Communications Server
for Windows®

ネットワーク管理の手引き

バージョン 6.1.3

SC88-5641-03
(英文原典：SC31-8656-03)

Communications Server
for Windows®

ネットワーク管理の手引き

バージョン 6.1.3

SC88-5641-03
(英文原典：SC31-8656-03)

お願い

本書および本書で紹介する製品をご使用になる前に、 203 ページの『付録 B. 特記事項』に記載されている情報をお読みください。

本書は、Communications Server for Windows バージョン 6.1.3、および新しい版またはテクニカル・ニュースレターで明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

IBM 発行のマニュアルに関する情報のページ

`http://www.ibm.com/jp/manuals/`

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： SC31-8656-03
Communications Server for Windows®
Network Administration Guide
Version 6.1.3

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第4版第1刷 2007.11

目次

図

表

本書について

IBM® Communications Server for Windows® は通信サービス・プラットフォームです。このプラットフォームは、ホスト・コンピューターおよび他のワークステーションと通信する Windows ワークステーション用の幅広い範囲のサービスを提供します。 Communications Server のユーザーは、さまざまなリモート接続オプションを選択することができます。

本書には、Communications Server 機能の概要、およびサポートするワークステーション用として Communications Server 構成の作成に必要なステップを記載してあります。用語の *Communications Server* は、特に指定されなければ、Windows バージョンの製品を指します。

本書の対象読者

この「ネットワーク管理の手引き」(Communications Server を使用する上での計画と管理の情報源) の対象読者は、この製品の使用と計画を行うご担当です。本書は、管理担当者、技術支援担当者、サービス・コーディネーター、および IBM 社員だけでなく、情報システムについて決定を行う責任のある方は、どなたにも役立ちます。

本書の構成

必要な情報の取得...	参照先...
Communications Server に関する情報	1 ページの『第 1 章 Communications Server 機能の紹介』
Communications Server が提供する SNA ネットワーク機能に関する情報	21 ページの『第 2 章 Communications Server および SNA』
AnyNet® サポートのインプリメンテーションに関する情報	73 ページの『第 3 章 AnyNet サポートの計画』
クライアント/サーバー通信のインプリメンテーションに関する情報	89 ページの『第 4 章 クライアント/サーバー通信の計画』
高性能経路指定 (HPR) サポートのインプリメンテーションに関する情報	95 ページの『第 5 章 HPR の計画』
SNA ゲートウェイ・サポートのインプリメンテーションに関する情報	101 ページの『第 6 章 SNA ゲートウェイの計画』
TN3270E サーバー機能のインプリメンテーションに関する情報	109 ページの『第 7 章 TN3270E サーバーの計画』
TN5250 サーバー機能のインプリメンテーションに関する情報	117 ページの『第 8 章 TN5250 サーバーの計画』
Secure Sockets Layer ベース・セキュリティーのインプリメンテーションに関する情報	123 ページの『第 9 章 Secure Sockets Layer ベース・セキュリティーの計画』
従属型 LU および LU6.2 セッションのロード・バランシングに関する情報	133 ページの『第 10 章 ロード・バランシングの計画』

必要な情報の取得...	参照先...
バックアップ・ホスト接続オプションに関する情報	137 ページの『第 11 章 バックアップ・ホスト接続の計画』
X.25 プランニングの考慮事項に関する情報	145 ページの『第 12 章 X.25 の計画』
ホスト接続のための構成方法に関する情報	149 ページの『第 13 章 ホスト接続の構成』
ネットワーク用ソフトウェアのインストールおよび構成に関する情報	173 ページの『第 14 章 Communications Server 構成のインプリメント』
Communication Server システム管理機能の概要について	193 ページの『第 15 章 システム管理機能』
Communications Server 環境を計画するための必要情報	197 ページの『付録 A. Communications Server の計画』

IBM サービスへの連絡方法

緊急に支援が必要な場合は、以下の Web サイトをご利用ください。
http://www.ibm.com/software/network/commserver/windows/support

たいていの問題はこの Web サイトで解決できます。この Web サイトで質問と問題報告書を、各種の診断情報をアクセスする場合と同様に、電子的に発信することができます。

問題診断と解決のために電話相談される場合は、いつでも IBM ソフトウェア・サポート・センター (1-800-IBM-SERV) に連絡してください。これに対する返信は 8 勤務時間内 (月曜日 - 金曜日、午前 8:00 - 午後 5:00、お客様の地方時間) に行います。

米国またはプエルトリコ以外のお客様は、IBM 担当員または担当の認可済み IBM ビジネス・パートナーに連絡してください。

本書で使用する規則および用語

本書で使用する規則は、より効率的な本書の使用に役立ちます。

- **太字体**の用途:
  - プログラムまたはコマンド・プロンプトで使用できる動詞、機能、パラメーター。これらの値には大文字小文字の区別があり、テキストに記載されているとおりに正確に入力しなければなりません。
  - リスト、チェック・ボックス、入力フィールド、プッシュボタン、およびメニュー選択などのウィンドウ制御の名前。
- *イタリック体* の用途:
  - 値を提供する変数
  - 資料の表題
  - 文字として使用されている文字、または単語として使用されている語。例えば、*a* と記載されている場合、それが *an* であってはいけないことを表しています。
- ***太字のイタリック体*** は、語を強調するために使用されます。

- 大文字は、プログラムまたはコマンド・プロンプトで使用できる定数、ファイル名、キーワード、およびオプションを表します。これらの値は、大文字でも小文字でも入力できます。
- 例のタイプは、コマンド・プロンプトまたはウィンドウに入力を指示する情報を表します。
- 二重引用符は、ウィンドウに表示されるメッセージを示します。 この一例には、エミュレーター・セッションの操作員情報域 (OIA) に表示されるメッセージがあります。
- 2 進数は、B'xxxx xxxx' または B'x' のように表されます。ただし、例外としては、テキストとともに表示されるある種の例 (「2 進数 xxxx xxxx の値は、...です」) の場合を除きます。
- ビット位置は右端 (最下位ビット) の位置である 0 から始まります。
- 5 桁以上の 10 進数は、メートル法で表されます。 3 桁のグループを区切る際には、コンマではなくスペースが使用されます。 例えば、16147 という数は、16 147 と記載されます。
- 16 進数は、16 進数 xxxx または X'xxxx' のテキストで表されます (『例えば、隣接ノードのアドレスが 16 進数 5D の場合、X'5D' としても指定されます。』)。

本書は、異なるタイプの情報を見つけやすくするために、テキスト内にアイコン (ピクチャー) も使用します。

このアイコンは「要注意」を表し、Communications Server の操作または作業の完了に影響を及ぼすことがある重要な情報であることを意味します。

このアイコンは作業の完了を支援することが可能なヒントまたは追加情報であることを表します。

本書で使用される用語および省略語の定義については、 IBM 用語の Web サイトで最新の IBM 用語を確認できます。

前提条件および関連情報

この節では、Communications Server または関連製品の使用時に役立つ情報元について説明します。

必須の情報

Communications Server ライブラリー

以下の文書は Communications Server for Windows CD-ROM で Adobe Acrobat Portable Document Format (PDF) の形式で提供されます。

表 1. Communications Server for Windows ライブラリー

資料番号	表題	記述
GC88-7699	*概説およびインストール*	Communications Server および当製品が提供するアクセス機能およびエミュレーターの概要を提供します。さらに、インストールおよび構成情報についても提供します。
SC31-8425	*Client/Server Communications Programming*	Communications Server によってサポートされる拡張プログラム間通信機能 (APPC) のアプリケーション・プログラミング・インターフェース (API) サポートについて解説しています。
SC88-5640	*構成ファイル解説書*	ASCII エディターを使用して構成ファイルのコピーまたは変更方法について解説しています。この資料には、構成ファイルのすべてのキーワードおよびその有効な値がリストされています。
SC88-5641	*ネットワーク管理の手引き*	Communications Server を使用するネットワークの計画と保守について、ネットワーク管理者が使用するための情報を提供します。
SC31-8426	*System Management Programming*	Communications Server を使用してプログラムを開発するための Node Operator Facility (NOF) API メッセージの使用法について解説しています。

本書に掲載されている資料の注文については、担当の IBM ビジネス・パートナーまたは営業担当員に連絡してください。

資料は CD-ROM から直接表示できます。 PDF ファイルは以下の場所にあります。

クライアント/サーバー・コミュニケーション・プログラミング

auxiliaryfiles¥sdk¥pubs¥<*lang*>¥cscsp.pdf

ここで、***<lang>*** は以下の言語のうちの 1 つです。

- chs
- cht
- deu
- enu
- esp
- fra
- ita
- jpn
- kor
- ptb

構成ファイル解説書

auxiliaryfiles¥doc¥<*lang*>¥cscfr.pdf

ここで、**<*lang*>** は以下の言語のうちの 1 つです。

- chs
- cht
- deu
- enu
- esp
- fra
- ita
- jpn
- kor
- ptb

ネットワーク管理の手引き

auxiliaryfiles¥doc¥<*lang*¥csnag.pdf

ここで、**<*lang*>** は以下の言語のうちの 1 つです。

- chs
- cht
- deu
- enu
- esp
- fra
- ita
- jpn
- kor
- ptb

概説およびインストール

auxiliaryfiles¥doc¥<*lang*¥csqkb.pdf

ここで、**<*lang*>** は以下の言語のうちの 1 つです。

- chs
- cht
- deu
- enu
- esp
- fra
- ita
- jpn
- kor
- ptb

SNA Management Services formats

auxiliaryfiles¥sdk¥pubs¥snams.pdf

SNA Format Reference

auxiliaryfiles¥sdk¥pubs¥snafmt.pdf

SNA Format Reference

auxiliaryfiles¥doc¥snafmt.pdf

システム管理プログラミング

auxiliaryfiles¥sdk¥pubs¥<*lang*>¥cssmp.pdf

ここで、**<*lang*>** は以下の言語のうちの 1 つです。

- chs
- cht
- deu
- enu
- esp
- fra
- ita
- jpn
- kor
- ptb

CPIC Reference

auxiliaryfiles¥sdk¥pubs¥cpicref.pdf

関連情報

追加情報は以下の関連資料にあります。

- *Common Programming Interface Communications Reference* SC26-4399

  CPI 通信について解説されています。この資料は CPI 通信をサポートしている通信製品を使用するアプリケーションの開発プログラマーを対象にしています。 Communications Server CD-ROM に HTML および PDF 形式で収められています。

- *IBM Dictionary of Computing*

  IBM 製品の文書に使用されている技術用語が定義されています。 Web サイトの http://www.ibm.com/networking/nsg/nsgmain.htm から使用できます。

- *Systems Network Architecture Formats* GA27-3136

  サブエリア・ノードと周辺ノード間、および APPN またはローエントリー・ネットワーキング (LEN) プロトコルをインプリメントするノード間で使用される SNA フォーマットについて解説されています。 Communications Server CD-ROM に PDF 形式で収められています。

- *Systems Network Management Services Reference* GC31-8302

  サブエリア・ネットワーク内のノード間、および APPN またはローエントリー・ネットワーキング (LEN) プロトコルあるいは両方をインプリメントするノード間で使用される SNA 管理サービス・フォーマットについて解説されています。 Communications Server CD-ROM に PDF 形式で収められています。

改訂の要約

SC88-5641-03
V6.1.3 の変更の要約

本書には V6.1 をサポートする SC88-5641-02 に既に提供されている情報が記載されています。

新規情報

- サーバーおよびリモート API クライアント オペレーティング・システムは、以下のプラットフォームでサポートされています。
  - Windows® Vista (32 ビットのみ)
- Windows NT® はサーバーでもうサポートされません。
- 以下のオペレーティング・システムの SNA API クライアント:
  - Windows Server 2003 (64 ビット)
  - Windows Vista (32 ビットおよび 64 ビット)
- Enterprise Extender は IPv6 をサポートします。
- Microsoft ソフトウェア・インストーラー (MSI) による簡易インストール
- Connection Network Reachability Awareness サポート
- HPR パフォーマンスを改善するための RTP 調整パラメーター
- LU 6.2 LU 6.2 セッション・レベルのタイムアウト。 39 ページの『LU 6.2 セッション・レベルのタイムアウト』を参照してください。
- 一層簡単なマイグレーションのための CPI-C Communication Server 互換性ツール
- Synchronous SLI Close for Microsoft の互換性により、Microsoft HIS Server から Communications Server for Windows にアプリケーションをマイグレーションできるようになります。

変更情報

- Tivoli® Plus サポートは IBM Tivoli License Manager (ITLM) で置き換えられます。

削除情報

- Windows NT オペレーティング・システム・サポート
- IBM AnyNet Sockets over SNA
- AS/400® 共用フォルダー
- Web 管理
- 通信ポート・サポート
- AS/400 接続のための Twinax サポート
- SDLC および X.25 WAC サポート

第 1 章 Communications Server 機能の紹介

この章では、Communications Server がサポートする通信機能とその機能を実行するためのシステムの構成方法について、概要を記載しています。 各機能と構成方法の詳細については、第 2 章以降で説明します。

サポートされる機能

このセクションでは、次の Communications Server 機能について説明します。

- SNA 通信サポート
- 拡張プログラム間通信機能 (APPC)。これには 拡張対等通信ネットワーク機能 (APPN) が含まれます。
- 32 ビット・アプリケーション・プログラミング・インターフェース (API)
- 高性能経路指定 (HPR)
- SNA データ圧縮
- サービス提供者のディスカバリー
- 従来型 LU アプリケーション (LUA)
- 従属 LU リクエスター (DLUR)
- SNA ゲートウェイ・サポート
- AnyNet サポート
  - AnyNet SNA over TCP/IP (アクセス・ノードとゲートウェイ)
- TN3270E サーバー
- TN5250 サーバー
- レガシー・データ・アクセス
  - iSeries™ OLE DB プロバイダー
- SNA API クライアント・サポート
- 構成および管理のサポート
- ロード・バランシング
- データ機密保護
- アダプター・サポート
- データ・リンク制御 (DLC) サポート
- APPN MIB サポート
- ホット・スタンバイ

SNA 通信サポート

Communications Server はシステム・ネットワーク体系 (SNA) タイプ 2.0 および SNA タイプ 2.1 ノードとして機能することができます。このサポートにより、他の多くの IBM SNA プロダクトと通信するプログラムを作成することができます。

APPC/APPN

Communications Server は、ワークステーションに拡張対等通信ネットワーク機能 (APPN) エンド・ノード、およびネットワーク・ノードのサポートを提供し、ネットワーク内でワークステーションが他のシステムと、一層柔軟に通信できるようにし

ます。 また、Branch Extender 機能によってブランチを切り離して、不必要な CP-CP トラフィックを回避することができます。

Communications Server は、トランザクション・プログラム (TP) と呼ばれる分散処理プログラム間の通信をサポートする、拡張プログラム間通信機能 (APPC) を提供します。TP は、ネットワーク中で APPC を提供するいずれのノードにあってもかまいません。 APPC は、LU 6.2 プロトコルを使用して別の論理装置 (LU) にあるプログラム間のデータ交換をします。さらに、APPC は、複数の同時リンクと並列セッションをサポートします。通信プログラム間の会話またはセッション機密保護も、 APPC を介してサポートされています。

Communications Server は、パフォーマンスが重要な意味を持つ LAN 環境で APPC スループットを向上させます。 Communications Server は、以下の接続のサポートを提供します。

表 2. サポートされる APPC 接続

プロトコル	接続	接続タイプ
チャネル	• CDLC (OEM) • MPC	
LAN (802.2)	• トークンリング • イーサネット • フレーム・リレー • ATM LAN エミュレーション	
SDLC	• 同期 • 非同期 • モデム	• 自動ダイヤル呼び出し、DTR ダイヤル呼び出し、永続 • 自動ダイヤル呼び出し • 自動ダイヤル呼び出し、永続
X.25	• 同期 • Hayes AutoSync • X.25 ネットワーク	• 自動ダイヤル呼び出し、半永続 • 自動ダイヤル呼び出し、永続 • 自動ダイヤル呼び出し
IP	SNA over IP	IP 提供の接続
IP	HPR over IP	IP 提供の接続

注: APPC/APPN にはさらにデータ圧縮機能があります。 データ圧縮に関する詳細については、 60 ページの『データ圧縮』を参照してください。 また、暗号化については、 63 ページの『SNA セッション・レベル暗号化』を参照してください。

SNA LU タイプ 6.2 サポート

LU 6.2 は、プログラム間通信のためのアーキテクチャーです。 Communications Server は、以下の任意選択の SNA LU 6.2 機能をサポートします。

- 基本およびマップ式会話
- 確認の同期レベル

- セッション・レベルおよび会話レベルの機密保護サポート
- 複数 LU
- 並列セッション。リモート・システムを使用してセッション数を変更する機能を含みます。
- 単方向同時モードまたは双方向同時モードのいずれかのトランザクション
- SSCP-PU セッションのある並行複数リンク。各リンクはそれぞれサブエリア・ネットワークと接続することができます。

機能の完全なリストは、「*Communications Server Programming Guide and Reference*」 を参照してください。

APPC 構成の拡張

基本エンド・ノード構成に必要なパラメーターは、ネットワーク ID、ローカル・ノード名、リンク・タイプ、宛先アドレスの 4 つのみです。 次のものにより、システム定義が少なくなりました。

- IBM 提供のモード
- 会話割り振り時のパートナー LU およびモード定義の暗黙作成
- セッション限度の暗黙の初期化 (CNOS 機能)。これにより、会話を割り振る前にセッション限度を明示的に初期化する必要がなくなります。
- ローカル LU およびパートナー LU のセッション限度の除去。これにより、モード・セッション限度の構成および初期化における自由度が拡大されます。
- トランザクション・プログラム名、操作、およびタイプのデフォルト値。これにより、適用されるプログラムのためのトランザクション・プログラム定義の必要がなくなります。
- 動的構成更新
- SNA ゲートウェイの暗黙ワークステーション定義
- 構成パラメーターを含む .ACG ファイルの編集機能
- Discovery でシステム定義情報を検出する機能

SNA 構成はテキスト・ファイルとして保管されるため、エディター、またはユーザーが作成したプログラムを使用して、迅速かつ容易にファイルを修正することができます。次に、Communications Server を停止せずに、アクティブな構成の検査および動的更新を行うことができます。

これで、複数のホストとの接続を構成できるようになり、複数のホスト接続を同時に活動状態にすることができます。要求時対応で開始するように接続を設定するか、あるいはホット・スタンバイの失敗の結果として接続を開始するように、設定できます。

Communications Server がディスカバリーをサポートすると、ノードでは、制御点名と、トークンリングまたはイーサネット LAN 上の別の Communications Server のネットワーク・ノード・サーバーのメディア・アクセス制御 (MAC) アドレスとサービス・アクセス・ポイント (SAP) アドレスを動的に検出できるようになります。つまり、パートナー・マシンへの接続を定義する前に、そのパートナー・マシンの制御点名、MAC アドレス、SAP アドレスをユーザーが知る必要はありません。 現在、iSeries Client Access、Host On-Demand、 Communications Server for Windows エンド・ノードおよびパーソナル・コミュニケーションズのユーザーがこの機能を使用できます。

APPC の基本概念

このセクションでは、APPC の概念と用語を紹介します。

トランザクション・プログラム

トランザクション・プログラム (TP) は、APPC 通信機能を使用する 1 つのプログラム、または 1 つのアプリケーション・プログラムの一部です。アプリケーション・プログラムはこれらの機能を使用して、 APPC をサポートする他のシステムのアプリケーション・プログラムと通信します。

Communications Server は APPC API を提供し、トランザクション・プログラムに対して IBM システム・アプリケーション体系 (SAA®) コミュニケーション・インターフェース (CPI-C) 呼び出しのための共通プログラミング・インターフェースをサポートします。

トランザクション・プログラムは、APPC 機能を呼び出すために、APPC パラメーターを渡します。 パラメーター とは一種の形式化された要求であり、それをトランザクション・プログラムが出し、APPC が実行します。あるプログラムは一連の APPC パラメーターを使用して別プログラムと通信します。 互いに通信する 2 つのプログラムは、別々のシステムにあっても同じシステムにあってもかまいません。いずれの場合にも APPC API は同じです。

あるトランザクション・プログラムが別トランザクション・プログラムとデータを交換時に、その別トランザクション・プログラムは、パートナー ・トランザクション・プログラムと呼ばれます。

トランザクション・プログラムは CPI-C 呼び出しを出すことができます。これらの呼び出しにより、アプリケーション・プログラムは SAA が提供する一貫性を利用することができます。

論理装置

各トランザクション・プログラムは、*論理装置* (LU) を介して SNA ネットワークにアクセスします。 LU とは、ユーザーのプログラムからパラメーターを受け入れ、それらのパラメーターに従って動作する SNA ソフトウェアです。 トランザクション・プログラムは、LU に APPC パラメーターを渡します。 これらのパラメーターによって、コマンドおよびデータが、ネットワークを経由してパートナー LU に流れるようになります。 LU は、トランザクション・プログラムとネットワークの中継者としても働き、トランザクション・プログラム間のデータの交換を管理します。 1 つの LU で、複数のトランザクション・プログラムにサービスを提供することができます。また、 1 つのノード内で複数 LU を同時に活動状態にすることができます。

LU タイプ

Communications Server は、LU タイプ 0、1、2、3、および 6.2 をサポートします。 LU タイプ 0、1、2、および 3 は、ホスト・アプリケーション・プログラムと、端末やプリンターなど各種の装置との間の通信をサポートします。

LU 6.2 は、タイプ 5 のサブエリア・ノードまたはタイプ 2.1 の周辺ノード、あるいはその両方にあるプログラム間の通信、およびプログラムと装置との通信をサポートします。 APPC は LU 6.2 体系を実現したものです。

LU セッション

トランザクション・プログラムが相互に通信できるまでは、LU は、セッションと呼ばれる相互関係で接続されている必要があります。 セッションは 2 つの LU を接続するので、LU-LU セッションと呼ばれます。 図 1 は、この通信関係を示しています。

図 1. 2 つの LU 間のセッション (LU-LU)

セッションは、SNA ネットワーク内の 1 対の LU 間のデータの移動を管理する導管として働きます。特に、セッションは、伝送されるデータの量、データ機密保護、ネットワーク経路指定、およびトラフィックの輻輳などを扱います。

セッションは LU によって維持されます。 通常、トランザクション・プログラムはセッション特性を取り扱いません。 セッション特性は、以下の処理を行うときにユーザーが定義します。

- システムを構成するとき。
- **SNA ノード・オペレーション** を使用するとき。
- 管理パラメーターを使用するとき。

トランザクション・プログラムの会話

トランザクション・プログラム間の通信は、*会話* と呼ばれます。電話での会話と同じように、一方のトランザクション・プログラムが相手を呼び出して「会話」を行い、一度に 1 つのトランザクション・プログラムだけが話をします。会話は一方のトランザクション・プログラムが話を終了するまで続きます。ある会話が始まるのは、トランザクション・プログラムが、会話を割り振る APPC パラメーターまたは CPI-C 呼び出しを出した時点です。会話は LU-LU セッションを介して行われます。

セッションに会話を割り振ると、会話に接続されたトランザクション・プログラム相互間に送受信の関係が確立されます。 1 つのトランザクション・プログラムは、データを送信するパラメーターを渡します。もう 1 つのトランザクション・プログラムは、データを受信するパラメーターを渡します。送信側トランザクション・プログラムは、データの送信を終了すると、会話の送信制御権を受信側トランザクション・プログラムに転送します。会話では制御情報およびデータを交換することができます。

6 ページの図 2 は、1 つのセッションを介する 2 つのトランザクション・プログラム間の会話を示しています。

図 2. 1 つのセッションで行われるトランザクション・プログラムの会話

1 つのセッションは、一度に 1 つしか会話をサポートしませんが、多数の会話を順次にサポートすることができます。複数の会話でセッションを再使用できるため、セッションは会話と比べて寿命の長い接続です。プログラムが会話を割り振り、かつ、すべての適用可能なセッションが使用中であった場合には、 LU は着信接続要求 (割り振り要求) を待ち行列に入れます。セッションが使用可能になると、 LU は割り振りを完了します。

2 つの LU が互いに並列セッションを確立して複数の並行した会話をサポートすることもできます。並列セッションが発生するのは、トランザクション・プログラムのいずれかが会話を割り振り、かつ、セッションが存在している場合です。ただし、会話により使用されている場合です。 LU は新しいセッションを要求して割り振りを行なうことができます。

図 3 は、2 つの LU 間の 3 つの並列セッションを示しています。それぞれのセッションで 1 つの会話が進行中です。

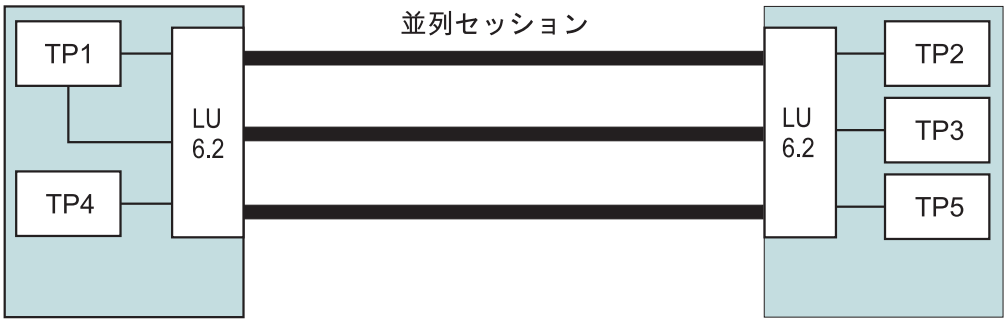

図 3. LU 間の並列セッション

拡張対等通信ネットワーク機能 (APPN)

拡張対等通信ネットワーキング (APPN) は、機能、形式、およびプロトコルの集合で、 SNA ネットワークの管理とネットワークで実行する APPC アプリケーションの使用可能度を大幅に拡張するものです。 APPN では、構成要件の減少、動的ディレクトリー探索、経路計算機能、および中間セッション経路指定を通してこれを実現しています。

APPN では、ユーザーは、基礎となるネットワークについて詳しい知識がなくてもプログラムを作成することができます。パートナー LU の名前さえ知っていれば、その位置は知らなくてもかまいません。 SNA がパートナー LU の位置とデータ経

路指定の最良のパスを判定します。基礎となるネットワークの変更、例えば物理アドレスの変更、新しいアダプターの追加、機械の再配置などは、 APPC プログラムには影響を及ぼしません。

Communications Server は、ワークステーションに拡張対等通信ネットワーキング (APPN) エンド・ノードおよびネットワーク・ノードのサポートを提供し、ネットワークの他のシステムとより柔軟に通信できるようにします。 また、Branch Extender 機能によってブランチを切り離して、不必要な CP-CP トラフィックを回避することができます。

- エンド・ノード機能によって、次のサービスが提供されます。
  - ディレクトリーおよび経路指定サービスのために、サービス提供するネットワーク・ノードにローカル・ノードとネットワーク・ノード・サーバーを接続。
  - エンド・ノードがネットワーク・ノード・サーバーを失ったときの、CP-CP セッションの自動再活動化。
- ネットワーク・ノード機能は次のサービスを提供します。
  - 経路選択サービス。セッションのために APPN ネットワークを介する最良の経路を計算します。
  - 中間セッション経路指定。隣接ノードにない 2 つの LU が相互のセッションを確立できるようにします。この場合、セッションは 1 つまたは複数の中間ノードをトラバースすることになります。
  - ディレクトリー・サービス。パートナー LU の位置を、動的に認識するための機能を提供します。
  - LAN または EEDLC に関する接続ネットワーク・サービス。これらの宛先アドレスを構成しなくてもそれを認識できる機能を提供します。

    この機能により、ノードは、宛先アドレスが構成されていない別ノードと直接にリンク接続を確立することができます。
  - Branch Extender 機能サポート。 LAN、エンド・ノード、および (従属および独立 LU、およびテラー・マシンなどのように PU を備えた) ロー・エンド・ネットワーク・ノードが設置されている事業所を、 1 つ以上の WAN に効率よく相互接続できるようにします。これにより、より多くのネットワーク・ノードを事業所のゲートウェイとして使用できるようになります。各事業所の LAN は、接続ネットワークとして構成することができます。

プログラミング・インターフェース

Communications Server サポートは、アプリケーション・プログラムの開発者用に、広範囲な 32 ビットのアプリケーション・プログラミング・インターフェース (API) をサーバー上でサポートします。これらの API はアプリケーション・プログラムが Communications Server 機能をアクセスするための簡単な方法を提供し、 IBM のコンピューターとその他のコンピューターの両方への接続に関する通信要件にアプリケーションが対処できるようにします。さらに、提供されたインターフェースは、SNA プロトコルをサポートしているので、標準化が保証されます。

サポートしている API には次のものがあります。

- 拡張プログラム間通信機能 (APPC)
- 通信用共通プログラミング・インターフェース (CPI-C)
- 従来型 LU アプリケーション・インターフェース (LUA) RUI および SLI

- ホスト・アクセス・クラス・ライブラリー (HACL)
- Java™ CPI-C (JCPI-C)
- ネットワーク・オペレーター機能
- 管理サービス
- 共通サービス

クライアントでは、拡張 APPC (EHNAPPC) API および Host Access Class Library (HACL) も提供されています。

Communications Server ソフトウェア開発者用ツールキット (Communications Server CD-ROM から別にインストールできる) もアプリケーション開発者が利用できます。このツールキットには、それぞれの API 用のサンプル、ヘッダー・ファイル、ライブラリー・ファイル、およびオンライン・マニュアルが入っています。

Communications Server プログラミング・インターフェースの詳細については、*「クライアント/サーバー・コミュニケーション・プログラミング」*および*「システム管理プログラミング」* を参照してください。

高性能経路指定

高性能経路指定 (HPR) は APPN の拡張であり、これを使用して、データの経路指定の性能と信頼性を向上させ、高速トランスポート・プロトコル (RTP) ノード間に仮想リンクを確立します。 HPR は、APPN で使用している経路指定方式である中間セッション経路指定を置き換えます。

HPR には、中間ノードでの伝送速度を高速化する機能、障害のあるノードとリンクを迂回してセッションを中断することなく再経路指定する機能、およびネットワークの輻輳 (ふくそう) を予測したり軽減したりしてトラフィックの流れを調整する機能があります。

Communications Server は、Enterprise Extender (IPv4 および IPv6)、同期データ・リンク制御 (SDLC)、LAN、WAN、チャネル、マルチパス・チャネル (MPC)、および X.25 の各接続における HPR 接続をサポートします。

SNA データ圧縮

セッション・レベルでのデータ圧縮は、通信リンクを介した大量のデータのスループットを増します。その結果、次のような利点があります。

- 低速回線におけるデータ・スループットの向上
- 高速回線での費用の削減
- より速い応答時間による生産性の向上

SNA データ圧縮は、zSeries® および iSeries のインプリメンテーションと互換性があり、すべての LU タイプで使用できます。

サービス提供者のディスカバリー

ディスカバリーとは一種の LAN アドレス解決プロトコルであり、指定された探索基準に一致する別ノードを検出するために LAN 上のノードが使用可能です。探索パラメーターを調整することにより、あるノードから、APPN ネットワーク・ノード (SNA 境界機能、iSeries、SNA ゲートウェイ、またはユーザー定義のサーバー・

クラスを提供するノード) を探索することができます。Communications Server for Windows は、クライアントからの要求に対して、ネットワーク・ノード・サーバー、PU 2.0 ゲートウェイ、またはユーザー定義のサーバーとして応答することができます。 また、Communications Server は、ディスカバリーを使用して、 APPN ノードと SNA ゲートウェイを見付けることができます。

従属 LU リクエスター (DLUR)

Communications Server は、従属 LU リクエスター (DLUR) のエンド・ノードおよびネットワーク・ノードのワークステーション用サポートを提供します。こうすると、従属 LU サーバー (DLUS) が提供する拡張されたシステム・サービス制御点 (SSCP) サポートを効果的に使用することができます。 DLUS は、VTAM® V4R2 およびそれ以降でサポートされます。このサポートを使用すると、従来型の SNA 従属 LU (例えば、エミュレーターおよびプリンターでも) で APPN ネットワークの多くの利点を生かすことができます。

その利点には、次のようなものがあります。

- 従属 LU をホストと隣接しないノードに配置することができる。
- APPN 検索ロジックを使用して、LU-LU セッションに最良のパスを提供することができる。

DLUR に関する詳細については、 56 ページの『従属論理装置リクエスター・サポート』を参照してください。

SNA ゲートウェイ

ゲートウェイにより、PU 2.0 ワークステーションをサポートするホストと、各種の DLC タイプを使用するワークステーションとの間の通信が可能になります。 SNA ゲートウェイでは次のことが可能です。

- 同じホスト・リンクをワークステーション間で共用することができる。
- 複数 PU 機能を持たないワークステーションに複数のホスト接続性を提供する。
- 専用 PU ダウンストリーム・ワークステーションに対して PU プールとして働く。
- DLC をそのリンク上 (ホスト・リンクで使用される DLC とは異なるリンク上) で使用するワークステーション相互間のプロトコル・コンバーターとして働く。例えば、ワークステーションは、ホスト接続が DLUR over EEDLC を使用している間は LAN 接続が可能です。
- ホストおよびワークステーションにおけるシステム定義の量を減少させる。
- ネットワーク定義を動的に変更し、ワークステーションを追加することができる。
- ホスト資源数とホスト接続数を減少させる。これは共用 (プール) LU を使用し、ユーザー指定の期間未使用のセッションを自動ログオフすることによって行います。
- ホストのバックアップ・リンクを提供して、信頼性を高める。

SNA ゲートウェイにより、zSeries ファミリーのホストは、LU 0、1、2、3、または従属 LU 6.2 (APPC) を実現するワークステーションをサポートすることができま

す。また、SNA ゲートウェイは iSeries ホスト用に LU 0、1、2、または 3 をサポートします。 iSeries ホストは zSeries ファミリーのホストへデータの受け渡しを行います。

各ホストは、SNA ゲートウェイを、ワークステーションごとに 1 つ以上の LU をサポートする SNA PU 2.0 ノードとして認識します。ホストに関しては、すべての LU は SNA ゲートウェイ PU に属します。 SNA ゲートウェイは複数のホスト接続を同時に維持することができ、指定されたホストに別々のワークステーション・セッションを割り当てることができます。ただし、フォーカル・ポイントとして機能するホストは 1 つだけあり (しかもこのホストは CP PU とリンクしていなければなりません)、ゲートウェイを介して経路指定されるすべての NMVT に制御点名が付加されます。

サポートされるワークステーションから見た SNA ゲートウェイは、SNA PU 4 通信制御装置であり、 BIND や UNBIND のようなホスト・メッセージの転送を行うものです。ネットワーク LU は SNA ゲートウェイを認識しません。ただし、SNA ゲートウェイはワークステーション上のすべての LU を認識します。

実際の SNA ゲートウェイは、特殊タイプの PU 2.0 です。 従属ワークステーションが非活動状態にある限り、SNA ゲートウェイは通常の PU 2.0 と同様にワークステーションに代わって LU 機能を実行します。ただし、そのワークステーションがホストとオンライン接続を確立すると、 SNA ゲートウェイはそのワークステーションで LU 機能を実行できるようにし、ワークステーションとホストの間でデータの受け渡しのみを行うようになります。

SNA ゲートウェイを使用すると、サポート対象のワークステーション・アプリケーションがサブエリア・ネットワーク上にあるリモートのサポート対象アプリケーションにアクセスできるようになります。この場合、各ワークステーション内では各ホストへの別の直接接続は不要です。 ホストから見れば、そのホストにはゲートウェイとの単一の接続があるだけです。

SNA ゲートウェイの使用法の詳細については、 101 ページの『第 6 章 SNA ゲートウェイの計画』を参照してください。

11 ページの図 4 は、SNA ゲートウェイを使用した接続の一例です。

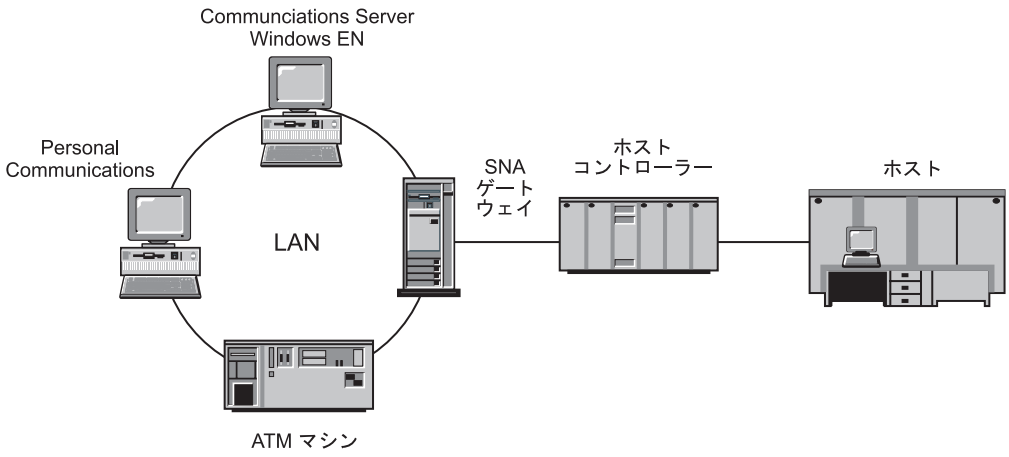

図 4. SNA ゲートウェイ接続の例

AnyNet サポート

Communications Server は AnyNet プロダクト・ファミリーの SNA over TCP/IP 機能を取り込みます。このサポートによって、SNA アプリケーションに変更を加えることなく TCP/IP ネットワーク上で通信することが可能になるため、ネットワークの拡張や単純化が容易になります。

SNA over TCP/IP

SNA over TCP/IP アクセス・ノード機能を使用すると、 IP ネットワーク上に存在する SNA アプリケーションが通信できるようになります。この機能は従属 LU リクエスター (DLUR) 付きまたはなしで、独立 LU6.2 と従属 LU 0、1、2、3、または 6.2 をサポートします。 さらに、SNA ゲートウェイと一緒に SNA over TCP/IP アクセス・ノードを使用して、 TCP/IP で SNA ゲートウェイ・セッションを使用可能にできます。

SNA over TCP/IP ゲートウェイ機能は、SNA アプリケーションの機能が及ぶ範囲を拡大します。これを行うには、SNA ネットワーク内の SNA アプリケーションと IP ネットワーク内の SNA アプリケーションが通信できるようにします。 SNA over TCP/IP ゲートウェイは、独立 LU 6.2 セッションをサポートします。

12 ページの図 5は、IP および SNA ネットワーク内で SNA over TCP/IP を介して通信する SNA アプリケーションを図示しています。

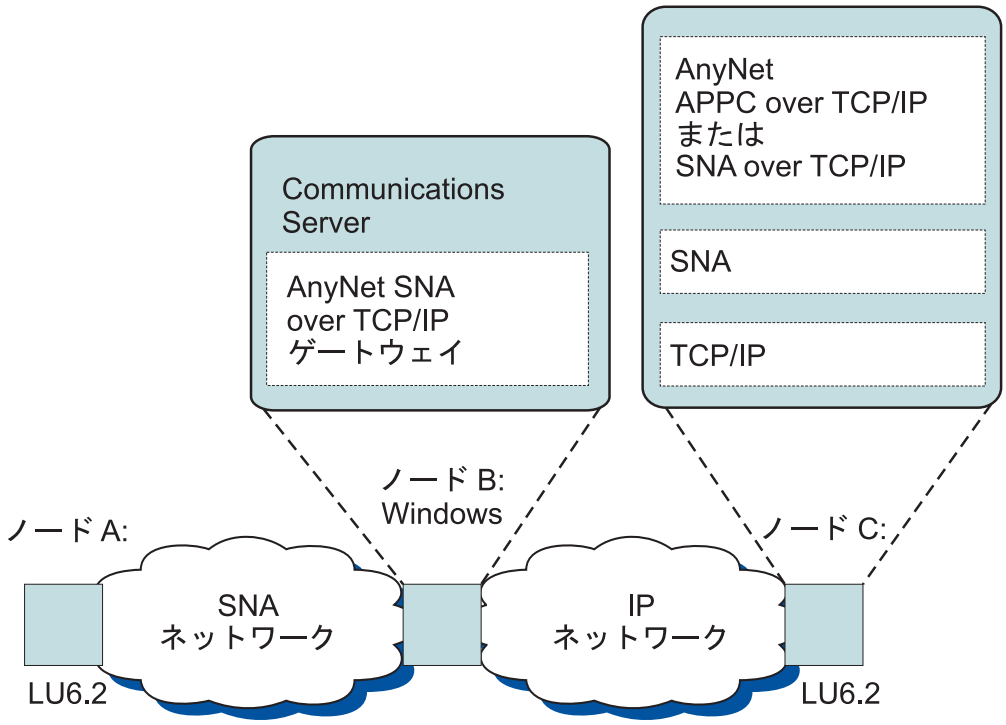

図 5. SNA over TCP/IP ゲートウェイ

TN3270E サーバー

TN3270E サーバー機能により、TCP/IP ユーザーは、SNA ネットワーク内のホスト・マシンにあるアプリケーションにアクセスすることができます。 業界標準の TN3270 または TN3270E クライアント・ワークステーションを、 TN3270E サーバー・ワークステーションに接続して、SNA ネットワークにアクセスすることができます。 TN3270E サーバーは、ATTN キーおよび SYSREQ キーの操作をサポートし、ユーザーがホストからワークステーションに接続されたプリンターへの印刷を行えるようにします。このためのプリンターは、ローカル接続のものでもネットワーク接続のものでもかまいません。

Communications Server は、クライアントがロード・バランシング用に使用できる場合は、同一ホスト・リソースに接続する TN3270E サーバーのクライアント接続用ロード・バランシングをサポートします。

TN3270E サーバーは、クライアント構成を変更せずに LU へのアクセス制御を可能にする、IP およびホスト名フィルターをサポートします。

また、TN3270E サーバーは TCP/IP ネットワークで、セキュア・アクセスを提供し、セキュア・ソケット・レイヤー (SSL) 認証および暗号化をサポートします。機密保護を指定する場合、サーバーは IBM Vault Registry や Verisign などの認証局が提供する認証がなければなりません。 Communications Server は、SSL バージョン 3 が使用する鍵および証明書を生成および管理するユーティリティーを提供します。 SSL 認証および暗号化の使用に関する詳細は、第 9 章の「Secure Sockets Layer ベースのセキュリティーの計画」を参照してください。

図 6は、TN3270E サーバー接続の一例です。

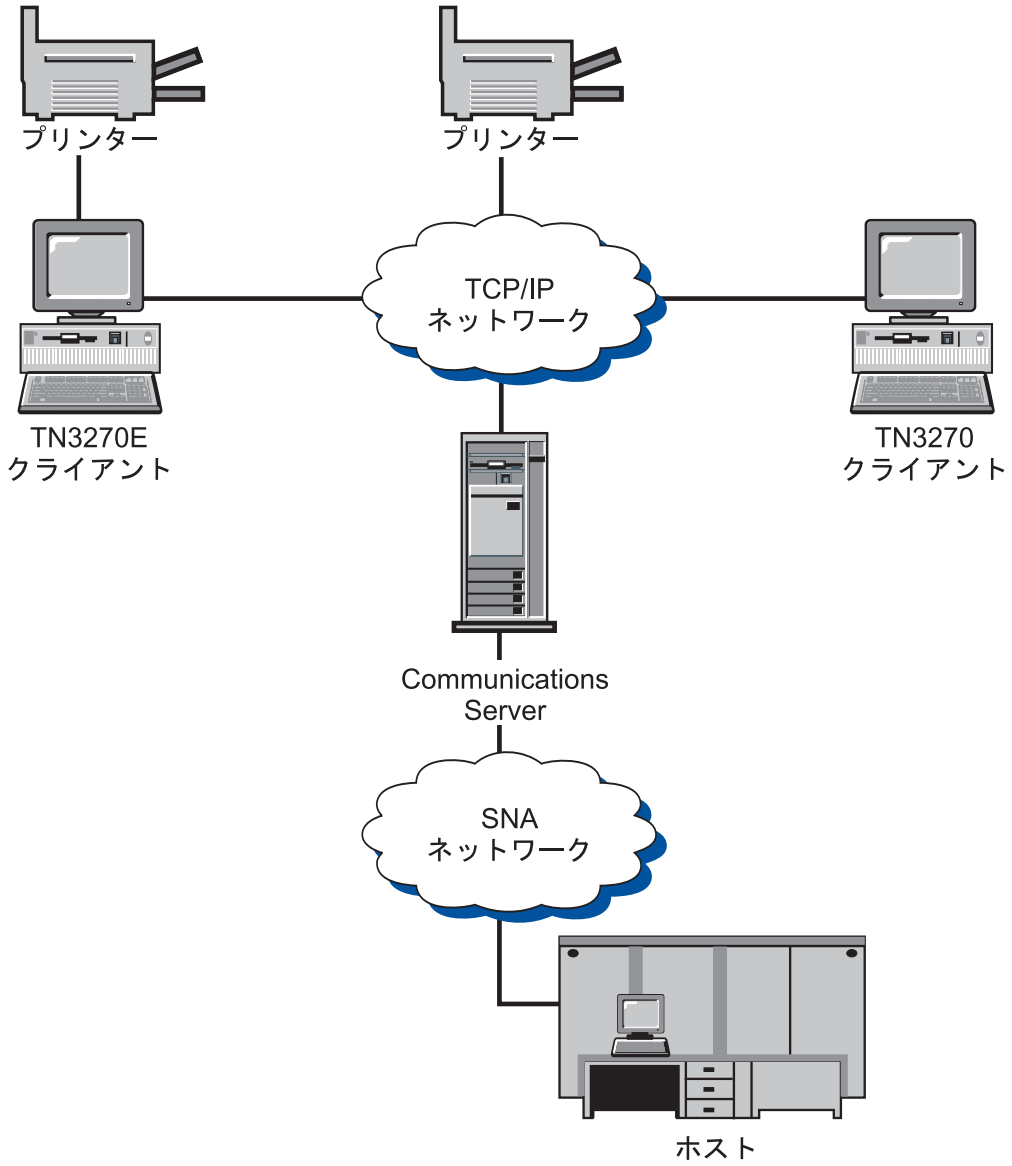

図 6. TN3270E サーバー接続

TN5250 サーバー

TN5250 サーバー機能により、TCP/IP ユーザーは、SNA ネットワーク内の iSeries にアクセスすることができます。 業界標準の TN5250 クライアント・ワークステーションを、TN5250 サーバーに接続して、 SNA ネットワークにアクセスすることができます。

クライアントがロード・バランシングを使用できる場合、Communications Server は、同じ iSeries に接続する TN5250 サーバーのクライアント接続のためのロード・バランシングをサポートします。

TN5250 サーバーは、クライアントを特定の iSeries に直結させるだけでなく、サーバーに対するクライアント・アクセスの中央管理を可能にする IP およびホスト名フィルター処理をサポートします。

また、TN5250 サーバーは TCP/IP ネットワークで、セキュア・アクセスを提供し、セキュア・ソケット・レイヤー (SSL) 認証および暗号化をサポートします。機密保護を指定する場合、サーバーは IBM Vault Registry や Verisign などの認証局が提供する認証がなければなりません。 Communications Server は、SSL バージョン 3 が使用する鍵および証明書を生成および管理するユーティリティーを提供します。 SSL 認証および暗号化の使用に関する詳細は、第 9 章の「Secure Sockets Layer ベースのセキュリティーの計画」を参照してください。

15 ページの図 7は、TN5250 サーバー接続の一例です。

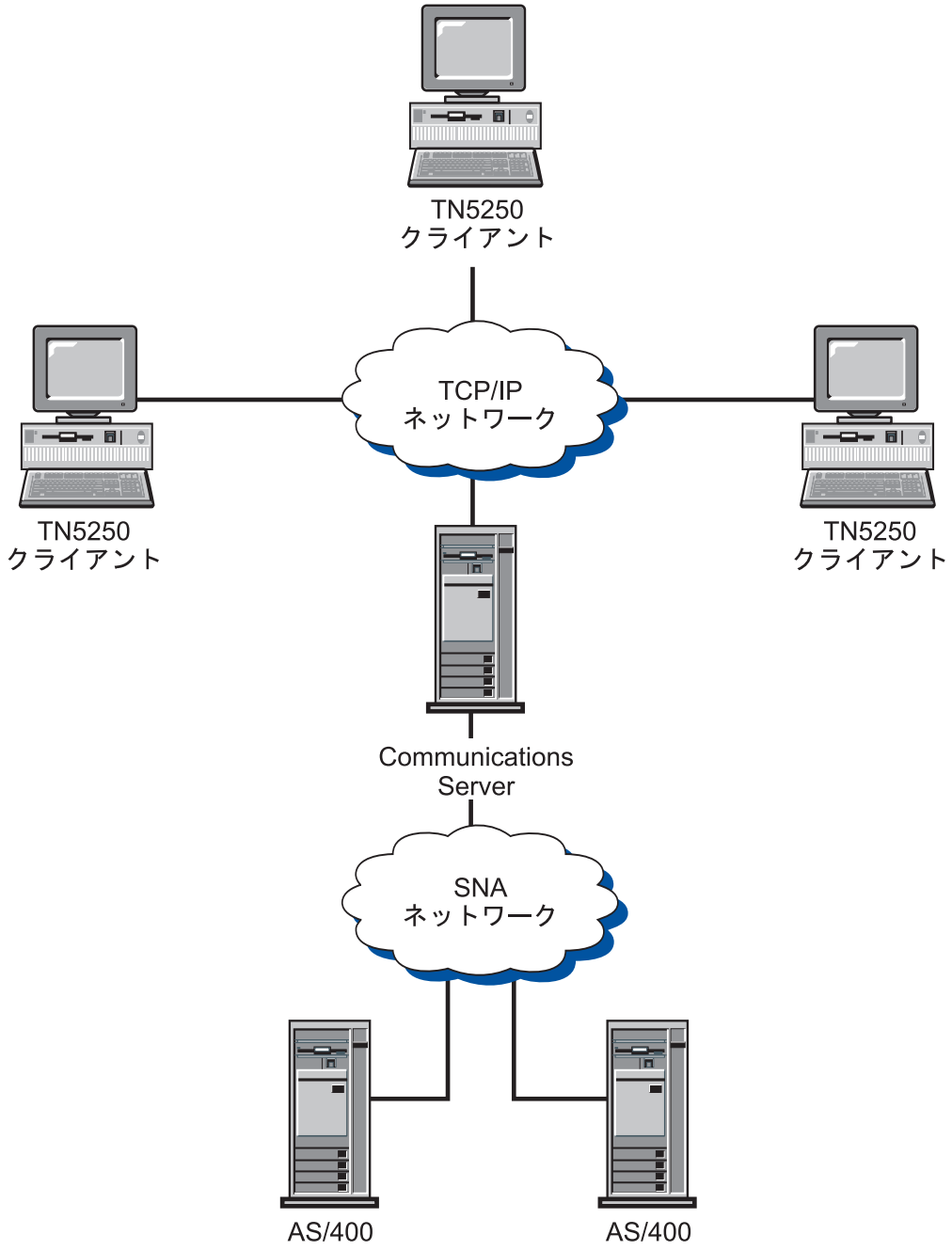

図 7. TN5250 サーバー接続

Communications Server クライアントのサポート

Communications Server は SNA API クライアント (CD-ROM で使用可能) のサポートを提供します。

SNA API クライアントのサポート

Communications Server SNA API クライアントのサポートを使用すると、TCP/IP 接続クライアントは、クライアントとサーバー間を流れる SNA プロトコルを要求せずに、SNA API にアクセスすることができます。これにより、SNA 構成の大半は中央サーバーで行うことができます。

Communications Server は、Windows 2000、Windows XP、Windows Server 2003 および Windows Vista で稼働する SNA API クライアントをサポートします。

SNA クライアントは、CPI-C、APPC、EHNAPPC、LUA SL1、LUA RUI および JCPI-C API の各インターフェースのサポートを提供する一方で、サーバーで実際の SNA 処理を行います。これらのクライアントは、サーバーの一部として引き渡されますが、実際にはクライアントにインストールされ、設定されます。

32 ビットの Windows クライアントには、次のような追加拡張機能があります。

- クライアントとサーバー間の暗号化
- 問題点を迅速にデバッグするのに役立つ、さらに詳細なトレース形式設定
- クライアントが実行中にトレースを開始、停止する機能
- アンインストールせずに、クライアントを再インストールする機能

Windows 2000、Windows XP、Windows Server 2003 および Windows Vista では、同じ実行可能ファイルから実行できます。この実行ファイルは、共用ドライブ上にインストールできます。すべてのクライアントに対しては、あらゆる修正が適用されます。 32 ビットの Windows クライアントは Communications Servers for Windows と通信します。

Communications Server の API クライアントの詳細については、 89 ページの『第 4 章 クライアント/サーバー通信の計画』を参照してください。

ロード・バランシング

Communications Server はすべてのクライアント・タイプにロード・バランシングをサポートします。ロード・バランシングにより、Communications Server 全体にわたって LU 0 から 3 および LU 6.2 の各セッションを分散することができます。サーバーは、ロード係数 (この係数をクライアントまたはサーバーが、サーバーを選択するために収集と編成可能) を含むサービスを公示します。

ディレクトリーの活用

構成プロセスを単純化するために、Lightweight Directory Access Protocol (LDAP) を使用して、中央設置場所から複数のクライアントを構成することができます。

ディレクトリーの使用に関する詳細については、 89 ページの『第 4 章 クライアント/サーバー通信の計画』を参照してください。

構成および管理のサポート

Communications Server は、リソースに関する構成および管理のための機能を提供します。

Communications Server 構成

このセクションでは、Communications Server 構成の構成要素の概要と、それらの構成要素の作成または変更の方法を説明します。 構成はプロダクトをインストールしたディレクトリーの PRIVATE サブディレクトリー (例えば、C:¥Program Files ¥IBM¥Communications Server¥PRIVATE) に保管された単一ファイル (ACG) からなります。 ACG ファイルは、**SNA ノード構成** を使用して作成できます。 ACG ファイルは、**SNA ノード構成**、または ASCII エディターを使用して変更できます。 使用する前に、ACG ファイルの妥当性を検査するために、検証 (vacgcon/vacgwin) プログラムを使用できます。

Communications Server 構成を作成または変更するには、次の方法を使用します。

SNA ノード構成

Communications Server が提供する SNA ノード構成アプリケーション (PCSCFG) を使用すれば、グラフィカル・インターフェースを用いて Communications Server 機能を構成することができます。また、デフォルト値がいくつか用意されているので、必要最小限のパラメーターを指定するだけで、それらを構成することができます。 構成中に、作成する各定義が検査され、有効であることが確認されます。構成を保管すると、必要な構成ファイルが作成されます。

ローカル構成は、クライアントとサーバーの両方のレベルでサポートされています。 サーバーのリモート構成は、Windows 2000、Windows XP、Windows Server 2003 および Windows Vista のクライアントからサポートされます。

構成の大半は、**SNA ノード構成**を使用して作成することができます。 ただし、一部のパラメーターと、他のパラメーターの一部のキーワードは、**SNA ノード構成**ではサポートされません。

SNA ノード操作

SNA ノード操作は、選択リソースの作成および変更の機能を提供します。

Communications Server 管理

Communications Server は、リソースの管理に次に示す機能を提供します。

- **SNA ノード操作**
- コマンド行ユーティリティー

これらの機能の詳細については、 193 ページの『第 15 章 システム管理機能』を参照してください。

ロード・バランシング

ロード・バランシングは、従属 LU (ホスト - ワークステーション) セッションと独立 LU 6.2 セッションを動的にバランスをとるための Communications Server の 1 つの機能です。これを行うには、これらのセッションを最も小さい負荷状態にある Communications Server に分散させます。 Communications Server がロード・バランシングを行う対象は、 Communications Server API プログラムとサード・パーティーの 3270 エミュレーター (TCP/IP プロトコル経由で接続) の場合、あるいは

サード・パーティーの TN3270 エミュレーターと TN5250 エミュレーターの場合です。バランシングを行う対象リソースは、セッションのタイプに応じて、次のようになります。

- 従属 LU セッションの場合、ロード (負荷) は指定の LU プールと指定のスコープ内にあるサーバーに分散されます。
- LU 6.2 セッションの場合、ロード (負荷) は名前を指定されたスコープ内の使用可能なサーバー全体に渡って、あるいは名前を指定されたサーバー・リスト内で選択されたサーバー全体に渡って分散されます。

Communications Server のロード・バランシング機能は、SNA クライアント API に組み込まれています。ロード・バランシングは **SNA クライアント構成**を使用するクライアント用に構成されます。

従属 LU セッションの場合、SNA クライアント API を使用するエミュレーターは、ロード・バランシングに参加することができます。従属 LU セッションでない場合、ロード・バランシングをサポートするサード・パーティーの 3270、TN3270、または TN5250 エミュレーター・ソフトウェアを購入しなければなりません。

LU 6.2 セッションの場合、SNA API クライアントが確立した初期の接続は、 LU 6.2 セッションをすべて管理するサーバーを決定します。

ロード・バランシングの詳細については、 133 ページの『第 10 章 ロード・バランシングの計画』を参照してください。

データ機密保護

Communications Server は、セッション・レベルおよび会話レベルでの基本的な機密保護サポートと拡張機密保護サポートを提供します。 SNA API クライアントを介して SNA 資源にアクセスできる Windows NT または Windows 2000 ユーザーを制限するセキュリティーがあります。会話機密保護には、パスワード置換に関するサポートが含まれています。 また、拡張 LU-LU 機密保護もあります。

Communications Server は、TN クライアントと TN3270E サーバーまたは TN5250 サーバーとの間の接続において、 Secure Sockets Layer (SSL) ベースの機密保護に関するサポートを提供します。 この機密保護は、署名済み証明書を使用したデータ暗号化およびサーバー認証を提供するために、 SSL バージョン 3 を使用します。

アダプター・サポート

Communications Server は、接続性のソリューション構築のために、アダプター製造業者に公開インターフェースを提供します。 Communications Server の SDLC および X.25 プロトコル・スタックが動作するように、シャロー (非プログラマブル) アダプター・インターフェースがアダプターの製造業者に提供されます。 製造業者が提供するデータ・リンク制御を使用する接続性のソリューションのために、ディープ (プログラマブル) アダプター・インターフェースがアダプターの製造業者に提供されます。

データ・リンク制御

Communications Server を使用すると、次の DLC で通信ができるようになります。

- AnyNet (SNA over TCP/IP)
- LAN (あらゆる NDIS 準拠ネットワーク・アダプター)
- X.25 SDLC (同期、非同期、AutoSync)
- OEM (サード・パーティー・アダプター・サポート)
- チャネル (アップストリームのみ)
- マルチパス・チャネル (HPR のみ)
- Enterprise Extender

AnyNet (SNA over TCP/IP) DLC

AnyNet SNA over TCP/IP DLC についての詳細は、11 ページの『SNA over TCP/IP』を参照してください。

IBM マルチパス・チャネル DLC

マルチパス・チャネル (MPC) DLC は、 ESCON (エンタープライズ・システム接続) チャネル・アダプター・カード (P/N 9663 001) 上の、 1 つ以上の zSeries MPC 可能ホストに対する大容量、高可用性のファイバー接続をサポートします。 MPC 接続は、物理的な接続が遮断されたり、一時的に使用不可状態になった時点の透過バックアップ付きで、高速データ伝送をサポートします。 このチャネル間接続により、LAN クライアントには、 zSeries のリソースおよびサービスへの迅速なアクセスを提供することができます。

Enterprise Extender DLC

Communications Server は、IPv4 および IPv6 ネットワークで UDP/IP パケットを使用する HPR 接続を提供しています。 HPR ネットワークに対しては、IP バックボーンは論理リンクとして見えます。 IP ネットワークに対しては、SNA トラフィックは UDP データグラムとして見えます。これらのデータグラムは、変更されずに IP バックボーンに経路指定されます。プロトコルの変換が何も行われないという理由で、およびトランスポート層にさらなるオーバーヘッドを与えずにルーティング層でパッケージングが行われるという理由で、 SNA クライアントの場合と同様に、SNA ベースのデータにアクセスする IP クライアント (例えば、 IBM ホスト・オンデマンドを使用する TN3270 クライアントまたは Web ブラウザー) のイントラネット・インフラストラクチャーを効果的に使用できるようになります。

APPN MIB サポート

Communications Server は、Simple Network Management Protocol (SNMP) 管理システムからの APPN 管理情報用に SNMP 要求をサポートします。

ホット・スタンバイ

Communications Server では、指定のクリティカル・サーバーが故障した場合に、自動的にアクティブにする特定のホスト・リンクを構成できます。ホストに対して構成された接続は、バックアップ・サーバーの代替接続がアクティブになるまで使用できます。この機能を、ホット・スタンバイと呼びます。

バックアップ・サーバー上のクリティカル・サーバー構成に名前を指定した接続がアクティブ化される時点は、バックアップ・サーバーがクリティカル・サーバーとの接続に失敗し、クリティカル・サーバーのライセンス交付責任がバックアップ・サーバー上で管理されている場合です。

注: ホット・スタンバイ機能が提供される対象は、バックアップ・サーバーでホスト接続をアクティブ化された場合に限定されており、クリティカル・サーバーが非アクティブ化された時点でバックアップ・サーバーへの代替経路指定をサポートするエミュレーター・ソフトウェアを使用しているかどうかに依存します。

バックアップ接続でのホット・スタンバイの使用に関する詳細については、 137 ページの『第 11 章 バックアップ・ホスト接続の計画』の「第 11 章 バックアップ・ホスト接続の計画」を参照してください。

第 2 章 Communications Server および SNA

この章では、Communications Server が提供する SNA ネットワーク機能と次の点について説明します。

- SNA 機能の概要
- データ・リンク制御 (DLC) 定義
- 拡張対等通信ネットワーク機能 (APPN)
- 高性能経路指定 (HPR)
- LU サポート
- データ圧縮
- 暗号化
- 管理サービス (MS)
- フロー制御
- SNA ゲートウェイ・サポート

SNA 機能の概要

このセクションでは、Communications Server がワークステーション上に SNA を実現する方法について概要を示します。 これは SNA 機能の包括的な説明ではありません。SNA に関する詳細については、以下の関連文献を参照してください。

- *Systems Network Architecture Concepts and Products*
- *Systems Network Architecture Technical Overview*
- *Systems Network Architecture Network Product Formats* (オンラインで Communications Server 文書リストから利用可能)
- *Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic for LU Type 6.2*

SNA は、ネットワーク (メインフレームから端末まで) 中の装置が相互に通信するために使用する標準、プロトコル、および機能を定義します。この通信では、これらの装置は情報と処理資源を透過的に共用することができます。つまり、ワークステーションのユーザーは、ネットワーク内部で何が行われているかを知らなくても、ホストの情報にアクセスしたり、別のユーザーと通信することができます。

SNA ネットワークは、ノードとリンクのシステムとして編成されます。この編成が論理編成であることを覚えておいてください。 SNA は、その機能、およびネットワーク中の他のノードに及ぼす制御の量に従ってノードを分類します。このノード・タイプは特定のタイプのハードウェアとは必ずしも関連しません。ノードの機能は、いろいろな装置で実行することができます。ゲートウェイとして働くワークステーションは、通信制御装置と同じ機能を実行します。 1 つの装置が複数のノードを持つことも可能です。

SNA ネットワークは、2 人のエンド・ユーザー間で、効率よく、整然と、確実にデータが移動できるようにします。例えば、あるワークステーションのユーザーが別のワークステーションにメッセージを送る場合、 SNA は次のことを行います。

- そのリンク・タイプで使用できる形式にメッセージをパッケージする。
- パッケージのアドレスを指定する。
- メッセージの経路を選択する。
- メッセージが確実に宛先に到着するように通信を監視する。
- 宛先で使用できる形式にメッセージを変換する。

これらの作業は、SNA の中で個別の機能層として定義されています。 ここではこれらの層について詳しくは触れませんが、SNA 層がすべて論理リンクの一部であることを覚えておいてください。

前に述べたように、SNA ノードは、その通信機能と、ネットワーク中の他のノードに及ぼす制御の量とによって分類されます。 SNA ノードは、サブエリア・ノードと周辺ノードに大別されます。サブエリア・ノードは、リンク・ハブであり、周辺ノードおよび他のサブエリア・ノードと通信することができます。サブエリア・ノードは、周辺ノードの資源を活動化し制御します。サブエリア・ノードはさらにタイプ 4 とタイプ 5 のノードに分類されます。タイプ 5 のノードには、システム・サービス制御点 (SSCP) が含まれます。これは、このノードに接続されたタイプ 4 のノードの中央制御点になります。タイプ 5 のノードは、ホスト・ノードと呼ばれることがあります。周辺ノードは、その接続先のサブエリア・ノードとしか直接通信することができません。しかし、周辺ノードは、接続先の装置を制御することができます。例えば、周辺ノードとして働くクラスター制御装置は、そこに接続される端末をサポートすることができます。周辺ノードは、タイプ 2 またはタイプ 2.1 のノードと呼ばれることがあります。

各ノードには、制御および通信の機能を実行するネットワーク・アクセス可能単位 (NAU) が含まれています。 これらの NAU の 1 つが物理装置 (PU) です。PU は、ノードの物理資源を管理します。論理装置 (LU) と呼ばれる別の NAU は、ネットワークへの論理アクセス・ポイントを提供します。論理アクセス・ポイントによって、各ノードのユーザーとアプリケーションの間の通信が可能になります。論理装置間の通信をセッションと呼びます。セッションは、ユーザーとアプリケーションの間の通信をサポートするだけでなく、処理資源を共用するためのアプリケーション相互間の通信もサポートします。アプリケーション間の通信は、拡張プログラム間通信 (APPC) として知られています。 APPC は、LU 6.2 を実現するプログラミング規則とプロトコルの集まりです。(APPC は、この LU タイプを実装したプロダクトの中の LU 6.2 機能に与えられた名前です。)

データ・リンク制御プロファイル

データ・リンク制御 (DLC) によって、2 つのノード間で、論理リンクを介してデータを正常に交換することができます。 DLC は、SNA ネットワークにおける 1 対のノード間で、信頼性のある基本伝送単位 (BTU) を配送するのに必要なプロトコルを提供します。 SNA ネットワークにアクセスするには、ワークステーションに適切な Communications Server DLC プロファイルを構成しなければなりません。

拡張対等通信ネットワーク機能

拡張対等通信ネットワーク機能 (APPN) は、SNA の拡張で、前のセクションで説明したもの以上の通信機能を加えるものです。 APPN の基本構成要素には次のものがあります。

- APPN ノード・タイプ
- 制御点
- Branch Extender 機能
- データ・リンク制御
- 論理リンク
- ディレクトリー・サービス
- トポロジー/経路選択サービス

APPN ノード・タイプ

このセクションでは、APPN ネットワークに参加できる 3 つのタイプのノード (Communications Server が実装) について説明します。

- ネットワーク・ノード
- エンド・ノード
- ロー・エントリー・ネットワーキング (LEN) ノード

さらに、Branch Extender 機能はネットワーク・ノードの拡張機能です。 これは、ネットワーク・ノードとしてエンド・ノードに対するサービスを提供しますが、このノードは、ネットワーク内では他ネットワーク・ノードに接続されたエンド・ノードのように見えます。 このタイプのノードにより、ネットワークを流れることになるデータ量は削減されます。

各ノードは固有の名前によってネットワーク内の他ノードと区別されます。この名前は、ネットワーク ID とローカル・ノード名という 2 つの部分からなります (ローカル・ノード名は制御点 [CP] 名とも呼ばれます)。各ノードは、ネットワーク内の他のすべてのノードにこの名前で識別されます。また、ノードは、複数の PU T4/5 ホストへの同時アクセスを行うために、複数 PU 名を保有できます。

あるノードはエンド・ノードまたはネットワーク・ノードとして構成することができますが、エンド・ノードに APPN ネットワーク・ノードとの CP-CP セッション (26 ページの『CP-CP セッション』を参照) がない場合、そのエンド・ノードは LEN ノードとして機能します。 LEN ノードは APPN 機能をサポートしません。

ノード・タイプについては、以下のセクションで詳しく説明します。 24 ページの図 8 に、あらゆるノード・タイプを組み込んでいるサンプル APPN ネットワークを図示します。

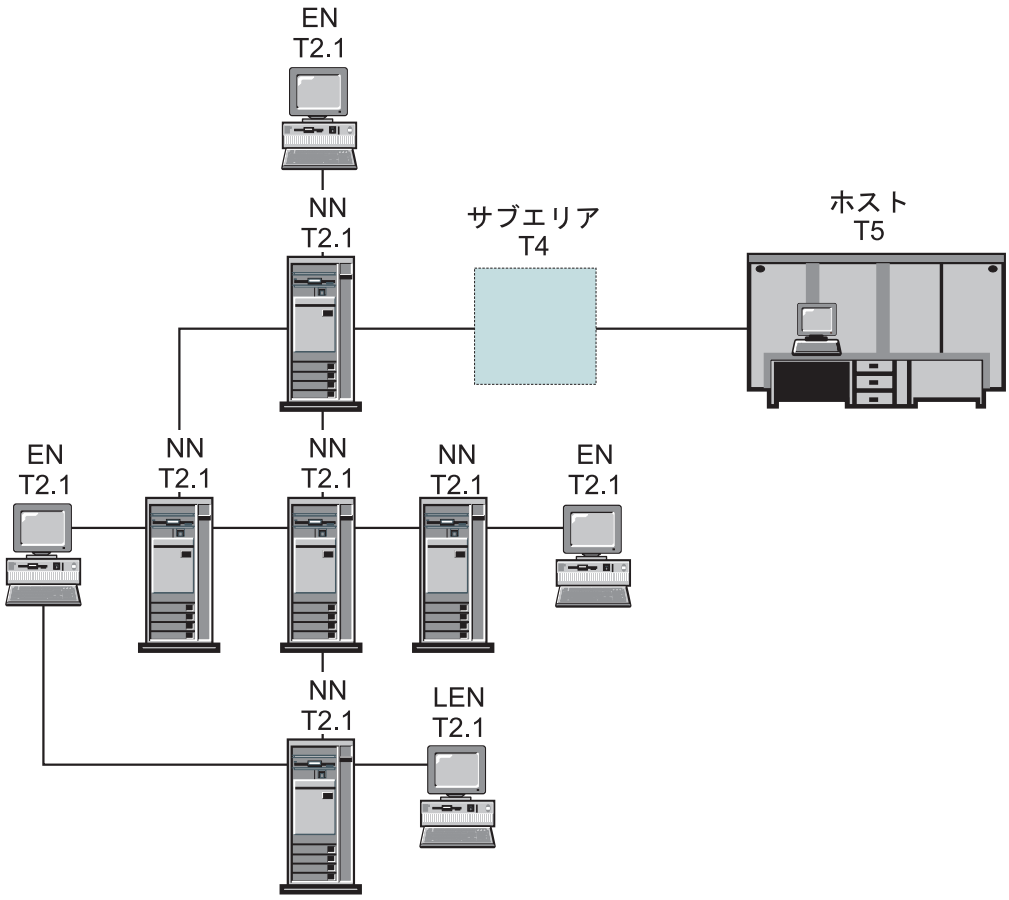

図 8. サンプル APPN ネットワークの部分。この図のネットワーク・トポロジーには、5 つのネットワーク・ノード (NN) があります。 3 つのエンド・ノード (EN) は、LEN ノード、サブエリアとともに接続されます。このネットワーク内のノード用の APPC アプリケーション・プログラムは、他のいずれのノードとでも通信することができます。

ネットワーク・ノード (NN)

ネットワーク・ノードは、それ自身のエンド・ユーザーをサポートし、エンド・ノードに、ディレクトリー・サービス、経路選択サービス、および管理サービスを提供し、そのノードを経由するセッションのデータの中間経路指定を行います。ネットワーク・ノードは、ネットワークを分散して探索して、パートナー LU を探し出し、ユーザー指定の基準に基づいて、起点ノードから宛先ノードへの最適経路を計算します。

ネットワーク・ノード・サーバーとは、あるネットワーク・ノードの役割を意味します。すなわち、そのネットワーク・ノードに接続された特定エンド・ノードに対して、ネットワークの入り口点として機能します。接続しているエンド・ノードは、いずれもネットワーク・ノード・サーバーのドメインに存在するものとして定義されます。例えば、これらのエンド・ノードの資源 (LU など) に関するすべてのディレクトリー要求が (そのノード自身の保有する資源と共に) 、ネットワーク・ノード・サーバーのディレクトリー・サービスを通じて渡されます。このようにして、ネットワーク・ノードは、APPN ネットワークに渡されるディレクトリー情報を収集して制御することができます。

ネットワーク・ノードは、以下のものを提供します。

- ローカルに存在するその LU に対する LU-LU セッション・サービス
- 中間セッション経路指定
- 接続されているエンド・ノードまたは LEN ノード (およびローカルに存在するそれ自身の LU) のためのネットワーク・サーバー機能 (ネットワーク・ディレクトリー探索と経路選択を行う)
- サービスを受け取るエンド・ノードと管理サービス・フォーカル・ポイント (FP) との間で管理サービス・データ (アラートなど) を転送するための管理サービス (MS) 経路指定機能
- LAN 接続に対して暗黙のインバウンド・リンクの特定番号だけを許可する、ポート構成のサポート

エンド・ノード

エンド・ノードは、LU-LU セッション (LU 6.2 プロトコルを使用) に対する対等環境で動作し、追加の APPN 機能を提供します。エンド・ノードは、そのノードのエンド・ユーザーに、ディレクトリー・サービスと経路選択サービスなどの APPN 機能を提供します。エンド・ノードは APPN ネットワークに参加することができます。これを行うには、セッション要求 (直接接続されていないノードも含む)) に対して、接続済みのネットワーク・ノード・サーバーのサービスを使用します。すなわち、エンド・ノードは、CP-CP セッションを使用して、隣接ネットワーク・ノード (そのサーバー) との間で、ディレクトリー・サービスの要求および応答を交換することによって行います。

APPN エンド・ノードは、そのネットワーク・ノード・サーバーに、ローカル LU を登録できます。エンド・ノードを登録することによって、ネットワーク・ノード・サーバーのネットワーク・オペレーターは、ネットワーク・ノードがサービスを提供する接続対象の全エンド・ノードに、その LU の LU 名をあらかじめ定義する必要がなくなります。

APPN エンド・ノードは複数のネットワーク・ノードに接続することができますが、一度には 1 つのネットワーク・ノードとの CP-CP セッションしかアクティブにできません。この CP-CP セッションを保有するネットワーク・ノードが、ネットワーク・ノード・サーバーになります。その他のネットワーク・ノードは、エンド・ノードに中間セッション経路指定を提供するために使用したり、主 (優先) ネットワーク・ノード・サーバーが使用できなくなった場合に、代替ネットワーク・ノード・サーバーとして使用することができます。エンド・ノード間に CP-CP セッションが確立されることはありません。

LEN ノード

LEN ノードは、APPN 拡張のない基本 T2.1 プロトコルを実装しているノードです。 LEN ノードでは、パートナー LU とのセッション開始前に、可能性のあるパートナー LU との接続すべてを事前定義する必要があります。 LEN ノード (隣接する APPN ネットワーク・ノードに接続されたノード) は、接続する可能性のあるパートナー LU がネットワーク・ノードに存在しているかのように事前定義することによって、 APPN の拡張機能を使用します。ネットワーク・ノードは引き続き自動的に LEN ノードのネットワーク・ノード・サーバーとして機能することができ、パートナー LU の実際の宛先を突きとめて最適経路を選択することができま

す。 LEN ノードは、ネットワーク・ノードを介することにより、すべてのノードと直接に接続されていなくても、 APPN ネットワークに参加することができます。

制御点

制御点 (CP) は、ノードとその資源を管理する責任を負います。 APPN ネットワーク・サービスを得るためには、 APPN エンド・ノードの制御点が隣接ネットワーク・ノードの制御点と通信しなければなりません。また、ネットワークを管理するためには、 APPN ネットワーク・ノードの制御点が隣接ネットワーク・ノードの制御点と通信しなければなりません。制御点は以下のような機能を管理します。

- アダプターの活動化と非活動化
- リンクの活動化と非活動化
- セッション開始と終了の際の LU の支援

ワークステーションをセットアップするときは、制御点名 (ローカル・ノード名とも呼ぶ) を定義しなければなりません。制御点も LU です。ワークステーションで定義される LU を 制御点 LU だけにするという選択も可能です。

CP-CP セッション

ディレクトリー・サービス、トポロジー・サービス、および経路選択サービスを実行するためには、 APPN ネットワーク全体の隣接ノードが 1 対の並列 CP-CP セッションを使用してネットワーク情報を交換します。ネットワーク・ノードは CP-CP セッションを使用して、ネットワーク・リンクのノードを監視します。この他、ディレクトリー・サービスおよびセッション・サービスをトラッキングします。ネットワーク・ノードは、隣接する各ネットワーク・ノードとの間およびサービスを受ける各エンド・ノードとの間に 2 つの並列セッションを確立します。 APPN エンド・ノードは、その現行サーバーとして働く単一の隣接ネットワーク・ノードとの間に 2 つの並列セッションを確立します。 LEN ノードは CP-CP セッションをサポートしません。

接続の確立が完了後は、この両ノードは識別情報の交換 (XID) を行います。そして、直接接続されたノードの制御点間で CP-CP セッションが開始されます。CP-CP セッションは LU 6.2 プロトコルを使用し、パートナー制御点同志が対話を開始し維持するには、その制御点間の 2 つのセッションが両方とも活動状態になっていなければなりません。ディレクトリー探索を行うためには、すべての CP-CP セッションが使用されます。

CP-CP セッションが確立後は、2 つのノードは制御点機能メッセージを交換し、互いに自分の能力を知らせます。ノードが両方ともネットワーク・ノードであれば、トポロジー・データベース更新 (TDU) メッセージを交換します。 TDU メッセージには、識別情報、ノードとリンクの特性、および資源の順序番号が含まれています。この資源の順序番号を使って、TDU 内に記述されている各資源の最新の更新を示します。

CP-CP 接続の活動化

Communications Server の始動時に、*始動時に活動化*する ものとして定義されたすべての接続の活動化を開始します。 NN サーバーへの接続が活動状態になると、Communications Server はその接続で CP-CP セッションを活動化します。最終的に優先 NN サーバーへの接続が活動状態になると、Communications Server は CP-CP セッションを優先 NN サーバー接続へ切り替えます。

注: この接続がローカル・ノードからの操作員要求によって非活動化された場合には、 CP-CP セッションは再活動化されません。 この接続がリモート・ノードからの操作員要求によって非活動化された場合には、 CP-CP セッションはローカル・ノードで再活動化されます。 NN ノード間のリンクの場合、要求時活動化リンク (隣接 CP 名が指定されていて、しかも、*始動時活動化* リンクとして定義されていないリンク) だけが活動化されます。

CP-CP 接続の再活動化

Communications Server は、CP-CP 接続の再活動化をサポートします。エンド・ノードとそのネットワーク・ノード・サーバーとの間の CP-CP セッション、および隣接ネットワーク・ノード間の CP-CP セッションが失われると、 APPN ネットワークの動作が妨げられる可能性があります。 CP-CP 接続の再活動化サポートでは、障害または接続の非活動化のためにこれらの重要なセッションが終了すると、そのセッションを再確立することで、APPN ネットワークの信頼性を向上させます。

CP-CP 接続の再活動化が開始されるのは、CP-CP リンクの活動化、CP-CP セッションの障害、または CP-CP 再試行タイマーの満了時です。 CP-CP セッションは、以下のうちの最初に発生したものを使用して Communications Server によって開始されます。

1. 優先サーバー CP-CP (以前に試みられていない場合)。
2. DLUR が構成されている場合、DLUR 登録をサポートする隣接 CP を使用。
3. まだ試行されていなくて活動リンクが存在している、最後の (最も新しく活動化された) NN。
4. Branch Extender 機能の場合に、上位レベルの他 NN のうちの最初のもの。

注: リンクの障害のために CP-CP セッションが終了した場合は、 Communications Server はリンクを再活動化しません。重要な接続をアクティブに保つために、接続を*自動再活動化* (無制限の再試行) として構成することもできます。

Branch Extender 機能

Branch Extender 機能は、一種のボーダー・ノードのサブセットであり、事業所と APPN WAN バックボーン・ネットワークを相互接続するために設計されています。相互接続ネットワークは、ネイティブ (つまり、両方のネットワーク ID が同じになっている場合) であっても、非ネイティブであってもかまいません。Branch Extender 機能をサポートするノードは、ブランチ・ネットワーク・ノードです。これは、典型的には LAN および WAN インターフェースを持ち、また DLUR および HPR を含むこともあります。

ノードにおいて Branch Extender 機能をサポートするリンクは、ブランチ・アップリンク またはブランチ・ダウンリンク として定義されています。 28 ページの図 9 は、ネットワーク内でのブランチ・ネットワーク・ノードの役割を示す例です。この図では、中央に示されているノードがブランチ・ネットワーク・ノードです。通常、隣接 CP (ブランチ・アップリンク) がブランチ・ネットワーク・ノードのネットワーク・ノード・サーバー (NNS) になります。ブランチ・ネットワーク・ノードは、ブランチ・アップリンク・ノードからはエンド・ノードのように見えます。

図 9. ブランチ・アップリンクとブランチ・ダウンリンクの概念的な概要

ブランチ・アップリンクは、ブランチ・ネットワーク・ノードでバックボーン・ネットワークに対するアップストリームとして定義されます。 アップリンクを含むノードは、バックボーン・ネットワークに周辺接続されているものと見なすことができます。

ブランチ・ダウンリンクは、ブランチ・ネットワーク・ノードからダウンストリームとして定義されます。このノードからは、ダウンリンクはドメイン内のエンド・ノード (制御点) への接続と見なされます。ブランチ・ダウンリンクは、典型的には LAN リンクですが、必ずしも LAN リンクである必要はありません。ブランチ・ダウンリンクを介して接続されたエンド・ノードは、ローカル資源と見なすことができます。ブランチ・ネットワーク・ノードは、これらのエンド・ノードのネットワーク・ノード・サーバーです。ブランチ・ダウンリンクでは、このノードにより、ドメイン・エンド・ノード、LEN エンド・ノード、従属側の T2.0 ノードと T2.1 ノード、およびローカルの LU と PU のためのネットワーク・ノード・サービスが提供されます。

ブランチ・ネットワーク・ノードは、そのドメインのネットワーク・ノード・サーバーとして働きます。このノードは、そのすべてのブランチ・ダウンリンク・ノー

ドに関するトポロジー情報を維持しますが、アップリンク・ネットワーク全体に関する完全な情報は維持しません。ブランチ・ネットワーク・ノードに含まれている情報だけでは不十分な場合には、このノードはアップリンク・ネットワーク・ノード・サーバーに LOCATE 要求を渡します。このサーバーは、別のブランチ・ネットワーク・ノードであっても、APPN ネットワーク・ノードであってもかまいません。

Branch Extender 機能は、基本的に交換回線ネットワークに基づく大規模な WAN に LAN ベースのブランチを接続しようとする管理者に対して、対等通信環境を最適化します。 Branch Extender 機能は、大規模な APPN ネットワークにおけるパフォーマンスを強化します。特に、以下のパフォーマンスが強化されます。

- 大規模な APPN ネットワークにおけるネットワーク・ノードの数が減少し、ブランチ・ネットワークを追加できるようになります。
- ブランチのトポロジー情報が隠されます。
- 同じ APPN 接続ネットワークで接続されているブランチ間での対等通信が可能になります。
- PU ゲートウェイ・サーバーの共存が可能になります。
- アップリンク CP-CP セッションのトラフィック (WAN トラフィック) が減少します。
- バックボーン WAN トラフィックのオーバーヘッドからブランチ・ネットワークが分離されます。

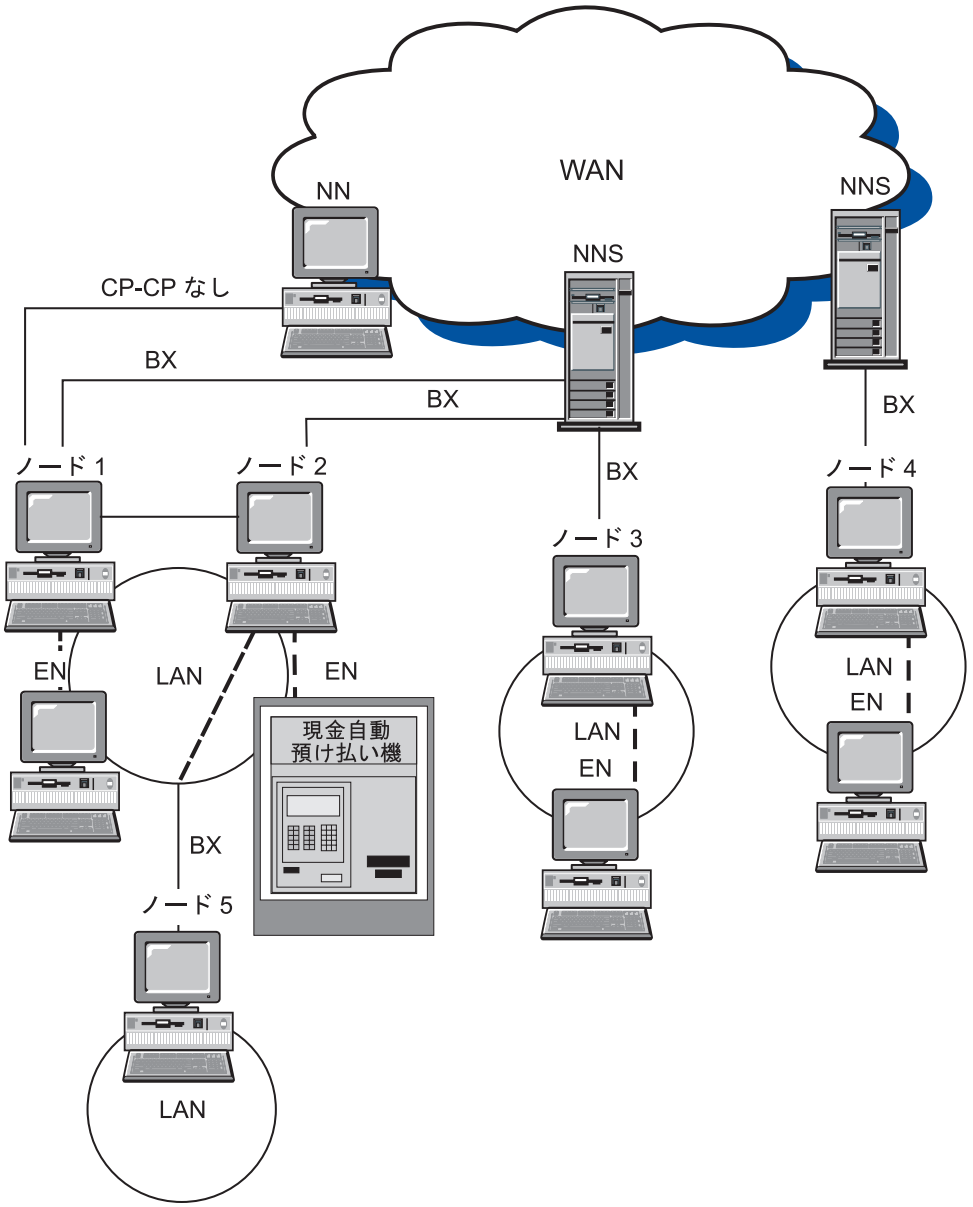

図 10. ネットワーク内の Branch Extender 機能

図 10 は、ネットワークにおけるブランチ・ネットワーク・ノードの働きを示しています。破線は論理リンクを表しています。「BX」 は Branch Extender アップリンクを意味します。この図では、ノード 1、2、3、4 および 5 は Branch Extender 機能をサポートするように構成されていて、エンド・ノードおよびネットワーク・ノードの両方の役割を果たします。これらのノードは、WAN ネットワークからダウンリンク・トポロジーを隠します。アップストリーム・ネットワーク・ノード・サーバーからはエンド・ノードに見えます。 LAN のダウンストリームにあるノードに対しては、ネットワーク・ノード・サーバーとして働きます。ノード 5 は、ノード 2 からはエンド・ノードに見えますが、その LAN にある他のエンド・ノードにとってはネットワーク・ノード・サーバー (NNS) です。 NNS にとって、ノード 5 はノード 2 にある LU に見えます。

ノード 1 によってサービスを受けるエンド・ノードが WAN 全体でエンド・ノードとのセッションを確立しようとすると、ノード 1 は、Branch Extender 機能リンクからネットワーク・ノード・サーバーに Locate (Send) 要求を送ることができます。ターゲット CP が検出されると、ネットワーク・ノード・サーバーはノード 1 からターゲット CP への経路を決定します。ノード 1 は、ソース・エンド・ノードに戻す前にこの経路を変更します。ソース・エンド・ノードは、セッション用にこの経路を使用します。

Branch Extender 機能の制約事項

Branch Extender 機能を使用するように構成されたネットワークには、以下の制約事項が適用されます。

- ブランチ・ネットワーク・ノードは、ブランチ・アップリンクを介してのみネットワーク・ノードに接続することができます。
- サーチ・ループを避けるために、ダウンリンク・エンド・ノードは、エンド・ノード・イメージを表すノードではなく、実エンド・ノードでなければなりません。
- 1 つのノードがブランチ・アップリンクとブランチ・ダウンリンクの両方を同時に介して、ブランチ・ネットワーク・ノードとの CP-CP セッションを持つことはできません。
- ブランチ・ネットワーク・ノードは、同時に 1 つのブランチ・アップリンクだけを介して CP-CP セッションを持つことができます。つまり、最大 1 つのネットワーク・ノード・サーバーとの CP-CP セッションを持つことができます。
- Branch Extender 機能ノードは、DLUR セッション・ダウンストリームを持つことができません。

Branch Extender 機能の構成

Branch Extender 機能を構成するには、まずブランチ・ネットワーク・ノードを構成しなければなりません。そして、DLC (暗黙リンクの場合) またはブランチ・ネットワーク・ノードのどちらかを構成する必要があります。 Branch Extender 機能をサポートするように構成されたリンクは、ブランチ・アップリンクです。ブランチ・ネットワーク・ノードでは、Branch Extender 機能をサポートするように構成されていないリンクはブランチ・ダウンリンクです。

ブランチ・ネットワーク・ノード相互間でリンクが定義されている場合、それらのブランチ・ネットワーク・ノードは対等接続として定義されていなければなりません。このように定義することにより、ACG ファイル内におけるこれらのノードのリンク・タイプが **LEARN** になります。 あるいは、このリンクを **ACTIVATE_AT_STARTUP=1** として定義し、常にリンクが活動状態になるようにすることもできます。 ブランチ・ノードが相互に接続されると、トポロジーでループが発生します。 リンクが常に活動状態になっている場合、または活動化されたときにリンクが確認される場合には、このループの発生は容認できます。リンクがブランチ・ネットワーク・ノード間で **END_NODE** または **NETWORK_NODE** リンクとして定義されている場合には、トポロジーがアップストリームとして報告されると、リンクが不適切に解釈され、割り振りが失敗する可能性があります。

ACG ファイルを使用して Branch Extender 機能を構成することもできます。

Branch Extender 機能の管理

以下のセクションでは、構成の検査方法、およびネットワークの構成方法に関する制約事項について説明します。

構成の検査

Branch Extender 機能をサポートするノードで **SNA ノード操作**を使用して、ローカル・ブランチが正常に構成されているかどうかを判別することができます。実行時に、ノードからのトポロジーの DISPLAY では、そのノード自体と、アップリンク・ネットワーク・ノード・サーバーの 2 つのネットワーク・ノード以外は表示されないはずです。

注: CP-CP で使用可能なアップリンクは 1 つだけです。 各ワークステーションは、優先ネットワーク・ノード・サーバーとしてブランチ・ネットワーク・ノードが定義された、エンド・ノードとして定義する必要があります。

SNA ノード操作を使用して、 DLC またはリンクが Branch Extender 機能を正しくサポートするように構成されているかどうかを検証することができます。また、**SNA ノード操作**は、活動リンクがブランチ・アップリンクであるのか、ブランチ・ダウンリンクであるのかを判別するために使用することもできます。 AnyNet を使用して登録されたダウンストリーム・エンド・ノードでは、ノードの資源が登録されません。

サポートされる機能

Communications Server は、APPN バージョン 2 の基本機能 (エンド・ノードとネットワーク・ノードの両方) をすべてサポートします。さらに、次のオプションもサポートされます。

- エンド・ノード

機能セット	オプション
162	MS_CAPS は制御範囲 (SOC) EN
171	アラートの問題診断データ
177	LAN アラート
178	SDLC/LAN LLC アラート
181	X.25 アラート
182	CPMS 用の保留アラート
1002	隣接リンク・ステーション名
1007	並列 TG
1011	複数のローカル独立 LU
1012	CP=LU
1018	登録前に EN 資源を削除
1067	従属 LU リクエスター
1070	セッション暗号化
1107	中央資源登録 (LU の)
1116	DLUS でサービスされる LU 登録
1200	ツリーおよび TG キャッシュ
1400	HPR ベース (ANR)
1401	高速トランスポート・プロトコル
1402	RTP での制御の流れ
1520	共通操作サービス
2355E	コンテンション解消

	N/A	Contention Network Reachability Awareness

- ネットワーク・ノード

機能セット	オプション
164	MS_CAPS はサブエリア・フォーカル・ポイントを持つ
171	アラートの問題診断データ
177	LAN アラート
178	SDLC/LAN LLC アラート
181	X.25 アラート
182	CPMS 用の保留アラート
1002	隣接リンク・ステーション名
1007	並列 TG
1011	複数のローカル独立 LU
1012	CP=LU
1018	登録前に EN 資源を削除
1067	従属 LU リクエスター
1070	セッション暗号化
1100	ディレクトリー・キャッシュのセーフ・ストア
1101	事前ロード・ディレクトリー・キャッシュ
1107	中央資源登録 (LU の)
1116	DLUS でサービスされる LU 登録
1118	EN TG ベクトル登録
1121	Branch Extender 機能
1200	ツリーおよび TG キャッシュ
1203	TDU War の検出と除去
1301	Nonpaced 中間セッション・トラフィック
1400	HPR ベース (ANR)
1401	高速トランスポート・プロトコル
1402	RTP での制御の流れ
1520	共通操作サービス
2355E	コンテンション解消

データ・リンク制御

DLC は APPN ネットワークの 1 対のノード間で基本伝送単位 (BTU) を確実に配信するために必要な、ノード間の論理接続を維持するプロトコルを提供します。

接続

接続リンクは、基礎となる DLC を介して 1 対の隣接ノードを接続します。

並列リンク

ローカル・ノードは、1 つの隣接ノードとの複数のリンクを持つことができます。この関連を*並列リンク* と呼びます。並列リンクにはそれぞれ固有の番号 (伝送グループ番号) が割り当てられ、異なるリンク特性が割り当てられることもあります。2 つのノード間に 2 つの並列リンクを確立する場合、それらのリンクのリンク・ステーションは、一方のリンクでは単一のアダプターに接続することができますが、他方のノードでは個別のアダプターに接続しなければなりません。つまり、アダプター番号と隣接 (または宛先) リンク・ステーション・アドレスの組み合わせは、リンクごとに固有でなければなりません。

リンクの活動化

ノードおよびリンクの特性を隣接ノードに伝達するメッセージ単位は、*交換識別* (XID) と呼ばれます。**USE_PU_NAME_IN_XID=1** の場合、PU 名が XID の CP 名フィールドで使用されます。 これは CP-CP セッションをサポートしない LEN リンクでのみ指定できます。 それ以外の場合には、制御点名がこのフィールドで使用されます。 XID は、リンクの活動化前および活動化中にはリンクとノードの特性の確立およびネゴシエーションのために交換され、リンクの活動化後にはこれらの特性の変更を通知するために交換されます。

APPN ノードは、他の T2.1 ノードまたは境界ノードと XID 形式 3 (XID3) を交換して、役割のネゴシエーションを行います。 PU 2.0 接続の場合には、**LINK_STATION** キーワードを使用して、 XID3 で交換される PU 名およびノード ID を指定します。 USE_PU_NAME_IN_XID=1 の場合、PU 名が XID の名前フィールドで使用されます。それ以外の場合には、制御点名がこのフィールドで使用されます。 送信側ノードの特性に関する情報が XID3 に入れられます。これには、リンク・ステーションの役割 (1 次、2 次、またはネゴシエーション可能)、 TG 番号、ノード・タイプ、論理リンク番号、受信可能な最大基本伝送単位のサイズ、ノード ID、および PU 名が含まれます。 PU 名は通常、制御点名ですが、同時 PU 2.0 接続をサポートするために、 **LINK_STATION** キーワードで代替 PU 名とノード ID を指定することができます。

リンク・タイプ

Communications Server ノードでは、一般に以下の 5 つのタイプのリンクが定義されます。

- 基本ネットワーク・アクセス、初期活動化 (APPN またはホスト)
- 基本ネットワーク・アクセス、ホスト・リンク
- 基本ネットワーク・アクセス、常時使用 (必要なときに使用)
- 2 次ネットワーク・アクセス、インバウンド・リンク (定義済みのリンク特性)
- 2 次ネットワーク・アクセス、限定使用 (限定資源リンクとも呼ばれます)

Communications Server 構成により、これらのリンク・タイプの使用を定義および制御する方法が提供されます。このセクションでは、使用されるノード、DLC、およびリンク構成パラメーター、およびこれらのパラメーター間の関連性と依存関係について説明します。以下のカテゴリーについて説明します。

- リンク定義および活動化パラメーター
- リンク非活動化パラメーター
- その他のリンク・パラメーター

以下のパラメーターについて説明します。

- **定義および活動化パラメーター**
  - 始動時活動化
  - 要求時活動化
  - 自動リンク再試行
  - 活動化試行の最大回数
  - ユーザー要求による再活動化

- **非活動化パラメーター**
  - 非活動状態タイムアウト
  - 限定資源
- **その他のリンク・パラメーター**
  - 接続ネットワーク
  - CP-CP セッション・サポート
  - 高性能経路指定 (HPR) サポート
  - 隣接ノード・タイプ
  - 優先ネットワーク・ノード・サーバー
  - SSCP セッション要求
  - PU 名 (SSCP セッション要求が **1** の場合)

注: これらのパラメーターは ACG ファイルに入っており、 (**SNA ノード構成**によって) パネルで使用できない場合があります。

リンク定義および活動化パラメーター

このセクションでは、定義パラメーターと活動化パラメーターについて説明します。

始動時活動化

*始動時活動化*リンクは、一般には、Communications Server を始動したときに最初に活動化される、基本ネットワーク・アクセス・リンクに使用されます。このリンクが活動化されるのは、使用するマシンで Communications Server を始動する場合であり、 Communications Server が実行中である限りは活動化状態のままです。

始動時にリンクを活動化するように定義するには、 ACG ファイルの **LINK_STATION** キーワードに **ACTIVATE_AT_STARTUP=1** を指定します。ネットワーク接続のために重要なリンクは、一般に、始動時活動化として構成されます。重要なリンクも、自動リンク再試行に構成できます (36 ページの『自動リンク再試行』 を参照)。

このタイプのリンクの例として、APPN エンド・ノード (EN) から優先ネットワーク・ノード (NN) サーバーへのリンクがあります。

始動時に非活動にするリンク (**ACTIVATE_AT_STARTUP=0** としてコーディングされます) の例として、 Communications Server の始動時に即時に必要にならないホスト・リンク、ノードによってリンク特性を制御する必要のあるインバウンド・リンク、常時活動状態にするとコストがかかりすぎるリンクなどがあります。これらのリンクは、始動時に非活動にするリンクとして定義され、リンク資源がアプリケーションによって要求されたとき (『要求時活動化』を参照)、あるいはパートナーによって要求されたときに活動化されます。

要求時活動化

要求時活動化 (「自動活動化」とも呼ぶ) リンクは、一般には、リンクの動的な活動化を必要とするパートナー LU にアクセスするために使用されます。

Communications Server の始動時は、このリンクは非活動状態のままです。ただし、隣接 CP 名が指定されている場合には、使用可能リンクとしてトポロジーに組み込まれます。このリンクが活動化されるのは、トランザクション・プログラム (TP) が、リモート LU (リンクを活動状態にする必要のある LU) への接続を要求した時点です。 Communications Server は、このリンクを活動化するために定義された完全修飾パートナー LU を使用します。

要求時活動化としてリンクを定義するには、起点ノードの ACG ファイルの **LINK_STATION** キーワードに **ACTIVATE_AT_STARTUP=0** および **FQ_ADJACENT_CP_NAME=**(netid.cpname) を構成しなければなりません。パートナーが **FQ_ADJACENT_CP_NAME** でない場合には、 **PARTNER_LU** キーワードを構成してください。

また、多くの場合、要求時活動化リンクは、必要でなくなったときに非活動化されるように、限定資源 (39 ページの『限定資源』を参照) として、あるいは非活動状態タイムアウト (39 ページの『限定資源』を参照) を指定して構成されます。

要求時活動化リンクの例として、限定された時間の間だけ活動状態になっている必要のあるパートナーへの接続を定義するリンクがあります。リンクを常に活動状態に維持しようとすると、予想以上にコストがかかる可能性があります。例えば、1 つまたは複数のコンピューターの集合を常時通信させるものとします。毎日の終業時に、いずれか 1 つのマシンがなんらかのリモート・マシンとのリンクを活動化させる必要があります。それにより、その日の結果を送信したり、データのバックアップを取ったりするためです。

別の例として、データ・サーバーまたはプリント・サーバーに接続する場合があります。この接続は、サーバー側の資源を必要とします。サーバー側でリンク・ステーションとセッションの最大数になる制限を避けるため、要求時活動化リンクを介する要求が完了したあとでデータ・サーバー側の資源を解放するように、要求時活動化リンクを構成してください。

要求時活動化リンクは、必ずしも限定資源リンクではありませんが、**LINK_STATION** キーワードに **LIMITED_RESOURCE=1** パラメーターを組み込むことにより、限定資源リンクとして定義することができます (39 ページの『限定資源』を参照)。

自動リンク再試行

この自動リンク再試行は、障害のあるリンクの使用可能性を向上させる、エラー回復機能です。失敗したあとでリンクを (ユーザー介入なしに) 再活動化させたい場合には、自動再活動化を使用することができます。自動リンク再試行により、次のパラメーターが **LINK_STATION** または **PORT** のいずれかのキーワードに指定されている場合には、自動再活動化がリンクを試行しようとします。

- **DELAY_APPLICATION_RETRIES**
- **RETRY_LINK_ON_DISCONNECT**
- **RETRY_LINK_ON_FAILED_START**
- **RETRY_LINK_ON_FAILURE**

これらのパラメーターのうちの 1 つが **PORT** キーワードに指定されている場合、**INHERIT_PORT_RETRY_PARMS** パラメーターが指定されていると、**LINK_STATION** キーワードがこの値を使用します。

活動化が正常に行われると、インターバル・タイマーは 0 にリセットされます。

以下の種類のリンクでは、自動再活動化を使用することをお勧めします。

- 始動時活動化に設定されている NN へのリンク。このリンクが失敗すると、ネットワーク・ノード・サーバー (NNS) リンクだけが再活動化されます。
- ホスト・リンク
- バックアップのある基本リンク (通常は、始動時活動化としても定義されます)。
- 常に活動状態になっている必要のあるリンク。

活動化試行の最大回数

活動化試行の最大回数 は、従属 LU ホストのトラフィック (例えば、ダウンストリーム・アプリケーションのためにホスト・リンクを活動化しようとする LUA、3270、LU 2 ゲートウェイ、および DLUR またはこれらのいずれか) が際限なくリンク活動化を試みないようにするためのメカニズムを提供するリンク活動化パラメーターです。 **INHERIT_PORT_RETRY_PARMS** 最大活動化試行パラメーターは、リンク活動化要求が試行される回数を表します。この試行回数に達すると、試行回数がリセットされるまでは、後続の試行要求は拒否されます。活動化試行の最大回数に達したあとで従属 LU リンク活動化要求が出されると、実際にリンクの活動化が試みられることがなく、ただちに要求が拒否されます。この場合、1 次戻りコード X'0003' と 2 次コード X'00000005'、DLC 再試行、センス・コード X'00000000' が戻されます。活動化試行の最大回数に達したあとで出された独立 LU リンク活動化要求は試行されますが、活動化試行の最大回数に達したことを通知するために、1 次戻りコード X'0003' および 2 次戻りコード X'00000005' とともにセンス・コード 081C0001 が戻されます。

注: LUA アプリケーションなどの TP が、従属 LU アプリケーションと同じホストへのセッションを活動化しようとしてループに入ると、従属アプリケーションが最初の要求を出す前に活動化試行の最大回数を超過してしまいます。

活動化試行の最大回数は次の場合にリセットされます。

- 独立 TP がリンクを活動化したとき。リンク活動化で無制限の活動化再試行が行われないように、センス・コードを検査して適切なプロトコルを実装することは、TP の役割です。
- ユーザーが **SNA ノード操作**を使用してリンクを活動化したとき。
- 他の方向から (例えば、パートナーによって) リンクが活動化されたとき。

SNA ノード操作がリンク活動化を試みている場合、活動化試行の最大回数は 1 だけ減らされ、結果は無視されます。ゲートウェイ・ホスト・リンクでこの限界を超えた場合、ワークステーション・リンクが活動状態になると、 30 分後にリンクの活動化が試みられます。 これにより、再試行は停止しますが、ワークステーションが再始動したときに再始動します。 ゲートウェイ、 LUA、または **SNA ノード操作**によってリンクが正常に活動化されると、活動化試行の最大回数は 0 にリセットされます。

リンクで活動化試行の最大回数を構成するために、
MAX_ACTIVATION_ATTEMPTS= n パラメーターを **LINK_STATION** キーワードに構成します。この n は -1 から 127 までの試行回数です。 -1 は、**PORT** キーワード上の値を使用すべきであることを示し、0 は無制限再試行を示します。

ユーザー要求による再活動化

ユーザー要求による再活動化 は、ユーザーが、 **SNA ノード操作**から、あるいは Communications Server などを使用してコマンド行から、リンクの再活動化を要求したときに行われます。

リンク非活動化パラメーター

以下のセクションでは、非活動化パラメーターについて説明します。

非活動状態タイムアウト

非活動状態タイムアウト は、リンクを非活動化させる時期を制御する SDLC リンク非活動化パラメーターです。非活動状態タイムアウト値には、リンクが非活動化するまでにアイドル状態にしておくことのできる時間 (秒単位) を指定します。これは、**LINK_STATION** キーワードの **LINK_DEACT_TIMER** に似ています。両者の相違は、**LINK_DEACT_TIMER** が、すべてのセッションが終了する (セッション・カウントが 0 になる) のを待ってからリンクの非活動化を開始する点にあります。**INACTIVITY_TIMER** はセッション・カウントを無視し、指定された時間リンクがアイドル状態になっていると、非活動化を開始します。

この機能は、エミュレーター・セッション、LUA、3270、または LEN 接続が誤って長い時間活動状態のままになっているような状況に対処するために実装されたものです。このタイプの接続で、 **INACTIVITY_TIMER** 期間内に活動が行われなかったことがノードによって検出されると、リンクにセッションおよび会話が存在しているかどうかにかかわらず、そのリンクは自動的に非活動化されます。定義上、**LINK_DEACT_TIMER** は非破壊的であると考えられていますが、**INACTIVITY_TIMER** は破壊的であると考えられています。

注:

1. 非活動状態タイムアウトは、限定資源リンクでも非限定資源リンクでも使用できます。あるリンクが限定資源として定義され、かつ、会話が活動状態のままになっている場合、限定資源タイムアウトは満了せず、非活動状態タイムアウトの満了時にそのリンクが非活動化します。あるリンクが非限定資源として定義されている場合には、リモート・エンドにある資源を解放するために、非活動状態タイムアウトを使用してリンクが非活動化されます。
2. 現在 HPR では、非活動状態タイムアウトは無視されます。この理由は、リンク上のトラフィックのタイプを HPR が判別できず、そのリンクがアイドルにならないように、HPR キープアライブ・プロトコルによって十分なトラフィックが生成されるからです。

SDLC 接続上の非活動タイムアウトを構成するには、 **INACTIVITY_TIMER=** n パラメーターを ACG ファイルの **LINK_STATION** キーワードの **LINK_STATION_SDLC_SPECIFIC_DATA** パラメーター上にコーディングします。この n は、40 から 160 までの値です。あるリンク上の非活動状態タイムアウトを

構成するには、 ACG ファイルの **LINK_STATION** キーワード上に、**LINK_DEACT_TIMER=** n パラメーターをコード化します。この n は 0 から 1000 までの値です。 0 は、タイムアウトなし、つまりそのリンクが活動状態のままになることを表します。 SDLC の省略時値は 80 で、リンクの省略時値は 10 です。

限定資源

限定資源リンクは、一般的には、限定的に使用される 1 次ネットワーク・アクセス・リンクおよび 2 次ネットワーク・アクセス・リンクで使用されます。限定資源リンクは、セッション・カウントが 0 になったときに自動的に非活動化されるリンクです。限定資源リンクは、**ACTIVATE_AT_STARTUP=1** または **ACTIVATE_AT_STARTUP=0** として定義できます。このリンクが **ACTIVATE_AT_STARTUP=1** の場合、Communications Server が開始されるとこのリンクが開始されます。この限定資源リンクが **ACTIVATE_AT_STARTUP=0** の場合に関してですが、隣接 CP 名を指定すると Communications Server の始動時にこの限定資源リンクがトポロジーに組み込まれ、サービス要求時に活動化されます。

注: 始動時活動化リンクは、活動状態にならなければトポロジーに組み込まれません。

限定資源リンクを構成するには、**LIMITED_RESOURCE=1** を、 ACG ファイルの **LINK_STATION** キーワードに指定します。 **LINK_STATION** キーワードに **LINK_DEACT_TIMER=** n を指定します。そして、**ADJACENT_NODE_TYPE=LEARN** パラメーターを指定する必要があります。

注: **CP_CP_SESSION_SUPPORT=1** の場合、リンクは限定資源リンクではありません。この状態のリンクには、構成検査で警告のフラグが付けられます。活動状態の CP-CP セッションがあると、そのリンクは非活動化されなくなります。

LU 6.2 セッション・レベルのタイムアウト

LU、パートナー LU、またはモードに基づく LU 6.2 セッション・レベルのタイムアウトにより、 LU 6.2 会話の完了時に LU 6.2 セッションを終了させることができます。この機能は Communications Server for Windows ASCII 構成ファイル内で構成可能です。この設定は、すべての LU 6.2 セッション全体に対して有効です (CPSVCMGR セッションなどの IBM サービス TP を除く)。詳細については、「コンフィギュレーション・リファレンス」 を参照してください。

接続ネットワーク

接続ネットワークを使用すると、LAN または EEDLC 内の APPN ノードは相互に直接リンクを確立できるようになります。その場合に各ノードでの論理リンク定義は不要です。この機能によりシステム定義を大幅に減少させます。この場合、すべてのセッションを 1 つのネットワーク・ノードを通して経路指定するためのパフォーマンス上の負荷が増加することはありません。また、この機能により、このプロトコルに追加された新規ノードが APPC 会話に完全に参加できるようになります。その場合に、他の各ノードでの定義変更は不要です。複数のプロトコルを同じ接続ネットワークの中に入れることはできないので注意してください。

LAN、EEDLC、IPv4 および EDLC IPv6 には、それぞれ個別の接続ネットワークが必要です。

接続ネットワーク内のネットワーク・ノードでは、 1 つの接続ネットワーク内のすべてのノードが相互に直接リンクを確立できるものと見なされます。セッションの経路を計算するとき、ネットワーク・ノードでは直結リンクが検討され、通常は直結リンクが最適経路として選択されます。直結経路の計算が終わると、ネットワーク・ノードは、リンクの活動化に使用するパートナーのアドレスをエンド・ノードに送信します。

接続ネットワークの機密保護が必要なレベルに満たない場合には、接続ネットワークの経路が使用されない可能性があります。 接続ネットワーク DLC が機密保護されておらず、 **MODE_NAME** パラメーターで #BATCHSC のようなモードが使用されている場合には、ネットワーク・ノードは接続ネットワークを無視して機密保護された経路を見つけようとします。

LAN ブリッジが使用されている場合には、APPN はブリッジされた LAN 全体を単一の論理ネットワークと見なします。 LAN 上の任意の 2 つのシステム間でリンクを活動化することができるため、必要な接続ネットワークは 1 つだけです。 LAN 上のすべての APPN システムで、この接続ネットワークを定義しなければなりません。 同様に、EEDLC 接続ネットワークが使用されている場合、IP ネットワーク全体は単一の論理ネットワークと見なされます。

ネットワーク・ノードは、EN 登録時および APPN ディレクトリー探索時に接続ネットワーク情報を取り込みます。これによって、ネットワーク・ノード・サーバーは、セッション・エンドポイント・ノード間の (中間ノードを介して経路指定しない) 直接接続を算出するのに十分な情報を持ちます。 接続対象ノードには、他のノードのネットワーク・ノード・サーバーと CP-CP 接続されたネットワーク・ノードを持つ CP-CP セッションが必要になります。

接続ネットワークの利点を生かせるのはエンド・ノードとネットワーク・ノードだけです。 LEN ノードへのリンクは、明示的に定義する必要があります。

41 ページの図 11 は、サンプル接続ネットワークの図です。この LAN の図には、LOCALNET.IBMLAN という名前を付けられた接続ネットワークが示されています。このタイプの定義では、NN1 がすべてのエンド・ノードの活動ネットワーク・ノード・サーバーである限り、どの EN も他の任意の EN と直接に接続することができます。

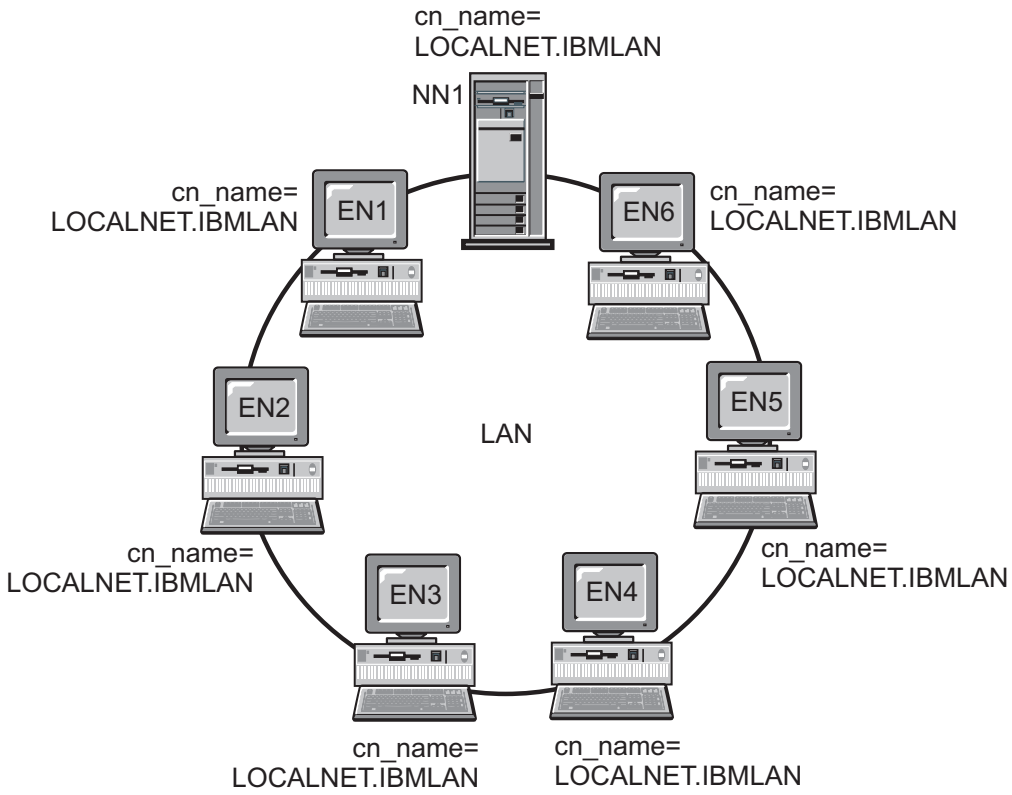

図 11. サンプル接続ネットワーク

その他のリンク・パラメーター

これまでのセクションで述べたその他の **LINK_STATION** キーワード・パラメーターのうち、明確でないもの、あるいは暗黙的に定義されているものは、以下のとおりです。

- 隣接ノード・タイプ
- 優先ネットワーク・ノード・サーバー
- SSCP セッション要求

このセクションでは、それぞれについて簡単に説明します。

隣接ノード・タイプ

隣接ノード・タイプでは、そのリンクを定義するノードに隣接するノードのタイプを指定します。有効なタイプには、次のものがあります。

- DSPU_NOXID
- DSPU_XID
- END_NODE
- HOST_DEP_LU_ONLY
- HOST_XID0
- LEARN

- NETWORK_NODE
- SUBAREA_LEN

詳細については、*「構成ファイル解説書」* を参照してください。

優先ネットワーク・ノード・サーバー

優先ネットワーク・ノード・サーバーでは、隣接ネットワーク・ノードを、定義されているリンクを介してネットワーク・ノード・サーバーとして使用するかどうかを指定します。

SSCP セッション要求

SSCP セッション要求では、定義されているリンクを介してホストから SSCP-PU セッションを要求するかどうかを指定します。

ディレクトリー・サービス

ネットワーク・ノードは、自身の内部にある LU に対して、また自身がサービスを提供するエンド・ノードの LU に対して、ディレクトリー・サービスを提供します。また、ネットワーク・ノードは、ネットワーク内の他ネットワーク・ノードが提供するディレクトリー・サービスを支援します。これを行うには、名前を指定された資源がローカル・ディレクトリー内で検出された場合に、受信したディレクトリー検索要求に肯定応答します。ローカル・ディレクトリーは、LU 名をその LU があるノードの制御点名に対応づけます。宛先制御点が LEN ノードまたはエンド・ノードの場合、ディレクトリーには、それらにサービス対象のネットワーク・ノードの名前が含まれます。

ディレクトリー・サービスの構成要素はどのノードにもありますが、その有効範囲と機能は、ノードでサポートされるディレクトリーのレベルによって異なります。

エンド・ノードは、そのノードの中にある LU に関する項目を含むローカル・ディレクトリーを維持します。さらに、エンド・ノードは、エンド・ノードとのセッションを持っていたことがある隣接ノードの LU のディレクトリー項目を維持します。隣接対等ノードとの LU-LU セッションの場合は、ローカル・ディレクトリーが探索されると、探索対象の LU と関連した適切な宛先制御点が戻され、正しい論理リンクの選択が可能になります。

LEN ノードの場合は、43 ページの図 12 に示すように、すべてのパートナー LU がディレクトリーに入れられます。隣接対等エンド・ノードになくても APPN ネットワークにある LU は、そのディレクトリーの中ではその指定ネットワーク・ノード・サーバーと関連づけられます。

LEN ノードは、そのディレクトリー内でそのサーバーに関連するすべての LU に代わって、 LU-LU セッション活動化 (BIND) 要求をそのノードのネットワーク・ノード・サーバーに送信します。すなわち、このサーバーは、この要求の宛先 LU を自動的に見つけて、BIND を適切に転送します。ネットワーク・ノードは Locate 探索を送り、応答を待ってから、BIND を送信します。

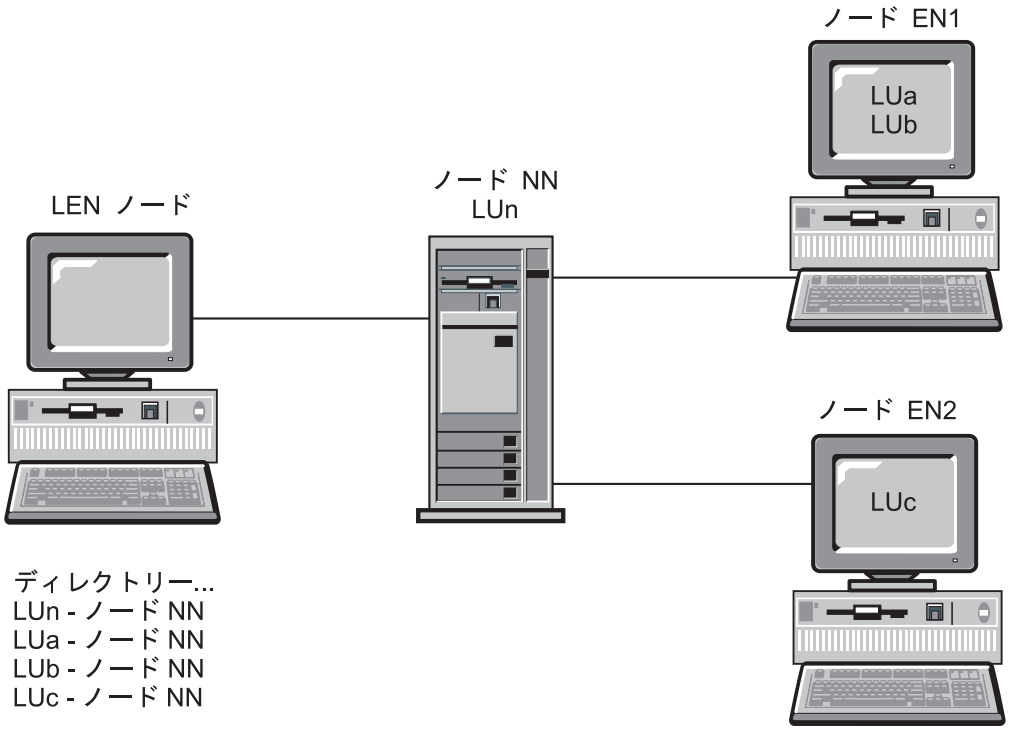

図 12. LEN ノード・ディレクトリー

LU がエンド・ノード・ディレクトリーに存在しない場合、エンド・ノードは Locate 探索を開始して、目的の LU を検出します。この探索を活動化するために、エンド・ノードはそのネットワーク・ノード・サーバーのサービスを呼び出します。 44 ページの図 13 は、エンド・ノード・ディレクトリーの例を示しています。

エンド・ノード (EN) は LU のロケーションを見つけるために、そのネットワーク・ノード・サーバーのサービスを使用します。 APPN ネットワークの LU はいずれもエンド・ノードで定義する必要はありません。しかし、隣接 LEN ノード LU は定義する必要があります。その理由は、隣接 LEN ノード LU は、ネットワーク・ノードに接続されておらず、APPN ネットワークの一部ではないからです。

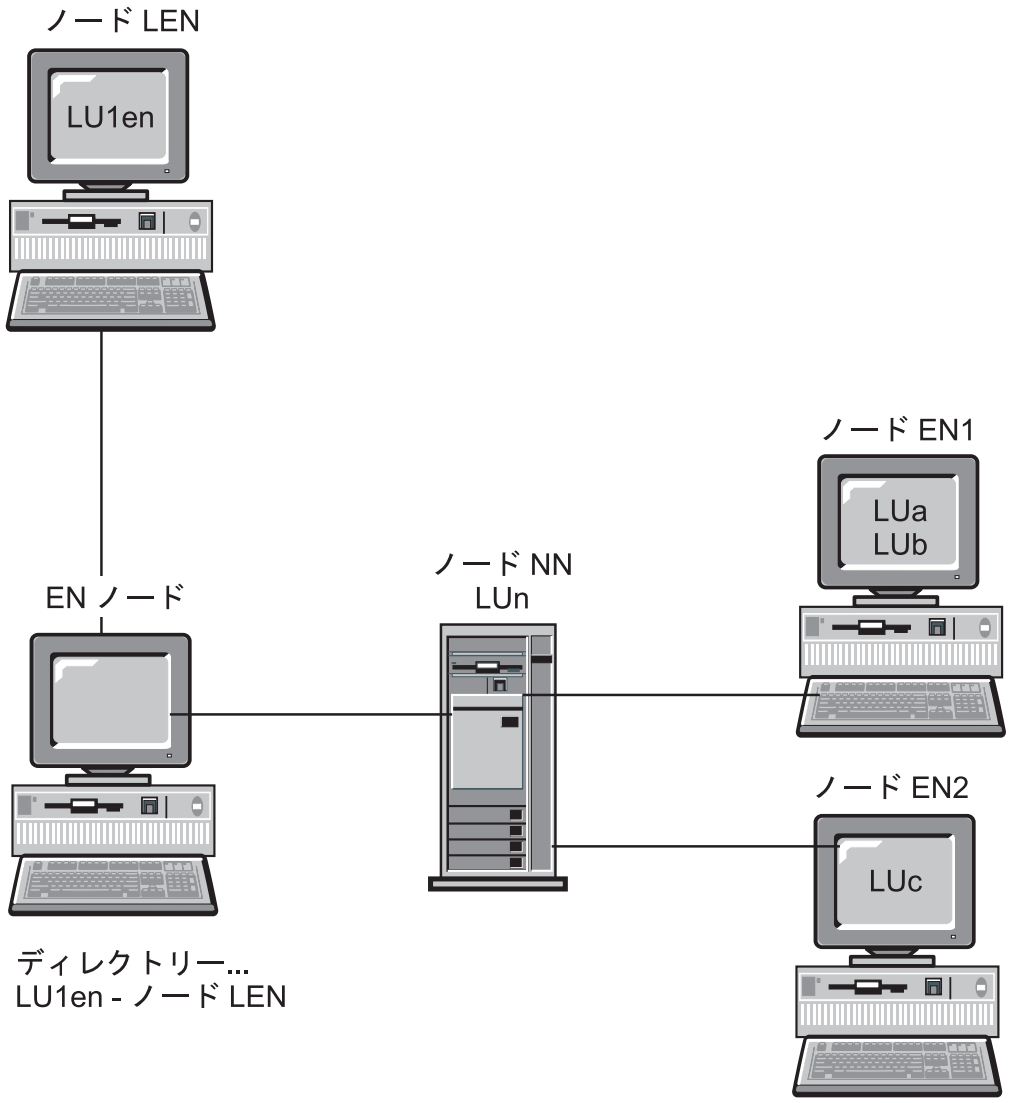

図 13. エンド・ノード・ディレクトリー

ネットワーク・ノードは APPN ネットワーク内の他のすべてのネットワーク・ノードと協力して、自分のサービスを受けるエンド・ノードに分散ディレクトリー・サービスを提供します。起点ネットワーク・ノードは、Locate 探索要求で宛先 LU の名前をサービス対象のエンド・ノードから受け取るか、あるいは BIND で 2 次 LU の名前を LEN ノードから受け取ります。該当の LU がネットワーク・ノードのディレクトリーに (ネットワーク・ノード自体にではなく) 存在する場合、ネットワーク・ノードはその LU の現在のロケーションを検査します。この検査は、宛先ネットワーク・ノード・サーバーに有向検索を送信することによって行われます。

LU が起点ネットワーク・ノードのディレクトリーにない場合、ネットワーク・ノードはネットワークの探索を開始します。この探索は各隣接ネットワーク・ノードにブロードキャスト探索を送信することによって開始されます。一方、各隣接ネットワーク・ノードはブロードキャストを順番に伝搬させ、成功または失敗を示す応答を戻します。成功したブロードキャスト探索で得られた情報は、ネットワーク・ノードによって、その後の必要に備えてキャッシュに入れられます。

また、APPN エンド・ノードは、ネットワーク・ノード・サーバーからの Locate 探索要求を受け取る (および応答する) こともできます。これを行う目的は、エンド・ノード内の特定の LU を探索するため、またはその LU が継続的に存在しているかを確認するためです。

ネットワーク・ノードに登録メッセージを送信することにより、各エンド・ノードはその LU をネットワーク・ノード・サーバーに登録できます。エンド・ノードがネットワーク・ノード・サーバーに登録されている場合、このネットワーク・ノードは、そのドメイン内にあるエンド・ノードに関する現行ディレクトリー情報を維持します。

図 14 はネットワーク・ノード・ディレクトリーを示しています。

ネットワーク・ノード (NN) のディレクトリーには、ネットワーク・ノードがサービスを提供するすべての LU が入っています。 エンド・ノード (EN) がその LU を登録します。 LEN ノード LU は構成する必要があります。

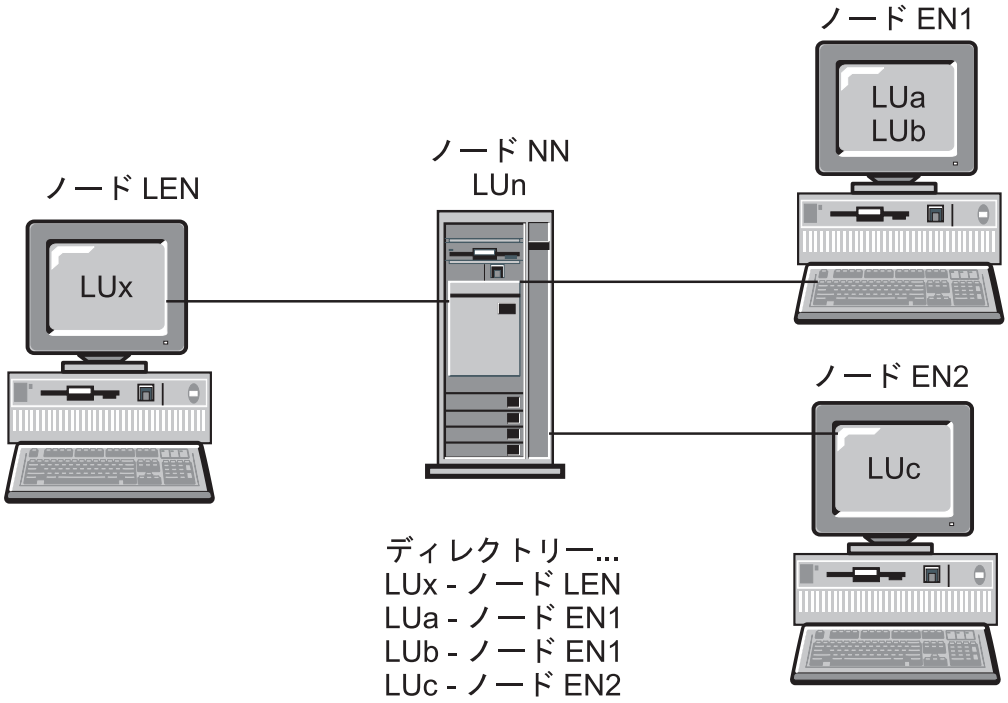

図 14. ネットワーク・ノード・ディレクトリー

トポロジーおよび経路選択サービス

ネットワーク・ノードは、そのノード自体およびそれがサービスするエンド・ノードへの経路選択サービスを提供します。ネットワーク・ノードは、内部ネットワーク・トポロジー・データベースを維持し、このデータベースには、ネットワークに関する完全な最新トポロジー情報が入っています。このトポロジー情報には、ネットワーク内のすべてのネットワーク・ノードの特性と、ネットワーク・ノード間のすべてのリンクの特性が含まれています。すべてのネットワーク・ノードに、トポロジー・データベースのコピーがあります。

ネットワーク・ノードは、ネットワーク・トポロジー・データベースを使用して、ネットワーク・ノード内の LU およびサービス先のエンド・ノードを起点とする、セッションの経路を計算します。ネットワーク・ノードが計算するそれぞれの経路は、起点 LU を含むノードから宛先 LU を含むノードへの経路のうち、現在時点での最小加重経路です。ネットワーク内での適切なパスを提供するために、この経路選択に使用するアルゴリズムは、まずリンクおよびノードに重みを割り当てます。要求されたサービス・クラスから見た特性の相対的重要度に基づいて、重み評価アルゴリズムは各ノードおよび論理リンク用のスカラー値を計算します。

トポロジー・データベース

ネットワーク・ノードにあるネットワーク・トポロジー・データベースには、すべてのネットワーク・ノードと、それらのネットワーク・ノードを相互に接続するすべての伝送グループに関する情報が入っています。このデータベースは完全な形で複製されて、ネットワーク内のすべてのネットワーク・ノードで共用され、経路選択に使用されます。データベースの保守に際しては、ブロードキャストによりすべてのネットワーク・ノードに更新情報を伝送する必要があります。この更新は、トポロジー・データベース更新 (TDU) メッセージによって行われます。このメッセージには、ノード識別情報、ノードとリンクの特性、および TDU で記述されている各資源の最新の更新を示す更新順序番号が入っています。

エンド・ノードにあるローカル・トポロジー・データベースには、そのエンド・ノードに関する情報と、そのエンド・ノードに直接接続されているノードに関する情報のみが入っています。

トポロジーおよび経路指定サービス構成要素は、ネットワーク・ノード間の CP-CP セッションを使用して、トポロジー・データベースの作成および保守のための情報を交換します。ネットワーク・ノードにあるこのトポロジー・データベースは、更新内容 (この更新内容は、資源 (ノードまたはリンク) の活動化または非活動化、あるいは既存の資源の特性の変更が起こるたびに、すべてのネットワーク・ノードに伝送される) を使用して最新状態に保たれます。

ローカル構成データベースおよびネットワーク・トポロジー・データベースは、48 ページの図 15 に図示されているように、各ネットワーク・ノードで維持されます。ローカル構成データベースはノードに固有ですが、ネットワーク・トポロジー・データベースはすべてのネットワーク・ノードに複製されます。

表 3 は、ローカル・ネットワーク・ノードの構成データベースに含まれている情報を示しています。

表 3. ローカル NN 構成データベース

ノード	リンク	接続
NN5	e	NN5-EN1
	a	NN5-NN7
	b	NN5-NN6
NN7	a	NN7-NN5
	d	NN7-NN8

表 3. ローカル NN 構成データベース (続き)

ノード	リンク	接続
NN6	b	NN6-NN5
	f	NN6-EN2
	c	NN6-NN8
	g	NN6-EN3
NN8	c	NN8-NN6
	d	NN8-NN7
	j	NN8-EN3
	h	NN8-EN4

表 4 は、ローカル・ネットワーク・ノードのネットワーク・トポロジー・データベースに含まれている情報を示しています。

表 4. ローカル NN ネットワーク・トポロジー・データベース

ノード	リンク	接続
1.NN5、NN6、NN7、NN8	a	NN5-NN7
	a	NN7-NN5
	b	NN5-NN6
	b	NN6-NN5
	c	NN6-NN8
	c	NN8-NN6
	d	NN7-NN8
	d	NN8-NN7

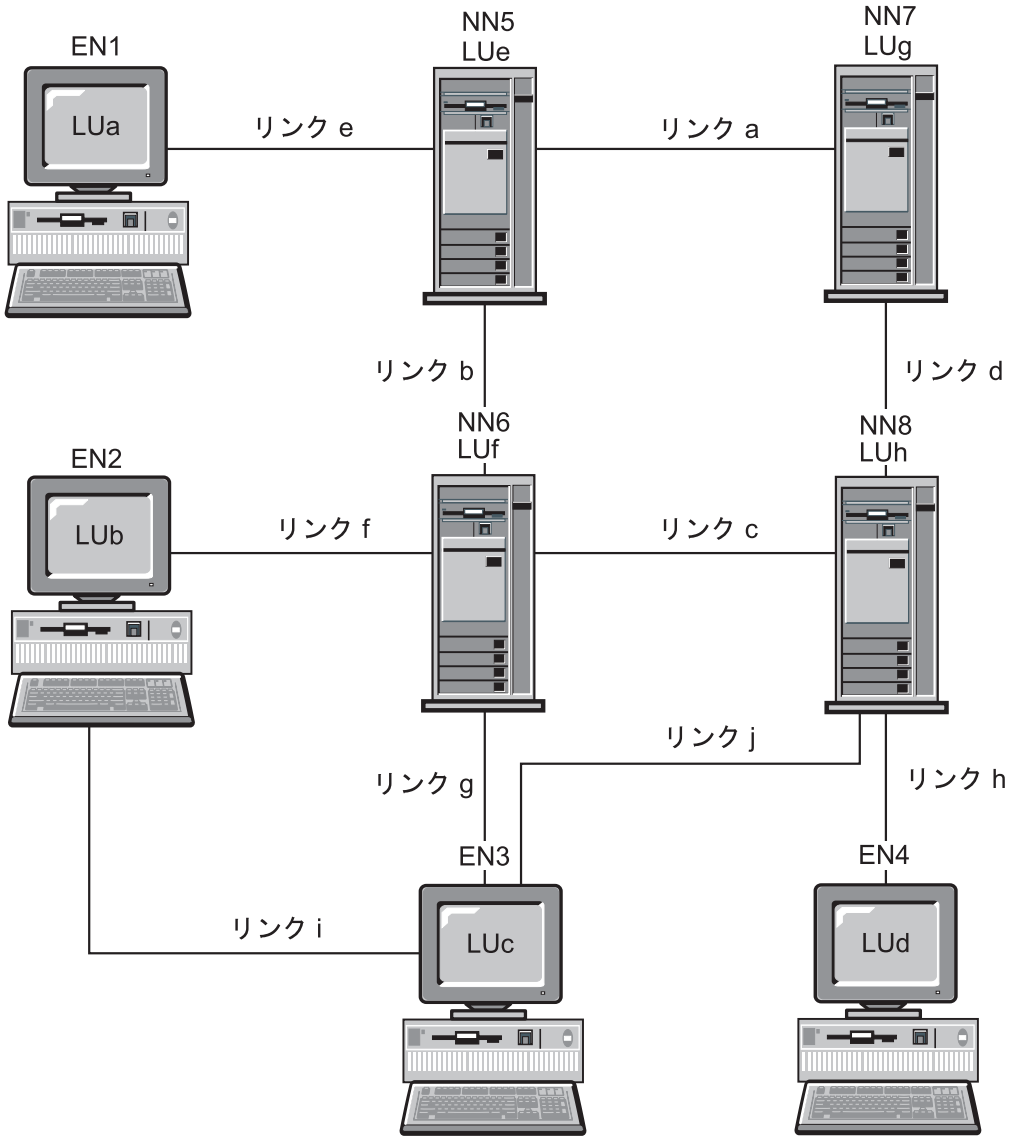

図 15. ネットワーク・ノード内のローカル構成データベースおよびネットワーク・トポロジー・データベース

モード

モードは、セッション特性の値とセッション・パートナー間のセッション数を決定します。例えば、セッションで交換される最大の要求単位 (RU) のサイズ (すなわち、*最大 RU サイズ*) は、モードの特性の 1 つです。モードはサービス・クラスも指定します。サービス・クラスはセッションの経路を選択するために使用されます。

サービス・クラス

セッション開始時に BIND でモード名を指定します。このモード名は、サービス・クラス (COS) 定義と関連づけられ、この COS 定義はセッションの起点ノードと宛先ノードの間で最も望ましい経路を決めるために使用されます。 COS 定義は、ノ

ードおよびリンクがセッション用に選択される経路に含まれるために必要な特性を指定します。経路選択アルゴリズムはこの指定を用いて、ノードまたはリンクが受け入れ可能であるかどうかを判定します。受け入れ可能な集合のうちから、経路選択アルゴリズムはセッション用として最良の経路を計算します。

COS 定義は変更可能であるため、起点ノードおよび宛先ノードが同じでも、指定されたモード名に応じてセッションごとに別々の経路を使用することができます。各ネットワーク・ノードはあらゆる宛先に至る、最も負荷が小さい (最も望ましい) 経路を計算することができます。

セッションが APPN ネットワークとサブエリア・ネットワークの両方を経由する場合、そのセッションは、以下の 2 つのサービス・クラスを使います。

- APPN ネットワークでは、セッションは、トランザクション・プログラムで使用されるモード用として定義された、サービス・クラス (COS) を使います。この定義は、ワークステーションで活動状態の構成内にあります。この COS は APPN ネットワーク内でセッションを経路指定する場合に使用されます。

  デフォルトのブランク・モードを使う場合、関連する COS は #CONNECT です。
- サブエリア・ネットワークでは、ログオン・モード・テーブル内のセッションで使用するモード名の項目に COS の名前を書き込むことができます。 VTAM プログラムは、この COS 名を使って、セッションをサブエリア・ネットワークを介して経路指定します。

  デフォルトのブランク・モードを使う場合、またはユーザーのログオン・モード・テーブルの項目で COS を定義していない場合は、 COS はデフォルト値として ISTSDCOS テーブルのブランク項目になります。

どちらの場合も、各ネットワークはモード名を使用して COS 名を検索しますが、2 つの COS 名は必ずしも同じである必要はありません。

SNA 伝送優先順位

伝送優先順位は、サービス・クラスで指定される値です。伝送優先順位は、サービス・クラス/伝送優先順位 (COS/TPF) 制御ベクトルの BIND で送られます。一度セッションが確立されると、後続するセッション・データは、 COS/TPF 制御ベクトルに指定された伝送優先順位で流れます。

優先順位が高いサービス・クラスを使用しているセッションで転送されるデータは、優先順位の低いセッションのデータを追越すことができます。エミュレーター・セッションのように、応答時間が重要である対話トラフィックを扱うセッションの優先順位は、高く設定してください。大量のデータを扱うセッション (例えば、 NetView® 分散管理プログラムのファイル転送)には、低い優先順位を設定する必要があります。伝送優先順位のサポートを使用して、大量のデータを転送するセッションが対話型セッションのトラフィック処理の障害とならないようにします。

伝送優先順位には、ネットワーク、高、中、低の 4 つがあります。ネットワーク優先順位は、トポロジー・サービスやディレクトリー・サービスのような、ネットワーク制御データに使用されます。その他の優先順位は、ユーザー・データに使用されます。

Communications Server では、LAN、SDLC、および X.25 リンクの伝送優先順位をサポートします。ネットワークの中に輻輳した低速リンクが含まれていると、この利点が最も明白になります。

経路選択

ネットワーク・ノード・サーバーが Locate 探索から応答を受け取ったあと、トポロジーおよび経路指定サービス構成要素は、要求された COS に基づいて、起点ノードから宛先ノードへの最適経路を計算します。トポロジー/経路指定サービス構成要素は資源の特性が変更されるたびにトポロジー・データベース更新を送受信するので、経路計算は常に最新情報を用いて行われます。

VTAM ユーザーのための経路選択

サブエリアを介して APPC トラフィックを経路指定するには、そのサブエリアに接続されたワークステーションが、 Communications Server のネットワーク・ノードとして定義されている必要があります。それぞれのネットワーク・ノードには、そのノードをサブエリアに接続するリンクが定義されています。ネットワーク・ノードから見た場合、サブエリアの内側にあるパートナー LU は、ホスト (LEN ノード) にあるものとして定義されます。ホストから見た場合、サブエリアに接続されたネットワーク・ノードは、それぞれ PU マクロで VTAM に定義されていなければなりません。ある特定の接続に対する APPN ネットワーク内のすべての宛先 LU 6.2 論理装置は、対応する PU (ネットワーク・ノード) の下に定義されます (あたかも実際にその PU の下にあるように)。しかし、実際は、LU はそのネットワーク・ノードに接続された APPN ネットワーク内であれば他のノードに置くことができます。ホストは、ネットワーク・ノード PU だけを認識します。ネットワーク・ノード PU は、ゲートウェイ PU にもなることができます。 NCP でパラメーターが YES にセットされていて、 PU セッションか制御点セッションがないときは、SETN トラフィック (**CP_CP_SESS_SUPPORT=NO**) は使用できません。

VTAM 定義の中の PU 名が Communications Server の制御点名と同じ場合、その制御点を VTAM 定義で LU として定義できないことに注意してください。 PU 名であっても、LU 名であっても、VTAM プログラム内の名前は固有にする必要があります。

PU の活動化の際に XID 交換を使うためには、PU マクロに **XID=YES** を含む必要があります。このパラメーターは、NCP 大ノードで定義されます。交換回線大ノードの PU ステートメントに、このパラメーターを入れないでください。

交換回線 SNA 装置の場合、PU マクロ内で新しいパラメーター **CPNAME**=cccccccc を使用できます。 このパラメーターには、サブエリアに接続されるネットワーク・ノードの制御点名を指定します。交換回線 PU 定義ステートメントでは、必ず **CPNAME** かまたは **IDBLK** および **IDNUM** を指定してください。 両方を指定することもできます。ネットワーク・ノードは、接続手順の中の XID 交換で、VTAM プログラムに対してそのネットワーク・ノードの制御点名を提供します。VTAM は、その制御点名を使って、それに対応する PU マクロを探します。対応する制御点を持つ PU マクロがない場合、 VTAM プログラムは、**IDNUM** および **IDBLK** を使ってその PU マクロを探します。

サブエリア経由の APPN ネットワークから、その APPN ネットワークの他の部分へ APPC トラフィックを経路指定するためには、オーナー VTAM のネットワーク名 (**NETID**) が APPN ネットワークのネットワーク ID と一致しなければなりません。 Communications Server では、(サブエリアに接続されたネットワーク・ノードの) ネットワーク ID は、 SNA ローカル・ノード特性プロファイルを使用して検出されます。

中間セッション経路指定

中間セッション経路指定は、ネットワーク・ノードが実行する機能です。この機能によって、ネットワーク・ノードは別のノード宛てのデータを受け取り、経路指定することができます。データの起点および宛先は、エンド・ノード、ネットワーク・ノード、または LEN ノードのいずれかです。 2 つの隣接ノード間のセッションの部分をセッション・ステージと呼びます。

高性能経路指定 (HPR) サポート

Communications Server は、Enterprise Extender (IP)、同期データ・リンク制御 (SDLC)、LAN、WAN、チャネル、マルチパス・チャネル (MPC)、および X.25 の各接続における高性能経路指定 (HPR) をサポートしています。 HPR の自動ネットワーク経路指定 (ANR) は、中間ノードの記憶域と処理の要件を最小限に抑えます。これは、エラー率の低い高速ネットワーク用のソリューションとして、 APPN 中間セッション経路指定 (ISR) よりも優れています。 HPR は、以下の主要な機能で SNA 経路指定を改善します。

- ステートレス中間ノード

  ステートレス中間ノードは、このノードを経由する接続について認識しません。

  HPR 中間ノードは、そのノードを通る接続をサポートするために制御ブロックやバッファー・プールを必要としません。経路指定情報が各パケットで運ばれるので、経路指定テーブルも必要ではありません。自動ネットワーク経路指定 (ANR) と呼ばれる手法を使用すると、HPR 中間ノードは、単にパケットを受信し、パケット・ヘッダーを調べて次のノードへの論理リンクの識別子を検出し、そのパケットをそのリンクで送信するだけで済みます。
- HPR 中間ノードには、以下の特徴があります。
  - HPR 接続エンドポイントが、高速トランスポート・プロトコル (RTP) を使用して失われたパケットの検出および回復を行うので、中間ノードはパケットの回復を行いません。

    LAN のエラー率が高い場合には、リンク・レベル・エラー回復手順 (ERP) サポートも選択することができます。ただし、エラー率が低い場合には、これは必要ないはずです。
  - HPR 接続エンドポイントによって、中間ノードは分割されたパケットの分解および再分割を行いません。その理由は、経路内のすべての中間ノードによってサポートされるパケット・サイズが自動的に選択されるからです。
  - 中間ノードはバッファーの積極的管理および輻輳の防止を行いません。その理由は、HPR 接続エンドポイントが中間ノードでの輻輳を防ぐフロー制御アルゴリズムを使用するからです。

– 中間ノードはテーブル検索によるパケットの経路の決定を行ないません。その理由は、HPR 接続エンドポイントが、各中間ノードが最適効率を達成するために選択したラベルを使用して、ソース経路指定を実行し、パケット経路指定情報を構築するからです。

ステートレス中間ノードが機能するためには、以下のことが必要です。

– 経路のエンドポイントには、経路指定遅延とアプリケーション・スループットとの組み合わせを反映するバッファー容量がなければなりません。バッファー容量は、ネットワーク構成に依存する値です。
– データ・リンクは、HPR ヘッダーを含んだ上で、アプリケーション・データを効率的に送るのに十分な大きさの I フィールド・サイズをサポートしなければなりません。
– エラー率が高いと HPR スループットに悪影響を及ぼすため、データ・リンクの信頼性は非常に高くなければなりません。

これらの条件を満たさない構成については、HPR なしの APPN を選ぶべきです。 HPR 技術は APPN の 1 つのオプションです。 HPR なしの APPN は引き続き使用可能であり、サポートされています。

- 輻輳の回避

  HPR ネットワークを使用すると、リンクの利用率を非常に高くすることができます。最適比率ベース (ARB) フロー制御という技法を使用して、 HPR 接続エンドポイントは、自動的にネットワーク輻輳を検知し、伝送負荷を減らします。この技法により、パケットの脱落を避けることができます。このパケットの脱落は、他の経路指定アルゴリズムを使用した場合には、中間ノードで使用可能なバッファーが不足しているために発生する可能性があります。

- 中断のない自動再経路指定

  HPR 接続エンドポイントが経路の障害を検出した場合、自動的に新しい経路を計算して、接続を再確立し、障害が原因で脱落したパケットを回復します。 HPR 中間ノードはステートレス (すなわち、そのノードを通る接続を認識していない) であるため、この回復手順には関与しません。経路が正常に切り換えられた場合、パケットは脱落しないので、その経路を使用しているアプリケーションが障害によって中断することはありません。

- 既存のハードウェアと互換性のあるソフトウェア

  HPR は、APPN のソフトウェア拡張です。したがって、既存の LAN または WAN アダプターとフレーム・リレー・リンクで HPR を使用することができます。 HPR は、専用帯域幅および保証されたリアルタイム・トランスポートを提供しないため (広帯域ネットワーク・サービスにこのレベルの機能を任せるので)、パケット転送遅延に対する効率上の制約は、HPR なしの APPN の場合と同じです。 HPR が使用する制御点プロトコルは、基本の APPN のプロトコルに少しだけ追加を行ったものです。 HPR ノードは、事前計画または調整を行わずに、既存の APPN ネットワークに追加としてインストールすることができます。

高速トランスポート・プロトコル

RTP は、最新のデータ通信メディアの利用、中間ノードでのオーバーヘッドの最小化、およびパス内でのリンク障害時の自動的なパスの切り替えを行うように設計された、メッセージ形式の集まりです。

RTP 接続は、*HPR* サブネット 内で確立され、セッション・トラフィックの転送に使用されます。 HPR サブネットは、APPN ネットワークの一部分であり、RTP 接続の確立と HPR セッション・トラフィックの転送を行う機能があります。 RTP 接続は、セッションがやりとりされる転送パイプ と考えることができます。この接続を使用すると、低レベルの中間経路指定を使用する超高速でデータを伝送し、エラー回復とフロー制御のためのリンク上のトラフィックを最小化することができます。これらのフローは RTP 接続エンドポイントが管理します。

RTP 接続の物理パスを自動的に切り替えることにより、セッションを中断せずに、障害のあったノードまたはリンクを通っていたデータを再経路指定することができます。障害時にネットワークにあったデータは、自動的に回復されます。

RTP は、リンク・レベルではなく終端間で、エラー回復を行います。このため、エラー回復に必要なフロー数が減り、パフォーマンスが向上します。リンク・レベル・エラー回復手順 (ERP) も、すべての接続でサポートされます。 ERP は、リンクの一方の終端でパケットが失われたときに、それを検知し、リンクの他方の終端に再送を依頼することによってパケットを回復します。 ERP を使用した場合、HPR パケットは番号付きの情報フレーム (I-FRAMES) として送信されます。フレームが脱落すると、DLC がその脱落を検知し、送信側がそのフレームを再送します。 ERP を使用しない場合、HPR パケットは無番号情報フレーム (UI-FRAMES) として送信されます。フレームが脱落した場合には、DLC はその脱落を検知することができず、 HPR の高速トランスポート・プロトコル (RTP) が接続の終端で脱落パケットを検知し、回復しなければなりません。

いずれの場合にも、RTP は常に、接続の終端で脱落パケットを検知し、回復します。指定されたどのような接続に対しても、ERP を使用する場合、または使用しない場合のリンク数に制限はありません。

ERP は、リンクごとに使用可能または使用不可にすることができます。 RTP は、接続終端で脱落パケットの検知と回復を行うため、ネットワーク構築時に ERP リンクを使用することも、非 ERP リンクを使用することもできます。これにより、パケット脱落率の高いリンクでリンク・レベル ERP を指定し、その他のリンクではリンク・レベル ERP を使用しないように指定して、スループットを最大化することができます。一般に、LAN では ERP の使用はお勧めしません。

注: ERP は広域ネットワーク (WAN) 環境では常に使用可能です。

RTP によるフロー制御と輻輳 (ふくそう) 制御も終端間で行われます。 RTP は、最適比率ベース (ARB) フロー制御という手法を使用して、可能な場合にはネットワーク帯域幅を完全に利用します。 RTP は、送信率の増加がネットワークでサポートされる場合は、パケットの送信率を増加します。輻輳は自動的に認識されるため、輻輳発生時はそれに従って送信率を減少させます。 接続パスにあるリンクの構成済み実効能力を使用して、初期の送信率と送信率増分の両方を判別することができます。

RTP 接続を介した制御流れ (CF) のサポートが、Communications Server の HPR で使用可能になりました。これまでは、制御流れでは (CP-CP セッションおよび経路設定メッセージを含めて) APPN 接続が使用され、一方、データ・フローでは HPR

接続が使用されていました。現在では、制御流れとデータ・フローの両方で RTP 接続を使用できるようになりました。このサポートには、CP-CP セッション用の自動パス・スイッチが含まれています。

RTP 接続の両終端がこの機能をサポートする場合には、制御流れは自動的に RTP を介して流れます。

自動ネットワーク経路指定 (ANR)

自動ネットワーク経路指定 (ANR) は、RTP によって使用可能にされるステートレス経路指定手法であり、到着したメッセージに付けられたラベルにより、パス内の次のホップが固有に識別されます。この手法は単純であるため、パスを使用する接続を認識しない低レベルで実施することができます。 ANR は、中間ノード経由のパケットを経路指定するためのプロセッサー・サイクル数と記憶域必要量を最小化します。

ANR の高速パケット交換機能は、中間ノードでのパフォーマンスを向上させます。これを行うには、APPN より低いレベルでの経路指定を行い、エラー回復、セグメント化、フロー制御、および輻輳制御を中間ノードでなくエンド・ノードで実行します。

中間 ANR ノードは、SNA セッションまたは RTP 接続を意識しません。各パケットの経路指定情報は、パケットに付加されたネットワーク・ヘッダーで運ばれます。各ノードが、パケットを転送する前に使用した情報をヘッダーから取り除くので、次のノードは、ヘッダーの固定位置に経路指定情報を見つけることができます。したがって、基本 APPN の場合のようにセッション・コネクター用に経路指定テーブルを維持する必要がないため、ノードを経由するパケットのスイッチングがより高速に行われます。

LU サポート

SNA は、LU タイプ 0、1、2、3、4、6.0、6.1、6.2、および 7 を定義します。LU タイプ 0、1、 2、3、1、および 7 は、アプリケーション・プログラムと各種のワークステーションの間の通信をサポートします。 LU タイプ 6.0 および 6.1 は、タイプ 5 のサブエリア・ノードにあるプログラム相互間の通信を提供します。 LU タイプ 6.2 は、タイプ 5 のサブエリア・ノードまたはタイプ 2.1 の周辺ノード、あるいはその両方にある 2 つのプログラム間の通信、およびプログラムと装置との間の通信をサポートします。

Communications Server は、以下のような装置をサポートするホスト・アプリケーションを通信を行う LU タイプ 0、1、2 および 3 をサポートします。

LU タイプ 0
4690 および 4700 金融機関端末

LU タイプ 1
3270 プリンター

LU タイプ 2
3270 対話式表示装置

LU タイプ 3
3270 プリンター

通信は同じ LU タイプの LU 間でのみ行われます。 例えば、LU 2 は別の LU 2 と通信しますが、LU 3 とは通信しません。また、Communications Server は LU タイプ 6.2 または APPC もサポートします。

Communications Server SNA 機能は、アプリケーションが APPC アプリケーション・プログラミング・インターフェース (API) を使用して、 2 つ以上のプログラムが協調して処理機能を実行する分散トランザクション処理機能を提供できるようにします。この機能は 2 つのプログラム間通信に関係し、それによって、2 つのプログラムがプロセッサー・サイクル、データベース、作業待ち行列のようなローカル資源、およびキーボードや表示装置のような物理インターフェースを共用できるようになります。

Communications Server は APPC API を介する APPC をサポートします。詳細については、次の資料を参照してください。

- *クライアント/サーバー・コミュニケーション・プログラミング*
- *システム管理プログラミング*

Communications Server の以下の機能は、ある範囲の LU タイプをサポートします。

- SNA ゲートウェイ

  SNA ゲートウェイは、IBM System/370™ (S/370) ホストまたは zSeries アーキテクチャーのホスト・コンピューター、あるいはその両方が LAN 接続ワークステーションをサポートできるようにします。これらのワークステーションは SNA ゲートウェイ・ワークステーションを介する通信に LU タイプ 0、1、2、3、または 6.2 を使用します。

  さらに、SNA ゲートウェイ機能は iSeries ホスト・コンピューターと接続する LU タイプ 1、2、または 3 をサポートします。 AS/400 ホスト・コンピューターは、データを処理するか、 S/370 または zSeries アーキテクチャーのホスト・コンピューターにデータを渡すことができます。
- 従来型 LU アプリケーション (LUA)

  LUA は、LU 0、1、2、および 3 をサポートするサービス・ルーチンを提供するシステム・ソフトウェアから構成されます。

SDDLU サポート

自己定義従属 LU (SDDLU) サポートによって、ホスト (VTAM) で、従属 LU を動的に定義したり活動化したりできるようになります。 VTAM では、従属 LU の動的定義 (DDDLU) と呼びます。 SDDLU を Communications Server で使用可能にするには、LU 定義で LU_MODEL ステートメントを指定します。

VTAM で DDDLU 機能を使用可能にするには、 PU 用の PU 定義ステートメントに LUGROUP オペランドを指定し、LU グループ大ノードを定義する必要があります。ユーザー用に LU 名を生成する IBM 提供の SDDLU 出口ルーチンを使用するには、 PU ステートメントで LUSEED オペランドを指定する必要もあります。

LUGROUP オペランドには、モデル LU 定義グループ名を指定します。この名前を VTAM がこの PU に対する LU の動的定義時に使用します。 LU グループ大ノードには、モデル定義ステートメントが含まれています。LU 用の動的定義は、この大ノードに含まれるモデル LU 定義を使用して構成されます。

LUSEED オペランドには、あるパターン名を指定します。このパターン名を SDDLU 出口ルーチンで使用して、動的に作られた LU 名を作成します。正しいステートメントを PU ステートメントに追加し、LU グループ大ノードを定義したあとで、使用可能対象とする SDDLU 機能に対して、これらの大ノードを活動化する必要があります。

従属論理装置リクエスター・サポート

従属論理装置リクエスター (DLUR) は、APPN ネットワークで従属 LU サポートを行うためのアーキテクチャーです。 Communications Server は、すべての基本 DLUR 機能と、以下の任意選択機能をサポートします。

- 自己定義従属 LU (SDDLU) サポート

  SDDLU サポートを使用すると、DLUR がサポートする LU が VTAM で動的に定義されて、その LU を事前定義しておく必要がなくなります。
- テークオーバー・サポート/正規の形態への戻しサポート

  このサポートによって、DLUR ノードと DLUS ノード間の接続に障害が発生したときでも、 LU-LU セッションを活動状態のままにすることができます。その接続は、同じ DLUS か別の DLUS との間で LU-LU セッションが中断されることなく再確立されます。
- 複数サブネット・サポート

  このサポートによって、DLUR ノード、DLUS ノード、およびアプリケーションを含むノードがすべて異なるサブネットワークに存在することも可能になります。
- DLUS がサービスする LU の登録

  エンド・ノード DLUR は、その LU を登録するので、ネットワーク・ノードは Locate 要求を DLUR に渡すことなしにこれらの LU を位置指定できます。
- バックアップ DLUS サポート

  主 DLUS との接続に障害が発生するか活動状態にならないときに、Communications Server は自動的にバックアップ DLUS との間に接続を試みます。

DLUR の使用

DLUR 機能を使用するには、**DLUR_DEFAULTS** 定義を構成し、その定義で指定されたリンク名を LUA、従属 LU 6.2 またはゲートウェイ定義でホスト・リンクとして使用してください。 Communications Server は、PUNAME、CPNAME、および NODEID を DLUS に送信します。この PUNAME は、信号情報の一部 (CV X'0E') として送信されます。

- DLUS は、(REQACTPU での CV X'0E' 検査をサポートする) 上位レベルである場合には、検索アルゴリズムで PUNAME を使用します。これは、VTAM 4.3 (PTF 適用) またはそれ以上で使用可能です。
- DLUS が下位レベルの場合には、DLUS は CV X'0E' を無視します。
- PUNAME と一致する名前がないか、あるいは DLUS が下位レベルである場合には、 DLUS は、(VTAM 交換回線大ノードで事前定義されたか、あるいは ISTEXCCS 出口を使用して動的に作成された) NODEID (IDBLK/IDNUM) または CP 名が一致する PU を見つけようとします。

ユーザーの選択項目 (トークンリング、SDLC、AnyNet など) の接続性を使用するネットワークへの接続は、DLUR-DLUS 接続が確立する前に構成され、アクティブになっていなければなりません。DLUR と DLUS 間に APPN 接続が存在した後は、制御セッションの対は、特殊モード CPSVRMGR を使用して、DLUR と DLUS の間に確立されます。この制御セッションの対は CP-SVR パイプとも呼ばれ、Communications Server へのリンクのように見えます。したがって、これを **SNA ノード操作**を使用して、活動化したり、非活動化したり、表示したりすることができます。

一度パイプが活動化されると、SSCP-PU および SSCP-LU サポートは、ホスト・リンクとしてパイプを定義した PU と LU に提供されます。 LU-LU セッションはパイプを使用しませんが、前述のとおり、そのネットワーク経由で利用可能な最適パスを使用します。

DLUR 環境では、専用 PU はいくつでも、LU 6.2 セッションで定義することができます。これにより、ゲートウェイが、専用 PU 経由でダウンストリーム・ワークステーションへのネットワーク管理アクセスを提供できます。この場合に、ホストへの膨大な物理リンク数は不要です。 58 ページの図 16 は、Communications Server のワークステーションが、ワークステーションおよび 4702 制御装置の両方の DLUR ゲートウェイとして機能する様子を図示しています。

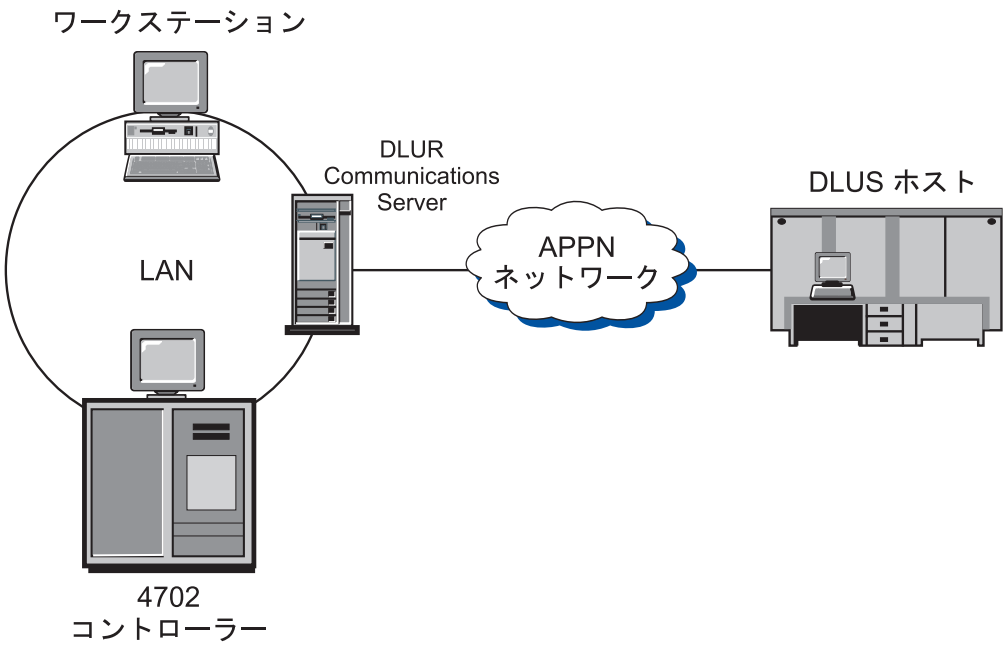

図 16. Communications Server ゲートウェイ経由でホストへの DLUR 接続

LU-LU セッション

Communications Server LU は、セッションの開始と、セッション開始要求への応答の両方を行うことができます。 LU がセッションを開始する方法と要求に応答する方法は、LU のタイプが独立であるか従属であるかによって決まります。

独立 LU (independent LU)

独立 LU は、SSCP からの援助なしに、LU-LU セッションで活動化する (つまり BIND 要求を送る) ことができます。したがって、SSCP-LU セッションは必要ありません。独立 LU は BIND の送信と受信の両方を行うことができます。 BIND 送信側は、1 次 LU (PLU) と呼ばれ、BIND 受信側は 2 次 LU (SLU) と呼ばれます。

独立 LU にすることができるのは独立型 LU 6.2 だけです。 Communications Server は他のタイプ 2.1 ノードだけでなく、ロー・エントリー・ネットワーキング・レベルのタイプ 5 サブエリア・ノードにも、独立 LU プロトコルをサポートします。

独立 LU は、同一ペアの LU 間で並列セッションを保有でき、また 1 つの LU と他のいくつかの LU との間で複数セッションを保有することもできます。これらの LU のセッション限度は、モード名を基準にして決められており、1 から 32767 までの範囲とすることができます。

59 ページの図 17 は複数セッションと並列セッションが独立 LU によって、どのように確立されるかについて図示しています。 LUx は、LUy との並列セッションおよび LUz との単一セッションをサポートしています。セッションの矢印の方向は、PLU-SLU 関係を示しています。この図で、LUx は、LUz とのセッションおよび LUy とのセッションの 1 つで PLU として働いています。 LUx は、また、LUy

との並列セッションの 1 つで SLU として働いています。

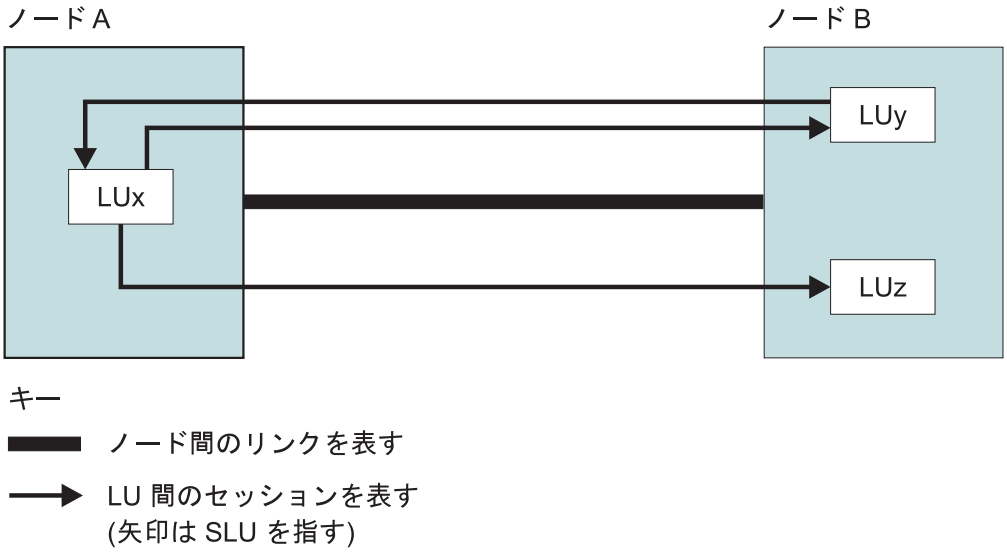

図 17. 複数セッションと並列セッション

従属 LU

従属 LU は、SNA ホスト・システムによって制御される LU です。従属 LU は、LU-LU セッションを活動化するために SSCP からの援助を必要とします。したがって、BIND を送信するためには SSCP-LU セッションを必要とします。従属 LU プロトコルは、タイプ 2.0 プロトコルを使用するタイプ 5 サブエリア・ノードの場合にのみ Communications Server によってサポートされ、他のタイプ 2.1 周辺ノードの場合にはサポートされません。従属 LU は SLU としてのみ機能し、LU-LU セッション限度は 1 です。ただし、Communications Server 内の複数の PU サポートにより、従属 LU セッションとの複数の同時 SSCP-PU セッションを確立できます。

従属 LU リクエスター (DLUR) 機能により、Communications Server は、従属 LU サーバー (DLUS) によって提供される拡張 SSCP サポートを利用することができます。この機能の利点の一部を以下に示します。

- 従属 LU をホストと隣接しないノードに配置することができる
- APPN 探索ロジックが LU-LU セッションに最良のパスを検出する
- SNA 従属 LU が APPN ネットワークを利用できる

DLUR を使用するには、**DEFINE_DEPENDENT_LU_SERVER** パラメーターを構成し、LUA、従属 LU 6.2、またはゲートウェイ定義で定義されたリンク名を使用します。

LU 6.2

LOCADDR=0 のコーディングによって、VTAM プログラムに独立 LU が定義されます。必要に応じて、 LOCADDR=0 で定義した多数の LU を持つことができます。しかし、注意すべきは、すべての LU 6.2 が必ずしも独立 LU でないことです。

APPN ネットワークの一部である LU を VTAM プログラムに定義する場合、ネットワーク・ノード (このノードは APPN ネットワークの該当部分をサブエリア・ネットワークに接続) に存在するものとしてこれらの LU を定義する必要があります。このネットワーク・ノードの PU 定義の後に、APPN ネットワークの他の部分からアクセスさせたい各 LU を定義します。制御点も LU であることを忘れないでください。

LU と 他の LU のセッションを確立したい場合、そのセッションがサブエリア・ネットワークを介するものであるときは、その LU を VTAM に定義する必要があります。これを避けるのに有効な方法がないため (例えば, APPN のワイルドカード)、 VTAM は各宛先 LU の名前を知っている必要があります。

APPN ネットワークは簡単に変更できるようになっているため、 APPN ネットワークの LU は可能なかぎり特別のメジャー・ノードに定義してください。 VTAM には、まだ存在しない LU も定義することができます。

他の LU

ネットワーク・ノードが、3270 エミュレーション用のサブエリア・ネットワークへの接続を使用する場合、 3270 エミュレーション用の LU タイプ 2 の LU は、APPN ネットワークの LU タイプ 6.2 の LU と同じ PU マクロで定義されます。このリンクは、3270 エミュレーションとホストの間の接続にも使われます。

APPN ネットワーク・ノード T2.1 サポート

APPN は IBM の SNA およびタイプ 2.1 (T2.1) ノード体系を拡張したものです。APPN では、サイズが大きく異なるシステムを、動的トポロジーのネットワークに、相互接続することができます。 APPN ネットワークは、従来の SNA ネットワークと比べて、より使いやすく、信頼性も高く、柔軟性に富んでいます。 APPN ネットワーク・ノードの追加情報については、*「3174 APPN Implementation Guide」* を参照してください。

データ圧縮

データ圧縮は、繰り返されるバイトまたは繰り返されるデータ・ストリングを圧縮して、レコードやブロックの長さを短縮するプロセスです。これによって、通信に必要な転送時間を短縮します。ホストとワークステーションのセッション間を転送されるデータの量を減らすと、速度が遅い回線でのスループットを上げ、費用のかかる回線でのビットごとのコストを下げることができます。

データ圧縮の使用により期待できるパフォーマンス向上 (転送されたバイト数で計算した場合) は、2:1 の比率になる可能性が高くなります。この意味は、データ圧縮をアクティブにしていると、下位のレベルのプロトコル変換で必要なバッファー内で、 2 バイトごとに 1 バイトを節約することを示しています。

データ圧縮は、次のことを必要とする場合に、役に立ちます。

- 特に低速回線において、応答時間を短縮したい。
- 料金がデータのボリュームにもとづく場合に、回線のコストを削減したい。
- 専用回線を少なくしたい。

ただし、データ圧縮には次のような欠点があるため、稼働している全セッションに適用しないでください。

- 圧縮と圧縮解除に追加の CPU サイクルが必要。
- データ・ストレージの増強が必要 (32 バイトから 9.0 キロバイトへ)。
- データ圧縮では、APPN サービス・クラス (COS) テーブルで定義したとおりの機密保護されたリンクが必要。
- 最良のパフォーマンスを得るには、RU サイズの調整が必要。 RU はそれぞれ、圧縮されてから送信されます。パケットが送信される場合、そのモードでより大きい RU サイズを指定しておくと、より大きなパケットを送信できるようになります。

注: 記憶域の増加量は、使用する圧縮アルゴリズムによって異なります。この増加は、メッセージに対して必要となる記憶域に加えて必要となります。

さまざまな圧縮アルゴリズムに関する詳細と技術的な説明については、次の資料を参照してください。

- *SNA 形式*
- *Better OPM/L Text Compression IEEE Transactions on Communications, vol COM-34, no 12*、1176-1182 ページ、1986
- *IBM ITSC VTAM V3R4 and V3R4.1 Planning Guide*
- *A Technical Guide to ESA/390 Compression*

以下の節は、SNA セッション・レベルの圧縮および Communications Server のインプリメンテーションの説明です。

SNA セッション・レベルの圧縮体系

SNA セッション・レベルの圧縮によって、LU-LU ハーフセッションでのデータ圧縮が実現します。 Communications Server では、サポートされる LU タイプ、つまり、LU タイプ 0、1、2、3 および 6.2 すべてで利用することができます。セッション・レベルでのデータ圧縮によって、次のような利点があります。

- 暗号化する前にデータを圧縮する方が効果的。
- データのタイプが異なる場合は、異なったアルゴリズムが効果的。
- アプリケーション・プログラムが、自身の圧縮ロジックを提供する必要がない。

SNA セッション・レベル圧縮では、一般的に 2 つのアルゴリズムが定義されています。ラン・レングス符号化方式 (RLE) と Lempel-Ziv (LZ) の形式です。Communications Serverは、次のアルゴリズムを使用して SNA セッション・レベル圧縮をサポートします。

- 圧縮なし。
- RLE 圧縮。 RLE は、ストリングまたは同一のバイトを短い符号化ストリングで置き換える、最も簡易で最も一般的に使用されるアルゴリズムです。
- LZ9 圧縮。LZ9 は、あらかじめ入力されたストリング (現在の RU か前の RU) を、圧縮/非圧縮テーブルの項目のゼロから始まる索引を表す 9 ビットのコードに圧縮する動的圧縮アルゴリズムです。テーブルの項目には、あらかじめ入力されたストリングが格納されます。

- LZ10 圧縮。LZ10 は、あらかじめ入力されたストリング (現在の RU か前の RU) を、圧縮/非圧縮テーブルの項目のゼロから始まる索引を表す 10 ビットのコードに圧縮する動的圧縮アルゴリズムです。テーブルの項目には、あらかじめ入力されたストリングが格納されます。

一般に、LZ は RLE より圧縮率が高くなりますが、メモリーと CPU 機能のコストが高くなります。

SNA セッション・レベル圧縮では、PLU-SLU と SLU-PLU の 2 つの方向から、セッションを識別します。 1 次論理装置 (PLU) は、セッションの活動化の責任がある LU です。 2 次論理装置 (SLU) は、応答する LU です。PLU は、セッション・バインド要求 (BIND) を、 BIND で応答する SLU に送ってセッションを活動化します。これは、PLU-SLU 方向と SLU-PLU 方向で、異なる圧縮アルゴリズムが使用されている可能性があるということを意味します。これは、圧縮レベルの BIND ネゴシエーションを介して実行されます。 LU 6.2 は、セッションの圧縮レベルのあらゆる組み合わせを使用することができます (例えば、PLU は RLE を、SLU-PLU は LZ9 を使用することができます)。その他のすべての LU タイプでは、圧縮が使用可能または使用不可にされています。使用可能の場合は、PLU-SLU 圧縮レベルは LZ9 で、SLU-PLU は RLE です。

Communications Server のデータ圧縮

Communications Server は、RLE 、LZ9、および LZ10 圧縮アルゴリズムで、SNA セッション・レベル・データ圧縮をサポートします。 Communications Server を使用すれば、CPI-C セッション (APPC セッションを介す)、 APPC (LU 6.2) セッション、および LUA (LU 0、LU 1、LU 2 および LU 3) セッションの通信で、データ圧縮を使用するように指定することができます。

データ圧縮を使用可能にするために、2 部構成が使用されます。データ圧縮のために Communications Server ノードを使用可能にする必要があり、 LU (APPC および LUA) を最初に使用可能にしなければなりません。 2 つのノード圧縮フィールド (レベルおよびトークン) は、「ローカル・ノード特性」ウィンドウ (.ACG ファイルの **NODE** キーワード) 上にあります。

圧縮レベル・フィールドは、どのようなセッションでも NONE、RLE 、LZ9、または LZ10 で開始できる、最大レベルを設定します。このフィールドは、構成または試行された全圧縮レベルに対して優先します (唯一の例外はスタンドアロン DFT であり、この場合はノード定義を必要としません)。 3270 エミュレーションまたはプリンターをサポートするために、 LUA (LU 0、LU 1、LU 2 および LU 3) を使用するセッションを構成する場合は、データ圧縮には LZ9 が必要です。その他の圧縮レベルは、これらの LU タイプのデータ圧縮を許可しません。

圧縮モード用のデフォルトの要求単位のサイズは、接続の基本伝送単位 (BTU) サイズの 2 倍です。パケット交換を使用している場合は、このデフォルトのサイズは使用せずに、より大きいサイズを使用して、パケットをセグメント化してください。

LU 6.2 圧縮は、以下の方法によって使用可能になります。

- Communications Server により提供された以下のモードを使用する
  - #INTERC
  - #BATCHC

- #BATCHCS
- #INTERCS

• 圧縮を使用可能にしたモードを変更または追加する

3 個のモード圧縮フィールド、圧縮要求、PLU->SLU 圧縮レベル、および SLU->PLU 圧縮レベルは、モード定義パネル (.ACG ファイルの **MODE** キーワード) 上に表示されます。

圧縮要求には、2 つの値を指定できます。

Prohibited
圧縮しません。

Requested
これを使用して、PLU->SLU 圧縮レベルおよび SLU->PLU 圧縮レベルで定義されている値を持つデータ圧縮を要求します。要求されたレベルは、以下のような場合採用されません。
• ノード設定値に許容レベルの制限がある
• SLU がレベル・ダウンをネゴシエーションした

ノード圧縮設定値で制限されない限り、SLU は PLU が要求した圧縮レベルに従います。

Communications Server 圧縮の詳細については、製品のオンライン・ヘルプ・テキストか、または*「構成ファイル解説書」* を参照してください。

SNA セッション・レベル暗号化

SNA セッション・レベル暗号化によって、ワークステーションとホストとの間で転送される全データまたは選択データの暗号化を行うことができます。暗号化を使用してワークステーション・データを保護する場合には、ホストも暗号を使用するように構成しておかなければなりません。

データの機密性を有効にするために、IBM SecureWay® 4758 PCI Cryptographic Coprocessor (IBM 4758 と呼ばれる) アダプターをサーバーにインストールする必要があります。このアダプターは、アダプターに付属の説明書に従って、初期化しなければなりません。

Communications Server では、LU 6.2 セッション・レベルの暗号化は、指定されたトランザクション・プログラム用に使用されるモード記述に基づいて構成されています。暗号化には 2 つのレベルがあります。

• APPC セッション・レベル

  必ず 2 つの LU 間で行われ、キーの変換に制御点は係らない。

• APPN セッション・キー変換

  開始側 LU の制御点 (EN または NN) およびおそらくその NN サーバーが開始側 LU に加えてキーを変換する。

暗号化のモードを構成するには、「SNA 機能」ウィンドウを開き、「**モード**」 を選択します。そして、「モード定義」ウィンドウの中の、「**セットアップ....**」を選択します。「圧縮およびセッション・レベル暗号化サポート」ウィンドウが表示されます。暗号化の構成のためのパラメーターは、2 つの部分に分かれています。

- セッション・レベルの暗号化には、暗号化が任意選択か (LU が交渉する)、または必須か (暗号化を使用しなければならない) を指定することができます。

  注: Communications Server からホストへの暗号化は、常に必須として設定されます。

- APPN セッション・キー変換には、LU のみがキーを変換するのか、エンド・ノードのみがセッション・キーを変換するのか、またはエンド・ノードとそのネットワーク・ノードがキーを変換するのかを指定することができます。

Communications Server には、キー保管とキー変換のために他のプロダクトが必要になります。キー保管のために、CCA (共通暗号化体系) プロダクトが必要です。これは、 IBM 4758 アダプターに付属のユーティリティーが管理しています。 Communications Server が CCA 製品を呼び出し、呼び出された CCA 製品が IBM 4758 アダプターと対話し、キーを入手してデータを暗号化します。

VTAM ユーザー:

Communications Server は SNASVCMG セッションを暗号化しません。ユーザーの VTAM アプリケーション定義の APPL ステートメントに、ENCR=OPT を指定してください。 VTAM で暗号化を行うためには、MODEENT ステートメントに暗号化を指定してください。 次は、その一例です。

```
ENCR=B'0011' FOR MANDATORY ENCRYPTION
```

VTAM 暗号化機能を使用するには、IBM プログラム式暗号機能 (PCF) を VTAM の始動前に開始しておくことが必要です。

VTAM V3R4.1 以降では、VTAM は、暗号サービス (セッション・レベル暗号化の提供など) のために統合暗号化サービス機能 /MVS (ICSF/MVS) への新しいインターフェースを使用します。このインターフェースは、ICSF/MVS が実装している共通暗号化体系 (CCA) に従っています。このサポートによって、VTAM の開始後に暗号化サービスの開始および停止を行うことができ、さらに、 VTAM または活動状態の LU-LU セッションを停止せずにマスター・キーを変更することができます。

データ暗号化の定義方法については、「*z/OS® Communications Server: SNA ネットワーク・インプリメンテーション・ガイド*」を参照してください。

管理サービス

Communications Server の管理サービス (MS) は、ネットワーク構成要素間に分散した機能で、ネットワークの操作、管理、および制御を行うものです。この機能は、「*Systems Network Architecture Management Services Reference*」 に文書化されている SNA 管理サービス体系に基づいています。

フォーカル・ポイント、サービス・ポイント、およびエントリー・ポイント

Communications Server は管理サービス・フォーカル・ポイント (FP)、サービス・ポイント (SP)、およびエントリー・ポイント (EP) アプリケーションのインストールを可能にするプログラミング・サポートを提供します。管理サービス SP アプリケ

ーションは、管理サービス EP アプリケーションの変形で、提供する機能の種類が異なるだけです。それ以外は、管理サービス EP アプリケーションと同じように管理サービス・フォーカル・ポイントと対話します。

フォーカル・ポイント

管理サービス・フォーカル・ポイントは、ネットワークを管理するための制御の中心点です。管理サービス・フォーカル・ポイントは、管理サービス SP アプリケーションまたは管理サービス EP アプリケーションから、ネットワークの操作に関連するデータ (問題データおよびパフォーマンス・データなど)、またはプロダクト ID を要求することができます。

また、管理サービス・フォーカル・ポイントは、管理サービス・データのカテゴリーに基づき、その管理下のノードからある種の非送信請求管理サービス・データを受け入れることができます。管理サービス・カテゴリーの一例としては、MS アラートがあります。 1 つの管理サービス・フォーカル・ポイントで 1 つまたは複数のカテゴリーの管理サービス・データを管理することができ、あるネットワークには、管理サービス・フォーカル・ポイントが 1 つ以上存在することができます。管理サービス・フォーカル・ポイント機能を提供するプロダクトの例としては、IBM Communications Server、 IBM NetView プログラム、および IBM OS/400® オペレーティング・システムがあります。

サービス・ポイント

管理サービス SP とは、あるノード内の機能であり、それにより、自分では管理 EP サービスとして機能することができない装置から、データ要求およびデータ収集を行うことができます。この種の装置には、例えば LAN プロトコルによって (ただし、高いレベルの SNA プロトコルによってではなく) 管理サービス SP ノードに接続された装置があります。非ローカル・データを収集することを除けば、管理サービス SP は、管理サービス・ フォーカル・ポイントとの関係において、管理サービス EP が機能するのと同じように機能します。IBM NetView/PC および IBM LAN ネットワーク・マネージャー・プログラム・プロダクトが管理サービス EP アプリケーションの例であり、これらが、管理サービス SP 機能および管理サービス EP 機能を提供します。

エントリー・ポイント

管理サービス EP とは、ノード内の機能であり、その機能がローカル管理サービス・データを捕そくし、処理のために管理サービス・フォーカル・ポイントにそのデータを送信します。これを行うのは、要求発生時、あるいは非送信請求発生時のいずれかです。 Communications Server は、アラートをアラート管理サービス・フォーカル・ポイントに送信するための管理サービス EP 機能を提供します。これらのアラートは、Communications Server 内部で生成されることもあり、それを使用する DLC で生成されることもあります。また、Communications Server は、アプリケーションのプログラミング・サポート (IBM NetView/PC および IBM LAN ネットワーク・マネージャー・プログラム・プロダクトなど) を提供します。これを行うには、アラート管理サービス・フォーカル・ポイントに送信されるアラートを提供します。

SNA 管理サービス体系のレベル

SNA プロダクトは特定のレベル (または世代) の SNA 管理サービス体系を実現しています。また、プロダクトのなかには、複数のレベルの体系をサポートするものもあります。 Communications Server は、管理サービス体系の 3 つのレベルのいずれかをインプリメントする SNA プロダクトとの間で、管理サービス・データの送受信を行うことができます。次の 3 つのレベルがあります。

マルチドメイン・サポート (MDS) レベル

管理サービス体系の MDS レベルをインプリメントする SNA 製品、例えば Communications Server および IBM NetView バージョン 2 リリース 2 (またはそれ以降)。このレベルは、MDS メッセージ単位 (MDS-MU) の送信および受信を行うことができます。 IBM NetView バージョン 2 リリース 2 は、制御点 (CP) としてではなくサブエリア LU として MDS レベルを提供し、 MDS-MU の移送に SNASVCMG モード・セッションを使用します。フォーカル・ポイントとしては、明示的、暗黙的 (1 次)、暗黙的 (バックアップ) の FP-EP 関係をサポートします。 NetView バージョン 2 リリース 2 は、MDS レベルのサポートのない EP プロダクトとのホスト FP-EP 関係も引き続きサポートしています。

移行レベル

前のレベルの管理サービス体系をサポートする SNA プロダクト、例えば、IBM OS/400 バージョン 1 リリース 3 モディフィケーション・レベル 0 (またはそれ以前)。移行レベルのプロダクトは、明示的、デフォルト、およびドメインの FP-EP 関係をサポートします。ドメイン FP-EP 関係は、移行レベルのノードとの CP-CP セッションが活動化されたときに暗示されます。移行レベルのサーバー・ネットワーク・ノード (NN) は、サービスされる側のエンド・ノード (EN) に FP 通知用 MS 機能を送信しません。また、移行レベルのサービスされる側の EN は、サーバー NN から FP 通知用 MS 機能を受け取りません。このレベルでは、CP-MSU の送信および受信を行うことができますが、MDS-MU の送信および受信を行うことはできません。フォーカル・ポイントとしては、アラート管理サポート・カテゴリーのみをサポートします。

ネットワーク管理ベクトル・トランスポート (NMVT) レベル

NMVT レベルの SNA 管理サービス体系を実現する SNA プロダクト、例えば、IBM NetView バージョン 2 リリース 1 (またはそれ以降)。 NMVT は、PU 管理サービスと制御点管理サービスの間の活動セッションを流れる管理サービス要求単位 (RU) です。 NMVT がゲートウェイを介してワークステーションから経路指定される場合には、ゲートウェイは NMVT にその制御点名を追加します。

フロー制御

ネットワークでのデータ・フローを管理するために、Communications Server は適応セッション・レベル・ペーシングを使用します。この適応セッション・レベル・ペーシングは、セッション経路に関与する隣接ノードの各対の間で実行されます。 2 つの隣接ノード間のペーシングは、経路中の他の隣接ノード間で使用されるペーシングとは独立しています。

セッション・レベル・ペーシング

適応セッション・レベル・ペーシングはウィンドウ・ベースの方式で行われます。この方式では、送信側は明示的に認可された許可につき限られた数またはウィンドウの要求単位しか一度に連続して送信することができません。ウィンドウ・サイズは受信側の状態に基づいて変更することができます。この機能によって、ノードは通常のセッション操作時に送受信するデータの量を制御することができることになります。ウィンドウ制御によって、受信側ノードは、セッション・バッファーにデータを受信する速度を管理することができます。適応セッション・レベル・ペーシングは、多数のセッションをサポートするノードに動的な手段を提供します。この目的は、活動が集中しているセッションに資源を割り振り、活動がないセッションの未使用の資源を再利用するためです。適応セッション・レベル・ペーシングは、受信ノードが使用可能なバッファー資源を効率的に使用できるようにするものです。

エンドポイント間の各セッション・ステージのペーシングはそれぞれ独立しているため、エンドポイント・ノードと中間ノードは、いずれも、ローカル混雑条件に従って、処理するセッションに対するペーシングを適合させることができます。この処置は、APPN ネットワークにおけるグローバル・フロー制御と輻輳 (ふくそう) 管理の基礎となります。

ただし、対話式セッションと大きなファイルを転送しているセッションがリンクを共用する場合は、対話式セッションのデータをできるだけ早く伝送する必要があります。このためには、次の 2 つの方法があります。

1. ファイル転送セッションに低い優先順位を割り当てる。 #BATCH は低い優先順位を使用します。
2. 小さいウィンドウ・サイズの固定ペーシングを使用して、ファイル転送セッションがペーシング応答を待っている時点で、対話式セッション・データがそのリンクを使用できるようにする。 NCP ホストに直接接続している場合は、定義されたモードの受信ウィンドウへの双方向のペーシングを設定するのに、双方向の固定ウィンドウ・ペーシングを使用することができます。

適応 BIND ペーシング

BIND の転送は、ノードまたはネットワークの始動時に特に過密になることがあります。したがって、2 つの隣接ノード間の BIND のフローを制御するための 適応 BIND ペーシングが存在します。セッション・レベル・ペーシングに使用するのと同じウィンドウ・アルゴリズムが使用されます。

セグメント化と再組み立て

特定のリンクで許可された最大サイズの基本伝送単位より長い RU を伝送するために、 Communications Server はデータのセグメント化と再組み立てをサポートします。セグメント化されたデータは、パートナー・ノードでもとの RU に再アセンブルされます。この処置により、セッションの RU のサイズを、経路に使用されるリンクと独立に定義することが可能となります。

高性能経路指定ペーシング

高性能経路指定 (HPR) を使用すると、最適比率ベース輻湊制御 (ARB) という新しいフロー制御方式を使用することができます。 ARB では、ネットワークの輻輳を

予測して、ネットワーク内へのノードの送信率を下げ、輻輳が起きてからそれに対応するのではなく、輻輳を予防することにより、トラフィック・フローを調整します。

固定ペーシング

固定ペーシングを使用すると、2 つのセッションの間で、物理接続を共用することができます。固定ペーシングを使用しないと、伝送されるデータは共通データ・リンク制御 (DLC) 待ち行列に入れられ、対話式データが、既に待機状態にあるデータの後にキューされることになります。固定ペーシングを使用すると、データを DLC 待ち行列に入れるのに使用できる記憶域の量を減らすこともできます。しかし一般的には、ノード間でデータ転送を行うのに最も効果的な方法は、適応ペーシングです。

固定ペーシングはリモート・エンドで構成できます。あるモードで **MAXIMUM_RECEIVE_PACING_WINDOW** キーワードを指定して、適応ペーシング・ウィンドウを制限し、固定ペーシングの良さを利用します。

伝送優先順位を使用すると、固定ペーシングのように、セッション間で物理リンクを共用することができます。ただし、データが DLC 待ち行列に入れられると、記憶域がロックされますが、固定ペーシングに必須のペーシング応答がさらに必要になるわけではありません。

ホスト間での LU の区分

複数のサブエリア・ホスト接続を定義する場合、 1 つのホストのドメインからのトラフィックは 1 つの論理リンクを通して行う必要があります。手動ダイヤル呼び出し接続は単一のリンクであることに注意してください。各ホストをサポートするために別々の PU を定義しなければなりません。制御点で定義されたホスト・リンクのみが CP-CP セッションを確立することができ、 APPN ネットワークに参加することができます。 **USE_PU_NAME_IN_XID=1** があるリンクは、 CP-CP セッションを使用することができません。それ以外のホスト・リンクは、CP-CP セッションを使用することができ、 APPN 通信にも参加することができます。
LINK_STATION キーワードは、PU 名と PU で使用する論理リンクを指定します。並列リンクが必要な場合 (254 を超える従属 LU がある場合) は、リンクの 1 つで CP-CP セッション・サポートを No に指定しなければなりません。

従属 LU は、それぞれ 1 つの PU とだけ関連するものとして定義しなければなりません。 **LOCAL_LU** キーワードは、従属 LU タイプ 6.2 に使用されるホスト・リンク名を指定します。 **LU_0_TO_3** キーワードは、LUA 用のホスト・リンク名を指定し、 3270 プロファイルは、 3270 エミュレーション・セッションごとにホスト・リンクを指定します。

制御点は、PU を自動的に制御点と同じ名前で定義します。 1 つのサブエリア SSCP で定義された従属 LU は制御点 PU と関連づけることができます。 (制御点用に自動定義される LU も実際には従属 LU として定義することができます。) 別のサブエリア・ホスト用に追加される PU 2.0 には、それぞれ別々のリンクおよび PU 定義が必要です。 PU は **LINK_STATION** キーワードで PU を指定して定義します。 LU がすべて独立である場合は、必要ありません。

SSCP-PU セッションでホストにアラートを送信するためには、.ACG ファイルの **NODE** キーワードでフォーカル・ポイント・リンクを定義しなければなりません。ホストがアラートを受信するためは、ホストとの制御点用論理リンクを指定しなければなりません。そのホストとのリンクが使用できない場合には、Communications Server はアラートをログに記録します。 PU 2.0 ホストから受け入れられるネットワーク管理要求は、制御点 PU に関するものだけです。応答は制御点 PU を使用して同じホストに送信されます。

各従属論理装置は、ホストで構成されているのと同じローカル・アドレスを構成していなければなりません。しかし、SNA ゲートウェイを使用すれば、ゲートウェイでのアドレス変換が可能になります。従属 LU 6.2 が、対等ノードには独立 LU として働くことができます。つまり、サブエリアに対してのみ従属となります。APPN ネットワークに同じサブエリア、すなわち制御 SSCP を含むサブエリアとの接続が別にある場合、このような LU をその APPN ネットワークの一部としてはなりません。サブエリアが独立である場合を除き、1 つの APPN ネットワークには 1 つのサブエリア接続しか認められません。ゲートウェイは同じサブエリアと並列リンクを持つことができますが、CP-CP セッションおよび APPN トラフィックで使用できるリンクは 1 つだけです。

サブエリア・ネットワークの SSCP は、リンクが確立されてから、制御下の従属 LU を活動化します。LU は活動化されなければセッションを始動することができません。 APPC が終了すると、ノード内の PU とセッション中の各活動ホストから切断が要求されます。各ホストは、まず LU を非活動化し、次に SSCP-PU セッションの PU を非活動化してから、リンクを解放します。

SNA ゲートウェイ・サポート

Communications Server は、フル機能のシステム・ネットワーク体系 (SNA) ゲートウェイを提供します。このゲートウェイにより、複数の LAN 接続ワークステーションは、1 つまたは複数の物理接続を介して、 1 つまたは複数のシステム /370 ホストまたは zSeries ホストにアクセスすることができます。これにより、ホスト接続に関するワークステーションあたりのコストを削減することができます。

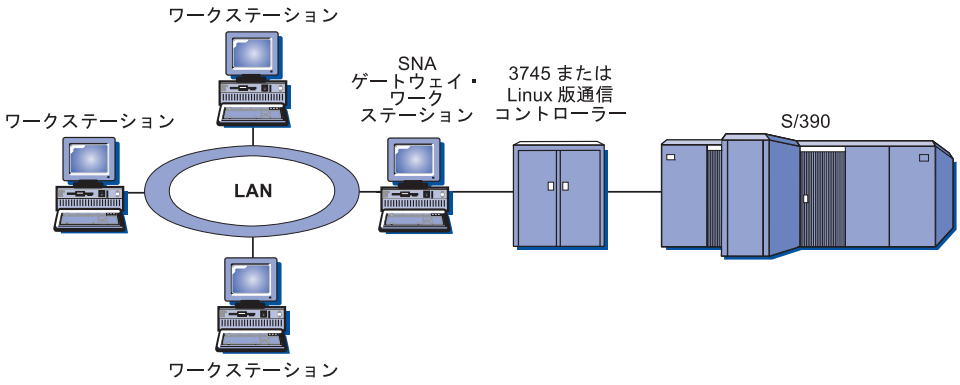

図 18. SNA ゲートウェイ構成の例

Communications Server ゲートウェイは、SNA プロトコル LU 0、1、2、3、と従属 LU 6.2 (APPC) をサポートします。 AnyNet SNA over TCP/IP 機能により、ダウンストリーム・ワークステーションは IP ネットワーク上の SNA ゲートウェイを介

して通信することができます。 このゲートウェイは、SNA パススルーを使用する iSeries ホストに対して LU 0、1、2、または 3 もサポートします。 iSeries ホストは zSeries ホストへデータの受け渡しを行います。

ゲートウェイは、LAN および WAN のホスト回線に接続されたワークステーション間のプロトコル変換装置としても動作します。

ゲートウェイに定義された LU は、特定のワークステーション専用に使用したり、複数のワークステーション間でプールして共用できます。LU をプールすることにより、ワークステーションが、共通 LU を共用することができます。これによって LU の使用効率が向上し、ホストにおける構成要件および開始要件が少なくなります。また、複数の LU プールを定義して、個々のプールを特定のアプリケーションに関連付けることもできます。また、複数のホストと関連している共通プールを定義することができます。クライアントがゲートウェイに接続している場合、ゲートウェイはこのプールから LU を 1 つ取り出してセッションを確立します。 セッションが終わると、その他のワークステーションがアクセスできるように、LU はプールに戻ります。

さらに、SNA ゲートウェイは、ワークステーションとホスト間でのネットワーク管理ベクトル・トランスポート (NMVT) の転送をサポートすることもできます。

各ホストは、SNA ゲートウェイを、ワークステーションごとに 1 つ以上の LU をサポートする SNA PU 2.0 ノードとして認識します。ホストに関しては、すべての LU は SNA ゲートウェイ PU に属します。 SNA ゲートウェイは複数のホスト接続を同時に維持することができ、指定されたホストに別々のワークステーション・セッションを割り当てることができます。

サポートされるワークステーションから見た SNA ゲートウェイは、SNA PU 4 通信制御装置であり、 BIND や UNBIND のようなホスト要求の転送を行うものです。ワークステーション LU は SNA ゲートウェイを認識しません。ただし、SNA ゲートウェイはワークステーション上のすべての LU を認識します。

LU 0、1、2、および 3 と従属 6.2 用の標準 SNA 接続プロトコルを使用し、 SNA ゲートウェイを介してホストと通信するダウンストリーム・アプリケーションは、Communications Server によってサポートされます。 表 5 は SNA ゲートウェイ機能の要約です。

表 5. SNA ゲートウェイの要約

機能	記述
アクティブ・ワークステーション	アダプターあたり 254 (LAN) 128 (X.25)
DLCs	AnyNet (SNA over TCP/IP) LAN (任意の NDIS** 準拠ネットワーク・アダプター X.25 SDLC (同期、非同期、AutoSync) OEM チャネル (アップストリームのみ) MPC チャネル (アップストリームのみ、DLU が必須) Enterprise Extender
ダウンストリーム・ワークステーション	LU 0、1、2、3、および 6.2 用の標準 SNA 接続プロトコルをサポートするあらゆるプロダクト。

表 5. SNA ゲートウェイの要約 (続き)

機能	記述
動的な追加と変更	可
暗黙的ワークステーション・サポート	可
LU プール	可
最大 LU 数	PU あたり 254。PU の数には制限なし。
操作モード	複数のダウンストリーム PU (ホストからは見えない)。 PU はホストからは見えない (DLUR からは見える)。
複数の PU サポート	可
セグメント化サポート	可
サポートしている LU タイプ	LU 0、1、2、3、および従属 6.2

第 3 章 AnyNet サポートの計画

Communications Server により、AnyNet SNA over TCP/IP のアクセス・ノードとゲートウェイに対するサポートが可能になります。

Communications Server の AnyNet SNA over TCP/IP 機能により、 SNA アプリケーションは IP ネットワークおよび SNA ネットワークを介して通信することができます。

SNA over TCP/IP のアクセス・ノード機能により、IP ネットワーク上にある SNA アプリケーション間の通信が可能になります。この機能は従属 LU リクエスター (DLUR) 付きまたはなしで、独立 LU6.2 と従属 LU 0、1、2、3、または 6.2 をサポートします。 さらに、SNA ゲートウェイと一緒に SNA over TCP/IP アクセス・ノードを使用して、 TCP/IP で SNA ゲートウェイ・セッションを使用可能にできます。

SNA over TCP/IP ゲートウェイ機能は、SNA アプリケーションの機能が及ぶ範囲を拡大します。これを行うには、SNA ネットワーク内の SNA アプリケーションと IP ネットワーク内の SNA アプリケーションが通信できるようにします。 SNA over TCP/IP ゲートウェイは、独立 LU 6.2 セッションをサポートします。

AnyNet SNA over TCP/IP の構成

このセクションでは、AnyNet SNA over TCP/IP の構成について詳しく説明します。

SNA 資源から IP アドレスへのマッピング

SNA over TCP/IP 通信を使用可能にするための最も大切なステップの 1 つは、Communications Server パネルからは実施されません。 SNA セッションまたは接続が確立される前に、SNA over TCP/IP はパートナーの IP アドレスを判別しなければなりません。これは、次のステップを使用して、パートナーの SNA ID を IP アドレスにマッピングすることによって達成できます。

1. SNA over TCP/IP は、Communications Server から次の形式のうちの 1 つで SNA ID を受信します。
   - LU 名の場合、`netid.luname`
   - CP 名の場合、`netid.cpname`
   - IDBLK 値と IDNUM 値の場合には、`Ablock ID` フィールドと `physical unit ID` フィールドの 2 フィールドがある `adjacent node ID` として構成
2. SNA over TCP/IP は ID をとり、ドメイン・ネームを生成します。
   - LU 名の場合、`luname.netid.snasuffix`
   - CP 名の場合、`cpname.netid.snasuffix`
   - IDBLK 値と IDNUM 値の場合、`bbbnnnnn.snasuffix`

   注: snasuffix のデフォルト値は SNA.IBM.COM です。 SNA over TCP/IP は IPV4 ネットワークだけで作動します。 SNA LU から IPV6 アドレスへの

マッピングはサポートされていません。 SNA ドメイン・ネーム接尾部に関する詳細については、オンライン・ヘルプを参照してください。

図 19 は、SNA over TCP/IP が生成したドメイン・ネームの例を示しています。

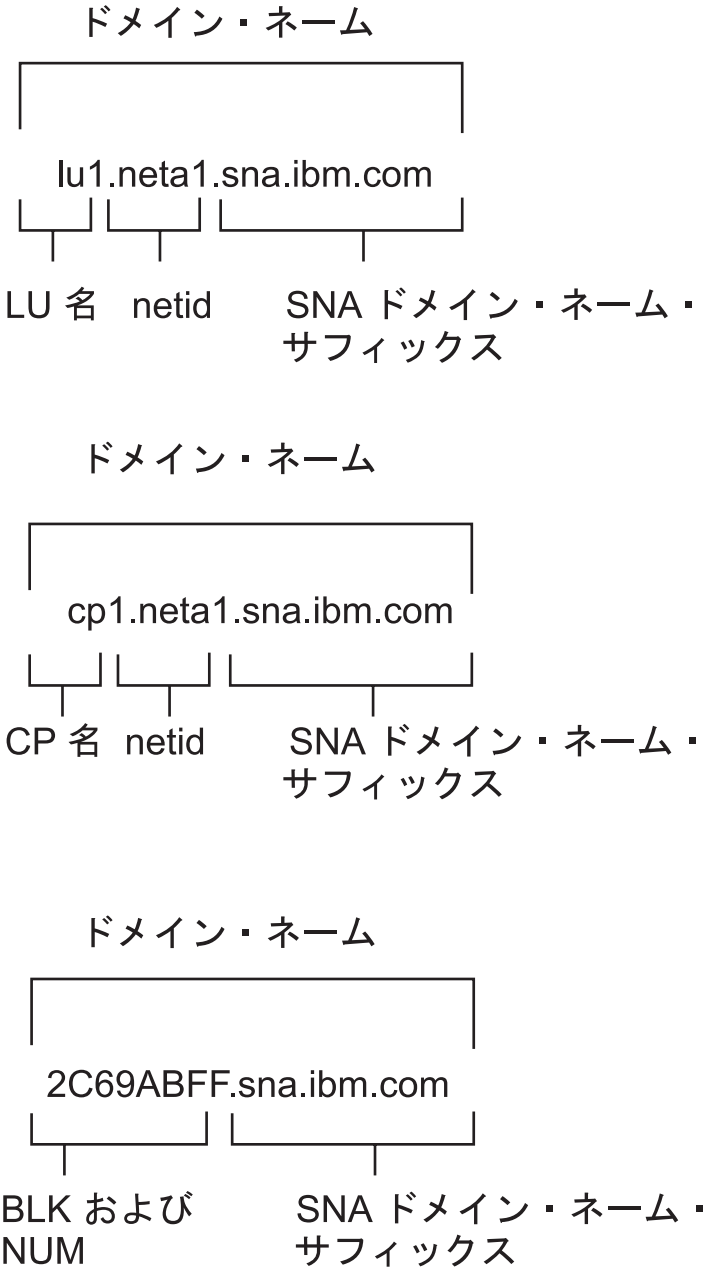

図 19. SNA over TCP/IP が作成するドメイン・ネームの形式

3. SNA over TCP/IP はドメイン・ネームを IP アドレスに変換することを要求します。
4. TCP/IP は HOSTS ファイルまたはドメイン・ネーム・サーバーを使用して、ドメイン・ネームを IP アドレス (例えば、9.67.192.28) に変換します。

IP ネットワークに SNA over TCP/IP ゲートウェイがあるときは、次に示す新たなアドレス・マッピング問題について考慮してください。

- ゲートウェイを通じてパートナー LU に到達できる場合、パートナーのドメイン・ネームは、ゲートウェイの IP アドレスにマップしなければなりません。並列ゲートウェイがある場合、ドメイン・ネームは各ゲートウェイの IP アドレスにマップする必要があります。
- AnyNet に必要なアドレス・マッピング情報を最小化するには、命名規則を考慮してください。命名規則では、LU 名は TCP/IP ホスト名と同じです。例えば、コンピューターのホスト名が PATR.ANYNET.OURCORP.COM であるとします。LU 名 PATR と netid ANYNET を使用しており、SNA ドメイン・ネーム接尾部を OURCORP.COM に設定している場合、 AnyNet は TCP/IP に対して名前 PATR.ANYNET.OURCORP.COM を解決するように依頼します。この名前は、既にドメイン・ネーム・サーバーに入っている必要があります。

ドメイン・ネームおよび IP アドレスの定義

このセクションでは、TCP/IP のネーム・レゾリューション機能について説明します。この機能は、 AnyNet が SNA 資源を IP アドレスにマップするのに使用します。この機能は、ローカル HOSTS ファイルと任意のドメイン・ネーム・サーバーの両方を照会して、ドメイン・ネーム (例えば、`lu1.neta1.sna.ibm.com`) を IP アドレス (例えば、`10.1.1.1`) に変換します。

HOSTS ファイル

TCP/IP ホスト・ファイルを使用して、ドメイン・ネームをネットワークの IP アドレスにマップします。ただし、ネットワークが大きくなり、各エンド・ユーザーのワークステーションでホスト・ファイルの維持に多くの時間を要するようになるにつれて、ドメイン・ネーム・サーバーを使用することを推奨します。

HOSTS ファイル (Windows システム・ディレクトリーの drivers¥etc サブディレクトリーにある) には、以下の項目をリストします。

- IP アドレス
- ドメイン・ネーム
- その他のドメイン・ネーム用の別名

例えば、IP アドレスが 10.1.1.1、ネットワーク ID が NETA1、 SNA 資源名が LUA1、SNA ドメイン・ネーム接尾部がデフォルト (`sna.ibm.com`) である場合には、ホスト・ファイルに以下を入力してください。

```
10.1.1.1      lua1.neta1.sna.ibm.com
```

ドメイン・ネーム・サーバー

ドメイン・ネームと IP アドレスは、ドメイン・ネーム・サーバー・データベースに定義することもできます。

各 SNA ID は、ドメイン・ネーム・サーバーによって、対応する IP アドレスにマップされます。これらのサーバーの位置は、コントロール・パネルのネットワーク・セクションに構成されます。

ホスト・ファイルおよびドメイン・ネーム・サーバーの詳細については、TCP/IP 資料を参照してください。ワークステーションで、Windows の TCP/IP サポートを使用している場合には、 Windows 製品に付属のオンライン TCP/IP 資料を参照してください。

SNA over TCP/IP ゲートウェイの考慮事項

次に示す情報は、ゲートウェイに関するものですが、ノード・ファンクションへのアクセスは行いません。

固有の CP 名と接続ネットワーク名の定義

SNA ネットワークを複数の IP ネットワークに接続する SNA over TCP/IP ゲートウェイが複数ある構成の場合、固有の SNA 制御点 (CP) 名と固有の SNA 接続ネットワーク名を各 IP ネットワークに定義する必要があります。

IP ネットワークのアクセス・ノードにある全 LU は、この CP 名を持つノード上にあるように見えます。

ドメイン・ネーム・サーバーまたはホスト・ファイルのリバース・データ・ファイルを使用して、指定の IP ネットワークについて、CP 名と接続ネットワーク名を定義します。 IP アドレス 127.0.0.3 を CP 名にマップし、IP アドレス 127.0.0.4 を接続ネットワーク名にマップします。

次の例は、リバース・データ・ファイル内の項目を示しています。SNA ネットワーク ID NETA、 CP 名 MYCPNAME 、接続ネットワーク名 MYCNET を持つ IP ネットワークの場合には、次の項目を定義することになります。

```
127.0.0.3 NETA.MYCPNAME.
127.0.0.4 NETA.MYCNET.
```

注:

1. 定義が DNS リバース・データ・ファイル内にある場合に限り、名前の最後にあるピリオドが必要です。ホスト・ファイル定義では、ピリオドは使用しません。
2. SNA ドメイン・ネーム接尾部は入れないでください。

Communications Server の AnyNet SNA over TCP/IP 機能は、デフォルトの CP 名 ($ANYNET.$GWCP) とデフォルトの接続ネットワーク名 ($ANYNET.$GWCNET) を提供します。 1 つの IP ネットワークを使用する構成では、CP 名または接続ネットワーク名を定義せずに、デフォルトを使用することができます。複数の IP ネットワークを接続する複数ゲートウェイを使用する構成では、1 つの IP ネットワークがデフォルトを使用できます。ただし、その他の IP ネットワークすべてについては、固有の CP 名と接続ネットワーク名を定義しなければなりません。 77 ページの図 20 は、2 つの IP ネットワークを使用する構成の場合の、 CP 名と接続ネットワーク名を定義する方法を示しています。

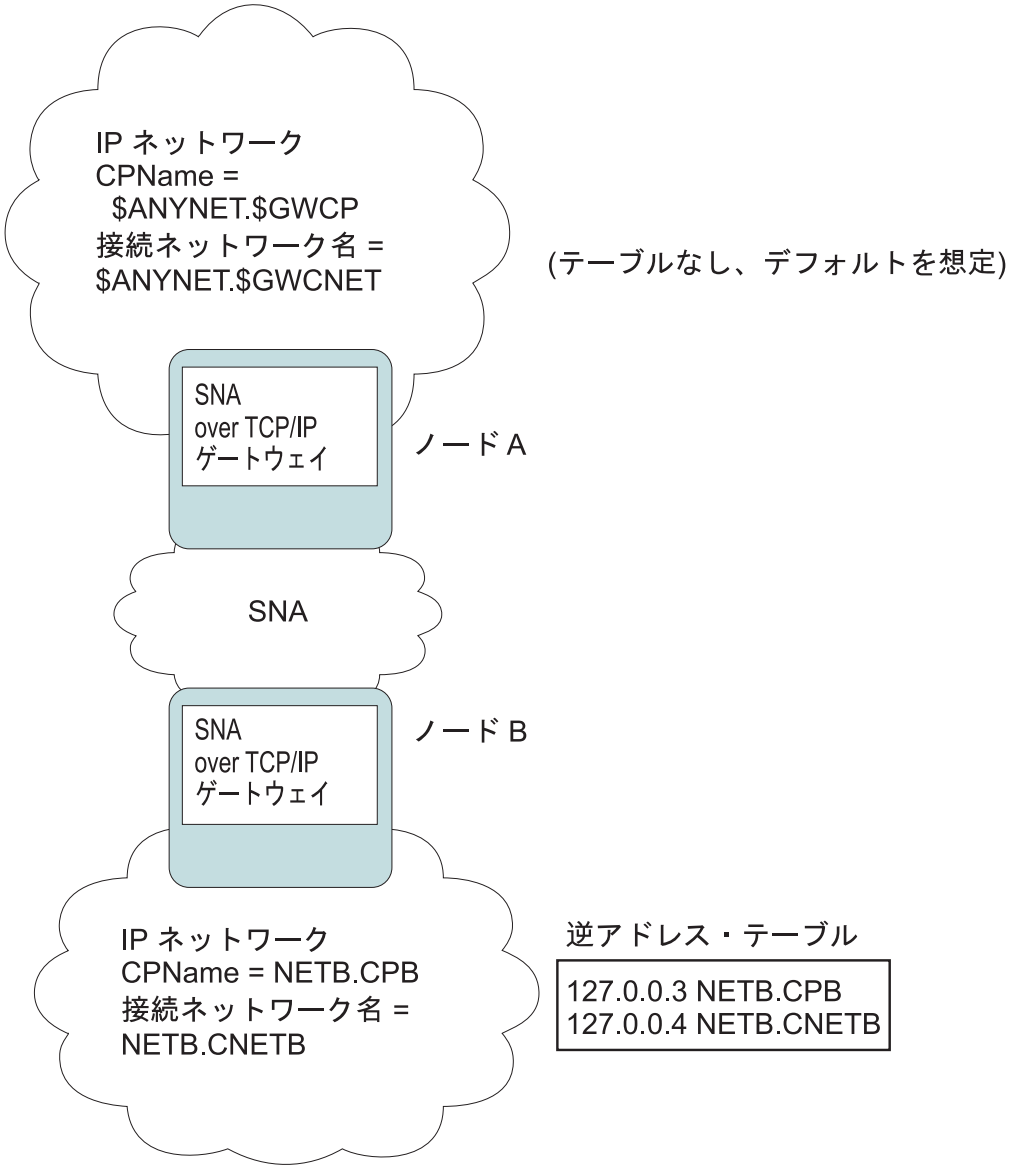

図 20. CP 名と接続ネットワーク名の定義

ドメイン・ネーム・サーバー定義を削減するためのワイルドカード項目の使用

SNA over TCP/IP ゲートウェイを使用しており、構成が以下の命名規約に準拠している場合、ドメイン・ネーム・サーバーのエントリー数を減少させることができます。それを行うには、1 つ以上の SNA over TCP/IP ゲートウェイ経由でアクセス可能な各 SNA ネットワーク ID ごとに、ドメイン・ネーム・エントリーを定義します。

- 各 SNA ネットワークには SNA ネットワーク ID が付いており、その ID がすべての SNA ネットワークの間で固有である必要がある。
- 各 IP ネットワークには SNA ネットワーク ID が付いており、その ID がすべての IP ネットワークの間で固有である必要がある。

- SNA ネットワークと IP ネットワークは、同じ SNA ネットワーク ID を付けることができます。

各 SNA ネットワーク ID ごとに単一のドメイン・ネーム・エントリーをコーディングすることによって、 IP ネットワークを通じて通信したい SNA ネットワーク内の各 LU にドメイン・ネーム・エントリーを定義する必要がなくなります。ワイルドカード・エントリー (*) を使用して、同じ SNA ネットワーク ID を持つすべての LU の LU 名を指定することができます。ワイルドカード・エントリーを *luname* の代わりに使用することによって、特定のネットワークにあるすべての LU を表す単一のドメイン・ネーム・サーバー・エントリーを定義します。

注: ワイルドカード・エントリーを使用する場合には、完全なワイルドカードを使用しなければなりません。 LUA* のような部分的なワイルドカードは無効です。

このワイルドカード・エントリーは、その SNA ネットワーク ID が付いたネットワークに到達するのに使用する最初の SNA over TCP/IP ゲートウェイの IP アドレスにマップされます。 図 21 に示すように、論理装置 (LU) SNAAPPL1、APPC1、APPC2、および LU5 は、ネットワーク NETB に存在しており、IP アドレス IPgwg を持つ SNA over TCP/IP ゲートウェイを介して、 IP ネットワークからのみ到達することができます。 SNA ドメイン・ネーム接尾部が SNA.IBM.COM の場合には、ドメイン・ネーム・サーバーに以下のエントリーを定義します。

```
*.NETB.SNA.IBM.COM IPgwg
```

このエントリーは、4 つの論理装置 (LU) すべてに使用されます。

注: 各論理装置 (LU) すべてを個別に定義するオプションがあります。

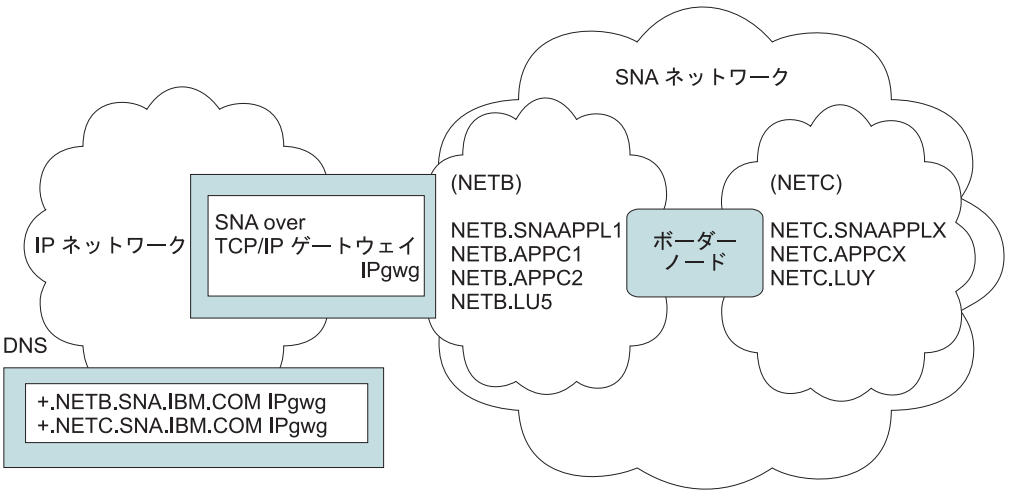

図 21. 2 つのネットワーク ID を持つ SNA ネットワークに接続されている単一のゲートウェイのドメイン・ネーム・サーバー定義

各 SNA ネットワークには、固有のエントリーがなければなりません。図 21 に示すように、 IP アドレス IPgwg を持つ SNA over TCP/IP ゲートウェイを介してのみ到達できるネットワーク NETC に SNAAPPLX、 APPCX、および LUY がある場合、ドメイン・ネーム・サーバー・エントリーは次のようになります。

```
*.NETB.SNA.IBM.COM IPgwg
*.NETC.SNA.IBM.COM IPgwg
```

さらに、各ゲートウェイには、固有のエントリーがなければなりません。 図 22 に示すように、前の例に対して、IP アドレス IPgwh を持つ並列 SNA over TCP/IP ゲートウェイを追加する場合、ドメイン・ネーム・サーバー・エントリーは次のようになります。

```
*.NETB.SNA.IBM.COM IPgwg
*.NETC.SNA.IBM.COM IPgwg
*.NETB.SNA.IBM.COM IPgwh
*.NETC.SNA.IBM.COM IPgwh
```

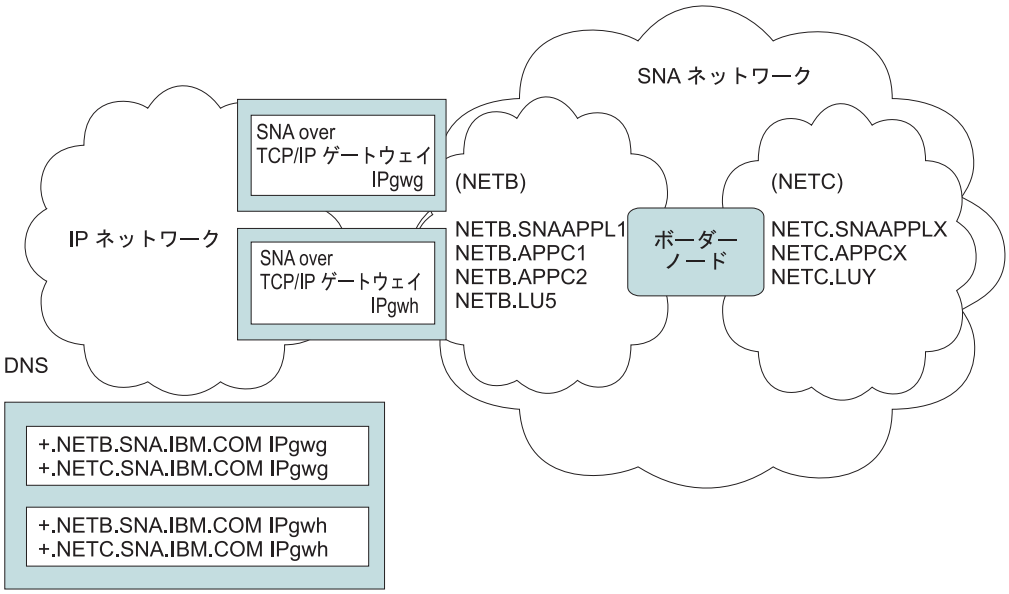

図 22. 2 つのネットワーク ID を持つ SNA ネットワークに接続されている並列ゲートウェイのドメイン・ネーム・サーバー定義

SNA over TCP/IP アクセス・ノード機能の考慮事項

次の情報は、アクセス・ノードに関連するもので、ゲートウェイに関連したものではありません。

AnyNet SNA over TCP/IP を介した SNA セッションの経路指定方法

SNA アプリケーションがセッションを開始するときは、Communications Server は使用するトランスポートを最初に決定しなければなりません。すなわち、SNA、IP、またはこの 2 つの組み合わせのいずれにするか決めなければなりません。

経路指定プリファレンスを設定することによって、希望するトランスポートを構成します。 AnyNet over TCP/IP 装置上で、またはパートナー LU 定義時の LU 単位で、デフォルトの経路指定プリファレンスを介してすべてのノードに経路指定プリファレンスを設定することができます。

注: ノードの経路指定プリファレンスは、そのノード (アクセス・ノード・セッション) から開始されるセッションのみを管理します。ノードを通過するセッションは、経路指定プリファレンスによる影響は受けません。

デフォルトの経路指定プリファレンスは、次のうちの 1 つに設定あるいは変更することができます。

Native first
要求は、SNA を介して経路指定されます。利用できる SNA 経路がない場合、要求は TCP/IP を介して経路指定されます。

Non-native
要求は、TCP/IP を介して経路指定されます。利用できる TCP/IP 経路がない場合、要求は SNA を介して経路指定されます。

Native only
要求は、SNA を介して経路指定されます。利用できる SNA 経路がない場合、接続は失敗します。

Non-native only
要求は、TCP/IP を介して経路指定されます。利用できる TCP/IP 経路がない場合、接続は失敗します。

AnyNet SNA over TCP/IP 構成の例

このセクションには、SNA over IP 通信を使用可能にする AnyNet の例が記載されています。次の構成手順は Windows オペレーティング・システムだけに使用できます。すべての例において、 SNA ドメイン・ネーム接尾部は SNA.IBM.COM になります。

このセクションで説明するその他のプラットフォーム (VTAM または iSeries など) における AnyNet の構成に関する詳細については、該当する資料を参照してください。

例 1: TCP/IP ネットワークを介した APPC または CPI-C アプリケーションの実行

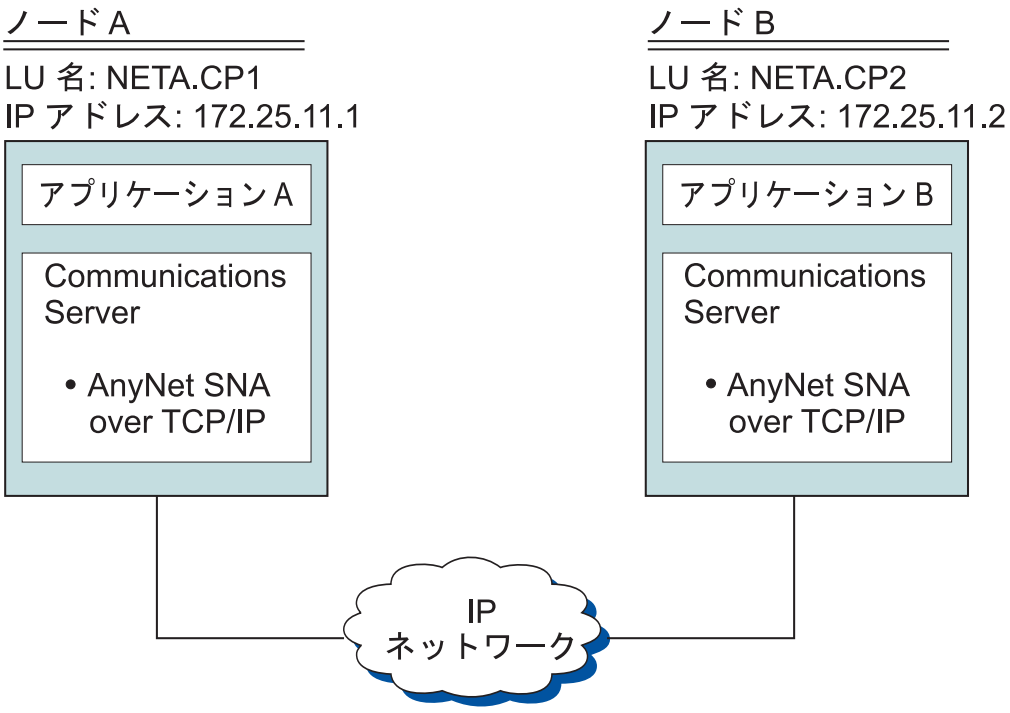

図 23. TCP/IP ネットワークを介した APPC または CPI-C アプリケーションの実行

ステップ: 2 つの Windows ノード間で通信を確立するには、次のステップに従ってください。この例では、CP 名は LU 名として使用されていることに注意してください。

ノード A については、次のようにします。

1. 次の項目をローカル・ホスト・ファイルに追加します。

   ```
   172.25.11.2 CP2.NETA.SNA.IBM.COM
   ```

2. ノード・セットアップ中は、**NETA.CP1** を制御点名として使用します。 経路指定プリファレンスは、TCP/IP を介してセッションを経路指定するように設定されていることを確認します。 詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

ノード B については、次のようにします。

1. 次の項目をローカル・ホスト・ファイルに追加します。

   ```
   172.25.11.1 CP1.NETA.SNA.IBM.COM
   ```

2. ノード・セットアップ中は、**NETA.CP2** を制御点名として使用します。 経路指定プリファレンスは、TCP/IP を介してセッションを経路指定するように設定されていることを確認します。 詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

例2: TCP/IP ネットワークを介する DLUR による 3270 エミュレーション

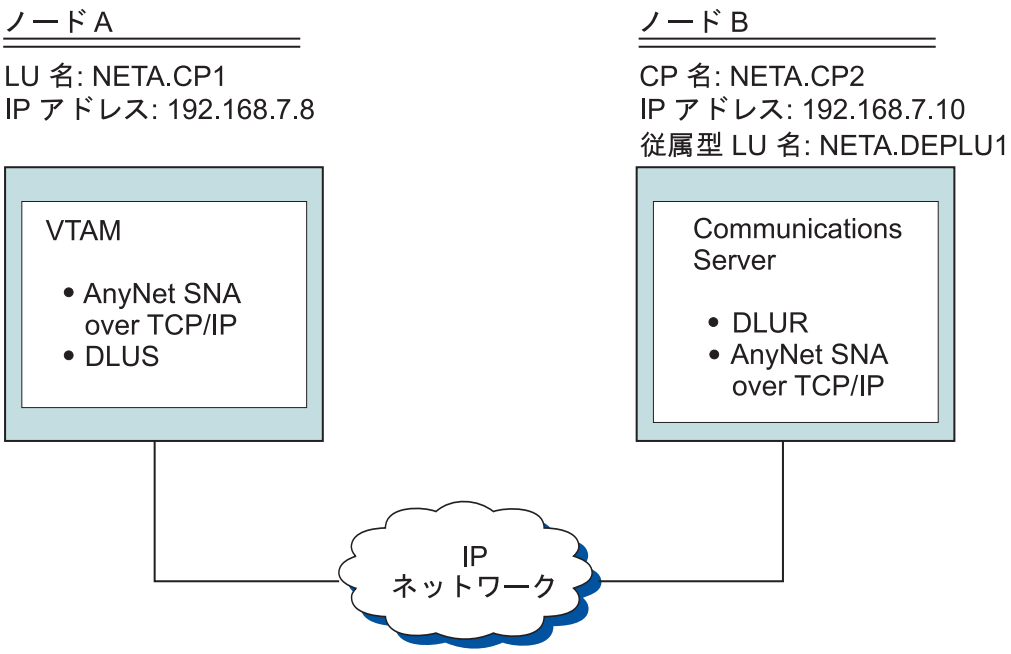

図 24. TCP/IP ネットワークを介する DLUR による 3270 エミュレーション

ステップ: ノード A とノード B 間で通信を確立するには、次のステップに従ってください。

ノード B については、次のようにします。

1. 次の項目をローカル・ホスト・ファイルに追加します。

   ```
   192.168.7.8 CP1.NETA.SNA.IBM.COM
   ```

2. ノード・セットアップ中は、**NETA.CP2** を制御点名として使用し、 DLUR PU を構成時は、**NETA.CP1** を DLUS 名として使用します。 経路指定プリファレンスは、TCP/IP を介してセッションを経路指定するように設定されていることを確認します。 詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

ノード A については、次の項目をホスト・ファイルに追加します。

```
192.168.7.10 CP2.NETA.SNA.IBM.COM
192.168.7.10 DEPLU1.NETA.SNA.IBM.COM
```

MVS™ AnyNet SNA over TCP/IP には、現在、従属 LU 通信のために DLUS/DLUR が必須であることに注意してください。

例 3: SNA と TCP/IP ネットワーク間で 3270 エミュレーションを使用可能にするための SNA ゲートウェイの使用

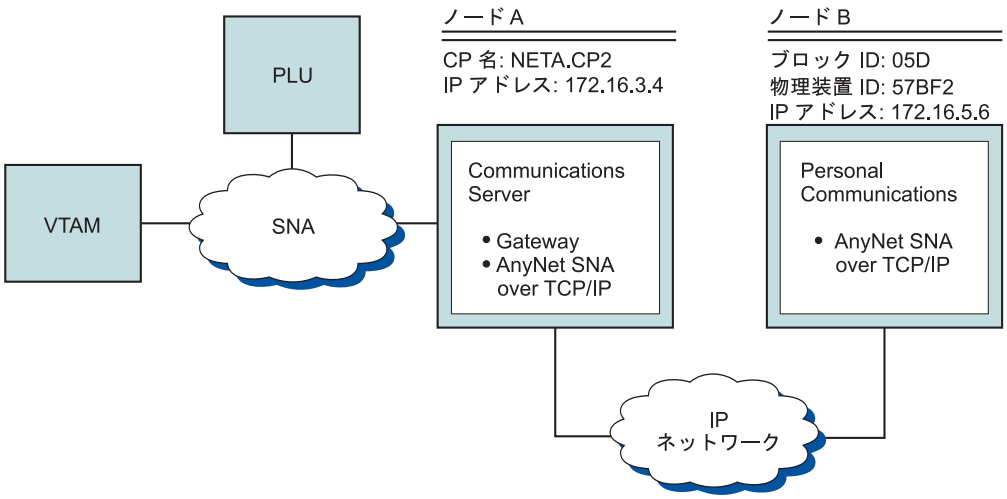

図 25. SNA と TCP/IP ネットワーク間で 3270 エミュレーションを使用可能にするための SNA ゲートウェイの使用

ステップ: ノード B と VTAM ホスト間で通信を確立するには、次のステップに従ってください。

ノード A については、次のようにします。

1. 次の項目をローカル・ホスト・ファイルに追加します。

   ```
   172.16.5.6 05D57BF2.SNA.IBM.COM
   ```

2. ノード・セットアップ中は、**NETA.CP2** を制御点名として使用し、クライアントの定義時は、暗黙テンプレートを割り当てるために ANYNET 装置を使用します。詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

ノード B には、次の項目を HOSTS ファイルに追加します。

```
172.16.3.4 CP2.NETA.SNA.IBM.COM
```

例 4: TCP/IP ネットワークを介する 3270 エミュレーションのための SNA ゲートウェイの使用

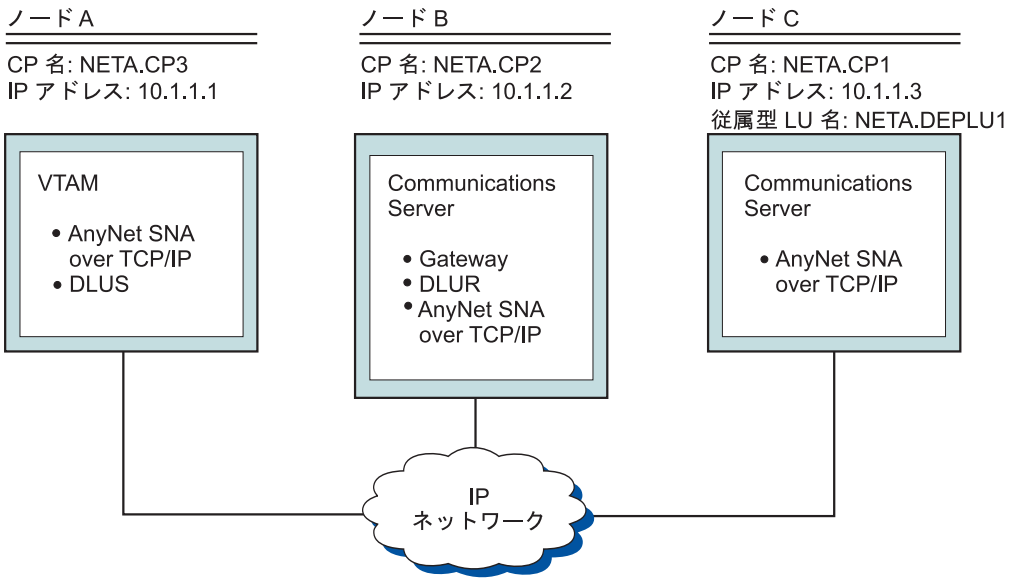

図 26. TCP/IP ネットワークを介する 3270 エミュレーションのための SNA ゲートウェイの使用

ステップ: ノード C とノード A 間で通信を確立するには、次のステップに従ってください。

ノード B については、次のようにします。

1. 次の項目をローカル・ホスト・ファイルに追加します。

   ```
   10.1.1.3 CP1.NETA.SNA.IBM.COM
   ```

2. ノード・セットアップでは制御点名に **NETA.CP2** を使用し、 ANYNET SNA over TCP/IP 接続定義の定義では隣接 CP 名に **NETA.CP1** を使用し、 DLUS をクライアント・テンプレートに割り当てるときは、DLUS 名に **NETA.CP3** を使用します。 NETA.CP3 の経路指定プリファレンスが「Non-native」に設定されていることを確認します。詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

ノード C については、次のようにします。

1. 次の項目をホスト・ファイルに追加します。

   ```
   10.1.1.2 CP2.NETA.SNA.IBM.COM
   ```

2. ノード・セットアップでは制御点名に **NETA.CP1** を使用し、 ANYNET SNA over TCP/IP 接続定義の定義では隣接 CP 名に **NETA.CP2** を使用します。詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

ノード A については、次の項目をホスト・ファイルに追加します。

```
10.1.1.2 CP2.NETA.SNA.IBM.COM
10.1.1.2 DEPLU1.NETA.SNA.IBM.COM
```

例 5: 別の IP ネットワーク上の 2 つの Windows ワークステーションからの 3270 エミュレーション

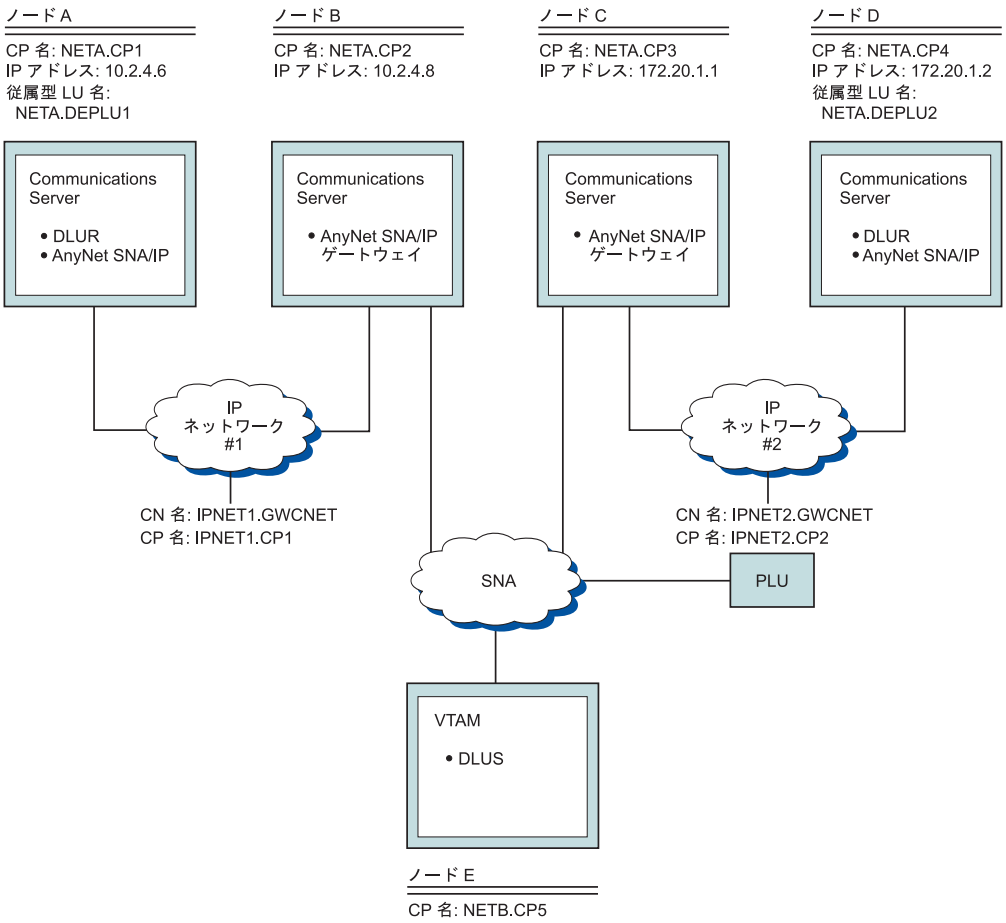

図 27. 別の IP ネットワーク上の 2 つの Windows ワークステーションからの 3270 エミュレーション

ステップ: ノード A と D からノード E へ通信を確立するには、次のステップに従ってください。

ノード A については、次のようにします。

1. 次の項目をローカル・ホスト・ファイルに追加します。

   ```
   10.2.4.8 CP5.NETB.SNA.IBM.COM
   127.0.0.4 IPNET1.GWCNET
   127.0.0.3 IPNET1.CP1
   ```

2. ノード・セットアップでは制御点名に **NETA.CP1** を使用し、 DLUS PU の構成では DLUS 名に **NETA.CP5** を使用します。 NETA.CP5 の経路指定プリファレンスが non-native に設定されていることを確認してください。詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

ノード B については、次の項目をホスト・ファイルに追加します。

```
10.2.4.6 CP1.NETA.SNA.IBM.COM
127.0.0.2 DEPLU1.NETA.SNA.IBM.COM
10.2.4.6 DEPLU1.NETA.SNA.IBM.COM
127.0.0.4 IPNET1.GWCNET
127.0.0.3 IPNET1.CP1
```

ノード C については、次の項目をホスト・ファイルに追加します。

```
172.20.1.2 CP4.NETC.SNA.IBM.COM
127.0.0.2 DEPLU2.NETC.SNA.IBM.COM
172.20.1.2 DEPLU2.NETC.SNA.IBM.COM
127.0.0.4 IPNET2.GWCNET
127.0.0.3 IPNET2.CP2
```

ノード D については、次のようにします。

1. 次の項目をホスト・ファイルに追加します。

   ```
   172.20.1.1 CP5.NETB.SNA.IBM.COM
   127.0.0.4 IPNET2.GWCNET
   127.0.0.3 IPNET2.CP2
   ```

2. ノード・セットアップでは制御点名に **NETA.CP4** を使用し、 DLUS PU の構成では DLUS 名に **NETA.CP5** を使用します。 NETA.CP5 の経路指定プリファレンスが non-native に設定されていることを確認してください。詳細については、「**SNA ノード構成**」ヘルプ・パネルを参照してください。

有効なヒント

このセクションでは、チューニング (SLIP または PPP 経由の TCP/IP の接続)、および動的な IP アドレスに関する有効なヒントを記載してあります。

チューニング: 複数の SNA over TCP/IP ゲートウェイを介して LU にアクセスすることができ、その LU 名を複数の IP アドレスにマップしてある場合、 AnyNet 基本パラメーターの構成時に **ANYNET_COMMOM_PARAMETERS** キーワードの **CONN_RETRY_SECS および CONNWAIT_SECS** パラメーターを増やします。これにより、すべての可能なアダプターおよびゲートウェイに対して、TCP 接続が試行されるようになります。 TCP 接続が非アクティブ IP アドレスに失敗するまでにはおよそ 90 秒かかります。

動的 IP アドレス: 一般的に、AnyNet SNA over TCP/IP を IP アドレスに静的にマップするには、SNA 資源 (例えば、LU 名、CP 名、idblk/num) に依存します。ただし、構成および接続の開始方法に応じて、IP アドレスが動的に割り当てられている環境 (例えば、DHCP) で、 AnyNet SNA over TCP/IP を使用することができます。

APPC または CPIC アプリケーション: 動的に割り当てられた IP アドレスを持つ SNA over TCP/IP アクセス・ノードは常に、静的な IP アドレスを持つ別の SNA over TCP/IP アクセス・ノードまたはゲートウェイに対してセッションを開始できます。

静的な IP アドレスを持つ SNA over TCP/IP アクセス・ノードまたはゲートウェイ (ノード A) が、動的な IP アドレスを持つパートナー (ノード B) に対してセッションを開始可能にする唯一の方法は、次のとおりです。

1. ノード B が最初にノード A に対してあるいはノード A を介してセッションを開始した。
2. ステップ 1 で開始されたセッションがまだアクティブである。

従属 LU アプリケーション:

注: このセクションの情報は、LU 0、1、2、3、または従属 6.2 アプリケーションに適用されます。

動的に割り当てられた IP アドレスを持つ SNA over TCP/IP アクセス・ノードは、次の基準が満たされていれば従属 LU 通信をサポートできます。

- 従属 LU 通信が、次のうちのいずれかを介して SNA ゲートウェイを通じて行われている。
  - APAR JR10461 が適用される Communications Server/2 4.1
  - Communications Server/2 V5
  - Communications Server for Windows 5.01 またはそれ以降
- 動的に割り当てられた IP アドレスを持つ SNA over TCP/IP アクセス・ノードが、静的な IP アドレスを持つ SNA ゲートウェイに対する接続を開始した。

DLUR ノードが IP アドレスを動的に割り当てている場合には、AnyNet SNA over TCP/IP を介し、 DLUS/DLUR を通じた従属 LU 通信はサポートされません。

第 4 章 クライアント/サーバー通信の計画

この章では、Communications Server 用の SNA API クライアントの計画について説明します。

SNA API クライアント

このセクションでは、SNA API クライアント特有の情報について説明します。

インストールおよび構成

Communications Server SNA API クライアントのインストールおよび構成に関する情報については、*「概説およびインストール」* を参照してください。

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) は、ディレクトリー・サービスにアクセスするための標準的な方法を提供します。 LDAP により、中央データベースまたは分散データベースから情報の読み取り、検索、追加、除去を行うことができます。 LDAP は、旧 X.500 ディレクトリー・アクセス・プロトコル (DAP) に似ていますが、OSI のセッション層およびプレゼンテーション層などのオーバーヘッドをなくしています。「**LDAP クライアント構成**」を使用して、SNA API クライアント情報を構成し、それを LDAP サーバーに格納することができます。

「**LDAP クライアント構成**」は、論理編成および、クライアントとクライアントの構成間の関係を示しています。

これらの大きな 3 つの区域の使用法については、「**LDAP クライアント構成**」のヘルプ・パネルを参照してください。

ディレクトリー情報ツリー

ディレクトリー情報ツリー (DIT) は、定義済みモデル内のすべてのディレクトリー・サービス・エージェント (DSA) を接続します。このモデルは、多数の基本オブジェクトからなる拡張可能な階層構造をしています。 基本的な LDAP DIT は、*countries* (c) が定義されている個所をルートとします。 countries の下は通常 *organizations* (o)、organization の下は *individuals* 、((cn) or (uid)) または *organizational units* (ou) です。例えば、完全に識別された LDAP 項目は次のように指定されることになります。

```
c=US, o=company.com, ou=Sales, cn=temp
```

クライアント階層

クライアント階層は、ユーザーがログインした LDAP DIT に関連を持っています。ユーザーまたは組織単位をクライアント階層に追加したり、ユーザーまたは組織単位をクライアント階層から削除したりすることができます。

構成階層

構成階層は、グラフィカル・ツリー・ビューを介してクライアント構成と、構成定義間のすべての関係を論理的に示します。 構成階層の使用により、ユーザーは定義を作成、変更、削除することができます。

Communications Server for Windows の共通 API クライアント

Communications Server とともに出荷されたクライアントを使用すると、クライアントはネットワーク内の IBM Communications Servers を見つけて、アクセスすることができます。

構成場所に関するオプションのインストール

クライアントのインストール中、ユーザーはクライアントの構成場所を選択することができます。次に示す 3 つの選択肢があります。

- INI ファイル構成。これは、前のバージョンの Communications Server が使用していた方式であり、 Communications Server に含まれている SNA API クライアントをインストールするときの、デフォルトの方式です。
- Lightweight Directory Access Protocol (LDAP)

構成場所には、サーバー・リスト、ユーザー名、その他のすべてのクライアント構成情報が含まれています。

構成場所

この情報は INI または LDAP のいずれかに保管できます。例えば、Communication Server の名前とアドレスは、API クライアントについて INI、または LDAP に保管できます。共通 SNA API クライアントの使用により、さまざまなサーバー・タイプを同じネットワーク上に簡単に統合できます。

構成ユーティリティー

インストール後のクライアントの構成場所 (INI または LDAP) を変更するには、「構成オプションの設定」ユーティリティーを使用します。

サーバーの位置決め

クライアントにより、ユーザーは TCP/IP トランスポート・プロトコルを使用して、 IBM Communications Server を見つけて、アクセスできます。

TCP/IP: TCP/IP トランスポート・プロトコルを使用してサーバーを見つける方式は同一です。ネットワーク管理者は、サーバー構成を通じてサーバーへのアクセスを制御できます。詳細については、 134 ページの『TCP/IP 有効範囲の計画』を参照してください。

デフォルトのローカル LU の割り当て

INI ファイル構成、または 32 ビットと 64 ビット Windows SNA API クライアント用の LDAP 構成のいずれかによって、デフォルトのローカル LU の別名を各ユーザーに割り当てることができます。

APPC プログラムは、直接指定する代わりにデフォルトのローカル LU の別名を使用できます。 APPC プログラムが、2 進ゼロまたはすべて ASCII のブランクに設

定されたローカル LU の別名フィールドを持つ TP_START verb を発行すると、APPC API は構成されたデフォルトのローカル LU の別名を使用します。

EHNAPPC プログラムは、直接指定する代わりにデフォルトのローカル LU の別名を使用できます。 iSeries 構成パネルのローカル LU フィールドが左方ブランクのときは、構成されたデフォルトのローカル LU の別名が使用されます。

CPI-C プログラムは、直接指定する代わりにデフォルトのローカル LU の別名を使用できます。 CPI-C 側のレコードのローカル LU の別名が左方ブランクで、APPCLLU 環境変数を使用して定義された値が何もないときは、 CPI-C API は会話を開始するときに、構成されたデフォルトのローカル LU の別名を使用します。

接続マネージャーが開始したプログラムは、直接指定する代わりにデフォルトのローカル LU の別名を使用できます。 接続マネージャー・レコードのローカル LU の別名が左方ブランクのときは、接続マネージャーは着信会話要求を処理するときに、構成されたデフォルトのローカル LU の別名を使用します。

デフォルトのパートナー LU の割り当て

INI ファイル構成、または 32 ビット Windows SNA API クライアント用の LDAP 構成のいずれかによって、デフォルトのパートナー LU の別名を各ユーザーに割り当てることができます。

APPC プログラムは、直接指定する代わりにデフォルトのパートナー LU の別名を使用できます。 APPC プログラムがパートナー LU の別名フィールドを持つ ALLOCATE verb を発行し、完全修飾パートナー LU フィールドが 2 進ゼロまたはすべて ASCII のブランクに設定されているときは、 APPC API は構成されたデフォルトのパートナー LU の別名を使用します。

CPI-C プログラムは、直接指定する代わりにデフォルトのパートナー LU の別名を使用できます。 CPI-C 側のレコードのパートナー LU の別名が左方ブランクのときは、 CPI-C API は変換を開始するときに、構成されたデフォルトのパートナー LU の別名を使用します。

デフォルトの LUA セッション名の割り当て

INI ファイル構成、または 32 ビット Windows SNA API クライアント用の LDAP 構成のいずれかによって、デフォルトのパートナー LU の別名を各ユーザーに割り当てることができます。

3270 エミュレーターのような LUA プログラムは、直接 LUA セッション名を指定せずに、デフォルトの LUA セッション名を使用することができます。 LUA プログラムが、 LUA LU 名フィールドが 2 進ゼロまたはすべて ASCII のブランクに設定されている、 RUI_INIT または SLI_OPEN verb を発行すると、RUI/SLI API は構成済みのデフォルト LUA セッション名を使用します。

クライアント/サーバーのデータ暗号化

クライアント/サーバーのデータ暗号化により、クライアントは、SNA API クライアントと Communications Server 間の通信で、アプリケーション・データのデータの暗号化を要求することができます。

データ暗号化は、オン、オフ、オプションがあります。オプションのデータ暗号化とは、サーバーが暗号化をサポートしている場合に、暗号化が使用されることを示しています。

クライアント/サーバーのセキュリティー

Communications Server を使用することにより、Windows の SNA API クライアントはユーザー ID とパスワードを再入力しなくても、 Windows ドメイン・セキュリティーを使用して、サーバーへのクライアント接続の権限を認証できます。この場合のクライアントは、 Communications Server ドメインに参加するかまたは同期したユーザー ID とパスワードでローカルにログインすることによって、 Windows ドメインの一部でなければなりません。

Windows ドメインの外側の SNA API クライアント・ユーザーは、ユーザー ID とパスワードを入力する必要があります。その場合、プロンプトによって行うか、またはクライアント構成ファイルにこれらの値を保管することによって行います。

クライアント・サーバーの許可ユーザーは、IBMCSAPI ローカル・グループ内に保持され、 Communications Server かまたは Communications Server が参加しているドメイン制御装置のいずれかに直接配置されます。このユーザー・グループは、インストール中に作成され、 Windows ユーザーのマネージャー・アプリケーションを使用して管理されます。

サーバーへの接続にユーザー ID とパスワードが必要かどうかは、サーバーの **LogonControl** 値項目の値で決めることができます。この値をゼロ (0) にすると、クライアントによるユーザー ID とパスワードの指定が不要になります。

サーバーへのクライアント接続に関する監査証跡レコードは、Windows イベント・ログに追跡記録されます。このレコードは、**アプリケーション**・ログ下の Windows イベント・ビューアーを使用して表示することができます。サーバーへのクライアント接続を記録したくない場合には、サーバーの **AuditTrail** 値項目をゼロ (0) に変更します。

次のキーのもとで、Windows レジストリー・エディターを使用して、**LogonControl** 値および **AuditTrail** 値項目にアクセスすることができます。

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/IBM SNA Client Services.
```

WTS

SNA API クライアントには **LUALIAS** 環境変数が組み込まれています。 **LUALIAS** はアプリケーションを WTS 環境に移行する場合に使用できます。

多くのクライアント・アプリケーションはハードコーディングされたローカル LU 別名を使用します。 WTS 環境への移行時には、このハードコーディングされたローカル LU 別名は、それぞれのユーザーごとに異なる LU 別名にマップする必要があります。例えば、user1 はローカル LU 別名 *x*、user2 は *y* にマップします。別の方法として、環境変数の **LUALIAS<TPsLUALIAS>** を構成することによりマップすることができます。

以下の方法により、WTS 環境における複数の LU 別名を構成します。

```
set LUALIAS<LocalLUAAlias>  = UserLUAlias
```

ここで: *LocalLUAlias* は構成ファイル (CPIC サイド情報) に構成される LU 別名、*UserLUAlias* は特定ユーザーに使用するために必要な LU 別名です。

注: 注: この環境変数はユーザー環境変数のもとで構成する必要があります。

トレースおよびロギング機能

IBM SNA API クライアント は問題判別のために、以下のトレースおよびロギング機能を提供します。

- 情報のロギング用の 2 つのメッセージ・ログ・ファイル (MsgLog.dat)
- デバッグ情報の収集のための複数のトレース・ファイル (複数の pcatrace.dat)

Infobundler はメッセージ・ログ・ファイルとすべてのデバッグ・トレース・ファイルの両方を収集できます。

第 5 章 HPR の計画

Communications Server は、Enterprise Extender (IPv4 および IPv6)、同期データ・リンク制御 (SDLC)、LAN、チャネル、マルチパス・チャネル (MPC)、および X.25 の各接続における高性能経路指定 (HPR) 接続をサポートします。

HPR の自動ネットワーク経路指定 (ANR) は、中間ノードの記憶域と処理の要件を最小化します。これは、エラー率の低い高速ネットワーク用のソリューションとして、 APPN 中間セッション経路指定 (ISR) よりも優れています。 HPR は代替パスへの無停止切り替えを可能にします。

Communications Server の HPR には、高速トランスポート・プロトコル (RTP)、自動ネットワーク経路指定 (ANR) のサポートが含まれています。

Communications Server はパラメーターを設定するための RTP_Tuning 構成を提供します。詳細については、*「構成ガイド」* を参照してください。

HPR リンク特性

上記にリストした利点を提供するために、HPR は、データ・リンクでフレーム損失率が低いことを前提としています。 HPR は、喪失フレームの原因となった状態からの回復を行いますが、その状態が長時間持続する場合には、ネットワーク輻輳が激しいために HPR スループットが低下したものと見なします。 リンク上で効率のよい HPR スループットを達成するには、送信ノード、2 つのノード間のリンクを構成する設備、および受信ノードの適切な構成が必要となります。

注: 回線設備上で頻繁にフレーム・ロスが発生する場合には、ERP 値を設定してください。

送信ノード

HPR とともに使用される一般的なアダプターは、低い障害率で回線上にフレームを送信します。イーサネットの場合に、多くの衝突によって LAN の負荷が重くなった場合 (例えば、負荷が通常のイーサネット速度に対して、およそ 30% から 40% より大きい場合など) には、HPR の動きが性能低下します。フレーム・リレーの場合、個々の接続がフレーム・リレー・ネットワークで輻輳 (ふくそう) 状態を引き起こすことなく、アクセス回線速度いっぱいに伝送できるように設備を構成しなければなりません。

回線設備

LAN および IP 設備には、実質的に見えない部分に複雑性が存在しています。それは、単一の LAN セグメントを共用する、非常に数多くのステーションから始まって、 LAN セグメント間のブリッジ (実質的には見えない低速リンクが存在する可能性) に至るまで、および複雑なサブネット上で作動するシミュレートされた LAN セグメントに至るまでの範囲に及びます。前提として、フレーム損失率が低くなければなりません。例えば、分割されたブリッジ間の WAN リンクは、エラー率が低い設備を使用するか、あるいは、ブリッジ間でリンク・レベルのエラー回復を使用してそれを補う必要が

あります。別の例として、ブリッジ・バッファーがオーバーランする状態 (ブロードキャスト・ストームや、ブロードキャスト・フレームのバースト) を防止しなければなりません。

受信ノード

HPR とともに使用される一般的なアダプターは、低い障害率で回線からフレームを受信します。ただし、連続したフレームがあまりにも速く到着する場合、中にはフレームを受信するのに失敗するアダプターもあります。受信側アダプターがインバウンド・フレームを欠落させずにそのトラフィックを処理できる場合、最高の HPR 効率を実現することができます。

ネットワークのエラー率が高い場合、システム管理担当者は、 HPR 接続上のスループットが期待したものより低くなるのに気付く場合があります。

HPR の考慮事項

HPR 機能は、フレーム・ヘッダーの中に追加情報を入れることにより実現されています。 HPR 機能が必要でない場合、この追加情報によるオーバーヘッドがネットワーク効率を低下させる場合があります。 中間ノードまたは代替経路がある場合には、HPR 機能は利点になります。ただし、リンク障害時に非介入回復を使用しない単一リンクによって接続されている 2 ノード間でハイパフォーマンスが必要な場合は、そのリンク構成時に HPR を使用不可にする必要があります。

しかし、EEDLC は常に HPR over TCP/IP を使用します。システムへの代替パスがある場合は、異なる宛先アドレス指定の別リンクを構成して、 HPR が代替パスへ無停止で切り替えることができるようにします。単一リンクがある場合は、リンクを再活動化を試みる前にリンク障害を検出する必要があります。パス・スイッチ・タイマーについては、 RTP 接続を無停止でリカバリーするためにリンク・タイムアウト時間より大きくする必要があります。

HPR は優先待ち行列を実装しています。 したがって、通常、対話型トラフィックは優先度の低いバッチ・トラフィックより速くネットワークを通過します。 フレームを待ち行列化するアダプターは、優先度に無関係に待ち行列化します。そのため、HPR の優先度待ち行列化に影響する場合があります。アダプターの待ち行列の大きさを減らして、低優先度のトラフィックが高優先度のトラフィックを遅延させないようにしなければならない場合があります (アダプターの待ち行列の大きさを設定するための手順については、アダプターの資料を参照してください)。 しかし、EEDLC は優先キューイングをインプリメントしません。

現在では、多くの PC で拡張電源管理 (Advanced power Management) 機能が採用され、キーボードまたはマウスが使用されていないときには (ディスク・ドライブなどの) 装置への電力供給を中断し、 CPU でのクロック速度を低下させて、消費電力を大幅に節約できるようになっています。これは、ワークステーションでは非常に優れた機能ですが、サーバー・プラットフォームでは、あるアダプターから別のアダプターにデータを経路指定しているときに (そしてまた、ディスク操作が行われていないときに) この機能が作動してしまう場合があります。 Communications Server の場合には、ブート中に (通常はハードウェアの初期化時に F1 を押して) BIOS 構成に入り、拡張電源管理およびハードウェア電源管理の両方のオプションを使用不可にしてください。 HPR は LAN アダプターをより多く使用するようになります。

パフォーマンスの向上および待ち行列化の増加に伴い、 HPR は従来以上に多くの LAN アダプター・メモリーを使用するようになります。多くの共用 RAM アダプターのデフォルト値は、8K バイトの共用 RAM を使用するようになっています。共用 RAM のサイズを 16K バイトにする必要があります。この構成を調整するためには、アダプター構成の資料を参照してください。この設定は、マシンの BIOS またはアダプターのスイッチ設定にあります。

注: 共用 RAM を 16K バイトに増加させないと、ネットワーク・パフォーマンスが低下します。

共用 RAM の値は 16K バイトよりも大きくしないでください。アダプター・メモリーの最適設定値は 16K バイトであるからです。

トラフィックが過重なために HPR リンクが失敗する場合には、受信タイマーの値を大きくすることができます。これにより、リンクは、送信フレームの肯定応答を受け取るためにより長い時間待つことができるようになります。

このタイマーは、SDLC リンクの場合には 1 次受信タイマー (Primary Receive Timer) です。受信タイマーは、DLC で設定することも、論理リンク・ステートメントで設定することもできます。

最小受信タイマー値を 10 分の 1 秒単位で計算するためには、次の式を使用してください。

```
[(send_window_count * max_i_field_size * 8) /actual line speed]* 10
```

LAN DLC でパラメーターを調整するための考慮事項

Communications Server が LAN リンクの障害と回復を行う速さを調整するために、8 つのパラメーターを使用することができます。低速リンク、HPR、またはバックアップ・ホスト接続を使用した場合に最善の結果が得られるように、これらのパラメーターを調整する必要が生じる場合があります。

SNA ノード で LAN 装置を定義するときは、以下のパラメーターについて考慮する必要があります。

Advanced タブの場合

テスト再試行間隔

テスト再試行間隔は、ローカル・エリア・ネットワーク (LAN) 上の隣接リンク・ステーションを見つけようとする試行と試行の間の時間を指定します。行われる試行回数は、テスト再試行限度に指定された値をベースにしています。

デフォルトの値は 8 です。

テスト再試行限度

テスト再試行限度は、ローカル・エリア・ネットワーク (LAN) 上の隣接リンク・ステーションを見つけようとする最大試行回数を指定します。この試行が行われるのは、テスト再試行間隔の値に設定された時間内に肯定応答を受信しない場合です。

デフォルトの値は 5 です。

最大 PIU サイズ

最大パス情報単位 (PIU) サイズは、このリンクの SNA セッションが使用するデータ・バッファーに含まれている最大バイト数です。最大 PIU サイズが、ローカル装置ドライバーがサポートしているフレーム・サイズを超える場合、値はそのフレーム・サイズに一致するするように縮小されます。

デフォルトの値は、65 535 です。

パフォーマンス・タブの場合:

アイドル・タイムアウト

アイドル・タイムアウトでは、LAN 装置ドライバーがフレームを受信しなかった時間数を経過すると、そのリンクが操作不能であると宣言するための、その時間数を指定します。

デフォルトの値は、30 秒です。

肯定応答遅延

肯定応答遅延では、ある時間数を指定して、その時間の間は受信フレームに対する応答を LAN 装置が抑止します。その目的は、同一の要求可能 (RR) を使用してより多くのフレームの受信と肯定応答を行えるようにします。

デフォルトの値は、100 ミリ秒です。

ポーリング応答タイムアウト

ポーリング応答タイムアウトは、ポーリング・ビット・セットで送信されたフレームに対する応答を LAN 装置が待機する時間を指定します。

デフォルトの値は、8 000 ミリ秒です。

予想される未処理の伝送数

予想される未処理の伝送数では、 LAN 装置がリンク・ステーションに待ち行列化する最大フレーム数を指定して、その数が待ち行列化されると、隣接リンク・ステーションに対して受信不可 (RNR) を送信します。

デフォルトの値は、16 フレームです。

受信バッファー・カウント

受信バッファー・カウントでは、受信データが処理可能になるまでホストから受信したデータを保持するために、メモリー内に予約されるバッファー数を指定します。各バッファーは、PIU のサイズになります。

デフォルトの値は、32 バッファーです。

HPR パス・スイッチ処理

HPR は、ある接続障害発生時に、別の接続に切り替える非中断のパス・スイッチを提供します。失敗した接続は、パス・スイッチを行う前に再試行されます。接続の失敗の判別に関係するパラメーター、およびパス・スイッチ開始までの時間については、以下に説明します。

アイドル・タイムアウトに指定した値に達すると、キープアライブ・フレームが送信されます。**アイドル・タイムアウト**のデフォルトは、30 秒です。

ポーリング応答タイムアウトに指定する値により、デバイスがキープアライブ・フレームに対する応答を待つ時間が決まります。**ポーリング応答タイムアウト** のデフ

ォルトは 8 秒 (8 000 ミリ秒) です。キープアライブ・フレームは 10 回の再試行を行います。この再試行カウントは変更できません。

キープアライブ・フレームに対して応答がない場合は、TEST コマンドがパートナー・システムに送信されます。**テスト再試行間隔**に指定する値により、TEST コマンド試行の間隔が決まり、**テスト再試行限界**に指定する値により、TEST コマンド試行の最大回数が決まります。**テスト再試行間隔**のデフォルトは、 8 秒間で、また、**テスト再試行限界**のデフォルトは 5 回の再試行です。

以下に示す計算は、接続が失敗したかどうか、およびパス・スイッチを開始するかどうかを判別するのに必要な時間を示します。

```
(Idle timeout) + (Poll response timeout * 10 retries) +
          (Test retry interval * Test retry limit) + 1
```

パラメーターにデフォルトを使用すると、接続失敗の判別およびパス・スイッチ開始に必要な時間は、 151 秒になります。

```
(30 seconds) + (8 seconds * 10 retries) +
          (8 seconds * 5 attempts) + 1 = 151 seconds
```

接続障害時に HPR を使用してパス・スイッチに長い時間がかかる (あるいは失敗する) 場合には、計算式の中のパラメーター値を小さくすることにより、この時間を短縮することができます。

EE (IPv4 または IPv6) DLC でパラメーターを調整するための考慮事項

EEDLC タイマーは HPR タイマーから独立しています。リンク障害検出タイマーはパス・スイッチを適切に機能させるために、エンドツーエンド RTP 接続タイムアウトより小さくしてください。また、「再活動化」フラグは異なるリンク障害検出の際に再試行するように、(デフォルトとして) 構成する必要があります。

IBM-EEDLC 装置構成では、以下のようにすべての再活動化フラグを検査する必要があります。

- 失敗した開始の試行後の再活動化
- リンク障害後の再活動化
- リモート端末が切断を送出した後の再活動化
- アプリケーションのリンク再活動化の試行の遅延
- 最大再活動化試行回数 (0-127): 0 (デフォルト)
- 再活動化遅延 (0-3600 秒): 30 (デフォルト)

その他の EEDLC 装置パラメーター:

接続タイマー
15 秒 (デフォルト)

接続再試行カウント
3 (デフォルト)

非活動状態タイマー
10 秒 (デフォルト)

再活動化の最大試行回数はゼロ (0) に設定すると、無限の再試行になります。この接続によるコスト増がある場合を除き、デフォルトをゼロ (0) にすることをお勧め

します。コスト増が発生するケースでは、この再活動化試行回数を使い切った後で、手動で接続を開始する必要があります。

再活動化遅延 のデフォルトは 30 秒に設定します。ただし、リンク障害発生後すぐに、リンクの活動化を再試行するように調整することも可能です。

接続タイマーは、TEST、XID、SABME、DISC などの制御コマンドに使用されます。**接続タイマー** は応答に対する待ち時間です。タイマーが応答を受信しないで満了すると、**接続再試行カウント**・パラメーターに定義された値に基づいて、コマンドが再送されます。

EE での HPR パス・スイッチ処理の例

信頼できるネットワークの場合、デフォルトのタイマーは特定の要件に基づいて変更できます。以下の値は単一リンクの場合の安定したネットワークでの推奨値です。

再活動化の最大試行回数
(0-127): 0 (デフォルト)

再活動化遅延
(0-3600 秒) 5 (変更する)

接続タイマー
10 秒 (変更する)

接続再試行カウント
2 (変更する)

非活動状態タイマー
10 秒 (デフォルト)

Path_Switch_Attempts
12 (ACG ファイルで RTP_TUNING verb を使用して変更する)

リンクに失敗が起こった場合、以下のように検出されます。

```
(connect_retry_count + !) * Inactivity_timer = 30 seconds here.
```

再活動化遅延後は、再接続が試みられます。再接続が正常に行われると、RTP 接続パス・スイッチの試行は新しいリンクで正常に経路指定されます。 **retry_count** および再活動化遅延を減らすことにより、リンクの障害は短時間に検出されるようになります。 **Path_Switch_Attempts** を増やすことにより、RTP 接続がパス・スイッチされるまでリンクを再活動化すると、遅延時間は小さくなります。

第 6 章 SNA ゲートウェイの計画

SNA ゲートウェイは次のものをサポートします。

- 各種の SNA プロトコル
- 各種のダウンストリーム・ワークステーション
- ゲートウェイとホスト間の各種リンク・タイプ (ホストでの DLUR から DLU までの使用を含む)
- ゲートウェイにおける LU (セッション) の共用 (プール)
- 暗黙ワークステーションの定義
- 非活動ワークステーションの定義の動的変更または追加
- 同時並行の複数のホスト
- ワークステーションとゲートウェイの間の各種のリンク・タイプ (組み合わせ可能なもの)

SNA ノード構成を使用して SNA ゲートウェイを構成する手順については、*「概説およびインストール」* を参照してください。

サポートされるワークステーションへの接続

SNA ゲートウェイは、次の接続形式で接続されたワークステーションをサポートします。

- LAN 接続
  - トークンリング
  - イーサネット
  - ATM (LAN エミュレーション)
- フレーム・リレー
- SDLC
  - 同期
- X.25 ネットワーク
- AnyNet TCP/IP (Microsoft TCP/IP サポート接続用)

SNA ゲートウェイは、定義されている PU ごとに最大 254 の LU をサポートすることができます。 ホスト接続ごとに異なる PU を定義することができます。 ダウンストリーム・ワークステーションがこの各 LU を使用して、ホスト接続を行います。サポートされるダウンストリーム・ワークステーション数は、接続タイプおよびゲートウェイ上のアダプター数などのいくつかの要因に依存します。 例えば、ゲートウェイ上に LAN アダプターが 1 つある場合は、 254 の LU を持つ 1 つのホスト・リンクを、253 のダウンストリーム・ワークステーションが並行して使用することができます。 2 つのアダプターを使用すると、ダウンストリーム・ワークステーション数を倍にすることができます。

SDLC ワークステーション接続

2 地点間構成および分岐接続構成において SDLC を使用した接続を選択できます。構成の完了後、ワークステーションとゲートウェイ間で SDLC を稼働するには、特別の考慮は不要です。

マルチドロップの 2 次ワークステーションを設定する場合、ポーリングのターンアラウンド・タイムを制御する様々な要因を考慮に入れてください。 1 次ワークステーションが、一番遠くにある 2 次ワークステーションをポーリングするのにかかる時間は、物理的制限に影響されます。 同じパラメーターを使用してすべての 2 次ワークステーションを定義すると、以下の計算を簡略化できます。

最少のワークステーション非活動時間を秒単位で計算するには、以下の式を使用します。

```
NS * (SW + RW) * (IS + 2) / (LS / 8)
```

ここで:

```
NS = Number of stations (ステーション数)
SW = Send window size  (送信ウィンドウ・サイズ)
RW = Receive window size (受信ウィンドウ・サイズ)
IS = I-field size (I フィールド・サイズ)
LS = Line speed (bps) (回線速度)
```

上記の値が、すべての 2 次ワークステーションで同じでない場合は、各グループまたはワークステーションごとに別々に計算し、それらを加算してワークステーション非活動タイマーに対して正確な値を計算する必要があります。例えば、14.4 Kbps の 16 台の 2 次ワークステーションを持つ分岐リンクで、各ワークステーションの送信ウィンドウ・サイズが 7、受信ウィンドウ・サイズが 7 および I フィールド・サイズが 521 の場合、非活動タイマーの計算は以下のようになります。

```
16 * (7 + 7) * (521 + 2) / (14400 / 8) = 65.1 seconds
```

注: バッファーとして、余分に数秒を加算してください。

X.25 ワークステーション接続

SNA ゲートウェイを構成し、ゲートウェイとワークステーション間に X.25 相手固定接続 (PVC) のみを使用する場合は、すべてのワークステーションおよびゲートウェイ PVC を、ネゴシエーション可能リンク・ステーションの役割を使用して構成することをお勧めします。ネゴシエーション可能リンク・ステーションの役割を持つワークステーションおよびゲートウェイ PVC を構成しない場合、ワークステーションはゲートウェイとの間に X.25 PVC リンクを確立できない場合があります。

PVC 接続および構成の詳細については、 145 ページの『第 12 章 X.25 の計画』を参照してください。

サポートされるホストへの接続

SNA ゲートウェイはホストとの次の接続をサポートします。

- LAN 接続
  - トークンリング
  - イーサネット

- SDLC
  - 同期
- X.25 ネットワーク
- AnyNet TCP/IP (Microsoft TCP/IP サポート接続用)
- DLUR 接続を使用する Enterprise Extender (Microsoft IPv4 または IPv6 サポート接続用)
- チャネル (CDLC)
- DLUR 接続を持つチャネル (MPC)

従属 LU トラフィックが使用するゲートウェイから複数ホストへの接続がある場合、制御点 PU 名を持ったホスト・リンクのみが以下を行うことができます。

- ホスト・フォーカル・ポイントとして働く。
- ホストとの CP-CP セッションを持つ。
- APPN 機能用に使用される。

制御点名と異なる PU 名で定義されたリンクは、ホストとの追加従属 LU 接続にのみ使用することができます。

ゲートウェイ・ホスト・リンクが限定資源リンクとして定義されている場合、最後の LU-LU セッションがアンバインドされたあとで、このリンクにより切断要求がホストへ送信されます。次に、ゲートウェイは、DACTLU をワークステーションに渡し、 DACTPU をホスト・リンクでしかセッションを持たないワークステーションに渡します。 ゲートウェイに接続しているワークステーションが限定資源として定義されている場合は、他のセッションが存在しない時には、ワークステーション・リンクは切断されます。 Communications Server では、明示的なクライアント接続を定義する際に、限定資源としてワークステーションを指定することができます。

ただし、このワークステーションに、ホスト・リンクを自動的に再活動化するアプリケーション (またはエミュレーター) がある場合は、このワークステーションがゲートウェイへのリンクを活動化するときに、ゲートウェイはホストへのゲートウェイ・リンクを再活動化します。 この意味は、ワークステーション定義が適切でないと、ゲートウェイで限定資源機能が働かないということを示します。

ホストの考慮事項

ホスト接続を計画する際は、以下のことを考慮に入れてください。

- お客様の環境でネットワーク制御点 (NCP)、37xx または Communication Controller for Linux® (CCL) NCPGEN を使用する場合、**LINE** マクロの **MAXLU** 値は、少なくとも Communications Server 上での LU 数より大きくなければなりません。
- VTAM ユーザーは、VTAM が制御装置に送り出す前に、データをバッファーに入れる時間間隔を制御することができます。 (コートテーリングと呼びます。) VTAM コートテーリング・パラメーター **DELAY = 0** が PU 定義のいずれかに指定されたときは、ホスト・プロセッサーの処理量は増えますが、ホスト送信応答時間は短くなります。

DELAY にゼロ以外の値を指定すると、ホスト・プロセッサーの命令数を節約しますが、その代わりに Communications Server ワークステーションの受信応答時間が長くなります。

コートテーリングに対して、デフォルト値 0.2 で開始してください。 0.2 秒の遅延では応答時間にそれほど影響がありませんが、トランザクションがおよそ毎秒 1 以上ある場合には、コートテーリングが発生します。

- LAN 上のダウンストリーム SNA ワークステーションはそれぞれ、それ自身の 1 セットの LU を持つ PU を実装していますが、SNA ゲートウェイは、ホストがゲートウェイ PU のみを認識するように実装されます。 したがって、ホストでは、1 つの PU の定義だけを行ないます。 この PU の定義には、LAN 上にある全 ステーション用 LU が含まれ、この LU はこのゲートウェイ経由でホストに接続します。

  ホスト VTAM が自己定義型従属 LU (SDDLU) をサポートする場合は、この機能の利点を活用しても構いません。ホスト LU の構成時は、LU モデル・タイプを指定するか、または、LU モデル名を指定します。この LU モデル・タイプまたは LU モデル名は、VTAM 交換回線大ノードで定義され、かつ VTAM SDDLU 出口ルーチンで使用される LUSEED オペランド値と一致する必要があります。

LAN 宛先アドレスの構成

サポートされる LAN 接続の 1 つを、ゲートウェイとホストの間、またはゲートウェイと明示定義済みワークステーションの間で使用する場合には、宛先アドレスを指定しなければなりません。各プロファイルに入力する正しい宛先アドレスを決める際には、両方のアドレス (ホストとワークステーション) は SNA ゲートウェイが宛先を知るためのものであるということを覚えておいてください。 図 28 は、このアドレスの関連性を示しています。

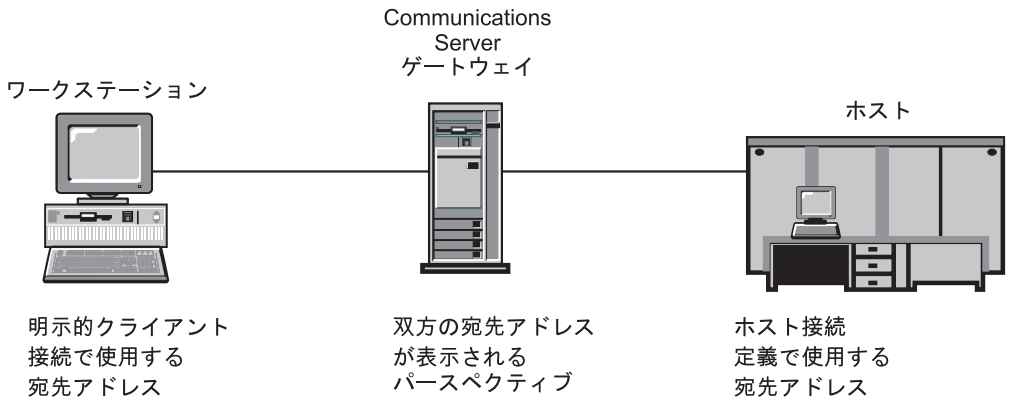

図 28. 宛先アドレス項目に使用するパースペクティブ

ゲートウェイ LU 定義の計画

SNA ゲートウェイは、*共用 (プール)* ホスト LU および*専用* ホスト LU の両方をサポートします。 SNA ゲートウェイでホスト接続ごとに LU が構成されると、それらの LU をグループ化して複数のプールに入れることができます。プールを作成することは、以下の場合に有益です。

- すべてのワークステーションのすべてのセッションが同時にホストと通信する必要がない場合、プール作成によりシステム資源を節約します。 LAN 上のワークステーション・セッションは同じ LU を共用することができますが、同時に共用できません。この機能により、ホストとゲートウェイ間に構成された LU 数より大きい数の LU を、ワークステーション・セッション用に SNA ゲートウェイで構成可能です。こうすると、ホスト資源の必要量とホスト・ワークステーション定義が削減され、再始動の速度が上がります。
- プールを使用すると、LU の管理と構成が容易になります。プールに対する LU の追加または削除により他の定義に影響を与えずに、プールのサイズを調整できます。

  共用 (プール) LU は、どの特定ワークステーションに対しても専用ではありませんし、ダウンストリーム・ゲートウェイ・ユーザー専用にする必要もありません。 SNA API クライアントおよびローカル・エミュレーター・セッションと同様、ダウンストリーム TN3270 ユーザーおよび SNA ゲートウェイ・ワークステーションは、単一のプールを共用することができます。 すべての従属 LU 使用に対して 1 つのプール (PUBLIC など) を構成したい場合は、これらのタイプ全体に渡ってそのユーザーを分散させる方法を知る必要はありません。
- プールを使用すると、同一プールの中で複数接続からの LU を定義する場合に、ダウンストリーム・ワークステーションに対して LU の使用可能性を向上することができます。各接続の中のある接続がアクティブで、他の接続が非アクティブである場合は、ユーザーは、アクティブ・リンク上の LU にアクセスできます。

以下のシナリオを考えてみましょう。

- Communications Server は、100 の LU があって、それぞれの接続について定義がされていて、すべてプール A に属している、ホスト接続を 2 つ持っています。 1 番目のリンクは、*始動時に活動化 (activate at startup)* するように構成されており、作動可能です。すべてのワークステーションは、1 番目のリンクとその LU を使用します。 2 番目のリンクは、*自動活動化 (auto-activate)* するものとして構成されています。 プールとリンク構成のこの組み合わせは、2 つの方法で優れた使用可能性を提供できます。 1 番目のリンクが失敗すると、回復用の従属セッションは自動的に 2 番目のリンクを活動化します。 1 番目のリンクが自分の持つ LU を使い果たしてしまうと、次の LU 要求 (101 番目の) が発生した時には、バックアップ・リンクが自動的に活動化されます。
- また、プールとリンク構成の組み合わせを使用して、使用可能なホスト接続全体に渡ってダウンストリーム・ワークステーションに対するロード・バランシングを実現できます。この例としては、Communications Server が、各接続上で定義した 100 LU (すべての LU がプール A に所属) との 2 ホスト接続を保有する場合です。両方のリンク共に、*始動時に活動化* するように構成されており、かつ作動可能です。 LU のプールにマップされているワークステーションは、両方の接続全体に渡って負荷が分散されて、両方の接続の間でその負荷を共用します。

ダウンストリーム・ワークステーションがゲートウェイに接続されると、SNA ゲートウェイは、プールされた LU をワークステーション・セッションに割り当てます。異なるホスト上で、専用 LU または共用 (プール) LU のいずれでも使用できるように、ワークステーション・セッションを定義することができます。

専用 LU はプールに属しません。専用 LU を明示的に定義されたクライアントが使用するように構成することができます。

図 29 は、専用 LU、共用 (プール) LU、あるいはその両方の LU を使用するワークステーションの場合の単純構成を記載してあります。 (結合線が LU を表します。)

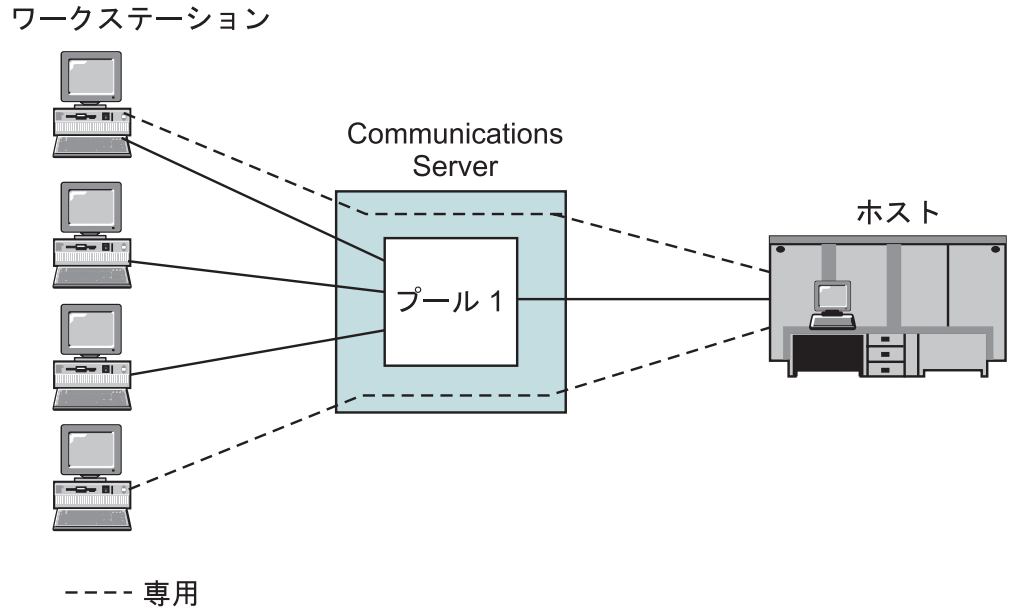

図 29. 共用 (プール) LU および専用 LU を使用する簡易シナリオ

明示接続および暗黙接続の使用

ゲートウェイをサポートするダウンストリーム・ワークステーションには、明示と暗黙の 2 つのタイプがあります。明示ワークステーションは、特定の DLC タイプ (例えば、イーサネット・ネットワークと SDLC) を介する宛先アドレスが定義されているワークステーションです。明示ワークステーションを構成するには、各ワークステーションの宛先アドレスか、完全修飾隣接制御点名または隣接ノード ID をお客様が知っている必要があります。そして、さらに各ワークステーション用にゲートウェイへの論理リンクを定義する必要があります。明示ワークステーション用に定義されている LU は、プール LU または専用 LU です。

暗黙ワークステーションは、構成がより容易ですが、共用 (プール) LU しか使用できません。ゲートウェイを用いる各ワークステーションとのリンクを定義する代わりに、ホスト LU プール (複数の場合もある) を定義し、ワークステーション接続が使用する装置 (DLC) を構成します。ゲートウェイに接続し、かつ、明示定義と一致しないワークステーションごとに、LU 定義用モデルとして使用する暗黙クライアント・テンプレートを構成します。例えば、イーサネット LAN にある各ワーク

ステーションに、 NAU アドレス 2 および 3 で 2 つの 3270 セッションが構成されている場合は、 2 つの LU (1 つは アドレス 2、もう 1 つは アドレス 3 用) を指定したクライアント・テンプレートを構成します。両方のアドレスが 1 つのホストへのセッションに使用されている場合は、両方のアドレスを同じホスト・プールへマップしてください。そうではなく、アドレス 2 が HOST_A への接続に使用され、アドレス 3 が HOST_B への接続に使用されている場合は、各アドレスを適切なホスト・プールへマップしてください。この例では、明示定義と一致しないワークステーションがイーサネットを介してゲートウェイへ接続するごとに、リンクが動的に作成され、 NAU 2 および 3 の 2 つの LU がホスト LU プール (複数の場合もある) から割り振られます。

暗黙ワークステーションの場合、ゲートウェイに接続するユーザーは、その暗黙ワークステーション用に構成されているゲートウェイ DLC のアダプター・アドレスと、ゲートウェイで定義されている NAU 値だけを知っていれば十分です。 これらユーザーでは、3270 セッションと論理プリンターの定義時にこれらの NAU 値を使用する必要があります。

Communications Server に接続しているダウンストリーム・パーソナル・コミュニケーションズ・ワークステーションは、 LAN ディスカバリーを使用して、グループ名 `IGO2HOST` を検索し、アダプター・アドレスを検索することができます。

SNA ゲートウェイ・パフォーマンス

ゲートウェイを介するパフォーマンスは、次のような多数の要因によって異なります。

- ゲートウェイの構成
- ホスト (複数の場合もある) との接続
- 各ホストに課せられる全体としての処理量
- サポートされるワークステーションとの接続
- サポートされるワークステーションの構成
- サポートされるワークステーションの数
- 各ワークステーションとのセッションの数
- SNA 伝送優先順位
- フロー制御
- 全セッションの「ペーシング」ウィンドウ
- 非ゲートウェイ・セッションのトラフィック

他の機能に対してソフトウェア・ゲートウェイを実装するワークステーションを使用すると、ゲートウェイのパフォーマンスも損なわれる場合があります。

上記のいずれの要因もパフォーマンスに悪影響を与えていない場合は、サポートされる SNA プロトコルを使用する個別ワークステーションでは、ホストとの直接接続の場合と、ホストに接続された SNA ゲートウェイを介する LAN 経由の間接接続のパフォーマンス上の差異は、わずかとなるはずです。 実際に、ホスト・リンクがゲートウェイで活動状態の場合は、ホストのオーバーヘッドによる遅延を除去することによって、ワークステーションの活動化パフォーマンスが改善される可能性

があります。しかし、多くの可変要因が関与するため、機能とパフォーマンスの望ましいバランスを得るためには、本格稼働環境でパフォーマンス・テストを行う必要があります。

DLUR の考慮事項

ホストへの接続に DLUR を使用すると、 SNA ゲートウェイを配置できる位置での柔軟性が高まります。 任意の APPN ネットワークを縦断してホストへの接続を行うことができ、 HOST/NCP に隣接していることに制限されません。 DLUS パイプへの DLUR が、DLUS VTAM に対して作成されて、従属セッションの制御フローに使用されます。

ホストへの DLUR 接続用に推奨される構成は、ゲートウェイをネットワーク・ノードとして定義し DLUS 情報を構成することです。明示クライアントおよび暗黙クライアントの構成時に、これらを DLUS へマップしてください。この構成が最も簡単です。その理由は、この構成を使用すると、ゲートウェイのダウンストリーム LU の知識を必要とせず、 VTAM がこの PU を認識するのでダウンストリーム装置の高度な可視性を VTAM に提供するからです。

VTAM がダウンストリーム PU を認識するようにしたくない場合は、ゲートウェイで (ホスト接続ではなく) 内部 PU を構成し、ダウンストリーム・ワークステーションをその内部 PU へマップすることができます。

パーソナル・コミュニケーションズなどのダウンストリーム・ワークステーションが DLUR 対応の場合、SNA ゲートウェイ機能ではなくネットワーク・ノード機能を使用して、ワークステーションに Communications Server 内を経路指定させる場合もあります。

第 7 章 TN3270E サーバーの計画

TN3270E サーバー機能で、 110 ページの図 30、または 111 ページの図 31 のようにネットワークを構成することができます。

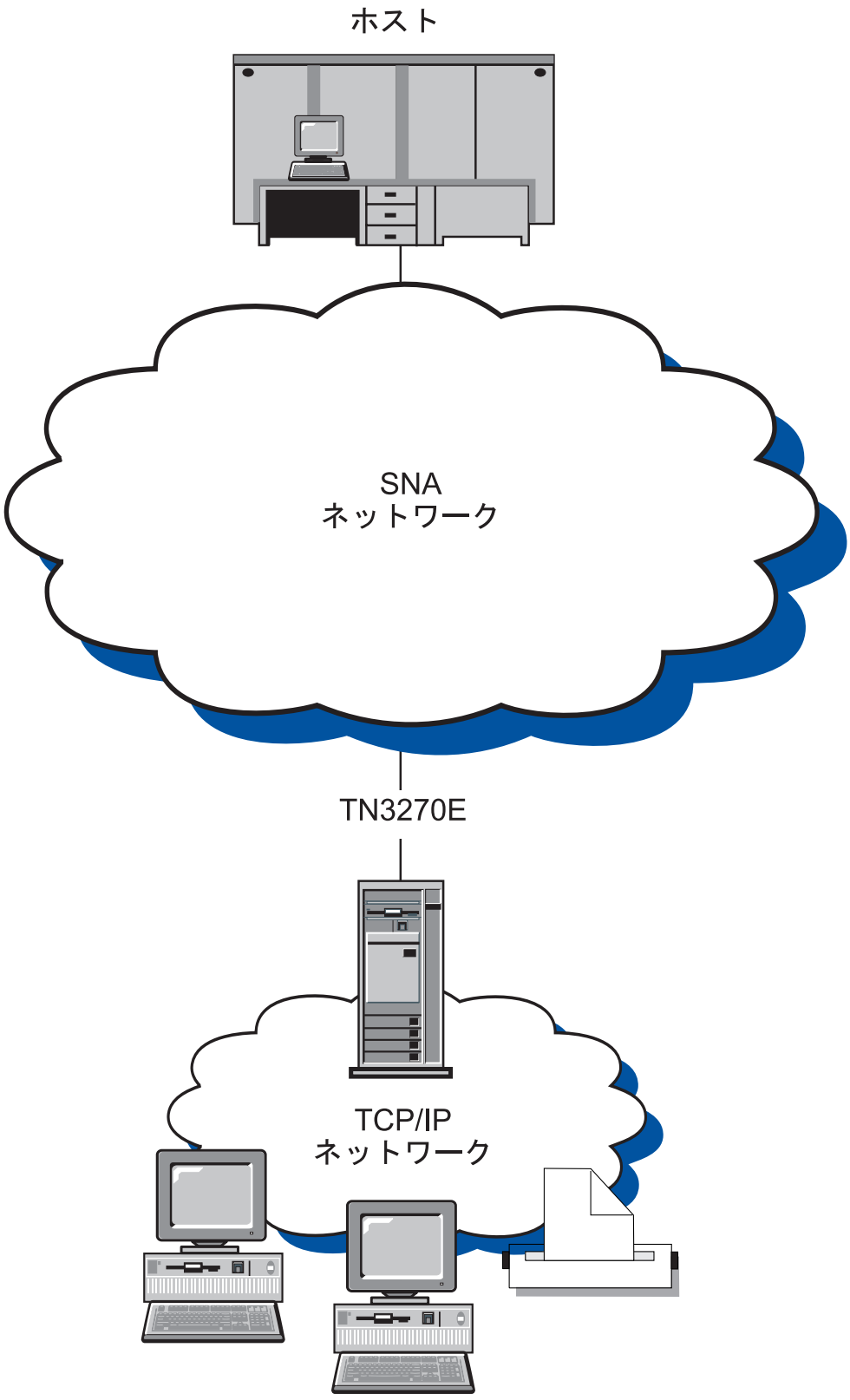

図 30. ワイド・エリア SNA ネットワークの TN3270E サーバーとして構成された Communications Server

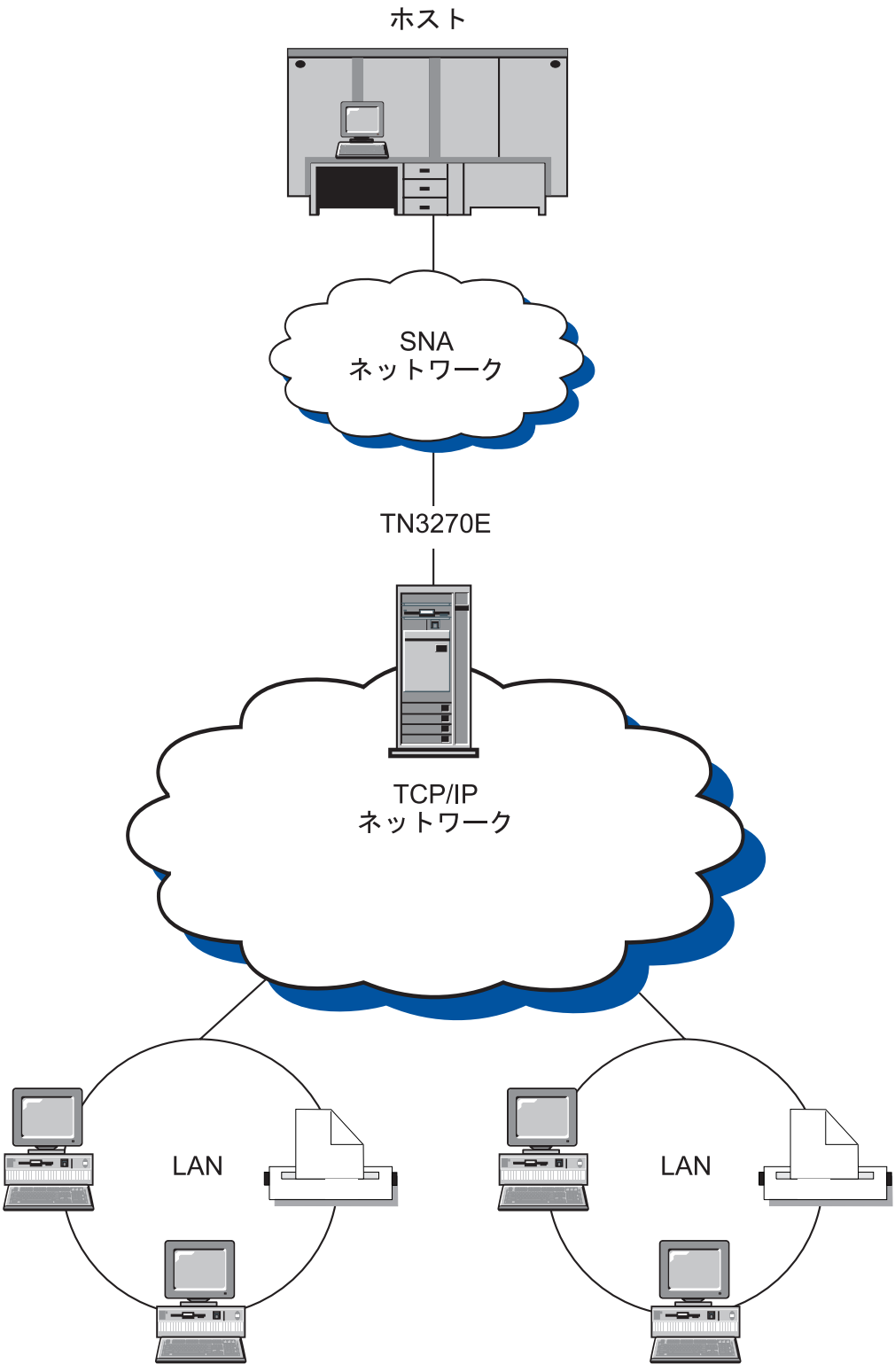

図 31. ワイド・エリア TCP/IP ネットワークの TN3270E サーバーとして構成された Communications Server

TN3270E サーバーの機能は、以下をサポートします。

- 複数のポート

TN3270E サーバーによって、構成するポートごとに、プール名、セキュリティー、クライアント認証、セキュリティーのレベル、証明書取り消しリスト (CRL) サポートを指定して複数のポートを構成することができます。

- LU エミュレーション

  TN3270E サーバーは LU 2 をサポートします。これにより、ユーザーは、対話型 3270 ディスプレイ・アプリケーション・プログラムを実行することができます。

- ホスト印刷

  Telnet 3270 標準拡張版 (TN3270E) を使用すると、ワークステーションに接続されたプリンターに、ホスト・アプリケーションから印刷させることができます。このプリンターは、ローカル接続でもネットワーク接続でもかまいません。 LU 1 および LU 3 セッションがサポートされます。 TN3270E サーバーには、RFC 1646 および RFC 1647 に記述されているプロトコルが実装されています。このプロトコルによって、サーバーは、TN3270E が使用可能なクライアントに LU 1 および LU 3 セッション・データを渡し、印刷要求に対するクライアントの確認を待ち、ホストに応答することができます。

- IP フィルター

  Communications Server は、IP アドレス、サブネットワーク、ホスト名、またはドメイン・ネームを使用する TCP/IP クライアント・フィルターの指定をサポートします。この機能を使用すると、TN3270E サーバーへの接続を許可されたクライアントを中央から管理すること、および各クライアントがアクセス可能な LU 名とプールを指定することに対応できます。

- 応答処理

  TN3270E 対応のクライアントは、肯定応答および否定応答の両方を送信することができます。この応答は、TN3270E サーバーがホストに送信するものです。 TN3270E サーバーは、標準 TN3270 クライアントに対して応答要求を生成します。

- ATTN および SYSREQ キー操作

  クライアントが ATTN キーまたは SYSREQ キーを送信する際、TN3270E サーバーで情報を変換し、ホストに転送することができます。 TN3270E に対応していないクライアントには、ATTN および SYSREQ に対して明示的な定義がありませんが、 TN3270E サーバーで、以下の Telnet コマンドを使用して、これらの機能を実装します。

表 6. 同等コマンド

Telnet	**TN3270E**	**標準 TN3270**
IP	ATTN	SYSREQ
AO	SYSREQ	SYSREQ
BREAK	N/A	ATTN

- LU クラス

  Communications Server では、LU クラスでユーザー接続を分類しています。この各クラスは、共通の特性を指定して構成された LU (例えば、特定のホスト接続を

必要とする LU) からなります。これによりユーザー・アクセスの単純化、必要なアプリケーション別のユーザーのグループ化、およびホスト資源の使用効率の最大化を行います。

- Secure Sockets Layer ベース (SSL ベース) 機密保護

  TN3270E サーバーのポートが保護されていることを指定して、そのポートの接続に SSL バージョン 3 を使用し、データ暗号化とデジタル証明書を使用した認証を提供することができます。ポートの接続に対するセキュリティーのレベルを指定するために、追加の構成パラメーターがサポートされています。この構成パラメーターによって、クライアント認証を処理するかどうかや、クライアント接続を受け入れる前に証明書取り消しリスト (CRL) を検査するかどうかを指定することができます。

TN3270E サーバーの構成手順についての詳細は、*「概説およびインストール」* を参照してください。

TN3270E サーバーでサポートされるクライアント・ワークステーション

TN3270E サーバーは、RFC 1576、1646、1647 および 2355 に完全に準拠しているすべての TN3270E クライアントおよび TN3270 クライアントをサポートしています。

ハイライト

このセクションには、TN3270E サーバーに対して構成することができるいくつかの機能の詳細が記載されています。

デフォルト・ポート番号の変更

「**TN3270E ポート**」構成パネルから、新規接続のためにサーバーが使用するポートを構成できます。デフォルト・ポート番号は 23 ですが、TN5250 サーバー・サポートなどの他の Telnet アプリケーションも、このポートを使用します。他の Telnet アプリケーションがポート 23 を使用している場合は、他のポートを使用しなければなりません。

ポート番号を変更する場合、他のアプリケーションで使用していることがわかっている番号は使用しないようにします。 2 つのアプリケーションが同じポート番号を使用すると、一方のアプリケーションが障害を起こします。

ポート番号を変更する場合、1 024 以上の数を使用してください。 1 024 より小さい数値は予約済みです。 予約済みポート番号についての詳細は、以下のインターネット・ロケーションを参照してください。

http://www.ietf.org/

ポート番号を変更する場合、エミュレーター・アプリケーションとポート番号が一致するように構成しなければならないため、 TN3270E クライアント・ユーザーに通知しなければなりません。

システム管理用トラフィック

未使用の接続を切断する頻度を制御するには、キープアライブ処理、自動ログオフおよび LU テークオーバー処理の 3 つの方法があります。

デフォルトでは、TN3270E サーバーはキープアライブ処理を使用しません。キープアライブ処理を使用する場合、NOP または タイミング・マークのいずれかを選択することができます。

- NOP 処理を使用すると、指定されたキープアライブ間隔の後、Telnet NOP コマンドが送信されます。これにより、データを接続上に伝送させ、TCP/IP に接続の切断を検出させます。サーバーは、クライアントからの応答を必要としません。TCP/IP に接続の故障率を検出させるにはかなりの時間がかかります。
- タイミング・マーク処理を使用すると、Telnet タイミング・マーク・コマンドがクライアントに送信されます。指定された時間内にクライアントが応答しない場合、接続はクローズされます。

タイミング・マーク処理では、NOP 処理よりシステム・トラフィックが増加しますが、未使用の接続は早く解放されます。

自動ログオフを選択すると、サーバーは、指定した期間にトラフィックがないセッションを切断します。 キープアライブ処理によるトラフィックでは、その接続をオープン状態のままに維持できないため、ホストとの間でデータを送受信しなければなりません。プリンター・セッションは、自動的にはログオフされません。

キープアライブ処理を行うようにクライアント・エミュレーターが構成されている場合でも、サーバー側でその処理をオフにしても構いません。また、キープアライブ処理をサーバーで実行する場合でも、ネットワーク・トラフィックを削減するためにクライアント側でその処理をオフにしても構いません。

LU テークオーバー処理を選択した場合は、そのサーバーは、特定の条件が満たされた場合にセッションを切断します。例えば、新しい TN3270E セッション要求で、サーバーで使用状態にある LU を指定すると、 TN3270E サーバーは、その接続のクライアントにタイミング・マークを送信します。指定した時間内にクライアントがタイミング・マークに応答しない場合は、サーバーはセッションを切断し、LU を新しい接続要求に割り当てます。 LU テークオーバー処理によって、キープアライブ検出のためのネットワーク・トラフィックを発生させずに、セッションが必要とされる場合に未使用のセッションを切断することができます。キープアライブ検出では、使用されていない接続をより頻繁に解放することができますが、ネットワーク・トラフィックが多くなります。

IP フィルター処理

Communications Server により、どの TCP/IP クライアントがサーバーに接続できるかを指定するために、 TN3270E フィルターを構成することができます。 個人 IP アドレス、IP サブネットワーク、または TCP/IP ホスト名 (ドメイン・ネーム) を使用して、クライアントを指定することができます。

Secure Sockets Layer (SSL) サポート

新規の TN3270E サーバー・ポートを構成する場合、ポートを保護接続用に使用する指定をすることができます。 保護用に複数のポートを指定できます。

機密保護を使用可能にするために、Communications Server は「**鍵管理**」ユーティリティーを提供して、SSL が要求する証明書およびキーを生成します。 詳細については、123 ページの『第 9 章 Secure Sockets Layer ベース・セキュリティーの計画』を参照してください。

構成が完了し機密保護が使用可能になると、SSL バージョン 3 をサポートする TN3270E クライアントは、保護ポート番号に接続し、保護接続を確立します。

SNA 接続の構成

TN3270E サーバー機能を使用する前に、ホスト接続およびホスト LU を構成する必要があります。ホスト・パラメーターを記述して説明する表については、*「概説およびインストレーション」* を参照してください。

プーリング

TN3270E サーバーに特有の LU 定義には、暗黙ワークステーション、明示ワークステーション、暗黙プリンター、および明示プリンターの 4 つのクラスがあります。これらのクラスは、RFC 1647 で規定されている端末総称クラス、端末特定クラス、プリンター総称クラス、プリンター特定クラスに対応します。

暗黙ワークステーション 定義は、接続要求を満足させるのに TN3270E サーバーが使用するプールの中に定義します。デフォルトのワークステーション・プールを構成して、クライアントがワークステーション LU またはワークステーション・プール名を指定しない場合の要求を満たすことができます。その他のすべてのワークステーション・プールは、名前を指定して要求しなければなりません。

特定 LU 名の要求を満たすのに使用される LU 定義のセットを定義することもできます。 これらの*明示ワークステーション* 定義によって、ホスト・アプリケーションが必要とする端末装置を、それを特定して要求しないクライアントには割り当てないことが保証されます。

同様に、特定の LU 名を必要としない接続の要求を満たすのに使用されるプリンター定義のプール (*暗黙プリンター*)、および特定の LU 名の要求を満たすのに使用される定義のセット (*明示プリンター*) を定義することができます。 デフォルトのプリンター・プールを、クライアントがプリンター LU またはプリンター・プール名を指定しない要求を満たすために構成することができます。 その他のすべてのプリンター・プールは、名前を指定して要求しなければなりません。

暗黙および明示ワークステーションの定義で、それぞれに関連プリンターをもたせることができます。端末定義ごとに割り当てられたプリンターをもたせることができ、プリンターごとに関連した端末定義をもたせることができます。これらのプリンターは、明示、または暗黙プリンターの定義には含まれていません。

関連プリンター の定義は、端末 LU 名を参照することによってしかアクセスすることができません。 これらの定義で、クライアント・ユーザーが必要とする情報量が減少されます。その理由は、ユーザーは、端末セッションおよびプリンター・セッションへ接続するには、その端末 LU 名を知っているだけで済むからです。

TN3270E サーバーのロード・バランシング

Communications Server は、複数の TN3270E サーバーに渡って、 TN3270 クライアントのロード・バランシングもサポートします。詳細については、 133 ページの『第 10 章 ロード・バランシングの計画』を参照してください。

第 8 章 TN5250 サーバーの計画

TN5250 サーバー機能で、 118 ページの図 32、または 119 ページの図 33 のようにネットワークを構成することができます。

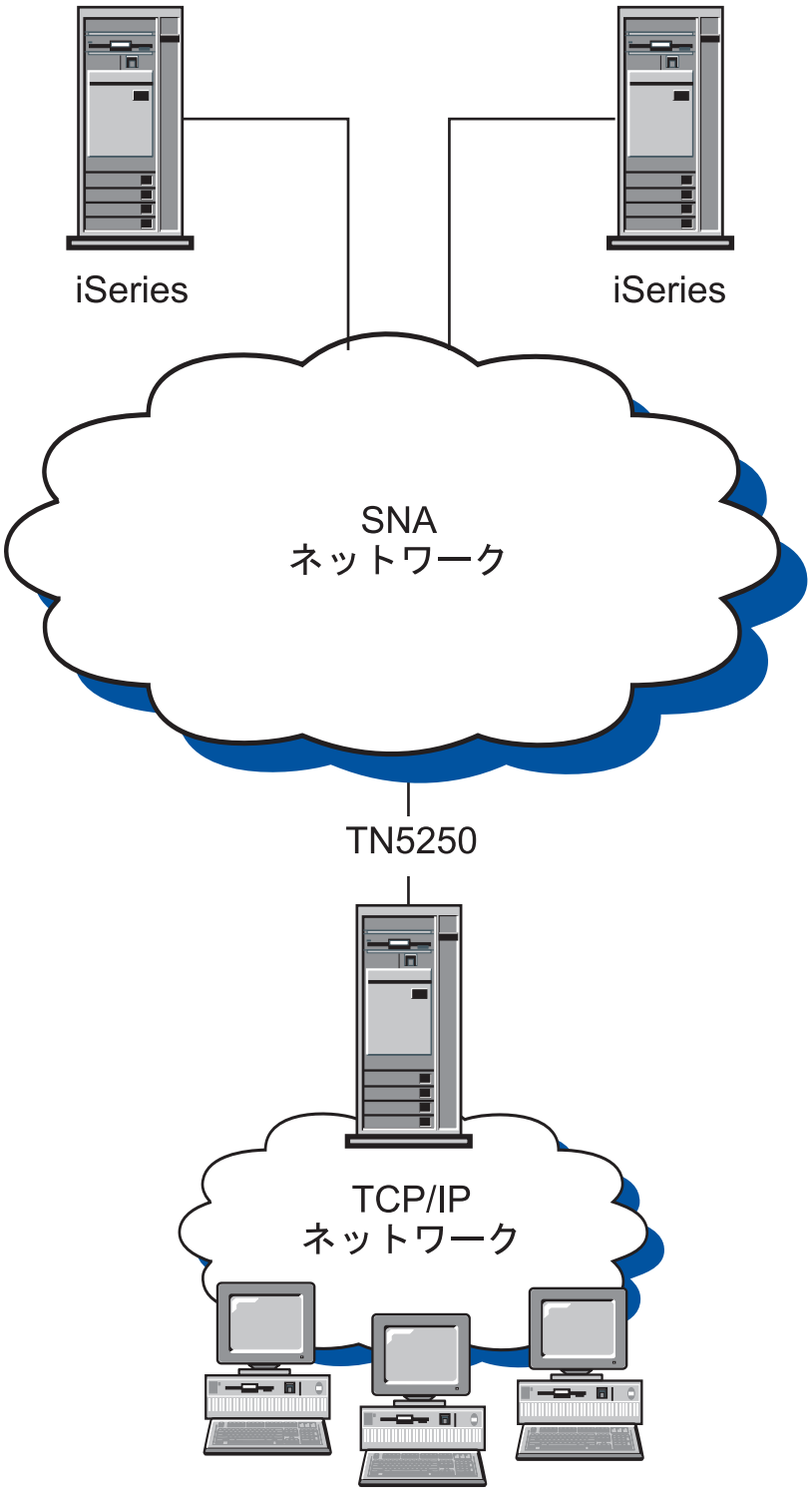

図 32. ワイド・エリア SNA ネットワークの TN5250 サーバーとして構成された Communications Server

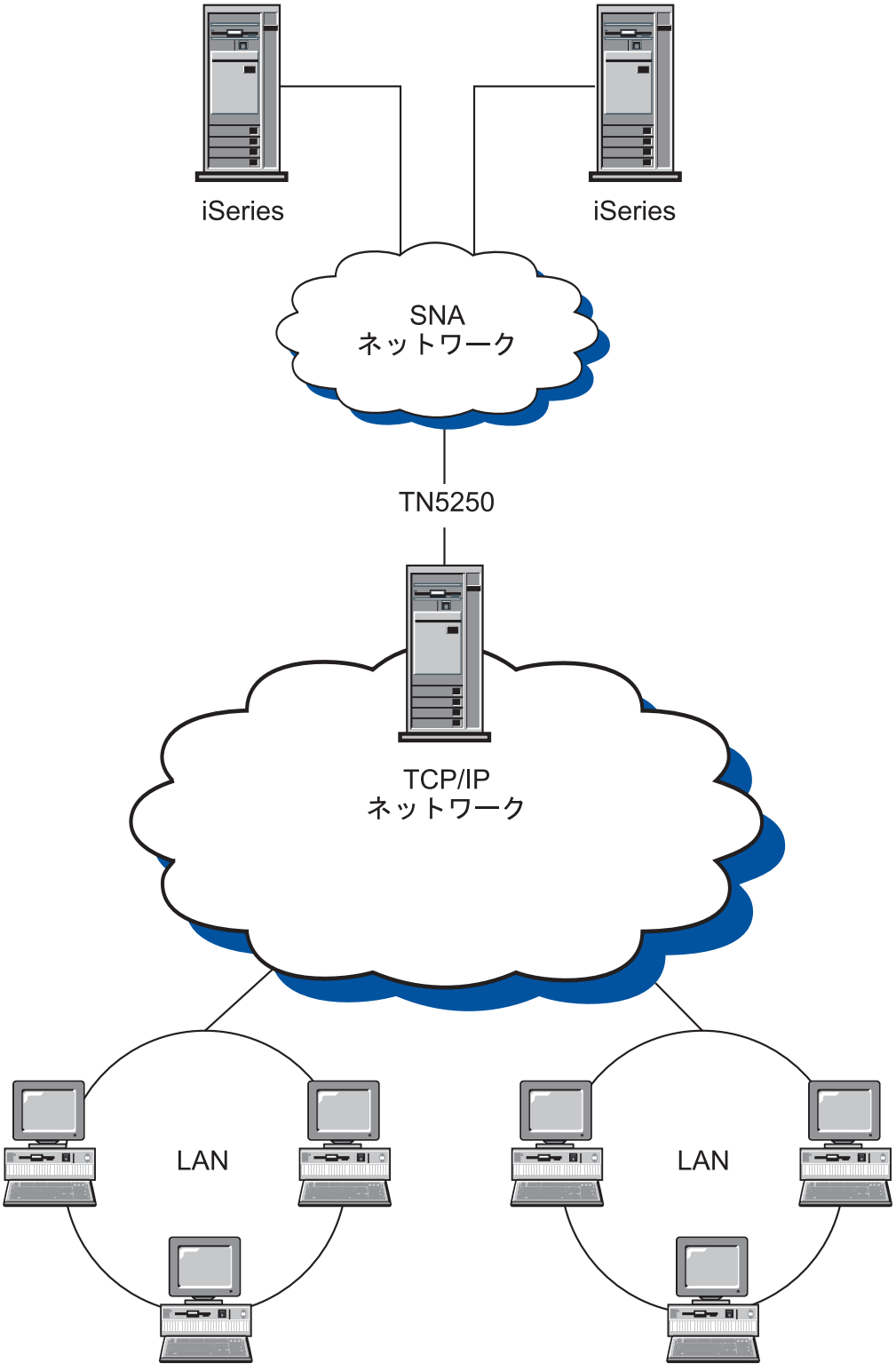

図 33. ワイド・エリア TCP/IP ネットワークの TN3270E サーバーとして構成された Communications Server

TN5250 サーバーの機能は、以下をサポートします。

- 複数のポート

TN5250 サーバーによって、構成するポートごとに、サーバー名、セキュリティー、クライアント認証、セキュリティーのレベル、証明書取り消しリスト (CRL) サポートを指定して複数のポートを構成することができます。

- 5250 ワークステーション・データ・ストリームを使用した TN5250 クライアントへの接続

  RFC 1205 内で概要が記載されたプロトコルを実装する場合、このサーバーは、IBM 5250 ワークステーションをエミュレートしている TCP/IP クライアントとの間で 5250 ワークステーション・データを渡します。このクライアントは、一般に TN5250 クライアントと呼ばれています。
- SNA ネットワーク上の 1 つ以上の iSeries ホストへのアクセス

  サーバーは、SNA LU 6.2 プロトコルを使用して iSeries ホストへ接続します。同じまたは異なるクライアント・ワークステーションからの 1 つ以上の iSeries ホストへのアクセスがサポートされます。
- IP フィルター

  Communications Server は、IP アドレス、サブネットワーク、ホスト名、またはドメイン・ネームを使用する TCP/IP クライアント・フィルターの指定に対応します。 この機能により、このサーバーへの接続を許可されたクライアントを中央から管理することに対応できます。この他、特定の iSeries ホストへクライアントを誘導するサポートにも対応します。
- Secure Sockets Layer ベース (SSL ベース) 機密保護

  TN5250 サーバーのポートが保護されていることを指定して、そのポートの接続に SSL バージョン 3 を使用し、データ暗号化とデジタル証明書を使用した認証を提供することができます。 ポートの接続に対するセキュリティーのレベルを指定するために、追加の構成パラメーターがサポートされています。この構成パラメーターによって、クライアント認証を処理するかどうかや、クライアント接続を受け入れる前に証明書取り消しリスト (CRL) を検査するかどうかを指定することができます。

TN5250 サーバーの構成方法に関する手順は、「*概説およびインストール*」を参照してください。

TN5250 サーバーでサポートされるクライアント・ワークステーション

TN5250 サーバーは、RFC 1205 に完全に準拠する TN5250 クライアントです。

ハイライト

このセクションには、TN5250 サーバーに対して構成することができるいくつかの機能の詳細が記載されています。

デフォルト・ポート番号の変更

TN5250 サーバー・サポートを構成する場合、デフォルト・ポート番号は 23 ですが、 TN3270E サーバー・サポートなどの他の Telnet アプリケーションもこのポートを使用します。 他の Telnet アプリケーションがポート 23 を使用して稼働している場合は、他のポートを使用しなければなりません。

ポート番号を変更する場合、他のアプリケーションで使用していることがわかっている番号は使用しないようにします。 2 つのアプリケーションが同じポート番号を使用すると、一方のアプリケーションが障害を起こします。

ポート番号を変更する場合、1 024 以上の数を使用してください。 1 024 より小さい数値は予約済みです。 予約済みポート番号についての詳細は、以下のインターネット・ロケーションを参照してください。

http://www.ietf.org/

ポート番号を変更する場合、エミュレーター・アプリケーションとポート番号が一致するように構成しなければならないため、 TN5250 クライアント・ユーザーに通知しなければなりません。

システム管理用トラフィック

未使用の接続を切断する頻度を制御するには、キープアライブ処理および自動ログオフの 2 つの方法があります。

デフォルトでは、TN5250 サーバーはキープアライブ処理を使用しません。 キープアライブ処理を使用する場合、NOP または タイミング・マークのいずれかを選択することができます。

- NOP 処理を使用すると、指定されたキープアライブ間隔の後、Telnet NOP コマンドが送信されます。これにより、データを接続上に伝送させ、TCP/IP に接続の切断を検出させます。サーバーは、クライアントからの応答を必要としません。TCP/IP に接続の故障率を検出させるにはかなりの時間がかかります。
- タイミング・マーク処理を使用すると、Telnet タイミング・マーク・コマンドがクライアントに送信されます。指定された時間内にクライアントが応答しない場合、接続はクローズされます。

タイミング・マーク処理では、NOP 処理よりシステム・トラフィックが増加しますが、未使用の接続は早く解放されます。

自動ログオフを選択すると、サーバーは、指定した期間にトラフィックがないセッションを切断します。 キープアライブ処理によるトラフィックでは、その接続をオープン状態のままに維持できないため、ホストとの間でデータを送受信しなければなりません。

キープアライブ処理を行うようにクライアント・エミュレーターが構成されている場合でも、サーバー側でその処理をオフにしても構いません。また、キープアライブ処理をサーバーで実行する場合でも、ネットワーク・トラフィックを削減するためにクライアント側でその処理をオフにしても構いません。

複数のポートを使用した iSeries ホストへのアクセスの指定

Communications Server は、2 つ以上の iSeries を構成を可能にし、着信接続を listen するために TN5250 サーバー用に 2 つ以上のポートを構成することができます。新規の TN5250 サーバー・ポートを構成する場合、 iSeries をポートに関連付けて指定することができます。 TN5250 サーバーによってポート上で受信された着信 TCP/IP 接続は、そのポートに関連付けられた iSeries へアクセスします。

特定の iSeries ホストに接続するエミュレーター・アプリケーション用に構成するポート番号を、 TN5250 クライアント・ユーザーに通知してください。

IP フィルター

Communications Server により、どの TCP/IP クライアントがサーバーに接続できるかを指定するために、 TN5250 フィルターを構成することができます。個人 IP アドレス、IP サブネットワーク、または TCP/IP ホスト名 (ドメイン・ネーム) を使用して、クライアントを指定することができます。

また、フィルターを使用して、ポートに関連付けられたものとは異なる iSeries を指定するように iSeries を構成することもできます。これは、フィルターに関連付けられたクライアントを、特定の iSeries に誘導するために使用することができます。

2 つ以上の iSeries を 1 つのフィルターで指定することができます。指定された最初の iSeries へのクライアントの接続試行が失敗した場合、フィルターで指定されているその他の iSeries ホストへの接続が試行されます。

Secure Sockets Layer (SSL) サポート

新規の TN5250 サーバー・ポートを構成する場合、ポートを保護接続用に使用する指定をすることができます。保護用に複数のポートを指定できます。

機密保護を使用可能にするために、Communications Server は「**鍵管理**」ユーティリティーを提供して、SSL が要求する証明書およびキーを生成します。 詳細については、 123 ページの『第 9 章 Secure Sockets Layer ベース・セキュリティーの計画』を参照してください。

構成が完了し機密保護が使用可能になると、SSL バージョン 3 をサポートする TN5250 クライアントは、保護ポート番号に接続し、保護接続を確立します。

SNA ネットワークの構成

TN5250 サーバーが iSeries ホストに接続できるように SNA ネットワークを構成する必要があります。 TN5250 サーバー用の SNA ネットワークの構成については、「*概説およびインストール*」を参照してください。

TN5250 サーバーのロード・バランシング

Communications Server は、複数の TN5250 サーバーに渡って、 TN5250 クライアントのロード・バランシングもサポートします。詳細については、 133 ページの『第 10 章 ロード・バランシングの計画』を参照してください。

第 9 章 Secure Sockets Layer ベース・セキュリティーの計画

Secure Sockets Layer ベース (SSL ベース) 機密保護を、 TN クライアントと TN3270E サーバー (または TN5250 サーバー) 間の接続で使用することができます。この機密保護は、SSL バージョン 3 を使用して、署名済み証明書を使用したデータ暗号化および認証を提供します。

SSL ベースの機密保護をサポートするために、特定のポートを構成することかできます。機密保護を指定する場合、サーバーには認証局 (CA) が提供する認証がなければなりません。 Communications Server は、 SSL バージョン 3 が使用した鍵と証明書を生成および管理するユーティリティーを提供します。

お客様は、クライアント認証を要求するようにポートを構成して、サーバーへのセキュア接続の確立をクライアントが許可されていることを検査します。さらに、クライアント認証が構成されている場合は、クライアント証明書の証明書取り消しリスト (CRL) 処理を要求することもできます。クライアント証明書が取り消されているかどうかを判別するための、 CRL を保持する LDAP サーバーのロケーションを指定します。

注: クライアント証明書の CRL 処理をサポートさせるには、 IBM Vault Registry 製品を使用する必要があります。この製品は、 LDAP サーバーに証明書取り消しリストを公開します。

ポートごとに必要とされるセキュリティーのレベルを構成することもできます。オプションには、HIGHEST、MEDIUM、および AUTHENTICATION ONLY があります。 HIGHEST の定義はインストールした Communications Server のバージョンに応じて異なります。 Communications Server で強い暗号化をサポートするには、強い暗号化をサポートしているクライアントからの接続のみ、ポートで受け入れるようにするために HIGHEST を指定します。エクスポートの暗号化のみサポートする Communications Server の場合、HIGHEST は MEDIUM と同じです。 MEDIUM は、ポートが、サポート対象の任意暗号化レベルで接続を確立できることを示します。 AUTHENTICATION ONLY は、接続の一方または両方の終端を認証するための証明書を交換しますが、データは暗号化されません。

この章では、Secure Sockets Layer ベース (SSL ベース) の機密保護の概説を説明します。 SSL ベース機密保護は、TN3270E サーバーおよび TN5250 サーバー構成の際にオプションとして提供されます。

SSL セキュリティーの使用法

Secure Sockets Layer (SSL) は、対称鍵および公開鍵の暗号テクノロジーを使用する業界標準プロトコルです。対称鍵暗号では、メッセージの暗号化と復号に同じ鍵を使用します。公開鍵暗号では、鍵ペア (公開鍵と秘密鍵) を使用します。各サーバーの公開鍵は公開されますが、秘密鍵は秘密を保持されます。サーバーへセキュア・メッセージを送信する際に、クライアントはサーバーの公開鍵を使用してメッセージを暗号化します。サーバーはそのメッセージを受信すると、秘密鍵を使用してメッセージを復号します。

SSL は、以下の 3 つの基本機密保護サービスを提供します。

- メッセージ・プライバシー

  メッセージ・プライバシーの実現には、公開鍵と対称鍵の暗号化の組み合わせを使用します。 SSL クライアントと SSL サーバー間のトラフィックはすべて、セッション・セットアップ中にネゴシエーションした、鍵および暗号化アルゴリズムを使用して暗号化されます。
- メッセージ保全性

  メッセージ保全性サービスにより、SSL セッションのトラフィックは最終の宛先への経路において変化しないことが保証されます。 SSL は、メッセージ保全性を保証するために、公開鍵/秘密鍵とハッシュ関数の組み合わせを使用します。
- 認証

  認証とは、クライアントとサーバーがお互いの識別を確信するプロセスです。クライアントおよびサーバーの識別は、公開鍵証明書内でエンコードされます。公開鍵証明書には、以下の構成要素が含まれています。
  - 件名の識別名
  - 差出人の識別名
  - 件名の公開鍵
  - 差出人のシグニチャー
  - 妥当性期間
  - シリアル番号

Communications Server の SSL サポート

Communications Server は、以下の SSL 機密保護構成要素をサポートします。

- SSL バージョン 3 をサポートする、 TN3270E サーバーおよび、TN3270 と TN3270E クライアント間のセキュア SSL セッション
- SSL バージョン 3 をサポートする、 TN5250 サーバーおよび TN5250 クライアント間のセキュア SSL セッション
- SSL バージョン 3
- メッセージのプライバシーおよび保全性
- サーバー側認証
- オプションのクライアント側認証
- クライアント認証が要求された場合の、オプションの証明書取り消しリスト (CRL) 処理

SSL セキュリティーの構成

TN3270E サーバー構成および TN5250 サーバー構成の際、接続のためにどのポートが SSL 機密保護を使用するかを指定します。セキュア・ポート構成の詳細については、 109 ページの『第 7 章 TN3270E サーバーの計画』および 117 ページの『第 8 章 TN5250 サーバーの計画』を参照してください。

サーバー認証

サーバー認証を使用して SSL 機密保護を使用可能にするには、公開鍵/秘密鍵および関連付けられた認証済み公開鍵証明書のセットが必要です。 Communications Server は「 **鍵管理**」ユーティリティーを提供して、 SSL が要求する公開鍵/秘密鍵および証明書を生成し、管理し、保管します。

「**鍵管理**」ユーティリティーを使用して、以下のいずれかを行なってください。

- 公開鍵/秘密鍵のペアを作成し、事前定義 (ウェルノウン) 認証局 (CA) のうちの 1 つから証明書を入手し保管します。 126 ページの『ウェルノウン・トラステッド CA を使用した SSL の構成』を参照してください。

  この手順では、鍵データベース・ファイルは、証明書を発行する機関から CA を識別するために要求される、ウェルノウン CA ルート証明書とともに事前構成されているので、セットアップにかかる手間が省けます。
- 公開鍵/秘密鍵のペアを作成し、 CA のルート証明書を入手して、鍵データベース・ファイルに保管することにより未承認 CA を定義し、未承認 CA から証明書を入手して保管します。詳細については、 128 ページの『未承認 CA を使用した SSL の構成』を参照してください。
- 自己署名証明書を作成し、鍵データベース・ファイルにその証明書を保管します。詳細については、 130 ページを参照してください。

  注: サイトの機密保護を十分に保証するために、自己署名証明書は、制御テスト目的のみに使用するようにしてください。

クライアント認証

クライアント認証用にセキュア・ポートが構成されている場合は、 SSL はクライアント証明書を要求します。サーバーで鍵データベース・ファイルが検査され、クライアント証明書の署名者が確認されます。

クライアント証明書が、

- ウェルノウン CA によって発行されている場合は、追加の構成は不要です。
- 未承認 CA によって発行されている場合は、その未承認 CA のルート証明書を取得して、署名者の証明書として鍵データベースに格納しなければなりません。詳細については、 131 ページの『クライアントの証明書の保管』 を参照してください。
- 自己署名クライアント証明書の場合は、自己署名証明書を取得して、署名者の証明書として鍵データベースに格納しなければなりません。詳細については、 131 ページの『クライアントの証明書の保管』 を参照してください。

証明書取り消しリスト (CRL) サポートが構成されている場合は、CRL を保持する LDAP サーバーに接続し、クライアント証明書が取り消されていないかどうかを判別します。

注: クライアント証明書の CRL 処理をサポートさせるには、 IBM Vault Registry 製品を使用する必要があります。この製品は、 LDAP サーバーに証明書取り消しリストを公開します。

鍵管理ユーティリティー

Communications Server の「**鍵管理**」ユーティリティーを使用すると Communications Server とクライアントの間での SSL 通信に必要な公開鍵/秘密鍵および証明書を、作成、管理、および保管することが可能になります。 SSL 通信の構成を開始する前に、Communications Server の鍵データベース・ファイルをオープンする必要があります。ファイルをオープンするには、以下のステップに従ってください。

1. メインメニューから「**鍵データベース・ファイル**」を選択し、「**オープン**」を選択して既存の鍵データベースをオープンします。
2. 「**オープン**」ウィンドウから、製品をインストールしたディレクトリーの**専用**サブディレクトリーを選択します (例えば、C:¥Program Files¥IBM¥Communications Server¥PRIVATE)。
3. **ibmcs.kdb** を鍵データベースとして選択します。
4. パスワード・プロンプトが出されたら、パスワードを入力します。

注: パスワードは、最初は **ibmcs** に設定されています。適切なセキュリティーのために、**鍵管理**タスクを行う前に、パスワードを変更しなければなりません。

パスワードの変更

カレント・データベースのパスワードを変更するには、以下のステップに従ってください。

1. メニューから「**鍵データベース・ファイル**」を選択し、「**パスワードの変更**」を選択して、現行データベースの鍵データベース・パスワードを変更します。「**パスワードの変更**」ファイル・ダイアログが表示されます。
2. 使用する新規パスワードを入力します。
3. 確認のために、同じパスワードを再び入力します。
4. パスワードに有効期限を付けたい場合は、「**有効期限の設定**」をクリックします。機密保護を十分にするには、パスワードに有効期限を付けてください。
5. パスワードに有効期限を付ける場合は、パスワード失効までの日数を指定します。
6. 「**パスワードを隠す**」をクリックして、カレント・データベースのパスワードを **ibmcs.sth** ファイルに隠します。 Communications Server では、パスワードを隠して鍵データベース・ファイルにアクセスする必要があります。

ウェルノウン・トラステッド CA を使用した SSL の構成

ウェルノウン CA によって発行された証明書を使用して SSL 機密保護を設定するには、このセクションのプロシージャーに従ってください。以下の CA 署名者証明書は、既に鍵データベースに保管されており、承認済み証明書としてマークされています。

- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA セキュア・サーバー CA (VeriSign からも入手できる)
- VeriSign クラス 4 共用 1 次 CA

- VeriSign クラス 3 共用 1 次 CA
- VeriSign クラス 2 共用 1 次 CA
- VeriSign クラス 1 共用 1 次 CA

ウェルノウン CA を使用して SSL 機密保護を設定するには、以下のプロシージャーが必要です。

- 鍵および証明書要求の作成
- CA への証明書要求の発信
- サーバー鍵データベース内の証明書の入手および保管

鍵および証明書要求の作成

公開鍵/秘密鍵および証明書要求を作成するには、「**鍵管理ユーティリティー**」を使用して、以下のステップに従ってください。

1. メインメニューのドロップダウン・リストから「**個人用証明書要求**」を選択し、「**新規作成**」をクリックして新規の鍵ペアと証明書要求を作成します。「**新規の鍵および証明書要求を作成**」ダイアログが表示されます。
2. データベース内で鍵および証明書を識別するために使用する名前 (ラベル) を入力します。
3. 使用したい鍵サイズの数値を入力します。長い鍵サイズを選択するほど機密保護は強化されますが、接続を確立する際に、より多くの処理がクライアントとサーバー側で必要になります。
4. 共通名 (wtr05306.raleigh.ibm.com など) として、Communications Server の TCP/IP ホスト名を入力します。
5. 組織名を入力します。
6. 組織単位を入力します (オプション)。
7. 市または地域名を入力します (オプション)。
8. 州または県名を入力します (オプション)。
9. 郵便番号を入力します (オプション)。
10. 国別コードを入力します。最低 2 文字を指定してください (US など)。
11. 証明書要求ファイル名を入力するか、デフォルトのファイル名を使用してください。

「**OK**」をクリックすると、提供した情報が処理されます。以下の 2 つのファイルが作成されます。

ibmcs.rdb
: 秘密鍵ファイル

certreq.arm
: 証明書要求ファイルのデフォルト名。ファイル名を割り当てた場合は、その名前の付いたファイルが作成されます。証明書要求ファイルは、強化された 64 形式の PKCS 10 タイプのファイルです。

これらのファイルを、編集または移動してはいけません。 **ibmcs.rdb** ファイルが見つからない場合、またはこのファイルが鍵データベースに証明書を入力しようとする際に破損した場合は、証明書要求を CA へ再発信しなければなりません。

証明書要求の発信

Web ブラウザーを開始し、CA の Web ページにアクセスします。提供された指示に従い、証明書要求を発信します。以下は、ウェルノウン CA の URL です。

- VeriSign: **http://www.verisign.com/**
- Thawte: **http://www.thawte.com/**

選択する CA に応じて、**鍵管理**ユーティリティーにより生成された証明書要求を e-mail するか、または、その証明書要求を CA により提供された形式またはファイルへ結合させてください。

証明書要求を CA へ発信したら、自己署名証明書を作成および保管することによって SSL 機密保護を使用可能にできます。自己署名証明書は、制御テスト目的にのみ使用するようにしてください。 詳細については、130 ページを参照してください。

鍵データベースへの証明書の保管

CA から証明書を受信したら、**鍵管理**ユーティリティーを使用して、証明書をサーバー上にある鍵データベース・ファイルの **ibmcs.kdb** に書き込みます。

1. 「**鍵管理**」ユーティリティーのドロップダウン・リストから、「**個人用証明書**」を選択し、「**取得**」をクリックして鍵ペアと証明書要求を受信します。「**ファイルからの証明書取得**」ダイアログが表示されます。
2. データ・タイプが、「**BASE64-encoded エンコード ASCII データ**」 (エンコードされた 64 形式) であることを確認してください。
3. 証明書ファイル名を入力します。
4. 証明書のロケーション (パス名) を入力します。 「**OK**」をクリックします。 保管された証明書が、第 1 項目として表示されます。
5. 保管された証明書を強調表示し、「**表示/編集**」をクリックします。「**鍵情報**」ダイアログが表示されます。
6. 「**この証明書をデフォルトとして設定**」をクリックします。選択した鍵がデフォルトになります。

未承認 CA を使用した SSL の構成

未承認 CA (データベースにまだ定義されていない) を使用して SSL 機密保護を設定するには、以下のプロシージャーが必要です。

- 鍵および証明書要求の作成
- CA への証明書要求の発信
- CA のルート証明書とユーザーの証明書の入手と、これらのサーバーの鍵データベースへの保管

鍵および証明書要求の作成

公開鍵/秘密鍵および証明書要求を作成するには、「**鍵管理**ユーティリティー」内で、以下のステップに従ってください。

1. メインメニューのドロップダウン・リストから「**個人用証明書要求**」を選択し、「**新規作成**」をクリックして新規の鍵ペアと証明書要求を作成します。「**新規の鍵および証明書要求を作成**」ダイアログが表示されます。
2. データベース内で鍵および証明書を識別するために使用する名前 (ラベル) を入力します。

3. 使用したい鍵サイズの数値を入力します。長い鍵サイズを選択するほど機密保護は強化されますが、接続を確立する際に、より多くの処理がクライアントとサーバー側で必要になります。
4. 共通名 (wtr05306.raleigh.ibm.com など) として、Communications Server の TCP/IP ホスト名を入力します。
5. 組織名を入力します。
6. 組織単位を入力します (オプション)。
7. 市または地域名を入力します (オプション)。
8. 州または県名を入力します (オプション)。
9. 郵便番号を入力します (オプション)。
10. 国別コードを入力します。最低 2 文字を指定してください (US など)。
11. 証明書要求ファイル名を入力するか、デフォルトのファイル名を使用してください。

「**OK**」をクリックすると、提供した情報が処理されます。以下の 2 つのファイルが作成されます。

ibmcs.rdb
秘密鍵ファイル

certreq.arm
証明書要求ファイルのデフォルト名。ファイル名を割り当てた場合は、その名前の付いたファイルが作成されます。証明書要求ファイルは、強化された 64 形式の PKCS 10 タイプのファイルです。

これらのファイルを、編集または移動してはいけません。 **ibmcs.rdb** ファイルが見つからない場合、またはこのファイルが鍵データベースに証明書を入力しようとする際に破損した場合は、証明書要求を CA へ再発信しなければなりません。

証明書要求の発信

証明書要求を発信するには、未承認 CA のプロシージャーに従います。

選択する CA に応じて、**鍵管理**ユーティリティーにより生成された証明書要求を e-mail するか、または、その証明書要求を CA により提供された形式またはファイルへ結合させてください。

証明書要求を CA へ発信したら、自己署名証明書を作成および保管することによって SSL 機密保護を使用可能にできます。自己署名証明書は、制御テスト目的にのみ使用するようにしてください。 詳細については、130 ページを参照してください。

鍵データベースへの証明書の保管

CA から証明書を受信する場合は、 CA に問い合わせて CA ルート証明書を入手してください。 CA ルート証明書は、適用した証明書を保管する前に、鍵データベースに保管する必要があります。 CA ルート証明書は、要求した証明書の妥当性を検査します。 CA ルート証明書の保管には、「**鍵管理**」ユーティリティーを使用します。

1. ドロップダウン・リストから「**署名者証明書**」を選択し、「**追加**」をクリックして CA ルート証明書を受信します。「**ファイルからの証明書追加**」ダイアログが表示されます。

2. データ・タイプが、「**BASE64-encoded エンコード ASCII データ**」 (エンコードされた 64 形式) であることを確認してください。
3. 証明書ファイル名を入力します。
4. 証明書のロケーション (パス名) を入力します。 「**OK**」をクリックします。 ファイルは、***承認済み*** とマークされて保管されます。

適用した証明書を保管するには、「**鍵管理**」ユーティリティーを使用して、証明書をサーバー上にある鍵データベース・ファイルの **ibmcs.kdb** に書き込みます

1. メインメニューのドロップダウン・リストから、「**個人用証明書**」を選択し、「**取得**」をクリックして鍵ペアと証明書要求を受信します。「**ファイルからの証明書取得**」ダイアログが表示されます。
2. データ・タイプが、「**BASE64-encoded エンコード ASCII データ**」 (エンコードされた 64 形式) であることを確認してください。
3. 証明書ファイル名を入力します。
4. 証明書のロケーション (パス名) を入力します。 「**OK**」をクリックします。 保管された証明書が、第 1 項目として表示されます。
5. 保管された証明書を強調表示し、「**表示/編集**」をクリックします。「**鍵情報**」ダイアログが表示されます。
6. 「**この証明書をデフォルトとして設定**」をクリックします。選択した鍵がデフォルトになります。

自己署名証明書の作成

ウェルノウン・トラステッド CA からの証明書受信は、3 週間かかることがあります。 共用サーバー証明書を受信するまでの間、自己署名証明書を作成すると、クライアントとサーバー間で SSL セッションを使用可能にできます。 自己署名証明書は、制御テスト目的にのみ使用するようにしてください。 サイトの機密保護を十分に保証するため、自己署名証明書は、実稼働環境で使用しないようにしてください。 「**鍵管理**」ユーティリティーを使用して、自己署名証明書を使用するようサイトを設定するには、以下のステップに従ってください。

1. 「**作成**」メニュー・オプションから「**新規自己署名証明書**」を選択し、新規の自己署名証明書を作成します。「**新規自己署名証明書の作成**」ダイアログが表示されます。
2. データベース内で鍵および証明書を識別するために使用する名前 (ラベル) を入力します。 証明書バージョンとして「**X509 V3**」を選択します。
3. 使用したい鍵サイズの数値を入力します。長い鍵サイズを選択するほど機密保護は強化されますが、接続を確立する際に、より多くの処理がクライアントとサーバー側で必要になります。
4. 共通名 (wtr05306.raleigh.ibm.com など) として、Communications Server の TCP/IP ホスト名を入力します。
5. 組織名を入力します。
6. 組織単位を入力します (オプション)。
7. 市または地域名を入力します (オプション)。
8. 州または県名を入力します (オプション)。
9. 郵便番号を入力します (オプション)。
10. 国別コードを入力します。最低 2 文字を指定してください (US など)。
11. 自己署名証明書の有効である日数を入力します。
12. 「**OK**」をクリックします。

13. 「**はい**」をクリックして、この鍵を鍵データベース内にデフォルトの鍵として設定します。

「**鍵管理**」ユーティリティーを使用して、IBM SecureWay Host On-Demand バージョン 4 または指定された自己署名証明書を必要とするその他の一部の SSL クライアントを使用している場合は、以下のステップに従ってください。

1. ドロップダウン・リストから「**個人用証明書**」を選択し、自己署名証明書を強調表示して「**証明書抽出**」をクリックします。 「**ファイルへの証明書抽出**」ダイアログが表示されます。
2. データ・タイプに「**バイナリ DER データ**」を選択します。
3. 証明書ファイル名を入力します。 このファイルは、ファイル・タイプ **der** を持っていなければなりません (ibmcs.der など)。
4. 証明書のロケーション (パス名) を入力します。
5. 「**OK**」をクリックします。

証明書ファイルは、サーバーへの接続が許可された各クライアントに提供されます。クライアントのクラス・ファイルまたは鍵データベースに CA ルート証明書として自己署名証明書を保管する手順については、クライアントの文書で確認してください。

クライアントの証明書の保管

クライアント証明書が、未承認 CA によって発行される場合、または自己署名証明書である場合は、未承認 CA のルート証明書または自己署名証明書を、鍵データベースに署名者証明書として保管する必要があります。 CA ルート証明書の保管には、「**鍵管理**」ユーティリティーを使用します

1. ドロップダウン・リストから「**署名者証明書**」を選択し、「**追加**」をクリックして CA ルート証明書を受信します。「**ファイルからの証明書追加**」ダイアログが表示されます。
2. データ・タイプが、「**BASE64-encoded エンコード ASCII データ**」 (エンコードされた 64 形式) であることを確認してください。
3. 証明書ファイル名を入力します。
4. 証明書のロケーション (パス名) を入力します。 「**OK**」をクリックします。 ファイルは、***承認済み*** とマークされて保管されます。

第 10 章 ロード・バランシングの計画

この章では、ロード・バランシングの計画についての概説を示します。ここで、従属 LU および LU6.2 6.2 ロード・バランシングの計画を説明します。

従属 LU ロード・バランシング

ロード・バランシングにより、複数サーバーにわたって従属ホスト・セッションを平衡化することが可能になります。ロード・バランシングは、SNA API クライアント、3270 エミュレーター、および TN3270 エミュレーターを経由して LUx API アプリケーションをサポートします。

Communications Server はクライアント要求に応えると、要求されたプールをサポートするサーバーを、ロードごとにソートします。従属 LU に対するロードは、特定サーバーから利用できる資源の割合を示します。

ロード・パーセンテージは、アクティブなアプリケーション接続数を、使用できる LU の合計数値 (0 から 3) で割って計算されます。 2 つのサーバー間の、使用可能メモリー、プロセッサー速度、および CPU 使用率などの差を補正するために、LU 0-3 のロード係数 (ホスト・セッション・ロード係数) を指定して、計算されたロードに影響を与えることができます。

また、LU 0-3 のロード係数を使用して、 Communications Server および Novell NetWare for SAA サーバー間のロードのバランスを保つこともできます。

注:

1. ロード・バランシングに関係するサーバーは、 LU プール・メンバーシップおよび有効範囲メンバーシップにより判別されます。同じ名前のプール内に LU を持つ Communications Server は、すべてロード・バランシングされます。
2. TCP/IP プロトコルを使用するクライアントは、ロード・バランシングを行うことができます。ただし、TCP/IP クライアントは IBM Communications Server 同士の間でしか、ロード・バランシングを行うことはできません。ロード・バランシングは、構成された有効範囲により判別されます。

Communications Server において、異なるサーバー上の LU プールが同じ名前を持つ場合、これらはロード・バランシング用に 1 つのプールとして機能します。複数の LU を 1 つの LU プールに割り当てる場合、サーバー上のホスト・リンクから選択し、選択したホスト・リンクから LU プールに LU を割り当ててください。これらの LU は、同じ LU タイプである必要はありません。また、結果のプールには複数のリンクから LU を含めることができます。

LU 6.2 ロード・バランシング

ロード・バランシングでは、独立 LU 6.2 セッションを複数のサーバーに分散させることによって、これらのセッションを平衡化することが可能になります。 ロード・バランシングは SNA API クライアントおよび TN5250 エミュレーターを経由して、 APPC API アプリケーションをサポートします。

独立 LU6.2 のロードは、特定のサーバーから利用できる資源の割合を示します。ロード・パーセンテージは、特定のサーバーのすべてのローカル LU 上にある会話の合計数値を、すべてのローカル LU 用の累積最大セッション限界値で除算することにより計算されます。最大セッション限界値は、構成時に指定した LU 6.2 セッション限界値です。 最大セッション限界値に、セッション限界値がないことを示すゼロ (0) に指定されている場合は、デフォルトの最大ローカル LU セッション限界値 (ローカル LU ごとに 512) が、ロード計算の際に使用されます。 デフォルトの最大ローカル LU セッション限界値を、構成時に指定することもできます。

2 つのサーバー間の、使用可能メモリー、プロセッサー速度、および CPU 使用率などの差を補正するために、LU 6.2 のロード係数 (APPC セッション・ロード係数) を指定して、計算されたロードに影響を与えることができます。また、LU 6.2 のロード係数を使用して、 Communications Server および Novell NetWare for SAA サーバー間のロードのバランスを保つこともできます。

注: TCP/IP プロトコルを使用するクライアントは、LU 6.2 ロード・バランシングを行うことができます。

TCP/IP 有効範囲の計画

有効範囲は、ネットワーク内で、サーバーへのアクセス制御および管理のために TCP/IP クライアントによって使用されるパラメーターです。これは、 RFC 2165 で言及されたサービス・ロケーション・プロトコル (SLP) の有効範囲と同じです。SLP は、TCP/IP ベースのロード・バランシングを行うために Communications Server によって使用されます。

制御有効範囲の提供が必要であるのは、以下の 2 つの理由によります。

- ネットワークが広がり、クライアント数とサーバー数が増加するに従って、増加するクライアント数ごとにこれらのサーバーへのアクセスを区分化して、ネットワーク上の全体的なトラフィックを削減する必要が生じます。
- 制御有効範囲により、管理者はユーザーおよびサーバーを管理グループ内へ編成することができます。

有効範囲値の意味は、ネットワーク管理者により定義されます。これらの値は、どのエンティティーも示すことができます。一般には有効範囲値は、部門の境界、地理的な境界、または組織上の境界のどれかになります。

一度構成されると、クライアントは同じ有効範囲とともに構成されたサーバー、または関連した有効範囲を持たないサーバー (非有効範囲のサービスまたはサーバー) を通じて、SNA ネットワークに到着することができます。

注: サーバーが非有効範囲として構成されると、サーバーは SLP および非有効範囲の要求に応答します。 SNA API クライアントが、非有効範囲サーバーに接続するように構成されている場合は、非有効範囲サーバーのみが応答します。

有効範囲およびクライアント・サーバーのセキュリティー

Communications Server を使用すると、Novell NetWare for SAA クライアントは、Windows NT ドメイン機密保護が使用可能になり、ユーザー ID とパスワードを再入力せずに、サーバーに接続する権限をクライアントに与えることができます。 この場合のクライアントは、 Communications Server ドメインに参加するかまたは同

期したユーザー ID とパスワードでローカルにログインすることによって、Windows NT ドメインの一部でなければなりません。

クライアント・サーバーの許可ユーザーは、IBMCSAPI ローカル・グループ内に保持され、 Communications Server かまたは Communications Server が参加しているドメイン制御装置のいずれかに直接配置されます。このユーザー・グループは、インストール中に作成され、 Windows NT ユーザーのマネージャー・アプリケーションを使用して管理されます。

Windows NT ドメイン外部の Novell NetWare for SAA のクライアント・ユーザーは、同一有効範囲により構成されているすべてのサーバーに対して、ユーザー ID とパスワードを複写する必要があります。

有効範囲の構成場所

サーバーごとに 1 つまたは複数の有効範囲が、 **SNA ノード構成**を通じて割り当てられます。 これらのサーバーを使用しているクライアントは、単一で特定の有効範囲内でサーバーに接続するか、または非有効範囲のサーバーに接続するように構成されなければなりません。クライアントの構成の詳細については、*「クライアント/サーバー・コミュニケーション・プログラミングおよび管理プログラミング」* を参照してください。

SLP と有効範囲の関連について

Communications Server 有効範囲は、直接、サービス・ロケーション・プロトコル (SLP) 範囲と関連しています。したがって、SLP ディレクトリー・エージェントは、 Communications Server 構成有効範囲をサポートするネットワークに存在することができます。有効範囲をベースにした Communications Server サービスをクライアントが配置できるようにしたい場合は、有効範囲が全体としてネットワークとどう関連付けられているかを考慮してください。有効範囲も使用されているネットワーク内に非有効範囲サービスがある場合、非有効範囲サービスは任意の有効範囲化された要求を満たす資格があります。これにより、非有効範囲サービスをサポートするサービス・エージェントおよびディレクトリー・エージェントに負荷がかかる可能性があります。

注: SNA API クライアントが、非有効範囲サーバーに接続するように構成されている場合は、非有効範囲サーバーのみが応答します。

ディレクトリー・エージェントをサイト・ネットワーク (上向きスケール) 内で使用する場合は、これらのエージェントを Communications Server 用に構成されたものと同じ有効範囲を処理するよう構成しなければなりません。また、非有効範囲サービスをネットワーク内でディレクトリー・エージェントとともに使用する場合は、少なくとも 1 つの非有効範囲ディレクトリー・エージェントを構成しなければなりません。

Communications Server には、SLP サービス・エージェントがあり、これは Communications Server をインストールしたすべてのサーバー上にインストールされています。 TCP/IP ロード・バランシングおよび Communications Server ディスカバリーを適切に作動させるために、さらに SLP サポートをネットワークにインストールする必要はありません。

現行ロードのトラッキング

Windows NT パフォーマンス・モニターを使用して、 LU 6.2 および従属 LU の両方の現行ロードを追跡することができます。「プログラム」メニューの「**管理ツール (共通)**」選択項目から、パフォーマンス・モニターを開始します。

「パフォーマンス・モニター」画面で、「**Edit**」プルダウン・メニューから「**Add to Chart**」を選択します。 「**Object**」フィールドで、「**IBM SNA ロード・バランシング**」を選択します。 以下の 2 つのカウンターがリストされます。

LU0/LU3 ロード
従属 LU のロードを追跡するには、このカウンターを使用します。

LU6.2 ロード
このカウンターは LU6.2 LU のロードを追跡する場合に使用します。

ロード追跡の結果は、保管して後で参照することができます。

第 11 章 バックアップ・ホスト接続の計画

ワークステーション・エミュレーター・セッションが使用中の 1 次接続に対して、バックアップ・ホスト接続を提供することが重要な環境の場合、Communications Server は、障害状況に応えて活動化するホスト接続構成を使用可能にするオプションを提供します。この目的で使用できるオプションは、お客様が提供したいバックアップ・レベル (以下) によって異なります。

- LAN ベース IP または IPX ワークステーション・エミュレーター・セッションをサポートしているサーバー・ノード間で完全なシステム・バックアップを使用可能にしたい場合は、ユーザー環境にホット・スタンバイを含めてください。
- LAN ベース IP または IPX ワークステーション・エミュレーター・セッション以外をサポートしているサーバー・ノード間で完全なシステム・バックアップを使用可能にしたい場合は、ユーザー環境にホット・スタンバイを含めないでください。バックアップ・システム上に、複製の Communications Server インストールを構成してください。
- サーバー・ノード内でバックアップを使用可能にする場合は、ホット・スタンバイを使用しないでください。バックアップ環境の接続定義にある通常オプションを使用してください。

これらのオプションについては、以下のセクションで説明します。

ホット・スタンバイを使用したサーバー間のバックアップ接続の計画

Communications Server では、クリティカル・サーバー障害時に自動的に活動化されるホスト・リンクを構成できます。構成されたホスト接続は、バックアップ・サーバー上の代替接続を活動化させることによって存続することができます。この機能を、ホット・スタンバイと呼びます。

あるホスト・マシン (Communications Server 障害が原因で初期接続が失敗に終わるマシン) とのワークステーション・エミュレーター・セッションのユーザーに対しては、ホット・スタンバイは、自動的に代替の Communications Server を経路指定して、引き続きホスト・マシンとの接続の再確立ができるようにします。接続を提供する最初のサーバーは、***クリティカル・サーバー*** と呼ばれます。クリティカル・サーバーの障害後にホスト・マシンへ接続を提供する代替サーバーは、***バックアップ・サーバー*** と呼ばれます。バックアップ・サーバーはクリティカル・サーバー障害の検出に応答して自動開始する接続を提供し、クリティカル・サーバーのホスト接続に関連するライセンス使用料は自動的にバックアップ・サーバー上で管理されます。

1 つのサーバーが、同時にクリティカル・サーバーおよびバックアップ・サーバーの両方になることができます。各サーバーは相互にバックアップ可能です。

ホット・スタンバイは、LAN ベース IP または IPX エミュレーター・セッションに対するバックアップ・サーバー・サポートを可能にします。ホット・スタンバイは、SNA 環境に対するバックアップ・サーバー・サポートを提供しません。

図 34 では、バックアップ・サーバーは、HOSTCON1 (この HOSTCON1 接続は、クリティカル・サーバー上で 1 次ホスト接続を提供) に対して完全なバックアップ接続を使用して構成されています。バックアップ・サーバーとワークステーション・エミュレーター・クライアントとの間の点線は、クリティカル・サーバーが稼働している間は非活動です。

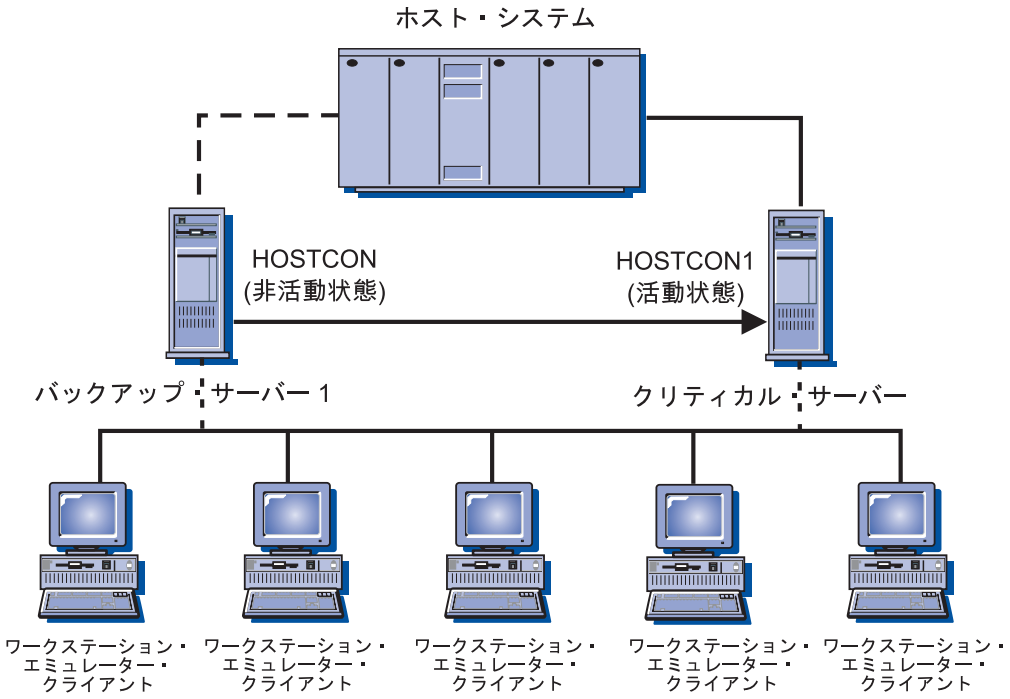

図 34. 1 台のバックアップ・サーバーを持つクリティカル・サーバー

139 ページの図 35 では、各バックアップ・サーバーは、HOSTCON1 (この HOSTCON1 接続は、クリティカル・サーバー上で 1 次ホスト接続を提供) に対して部分的なバックアップ接続を使用して構成されています。 2 つのバックアップ・サーバーの組み合わせで、 HOSTCON1 の完全なバックアップを提供します。バックアップ・サーバーとワークステーション・エミュレーター・クライアントとの間の点線は、クリティカル・サーバーが稼働している間は非活動です。

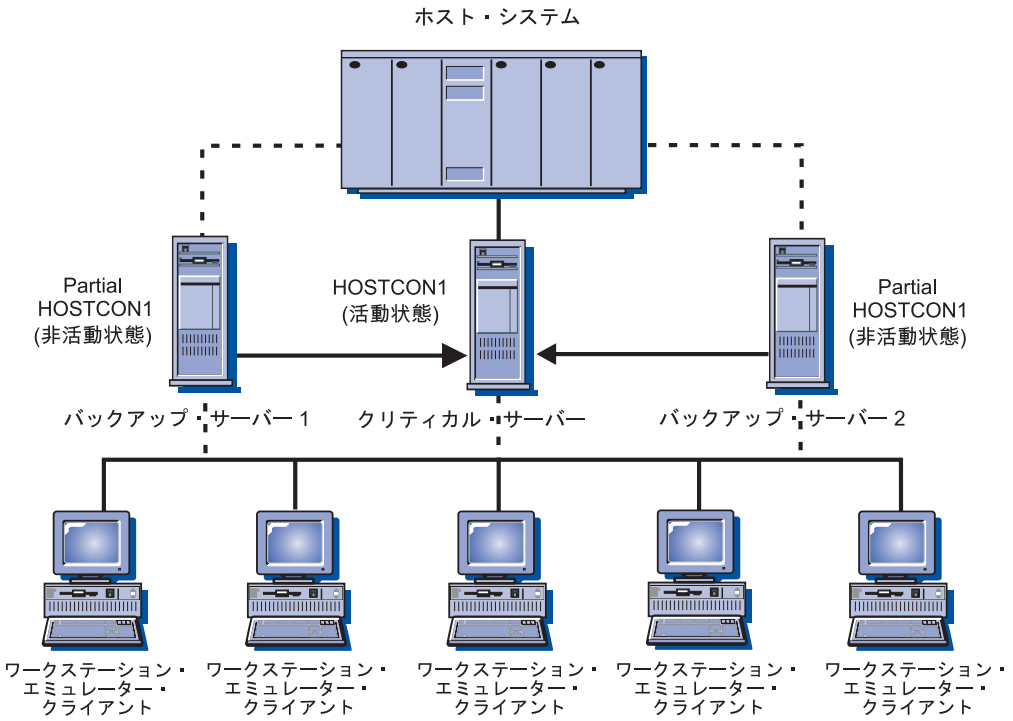

図 35. 2 台のバックアップ・サーバーを持つクリティカル・サーバー

クリティカル・サーバーが失敗すると、以下のように回復されます。

1. バックアップ・サーバー、ホスト、およびワークステーション上のワークステーション・エミュレーター・ソフトウェアが、ほとんど同時に障害を検出します。
2. バックアップ・サーバーのクリティカル・サーバー構成内で名前を指定された接続が自動的に活動化され、ホスト・マシンへの接続が確立されます。
3. ワークステーションは、たった今クリティカル・サーバー接続を活動化させたバックアップ・サーバーと新規セッションを確立します。
4. ワークステーションは、ホスト・マシンに連絡し、ユーザー用のログオン・プロンプトを表示します。

注: クリティカル・サーバーが再活動化しても、障害のために活動化されたバックアップ・サーバー接続は自動的に非活動になりません。バックアップ・サーバー接続を手動で非活動にする必要があります。

ホット・スタンバイ用の実動または専用バックアップ・サーバーの使用

同じ Communications Server ライセンスを、同じネットワーク上で稼働している複数のサーバー上にインストールすることはできません。追加サーバーごとにさらに Communications Server パッケージを購入して、複数のサーバーに Communications Server をインストールしてください。

Communications Server をホット・スタンバイ用に構成する前に、 Communications Server を、実動サーバーとバックアップ・サーバーの両方として、または専用バックアップ・サーバーとして、どちらとして稼働させるかどうかを決めてください。

実動サーバーの使用

実動サーバー は、毎日の通信要件を扱う Communications Server です。この環境は、クリティカル・サーバー障害シナリオ外部で活動化されるホスト接続とともに、 Communications Server を構成します。この接続の活動化および使用には、接続のための適切なライセンスの購入が必要です。同じ Communications Server ライセンスを、複数のサーバー上にインストールすることはできません。
Communications Server を複数のシステム上で実動サーバーとして使用するには、追加サーバーのインストールごとにさらに Communications Server パッケージを購入して、複数のサーバーに Communications Server をインストールしてください。

Communications Server を実動サーバーおよびバックアップ・サーバーの両方として使用する場合は、特別なライセンス考慮事項はありません。 Communications Server、および Communications Server を実動サーバーとして使用する目的で購入したライセンスをインストールします。

バックアップ・サーバーとしての Communications Server の役割では、バックアップ・サーバーが監視するクリティカル・サーバー用に購入した基本のライセンス交付を超えた追加のライセンス交付を必要としません。バックアップ・サーバー上では、特別なライセンス考慮事項は不要です。バックアップ・サーバーはクリティカル・サーバーの障害を検出すると、クリティカル・サーバー用に構成された接続を自動的に活動化して、クリティカル・サーバーに対して有効状態のライセンスに基づいて、バックアップ・サーバーのライセンスを調整します。 Communications Server は、ユーザーが介入することなく、ホット・スタンバイ・ライセンスを管理します。

ただし、クリティカル・サーバー用に構成された接続が、クリティカル・サーバー障害シナリオ外で既に活動化されている場合は、クリティカル・サーバーのライセンスに対するバックアップ・サーバーの調整は行われず、バックアップ・サーバー上で個別のライセンスの交付が必要になります。

専用サーバーの使用

専用バックアップ・サーバーは実動サーバーとして機能せず、クリティカル・サーバー障害シナリオ以外の接続については活動化しません。このサーバー上では、スタートアップでどの接続も活動化されず、手動で活動化させることもできません。専用バックアップ・サーバーの機能は、 1 つまたは複数のクリティカル・サーバーを監視することです。

専用バックアップ・サーバーは、バックアップ・サーバーが監視するクリティカル・サーバー用に購入した基本のライセンス交付を超えた追加のライセンス交付を必要としません。 Communications Server は、ユーザーが介入することなく、ホット・スタンバイ・ライセンスを管理します。

完全なホット・スタンバイ環境の計画

ホット・スタンバイ使用のシナリオには、ある特定のホット・スタンバイ操作とともに、IP または IPX 経由の LAN ベースのエミュレーター・クライアントをサポートする、通常の Communications Server 機能シナリオが含まれています。

ホット・スタンバイ環境を構成するには、以下の 2 つの基本的な依存関係があります。

- ホスト・マシンとの互換性のある接続を提供するように、 2 つ以上の Communications Server を構成する必要があります。バックアップとして使用するサーバーは、ホスト・マシンへの 1 次接続を提供するサーバーとして、クリティカル・サーバー構成を使用して構成する必要があります。
- ホスト・マシン上でエミュレーター・セッションをユーザーに提供するために、このサーバー経由の接続に使用されるワークステーション・エミュレーター・クライアント・ソフトウェアは、クリティカル・サーバー障害発生時にバックアップ・サーバーへの代替経路指定を行ういくつかの方法をサポートする必要があります。

いくつかのエミュレーター・クライアントは、代替経路指定を提供しません。ホット・スタンバイ環境の計画には、エミュレーター・ソフトウェアの念入りな評価、およびクライアントとサーバー間で使用される接続タイプが必要になります。以下は、代替経路指定における選択項目です。

- **ホット・ロールオーバー** - この意味は、名前を指定した、連絡対象の複数サーバーを構成することに対するエミュレーター・クライアントでのサポートを示します。これは、特定の順序で、あるエミュレーター・セッションに関してこのサーバー経由でホスト・マシンへの接続を確立させるためです。ホット・ロールオーバーを使用すると、クリティカル・サーバーへの連絡が失敗した場合に、バックアップ・サーバーに連絡できるように構成できます。クリティカル・サーバーが失敗してバックアップ・サーバー上の資源が活動化している場合、エミュレーター・クライアントはバックアップ・サーバーに連絡し、そのバックアップ・サーバー経由でホスト・マシンへ接続するように代替経路を確立させます。
- **LU プール** - この意味は、エミュレーター・クライアント内にあるサポートを示しています。これにより、名前が指定されたプールで使用可能な複数 LU に対する照会に現在応答しているサーバー経由で、エミュレーター・セッション用のホスト・マシンへの接続を動的に確立させます。 LU プール・サポートにより、バックアップ・サーバーとクリティカル・サーバーは、同じプールに複数 LU を提供できます。バックアップ・サーバーは最初に定義されますが、活動状態ではありません。クリティカル・サーバーに障害が発生し、バックアップ・サーバー上の資源が活動化している場合、バックアップ・サーバーは、プールからの LU に対するエミュレーター・クライアントの要求に応答し、バックアップ・サーバー経由でホスト・マシンへ接続するように代替経路を確立させます。 LU プールには、各 LU プールごとに、以下のようなクライアント・サポートのタイプがあります。
  - 事前 SLP サポート: Communications Server SLP サポートより前は、 LU プールのクライアント・アクセスは、ランダムに行なわれるか、あるいは指定されたサーバー順序で行われました。
  - SLP サポート: Communications Server SLP サポートは、プールに関係している各サーバー全体に渡ってセッション・ロードを平衡化させて、 LU プールのクライアント・アクセスを行います。
- **複数のエミュレーター・セッション** - この意味は、複数エミュレーター・セッション構成用のエミュレーター・クライアント内のサポートを示します。ユーザーはホスト・マシンに接続するために、バックアップ・サーバーとクリティカル・サーバーを使用して、別々のセッションを構成することができます。複数エミュレーター・セッションを使用すると、ホット・ロールオーバーまたは LU プール・サポートほど容易ではありません。その理由は、この方法の場合、障害発生時に代替経路指定を使用してその支援を行うために、エミュレーター・ユーザー

による手動介入が必要となるからです。クリティカル・サーバー接続に障害が発生すると、ユーザーは、バックアップ・サーバーを使用するように構成されたセッションを手動開始して、ホスト・マシンへの接続を再確立させます。

TN3270E、TN5250、API、または QEL/MU エミュレーター・クライアント用の IBM パーソナル・コミュニケーションズ・サポートでは、 1 つ以上のホット・ロールオーバー、 LU プール、または複数のエミュレーター・セッションのオプションを通じて、代替経路指定オプションを提供します。いくつかのベンダー・エミュレーター・クライアントは、代替経路指定オプションを提供します。

バックアップ・サーバーでのホット・スタンバイの構成

「**SNA ノード構成**」拡張機能パネルで、「ホット・スタンバイのクリティカル・サーバー構成」の構成オプションを使用してバックアップ・サーバー上でホット・スタンバイを構成します。

クリティカル・サーバーではホット・スタンバイ構成を行う必要ありませんが、バックアップ・サーバーではホット・スタンバイ構成が必要です。「**SNA ノード構成**」拡張機能オプションを使用して、クリティカル・サーバー定義とともにバックアップ・サーバーを構成します。 クリティカル・サーバー定義には、バックアップ・サーバーにより監視されるクリティカル・サーバー名、およびクリティカル・サーバー障害時に活動状態になる接続名が指定されています。 複数のクリティカル・サーバー定義を構成することができます。こうすることで、バックアップ・サーバーは複数のクリティカル・サーバーのバックアップを監視し提供することができます。 バックアップ・サーバー上でクリティカル・サーバー定義を構成した後は、変更を有効にするためにバックアップ・サーバー・ノードを再始動してください。 ホット・スタンバイ構成の詳細については、オンライン・ヘルプの「**SNA Node Configuration**」を参照してください。

ホット・スタンバイ環境の構成

ホット・スタンバイ環境を構成するには、以下のステップに従ってください。

1. **クリティカル・サーバーの構成:** クリティカル・サーバーは、ホット・スタンバイ関連の構成を使用せずに構成されます。エミュレーター・クライアントと、使用する代替経路指定オプションを一致させるようにホスト接続を構成してください。
2. **バックアップ・サーバーの構成:** バックアップ・サーバー構成には、以下の 2 つの重要な概念が含まれています。
   a. バックアップ・サーバー上のホスト接続構成は、ホスト接続が手動で開始されるように構成されていることを除けば、クリティカル・サーバー上の構成と似ています。
   b. ホスト接続を定義するバックアップ・サーバー上のクリティカル・サーバー構成は、クリティカル・サーバー障害が検出されたときに開始されます。
3. **エミュレーター・クライアントの構成:** ワークステーション・エミュレーター・クライアントを構成して、サーバー提供の接続に、代替経路指定オプションを一致させます。
4. **クリティカル・サーバーとバックアップ・サーバーの各ノードの開始:** 通常どおりノードを開始してください。 **SNA ノード操作**により、クリティカル・サーバーおよびバックアップ・サーバーのホット・スタンバイ状況を検査することができます。

5. **クリティカル・サーバーの障害:** クリティカル・サーバーが失敗すると、以下のように回復作業が行われます。
   a. バックアップ・サーバー、ホスト、およびクライアント上のワークステーション・ エミュレーター・ソフトウェアが、ほとんど同時に障害を検出します。
   b. バックアップ・サーバー上のクリティカル・サーバー構成内に名前のある接続が活動化され、ホスト・マシンへの接続が確立されます。
   c. ワークステーション・エミュレーター・クライアントは、バックアップ・サーバーと新規のセッションを確立します。バックアップ・サーバーは、クリティカル・サーバー障害時にバックアップ・サーバー上で活動化された接続経由で、ホスト・マシンへセッションを経路指定します。
   d. ワークステーションは、ホスト・マシンに連絡し、ユーザー用のログオン・プロンプトを表示します。
6. **クリティカル・サーバーの回復:** クリティカル・サーバーが再び活動状態になると、新規のワークステーション・エミュレーター・セッションが、クリティカル・サーバーのホスト接続を使用します。バックアップ・サーバーを通じて経路指定された、既に開始されているワークステーション・エミュレーター・セッションは、セッションがクローズされるまで操作を続けます。

   バックアップ・サーバーのホスト接続は、手動で非活動化状態にしなければなりません。バックアップ・サーバーの接続の非活動化は、時間外に行ってください。接続を非活動化する前に、バックアップ・サーバーを使用しているワークステーション・エミュレーター・セッションのユーザーに通知してください。

ホット・スタンバイを使用しないサーバー間のバックアップ接続の計画

ホット・スタンバイは、LAN ベース IP または IPX ワークステーション・エミュレーター・セッションをサポートする環境に限定されているために、いくつかの環境では、バックアップ接続用にホット・スタンバイが使用できません。ホット・スタンバイを使用せずにバックアップ環境を計画する際の考慮事項の多くは、ホット・スタンバイを使用するバックアップ計画の場合と似ています。ホット・スタンバイを使用せずにバックアップ環境を構成するには、以下のステップに従ってください。

1. バックアップ・サーバー上で、1 次サーバーへのバックアップ・ホスト接続を提供するために、適切なライセンスを持つ別々に購入した Communications Server パッケージをインストールします。
2. バックアップ・サーバー上で、バックアップとして使用されるホスト接続を、必要に応じて活動化するように構成します。
3. 1 次サーバー障害時、バックアップ・サーバー上の資源へ自動的に経路指定を行うように、ワークステーション・エミュレーター・クライアントを構成します。ただし、経路指定は、1 次サーバー障害の検出時のみ、バックアップ・サーバーにアクセスするように限定する必要があります。
4. 両方のノードが開始されますが、アクティブなアップストリーム接続を持つ 1 次ノードのみが最初にホストへ接続します。
5. 1 次サーバー障害時、ワークステーション・エミュレーター・エミュレーターは、バックアップ・サーバー経由で引き続き接続を試行します。 バックアップ・サーバーのホスト接続は活動化されます。

6. バックアップ・サーバー上にインストールされた重複したライセンス交付により、 1 次サーバー経由で事前に経路指定されたクライアントは、バックアップ・サーバーを使用することができます。
7. 1 次サーバーが再び活動化したら、バックアップ・サーバー上の接続を手動で非活動化します。

単一サーバーでのバックアップ接続の計画

ホット・スタンバイは、複数のサーバー間でバックアップ接続を持つ環境にしか適用しないために、単一のサーバーでバックアップ接続用にホット・スタンバイを使用することはできません。ただし、単一のサーバー内でバックアップ環境を計画する際の考慮事項のいくつかは、ホット・スタンバイを使用するバックアップ計画の場合と似ています。相違点は、単一サーバーでバックアップ接続を行う以下のステップに要約されています。

1. ホストへのゲートウェイとして作動しているサーバー上で、複数の LU を同一 LU プールに提供する 1 次接続およびバックアップ接続を構成しますが、その場合、バックアップ接続が要求時対応で活動化されるように構成された状態にします。
2. LU プールを通じて接続するように、ワークステーション・エミュレーター・クライアントを構成します。
3. 1 次接続が失敗した場合、またはプール内の LU が空になった場合、プールへの接続を試行することによりバックアップ接続が活動化されます。
4. 1 次サーバーが再び活動化したら、バックアップ・サーバー上の接続を手動で非活動化します。

第 12 章 X.25 の計画

ネットワーク管理者は X.25 構成の計画を慎重に作成する必要があります。 次の事項を考慮してください。

- 公衆 PSDN を使用するには、必要な回線 (リンク) ごとにネットワークへの加入を申し込む必要があります。 回線が提供されるまでに時間がかかることがありますから、X.25 ネットワーク・プロバイダーにあらかじめ確認しなければなりません。
- X.25 ネットワークで使用可能な機能と必要な機能とを知っている必要があります。 通常、ネットワーク提供者はネットワークの技術上の手引きを提供するので、これを入手して検討してください。
- PVC および SVC に必要な論理チャネルに関する情報を集めてください。
  - 256 の論理チャネルのグループを 16 まで定義することができます。
  - グループ番号の範囲は 0 から 15 までです。
  - グループ内の論理チャネル番号は 0 から 255 までです。

    グループ番号に 256 を掛け、論理チャネル番号を加えた数は、 0 から 4095 までの範囲にあります。この数が論理チャネルを固有に識別します。 この組み合わせた数を論理チャネル番号と呼ぶことがあります。

    注:

    1. CCITT を 1984 または 1988 と指定すると、論理チャネルの最大数は 4095 です。
    2. CCITT を 1980 に指定すると、論理チャネルの最大数は 1024 です。
  - 論理チャネルのグループは着呼専用 (他の DTE からの呼び出しに予約される)、発呼専用 (他の DTE へ呼び出しに予約される)、または双方向とすることができます。
- 計画中の SNA の用途に必要なバーチャル・サーキットの数
- 必要な PVC の種類
- 着呼専用、発呼専用、および双方向論理チャネルの混用
- 必要なパケットの最大サイズと、X.25 ネットワークでサポートされているパケットのサイズ
- X.25 アプリケーション・プログラムが使用する任意選択の X.25 ファシリティーの詳細

  CCITT X.25 勧告は、ネットワークがサポートできるいくつかの任意選択ファシリティーを定義しています。

  ファシリティーによっては、発呼要求、着呼受付、および復旧要求のパケットのファシリティー・フィールドを用いて、呼設定および呼解放時にアプリケーション・プログラムが指定または折衝できるパラメーターがあります。

  X.25 接続では、呼設定時に次のファシリティーをサポートするよう構成できます。

– 閉域ユーザー・グループ
– ネットワークのユーザー ID
– パケットおよびウィンドウ・サイズのネゴシエーション
– 着信課金

これらのファシリティーは、X.25 DLC の構成中に定義してください。

- フレーム・パラメーターおよびパケット・パラメーターに関する特殊要件の詳細。 これらの構成パラメーターの省略時の値は、大半の条件に適するように慎重に選択してあります。 ただし、ネットワーク・プロバイダーが別の値を要求または推奨することがあり、

  問題を避けるために、構成パラメーターはネットワーク加入の詳細と一致させなければなりません。例えば、構成した 20 の SVC 論理チャネルのうち 10 しか加入していない場合、 11 番目の論理チャネルを使用しようとすると、DCE はエラー状態を検出します。

可能な X.25 接続

図 36 は、X.25 ネットワークが SNA ゲートウェイからホストへの接続を提供する方法を示しています。

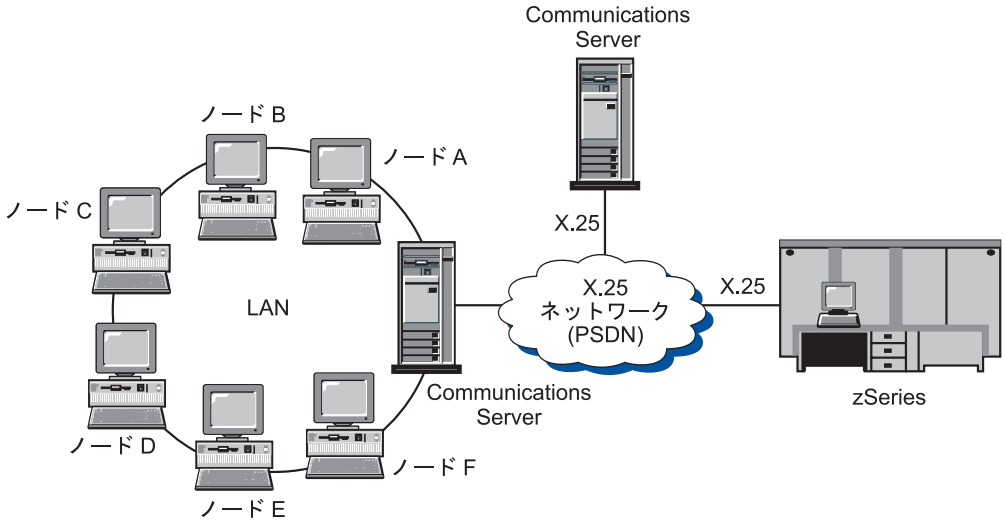

図 36. X.25 および SNA ゲートウェイの接続性

X.25 ネットワーク課金

実際の課金は X.25 ネットワーク提供者が採用している請求方式によって異なりますが、通常、課金には次の要素の一部または全部が含まれます。

- 加入料

  X.25 ネットワークに初めて加入するときの一回払いの加入料。

- 定期払いレンタル料

この課金は、ネットワーク提供者が提供するファシリティーによって決まります。 例えば、加入したオプションのネットワーク・ファシリティーごとに課金されることがあります。また、使用可能な論理チャネルごとに課金されることがあります。 PVC は専用ネットワーク資源を必要とするため、SVC より料金が高くなるのが普通です。

- 使用料

  この課金は、ネットワークと論理的に接続している時間の長さに応じて決まりますが、基本料金によって異なることもあります。

- 従量使用料

  この課金は、請求対象となる期間中にネットワークを通して伝送されたデータの量により異なります。

第 13 章 ホスト接続の構成

Communications Server を実行しているワークステーションを、zSeries (システム /370 を含む) または iSeries ホストへ接続することができます。Communications Server 構成に指定する値の多くは、ホストを構成する際にも使用されます。この章では、Communications Server 構成時に指定する構成パラメーターとホストで指定するパラメーターとの間のマッピングについて説明します。この章ではまた、パラメーターをリストしたテーブルを記載してあります。これを使用して、Communications Server とホスト間で発行される各マクロ上の共通パラメーターを除去できます。

注: LINE、PU、および LU マクロから発行された多くの NCP パラメーターを、読みやすく、またコーディングしやすいように GROUP マクロ内に指定することができます。このパラメーターを一致させることにより、共通パラメーターを次のマクロごとに含める必要がなくなりますが、必要に応じてオーバーライドすることができます。

VTAM および Communications Server を使用した NCP トークンリング (NTRI)

表 7 では、 IBM トークンリング・ネットワーク接続用の、ホスト・パラメーターと Communications Server パラメーターを比較しています。

表 7. ホスト /PC パラメーター相互参照: IBM トークンリング・ネットワーク NTRI 定義

NTRI/NCP	Communications Server プロファイル/パラメーター	注釈
GROUP ECLTYPE = PHY	DLC タイプ: LAN	
LINE LOCADDR	構成接続 LAN **宛先アドレス**	Communications Server においてこのパラメーターに設定される値は、ホスト制御装置内の IBM トークンリング・ネットワーク・アダプターのアドレスでなければなりません。

VTAM 交換回線ネットワークおよび Communications Server を使用したトークンリング

表 8 では、ホスト・パラメーターと Communications Server パラメーター (VTAM 交換回線ネットワークを使用した IBM トークンリング・ネットワーク接続用パラメーター) の比較を記載してあります。

表 8. ホスト /PC パラメーター相互参照: IBM トークンリング・ネットワーク VTAM 交換回線ネット

VTAM	Communications Server プロファイル/パラメーター	注釈
IDBLK=	構成ノード ローカル・ノード ID **ブロック ID**	ホスト IDBLK は、**ローカル・ノード ID** の 16 進文字のうちの最初の 3 文字と一致させなければなりません。Communications Server 用のデフォルトは X'05D' です。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
IDNUM=	構成ノード ローカル・ノード ID **物理装置 ID**	ホスト IDNUM は、**ローカル・ノード ID** の 16 進文字のうち、最後の 5 文字を一致させる必要があります。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
CPNAME=	ノード定義 構成ノード **完全修飾 CP 名 (第 2 フィールド)**	交換回線を使用している際はこのパラメーターを指定し、IDBLK= および IDNUM= を使用している際は省略します。
LOCADDR	ホスト LU の構成 **NAU アドレス**	これらのパラメーターは、同じ値を持つ必要があります。独立 LU の場合、VTAM では LOCADDR=0 をコーディングする代わりに CDRSC 定義の作成または DYNLU オペランドの使用をお勧めします。独立 LU の CDRSC 定義のコーディングについて詳しくは、「VTAM Network Implementation Guide」を参照してください。 SDDLU または動的定義が VTAM 3.4 またはそれ以降で独立 LU に使用される場合は、従属 LU 用にホスト定義は必要ありません。

表 8. ホスト /PC パラメーター相互参照: IBM トークンリング・ネットワーク VTAM 交換回線ネット (続き)

MAXDATA	構成 LAN 装置 **最大 PIU サイズ** (265-62235)	これらの値は、一致させる必要はありません。
MAXOUT	構成 LAN 装置 **受信バッファー数** (2-64)	Communications Server の**受信バッファー数**は、ホストの MAXOUT パラメーターと等しくなければなりません。

9370 IBM トークンリング・ネットワーク・アダプターおよび Communications Server

表 9 では、ホスト・パラメーターと Communications Server パラメーター (VTAM 交換回線ネットワークを使用した IBM トークンリング・ネットワーク接続用パラメーター) の比較を記載してあります。

表 9. ホスト /PC パラメーター相互参照: IBM トークンリング・ネットワーク 9370 VTAM LAN

VTAM	**Communications Server プロファイル/パラメーター**	**注釈**
VBUILD TYPE=LAN	DLC タイプ: LAN	
PORT MACADDR=	構成接続 LAN **宛先アドレス**	Communications Server カスタマイズ中で指定する宛先アドレスは、 9370 IBM トークンリング・アダプターのアドレスでなければなりません。
PORT SAPADDR=04	構成接続 LAN **リモート SAP**	これらの値は一致させる必要があります。
ADDR=04 (発信のみ)	構成接続 LAN **ローカル SAP**	これらの値は一致させる必要があります。

VTAM 交換回線ネットワークおよび Communications Server を使用したイーサネット

表 10 では、 VTAM 交換回線ネットワークを使用したイーサネット・ネットワーク接続用の、ホスト・パラメーターと Communications Server パラメーターを比較します。

表 10. ホスト /PC パラメーター相互参照: イーサネット・ネットワーク VTAM 交換回線ネットワーク

VTAM	**Communications Server プロファイル/パラメーター**	**注釈**

表 10. ホスト /PC パラメーター相互参照: イーサネット・ネットワーク VTAM 交換回線ネットワーク (続き)

IDBLK	構成ノード ローカル・ノード ID **ブロック ID**	ホスト IDBLK は、**ローカル・ノード ID** の 16 進文字のうちの最初の 3 文字と一致させなければなりません。 Communications Server 用のデフォルトは X'05D' です。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
IDNUM	構成ノード ローカル・ノード ID **物理装置 ID**	ホスト IDNUM は、**ローカル・ノード ID** の 16 進文字のうち、最後の 5 文字を一致させる必要があります。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
CPNAME	ノード定義 構成ノード **完全修飾 CP 名** (第 2 フィールド)	交換回線を使用している際はこのパラメーターを指定し、IDBLK= および IDNUM= を使用している際は省略します。
LOCADDR	ホスト LU の構成 **NAU アドレス**	これらのパラメーターは、同じ値を持つ必要があります。独立 LU の場合、VTAM では LOCADDR=0 をコーディングする代わりに CDRSC 定義の作成または DYNLU オペランドの使用をお勧めします。独立 LU の CDRSC 定義のコーディングについて詳しくは、「*VTAM Network Implementation Guide*」を参照してください。 VTAM 3.4 (またはそれ以降) の独立 LU 用に SDDLU または動的定義が使用されている場合には、従属 LU 用にホスト定義は必要ありません。
MAXDATA	構成 LAN 装置 **NAU アドレス** (265-65535)	これらの値は、一致させる必要はありません。
MAXOUT	構成 LAN 装置 **NAU アドレス** (2-64)	Communications Server の受信バッファー数は、ホストの MAXOUT パラメーターと等しくなければなりません。

VTAM/NCP および Communications Server (SDLC)

表 11 では、VTAM/NCP ホスト・パラメーターを、 SDLC 接続用の Communications Server パラメーターと比較します。

表 11. ホスト /PC パラメーター相互参照: SDLC

VTAM/NCP	Communications Server プロファイル/パラメーター	注釈
NETID=	構成ノード **完全修飾 CP 名** (第 1 フィールド)	このパラメーターは、専用回線と交換回線の両方に使用できます。これは、Communications Server を使用して接続する SNA ネットワークを識別します。
NAME PU		常に NAME PU を使用します。制御点の LU を定義するために、この PU 名をローカル CP 名と同じ名前にしてはなりません。
IDBLK=	構成ノード ローカル・ノード ID **ブロック ID**	ホスト IDBLK は、**ローカル・ノード ID** の 16 進文字のうちの最初の 3 文字と一致させなければなりません。 Communications Server 用のデフォルトは X'05D' です。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
IDNUM=	構成ノード ローカル・ノード ID **物理装置 ID**	ホスト IDNUM は、ローカル・ノード ID の 16 進文字のうち、最後の 5 文字を一致させる必要があります。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
CPNAME	ノード定義 構成ノード **完全修飾 CP 名** (第 2 フィールド)	交換回線を使用している際はこのパラメーターを指定し、 IDBLK= および IDNUM= を使用している際は省略します。
LNCTL=SDLC	DLC タイプ= SDLC-WAC、SDLC-MPA、COM ポート (使用ハードウェアによる)	SDLC をここで選択する必要があります。このパラメーターは、専用回線と交換回線の両方に使用されます。

表 11. ホスト /PC パラメーター相互参照: SDLC (続き)

LOCADDR	ホスト LU の構成 **NAU アドレス**	これらのパラメーターは、同じ値を持つ必要があります。独立 LU の場合、VTAM では LOCADDR=0 をコーディングする代わりに CDRSC 定義の作成または DYNLU オペランドの使用をお勧めします。独立 LU の CDRSC 定義のコーディングについて詳しくは、「VTAM Network Implementation Guide」を参照してください。 VTAM 3.4 (またはそれ以降) の独立 LU 用に SDDLU または動的定義が使用されている場合には、従属 LU 用にホスト定義は必要ありません。
NRZI=YES/NO	構成接続 SDLC-WAC、SDLC-MPA、COM ポート **NRZI 符号化**	Communications Server は、USE_NRZI_ENCODING=0 および USE_NRZI_ENCODING=1 を使用します。 これらのパラメーターは、モデム・タイプ : Synchronous Switched、Synchronous Non-Switched、および AutoSync の PCM 上にのみ検出されます。 コード化体系の NRZI または NRZ は、接続の両端では同じ方法で構成されていなければなりません。コード化体系が同じでない場合は、モデムは接続されますがデータ転送は正常に行われず、接続は、リンク・レベル・タイムアウト (一般には 40 秒) 後に Communications Server により切断されます。 IBM 広域コネクターを使用して X.25 に接続する場合は、NRZ コード化体系をお勧めします。

表 11. ホスト /PC パラメーター相互参照: SDLC (続き)

DUPLEX=FULL/ HALF	構成接続 SDLC-WAC および COM ポートのみ **全二重通信**	それぞれのサイドで設定される値は、モデム・タイプおよび構成と整合させる必要があります。このパラメーターは、専用回線と交換回線の両方に使用されます。
(TRANSFER * BFRS) -47	構成装置 SDLC-WAC、SDLC MPA、COM ポートのみ **最大 PIU** (265-4105)	I フィールド・サイズの最大値は、ホストで指示される (TRANSFR * BFRS) - 47 の値より小さいか、または等しくなければなりません。このパラメーターは、専用回線と交換回線の両方に使用されます。
MAXDATA=	構成装置 SDLC-WAC、SDLC MPA、COM ポートのみ **最大 PIU** (265-4105)	これらの値は、一致させる必要はありません。 このパラメーターは、専用回線と交換回線の両方に使用されます。最も低い値が使用されます。
MAXOUT=	構成装置 SDLC-WAC、SDLC MPA、COM ポートのみ **最大 PIU** (265-4105)	Communications Server の**受信ウィンドウ数**は、ホストの MAXOUT パラメーターと等しくなければなりません。 このパラメーターは、専用回線と交換回線の両方に使用されます。
ADDR	構成装置 SDLC-WAC、SDLC MPA、COM ポートのみ **リンク局アドレス** (01-FE)	これらのパラメーターは、同じ値を持つ必要があります。 Communications Server および VTAM/NCP については、16 進数でコード化されています。このパラメーターは、専用回線と交換回線の両方に使用されます。

VTAM および Communications Server (APPC)

表 12 では、VTAM ホスト・パラメーターを、 APPC 接続用の Communications Server パラメーターと比較します。

表 12. ホスト /PC パラメーター相互参照: APPC

VTAM	Communications Server プロファイル/パラメーター	注釈

表 12. ホスト /PC パラメーター相互参照: APPC (続き)

LUNAME	ホスト LU の構成 **ローカル LU 名** または 構成ノード **完全修飾 CP 名** (第 2 フィールド)	
LOCADDR	ホスト LU の構成 **NAU アドレス**	これらのパラメーターは、同じ値を持つ必要があります。 独立 LU の場合、VTAM は、LOCADDR=0 をコーディングする代わりに、 CDRSC 定義の作成または DYNLU オペランドの使用を推奨します。 独立 LU の CDRSC 定義のコーディングについて詳しくは、「VTAM Network Implementation Guide」を参照してください。 SDDLU または動的定義が VTAM 3.4 またはそれ以降で独立 LU に使用される場合は、従属 LU 用にホスト定義は必要ありません。
NETID APPL	構成パートナー LU 6.2 **パートナー LU 名**	
VTAM 解釈テーブル	構成パートナー LU 6.2 **パートナー LU 名**	これは、従属 LU の場合のみです。
LOGMODE テーブル LOGMODE=	構成モード **モード名**	これらのパラメーターは一致させる必要があります。
LOGMODE テーブル RUSIZES=	構成モード **最大 RU サイズ** (256-32767)	最終的な値はネゴシエーションされる。

VTAM および Communications Server (MPC)

表 13 および 157 ページの表 14 では、IOCP/HCD および VTAM ホスト・パラメーターを、マルチパス・チャネル (MPC) 接続用の Communications Server パラメーターと比較します。

表 13. IOCP/HCD パラメーター相互参照: MPC

IOCP/HCD	**Communications Server プロファイル/パラメーター**	**注釈**
IOCP IODEVICE UNIT=SCTC	DLC タイプ: IBM-MPC	
HCD 装置タイプ SCTC	DLC タイプ: IBM-MPC	

表 14. VTAM パラメーター相互参照: MPC

VTAM 定義ステートメント	**オペランド**	**Communications Server プロファイル/パラメーター**	**注釈**
VBUILD,TYPE=TRL			
	LNCTL=MPC	DLC タイプ: IBM-MPC	
	MPCLEVEL=HPDT		Communications Server IBM-MPC 接続には HPR/HPDT が必要
	MAXBFRU	MPC DLC の構成 **最大 PIU サイズ**	パフォーマンスまたは VTAM 使用記憶域、もしくはその両方に影響を及ぼす場合があります。
	MAXREADS	MPC DLC の構成 **受信バッファー・カウント**	パフォーマンスまたは VTAM 使用記憶域、もしくはその両方に影響を及ぼす場合があります。
	READ	MPC DLC の構成	VTAM READ IODEVICE アドレスのリストは、 READ サブチャネルの Communications Server MPC DLC リストに一致しなければなりません。
	WRITE	MPC DLC の構成	VTAM READ IODEVICE アドレスのリストは、 WRITE サブチャネルの Communications Server MPC DLC リストに一致しなければなりません。
VBUILD,TYPE=LOCAL			

表 14. VTAM パラメーター相互参照: MPC (続き)

VTAM 定義ステートメント	オペランド	Communications Server プロファイル/パラメーター	注釈
	CONNTYPE=APPN	構成接続 IBM-MPC **APPN サポート**	Communications Server IBM-MPC 接続には APPN が必要
	XID=YES	構成接続 IBM-MPC **APPN サポート**	Communications Server IBM-MPC 接続には PU2.1 が必要
	CP-CP=YES	構成接続 IBM-MPC **APPN**	Communications Server IBM-MPC 接続には APPN が必要
	HPR=YES	構成接続 IBM-MPC **HPR サポート**	Communications Server IBM-MPC 接続には HPR が必要
	NN	構成ノード **ノード・タイプ**	VTAM PU ノード・タイプは、Communications Server 定義と一致させる必要があります。
	DELAY		パフォーマンスまたは VTAM の CPU 使用、もしくはその両方に影響を及ぼす場合があります。

ES/9000® および Communications Server (SDLC)

表 15 では、9370 情報システム・パラメーターを SDLC 接続用の Communications Server パラメーターと比較します。

表 15. ホスト /PC パラメーター相互参照: SDLC 経由の 9370 情報システム

9370/VTAM	Communications Server プロファイル/パラメーター	注釈
QFI: 非ゼロ復帰反転 (マイクロコード構成)	構成接続 SDLC-WAC、SDLC-MPA、COM ポート **NRZI 符号化**	これらのパラメーターは一致させる必要があります。 このパラメーターは、専用回線と交換回線の両方に使用されます。 Communications Server は、USE_NRZI_ENCODING=0 および USE_NRZI_ENCODING=1 を使用します。これは、同期データ・ストリームです。

表 15. ホスト /PC パラメーター相互参照: SDLC 経由の 9370 情報システム (続き)

QFI: プロトコル (マイクロコード構成) VTAM: GROUP LNCRL=SDLC	DLC タイプ SDLC-WAC、SDLC-MPA、COM ポート	マイクロコードと VTAM パラメーターは、一致させる必要があります。このパラメーターは、専用回線と交換回線の両方に使用されます。
MAXDATA	構成装置 SDLC-WAC、SDLC-MPA、COM ポート **最大 PIU サイズ** (265-4105)	これらの値は、一致させる必要はありません。 このパラメーターは、専用回線と交換回線の両方に使用されます。
MAXBFRU * IOBUF サイズ	構成パートナー LU 6.2 SDLC-WAC、SDLC-MPA、COM ポート **最大 PIU サイズ** (265-4105)	I フィールド・サイズの最大値は、ホストで指示される IOBUF サイズに MAXBFRU を乗じた値と、等しいかそれより小さくなければなりません。このパラメーターは、専用回線と交換回線の両方に使用されます。
MAXOUT=	構成装置 **受信ウィンドウ数** (1-30)	Communications Server の**受信ウィンドウ数**は、ホストの MAXOUT パラメーターと等しくなければなりません。 このパラメーターは、専用回線と交換回線の両方に使用されます。
ADDR=	構成装置 **リンク局アドレス** (01-FE)	これらのパラメーターに設定された値は、一致させる必要があります。このパラメーターは、専用回線と交換回線の両方に使用されます。
IDBLK=	構成ノード ローカル・ノード ID **ブロック ID**	ホスト IDBLK は、**ローカル・ノード ID** の 16 進文字のうちの最初の 3 文字と一致させる必要があります。Communications Server 用のデフォルトは X'05D' です。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
IDNUM=	構成ノード ローカル・ノード ID **物理装置 ID**	ホスト IDNUM は、**ローカル・ノード ID** の 16 進文字のうち、最後の 5 文字を一致させる必要があります。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。

表 15. ホスト /PC パラメーター相互参照: SDLC 経由の 9370 情報システム (続き)

CPNAME=	構成ノード **完全修飾 CP 名** (第 2 フィールド)	交換回線を使用している際はこのパラメーターを指定し、IDBLK= または IDNUM= を使用している際は省略します。
LOCADDR	ホスト LU の構成 **NAU アドレス**	LOCADDR および NAU パラメーターは、同じ値を持つ必要があります。独立 LU の場合、VTAM では LOCADDR=0 をコーディングする代わりに CDRSC 定義の作成または DYNLU オペランドの使用をお勧めします。独立 LU の CDRSC 定義のコーディングについて詳しくは、「*VTAM Network Implementation Guide*」を参照してください。このパラメーターは、専用回線と交換回線の両方に使用されます。

Host および Communications Server (DLUR)

表 16 では、VTAM の DLUR への接続用の、ホストおよび Communications Server のパラメーターを比較します。

表 16. VTAM Communications Server パラメーター相互参照: DLUR 使用

VTAM	Communications Server	注釈
IDBLK=	構成 DLUR PU **ブロック ID**	IDBLK はノード ID の 16 進文字のうち最初の 3 桁が一致していなければなりません。このノード ID のデフォルトは Communications Server の場合、X'05D' です。このパラメーターは、CPNAME= を使用していないときに指定してください。
IDNUM=	構成 DLUR PU **物理装置 ID**	ホスト IDNUM はノード ID の 16 進文字のうち、最後の 5 文字が一致していなければなりません。このパラメーターは、CPNAME= を使用していないときに指定してください。

表 16. VTAM Communications Server パラメーター相互参照: DLUR 使用 (続き)

CPNAME=	構成 DLUR PU **PU 名**	CPNAME は、ローカル PU 名と一致させる必要があります。このパラメーターは、IDNUM= および IDBLK= を使用していないときに指定してください。

表 17 は、ホストからワークステーションへの接続を確立する時に使用する PATH ステートメントの、以下のパラメーターをリストしたものです。

表 17. VTAM と Communications Server DLUR パラメーターが一致している、ホストからワークステーションへの接続

VTAM	Communications Server	注釈
DLURNAME=	構成 DLUR **完全修飾 CP 名** (第 2 フィールド)	DLURNAME は、DLUR PU を持つ DLUR ノード名を提供します。Communications Server の場合、これは完全修飾 CP 名です。
DLCADDR= (1,C,INTPU)		DLURNAME は、DLUR PU を持つ DLUR ノード名を提供します。Communications Server の場合、これは完全修飾 CP 名です。
DLCADDR= (2,X,zzzzzzzz)	構成 DLUR PU **ブロック ID および物理装置 ID**	DLCADDR=(2,X,zzzzzzzz) の中の zzzzzzzz はノード ID と一致させる必要があります。このパラメーターは、DLCADDR=(3,C,puname) を使用しない場合に指定します。
DLCADDR= (3,C,puname)	構成 DLUR PU **PU 名**	DLCADDR=(3,C,puname) の中の PU 名は、ローカル PU 名と一致させる必要があります。このパラメーターは、DLCADDR=(2,X,zzzzzzzz) を使用していないときに指定してください。

NPSI および Communications Server (X.25)

Communications Server X.25 サポートを使用すると、SNA フレームの X.25 ネットワークへの伝送が使用可能になります。 X.25 は、SNA フレームを生データとして扱い、SNA フレームをデータ内のデータのパケットとして伝送します。この 2 つのネットワーク・ノードは、直接接続はしていませんが、両方とも中継呼び出しさ

れる、パケット交換データ網 (PSDN) と接続しています。X.25 ネットワークには、X.25 接続の一部を持たせることができます。

PSDN と対話し、SNA データをパケットにまとめて、そのデータをそのまま抽出するソフトウェアは、Communications Server の不可欠な一部分となっています。S/370 のホスト・サイドでは、X.25 ファンクションは、 X.25 ネットワーク制御プログラム・パケット交換インターフェース (NPSI) と呼ばれる、独立したソフトウェア・プロダクトにより、ハンドルされます。NPSI 定義は、 NCP に従って生成され、また、NPSI ソフトウェアは NCP と同調して、同じ 3705、3725、3720、または 3745 制御装置で実行されます。

Communications Server および NPSI に指定される大部分の X.25 パラメーターは、2 つのノード間によってではなく、ユーザーおよび X.25 ネットワーク・プロバイダーによって同意された値をとります。例えば、専用回線上の SDLC 接続により、ホスト制御装置 (NCP) は特定の 2 次アドレスをポーリングするように構成されます。 Communications Server は、Communications Server ワークステーションとホスト間の物理リンク上のそのアドレスに応答するように構成されます。

X.25 上での NPSI 接続

表 18 では、X.25 上での NPSI 接続用の、ホストおよび Communications Server パラメーターを比較します。

表 18. ホスト /PC パラメーター相互参照: X.25 での NPSI 接続

NPSI	Communications Server プロファイル/パラメーター	注釈
X25.LINE TYPE=	DLC タイプ X.25 COM ポート、X.25-WAC	PVC には **TYPE=P** を、また、NPSI X.25 回線定義用の SVC には **TYPE=S** を指定します。
CALL= (type = S の場合のみ)	DLC タイプ X.25 COM ポート、X.25-WAC **バーチャル・サーキットの範囲**	バーチャル・サーキットの範囲は、ユーザーの X.25 ネットワーク加入に対応するものでなければなりません。
MAXDATA=	構成装置 X.25 COM ポート、X.25-WAC **最大 PIU サイズ** (256-4105)	これらの値は、一致させる必要はありません。
VWINDOW	構成装置 X.25 COM ポート、X.25-WAC **ウィンドウ・サイズ** (1-7)	**SVC/PVC ウィンドウ・サイズは、** X.25 加入と一致させる必要があります。
MWINDOW	構成装置 X.25 COM ポート、X.25-WAC **ウィンドウ・サイズ** (1-7)	

表 18. ホスト /PC パラメーター相互参照: X.25 での NPSI 接続 (続き)

FRMLGTH	構成装置 X.25 COM ポート、X.25-WAC フレーム順序 **モジュロ**	ホストの **FRMLGTH** 値は、モジュロ 8 の実行時には少なくとも MAXPKT +3 、またはモジュロ 128 の実行時には少なくとも MAXPKT +4 でなければなりません。ホストおよび Communications Server のモジュロ・サイズ、およびパケット・サイズは、ユーザーの X.25 加入と一致させる必要があります。 MAXPKTL 構成装置 X.25 COMポート、X.25-WAC パケット・サイズ、ホスト SVC/PVC
MAXPDTL	構成装置 X.25 COM ポート、X.25-WAC **パケット・サイズ**	ホストの **SVC/PVC パケット・サイズ**は、X.25 加入値と一致させる必要があります。

VTAM/NCP および Communications Server (X.25)

表 19 では、ホストおよび Communications Server の X.25 (VTAM/NCP) 用パラメーターを比較します。

表 19. ホスト /PC パラメーター相互参照: X.25 (VTAM/NCP)

VTAM/NCP	**Communications Server プロファイル/パラメーター**	**注釈**
NETID=	構成ノード **完全修飾 CP** 名 (第 1 フィールド)	これは、Communications Server を使用して接続する SNA ネットワークを識別します。
PU NAME		常に PU 名を使用します。制御点の LU を定義するために、この PU 名をローカル CP 名と同じにしてはいけません。
IDBLK=	構成ノード ローカル・ノード ID **ブロック ID**	**ローカル・ノード ID** の 16 進文字の最初の 3 文字。Communications Server に対するデフォルトは X'05D' です。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。

表 19. ホスト /PC パラメーター相互参照: X.25 (VTAM/NCP) (続き)

IDNUM=	構成ノード ローカル・ノード ID **物理装置 ID**	ホスト IDNUM は、**ローカル・ノード ID** の 16 進文字のうち、最後の 5 文字を一致させる必要があります。交換回線を使用している際はこのパラメーターを指定し、または CPNAME= を使用している際は省略します。
CPNAME=	構成ノード **完全修飾 CP 名** (第 2 フィールド)	交換回線を使用している際はこのパラメーターを指定し、IDBLK= および IDNUM= を使用している際は省略します。
(TRANSFR * BFRS) - 47	構成装置 X.25 COM ポート、 X.25-WAC **最大 PIU サイズ** (265-4105)	**最大 PIU サイズ**は、ホストで設定された値と等しくする必要があります。
MAXDATA	構成装置 X.25 COM ポート、 X.25-WAC **最大 PIU サイズ** (265-4105)	これらの値は、一致させる必要はありません。
LOCADDR	ホスト LU の構成 **NAU アドレス**	これらのパラメーターは、同じ値を持つ必要があります。独立 LU の場合、VTAM では LOCADDR=0 をコーディングする代わりに CDRSC 定義の作成または DYNLU オペランドの使用をお勧めします。独立 LU の CDRSC 定義のコーディングについて詳しくは、「*VTAM Network Implementation Guide*」を参照してください。 VTAM 3.4 (またはそれ以降) の独立 LU 用に SDDLU または動的定義が使用されている場合には、従属 LU 用にホスト定義は必要ありません。

APPC over X.25

表 20 は、X.25 によりホストと接続している拡張プログラム間通信機能 (APPC) を実行する、 Communications Server ワークステーション用のパラメーターと一致させます。

表 20. ホスト /PC パラメーター相互参照: X.25 によりホストに接続する IBM トークンリング・ネットワーク上の APPC

NCP	Communications Server プロファイル/パラメーター	注釈
LU NAME	構成ローカル LU 6.2 **ローカル LU 名** または 構成ノード **完全修飾 CP 名** (第 2 フィールド)	
LOCADDR	ホスト LU の構成 **NAU アドレス**	これらのパラメーターは、同じ値を持つ必要があります。独立 LU の場合、VTAM では LOCADDR=0 をコーディングする代わりに CDRSC 定義の作成または DYNLU オペランドの使用をお勧めします。独立 LU の CDRSC 定義のコーディングについて詳しくは、「*VTAM Network Implementation Guide*」を参照してください。 VTAM 3.4 (またはそれ以降) の独立 LU 用に SDDLU または動的定義が使用されている場合には、従属 LU 用にホスト定義は必要ありません。
NETID APPL	構成パートナー LU 6.2 **パートナー LU 名**	
VTAM 解釈テーブル	構成パートナー LU 6.2 **パートナー LU 名**	これは従属 LU の場合のみです。
LOGMODE テーブル LOGMODE=	構成モード **モード名**	これらの値は一致させる必要があります。

iSeries ホスト回線定義

iSeries ホスト回線定義には、 Communications Server パラメーターと一致させる OS/400 ホスト・プログラム・パラメーターが含まれています。表 21 は、 SDLC 回線パラメーターを内容としています。

表 21. iSeries Communications Server パラメーター相互参照: OS/400 ホスト・プログラム回線定義

OS/400	Communications Server プロファイル/パラメーター	注釈
NRZI= データ符号化	構成装置 SDLC-WAC、SDLC-MPA、COM ポート **NRZI 符号化**	Communications Server は、USE_NRZI_ENCODING=0 および USE_NRZI_ENCODING=1 を使用します。 これらのパラメーターは、モデム・タイプ : Synchronous Switched、 Synchronous Non-Switched、および AutoSync の PCM 上にのみ検出されます。
モデム・データ転送率選択	構成装置 COM ポートのみ **構成モデム**	モデム接続タイプ (非同期交換回線) の双方のシステムでのパラメーターは、一致していなければなりません。
最大フレーム・サイズ (MAXFRAME)	構成装置 SDLC-WAC、SDLC-MPA、COM ポート **受信ウィンドウ数** (1-30)	非同期専用回線の値は、一致させる必要はありません。
最大未処理フレーム (MAXOUT)	構成装置 SDLC-WAC、SDLC-MPA、COM ポート **受信ウィンドウ数** (1-30)	Communications Server の受信ウィンドウ数は、 iSeries ホストの MAXOUT パラメーターと等しくなければなりません。

iSeries ホスト制御装置定義

iSeries ホスト制御装置の定義には、 Communications Server パラメーターと一致させる OS/400 ホスト・プログラム・パラメーターが含まれています。

表 22 は、OS/400 ホスト・プログラム・パラメーターを示しています。

表 22. iSeries Communications Server パラメーター相互参照: 制御装置パラメーター

OS/400	Communications Server プロファイル/パラメーター	注釈

表 22. iSeries Communications Server パラメーター相互参照: 制御装置パラメーター (続き)

Linktype: *SDLC	DLC タイプ SDLC-WAC、SDLC-MPA、 COM ポート	双方のシステムにあるリンク・タイプは一致させる必要があります。このパラメーターは回線記述中にあり、記述を完全なものにするためのものです。
付加専用回線	DLC タイプ SDLC-WAC、SDLC-MPA、 COM ポート **交換回線**	このパラメーターは専用回線接続用です。この値は、事前定義のホスト回線定義と一致させる必要があります。
交換回線リスト	(なし)	このパラメーターは、交換回線接続用です。この値は、事前定義のホスト回線定義と一致させる必要があります。
最大フレーム・サイズ	構成装置 SDLC-WAC、SDLC-MPA、 COM ポート **最大 PIU サイズ** (265-4105)	これらの値は、一致させる必要はありません。
リモート・ネットワーク識別子	構成ノード **完全修飾 CP 名** (第 1 フィールド)	これらの値は一致させる必要があります。
リモート制御点名	構成ノード **完全修飾 CP 名** (第 2 フィールド)	これらの値は一致させる必要があります。
データ・リンク・ロール	構成接続 SDLC-WAC、SDLC-MPA、 COM ポート **リンク・ステーション・ロール**	双方のシステムにあるパラメーターは互いに補完します。ホスト・ロールがプライマリーである場合は、 Communications Server ワークステーションは、セカンダリーまたはネゴシエーション可能として構成される必要があります。分岐 (*MP) が使用されない場合は、データ・リンク・ロールをネゴシエーション可能 (*NEG) に設定します。
局アドレス	構成接続 SDLC-WAC、SDLC-MPA、 COM ポート **リンク局アドレス** (01-FE)	これらの値は一致させる必要があります。
APPN CP セッション・サポート: (はい/いいえ)	構成接続 SDLC-WAC、SDLC-MPA、 COM ポート **APPN サポート**	CP-CP セッションが必要であれば、これらの値は一致させる必要があります。

表 22. iSeries Communications Server パラメーター相互参照: 制御装置パラメーター (続き)

APPN ノード・タイプ:	構成接続 SDLC-WAC、SDLC-MPA、COM ポート **隣接 CP タイプ**	これらの値は一致させる必要があります。

iSeries ホスト装置定義

Communications Server ワークステーションが以前に定義されたデバイス定義を持たないで接続する場合は、 iSeries ホストは、デバイス定義を作成することができます。

表 23 に、OS/400 ホスト・プログラム・パラメーターを示します。

表 23. iSeries Communications Server パラメーター相互参照: 装置パラメーター

OS/400	Communications Server プロファイル/パラメーター	注釈
リモート・ロケーション名	構成ローカル LU 6.2 **ローカル LU 名** または 構成ノード **完全修飾 CP 名** (第 2 フィールド)	これらの値は一致させる必要があります。
付加制御装置	(なし)	このパラメーターは専用回線接続用です。この値は、事前定義のホスト回線定義と一致させる必要があります。
ローカル・ロケーション名		提供されたデフォルトを使用します。
リモート・ネットワーク識別子	構成ノード **完全修飾 CP 名** (第 1 フィールド)	提供されたデフォルトを使用します。
モード	構成モード **モード名**	提供されたデフォルトを使用します。

iSeries ホスト回線記述および Communications Server

表 24 に、iSeries ホスト・プログラム回線記述を示します。

表 24. ホスト /PC パラメーター相互参照: 回線記述

OS/400	Communications Server プロファイル/パラメーター	注釈
ローカル・アダプター・アドレス:	構成ローカル LU 6.2 **LAN 宛先アドレス**	通信を行うには、2 つのアドレスを一致させる必要があります。

iSeries ホスト制御装置記述および Communications Server

表 25 に、OS/400 ホスト・プログラム制御装置記述を示します。

表 25. ホスト /PC パラメーター相互参照: 制御装置記述

OS/400	Communications Server プロファイル/パラメーター	注釈
アクティブ交換回線	(なし)	このパラメーターは専用回線接続用です。この値は、事前定義のホスト回線定義と一致させる必要があります。
リモート制御点	構成ノード **完全修飾 CP 名** (第 2 フィールド)	名前を一致させる必要があります。
リモート・ネットワーク識別子	構成ノード **完全修飾 CP 名** (第 1 フィールド)	iSeries ローカル・ネットワーク ID と異なる場合は、デフォルトを使用するか、またはパラメーターを一致させます。
モデル制御装置記述		iSeries が接続ネットワークを使用する場合は、このパラメーターを YES にしなければなりません。
接続ネットワーク ID および接続ネットワーク CP 名	構成接続ネットワーク **接続ネットワーク名**	これらの値は、接続ネットワークに参加するすべてのノードに対して一致させる必要があります。

iSeries ホスト回線定義 (X.25)

iSeries ホスト回線定義には、 Communications Server パラメーターと一致させる OS/400 ホスト・プログラム・パラメーターが含まれています。表 26 に、X.25 回線パラメーターを示します。

表 26. iSeries Communications Server パラメーター相互参照: OS/400 ホスト・プログラム回線定義 (X.25)

OS/400	Communications Server プロファイル/パラメーター	注釈
ローカル・ネットワーク・アドレス	構成装置 **ローカル・アドレス**	通常は、両方のアドレスともネットワーク・プロバイダーが決定します。
接続タイプ	構成装置 X.25-COM ポート X.25-WAC **交換回線**	両方のシステムの結合タイプは、一致させる必要があります。
X.25 DCE	N/A	通常は、両方のアドレスともネットワーク・プロバイダーが決定します。

表 26. iSeries Communications Server パラメーター相互参照: OS/400 ホスト・プログラム回線定義 (X.25) (続き)

最大フレーム・サイズ	構成装置 X.25-COM ポート X.25-WAC **最大 PIU サイズ**	両方のシステムの最大フレーム・サイズは同じにする必要があります。
デフォルト・パケット・サイズ	構成装置 X.25-COM ポート X.25-WAC **パケット・サイズ**	この値はネットワーク・プロバイダーが決定するもので、伝送および受信にも同じ値を使用します。
最大パケット・サイズ	N/A	この値はネットワーク・プロバイダーが決定します。
モジュラス	構成装置 X.25-COM ポート X.25-WAC **順序付け**	この値はネットワーク・プロバイダーが決定します。
デフォルト・ウィンドウ・サイズ	構成装置 X.25-COM ポート X.25-WAC **ウィンドウ・サイズ**	この値はネットワーク・プロバイダーが決定するもので、伝送および受信にも同じ値を使用します。
ネットワーク・アドレスの挿入	構成装置 X.25-COM ポート X.25-WAC	この値はネットワーク・プロバイダーが決定するもので、両方のシステムの値が等しくなければなりません。
論理チャネル項目	構成装置 X.25-COM ポート X.25-WAC **バーチャル・サーキットの範囲**	この値は使用するネットワーク・プロバイダーおよび X.25 バーチャル・サーキット・タイプにより決定されます。

iSeries ホスト制御装置定義 (X.25 PVC)

iSeries ホスト制御装置定義には、 Communications Server パラメーターと一致させる OS/400 ホスト・プログラム・パラメーターが含まれています。表 27 は、X.25 PVC 用の OS/400 ホスト・プログラム・パラメーターを示しています。

表 27. iSeries Communications Server X.25 PVC パラメーター相互参照: 制御装置パラメーター

OS/400	**Communications Server プロファイル/パラメーター**	**注釈**
X.25 論理チャネル ID	構成接続 X.25-COM ポート X.25-WAC **論理チャネル番号**	これらの値はネットワーク・プロバイダーが決定します。
Linktype: *X25	構成接続	双方のシステムにあるリンク・タイプは一致させる必要があります。
交換接続: *NO		すべての PVC は非交換です。

表 27. iSeries Communications Server X.25 PVC パラメーター相互参照: 制御装置パラメーター (続き)

最大フレーム・サイズ	構成装置 X.25-COM ポート X.25-WAC **最大 PIU サイズ**	最大フレーム・サイズ値は、同じにする必要はありません。
データ・リンク・ロール	構成装置 X.25-COM ポート X.25-WAC **リンク・ステーション・ロール**	双方のシステムにあるパラメーターは互いに補完します。ホスト・ロールがプライマリーである場合は、Communications Server ワークステーションは、セカンダリーまたはネゴシエーション可能として構成される必要があります。
X.25 ネットワーク・レベル	構成装置 X.25-COM ポート X.25-WAC **CCITT 対応**	これらの値はネットワーク・プロバイダーが決定します。
X.25 リンク・レベル・プロトコル: *QLLC		この値は QLLC でなければなりません。

iSeries ホスト制御装置定義 (X.25 SVC)

iSeries ホスト制御装置定義には、 Communications Server パラメーターと一致させる OS/400 ホスト・プログラム・パラメーターが含まれています。表 28 は、X.25 SVC 用の OS/400 ホスト・プログラム・パラメーターを示しています。

表 28. iSeries Communications Server X.25 SVC パラメーター相互参照: 制御装置パラメーター

OS/400	**Communications Server プロファイル/パラメーター**	**注釈**
Linktype: *X25	構成接続	双方のシステムにあるリンク・タイプは一致させる必要があります。
交換接続: *YES		すべての SVC は交換機です。
最大フレーム・サイズ	構成装置 X.25-COM ポート X.25-WAC **最大 PIU サイズ**	最大フレーム・サイズ値は、同じにする必要はありません。
接続番号	構成装置 X.25-COM ポート X.25-WAC **ローカル DTE アドレス**	この値はネットワーク・プロバイダーが決定します。

表 28. iSeries Communications Server X.25 SVC パラメーター相互参照: 制御装置パラメーター (続き)

データ・リンク・ロール	構成装置 X.25-COM ポート X.25-WAC **リンク・ステーション・ロール**	双方のシステムにあるパラメーターは互いに補完します。ホスト・ロールがプライマリーである場合は、Communications Server ワークステーションは、セカンダリーまたはネゴシエーション可能として構成される必要があります。
X.25 ネットワーク・レベル	構成装置 X.25-COM ポート X.25-WAC **CCITT 対応**	これらの値はネットワーク・プロバイダーが決定します。
X.25 リンク・レベル・プロトコル: *QLLC		この値は QLLC でなければなりません。

第 14 章 Communications Server 構成のインプリメント

ネットワークのソフトウェアのインストールおよび構成のための推奨手順は、次のとおりです。

1. ハードウェアの計画
2. ソフトウェア・アプリケーションの計画
3. 命名規則の作成
4. ネットワーク・アドレスの定義
5. 構成ツールとインストール・ツールの選択
6. Communications Server 機能の選択
7. 構成の作成およびインストール
8. ユーザー資料の作成
9. ネットワークの保守

この章では、推奨手順を完了するために必要な事柄について説明しています。

はじめに

テンプレート構成では、サーバーのグループに共通する構成情報を定義します。 1 つ以上のテンプレート構成を作成する場合もあります。各サーバー構成ファイルはテンプレート構成で始めて、その後に、各サーバー用に構成をカスタマイズするために必要ないくつかのパラメーターを含めます。こうすることにより、サーバー構成が単純化されます。

テンプレート構成ファイルは、応答ファイルを使用して指定することのできない構成オプションを指定するためにも使用することができます。

構成およびインストール用の応答ファイルおよびテンプレート・ファイルの使用法の詳細については、 183 ページの『テンプレート・ファイルおよび応答ファイル構成』 を参照してください。

下記ステップで情報収集時は、各ワークステーションごとに RAM とハード・ディスクのスペースの必要容量の総計を足し合わせてください。 このようにして、お客様が選択したソフトウェアの使用開始時に、適切なハードウェアが備わっているかどうか確認することができます。

ステップ 1. ハードウェアの計画

既存サーバーが使用可能であるとお客様が既に判断している場合には、既存ハードウェアのメモリーとハード・ディスク・スペースが適切なものであるか確認する必要があります。既存のハードウェアには、それにインストールされるソフトウェアに対して適切なシステム装置、表示装置、プリンター、キーボード、アダプター、モデム、およびケーブルも備わっていなければなりません。

新しいサーバーを使用する予定があれば、そのサーバーのユーザー向けに準備するハードウェアをワークシート上に記録してください。

記憶域

Communications Server の記憶域要件については、*「概説およびインストール」* を参照してください。

メモリー容量

Communications Server の実行用にハードウェアを計画中の場合、容量の点でサーバーをどのように使用するかを見積もることが重要です。どのタイプのセッションを Communications Server がサポートするかを決定してください。これらのセッションには、ホストへの TN3270E セッション、SNA API クライアント・セッション、および従来の SNA セッションなどが含まれます (ただし、これらには限定されません)。このセッション数に基づいて、サーバー上の平均ロードを計算し、サーバーの正しいメモリー容量を決定できます。

注: これらの見積もりは、基本オペレーティング・システムおよび同じシステム上で同時に稼働しているその他のアプリケーションの要件に付加されます。

表 29を使用して、サーバー上の平均ロードを決定してください。

表 29. メモリー容量

クライアント・セッション・タイプ	セッションごとのメモリー使用量
SNA ゲートウェイ (従来)	29.9 KB
SNA API クライアント	25.2 KB
TN3270E	15.8 KB

アクティブなリンクやセッションを何も使用していない状態でのアクティブな Communications Server の見積もりメモリー使用量は、21 MB です。パフォーマンスの損失を最小化するためには、発生するページング回数 (メモリー・セグメントのディスクへのスワッピング) を削減することが最善な方法です。できる限り、実行するソフトウェアが必要とするメモリーと同サイズの実メモリーがシステム上で使用できるようにしてください。 (バッファーとしてさらに 5 MB から 10 MB を確保してください。)例えば、 TN3270E クライアント・セッション数を 1000 個サポートする Communications Server インストールには、以下の容量のメモリーが必要です。 (表 29 の値に基づきます。)

Microsoft Windows サーバー・オペレーティング・システム	19.0 MB (見積もり)
Communications Server for Windows	21.0 MB
TN3270E セッション (1 000 X 15.8 KB)	15.8 MB
不測の事態に対する備え	10.0 MB
推奨される合計メモリー容量	65.8 MB

注: 65.8 MB は、TN3270E セッションを 1000 個稼働するメモリー容量としては、必ずしも必須ではありません。これは最高のパフォーマンスを実現するための推奨値です。

CPU 速度

必要とされる最小プロセッサー速度を決定する場合、 1 秒ごとにサーバーが処理する必要のある平均トランザクション量を知っておかなければなりません。トランザクションでは、サーバー経由でクライアントとホスト間での情報のやりとりが発生します。その場合、画面の最新表示でも、要求されたデータベース入力でもこのやりとりがあります。

平均の CPU 負荷を計算するには、同時に発生する平均セッション数と、 1 セッションごとに 1 秒間に発生する平均トランザクション数と、以下のテーブルのスケール係数 (セッション・タイプに基づく) を乗算します。

クライアント・セッション・タイプ	CPU ロード因数 (100 Mhz)	CPU ロード因数 (166 Mhz)
SNA ゲートウェイ (従来)	.004	.002
SNA API クライアント	.021	.011
TN3270E	.011	.006

例えば、1 秒平均 6.7 トランザクションの 1 000 の同時 TN3270E セッションをサポートするには、 166 Mhz CPU 上での平均ロードは、 1000 X 6.7 X .006 で計算され、40.2% となります。 CPU 使用率が 80% を超えると、急速にパフォーマンスが低下します。 CPU が高速であればそれだけ、Communications Server およびシステムのパフォーマンスが向上します。 より多くのユーザーとトランザクションが、サーバーを同時に使用することができます。 Communications Server によりサポートされる最大 CPU 速度はありませんが、 100 Mhz が最小の推奨値です。

ステップ 2. ソフトウェア・アプリケーションの計画

Communications Server に対する要件に加えて、ソフトウェア・アプリケーションの要件があります。 詳細については、ソフトウェア・アプリケーション資料を参照してください。

ステップ 3. 命名規則の作成

Communications Server 使用して作成されるネットワークでは、ネットワーク上の複数のオブジェクトに対して非常に多くの名前を付けて使用することになります。 この名前の一部には、どのサーバーでも同じにして構わないものもありますが、それ以外の名前は、ネットワーク上で一意になるようにして、ネットワーク資源のアクセス時にサーバー相互間で矛盾がないようにします。

例えば、2 つの LAN でいくつかの同じ名前のドメイン・ネームが定義されている場合があります。これらの LAN が接続されていなければ、何も矛盾はありません。 しかし、それらの LAN が後になって基幹 LAN に接続されることになると、LAN 上で名前の競合が生じます。

これが命名規則の作成が必要となる理由です。 命名規則は、各種のネットワーク資源に名前を割り当てるときに従わなければならない規則であり基準でもあります。

次の節には、計画の必要がある命名規則が示されています。 計画にあたり、使用する命名規則が分かっている場合には、ネットワークの計画段階で該当の命名規則を記録しておいてください。

命名の基準

命名規則の作成時には、次の事柄を決めてください。
- ネットワークでの名前とアドレスを作成するために使用する基準。
- 名前とアドレスに一貫性をもたせる方法および必要に応じてネットワーク内で名前とアドレスを固有のものとする方法。

ホスト・コンピューター・ネットワークにサーバーを接続している場合には、例えばご使用のネットワークで使用しなければならない名前の大部分が、読者に代わってホストの担当者により選択済みとなっていることがあります。この場合には、ホストが必要とする物理装置と論理装置については、ご使用のサーバーの構成ファイルに対してそれらの名前を記録しておかなければなりません。

別の例として、ネットワークのサーバーに名前を付ける際に、それらのワークステーションを使用する人の名前を用いることがあります。小規模ネットワークの場合、名前の数が少なくその名前を固有なものに保つことができる限り、これは可能です。 しかし、大規模ネットワークの場合、人々の名前は通常固有のものではないので、これは不可能です。したがって、大規模ネットワークの場合、ワークステーションの名前として別の規則を作成しなければなりません。

名前に関して、どの基準を選ぶにしても、必ずそれらを記録しておいてください。このようにすることにより、新しい資源をネットワークに追加するときはいつでも適切な情報を参照することができます。

名前のタイプと制限

大部分の名前は、それらが使用されるネットワーク内で固有のものとしなければなりません。この節では、ネットワークの計画、インストール、構成を行うときに使用する可能性のある名前のタイをリストします。 ネットワークの計画を始める前に、リストされている名前を一覧し、よく理解しておいてください。

次の情報は、おのおのの名前ごとに提供されています。
- 定義
- ネットワーク内で、固有でなければならないかどうか
- 命名上の制約事項

2 つ以上の構成要素によって使用される名前

2 つ以上の構成要素によって使用される名前は次のとおりです。
- ネットワーク ID
- パスワード
- ユーザー ID
- ネットワーク・アドレス単位 (NAU) 名

ネットワーク ID: ネットワーク ID はネットワークに与えられる名前であり、特定のネットワーク内のすべてのサーバーとワークステーション (ノード) で使用されて、接続された全ネットワークを通じて固有の ID を維持します。また、ネットワーク ID は、ネットワーク・システムのエラーに関連したエラー・ログとネットワーク管理アラートでも用いられます。

ネットワークについては 2 とおりの見方があります。 その 1 つは物理ネットワークとみなすものです。物理ネットワークは、トークンリング環境では 1 つの “リン

グ” から、イーサネットまたは PC ネットワーク環境では 1 つの “ストリング” から成るものです。 もう 1 つは、論理ネットワークとみなすものです。論理ネットワークは物理ネットワークとは異なったものとなることがあります。 2 つ以上の物理ネットワーク (例えば、2 つのトークンリングと 1 つのイーサネット・ストリングから成るもの) を同じ論理ネットワーク内で保持する意図で接続することができます。

ネットワーク ID は、論理ネットワーク内で固有のものです。そうでなければ、ネットワークは論理的に同じネットワークになってしまいます。 1 つの論理ネットワーク内では、LU 名を固有のものとして命名上で競合をきたすことのないようにしなければなりません。 論理ネットワーク相互間では、ネットワーク ID により固有名が保証されます。 LU 名は、2 つの論理ネットワークで同じであっても構いません。しかし、各論理ネットワークごとのネットワーク ID が、完全に修飾された LU 名を固有にします。ネットワークが現在、接続されていない場合でも、将来においてネットワークを接続する予定であれば、ネットワーク ID を固有のものとしておいてください。

ネットワーク ID を IBM に登録するようにしてください。 これにより、後日、アドレス指定上の競合をきたすことなく、SNA ネットワークを相互に接続することができます。 ネットワーク ID の登録に関する詳細については、最寄りの IBM 事業所にご連絡ください。

ネットワーク ID に関する制約事項は、次のとおりです。
- 長さ: 1 文字から 8 文字
- 使用できる文字: A から Z、0 から 9、$、@、#

パスワード: パスワードは、正しく構成されたアプリケーションとサービスで必要な機密保護機能であり、データを保護し、資源へのアクセスを制限するために使用するものです。

パスワードは、ネットワーク内で固有にする必要はありません。 パスワードはユーザーが指定します。

LU-LU パスワードに関する制約事項は、次のとおりです。
- 長さ: 1 文字から 8 文字
- 使用できる文字: 16 進ストリング

CPI-C および iSeries 接続内のパスワードなど、その他のパスワードの制約事項は以下のとおりです。
- 長さ: 1 文字から 10 文字
- 使用できる文字: ASCII ストリング

ユーザー ID: ユーザー ID は、ネットワーク資源のユーザーに管理担当者が与える固有の識別名であり、これにより、ユーザーは端末エミュレーションを使用してデータベース、LAN、ホスト資源にアクセスすることができます。

ユーザー ID は、ネットワークで固有でなければなりません。

ユーザー ID に関する制約事項は、次のとおりです。
- 長さ: 1 文字から 8 文字

- 使用できる文字: A から Z、a から z、0 から 9、$、@、# ネットワーク・アドレス可能単位 (NAU) 名

ネットワーク・アドレス単位 (NAU) 名

次に示すものは、Communications Server で指定しなければならない名前のタイプです。

- 制御点 (CP) 名 (ローカル・ノード名)
- 論理装置 (LU) 名

制御点 (CP) 名 (ローカル・ノード名): 制御点 (CP) は、ノードとその資源を管理する責任を負います。 APPN エンド・ノードでは、制御点は隣接するネットワーク・ノードの制御点と通信して、APPN ネットワーク・サービスを得る必要があります。 APPN ネットワーク・ノードでは、制御点は隣接するネットワーク・ノードの制御点と通信して、ネットワークを管理する必要があります。 制御点は、アダプターの活動化と非活動化、リンクの活動化と非活動化といった機能を管理し、LU のセッション開始と終了とを援助します。

制御点 (CP) の名前は、完全修飾 CP 名 (Communications Server の NODE 定義にある) の後半部分です。

制御点名は、ネットワーク内で固有にする必要があります。 しかし、1 つのノードには複数の PU 名を付けることができ、その PU 名は接続 (**LINK_STATION**) 定義で指定され、 XID3 で異なったホストと交換されます。この複数の PU 名は、ノード内および接続対象ホスト内で固有にする必要があります。

PU および制御点は、サブエリア VTAM に対して同じではありません。 ある VTAM のドメイン内の各周辺ノードごとの PU 名はその VTAM で定義されており、周辺ノードの VTAM 側からの見方を表します。 VTAM での PU 名は、周辺ノードには認識されません。つまり、 VTAM は PU 名を周辺ノードに送信しません。 周辺ノードで PU 名を VTAM で定義されたものと同じものにしたい場合は、調整が必要です。 この調整を行うことをお勧めしますが、SNA の場合にはこの調整は不要です。

VTAM に対しては、この制御点は一種の LU であり、制御点と VTAM LU (CICS® など) との間の LU 6.2 セッションの活動化時に使用されます。VTAM が制御点に対して LU 6.2 セッションを開始する場合には、周辺ノードで定義された制御点名と VTAM での LU 定義とを一致させる必要があります。 そうしないと、VTAM は周辺ノードが VTAM LU に対してセッションを開始した時点で制御点名を知ることになります。

Communications Server の場合、制御点名 (ネットワーク ID を除く) は、ローカル・ノードの制御点名とその PU 名の両方として扱われます。 周辺ノードの PU 名が入っている唯一の伝送フローはアラートです。 しかし、Communications Server (APPC/APPN) によるアラート送信時は、このアラートには制御点名 (資源タイプが CP) が含まれます。PU 名ではありません。エミュレーターがアラートの中で PU 名を送信する場合、その PU 名は制御点名と同じものになります (Communications Server がノードの PU 名として制御点名を使用するため)。 ホスト・フォーカル・ポイントは、PU 名と制御点名とが同じであるリンク上でのみ定義することができます。 さらに、制御点名以外の PU 名が付いたホスト・リンクでは、ホストとの CP-CP セッションを使用できないか、あるいはそのリンクを介した APPN トラフ

ィックを経路指定できません。別の PU を使用しているリンク上の条件によりアラートが引き起こされても、すべてのアラートには制御点名が含まれます。

ローカル・ノード名に関する制約事項は、次のとおりです。
- 長さ: 1 文字から 8 文字
- 使用できる文字: A から Z、0 から 9、$、@、#
- 先頭文字: A から Z、$、@、#

論理装置 (LU) 名: 論理装置 (LU) 名は、ノード内のトランザクション処理のための機能をサポートする SNA 論理ポートに付ける名前です。 これによって、ユーザーはホスト・アプリケーション・プログラムを含めネットワークの他の LU と通信することができます。

LU 名に関する制約事項は、次のとおりです。
- 長さ: 1 文字から 8 文字
- 使用できる文字: A から Z、0 から 9、$、@、#

Socket over SNA LU 名: Socket over SNA ゲートウェイには、LU 名を付ける必要があり、その LU 名に対して、このゲートウェイが正常に開始できるように構成されている必要があります。Socket over SNA ゲートウェイは、初期化時に Communications Server に対してこの構成された LU 名を動的に定義します。

Socket over SNA LU に対して事前定義した命名規則を使用すると、以下の点で便利です。
- どの名前が Socket over SNA ゲートウェイ LU を表す名前で、どの名前がネットワーク内の他 LU を表す名前かを管理する。
- マッピング・エラーや経路指定エラーが起こったときに、分析したり解決したりする。
- IP アドレスを Socket over SNA の LU 名にマッピング時、アルゴリズム的マッピングを使用可能にする。

ステップ 4. ネットワーク・アドレスの定義

ネットワーク内でこのアドレスに整合性と一意性があることを確認します。各アドレスは唯一無二にする必要があります。定義するアドレスはネットワークを構成する方法によって決まります。 次の節では、下記のものに対するアドレスについて説明します。
- LAN
- SDLC
- X.25

使用するアドレスを記録し、必要ならば、アドレスに矛盾がないこと、およびアドレスが選択した命名規則に従っていることも確認してください。

LAN アダプター・アドレス

LAN アダプター・アドレスは、12 文字の 16 進数であり、製造会社がアダプター・カード内にコード化する (出荷時設定アダプター・アドレス) か、またはネットワーク管理者が割り当てます (ローカル管理アドレス)。 LAN 通信用に構成するワークステーションの各ネットワーク・アダプター・カードのアドレスは、固有のものでなければなりません。

使用するネットワーク・アダプター・カードのアダプター・アドレスとして、 “組み込みアドレス” とも呼ばれる出荷時設定アドレスを用いることも、またはローカル管理アドレスアドレスを割り当てることもできます。 LAN アダプター・アドレスはネットワーク内で固有のものとしなければなりません。ローカルに設定されたアドレスを使用する場合には、アドレスがネットワーク内で固有のものであることを確認してください。

ローカル管理アドレスは、アダプターの交換が必要となるようなアダプター障害発生時に大きな利点が発揮されます。既存のアドレスを、交換するアダプターに移すことができるので、このアドレスを参照している構成は何も変更しなくてすみます。 出荷時設定アドレスを用いる場合、障害のあるアダプター・カードにアクセスする全ワークステーションに対して、この障害のあるネットワーク・アダプター・カード・アドレスを変更する必要があります。

LAN アダプター・アドレスの構成に関する制約事項は、次のとおりです。
- **長さ**: 12 文字
- **使用できる文字**: A、B、C、D、E、F、0 から 9
- **範囲**: X’400000000000’ から X’7FFF FFFF FFFF’

LAN 上で、ローカルに設定された LAN アダプター・アドレスの使用を選択することもあります。これにより、LAN アダプターに組み込まれている出荷時に設定された LAN アダプター・アドレスを使用せずに、 16 進数を LAN アダプター・アドレスとして各 LAN アダプターに割り当てます。 以下の基準を持つ規則を使用することができます。
- 最初の 4 桁は、常に X’4000’ v
- 続く 3 桁は常に X’268’ であり、お客様の部門を表します。
- 最後の桁は X’01000’ から X’FFFFF’ の範囲内であり、お客様のネットワークの個々のワークステーションを表します。

イーサネット上での出荷時設定アドレスは、イーサネット形式になります。ローカル管理アドレスを使用する場合には、形式のタイプ (イーサネットかトークンリング) を指定することができます。 SNA 接続での宛先アドレスを構成する際には、アドレス形式がリモート側で指定したものと同じであるようにしてください。ブリッジングにより、トークンリング上でローカルに存在すること、およびイーサネット上にリモート・ステーション端末を置いてイーサネット形式のアドレス (バイト・スワップの) を使用することができます。

SDLC 2 次局アドレス

端末アドレスは、ネットワークで 2 次局を識別するのに使用されます。

2 次局アドレスは、ネットワーク内で固有のものでなければなりません。 1 次局は、その 2 次局の端末アドレスを使用して、 2 次局と通信します。 2 次局は、それ自体のアドレスを使用して 1 次局と通信します。

2 地点間接続の場合、2 次局がブロードキャスト・アドレス X’FF’ をサポートしていると、 1 次局はリモート側の 2 次局アドレスを知ることができます。 2 次局は、X’01’ から X’FE’ までの値を指定することができます。

1 次局がブロードキャスト・アドレスをサポートしていない場合、2 次局アドレスは 1 次局で定義されているものと同じ値に設定しなければなりません。 値は X'01' から X'FE' までです。

注: ほとんどの場合、端末はブロードキャスト・アドレスをサポートしているので、 1 次局では 2 次局アドレスとして X'FF' が使用されます。

ネゴシエーション可能な端末は、X'01' から X'FE' までの間で構成されたローカル 2 次局アドレスを持っています。ネゴシエーションの結果 2 次局になったステーション側の 2 次局アドレスが使用されます。

分岐回線接続の 2 次局の場合、アドレスは、分岐回線 1 次サーバー機能を提供するノードで指定された値と一致しなければなりません。アドレスは、X'01' から X'FE' までの範囲です。

X.25 アドレス

X.25 アドレスは、X.25 ネットワーク上で通信している資源を識別するために用いられます。 X.25 ネットワークは、CCITT 勧告を実装しています。この勧告では、データ端末装置とパケット交換ネットワークとの間のインターフェースを定義しています。X.25 アドレスは、ネットワーク内で固有のものとしなければなりません。このアドレスは X.25 ネットワークの提供元から得ることができます。

IP アドレス

インターネット・プロトコル (IP) アドレスを使用して、ネットワークを経由するデータの経路指定を行います。各 TCP/IP ホストには、最低 1 つの固有な IP アドレスが割り当てられています。 ホストに割り当てられている IP アドレスは、ネットワーク上のホストを定義するのではなく、そのホスト上のネットワークへのネットワーク・インターフェースを定義します。

Communications Server ノードは、そのノード経由で TCP/IP データを経路指定する固有な IP アドレスを、各ネットワーク・インターフェースごとに保有している必要があります。例えば、EEDLC IPv4 および IPv6 を使用して SNA ネットワーク経由で TCP/IP トラフィックを経路指定している Communications Server ノードは、両方のネットワーク用の固有の IP アドレスが必要になります。 Windows Server 2003、Windows XP および Windows Vista は IPv4 接続と IPv6 接続の両方をサポートしますが、それぞれの Windows オペレーティング・システムはホスト名を 1 つだけ持っています。

IP アドレスは 2 つの部分の 32 ビット・アドレス・フィールドによって構成されます。アドレス・フィールドの最初の部分には、ネットワーク・アドレスが入ります。 2 番目の部分には、ホスト・アドレスが入ります。

IPv4 アドレスは、通常、ドット 10 進形式で指定されます。次は、その一例です。

```
a.b.c.d
```

ここで、a、b、c および d は 0 から 255 までの値です。

IPv6 アドレスは、通常、ホスト名で指定されますが、実アドレスは以下の形式でも使用できます。

```
2002:905:D0A1::905:DOAL
```

ステップ 5. 構成およびインストール・ツールの選択

Communications Server は、次の節で説明している構成ツールを使用します。これらのツールについての詳細は、*「概説およびインストール」* を参照してください。

ノード構成アプリケーション

SNA ノード構成アプリケーションは、 SNA 構成情報を管理できるグラフィック・ウィンドウ・アプリケーションです。 このアプリケーションは、定義間の関係を表示するためにツリー・ビューを使用して SNA 構成データを編成します。 構成を作成する際に、ユーザーの作業は統合タスク・リスト、およびコンテキスト・ヘルプにより支援されます。アプリケーションにはユーザーの構成ファイルを作成し、提供されたデータを検査する責任があります。

リモート構成

SNA ノード構成を、リモートの Communications Server へ接続し、直接その資源を構成するためにも使用することができます。ユーザーは、ネットワーク内の任意の場所にある Communications Server の構成をリモートで管理することができます。

リモート管理クライアントは、**SNA ノード構成**を含む管理アプリケーションのみを、クライアント上にインストールします このクライアントから、ユーザーは、ネットワーク内のどの Communications Server も完全に管理および構成することができます。

Windows 2000、Windows XP、Windows Server 2003 および Windows Vista のリモート管理クライアントは、 Windows ドメイン・セキュリティーを使用することにより、ユーザー ID とパスワードを再入力しなくても、サーバーへのクライアント接続の権限を認証します。この場合のクライアントは、 Communications Server ドメインに参加するか、または同期したユーザー ID とパスワードでローカルにログインすることによって、 Windows ドメインの一部になる必要があります。

Windows ドメインにないリモート管理クライアント・ユーザーは、ユーザー ID とパスワードを入力する必要があります。これを行うには、プロンプトを通じて入力するか、あるいはクライアント構成ファイルにこれらの値を保管するかのいずれかを行います。

リモート管理クライアントに対する許可ユーザーは、IBMCSADMIN ローカル・グループ内に保持され、そのグループは Communications Server 上に直接、または Communications Server が参加しているドメイン制御装置のいずれかに配置されます。 このユーザー・グループは、インストール中に作成され、 Windows ユーザーのマネージャー・アプリケーションを使用して管理されます。リモート管理クライアント・ユーザーには、IBMCSADMIN グループ内でのユーザー権限が与えられて、サーバーにローカルにログオンする必要があります。

ASCII 構成ファイル

Communications Server **SNA ノード構成**は、人間が読める形式で ASCII 構成ファイルにその構成データを保管します。 これにより、ユーザーは、**SNA ノード**を使用せずに、構成ファイルを変更することができます (このファイルおよび構文についての詳細は、*「構成ファイル解説書」* を参照してください)。このファイルを使用

して、ネットワーク管理者はスクリプト記述などの自動化されたタスク、あるいは Tivoli ソフトウェア配布サポートまたは Microsoft System Management Server などのソフトウェア配布サービスを使用する構成に素早く変更を加えることができます。

多数のサーバーをインプリメントするように構成を作成する場合、ネットワーク管理者は、すべてのサーバーに共通の構成要素を表示するテンプレート構成ファイルを作成することができます。 サーバーごとに必要な変更のみを持つ応答ファイルを使用し、管理者は、テンプレートおよび応答ファイルを配布し、この 2 つをマージしてターゲット構成を作成することができます。構成およびインストール用のテンプレート・ファイルおよび応答ファイルの使用法の詳細については、「テンプレートおよび応答ファイルによる構成」を参照してください。

テンプレート・ファイルおよび応答ファイル構成

Communications Server テンプレートを使用すると、エディターを使用して構成を作成したり変更したりすることができます。 Communications Server 構成キーワード・パラメーターはすべて、応答ファイルで構成することができます。テンプレートは Communication Server 構成 (.ACG) ファイルと同じ形式です。

注: .ACG ファイルの形式は、 Communications Server のインストール・ディレクトリー (例えば、C:¥Program Files¥IBM¥Communications Server) にある OCDNTS50.DAT ファイルに文書化されています。 .ACG ファイル内で使用されるキーワードおよびパラメーターについての詳細は、*「構成ファイル解説書」* を参照してください。

テンプレート・ファイルを使用すると、リモート・サーバーに大量の構成を配布する作業を軽減することができます。テンプレート・ファイルには、いくつかのサーバーに共通のキーワードを指定することができます。例えば、複数のサーバーを、暗黙的なクライアント・サポートを持つ SNA ゲートウェイとして構成する場合に、多くのキーワードが同一になります。これらの共通キーワードを反映したテンプレート構成ファイルを作成することができます。

テンプレート・ファイルと応答ファイルを使用して構成を作成する場合、検査ユーティリティーは、以下の順番でディレクトリーを検索します。

1. 検査ユーティリティーが呼び出されているローカル・ディレクトリー
2. Communications Server インストール・ディレクトリー内の PRIVATE サブディレクトリー

検査ユーティリティーが、テンプレート・ファイルおよび応答ファイルを検索できるように、これらのファイルを PRIVATE サブディレクトリーに保管してください。 PRIVATE サブディレクトリーは、構成 (.ACG) ファイルが保管される場所でもあります。

キー・フィールド

キー・フィールドは、キーワードに名前を付けて一意的に他の同じタイプのキーワードと識別する、キーワード内にあるパラメーターです。 @KEY_NAME パラメーターは、キーワードにキー・フィールドを指定します。

キー・フィールドは常に、キー・フィールドを持つキーワード内の最初のパラメーターです。 (例えば **MODE** キーワード内の **MODE_NAME** など)

一部のキーワードにはキー・フィールドがないものもあります。その理由は、このキーワードは構成ファイル内で一度だけしか指定できないからです。一度しか指定できないキーワードの例には、 **TN3270E_DEF** キーワードがあります。

テンプレート・ファイルへのキーワードの追加

応答ファイルを使用して新規のキーワード定義を追加するには、キーワード全体を指定する必要があります。キー・フィールドには、固有値を指定する必要があります。キーワードにどのサブフィールドも無指定の場合、これらのフィールドに対するデフォルトが使用されます。例えば、**MODE** キーワードを構成に追加するには、応答ファイルには以下のキーワードが含まれます。

```
MODE=(
MODE_NAME=MYMODE
COS_NAME=#INTER
CRYPTOGRAPHY=NONE
DEFAULT_RU_SIZE=1
MAX_NEGOTIABLE_SESSION_LIMIT=8192
MAX_RU_SIZE_UPPER_BOUND=4096
MIN_CONWINNERS_SOURCE=4096
)
```

上記の応答ファイル内容の想定としては、MODE_NAME=MYMODE のパラメーターを指定した **MODE** キーワードが、テンプレート内に存在しないということです。このキーワードが存在する場合は、応答ファイル内に指定された値を使用してパラメーターは更新されることになります。

MODE_NAME パラメーターが応答ファイルで無指定の場合、 MODE_NAME パラメーターを一意的に識別できないために、構成検査中にエラーが起こります。
MODE キーワードに使用可能なすべてのパラメーターが、必ずしも応答ファイルに指定されていたわけではありません。残りのパラメーターは、 OCDSNT50.DAT ファイルで割り当てられたデフォルトを使用します。この構成への追加結果は、以下のようになります。

```
MODE=(
MODE_NAME=MYMODE
AUTO_ACT=0
COMPRESSION=PROHIBITED
COS_NAME=#INTER
CRYPTOGRAPHY=NONE
DEFAULT_RU_SIZE=1
MAX_NEGOTIABLE_SESSION_LIMIT=8192
MAX_RU_SIZE_UPPER_BOUND=4096
MIN_CONWINNERS_SOURCE=4096
PLU_MODE_SESSION_LIMIT=8192
RECEIVE_PACING_WINDOW=20
)
```

テンプレート・ファイル内のキーワードの変更

応答ファイルを使用して既存のキーワード定義を変更する場合は、オリジナルのキーワードがテンプレート・ファイル内になければなりません。オリジナルのキーワードがテンプレート・ファイル内にない場合、応答ファイルにはエントリーが新規構成に追加します。キー・パラメーターを応答ファイル内に指定して、ターゲットのキーワードを識別する必要があります。応答ファイルのキーワードで指定された

これらのパラメーターのみが、テンプレート・ファイルのキーワードの中で更新されます。応答ファイルに指定されていないパラメーターは未変更のまま残されます。例えば、以下の **MODE** キーワードがテンプレート・ファイルにある場合、

```
MODE=(
MODE_NAME=#INTER
AUTO_ACT=0
COMPRESSION=PROHIBITED
COS_NAME=#INTER
CRYPTOGRAPHY=NONE
DEFAULT_RU_SIZE=1
MAX_NEGOTIABLE_SESSION_LIMIT=8192
MAX_RU_SIZE_UPPER_BOUND=4096
MIN_CONWINNERS_SOURCE=4096
PLU_MODE_SESSION_LIMIT=8192
RECEIVE_PACING_WINDOW=20 )
```

以下のキーワードが応答ファイルで指定されているとします。

```
MODE=(
MODE_NAME=#INTER
AUTO_ACT=10
)
```

結果構成には、以下の MODE キーワード定義が存在することになります。

```
MODE=(
MODE_NAME=#INTER
AUTO_ACT=10
COMPRESSION=PROHIBITED
COS_NAME=#INTER
CRYPTOGRAPHY=NONE
DEFAULT_RU_SIZE=1
MAX_NEGOTIABLE_SESSION_LIMIT=8192
MAX_RU_SIZE_UPPER_BOUND=4096
MIN_CONWINNERS_SOURCE=4096
PLU_MODE_SESSION_LIMIT=8192
RECEIVE_PACING_WINDOW=20
)
```

テンプレート・ファイルからのキーワードの削除

応答ファイルを使用してテンプレートからキーワードを削除する場合、キーワードを識別する、キー・パラメーターと値を DELETE キーワードと一緒に指定する必要があります。例えば、テンプレート・ファイルに以下のキーワードが指定されている場合、

```
MODE=(
MODE_NAME=#INTER
AUTO_ACT=0
COMPRESSION=PROHIBITED
COS_NAME=#INTER
CRYPTOGRAPHY=NONE
DEFAULT_RU_SIZE=1
MAX_NEGOTIABLE_SESSION_LIMIT=8192
MAX_RU_SIZE_UPPER_BOUND=4096
MIN_CONWINNERS_SOURCE=4096
PLU_MODE_SESSION_LIMIT=8192
RECEIVE_PACING_WINDOW=20
)
```

応答ファイルには以下のキーワードが入っているとします。

```
MODE=(
MODE_NAME=#INTER
DELETE
)
```

結果構成に、#INTER モード定義は含まれません。 **DELETE** キーワードは、*parameter=value* 指定の後に指定するか、またはパラメーターの前か後の行に単独で指定します。例えば、以下のような **DELETE** キーワードの使用が有効です。

```
MODE=(
MODE_NAME=#INTER
DELETE
)
MODE=(
DELETE
MODE_NAME=#INTER
)
MODE=(
MODE_NAME=#INTER DELETE
)
```

DELETE キーワードは、同じ行の parameter=value 指定の前に指定できません。例えば、以下のような **DELETE** キーワードの使用は無効です。

```
MODE=(
DELETE MODE_NAME=#INTER
)
```

特定のタイプのすべてのキーワードを削除したり、キー・フィールドを持たない 1 つのキーワードを削除するには、そのキーワードと **DELETE** キーワードがあればよいだけです。例えば、以下のとおりです。

```
TN3270E_DEF=(
DELETE
)
```

ステップ 6. Communications Server 機能の選択

Communications Server 用にサポートされている機能は、次のとおりです。 ユーザーの接続タイプに対して、次の内の一部または全部の機能がサポートされています。

SNA ゲートウェイ構成

SNA ゲートウェイを構成することによって、ダウンストリーム・クライアント・ワークステーションとシステム・ネットワーク体系 (SNA) メインフレーム・ホスト・コンピューター間でデータを交換することができます。このゲートウェイは、Communications Server によりサポートされる通信メディア全域にわたって、 1 つ以上のホストからの LU 資源とホスト PU を、ダウンストリーム SNA クライアント・ワークステーションで使用可能にする集線装置の機能を果たします。

TN3270E サーバー構成

TN3270E ゲートウェイを構成することによって、 TN3270E (または TN3270) アプリケーションを実行しているダウンストリーム TCP/IP クライアント・ワークステーションとシステム・ネットワーク体系 (SNA) メインフレーム・ホスト・コンピューター間でデータを交換することができます。このサーバーは、Communications Server によりサポートされる通信メディア全域にわたって、 1 つ以上のホストから

の LU 資源とホスト PU を、ダウンストリーム TN3270E (または TN3270) セッションで使用できるようにする集線装置の機能を果たします。

TN5250 サーバー構成

TN5250 サーバーを構成することによって、 TN5250 アプリケーションを実行している、TCP/IP ネットワーク上のダウンストリーム・クライアント・ワークステーションと SNA ネットワーク上の iSeries との間でデータを交換することができます。サーバーは、 Communications Server によりサポートされる通信メディア全域にわたって、 iSeries 表示セッションを、ダウンストリーム TN5250 クライアントが使用できるようにするゲートウェイの機能を果たします。

APPN ネットワーク・ノード構成

ネットワーク・ノードは、APPN ネットワークを通じて情報を維持し経路指定する責任を負います。これらは、 APPN ネットワーク内のすべてのネットワーク・ノードのトポロジーを維持するのと同様、直接付加されたエンド・ノード上で使用できるすべての資源 (LU) のディレクトリーも維持します。独立 LU 6.2 セッションがネットワーク内のノードによって要求されると、ネットワーク・ノードは、セッションによって要求されたリモート資源を見つけ、この 2 つのノード間でセッションの確立と経路指定を行う責任があります。

DLUR/DLUS 構成

Communications Server は、APPN ネットワーク全域で従属 LU セッションをサポートします。これにより、Communications Server は、ホストに常駐する従属 LU サーバー (DLUS) から経路指定サービスを要求する、従属 LU リクエスター (DLUR) として機能するよう要求されます。

Communications Server は、ダウンストリーム・セッションおよび装置同様、ローカル・セッションおよび装置両方用の DLUR をサポートします。いずれの場合にも、ローカル・ノードが APPN ネットワークへ接続するように構成されていなければなりません。

AnyNet SNA over TCP/IP ゲートウェイ構成

SNA over TCP/IP ゲートウェイは、TCP/IP および SNA ネットワーク間で SNA トラフィック (独立 LU 6.2) を経路指定します。例えば、SNA over TCP/IP ゲートウェイにより、別の AnyNet SNA over TCP/IP アクセス・ノードで稼働している APPC または CPI-C アプリケーションは、 SNA ネットワーク上の SNA ピア・ノードと通信できるようになります。

AnyNet SNA over TCP/IP ゲートウェイは、 APPN ネットワーク・ノードとして構成されなければなりません。これにより、APPC セッションは適切な SNA ピア・ノードに経路指定されます。

SNA API クライアント構成

SNA API クライアントは、Communications Server とは別のマシンで、実際にセッションを管理するために Communications Server ノード上の SNA コードを使用しながら、 SNA アプリケーションを実行することができます。 Communications Server は、その発信元がローカル・ノードであったかのように、単にセッションを

確立し管理しますが、アプリケーション・データをそれ自身のアプリケーション API へ転送せずに、SNA API クライアントへ転送します。

SNA API クライアントを使用すると、 Communications Server for Windows などの SNA 通信スタックを同じマシン上にインストールしなくとも、 SNA アプリケーションを実行することができます。したがって、あまり強力でない小型のマシンを使用して SNA アプリケーションを実行します。一方では、これらの SNA API クライアント用の SNA サーバーとして強力なマシンを専用に集中化して使用できます。

SNA API クライアントは、 APPC (独立 LU 6.2) アプリケーションおよび LUA API アプリケーション (3270 エミュレーターなど) の 2 種類のアプリケーションをサポートします。

CPI-C または APPC 構成

Communications Server は、CPI-C または APPC アプリケーション (iSeries システムへの APPC3270 または 5250 エミュレーションなど) をサポートします。 APPC ネットワーキングは、非常に柔軟性があり多目的に使用できるために複雑になる場合があります。この構成の複雑さは、Communications Server の使用方法、およびアプリケーションで実施する作業の量によって異なります。

ホストへの従属 LU 6.2 セッション

Communications Server は、ホスト PU とともに従属 LU 6.2 セッションをサポートします。

3270 構成

Communications Server は、ホストとともに 3270 セッションをサポートします。

フォーカル・ポイント構成

Communications Server は、特定の管理サービス・アプリケーションのアラート情報を経路指定するために、リモートのフォーカル・ポイント・ロケーションをサポートします。ローカル・ノードは、APPN ネットワークを通じてリモートのフォーカル・ポイントを探し出します。

ステップ 6.1 アプリケーション・プログラムの計画

特に、次の要件について調べてください。

- モード
- トランザクション・プログラム (TP)
- LU 定義 (ホスト、LU 6.2)
- パートナー LU

ステップ 7. 構成の作成およびインストール

Communications Server をお客様のサーバーにどのように構成およびインストールするかを決める必要があります。次のようなことができます。

- ユーザーに Communications Server のインストールおよび構成に関する指示を与えます。 独自の指示を作成することも、「概説およびインストール」の印刷コピーを作成することもできます。また、ネットワーク ID、制御点名、ネットワーク・アドレスといった各サーバーの特有の情報を指定してください。
- 既存の構成またはテンプレート・ファイルを使って Communications Server をインストールするよう、ユーザーに指示してください。 また、Communications Server の CD または CD イメージへのアクセスだけでなく、各サーバーに合わせて作成された応答ファイルを提供する必要があります。
- Communications Server を、自力でユーザー・サーバー上に構成し、かつインストールする。ユーザーのグループが非常に小さいものでない限り、複数ワークステーションに対してソフトウェアの構成、インストール、および配布を支援する製品の使用が必要になる場合があります。この種の製品の例として挙げられるのは、IBM NetView 分散管理プログラム /2 (NVDM/2)、 Tivoli ソフトウェア配布サポート、および Microsoft System Management Server (SMS) です。

応答ファイルの構成とインストールの使用

応答ファイルの構成とインストールを選択し使用する場合には、 183 ページの『テンプレート・ファイルおよび応答ファイル構成』を参照してください。

ステップ 8. ユーザー資料の作成

ネットワークの計画を終了し、計画をインプリメントする方法が決まったら、ユーザー資料を作成してください。 つまり、インストール、構成、日常的な使用法についての資料、およびバックアップ・プロシージャーを準備してください。

資料の準備

一組のカスタマイズされた資料を準備して、ユーザーがインストールや構成を行ったり、ユーザーが特定の必要に応じて Communications Server およびローカル・アプリケーションを使用するのを援助します。 以下に、ユーザーの操作説明書に含めるべき情報の種類について記述します。

構成と導入の資料とプロシージャー

Communications Server のインストールの援助として、*概説およびインストール* とオンライン・インストール操作のヘルプを使用することができます。ソフトウェアをインストールする際には、以下のいずれの手順を実行すべきかをユーザーに指示しなければなりません。

- 構成ファイルをいつバックアップするか
- Communications Server の構成ファイルを作成するためにデフォルトを受け入れるかどうかについては、ネットワーク情報 (LAN アダプター・アドレスなど) を準備する必要が生じる可能性があります。
- 準備した応答ファイルを用いていつインストールしたらよいか
- 準備したカスタマイズ済み構成ファイルを用いていつインストールしたらよいか

必要に応じて、適切な資料をユーザーに提供してください。

Communications Server の資料とプロシージャー

Communications Server 機能と API を使用する際には、以下の資料を参照することをお勧めします。

- 概説およびインストール
- 選択した Communications Server API 用のユーザー作成プログラム

Communications Server の開始と停止

Communications Server を開始または停止させる手順については、*「概説およびインストール」* を参照してください。

開始と停止について様々な指示がある場合、これらの指示をユーザーに伝えなければなりません。
- 問題判別のためにホスト側に援助を求めるための電話番号 (ホスト側の担当者に連絡してください)
- ホスト・システムまたはアプリケーション・プログラムのためのログオン手順
- ホスト・アプリケーションを停止させる手順 (ホスト側の担当者に連絡してください)
- ログオフ手順

指示に、システムまたはアプリケーション・プログラムをログオフするために特別な要件がある場合は、それを含めなければなりません。 この情報は、ホスト側の担当者から得ることができます。

アプリケーション・プログラムに関する資料とプロシージャー

管理担当者は、ネットワークで使用することになるアプリケーション・プログラムに関しては、手順とその他の情報をユーザーに提供してください。 通常、アプリケーション・プログラムのために以下の手順を提供しなければなりません。
- アプリケーション・プログラムを開始させる手順
- アプリケーション・プログラムを実行させる手順
- プリケーション・プログラムが生成したメッセージに応答する手順
- 問題判別に関する手順
- 必要な場合、アプリケーション・プログラムを停止させる手順

以上の手順については、アプリケーション・プログラマーにお問い合わせください。

問題判別の資料と手順

問題判別および報告の手順については、*「概説およびインストール」* を参照してください。

バックアップ手順の準備

時折、ユーザーが、構成ファイル、レジストリー、ファイル・システム、アプリケーション・プログラム、およびローカルに作成した他のプログラムやファイルを、消去したり変更したりすることがあります。その上、サーバーが、消去の検出、または容認できない変更の検出を行う場合があります。特に、就業時間中、多くのユーザーがサーバー・ワークステーションにアクセス時に、そうしたことが生じがちです。

以上の理由で、ネットワークのバックアップ手順を用意し文書化する必要があります。 さらに、サーバー上で選択したファイルの属性を、読み取り専用に変更することにより、ユーザーがそれらを変更できないようにしても構いません。

ステップ 9. ネットワークの保守

ネットワークの計画、インストール、構成が完了し、そのネットワークが日常的に運用されている場合、管理担当者に残された作業は保守です。ユーザーは、ネットワーク内の資源およびユーザーの追加、変更、または削除の計画、および問題解決の計画を立てなければなりません。

ネットワークに対して変更がある場合、初期セットアップで実行したのと同じレベルの計画と実行の手順を行う必要があります。 ネットワークに対してこれらの変更を行う場合、初期の変更、インストール、構成で用いたのと同じ手順に従うことをお奨めします。

Communications Server が提供する次のようなツールは、ネットワークの日常のパフォーマンスを監視するのに役立ちます。

- **SNA ノード操作**
- コマンド行ユーティリティー
- リモート管理クライアント
- システム管理 API
- SNMP サブエージェント
- パフォーマンス・モニター

以下のプロダクトも、ネットワークの日々の管理で役に立ちます。

- IBM NetView
- IBM LAN ネットワーク・マネージャー
- Tivoli ソフトウェア配布サポート

第 15 章 システム管理機能

この章では、Communications Server システム管理機能の概説を提供し、各管理機能に共通の機能を説明します。各管理機能には、固有の機能もいくつかあります。これらの機能については管理機能ごとに説明します。

システム管理機能は Communications Server の通信資源のモニターと制御を可能にします。この機能により、通信資源を調整し、SNA 通信サービスの効率化を改善したり、問題判別時に当該サービスの監視およびテストを行ったりすることができます。

管理可能な資源のリストについては、*「概説およびインストール」* を参照してください。

以下の管理機能を使用して Communications Server を管理することができます。
- **SNA ノード操作**
- リモート管理
- コマンド行ユーティリティー
- SNA ノード操作 ActiveX コントロール
- APPN MIB サポート
- zSeries リモート・オペレーション・サポート (ROPS)

Communications Server 管理用に、これらの管理機能のどの組み合わせも使用することができます。

システム管理機能の共通機能

各システム管理機能は、資源に対して以下のアクションを行うことができます。
- 資源情報の表示
- 資源の開始
- 資源の停止
- 資源の削除
- パス・スイッチの開始

表 30 に示すように、資源ごとにこれらのアクションのサブセットを実行することができます。

表 30. Communications Server 資源の管理活動

資源	表示	開始	停止	削除	パス・スイッチ
接続	X	X	X	X	
CPI-C サイド情報	X			X	
装置	X	X	X	X	
DLUR PU	X	X	X		
ローカル LU 0 - 3	X			X	
ローカル LU 6.2	X			X	

表 30. Communications Server 資源の管理活動 (続き)

資源	表示	開始	停止	削除	パス・スイッチ
LU 6.2 セッション	X		X		
PU 2.0/DLUR ゲートウェイ	X			X	
RTP 接続	X				X
TN3270e セッション	X		X		
TN5250 セッション	X		X		

SNA ノード操作

SNA ノード操作 は、 Communications Server により保守される通信資源を監視し制御する、オンラインの管理機能です。**SNA ノード操作**により、ネットワーク内の資源を変更、削除、およびモニターすることができます。

SNA ノード操作を使用して、ネットワーク内の資源の管理に役立てることができます。 Communications Server のシステム管理プログラミング機能によって、ユーザーの SNA ネットワーク内のノードの構成と管理を行うことができます。 **SNA ノード操作**は、階層グラフィック・インターフェース内の資源の選択および変更を可能にする構成のツリー・ビュー・ダイアグラムを提供します。

「**SNA ノード操作**」メインウィンドウ内では、複数のウィンドウを管理できます。

2 つ以上の Communications Server 構成を定義して、必要に応じて構成を切り替えることができます。 Communications Server を開始したら、他の構成を指定しない限り、ノード構成またはノード操作の最初の選択項目としてデフォルト構成が提供されます。新規構成が完了したら、デフォルト構成を新規構成に置換することができます。「SNA ノード操作」を使用して新規構成を適用し、製品の関連部分が構成したとおりに稼働することを確認してください。

SNA ノード操作を使用して、**ログ・ビューアー**、**トレース機能**、または **SNA ノード構成**などの他の Communications Server プログラムを起動することができます。

リモート管理

SNA ノード操作は、リモートの Communications Server へ接続し、直接その資源を管理するためにも使用することができます。ユーザーは、ネットワーク内の任意の場所にある Communications Server のリソースを、リモートで管理することができます。

リモート管理クライアントは、SNA ノード操作を含む管理アプリケーションのみをクライアント上にインストールします。このクライアントから、ユーザーは、ネットワーク内のどの Communications Server でも完全に管理することができます。

Windows のリモート管理クライアントはユーザー ID とパスワードを再入力しなくても、 Windows ドメイン・セキュリティーを使用して、サーバーへのクライアント接続を認証します。この場合のクライアントは、 Communications Server ドメインに参加するか、または同期したユーザー ID とパスワードでローカルにログインすることによって、 Windows ドメインの一部になる必要があります。

Windows ドメインにないリモート管理クライアント・ユーザーは、ユーザー ID とパスワードを入力する必要があります。これを行うには、プロンプトを通じて入力するか、あるいはクライアント構成ファイルにこれらの値を保管するかのいずれかを行います。

リモート管理クライアントに対する許可ユーザーは、IBMCSADMIN ローカル・グループ内に保持され、そのグループは Communications Server 上に直接、または Communications Server が参加しているドメイン制御装置のいずれかに配置されます。 このユーザー・グループは、インストール中に作成され、 Windows ユーザーのマネージャー・アプリケーションを使用して管理されます。リモート管理クライアント・ユーザーには、IBMCSADMIN グループ内でのユーザー権限が与えられて、サーバーにローカルにログオンする必要があります。

コマンド行プログラム

コマンド行プログラムを使用すると、 Windows のプロンプト・ウィンドウからコマンドを発行することができます。 コマンドの出力は画面に表示されますが、出力をファイルへリダイレクトすることができます。

使用可能なコマンド行プログラムのリストについては、*「概説およびインストール」* を参照してください。

SNA ノード操作 ActiveX コントロール

SNA ノード操作の ActiveX コントロール・バージョンがあります。この制御を使用すると、ユーザーは、**SNA ノード操作**をアプリケーションに組み込むことができ、 Microsoft Management Console (MMC) のような組み込み制御を行うことができます。この制御は CSNTACTX という名前を持ち、製品インストール・ディレクトリーに配置されています。この制御は、すべての **SNA ノード操作**ファンクションを持っており、 **SNA ノード操作**の他のアプリケーションへの組み込みによる利点を提供するもので、製品横断的な管理を可能にします。

APPN MIB サポート

Communications Server は、Simple Network Management Protocol (SNMP) 管理システムからの APPN 管理情報用に SNMP 要求をサポートします。

SNMP サービスは「Windows コントロール パネル」の「ネットワーク」プルダウンの下の「サービス」タブからインストールされます。 SNMP サービス・ソフトウェアをコンピューターにインストールしたら、 SNMP が稼働するのに有効な情報を使用して、このソフトウェアを構成する必要があります。

ユーザーは、SNMP を構成するローカル・コンピューターの管理グループのメンバーとしてログオンされなければなりません。

SNMP 構成情報は、コミュニティーおよびトラップの宛先を識別します。

NetView プログラム用の zSeries リモート・オペレーション・サポート (ROPS)

RUNCMD を NetView から発行する場合は、APPL パラメーターの値は APPL=CSRCMDS と指定する必要があります。

RUNCMD コマンドでは、 RUNCMD コマンド発行時に Netview の抑止文字を使用しない限り、 ID およびパスワードを含むすべての情報がそのまま伝送され、いかなる機密保護もされません。伝送された情報は画面に表示され、Netview ログに記録されます。パスワードが ROPS サービスに伝送される場合、Netview 端末とその Netview ログの機密保護を行い、デリケートなデータが損なわれないようにすることは、ユーザーの責任です。

付録 A. Communications Server の計画

モデム

Communications Server は V.24bis コマンド・セットをサポートする同期モデムおよび CSU/DSU 装置をサポートします。適切な接続タイプおよびモデムについては、ネットワーク提供者に問い合わせてください。

セッション・レベル暗号化アダプター

セッション・レベルの暗号化を使用するには、プログラム式暗号機能プログラムと、次のアダプターの 1 つが必要です。

- IBM SecureWay 4758 PCI 暗号コプロセッサー・アダプター
- IBM 共通暗号化体系に準ずるその他のアダプター

注: IBM 4758 以外のアダプターを使用している場合は、代わりに暗号 API verb を使用する必要があります。詳細については、「*Communications Server Programming Guide and Reference*」を参照してください。

データ圧縮の考慮事項

SNA データ圧縮の使用に先立って、関係するシステムでいくつかの構成作業を実施しておく必要があります。 SNA データ圧縮は、以下においてサポートされています。

- VTAM V3R4.1 またはそれ以降
- OS/400 V2R3 またはそれ以降

圧縮が行われるときに、RU はそれぞれ別々に圧縮され、圧縮ヘッダーが RU に追加されます。 TH と RH は圧縮されません。 RU が 20 バイトより小さい場合、または 64K バイトより大きい場合、もしくは RLE の場合のみ、圧縮されたデータのサイズ (圧縮ヘッダーを含む) が元のデータよりも大きい場合は、圧縮は行われません。

パートナー・システムがデータ圧縮をサポートすることが可能であること、およびその準備ができていることを確認してから、データ圧縮用に Communications Server の適切な機能の構成を開始します。

ホスト/VTAM 接続の計画

VTAM バージョン 3 リリース 4.1 (VTAM V3R4.1) をインストールし、データ圧縮要求をネゴシエーションするよう構成してから、3270 エミュレーションまたは LU 6.2 型通信を行っている S/370 または zSeries® ホストへのセッション上でデータ圧縮を要求します。

データ圧縮に必要な VTAM 定義は、ホストの VTAM のシステム・プログラマーが提供します。 以下に、必要な定義のリストを要約したものを挙げます。 このリストの後に、例が記載されています。

- VTAM 始動オプションに **CMPVTAM=x** パラメーターが含まれていなければならない
- **COMPRES=** パラメーターに LOGMODE 項目が必要である
- この LOGMODE が、ユーザーが使用しているモード・テーブルになければならない
- ユーザーが使用するアプリケーションには、VTAM APPL ステートメントに **CMPAPPLI=** パラメーターおよび **CMPAPPLO=** パラメーターが指定されていなければならない
- ユーザーのセッションの VTAM LU 定義で、圧縮のために定義された LOGMODE およびモード・テーブルが指定されていなければならない

CMPVTAM

これは VTAM 始動オプション・パラメーターであり、このホストに接続される全セッションに許可される最大圧縮レベルを示します。このパラメーターの構文は以下のとおりです。

```
CMPVTAM=n
```

ここで、n は要求に対して許可されている圧縮レベルで、0 から 4 の範囲を指定可能です。値 4 の使用をお勧めします。これによりあらゆるレベルのデータ圧縮が認められます。

COMPRES

これは、ユーザーの LU が使用する LOGMODE 定義内の VTAM MODEENT 表項目です。 構文は以下のとおりです。

```
COMPRES=value
```

ここで、value は SYSTEM、REQUESTED または PROHIBITED を表します。 サポート対象の全 LU タイプに対して SYSTEM を指定する必要があります。

CMPAPPLO

これは VTAM アプリケーション (APPL) 定義パラメーターであり、アウトバウンド要求/応答単位 (RU) データに対して要求された圧縮レベルを設定します。構文は以下のとおりです。

```
CMPAPPLO=n
```

ここで、*n* は PLU → SLU 方向のデータ・フロー (アウトバウンド・データとも呼ばれる) に対して要求されたデータ圧縮レベルです。 Communications Server がサポートするすべての LU タイプ・セッションに対して、値 *n* には、それぞれデータ圧縮のレベル 0、レベル 1、レベル 2 を表す 0、1、または 2 を指定できます。ただし、LU タイプ 0、 1、 2、 3 の場合、Communications Server は常にレベル 2 で圧縮リソースを指定します。

CMPAPPLI

これは VTAM アプリケーション (APPL) 定義パラメーターであり、インバウンド要求/応答単位 (RU) データに対して、要求された圧縮レベルを設定する VTAM アプリケーション (APPL) 定義パラメーターです。 構文は以下のとおりです。

```
CMPAPPLI=m
```

ここで、*m* は SLU → PLU データ・フロー (インバウンド・データとも呼ばれる) に対して要求されたデータ圧縮レベルです。 *m* の値は、セッションに使用される LU タイプによって異なります。

- 3270 LU タイプ・セッションの場合、*m* には 0 または 1 を指定できます。
- LU 6.2 タイプ・セッションの場合、*m* には 0、1 または 2 を指定できます。

注: VTAM は常に 1 次 LU (PLU) に相当し、Communications Server は LU タイプ 0、1、2、3 に対応する 2 次 LU (SLU) に相当します。

指定の例を以下に挙げます。この例は、オリジナルの VTAM リストから抜き出したもので、上記のパラメーターの使用法と位置を示しています。 強調表示されている行に、特に注意してください。

```
************************************************************
SSCPID=20,HOSTSA=20,XNETALS=YES,                             X
GWSSCP=YES,                                                  X
NODELST=NODES1,                                              X
CMPVTAM=4,                                    X
CONFIG=K0,SUPP=NOSUP,                                        X
NETID=USIBMRA,HOSTPU=ISTPUS20,HOSTSA=20,SSCPNAME=RAK,        X
SSCPDYN=YES,SSCPORD=PRIORITY,                                X
ASYDE=TERM,                                                  X
NOTRACE,TYPE=VTAM,IOINT=0,                                   X
NOTRACE,TYPE=SMS,ID=VTAMBUF,                                 X
PPOLOG=YES,                                                  X
NODETYPE=NN,                                                 X
CPCP=YES,                                                    X
CSALIMIT=0,                                                  X
NOTNSTAT,DYNLU=YES,                                          X
IOBUF=(3500,256,3,,1,58),                                    X
LPBUF=(1100,,2,,1,4),                                        X
LFBUF=(100,,,,1,1),                                          X
CRPLBUF=(2400,,,,1,4),                                       X
SFBUF=(60,,,,1,1)
************************************************************
```

図 37. この VTAM では、4 までの VTAM 始動パラメーターの圧縮レベルが許可されています。

```
*************************************************************************
* LOGMODE FOR COMPRESSION TEST - BASED ON D4C32XX3                      *
*************************************************************************
*                                                                       *
*                    3274 MODEL 1C (REMOTE SNA) @OY02946                *
*                    PRIMARY SCREEN 24 X 80 (1920)                      *
*                    ALTERNATE SCREEN TO BE DETERMINED BY APPLICATION   *
*                                                                       *
*************************************************************************
D4C3COMP MODEENT LOGMODE=D4C3COMP,                                      *
                 FMPROF=X'03',                                          *
                 TSPROF=X'03',                                      *
                 PRIPROT=X'B1',                                         *
                 SECPROT=X'90',                                         *
                 COMPROT=X'3080',                                       *
                 RUSIZES=X'87F8',                                       *
                 PSERVIC=X'028000000000000000000300',                   *
                 APPNCOS=#CONNECT,                                      *
                 COMPRES=REQD
```

図 38. VTAM ログモード・テーブル: MODEENT マクロは要求されたデータ圧縮とともに構成されています。

```
     VBUILD TYPE=APPL
*************************************************************************
* VTAM APPL STATEMENTS FOR CICS/MVS* 3.3                              *
*************************************************************************
RAKAC001 APPL ACBNAME=RAKAC001,                                         *
              MODETAB=MTAPPC,                                           *
              EAS=20,                                                   *
              SONSCIP=YES,                                              *
              AUTH=(ACQ,VPACE,PASS),                                    *
              PARSESS=YES,                                              *
              VPACING=5,                                                *
              CMPAPPLI=1                                                *
              CMPAPPLO=2
```

図 39. VTAM アプリケーション・アプリケーション: このセッションの最大サポート・レベルを制御します。

```
WTCC1102 PU ADDR=13,
            IDBLK=05D,
            IDNUM=32289,
            etc.
            DLOGMOD=D4C3COMP
            MODETAB=AMODETAB
            etc.


RACC1102 LU LOCADDR=2,DLOGMOD=D4C3COMP,MODETAB=AMODETAB
         LU
         etc.
```

図 40. VTAM PU および LU 定義: LU RACC1102 は AMODETAB モード・テーブルにあるログモード D4C3COMP を使用します。

iSeries データ圧縮の計画

iSeries システムに接続する際には、OS/400 V2R3 でデータ圧縮を使用可能にする必要があります。最低限必要なのは、MODE 定義で圧縮サポートを指定していること

です。 3 つのパラメーターが “Create Mode Description” プロファイルに必要です。このプロファイルは、CRTMODD コマンドまたはメニューを通じて得ることができます。 3 つのパラメーターは次のとおりです。

DTACPR

このパラメーターは、データ圧縮の使用を制御します。 有効なパラメーターは以下のとおりです。

NETATR
このパラメーターには、システム規模のネットワーク値を使用してください。

NONE データ圧縮は認められません。

ALLOW
リモート・システムがデータ圧縮を要求すると、ローカル・システムがそのセッションの確立を許可します。

REQUEST
ローカル・システムがデータ圧縮を要求します。

REQUIRE
データ圧縮の使用が必要です。 システムの 1 つが、要求されたレベルでデータ圧縮を行えない場合、セッションは確立されません。

INDTACPR

この値は、インバウンド・データに使用される圧縮の最大レベルを表します。

OUTDTACPR

この値は、アウトバウンド・データに使用される圧縮の最大レベルを表します。

LU 6.2 セッションの場合、データ圧縮レベル 0、1、2 は両方向 (つまり、アウトバウンド・データ・フローとインバウンド・データ・フロー) でサポートされます。

Communications Server がデータ圧縮に対応できるようにするには、「*概説およびインストール*」を参照してください。

パフォーマンスの考慮

コンピューター通信のパフォーマンスは、一般的に (Communications Server の場合は特に)、多くの変数の影響を受けやすいものです。 Communications Server 環境での通信パフォーマンスに影響を与えるいくつかの要素について、以下に紹介します。

通信パフォーマンスは、通信回線の速度に影響を受けます。 この速度は、通常、回線上で送信できるビット/秒 (bps) で表されます。一般に、bps が高くなればなるほど、回線上で実行できる通信パフォーマンスは向上します。

ビット伝送速度だけでなく、回線に関連するその他の要素も、通信パフォーマンスに影響を与えることがあります。 例えば、一度に一方向にしかデータを送れない回線があります。 通信の方向を変更 (送信を行える側を変更) するには、端末で送信

要求 (RTS) を出し、*送信可* (CTS) が出されるまで待機します。このためには、*回線反転* (モデムにより異なる) の時間がさらに必要になります。 その他の要素として、通信回線の伝送品質が挙げられます。

回線エラー発生時は、大部分のプロトコルはこのエラーを検出し、データを再送します。 伝送エラーが少ない回線ではより大きいスループットが得られます。

プロトコルが*全二重* データ伝送モードで操作を行っている場合は、プロトコルは受信と送信を同時に行うことができるので、より大きいスループットも可能になります。 LAN および X.25 は全二重プロトコルです。 SDLC は、全二重モードと半二重モードの両方で操作を行うことができます。

SDLC で全二重を使用するには、適切なアダプター (MPA アダプターは全二重をサポートできません) を使用してください。 全二重をサポート可能なリモート・ステーションが必要です。

回線速度が上がるに従って、回線のビット伝送速度が、パフォーマンスの制約となることは少なくなります。 その代わり制約は、通信回線を使用している装置内の遅延に関連したもの (モデム、制御装置、またはコンピューターの内部制約) になります。非常に速い速度の場合、このような装置関連の遅延は、回線のビット伝送速度の容量より以上に、通信パフォーマンスに大きく影響を与える可能性があります。

こうした状態を分析するのには、多少の手間がかかります。 例えば、予想よりも長い通信遅延は、以下のいずれかが原因で起こる場合があります。

- 通信回線の過負荷
- ホスト・システムの過負荷
- 3X74 制御装置の過負荷
- 37xx ネットワーク・コントローラーの過負荷
- VTAM 定義または NCP 定義が最適な定義になっていない
- 不十分なネットワーク設計またはネットワーク管理
- オペレーティング・システム・メモリーのオーバーコミットおよびスワッピング

LAN のような高速通信環境においては、通信回線のビット伝送速度はあまり重要ではありません。通信能力は、ほとんど通信装置の速度で決まるからです。 通信パフォーマンスをより良くするには、ワークステーション、ホスト、もしくはその他のネットワーク構成要素の処理能力を上げてください。 こうすることによって、LAN ネットワークのビット伝送速度が制約になるようなことはありません。むしろ、LAN のパフォーマンスが著しく低下する前に、いくつかのコンピューターがそれ自体の通信能力で実行されていることが必要です。

つまり、ほとんどの場合、Communications Server のパフォーマンスは、使用されている通信ネットワークに関連する要素によって決まります。通信パフォーマンスを低コストで行うには、全体的なネットワークの理解と、ネットワークの各構成要素の分析の両方が必要です。

付録 B. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものであり、本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
TL3B/062
3039 Cornwallis Road
RTP, NC 27709-2195
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

AIX
AS/400

Advanced Peer-to-Peer Networking
AnyNet
IBMNetView
OS/2
System/370
System/390
S/370
S/390
Tivoli、Manage
TME
Tivoli Ready
Tivoli Enterprise
VTAM

Java およびすべての Java 関連の商標およびロゴは Sun Microsystems, Inc.の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT、Windows XP、Windows Server 2003、Windows Vista および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

[数字]

A

B

C

H

I

L

P

S

T

X

Printed in Japan

SC88-5641-03

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12