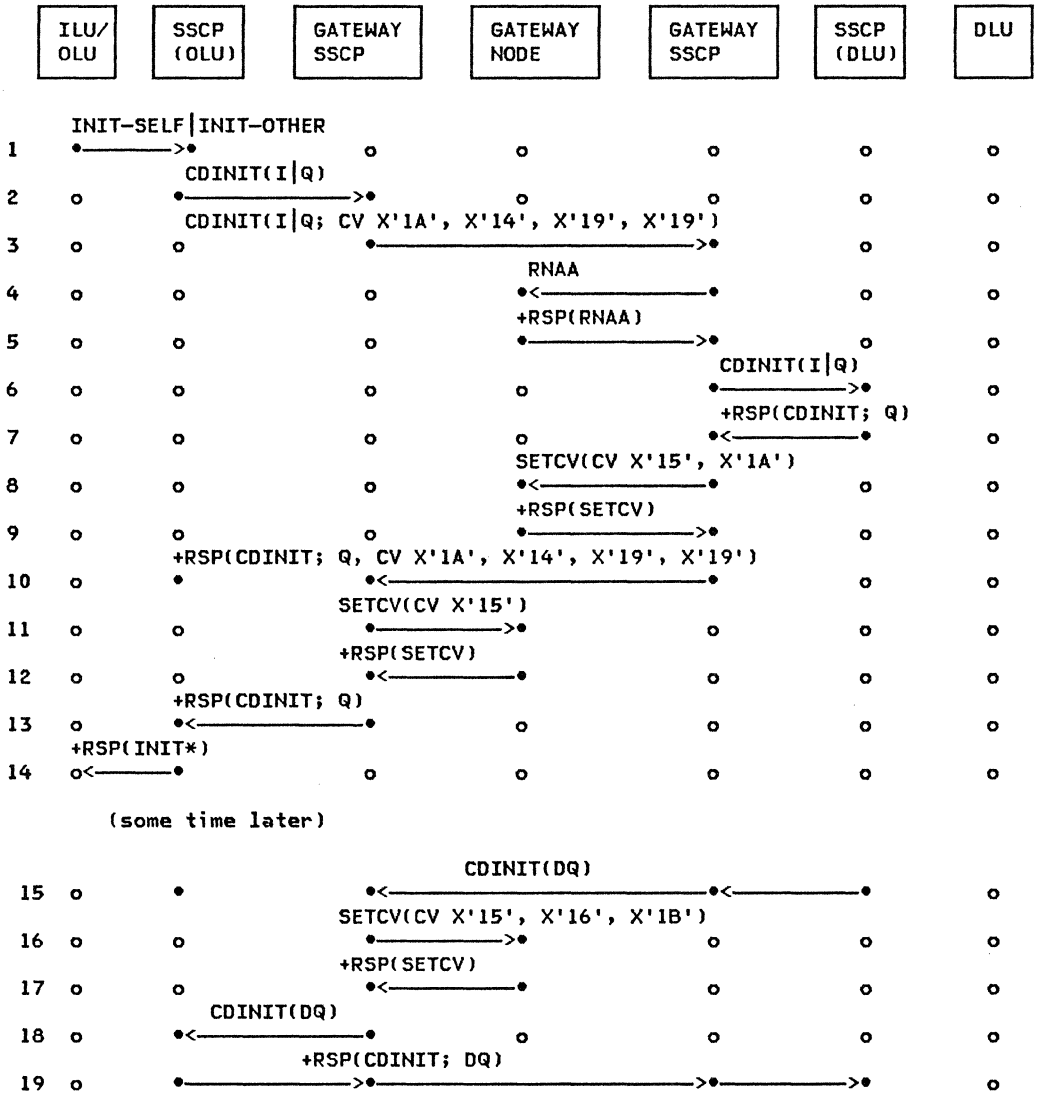


Figure 1-33. CDINIT Queuing and Dequeuing Through a Gateway

CDINIT QUEUING

As shown in Figure 1-33, a CDINIT can cause a request for session resources to be queued at the SSCP of the DLU, if the CDINIT request indicates that the session should be initiated or queued (I/Q) and the resources for the session are not available when the CDINIT is received. In that case, the address transform is set up when the first CDINIT flows (4, 5, 8, 9). The gateway SSCP on the OLU side sends SETCV to the gateway PU to indicate its participation in the session setup so that it can be notified when the session status changes (11).

When the resources become available, the SSCP of the DLU sends a dequeue CDINIT(DQ) to the SSCP of the OLU to complete the initiation phase of session establishment (15, 18). This RU follows the session setup path set up by the earlier CDINIT and uses the address transform already established. This phase is followed by the session setup phase, which is shown in Figure 1-34 on page 1-39.

The name transform and VR identifier list are sent to the gateway node (16) after after the dequeue CDINIT is processed (15).

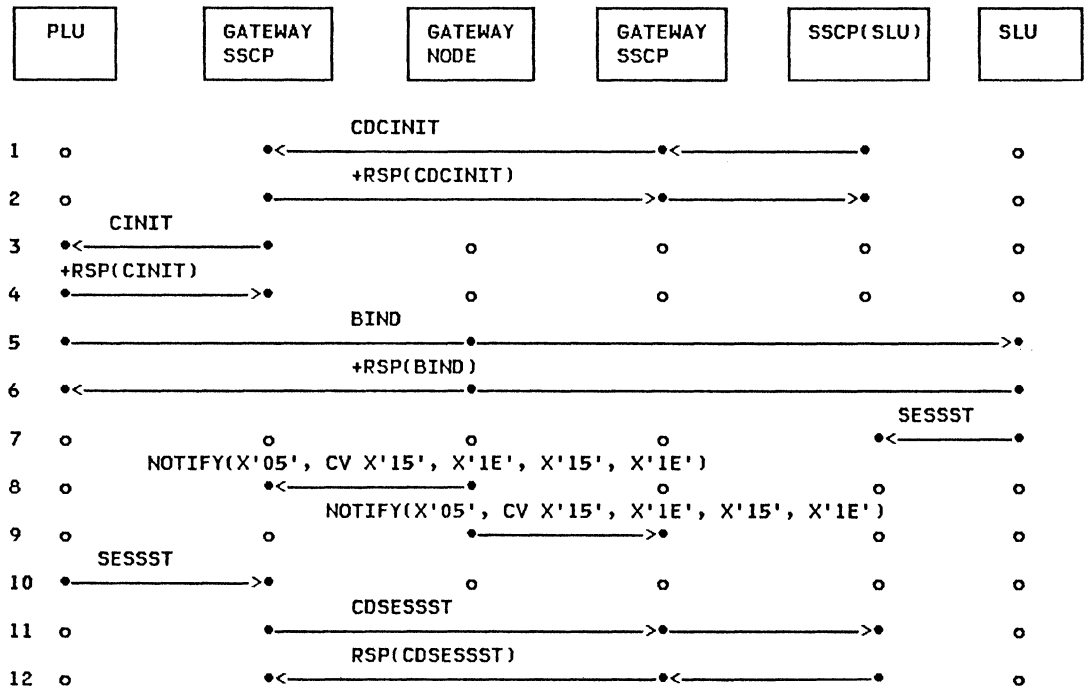


Figure 1-34. LU–LU Session Setup: This sequence is affected by the PLU/SLU polarity of the LU–LU session. It follows the LU–LU initiation sequence shown in Figure 1-32 on page 1-37.

LU-LU SESSION SETUP

The SSCP of the SLU sends CDCINIT containing session parameters for the BIND image (1). This request follows the session setup path established for the session in Figure 1-32 on page 1-37.

The SSCP of the PLU sends a CINIT request with the BIND image to the PLU (3).

After a successful exchange of BIND RUs (5, 6) the SLU and the PLU each send SESSST RUs to their SSCPs (7, 10). If the SLU is in a peripheral node, boundary function sends SESSST on its behalf. The SSCP of the PLU sends CDSESSST to the SSCP of the SLU along the session setup path (11). The SSCPs update their session awareness records to show that the session is active, as shown in Figure 1-26 on page 1-29.

The gateway node notifies all gateway SSCPs in its gateway that the session has started (8, 9). The NOTIFY(X'05') RU carries two VR-ER Mapping Data (X'1E') control vectors, identifying the virtual route used for the session in both networks.

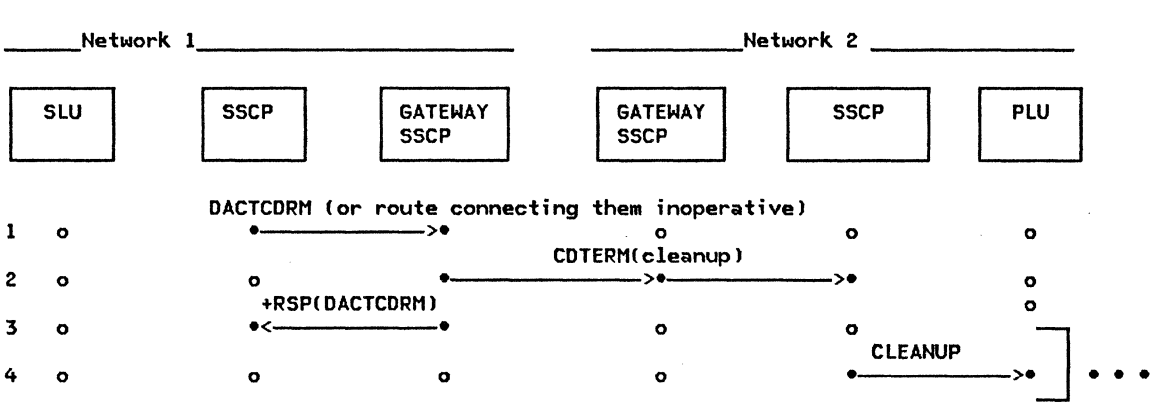


Figure 1-35. Deactivation of a Cross-Network SSCP-SSCP Session

DEACTIVATION OF CROSS-NETWORK SSCP-SSCP SESSIONS

Figure 1-35 shows the actions of a gateway SSCP on receiving a DACTCDRM request or on learning that the route connecting it to another SSCP is inoperative (1). It resets all pending-active and queued LU-LU sessions associated with its session partner.

The figure shows only the cases where the PLU and gateway SSCP are in different subnetworks. If they are in the same subnetwork, normal takedown procedures described in SNA Format and Protocol Reference Manual: Architecture Logic take place.

For each LU-LU session with a PLU in a different subnetwork, the gateway SSCP sends CDTERM(cleanup) to the SSCP of the PLU (2), prompting it to send CLEANUP to the PLU (4).

The gateway SSCPs receiving the CDTERM(cleanup) immediately destroy the session setup path associated with the session.

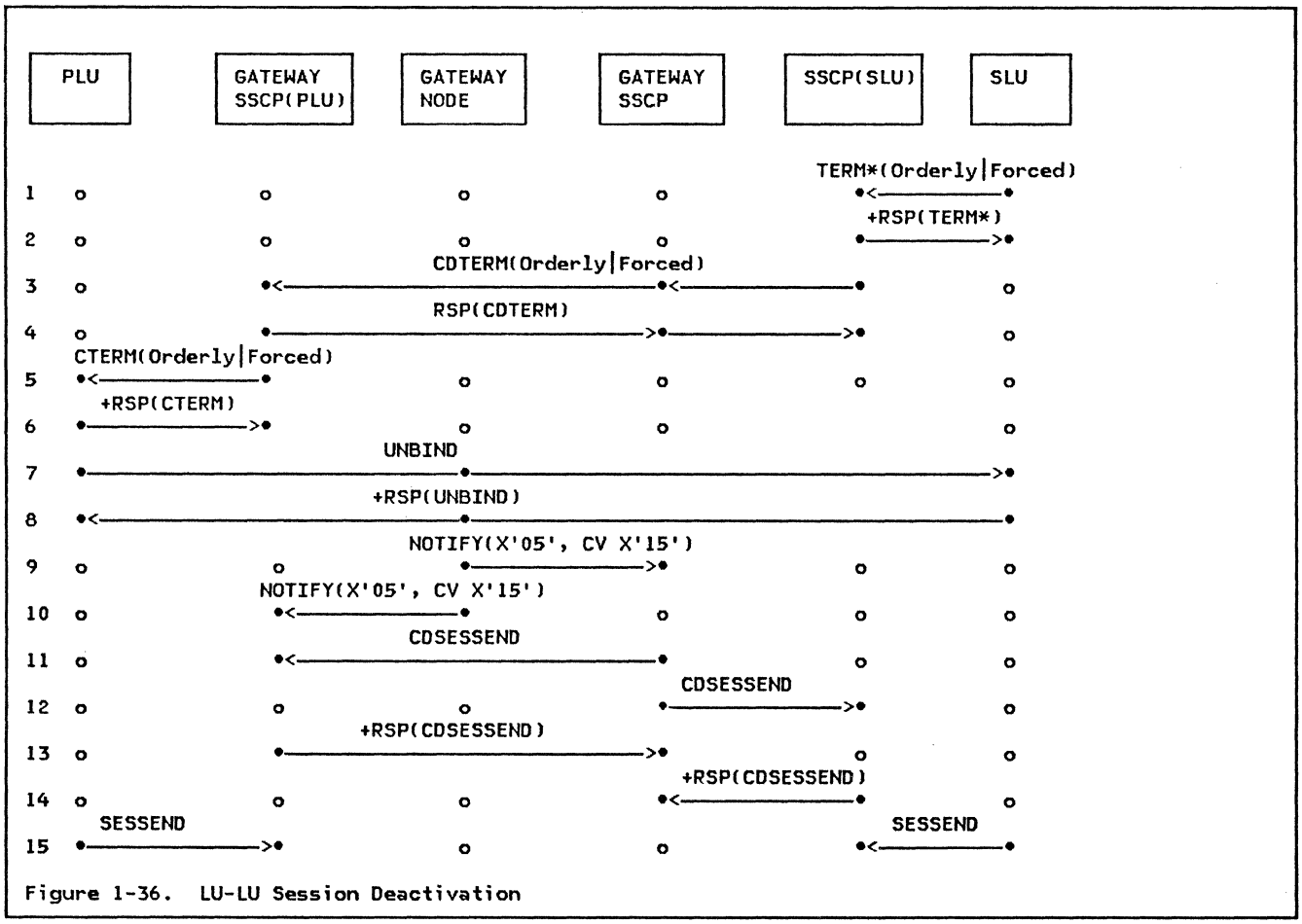


Figure 1-36. LU-LU Session Deactivation

DEACTIVATION OF CROSS-NETWORK LU-LU SESSIONS

Figure 1-36 gives an example of the deactivation of a cross-network LU-LU session. In this case, the SLU starts the procedure by sending a TERM-SELF or TERM-OTHER RU, and a cross-network CDTERM is sent to the SSCP of the PLU (3). In the case of the PLU sending TERM-SELF or TERM-OTHER, the UNBIND is the first cross-network RU.

After the exchange of UNBIND RUs (7, 8), the gateway node sends NOTIFY to its gateway SSCPs (9, 10). The Network-Qualified Address Pair (X'15') control vector on the NOTIFY RU identifies the terminated session. As soon as it receives the NOTIFY, the gateway SSCP on the SLU side sends CDSESSEND to its neighboring SSCPs (11, 12). The gateway SSCP on the PLU side receives the CDSESSEND before it is ready to send CDSESSEND (11), and responds immediately (13).

The gateway SSCP on the PLU side releases its session awareness when it has received NOTIFY from the gateway node (10), SESSEND from the PLU (15), and CDSESSEND from its adjacent SSCP (11). The gateway SSCP on the SLU side releases its session awareness when it has received NOTIFY from the gateway node (9) and responses to CDSESSEND from both neighboring SSCPs (13, 14).

APPENDIX E. REQUEST-RESPONSE UNIT (RU) FORMATS

This appendix defines detailed RU formats. A categorized list of RU abbreviations is presented first, followed by an alphabetic list of request RU format descriptions, a summary of response RUs, and a list of response format descriptions for those positive response RUs that return data in addition to the request code. Two final sections describe control vectors, control lists and session keys, which are used in multiple RUs.

The initial line for each RU in the two RU format description lists is in one of the following formats:

Requests

"RU ABBREVIATION; Origin NAU-->Destination NAU, Normal (Norm) or Expedited (Exp) Flow; RU Category (RU NAME)"

Responses

"RSP(RU ABBREVIATION); Origin NAU-->Destination NAU, Norm or Exp Flow; RU Category"

Notes:

1. "RU Category" is abbreviated as follows:

SC	session control
NC	network control
FMD NS(c)	function management data, network services, configuration services
FMD NS(ma)	function management data, network services, maintenance services
FMD NS(s)	function management data, network services, session services

2. The formats of character-coded FMD NS RUs are implementation dependent.

3. All values for field-formatted RUs that are not defined in this section are reserved.

4. The request code value X'FF' and the NS header values X'(3|7|B|F)F****' and X'**(3|7|B|F)F**' are set aside for implementation internal use, and will not be otherwise defined in SNA.

5. Throughout this appendix the following symbol-string types are used:

   - Symbol-string type A (Assembler oriented): a byte string consisting of one or more EBCDIC upper-case letters (A through Z), numerics (0 through 9), $, #, and @, the first character of which is nonnumeric.

   - Symbol-string type USS ("Unformatted System Services" or character-coded subset of the SNA character set): a byte string consisting of one or more EBCDIC upper-case letters (A through Z), numerics (0 through 9), $, #, @, line feed (X'15'), space (X'40') and the following 11 special characters: '=(),+-*./& with no restriction on the first character.

   - Symbol-string type AE (A extended): a byte string consisting of one or more EBCDIC lower-case letters (a through z), upper-case letters (A through Z), numerics (0 through 9), $, #, @, and period (.), with no restriction on the first character.

   - Symbol-string type GR (EBCDIC graphics): a byte string consisting of one or more EBCDIC characters in the range X'41' through X'FE', with no restriction on the first character.

   - Symbol-string type G (general): a byte string consisting of one or more bytes of binary values 0 through 255.

   The variable to which a type-A, type-AE, or type-GR symbol string is assigned may be longer than the symbol string; in this case, the symbol string is left-justified within the field, which is filled out to the right with space (X'40') characters. Space characters, if present, are not part of the symbol string. If the symbol string is formed from the concatenation of two or more individual symbol strings, such as the fully-qualified LU name, the concatenated symbol string as a whole is left-justified within the field, which is filled

out to the right with space characters. Space characters, if present, are not part of the concatenated symbol string.

6. Throughout this appendix, reserved is used as follows: reserved bits, or fields, are currently set to 0's (unless explicitly stated otherwise); reserved values are those that currently are invalid. Correct usage of reserved fields is enforced by the sender; no receive checks are made on these fields.

7. Throughout this appendix, retired fields and values are those that were once defined by SNA but are no longer defined. To accommodate implementations of back-level SNA, current implementations of SNA treat retired fields as follows: send checks enforce the setting of retired fields to all 0's except where other unique values are required (described individually in this appendix); no receive checks are made on these fields, thereby accepting back-level settings of these fields. Special handling of retired fields, such as echoing or passing on retired fields as received, is discussed where appropriate.

SUMMARY OF REQUEST RU'S BY CATEGORY

SC

*ACTCDRM	*BIND	DACTPU	UNBIND
*ACTPU	DACTCDRM		

NC

NC-ER-TEST-REPLY

FMD NS(c)

CONTACTED	REQACTCDRM	ROUTE-INOP	SETCV
NOTIFY	*RNAA		

FMD NS(ma)

ER-TESTED	*ROUTE-TEST

FMD NS(s)

BINDF	CDSESSTF	*DSRLST	SESSEND
CDCINIT	*CDTERM	JNIT-OTHER	SESSST
*CDINIT	*CINIT	*lNIT-OTHER-CD	TERM-OTHER
CDSESSEND	CLEANUP	INIT-SELF	TERM-SELF
CDSESSSF	CTERM	NOTIFY	UNBINDF
CDSESSST			

* These request RUs require response RUs that, if positive, may contain data in addition to the NS header or request code. See "Summary of Response RU's" on page E-43 and "Positive Response RU's with Extended Formats" on page E-43.

INDEX OF RUS BY NS HEADERS AND REQUEST CODES

Within NC, SC, or any specific FMD NS category, the request code is unique. However, while a request code has only one meaning in a specific category, a given code (e.g., X'05') can represent different requests in separate categories (e.g., NC, and configuration services). DSRLST, NOTIFY, and SETCV are exceptions: these three requests have request codes--X'27', X'20', and X'11', respectively--that are unique across all the FMD NS categories.

FMD NS Headers (Third byte is the request code)

X'010211'	SETCV (FMD NS(c))
X'010280'	CONTACTED
X'010681'	INIT-SELF (Format 0)
X'010683'	TERM-SELF (Format 0)
X'410210'	RNAA
X'410220'	NOTIFY (SSCP-->PU, PU-->SSCP)
X'410289'	ROUTE-INOP
X'41028A'	REQACTCDRM
X'410307'	ROUTE-TEST
X'410386'	ER-TESTED
X'810601'	CINIT
X'810602'	CTERM
X'810620'	NOTIFY (SSCP<-->SSCP, SSCP-->LU)
X'810629'	CLEANUP
X'810680'	INIT-OTHER
X'810681'	INIT-SELF (Format 1)
X'810682'	TERM-OTHER
X'810683'	TERM-SELF (Format 1)
X'810685'	BINDF
X'810686'	SESSST
X'810687'	UNBINDF
X'810688'	SESSEND
X'818627'	DSRLST
X'818640'	INIT-OTHER-CD
X'818641'	CDINIT
X'818643'	CDTERM
X'818645'	CDSESSSF
X'818646'	CDSESSST
X'818647'	CDSESSTF
X'818648'	CDSESSEND
X'81864B'	CDCINIT

SC Request Codes

X'11'	ACTPU
X'12'	DACTPU
X'14'	ACTCDRM
X'15'	DACTCDRM
X'31'	BIND
X'32'	UNBIND

NC Request Codes

X'0A'	NC-ER-TEST-REPLY

REQUEST RU FORMATS

ACTCDRM; SSCP-->SSCP, Exp; SC (ACTIVATE CROSS-DOMAIN RESOURCE MANAGER)

ACTCDRM is sent from one SSCP to another SSCP to activate a session between them and to exchange information about the SSCPs.

0	X'14' request code
1	bits 0-3, format: X'0' (only value defined) bits 4-7, type activation requested: X'1' cold X'2' ERP

2 FM profile
3 TS profile
4-11 Contents ID: eight-character EBCDIC symbolic name that represents implementation and installation dependent information about the SSCP issuing the ACTCDRM; eight space (X'40') characters is the value used if no information is to be conveyed (This field could be used to provide a check for a functional and configurational match between the SSCPs.)
12-17 SSCP ID: a six-byte field that includes the ID of the SSCP issuing the ACTCDRM; the first four bits specify the format for the remaining bits:
bits 0-3, format 0000 (only value defined)
bits 4-7, physical unit type of the node containing the SSCP
bits 8-47, implementation and installation dependent binary identification
18 TS Usage
bits 0-1, reserved
bits 2-7, primary CPMGR receive window size (0 means no pacing of requests flowing to the primary)
19-n One or more control vectors, as described in the section "Control Vectors" on page E-49
Note: The following vector keys may be used in ACTCDRM:
X'06' CDRM control vector
X'09' Activation Request/Response Sequence Identifier control vector
X'13' Gateway Support Capabilities control vector
X'18' SSCP Name control vector

ACTPU; SSCP|PUCP-->PU, Exp; SC (ACTIVATE PHYSICAL UNIT)

ACTPU is sent by the SSCP to activate a session with the PU, and to obtain certain information about the PU.

0 X'11' request code
1 bits 0-3, format:
X'0' Format 0
X'3' Format 3—same as Format 0, except that it always includes one or more control vectors in bytes 9-n (sent only to PU_T4|5s that support ERs and VRs)
bits 4-7, type activation requested:
X'1' cold
X'2' ERP
2 bits 0-3, FM profile:
X'0' FM profile 0
X'5' FM profile 5
bits 4-7, TS profile:
X'1' TS profile 1
X'5' TS profile 5
3-8 A six-byte field that specifies the ID of the SSCP issuing ACTPU; the first four bits specify the format for the remaining bits:
bits 0-3, format: 0000 (only value defined)
bits 4-7, PU type of the node containing the CP
bits 8-47, implementation and installation dependent binary identification
Note: End of Base Format

9-n One or more optional control vectors, as described in the section "Control Vectors" on page E-49
Note: The following vector keys may be used in ACTPU:
X'09' Activation Request/Response Sequence Identifier control vector
X'0B' SSCP-PU Session Capabilities control vector
X'18' SSCP Name control vector

BIND; PLU-->SLU, Exp; SC (BIND SESSION)

BIND is sent from a primary LU to a secondary LU to activate a session between the LUs. The secondary LU uses the BIND parameters to help determine whether it will respond positively or negatively to BIND.

0 X'31' request code
1 bits 0-3, format: 0000 (only value defined)
bits 4-7, type:
0000 negotiable (only value defined for LU 6.2)
0001 nonnegotiable
2 FM profile:
X'02' FM profile 2

X'03' FM profile 3
X'04' FM profile 4
X'07' FM profile 7
X'12' FM profile 18
X'13' FM profile 19 (only value defined for LU 6.2)

3 TS profile:
X'02' TS profile 2
X'03' TS profile 3
X'04' TS profile 4
X'07' TS profile 7 (only value defined for LU 6.2)

FM Usage—Primary LU Protocols for FM Data

4 bit 0, chaining use selection:
0 only single-RU chains allowed from primary LU half-session
1 multiple-RU chains allowed from primary LU half-session (only value defined for LU 6.2)

bit 1, request control mode selection:
0 immediate request mode (only value defined for LU 6.2)
1 delayed request mode

bits 2-3, chain response protocol used by primary LU half-session for FMD requests; chains from primary will ask for:
00 no response
01 exception response
10 definite response
11 definite or exception response (only value defined for LU 6.2)

bit 4, 2-phase commit for sync point (reserved if any TS profile other than 4):
0 2-phase commit not supported
1 2-phase commit supported

bit 5, reserved

bit 6, compression indicator (reserved for LU 6.2):
0 compression will not be used on requests from primary
1 compression may be used

bit 7, send End Bracket indicator:
0 primary will not send EB (only value defined for LU 6.2)
1 primary may send EB

FM Usage—Secondary LU Protocols for FM Data

5 bit 0, chaining use selection:
0 only single-RU chains allowed from secondary LU half-session
1 multiple-RU chains allowed from secondary LU half-session (only value defined for LU 6.2)

bit 1, request control mode selection:
0 immediate request mode (only value defined for LU 6.2)
1 delayed request mode

bits 2-3, chain response protocol used by secondary LU half-session for FMD requests; chains from secondary will ask for:
00 no response
01 exception response
10 definite response
11 definite or exception response (only value defined for LU 6.2)

bit 4, 2-phase commit for sync point (reserved if any TS profile other than 4):
0 2-phase commit not supported
1 2-phase commit supported

bit 5, reserved

bit 6, compression indicator (reserved for LU 6.2):
0 compression will not be used on requests from secondary
1 compression may be used

bit 7, send End Bracket indicator:
0 secondary will not send EB (only value defined for LU 6.2)
1 secondary may send EB

FM Usage—Common LU Protocols

6 bit 0, session segmenting support:
0 this LU supports reception of segments on this session
1 this LU does not support reception of segments on this session; the BIND sender and receiver set the maximum RU sizes, in bytes 10-11 of BIND and RSP(BIND), so that segmenting will not occur on the peripheral link for this half-session

bit 1, FM header usage:
0 FM headers not allowed
1 FM headers allowed (only value defined for LU 6.2)

bit 2, brackets usage and reset state:
0 brackets not used if neither primary nor secondary will send EB, i.e., if byte 4, bit 7 = 0 and byte 5, bit 7 = 0; brackets are used and bracket state managers' reset states are INB (1) if either primary or secondary, or both, may send EB, i.e., if byte 4, bit 7 = 1 or byte 5, bit 7 = 1; or (2) if FM profile 19 is specified (only value defined for LU 6.2)

1 brackets are used and bracket state managers' reset states are BETB

bit 3, bracket termination rule selection (reserved if brackets not used, i.e., if byte 6, bit 2 = 0, byte 4, bit 7 = 0, and byte 5, bit 7 = 0; or if FM profile is not 19):
0 Rule 2 (unconditional termination) will be used during this session
1 Rule 1 (conditional termination) will be used during this session (only value defined for LU 6.2)

bit 4, alternate code set allowed indicator:
0 alternate code set will not be used
1 alternate code set may be used

bit 5, sequence number availability for sync point resynchronization (reserved if any TS profile other than 4 is used):
0 sequence numbers not available
1 sequence numbers available
Note: Sequence numbers are transaction program sequence numbers from the previous activation of the session with the same session name; they are associated with the last acknowledged requests and any pending requests to commit a unit of work. If no previous activation existed, the numbers are 0, and this bit is set to 0.

bit 6, BIS sent (reserved for TS profiles other than 4):
0 BIS not sent
1 BIS sent

bit 7, BIND response queue capability:
0 BIND response cannot be held/queued
1 BIND sender allows BIND receiver to queue BIND and withhold BIND response for an indefinite period
Note: BIND sender may provide a timer or operator interface to send UNBIND if session activation time exceeds BIND sender's limits. BIND queuing is terminated by sending UNBIND to the BIND receiver.

7 bits 0-1, normal-flow send/receive mode selection:
00 full-duplex
01 half-duplex contention
10 half-duplex flip-flop (only value defined for LU 6.2)
11 reserved

bit 2, recovery responsibility (reserved if normal flow send/receive mode is FDX, i.e., if byte 7, bits 0-1 = 00):
0 contention loser responsible for recovery (see byte 7, bit 3 for specification of which half-session is the contention loser)
1 symmetric responsibility for recovery (only value defined for LU 6.2)

bit 3, contention winner/loser (reserved if normal flow send/receive mode is FDX, i.e., if byte 7, bits 0-1 = 00; or if the normal flow send/receive mode is HDX-FF, brackets are not used, FM profile is not 19, and symmetric responsibility for recovery is used, i.e., if byte 7, bits 0-1 = 10, byte 4, bit 7 = 0, byte 5, bit 7 = 0, byte 6, bit 2 = 0, and byte 7, bit 2 = 1):
0 secondary is contention winner and primary is contention loser
1 primary is contention winner and secondary is contention loser
Note: Contention winner is also brackets first speaker if brackets are used.

bits 4-5, alternate code processing identifier (reserved unless Alternate Code Set Allowed indicator [byte 6, bit 4] is 1):
00 process alternate code FMD RUs as ASCII-7
01 process alternate code FMD RUs as ASCII-8 (only value defined for LU 6.2)
Note: When the Alternate Code Processing Identifier indicator is set to the value 01, the entire FMD request RU is to be translated using the transforms defined by the ANSI X3.26 Hollerith Card Code.

bit 6, reserved

bit 7, half-duplex flip-flop reset states (reserved unless (1) normal-flow send/receive mode is half-duplex flip-flop (byte 7, bits 0-1 = 10) and (2) brackets are not used or bracket state manager's reset state is INB (byte 6, bit 2 = 0)):
0 HDX-FF reset state is RECEIVE for the primary and SEND for the secondary (e.g., the secondary sends normal-flow requests first after session activation)
1 HDX-FF reset state is SEND for the primary and RECEIVE for the secondary (e.g., the primary sends normal-flow requests first after session activation) (only value defined for LU 6.2)

TS Usage

8 bit 0, staging indicator for secondary TC to primary TC normal flow:
0 pacing in this direction occurs in one stage
1 pacing in this direction occurs in more than one stage
Note: The meanings of 0 and 1 are reversed from the staging indicator for primary TC to secondary TC.

bit 1, reserved

bits 2-7, secondary TC's send window size: 0 means no pacing of requests flowing from the secondary

9 bits 0-1, reserved
bits 2-7, secondary TC's receive window size: a value of 0 causes the boundary function to substitute the value set by a system definition pacing parameter (if the system definition includes such a parameter) before it sends the BIND RU on to the secondary half-session; a value of 0 received at the secondary is interpreted to mean no pacing of requests flowing to the secondary

10 Maximum RU size sent on the normal flow by the secondary half-session: if bit 0 is set to 0 then no maximum is specified and the remaining bits 1-7 are ignored; if bit 0 is set to 1, the byte is interpreted as X'ab' = a*2**b (Notice that, by definition, a≥8 and therefore X'ab' is a normalized floating point representation.) See Figure E-1 on page E-10 for all possible values.

11 Maximum RU size sent on the normal flow by the primary half-session: identical encoding as described for byte 10

12 bit 0, staging indicator for primary TC to secondary TC normal flow:
1 pacing in this direction occurs in one stage
0 pacing in this direction occurs in two stages
Note: The meanings of 0 and 1 are reversed from the staging indicator for secondary to primary TC.
bit 1, reserved
bits 2-7, primary TC's send window size: a value of 0 causes the value set by a system definition pacing parameter (if the system definition includes such a parameter) to be assumed for the session; if this is also 0, it means no pacing of requests flowing from the primary (For single-stage pacing in the primary-to-secondary direction, this field is redundant with, and will indicate the same value as, the secondary TC's receive window size—see byte 9, bits 2-7, above.)

13 bits 0-1, reserved
bits 2-7, primary TC's receive window size: a value of 0 means no pacing of requests flowing to the primary (For single-stage pacing in the secondary-to-primary direction, this field is redundant with, and will indicate the same value as, the secondary TC's send window size—see byte 8, bits 2-7, above.)

PS Profile

14 bit 0, PS Usage field format:
0 basic format (only value defined)
bits 1-7, LU type:
0000000 LU type 0
0000001 LU type 1
0000010 LU type 2
0000011 LU type 3
0000100 LU type 4
0000110 LU type 6
0000111 LU type 7

PS Usage characteristics

Note: The following format for bytes 15-25 applies only to LU 6.2; for information on PS usage bytes 15-25 for other than LU 6.2 (indicated by byte 14, bits 1-7 = 0000110 and byte 15 = 00000010), see SNA—Sessions Between Logical Units.

15 LU-6 level:
X'02' Level 2 (i.e., LU 6.2)

16-22 Reserved

23 bits 0-2, retired
bit 3, conversation-level security support:
0 Access Security Information field will not be accepted on incoming FMH-5s
1 Access Security Information field will be accepted on incoming FMH-5s
bits 4-5, reserved
bit 6, already-verified function support:
0 Already Verified indicator will not be accepted on incoming FMH-5s
1 Already Verified indicator will be accepted on incoming FMH-5s
bit 7, reserved

24 bit 0, reserved
bits 1-2, synchronization level:
01 confirm is supported
10 confirm, sync point, and backout are supported
bit 3, reserved
bits 4-5, responsibility for session reinitiation:
00 operator controlled
01 primary half-session will reinitiate
10 secondary half-session will reinitiate
11 either may reinitiate
bit 6, parallel session support for LU-LU pair:
0 not supported
1 supported
bit 7, Change Number of Sessions GDS variable flow support (set to 1 if byte 24, bit 6 = 1):
0 not supported

1 supported

25 Reserved

End of PS Usage Field

26-k Cryptography Options

26 bits 0-1, private cryptography options (reserved for LU 6.2):
- 00 no private cryptography supported
- 01 private cryptography supported: the session cryptography key and cryptography protocols are privately supplied by the end user

bits 2-3, session-level cryptography options:
- 00 no session-level cryptography supported
- 01 session-level selective cryptography supported; all cryptography key management is supported by the SSCP and LU; exchange (via +RSP(BIND)) and verification (via CRV) of the cryptography session-seed value is supported by the LUs for the session; all FMD requests carrying ED are enciphered/deciphered by the TCs
- 10 reserved
- 11 session-level mandatory cryptography supported; all cryptography key management is supported by the SSCP and LU; exchange (via +RSP(BIND)) and verification (via CRV) of the cryptography session-seed value is supported by the LUs for the session; all FMD requests are enciphered/deciphered by TC

Note: Only values 00 and 11 are defined for LU 6.2.

bits 4-7, session-level cryptography options field length:
- X'0' no session-level cryptography specified; following additional cryptography options fields (bytes 27-k) omitted
- X'9' session-level cryptography specified; additional options follow in next nine bytes

27 bits 0-1, session cryptography key encipherment method:
- 00 session cryptography key enciphered under SLU master cryptography key using a seed value of 0 (only value defined)

bits 2-4, reserved

bits 5-7, cryptography cipher method:
- 000 block chaining with seed and cipher text feedback, using the Data Encryption Standard (DES) algorithm (only value defined)

28-k Session cryptography key enciphered under secondary LU master cryptography key; an eight-byte value that, when deciphered, yields the session cryptography key used for enciphering and deciphering FMD requests

k+1-m Primary LU Name Field

k+1 Length of primary LU name

Note: X'00' = no primary LU name present.

k+2-m Primary LU name or, if the secondary LU issued the INIT-SELF (or INIT-OTHER), the uninterpreted name as carried in that RU (and also in CDINIT for a cross-domain session)

m+1-n User Data Field

m+1 Length of user data

Note: X'00' = no User Data field present; if unstructured user data present, values 1 to 65 are valid.

m+2-n User data

m+2 User data key:

X'00' structured subfields follow (only value defined for LU 6.2)

Note: Individual structured subfields may be omitted entirely. When present, they appear in ascending subfield-number order.

¬X'00' first byte of unstructured user data

- For unstructured user data:

m+3-n Remainder of unstructured user data

- For structured user data:

m+3-n Structured subfields (For detailed definitions, see "User Data Structured Subfield Formats" on page E-41.)

n+1-p User Request Correlation Field

n+1 Length of user request correlation (URC) field (values 0 to 12 are valid)

Note: X'00' = no URC present.

n+2-p URC: LU-defined identifier (present only if carried in INIT from SLU)

p+1-r Secondary LU Name Field (present only in negotiable BIND)

p+1 Length of secondary LU name

Note: X'00' = no secondary LU name present.

p+2-r Secondary LU name

Note 1: The length of the BIND RU cannot exceed 256 bytes, lest a negative response be returned.

Note 2: If the last byte of a format 0 request is a length field and that field is 0, that byte may be omitted from the BIND request.

	Mantissa (a)							
Exponent (b)	8	9	A (10)	B (11)	C (12)	D (13)	E (14)	F (15)
0	8	9	10	11	12	13	14	15
1	16	18	20	22	24	26	28	30
2	32	36	40	44	48	52	56	60
3	64	72	80	88	96	104	112	120
4	128	144	160	176	192	208	224	240
5	256	288	320	352	384	416	448	480
6	512	576	640	704	768	832	896	960
7	1024	1152	1280	1408	1536	1664	1792	1920
8	2048	2304	2560	2816	3072	3328	3584	3840
9	4096	4608	5120	5632	6144	6656	7168	7680
A (10)	8192	9216	10240	11264	12288	13312	14336	15360
B (11)	16384	18432	20480	22528	24576	26624	28672	30720
C (12)	32768	36864	40960	45056	49152	53248	57344	61440
D (13)	65536	73728	81920	90112	98304	106496	114688	122880
E (14)	131072	147456	163840	180224	196608	212992	229376	245760
F (15)	262144	294912	327680	360448	393216	425984	458752	491520

Note: A value of X'ab' in byte 10 or byte 11 of BIND represents a•2**b. For example, X'C5' represents (in decimal) 12•2**5 = 384.

Figure E-1. RU Sizes Corresponding to Values X'ab' in BIND

BINDF; PLU-->SSCP, Norm; FMD NS(s) (BIND FAILURE)

BINDF is sent, with no-response requested, by the PLU to notify the SSCP that the attempt to activate the session between the specified LUs has failed.

0-2 X'810685' NS header
3-6 Sense data
7 Reason:
bit 0, reserved
bit 1, 1 BIND error in reaching SLU
bit 2, 1 setup reject at PLU
bit 3, 1 setup reject at SLU
bits 4-7, reserved
8-m Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

CDCINIT; SSCP-->SSCP, Norm; FMD NS(s) (CROSS-DOMAIN CONTROL INITIATE)

CDCINIT passes information about the SLU from the SSCP(SLU) to the SSCP(PLU) and requests that the SSCP(PLU) send CINIT to the PLU.

0-2 X'81864B' NS header
3 Format
bits 0-3, X'0' Format 0: session pair identified by network addresses
X'1' Format 1: session pair identified by a session key
bits 4-7, reserved
4 Reserved
5-12 PCID: a unique value used as a session identifier
13-m Session Pair Identifier
- For format 0:

13-14 Network address of PLU
15-16(=m) Network address of SLU
- For format 1:

13-m Session key, as described in the section "Session Keys" on page E-58
Note: The following session key is used:
X'15' network-qualified address pair: PLU and SLU, respectively (only value defined)
m+1-m+2 Length, in binary, of BIND image
m+3-n BIND image: bytes 1-p of the BIND RU (see BIND format description), i.e., through the URC field
Notes on BIND image:
- If the last byte of the BIND image is a length field and that length field is 0, that byte may be omitted from the BIND image.
- For SLUs not in the sending SSCP's node, the session cryptography key is enciphered under the SLU master cryptography key; for SLUs in the SSCP's node, the sending SSCP enciphers the session cryptography key under a dummy SLU master cryptography key.

n+1-n+2 Length, in binary, of LU or non-SNA device characteristics field and format—i.e., bytes n+3-p (X'00' = no characteristics/format field.)
n+3 LU or non-SNA device characteristics format:
X'01' Format 1: access method unique device characteristics (only value defined)
n+4-p LU or non-SNA device specifications (See CINIT for the format of this field.)
p+1 Length, in binary, of session cryptography key
Note: X'00' = no Session Cryptography Key field is present.
p+2-q Session cryptography key for primary: the session cryptography key, enciphered under the cross-domain cryptography key defined for the SSCP(SLU) to SSCP(PLU) direction (a different cross-domain cryptography key is defined for the opposite direction) and using a seed value of 0

CDINIT; SSCP-->SSCP, Norm; FMD NS(s) (CROSS-DOMAIN INITIATE)

CDINIT from the SSCP(OLU) requests that the SSCP(DLU) assist in initiating an LU-LU session for the specified (OLU,DLU) pair.

0-2 X'818641' NS header
3 Format
bits 0-3, X'0' Format 0: used when Type = I, I/Q, or Q; bytes 17-18 are reserved and no COS fields are specified for Format 0; Format 0 includes bytes 0 through s

X'1' Format 1: used when Type = DQ and specifies a subset of the parameters; Format 1 includes bytes 0 through 18
X'2' Format 2: specifies COS fields and an additional OLU status (byte 6, bit 5) in addition to the parameters in Format 0; Format 2 includes bytes 0 through (s+9)
X'3' Format 3: used when Type = I, I/Q, or Q; includes bytes 0 through (s+9) as in Format 2; control vectors are appended following byte (s+9)
X'4' Format 4: used when Type = DQ and specifies a subset of the parameters; Format 4 includes Format 1, plus X'15' Network-Qualified Address Pair session key

bits 4-7, reserved

Note: Formats 0, 2, and 3 continue (See Format 1 and 4 continuation below)

4 Type
bits 0-1, 00 reserved
01 initiate only (I)
10 queue only (Q)
11 initiate or queue (I/Q)
bits 2-3, retired
bit 4, reserved
bit 5, retired
bit 6, 0 DLU is PLU
1 OLU is PLU
bit 7, retired

5 Queuing Conditions For DLU (reserved when Type = I)
bit 0, 0 do not queue if session limit exceeded
1 queue if session limit exceeded
bit 1, 0 do not queue if DLU is not currently able to comply with the PLU/SLU specification (as given in byte 4, bit 6)
1 queue if DLU is not currently able to comply with the PLU/SLU specification
bit 2, reserved
bit 3, 0 do not queue if no SSCP(DLU)-DLU path
1 queue if no SSCP(DLU)-DLU path
bit 4, reserved
bits 5-6, queuing position/service
00 put this request on the bottom of the queue (this request is put at the bottom of the queue and serviced last)
01 enqueue this request FIFO
10 enqueue this request LIFO
11 reserved
bit 7, reserved
Note: Queuing is not done if the DLU is unknown, or if the domain of the DLU is in takedown status.

6 OLU status
bit 0, reserved
bit 1, 0 LU is not available
1 LU is available
bits 2-3, (used if LU is not available; otherwise, reserved)
00 LU session limit exceeded
01 reserved
10 LU is not currently able to comply with the PLU/SLU specification
11 reserved
bit 4, 0 existing SSCP to LU path
1 no existing SSCP to LU path (connectivity is lost)
bit 5, (reserved in format 0)
0 UNBIND and SESSEND cannot be sent by the LU or by its boundary function (if any)
1 UNBIND and SESSEND may be sent by the LU or by its boundary function (if any)
bits 6-7, 01 OLU is PLU
10 OLU is SLU

7-14 PCID: a unique value used as a session identifier

15-16 Network address of OLU (retired for format 3)

17-18 Reserved

19 bit 0, INITIATE origin:
0 ILU is OLU
1 ILU is not OLU
bits 1-2, reserved
bit 3, initiator:
0 network user is the initiator
1 network manager is the initiator
bits 4-7, reserved

20 NOTIFY specification:
bits 0-1, NOTIFY(X'01') condition

00 do not send NOTIFY to LUs in session with DLU
01 reserved
10 send NOTIFY to all LUs in session with DLU only if the CDINIT request is queued
11 reserved

bits 2-5, reserved

bits 6-7, request for notification of resource availability: if a resource required for setup of the requested session is temporarily unavailable and subsequently becomes available to one or more OLUs in the domain of the SSCP(OLU), NOTIFY NS(s) key X'07' or X'08' is requested to notify the SSCP(OLU) of the resource's availability
00 do not send NOTIFY to the SSCP(OLU)
01 send a general NOTIFY NS(s) key X'07' or X'08' that does not specify the OLU; the SSCP(OLU) will consider the resource to have become available to any and all OLUs in its domain
10 send NOTIFY NS(s) key X'07' or X'08' specifying the OLU to which the resource has become available
11 send NOTIFY NS(s) key X'07' or X'08' with or without specifying the OLU, depending on the scope of the resource's availability

21-28 Mode name: an eight-character symbolic name (implementation and installation dependent) that identifies the set of rules and protocols to be used for the session; used by the SSCP(SLU) to select the BIND image to be used by the SSCP(PLU) to build the CINIT request
Note: For format 3 (cross-network), this mode name represents the mode name as known in the network of the OLU.

29-m Network Name of DLU
29 Type: X'F3' logical unit
30 Length, in binary, of symbolic name
31-m Symbolic name, in EBCDIC characters

m+1-m+2 Retired: set to X'0000'

m+3-q User Field
m+3 Length, in binary, of user data
Note: X'00' = no user data is present.

m+4-q User data: user-specific data that is passed to the primary LU on the CINIT request
m+4 User data key
X'00' structured subfields follow
¬X'00' first byte of unstructured user data
Note: Individual structured subfields may be omitted entirely. When present, they appear in ascending field number order.

- For unstructured user data

m+5-q Remainder of unstructured user data

- For structured user data

m+5-q Structured subfields (For detailed definitions, see "User Data Structured Subfield Formats" on page E-41.)

q+1-r Network Name of OLU
q+1 Type: X'F3' logical unit
q+2 Length, in binary, of symbolic name
q+3-r Symbolic name in EBCDIC characters

r+1-s Uninterpreted Name of DLU
r+1 Type: X'F3' logical unit
r+2 Length, in binary, of DLU name
Note: X'00' = no uninterpreted name is present.
r+3-s EBCDIC character string; when present, this name is obtained from the preceding INIT-SELF or INIT-OTHER (when ILU=SLU)

Note: End of Format 0; Formats 2 and 3 continue below.

s+1 COS name initialization indicators:
bit 0, 0 COS name not received from ILU (see bits 1-2)
1 COS name received from ILU
bits 1-2, (reserved if byte s+1, bit 0 = 1)
01 SSCP(DLU) is to initialize COS name (DLU is SLU)
10 SSCP(OLU) has initialized COS name (OLU is SLU)
bits 3-7, reserved

s+2-s+9 COS name (If byte s+1, bit 0 = 0 and bits 1-2 = 01 this field carries unpredictable values and is not used): symbolic name of class of service in EBCDIC characters
Note: For format 3 (cross-network) this COS name represents the COS name as known in the network of the OLU.

Note: End of Format 2; Format 3 continues below:

s+10-t One or more control vectors, as described in the section "Control Vectors" on page E-49
Note: Vector key X'1A' is required for format 3; the other vectors are optional. If present, they appear in the order specified below.

X'1A' NAU Address control vector: this control vector contains the OLU network address

Note: Between gateways, the OLU address is an address recognized in the subnetwork on the DLU side of the sending gateway. Within a gateway, the OLU address is an address recognized in the network on the OLU side of the gateway node, until the SSCP with address alias responsibility is reached. This SSCP replaces the received address with an address recognized in the network on the DLU side of the gateway node.

Note: The network ID is identified in the X'19' control vector for the OLU.

X'14' Session Initiation control vector:
X'19' Resource Identifier control vector (for destination LU):
X'19' Resource Identifier control vector (for origin LU):

Note: End of Format 3; Formats 1 and 4 continue below.

4 Type
bits 0-1, 00 dequeue (DQ)
bits 2-3, 00 leave on queue if dequeue retry is unsuccessful
01 remove from queue if dequeue retry is unsuccessful
10 do not retry—remove from queue
11 reserved
bit 4, reserved
bits 5-6, 00 LU2 is PLU
01 LU2 is SLU
10 reserved
11 reserved
bit 7, reserved

5 Queuing Status (For LU associated with SSCP sending CDINIT(DQ))
bits 0-4, reserved
bits 5-6, 00 request on bottom of queue
01 enqueued request FIFO
10 enqueued request LIFO
11 reserved
bit 7, reserved

6 LU Status (For LU associated with SSCP sending CDINIT(DQ))
bit 0, reserved
bit 1, 0 LU is unavailable
1 LU is available
bits 2-5, reserved
bits 6-7, 01 LU is PLU
10 LU is SLU

7-14 PCID: a unique value used as a session identifier
Note: This PCID must be the same as in the original CDINIT request.

15-16 Network address of LU1 (retired for format 4)

17-18 Network address of LU2 (retired for format 4)

Note: End of Format 1; Format 4 continues below.

19-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'15' network-qualified address pair: LU1 and LU2, respectively (only value defined)

CDSESSEND; SSCP(PLU)<-->SSCP(SLU), Norm; FMD NS(s) (CROSS-DOMAIN SESSION ENDED)

CDSESSEND notifies the SSCP that the LU-LU session identified by the Session Key has been successfully deactivated.

0-2 X'818648' NS header

3-10 PCID: a unique value used as a session identifier
Note: PCID is used in CDSESSEND only to aid in PIU trace correlation.

11 bits 0-3, format: X'0' (only value defined)
bits 4-7, reserved

12-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' network name pair: PLU and SLU, respectively
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

CDSESSSF; SSCP(PLU)-->SSCP(SLU), Norm; FMD NS(s) (CROSS-DOMAIN SESSION SETUP FAILURE)

CDSESSSF notifies the SSCP(SLU) that the LU-LU session initiation identified by the Session Key Content field and the specified PCID for the initiation procedure has failed.

0-2 X'818645' NS header
3-10 PCID: a unique value used as a session identifier
11-14 Sense data
15 Reason
bit 0, 1 CINIT error in reaching PLU
bit 1, 1 BIND error in reaching SLU
bit 2, 1 setup reject at PLU
bit 3, 1 setup reject at SLU
bits 4-7, reserved
16-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' network name pair: PLU and SLU, respectively
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

CDSESSST; SSCP(PLU)-->SSCP(SLU), Norm; FMD NS(s) (CROSS-DOMAIN SESSION STARTED)

CDSESSST notifies the SSCP(SLU) that the LU-LU session identified by the Session Key Content field and the specified PCID for the initiation procedure has been successfully activated.

0-2 X'818646' NS header
3-10 PCID: a unique value used as a session identifier
11 Reserved
12-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' network name pair: PLU and SLU, respectively
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

CDSESSTF; SSCP(PLU)-->SSCP(SLU), Norm; FMD NS(s) (CROSS-DOMAIN SESSION TAKEDOWN FAILURE)

CDSESSTF notifies the SSCP(SLU) that the termination procedure for the LU-LU session identified by the Session Key has failed.

0-2 X'818647' NS header
3-10 PCID: a unique value used as a session identifier
Note: PCID is used in CDSESSTF only to aid in PIU trace correlation.
11-14 Sense data
15 Reason:
bit 0, 1 CTERM error in reaching PLU
bit 1, 1 UNBIND error in reaching SLU
bit 2, 1 takedown reject at PLU
bits 3-7, reserved
16-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' network name pair: PLU and SLU, respectively
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

CDTERM; SSCP(OLU)-->SSCP(DLU), Norm; FMD NS(s) (CROSS-DOMAIN TERMINATE)

CDTERM from the SSCP(OLU) requests that the SSCP(DLU) assist in the termination of the cross-domain LU-LU session identified by the Session Key and the Type byte of the RU. Each SSCP executes that portion of termination processing that relates to the LU in its domain.

0-2 X'818643' NS header
3 bits 0-3, 0000 Format 0 (only value defined)
bits 4-7, reserved
4 Type:
bits 0-1, 00 request applies to active and pending-active sessions
01 request applies to active, pending-active, and queued sessions
10 request applies to queued sessions only
11 request applies to pending and queued sessions only
bit 2, reserved if byte 4, bit 7 = 1; otherwise:
0 forced termination, session to be deactivated immediately and unconditionally
1 orderly termination, permitting an end-of-session procedure to be executed at the PLU before the session is deactivated

bit 3, 0 do not send DACTLU to DLU; another session initiation request will be sent for DLU
1 send DACTLU to DLU when appropriate; no further session initiation request will be sent (from this sender) for DLU
bit 4, reserved
bits 5-6, retired
bit 7, 0 orderly or forced (see byte 4, bit 2)
1 cleanup

5-12 PCID: a unique value used as a session identifier
Note: This PCID is used in CDTERM only to aid in PIU trace correlation.

13 Reason:
bit 0, 0 network user
1 network manager
bit 1, 0 normal
1 abnormal
bits 2-7, reserved

14-15 Reserved

16-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'05' PCID: generated by the SSCP(ILU)
X'06' network name pair: OLU and DLU, respectively
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

n+1-n+2 Retired

CINIT; SSCP-->PLU, Norm; FMD NS(s) (CONTROL INITIATE)

CINIT requests the PLU to attempt to activate, via a BIND request, a session with the specified SLU.

0-2 X'810601' NS header

3 Format
bits 0-3, 0000 Format 0 (only value defined)
Note: CINIT format 0 may carry control vectors at the end of the basic RU.
bits 4-7, reserved

4 bit 0, INITIATE origin:
0 ILU is OLU
1 ILU is not OLU
bit 1, reserved
bit 2, 0 SLU is OLU
1 PLU is OLU
bit 3, initiator:
0 network user is the initiator
1 network manager is the initiator
bits 4-7, reserved

5-9 Session key, as described in the section "Session Keys" on page E-58
Note: The following session key is used:
X'07' network address pair: PLU and SLU, respectively
Note: If control vector X'15' is supported by the LU, then bytes 5-9 are reserved; otherwise, these bytes contain session key X'07'.

10-11 Length, in binary, of BIND Image field

12-m BIND image: bytes 1-p of the BIND RU, i.e., through the URC field (see BIND format description)
Note: The URC Length field is included, even if it is set to 0.

m+1-n Name of SLU

m+1 Type: X'F3' logical unit

m+2 Length, in binary, of symbolic name

m+3-n Symbolic name, in EBCDIC characters

n+1-n+2 Retired:

n+3-r User Field (from INITIATE RU)

n+3 Length, in binary, of user data
Note: X'00' = no user data is present.

n+4-r User data: user-specific data

n+4 User data key:
X'00' structured subfields follow
¬X'00' first byte of unstructured user data
Note: Individual structured subfields may be omitted entirely. When present, they appear in ascending field number order.

- For unstructured user data

n+5-r Remainder of unstructured user data

- For structured user data

n+5-r Structured subfields (For detailed definitions, see "User Data Structured Subfield Formats" on page E-41.)

r+1-s LU or Non-SNA Device Specifications
r+1-r+2 Length, in binary, of characteristics field, including both format and characteristics fields—i.e., bytes r+3-s
Note: X'0000' = no Format and no Characteristics fields are present.
r+3-s Characteristics field
r+3 Characteristics format:
X'01' device characteristics (only value defined)
r+4-s LU or Non-SNA Device Characteristics
- Format X'01': (This format represents an access-method-unique LU/device characteristics definition. For more specific information refer to access method implementation documentation.)

r+4 Scheduling information:
X'80' input device
X'40' output device
X'20' conversational mode
X'10' reserved
x'08' start print sensitive
X'04' reserved
X'02' additional information provided (always on)
X'01' specific poll=on general poll=off
r+5 Device type:
X'00' undefined device type
X'04' 2741
X'08' WTTY
X'10' 115A
X'20' TWX (33-35)
X'30' 83B3
X'40' 2740
X'80' 1050
X'90' 2780
X'19' 3277
X'1A' 3284
X'1B' 3286/3288
X'1C' 3275
X'91' 3780
X'6D' SNA logical unit
r+6 Model information:
X'00' Model 1
X'01' Model 2
r+7 Feature information:
bits 0-1, 00 SDLC
01 start/stop
10 BSC
11 reserved
bits 2-7, X'20' XMIT interrupt feature
X'10' SWITCHED LINE = ON; LEASED LINE = OFF
X'08' attention
X'04' checking
X'02' station control
X'01' selector pen
r+8 Physical device address
r+9 Miscellaneous flags:
X'80' SNA compatible application program interface (always on)
X'40' non-SNA application program interface (always off)
X'20' buffered
X'10' continue mode
X'08' contention mode
X'04' inhibit mode (text timeout)
X'02' end-to-end control
X'01' 3270 extended data stream requiring BSC transparency
r+10 Device data stream compatibility characteristics: (This field is used in conjunction with the Device Type field, r+5, when that field is set to X'6D': SNA logical unit; otherwise, it is reserved.):
X'00' no data stream characteristics defined here
X'04' 2741
X'08' WTTY
X'10' 115A
X'20' TWX (33-35)
X'30' 83B3
X'40' 2740
X'80' 1050
X'90' 2780
X'19' 3277
X'1A' 3284

X'1B' 3286/3288
X'1C' 3275
X'91' 3780
X'A0'-X'FF' available for installation-defined use

r+11 Reserved

r+12-r+16 Screen size (see the PS Usage field in the BIND RU for format)

r+17-s Work Area (This field is optional—if not present, s = r+16.):

r+17 Work area format
X'00' unformatted
X'01' TCAM format

r+18-s Work area excluding format

s+1 Length of Session Cryptography Key field
Note: X'00' = no Session Cryptography Key field present.

s+2-t Session Cryptography Key field: session cryptography key enciphered under PLU master cryptography key

Note: End of base RU

t+1-u Control vector, as described in the section "Control Vectors" on page E-49
Note: The following vector keys are used in CINIT:
X'0D' Mode/Class of Service/Virtual Route List
X'15' network-qualified address pair: PLU and SLU, respectively

CLEANUP; SSCP-->PLU|SLU, Norm; FMD NS(s) (CLEAN UP SESSION)

> CLEANUP is sent by the SSCP to an LU (in a subarea node or BF for peripheral LU) requesting that the LU or BF attempt to deactivate the session for the specified (PLU,SLU) network address pair.

0-2 X'810629' NS header

3 bits 0-3, 0000 Format 0 (only value defined)
bits 4-7, reserved

4 Reserved

5 Reason:
bit 0, 0 network user
1 network manager
bit 1, 0 normal
1 abnormal
bits 2-7, reserved

6-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' uninterpreted name pair: PLU and SLU, respectively
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

CONTACTED; PU_T4|5-->SSCP, PU-->PUCP, Norm; FMD NS(c) (CONTACTED)

> CONTACTED is issued by the PU to indicate to the SSCP the completion of the DLC contact procedure. A status parameter conveyed by this request informs SSCP configuration services whether or not the contact procedure was successful; if not successful, the status indicates whether an adjacent node load is required or whether an error occurred on the contact procedure.

0-2 X'010280' NS header

3-4 Element address of adjacent link station in the node being contacted, if ENA is supported; otherwise, its network address

5 Status of adjacent link station or node associated with adjacent link station:
X'01' loaded (no field follows)
X'02' load required (no field follows)
X'03' error on CONTACT (no field follows)
X'04' loaded (additional field, bytes 6-p, follows)
X'05' exchanged parameters in XID Format 2 I-field not compatible (additional field, bytes 6-p, follows)
X'07' no routing capability to adjacent node (additional field, bytes 6-p, follows)
X'08' incompatible parameters in XID Format 2 I-field for addition of link station to currently active TG (additional field, bytes 6-p, follows)
X'09' loaded, in another subnetwork (bytes 19-26 are added after byte 18 of X'04' status)

Note: End of RU for status bytes X'01', X'02', and X'03'; RU continues for status bytes X'04', X'05', X'07', X'08', and X'09'

6-p Additional fields for status bytes X'04', X'05', X'07', X'08', and X'09'
- For status bytes X'04' and X'09'

6 Resolved TG number
7-10 Adjacent node subarea address (right-justified with leading 0's)
11-18(=p) IPL load module ID received from the adjacent node: an eight-character EBCDIC symbolic name of the IPL load module currently operating in the adjacent node
Note: X'40...40' = no information conveyed.
Note: End of RU for status byte X'04'; RU continues for status byte X'09'

19-26(=p) Network ID of the subnetwork that contains the contacted station
Note: End of RU for status byte X'09'

- For status bytes X'05', X'07', and X'08'

6 Length, in binary, of XID Format 2 I-field received
7-n XID Format 2 I-field received (See SNA Reference Summary for format details.)
n+1 Length, in binary, of XID Format 2 I-field sent
n+2-p XID Format 2 I-field sent (See SNA Reference Summary for format details.)
Note: End of RU for status bytes X'05', X'07', and X'08'

CTERM; SSCP-->PLU, Norm; FMD NS(s) (CONTROL TERMINATE)

CTERM requests that the PLU attempt to deactivate a session identified by the specified (PLU,SLU) network address pair.

0-2 X'810602' NS header
3 bits 0-3, 0000 Format 0 (only value defined)
bits 4-7, reserved
4 Type:
bits 0-1, reserved
bits 2-3, 00 reserved
01 orderly
10 forced
11 reserved
bits 4-7, reserved
5 Reason:
bit 0, 0 network user
1 network manager
bit 1, 0 normal
1 abnormal
bits 2-7, reserved
6-7 Reserved
8-m Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively
m+1-m+2 Retired

DACTCDRM; SSCP-->SSCP, Exp; SC (DEACTIVATE CROSS-DOMAIN RESOURCE MANAGER)

DACTCDRM is sent to deactivate an SSCP-SSCP session.

0 X'15' request code
1 bits 0-3, format: X'0' (only value defined)
bits 4-7, type deactivation requested:
X'1' normal end of session
X'2' invalid activation parameter, sent by the primary half-session to deactivate the session and to indicate to the secondary that the response to ACTCDRM contained an invalid parameter
X'3' session outage notification (SON)
- End of Type 1; Type 2 Continues

2-5 Reason code (included only if type deactivation requested is invalid activation parameter, i.e., byte 1, bits 4-7 = X'2'): sense data (see Appendix G) corresponding to the error
- End of Type 2; Type 3 Continues

2 Cause of session outage notification:
X'07' virtual route inoperative: the virtual route being used by the SSCP-SSCP session has become inoperative, thus forcing the deactivation of the SSCP-SSCP session
X'0B' virtual route deactivated: the identified SSCP-SSCP session is being deactivated because of a forced deactivation of the virtual route being used by the session

X'0C' SSCP failure—unrecoverable: the identified SSCP-SSCP session had to be deactivated because of an abnormal termination of one of the SSCPs of the session; recovery from the failure was not possible

X'0D' session override: the subject session has to be deactivated because of a more recent session activation request for the same session over a different virtual route

X'0E' SSCP failure—recoverable: the identified SSCP-SSCP session had to be deactivated because of an abnormal termination of one of the SSCPs of the session; recovery from the failure may be possible

X'0F' cleanup: the SSCP is resetting its half-session before it receives the response from the partner SSCP receiving the DACTCDRM

X'10' SSCP contention: two SSCPs have sent each other an ACTCDRM request over different virtual routes; the SSCP receiving the ACTCDRM from the SSCP with the greater SSCP ID sends DACTCDRM, with this SON code, to the other SSCP over the same virtual route on which the contention-losing ACTCDRM was sent

X'11' gateway node cleanup: a gateway node is cleaning up the session because the gateway SSCP session partner has forced deactivation of the session (via NOTIFY) Note: In this case, the receiving SSCP does not send NOTIFY to the gateway node.

3 Reserved

DACTPU; SSCP|PUCP-->PU, PU-->SSCP, Exp; SC (DEACTIVATE PHYSICAL UNIT)

DACTPU is sent to deactivate the session between the SSCP and the PU.

0 X'12' request code

1 Type deactivation requested:

X'01' final use, physical connection may be broken

X'02' not final use, physical connection should not be broken

X'03' session outage notification (SON)

2 Cause (not present if byte 1 ≠ X'03'):

X'07' virtual route inoperative: the virtual route for the SSCP-PU session has become inoperative, thus forcing the deactivation of the SSCP-PU session

X'08' route extension inoperative: the route extension serving the SSCP-PU session has become inoperative, thus forcing the deactivation of the SSCP-PU session

X'09' hierarchical reset: the identified session is being deactivated because of a +RSP(ACTPU, Cold)

X'0B' virtual route deactivated: the identified SSCP-PU session is being deactivated because of a forced deactivation of the virtual route being used by the session

X'0C' SSCP or PU failure—unrecoverable: the identified SSCP-PU session had to be deactivated because of an abnormal termination of the SSCP or PU of the session; recovery from the failure was not possible

X'0D' session override: the SSCP-PU session has to be deactivated because of a more recent session activation request for the SSCP to subarea PU session over a different virtual route

X'0E' SSCP or PU failure—recoverable: the identified SSCP-PU session had to be deactivated because of an abnormal termination of the SSCP or PU of the session; recovery from the failure may be possible

X'0F' cleanup: the SSCP is resetting its half-session before receiving the response from the PU that is being deactivated.

DSRLST; SSCP-->SSCP, Norm; FMD NS(s) (DIRECT SEARCH LIST)

DSRLST identifies a control list type and specifies a list search argument to be used at the receiving SSCP.

0-2 X'818627' NS header

3 Search argument type:

X'01' network name of an LU for which an LU Status control list (type X'01') is to be returned

X'02' Resource Identifier control vector identifying an LU in another network for which an LU Status control list (type X'01') is to be returned

X'03' Resource Identifier control vector identifying an LU in another network for which an SSCP Capability control list (type X'03') is to be returned

- For search argument X'01'

4-m Network Name of LU

4 Type: X'F3' logical unit

5 Length, in binary, of symbolic name

6-m Symbolic name in EBCDIC characters

- For search argument X'02'

4-m Resource Identifier (X'19') control vector (This control vector identifies the LU as known by the originating SSCP.)

- For search argument X'03'

4-m Resource Identifier (X'19') control vector (This control vector identifies the LU as known to the originating SSCP—the SSCP name, if known, is the name of the SSCP in whose domain the target LU is defined, not the name of the SSCP on the target side of this gateway.)

ER-TESTED; PU_T4|5-->SSCP, Norm; FMD NS(ma) (EXPLICIT ROUTE TESTED)

> ER-TESTED is sent by a subarea node to one or more SSCPs to provide the status of an ER as determined by explicit route test procedures.

0-2 X'410386' NS header

3 Format:
X'1' Format 1
X'2' Format 2; same as Format 1, except that it includes bytes 48-n

4 Type:
X'00' the corresponding NC-ER-TEST reached its destination subarea
X'02' ER not reversible since there is no reverse ERN defined
X'03' Retired
X'04' ER length exceeded that specified in the NC-ER-TEST request
X'05' ER requires a TG that is not active
X'06' ER is not defined in the NC-ER-TEST-REPLY originating node
X'07' Retired

5 Explicit route length, in terms of the number of transmission groups in the explicit route, as accumulated in NC-ER-TEST

6 Maximum ER length, as specified in the NC-ER-TEST request

7-10 Subarea address of the destination PU of the corresponding NC-ER-TEST

11 Reserved

12 bits 0-3, reserved
bits 4-7, ERN of the ER tested

13-16 Subarea address of the originating PU of the corresponding NC-ER-TEST

17-18 Reverse ERN mask: A bit is on if the corresponding ERN can be used to route from the NC-ER-TEST-REPLY originating subarea to the NC-ER-TEST originating subarea (Bit 0 corresponds to ERN 0, bit 1 to ERN 1, and so forth.)

19-20 Maximum PIU length allowed on the reverse ERN specified in byte 17-18:
X'00' no restriction (only value defined)

21-22 Maximum PIU size accumulated by the corresponding NC-ER-TEST:
X'00' no restriction (only value defined)

23-28 Network address of the SSCP originating the test request

29-38 Request Correlation field, as specified in the corresponding ROUTE-TEST

39-42 Subarea address of the PU that originated the corresponding NC-ER-TEST-REPLY

43-46 Subarea address depending on the Type field (byte 4) as follows:

Type	Contents of this field
X'00'	reserved
X'02'	subarea on the ER prior to that with no reverse ERN defined
X'03'	reserved
X'04'	subarea on the ER preceding the subarea where the explicit route length (byte 5 of NC-ER-TEST) is incremented to a value one more than the maximum ER length limit (byte 6)
X'05'	subarea on the other end of the TG that is not active
X'06'	subarea on the ER from which the PU (that does not have the ER defined) received the corresponding NC-ER-TEST
X'07'	reserved

47 TGN of the TG between the subareas specified in bytes 39-42 and 43-46; reserved if Type is X'00'

Note: End of Format 1; Format 2 continues below

48-51 Subarea address of the adjacent node through which the tested explicit route flows from the node receiving ROUTE-TEST
Note: Bytes 48-51 are reserved if this request is built by nodes other than the original receiver of ROUTE-TEST.

52 Transmission group number of the TG (to the node identified in bytes 48-51) over which the tested explicit route flows from the node receiving ROUTE-TEST
Note: Byte 52 is reserved if this request is built by nodes other than the original receiver of ROUTE-TEST

53-60 Network ID of subnetwork containing the ER
Note: This network ID defines the subnetwork in which the above addresses are valid.

61-62 Bit mask of VRs that use the ER specified by bytes 7-16 (bit n corresponds to VRN n)

Note: Bytes 61-62 are reserved if this request is built by nodes other than the original receiver of ROUTE-TEST.

63-n One or more control vectors, as described in the section "Control Vectors" on page E-49 .
Note: The following vector key may be used in ER-TESTED format 2:
X'1F' ER Configuration control vector one X'1F' control vector is included for each node along the route that supports this vector in NC-ER-TEST-REPLY.)

INIT-OTHER; ILU-->SSCP, Norm; FMD NS(s) (INITIATE-OTHER)

> INIT-OTHER from the ILU requests the initiation of a session between the two LUs named in the RU. The requester may be a third-party LU or one of the two named LUs. This RU is not used by LU 6.2, although it can be used by a third-party LU for LU 6.2.

0-2 X'810680' NS header
3 Format:
bits 0-3, 0001 Format 1
0010 Format 2: specifies the COS name field in addition to the parameters in Format 1
bits 4-7, reserved
4 Type:
bits 0-1, 00 dequeue (DQ) a previously enqueued initiate request (See bits 2-3 for further specification of dequeue actions.)
01 initiate only (I): do not enqueue
10 enqueue only (Q) (See bytes 5-6 for further specification of queuing conditions.)
11 initiate/enqueue (I/Q): enqueue the request if it cannot be satisfied immediately
bits 2-3, (used for DQ; otherwise, reserved)
00 leave on queue if dequeuing attempt is unsuccessful
01 remove from queue if dequeuing attempt is unsuccessful
10 remove from queue; do not attempt initiation
11 reserved
bit 4, reserved
bits 5-6, PLU/SLU specification:
00 LU1 is PLU
01 LU2 is PLU
bit 7, reserved
5 Queuing conditions for LU1 (reserved when Type = DQ)
bit 0, 0 do not enqueue if session limit will be exceeded
1 enqueue if session limit will be exceeded
bit 1, 0 do not enqueue if the LU is not currently able to comply with the PLU/SLU specification (as given in byte 4, bits 5-6)
1 enqueue even though the LU might not be currently able to comply with the PLU/SLU specification
bit 2, reserved
bit 3, 0 do not enqueue if there are no SSCP-LU paths
1 enqueue if there are no SSCP-LU paths
bit 4, reserved
bits 5-6, queuing position/service
00 enqueue this request at the bottom of the queue (the request is put at the bottom of the queue and serviced last)
01 enqueue this request FIFO
10 enqueue this request LIFO
11 reserved
bit 7, reserved
Note: Enqueueing is not performed if the DLU is unknown, or if the domain of either LU is in takedown status.
6 Queuing conditions for LU2 (reserved when Type = DQ):
bit 0, 0 do not enqueue if session limit will be exceeded
1 enqueue if session limit will be exceeded
bit 1, 0 do not enqueue if the LU is not currently able to comply with the PLU/SLU specification (as given in byte 4, bits 5-6)
1 enqueue even though the LU might not be currently able to comply with the PLU/SLU specification
bit 2, reserved
bit 3, 0 do not enqueue if there are no SSCP-LU paths
1 enqueue if there are no SSCP-LU paths
bit 4, reserved
bits 5-6, queuing position/service

00 enqueue this request at the bottom of the queue (the request is put at the bottom of the queue and serviced last)
01 enqueue this request FIFO
10 enqueue this request LIFO
11 reserved

bit 7, reserved

Note: Enqueueing is not performed if the DLU is unknown, or if the domain of either LU is in takedown status.

7 bits 0-2, reserved
bit 3, initiator (reserved when Type = DQ):
0 network user is the initiator
1 network manager is the initiator
bits 4-7, reserved

8 NOTIFY specifications:
bits 0-3, NOTIFY(X'01') conditions (reserved when Type = DQ)
bits 0-1, 00 do not send NOTIFY to LUs in session with LU1
01 reserved
10 send NOTIFY to all LUs in session with LU1 only if the request is queued
11 reserved
bits 2-3, 00 do not send NOTIFY to LUs in session with LU2
01 reserved
10 send NOTIFY to all LUs in session with LU2 only if the request is enqueued
11 reserved
bit 4, reserved
bit 5, NOTIFY(X'03') conditions
0 do not send NOTIFY to the ILU when the requested session is set up
1 send NOTIFY to the ILU when the requested session is set up
bit 6, reserved
bit 7, request for notification of resource availability: if a resource required for setup of the requested session is temporarily unavailable and subsequently becomes available, NOTIFY NS(s) key X'07' is requested to notify the initiator of the resource's availability
0 do not send NOTIFY to the initiator
1 send NOTIFY NS(s) key X'07' to the initiator

9-16 Mode name: an eight-character symbolic name (implementation and installation dependent) that identifies the set of rules and protocols to be used for the session; used by the SSCP(SLU) to select the BIND image that will be used by the SSCP(PLU) to build the CINIT request (reserved when Type = DQ)

17-m Uninterpreted name of LU1
17 Type: X'F3' logical unit
18 Length, in binary, of LU1 name
19-m EBCDIC character string

m+1-n Uninterpreted name of LU2
m+1 Type: X'F3' logical unit
m+2 Length, in binary, of LU2 name
m+3-n EBCDIC character string

n+1-n+2 Retired

n+3-r User Field (reserved when Type = DQ)
n+3 Length, in binary, of user data
Note: X'00' = no user data is present.
n+4-r User data
n+4 User data key
X'00' structured subfields follow
¬X'00' first byte of unstructured user data
Note: Individual structured subfields may be omitted entirely. When present, they appear in ascending field number order.

- For unstructured user data

n+5-r Remainder of unstructured user data

- For structured user data

n+5-r Structured subfields (For detailed definitions, see "User Data Structured Subfield Formats" on page E-41.)

r+1-s User Request Correlation (URC) field (When type = DQ, the URC must be the same as on the original INIT-OTHER request.)
r+1 Length, in binary, of URC
Note: X'00' = no URC.
r+2-s URC: LU-defined identifier; this value can be returned by the SSCP in a subsequent NOTIFY to correlate a given session to the initiating request

End of Format 1; Format 2 Continues

s+1-s+8 COS name: symbolic name of class of service in EBCDIC characters (A value of eight space (X'40') characters may be specified; in this case, the COS name is derived from the mode name table, using the mode name received in byes 9-16.)

INIT-OTHER-CD; SSCP-->SSCP, Norm; FMD NS(s) (INITIATE-OTHER CROSS-DOMAIN)

> INIT-OTHER-CD from the SSCP(ILU) requests that a session be initiated between the two LUs named in the RU. The INIT-OTHER-CD request simply transports an INIT-OTHER from the SSCP(ILU) (a third party SSCP in this case) to the SSCP(OLU).

0-2 X'818640' NS header

3 Format:
bits 0-3, 0000 Format 0
0010 Format 2 specifies COS name field in addition to the parameters in Format 0
0011 Format 3 is the cross-network version of format 2 and includes a Resource Identifier control vector for rerouting in addition to the parameters in Format 2
bits 4-7, reserved

4 Type:
bits 0-1, 00 dequeue (DQ) a previously enqueued initiate request. (See bits 2-3 for further specification of dequeue actions.)
01 initiate only (I): do not enqueue
10 enqueue only (Q): (See bytes 5-6 for further specification of queuing conditions.)
11 initiate/enqueue (I/Q): enqueue the request if it cannot be satisfied immediately
bits 2-3, (used for DQ; otherwise, reserved)
00 leave on queue if dequeuing attempt is unsuccessful
01 remove from queue if dequeuing attempt is unsuccessful
10 remove from queue, do not attempt initiation
11 reserved
bit 4, reserved
bits 5-6, PLU/SLU specification:
00 LU1 is PLU
01 LU2 is PLU
bit 7, reserved

5 Queuing conditions for LU1 (When Type = DQ, bits 0-7 are reserved.):
bit 0, 0 do not enqueue if session limit will be exceeded
1 enqueue if session limit will be exceeded
bit 1, 0 do not enqueue if the LU is not currently able to comply with the PLU/SLU specification (as given in byte 4, bits 5-6)
1 enqueue if the LU is not currently able to comply with the PLU/SLU specification
bit 2, reserved
bit 3, 0 do not enqueue if there are no SSCP-LU paths
1 enqueue if there are no SSCP-LU paths
bit 4, reserved
bits 5-6, 00 enqueue this request at the bottom of the queue (the request is put at the bottom of the queue and serviced last)
01 enqueue this request FIFO
10 enqueue this request LIFO
11 reserved
bit 7, reserved
Note: Enqueuing is not performed if the DLU is unknown, or if the domain of either LU is in takedown status.

6 Queuing conditions for LU2 (When Type = DQ, bits 0-7 are reserved.):
bit 0, 0 do not enqueue if session limit will be exceeded
1 enqueue if session limit will be exceeded
bit 1, 0 do not enqueue if the LU is not currently able to comply with the PLU/SLU specification (as given in byte 4, bits 5-6)
1 enqueue even though the LU might not be currently able to comply with the PLU/SLU specification
bit 2, reserved
bit 3, 0 do not enqueue if there are no SSCP-LU paths
1 enqueue even if there are no SSCP-LU paths
bit 4, reserved
bits 5-6, queuing position/service:
00 enqueue this request at the bottom of the queue (the request at the bottom of the queue and is serviced last)
01 enqueue this request FIFO
10 enqueue this request LIFO
11 reserved
bit 7, reserved
Note: Enqueuing is not performed if the DLU is unknown, or if the domain of either LU is in takedown status.

7-14 PCID: a unique value used as a session identifier
Note: When Type = DQ, the PCID is the same as in the original INIT-OTHER-CD request.
15 bits 0-2, reserved
bit 3, initiator (reserved when Type = DQ):
0 network user is the initiator
1 network manager is the initiator
bits 4-7, reserved
16 NOTIFY specifications:
bits 0-3, NOTIFY(X'01') conditions (reserved when type = DQ)
bits 0-1, 00 do not send NOTIFY to LUs in session with LU1
01 reserved
10 send NOTIFY to all LUs in session with LU1 only if the request is enqueued
11 reserved
bits 2-3, 00 do not send NOTIFY to LUs in session with LU2
01 reserved
10 send NOTIFY to all LUs in session with LU2 only if the request is enqueued.
11 reserved
bit 4, reserved
bit 5, NOTIFY(X'03') condition
0 do not send NOTIFY to the SSCP(ILU) when the requested session is set up
1 send NOTIFY to the SSCP(ILU) when the requested session is set up
bits 6-7, reserved
17-24 Mode name: an eight-character symbolic name (implementation and installation dependent) that identifies the set of rules and protocols to be used for the session; used by the SSCP(SLU) to select the BIND image that will be used by the SSCP(PLU) to build the CINIT request (reserved when type = DQ)
25-m Network Name of LU1
25 Type: X'F3' logical unit
26 Length, in binary, of symbolic name
27-m Symbolic name, in EBCDIC characters
m+1-n Network Name of LU2
m+1 Type: X'F3' logical unit
m+2 Length, in binary, of symbolic name
m+3-n Symbolic name, in EBCDIC characters
n+1-n+2 Retired: set to X'0000'
n+3-r User Field (reserved when type = DQ)
n+3 Length, in binary, of user data
Note: X'00' = no user data is present.
n+4-r User data: user-specific data that is passed to the primary LU on the CINIT request
n+4 User data key
X'00' structured subfields follow
¬X'00' first byte of unstructured user data
Note: Individual structured subfields may be omitted entirely. When present, they appear in ascending field number order.
• For unstructured user data
n+5-r Remainder of unstructured user data
• For structured user data
n+5-r Structured subfields (For detailed definitions, see "User Data Structured Subfield Formats" on page E-41.)
Note: With the exception of the NS header and PCID, all the fields in the INIT-OTHER-CD RU are derived from its corresponding INIT-OTHER RU.

Note: End of Format 0; Formats 2 and 3 continue below.

r+1 COS name field initialization indicator:
bit 0, 0 ILU did not specify COS name
1 ILU did specify COS name
bits 1-7, reserved
r+2-r+9 COS name (reserved if byte r+1, bit 0 = 0): symbolic name of class of service in EBCDIC characters (A value of eight space (X'40') characters may be specified; in this case, the COS name is derived from the mode name table using the mode name received in bytes 17-24.)

Note: End of Format 2; Format 3 continues below.

r+10-r+17 Network ID of subnetwork in which the ILU is located and the names of LU1 (bytes 27-m) and LU2 (bytes m+3-n) are known
r+18-r+25 Network ID of subnetwork in which the following COS name is defined
r+26-r+33 COS name as known in the above network
Note: Bytes r+26-r+33 contain the class of service name that results from translation of the COS name in bytes r+2-r+9 to the corresponding COS name in the network indicated in bytes r+18-r+25.
r+34-r+41 Mode Name as known in the network of the target LU

r+42-s Control vectors, as described in the section "Control Vectors" on page E-49
Note: The following control vector keys are used:
X'19' Resource Identifier control vector for LU1
X'19' Resource Identifier control vector for LU2
Note: One of the LUs is selected by the SSCP(ILU) as the target LU. The X'19' vector that represents the selected LU has the "target resource indicator" bit set to 1.

INIT-SELF; ILU-->SSCP, Norm; FMD NS(s) (INITIATE-SELF)

> INIT-SELF from the ILU requests that the SSCP authorize and assist in the initiation of a session between the LU sending the request (that is, the ILU, which also becomes the OLU) and the LU named in the request (the DLU). This RU is not used for LU 6.2; refer to INIT-SELF Format 1.

0-2 X'010681' NS header
3 bits 0-3, format:
0000 Format 0: specifies a subset of the parameters shown in Format 1 of INIT-SELF (described separately, because the NS header differs in the first byte), with the receiver supplying default values
bit 4, reserved
bits 5-6, 00 DLU is PLU
01 DLU is SLU
bit 7, 0 initiate only (I): do not enqueue.
1 initiate/enqueue (I/Q): enqueue the request if it cannot be satisfied immediately
4-11 Mode name: an eight-character symbolic name (implementation and installation dependent) that identifies the set of rules and protocols to be used for the session; used by the SSCP(SLU) to select the BIND image that will be used by the SSCP(PLU) to build the CINIT request
12-m Uninterpreted Name of DLU
12 Type: X'F3' logical unit
13 Length, in binary, of DLU name
14-m EBCDIC character string
m+1-m+2 Retired
m+3-n User Field
m+3 Length, in binary, of user data
Note: X'00' = no user data is present.
m+4-n User data: user-specific data that is passed to the primary LU on the CINIT request
m+4 User data key
X'00' structured subfields follow
¬X'00' first byte of unstructured user data
Note: Individual structured subfields may be omitted entirely. When present, they appear in ascending field number order.
• For unstructured user data
m+5-n Remainder of unstructured user data
• For structured user data
m+5-n Structured subfields (For detailed definitions, see "User Data Structured Subfield Formats" on page E-41.)

Note: The following default values are supplied by the SSCP(ILU) receiving the Format 0 INIT-SELF request:

- Queuing conditions (if queuing is specified):
  - Enqueue if session limit exceeded.
  - Enqueue this request FIFO.
- Initiate origin: network user is the initiator.
- NOTIFY: do not notify

INIT-SELF; ILU-->SSCP, Norm; FMD NS(s) (INITIATE-SELF)

> INIT-SELF from the ILU requests that the SSCP authorize and assist in the initiation of a session between the LU sending the request (that is, the ILU, which also becomes the OLU) and the LU named in the request (the DLU).

0-2 X'810681' NS header
3 bits 0-3, format:

0001 Format 1: specifies queuing, initiate origin, NOTIFY, and URC in addition to the parameters in Format 0 (only value defined for LU 6.2)
0010 Format 2: specifies the COS name field in addition to the parameters in Format 1

bits 4-7, reserved

4 Type:

bits 0-1, 00 dequeue (DQ) a previously enqueued initiate request (See bits 2-3 for further specification of setup actions.)
Note: Value 00 is defined only for Format 1.
01 initiate only (I): do not enqueue
10 enqueue only (Q) (See byte 5 for further specification of queuing conditions.)
11 initiate/enqueue (I/Q): enqueue the request if it cannot be satisfied immediately
Note: Only values 01 and 11 are defined for LU 6.2.

bits 2-3, (used for DQ; otherwise, reserved)
00 leave on queue if setup attempt is unsuccessful
01 remove from queue if setup attempt is unsuccessful
10 remove from queue; do not attempt setup
11 reserved

bit 4, reserved

bits 5-6, PLU/SLU specification:
00 DLU is PLU
01 DLU is SLU

bit 7, reserved

5 Queuing conditions for DLU (reserved when Type = DQ):

bit 0, 0 do not enqueue if session limit exceeded
1 enqueue if session limit exceeded

bit 1, 0 do not enqueue if DLU is not currently able to comply with the PLU/SLU specification (as given in byte 4, bits 5-6)
1 enqueue if DLU is not currently able to comply with the PLU/SLU specification

bit 2, reserved

bit 3, reserved for LU 6.2; otherwise:
0 do not enqueue if no SSCP(DLU)-DLU path
1 enqueue if no SSCP(DLU)-DLU path

bit 4, reserved

bits 5-6, queuing position/service:
00 put this request at the bottom of the queue (the request is put at the bottom of the queue and serviced last)
01 enqueue this request FIFO (only value defined for LU 6.2)
10 enqueue this request LIFO
11 reserved

bit 7, reserved

Note: Since queuing conditions are specified for the DLU only, the following default values are used by SSCP(OLU) for the OLU:

- Enqueue if session limit exceeded.
- Enqueue this request at the foot of the queue (FIFO).

6 Reserved for LU 6.2; otherwise:

bits 0-2, reserved

bit 3, initiator (reserved when Type = DQ):
0 network user is the initiator
1 network manager is the initiator

bits 4-7, reserved

7 NOTIFY specifications (reserved when Type = DQ and for LU 6.2):

bits 0-1, NOTIFY(X'01') conditions:
00 do not notify LUs in session with DLU
01 reserved
10 notify LUs in session with DLU only if request is queued
11 reserved

bits 2-7, reserved

8-15 Mode name: an eight-character symbolic name (implementation and installation dependent) that identifies the set of rules and protocols to be used for the session; used by the SSCP(SLU) to select the BIND image that will be used by the SSCP(PLU) to build the CINIT request (reserved when Type = DQ)

16-n Uninterpreted Name of DLU

16 Type: X'F3' logical unit

17 Length, in binary, of DLU name

18-n DLU name EBCDIC character string

n+1-n+2 Retired

n+3-r User Field (reserved when Type = DQ and for LU 6.2)

n+3 Length, in binary, of user data
Note: X'00' = no user data is present.

n+4-r User data: user-specific data that is passed to the primary LU on the CINIT request

INIT-SELF Format 1 and 2

n+4 User data key
X'00' structured subfields follow
-X'00' first byte of unstructured user data
Note: Individual structured subfields may be omitted entirely. When present, they appear in ascending field number order.
• For unstructured user data
n+5-r Remainder of unstructured user data
• For structured user data
n+5-r Structured subfields (For detailed definitions, see "User Data Structured Subfield Formats" on page E-41.)
r+1-s User Request Correlation (URC) Field (When Type = DQ, the URC must be the same as in the original INIT-SELF request.)
r+1 Length, in binary, of URC
Note: X'00' = no URC. (The length field is always present.)
r+2-s URC: LU-defined identifier; this value can be returned by the SSCP in a subsequent NOTIFY to correlate a given session to this initiating request
End of Format 1; Format 2 Continues
s+1-s+8 COS name: symbolic name of class of service in EBCDIC characters (A value of eight space characters may be specified; in this case, the COS name is derived from the mode name table using the mode name received in bytes 8-15.)

NC-ER-TEST-REPLY; PU_T4|5-->PU_T4|5, EXP; NC (EXPLICIT ROUTE TEST REPLY)

NC-ER-TEST-REPLY is returned to signal the successful or unsuccessful completion of the NC-ER-TEST.

0 X'0A' request code
1-2 Reserved
3 Format: X'01' (only value defined)
4 Type:
X'00' The corresponding NC-ER-TEST reached its destination subarea
X'02' ER not reversible since there is no reverse ERN defined
X'03' Retired
X'04' ER length exceeded the limit specified in the NC-ER-TEST request
X'05' ER requires a TG that is not active
X'06' ER is not defined in the NC-ER-TEST-REPLY originating node
X'07' Retired
5 Explicit route length, in terms of number of the transmission groups in the explicit route as accumulated in NC-ER-TEST.
6 Maximum ER length, as specified in the NC-ER-TEST request
7-10 Subarea address of the destination PU for corresponding NC-ER-TEST
11 Reserved
12 bits 0-3, reserved
bits 4-7, ERN of the ER being tested
13-16 Subarea address of the PU that originated the corresponding NC-ER-TEST
17-18 Reverse ERN mask: a bit is on if the corresponding ERN can be used to route to the originating subarea
19-20 Maximum PIU size permitted on the reverse ERN specified in bytes 17-18:
X'0000' no restriction (only value defined)
21-22 Maximum PIU size accumulated by the NC-ER-TEST:
X'0000' no restriction (only value defined)
23-28 Network address of the SSCP originating the corresponding NS test request
29-38 Request correlation field: same value as specified in the corresponding NC-ER-TEST
39-42 Subarea address of the PU that originated this NC-ER-TEST-REPLY
43-46 Subarea address depending on the type field (byte 4) as follows:

Type	Contents of this field
X'00'	reserved
X'02'	subarea on the ER prior to that with no reverse ERN defined
X'03'	reserved
X'04'	subarea on the ER preceding the subarea where the explicit route length (byte 5 of NC-ER-TEST) is incremented to a value one more than the maximum ER length limit (byte 6)
X'05'	subarea on the other end of the TG that is not active
X'06'	subarea on the ER from which the PU (that does not have the ER defined), received the corresponding NC-ER-TEST
X'07'	reserved

47 TGN of the TG between the subareas specified in bytes 39-42 and 43-46; reserved if Type is X'00'
Note: For nodes supporting generation of the X'1F' Control Vector, format 1 continues below:

48-n One or more control vectors, as described in the section "Control Vectors" on page E-49

Note: The following vector key may be used in NC-ER-TEST-REPLY:

X'1F' ER Configuration control vector: one X'1F' control vector is included by each node that supports the X'1F' control vector along the route being tested

NOTIFY; SSCP<-->PU, Norm; FMD NS(c) (NOTIFY)

> NOTIFY is used to synchronize awareness between the SSCP and PU of the status of a cross-network session.
>
> NOTIFY is sent by the SSCP to inform the PU that a session initiation process could not complete. It is sent by the PU to inform the SSCP:
>
> - That a session initiation sequence could not be completed because of inability to activate a VR
> - That SON was received for a pending or pending active session
> - That a session terminated normally

0-2 X'410220' NS header

3-4 Element address of the PU, if ENA is supported; otherwise, its network address

5 NOTIFY vector key:

X'05' cross-network session synchronism: used to maintain synchronization between the SSCP and the PU for the mutually supported cross-network LU-LU or SSCP-SSCP session identified by the Network-Qualified Address Pair (X'15') control vector (only value defined)

6-n NOTIFY vector data

- For NOTIFY vector key X'05' (for the PU-->SSCP flow)

6 Cause: the PU sends NOTIFY to the SSCP when it has cleaned up the indicated cross-network session for the cause indicated by one of the following values:

X'00' VR activation failure: the gateway node was unable to activate a VR from the VRID list contained in bytes 12-n

X'01' session ended: the gateway node has received a response to a cross-network session-deactivation request

X'02' session-activation request rejected: the gateway node has received a negative response to a session activation request

X'03' session started: the gateway node has received a positive response to a session activation request.

- For NOTIFY vector key X'05' (for the SSCP-->PU flow)

6 Cause: the SSCP sends NOTIFY to direct the PU to clean up the indicated cross-network session for the cause indicated by one of the following values:

X'04' session terminated: the SSCP is forcing the deactivation of the session (for example, because of operator action)

X'05' session setup failure: the SSCP has detected a session setup failure

X'06' session takedown failure: the SSCP has detected a session takedown failure

7-10 If byte 6 = X'00' or X'02', this field contains the sense data from the negative response to a session activation request; otherwise, it contains 0's

11 Correlation indicators:

bit 0, retention indicator:

0 do not retain the address pair for future use

1 retain the address pair for potential re-use

Note: This indicator is used on the PU-to-SSCP flow and on the SSCP-to-PU flow to override the retention indicator that was carried on RNAA.

bits 1-7, reserved

12-n One or more control vectors, as described in the section "Control Vectors" on page E-49

Note: The following vector keys may be used in NOTIFY(c):

X'15' Network-Qualified Address Pair control vector

Control vector X'15' is used to identify the session to which this request applies and always precedes the additional control vectors, if present.

For LU-LU sessions the addresses are PLU, SLU, respectively.

For SSCP-SSCP sessions the addresses may be in any order.

- For the SSCP-->PU flow, the addresses contained within the X'15' control vector are as defined below:

NAU1 and NAU2 are both addresses within the network identified by the network ID field of the vector. NAU2 contains an alias address assigned within the gateway node receiving this vector. This order applies to the Address Pair session key on both the origin NAU and destination NAU side of the gateway node.

Prior to the NAU Address control vector (X'1A') being received by the gateway node, the X'15' control vector contains the address pair for the network adjacent to the gateway node PU on the origin-NAU side of the PU. After X'1A' has been received in the gateway node, the control vector may carry the session address pair on either side of the gateway node PU.

- For the PU-->SSCP flow, the control vector identifies the session in one network or the other as follows:
  - When the cause code (byte 6) is X'00', VR activation failure, the control vector identifies the session in the network of the VR activation failure.
  - When the cause code (byte 6) is not X'00', the control vector identifies the session in the network the origin-NAU side of the gateway node PU.

X'1B' VRID List control vector (this control vector included only for the PU-to-SSCP flow and when byte 6 = X'00'—VR activation failure)

Note: The following additional vector keys may be used in NOTIFY(c) sent from the PU to SSCP to carry information about the cross-network LU-LU sessions that have been activated:

X'1E' VR-ER Mapping Data control vector

Note: This information is the same as provided in the SESSST RUs that are sent by the LUs to the SSCPs with which they have active sessions. One pair of vectors (X'15' and X'1E') specify the required data for each side of the gateway (i.e.; four vectors are appended to NOTIFY when the NOTIFY Vector Key field (byte 5) is set to X'05' and the Cause field (byte 6) is set to X'03'. These vectors always appear in the order X'15', X'1E', X'15', X'1E'. In this use of control vector X'15', NAU 1 is the PLU address and NAU 2 the SLU address.

NOTIFY; SSCP-->SSCP|LU, LU-->SSCP, Norm; FMD NS(s) (NOTIFY)

NOTIFY is used to send information from an SSCP to another SSCP or to an LU, or from an LU to an SSCP. NOTIFY carries information in the form of a (vector key, vector data) pair.

0-2 X'810620' NS header (for SSCP-->LU and LU-->SSCP)
0-2 X'818620' NS header (for SSCP-->SSCP)
3-p One NOTIFY vector as described in detail below

Note: One of the following vector keys is used:

X'01' Resource Requested: used to inform the current users (LUs) or actively controlling SSCPs of a resource (LU) that another LU wishes to use the resource

X'03' ILU/TLU or Third-party SSCP Notification:
- ILU/TLU notification: used to inform the sender of an INIT or TERM request of the status of the session
- third-party notification: used to inform a third-party SSCP (the SSCP whose LU issued an INIT-OTHER) of the status of the setup procedure

X'04' retired

X'06' Cross-Gateway Resource Requested: same meaning as for X'01' except that the LU wishing to use the resource (LU) is in a subnetwork different from that of the target LU

X'07' Resource Available: used to inform the sender of INIT (i.e., the ILU or SSCP(ILU)) or CDINIT that the required resource is now available.

X'08' Cross-network Resource Available: used to inform the sender of INIT (i.e., the ILU or SSCP(ILU)) or CDINIT that the DLU is now available;

Note: NOTIFY NS(s) key X'08' is used when resource availability information is subject to trial-and-error rerouting.

X'0C' LU-LU Session Services Capabilities: used to inform the SSCP having an active session with the sending LU of the current LU-LU session services capability of that LU

NOTIFY vectors (described zero-origin)

Resource Requested NOTIFY Vector
0 Key: X'01'

1-m Network name of requested LU
1 Type: X'F3' logical unit
2 Length, in binary, of symbolic name of LU
3-m Symbolic name in EBCDIC characters
m+1-n Network name of requesting LU
m+1 Type: X'F3' logical unit
m+2 Length, in binary, of symbolic name
m+3-n Symbolic name in EBCDIC characters

ILU/TLU or Third-party SSCP Notification NOTIFY Vector
0 Key: X'03'
1 Status:
X'00' SSCP(OLU) and SSCP(DLU) not logically connected, i.e., no session or session setup path (if rerouting is required) exists between them
X'01' session terminated
X'02' session set up (i.e., in the same-domain case, +RSP(SESSST) has been sent and, in the cross-domain case, +RSP(CDSESSST) has been sent or received)
X'03' procedure error
2-9 PCID: a unique value used as a session identifier
10 Reason (defined for Status field value of X'03' only)
Note: There are two encodings of the Reason byte:
- If bit 4 = 0, then the Reason byte is encoded for a setup procedure error.
- If bit 4 = 1, then the Reason byte is encoded for a takedown procedure error.

Setup Procedure Error
bit 0, 1 CINIT error in reaching the PLU
bit 1, 1 BIND error in reaching the SLU
bit 2, 1 setup reject at the PLU
bit 3, 1 setup reject at the SLU
bit 4, 0 setup procedure error
bit 5, reserved
bit 6, 1 setup reject at SSCP
bit 7, reserved

Takedown Procedure Error
bit 0, 1 CTERM error in reaching the PLU
bit 1, 1 UNBIND error in reaching the SLU
bit 2, 1 takedown reject at the PLU
bit 3, 1 takedown reject at the SLU
bit 4, 1 takedown procedure error
bit 5, 1 takedown reject at the SSCP
bit 6, 0 see following Note
bit 7, reserved

Note: The bit combination of 11 for bits 4 and 6 is set aside for implementation internal use and will not be otherwise defined.

11-14 Sense data (defined for Status value of X'03' only)
15-m Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' network name pair: (PLU or OLU or LU1) and (SLU or DLU or LU2), respectively
X'07' network address pair: PLU and SLU, respectively
X'0A' URC
Note: This session key is applicable within a NOTIFY only for SSCP-to-TLU; it is the URC carried in the Session Key field (as opposed to the URC field) in TERM, and differs from the URC in bytes m+1 through n below.
X'15' network-qualified address pair: PLU and SLU, respectively
m+1-n User Request Correlation (URC) Field
m+1 Length, in binary, of the URC
m+2-n URC: LU-defined identifier, specified in an INIT or TERM request; used to correlate the NOTIFY to the initiating or terminating requests
Note: The URC length is 0 for SSCP-to-SSCP.

Cross-Gateway Resource Requested NOTIFY Vector
0 Key: X'06'
1-m Three control vectors (as described in the section "Control Vectors" on page E-49) are used in NOTIFY key X'06' to identify the LUs involved in the resource request:
X'19' Resource Identifier control vector: identifies the current session partner of the requested LU and is the target LU
X'19' Resource Identifier control vector: identifies the requested LU
X'19' Resource Identifier control vector: identifies the requesting LU
Note: If the length is 0, the indicated LU name is unavailable.

Resource Available NOTIFY Vector

0 Key: X'07'
1-4 Sense data: same as returned in corresponding -RSP(CDINIT)
5-m Session key, as described in the section, "Session Keys" on page E-58
Note: One of the following session keys is used:
X'01' Network Name or Uninterpreted Name: this session key (X'01') identifies the DLU of an earlier CDINIT request that failed because of the unavailability of a required resource. Session key X'01' is used to signal the general availability of the resource to any and all LUs in the domain of the SSCP being notified.
Note: This session key (X'01') is applicable within a NOTIFY (X'07') only for SSCP-to-SSCP.

Cross-Gateway Resource Available NOTIFY Vector
0 Key: X'08'
1-4 Sense data: same as returned in corresponding -RSP(CDINIT)
5-m The following two control vectors are used in NOTIFY NS(s) key X'08' to identify the target resource being notified and the DLU of an earlier CDINIT request that failed because of the unavailability of a required resource. The vector identifying the target resource appears first.
X'17' SSCP Identifier control vector: identifies the SSCP being notified of the general availability of a resource required for a successful session setup with the DLU specified in the accompanying X'19' control vector. The SSCP identified herein is the target SSCP.
X'19' Resource Identifier control vector: identifies the LU that was earlier named as the DLU in a CDINIT request that could not be satisfied due to the unavailabilitly of a resource that has since become available.

LU-LU Session Services Capabilities NOTIFY Vector
0 Key: X'0C'
1 Length, in binary, of Vector Data field
2-m Vector Data
2 bits 0-3, primary LU capability:
0000 PLU capability is inhibited, sessions can neither be queued nor started
0001 PLU capability is disabled, sessions can be queued but not started
0010 reserved
0011 PLU capability is enabled, sessions can be queued or started
bits 4-7, secondary LU capability:
0000 SLU capability is inhibited, sessions can neither be queued nor started
0001 SLU capability is disabled, sessions can be queued but not started
0010 reserved
0011 SLU capability is enabled, sessions can be queued or started
3-4 LU-LU session limit (where a value of 0 means that no session limit is specified)
5-6 LU-LU session count: the number of LU-LU sessions that are not reset, for this LU, and for which SESSEND will be sent to the SSCP
7 bit 0, parallel session capability:
0 parallel sessions not supported
1 parallel sessions supported
bit 1, retired
bit 2, reserved in NOTIFY(s); SESSST capability in RSP(ACTLU):
0 SESSST RU is suppressed if SLU
1 SESSST RU is sent if SLU
bits 3-6, reserved
bit 7, boundary function network address pair (X'15') session key support (reserved for peripheral nodes):
0 boundary function does not support session key X'15'
1 boundary function does support session key X'15'
Note: Boundary function support for session key X'15' cannot be changed after RSP(ACTLU); in NOTIFY, the sender sets bit 7 to 0, which is then ignored by the receiver.
8-15(=m) Retired (set to X'4040404040404040') or omitted

REQACTCDRM; PU-->SSCP, Exp; FMD NS(c) (REQUEST ACTIVATION OF CROSS-NETWORK RESOURCE MANAGER)

REQACTCDRM prompts the receiving SSCP to issue RNAA and SETCV to set up a cross-network address transform. ACTCDRM will then be sent to activate an SSCP-SSCP session with the other-network SSCP identified in this request.

0-2 X'41028A' NS Header
3-4 Reserved
5 Format: X'01' (only value defined)
6 Activation subfunction indicators:
bit 0, transform setup requirement

0 transform setup not required; the addresses are left over from a previous session setup request
1 RNAA required to set up a cross-network address transform

bit 1, VRID list setup required:
0 SETCV not required with VRID list
1 SETCV required with at least one VRID list

bits 2-7, reserved

7-m Session key, as described in the section, "Session Keys" on page E-58
Note: The following session key is used:
X'15' network-qualified address pair: sending SSCP's real address and target SSCP's alias addresses, respectively, in the address space defined by the network ID

m+1-n Received ACTCDRM that failed because of incomplete gateway node transform: This field contains the received TH, RH, and the complete ACTCDRM RU (including control vectors).

RNAA; SSCP-->PU_T4|5, Norm; FMD NS(c) (REQUEST NETWORK ADDRESS ASSIGNMENT)

RNAA requests the PU to assign element addresses:

- To one or more adjacent link stations and their BF.PUs, as identified in the RNAA request by a link element address and secondary link station link-level addresses
- To one or more BF.LUs, where the BF.LUs are identified in the RNAA request by an adjacent link station element address and the LU local addresses
- To an LU that supports parallel sessions; in order to assign an additional element address the LU is identified in the RNAA request by the LU element address used for the SSCP-LU session—the PU returns the element addresses in the RNAA response
- As alias addresses for a cross-network SSCP-SSCP or LU-LU session, where the name pair and session characteristics are identified in the RNAA request

If ENA is not supported on this SSCP-to-PU_T4|5 session, the entire network address is in each Element Address field throughout this RU.

0-2 X'410210' NS header

3-4 Element address of target link, adjacent link station, LU, or PU

5 Assignment type:
X'00' request is for element address assignment of adjacent link station(s) associated with target link
X'01' request is for element address assignment of BF.LU(s) associated with the target adjacent link station; the address must be pre-ENA compatible
X'02' request is for an additional element address assignment for the target LU; bytes 3-4 contain the LU element address used in the SSCP-LU session; the address must be pre-ENA compatible
X'03' request is for cross-network address transform
X'11' request is for element address assignment of BF.LU(s) associated with the target adjacent link station; an address that is ENA compatible is preferred
X'12' request is for an additional element address assignment for the target LU; bytes 3-4 contain the LU element address used in the SSCP-LU session; an address that is ENA compatible is preferred
X'21' request is for element address assignment of BF.LU(s) associated with the target adjacent link station; an address that is pre-ENA compatible is preferred
X'22' request is for an additional element address assignment for the target LU; bytes 3-4 contain the LU element address used in the SSCP-LU session; an address that is pre-ENA compatible is preferred

6 Number of element addresses to be assigned

7-8 DLC Header Link Station Address, LU Local Address, or LU Element Address Entry

- For Assignment Type X'00'

7 Reserved

8 DLC header link station address associated with the adjacent link station for which an element address is requested

- For Assignment Types X'01', X'11', and X'21'

7 Reserved

8 Local address of a BF.LU for which an element address is requested, where the local address has either the one-byte format of FID2 or the six-bit local address format of FID3 (in which case, bits 0-1 of byte 8 are reserved)

- For Assignment Types X'02', X'12', and X'22'

7-8 Reserved
9-n Any additional two-byte entries in the same format as bytes 7-8 for assignment types X'00' and X'01' (not present for assignment type X'02')

* For Assignment Type X'03'

7 Session characteristics

Note: For an SSCP-SSCP session, origin-NAU and destination-NAU refer to the SSCP that sent RNAA and to the target SSCP, respectively. The parallel session indicators specify that the SSCPs do not have the capability to support parallel SSCP-SSCP sessions (byte 7, bit 0 and bit 1 = 0)

bit 0, parallel session capability of the adjacent SSCP on the origin-NAU side of the PU:
0 SSCP does not have parallel session capability
1 SSCP does have parallel session capability

bit 1, parallel session capability of the adjacent SSCP on the destination-NAU side of the PU:
0 SSCP does not have parallel session capability
1 SSCP does have parallel session capability

bit 2, primary/secondary nature of OLU (reserved for session type = SSCP-SSCP, i.e., bit 4 = 1):
0 OLU=PLU
1 OLU=SLU

bit 3, retention flag:
0 do not retain address transform after session termination
1 retain address transform after session termination

bit 4, session type:
0 LU-LU session
1 SSCP-SSCP session

bit 5, ENA capability of adjacent SSCP on origin NAU side of PU:
0 must be pre-ENA compatible
1 may be ENA compatible

bit 6, ENA capability of adjacent SSCP on destination NAU side of PU:
0 must be pre-ENA compatible
1 may be ENA compatible

bit 7, reserved

8 Reserved
9-14 Origin-NAU's (real) address as known in the network adjacent to the PU and on the origin-NAU side of the PU
15-22 Network ID of the network adjacent to the PU, on the origin-NAU side of the PU
23-30 Network ID of network adjacent to the PU, on the destination-NAU side of the PU
31-38 Network ID of the origin-NAU's network
39 Length of origin-NAU name
40-m Origin-NAU's (real) name
m+1-m+8 Network ID of the destination-NAU's network
m+9 Length of the destination-NAU name
m+10-n Destination-NAU's (real) name

ROUTE-INOP; PU-->SSCP, Norm; FMD NS(c) (ROUTE INOPERATIVE)

> ROUTE-INOP notifies the CP when either a virtual or an explicit route has become inoperative as the result of a transmission group having become inoperative somewhere in the network.

0-2 X'410289' NS header
3 Format: X'01' (only value defined)
4 Reason code:
X'01' unexpected routing interruption over a transmission group; e.g., the last active link in a TG has failed
X'02' controlled routing interruption, such as the result of DISCONTACT
5-8 Subarea address of the PU that originated the NC-ER-INOP
9-12 Subarea address on other end of the transmission group that had the routing interruption
13-16 Subarea address at the route origin
Note: This is the subarea address of the sender in the address space as defined by the network ID contained in bytes 18-25.
17 TGN of the transmission group that had the routing interruption
18-25 Network ID of the subnetwork in which this inoperative report applies
Note: If the Network ID field contains all space (X'40') characters, the reported route is in the receiver's own subnetwork
26 Number of Route fields that follow
27-42 Route Field
27-30 Subarea address for which routing has been interrupted
31-32 ER mask: a bit is on for each ER to the destination subarea identified in bytes 27-30 for which routing has been interrupted (Bit n corresponds to ERN n)

33-34 VR mask: a bit is on for each VR to the destination subarea identified in bytes 27-30 for which routing has been interrupted (Bit n corresponds to VRN n)
35-42 VR-to-ER mapping list: each 4-bit field (16 fields in all) corresponds to a VR number and contains the ERN to which that VR number is assigned (If field 0 contains B'0010', VR0 assigned to ER 2 has failed.)
43-m Additional Route fields in the same format as bytes 27-42

ROUTE-TEST; SSCP-->PU_T4|5, Norm; FMD NS(ma) (ROUTE TEST)

> ROUTE-TEST requests the PC_ROUTE_MGR component of PU.SVC_MGR to return the status (for example, active, operative, not defined), as known in the control blocks in the node, of various explicit and/or virtual routes.

0-2 X'410307' NS header
3-4 Element address of PU originating the test (as known in the sender's subnetwork), if ENA is supported; otherwise, its network address
5 Format: X'01' (only value defined)
6 Test code:
X'01' test regardless of the states of ERs
X'02' test each ER that is not inoperative
X'03' test each ER that is inoperative
X'04' do not test the ER; respond with the current ER state (See RSP(ROUTE-TEST))
7 Choice of routes to be tested:
X'01' test the ERs corresponding to the ERNs specified in bytes 15-16 and also report the status of the VRs supported by these ERs
X'02' test the VRs corresponding to the VRNs specified in bytes 15-16; byte 6 applies to the underlying ERs for the VRs; these ERs are also tested
X'03' test the ERs corresponding to the defined TG for the ERNs specified in bytes 15-16 and also report the status of the VRs supported by these ERs
8 bits 0-5, reserved
bits 6-7, transmission priority for NC-ER-TEST (reserved if the value of byte 6 is X'04'):
00 low priority
01 medium priority
10 high priority
9 Reserved
10 Maximum expected ER length of any ER being tested
11-14 Subarea address of destination PU for the NC-ER-TEST request
15-16 A bit is on if the corresponding ERN or VRN (depending on the route type specified in byte 7) is to be tested (Bit 0 corresponds to ERN or VRN 0, bit 1 to ERN or VRN 1, and so forth.)
17-26 Request correlation field: an implementation-defined value that is returned in ER-TESTED for correlation of reply to request
27-34 Network ID of the subnetwork wherein the route to be tested resides
Note: If the Network ID field contains all space (X'40...40') characters, the route to be tested is in the sender's own network.

SESSEND; LU-->SSCP, Norm; FMD NS(s) (SESSION ENDED)

> SESSEND is sent, with no-response requested, by the LU (or boundary function on behalf of the LU in a peripheral node) to notify the SSCP that the session between the specified LUs has been successfully deactivated.

0-2 X'810688' NS header
3 bits 0-3, format:
0000 format 0 (supported only for nodes that are not at the current level of SNA)
0010 format 2
bits 4-7, reserved
Format 0
4-8 Session key, as described in the section "Session Keys" on page E-58
Note: The following session key is used:
X'07' network address pair: PLU and SLU, respectively (only value defined)
Format 2
4 Cause: indicates the reason for the deactivation of the LU-LU session (see UNBIND for values)
5 Action: indicates if any resultant action is to be taken and by whom:
X'01' normal, no resultant automatic action (only value defined for LU 6.2)
X'02' primary half-session will restart
X'03' secondary half-session will restart

6-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' network name pair: PLU and SLU, respectively
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively
Note: Only session keys X'07' and X'15' are defined for LU 6.2.

SESSST; LU-->SSCP, Norm; FMD NS(s) (SESSION STARTED)

> SESSST is sent, with no response requested, by the LU (or the boundary function on behalf of the LU in a peripheral node) to notify the SSCP that the session between the specified LUs has been successfully activated.

0-2 X'810686' NS header
3 Format:
X'00' Format 0: no control vectors present
X'01' Format 1: control vectors present in bytes n+1-p
4-n Session Key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

Note: End of Format 0; Format 1 continues below

n+1-p One or more control vectors, as described in the section "Control Vectors" on page E-49
Note: The following vector keys may be used in SESSST:
X'1E' VR-ER Mapping Data
X'23' Local Form Session Identifier

SETCV; SSCP-->PU_T4|5, Norm; FMD NS(c) (SET CONTROL VECTOR)

> SETCV sets a control vector that is maintained by the PU receiving the request and that is associated with the network address specified in the RU.

0-2 X'010211' NS header
3-4 Element address of resource to which control vector applies, if ENA is supported; otherwise, its network address
Note: For control vectors X'15', X'16', X'1A', and X'1B', this field contains the PU address, and the X'15' control vector identifies the cross-network session to which the data contained in control vectors X'16', X'1A', and X'1B' apply.
5-n One or more control vectors, as described in the section "Control Vectors" on page E-49
Note: The following vector keys may be used in SETCV (configuration services):
X'01': Date-Time
X'02': Subarea Routing
X'03': SDLC Secondary Station
X'04': LU
X'05': Channel
X'15': Network-Qualified Address Pair
X'16': Names Substitution
X'1A': NAU Address
X'1B': VRID List
Note: See SNA Reference Summary for the formats of the first five control vectors mentioned above. They are not related to gateway services.
Note: The following table shows the relationship between the control vector included and the resource identified in bytes 3 and 4.

Key (Byte 5)	Resource (Bytes 3-4)
X'01'	PU
X'02'	Link to be used for routing to the subarea specified in byte 6
X'03'	SPU
X'04'	LU
X'05'	Link (S/370 channel)
X'15'	PU
X'16'	PU
X'1A'	PU
X'1B'	PU

Note: Control vector X'15' is used to identify the session to which vectors X'16', X'1A and X'1B' apply and precedes these vectors. The addresses contained within this X'15' control vector are as defined below:

NAU 1 and NAU 2 are both addresses within the network carried in the network ID field of the vector. NAU 2 contains an alias address assigned within the gateway node receiving this vector. This order applies to the address pair session key on both the origin NAU and destination NAU side of the gateway node.

Prior to the X'1A' vector being received by the gateway node, the X'15' control vector contains the address pair for the network adjacent to the gateway node PU on the origin-NAU side of the PU. After X'1A' has been received in the gateway node, the X'15' control vector may carry the session address pair on either side of the gateway node PU.

TERM-OTHER; TLU-->SSCP, Norm; FMD NS(s)(TERMINATE-OTHER)

> TERM-OTHER from the TLU requests that the SSCP assist in terminating session(s) between the two LUs named in the RU. The requester may be a third party LU or one of the two named LUs. This RU is not used by LU 6.2, although it can be used by a third-party LU for LU 6.2.

0-2 X'810682' NS header

3 bits 0-3, Format:
0001 Format 1 (Only value defined)
bits 4-7, reserved

4 Type
bits 0-1, 00 the request applies to active and pending-active sessions
01 the request applies to active, pending-active, and queued sessions
10 the request applies to queued sessions only
11 the request applies to pending-active and queued sessions only
bit 2, reserved if byte 4, bit 7 = 1; otherwise:
0 forced termination—session to be deactivated immediately and unconditionally
1 orderly termination—permitting an end-of-session procedure to be executed at the PLU before the session is deactivated
bit 3, 0 do not send DACTLU to LU1; another session initiation request will be sent for LU1
1 send DACTLU to LU1 when appropriate; no further session initiation request will be sent (from this sender) for LU1
bit 4, 0 do not send DACTLU to LU2; another session initiation request will be sent for LU2
1 send DACTLU to LU2 when appropriate; no further session initiation request will be sent (from this sender) for LU2
bits 5-6, session selection (reserved when session key X'06' not used)
00 select session(s) for which LU1 is PLU
01 select session(s) for which LU2 is PLU
10 select session(s) regardless of whether LU is PLU or SLU
11 reserved
bit 7, 0 orderly or forced (see byte 4, bit 2)
1 cleanup

5 Reason
bit 0, 0 network user
1 network manager
bit 1, 0 normal termination
1 abnormal termination
bits 2-7, reserved

6 NOTIFY specifications:
bits 0-5, reserved
bit 6, NOTIFY(X'03') condition
0 do not notify TLU when the session takedown procedure is complete
1 notify the TLU when the session takedown procedure is complete
bit 7, reserved

7 Type extension (see byte 4)
X'00' terminate specified session and perform notification based on the NOTIFY specification (byte 6)
X'01' do not terminate specified session, but perform notification based on the NOTIFY specification (byte 6)
X'02' retired
X'03' retired

8-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'06' network name pair

Note: If the length of one of the names (LU1 or LU2, but not both) is 0 then all sessions for the named LU, as specified by the Type byte, are terminated as a result of this TERM-OTHER request.

X'07' network address pair: PLU and SLU, respectively

X'0A' URC

Note: This URC is the one carried in the INIT issued previously by the same LU (i.e., ILU = TLU), and differs from the one in bytes n+4 through p.

X'15' network-qualified address pair: PLU and SLU, respectively

n+1-n+2 Retired

n+3-p User Request Correlation (URC) Field

n+3 Length, in binary, of the URC

Note: X'00' = no URC.

n+4-p URC: LU-defined identifier; this value can be returned by the SSCP in a subsequent NOTIFY to correlate the NOTIFY to this terminating request

TERM-SELF; TLU-->SSCP, Norm; FMD NS(s) (TERMINATE-SELF)

TERM-SELF from the TLU requests that the SSCP assist in the termination of one or more sessions between the sender of the request (TLU = OLU) and the DLU. This RU is not used for LU 6.2; refer to TERM-SELF Format 1.

0-2 X'010683' NS header

3 Type:

bits 0-1, 00 the request applies to active and pending-active sessions
01 the request applies to active, pending-active, and queued sessions
10 the request applies to queued only sessions
11 reserved

bit 2, reserved if byte 3, bit 4 = 1; otherwise:
0 forced termination—session to be deactivated immediately and unconditionally
1 orderly termination—permitting an end-of-session procedure to be executed at the PLU before the session is deactivated

bit 3, 0 do not send DACTLU to OLU; another session initiation request will be sent for OLU
1 send DACTLU to OLU when appropriate; no further session initiation request will be sent (from this sender) for OLU

bit 4, 0 orderly or forced (see byte 3, bit 2)
1 clean up

bits 5-6, 00 select session(s) for which DLU is PLU
01 select session(s) for which DLU is SLU
10 select session(s) regardless of whether DLU is SLU or PLU
11 reserved

bit 7, 0 indicates that the format of the RU is Format 0 and that byte 3 is the Type byte.

4-m Uninterpreted Name of DLU

4 Type: X'F3' logical unit

5 Length, in binary, of DLU name

Note: If the length value of the DLU name is 0, then the TERM-SELF applies to all sessions, as specified in the Type byte, where the TLU is a partner.

6-m EBCDIC character string

Note: The following defaults are supplied by the SSCP receiving a Format 0 TERM-SELF:

- Reason: network user, normal
- Notify: do not notify
- URC is not used in mapping to subsequent requests.

TERM-SELF; TLU-->SSCP, Norm; FMD NS(s) (TERMINATE-SELF)

TERM-SELF from the TLU requests that the SSCP assist in the termination of one or more sessions between the sender of the request (TLU = OLU) and the DLU.

0-2 X'810683' NS header

3 bits 0-3, format:
0001 Format 1 (only value defined)

bits 4-6, reserved

bit 7, 1 indicates that byte 3, bits 0-3, contain the format value

4 Type:

bits 0-1, 00 the request applies to active and pending-active sessions
01 the request applies to active, pending-active, and queued sessions (only value defined for LU 6.2)

10 the request applies to queued sessions only
11 reserved

bit 2, reserved if byte 4, bit 7 = 1; otherwise:
0 forced termination—session to be deactivated immediately and unconditionally
1 orderly termination—permitting an end-of-session procedure to be executed at the PLU before the session is deactivated

bit 3, 0 do not send DACTLU to OLU; another session initiation request will be sent for OLU
1 send DACTLU to OLU when appropriate; no further session initiation request will be sent (from this sender) for OLU (only value defined for LU 6.2)

bit 4, reserved

bits 5-6, 00 select session(s) for which DLU is PLU
01 select session(s) for which DLU is SLU
10 select session(s) regardless of whether DLU is SLU or PLU
11 reserved

bit 7, 0 orderly or forced (see byte 4, bit 2)
1 clean up

5 Reason:

bit 0, 0 network user (only value defined for LU 6.2)
1 network manager

bit 1, 0 normal termination
1 abnormal termination

bits 2-7, reserved

6 NOTIFY specifications (reserved for LU 6.2):

bits 0-5, reserved

bit 6, 0 do not notify TLU when the session takedown procedure is complete
1 notify the TLU when the session takedown procedure is complete

bit 7, reserved

7 Reserved

8-n Session key, as described in the section "Session Keys" on page E-58

Note: One of the following session keys is used:

X'01' uninterpreted name
Note: If the length value is 0, then the TERM-SELF applies to all sessions specified in the Type byte where the TLU is a partner.

X'07' network address pair: PLU and SLU, respectively

X'0A' URC (only session key defined for LU 6.2)
Note: This URC is the one carried in the INIT issued previously by the same LU (i.e., ILU = TLU), and differs from the one in bytes n+4 through p.

X'15' network-qualified name pair: PLU and SLU, respectively

n+1-n+2 Retired: set to X'0000'

n+3-p User Request Correlation (URC) Field

n+3 Length, in binary, of URC field

Note: X'00' = no URC.

n+4-p URC: LU-defined identifier; this value can be returned by the SSCP in a subsequent NOTIFY to correlate the NOTIFY to this terminating request

UNBIND; LU-->LU, Exp; SC (UNBIND SESSION)

UNBIND is sent to deactivate an active session between the two LUs.

0 X'32' request code

1 Type UNBIND:

X'01' normal end of session

X'02' BIND forthcoming; retain the node resources allocated to this session, if possible

X'06' invalid session parameters: the BIND negotiation has failed due to an inability of the primary half-session to support parameters specified by the secondary

X'07' virtual route inoperative: the virtual route used by the LU-LU session has become inoperative, thus forcing the deactivation of the identifed LU-LU session

X'08' route extension inoperative: the route extension used by the LU-LU session has become inoperative, thus forcing the deactivation of the identified LU-LU session

X'09' hierarchical reset: the identified LU-LU session is being deactivated because of a +RSP((ACTPU | ACTLU), Cold)

X'0A' SSCP gone: the identified LU-LU session had to be deactivated because of a forced deactivation of the SSCP-PU or SSCP-LU session (e.g., DACTPU, DACTLU, or DISCONTACT)

X'0B' virtual route deactivated: the identified LU-LU session had to be deactivated because of a forced deactivation of the virtual route being used by the LU-LU session

X'0C' LU failure—unrecoverable: the identified LU-LU session had to be deactivated because of an abnormal termination of the PLU or SLU; recovery from the failure was not possible
X'0E' LU failure—recoverable: the identified LU-LU session had to be deactivated because of an abnormal termination of one of the LUs of the session; recovery from the failure may be possible
X'0F' cleanup: the LU sending UNBIND is resetting its half-session before receiving the response from the partner LU
X'11' gateway node cleanup: a gateway node is cleaning up the session because a gateway SSCP has directed the gateway node (via NOTIFY) to deactivate the session (e.g., a session setup error or session takedown failure has occurred)
X'FE' format or protocol error: the LU sending UNBIND has detected a format or protocol error; the error is identified by the associated sense code

2-5 Sense data (included only when Type = X'FE'; otherwise, this field is omitted): same value as generated at the time the error was originally detected (e.g., for a negative response, receive check, or EXR)

UNBINDF; PLU-->SSCP, Norm; FMD NS(s) (UNBIND FAILURE)

> UNBINDF is sent, with no-response requested, by the PLU to notify the SSCP that the attempt to deactivate the session between the specified LUs has failed (for example, because of a path failure).

0-2 X'810687' NS header
3-6 Sense data
7 Reason:
bit 0, reserved
bit 1, 1 UNBIND error in reaching SLU
bit 2, 1 takedown reject at PLU
bits 3-7, reserved
8-n Session key, as described in the section "Session Keys" on page E-58
Note: One of the following session keys is used:
X'07' network address pair: PLU and SLU, respectively
X'15' network-qualified address pair: PLU and SLU, respectively

USER DATA STRUCTURED SUBFIELD FORMATS

The structured subfields of the User Data field are defined as follows (shown with zero-origin indexing of the subfield bytes—see the individual RU description for the actual displacement within the RU). Each subfield starts with a one-byte binary Length field and is identified by a subfield number in the following byte. The length does not include the Length byte itself. When more than one subfield is included, they appear in ascending order by subfield number.

For LU type 6.2, the Structured User Data field of BIND and RSP(BIND) may contain the Unformatted Data, Mode Name, Fully Qualified PLU Network Name, Fully Qualified SLU Network Name, and Session Instance Identifier subfields. Any subfields received in the Structured User Data field of BIND that are not recognized by the SLU are discarded and not returned as part of the Structured User Data field of the RSP(BIND).

Unformatted Data Structured Data Subfield

The Unformatted Data subfield may optionally be sent in BIND, RSP(BIND), or any of the INITIATE RUs. The content is implementation-defined.

0	Length of the remainder of the Unformatted Data subfield: values 1 to 17 (X'11') are valid for LU 6.2; otherwise, values 1 to 65 (X'41') are valid
1	X'00'
2-n	Unformatted data: a type-G symbol string

Session Qualifier Structured Data Subfield

The Session Qualifier subfield is used for LU 6.1. It may be carried in BIND, RSP(BIND), or any of the INITIATE RUs.

0	Length of the remainder of the Session Qualifier subfield (If Session Qualifier subfield is present, values 3 to 19 (X'13') are valid.)
1	X'01'
2	Length of primary resource qualifier: values 0 to 8 are valid (X'00' means no primary resource qualifier is present)
3-m	Primary resource qualifier
m+1	Length of secondary resource qualifier: values 0 to 8 are valid (X'00' means no secondary resource qualifier is present)
m+2-n	Secondary resource qualifier

Mode Name Structured Data Subfield

The Mode Name subfield is present in both BIND and RSP(BIND) if the PLU knows the mode name being used by the session.

0	Length of the remainder of the Mode Name subfield: values 1 to 9 are valid
1	X'02'
2-n	Mode name: 0 to 8 type-A symbol string characters with optional (but not significant) trailing blanks

Session Instance Identifier Structured Data Subfield

The Session Instance Identifier subfield may be present in both BIND and RSP(BIND).

0	Length of the remainder of the Session Instance Identifier subfield: values 3 to 9 are valid
1	X'03'
2-n	Session instance identifier: a type-G symbol string Note: In BIND, the PLU sets a unique session instance identifier of length 1 to 7 and appends it to X'00'. If known, the SLU compares its fully qualified name with that of the PLU; if the PLU name > SLU name then the SLU changes the first byte of the Session Instance Identifier subfield in the response from X'00' to X'F0', if the PLU name < SLU name then the subfield is simply echoed.

Fully Qualified PLU Network Name Structured Data Subfield

BIND contains the Fully Qualified PLU Network Name subfield (if the name is known by the PLU).

User Data Subfields

0	Length of the remainder of the Fully Qualified PLU Network Name subfield: values 2 to 18 (X'12') are valid
1	X'04'
2-n	Fully qualified PLU network name Note: The fully qualified PLU network name is 1 to 17 bytes in length, consisting of an optional 1- to 8-byte network ID and a 1- to 8-byte LU name, both of which are type-A symbol strings. When present, the network ID is concatenated to the left of the LU name, using a separating period and having the form "NWID.NAME"; when the network ID is omitted, the period is also omitted.

Fully Qualified SLU Network Name Structured Data Subfield

> The RSP(BIND) contains the Fully Qualified SLU Network Name subfield (if the name is known by the SLU).

0	Length of the remainder of the Fully Qualified SLU Network Name subfield: values 2 to 18 (X'12') are valid
1	X'05'
2-n	Fully qualified SLU network name Note: The fully qualified SLU network name is 1 to 17 bytes in length, consisting of an optional 1- to 8-byte network ID and a 1- to 8-byte LU name, both of which are type-A symbol strings. When present, the network ID is concatenated to the left of the LU name, using a separating period and having the form "NWID.NAME"; when the network ID is omitted, the period is also omitted.

Clear Data Structured Data Subfield

> The Clear Data subfield contains the random data used in session-level security verification. When session-level security verification is in effect, this subfield is present in both BIND and RSP(BIND).

0	Length of the remainder of the Clear Data subfield: 10 is the only valid value
1	X'11'
2	Reserved
3-10	Clear data: a type-G random value generated for subsequent checking in RSP(BIND) or FMH-12

Enciphered Data Structured Data Subfield

> The Enciphered Data subfield is present in the RSP(BIND) when session-level security verification is in effect. This subfield contains the enciphered version of the clear data received in BIND.

0	Length of the remainder of the Enciphered Data subfield: 9 is the only valid value
1	X'12'
2-9	Enciphered version of the Clear Data field carried in BIND (using the DES algorithm and the installation-defined LU-LU password as the cryptographic key)

SUMMARY OF RESPONSE RU'S

Apart from the exceptions cited below, response RUs return the number of bytes specified in the following table; only enough of the request RU is returned to include the field-formatted request code.

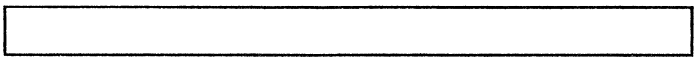
RU Category of Response	Number of Bytes in RU
DFC	1
SC	1
NC	1
FMD NS (FI=1) (field-formatted)	3
FMD NS (FI=0) (character-coded)	0
FMD (LU-LU)	0

Various positive response RUs return additional data. See "Positive Response RU's with Extended Formats" for details.

All negative responses return four bytes of sense data in the RU, followed by either (1) the number of bytes specified in the table above or (2) three bytes (or the entire request RU, if shorter than three bytes). The second option applies to PU.SVC_MGR.CSC_MGR and PC (where a sensitivity to SSCP-based sessions versus LU-LU sessions does not necessarily exist) and can be chosen for other layers for implementation simplicity. Refer to Appendix G for sense data values and their corresponding meanings.

POSITIVE RESPONSE RU'S WITH EXTENDED FORMATS

RSP(ACTCDRM); SSCP-->SSCP, Exp; SC



0 X'14' request code

1 bits 0-3, format: X'0' (only value defined)
bits 4-7, type activation performed:
X'1' cold
X'2' ERP

2 FM profile

3 TS profile

4-11 Contents ID: eight-character EBCDIC symbolic name that represents implementation and installation dependent information about the SSCP issuing the response to ACTCDRM; eight space (X'40') characters is the value used if no information is to be conveyed (This field could be used to provide a check for a functional and configurational match between the SSCPs.)

12-17 SSCP ID: a six-byte field that includes the ID of the SSCP issuing the ACTCDRM response; the first four bits specify the format for the remaining bits:
bits 0-3, 0000
bits 4-7, physical unit type of the node containing the SSCP
bits 8-47, implementation and installation dependent binary identification

18 TS Usage
bits 0-1, reserved
bits 2-7, secondary CPMGR receive window size (0 means no pacing of requests flowing to the secondary)

19-n Control vector, as described in the section "Control Vectors" on page E-49
Note: The following vector keys may be used in RSP(ACTCDRM):
X'06' CDRM control vector
X'09' Activation Request/Response Sequence Identifier control vector
X'13' Gateway Support Capabilities control vector
X'18' SSCP Name control vector
X'FE' one or more control vector keys not recognized in the corresponding request

RSP(ACTPU); PU-->SSCP|PUCP, Exp; SC

0 X'11' request code

1 bits 0-1, reserved
bits 2-3, format of response:
00 format 0
01 format 1
10 format 2 (this format requires that bits 4-7 be set to X'3')

11 format 3 (only for PU_T4|5s)
bits 4-7, type activation selected:
X'1' cold, IPL not required
X'2' ERP
X'3' cold, IPL required

2-9 Contents ID: eight-character EBCDIC symbolic name of the load module currently operating in the node; eight space (X'40') characters is the default value

Note: End of Format 0; Formats 1-3 continue below.

10-n Format 1 Continues
10-11 Reserved
12-n Control vector as described in the section "Control Vectors" on page E-49
Note: The following control vectors may be used in RSP(ACTPU):
X'07' PU FMD-RU-Usage control vector
X'24' IPL Load Module Request control vector
X'FE' vector key not recognized in the corresponding request
10-n Format 2 Continues
10-17 Load module ID: an eight-character EBCDIC symbolic name of the requested IPL load module:
X'4040...40' any load module will be accepted
¬X'4040...40' identifies specific load module name
18-19 Reserved
20-n Control vector as described in the section "Control Vectors" on page E-49
Note: The following control vectors may be used in RSP(ACTPU):
X'07' PU FMD-RU-Usage
X'FE' vector key not recognized in the corresponding request
10-n Format 3 Continues
10-n Control vector as described in the section "Control Vectors" on page E-49
Note: The following control vectors may be used in RSP(ACTPU):
X'09' Activation Request/Response Sequence Identifier control vector
X'0B' SSCP-PU Session Capabilities control vector (this control vector is not included in RSP(ACTPU) if all requested functions are supported as specified in the received X'0B' control vector (see X'0B' control vector))
X'FE' one or more vector keys not recognized in the corresponding request

RSP(BIND); SLU-->PLU, Exp; SC
0 X'31' request code
Note: The following bytes are returned for the extended nonnegotiable BIND response or for the negotiable BIND response. (The request code alone is sent if a nonnegotiable BIND request specifies no session-level cryptography.)

1 bits 0-3, format: 0000 (only value defined)
bits 4-7, type:
0000 negotiable (only value defined for LU 6.2)
0001 nonnegotiable
2-25 Bytes as received on BIND request, for nonnegotiable response; or bytes having the same format, but possibly with values changed from those received on the BIND request, for negotiable response
26-k Cryptography Options (see Note 4)
26 bits 0-1, private cryptography options: for a nonnegotiable response, same value returned as received in the request, if present
bits 2-3, session-level cryptography options: for a nonnegotiable response and an LU 6.2 response, same value returned as received in the request, if present
bits 4-7, session-level cryptography options field length: same value returned as received in the request, if present (Bytes 27-k are omitted if this length field is omitted or set to 0.)
27 bits 0-1, session cryptography key encipherment method: same value returned as received in the request, if present
bits 2-4, reserved
bits 5-7, cryptography cipher method: same value returned as received in the request, if present
28-k An eight-byte implementation-chosen, nonzero, pseudo random session-seed cryptography value enciphered under the session cryptography key, if session-level cryptography is specified; otherwise, omitted
k+1-r Bytes as received on BIND request, for nonnegotiable response; or bytes having the same format, but possibly with values changed from those received on the BIND request, for negotiable response

Note 1: The extended format is required for the negotiable BIND response or if session-level cryptography is specified in the BIND request; otherwise, only the short form (request code) is used.

Note 2: On a response, if the last byte of a response without control vectors (byte 7, bit 6 = 0) is a length field and that field is 0, that byte may be omitted from the response. This applies also to byte 26 (where the count occupies only bits 4-7) if bits 0-3 are also 0—the entire byte may be omitted if no bytes follow.

Note 3: Reserved fields in the BIND are set by the SLU to binary 0's in the RSP(BIND); any fields at the end of the BIND that are not recognized by the SLU are discarded and not returned in the RSP(BIND).

Note 4: The Cryptography Options field is returned on the response for a nonnegotiable BIND and LU 6.2 BIND only when session-level cryptography was specified, or for a non-LU 6.2 negotiable BIND.

RSP(CDINIT); SSCP-->SSCP, Norm; FMD NS(s)

0-2 X'818641' NS header

3 bits 0-3, format: same value as received in corresponding request
bits 4-7, reserved

4 Procedure status:
bits 0-3, reserved
bits 4-7, status at SSCP receiving CDINIT:
0000 reserved
0001 initiate successful—proceed
0010 initiate successful—queued
0011 dequeued—successful

5-6 Retired

7 LU status for LU associated with the SSCP receiving the CDINIT request:
bit 0, reserved
bit 1, 0 LU is unavailable
1 LU is available
bits 2-3, (reserved if LU is available)
00 LU session limit exceeded
01 reserved
10 LU is not currently able to comply with the PLU/SLU specification
11 reserved
bit 4, 0 existing SSCP to LU path
1 no existing SSCP to LU path
bit 5, (reserved in formats 0 and 1)
0 UNBIND and SESSEND cannot be sent by the LU or by its boundary function (if any)
1 UNBIND and SESSEND will be sent by the LU or by its boundary function (if any)
bits 6-7, 00 reserved
01 LU is PLU
10 LU is SLU
11 reserved

Note: End of Formats 0, 1, and 4; Formats 2 and 3 continue below

8 COS origin:
bit 0, 0 no COS name from ILU
1 COS name from ILU
bits 1-2, (reserved if byte 8, bit 0 ≠ 0)
01 SSCP(DLU) chose COS name (DLU is SLU)
10 SSCP(OLU) chose COS name (OLU is SLU)
bits 3-7, reserved

9-16 COS name (if byte 8, bit 0 = 0 and bits 1-2 ≠ 01, this field carries unpredictable values and is not used): symbolic name of class of service in EBCDIC characters
Note: For format 3 this COS name represents the COS name as known in the network of the DLU.

17-24 Mode name (if byte 8, bits 1-2 ≠ 01, this field carries unpredictable values and is not used): an eight-byte symbolic name (implementation and installation dependent) that identifies the set of rules and protocols to be used for the session (included here for use in reactivating the (LU,LU) session, if necessary; see CINIT and SESSEND for other details)

RSP(CDINIT)

Note: End of Format 2; Format 3 continues below.

25-n One or more control vectors, as described in the section "Control Vectors" on page E-49
Note: Vector key X'1A' is required for format 3; the other vectors are optional. If present, they appear in the order specified below.
X'1A' NAU Address control vector (contains the DLU network address)
Note: Between gateways, the DLU address is an address recognized in the subnetwork on the OLU side of the sending gateway. Within a gateway, the DLU address is an address recognized in the network on the DLU side of the gateway node, until the SSCP with address alias responsibility is reached. This SSCP replaces the received address with an address recognized in the network on the OLU side of the gateway node.

The network ID is identified in the X'19' vector for the DLU.
X'14' Session Initiation control vector
X'19' Resource Identifier control vector (for destination LU)
X'19' Resource Identifier control vector (for origin LU)

RSP(CDTERM); SSCP(DLU)-->SSCP(OLU), Norm; NS(s)
0-2 X'818643' NS header
3 bits 0-3, 0000 Format 0 (only value defined)
bits 4-7, reserved
4-6 Reserved

RSP(CINIT); PLU-->SSCP, Norm; FMD NS(s)
0-2 X'810601' NS header
3-n Control vectors as described in the section "Control Vectors" on page E-49
Note: The following control vector key is used in RSP(CINIT):
X'FE' control vector keys not recognized

RSP(DSRLST); SSCP-->SSCP, Norm; NS(s)
0-2 X'818627' NS header
3-n Control list entry data for list type (See "Control Lists" on page E-57 for detailed descriptions)
Note: One of the following control list entries is used:
- When control list search argument is X'01' (LU Status List)

3-n X'01' LU Status List
- When control list search argument is X'02' (Cross-Network LU Status List)

3-n X'01' LU Status List
- When control list search argument is X'03' (Cross-Network SSCP List)

3-n X'03' Cross-Network SSCP List

RSP(INIT-OTHER-CD); SSCP-->SSCP, Norm; FMD NS(s)
0-2 X'818640' NS header
3 Format
bits 0-3, 0000 Format 0 (only value defined)
bits 4-7, reserved
4 Procedure Status:
bits 0-3, Status for SSCP(LU1)
0000 reserved
0001 initiate successful—proceed
0010 initiate successful—queued
bits 4-7, Status for SSCP(LU2)
0000 reserved
0001 initiate successful—proceed
0010 initiate successful—queued
5 LU1 Status
bit 0, reserved
bit 1, 0 LU1 is unavailable
1 LU1 is available
bits 2-3, (reserved if LU1 is available)
00 LU1 session limit exceeded
01 reserved
10 LU1 is not currently able to comply with the PLU/SLU specification
11 reserved
bits 4-5, reserved
bits 6-7, 00 reserved
01 LU1 is PLU
10 LU1 is SLU
11 reserved
6 LU2 Status:
bit 0, reserved
bit 1, 0 LU2 is unavailable

```
              1 LU2 is available
          bits 2-3, (reserved if LU2 is available)
                    00 LU2 session limit exceeded
                    01 reserved
                    10 LU2 is not currently able to comply with the PLU/SLU specification
                    11 reserved
          bits 4-5, reserved
          bits 6-7, 00 reserved
                    01 LU2 is PLU
                    10 LU2 is SLU
                    11 reserved
```

RSP(RNAA); PU_T4|5-->SSCP, Norm; FMD NS(c)

> If ENA is not supported on this SSCP-to-PU_T4|5 session, the entire network address is in each Element Address field throughout this RU.

0-2 X'410210' NS header

3-5 Set to same value as bytes 3-5 in RNAA request

6 Number of element addresses returned

- For assignment types X'00', X'01', X'02', X'11', X'12', X'21', X'22':

7-8 Element address assigned: adjacent link station address for assignment type X'00'; BF.LU element address for assignment types X'01', X'11', and X'21': LU address for assignment types X'02', X'12', and X'22'

9-n Any additional element addresses assigned (2-byte multiples), in the same format as bytes 7-8; the order of the element addresses returned corresponds to the order of the entries (bytes 7-n) in the RNAA request

- For assignment type X'03':

7-12 Destination-NAU alias address, applicable in the subnetwork adjacent to the PU, on the origin-NAU side of the PU

13-18 Origin-NAU alias address, applicable in the subnetwork adjacent to the PU, on the destination-NAU side of the PU

RSP(ROUTE-TEST); PU_T4|5-->SSCP, Norm; FMD NS(ma)

0-2 X'410307' NS header

3 Format: X'01'

4 Number of Route Data fields

5-14 Route Data: information about the ERs and VRs that were tested

5 Virtual route identifier:
bits 0-3, VRN of the VR tested
bits 4-5, reserved
bits 6-7, transmission priority field of the VR tested

6 VR status:
X'00' VR is not defined
X'01' VR is in reset state
X'02' activation of the VR is pending notification of the activation of the underlying ER
X'03' an NC-ACTVR was sent to activate the VR, but no RSP(NC-ACTVR) has been received
X'04' an NC-ACTVR was received to activate the VR, but no RSP(NC-ACTVR) has been sent
X'05' an NC-DACTVR(Orderly) has been sent, but no RSP(NC-DACTVR) has been received
X'06' an NC-DACTVR(Orderly) was received, but no RSP(NC-DACTVR) has been sent
X'07' an NC-DACTVR(Forced) was received, but no RSP(NC-DACTVR) has been sent
X'08' an NC-DACTVR(Forced) was sent but no RSP(NC-DACTVR) has been received
X'09' VR is active
X'0A' retired

7 bits 0-3, reserved
bits 4-7, ERN of the ER tested

8 ER status:
X'00' ER is not defined and not currently operative
X'01' ER is defined but not currently operative
X'02' ER is defined and operative, but not currently active
X'03' an NC-ER-ACT was sent, but no NC-ER-ACT-REPLY has been received
X'04' an NC-ER-ACT was received, but no NC-ER-ACT-REPLY has been sent
X'05' an NC-ER-ACT was received and an NC-ER-ACT-REPLY was sent; an NC-ER-ACT was sent, but no NC-ER-ACT-REPLY has been received
X'06' an NC-ER-ACT was received but no ER is defined; should the ER subsequently become defined, an NC-ER-ACT will be sent
X'07' an NC-ER-ACT was received and an NC-ER-ACT-REPLY was sent (no NC-ER-ACT has been sent from this end)
X'08' ER is active and each node on the ER supports ER-VR protocols
X'09' ER is operative but not currently defined

	X'0A' ER is active and traverses a node that does not support ER-VR protocols
9-12	Subarea address of the adjacent node through which the ER being tested flows from this node
13	Transmission group number of the TG (to the node identified in bytes 9-12) over which the ER being tested flows from this node
14	Reserved
15-m	Any additional 10-byte entries in the same format as bytes 5-14
m+1-m+4	Subarea address at the route origin Note: This is the subarea address of the sender in the address space as defined by the network ID contained in bytes m+5-m+12
m+5-m+12	Network ID of the subnetwork wherein the tested route resides (same as bytes 27-34 of corresponding ROUTE-TEST request)

CONTROL VECTORS, CONTROL LISTS AND SESSION KEYS

CONTROL VECTORS

The following table shows, by key value, the control vector and the message-unit structures that can carry the control vector.

Key	Control Vector	Applicable Message-Unit Structures
X'06'	CDRM	ACTCDRM, RSP(ACTCDRM)
X'07'	PU FMD-RU-Usage	RSP(ACTPU)
X'09'	Activation Request/Response Sequence Identifier	ACTCDRM, ACTPU, RSP(ACTCDRM|ACTPU)
X'0B'	SSCP-PU Session Capabilities	ACTPU, RSP(ACTPU)
X'0D'	Mode / Class-of-Service / Virtual-Route-Identifier-List	CINIT
X'13'	Gateway Support Capabilities	ACTCDRM, RSP(ACTCDRM)
X'14'	Session Initiation	CDINIT, RSP(CDINIT)
X'15'	Network-Qualified Address Pair	SETCV, NOTIFY(c), CINIT
X'16'	Names Substitution	SETCV
X'17'	SSCP Identifier	NOTIFY(s)
X'18'	SSCP Name	ACTPU, ACTCDRM, RSP(ACTCDRM)
X'19'	Resource Identifier	CDINIT, RSP(CDINIT), INIT-OTHER-CD, DSRLST, NOTIFY(s)
X'1A'	NAU Address	SETCV, CDINIT, RSP(CDINIT)
X'1B'	VRID List	SETCV, NOTIFY(c)
X'1E'	VR-ER Mapping Data	NOTIFY(c), SESSST
X'1F'	ER Configuration	NC-ER-TEST-REPLY, ER-TESTED
X'23'	Local-Form Session Identifier	SESSST
X'24'	IPL Load Module Request	RSP(ACTPU)
X'FE'	Control Vector Keys Not Recognized	RSP(ACTCDRM), RSP(ACTPU), RSP(BIND), RSP(CINIT)

Note: Control vector X'FE' is used to report receipt of one or more unrecognized control vectors. The receiver responds using a X'FE' control vector that identifies each unrecognized control vector by key; this allows the response sender to indicate that some control vectors have been processed, while others have not.

The control vectors are defined as follows (with zero-origin indexing of the vector bytes—see the individual RU description for the actual displacement within the RU):
Note: When more than one control vector may appear in an RU, unless otherwise stated, the vectors may appear in any order.

CDRM Control Vector
0 Key: X'06'
1 Length, in binary, of Vector Data field (X'00' = no Vector Data field present.)
2-n Vector Data
2 CDRM profile: X'00' (only value defined)
3-5(=n) CDRM usage:
bit 0, 0 name pair (X'06') session key supported
1 name pair session key not supported
bit 1, 0 address pair (X'07) session key not supported
1 address pair session key supported
Note: If the control vector is omitted or the length is 0, the corresponding request or response implicitly specifies that the name pair (X'06') session key is supported and the others are not.
bit 2, 0 parallel sessions not supported
1 parallel sessions supported
bit 3, 0 URC not supported by SSCP (and all PLUs within its domain) in cross-domain session initiation
1 URC supported by SSCP (and all PLUs within its domain) in cross-domain session initiation
bit 4, 0 CDINIT (TYPE=DQ) (Format 1 or 4) with Type field bits specifying "leave on queue if dequeue retry is unsuccessful" not supported
1 CDINIT (TYPE=DQ) (Format 1 or 4) with Type field bits specifying "leave on queue if dequeue retry is unsuccessful" supported
bit 5, 0 PCID (X'05') session key not supported
1 PCID session key supported

bit 6, 0 CDSESSEND from SSCP(SLU) and CDINIT(Format 2) not supported; requires NS-LSA (see SNA Reference Summary) to reset session knowledge; therefore, all sessions managed by the SSCP use virtual routes mapping to ER0 from the subarea of the SLU to the subarea of the PLU
1 CDSESSEND from SSCP(SLU) and CDINIT(Format 2) supported; NS-LSA is not used to reset session knowledge; therefore, no ER restrictions exist for sessions managed by this SSCP
bit 7, reserved
bit 8, 0 SSCP does not support the PLU capability indicator in LU Status (X'01') Control List
1 SSCP supports the PLU capability indicator in LU Status (X'01') Control List
bit 9, 0 network-qualified address pair (X'15') session key not supported
1 network-qualified address pair session key supported
bit 10, 0 INIT-OTHER-CD Format 2 not supported
1 INIT-OTHER-CD Format 2 supported
bit 11, 0 INIT-OTHER-CD Format 3 not supported
1 INIT-OTHER-CD Format 3 supported
bit 12, 0 Format 3 and 4 of CDINIT not supported
1 Format 3 and 4 CDINIT supported: includes NAU Address (X'1A') control vector
Note: If control vector X'13' is also included in this ACTCDRM request or response, CDINIT format 3 or 4 may include additional control vectors for cross-network session setup
bit 13, 0 Format 1 of CDCINIT not supported: includes Network-Qualified Address Pair (X'15') session key
1 Format 1 CDCINIT supported
bit 14, 0 NOTIFY NS(s) key X'06' not supported
1 NOTIFY NS(s) key X'06' supported
bit 15, 0 notification of lost session (LU-LU) awareness not supported
1 notification of lost session (LU-LU) awareness supported (The SSCP sends CDSESSEND if it has lost awareness of the session identified by the Session Key Content field in the CDSESSEND.)
bit 16, Support of CDINIT request for notification of DLU availability:
0 CDINIT (byte 20 bits 6-7) request for notification of DLU availability not supported
1 CDINIT (byte 20 bits 6-7) request for notification of DLU availability supported. NOTIFY NS(s) key X'07' with session key X'01' or NOTIFY NS(s) key X'08' is sent.
bit 17, 0 backup session request is not supported in CDINIT
1 backup session request is supported in CDINIT
bit 18, ENA support:
0 ENA not supported
1 ENA supported
bit 19, 0 network-qualified names support indicator in CDINIT and RSP(CDINIT) not supported
1 network-qualified names support indicator in CDINIT and RSP(CDINIT) supported; this implies that the sending SSCP supports sending and receiving fully-qualified PCID on the CDRM session

Note: This vector is sent on ACTCDRM and RSP(ACTCDRM) to define the receive capabilities of the SSCP building the request or response. An SSCP reports all its capabilities. If an SSCP does not report support of a particular function, its session partner SSCP is responsible for not invoking that function. An SSCP receiving the vector in an ACTCDRM request or response ignores bits within the usage indicators that it does not understand. In its own vector, the SSCP sets such bits to 0, indicating that it does not support the function.

PU FMD-RU-Usage Control Vector
0 Key: X'07'
1 bits 0-5, reserved
bit 6, adjacent PU load capability (initialized to 0 by the PU_T2):
0 adjacent PU cannot load the PU_T2 node
1 adjacent PU can load the PU_T2 node (set by the boundary function in the adjacent subarea node)
bit 7, FMD request capability of the node:
0 PU cannot receive FMD requests from the SSCP
1 PU can receive FMD requests from the SSCP
2-7 Reserved

Activation Request/Response Sequence Identifier Control Vector
0 Key: X'09'
1 Length, in binary, of Vector Data field
2-n Vector Data
2-9(=n) Activation request/response sequence identifier: an eight-byte binary value, generated by the sender of ACTCDRM, RSP(ACTCDRM), ACTPU, and echoed in RSP(ACTPU), and used by the receiver to determine whether the current RU supersedes a previously received

RU from the same sender (If the current RU has an activation request/response sequence identifier value greater than the corresponding activation request/response sequence identifier value of the earlier ACTPU, ACTCDRM, or RSP(ACTCDRM), the current RU is accepted and processed, while the earlier RU is superseded. The eight-byte field has the following characteristic: If n1 was generated at time t1, and n2 was generated at time t2, and t1 < t2, then n1 < n2.)

SSCP-PU Session Capabilities Control Vector

0 Key: X'0B'
1 Length, in binary, of Vector Data field
2-n Vector Data
2 bit 0, lost subarea requirement:
0 NS-LSA (see SNA Reference Summary) required
1 NS-LSA not required
bit 1, ALS station support:
0 adjacent link station network address not supported
1 adjacent link station network address supported
bit 2, gateway support:
0 no gateway support
1 this component supports gateway function
bit 3, notification of other-network lost route:
0 do not notify the SSCP (via ROUTE-INOP or ER-TESTED) of an inoperative route in subnetworks other than this SSCP's
1 notify the SSCP (via ROUTE-INOP or ER-TESTED format 2) of an inoperative route in subnetworks other than this SSCP's
bit 4, notification of same-network lost route:
0 do not send ROUTE-INOP; send ER-TESTED format 1 for routes in the sender's subnetwork
1 send ROUTE-INOP if a VR or ER is lost in this SSCP's own subnetwork; send ER-TESTED format 2
Note: An SSCP always receives ER-TESTED for routes in the SSCP's own subnetwork; additionally, this bit indicates whether ROUTE-INOP may flow for lost ERs or VRs in the SSCP's own subnetwork.
bit 5, CONTACTED(Loaded) format:
0 send CONTACTED (X'04')
1 send CONTACTED (X'09')
bit 6, ENA support:
0 ENA is not supported
1 ENA is supported
bit 7, reserved

Note: This control vector is not sent on RSP(ACTPU) if the PU is willing and able to operate at the capabilities level requested by the sending SSCP. If the PU is not capable of the requested support, the bits are turned off that are not supported and the control vector is returned to the SSCP as X'0B' control vector in RSP(ACTPU).

Mode/COS/VRID List Control Vector

0 Key: X'0D'
1 Length, in binary, of Vector Data field
2-n Vector Data
2-9 Mode name: an eight-character symbolic name (implementation and installation dependent) of type-A symbol string characters that identifies the set of rules and protocols to be used for the session; used by the SSCP(SLU) to select the BIND image that will be used by the SSCP(PLU) to build the CINIT request
10-17 COS name: symbolic name of class of service in EBCDIC characters
18-n Virtual Route Information
18 Length (in bytes)—including format, type, number of entries, and entries of Virtual Route Information field
19 Format of virtual route identifier list:
X'00' format 0 (only value defined)
20 Type of virtual route required:
X'00' only virtual routes mapping to ER0 from the subarea of the SLU to the subarea of the PLU may be used
X'01' virtual routes mapping to any ERN may be used
21 Number of entries in the virtual route identifier list
22-n Virtual route identifier list: two-byte (VRN, TPF) entries where VRN is one byte and TPF is one byte

Network Name Control Vector

0 Key: X'0E'
1 Length, in binary, of Vector Data field
2-n Vector Data
2 Network name type:
3-n Network-qualified name: a 1- to 17-byte name consisting of an optional qualifier concatenated to a 1- to 8-byte name; when present, the qualifier contains a 1- to 8-byte

network identifier concatenated with a period (when the qualifier is not present, the period is omitted). The network-qualified name appears as follows: NETID.NAME, with no imbedded blanks and with optional but not significant trailing blanks.

Gateway Support Capabilities Control Vector

0 Key: X'13'

1 Length, in binary, of Vector Data field

2-m Vector Data

2-m A pair of session keys as described in the section "Session Keys" on page E-58

Note: These session keys appear in the following order:

X'15' network-qualified address pair (NAU 1 and NAU 2 define the sender's address and the destination address, respectively, as known in the network of the sender.)

X'15' network-qualified address pair (NAU 1 and NAU 2 define the origin address and the destination address, respectively, as known in the network adjacent to the sender.)

Session Initiation Control Vector

0 Key: X'14'

1 Length, in binary, of Vector Data field

2-n Vector Data

2-9 Network ID 1: For CDINIT this is the network ID of the subnetwork containing the DLU. For RSP(CDINIT) this is the network ID of the subnetwork on the DLU side of the gateway node.

Note: Network ID 1 and COS name 1 fields are reserved in CDINIT if COS name not received from the ILU or if Control Vector X'19' for the DLU indicates that the translation of alias to real DLU name has not occurred.

10-17 COS name 1: For CDINIT and RSP(CDINIT), this is the COS name as known in the above network.

18-25 Network ID 2: This field and the subsequent COS name 2 field are used in conjunction with the network ID 1 and COS name 1 fields to distribute the COS name as known on both sides of the gateway node to the gateway SSCP responsible for COS name to VRID resolution in the shared control gateway environment. Network ID 2 identifies the subnetwork on the OLU side of the gateway node.

Note: Network ID 2 is reserved for CDINIT or when RSP(CDINIT) is flowing from one gateway to another and if COS name translation has not yet occurred in this gateway for RSP(CDINIT).

26-33 COS name 2: For RSP(CDINIT), this is the COS name as known in the above network.

Note: COS name 2 is reserved for CDINIT or when RSP(CDINIT) is flowing from one gateway to another and if COS name translation has not yet occurred in this gateway for RSP(CDINIT).

34 Usage indicators:

bit 0, parallel session capabilities of adjacent SSCP on the OLU side of the gateway node:

0 parallel sessions not supported

1 parallel sessions supported

Note: This bit is set by the first gateway SSCP on each gateway for CDINIT and is reserved for RSP(CDINIT).

bit 1, configuration information:

0 The RU sender and receiver are not in the same gateway (i.e., the gateway that is to be used by the intended cross-network LU-LU session)

1 The RU sender and receiver are in the same gateway (The gateway reference is relative to the cross-network LU-LU session, not the cross-network SSCP-SSCP session between the RU sender and receiver.)

Note: Network ID 2, COS name 2, and the second instance of session key X'15' are reserved in CDINIT and RSP(CDINIT) flowing from one gateway to another (when bit 1 = 0).

bit 2, address aliasing support (reserved when byte 34, bit 1 is 0):

0 sender is not designated for address aliasing support

1 sender is designated for address aliasing support

Note: This bit is used to signal whether the sender is the predesignated gateway SSCP for address aliasing support of the gateway node specified in bytes 43-46.

bits 3-7, reserved

35-42 Mode name as known in the destination network

Note: The mode name as known in the network of the OLU is contained in bytes 21-28 of CDINIT.

43-46 Subarea address of the gateway PU that is to be used for the intended LU-LU session (reserved when byte 34, bit 1 is 0)

47-54 Network ID of the subnetwork in which the above subarea address is valid (reserved when byte 34, bit 1 is 0)

55-n A pair of session keys as described in the section "Session Keys" on page E-58

Note: The following session keys are used:

X'15' network-qualified address pair (session key 1): OLU and DLU respectively

Between gateways, usage is as follows:

- CDINIT: address pair on the OLU side of the gateway when received, on the DLU side of the gateway when sent. The DLU address is reserved.

- RSP(CDINIT): address pair on the DLU side of the gateway when received, on the OLU side of the gateway when sent.

Within a gateway, usage is as follows:

- CDINIT: address pair on the DLU side of the gateway; if the SSCP with alias address responsibility has not been reached, session key 1 is reserved (i.e., it is present with a length of 0, or present with nonzero length and contents of 0's). Otherwise, only the DLU portion of the address pair is reserved.

- RSP(CDINIT): address pair on the OLU side of the gateway.

Note: Session key 1 is used both between gateways (byte 34, bit 1 = 0) and within a gateway (byte 34, bit 1 = 1).

X'15' network-qualified address pair (session key 2): OLU and DLU respectively

Between gateways, session key 2 is reserved (as described above).

Within a gateway, usage is as follows:

- CDINIT: address pair on the OLU side of the gateway; upon entry into a gateway, session key 1 in the input CDINIT is copied into session key 2 of the output CDINIT. The DLU address is reserved until the SSCP with alias address responsibility is reached.

- RSP(CDINIT): address pair on the DLU side of the gateway; upon entry into a gateway, session key 1 in the input RSP(CDINIT) is copied into session key 2 of the output RSP(CDINIT).

Note: Session key 2 is used only within a gateway; otherwise, it is reserved (i.e., it is present with a length of 0, or present with nonzero length and contents of 0's).

Network-Qualified Address Pair Control Vector

0	Key: X'15'
1	Length, in binary, of Vector Data field
2-n	Vector Data
2-7	NAU 1 network address
8-13	NAU 2 network address
	Note: See the RUs that carry this vector for NAU1/NAU2 definitions and order requirements.
14-21(=n)	Network ID of the subnetwork in which the above addresses are valid
	Note: If the Network ID field contains all space (X'40...40') characters, the network addresses are in the sender's network.

Names Substitution Control Vector

0	Key: X'16'
1	Length, in binary, of the Vector Data field
2-n	Vector Data
2	Length of PLU alias name
3-m	PLU alias name
m+1	Length of SLU real name
m+2-n	SLU real name

Note: The Network-Qualified Address Pair control vector always accompanies this vector in SETCV.

SSCP Identifier Control Vector

0	Key: X'17'
1	Length, in binary, of the Vector Data field
2-n	Vector Data
2	SSCP visit count (set by the first gateway SSCP and then decremented at each gateway SSCP on the path) Note: This field is ignored by the receiver if byte 3, bit 1 is 0.
3	Usage indicators: bit 0, reserved bit 1, target resource indicator: 0 the resource named in this vector is not the target resource 1 the resource named in this vector is the target resource

```
          bits 2-7, reserved
4         Length of network ID
5-m       Network ID of the subnetwork containing the SSCP
m+1       Length of SSCP name
m+2-n     Name of the SSCP

SSCP Name Control Vector
0         Key:  X'18'
1         Length, in binary, of the Vector Data field
2-n       Vector Data
2-9       Name of SSCP:  symbolic name in EBCDIC characters
10-17(=n) Network ID of the subnetwork containing the SSCP

Resource Identifier Control Vector
0         Key:  X'19'
1         Length, in binary, of the Vector Data field
2-r       Vector Data
2         SSCP visit count (set by the first gateway SSCP and then decremented at each gateway
          SSCP on the path)
          Note:  This field is ignored by the receiver if byte 3, bit 1 is 0.
3         Usage indicators:
          bit  0, name translation:
                  0 translation has not occurred for this name
                  1 translation has occurred for this name
          bit  1, target resource indicator:
                  0 the resource named in this vector is not the target resource
                  1 the resource named in this vector is the target resource
          bits 2-7, reserved
4         Length of SSCP name
5-m       Name of SSCP that controls the LU:  symbolic name in EBCDIC characters
m+1       Length of network ID
m+2-n     Network ID of the subnetwork containing the LU
n+1       Length of LU name
n+2-p     Network name of the LU (real name)
p+1       Length of network ID
p+2-q     Network ID of the subnetwork in which the LU name alias is known
q+1       Length of LU name
q+2-r     Alias LU name

NAU Address Control Vector
0         Key:  X'1A'
1         Length, in binary, of the Vector Data field
2-n       Vector Data
2-7       Network address of the NAU
8(=n)     ENA support:
          bit  0, 0 NAU does not support ENA
                  1 NAU supports ENA
          bits 1-7, reserved

VRID List Control Vector
0         Key:  X'1B'
1         Length, in binary, of Vector Data field
2-n       Vector Data
2-9       Network ID
10-n      Virtual Route Information Field
10        Format of virtual route list:
          X'00' format 0 (only value defined)
11        Type of virtual route required:
          X'00' only virtual routes mapping to ER0 from the subarea of the SLU to the subarea of
                the PLU may be used
          X'01' virtual routes mapping to any ERN may be used
12        Number of entries in the Virtual Route Information field:
13-n      Virtual route list:  two-byte (VRN, TPF) entries, where VRN is one byte and TPF is one
          byte

VR-ER Mapping Data Control Vector
0         Key:  X'1E'
1         Length, in binary, of Vector Data field
2-n       Vector Data
2         VRN and TPF data:
          bits 0-3, virtual route number (VRN) assigned to the session indicated in the contain-
                    ing RU
          bits 4-5, reserved
```

bits 6-7, Transmission Priority field (TPF) assigned to the session indicated in the containing RU

3 Explicit route data:
bits 0-3, reserved
bits 4-7, outbound ERN for the VRN specified in byte 2, bits 0-3

4(=n) Reverse explicit route data:
bits 0-3, reserved
bits 4-7, RERN corresponding to the ERN in byte 3

ER Configuration Control Vector

0 Key: X'1F'

1 Length, in binary, of Vector Data field

2-p Vector Data

2 Outbound TG number (reserved in last vector)

3 Inbound TG number (reserved in first vector)

4-7 Subarea address of the PU that has appended this control vector, in the network in which the containing RU is flowing

8 Number of SSCP Address fields in bytes 9-m

9-m SSCP address fields: list of 8-byte fields, one for each SSCP that currently controls at least one active link in any TG underlying the tested ER or has an active SSCP-PU session

Note: The format of each 8-byte field is (shown zero-origin):

0 Reserved

1 bits 0-5, reserved
bit 6, set to 1 if this SSCP has at least one link active in the TG over which the ER test will be sent, as specified in the Outbound TG Number field (byte 2 of this control vector)
bit 7, set to 1 if this SSCP has at least one link active in the TG over which the ER test was received, as specified in the Inbound TG Number field (byte 3 of this control vector)

Note: If bits 6 and 7 are both 0, the address in bytes 2 through 7 is the address of an SSCP that did not issue an ACTLINK for any link in either the inbound or outbound TG. In this case, it is an SSCP that has an SSCP-PU session with this node.

2-7 Address of the SSCP

Note: End of the 8-byte field format

m+1 Length, in binary, of network ID

Note: When the length is 0, the network ID is the same as that of the sub-network containing the ER, and the fields defined in bytes m+2-p are not included.

m+2-n Network ID of the network in which the SSCP addresses are known

n+1-p Four byte Subarea address of the PU that has appended this control vector, as known in the network defined in bytes m+2-n

Local Form Session Identifier Control Vector

0 Key: X'23'

1 Length, in binary, of Vector Data field

2-p Vector Data

2 Format:
X'02' Format 2: FID 2 session identifier
X'03' Format 3: FID 3 session identifier

- For format 2—FID 2

3-p Session identifier (SID) for Format 2—FID 2

3 SID High (SIDH): OAF' from the TH of the BIND request

4 SID Low (SIDL): DAF' from the TH of the BIND request

5(=p) Flags:
bits 0-5, reserved
bit 6, ODAI field from TH of the BIND request
bit 7, reserved

- For format 3—FID 3

3-p Session identifier for Format 3—FID 3

3(=p) LSID from TH of the BIND request

IPL Load Module Request Control Vector

0 Key: X'24'

1 Length, in binary, of Vector Data field

2-n Vector Data

2-9(=n) Load module ID: an eight-character type-A symbol string symbolic name of the requested IPL load module:
X'4040...40' any load module will be accepted
¬X'4040...40' identifies specific load module name

Control Vector Keys Not Recognized Control Vector

0	Key: X'FE'
1	Length, in binary, of Vector Data field
2-n	Vector data: one or more one-byte control vector key values that were not recognized in the corresponding request

CONTROL LISTS

The following table shows, by list type, the control lists and the message structures that can carry the control list.

Type	Control List	Applicable Message-Unit Structures
X'01'	LU Status	+RSP(DSRLST)
X'03'	Other-Network SSCP	+RSP(DSRLST)

The control lists are defined, by type, as follows (with zero-origin indexing of the list bytes; see the individual RU description for the actual displacement within the RU):
Note: Control List data is requested by type; however, the type is not included in the reply RU that carries the request control list.

LU Status Control List
- Type: X'01'

0 LU status
- bit 0, reserved
- bit 1, 0 LU is unavailable
  1 LU is available
- bits 2-3, (if LU is unavailable)
  00 LU session count exceeded
  01 LU is being taken down (not accepting new sessions)
  10 LU is not currently able to comply with the PLU specification
  11 reserved
- bit 4, 0 existing SSCP to LU path
  1 no existing SSCP to LU path
- bits 5-7, reserved

1 LU information:
- bit 0, 0 LU does not reside in a PU_T5 node
  1 LU resides in a PU_T5 node
- bit 1, PLU capability
  0 LU capability of acting as PLU not determined
  1 LU is capable of acting as PLU (capability may be disabled now and thus the session will be queued)
- bits 2-6, reserved
- bit 7, 0 LU is accepting INITIATEs/logons
  1 LU is temporarily not accepting INITIATEs/logons

2-3 Session count (range: 0-65535)

Other-Network SSCP Control List
- Type: X'03'

0 Capability byte:
- bit 0, parallel (LU-LU) session capability of the SSCP to which the gateway SSCP on the DLU side of the gateway node will forward CDINIT:
  0 SSCP does not have parallel session capability
  1 SSCP has parallel session capability
- bit 1, ENA support
  0 DLU does not support ENA
  1 DLU supports ENA
- bits 2-7, reserved

1-8 Network ID of the adjacent subnetwork

SESSION KEYS

The following table shows, by key value, the session key and the message-unit structures that can carry the session key.

Key	Session Key	Applicable Message-Unit Structures
X'01'	Uninterpreted name	TERM-SELF
X'01'	Network name	NOTIFY(s)
X'05'	PCID	CDTERM and NOTIFY
X'06'	Uninterpreted name pair	CLEANUP and TERM-OTHER
X'06'	Network name pair	CDSESSEND, CDSESSSF, CDSESSST, CDSESSTF, CDTERM, NOTIFY, and SESSEND
X'07'	Network address pair	BINDF, CDSESSEND, CDSESSSF, CDSESSST, CDSESSTF, CDTERM, CINIT, CLEANUP, CTERM, NOTIFY, SESSEND, SESSST, TERM-OTHER, TERM-SELF, and UNBINDF
X'0A'	URC	NOTIFY, TERM-OTHER, and TERM-SELF
X'15'	Network-Qualified address pair	BINDF, CDCINIT, CDINIT, CDSESSEND, CDSESSSF, CDSESSST, CDSESSTF, CDTERM, CLEANUP, CTERM, NOTIFY, REQACTCDRM, SESSEND, SESSST, TERM-OTHER, TERM-SELF, UNBINDF, and Control Vectors X'13' and X'14'

The session keys are defined as follows (with zero-origin indexing of the key bytes—see the individual RU description for the actual displacement within the RU.

Network or Uninterpreted Name Session Key

0	Key: X'01'
1	Type: X'F3' logical unit
2	Length, in binary, of name
3-n	Network or Uninterpreted Name

Note: For a Network Name session key, the name is a symbolic name; for an Uninterpreted Name session key, the name is any EBCDIC character string.

PCID Session Key

0	Key: X'05'
1-2	Network address of the SSCP generating this PCID
3-8	A unique 6-byte value, generated by the SSCP initiating the cross-domain procedure, that is retained and used in all cross-domain requests dealing with the same procedure until it is completed

Network Name Pair or Uninterpreted Name Pair Session Key

0	Key: X'06'
1	Type: X'F3' logical unit
2	Length, in binary, of PLU (or OLU or LU1) name
3-m	Name in EBCDIC characters (see Note below)
m+1	Type: X'F3' logical unit
m+2	Length, in binary, of SLU (or DLU or LU2) name
m+3-n	Name in EBCDIC characters (see Note below)

Note: For a Network Name Pair session key, the names consist of type-A symbol-string characters; for an Uninterpreted Name Pair session key, the names are any EBCDIC strings.

Network Address Pair Session Key

0	Key: X'07'
1-2	Network address of NAU1
3-4	Network address of NAU2

Note: See the RUs that carry this session key for NAU1/NAU2 definitions and order requirements.

URC Session Key

0	Key: X'0A'
1	Length, in binary, of the URC
2-n	URC: LU-defined identifier

Network-Qualified Address Pair Session Key

0	Key: X'15'
1	Length, in binary, of Key Data field
2-21	KEY Data field
2-7	NAU1 network address
8-13	NAU2 network address Note: See the RUs that carry this session key for NAU1/NAU2 definitions and order requirements.
14-21	Network ID of the subnetwork in which the above addresses are valid Note: The Length byte is set to 12 when network ID is not included and to 20 when network ID is included. If the Network ID contains all space (X'40...40') characters, the network addresses are in the sender's network.

APPENDIX G. SENSE DATA

The sense data included with an EXCEPTION REQUEST (EXR), a negative response, an UNBIND request, a function management header type 7 (FMH-7), or a send or receive check is a four-byte field (see Figure G-1) that generally includes a one-byte category value, a one-byte modifier value, and two bytes of sense code specific information, whose format is defined along with the sense code definition, below.

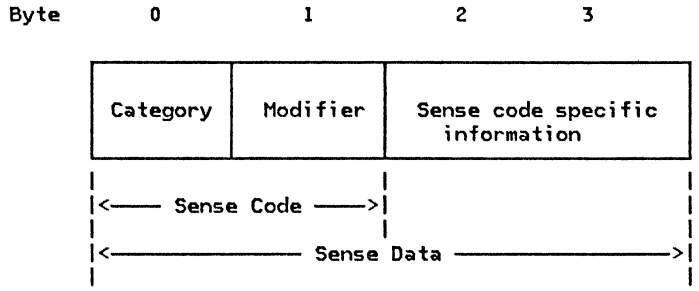


Figure G-1. Sense Data Format

Together, the category byte 0, the modifier byte 1, and the sense code specific bytes 2 and 3 hold the sense data defined for the exception condition that has occurred.

The following categories are defined; all others are reserved:

VALUE	CATEGORY
X'00'	User Sense Data Only
X'08'	Request Reject
X'10'	Request Error
X'20'	State Error
X'40'	Request Header (RH) Usage Error
X'80'	Path Error

The category User Sense Data Only (X'00') allows the end users to exchange sense data in bytes 2-3 for conditions not defined by SNA within the other categories (and perhaps unique to the end users involved). The modifier value is also X'00'. In earlier versions of SNA, user data (as well as implementation-specific data) generally could be carried in bytes 2-3 for all categories. This is no longer permitted. Bytes 2-3 are used only for SNA-defined conditions for non-zero categories.

The sense codes for the other categories are discussed below.

REQUEST REJECT (CATEGORY CODE = X'08')

This category indicates that the request was delivered to the intended component and was understood and supported, but not executed.

Category and modifier (in hexadecimal):

0801 Resource Not Available: The LU, PU, or link specified in an RU is not available.

0802 Intervention Required: Forms or cards are required at an output device, or a device is temporarily in local mode, or other conditions require intervention.

0803 Missing Password: The required password was not supplied.

0804 Invalid Password: Password was not valid.

0805 Session Limit Exceeded: The requested session cannot be activated, as one of the NAUs is at its session limit (e.g., LU-LU session limit, or [LU, mode] session limit). Applies to ACTCDRM, INIT, BIND, and CINIT requests.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0001 If accepted, the BIND request would prevent either the receiving LU or the sending LU from activating the number of contention winner sessions to the partner LU that were agreed upon during a change-number-of-sessions procedure.

0806 Resource Unknown: The request contained a name or address not identifying a PU, LU, link, or link station known to the receiver.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

0001 The resources identified in a subvector carrying an address list are unknown to the receiver.

Note: When this sense data flows in a -RSP to an NMVT, the referenced subvector carrying an address list is the one that was present in the request NMVT to which the -RSP corresponds. When this sense data flows in a Sense Data (X'7D') MS common subvector, the referenced subvector is present with the X'7D' subvector in the same major vector.

Note: In an interconnected network environment, this sense code may be set by an SSCP in whose subnetwork and domain the LU was expected to reside; it is not set by an SSCP that is only an intermediary on the session-setup path. A gateway SSCP examines the Resource Identifier control vector in a session setup request (e.g., CDINIT), to determine whether the LU is in the SSCP's subnetwork and domain.

0807 Resource Not Available--LUSTAT Forthcoming: A subsidiary device will be unavailable for an indeterminate period of time. LUSTAT will be sent when the device becomes available.

0808 Invalid Contents ID: The contents ID contained on the ACTCDRM request was found to be invalid.

0809 Mode Inconsistency: The requested function cannot be performed in the present state of the receiver.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

001C The RNAA request contains a network ID that is not known to the gateway PU.

001D An address pair session key in a Network-Qualified Address Pair control vector (X'15') is not known to the gateway PU.

001E A gateway PU received an RNAA request for a cross-network session and all possible address transforms for the named resource are allocated.

001F An SSCP has detected a specification of gateway responsibility in the CDINIT request that is not consistent with its own definition. For example, an SSCP that has predesignated responsibility to control a gateway node specified in the CDINIT request sends this sense data when it receives the CDINIT from a session partner and the CDINIT indicates that the session partner also has predesignated responsibility for the gateway node; in this situation, a mismatch exists in the responsibilities of the SSCPs, because both cannot simultaneously have predesignated responsibility for the gateway node.

0020 The gateway node receiving an RNAA request cannot support another session between the named resource pair.

0024 A PU received an ACTPU request with the SSCP-PU Session Capabilities control vector (X'0B') indicating that the sending SSCP does not support ENA, but the PU does not know the SSCP's maximum subarea address value.

0027 A request for a function was received by a component but the function was not enabled/activated.

080A Permission Rejected: The receiver has denied an implicit or explicit request of the sender; when sent in response to BIND, it implies either that the secondary LU will not notify the SSCP when a BIND can be accepted, or that the SSCP does not recognize the NOTIFY vector key X'0C'. (See the X'0845' sense code for a contrasting response.)

080B Bracket Race Error: Loss of contention within the bracket protocol. This error can arise when bracket initiation/termination by both NAUs is allowed

080C Procedure Not Supported: A procedure (Test, Trace, IPL, REQMS type, MS major vector key) specified in an RU is not supported by the receiver.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

0005 The MS major vector key is not supported by the receiver.

0006 The MS major vector is identified as one that contains a command, but the receiver does not recognize or support the command subvector. (See the X'086C' sense code for the case in which the command subvector is identified, but an additional required subvector is missing.)

0007 A request for a function is supported by the receiver, but the resource identified in the request does not support that function (no function is specifically indicated).

000A A request was received containing an address list MS subvector with multiple entries, but the receiver supports only a single entry in such a subvector.

080D NAU Contention: A request to activate a session was received while the receiving half-session was awaiting a response to a previously sent activation request for the same session; e.g., the SSCP receives an ACTCDRM from the other SSCP before it receives the response for an ACTCDRM that it sent to the other SSCP and the SSCP ID in the received ACTCDRM was less than or equal to the SSCP ID in the ACTCDRM previously sent.

080E NAU Not Authorized: The requesting NAU does not have access to the requested resource.

080F End User Not Authorized: The requesting end user does not have access to the requested resource.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

6051 Access Security Information Invalid: The request specifies an Access Security Information field that is unacceptable to the receiver; for security reasons, no further detail on the error is provided. This sense data is sent in FMH-7 or UNBIND.

0810 Missing Requester ID: The required requester ID was missing.

0811 Break: Asks the receiver of this sense code to terminate the present chain with CANCEL or with an FMD request carrying EC. The half-session sending the Break sense code enters chain-purge state when Break is sent; the half-session receiving the Break sense code discards the terminated chain without ever retransmitting it.

0812 Insufficient Resource: Receiver cannot act on the request because of a temporary lack of resources.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0004 The RNAA request indicates that the requested address must be pre-ENA compatible, but no pre-ENA compatible address is available.

0813 Bracket Bid Reject--No RTR Forthcoming: BID (or BB) was received while the first speaker was in the in-bracket state, or while the first speaker was in the between-brackets state and the first speaker denied permission. RTR will not be sent.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0001 Bracket Bid Reject: The component was in the in-bracket state when a bracket request was received.

0002 Bracket Bid Reject: The component was in the between-bracket state when a bracket request was received.

0814 Bracket Bid Reject--RTR Forthcoming: BID (or BB) was received while the first speaker was in the in-bracket state, or while the first speaker was in the between-brackets state and the first speaker denied permission. RTR will be sent.

0815 Function Active: A request to activate a network element or procedure was received, but the element or procedure was already active.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0001 A session activation request was received by a boundary function to activate a session that was already active.

0816 Function Inactive: A request to deactivate a network element or procedure was received, but the element or procedure was not active.

0817 Link or Link Resource Inactive: A request requires the use of a link or link resource that is not active.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

0001 Link inactive.

0002 Link station inactive.

0003 Switched link connection inactive.

0818 Link Procedure in Process: CONTACT, DISCONTACT, IPL, or other link procedure in progress when a conflicting request was received.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies

0004 Reserved.

0005 Link problem determination test for a modem in progress.

0006 Online terminal test in progress.

0007 SDLC link test, level 2, in progress.

0819 RTR Not Required: Receiver of READY TO RECEIVE has nothing to send.

081A Request Sequence Error: Invalid sequence of requests.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

0004 An NC_ER_TEST was to be sent as a result of receiving a ROUTE_TEST request. The ROUTE_TEST was sent in one subnetwork, the NC_ER_TEST was to be sent in another. The SSCP sending the ROUTE_TEST did not have a required alias address within the subnetwork where the NC_ER_TEST was to be sent. (Before sending ROUTE_TEST, the SSCP sends RNAA, or the installation predefines the alias address, so that an origin SSCP address is available within the subnetwork of the route being tested. This address is then specified in the NC_ER_TEST RU.)

081B Receiver in Transmit Mode: A race condition: normal-flow request received while the half-duplex contention state was not-receive, (*S,¬R), or while resources (such as buffers) necessary for handling normal-flow data were unavailable. (Contrast this sense code with X'2004', which signals a protocol violation.)

081C Request Not Executable: The requested function cannot be executed, because of a permanent error condition in the receiver.

081D Invalid Station/SSCP ID: The station ID or SSCP ID in the request was found to be invalid.

081E Session Reference Error: The request contained reference to a half-session that was neither active nor in the process of being activated (generally applies to network services requests).

081F Reserved

0820 Control Vector Error: Invalid data for the control vector specified by the target network address and key.

0821 Invalid Session Parameters: Session parameters were not valid or not supported by the half-session whose activation was requested.

0822 Link Procedure Failure: A link-level procedure has failed due to link equipment failure, loss of contact with a link station, or an invalid response to a link command. (This is not a path error, since the request being rejected was delivered to its destination.)

0823 Unknown Control Vector: The control vector specified by a network address and key is not known to the receiver.

0824 Logical Unit of Work Aborted: The current unit of work has been aborted; when sync point protocols are in use, both sync point managers are to revert to the previously committed sync point.

Bytes 2 and 3 may contain the following sense code specific information:

0000 For LU 6.2, Backout Initiated: A transaction program or its LU has initiated backout. The protected resources for the distributed logical unit of work are to be restored to the previously committed sync point. This sense data is sent only in FMH-7.

For non-LU 6.2, no specific code applies.

0825 Component Not Available: The LU component (a device indicated by an FM header) is not available.

0826 FM function not supported: A function requested in an FMD RU is not supported by the receiver.

0827 Intermittent Error--Retry Requested: An error at the receiver caused an RU to be lost. The error is not permanent, and retry of the RU (or chain) is requested.

0828 Reply Not Allowed: A request requires a normal-flow reply, but the outbound data flow for this half-session is quiesced or shut down, and there is no delayed reply capability.

0829 Change Direction Required: A request requires a normal-flow reply, but the half-duplex flip-flop state is not-send, (¬S,*R), CD was not set on the request, and there is no delayed reply capability.

082A Presentation Space Alteration: Presentation space altered by the end user while the half-duplex state was not-send, (¬S,*R); request executed.

082B Presentation Space Integrity Lost: Presentation space integrity lost (e.g., cleared or changed) because of a transient condition--for example, because of a transient hard-

ware error or an end user action such as allowing presentation services to be used by the SSCP. (Note: The end-user action described under X'082A' and X'084A' is excluded here.)

082C Resource-Sharing Limit Reached: The request received from an SSCP was to activate a half-session, a link, or a procedure, when that resource was at its share limit.

082D LU Busy: The LU resources needed to process the request are being used; for example, the LU resources needed to process the request received from the SSCP are being used for the LU-LU session.

082E Intervention Required at LU Subsidiary Device: A condition requiring intervention, such as out of paper, or power-off, or cover interlock open, exists at a subsidiary device.

082F Request Not Executable because of LU Subsidiary Device: The requested function cannot be executed, due to a permanent error condition in one or more of the receiver's subsidiary devices.

0831 LU Component Disconnected: An LU component is not available because of power off or some other disconnecting condition.

0832 Invalid Count Field: A count field contained in the request indicates a value too long or too short to be interpreted by the receiver, or the count field is inconsistent with the length of the remaining fields. Bytes 2 and 3 are used for sense code specific information:

nnnn Bytes 2 and 3 contain a binary count that indexes (zero-origin) the first byte of the invalid count field.

0833 Invalid Parameter (with Pointer and Complemented Byte): One or more parameters contained in fixed- or variable-length fields of the request are invalid or not supported by the NAU that received the request. Bytes 2 and 3 are used for sense code specific information:

nnmm Byte 2 contains a binary value that indexes (zero-origin) the first byte that contained an invalid parameter. Byte 3 contains a transform of the first byte that contained an invalid parameter: the bits that constitute the one or more invalid parameters are complemented, and all other bits are copied.

0834 RPO Not Initiated: A power-off procedure for the specified node was not initiated because one or more other SSCPs have contacted the node, or because a CONTACT, DUMP, IPL, or DISCONTACT procedure is in progress for that node.

0835 Invalid Parameter (with Pointer Only): The request contained a fixed- or variable-length field whose contents are invalid or not supported by the NAU that received the request. Bytes 2 and 3 are used for sense code specific information:

nnnn Bytes 2 and 3 contain a two-byte binary count that indexes (zero-origin) the first byte of the fixed- or variable-length field having invalid contents.

Note: This sense code is not used to report an invalid value in an MS major vector. If the invalid value occurs in a formatted MS subvector, then 086B is used. If it occurs in an unformatted subvector, then 0870 is used.

0836 PLU/SLU Specification Mismatch: For a specified LU-LU session, both the origin LU (OLU) and the destination LU (DLU) have only the primary capability or have only the secondary capability.

0837 Queuing Limit Exceeded: For an LU-LU session initiation request (INIT, CDINIT, or INIT-OTHER-CD) specifying (1) Initiate or Queue (if Initiate not possible) or (2) Queue Only, the queuing limit of either the OLU or the DLU, or both, was exceeded.

0838 Reserved

0839 LU-LU or SSCP-LU Session Being Taken Down: At the time an LU-LU session initiation or termination request is received, the SSCP of at least one of the LUs is either processing a CDTAKED request or is in the process of deactivating the associated SSCP-LU session.

083A LU Not Enabled: At the time an LU-LU session initiation request is received at the SSCP, at least one of the two LUs, although having an active session with its SSCP, is not ready to accept CINIT or BIND requests.

083B Invalid PCID: the received PCID for a new session duplicated the PCID assigned to another session, or the received PCID intended as an identifier for an existing session could not be associated with such an existing session.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

0001 The PCID contained in CDINIT(Initiate or Queue), INIT-OTHER-CD, or CDTAKED duplicates a PCID received previously in one of these requests.

083C Domain Takedown Contention: While waiting for a response to a CDTAKED, a CDTAKED request is received by the SSCP containing the SSCP-SSCP primary half-session. Contention is resolved by giving preference to the CDTAKED sent by the primary half-session.

083D Dequeue Retry Unsuccessful--Removed from Queue: The SSCP cannot successfully honor a CDINIT(Dequeue) request (which specifies "leave on queue if dequeue-retry is unsuccessful") to dequeue and process a previously queued CDINIT request (e.g., because the LU in its domain is still not available for the specified session), and removes the queued CDINIT request from its queue.

083E Reserved

083F Terminate Contention: While waiting for a response to a CDTERM, a CDTERM is received by the SSCP of the SLU. Contention is resolved by giving preference to the CDTERM sent by the SSCP of the SLU.

0840 Procedure Invalid for Resource: The named procedure is not supported in the receiver for this type of resource (e.g., (1) SETCV specifies boundary function support for a type 1 node but the capability is not supported by the receiving node, or (2) the PU receiving an EXECTEST or TESTMODE is not the primary PU for the target link.)

0841 Duplicate Network Address: In a cross-domain LU-LU session initiation request, the SSCP of the DLU determines that the OLU network address specified in the CDINIT request is a duplicate of an LU network address assigned to a different LU name.

0842 SSCP-SSCP Session Not Active: The SSCP-SSCP session, which is required for the processing of a network services request, is not active; e.g., at the time an LU-LU session initiation or termination request is received, at least one of the following conditions exists:

- The SSCP of the ILU and the SSCP of the OLU do not have an active session with each other, and therefore INIT-OTHER-CD cannot flow.
- The SSCP of the OLU and the SSCP of the DLU do not have an active session with each other, and therefore CDINIT or CDTERM cannot flow.

0843 Required Synchronization Not Supplied: For example, a secondary LU (LU type 2 or 3) received a request with Write Control Code = Start Print, along with RQE and ¬CD.

0844 Initiation Dequeue Contention: While waiting for a response to a CDINIT(Dequeue), a CDINIT(Dequeue) is received by the SSCP of the SLU. Contention is resolved by giving preference to the CDINIT(Dequeue) sent by the SSCP of the SLU.

0845 Permission Rejected--SSCP Will Be Notified: The receiver has denied an implicit or explicit request of the sender; when sent in response to BIND, it implies that the secondary LU will notify the SSCP (via NOTIFY vector key X'0C') when a BIND can be accepted, and the SSCP of the SLU supports the notification. (See the X'080A' sense code for a contrasting response.)

0846 ERP Message Forthcoming: The received request was rejected for a reason to be specified in a forthcoming request.

0847 Restart Mismatch: Sent in response to STSN, SDT, or BIND to indicate that the secondary half-session is trying to execute a resynchronizing restart but has received insufficient or incorrect information.

0848 Cryptography Function Inoperative: The receiver of a request was not able to decipher the request because of a malfunction in its cryptography facility.

0849 Reserved

084A Presentation Space Alteration: The presentation space was altered by the end user while the half-duplex state was not-send, (¬S,*R); request not executed.

084B Requested Resources Not Available: Resources named in the request, and required to honor it, are not currently available. It is not known when the resources will be made available.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

6002 The resource identified by the destination program name (DPN) is not supported.

6003 The resource identified by the primary resource name (PRN) is not supported.

6031 Transaction Program Not Available--Retry Allowed: The FMH-5 Attach command specifies a transaction program that the receiver is unable to start. Either the program is not authorized to run or the resources to run it are not available at this time. The condition is temporary. The sender is responsible for subsequent retry. This sense data is sent only in FMH-7.

084C Permanent Insufficient Resource: Receiver cannot act on the request because resources required to honor the request are permanently unavailable. The sender should not retry immediately because the situation is not transient.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 For LU 6.2, Transaction Program Not Available--No Retry: The FMH-5 Attach command specifies a transaction program that the receiver is unable to start. The condition is not temporary. The sender should not retry immediately. This sense data is sent only in FMH-7.

For non-LU 6.2, no additional information is specified.

hnnn where h≥8, i.e., the high-order bit in byte 2 is set to 1. The 15 low-order bits of bytes 2 and 3 contain a binary count that indexes (zero-origin) the first byte of the field found to be in error.

084D Invalid Session Parameters--BF: Session parameters were not valid or were unacceptable to the boundary function. Bytes 2 and 3 following the sense code contain a binary count that indexes (zero origin) the first byte of the fixed- or variable-length field having invalid contents.

084E Invalid Session Parameters--PRI: A positive response to an activation request (e.g., BIND) was received and was changed to a negative response because of invalid session parameters carried in the response. The services manager receiving the response will send a deactivation request for the corresponding session.

084F Reserved

0850 Link-Level Operation Cannot Be Performed: An IPL, dump, or RPO cannot be performed through the addressed link station because the system definition or current state of the hardware configuration does not allow it.

0851 Session Busy: Another session that is needed to complete the function being requested on this session is temporarily unavailable.

0852 Duplicative Session Activation Request: Two session activation requests have been received with related identifiers. The relationship of the identifiers and the resultant action varies by request. For BIND, it means that the BIND request was received with the same session instance identifier (in the structured subfield X'03' of the User Data field) as an active session's; the current request is refused.

0853 TERMINATE(Cleanup) Required: The SSCP cannot process the termination request, as it requires cross-domain SSCP-SSCP services that are not available. (The corresponding SSCP-SSCP session is not active.) TERMINATE(Cleanup) is required.

0854 Retired, formerly used for product-specific information.

0855 Reserved

0856 SSCP-SSCP Session Lost: Carried in the Sense Data field in a NOTIFY (Third-Party Notification vector, X'03') or -RSP(INIT_OTHER) sent to an ILU to indicate that the

activation of the LU-LU session is uncertain because the SSCP(ILU)-SSCP(OLU) session has been lost. (Another sense code, X'0842', is used when it is known that the LU-LU session activation cannot be completed.)

0857 SSCP-LU Session Not Active: The SSCP-LU session, required for the processing of a request, is not active; e.g., in processing REQECHO, the SSCP did not have an active session with the target LU named in the REQECHO RU.

0858 Reserved

0859 REQECHO Data Length Error: The specified length of data to be echoed (in REQECHO) violates the maximum RU size limit for the target LU.

085A Reserved

085B Reserved

085C Reserved

085D Reserved

085E Reserved

085F Reserved

0860 Function Not Supported--Continue Session: The function requested is not supported; the function may have been specified by a request code or some other field, control character, or graphic character in an RU. Bytes 2 and 3 are used for sense code specific information:

nnnn Bytes 2 and 3 contain a two-byte binary count that indexes (zero-origin) the first byte in which an error was detected. This sense code is used to request that the session continue, thereby ignoring the error.

0861 Invalid COS Name: The class of service (COS) name, either specified by the ILU or generated by the SSCP of the SLU from the mode table is not in the "COS name to VR identifier list" table used by the SSCP of the PLU.

Bytes 2 and 3 may contain the following sense code specific information:

0000 COS name was generated by the SSCP.

0001 COS name was generated by the ILU.

0003 CDINIT request (or response) contains a Session Initiation control vector that has class of service (COS) name fields that have not been properly specified. If the RU is a positive response, it is changed into a negative response and sent to the request sender; a CDTERM is sent to the CDINIT response sender. (This is to cover a system definition error in the event a gateway SSCP downstream from another gateway SSCP receives a CDINIT or RSP(CDINIT) without valid information in the appropriate COS name fields of the Session Initiation control vector.)

0862 Medium Presentation Space Recovery: An error has occurred on the current presentation space. Recovery consists of restarting at the top of the current presentation space. The sequence number returned is of the RU in effect at the top of the current presentation space.

nnnn Bytes 2 and 3 following the sense code contain the byte offset from the beginning of the RU to the first byte of the RU that is displayed at the top of the current presentation space.

0863 Referenced Local Character Set Identifier (LCID) Not Found: A referenced character set does not exist. Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code appplies.

hnnn where h≥8, i.e., the high-order bit in byte 2 is set to 1. The 15 low-order bits of bytes 2 and 3 contain a binary count that indexes (zero-origin) the first byte of the field found to be in error.

0864 Function Abort: The conversation was terminated abnormally. Other terminations may occur after repeated reexecutions; the request sender is responsible to detect such a loop.

Bytes 2 and 3 may contain the following sense code specific information:

0000 For LU 6.2, Premature Conversation Termination: The conversation is terminated abnormally; for example, the transaction program may have issued a DEALLOCATE_ABEND verb, or the program may have terminated (normally or abnormally) without explicitly terminating the conversation. This sense data is sent only in FMH-7.

For non-LU 6.2, no additional information is specified.

0001 System Logic Error--No Retry: A system logic error has been detected. No retry of the conversation should be attempted. This sense data is sent only in FMH-7.

0002 Excessive Elapsed Time--No Retry: Excessive time has elapsed while waiting for a required action or event. For example, a transaction program has failed to issue a conversation-related protocol boundary verb. No retry of the conversation should be attempted. This sense data is sent only in FMH-7.

0865 Retired.

0866 Retired.

0867 Sync Event Response: Indicates a required negative response to an (RQE,CD) synchronizing request.

0868 No Panels Loaded: Referenced format not found because no panels are loaded for the display.

0869 Panel Not Loaded: The referenced panel is not loaded for the display.

086A Subfield Key Invalid: A subfield key in an MS subvector was not valid in the conditions under which it was processed.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

nnmm Byte 2 following the sense code contains the subvector key (nn) of the subvector containing the unrecognized subfield, and byte 3 contains the unidentified subfield key (mm).

086B Subfield Value Invalid: The value of a subfield in an MS subvector is invalid for the receiver.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

nnmm Byte 2 following the sense code contains the subvector key (nn) of the subvector containing the invalid subfield, and byte 3 contains the subfield key (mm) of the invalid subfield.

(See sense code 0870 for the case in which the invalid value occurs in an unformatted subvector (that is, one not containing subfields with keys and lengths), or in the unformatted portion of a partially formatted subvector.)

086C Required Subvector Missing: One or more MS subvectors that are required by the receiver to perform some function are missing from the received list of subvectors.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

nn00 Byte 2 following the sense code contains the subvector key (nn) of one of the subvectors that is missing. Byte 3 is reserved (00).

Note: See the X'080C0006' sense data for the case in which the major vector key is recognized but a subvector representing the function to be performed cannot be identified.

0401 The SNA Address List (X'04') subvector is required, but was not the first subvector in the major vector.

086D Required Subfield Missing: An NMVT subvector lacks one or more subfield keys that are required by the receiver to perform the function requested.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

nnmm Byte 2 following the sense code contains the subvector key (nn) of the subvector lacking a required subfield, and byte 3 contains the subfield key (mm) of a missing subfield.

086F Length Error: A length field within an MS major vector is invalid, or two or more length fields are incompatible.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 Reserved

0001 The MS major vector length is incompatible with the RU length.

0002 The sum of the MS subvector lengths is incompatible with the MS major vector length.

nn03 The sum of the subfield lengths in a MS subvector is incompatible with the subvector length. Byte 3 following the sense code contains the subvector key (nn).

nn05 MS subvector length invalid. Byte 2 following the sense code contains the relevant subvector key (nn). (This is specified only if the sum of the subvector lengths is compatible with the major vector length.)

nn06 Subfield length invalid. Byte 2 following the sense code contains the subvector key (nn) of the MS subvector containing the invalid subfield length. (This is specified only if the sum of the subfield lengths is compatible with the subvector length.)

0870 Unformatted Subvector Value Invalid: A value in an unformatted MS subvector, or in an unformatted portion of a partially formatted MS subvector, is invalid.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

nnxx Byte 2 following the sense code contains the subvector key (nn) of the MS subvector containing the invalid value. Byte 3 contains a one-byte binary count that indexes the first byte in which the invalid value falls. The indexing is zero-origin, from the beginning of the subvector.

(See sense code 086B for the case in which the invalid value occurs in a formatted MS subvector, that is, one containing subfields with keys and lengths, or in the formatted portion of a partially formatted subvector.)

0871 Read Partition State Error: A Read Partition structured field was received while the display was in the retry state.

0872 Orderly Deactivation Refused: An NC_DACTVR(Orderly) request has been received, but sessions are assigned to the VR and it will not be deactivated.

0873 Virtual Route Not Defined: No ERN is designated to support this VRN.

0874 ER Not in a Valid State: The ER supporting the requested VR is not in a state allowing VR activation.

0875 Incorrect or Undefined Explicit Route Requested: The reverse ERNs specified in the NC_ACTVR do not contain the ERN defined to be used for the VR requested, or the ERN designated to be used for the VR is not defined.

0876 Nonreversible Explicit Route Requested: The ERN used by the NC_ACTVR does not use the same sequence of transmission groups (in reverse order) as the ERN that should be used for the RSP(NC_ACTVR).

0877 Resource Mismatch: The receiver of a request has detected a mismatch between its definition of an affected resource and the actual configuration.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0001 Link Defined as Switched Is Nonswitched: A link defined to an ACTLINK receiver as being switched was found to be nonswitched during the activation attempt.

0002 Link Defined as SDLC Is Non-SDLC: A link defined to an ACTLINK receiver as being SDLC was found to be non-SDLC during the activation attempt.

0003 Link Defined as Having Automatic Connect-Out Capability Does Not: A link defined to an ACTLINK receiver as having automatic connect-out capability was found to lack it during the activation attempt.

0004 ACTLINK Received for a Resource Other Than a Link: An ACTLINK was received that resolved to a local device address representing a device other than a link.

0878 Insufficient Storage: The storage resource required for a data format is not available.

0879 Storage Medium Error: A permanent error has occurred involving a storage medium.

087A Format Processing Error: A processing error occurred during data formatting.

087B Resource Unknown: The request contains a session key that does not identify a session known to some gateway node; e.g., a session activation request arrives at a gateway node after it has released the address transform for the intended session.

087C SSCP-PU Session Not Active: A gateway SSCP-PU session that is needed to establish an address transform for the intended cross-network LU-LU session was not active.

087D Session Services Path Error: A session services request--CDINIT, INIT_OTHER_CD, NOTIFY, or DSRLST--cannot be rerouted along a path of SSCP-SSCP sessions. This capability is required, for example, to set up a cross-network LU-LU session.

Bytes 2 and 3 contain sense code specific information that indicates the specific reason for not rerouting the request. Settings allowed are:

0000 Reserved

0001 An SSCP has attempted unsuccessfully to reroute a session services request to its destination via one or more adjacent SSCPs; this value is sent by a gateway SSCP when it has exhausted trial-and-error rerouting.

0002 An SSCP is unable to reroute a session services request because a necessary routing table is not available, that is, there is no adjacent SSCP table corresponding to the rerouting key in the Resource Identifier control vector. The receiver of this value will, if possible, try rerouting to another SSCP.

0003 An LU definition is needed to process the session services request. The LU has not been predefined and the request receiver does not support dynamic definition of LUs residing in other subnetworks or domains.

0004 Reserved

0005 An SSCP is unable to use the gateway node specified in CDINIT because that gateway node cannot allocate an address transform for the intended cross-network LU-LU session.

0006 An SSCP is able to use only a subset of the alternate gateway nodes available to it. However, for the subset that it can use, none can provide the needed alias address pair.

0007 Reserved

0008 A gateway SSCP is unable to reroute a CDINIT request because the adjacent SSCP does not support notification of resource availability (see control vector X'06' byte 5, bit 0) as requested in the received CDINIT. Resource availability notification support must have been indicated by the SSCP on the DLU side of a gateway SSCP if CDINIT rerouting is required.

087E SSCP Visit Count Exceeds Limit: The SSCP visit count specified in the session services request--CDINIT, INIT_OTHER_CD, or DSRLST--has been decremented to 0. The ses-

sion services request has been routed through an excessive number of SSCPs. (The SSCPs are not necessarily distinct.)

0881 ACTCDRM Failure--REQACTCDRM Sent: An SSCP-SSCP session-activation request, ACTCDRM, cannot be rerouted to a gateway SSCP because, at some gateway PU, the necessary transform is not complete and the gateway PU has sent REQACTCDRM to the gateway SSCP.

0884 ACTCDRM Failure--No REQACTCDRM Sent: An SSCP-SSCP session activation request, ACTCDRM, cannot be rerouted to the destination SSCP because, at some gateway node PU, the necessary transform is not complete and REQACTCDRM cannot be sent to the destination SSCP because the gateway SSCP-PU session is not active or the intended SSCP session partner does not provide gateway services.

0886 Subnetwork Rerouting Not Supported: An SSCP received a session services request--CDINIT, INIT_OTHER_CD, NOTIFY(Vector Key=X'01'), or DSRLST--from an SSCP in its subnetwork that, if rerouted, would not cross a subnetwork boundary. The SSCP does not support rerouting within a subnetwork.

0887 Dequeue Retry Unsuccessful--Session Remains Queued: The SSCP cannot successfully honor a CDINIT(Dequeue) request. The request specifies "leave on queue if dequeue-retry is unsuccessful." The SSCP has left the queued session on its queue.

0888 Name Conflict: A name specified in an RU is unknown for the specified resource type. When a name conflict is detected, further name checking ceases; multiple name conflicts are not reported or detected.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 Reserved.

0001 DLU real network name is unknown.

0002 DLU alias network name is unknown.

0003 OLU real network name is unknown.

0004 OLU alias network name is unknown.

0889 Transaction Program Error: The transaction program has detected an error.

This sense code is sent only in FMH-7.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 Program Error--No Data Truncation: The transaction program sending data detected an error but did not truncate a logical record.

Program Error--Purging: The transaction program receiving data detected an error. All remaining information, if any, that the receiving program had not yet received, and that the sending program had sent prior to being notified of the error, is discarded.

0001 Program Error--Data Truncation: The transaction program sending data detected an error and truncated the logical record it was sending.

0100 Service Transaction Program Error--No Data Truncation: The service transaction program sending data detected an error and did not truncate a logical record.

Service Transaction Program Error--Purging: The service transaction program receiving data detected an error. All remaining information, if any, that the receiving service transaction program had not yet received, and that the sending service transaction program had sent prior to being notified of the error, is discarded.

0101 Service Transaction Program Error--Data Truncation: The service transaction program sending data detected an error and truncated the logical record it was sending.

088A Resource Unavailable--NOTIFY Forthcoming: The SSCP cannot satisfy the request because a required resource is temporarily unavailable. When the required resource becomes available, NOTIFY NS(s) key X'07' or X'08' will be sent.

Bytes 2 and 3 may contain the following sense code specific information that indicates the specific reason for not rerouting the request:

0000 Reserved

0001 SSCP-SSCP Session Not Active: A SSCP-SSCP session required to reroute the cross-network request was not active.

0002 Reserved

0003 SSCP-LU session not active: The SSCP(DLU) is currently not in session with the DLU.

0004 LU session limit exceeded: The DLU is currently at its session limit and the requested session would cause the limit to be exceeded.

088B BB Not Accepted--BIS Reply Requested: Sent in response to a BB (either an LUSTAT bid or an Attach) to indicate that the receiver has sent a BIS request and wishes to terminate the session without processing any more conversations, but without sending an UNBIND. A BIS reply is requested so that the negative response sender may send a normal UNBIND. This sense code is sent only by LUs not supporting change-number-of-session protocols.

088D Duplicate Network Name: An SSCP has detected a violation of the requirement that network names used across multiple domains be unique within the multiple-domain network. For example, the SSCP(DLU) has detected that the OLU name received in CDINIT is currently also defined in the domain of the SSCP(DLU).

088E ENA Address Mismatch: An SSCP detected that an ENA LU has an address too large for one of the pre-ENA components (LU or SSCP) involved in the session to support. If both LUs are in the same domain, the SSCP responds negatively to the INIT-SELF or INIT-OTHER with this sense code. If the LUs are in different domains, either:

- The SSCP(OLU) detected the mismatch, and responds negatively to the INIT-SELF or INIT-OTHER with this sense code; or
- The SSCP(OLU) could not detect the mismatch and sent CDINIT to the SSCP(DLU), which detected the mismatch and responds negatively to the CDINIT with this sense code; upon receiving the -RSP(CDINIT), the SSCP(OLU) responds negatively to the INIT-SELF or INIT-OTHER with this sense code.

REQUEST ERROR (CATEGORY CODE = X'10')

This category indicates that the RU was delivered to the intended NAU component, but could not be interpreted or processed. This condition represents a mismatch of NAU capabilities.

Category and modifier (in hexadecimal):

1001 RU Data Error: Data in the request RU is not acceptable to the receiving component; for example, a character code is not in the set supported, a formatted data field is not acceptable to presentation services, a value specified in the length field (LL) of a structured field is invalid, or a required name in the request has been omitted.

1002 RU Length Error: The request RU was too long or too short.

1003 Function Not Supported: The function requested is not supported. The function may have been specified by a formatted request code, a field in an RU, or a control character.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

0001 The half-session receiving the request did not perform the function because it is not capable of doing so. The requesting half-session requested a function that the receiver does not support and the receiver did not specify that it was capable of supporting the function at session activation; consequently, there is an apparent mismatch of half-session capabilities.

Note: This is to cover a system error. For example, if the PU receiving a SETCV(Vector Key=X'15') is not a gateway PU, that is, the PU did not indicate in the ACTPU response that it is a gateway PU, the PU reports to the SSCP that sent the SETCV that there is an apparent mismatch of half-session capabilities.

0002 The half-session receiving the request did not perform the function, though it is capable of doing so. The requesting half-session did not specify at session activation that it was capable of supporting the function; consequently, there is an apparent mismatch of half-session capabilities.

Note: This is to cover a system error. For example, if the SSCP sending a SETCV(Vector Key=X'15') is not known to the receiving PU as a gateway SSCP, that is, the SSCP did not indicate in ACTPU that it is a gateway SSCP, the PU reports a mismatch of capabilities.

0003 The component received an unsupported normal-flow DFC command.

0004 The component received an unsupported expedited-flow DFC command.

0005 The component received a network control command during an LU-SSCP session.

0006 The component received an unsupported session control command during an LU-SSCP session.

0007 The component received an unsupported data flow control command with LU-SSCP session specified.

6002 The resource identified by the destination program name (DPN) is not supported.

6003 The resource identified by the primary resource name (PRN) is not supported.

(Note: This sense code can also be used instead of sense code X'0826'.)

1004 Reserved.

1005 Parameter Error: A parameter modifying a control function is invalid, or outside the range allowed by the receiver.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0001 For NMVT, the address type field in an SNA Address List subvector does not match the address type required by the command subvector.

1006 Reserved

1007 Category Not Supported: DFC, SC, NC, or FMD request was received by a half-session not supporting any requests in that category; or an NS request byte 0 was not set to a defined value, or byte 1 was not set to an NS category supported by the receiver.

1008 Invalid FM Header: The FM header was not understood or translatable by the receiver, or an FM header was expected but not present. This sense code is sent in FMH-7 or UNBIND.

Bytes 2 and 3 may contain the following sense code specific information:

0000 Reserved.

200E Invalid Concatenation Indicator: The concatenation indicator is on but concatenation is not allowed.

201D FM Header and Associated Data Mismatch: The FM header indicated associated data would or would not follow (e.g., FM header 7 followed by log data, or FM header 5 followed by program initialization parameters), but this indication was in error; or a previously received RU [e.g., -RSP(0846)] implied that an FM header would follow, but none was received.

4001 Invalid FM Header Type: The type of the FM header is other than 5 or 7.

6000 FM Header Length Not Correct: The value in the FM header Length field differs from the sum of the lengths of the subfields of the FM header.

6005 Access Security Information Length Field Not Correct: The value in the Access Security Information Length field differs from the sum of the lengths of the Access Security Information subfields.

6009 Invalid Parameter Length. The field that specifies the length of fixed-length parameters has an invalid setting.

600B Unrecogized FM Header Command Code: The partner LU received an FM header command code that it does not recognize. For LU 6.2, this sense data is sent only in FMH-7.

6011 Invalid Logical Unit of Work: The LUW Length field (in a Compare States GDS variable or an FMH-5) is incorrect or the LUW is invalid or a LUWID is not present but is required by the setting of the synchronization level field.

6021 Transaction Program Name Not Recognized: The FMH-5 Attach command specifies a transaction program name that the receiver does not recognize. This sense data is sent only in FMH-7.

6031 PIP Not Allowed: The FMH-5 Attach command specifies program initialization parameter (PIP) data is present but the receiver does not support PIP data for the specified transaction program. This sense data is sent only in FMH-7.

6032 PIP Not Specified Correctly: The FMH-5 Attach command specifies a transaction program name that requires program initialization parameter (PIP) data and either the FMH-5 specifies PIP data is not present or the number of PIP subfields present does not agree with the number required for the program. This sense data is sent only in FMH-7.

6034 Conversation Type Mismatch: The FMH-5 Attach command specifies a conversation type that the receiver does not support for the specified transaction program. This sense data is sent only in FMH-7.

6040 Invalid Attach Parameter: A parameter in the FMH-5 Attach command conflicts with the statement of LU capability previously provided in the BIND negotiation.

6041 Synchronization Level Not Supported: The FMH-5 Attach command specifies a synchronization level that the receiver does not support for the specified transaction program. This sense data is sent only in FMH-7.

1009 Format Group Not Selected: No format group was selected before issuing a Present Absolute or Present Relative Format structured field to a display.

STATE ERROR (CATEGORY CODE = X'20')

This category indicates a sequence number error, or an RH or RU that is not allowed for the receiver's current session control or data flow control state. These errors prevent delivery of the request to the intended component.

Category and modifier (in hexadecimal):

2001 Sequence Number: Sequence number received on normal-flow request was not 1 greater than the last.

2002 Chaining: Error in the sequence of the chain indicator settings (BCI, ECI), such as first, middle, first.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0001 The receiver received a middle or end-chain request when in the in-chain state.

0002 The receiver received a begin-chain request when in the in-chain state.

2003 Bracket: Error resulting from failure of sender to enforce bracket rules for session. (This error does not apply to contention or race conditions.)

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000 No specific code applies.

0001 The receiver received a begin-bracket request before receiving a response to its own previously sent begin-bracket request.

0002 The receiver received a begin-bracket request not specifying begin-bracket when in the between-bracket state.

0003 The receiver received an out-of-sequence LUSTAT command.

2004 Direction: Error resulting from a normal-flow request received while the half-duplex flip-flop state was not Receive.

2005 Data Traffic Reset: An FMD or normal-flow DFC request received by a half-session whose session activation state was active, but whose data traffic state was not active.

2006 Data Traffic Quiesced: An FMD or DFC request received from a half-session that has sent QUIESCE COMPLETE or SHUTDOWN COMPLETE and has not responded to RELEASE QUIESCE.

2007 Data Traffic Not Reset: A session control request (e.g., STSN), allowed only while the data traffic state is reset, was received while the data traffic state was not reset.

2008 No Begin Bracket: An FMD request specifying BBI=BB was received after the receiver had previously received a BRACKET INITIATION STOPPED request.

2009 Session Control Protocol Violation: An SC protocol has been violated; a request, allowed only after a successful exchange of an SC request and its associated positive response, has been received before such successful exchange has occurred (e.g., an FMD request has preceded a required CRYPTOGRAPHY VERIFICATION request). The request code of the particular SC request or response required, or X'00' if undetermined, appears in the fourth byte of the sense data.

200A Immediate Request Mode Error: The immediate request mode protocol has been violated by the request.

200B Queued Response Error: The Queued Response protocol has been violated by a request, i.e., QRI=¬QR when an outstanding request had QRI=QR.

200C ERP Sync Event Error: The ERP sync event protocol in DFC has been violated, e.g., after receiving a negative response to a chain, a request other than a request soliciting a synchronization event response was sent to DFC_SEND and rejected.

200D Response Owed Before Sending Request: An attempt has been made in half-duplex (flip-flop or contention) send/receive mode to send a normal-flow request when a response to a previously received request has not yet been sent.

200E Response Correlation Error: A response was received that cannot be correlated to a previously sent request.

200F Response Protocol Error: A violation has occurred in the response protocol; e.g., a +RSP to an RQE chain was generated.

2010 BIS Protocol Error: A BIS protocol error was detected; e.g., a BIS request was received after a previous BIS was received and processed.

2011 Pacing Error: A normal-flow request is received by a half-session after the pacing count has been reduced to 0 and before a pacing response has been sent.

2012 Invalid Sense Code Received: A negative response was received that contains an SNA-defined sense code that cannot be used for the sent request.

RH USAGE ERROR (CATEGORY CODE = X'40')

This category indicates that the value of a field or combination of fields in the RH violates architectural rules or previously selected BIND options. These errors prevent delivery of the request to the intended component and are independent of the current states of the session. They may result from the failure of the sender to enforce session rules. Detection by the receiver of each of these errors is optional.

Category and modifier (in hexadecimal):

4001 Invalid SC or NC RH: The RH of a session control (SC) or network control (NC) request was invalid. For example, an SC RH with pacing request indicator set to 1 is invalid.

4002 Reserved

4003 BB Not Allowed: The Begin Bracket indicator (BBI) was specified incorrectly, e.g., BBI=BB with BCI=¬BC.

4004 CEB or EB Not Allowed: The Conditional End Bracket indicator (CEBI) or End Bracket indicator (EBI) was specified incorrectly, e.g., CEBI=CEB when ECI=¬EC or EBI=EB with BCI=¬BC, or by the primary half-session when only the secondary may send EB, or by the secondary when only the primary may send EB.

4005 Incomplete RH: Transmission shorter than full TH-RH.

4006 Exception Response Not Allowed: Exception response was requested when not permitted.

4007 Definite Response Not Allowed: Definite response was requested when not permitted.

4008 Pacing Not Supported: The Pacing indicator was set on a request, but the receiving half-session or boundary function half-session does not support pacing for this session.

4009 CD Not Allowed: The Change Direction indicator (CDI) was specified incorrectly, e.g., CDI=CD with ECI=¬EC , or CDI=CD with EBI=EB.

400A No-Response Not Allowed: No-response was specified on a request when not permitted. (Used only on EXR.)

400B Chaining Not Supported: The chaining indicators (BCI and ECI) were specified incorrectly, e.g., chaining bits indicated other than (BC,EC), but multiple-request chains are not supported for the session or for the category specified in the request header.

400C Brackets Not Supported: The bracket indicators (BBI, CEBI, and EBI) were specified incorrectly, e.g., a bracket indicator was set (BBI=BB, CEBI=CEB, or EBI=EB), but brackets are not used for the session.

400D CD Not Supported: The Change-Direction indicator was set, but is not supported.

400E Reserved

400F Incorrect Use of Format Indicator: The Format indicator (FI) was specified incorrectly, e.g., FI was set with BCI=¬BC, or FI was not set on a DFC request.

4010 Alternate Code Not Supported: The Code Selection indicator (CSI) was set when not supported for the session.

4011 Incorrect Specification of RU Category: The RU Category indicator was specified incorrectly, e.g., an expedited-flow request or response was specified with RU Category indicator = FMD.

4012 Incorrect Specification of Request Code: The request code on a response does not match the request code on its corresponding request.

4013 Incorrect Specification of (SDI, RTI): The Sense Data Included indicator (SDI) and the Response Type indicator (RTI) were not specified properly on a response. The proper value pairs are (SDI=SD, RTI=negative) and (SDI=¬SD, RTI=positive).

4014 Incorrect Use of (DR1I, DR2I, ERI): The Definite Response 1 indicator (DR1I), Definite Response 2 indicator (DR2I), and Exception Response indicator (ERI) were specified incorrectly, e.g., a SIGNAL request was not specified with DR1I=DR1, DR2I=¬DR2, and ERI=¬ER.

4015 Incorrect Use of QRI: The Queued Response indicator (QRI) was specified incorrectly, e.g., QRI=QR on an expedited-flow request.

4016 Incorrect Use of EDI: The Enciphered Data indicator (EDI) was specified incorrectly, e.g., EDI=ED on a DFC request.

4017 Incorrect Use of PDI: The Padded Data indicator (PDI) was specified incorrectly, e.g., PDI=PD on a DFC request.

4018 Incorrect Setting of QRI with Bidder's BB: The first speaker half-session received a BB chain requesting use of a session (via LUSTAT(X'0006')), but the QRI was specified incorrectly, i.e., QRI = ¬QR.

4019 Incorrect Indicators with Last-In-Chain Request: A last-in-chain request has specified incompatible RH settings, e.g., RQE*, CEBI=¬CEB, and CDI=¬CD.

4021 QRI Setting in Response Different From That in Request: The QRI setting in the response differs from the QRI setting in the corresponding request.

PATH ERROR (CATEGORY CODE = X'80')

This category indicates that the request could not be delivered to the intended receiver, because of a path outage, an invalid sequence of activation requests, or one of the listed path information unit (PIU) errors. Some PIU errors fall into other categories; for example, sequence number errors are sense code category X'20'. A path error received while the session is active generally indicates that the path to the session partner has been lost.

Category and modifier (in hexadecimal):

8001 Intermediate Node Failure: Machine or program check in a node providing intermediate routing function. A response may or may not be possible.

8002 Link Failure: Data link failure.

8003 NAU Inoperative: The NAU is unable to process requests or responses, e.g., the NAU has been disrupted by an abnormal termination.

8004 Unrecognized Destination: A node in the path has no routing information for the destination specified either by the SLU name in a BIND request or by the TH.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0001 A request was received by a gateway function that could not be rerouted because of invalid or incomplete routing information.

8005 No Session: No half-session is active in the receiving end node for the indicated origination-destination pair, or no boundary function half-session component is active for the origin-destination pair in a node providing the boundary function. A session activation request is needed.

Bytes 2 and 3 may contain the following sense code specific information:

0000 No specific code applies.

0001 The receiver received a request other than session control request when no LU-LU session was active.

0002 The receiver received a request other than session control request when no LU-SSCP session was active.

0003 The receiver received a session control request other than BIND/UNBIND when no LU-LU session was active.

0004 The receiver received an UNBIND when no LU-LU session was active.

0005 The receiver received a session control request other than ACTLU/DACTLU for the LU-SSCP session when no LU-SSCP session was active.

0006 The receiver received DACTLU when no LU-SSCP session was active.

8006 Invalid FID: Invalid FID for the receiving node. (Note 1)

8007 Segmenting Error: First BIU segment had less than 10 bytes; or mapping field sequencing error, such as first, last, middle; or segmenting not supported and MPF not set to 11. (Note 2)

8008 PU Not Active: The SSCP-PU secondary half-session in the receiving node has not been activated and the request was not ACTPU for this half-session; for example, the request was ACTLU from an SSCP that does not have an active SSCP-PU session with the PU associated with the addressed LU.

8009 LU Not Active: The destination address specifies an LU for which the SSCP-LU secondary half-session has not been activated and the request was not ACTLU.

800A Too-Long PIU: Transmission was truncated by a receiving node because the PIU exceeded a maximum length or sufficient buffering was not available.

800B Incomplete TH: Transmission received was shorter than a TH. (Note 1)

800C DCF Error: Data Count field inconsistent with transmission length.

800D Lost Contact: Contact with the link station for which the transmission was intended has been lost, but the link has not failed. If the difference between link failure and loss of contact is not detectable, link failure (X'8002') is sent.

800E Unrecognized Origin: The origin address specified in the TH was not recognized.

800F Invalid Address Combination: The (DAF',OAF') (FID2) combination or the LSID (FID3) specified an invalid type of session, e.g., a PU-LU combination.

8010 Segmented RU Length Error: An RU was found to exceed a maximum length, or required buffer allocation that might cause future buffer depletion.

8011 ER Inoperative or Undefined: A PIU was received from a subarea node that does not support ER and VR protocols, and the explicit route to the destination is inoperative or undefined.

8012 Subarea PU Not Active or Invalid Virtual Route: A session-activation request for a peripheral PU or LU cannot be satisfied because there is no active SSCP-PU session for the subarea node providing boundary function support, or the virtual route for the specified SSCP-PU_T1|2 or SSCP-LU session is not the same as that used for the SSCP-PU session of the PU_T1|2's or LU's subarea PU.

8013 COS Not Available: A session activation request cannot be satisfied because none of the virtual routes requested for the session is available.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

Byte 2 indicates the environment in which the failure was detected:

00 Single network

01 Interconnected network: Failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

Byte 3 indicates the reason for the session-activation failure:

00 No Specific Code Applies: This means an error occured, but none of the conditions listed below applies.

01 No Mapping Specified: A session-activation request cannot be satisfied because for each VR in the VR identifier list for the session, no VR to ER mapping is specified.

02 No Explicit Routes Defined: A session-activation request cannot be satisfied because each VR in the VR identifier list for the session maps to a corresponding ER that is not defined.

03 No VR Resource Available: A session-activation request cannot be satisfied because each VR specified in the VR identifier list for the session requires a node resource that is not available.

04 No Explicit Routes Operative: A session-activation request cannot be satisfied because no underlying ER is operative for any VR specified in the VR identifier list for the session.

05 No Explicit Route Can Be Activated: A session-activation request cannot be satisfied because no VR specified in the VR identifier list for the session mapped to a defined and operative ER that could be activated.

06 No Virtual Route Can Be Activated: A session-activation request cannot be satisfied because no VR specified in the VR identifier list for the session can be activated by the PU, though for at least one VR an underlying ER is defined, operative, and activated.

07 No Virtual Route Identifier List Available: A session-activation request cannot be satisfied because a VR identifier list is not available.

Note: If none of the virtual routes specified in the VR identifier list for the session is active or can be activated, the reported reason is set based on a hierarchy of failure events. The "highest" of the failures that occurred within the set of virtual routes is returned on the response. For example, if the VR manager receives a negative response to an NC_ACTVR request for a VR specified in the VR identifier list and for all other VRs in the list no VR to ER mapping is specified, then reason X'06' is reported. The hierarchy of the failure reasons is in ascending numeric order, that is, reason X'02' is higher than reason X'01'.

8017 PIU from Adjacent Pre-ER-VR Subarea Node Rejected: A PIU that requires intermediate path-control routing was received by a subarea node from an adjacent subarea node that does not support ER-VR protocols, but the receiving subarea node does not support intermediate path-control routing for adjacent subarea nodes that do not support ER-VR protocols.

Notes:

1. It is generally not possible to send a response for this exception condition, since information (FID, addresses) required to generate a response is not available. It is logged as an error if this capability exists in the receiver.

2. If segmenting is not supported, a negative response is returned for the first segment only, since this contains the RH. Subsequent segments are discarded.

APPENDIX N. NOTATION

Figure N-1 illustrates the notation used in the flow diagrams in this book.

SNA-defined message units, such as the CDINIT RU, are capitalized. Representations of classes of RUs are in mixed case. The symbol "|" is used to mean "exclusive or." For example, "INIT-SELF|INIT-OTHER" means either INIT-SELF or INIT-OTHER. The symbol "*" is used to denote "any value." For example, "TERM*" means any RU whose acronym starts with "TERM".

Flows are shown by arrows, with "•" symbols in the columns of the components that send or receive the message unit. For example, component C sends RU 1 to component A; component B does not process the RU. Component C sends RU 2 to component B, which processes it and forwards it to component A.

A component must do something with the message unit besides the cross-network address transformation in order to have a "•" symbol in its column. Thus, even though an RU flowing between two gateway SSCPs is transferred between two networks by the gateway node, no "•" symbol appears in the gateway node column unless it does some processing related to the RU, such as requesting a virtual route in the second network in response to an ACTCDRM RU.

The numbers on the left correspond to explanations in the text.

Many RUs carry a list of optional control vectors. A list of control vectors is denoted "CV X'##', X'##',...," where ## is the hexadecimal number of a control vector.

The purpose of a NOTIFY RU is indicated by a NOTIFY vector. NOTIFY vectors are shown as the first parameter of a NOTIFY RU: "NOTIFY(X'##')," where ## denotes a hexadecimal number.

Negative responses carry sense data indicating the reason for the rejection of the request. Sense data is denoted "SD X'########'," where ## denotes a hexadecimal number. The final two bytes are generally omitted when they are X'0000'.

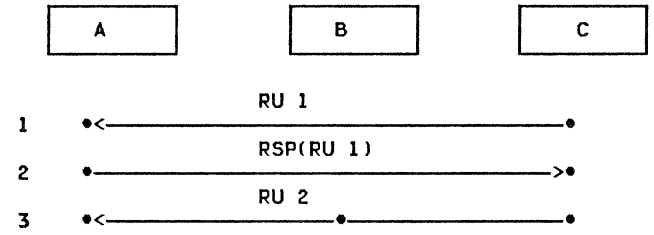


Figure N-1. Flow Notation Examples

APPENDIX T. TERMINOLOGY: ACRONYMS AND ABBREVIATIONS

ACTCDRM	ACTIVATE CROSS-DOMAIN RESOURCE MANAGER
ACTPU	ACTIVATE PHYSICAL UNIT
ASCII	American Standard Code for Information Interchange
BIND	BIND SESSION
BINDF	BIND FAILURE
CDCINIT	CROSS-DOMAIN CONTROL INITIATE
CDINIT	CROSS-DOMAIN INITIATE
CDRM	Cross-Domain Resource Manager
CDSESSEND	CROSS-DOMAIN SESSION ENDED
CDSESSSF	CROSS-DOMAIN SESSION SETUP FAILURE
CDSESSST	CROSS-DOMAIN SESSION STARTED
CDSESSTF	CROSS-DOMAIN SESSION TAKEDOWN FAILURE
CDTERM	CROSS-DOMAIN TERMINATE
CINIT	CONTROL INITIATE
CLEANUP	CLEAN UP SESSION
CONTACTED	CONTACTED
COS	class of service
CTERM	CONTROL TERMINATE
CV	control vector
DCTCDRM	DEACTIVATE CROSS-DOMAIN RESOURCE MANAGER
DACTPU	DEACTIVATE PHYSICAL UNIT

DLU	destination LU
DQ	dequeue
DSRLST	DIRECT SEARCH LIST
ENA	Extended Network Addressing
ER	explicit route
ER_TESTED	EXPLICIT ROUTE TESTED
Exp	expedited
EXR	EXCEPTION REQUEST
FM	function management
FMD	function management data
FMD NS(c)	function management data, network services, configuration services
FMD NS(ma)	function management data, network services, maintenance services
FMD NS(s)	function management data, network services, session services
FMH	FM header
FMP	FM profile
I	initiate
ID	identifier, identification
ILU	initiating LU (LU sending INIT-SELF)
INIT	initiate
INIT-OTHER	INITIATE-OTHER
INIT-OTHER-CD	INITIATE-OTHER CROSS DOMAIN
INIT-SELF	INITIATE-SELF

IPL	Initial Program Load
LNS	logical unit network services
LU	logical unit
MU	message unit
NAU	network addressable unit
NC	network control
NC-ER-TEST-REPLY	EXPLICIT ROUTE TEST REPLY
Norm	normal
NS	network services
OLU	origin LU
PC	path control
PCID	procedure correlation identifier
PLU	primary LU
PU	physical unit
PU_T4|5	physical unit in a type 4 or type 5 node
PUCP	physical unit control point
Q	queue, queued
REQACTCDRM	REQUEST ACTIVATION OF CROSS-NETWORK RESOURCE MANAGER
RH	request/response header
RNAA	REQUEST NETWORK ADDRESS ASSIGNMENT

ROUTE-INOP	ROUTE INOPERATIVE
ROUTE-TEST	ROUTE TEST
RQ	request
RSP	response
RU	request/response unit
SA	search argument
SC	session control
SC	session connector
SD	sense data
SESSEND	SESSION ENDED
SESSST	SESSION STARTED
SETCV	SET CONTROL VECTOR
SLU	secondary LU
SNA	Systems Network Architecture
SNI	SNA Network Interconnection
SON	session outage notification
SSCP	system services control point
TERM	terminate, terminating, termination, terminal
TERM-OTHER	TERMINATE-OTHER
TERM-SELF	TERMINATE-SELF
TH	transmission header
TLU	terminating logical unit (LU sending TERM)

UNBIND	UNBIND SESSION
UNBINDF	UNBIND FAILURE
URC	user request correlation
VR	virtual route

SPECIAL CHARACTERS

A

B

C

D

E

F

G

I

L

M

N

T

U

V

Systems Network Architecture
Format and Protocol
Reference Manual:
SNA Network
Interconnection

Order No. SC30-3339-0

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Note: Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

What is your occupation?_____

Number of latest Newsletter associated with this publication:_____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Reader's Comment Form

Fold and tape | Please Do Not Staple | Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Dept. E01
P.O. Box 12195
Research Triangle Park, N.C. 27709-2195

Fold and tape | Please Do Not Staple | Fold and tape

SC30-3339-00