eNetwork Communications Server version 6.0 pour Windows NT

Guide d'administration réseau

Version 6.0

SC11-1493-00

eNetwork Communications Server version 6.0 pour Windows NT

Guide d'administration réseau

Version 6.0

SC11-1493-00

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section Annexe B, «Remarques», à la page 223.

Réf. US : SC31-8656-00

Première édition (juillet 1998)

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.ibm.fr (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux États-Unis)

Par ailleurs, vous pouvez nous adresser tout commentaire sur ce document en utilisant le formulaire intitulé "REMARQUES DU LECTEUR" qui se trouve à la fin du document. IBM pourra disposer comme elle l'entendra des informations contenues dans vos commentaires, sans aucune obligation de sa part. Il va de soi que ces informations pourront continuer à être utilisées par leur auteur.

Dépôt légal : 2e trimestre 1998

Table des matières

Avis aux lecteurs canadiens

Le document que vous avez entre les mains a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien, de type QWERTY.

OS/2 — Paramètres canadiens

Au Canada, on utilise :

les pages de codes 850 (multilingue) et 863 (français-canadien),
le code pays 002,
le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	États-Unis
↖ (Pos1)	↖	Home
Fin	Fin	End
⇞ (PgAr)	⇞	PgUp

France	Canada	États-Unis
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Échap	Échap	Esc
Attn	Intrp	Break
Impr écran	ImpÉc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
Alt Gr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Figures

Tableaux

Préface

IBM eNetwork Communications Server pour Windows NT (désigné dans le présent manuel par *Communications Server*) est une plate-forme de services de communication qui fournit un grand nombre de services pour les postes de travail Windows NT communiquant avec les ordinateurs hôtes et avec d'autres postes de travail. Les utilisateurs de Communications Server peuvent choisir parmi les différentes options de connectivité distante.

Le *Guide d'administration réseau* sert de source de planification et d'administration à la personne qui utilise ou qui envisage d'utiliser Communications Server. Le présent manuel sera utile au personnel administratif, au personnel d'assistance technique, aux coordinateurs de maintenance et au personnel IBM, ainsi qu'à toute personne chargée de prendre des décisions relatives aux systèmes d'information. Il décrit les fonctions de Communications Server et les étapes nécessaires à la création des configurations de Communications Server pour les postes de travail pris en charge.

On considère que vous utilisez le système d'exploitation de base Windows NT 4.0 Server.

Utilisation du présent manuel

Le manuel *Guide d'administration réseau* permet d'effectuer la planification nécessaire à l'installation et à la configuration d'un réseau de postes de travail, notamment les opérations suivantes :

- Planification du réseau
- Choix des outils de configuration et d'installation
- Création d'un modèle de fichier de configuration
- Mise en œuvre d'un plan de réseau
- Maintenance du réseau

L'installation d'un réseau de postes de travail requiert une planification minutieuse et approfondie. Lors de la création d'un réseau, il est nécessaire de connaître les éléments suivants :

- Le nom des postes de travail, des profils, des fichiers de configuration et autres noms utilisés dans le réseau
- L'emplacement du point focal pour l'envoi d'alertes
- Les postes de travail disponibles que vous pouvez continuer à utiliser, ainsi que le nombre des nouveaux postes de travail requis
- Le rôle de chaque poste de travail dans le réseau
- Le module à installer sur chaque poste de travail de sorte qu'il puisse remplir le rôle qui lui est affecté
- Les ressources matérielles et logicielles existantes que vous souhaitez conserver ou mettre à niveau
- Les nouvelles ressources matérielles et logicielles requises avant la mise en œuvre du plan de réseau

- La méthode de maintien à long terme du réseau et des ressources associées
- Le nombre et le type de connexions hôte et les postes de travail à connecter aux systèmes hôte via la passerelle et la définition de passerelle

Les étapes de la section «Mise en œuvre des configurations de Communications Server», à la page 185, fournissent une procédure permettant de déterminer ces informations pour votre réseau. Si vous disposez déjà d'une procédure appropriée, vous pouvez l'utiliser mais vous devez consulter la procédure du chapitre avant de prendre cette décision.

Conventions utilisées dans ce manuel

Les conventions suivantes sont utilisées dans le présent manuel.

Texte

Gras	Les caractères en gras indiquent les éléments suivants : ▫ Verbes, fonctions, mots clés et paramètres pouvant être utilisés dans un programme ou à une invite. Ces valeurs distinguent les majuscules des minuscules et doivent être saisies rigoureusement telles qu'elles apparaissent dans le texte. ▫ Noms des commandes associées aux fenêtres (listes, cases à cocher, zones de saisie, boutons de fonction et options de menu.
Italique	Les caractères en italique indiquent les éléments suivants : ▫ Variable pour laquelle vous définissez une valeur. ▫ Titres de manuels. ▫ Caractère ou chaîne de caractères à respecter très rigoureusement. Par exemple, lorsque vous avez *un*, assurez-vous qu'il ne s'agit pas de *une*.
Gras italique	Les caractères gras en italique sont utilisés pour mettre un mot en évidence.
MAJUSCULES	Les caractères en majuscules s'appliquent à des constantes, des noms de fichiers et des options pouvant être utilisés dans un programme ou à une invite. Vous pouvez entrer ces valeurs en majuscules ou en minuscules.
Guillemets	Les guillemets sont utilisés pour les messages apparaissant dans une fenêtre (messages de la zone d'information opérateur (ZIO) d'une session d'émulation, par exemple).
`Exemple :`	Il s'agit des données que l'utilisateur est invité à entrer à une invite de commande ou dans une fenêtre.

Nombres

Nombres binaires	Les nombre binaires apparaissent sous la forme B'xxxx xxxx' ou B'x' sauf dans certains cas où ils sont représentés par du texte («Une valeur de xxxx xxxx binaire est égale à...»).
Positions de bits	Les positions de bits commencent par 0 à la position la plus à droite (bit le moins significatif).
Nombres décimaux	Les nombres décimaux dépassant 4 chiffres sont représentés en style métrique. Un espace est utilisé au lieu d'une virgule pour séparer les groupes de 3 chiffres. Par exemple, le nombre seize mille cent quarante sept s'écrit 16 147.
Nombres hexadécimaux	Les nombres hexadécimaux apparaissent dans le texte sous la forme de hex xxxx ou X'xxxx' («L'adresse du nœud adjacent est hex 5D, spécifié sous la forme X'5D'.»)

Où trouver des informations complémentaires

Pour de plus amples informations, consultez le *Guide d'utilisation* qui contient une description complète de la bibliothèque Communications Server et des publications associées.

La page d'accueil de Communications Server sur Internet comporte des informations générales sur le produit, ainsi que des informations de maintenance relatives aux APAR et aux corrections. Pour accéder à la page d'accueil, utilisez l'une des deux méthodes suivantes :

1. Dans Communications Server, sélectionnez l'icône **Visitez notre site web**.
2. Utilisez un navigateur Internet pour accéder à l'URL suivant :

   http://www.software.ibm.com/enetwork/commserver/about/csnt.html

Présentation générale et concepts

Présentation des fonctions de Communications Server

Le présent chapitre décrit les fonctions de communication prises en charge par Communications Server et des méthodes permettant de configurer vos systèmes afin d'effectuer ces fonctions. Les chapitres suivants de ce manuel fournissent une description plus détaillée des fonctions et des méthodes de configuration.

Fonctions prises en charge

La présente section décrit les fonctions suivantes de Communications Server :

- Support de communication SNA
- APPC (Advanced Program-to-Program Communications) qui comporte APPN (Advanced Peer-to-Peer Networking)
- Interfaces de programmation 32 bits (API)
- Routage hautes performances (HPR)
- Compression de données SNA
- Découverte de prestataires de services
- Application LU conventionnelle (LUA)
- Demandeur d'unités logiques dépendantes (DLUR)
- Passerelle SNA
- Support AnyNet
  - AnyNet SNA sur TCP/IP (passerelle et nœud d'accès)
  - AnyNet Sockets sur SNA (passerelle et nœud d'accès)
- Serveur TN3270E
- Serveur TN5250
- Accès aux données existantes
  - AS/400 OLE DB Provider
  - Host Publisher
  - Serveur de dossiers partagés AS/400
- Support client API SNA
- Support client Novell IntranetWare pour SAA
- Support de configuration et d'administration
- Équilibrage de charge
- Sécurité de données
- Support de cartes
- Support DLC (commande de liaison de données)
- Support MIB APPN
- Secours automatique
- Fonctions d'émulateur de base

Support de communication SNA

Communications Server peut servir de nœud SNA (Systems Network Architecture) de types 2.0 et 2.1. Ce support permet d'écrire des programmes pour communiquer avec la plupart des produits SNA d'IBM.

APPC/APPN

Communications Server fournit un nœud d'extrémité APPN (Advanced Peer-to-Peer Networking) et un support de nœud de réseau pour les postes de travail, ce qui permet à ces derniers de communiquer de manière plus souple avec les autres systèmes du réseau. En outre, une fonction d'extension de réseau permet d'isoler les branchements pour éviter un trafic CP-CP non nécessaire.

Communications Server fournit un support de communication APPC (Advanced Program-to-Program Communications) entre les programmes de traitement réparti appelés programmes de transactions (TP). Ces derniers peuvent être situés dans n'importe quel nœud du réseau fournissant APPC. APPC utilise le protocole LU 6.2 pour échanger des données entre les programmes situés dans différentes unités logiques (LU). En outre, APPC prend en charge plusieurs liaisons simultanées et sessions parallèles. La sécurité de la conversation ou de la session entre les programmes communiquant est également prise en charge via APPC.

Communications Server fournit un débit APPC dans les environnements de réseau local dont les performances sont critiques. Communications Server prend en charge les connectivités suivantes :

Tableau 1. Connexions APPC prises en charge

Protocoles	Connexion	Type de connexion
Channel	▫ CDLC (OEM) ▫ MPC	
Réseau local (802.2)	▫ Token-Ring ▫ Ethernet ▫ Frame Relay ▫ Émulation de réseau local ATM	
SDLC	▫ Synchrone ▫ Autosynchrone ▫ Modems	▫ Numérotation automatique, Numérotation DTR, Permanente ▫ Numérotation automatique ▫ Numérotation automatique, Permanente ▫ Numérotation automatique
X.25	▫ Synchrone ▫ Hayes** AutoSync ▫ Réseau X.25	▫ Numérotation automatique, Semi-permanente ▫ Numérotation automatique, Permanente ▫ Numérotation automatique
IP	SNA sur IP	Connexions fournies par IP
IP	HPR sur IP	Connexions fournies par IP

Remarque : APPC/APPN est également doté d'une fonction de compression de données. Pour plus de détails, reportez-vous à la section «Compression de données», à la page 63. De même, pour de plus

amples informations sur le chiffrement, reportez-vous à la section «Chiffrement au niveau des sessions SNA», à la page 66.

Support LU SNA de type 6.2

LU 6.2 est une architecture destinée aux communications de programme à programme. Communications Server prend en charge les fonctions de LU 6.2 SNA facultatives suivantes :

- Conversations de base et mappées
- Niveau de confirmation de synchronisation
- Support de sécurité aux niveaux de la session et de la conversation
- Plusieurs LU
- Sessions parallèles, y compris la possibilité d'utilisation d'un système éloigné pour modifier le nombre de sessions
- Transactions en mode simultané unidirectionnel ou bidirectionnel
- Plusieurs liaisons simultanées avec les sessions SSCP-PU, chacune pouvant être connectée à un réseau de secteur

Pour obtenir une liste complète des fonctions, consultez le manuel *Communications Server Programming Guide and Reference*.

Améliorations de configuration APPC

La configuration de base d'un nœud d'extrémité requiert les quatre paramètres suivants : ID réseau, nom du nœud local, type de liaison et adresse de destination. La définition système est réduite par :

- les modes fournis par IBM ;
- la création implicite des définitions de LU partenaire et de mode lors de l'allocation d'une conversation ;
- l'initialisation implicite des limites de session (fonction CNOS), ce qui permet de supprimer l'initialisation explicite requise des limites de session avant que des conversations puissent être allouées ;
- la suppression des limites de session pour les LU locales et partenaire, ce qui permet une plus grande liberté de configuration et d'initialisation des limites de session de mode ;
- les valeurs par défaut des noms, types et modes de fonctionnement des programmes de transactions, ce qui permet d'éliminer le besoin de configurer des définitions de programme de transactions pour des programmes applicables ;
- les mises à jour de configuration dynamiques ;
- les définitions de postes de travail implicites de passerelle SNA ;
- la fonction d'édition d'un fichier .ACG contenant des paramètres de configuration ;
- la fonction de recherche des informations de définition système à l'aide de la fonction de découverte.

Dans la mesure où la fonction SNA est stockée sous forme de fichier texte, il est possible de modifier le fichier rapidement et aisément à l'aide d'un éditeur ou d'un programme écrit par un utilisateur.

Vous pouvez ensuite procéder à la vérification et la mise à jour dynamique d'une configuration active (sans arrêter Communications Server).

À présent, vous pouvez configurer des connexions à plusieurs hôtes, plusieurs connexions hôte pouvant être actives en même temps. Vous pouvez définir les connexions de manière à les démarrer à la demande ou à la suite d'un incident en mode de secours automatique.

La fonction de découverte de Communications Server permet à un nœud de rechercher de façon dynamique le nom du point de contrôle, l'adresse MAC (Medium Access Control) et l'adresse SAP (Service Access Point) d'un autre serveur de nœud de réseau Communications Server sur un réseau local Token Ring ou Ethernet. Cela signifie que l'utilisateur n'a pas besoin de connaître le nom du point de contrôle et les adresses MAC et SAP d'une machine partenaire avant de pouvoir définir une connexion à cette machine. Actuellement, les utilisateurs de Client Access/400 et de Communications Personnelles peuvent faire appel à cette fonction.

Concepts APPC fondamentaux

Cette section présente les concepts et termes APPC.

Programmes de transactions : Il s'agit d'un programme ou d'une partie d'un programme d'application qui utilise les fonctions de communication APPC. Les programmes d'application utilisent ces fonctions pour communiquer avec des programmes d'application d'autres systèmes prenant en charge APPC.

Communications Server fournit l'API APPC et prend en charge le appels CPI-C (Common Programming Interface for Communications) SAA (Systems Application Architecture) d'IBM pour les programmes de transactions.

Les programmes de transactions émettent des paramètres APPC pour appeler des fonctions APPC. Un ***paramètre*** correspond à une demande formatée émise par un programme de transactions et exécutée par APPC. Un programme utilise des séquences de paramètres APPC pour communiquer avec un autre programme. Deux programmes qui communiquent ensemble peuvent être situés sur des systèmes différents ou sur le même système. L'API APPC est la même dans les deux cas.

Lorsqu'un programme de transactions échange des données avec un autre, ce dernier est désigné par programme de transactions ***partenaire***.

Les programmes de transactions peuvent émettre des appels CPI-C. Ces derniers permettent aux programmes d'application de tirer parti de la cohérence fournie par SAA.

Unités logiques : Chaque programme de transactions accède à un réseau SNA via une ***unité logique*** (LU). Une LU est un logiciel SNA qui accepte les paramètres de vos programmes et qui intervient sur ces paramètres. Un programme de transactions émet des paramètres APPC à sa LU. Ces paramètres permet le flux des commandes et données via le réseau à destination d'une LU partenaire. Une LU sert également d'intermédiaire entre les programmes de transactions et le réseau, afin de gérer l'échange de données entre les programmes de transactions.

Une seule LU peut fournir des services destinés à plusieurs programmes de transactions. Plusieurs LU peuvent être simultanément actives dans le nœud.

Types de LU : Communications Server prend en charge les LU de types 0, 1, 2, 3 et 6.2. Les LU de types 0, 1, 2 et 3 prennent en charge la communication entre les programmes d'application hôte et les différents types de périphériques tels que les terminaux et les imprimantes.

La LU 6.2 prend en charge les communications entre deux programmes situés sur des nœuds de secteur de type 5 et/ou des nœuds périphériques de type 2.1, et entre des programmes et des périphériques. APPC est une mise en œuvre de l'architecture LU 6.2.

Sessions LU : Avant qu'une communication puisse être établie entre deux programmes de transactions, les LU associées doivent être connectées dans le cadre d'une relation mutuelle appelée ***session***. Une session permet la connexion de deux LU ; elle est donc désignée par session ***LU-LU***. La figure 1 présente cette relation de communication.

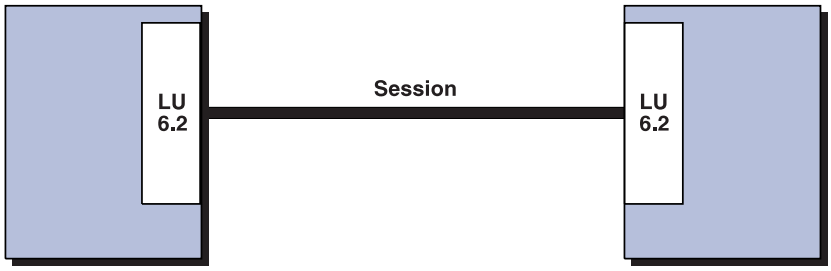


Figure 1. Une session entre deux LU (LU-LU)

Les sessions servent d'intermédiaire gérant le transfert de données entre une paire de LU dans un réseau SNA. En particulier, les sessions traitent des éléments tels que la quantité de données transmises, la sécurité des données, le routage de réseau et l'encombrement de trafic.

Les sessions sont maintenues par des LU. En général, les programmes de transactions ne fonctionnent pas à l'aide des caractéristiques de session. Vous définissez ces dernières lorsque vous :

- configurez votre système ;
- utilisez le **Fonctionnement du nœud SNA** ;
- utilisez les paramètres de gestion.

Conversations de programmes de transactions : La communication entre les programmes de transactions est désignée par ***conversation***. Tout comme une conversation téléphonique, un programme de transactions appelle un autre ; ils engagent une «conversation», un seul programme de transactions communiquant à la fois, jusqu'à ce qu'un programme de transactions mette fin à la conversation. Une conversation démarre lorsqu'un programme de transactions émet un paramètre APPC ou un appel CPI-C qui alloue une conversation. Les conversations ont lieu via des sessions LU-LU.

L'allocation d'une conversation à une session permet d'établir une relation d'émission-réception entre les programmes de transactions connectés à la conversation.

Un des programmes de transactions émet des paramètres pour envoyer des données alors que l'autre émet des paramètres pour recevoir des données. Lorsque le programme de transactions émetteur met fin à l'émission de données, il peut transmettre le contrôle d'émission de la conversation au programme de transactions récepteur. Les conversations peuvent échanger des informations et données de contrôle.

La figure 2 présente une conversation entre deux programmes de transactions qui est établie via une session.

Figure 2. Établissement d'une conversation entre des programmes de transactions via une session

Une session ne peut prendre en charge qu'une seule conversation à la fois, mais une seule session peut prendre en charge plusieurs conversations en série. Dans la mesure où plusieurs conversations peuvent réutiliser les sessions, une session est une connexion de longue durée par comparaison avec une conversation. Lorsqu'un programme alloue une conversation et que toutes les sessions applicables sont en cours d'utilisation, la LU place la connexion entrante (demande d'allocation) dans une file d'attente. Elle effectue l'allocation lorsqu'une session est disponible.

Deux LU peuvent également établir entre elles des sessions parallèles, afin de prendre en charge plusieurs conversations simultanées. Une session parallèle est établie lorsque l'un des programmes de transactions alloue une conversation et qu'une session est disponible, cette dernière étant toutefois utilisée par une conversation. La LU peut demander une nouvelle session afin de répondre à l'allocation.

La figure 3 présente trois sessions parallèles entre deux LU, chaque session acheminant une conversation.

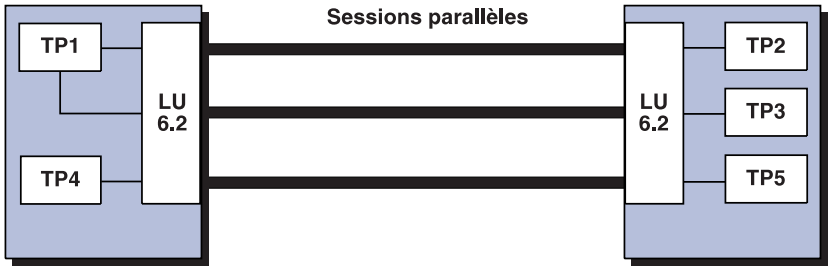


Figure 3. Sessions parallèles entre des LU

APPN

APPN (Advanced Peer-to-Peer Networking) est un ensemble de fonctions, de formats et de protocoles qui permettent d'améliorer considérablement la gestion d'un réseau SNA et la possibilité d'utilisation des applications APPC qui sont en cours d'exécution dans le réseau. APPN réalise ces tâches grâce à la réduction de la configuration requise, aux recherches dynamiques dans les répertoires, aux fonctions de calcul de chemins et au routage de session intermédiaire.

Grâce à APPN, vous pouvez écrire des programmes sans connaître les détails du réseau sous-jacent. Il suffit de connaître le nom de la LU partenaire et non son emplacement. SNA détermine l'emplacement de la LU partenaire et le meilleur chemin de routage de données. Une modification du réseau sous-jacent, par exemple, un changement d'adresse physique, l'ajout d'une nouvelle carte ou le transfert d'une machine, n'ont aucune incidence sur les programmes APPC.

Communications Server fournit un nœud d'extrémité APPN et un support de nœud de réseau pour les postes de travail, ce qui permet à ces derniers de communiquer de manière plus souple avec les autres systèmes du réseau. En outre, une fonction d'extension de réseau permet d'isoler les réseaux pour éviter un trafic CP non nécessaire.

- La fonction de nœud d'extrémité fournit les services suivants :
  - Connexion du nœud local à un nœud de réseau pour les services de répertoire et de routage
  - Réactivation automatique des sessions CP-CP lorsqu'un nœud d'extrémité perd son serveur de nœud de réseau.
- La fonction de nœud de réseau fournit les services suivants :
  - Services de sélection d'acheminement permettant le calcul du meilleur chemin d'une session via un réseau APPN
  - Routage de session intermédiaire permettant l'établissement d'une session entre deux LU figurant dans des nœuds non adjacents, la session traversant un ou plusieurs nœuds intermédiaires
  - Services de répertoire permettant l'identification dynamique des emplacements de LU partenaire
  - Services de réseau de connexion destinés au réseau local, permettant d'identifier les adresses de destination de réseau local sans qu'il soit nécessaire de les configurer

    Cette fonction permet à un nœud d'établir une connexion de liaison directe à un autre nœud lorsqu'aucune adresse de destination de réseau local n'est configurée.
  - Support d'extension de réseau permettant l'interconnexion efficace d'un central de branchement doté de réseaux locaux, de nœuds d'extrémité et de nœuds de réseau bas de gamme comportant des LU dépendantes et indépendantes, et des PU telles que les distributeurs automatiques à un ou plusieurs réseaux longue distance. Cela permet à un nombre plus important de nœuds de réseau de servir de passerelle vers des centraux de dérivation. Un réseau local dans chaque central de dérivation peut être configuré en tant que réseau de connexion.

Interfaces de programmation

Communications Server prend en charge un grand nombre d'interfaces de programmation 32 bits (API) sur le serveur destinées au développeur de programmes d'application. Ces API permettent aux programmes d'application d'accéder aisément aux fonctions de Communications Server et permettent aux applications d'adresser les besoins de communication des connexions aux ordinateurs IBM et non IBM. En outre, les interfaces fournies prennent en charge des protocoles SNA de manière à assurer une normalisation.

Voici les API prises en charge :

- APPC (Advanced Program-to-Program Communications)
- CPI-C (Common Programming Interface for Communications)
- RUI et SLI d'interface d'application LU (LUA) conventionnelle
- Bibliothèques HACL (Host Access Class Libraries)
- CPI-C Java (JCPI-C)
- WinSock (en association avec AnyNet Sockets sur SNA)
- Fonction NOF (Network Operator Facility)
- Services de gestion
- Services communs

Côté clients, l'API EHNAPPC (Enhanced APPC) est également fournie.

Le kit de développement logiciel de Communications Server (qui peut séparément être installé à partir du CD-ROM Communications Server) est également disponible pour les développeurs d'application. Ce kit contient des modèles, des fichiers d'en-tête, des fichiers de bibliothèque et des manuels en ligne pour chacune des API.

Pour plus de détails sur les interfaces de programmation de Communications Server, consultez les manuels *Client/Server Communications Programming* et *System Management Programming*.

Routage hautes performances (HPR)

Il s'agit d'une amélioration apportée à APPN, permettant d'augmenter la fiabilité et les performances de routage de données, et d'établir une liaison virtuelle entre les nœuds RTP. HPR remplace le routage de session intermédiaire qui correspond à la technique de routage utilisée dans l'APPN.

HPR fournit une transmission plus rapide au niveau des nœuds intermédiaires, réachemine les sessions sans interruption autour des nœuds et liaisons défectueux et régule le flux de trafic en prévoyant et réduisant l'encombrement au sein du réseau.

Communications Server prend en charge les connexions HPR via des liaisons Enterprise Extender (IP), SDLC (commande de liaison de donnée synchrones), par réseau local, par réseau longue distance, par canal, MPC (Multi-Path Channel) et X.25.

Compression de données SNA

La compression de données au niveau de la session augmente le débit des grandes quantités de données via les liaisons de communication, ce qui donne lieu aux avantages suivants :

- Amélioration du débit de données sur les lignes à faible vitesse
- Réduction des coûts sur des lignes à coût élevé
- Temps de réponse plus rapides, donnant lieu à des améliorations de productivité

La compression de données SNA est compatible avec les mises en œuvre IBM 390 et AS/400 et peut être utilisée avec tous les types de LU.

Découverte de prestataires de services

La fonction de découverte s'appuie sur un protocole de résolution d'adresses de réseau local qui peut être utilisé par un nœud sur le réseau local, afin de rechercher un autre nœud selon des critères spécifiques. Si vous affinez les paramètres de la fonction, un nœud peut rechercher des nœuds de réseau APPN, des nœuds assurant des fonctions de frontières SNA, des systèmes AS/400, des passerelles SNA ou des classes de serveur définies par l'utilisateur. Un serveur Communications Server pour Windows NT peut répondre aux requêtes des clients en tant que serveur de nœud de réseau, passerelle PU 2.0 ou classe de serveur définie par l'utilisateur. Un Communications Server peut également utiliser la fonction de découverte pour rechercher des nœuds APPN et des passerelles SNA.

Demandeur de LU dépendantes (DLUR)

Communications Server fournit un support de nœud d'extrémité DLUR et de nœud de réseau pour les postes de travail, permettant à ces derniers de tirer parti du support SSCP (centre directeur des services système) évolué fourni par un serveur de LU dépendantes (DLUS). Le serveur DLUS est pris en charge par VTAM version 4, édition 2 et ultérieure. Ce support permet aux LU dépendantes SNA traditionnelles, par exemple, les émulateurs voire les imprimantes, de bénéficier des nombreux avantages d'un réseau APPN.

Voici quelques-uns de ces avantages :

- Possibilité pour les LU dépendantes de résider sur des nœuds non adjacents à l'hôte ;
- Utilisation de la logique de recherche APPN afin de fournir le meilleur chemin pour les sessions LU-LU.

Pour plus d'informations sur le demandeur DLUR, reportez-vous à la section «Support de demandeur d'unités logiques dépendantes», à la page 59.

Passerelle SNA

Une passerelle permet la communication entre les systèmes hôtes qui prennent en charge des postes de travail PU 2.0 et des postes de travail utilisant des types de DLC différents. Une passerelle SNA peut :

- permettre aux postes de travail de partager la même liaison hôte ;
- fournir la connectivité de plusieurs hôtes aux postes de travail qui ne prennent pas en charge plusieurs PU ;

- servir de groupe de PU pour les postes de travail PU en aval dédiés ;
- servir de convertisseur de protocole entre les postes de travail qui utilisent sur leurs liaisons des DLC différentes de celle utilisée sur la liaison hôte ;
- réduire le nombre des définitions système au niveau de l'hôte et des postes de travail ;
- permettre la modification dynamique des définitions de réseau et l'ajout de postes de travail ;
- réduire les ressources hôte et le nombre de connexions hôte à l'aide de groupes de LU et de la fermeture automatique des sessions qui ne sont pas utilisées pendant une durée indiquée par l'utilisateur ;
- améliorer la fiabilité en assurant une liaison de secours à l'hôte.

La passerelle SNA permet à un hôte de la famille IBM 390 de prendre en charge des postes de travail qui mettent en œuvre la LU 0, 1, 2 ou 3, ou la LU 6.2 dépendante (APPC). La passerelle SNA prend également en charge la LU 0, 1, 2 ou 3 vers un hôte AS/400. L'hôte AS/400 transmet les données à un hôte de la famille IBM 390.

La passerelle SNA est considérée par chaque hôte comme un nœud SNA PU 2.0 prenant en charge une ou plusieurs LU par poste de travail. En ce qui concerne l'hôte, toutes les LU font partie de la PU de passerelle SNA. La passerelle SNA peut disposer de plusieurs connexions simultanées à l'hôte et diriger des sessions de postes de travail différentes à des hôtes spécifiques. Cependant, un seul hôte (qui doit également figurer sur une liaison avec une PU CP) peut servir de point focal, et le nom du point de contrôle est ajouté à tous les NMVT (Network Management Vector Transport) acheminés via la passerelle.

La passerelle SNA est considérée par les postes de travail pris en charge comme un contrôleur de communication SNA PU 4 ; elle transmet des messages d'hôte tels que BIND et UNBIND. Les LU de réseau ne sont pas informées de l'existence de la passerelle SNA. Cependant, cette dernière est informée de toutes les LU des postes de travail.

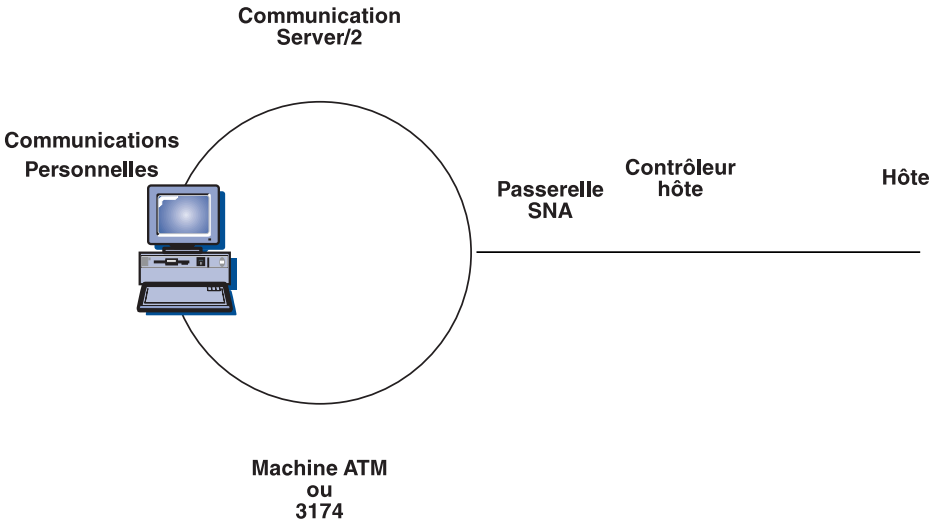
En effet, la passerelle SNA est un type particulier de PU 2.0. Aussi longtemps qu'un poste de travail dépendant est inactif, la passerelle SNA met en œuvre les fonctions de LU pour le poste de travail selon la même procédure utilisée par une vraie PU 2.0. Cependant, dès qu'un poste de travail est connecté à l'hôte, la passerelle SNA permet à ce poste de mettre en œuvre des fonctions de LU et transmet simplement des données entre les postes de travail et l'hôte.

Une passerelle SNA permet aux applications de postes de travail prises en charge d'accéder aux applications distantes prises en charge sur un réseau de secteur sans qu'une connexion directe distincte à chaque hôte de chaque poste de travail soit nécessaire. L'hôte considère qu'il est doté d'une seule connexion à la passerelle.

Pour plus de détails sur l'utilisation d'une passerelle SNA, reportez-vous à la section «Planification de la passerelle SNA», à la page 119.

La figure 4 illustre un exemple de connexion utilisant une passerelle SNA.

Présentation des fonctions de Communications Server



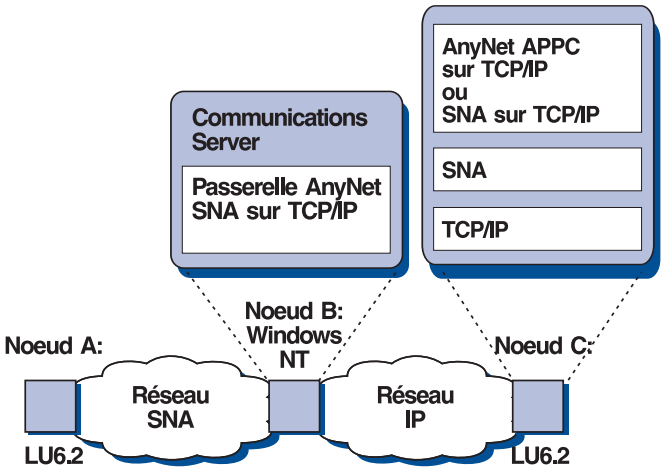


Figure 5. Passerelle SNA sur TCP/IP

Sockets sur SNA

La fonction de nœud d'accès Sockets sur SNA permet aux programmes d'application TCP/IP utilisant les interfaces Socket WinSock 1.1 et WinSock 2.0 de communiquer via un réseau SNA.

La fonction de passerelle Sockets sur SNA permet aux applications Socket des réseaux SNA et TCP/IP de communiquer. Les passerelles Sockets sur SNA servent généralement à connecter des réseaux TCP/IP isolés, à l'aide d'un réseau fédérateur SNA.

La figure 6 présente des applications Socket communiquant via une passerelle Sockets sur SNA à travers des réseaux IP et SNA.

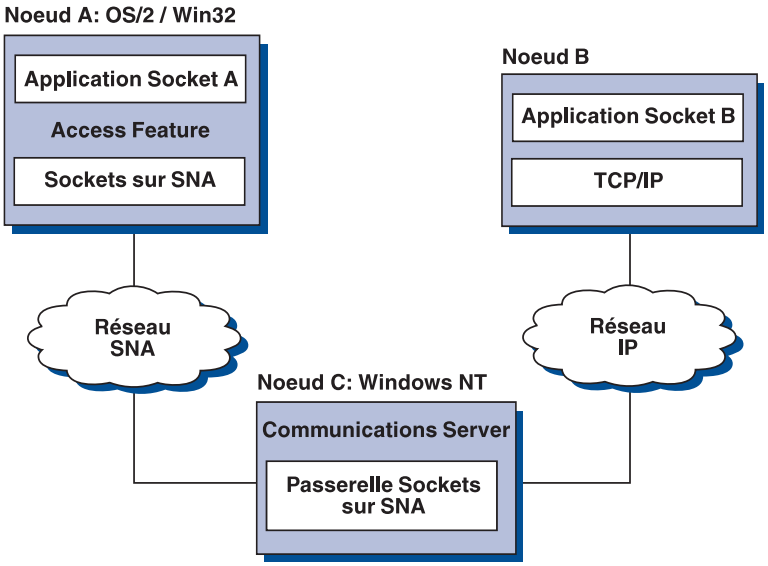


Figure 6. Passerelle Sockets sur SNA

Serveur TN3270E

La fonction de serveur TN3270E permet aux utilisateurs TCP/IP d'accéder aux applications d'une machine hôte au sein d'un réseau SNA. Tout poste de travail client TN3270 ou TN3270E conforme aux normes de l'industrie peut se connecter au serveur TN3270E afin d'accéder aux réseaux SNA. Le serveur TN3270E prend en charge la gestion des touches ATTN et SYSREQ et permet aux utilisateurs d'imprimer à partir d'applications hôte sur des imprimantes connectées à leur poste de travail. Il se peut que ces imprimantes soient connectées en local ou en réseau.

Communications Server prend en charge l'équilibrage de charge pour les connexions client d'un serveur TN3270E qui se connecte aux mêmes ressources hôte si l'équilibrage de charge est activé au niveau du client.

Le serveur TN3270E prend en charge le filtrage d'adresses IP et de noms d'hôte qui permet un accès contrôlé aux LU sans modifier les configurations de client.

Le serveur TN3270E prend également en charge les fonctions d'authentification et de chiffrement SSL (Secure Sockets Layer) assurant un accès sécurisé via le réseau TCP/IP. Si une sécurité est définie, le serveur doit disposer d'un certificat authentifié fourni par une autorité de certification telle que Verisign. Communications Server fournit un utilitaire qui génère et gère les clés et les certificats utilisés par SSL version 3.

La figure 7 illustre un exemple de connexions de serveur TN3270E.

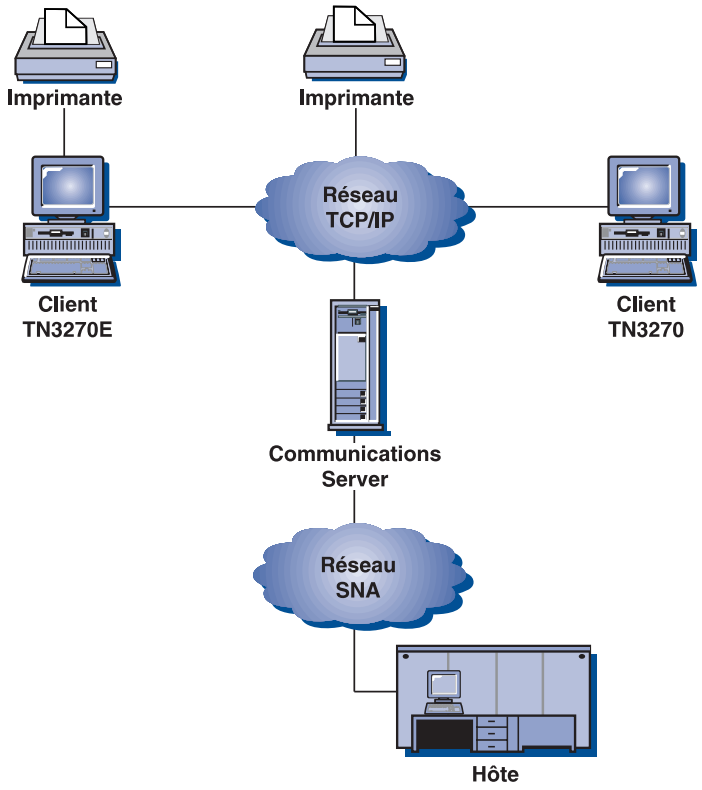


Figure 7. Connexions de serveur TN3270E

Serveur TN5250

La fonction de serveur TN5250 permet aux utilisateurs TCP/IP d'accéder aux applications d'un AS/400 au sein d'un réseau SNA. Tout poste de travail client TN5250 conforme aux normes de l'industrie peut se connecter au serveur TN5250 afin d'accéder aux réseaux SNA.

Communications Server prend en charge l'équilibrage de charge pour les connexions client d'un serveur TN5250 qui se connecte aux mêmes AS/400 si l'équilibrage de charge est activé au niveau du client.

Le serveur TN5250 prend en charge le filtrage d'adresses IP et de noms d'hôte qui permet l'administration centralisée de l'accès client au serveur, ainsi que l'orientation des clients vers des AS/400 spécifiques.

Le serveur TN5250 prend également en charge les fonctions d'authentification et de chiffrement SSL (Secure Sockets Layer) assurant un accès sécurisé via le réseau TCP/IP. Si une sécurité est définie, le serveur doit disposer d'un certificat authentifié fourni par une autorité de certification telle que Verisign. Communications Server fournit un utilitaire qui génère et gère les clés et les certificats utilisés par SSL version 3.

La figure 8 illustre un exemple de connexions de serveur TN5250.

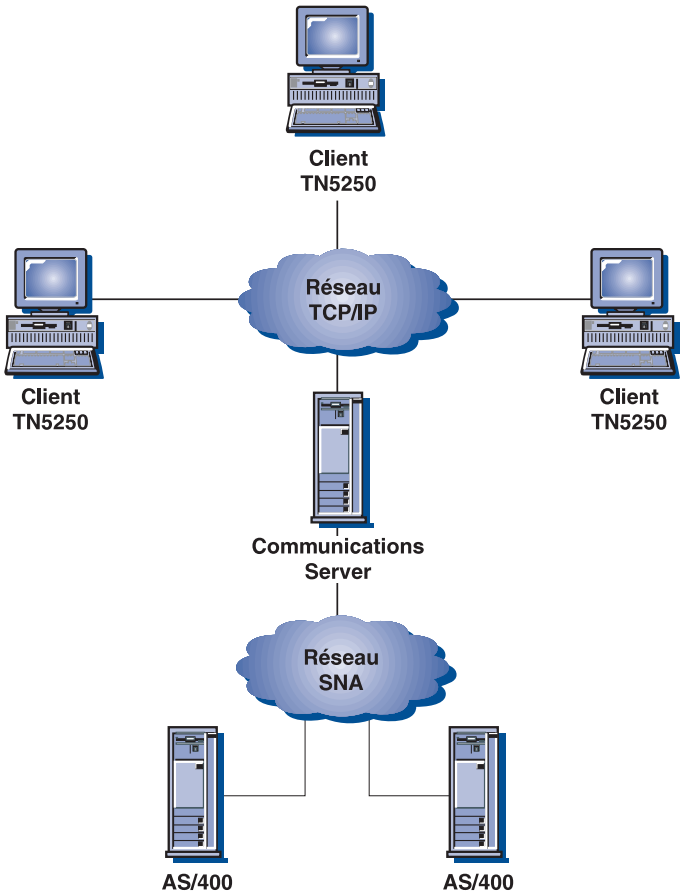


Figure 8. Connexions de serveur TN5250

Accès aux données existantes

Communications Server permet d'accéder aux données des machines hôte, des AS/400 et des postes de travail des réseaux SNA, à l'aide des fonctions suivantes :

- AS/400 OLE DB Provider
- Host Publisher
- Serveur de dossiers partagés AS/400

AS/400 OLE DB Provider

Les applications qui utilisent OLE DB ou ActiveX peuvent communiquer via Communications Server pour l'accès de niveau enregistrement aux fichiers d'un système AS/400. La documentation de cette fonction et les informations relatives au développement de ces applications utilisant Client Access sont fournies dans le répertoire `csnt\sdk\as4▫▫_oledb`.

Host Publisher

Host Publisher permet d'accéder aux sites Web à grand volume Web ayant un contenu dynamique. Vous pouvez utiliser Host Publisher pour accéder aux données d'hôtes IBM 390 ou AS/400 et pour les publier sur des pages Web créées de façon dynamique à partir de votre modèle.

Serveur de dossiers partagés AS/400

Le système AS/400 utilise une structure appelée dossier pour stocker et organiser des documents, du courrier et d'autres objets associés. Communications Server permet de créer sur le serveur des unités de disque communiquant avec des dossiers AS/400 via le système de fichiers intégré (IFS) AS/400. En outre, si le serveur partage ces unités de disque, les clients peuvent se connecter à elles à l'aide de la commande NET USE. Plusieurs clients peuvent ainsi se connecter aux dossiers du système AS/400 comme s'il s'agissait d'unités sur leurs postes de travail.

L'utilisation des dossiers partagés permet de bénéficier des fonctions suivantes :

- Utilisation du système de sécurité AS/400 pour limiter l'accès aux fichiers des postes de travail
- Partage de données entre plusieurs utilisateurs à la fois
- Sauvegarde des fichiers des postes de travail dans un dossier AS/400

Support client de Communications Server

Communications Server fournit un support pour les clients API SNA (disponible sur le CD-ROM) et pour les clients Novell IntranetWare pour SAA.

Support Client API SNA

Le support Client API SNA de Communications Server permet aux clients connectés via TCP/IP et IPX d'accéder aux API SNA sans qu'un flux de protocoles SNA soit nécessaire entre les clients et le serveur. Ainsi, la plus grande partie de la configuration SNA s'effectue au niveau du serveur central.

Communications Server prend en charge les clients API SNA sous Windows 95, Windows NT, Windows 3.1 et OS/2.

Les clients SNA fournissent un support pour les interfaces API CPI-C, APPC, EHNAPPC, LUA RUI, JCPI-C et HACL, tout en assurant le réel traitement SNA au niveau du serveur. Ces clients sont livrés dans le cadre du serveur ; cependant, ils sont installés et configurés au niveau du client.

Les clients Windows et OS/2 32 bits font l'objet des améliorations supplémentaires suivantes :

- Chiffrement entre le client et le serveur
- Formatage de trace plus détaillé, permettant un débogage plus rapide des incidents
- Possibilité de lancement et d'arrêt de la fonction de trace lors de l'exécution du client
- Possibilité de réinstallation du client sans désinstallation

Les clients Windows NT et Windows 95 s'exécutent à partir du même exécutable. Ce dernier peut être installé sur une unité partagée ; toute modification s'applique aux deux clients. Le nouveau client Windows 32 bits peut communiquer avec les serveurs Communications Server, Novell IntranetWare ou NetWare pour SAA.

Pour plus de détails sur les clients API de Communications Server, reportez-vous à la section «Planification des communications client/serveur», à la page 99.

Support Client Novell IntranetWare pour SAA

Communications Server prend en charge les clients connectés via IPX ou TCP/IP qui exécutent des progiciels d'émulateur mettant en œuvre l'architecture QEL/MU (Queue Element/Message Unit) de Novell pour l'émulation 3270, ce qui permet aux clients d'accéder aux données hôte de l'ordinateur central. Le support des fonctions client courantes y est inclus, notamment les catégories de LU spécifiques, de groupe et publiques (parfois désignées par types de ressources).

Communications Server prend en charge les clients Novell IntranetWare pour SAA sous Windows 95, Windows NT, Windows 3.1 et OS/2.

Pour plus de détails sur le développement de ces clients, consultez le manuel *Novell NetWare for SAA 3270 Client Interface Guide and Reference* réf. 100–002018–001.

Équilibrage de charge

Communications Server prend désormais en charge l'équilibrage de charge pour tous les types de clients. L'équilibrage de charge permet de répartir des sessions LU 0 à 3 et LU 6.2 via les serveurs Communications Server et IntranetWare pour SAA. Le serveur fait de la publicité pour des services, notamment les facteurs de charge, que les clients ou les serveurs peuvent rassembler et organiser pour sélectionner un serveur.

Exploitation de répertoire

Vous pouvez configurer plusieurs clients à partir d'un emplacement central, à l'aide du protocole LDAP (Lightweight Directory Access Protocol), afin de simplifier le processus de configuration.

Pour plus de détails, reportez-vous à la section «Planification des communications client/serveur», à la page 99.

Support de configuration et d'administration

Communications Server fournit des fonctions permettant la configuration et l'administration des ressources.

Configuration de Communications Server

La présente section donne un aperçu des composants de configuration de Communications Server et des méthodes servant à les créer ou à les modifier. La configuration est constituée d'un seul fichier (ACG) stocké dans le sous-répertoire PRIVATE du répertoire d'installation du produit (par exemple, C:\IBMCS\PRIVATE). Le fichier ACG peut être créé ou modifié par à l'aide de l'utilitaire **Configuration du nœud**, ou d'un éditeur ASCII. Un programme de vérification permet de vérifier la validité du fichier ACG avant que ce dernier soit utilisé.

Les méthodes suivantes vous permettent de créer ou de modifier une configuration Communications Server :

- **Configuration du nœud**
- Configuration du fichier réponses

Configuration du nœud : Communications Server fournit l'application **Configuration du nœud** (PCSCFG) qui permet de configurer les fonctions de Communications Server à l'aide d'une interface graphique et qui fournit des valeurs par défaut permettant de configurer aisément ces fonctions à l'aide d'un minimum de paramètres. Lors d'une configuration, une étape de vérification automatique permet d'examiner la configuration créée et, en l'absence de conflits, de créer les fichiers de configuration requis. En l'absence de conflits, les erreurs sont signalées de sorte qu'elles puissent être corrigées dans la configuration.

La configuration locale est prise en charge au niveau du client et du serveur. La configuration distante du serveur est prise en charge à partir de clients Windows NT et Windows 95.

La plupart des configurations peuvent être créées à l'aide de l'application **Configuration du nœud**. Cependant, cette dernière ne prend pas en charge certains mots clés et paramètres de mots clés.

Configuration du fichier réponses : La configuration du fichier réponses permet de personnaliser un modèle de fichier de configuration répondant aux besoins de certains utilisateurs. Pour plus de détails sur l'utilisation des fichiers réponses à des fins de configuration, reportez-vous à la section «Configuration à l'aide de fichiers modèles et réponses», à la page 196.

Fonctionnement du nœud SNA : permet de créer et de modifier des ressources sélectionnées.

Administration de Communications Server

Communications Server fournit les fonctions suivantes pour l'administration des ressources.

- **Fonctionnement du nœud SNA**
- Utilitaires de la ligne de commande
- Administration Web
- Module Tivoli Plus

Pour plus de détails sur ces fonctions, reportez-vous à la section «Outils de gestion système», à la page 207.

Équilibrage de charge

Il s'agit d'une fonction de Communications Server qui permet l'équilibrage dynamique des sessions LU dépendantes (hôte-poste de travail) et des sessions LU 6.2 indépendantes en les distribuant au serveur de communication à l'aide d'une charge minimale. Communications Server effectue un équilibrage de charge pour les programmes API de Communications Server et pour les émulateurs 3270 tiers qui se connectent via des protocoles TCP/IP, ou pour les émulateurs TN3270 et TN5250 tiers. Les ressources permettant cet équilibrage sont fonction du type de session :

- Pour les sessions LU dépendantes, la charge est répartie à travers les serveurs dans un groupe de LU et un secteur définis.
- Pour les sessions LU 6.2, la charge est répartie à travers tous les serveurs disponibles dans un secteur défini ou à travers des serveurs sélectionnés d'une liste de serveurs définie.

Les fonctions d'équilibrage de charge de Communications Server sont intégrées aux API client SNA. L'équilibrage de charge est configuré pour les clients à l'aide de l'utilitaire **Configuration du client SNA**.

Pour les sessions LU dépendantes, les émulateurs qui utilisent des API client SNA peuvent participer à l'équilibrage de charge. Dans les autres cas, vous devez vous procurer un logiciel d'émulation 3270, TN3270 ou TN5250 tiers qui prend en charge l'équilibrage de charge.

Pour les sessions LU 6.2, la première connexion établie par un client API SNA détermine le serveur qui gère toutes les sessions LU 6.2 ultérieures.

Pour plus de détails sur l'équilibrage de charge, reportez-vous à la section «Planification de l'équilibrage de charge», à la page 147.

Sécurité de données

Communications Server fournit un support de sécurité de base et évolué aux niveaux de la session et de la conversation. La sécurité consiste à déterminer les utilisateurs Windows NT qui peuvent accéder aux ressources SNA via les clients API SNA. La sécurité de la conversation comporte un support permettant la substitution de mots de passe. Une sécurité LU-LU évoluée est également disponible.

Communications Server fournit un support de sécurité SSL (Secure Sockets Layer) pour les connexions entre les clients TN et le serveur TN3270E ou TN5250.

Cette sécurité utilise SSL version 3 pour fournir le chiffrement de données et l'authentification du serveur à l'aide de certificats signés.

Support de cartes

Communications Server fournit une interface ouverte destinée aux constructeurs de cartes de sorte que ces derniers apportent des solutions de connectivité. Une interface de carte mince (non programmable) permet aux constructeurs de cartes de gérer la pile de protocole SDLC et X.25 de Communications Server. Une interface de carte profonde (programmable) permet aux constructeurs de cartes d'apporter des solutions de connectivité à l'aide des commandes de liaison de données fournies par les constructeurs.

DLC (commande de liaison de données)

Communications Server permet de communiquer via les DLC suivants :

- AnyNet (SNA sur TCP/IP)
- Twinaxial (en amont uniquement)
- Réseau local (toute carte réseau conforme à NDIS**)
- SDLC X.25 (synchrone, asynchrone et AutoSync)
- OEM (support de carte d'un constructeur tiers)
- Channel (en amont uniquement)
- MPC (Multi-Path Channel) (HPR uniquement)
- Enterprise Extender

DLC AnyNet (SNA sur TCP/IP)

Pour plus de détails sur le DLC AnyNet SNA sur TCP/IP DLC, reportez-vous à la section «SNA sur TCP/IP», à la page 14.

DLC IBM MPC

Le DLC MPC (Multi-Path Channel) fournit des connexions par fibres optiques à grande capacité et à haute disponibilité à un ou plusieurs hôtes IBM 390 prenant en charge MPC via la carte Channel ESCON (réf. 9663 001). Les connexions MPC fournissent des vitesses de transmission de données élevées avec un système de secours transparent lors de l'interruption ou de la non disponibilité temporaire des connexions physiques. Cette connexion de canal à canal vous permet de fournir aux clients de réseau local d'accéder aisément aux ressources et services IBM 390.

DLC Enterprise Extender

Communications Server fournit désormais des connexions HPR sur les réseaux IP à l'aide de paquets UDP/IP. Pour le réseau HPR, le réseau fédérateur IP s'avère une liaison logique. Pour le réseau IP, le trafic SNA semble être des datagrammes UDP. Ces derniers sont acheminés sans aucune modification au réseau fédérateur IP. Étant donné qu'il n'y a pas de transformation de protocole et que le regroupement a lieu au niveau de la couche routage sans autres couches de transport, il en résulte une utilisation efficace de l'infrastructure Intranet pour les clients IP qui accèdent aux données basées sur SNA (par exemple, clients TN3270 ou navigateurs Web utilisant IBM Host on Demand), ainsi que pour les clients SNA.

Support MIB APPN

Communications Server prend en charge les demandes SNMP (Simple Network Management Protocol) relatives aux informations de gestion APPN de tout système de gestion SNMP.

Secours automatique

Communications Server permet de configurer certaines liaisons hôte de sorte que celles-ci s'activent automatiquement en cas d'incident au niveau d'un serveur critique défini. Les connexions configurées à un hôte peuvent continuer de fonctionner grâce à l'activation de connexions secondaires sur un serveur de secours. Il s'agit de la fonction de secours automatique.

Les connexions définies dans une configuration de serveur critique sur le serveur de secours sont activées lorsque ce dernier détecte une perte de contact au niveau du serveur critique et que des redevances de licence afférentes au serveur critique sont gérées sur le serveur de secours.

Remarque : La fonction de secours automatique permet l'activation de connexions hôte sur un serveur de secours et dépend de l'utilisation du logiciel d'émulation qui prend en charge le routage secondaire vers le serveur de secours lorsqu'un serveur critique devient inactif.

Pour plus de détails sur l'utilisation de la fonction de secours automatique pour les connexions de secours, reportez-vous à la section «Planification des connexions hôte de secours», à la page 151.

Fonctions d'émulateur de base

Communications Server comporte une version de base de l'émulateur Communications Personnelles 3270 et 5250 à des fins administratives. Cet émulateur fournit sur le serveur un support 5250 et 3270 de base qui contient un sous-ensemble des fonctions et caractéristiques de la famille des émulateurs Communications Personnelles d'IBM à fonctions intégrales.

Voici les fonctions d'émulation de base fournies :

- Définition des couleurs
- Transfert de la ligne de commande (3270 uniquement)
- Jeu complet de polices de caractères
- Tailles d'écran mod 2-5
- Deux sessions

Bien que la redéfinition de clavier graphique ne soit pas prise en charge pour l'émulateur de base, vous pouvez utiliser les fichiers de redéfinition générés par l'émulateur à fonctions intégrales.

Communications Server et SNA

Le présent chapitre décrit les fonctions de réseau SNA fournies par Communications Server et comporte les rubriques suivantes :

- Présentation générale des fonctions SNA
- Définitions DLC
- APPN (Advanced Peer-to-Peer Networking)
- Routage hautes performances (HPR)
- Support de LU
- Compression de données
- Chiffrement
- Services de gestion
- Contrôle de flux
- Support de passerelle SNA

Présentation générale des fonctions SNA

La présente section explique comment Communications Server met en œuvre SNA sur un poste de travail. Il ne s'agit pas d'une description détaillée des fonctions SNA. Pour de plus amples informations sur SNA, consultez les manuels suivants :

- *Systems Network Architecture Concepts and Products*
- *Systems Network Architecture Technical Overview*
- *Systems Network Architecture Network Product Formats* (disponible en ligne dans la liste de documentation de Communications Server)
- *Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic for LU Type 6.2*

SNA définit les normes, les protocoles et les fonctions utilisés par les périphériques du réseau (ordinateurs centraux, terminaux, etc.) pour communiquer entre eux. Cette communication permet à ces périphériques de partager de façon transparente les informations et les ressources de traitement. En d'autres termes, il n'est pas nécessaire qu'un utilisateur de poste de travail soit informé des événements qui se produisent à l'arrière-plan pour accéder aux informations résidant sur un hôte ou pour communiquer avec un autre utilisateur.

Un réseau SNA est organisé sous la forme d'un système de nœuds et de liaisons. Il est important de se rappeler que cette organisation est logique. SNA classe les nœuds en fonction de leurs capacités et de la quantité de contrôle qu'ils exercent sur les autres nœuds du réseau. Le type de nœud n'est pas nécessairement associé à un type de matériel spécifique. Les fonctions d'un nœud peuvent être effectuées par des périphériques différents. Un poste de travail servant de passerelle peut effectuer les mêmes fonctions qu'un contrôleur de communication. Il se peut également qu'un seul périphérique contienne plusieurs nœuds.

Le réseau SNA est responsable du transfert de données entre deux utilisateurs finals de manière efficace, ordonnée et fiable.

Par exemple, lorsqu'un utilisateur d'un poste de travail envoie un message à un autre poste de travail, SNA effectue les opérations suivantes :

- Présentation du message dans un format pouvant être utilisé sur le type de liaison
- Adressage du module
- Sélection d'un chemin pour le message
- Surveillance de la communication pour assurer que le message arrive à destination
- Reconversion du message à un format pouvant être utilisé à destination

Ces tâches sont définies dans SNA sous forme de couches fonctionnelles distinctes. Ces dernières ne font pas partie de la présente description ; cependant, il est important de se rappeler que toutes les couches SNA font partie d'une liaison logique.

Comme indiqué plus haut, les nœuds SNA sont classés en fonction de leurs capacités de communication et de la quantité de contrôle exercée par le nœud sur les autres nœuds du réseau. Les nœuds SNA sont généralement classés sous forme de nœuds de secteur et de nœuds périphériques. Les nœuds de secteur ressemblent aux concentrateurs et peuvent communiquer avec les nœuds périphériques et avec d'autres nœuds de secteur. Les nœuds de secteur activent et contrôlent les ressources des nœuds périphériques. Ils sont également classés comme nœuds de type 4 ou 5. Les nœuds de type 5 contiennent un centre directeur des services système (SSCP) qui fournit un point de contrôle central pour les nœuds de type 4 qui lui sont connectés. Un nœud de type 5 est parfois désigné par nœud hôte. Un nœud périphérique ne peut communiquer directement qu'avec le nœud de secteur qui lui est connecté. Cependant, un nœud périphérique peut contrôler les périphériques auxquels il est relié. Par exemple, un contrôleur de grappe servant de nœud périphérique peut prendre en charge les terminaux qui lui sont connectés. Les nœuds périphériques sont également désignés par nœuds de type 2 ou 2.1.

Chaque nœud contient des unités adressables de réseau (NAU) qui effectuent des fonctions de contrôle et de communication. Une de ces unités NAU correspond à une unité physique (PU). La PU gère les ressources physiques du nœud. Les autres NAU appelées unités logiques (LU) fournissent des points d'accès logique au réseau, qui permettent une communication entre les utilisateurs et les applications de chaque nœud. La communication entre les unités logiques est désignée par session. Les sessions prennent en charge non seulement les communications entre les utilisateurs et les applications mais aussi celles entre les applications afin de partager les ressources de traitement. La communication entre les applications est désignée par APPC (Advanced Program-to-Program Communication). APPC est un ensemble de protocoles et de conventions de programmation mettant en œuvre LU 6.2. (APPC est le nom attribué à la fonction LU 6.2 dans les produits qui mettent en œuvre ce type de LU.)

Profils DLC

La procédure DLC (Data Link Control) permet des échanges de données ordonnés entre deux nœuds via une liaison logique. Le DLC fournit les protocoles nécessaires au transfert fiable des unités de transmission de base (BTU) entre une paire de nœuds dans le réseau SNA. Vous devez configurer les profils DLC appropriés de Communications Server de sorte qu'un poste de travail accède à un réseau SNA.

Pour plus de détails sur la configuration des profils DLC appropriés, consultez le *Tutorial* en ligne.

APPN

APPN (Advanced Peer-to-Peer Networking) est une extension de SNA qui ajoute des fonctions de communication à celles décrites dans les sections précédentes. En voici les composants de base :

- Types de nœuds APPN
- Points de contrôle
- Extension de réseau
- Procédure DLC
- Liaisons logiques
- Services de répertoire
- Services de topologie et de sélection d'acheminement

Types de nœuds APPN

La présente section décrit les trois types de nœuds mis en œuvre par Communications Server, qui peuvent participer dans un réseau APPN :

- Nœud de réseau
- Nœud d'extrémité
- Nœud réseau de niveau inférieur (LEN)

Par ailleurs, l'extension de réseau est une fonction qui s'ajoute à un nœud de réseau. Même si elle fournit des services aux nœuds d'extrémité comme un nœud de réseau, elle apparaît dans le réseau comme un nœud d'extrémité connecté à d'autres nœuds de réseau.

La distinction entre chaque nœud du réseau se fait à l'aide d'un nom unique constitué de deux parties : un ID réseau et un nom de nœud local (également désigné par nom de point de contrôle [CP]). Ce nom identifie chaque nœud pour tous les autres nœuds du réseau. De même, le nœud peut porter plusieurs noms de PU pour accéder simultanément à plusieurs hôtes PU T4/5.

Un nœud peut être configuré comme nœud d'extrémité ou nœud de réseau mais, lorsqu'un nœud d'extrémité ne dispose pas de sessions CP-CP (voir la section «Sessions CP-CP», à la page 30) avec un nœud de réseau APPN, il sert de nœud LEN. Un nœud LEN ne prend pas en charge les fonctions APPN.

Un nœud de réseau fournit les fonctions suivantes :

- Services de session LU-LU pour ses LU locales
- Routage de session intermédiaire
- Fonctions de serveur de réseau (permettant d'effectuer des recherches de répertoire de réseau et la sélection d'acheminement) destinées aux nœuds d'extrémité et aux nœuds LEN (ainsi que pour ses propres LU locales)
- Fonction de routage de services de gestion aux fins de transmission des données de service de gestion (par exemple, les alertes) entre un nœud d'extrémité pris en charge et un point focal de services de gestion.

Nœud d'extrémité

Un nœud d'extrémité fonctionne dans un environnement d'égal à égal destiné aux sessions LU-LU (utilisant les protocoles LU 6.2) tout en fournissant d'autres fonctions APPN. Un nœud d'extrémité fournit des fonctions APPN, par exemple, des services de répertoire et de sélection d'acheminement aux utilisateurs finals de son propre nœud. Il peut participer au réseau APPN en utilisant les services d'un serveur de nœud de réseau connecté pour les requêtes de session impliquant les nœuds non connectés directement ; pour ce faire, il échange des requêtes et réponses relatives aux services de répertoire avec un nœud de réseau adjacent (son serveur), à l'aide de sessions CP-CP.

Les nœuds d'extrémité APPN peuvent enregistrer leurs LU locales sur leur serveur de nœud de réseau. Ainsi, l'opérateur de réseau du serveur de nœud de réseau n'a pas besoin de prédéfinir le nom des LU de tous les nœuds d'extrémité connectés pour lesquels le nœud de réseau fournit des services.

Un nœud d'extrémité APPN peut être connecté à plusieurs nœuds de réseau mais il ne peut disposer de sessions CP-CP actives qu'avec un seul nœud de réseau à la fois : son serveur de nœud de réseau. Les autres nœuds de réseau peuvent être utilisés pour assurer le routage de session intermédiaire pour le nœud d'extrémité, ou servir en tant que remplaçant du serveur de nœud de réseau si le serveur de nœud de réseau principal n'est pas disponible. Les sessions CP-CP ne sont jamais établies entre deux nœuds d'extrémité.

Nœuds LEN

Il s'agit d'un nœud qui met en œuvre les protocoles T2.1 de base sans les améliorations d'APPN. Dans un nœud LEN, toutes les éventuelles connexions avec des LU partenaire sont prédéfinies avant que des session soient établies avec celles-ci. Un nœud LEN connecté à un nœud de réseau APPN adjacent utilise les fonctions évoluées d'APPN en prédéfinissant des connexions potentielles avec des LU partenaire comme si elles existaient au niveau de ce nœud de réseau Quant au nœud de réseau, il peut automatiquement servir de serveur de nœud de réseau du nœud LEN, localiser la réelle destination de la LU partenaire et sélectionner le meilleur chemin menant à celle-ci. Le nœud LEN traverse un nœud de réseau pour participer dans un réseau APPN sans que des connexions directes à tous les nœuds soient nécessaires.

Points de contrôle

Le point de contrôle (CP) est responsable de la gestion du nœud et des ressources de ce dernier. Pour accéder aux services de réseau APPN, le point de contrôle d'un nœud d'extrémité APPN doit communiquer avec le point de contrôle d'un nœud de réseau adjacent. De même, pour gérer le réseau, le point de contrôle d'un nœud de réseau APPN doit communiquer avec les points de contrôle des nœuds de réseau adjacents. Le point de contrôle dirige des fonctions telles que l'activation et la désactivation des cartes et des liaisons, puis apporte son concours aux LU lors de l'établissement et de l'arrêt des sessions.

Lors de la configuration d'un poste de travail, vous devez définir le nom de point de contrôle (également désigné par nom de nœud local). Le point de contrôle correspond également à une LU ; vous pouvez choisir de définir la LU de point de contrôle comme la seule LU définie sur votre poste de travail.

Sessions CP-CP

Pour effectuer des services de répertoire, de topologie et de sélection d'acheminement, les nœuds adjacents de l'ensemble du réseau APPN utilisent une paire de sessions CP-CP parallèles pour échanger des informations de réseau. Les nœuds de réseau utilisent des sessions CP-CP pour surveiller les nœuds d'une liaison réseau et pour assurer le suivi des services de répertoire et de session. Un nœud de réseau établit deux sessions parallèles avec chaque nœud de réseau adjacent et avec chaque nœud d'extrémité pris en charge. Un nœud d'extrémité APPN établit deux sessions parallèles avec un seul nœud de réseau adjacent intervenant comme son serveur en cours. Les nœuds LEN ne prennent pas en charge les sessions CP-CP.

Une fois qu'une connexion a été établie, les nœuds échangent des informations d'identification (XID). Des sessions CP-CP sont ensuite lancées entre les points de contrôle des nœuds connectés directement. Les sessions CP-CP utilisent des protocoles LU 6.2 et les deux sessions d'une paire donnée doivent être actives de sorte que les points de contrôle partenaire démarrent et maintiennent leurs interactions. Toutes les sessions CP-CP servent à effectuer des recherches de répertoire.

Une fois les sessions CP-CP établies, les deux nœuds échangent des messages de capacité de point de contrôle qui informent chaque nœud des capacités de l'autre. Lorsque les deux nœuds sont des nœuds de réseau, ils échangent des messages de mise à jour de base de données de topologie (TDU). Ces derniers contiennent des informations d'identification, des caractéristiques de nœud et de liaison et des numéros de séquence de ressources permettant d'identifier les mises à jour les plus récentes de chacune des ressources décrites dans le message TDU.

Activation de connexion CP-CP

Lors du démarrage de Communications Server, ce dernier tente d'activer en premier la connexion au réseau NN privilégié. Communications Server essaie d'activer toutes les autres connexions définies pour être ***activées au démarrage***. En présence d'une liaison parallèle secondaire à la connexion au serveur NN privilégié, Communications Server n'attend pas les résultats de la tentative d'activation de cette connexion avant d'établir une liaison secondaire mais tente d'activer les sessions CP-CP sur la liaison secondaire.

Remarque : Si la connexion a été désactivée par une requête de l'opérateur à partir du nœud local, les sessions CP-CP ne sont pas réactivées. Si la connexion a été désactivée par une requête de l'opérateur à partir du nœud distant, les sessions CP-CP sont réactivées au niveau du nœud local. En ce qui concerne les liaisons entre des nœuds NN, seules les liaisons activées à la demande (liaisons dont le nom de CP adjacent est précisé et qui ne sont pas définies pour être ***activées au démarrage***) sont activées.

Réactivation de connexion CP-CP

Communications Server fournit un support de réactivation de connexions CP-CP. La perte des sessions CP-CP entre un nœud d'extrémité et son serveur de nœud de réseau et entre des nœuds de réseau adjacents peut perturber le fonctionnement d'un réseau APPN. Le support de réactivation de connexions CP-CP améliore la fiabilité d'un réseau APPN en établissant de nouveau ces sessions importantes lorsqu'elles s'arrêtent en raison d'un incident ou d'une désactivation de connexion.

Une tentative de réactivation de connexions CP-CP est lancée par une activation de liaison CP-CP, par un incident de session CP-CP ou par l'expiration du délai de réactivation CP-PC. Des sessions CP-CP sont établies par Communications Server à l'aide du premier des éléments suivants :

1. Le CP-CP du serveur privilégié (s'il n'a pas déjà été tenté).
2. Si un DLUR est configuré, utilisez un CP adjacent qui prend en charge l'enregistrement de DLUR.
3. La dernière activation (la plus récente) des NN, qui n'a pas été tentée et à laquelle une connexion active est établie.
4. Le premier de tout autre NN de haut niveau destiné à l'extension de réseau.

Remarque : Si les connexions CP-CP ont été arrêtées en raison d'un incident de liaison, Communications Server ne réactive pas la liaison. Vous pouvez configurer une connexion en ***réactivation automatique*** (tentatives illimitées) afin que les connexions importantes restent actives.

Extension de réseau

Il s'agit d'un sous-ensemble de nœuds frontaliers permettant l'interconnexion d'un central de branchement à un réseau fédérateur longue distance APPN. Les réseaux interconnectés peuvent être natifs (c'est-à-dire qu'ils ont le même ID réseau) ou non natifs. Un nœud prenant en charge l'extension de réseau est un nœud de réseau de branchement qui, en général, dispose d'interfaces de réseau local et de réseau longue distance, et peut également inclure le DLUR et le HPR.

Les liaisons d'un nœud, qui prennent en charge l'extension de réseau sont définies comme ***liaisons montantes de branchement*** ou ***liaisons descendantes de branchement***. La figure 10, à la page 32 illustre un exemple de fonctionnement d'un nœud de réseau de branchement au sein d'un réseau. Dans cette figure, le nœud du centre correspond à un nœud de réseau de branchement. En général, le CP adjacent (nœud de liaison montante de branchement) sera le serveur de nœud de réseau (NNS) du nœud de réseau de branchement, qui ressemble à un nœud d'extrémité relié au nœud de liaison montante de branchement.

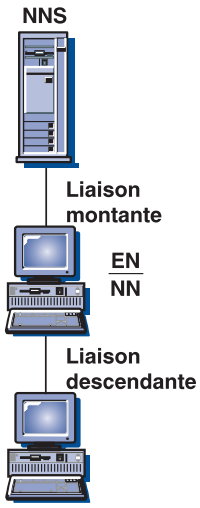


Figure 10. Présentation conceptuelle des liaisons montantes et descendantes de branchement

Les liaisons montantes de branchement sont définies au niveau du nœud de réseau de branchement en amont du réseau fédérateur. Vous pouvez considérer qu'un nœud doté d'une liaison montante est relié via une connexion périphérique au réseau fédérateur.

Les liaisons descendantes de branchement sont définies à partir du nœud de réseau de branchement en aval. Le nœud considère que les liaisons descendantes sont des connexions aux nœuds d'extrémité (points de contrôle) du domaine. Les liaisons descendantes de branchement sont généralement des liaisons de réseau local (ce qui n'est pas obligatoire). Vous pouvez considérer que les nœuds d'extrémité connectés via des liaisons descendantes de branchement sont des ressources locales. Le nœud de réseau de branchement correspond au serveur de nœud de réseau destiné à ces nœuds d'extrémité. Au niveau des liaisons descendantes de branchement, il fournit des fonctions de nœud de réseau pour les nœuds d'extrémité de domaine, les nœuds d'extrémité LEN, les nœuds T2.0 et T2.1 dépendants et les LU et PU locales.

Un nœud de réseau de branchement fonctionne comme un serveur de nœud de réseau pour son domaine. Il maintient des informations de topologie concernant tous ses nœuds de liaisons descendantes de branchement mais ne maintient pas d'informations complètes sur l'ensemble du réseau de liaisons montantes. Si les informations du nœud ne sont pas suffisantes, celui-ci transmet les requêtes LOCATE à son serveur de nœud de réseau de liaisons montantes qui correspond peut-être à un autre nœud de réseau de branchement ou à un nœud de réseau APPN.

L'extension de réseau optimise l'environnement de communication d'égal à égal pour les administrateurs qui souhaitent connecter des branchements basés sur le réseau local à un seul réseau longue distance principalement basé sur un réseau commuté. L'extension de réseau améliore les performances des réseaux APPN de grande taille. En particulier, il :

- réduit le nombre de nœuds des grands réseaux APPN, ce qui vous permet d'ajouter d'autres réseaux de branchement ;
- masque les informations de topologie de branchement ;

- permet une communication d'égal à égal entre les branchements connectés au même réseau de connexion APPN ;
- permet une coexistence avec des serveurs de passerelle PU ;
- réduit le trafic de session CP-CP de liaisons montantes (trafic de réseau longue distance) ;
- isole le réseau de branchement de la surcharge de trafic du réseau fédérateur longue distance.

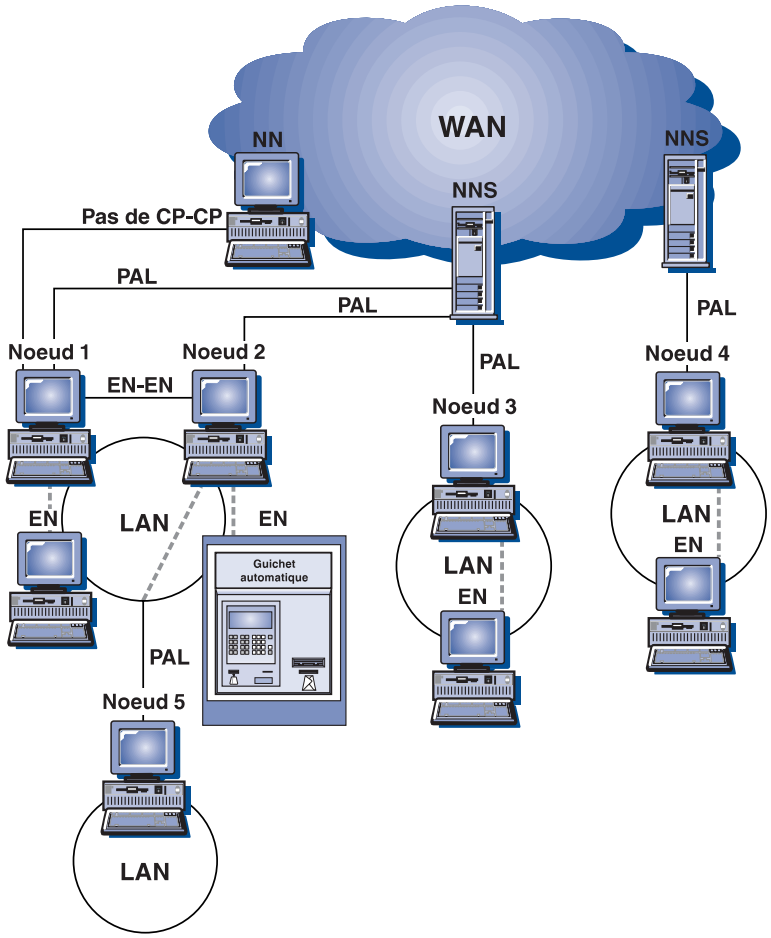


Figure 11. L'extension de réseau dans un réseau

La figure 11 illustre le mode de fonctionnement des nœuds de réseau de branchement dans un réseau. Les traits discontinus représentent des liaisons logiques. Dans cette figure, les nœuds 1, 2, 3 et 4 sont configurés de manière à prendre en charge l'extension de réseau et fonctionnent à la fois comme nœuds d'extrémité et nœuds de réseau. Ils masquent leur topologie de liaisons descendantes à partir du réseau longue distance (cela signifie qu'ils sont considérés par les serveurs de nœud de réseau en amont comme étant des nœuds d'extrémité). Pour les nœuds situés sur les réseaux locaux en aval, ils fonctionnent comme des serveurs de nœud de réseau. Le nœud 5 apparaît comme nœud d'extrémité pour le nœud 2 mais comme serveur de nœud de réseau (NNS) pour les autres nœuds d'extrémité de son réseau local. Pour le NNS, le nœud 5 apparaît comme une LU sur le nœud 2.

Lorsqu'un nœud d'extrémité pris en charge par le nœud 1 tente d'établir une session avec un nœud d'extrémité via le réseau longue distance, le nœud 1 peut émettre une requête Locate (Send) sur sa liaison d'extension de réseau à destination de son serveur de nœud de réseau. Si le CP cible est trouvé, le serveur de nœud de réseau détermine un chemin entre le nœud 1 et le CP cible. Le nœud 1 modifiera le chemin avant de le renvoyer au nœud d'extrémité source. Ce dernier utilise ce chemin pour sa session.

Restrictions applicables à l'extension de réseau

Les restrictions suivantes s'appliquent aux réseaux configurés pour utiliser l'extension de réseau :

- Un nœud de réseau de branchement ne peut se connecter à un nœud de réseau que via une liaison montante de branchement.
- Pour éviter le bouclage de l'opération de recherche, les nœuds d'extrémité de liaisons descendantes doivent être des nœuds d'extrémité réels et non des nœuds présentant une image de nœud d'extrémité.
- Un nœud ne peut pas établir de sessions CP-CP avec le nœud de réseau de branchement simultanément via des liaisons montantes et descendantes de branchement.
- Le nœud de réseau de branchement peut établir des sessions CP-CP via une seule liaison montante de branchement à la fois ; cela signifie qu'il peut établir des sessions CP-CP avec au maximum un serveur de nœud de réseau.
- L'extension de réseau ne fournit pas de support twinaxial.
- Un nœud d'extension de réseau ne peut pas établir de sessions DLUR en aval.

Configuration de l'extension de réseau

Avant de configurer l'extension de réseau, vous devez configurer un nœud de réseau de branchement. Vous devez ensuite configurer un DLC (pour une liaison implicite) ou un nœud de réseau de branchement. Une liaison configurée pour prendre en charge l'extension de réseau correspond à une liaison montante de branchement. Sur un nœud de réseau de branchement, les liaisons qui ne sont pas configurées pour prendre en charge cette fonction sont des liaisons descendantes de branchement.

Si les nœuds de réseau de branchement sont connectés entre eux via des liaisons, ils doivent être définis comme connexions ***d'égal à égal***, ce qui leur attribue un type de liaison de **LEARN** dans le fichier ACG. Vous avez également la possibilité de définir la liaison comme **ACTIVATE_AT_STARTUP=1** de sorte qu'elle soit toujours active. Lorsque des nœuds de branchement sont connectés l'un à l'autre, des boucles se produisent dans la topologie. Cela est acceptable aussi longtemps que les liaisons restent actives, ou elles sont établies à mesure qu'elles sont activées. Si des liaisons sont définies entre des nœuds de réseau de branchement sous forme de liaisons **END_NODE** ou **NETWORK_NODE**, la topologie signalée en amont risque d'interpréter les liaisons de manière inappropriée et d'occasionner des incidents d'allocation.

Vous pouvez également utiliser un fichier ACG pour configurer l'extension de réseau.

Administration de l'extension de réseau

Les sections suivantes expliquent comment vérifier une configuration et décrivent les restrictions applicables à la configuration du réseau.

Vérification de la configuration : Vous pouvez utiliser **Fonctionnement du nœud SNA** au niveau d'un nœud qui prend en charge l'extension de réseau, afin de déterminer si un branchement local a été configuré correctement. Au moment de l'exécution, la topologie du nœud ne doit jamais afficher plus de deux nœuds de réseau : lui-même et le serveur de nœud de réseau de liaisons montantes.

Remarque : Une seule liaison montante est disponible pour CP-CP. Chaque poste de travail doit être configuré sous forme de nœud d'extrémité, le nœud de réseau de branchement étant défini comme son serveur de nœud de réseau privilégié.

Vous pouvez utiliser **Fonctionnement du nœud SNA** afin de vérifier si le DLC ou la liaison a été configurée pour prendre correctement en charge l'extension de réseau. Vous pouvez également utiliser **Fonctionnement du nœud SNA** pour déterminer si une liaison active correspond à une liaison montante de branchement ou à une liaison descendante de branchement. Les nœuds d'extrémité en aval enregistrés à l'aide d'AnyNet n'enregistreront pas leurs ressources.

Fonctions prises en charge

Communications Server prend en charge toutes les fonctions de base d'APPN version 2 (nœud d'extrémité et nœud de réseau). En outre, les options suivantes sont prises en charge :

- Nœud d'extrémité

Ensemble de fonctions	Option
162	MS_CAPS Be Sphere of Control (SOC) EN
171	Données de diagnostic d'incident dans l'alerte
177	Alerte de réseau local
178	Alerte LLC SDLC/RL
181	Alerte X.25
182	Alerte de CPMS en attente
1002	Nom de poste de liaison adjacent
1007	TG parallèles
1011	Plusieurs LU indépendantes locales
1012	CP=LU
1018	Suppression de ressources EN avant enregistrement
1067	Demandeur de LU dépendantes
1070	Chiffrement de session
1107	Enregistrement de ressources centralisé (des LU)
1116	Enregistrement de LU pris en charge par le DLUS

1200	Mise en antémémoire d'arborescence et de TG
1400	Base HPR (ANR)
1401	Protocole RTP
1402	Flux de contrôle via RTP
1520	Services d'opérations communs

- Nœud de réseau

Ensemble de fonctions	**Option**
164	Point focal de secteur de MS_CAPS
171	Données de diagnostic d'incident dans l'alerte
177	Alerte de réseau local
178	Alerte LLC SDLC/RL
181	Alerte X.25
182	Alerte de CPMS en attente
1002	Nom de poste de liaison adjacent
1007	TG parallèles
1011	Plusieurs LU indépendantes locales
1012	CP=LU
1018	Suppression de ressources EN avant enregistrement
1067	Demandeur de LU dépendantes
1070	Chiffrement de session
1100	Stockage sécurisé de l'antémémoire des répertoires
1101	Antémémoire de répertoire pré-chargée
1107	Enregistrement de ressources centralisé (des LU)
1116	Enregistrement de LU pris en charge par le DLUS
1118	Enregistrement de vecteur TG EN
1121	Fonction d'extension de réseau
1200	Mise en antémémoire d'arborescence et de TG
1203	Détection et élimination des conflits TDU
1301	Trafic de session intermédiaire non régulé
1400	Base HPR (ANR)
1401	Protocole RTP
1402	Flux de contrôle via RTP
1520	Services d'opérations communs

DLC

Le DLC fournit les protocoles nécessaires au transfert fiable des unités de transmission de base (BTU) entre une paire de nœuds dans le réseau APPN, et au maintien des connexions logiques entre des nœuds.

Connexions

Une connexion permet de relier une paire de nœuds adjacents à travers le DLC sous-jacent.

Liaisons parallèles

Votre nœud local peut établir plusieurs liaisons avec un nœud adjacent. Cette association est désignée par ***liaisons parallèles***. Un numéro unique (numéro de groupe de transmission) est attribué à chacune de ces liaisons parallèles qui peuvent présenter des caractéristiques différentes. Pour avoir deux liaisons parallèles entre deux nœuds, les postes de liaison correspondants peuvent être situés sur une seule carte dans un nœud mais doivent être situés sur des cartes distinctes dans l'autre nœud ; cela signifie que la combinaison du numéro de carte et de l'adresse du poste de liaison adjacent (ou de destination) doit être unique pour chaque liaison.

Activation de liaison

L'unité de message servant à acheminer les caractéristiques du nœud et de la liaison vers un nœud adjacent est désignée par ***Échange d'identification*** (XID). Si **USE_PU_NAME_IN_XID=1**, le nom de PU est utilisé dans la zone de nom de CP du XID. Sinon, le nom du point de contrôle est utilisé dans cette zone. Des XID sont échangés entre des nœuds avant et pendant l'activation de la liaison, afin d'établir et de négocier des caractéristiques de liaison et de nœud, et après l'activation de la liaison pour communiquer les modifications de ces caractéristiques.

Les nœuds APPN échangent un XID de format 3 (XID3) avec d'autres nœuds T2.1 ou frontaliers afin d'effectuer une négociation de rôle. Quant aux connexions PU 2.0, utilisez le mot clé **LINK_STATION** pour indiquer un nom de PU et un ID nœud qui sont échangés sur XID3. Si **USE_PU_NAME_IN_XID=1**, le nom de PU est utilisé dans la zone de nom du XID. Sinon, le nom du point de contrôle est utilisé dans cette zone. Les informations relatives aux caractéristiques du nœud émetteur sont contenues dans le XID3, notamment le rôle du poste de travail (principal, secondaire ou négociable), le numéro de TG, le type de nœud, le numéro de liaison logique, la taille maximale de BTU pouvant être reçue, l'ID nœud et le nom de PU. Ce dernier correspond généralement au nom du point de contrôle mais un autre nom de PU et un autre ID nœud peuvent être indiqués dans le mot clé **LINK_STATION** pour prendre en charge des connexions PU 2.0 simultanées.

Types de liaison

Les six types de liaison suivants sont généralement définis dans les nœuds de Communication Server :

- Accès au réseau principal, activé à l'origine (APPN ou hôte)
- Accès au réseau principal, liaison hôte
- Accès au réseau principal, utilisation à plein temps (à utiliser le cas échéant)

- Accès au réseau secondaire, liaison entrante (caractéristiques de liaison prédéfinies)
- Accès au réseau secondaire, utilisation limitée (également désigné par liaison à ressources limitées)

La configuration de Communications Server permet de définir et de contrôler l'utilisation de ces types de liaison. La présente section décrit les paramètres de nœud, de DLC, et de configuration de liaison utilisés, ainsi que les relations et les dépendances qui existent entre ces paramètres. Les catégories suivantes sont décrites :

- Paramètres de définition et d'activation de liaison
- Paramètres de désactivation de liaison
- Autres paramètres de liaison

Les paramètres suivants sont décrits :

- **Paramètres de définition et d'activation**
  - Activation au démarrage
  - Activation à la demande
  - Réactivation de liaison automatique
  - Nombre maximal des tentatives d'activation
  - Réactivation demandée par l'utilisateur
- **Paramètres de désactivation**
  - Délai d'inactivité
  - Ressource limitée
- **Autres paramètres de liaison**
  - Réseau de connexion
  - Support de session CP-CP
  - Support de routage hautes performances (HPR)
  - Type de nœud adjacent
  - Serveur de nœud de réseau privilégié
  - Solliciter des sessions SSCP
  - Nom de PU (lorsque le paramètre Solliciter des sessions SSCP a pour valeur **1**)

Remarque : Ces paramètres se trouvent dans le fichier ACG et ne sont peut-être pas disponibles sur les panneaux (via l'utilitaire **Configuration du nœud**).

Paramètres de définition et d'activation de liaison

La présente section décrit les paramètres de définition et d'activation.

Activation au démarrage

Ce type de liaison est généralement utilisé pour les liaisons d'accès au réseau principal, qui sont à l'origine activées lors du démarrage de Communications Server. La liaison est activée au démarrage de Communications Server sur votre machine et reste active tout au long de l'exécution de Communications Server.

Pour définir une liaison de sorte qu'elle soit activée au démarrage, indiquez **ACTIVATE_AT_STARTUP=1** dans le mot clé **LINK_STATION** du fichier ACG. Les liaisons sont généralement configurées aux fins d'activation au démarrage lorsqu'elles sont importantes pour la connectivité de réseau. Une liaison importante peut également être configurée pour faire l'objet de réactivations de liaison automatique (voir la section «Réactivation automatique des liaisons», à la page 40).

La liaison entre un nœud d'extrémité APPN et son serveur de nœud de réseau privilégié est un exemple de ce type de liaison.

En ce qui concerne les liaisons non activées au démarrage, désignées par **ACTIVATE_AT_STARTUP=0**, on peut citer, par exemple, une liaison hôte qui n'est pas requise immédiatement lors du démarrage de Communications Server, une liaison entrante qu'un nœud souhaite en contrôler les caractéristiques de liaison, ou une liaison qui est peut-être trop coûteuse pour rester active en continu. Ces liaisons sont définies comme ne faisant pas l'objet d'une activation au démarrage et elles sont activées lorsque les ressources de liaison sont demandées par une application (voir la section «Activation à la demande») ou par le partenaire.

Activation à la demande

Une liaison objet d'une ***activation à la demande*** (également désignée par «auto-activation») permet généralement d'accéder à une LU partenaire qui requiert l'activation dynamique de la liaison. Lors du démarrage de Communications Server, la liaison reste inactive. Cependant, elle est placée dans la topologie sous la forme d'une liaison disponible, si un nom de CP adjacent est indiqué. La liaison est activée lorsqu'un programme de transactions (TP) demande à une LU éloignée une connexion qui requiert l'activation de la liaison. Communications Server utilise le nom qualifié de la LU partenaire pour activer la liaison.

Pour définir une liaison objet d'une activation à la demande, **ACTIVATE_AT_STARTUP=0** et **FQ_ADJACENT_CP_NAME**=(netid.cpname) doivent être configurés dans le même mot clé **LINK_STATION** dans le fichier ACG du nœud d'origine. Si le partenaire n'est pas **FQ_ADJACENT_CP_NAME**, configurez le mot clé **PARTNER_LU**.

En général, une liaison objet d'une activation à la demande est également configurée sous la forme d'une ressource limitée (voir la section «Ressource limitée», à la page 43) or avec un délai d'inactivité (voir la section «Délai d'inactivité», à la page 42) de sorte que la liaison soit désactivée lorsqu'elle n'est plus requise.

À titre d'exemple, on peut citer une liaison définissant une connexion à un partenaire, qui doit être active pendant une durée limitée.

Il se peut que le coût de la liaison soit supérieur à celui que vous êtes prêt à payer pour qu'elle reste active à tout moment. Par exemple, vous disposez d'un ou de plusieurs ordinateurs qui communiquent régulièrement. À la fin de chaque journée, une des machines doit activer une liaison à une machine éloignée afin d'envoyer les résultats quotidiens ou de faire une sauvegarde des données.

La connexion à un serveur de données ou à un serveur d'impression peut constituer un autre exemple. Cette connexion requiert des ressources au niveau du serveur. Pour éviter de limiter le nombre maximal de postes de liaison et de sessions au niveau du serveur, configurez une liaison à activation à la demande, afin de libérer les ressources sur le serveur de données une fois que les requêtes via cette liaison sont terminées.

Une liaison à activation à la demande n'est pas nécessairement une liaison à ressources limitées ; cependant, vous pouvez la définir comme telle en ajoutant le paramètre **LIMITED_RESOURCE=1** au mot clé **LINK_STATION** (voir la section «Ressource limitée», à la page 43).

Réactivation automatique des liaisons

Il s'agit d'une fonction de reprise sur incident, qui améliore la disponibilité d'une liaison défectueuse. Si une liaison doit être réactivée (sans l'intervention de l'utilisateur) à la suite d'un incident, la fonction de réactivation de liaison automatique peut être utilisée. Cette fonction permet des tentatives de réactivation automatique de la liaison si les paramètres suivants ont été indiqués dans les mots clés **LINK_STATION** ou **PORT** :

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

Si un de ces paramètres est indiqué dans le mot clé **PORT**, les valeurs sont utilisées par le mot clé **LINK_STATION** si le paramètre **INHERIT_PORT_RETRY_PARMS** a été défini.

Une fois que l'activation aboutit, le compteur d'intervalle est remis à zéro.

Il est peut-être avantageux d'utiliser la fonction de réactivation de liaison automatique sur l'un des types de liaison suivants :

- Une liaison à un NN qui fait l'objet d'une activation au démarrage. Si la liaison échoue, une seule liaison au serveur de nœud de réseau serait réactivée.
- Liaison hôte
- Liaison principale dotée d'un système de secours (également définie comme liaison à activation au démarrage)
- Toute liaison devant rester active à tout moment.

Nombre maximal des tentatives d'activation

Il s'agit d'un paramètre d'activation de liaison qui permet d'empêcher le trafic hôte de LU dépendantes (par exemple, une application LUA ou 3270, une passerelle LU 2 et/ou un DLUR tentant d'activer une liaison hôte pour une application en aval) de refaire des tentatives d'activation de liaison illimitées. Le paramètre **INHERIT_PORT_RETRY_PARMS** représente le nombre de tentatives d'une demande d'activation de liaison. Une fois ce nombre de tentatives atteint, les demandes ultérieures sont rejetées tant que le nombre de tentatives n'est pas réinitialisé. Les demandes d'activation de liaison de LU dépendantes émises une fois que le nombre maximal de tentatives d'activation est atteint sont immédiatement rejetées sans aucune réelle tentative d'activation de la liaison. Dans ce cas, un code retour principal de X'0003' et un code secondaire de X'00000005' (nouvelle tentative DLC), ainsi qu'un code d'analyse de X'00000000' sont renvoyés. Des demandes d'activation de liaison de LU indépendantes émises une fois le nombre maximal de tentatives d'activation atteint sont tentées mais, conjointement avec les codes retour principal X'0003' et secondaire X'00000005', un code d'analyse de 081C0001 est renvoyé, afin d'indiquer que le nombre maximal de tentatives d'activation a été atteint.

Remarque : Si un TP tel qu'une application LUA se trouve dans une boucle tentant d'activer une session avec le même hôte que l'application de LU dépendantes, le TP fait en sorte que le nombre maximal de tentatives d'activation soit dépassé avant que l'application dépendante puisse émettre sa première demande.

Le nombre maximal des tentatives d'activation est réinitialisé comme suit :

- Lorsqu'un TP indépendant active la liaison. Il incombe aux TP de vérifier le code d'analyse et de mettre en œuvre un protocole d'activation de liaison raisonnable qui ne permet pas des tentatives d'activation illimitées.
- Lorsque l'utilisateur active la liaison à l'aide de l'utilitaire **Fonctionnement du nœud SNA**.
- Lorsque la liaison est activée à partir de l'autre direction (par exemple, par le partenaire).

Si l'utilitaire **Fonctionnement du nœud SNA** tente une activation de liaison, le nombre maximal des tentatives d'activation est réduit de 1 et le résultat n'est pas pris en compte. Si le nombre maximal a été dépassé sur une liaison entre l'hôte et la passerelle, l'activation de la liaison sera tentée au bout de 30 minutes si une liaison de poste de travail est devenue active. Ainsi, les nouvelles tentatives s'arrêtent, même si elles sont relancées ultérieurement lors du redémarrage des postes de travail. Une fois que l'activation d'une liaison par la passerelle, la LUA ou l'utilitaire **Fonctionnement du nœud SNA** aboutit, le nombre maximal des tentatives d'activation est remis à zéro.

Pour configurer le nombre maximal des tentatives d'activation sur une liaison, le paramètre **MAX_ACTIVATION_ATTEMPTS**= n est configuré dans le mot clé **LINK_STATION**, n représentant le nombre de tentatives compris entre - 1 et 127. -1 indique que la valeur du mot clé **PORT** doit être utilisée, et 0 indique un nombre de tentatives illimité.

Réactivation demandée par l'utilisateur

Cette option est utilisée lorsque l'utilisateur demande la réactivation d'une liaison à partir de l'utilitaire **Fonctionnement du nœud SNA** ou de la ligne de commande en utilisant, par exemple, Communications Server.

Paramètres de désactivation de liaison

Les sections qui suivent décrivent les paramètres de désactivation.

Délai d'inactivité

Il s'agit d'un paramètre de désactivation de liaison SDLC qui contrôle le moment de désactivation des liaisons. La valeur du délai d'inactivité indique la durée (en secondes) pendant laquelle une liaison peut être inactive avant qu'elle soit désactivée. Il est similaire au paramètre **LINK_DEACT_TIMER** du mot clé **LINK_STATION**, à ceci près que le paramètre **LINK_DEACT_TIMER** attend la fin de toutes les sessions (lorsque le nombre de session atteint 0) avant de déclencher la désactivation de la liaison. Le paramètre **INACTIVITY_TIMER** ne prend pas en compte le nombre de sessions et déclenche la désactivation une fois que la liaison a été inactive pendant la durée indiquée.

La fonction de délai d'inactivité a été mise en œuvre pour gérer le cas où une session d'émulateur, une application LUA ou 3270, ou une connexion LEN est accidentellement restée active pendant de longues périodes de temps. Lorsque le nœud ne détecte aucune activité sur ce type de connexion pendant la durée indiquée au paramètre **INACTIVITY_TIMER**, la liaison est automatiquement désactivée, sans égard aux sessions ou conversations présentes sur la liaison. Par définition, le paramètre **LINK_DEACT_TIMER** est considéré comme non perturbateur contrairement au paramètre **INACTIVITY_TIMER** qui est considéré comme perturbateur.

Remarques :

1. Le délai d'inactivité peut être utilisé sur des liaisons à ressources limitées ou à ressources non limitées. Si une liaison est définie comme étant à ressources limitées et que des conversations restent actives, le délai de ressources limitées n'arrive pas échéance et la liaison est désactivée lors de l'expiration du délai d'inactivité. Si une liaison est définie comme étant à ressources non limitées, le délai d'inactivité sert à désactiver la liaison pour libérer des ressources à l'extrémité éloignée.
2. Actuellement avec HPR, le délai d'inactivité n'est pas pris en compte parce que HPR ne peut pas distinguer le type de trafic de la liaison et que le protocole de connexion HPR génère suffisamment de trafic pour que la liaison ne soit jamais inactive.

Pour configurer le délai d'inactivité sur une connexion SDLC, le paramètre **INACTIVITY_TIMER**= n est codifié dans le paramètre **LINK_STATION_SDLC_SPECIFIC_DATA** du mot clé **LINK_STATION** du fichier ACG, où n représente une valeur comprise entre 40 et 160. Pour configurer le délai d'inactivité sur une liaison, le paramètre **LINK_DEACT_TIMER**= n est codifié dans le mot clé **LINK_STATION** du fichier ACG, où n représente une valeur comprise entre 0 et 1000. 0 indique aucun délai d'inactivité (la liaison reste active). La valeur par défaut du SDLC est égale à 80 et celle de la liaison à 10.

Ressource limitée

Une liaison à ressources limitées est généralement utilisée pour les liaisons d'accès aux réseaux principal et secondaire dont l'utilisation est limitée. Il s'agit d'une liaison qui est automatiquement désactivée lorsque le nombre de sessions atteint 0. La liaison à ressources limitées peut être définie comme **ACTIVATE_AT_STARTUP=1** ou **ACTIVATE_AT_STARTUP=0**. Dans le cas d'une liaison **ACTIVATE_AT_STARTUP=1**, celle-ci est lancée lors du démarrage de Communications Server. Dans le cas d'une liaison **ACTIVATE_AT_STARTUP=0**, celle-ci est placée dans la topologie lors du démarrage de Communications Server, si le nom de CP adjacent est indiqué ; elle est ensuite activée lors de la demande de services.

Remarque : Les liaisons à activation au démarrage ne sont placées dans la topologie que si elles sont actives.

Pour configurer une liaison à ressources limitées, **LIMITED_RESOURCE=1** est indiqué dans le mot clé **LINK_STATION** du fichier ACG. Le paramètre **LINK_DEACT_TIMER**= n est indiqué dans le mot clé **LINK_STATION** et le paramètre **ADJACENT_NODE_TYPE=LEARN** doit être défini.

Remarque : Si **CP_CP_SESSION_SUPPORT=1**, il ne s'agit pas d'une liaison à ressources limitées, ce qui est indiqué par la fonction de vérification de la configuration comme étant un avertissement. Les sessions CP-CP actives empêcheront la désactivation de la liaison.

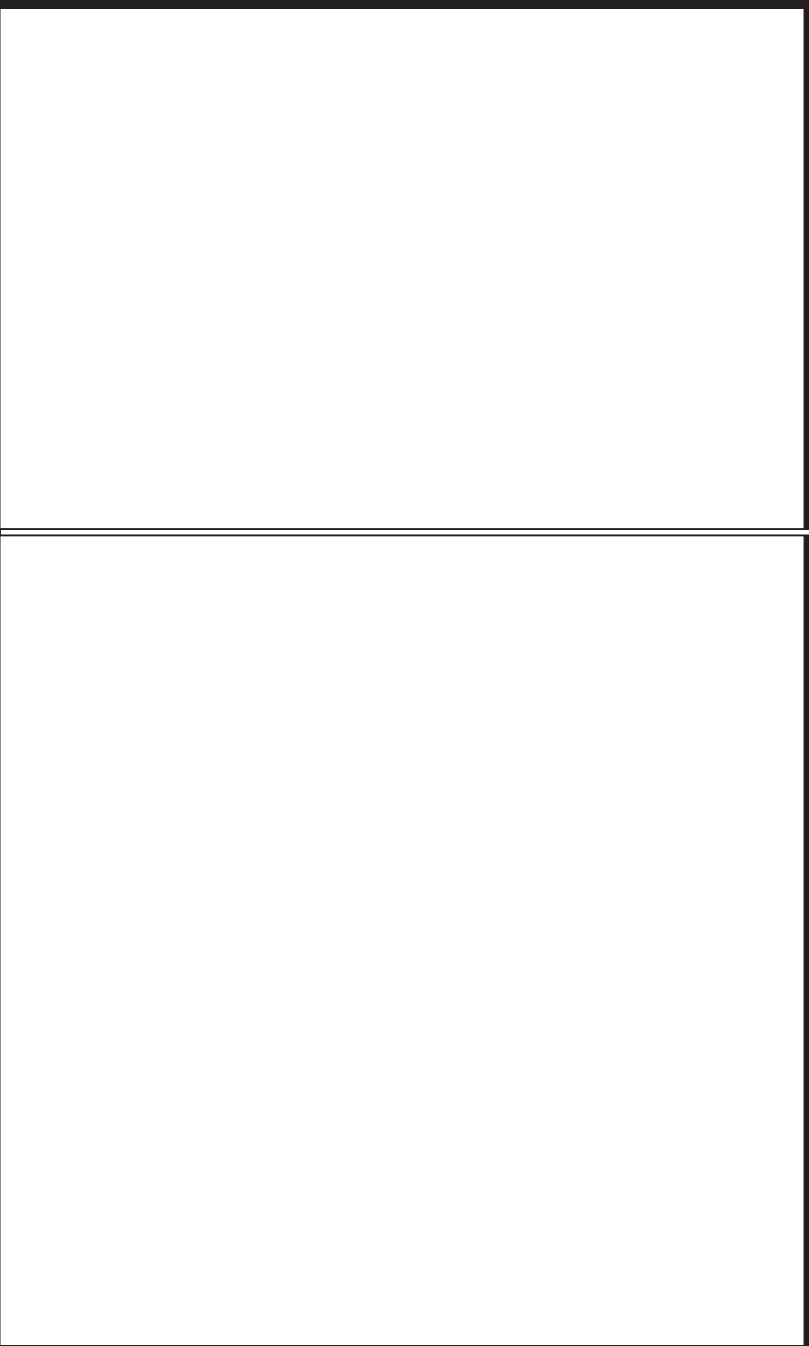
Réseaux de connexion

Les réseaux de connexion permettent des liaisons directes entre les nœuds APPN d'un réseau local sans que des définitions de liaison logique soient nécessaires au niveau de chaque nœud. Cette caractéristique permet de réduire considérablement la définition système sans ajouter la charge représentée par le routage de toutes les sessions via un nœud de réseau. Elle permet également aux nouveaux nœuds ajoutés dans le réseau local de participer entièrement aux conversations APPC sans que des modifications de définition soient nécessaires tous les deux nœuds.

Un nœud du réseau de connexion considère que tous les nœuds de ce réseau peuvent établir entre eux des liaisons directes. Lors du calcul du chemin d'une session, le nœud de réseau prend en compte la liaison directe, puis sélectionne généralement cette dernière comme chemin optimal. Une fois le chemin direct calculé, le nœud de réseau envoie simplement au nœud d'extrémité l'adresse du partenaire aux fins d'activation de la liaison.

Il se peut que le chemin du réseau de connexion ne soit pas utilisé lorsque la sécurité de réseau de connexion est inférieure à celle qui est requise. Si le DLC du réseau de connexion n'est pas sécurisé et qu'un mode tel que #BATCHSC est utilisé au paramètre **MODE_NAME**, le nœud de réseau tente de rechercher un chemin sécurisé, ne tenant pas compte du réseau de connexion.

Si des ponts de réseau local sont en cours d'utilisation, APPN considère que l'ensemble du réseau local en dérivation est un seul réseau logique. Dans la mesure où des liaisons peuvent être activées entre deux systèmes du réseau local, un seul réseau de connexion est requis. Ce dernier doit être défini au niveau de tous les systèmes APPN du réseau local.



Type de nœud adjacent

Ce paramètre indique le type du nœud adjacent au nœud qui définit la liaison. Voici les types admis :

- DSPU_NOXID
- DSPU_XID
- END_NODE
- HOST_DEP_LU_ONLY
- HOST_XID0
- LEARN
- NETWORK_NODE.
- SUBAREA_LEN

Pour plus de détails, consultez le manuel *Configuration File Reference*.

Serveur de nœud de réseau privilégié

Ce serveur indique si le nœud de réseau adjacent doit être utilisé comme serveur de nœud de réseau sur la liaison qui est en cours de définition.

Solliciter des sessions SSCP

Ce paramètre indique si des sessions SSCP-PU sont demandées ou non à l'hôte sur la liaison qui est en cours de définition.

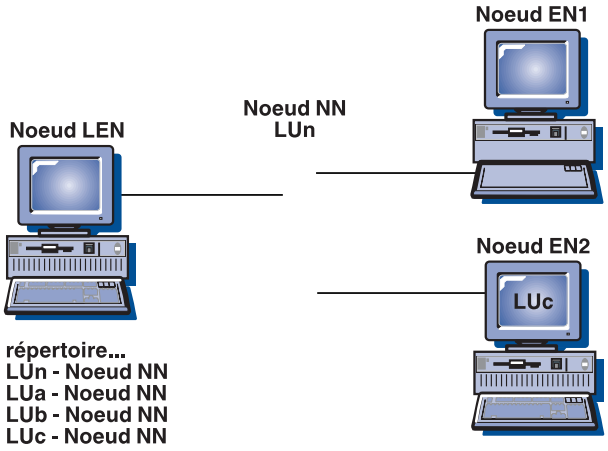
Services de répertoire

Un nœud de réseau fournit des services de répertoire aux LU du nœud de réseau et aux LU des nœuds d'extrémité pris en charge par le nœud de réseau. Le nœud de réseau apporte également son concours dans le cadre des services de répertoire fournis par les autres nœuds du réseau en répondant de façon positive aux demandes de recherche de répertoire reçues, lorsque la ressources définie est trouvée dans le répertoire local. Ce dernier procède au mappage d'un nom de LU avec le nom de point de contrôle du nœud qui contient cette LU. Si le point de contrôle de destination correspond à un nœud LEN ou à un nœud d'extrémité, le répertoire comporte le nom du nœud de réseau de desserte.

Le composant de services de répertoires réside dans chaque nœud ; cependant, le secteur et les fonctions associés varient en fonction du niveau du support de répertoire du nœud.

Un nœud d'extrémité maintient un répertoire local contenant des entrées destinées aux LU locales. En outre, le nœud d'extrémité maintient des entrées de répertoire pour les LU des nœuds adjacents avec lesquelles le nœud d'extrémité a établi une session. En ce qui concerne une session LU-LU avec un nœud d'égal à égal adjacent, une recherche dans le répertoire local renvoie le point de contrôle de destination approprié, associé à la LU recherché, ce qui permet de sélectionner la liaison logique correcte.

Dans un nœud LEN, toutes les LU partenaire sont entrées dans le répertoire, comme l'indique l'exemple de la figure 13. Les LU qui ne figurent pas dans un nœud d'extrémité d'égal à égal adjacent mais dans le réseau APPN sont associées dans son répertoire au serveur de nœud de réseau désigné. Le nœud LEN envoie une demande d'activation de session LU-LU (BIND) à son serveur de nœud de réseau pour toute LU associée dans son répertoire à son serveur ; le serveur localise automatiquement la LU de destination correspondante, puis transmet la demande BIND de manière appropriée. Le nœud de réseau peut envoyer une recherche Locate, attendre une réponse, puis émettre la demande BIND.



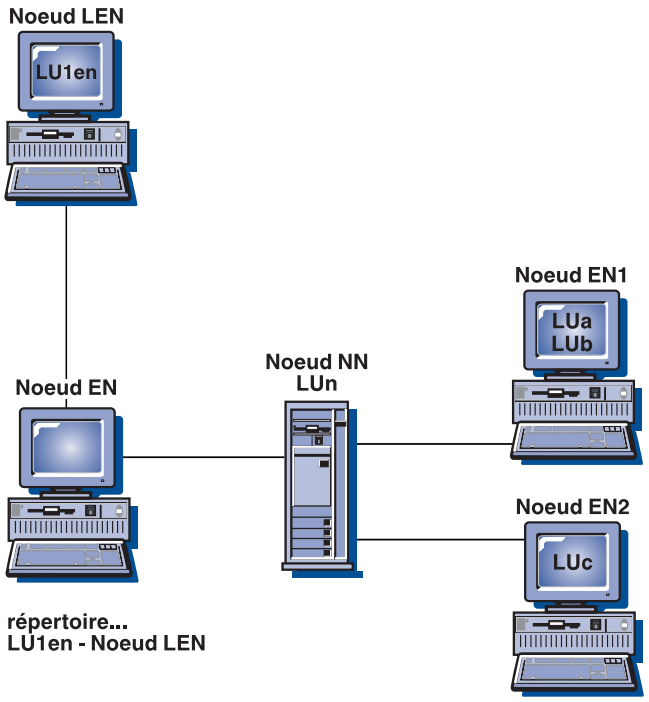


Figure 14. Répertoire de nœud d'extrémité. Le nœud d'extrémité (EN) utilise les services de son serveur de nœud de réseau pour localiser les LU. Il n'est pas nécessaire qu'une LU du réseau APPN soit définie dans le nœud d'extrémité. Cependant, la LU du nœud LEN adjacent doit être définie car elle n'est pas connectée au nœud de réseau et ne fait pas pas partie du réseau APPN.

En collaboration avec tous les autres nœuds du réseau APPN, un nœud de réseau fournit des services de répertoire répartis à ses nœuds d'extrémité pris en charge. Le nœud de réseau d'origine reçoit le nom d'une LU de destination dans une demande de recherche Locate provenant d'un nœud d'extrémité pris en charge, ou le nom d'une LU secondaire dans un BIND provenant d'un nœud LEN. Le nœud de réseau vérifie l'emplacement en cours de la LU si celle-ci est représentée dans le répertoire du nœud de réseau (mais qu'elle ne figure pas dans le nœud de réseau lui-même). Cette vérification se fait grâce à l'envoi d'une recherche dirigée au serveur de nœud de réseau de destination.

Si la LU ne figure pas dans le répertoire du nœud de réseau d'origine, le nœud de réseau lance une recherche dans le réseau, en envoyant une recherche par diffusion à tous les nœuds de réseau adjacents, chacun à son tour propageant la diffusion et renvoyant des réponses indiquant l'aboutissement ou l'échec. Pour ses besoins futurs, un nœud de réseau met en antémémoire les informations résultant des recherches par diffusion qui ont abouti.

Un nœud d'extrémité APPN peut également recevoir des demandes de recherche Locate de son serveur de nœud de réseau (et répondre à celles-ci), afin de rechercher ou d'assurer la présence permanente des LU spécifiques du nœud d'extrémité.

Chaque nœud d'extrémité peut enregistrer ses LU sur son serveur de nœud de réseau en envoyant au nœud de réseau un message d'enregistrement. Si le nœud d'extrémité est enregistré sur le serveur de nœud de réseau, le nœud de réseau tient à jour des informations de répertoire relatives aux nœuds d'extrémité de son domaine.

La gure 15, à la p un exemple de

répertoire...
LUx - Noeud LEN
LUa - Noeud EN1
LUb - Noeud EN
Noe

Base de d nées de topologie

de données de topo gie réseau d'un nœud de réseau contient des in-
tions relatives à de réseau et à tous les groupes de transmis-
n qui en assurent onnexion. Il s'agit d'une
liquée qui e entre tous les nœuds du réseau et utilisés aux fins de
sél Le maintien de la base de données requiert des mises à
r diffusion entre tous

Ces mises à jour sont effectuées via des messages TDU (mise à jour de base de données de topologie) qui contiennent des informations d'identification de nœud, des caractéristiques de nœud et de liaison, ainsi que des numéros de séquence de mise à jour permettant d'identifier les modifications les plus récentes de chacune des ressources décrites dans une TDU.

Une base de données de topologie locale d'un nœud d'extrémité contient des informations relatives uniquement à ce dernier et aux nœuds directement connectés.

Le composant de services de topologie et de routage utilise les sessions CP-CP entre les nœuds de réseau pour échanger des informations permettant de créer et de maintenir une base de données de topologie. Cette base de données de topologie des nœuds de réseau est tenue à jour à l'aide des mises à jour qui sont transmises à tous les nœuds de réseau lors de chaque activation ou désactivation d'une ressource (nœud ou liaison) ou lors de la modification des caractéristiques d'une ressource existante.

Une base de données de configuration locale et une base de données de topologie du réseau sont maintenues au niveau de chaque nœud de réseau comme l'indique la figure 16, à la page 50. La première est unique au nœud alors que la seconde est dupliquée au niveau de tous les nœuds de réseau.

Le tableau 2, présente les informations contenues dans la base de données de configuration du nœud de réseau local.

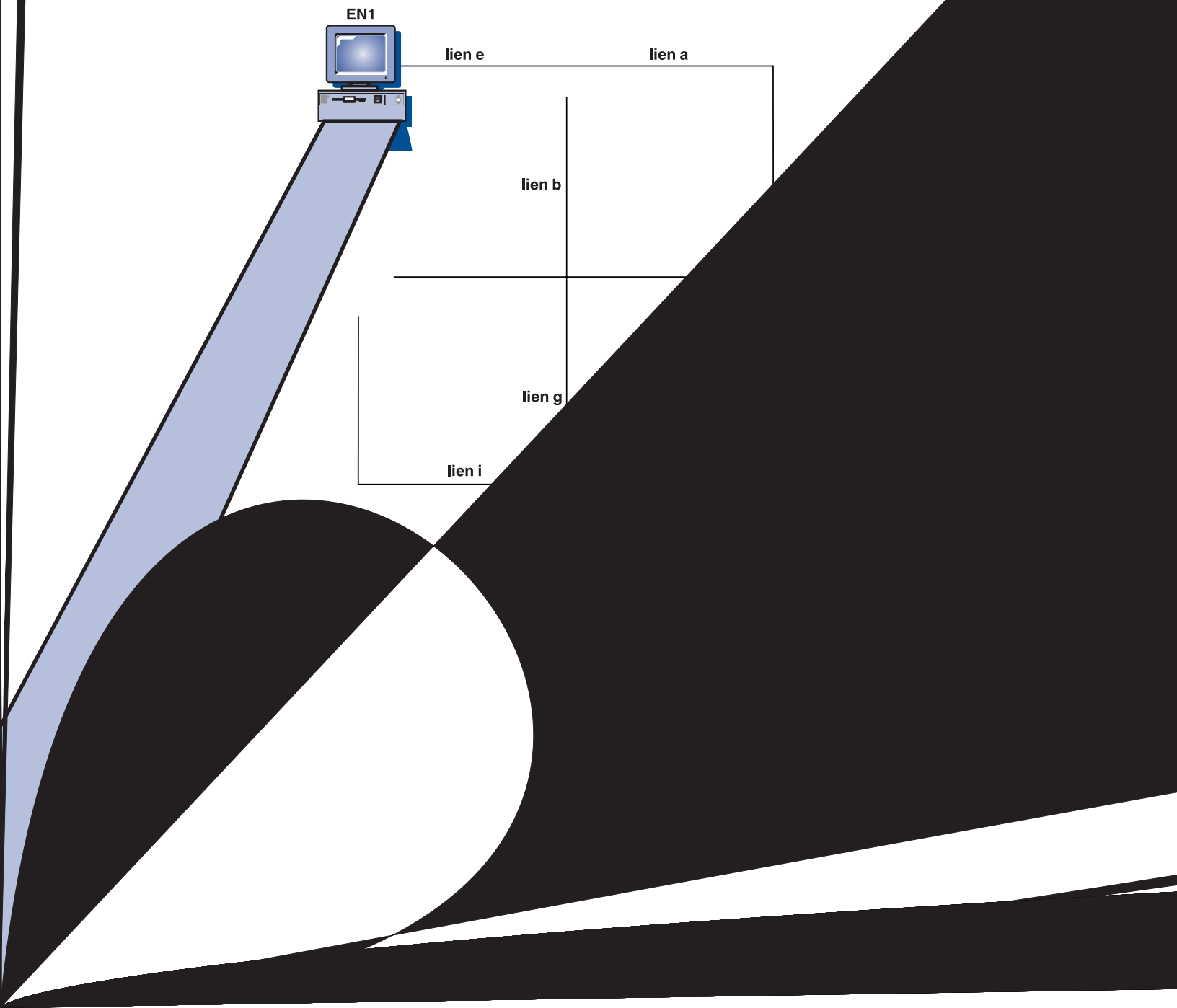
Tableau 2. Base de données de configuration du nœud de réseau local

Nœud	Liaisons	Connexion
NN5	e	NN5—EN1
	a	NN5—NN7
	b	NN5—NN6
NN7	a	NN7—NN5
	d	NN7—NN8
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

Le tableau 3, à la page 50, présente les informations contenues dans la base de données de topologie réseau du nœud de réseau local.

Tableau 3. Base de données de topologie réseau du nœud de réseau local

Nœud	Liaisons	Connexion
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



Classe de service

Lors de l'activation d'une session, le BIND indique un nom de mode. Ce dernier est associé à une définition de classe de service (COS) qui sert à déterminer le chemin le plus souhaitable entre les nœuds d'origine et de destination de la session. Les définitions de COS indiquent les caractéristiques que les nœuds et les liaisons doivent présenter pour être inclus dans le chemin sélectionné pour la session. Cette spécification permet à l'algorithme de sélection d'acheminement de déterminer si un nœud ou une liaison est acceptable. L'algorithme utilise l'ensemble qui est acceptable, afin de calculer le meilleure chemin de la session.

Dans la mesure où les définitions de COS sont variables, différentes sessions peuvent utiliser des chemins différents entre les mêmes nœuds d'origine et de destination, en fonction du nom de mode indiqué. Chaque nœud de réseau est en mesure de calculer le chemin de poids faible (le plus souhaitable) menant à n'importe quelle destination.

Lorsqu'une session traverse un réseau APPN et un réseau de secteur, elle utilise les deux classes de service suivantes :

- Dans le réseau APPN, la session utilise la classe de service (COS) définie pour le mode qui est utilisé par le programme de transactions. Cette définition se trouve dans la configuration active du poste de travail. Cette classe de service permet d'acheminer la session dans le réseau APPN.

  Si le mode à blanc par défaut est utilisé, la classe de service associée est #CONNECT.

- Dans le réseau de secteur, le nom de la classe de service peut être écrit dans la table de mode d'ouverture de session, dans l'entrée relative au nom de mode utilisé par la session. Ce nom de COS est utilisé par le programme VTAM pour acheminer la session via le réseau de secteur.

  Si le mode à blanc par défaut est utilisé ou si aucune classe de service n'est définie dans une entrée de la table de mode d'ouverture de session, l'entrée en blanc de la table ISTSDCOS est affectée par défaut à la classe de service.

Dans les deux cas, chaque réseau utilise le nom de mode pour rechercher le nom de COS ; cependant, les deux noms de COS ne sont pas nécessairement identiques.

Priorité de transmission SNA

La priorité de transmission correspond à une valeur indiquée dans la classe de service. Elle est envoyée dans le BIND du vecteur de contrôle COS/TPF (classe de service/priorité de transmission). Une fois la session établie, les données de sessions ultérieures sont acheminées selon la priorité de transmission indiquée dans le vecteur de contrôle COS/TPF.

Les données acheminées au niveau des sessions utilisant une classe de service à priorité élevée peuvent transmettre des données sur les sessions à priorité inférieure. Vous devez attribuer une priorité élevée aux sessions qui acheminent un trafic interactif où le temps de réponse est important, par exemple, des sessions d'émulation. Par contre, vous devez attribuer une faible priorité aux sessions qui acheminent de grandes quantités de données, par exemple, les transferts de fichiers destinés à NetView Distribution Manager.

Le support de priorité de transmission permet d'empêcher les sessions à haut volume de bloquer le trafic au niveau des sessions interactives.

Voici les quatre priorités de transmission disponibles : Réseau, Elevée, Moyenne et faible. La priorité Réseau est utilisée pour les données de contrôle de réseau telles que les services de topologie et de répertoire. Les autres priorités sont utilisées pour les données utilisateur.

Communications Server prend en charge la priorité de transmission pour les liaisons de réseau local, SDLC et X.25. L'intérêt est essentiellement apparent lorsque le réseau contient des liaisons lentes encombrées.

Sélection d'acheminement

Une fois que le serveur de nœud de réseau reçoit une réponse résultant de sa recherche Locate, le composant des services de topologie et de routage calcule le meilleur chemin entre le nœud d'origine et le nœud de destination pour la classe de service demandée. Dans la mesure où ce composant envoie et reçoit des mises à jour de base de données de topologie lors de la modification des caractéristiques d'une ressource, chaque chemin est calculé à l'aide des informations les plus récentes.

Sélection d'acheminement pour les utilisateurs VTAM

Pour acheminer le trafic APPC via un secteur, les postes de travail connectés à ce secteur doivent être définis sous forme de nœuds de réseau dans Communications Server. Dans chaque nœud de réseau, une liaison est définie ; celle-ci permet de connecter le nœud au secteur. Le nœud de réseau considère que les LU partenaire situées à l'autre extrémité du secteur sont définies comme étant sur l'hôte (un nœud LEN). L'hôte considère que chaque nœud de réseau connecté au secteur doit être défini pour le programme VTAM à l'aide d'une macro de PU. Toutes les unités logiques LU 6.2 de destination qui se trouvent sur le réseau APPN et qui sont destinées à une connexion particulière sont définies dans le cadre de la PU (nœud de réseau) comme si elles étaient effectivement situées au niveau de la PU. Cependant, les LU peuvent réellement être situées au niveau des autres nœuds du réseau APPN connecté au nœud de réseau. L'hôte ne tient compte que de la PU du nœud de réseau. Celle-ci peut également correspondre à une PU passerelle. Le trafic SETN (**CP_CP_SESS_SUPPORT=NO**) n'est pas admis lorsque le paramètre a pour valeur YES sur le NCP et qu'aucune session de point de contrôle ou de PU n'est disponible.

Si le nom de PU de la définition VTAM est identique au nom de point de contrôle défini dans Communications Server, il est à noter que vous n'êtes pas autorisé à définir le point de contrôle sous la forme d'une LU dans les définitions VTAM. Les noms doivent être uniques dans le programme VTAM, qu'il s'agisse de noms de PU ou de LU.

La macro de PU doit contenir le paramètre **XID=YES** pour utiliser un échange XID lors de l'activation de la PU. Ce paramètre est codifié dans le nœud principal du NCP. Il ne doit pas figurer dans l'instruction de PU d'un nœud principal commuté.

En ce qui concerne les périphériques SNA commutés, vous pouvez utiliser un nouveau paramètre dans la macro de PU : **CPNAME**=cccccccc. Ce dernier indique le nom de point de contrôle du nœud de réseau connecté au secteur.

CPNAME ou **IDBLK** et **IDNUM** doivent être indiqués dans une instruction de définition de PU commutée. Les deux paramètres peuvent être indiqués. Le nœud de réseau fournit son nom de point de contrôle au programme VTAM dans l'échange XID lors de la séquence de connexion. Le programme VTAM utilise ce nom pour localiser la macro de PU correspondante. En l'absence d'une macro de PU portant le nom de point de contrôle correspondant, le programme VTAM utilise **IDNUM** et **IDBLK** pour localiser la macro de PU.

Pour acheminer le trafic APPC à partir d'un réseau APPN via le secteur et vers une autre partie du réseau APPN, le nom de réseau (**NETID**) du VTAM propriétaire doit être conforme à l'ID du réseau APPN. Dans Communications Server, l'ID réseau (du nœud de réseau connecté au secteur) peut être recherché à l'aide du profil de caractéristiques du nœud local SNA.

Routage de session intermédiaire

Il s'agit d'une fonction effectuée par un nœud de réseau. Elle permet à ce dernier de recevoir et d'acheminer des données destinées à un autre nœud. L'origine et la destination des données peuvent correspondre à un nœud d'extrémité, à un nœud de réseau ou à un nœud LEN. La partie de la session entre deux nœuds adjacents est désignée par étape de session.

Support de routage hautes performances (HPR)

Communications Server prend en charge le routage hautes performances (HPR) via des connexions Enterprise Extender (IP), SDLC (commande de liaison de donnée synchrones), par réseau local, par réseau longue distance, par canal, MPC (Multi-Path Channel) et X.25.

Le routage ANR (Automatic Network Routing) HPR minimise la mémoire et le traitement requis dans les nœuds intermédiaires, ce qui correspond à une meilleure solution que celle du routage de session intermédiaire (ISR) APPN destiné aux réseaux rapides dont les taux d'erreur sont faibles.

HPR améliore le routage SNA à l'aide des principales caractéristiques suivantes :

- Nœuds intermédiaires sans statut

  Ces nœuds ne disposent d'aucune information sur les connexions qui les traversent.

  Un nœud intermédiaire HPR ne requiert aucun bloc de contrôle ou pool de mémoire tampon pour prendre en charge les connexions qui le traversent. De même, il n'a pas besoin de tables de routage car les informations de routage sont transférées dans chaque paquet. ANR permet à un nœud intermédiaire HPR de recevoir un paquet, d'examiner l'en-tête de paquet pour rechercher un identificateur pour la liaison logique au nœud suivant, puis d'envoyer le paquet sur cette liaison.

- Un nœud intermédiaire HPR :
  - ne récupère pas de paquets car les points d'extrémité de connexion HPR détectent et récupèrent les paquets perdus, à l'aide du protocole RTP ;

    Si votre réseau local comporte des taux d'erreur élevés, vous pouvez également choisir le support de protocole ERP (Error Recovery Protocol) au niveau de la liaison.

Cependant, cela ne doit pas être nécessaire sur les liaisons dont les taux d'erreur sont faibles.

- ne réassemble pas les paquets segmentés et ne segmente pas ces derniers de nouveau, car les points d'extrémité de connexion HPR choisiront automatiquement une taille de paquet prise en charge pour tous les nœuds intermédiaire du chemin ;
- ne gère pas activement les mémoires tampon et n'empêche pas l'encombrement car les points d'extrémité de connexion HPR emploient des algorithmes de contrôle de flux qui empêchent l'encombrement au niveau des nœuds intermédiaires ;
- ne détermine pas le chemin d'un paquet en lançant une recherche dans la table, car les points d'extrémité de connexion HPR effectuent un routage source et créent les informations de routage de paquets à l'aide des labels choisis pour optimiser les performances de chaque nœud intermédiaire.

Pour accéder aux nœuds intermédiaires sans statut :

- Les points d'extrémité du chemin doivent être dotés de capacités de mémoire tampon reflétant la combinaison du délai d'acheminement et de la capacité de traitement des applications ; cette valeur est fonction de votre configuration de réseau.
- Les liaisons de données doivent prendre en charge des tailles de zone d'information suffisamment importantes pour contenir les en-têtes HPR et pour assurer néanmoins l'acheminement efficace des données d'application.
- Les liaisons de données doivent être très fiables car un taux d'erreur élevé peut avoir une incidence défavorable sur la capacité de traitement HPR.

En ce qui concerne les configurations où ces conditions ne peuvent pas être remplies, APPN sans HPR reste un choix de mise en œuvre valide. La technologie HPR est une option d'APPN et APPN sans HPR est néanmoins disponible et pris en charge.

- Prévention d'encombrement

  Un réseau HPR peut exploiter les liaisons de manière très optimale. Une technique appelée contrôle de flux ARB (Automatic Rate Based) permet aux points d'extrémité de connexion HPR de détecter automatiquement l'encombrement du réseau et de réduire la charge de transmission. Cela empêche la perte de paquets qui, dans d'autres algorithmes de routage, peut être occasionnée par l'absence de mémoires tampon disponibles dans les nœuds intermédiaires.

- Reroutage automatique sans interruption

  Lorsqu'un point d'extrémité de connexion HPR détecte l'échec d'un chemin, il calcule automatiquement un autre chemin, établit de nouveau la connexion, puis récupère les paquets perdus en raison de l'incident. Dans la mesure où les nœuds intermédiaires HPR n'ont pas de statut (cela signifie qu'ils n'ont aucune information sur les connexions qui les traversent), ils ne participent pas dans ce protocole de récupération. Étant donné qu'aucun paquet n'est perdu si la commutation du chemin aboutit, les applications utilisant le chemin ne sont pas interrompues par l'incident.

- Logiciel compatible avec le matériel existant

HPR est une extension logicielle d'APPN ; vous pouvez utiliser HPR sur les cartes de réseau local ou longue distance existantes ou sur les liaisons Frame Relay.

Dans la mesure où HPR ne tente pas de fournir une bande passante dédiée et un acheminement en temps réel garanti (laissant ce niveau de fonction à la charge de Broad Band Networking Services), les contraintes de performances applicables aux délais de transmission de paquet sont identiques à celles d'APPN sans HPR. Les protocoles de points de contrôle utilisés par HPR correspondent à ceux d'APPN de base avec quelques petites adjonctions ; les nœuds HPR peuvent donc être installés progressivement au sein d'un réseau APPN existant sans planification préalable ou coordination.

Protocole RTP

RTP est un ensemble de protocoles et de formats de messages permettant d'utiliser les supports de communication de données modernes, de minimiser les frais généraux des nœuds intermédiaires et de changer automatiquement de chemin lorsqu'une liaison du chemin échoue.

Les connexions RTP sont établies dans un ***sous-réseau HPR*** et servent à acheminer le trafic de session. Un sous-réseau HPR correspond à la partie d'un réseau APPN qui est en mesure d'établir des connexions RTP et d'acheminer le trafic de session HPR. Les connexions RTP peuvent être considérées comme des ***canaux de communication*** via lesquels les sessions sont acheminées. Ces connexions peuvent acheminer des données à des vitesses très élevées à l'aide du routage intermédiaire de bas niveau, et minimiser le trafic via les liaisons aux fins de contrôle de flux et de reprise sur incident. Ces flux sont gérés par les points d'extrémité de connexion RTP.

Le chemin physique d'une connexion RTP peut être commuté automatiquement pour réacheminer des données autour d'un nœud ou d'une liaison défectueuse sans interrompre les sessions. Les données du réseau au moment de l'incident sont automatiquement rétablies.

RTP effectue une reprise sur incident de bout en bout et non au niveau de la liaison. Les performances sont améliorées grâce à la réduction du nombre de flux requis pour effectuer la reprise sur incident. Les protocoles de reprise sur incident (ERP) au niveau de la liaison sont également pris en charge pour toutes les connexions. ERP est une méthode consistant à détecter un paquet perdu sur une des extrémités d'une liaison et à procéder à une reprise en demandant à l'autre extrémité de la liaison de retransmettre le paquet. Si le protocole ERP est utilisé, les paquets HPR sont envoyés sous forme de trames d'information numérotées (I-FRAMES). En cas de perte d'une trame, le DLC détecte l'incident et l'émetteur retransmet la trame. Si le protocole ERP n'est pas utilisé, les paquets HPR sont envoyés sous forme de trames d'information non numérotées (UI-FRAMES). En cas de perte d'une trame, le DLC ne peut pas détecter l'incident ; le protocole HPR doit détecter et récupérer les paquets perdus, au niveau des points d'extrémité de la connexion.

Dans l'un ou l'autre cas, le protocole RTP détecte et récupère systématiquement les paquets perdus, au niveau des points d'extrémité de la connexion. En ce qui concerne une connexion donnée, le nombre des liaisons qui utilisent ou non le protocole ERP n'est en aucun cas limité.

ERP peut être activé ou désactivé liaison par liaison. Dans la mesure où RTP détecte et récupère les paquets perdus, au niveau des points d'extrémité de la connexion, vous pouvez utiliser des liaisons ERP ou non lors de la création du réseau.

Cela vous permet d'indiquer le protocole ERP sur les liaisons ont le taux de perte de paquets est élevé, et de maximiser la capacité de traitement sur les autres liaisons en précisant que celles-ci n'utilisent pas de protocole ERP au niveau de la liaison. En général, l'utilisation du protocole ERP n'est pas recommandée dans les réseaux locaux.

Remarque : ERP est toujours activé dans environnement de réseau longue distance.

Un contrôle de flux et un contrôle d'encombrement sont également effectués par RTP de bout en bout. RTP utilise une technique appelée contrôle de flux ARB (Automatic Rate Based) pour utiliser en intégralité la bande passante du réseau lorsque cela s'avère possible. RTP augmente la vitesse de transmission des paquets lorsque le réseau prend en charge cette augmentation de vitesse de transmission. Un encombrement est automatiquement identifié ; la vitesse de transmission sera réduite en conséquence lors de l'encombrement. Les capacités effectives configurées des liaisons du chemin de connexion servent à déterminer la vitesse de transmission initiale et l'augmentation de vitesse.

Un support de flux de contrôle sur les connexions RTP est désormais disponible avec HPR dans Communications Server. Auparavant, les flux de contrôle, notamment les sessions CP-CP et les messages de configuration d'acheminement utilisaient des connexions APPN lorsque les flux de données utilisaient des connexions HPR. À présent, les flux de contrôle et les flux de données peuvent utiliser des connexions RTP. Ce support présente notamment l'avantage de changement automatique du chemin des sessions CP-CP.

Les flux de contrôle sont automatiquement acheminés via RTP si les deux points d'extrémité de la connexion prennent en charge cette fonction.

ANR (Automatic Network Routing)

ANR (Automatic Network Routing) est une technique de routage sans statut activée par RTP lors de l'arrivée d'un message dont le label permet d'identifier de manière unique le prochain segment du chemin. En raison de sa simplicité, le routage ANR peut être effectué à un niveau inférieur sans aucune information sur les connexions utilisant le chemin. ANR minimise les cycles et la mémoire requise pour l'acheminement des paquets via des nœuds intermédiaires.

La fonction de commutation de paquets rapide d'ANR améliore les performances des nœuds intermédiaires au moyen d'un routage à un niveau inférieur à celui d'APPN et à l'aide des opérations de reprise sur incident, de segmentation, de contrôle de flux et de contrôle d'encombrement au niveau du nœud d'extrémité et non du nœud intermédiaire.

Les nœuds ANR intermédiaires ne sont pas informés des sessions SNA ou des connexions RTP. Les informations de routage relatives à chaque paquet sont acheminées dans un en-tête de réseau avec le paquet. Chaque nœud supprime les informations qu'il a utilisées dans l'en-tête avant de transmettre le paquet ; le nœud suivant peut donc rechercher ses informations de routage dans un emplacement déterminé de l'en-tête. Il n'est pas nécessaire de conserver des tables de routage pour les connecteurs de session comme dans l'APPN de base ; Les paquets peuvent donc être commutés plus rapidement à travers les nœuds.

Support de LU

SNA définit des LU de types 0, 1, 2, 3, 4, 6.0, 6.1, 6.2 et 7. Les LU de types 0, 1, 2, 3, 4 et 7 prennent en charge les communications entre les programmes d'application et les différents types de postes de travail. Les LU 6.0 et 6.1 assurent les communications entre les programmes situés au niveau des nœuds de secteur de type 5. La LU 6.2 prend en charge les communications entre deux programmes situés sur des nœuds de secteur de type 5 et/ou des nœuds périphériques de type 2.1, et entre des programmes et des périphériques.

Communications Server supporte les LU de types 0, 1, 2 et 3 qui assurent les communications avec les applications hôte prenant en charge les périphériques suivants :

LU de type 0 Terminaux financiers 3650 et 4700

LU de type 1 Imprimantes 3270

LU de type 2 Claviers-écrans interactifs 3270

LU de type 3 Imprimantes 3270

Les communications ont lieu uniquement entre des LU du même type. Par exemple, une LU 2 communique avec une autre LU 2 et non avec une LU 3. Communications Server prend également en charge la LU de type 6.2 ou APPC.

Les fonctions SNA de Communications Server permettent aux applications d'utiliser l'API APPC pour fournir une fonction de traitement de transaction réparti permettant à un minimum de deux programmes de collaborer afin d'effectuer une fonction de traitement. Cette fonction implique une communication entre les deux programmes ; ces derniers peuvent donc partager des ressources locales, par exemple, les cycles de processeur, les bases de données, les files d'attente de travail et les interfaces physiques telles que les claviers et les écrans.

Communications Server prend en charge APPC via les API APPC. Pour plus de détails, consultez les manuels suivants :

- *Client/Server Communications Programming*
- *System Management Programming*

Les fonctions suivantes de Communications Server prennent en charge une gamme de types de LU :

- Passerelle SNA

  Elle permet aux hôtes IBM 370 (S/370) et/ou aux ordinateurs hôte à architecture IBM 390 (S/390) de prendre en charge les postes de travail connectés au réseau local qui utilisent des LU de types 0, 1, 2, 3 ou 6.2 pour communiquer via un poste de travail de passerelle SNA.

  La passerelle SNA prend également en charge les LU de types 1, 2 ou 3 d'ordinateurs hôte A/400 qui peuvent traiter les données ou transmettre ces dernières via des ordinateurs hôte à architecture IBM 370 ou 390.

- Application de LU conventionnelle (LUA)

  La LU est constituée de logiciels système fournissant des programmes de services qui permettent la prise en charge des LU 0, 1, 2 et 3.

Support SDDLU

Le support de LU dépendante à définition automatique (SDDLU) permet de définir et d'activer automatiquement une LU dépendante au niveau (VTAM). Dans VTAM, cette procédure est désignée par définition dynamique des LU dépendantes (DDDLU). La fonction SDDLU est activée dans Communications Server au moyen de la codification d'une instruction LU_MODEL dans une définition de LU.

Pour activer la fonction DDDLU dans VTAM, codifiez l'opérande LUGROUP dans l'instruction de définition de la PU, puis codifiez un nœud principal de groupe de LU. Pour utiliser l'exit SDDLU fourni par IBM, qui permet de générer les noms de LU à votre place, vous devez également codifier l'opérande LUSEED dans l'instruction de PU.

L'opérande LUGROUP indique le nom du groupe de définition de LU modèle utilisé par VTAM lors de la définition dynamique des LU de cette PU. Le nœud principal de groupe de LU contient les modèles d'instructions de définition. Des définitions dynamiques relatives aux LU sont créées à l'aide des modèles de définition de LU contenus dans ce nœud principal.

L'opérande LUSEED fournit un modèle de nom utilisé avec l'exit SDDLU afin de créer un nom pour la LU créée de façon dynamique. Une fois les instructions correctes ajoutées dans l'instruction de PU et le nœud principal de groupe de LU codifié, il est nécessaire que ces nœuds principaux soient actifs de sorte que la fonction SDDLU soit activée.

Support de demandeur d'unités logiques dépendantes

Le demandeur d'unités logiques dépendantes (DLUR) est une architecture qui fournit un support de LU dépendantes dans un réseau APPN. Communications Server prend en charge toutes les fonctions DLUR et les fonctions facultatives suivantes :

- Support SDDLU (Self-Defining Dependent LU)

  Ce support permet la définition dynamique des LU prises en charge par le DLUR pour VTAM ; une définition préalable de ces LU n'est donc plus nécessaire.

- Support TakeOver/GiveBack

  Ce support permet aux sessions LU-LU de rester actives même lorsque la connexion entre les nœuds DLUR et DLUS a échoué. La connexion peut être établie de nouveau avec le même DLUS ou avec un autre, sans que les sessions LU-LU soient interrompues.

- Support MultiSubnet

  Ce support permet aux nœuds DLUR et DLUS et au nœud contenant l'application de résider dans des sous-réseaux différents.

- Enregistrement de LU pris en charge par le DLUS

  Un DLUR de nœud d'extrémité enregistre ses LU de sorte que le nœud de réseau puisse localiser ces LU sans avoir à transmettre les requêtes Locate au DLUR.

- Support DLUS de secours

Lorsque la connexion au DLUS principal échoue ou qu'elle ne s'active pas, Communications Server tente automatiquement d'établir une connexion avec le DLUS de secours.

Utilisation du DLUR

Pour utiliser la fonction DLUR, configurez une définition **DLUR_DEFAULTS**, puis utilisez le nom de liaison de cette définition en tant que liaison hôte destinée à vos définitions de LUA, de LU 6.2 dépendante ou de passerelle. Communications Server transmet les paramètres PUNAME, CPNAME et NODEID au DLUS. Le paramètre PUNAME est envoyé dans le cadre des informations de signalisation (CV X'0E').

- Si le DLUS est de niveau supérieur (il prend en charge la vérification du CV X'0E' dans REQACTPU), il utilise le paramètre PUNAME dans son algorithme de recherche. Cela est disponible dans VTAM 4.3 avec PTF ou dans une version ultérieure.
- Si le DLUS est de niveau inférieur, il ne tient pas compte du CV X'0E'.
- Si PUNAME n'est pas concordant ou que le DLUS est de niveau inférieur, celui-ci tente de localiser une PU dont le nom de CP ou le NODEID (IDBLK/IDNUM) est concordant, et qui est prédéfinie dans un nœud principal de commutateur VTAM ou créée de façon dynamique à l'aide de l'exit ISTEXCCS.

Les connexions au réseau à l'aide de la connectivité de votre choix (Token Ring, SDLC, AnyNet, etc.) doivent être configurées et actives avant que la connexion du DLUR au DLUS soit établie. Une fois qu'une connexion APPN est disponible entre le DLUR et le DLUS, une paire de sessions de contrôle est établie entre le DLUR et le DLUS à l'aide d'un mode spécial, CPSVRMGR. Cette paire de sessions de contrôle est également désignée par canal de communication CP-SVR et apparaît sous forme de liaison à Communications Server. Par conséquent, elle peut être activée, désactivée et affichée à l'aide de l'utilitaire **Fonctionnement du nœud SNA**.

Une fois le canal de communication activé, le support SSCP à PU et SSCP à LU peut être fourni aux PU et LU qui ont défini le canal de communication comme leur liaison hôte. Les sessions LU à LU n'utilisent pas le canal de communication mais le meilleur chemin disponible via le réseau.

Dans l'environnement DLUR, tout nombre de PU dédiées peut être défini sur les sessions LU 6.2. Cela permet à la passerelle de fournir un accès de gestion au réseau via la PU dédiée vers des postes de travail en aval, sans que de nombreuses liaisons physiques aux hôtes soient nécessaires.

La figure 17, à la page 61, illustre un poste de travail Communications Server qui sert de passerelle DLUR à un poste de travail et à un contrôleur 4702.

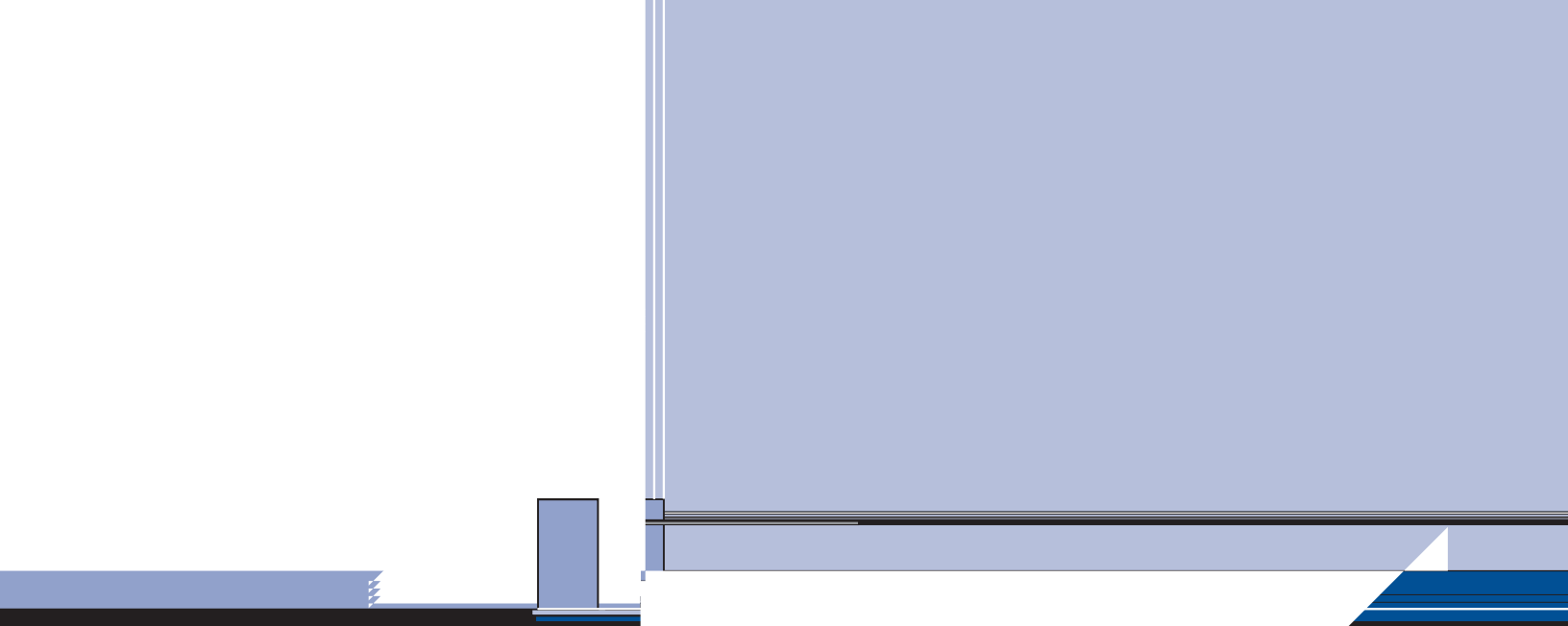


Figure 17. Connexion DLUR à un hôte via une passerelle Communications Server

Sessions LU-LU

Les LU de Communications Server peuvent activer des sessions et répondre aux demandes d'activation de session. Une LU active les demandes et répond à celles-ci en fonction du type de la LU (indépendante ou dépendante).

LU indépendante

Une LU indépendante est en mesure d'activer une session LU-LU (c'est-à-dire, d'envoyer une requête BIND) sans aucune assistance de la part du SSCP ; par conséquent, elle ne comporte pas de session SSCP-LU. Une LU indépendante peut envoyer et recevoir des BIND. L'émetteur du BIND est désigné par LU principale (PLU) et le récepteur du BIND par LU secondaire (SLU).

Seule une LU 6.2 peut être une LU indépendante. Communications Server prend en charge les protocoles de LU indépendantes pour les autres nœuds de type 2.1 et les nœuds de secteur LEN de type 5.

Les LU indépendantes peuvent établir des sessions parallèles entre la même paire de LU, ainsi que plusieurs sessions entre une seule LU et plusieurs autres LU. Le nombre maximal de sessions est établi en fonction du nom de mode ; il peut être compris entre 1 et 32 767.

La figure 18, à la page 62, explique comment des sessions multiples et parallèles peuvent être établies par une LU indépendante. LUx prend en charge des sessions parallèles avec LUy, et une seule session avec LUz. Le sens des flèches des sessions indique la relation PLU-SLU. LUx sert de PLU à la session établie avec LUz, et à une des sessions avec LUy. LUx sert également de SLU à une des sessions parallèles avec LUy.

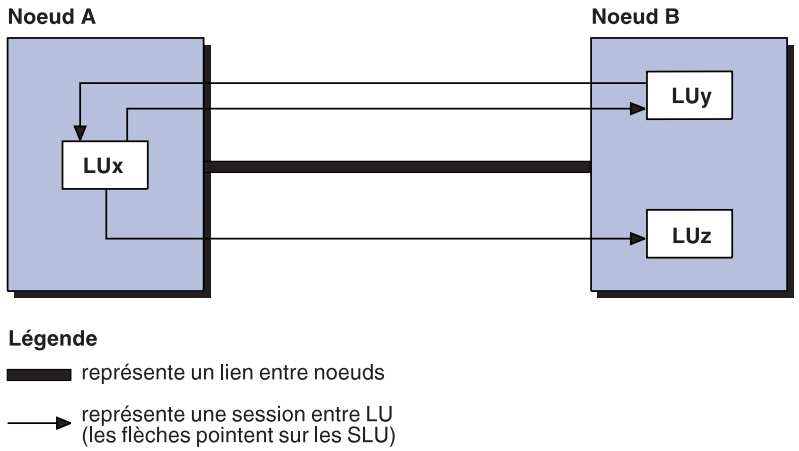


Figure 18. Sessions multiples et parallèles

LU dépendante

Il s'agit d'une LU qui est contrôlée par un système hôte SNA. Pour activer une session LU-LU, une LU dépendante nécessite l'assistance d'un SSCP. Elle requiert l'envoi d'un BIND par une session SSCP-LU. Les protocoles de LU dépendantes sont supportés par Communications Server mais uniquement pour les nœuds de secteur de type 5 utilisant des protocoles de type 2.0 et non aux autres nœuds périphériques de type 2.1. Les LU dépendantes servent uniquement de SLU et ne peuvent établir qu'une seule session LU-LU. Cependant, le support multi-PU de Communications Server permet d'établir plusieurs sessions SSCP-PU simultanées avec des sessions LU dépendantes.

La fonction DLUR (demandeur de LU dépendantes) permet à Communications Server de tirer parti du support SSCP évolué fourni par un serveur de LU dépendantes (DLUS). Voici quelques-uns des avantages de cette fonction :

- Les LU dépendantes peuvent résider sur des nœuds non adjacents à l'hôte ;
- La logique de recherche APPN recherche le meilleur chemin pour les sessions LU-LU ;
- Les LU dépendantes SNA peuvent bénéficier des avantages d'un réseau APPN.

Pour utiliser la fonction DLUR, configurez un paramètre **DEFINE_DEPENDENT_LU_SERVER**, puis utilisez le nom de liaison de cette définition pour vos définitions de LU, de LU 6.2 dépendantes ou de passerelle.

LU 6.2

Pour définir des LU dépendantes pour le programme VTAM, codifiez LOCADDR=0. Vous pouvez en définir autant que vous le souhaitez. Cependant, il est à noter que toutes les LU 6.2 ne sont pas des LU indépendantes.

Lors de la définition des LU d'une partie du réseau APPN pour le programme VTAM, elles doivent être définies comme étant dans le nœud de réseau qui connecte cette extrémité du réseau APPN au réseau de secteur. À la suite de la définition de PU de ce nœud de réseau, définissez chacune des LU auxquelles vous voulez accéder à partir de l'autre extrémité du réseau APPN. Rappelez-vous que les points de contrôle sont des LU.

Une LU doit être définie dans VTAM pour établir une session avec une autre LU si cette session traverse le réseau de secteur. Il n'est pas possible de contourner cette procédure (par exemple, les caractères génériques d'APPN) ; VTAM doit identifier le nom de chaque LU de destination.

Dans la mesure où un réseau APPN est conçu pour être modifié aisément, les LU du réseau APPN doivent être définies dans un nœud principal particulier chaque fois que cela s'avère possible. Vous pouvez également définir, dans VTAM, des LU qui n'existent pas encore.

Autres LU

Si le nœud de réseau utilise sa connexion au réseau de secteur pour une émulation 3270, les LU de type 2 de LU de l'émulation 3270 sont définies dans la même macro de PU que les LU de type 6.2 de LU du réseau APPN. La liaison est également utilisée pour la connexion entre l'émulation 3270 et l'hôte.

Nœud de réseau APPN et support T2.1

APPN est une extension de l'architecture de nœud de type 2.1 (T2.1) et SNA d'IBM. APPN permet une interconnexion entre les systèmes de taille très différente et les réseaux d'une topologie dynamique. Un réseau APPN est plus facile à utiliser ; il est plus fiable et fournit une souplesse supérieure à celle des réseaux SNA traditionnels.

Pour plus de détails sur les nœuds de réseau APPN, consultez le manuel *3174 APPN Implementation Guide*.

Compression de données

La compression de données consiste à comprimer des octets ou des chaînes de données identiques afin de réduire la taille des enregistrements ou des blocs. Cela permet de réduire le temps de transfert requis pour les communications. En réduisant la quantité des données transférées entre des sessions d'hôte et de poste de travail, vous pouvez augmenter le débit lors des connexions à faible vitesse et baisser le coût par bit lors des connexions coûteuses.

Le gain de performances (mesuré à l'aide du nombre d'octets transférés) que vous pouvez escompter en utilisant la compression de données correspond généralement à un rapport de 2:1. Cela signifie que, lorsque la compression de données est active, vous économisez environ un octet sur deux dans les mémoires tampon requises pour la conversion de protocole de niveau inférieur.

La compression de données présente les avantages suivants :

- temps de réponse améliorés, notamment lors des connexions à faible vitesse ;
- coûts réduits pour certains types de liaison dont les coûts sont déterminés par la quantité de données ;
- nombre inférieure de liaisons spécialisées.

Cependant, la compression de données ne doit pas être appliquée à toutes les sessions en cours d'exécution dans la mesure où les inconvénients suivants doivent être pris en compte :

- La compression et la décompression requièrent des cycles processeurs supplémentaires.
- Une mémoire de données supplémentaire (32 octets à 9,0 ko) est nécessaire.
- La compression de données requiert une liaison sécurisée comme défini dans votre table de classe de service APPN.
- Un réglage de la taille de RU est peut-être requis pour optimiser les performances. Chaque RU est comprimée, puis transmise. Si des paquets sont en cours de transmission, une taille de RU plus importante sur le mode permet d'envoyer des paquets plus complets.

  Remarque : L'augmentation de l'espace mémoire est fonction de l'algorithme de compression utilisé. Cette augmentation s'ajoute à la mémoire requise pour le message.

Pour plus de détails sur les différents algorithmes de compression, consultez les manuels suivants :

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

Les sections suivantes décrivent la compression au niveau des sessions SNA, ainsi que la mise en œuvre de Communications Server.

Architecture de compression au niveau des sessions SNA

La compression au niveau des sessions SNA est mise en œuvre dans une demi-session LU-LU. Dans Communications Server, elle est accessible à tous les types de LU pris en charge : LU de types 0, 1, 2, 3 et 6.2. La compression de données au niveau des sessions présente les avantages suivants :

- Plus grande efficacité de la compression des données avant le chiffrement de ces dernières
- Meilleures performances des différents algorithmes pour des types de données différents
- Logique de compression désormais inutile pour les programmes d'application

Les deux algorithmes suivants sont généralement définis pour la compression au niveau des sessions SNA : RLE (Run Length Encoding) et un type de LZ (Lempel-Ziv). Communications Server prend en charge la compression au niveau des sessions SNA, à l'aide des algorithmes suivants :

- Aucune compression
- Compression RLE : RLE représente l'algorithme le plus simple et le plus couramment utilisé ; il remplace des chaînes ou des octets identiques par de courtes chaînes codifiées.

- Compression LZ9 : LZ9 est un algorithme de compression dynamique qui convertit des chaînes déjà relevées (dans les RU précédentes ou dans la RU en cours) en code de 9 bits ; ce code représente l'index d'origine zéro d'une entrée dans la table de compression/décompression. Les entrées de la table contiennent les chaînes déjà répertoriées.
- Compression LZ10 : LZ10 est un algorithme de compression dynamique qui convertit des chaînes déjà relevées (dans les RU précédentes ou dans la RU en cours) en code de 10 bits ; ce code représente l'index d'origine zéro d'une entrée dans la table de compression/décompression. Les entrées de la table contiennent les chaînes déjà répertoriées.

En général, l'algorithme LZ est plus efficace que la méthode RLE mais son coût, en termes de mémoire et de cycles processeurs, demeure plus élevé.

La compression au niveau des sessions SNA considère la session dans les deux sens suivants : PLU-SLU et SLU-PLU. L'unité logique principale (PLU) est la LU responsable de l'activation de la session. L'unité logique secondaire (SLU) est la LU qui répond. La PLU active une session en envoyant une requête de session BIND à la SLU qui répond à l'aide d'une BIND. Cela signifie que des algorithmes de compression différents peuvent être utilisés dans les sens PLU-SLU et SLU-PLU, au moyen d'une négociation BIND des niveaux de compression. LU 6.2 peut utiliser n'importe quelle combinaison de niveaux de compression pour une session (par exemple, PLU peut utiliser l'algorithme RLE et SLU-PLU l'algorithme LZ9). La fonction de compression de tous les autres types de LU est activée ou désactivée. Lorsqu'elle est activée, le niveau de compression PLU-SLU est LZ9 et celui de SLU-PLU est RLE.

Compression de données Communications Server

Communications Server prend en charge la compression de données au niveau des sessions SNA, à l'aide des algorithmes de compression RLE, LZ9 et LZ10. Communications Server permet d'indiquer l'utilisation de la compression de données pour les communications sur des sessions CPI-C (via une session APPC), APPC (LU 6.2) et LUA (LU 0, LU 1, LU 2 et LU 3).

Une configuration constituée de deux parties permet d'activer la compression de données.- Le nœud de Communications Server doit être activé pour la compression de données, la LU (APPC et LUA) devant être activée en premier. Les deux zones de compression de nœud (niveau et jetons) figurent dans la fenêtre des caractéristiques locales du nœud (mot clé **NODE** du fichier .ACG).

La zone de niveau de compression définit le niveau maximal qui permet de lancer une session : NONE, RLE, LZ9 ou LZ10. Cette zone est prioritaire sur tous les niveaux de compression configurés ou tentés (à la seule exception du DFT autonome qui ne requiert pas la définition du nœud). Si une session utilisant LUA (LU 0, LU 1, LU 2 et LU 3) est en cours de configuration pour la prise en charge des imprimantes ou de l'émulation 3270, l'algorithme LZ9 est requis pour la compression de données. Les autres niveaux de compression ne permettent pas la compression de données pour ces types de LU.

La taille par défaut des unités de requête des modes comprimés est égale à deux fois la taille des BTU de la connexion. Si une commutation de paquets en cours, il n'est peut-être pas souhaitable d'utiliser la taille par défaut ; utilisez une taille plus importante, puis segmentez les paquets.

La compression LU 6.2 peut être activée à l'aide des opérations suivantes :

- Utilisation des modes fournis avec Communications Server :
  - #INTERC
  - #BATCHC
  - #BATCHCS
  - #INTERCS
- Modification ou ajout de modes, la compression étant activée

Trois zones de compression de mode (Besoin de compression, Niveau de compression PLU/SLU, niveau de compression SLU/PLU) s'affichent sur le panneau Définition de mode (mot clé **MODE** du fichier .ACG).

La zone Besoin de compression peut comporter deux valeurs :

Interdite Aucune compression.

Demandée Permet de demander une compression de données à l'aide des valeurs définies dans les niveaux de compression PLU/SLU et SLU/PLU. Il se peut que le niveau demandé ne soit pas obtenu pour les raisons suivantes :

- Les paramètres du nœud ont limité le niveau admissible
- La SLU a négocié des valeurs faibles pour les niveaux

La SLU traite les niveaux de compression demandés par la PLU, sauf s'ils sont limités par les paramètres de compression du nœud.

Pour plus de détails sur la compression Communications Server, consultez l'aide en ligne du produit ou le manuel *Configuration File Reference*.

Chiffrement au niveau des sessions SNA

Le chiffrement au niveau des sessions SNA permet de chiffrer tout ou partie des données transférées entre le poste de travail et l'hôte. Pour protéger les données du poste de travail à l'aide de la fonction de chiffrement, l'hôte doit également être configuré pour utiliser le chiffrement.

Une carte IBM 4758 (ou IBM SecureWay 4758 PCI Cryptographic Coprocessor) doit être installée sur le serveur pour assurer la confidentialité des données. Cette carte doit être initialisée par les instructions suivantes qui l'accompagnent.

Dans Communications Server, le chiffrement au niveau des sessions LU 6.2 est configuré en fonction de la description de mode utilisée pour un programme de transactions donné. Les deux niveaux de chiffrement suivants sont disponibles :

- Niveau de session APPC

  Uniquement entre deux LU, aucun point de contrôle ne s'implique dans les clés de conversion

- Conversion de clés de session APPC

  Le point de contrôle de la LU d'origine (EN ou NN) et éventuellement son serveur NN convertissent les clés en plus de la LU d'origine.

Pour configurer un mode de chiffrement, affichez la fenêtre Fonctions SNA, puis sélectionnez **MODES**. Dans la fenêtre Définition de mode, sélectionnez **Configurer...**. La fenêtre Support de compression et de chiffrement au niveau des sessions apparaît. Les paramètres de la configuration de chiffrement sont constitués des deux parties suivantes :

- Pour le chiffrement au niveau des sessions, vous pouvez indiquer s'il s'agit d'un chiffrement facultatif (les LU négocient) ou obligatoire (le chiffrement doit être utilisé).

  Remarque : Le chiffrement à partir de Communications Server vers un hôte est systématiquement obligatoire.

- En ce qui concerne la conversion des clés de session APPN, vous pouvez indiquer que la clé de session est convertie par la LU seule, par le nœud d'extrémité seul ou par le nœud d'extrémité et le nœud de réseau.

Communications Server requiert d'autres produits pour le stockage et la conversion des clés. Un produit CCA (Common Cryptographic Architecture) est nécessaire au stockage des clés ; il est géré par les utilitaires fournis avec la carte IBM 4758. Communications Server fait appel à un produit CCA qui dialogue avec la carte IBM 4758 pour accéder aux clés et chiffrer les données.

Utilisateurs VTAM :

Communications Server ne permet pas le chiffrement de la session SNASVCMG. Vous devez indiquer ENCR=OPT dans l'instruction APPL de votre définition d'application VTAM. Sous VTAM, le chiffrement doit être précisé dans l'instruction MODEENT. Par exemple :

```
ENCR=B'□□11' FOR MANDATORY ENCRYPTION
```

Pour utiliser la fonction de chiffrement de VTAM, vous devez activer la fonction PCF (Programmed Cryptographic Facility) d'IBM avant de lancer VTAM.

À partir de VTAM V3R4.1, VTAM utilise une nouvelle interface à ICSF/MVS (Integrated Cryptographic Service Facility/MVS) pour les services de chiffrement, par exemple, un chiffrement au niveau des sessions. Cette interface est conforme à l'architecture CCA (Common Cryptographic Architecture) mise en œuvre par ICSF/MVS. Ce support permet de démarrer et d'arrêter la fonction de chiffrement une fois VTAM lancé, et de modifier la clé principale sans interrompre VTAM ou les sessions LU-LU actives.

Pour plus de détails sur le mode de définition du chiffrement de données, consultez le manuel *OS/390 eNetwork Communications Server: SNA Network Implementation*.

Services de gestion

Les services de gestion de Communications Server sont des fonctions réparties entre les composants de réseau aux fins d'exploitation, de gestion et de contrôle d'un réseau. Cette fonction est fondée sur l'architecture de services de gestion SNA documentée dans le manuel *Systems Network Architecture Management Services Reference*.

Points focaux, points de service et points d'entrée

Communications Server fournit un support de programmation qui permet l'installation des applications de points focaux (FP), de points de service (SP) et de points d'entrée (EP) des services de gestion. Les applications SP de services de gestion correspondent simplement à une variante des applications EP de services de gestion, seuls les types de fonction qu'ils fournissent étant différents ; sinon, ils dialoguent avec un point focal de services de gestion sous forme d'applications EP de services de gestion.

Point focal Un point focal de services de gestion est un point central de contrôle permettant la gestion d'un réseau. À partir d'une application SP ou EP de services gestion, le point focal peut demander certaines données relatives au fonctionnement d'un réseau, par exemple, des données d'incident et de performances ou l'identification du produit.

Le point focal de services de gestion peut également accepter des nœuds qu'il gère certaines données de services de gestion non sollicitées, en fonction de la catégorie des données de services de gestion. À titre d'exemple de catégorie de services de gestion, on peut citer les alertes MS. Un point focal de services de gestion peut gérer une ou plusieurs catégories de données de services de gestion, un réseau pouvant contenir un ou plusieurs points focaux des services de gestion. À titre d'exemple, les produits Communications Server, NetView et le système d'exploitation OS/400 fournis par IBM assurent la fonction de point focal de services de gestion.

Point de service Il s'agit de la fonction d'un nœud qui permet la demande et la capture de données à partir des périphériques qui seuls ne peuvent pas servir de points d'entrée de services de gestion, par exemple, les périphériques connectés par des protocoles de réseau local (et non des protocoles SNA de niveau supérieur) au nœud SP de services de gestion. En plus de la collecte des données non locales, un SP de services de gestion fonctionne comme un EP de services de gestion dans ses rapports avec le point focal de services de gestion. Les programmes IBM NetView/PC et IBM LAN Network Manager constituent des exemples d'applications EP de services de gestion qui fournissent des fonctions SP et EP de services de gestion.

Point d'entrée Il s'agit de la fonction d'un nœud qui permet la capture des données de services de gestion locales et la transmission de ces dernières à un point focal de services de gestion aux fins de traitement, à la demande ou non. Communications Server assure la fonction EP de services de gestion pour envoyer des alertes au point focal de services de gestion d'alertes. Ces alertes peuvent provenir de Communications Server ou des DLC que celui-ci utilise. Communications Server fournit également un support de programmation destiné aux applications telles que les programmes IBM NetView/PC et IBM LAN Network Manager, en fournissant des alertes à envoyer au point focal de services de gestion d'alertes.

Niveaux de l'architecture de services de gestion SNA

Un produit SNA met en œuvre un niveau (ou une génération) particulier de l'architecture de services de gestion SNA, certains produits prenant en charge plusieurs niveaux de l'architecture. Communications Server peut envoyer ou recevoir des données de services de gestion en provenance ou à destination des produits SNA qui mettent en œuvre l'un des trois niveaux suivants de l'architecture de services de gestion :

Niveau MDS (Multiple Domain Support) Produit SNA mettant en œuvre le niveau MDS de l'architecture de services de gestion, par exemple, Communications Server et IBM NetView version 2, édition 2 (ou ultérieure). Il peut envoyer et recevoir des unités de message MDS. IBM NetView version 2 édition 2 fournit le niveau MDS sous forme de LU de secteur et non de point de contrôle (CP), et utilise des sessions en mode SNASVCMG pour transporter des unités de message MDS. En tant que point focal, il prend en charge des relations FP-EP explicites, implicites (principales) et implicites (secondaires). NetView version 2 édition 2 continue également de prendre en charge la relation FP-EP hôte avec les produits EP qui ne sont pas dotés du support de niveau MDS.

Niveau de migration Produit SNA mettant en œuvre le niveau précédent de l'architecture de services de gestion, par exemple, IBM OS/400 version 1, édition 3, niveau de modification 0 (ou antérieure). Un produit de niveau migration peut prendre en charge des relations FP-EP explicites, par défaut et de domaine. La relation FP-EP de domaine est déduite lorsque les sessions CP-CP sont activées sur un nœud de niveau migration. Un nœud de réseau de niveau migration ne transmet pas MS Capabilities for FP Notification à ses nœuds d'extrémité pris en charge ; un nœud d'extrémité de niveau migration n'accepte pas MS Capabilities for FP Notification à partir de son nœud de réseau. Il peut transmettre et recevoir des MSU CP et non des MU MDS. En tant que point focal, il ne prend en charge que la catégorie MS d'alerte.

Niveau NMVT (Network Management Vector Transport) Produit SNA mettant en œuvre le niveau NMVT de l'architecture de services de gestion, par exemple, IBM NetView version 2, édition 1 (ou ultérieure). NMVT est une unité de requête (RU) de services de gestion qui circule via une session active entre des services de gestion de PU et des services de gestion de point de contrôle. Si un NMVT est acheminé à partir d'un poste de travail via une passerelle, cette dernière ajoute son nom de point de contrôle dans le NMVT.

Contrôle de flux

Pour gérer le flux de données via un réseau, Communications Server utilise la régulation adaptative au niveau des sessions. Cette régulation a lieu entre chaque paire de nœuds adjacents participant au chemin de session. La régulation entre deux nœuds adjacents est indépendante de celle utilisée entre les autres nœuds adjacents du chemin.

Régulation au niveau des sessions

La régulation adaptative au niveau des sessions utilise un système de fenêtres permettant à un émetteur d'envoyer uniquement un nombre limité ou une ***fenêtre*** d'unités de requête par autorisation explicite de poursuite. La taille de la fenêtre peut être modifiée en fonction des conditions en vigueur au niveau du destinataire. Cette fonction permet à un nœud de contrôler la quantité des données transmises et reçues lors du fonctionnement normal des sessions. Le contrôle de fenêtre permet au nœud récepteur de gérer la vitesse de réception des données dans ses mémoires tampon de session. La régulation adaptative au niveau des sessions permet à un nœud qui prend en charge plusieurs sessions d'allouer de manière dynamique des ressources à une session très active et de récupérer les ressources non utilisées des sessions sans activité. La régulation adaptative au niveau des sessions permet au nœud récepteur d'utiliser de manière efficace les ressources disponibles de ses mémoires tampon.

Dans la mesure où chaque étape de session entre les points d'extrémité est régulée de manière indépendante, les deux nœuds de points d'extrémité et les nœuds intermédiaires peuvent adapter la régulation des sessions qu'ils traitent conformément à leurs propres conditions d'encombrement locales. Cette action sert de base au contrôle de flux global et à la gestion d'encombrement au sein des réseaux APPN.

Si, cependant, une session interactive et une session transférant un fichier volumineux partagent une liaison, les données de la session intermédiaire doivent être transmises aussi rapidement que possible. Pour ce faire, procédez de l'une des deux manières suivantes ::

1. Attribuez une priorité plus faible à la session de transfert de fichiers. #BATCH utilise une faible priorité.
2. Utilisez la régulation fixe en indiquant une petite taille de fenêtre pour la session de transfert de fichiers, afin de permettre aux données de la session active d'utiliser la liaison lorsque la session de transfert de fichiers attend la réponse de régulation. En cas de connexion directe à un hôte NCP, la régulation de fenêtre fixe bidirectionnelle peut être utilisée pour paramétrer la régulation dans les deux sens sur la fenêtre de réception du mode défini.

Régulation BIND adaptative

Le trafic BIND peut avoir lieu en rafales, notamment au démarrage du nœud ou du réseau. Par conséquent, la régulation BIND adaptative permet de contrôler le flux des BIND entre deux nœuds adjacents. Le même algorithme de fenêtre destiné à la régulation au niveau des sessions est utilisé.

Segmentation et Réassemblage

Pour transmettre des RU dont la taille est supérieure à la taille de BTU maximale admise par une liaison particulière, Communications Server prend en charge la segmentation et le réassemblage des données. Ces segments sont réassemblés dans des RU complètes au niveau du nœud partenaire. Ainsi, la taille de RU définie pour une session est indépendante de la liaison qui est utilisée pour le chemin.

Régulation HPR

Le routage hautes performances (HPR) fournit une nouvelle méthode de contrôle de flux appelée contrôle d'encombrement ARB (Adaptive Rate-Based). ARB régule le flux de travail en prévoyant l'encombrement du réseau et en réduisant la vitesse d'émission d'un nœud dans le réseau, afin d'empêcher l'encombrement au lieu d'y remédier.

Régulation fixe

La régulation fixe permet de partager une connexion physique entre deux sessions. En l'absence d'une régulation fixe, les données à transmettre sont placées dans une file d'attente DLC commune et des données interactives suivent les données précédemment mises en file d'attente. La régulation fixe réduit également l'espace mémoire qui permet de placer les données dans la file d'attente DLC. Une régulation fixe bidirectionnelle peut être utilisée avec un NCP, afin d'éviter de définir une régulation fixe hôte. Cependant, la régulation adaptative est généralement la méthode de transfert de données la plus efficace entre les nœuds.

La priorité de transmission, comme la régulation fixe, permet le partage d'une liaison physique entre les sessions. Cependant, elle bloque la mémoire à mesure que des données sont placées dans les files d'attente DLC, mais elle ne requiert pas les réponses de régulation supplémentaires qui sont nécessaires à la régulation fixe.

Partitionnement des LU entre les hôtes

Lors de la définition de plusieurs connexions hôte de secteur, il est nécessaire que le trafic provenant du domaine d'un hôte donné accède à une seule liaison logique. Il est à noter que les connexions commutées manuelles apparaissent comme étant une seule liaison. Vous devez définir une PU différente pour la prise en charge de chaque hôte. Seules les liaisons hôte définies sur le point de contrôle peuvent établir des sessions CP-CP et participer au réseau APPN. Les liaisons ayant pour valeur **USE_PU_NAME_IN_XID=1** ne peuvent pas établir de sessions CP-CP. Dans les autres cas, les liaisons hôte peuvent établir des sessions CP-CP et participer à une communication APPN. Le mot clé **LINK_STATION** indique le nom de PU et la liaison logique à utiliser pour la PU. Si des liaisons parallèles sont requises (lorsque plus de 254 LU dépendantes sont disponibles), le support de session CP-CP d'une des liaisons doit avoir pour valeur Non.

Chaque LU dépendante peut être définie comme étant associée à une seule PU. Le mot clé **LOCAL_LU** indique le nom de liaison hôte utilisé pour une LU dépendante de type 6.2. Le mot clé **LU_0_TO_3** définit le nom de liaison hôte destiné à la LUA alors que le profil 3270 indique la liaison hôte de chaque session d'émulation 3270.

Une PU automatiquement définie par le point de contrôle porte le même nom que ce dernier. Les LU dépendantes qui sont définies sur un seul SSCP de secteur peuvent être associées à la PU de point de contrôle. (En effet, la LU automatiquement définie pour le point de contrôle peut également être indiquée comme étant dépendante.) Chaque PU 2.0 supplémentaire destinée à un hôte de secteur différent requiert une définition de PU et de liaison distincte. Pour définir une PU, indiquez PU dans un mot clé **LINK_STATION**. Cela n'est pas nécessaire si toutes les LU sont indépendantes.

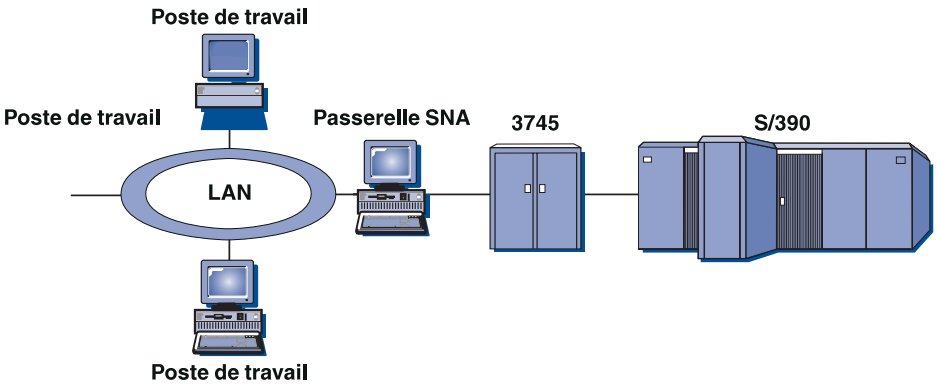
Si la session SSCP-PU est amenée à envoyer des alertes à l'hôte, la liaison de point focal doit être définie à l'aide du mot clé **NODE** du fichier .ACG. Si un hôte est amené à recevoir des alertes, une liaison logique à l'hôte doit être indiquée pour le point de contrôle. Si la liaison à cet hôte n'est pas disponible, Communications Server consigne les alertes. Les seules demandes de gestion de réseau qui sont acceptées d'un hôte PU 2.0 sont celles de la PU de point de contrôle. Des réponses sont envoyées au même hôte à l'aide de la PU de point de contrôle.

Chaque unité logique dépendante doit comporter une adresse locale configurée qui est identique à celle configurée au niveau de l'hôte. Cependant, l'utilisation de la passerelle SNA permet une conversion d'adresse de passerelle. Une LU 6.2 dépendante peut servir de LU indépendante à un nœud d'égal à égal ; cela signifie qu'elle n'est dépendante que pour le secteur. Ce type de LU ne doit pas faire partie d'un réseau APPN doté d'une autre connexion au même secteur, c'est-à-dire, le secteur qui contient le SSCP de contrôle. Une seule connexion de secteur est admise pour un réseau APPN, sauf si les secteurs sont indépendants. Même si une passerelle peut établir des connexions parallèles au même secteur, une seule de ces connexions peut avoir des sessions CP-CP et un trafic APPN.

Un SSCP du réseau de secteur active les LU dépendantes qu'il contrôle, une fois la liaison au SSCP établie. La LU ne peut pas démarrer de session tant qu'une LU n'est pas activée. Lorsque APPC est démonté, une déconnexion est demandée à chaque hôte actif ayant établi une session avec une PU du nœud. Chaque hôte libère la liaison après avoir activé les LU, puis la PU de la session SSCP-PU.

Support de passerelle SNA

Communications Server fournit une passerelle SNA (Systems Network Architecture) à fonctions intégrales. Cette passerelle permet à plusieurs postes de travail connectés au réseau local d'accéder aux hôtes IBM 370 ou IBM 390 via une ou plusieurs connexions physiques à un ou plusieurs hôtes. Cela permet de réduire le coût, par poste de travail, des connexions à l'hôte.



Une passerelle peut également servir de convertisseur de protocole entre les postes de travail connectés à un réseau local et à une liaison hôte longue distance.

Les LU définies dans la passerelle peuvent être dédiées à un poste de travail particulier ou regroupées entre plusieurs postes de travail. Ce regroupement permet aux postes de travail de partager des LU communes, ce qui augmente l'efficacité des LU et réduit les configurations et démarrages requis au niveau de l'hôte. Vous pouvez également définir plusieurs groupes de LU, chacun associé à une application particulière. Vous avez également la possibilité de définir des groupes communs associés à plusieurs hôtes. Lorsqu'un client se connecte à la passerelle, cette dernière extrait une LU du groupe pour établir une session. La LU est renvoyée au groupe de sorte qu'elle soit accessible à d'autres postes de travail à la fin de la session.

En outre, une passerelle SNA peut prendre en charge la transmission de NMVT entre les postes de travail et l'hôte.

La passerelle SNA est considérée par chaque hôte comme un nœud SNA PU 2.0 prenant en charge une ou plusieurs LU par poste de travail. En ce qui concerne l'hôte, toutes les LU font partie de la PU de passerelle SNA. La passerelle SNA peut disposer de plusieurs connexions simultanées à l'hôte et diriger des sessions de postes de travail différentes à des hôtes spécifiques.

La passerelle SNA est considérée par les postes de travail pris en charge comme un contrôleur de communication SNA PU 4 ; elle transmet des requêtes hôte telles que BIND et UNBIND. Les LU de postes de travail ne sont pas informées de l'existence de la passerelle SNA. Cependant, cette dernière est informée de toutes les LU des postes de travail.

Les applications en aval qui utilisent les protocoles de connectivité SNA pour les LU 0, 1, 2 et 3 et la LU 6.2 dépendante, et qui communiquent via une passerelle SNA avec un hôte, sont prises en charge par Communications Server. Le tableau 4, à la page 74 récapitule les caractéristiques de la passerelle SNA.

Tableau 4. Récapitulatif de la passerelle SNA

Caractéristiques	Description
Postes de travail actifs	254 (RL) par carte 128 (X.25)
DLC	AnyNet (SNA sur TCP/IP) Twinaxial (en amont uniquement) Réseau local (toute carte réseau conforme à NDIS**) X.25 SDLC (synchrone, asynchrone et AutoSync) OEM Channel (en amont uniquement) MPC Channel (en amont uniquement, requiert le DLUR) Enterprise Extender
Postes de travail en aval	Tout produit prenant en charge les protocoles de connectivité SNA standard destinés aux LU 0, 1, 2, 3 et 6.2.
Ajouts et modifications dynamiques	Oui
Support de poste de travail implicite	Oui
Regroupement de LU	Oui
Nombre maximal de LU	254 par PU ; le nombre de PU n'est pas limité
Mode de fonctionnement	Plusieurs PU en aval. Les PU ne sont pas visibles au niveau de l'hôte (sauf via le DLUR)
Support multi-PU	Oui
Support de segmentation	Oui
Types de LU pris en charge	LU 0, 1, 2, 3 et LU 6.2 dépendante

Planification et installation

Planification du support AnyNet

Communications Server permet deux types de support AnyNet :

- Passerelle et nœud d'accès AnyNet SNA sur TCP/IP
- Passerelle et nœud d'accès AnyNet Sockets sur SNA

La fonction AnyNet SNA sur TCP/IP de Communications Server permet aux applications SNA de communiquer via des réseaux IP et SNA interconnectés.

La fonction de nœud d'accès SNA sur TCP/IP permet aux applications SNA résidant sur un réseau IP de communiquer. Cette fonction prend en charge la LU 6.2 indépendante et les LU 0, 1, 2, 3 ou 6.2 dépendantes avec ou sans demandeur de LU dépendantes (DLUR). En outre, le nœud d'accès SNA sur TCP/IP peut être utilisé conjointement avec une passerelle SNA pour activer des sessions de passerelle SNA sur TCP/IP.

La fonction de passerelle SNA sur TCP/IP permet l'extension de la portée des applications SNA en permettant aux applications SNA d'un réseau SNA de communiquer avec des applications SNA d'un réseau IP. La passerelle SNA sur TCP/IP prend en charge les sessions LU 6.2 indépendantes.

Pour plus de détails sur le mode de configuration d'AnyNet SNA sur TCP/IP, reportez-vous à la section «Configuration d'AnyNet SNA sur TCP/IP».

La fonction de nœud d'accès Sockets sur SNA permet aux programmes d'application TCP/IP utilisant les interfaces Socket WinSock 1.1 et WinSock 2.0 de communiquer via un réseau SNA.

La fonction de passerelle Sockets sur SNA permet aux applications Socket des réseaux SNA et TCP/IP de communiquer. Les passerelles Sockets sur SNA servent généralement à connecter des réseaux TCP/IP isolés, à l'aide d'un réseau fédérateur SNA.

Pour plus de détails sur la configuration de Sockets sur SNA, reportez-vous à la section «Configuration d'AnyNet Sockets sur SNA», à la page 90.

Configuration d'AnyNet SNA sur TCP/IP

La présente section contient des informations détaillées sur la configuration d'AnyNet SNA sur TCP/IP.

Mappage des ressources SNA aux adresses IP

Une des étapes les plus importantes permettant une communication SNA sur TCP/IP n'est pas effectuée via les panneaux de Communication Server. Avant l'établissement de sessions ou de connexions SNA, SNA sur TCP/IP doit déterminer l'adresse IP du partenaire en mappant l'identificateur SNA du partenaire à une adresse IP à l'aide des étapes suivantes :

1. SNA sur TCP/IP reçoit l'identificateur SNA de Communications Server dans l'un des formats suivants :
   - Pour les noms de LU, `idres.nomlu`

- Pour les noms de CP, idres.nomcp
- Pour les valeurs IDBLK et IDNUM configurées comme ID nœud adjacent, à l'aide des deux zones suivantes :: ID de bloc et ID d'unité physique.

2. SNA sur TCP/IP utilise l'identificateur et génère un nom de domaine :
   - Pour les noms de LU, nomlu.idres.suffixesna
   - Pour les noms de CP, nomcp.idres.suffixesna
   - Pour les valeurs IDBLK et IDNUM values, bbbnnnnn.suffixesna

     Remarque : La valeur par défaut de suffixesna est **SNA.IBM.COM**. Pour plus de détails sur le suffixe de nom de domaine SNA, consultez l'aide en ligne.

   La figure 20 illustre des exemples de noms de domaine générés par SNA sur TCP/IP.

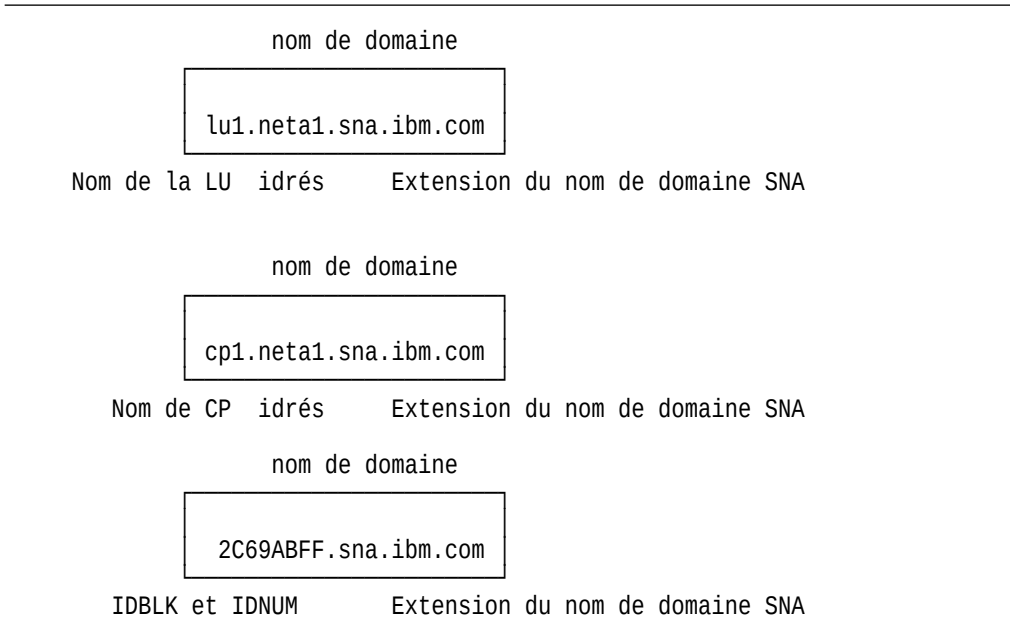


Figure 20. Formats des noms de domaine créés par SNA sur TCP/IP

3. SNA sur TCP/IP demande la conversion du nom de domaine en une adresse IP.
4. TCP/IP utilise le fichier HOSTS ou le serveur de noms de domaine pour convertir le nom de domaine en une adresse IP (par exemple, 9.67.192.28).

Lorsque le réseau IP comporte des passerelles SNA sur TCP/IP, prenez en considération les remarques supplémentaires suivantes relatives au mappage d'adresses :

- Si la LU partenaire est accessible via une passerelle, le nom de domaine du partenaire doit être mappé à l'adresse IP de la passerelle. En présence de passerelles parallèles, le nom de domaine doit être mappé à chaque adresse IP de passerelle.

- Pour minimiser les informations de mappage d'adresses requises pour AnyNet, pensez à utiliser une convention de dénomination dans laquelle le nom de LU est identique au nom d'hôte TCP/IP. Par exemple, considérez que le nom d'hôte de votre ordinateur est PATR.ANYNET.OURCORP.COM. Si vous utilisez le nom de LU PATR et l'ID réseau ANYNET et que vous attribuez au suffixe de nom de domaine SNA la valeur OURCORP.COM, AnyNet demande à TCP/IP de résoudre le nom PATR.ANYNET.OURCORP.COM. Ce nom doit déjà figurer dans votre serveur de noms de domaine.

Définition des noms de domaine et des adresses IP

La présente section décrit la fonction de résolution de nom de TCP/IP utilisée par AnyNet pour mapper les ressources SNA aux adresses IP. Cette fonction interroge le fichier HOSTS local et les serveurs de noms de domaine pour convertir un nom de domaine (par exemple, `lu1.neta1.sna.ibm.com`) en une adresse IP (par exemple, 10.1.1.1).

Fichier HOSTS Vous pouvez utiliser des fichiers HOSTS TCP/IP pour mapper les noms de domaine aux adresses IP de votre réseau. Cependant, à mesure que le réseau s'agrandit et que le maintien du fichier HOSTS sur chaque poste de travail d'utilisateur final prend trop de temps, il est conseillé d'utiliser un serveur de noms de domaine.

Le fichier HOSTS (du sous-répertoire drivers\etc de votre répertoire système Windows NT) répertorie les éléments suivants :

- Adresse IP
- Nom de domaine
- Autres alias du nom de domaine

Par exemple, si l'adresse IP a pour valeur 10.1.1.1, l'ID réseau RESA1, le nom de ressource SNA LUA1 et que le suffixe de nom de domaine SNA correspond à la valeur par défaut (`sna.ibm.com`), les valeurs suivantes doivent être entrées dans le fichier HOSTS :

```
1□.1.1.1      lua1.neta1.sna.ibm.com
```

Serveur de noms de domaine Les noms de domaine et les adresses IP peuvent également être définies dans la base de données du serveur de noms de domaine.

Chaque identificateur SNA est mappé par un serveur de noms de domaine à une adresse IP correspondante. L'emplacement de ces serveurs est configuré dans la section Réseau du Panneau de configuration.

Pour plus de détails sur les fichiers HOSTS et sur les serveurs de noms de domaine, consultez la documentation TCP/IP. Si votre poste de travail utilise le support TCP/IP sous Windows NT, consultez la documentation TCP/IP en ligne qui accompagne le produit Windows NT.

Remarques relatives aux passerelles SNA sur TCP/IP

La présente section décrit les passerelles et non les fonctions de nœud d'accès.

Définition des noms de CP et de réseau de connexion uniques

En ce qui concerne les configurations dont au moins deux passerelles SNA sur TCP/IP connectent un réseau SNA à au moins deux réseaux IP, il est nécessaire de définir un nom de point de contrôle (CP) SNA unique et un nom de réseau de connexion SNA unique pour chaque réseau IP.

Toutes les LU qui résident sur des nœuds d'accès du réseau IP semblent résider sur un nœud portant ce nom de CP.

Utilisez le fichier de données inverse du serveur de noms de domaine ou le fichier HOSTS afin de définir le nom de CP et le nom de réseau connexion pour un réseau IP donné. Mappez l'adresse IP 127.0.0.3 au nom de CP, puis l'adresse IP 127.0.0.4 au nom de réseau de connexion.

L'exemple suivant présente des entrées du fichier de données inverse. Pour un réseau IP dont l'ID réseau SNA est RESA, le nom de CP MONNOMCP et le nom de réseau de connexion MONRES, définissez les entrées suivantes :

```
127.□.□.3       RESA.MONNOMCP.
127.□.□.4       RESA.MONRES.
```

Remarques :

1. Un point est requis à la fin du nom uniquement si la définition se trouve dans le fichier de données inverse DNS. Aucun point n'est utilisé dans les définitions de fichier HOSTS.
2. N'entrez pas le suffixe de nom de domaine SNA.

La fonction AnyNet SNA sur TCP/IP de Communications Server fournit un nom de CP par défaut ($ANYNET.$GWCP) et un nom de réseau de connexion par défaut ($ANYNET.$GWCNET). Dans les configurations comportant un seul réseau IP, vous pouvez utiliser la valeur par défaut en ne définissant pas de nom de CP ou de nom de réseau de connexion. Dans les configurations dont plusieurs passerelles connectent plusieurs réseaux IP, un seul réseau IP peut utiliser la valeur par défaut. Cependant, vous devez définir un nom de CP et un nom de réseau de connexion uniques pour tous les autres réseaux IP.

La figure 21, à la page 81 explique comment définir le nom de CP et le nom de réseau de connexion pour une configuration dotée de deux réseaux IP.

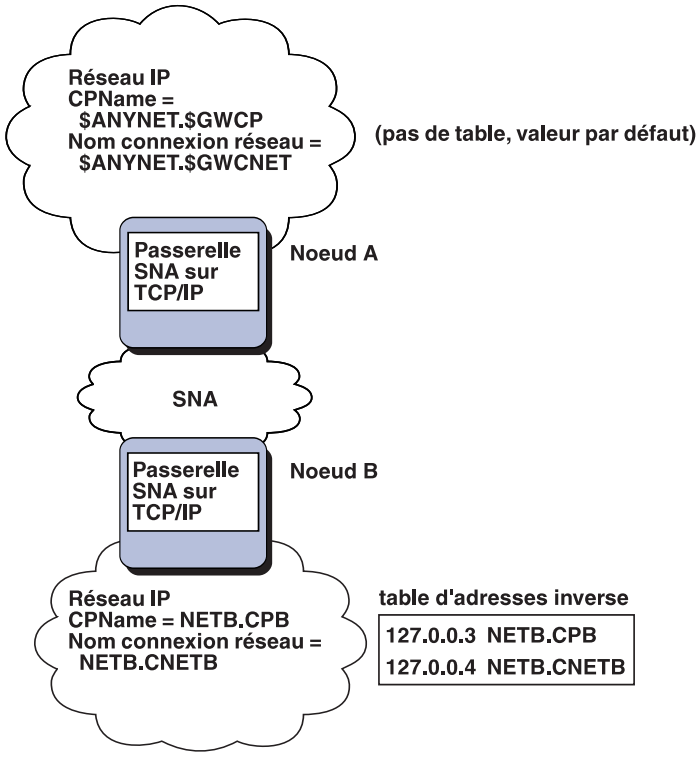


Figure 21. Définition d'un nom de CP et d'un nom de réseau de connexion

Réduction des définitions de serveur de noms de domaine à l'aide de noms génériques

Si vous utilisez la passerelle SNA sur TCP/IP et que votre configuration remplit les conditions de dénomination restrictives suivantes, vous pouvez réduire le nombre des entrées de serveur de noms de domaine en définissant une entrée de nom de domaine pour chaque ID réseau SNA accessible via une ou plusieurs passerelles SNA sur TCP/IP.

- Chaque réseau SNA doit comporter un ID réseau SNA unique parmi tous les réseaux SNA.
- Chaque réseau IP doit comporter un ID réseau SNA unique parmi tous les réseaux IP.
- Un réseau SNA et un réseau IP peuvent comporter le même ID réseau SNA.

En codifiant une seule entrée de nom de domaine pour chaque ID réseau SNA, vous n'avez pas à définir une entrée de nom de domaine pour chaque LU du réseau SNA avec laquelle vous souhaitez communiquer via le réseau IP. Vous pouvez utiliser un nom générique (*) pour indiquer le nom de toutes les LU comportant le même ID réseau SNA. Le remplacement du *nom de LU* par un nom générique vous permet de définir une seule entrée de serveur de noms de domaine qui représente toutes les LU de ce réseau particulier.

Remarque : Si le nom générique est utilisé, celui-ci doit être entré en intégralité. Les noms génériques partiels tels que LUA* ne sont pas admis.

Le nom générique est mappé à l'adresse IP de la première passerelle SNA sur TCP/IP servant à accéder au réseau à l'aide de cet ID réseau SNA. Comme l'indique la figure 22, les unités logiques SNAAPPL1, APPC1, APPC2 et LU5 résident dans le réseau NETB et ne sont accessibles qu'à partir du réseau IP via une passerelle SNA sur TCP/IP dont l'adresse IP est IPgwg. Si le suffixe de nom de domaine SNA est SNA.IBM.COM, l'entrée suivante doit être définie dans le serveur de noms de domaine :

```
▫.NETB.SNA.IBM.COM        IPgwg
```

Cette entrée est utilisée pour toutes les quatre unités logiques.

Remarque : Vous avez la possibilité de définir chaque unité logique séparément.

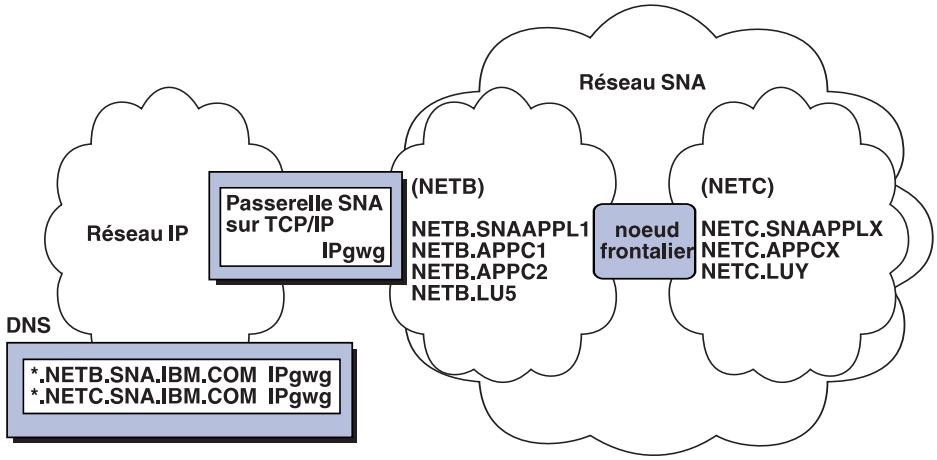


Figure 22. Définitions du serveur de noms de domaine pour une seule passerelle connectée à un réseau SNA comportant deux ID réseau

Chaque réseau SNA doit comporter une entrée unique. Comme l'indique la figure 22, si le réseau NETC contient également SNAAPPLX, APPCX et LUY qui ne sont accessibles que via la passerelle SNA sur TCP/IP dont l'adresse IP est IPgwg, les entrées du serveur de noms de domaine sont les suivantes :

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

En plus, chaque passerelle doit comporter une entrée unique. Si une passerelle SNA sur TCP/IP parallèle dont l'adresse IP est IPgwh (voir la figure 23, à la page 83 est ajoutée à l'exemple précédent, les entrées du serveur de noms domaine sont les suivantes :

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

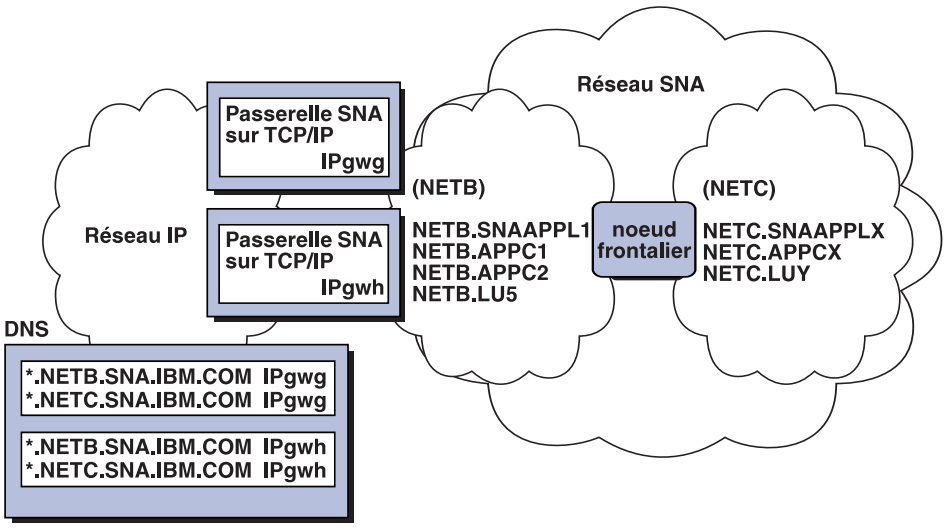


Figure 23. Définitions du serveur de noms de domaine pour les passerelles parallèles connectées à un réseau SNA comportant deux ID réseau

Remarques relatives sur la fonction de nœud d'accès SNA sur TCP/IP

La présente section décrit uniquement les nœuds d'accès et non les passerelles.

Mode de routage des sessions SNA via AnyNet SNA sur TCP/IP

Lorsqu'une application SNA active une session, Communications Server doit déterminer en premier le mode de transport à utiliser : SNA, IP ou une combinaison des deux.

Pour configurer le transport de votre choix, paramétrez la préférence de routage. Cette dernière peut être définie pour l'ensemble du nœud à l'aide de la préférence de routage par défaut sur le périphérique AnyNet sur TCP/IP, ou pour chaque LU lors de la définition des LU partenaire.

La table de préférences de routage n'est utilisée que pour les nouvelles sessions. Les sessions déjà existantes utilisent le même transport ; elles ne sont pas arrêtées ou réacheminées si la table de préférences de routage est modifiée.

Remarque : La préférence de routage relative à un nœud régit les sessions qui sont activées à partir de ce nœud (sessions de nœud d'accès). Les sessions qui traversent un nœud ne sont pas affectées par la préférence de routage.

Vous pouvez définir ou modifier la préférence de routage par défaut en affectant une des valeurs suivantes :

Natif d'abord Les requêtes sont acheminées via SNA. Si aucun chemin SNA n'est disponible, les requêtes sont acheminées via TCP/IP.

Non natif d'abord Les requêtes sont acheminées via TCP/IP. Si aucun chemin TCP/IP n'est disponible, les requêtes sont acheminées via SNA.

Natif uniquement Les requêtes sont acheminées uniquement via SNA. Si aucun chemin SNA n'est disponible, la connexion échoue.

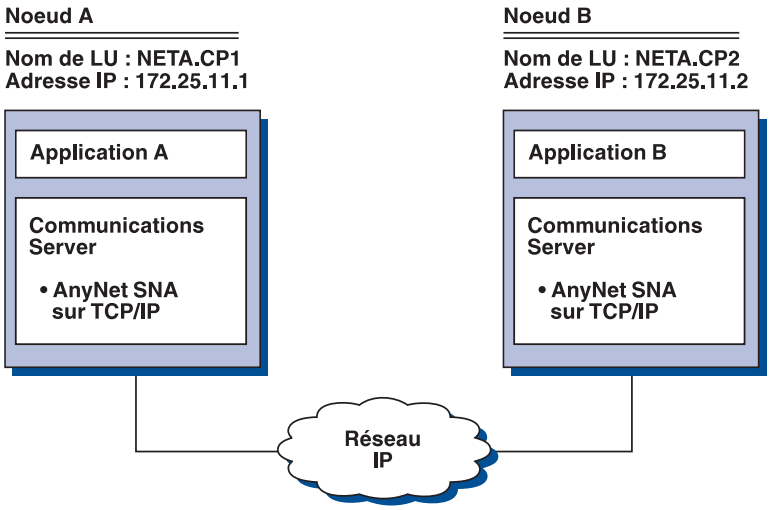
Non natif uniquement Les requêtes sont acheminées uniquement via TCP/IP. Si aucun chemin TCP/IP n'est disponible, la connexion échoue.

Exemples de configuration d'AnyNet SNA sur TCP/IP

La présente section contient des exemples d'activation de communications SNA sur IP par AnyNet. Les instructions de configuration suivantes ne sont complètes que pour le systèmes d'exploitation Windows NT. Dans tous les exemples, le suffixe de nom de domaine est SNA.IBM.COM.

Pour plus de détails sur la configuration d'AnyNet pour les autres plates-formes mentionnées dans la présente section (par exemple, VTAM ou AS/400), consultez la documentation de produit appropriée.

Exemple 1. Exécution des applications APPC ou CPI-C sur un réseau TCP/IP



Étapes

Suivez les étapes ci-après pour établir des communications entre les deux nœuds Windows NT. Il est à noter que, dans cet exemple, les noms de CP sont utilisés comme noms de LU.

Pour le nœud A, procédez comme suit :

1. Ajoutez l'entrée suivante dans le fichier HOSTS local :

   ```
   172.25.11.2  CP2.RESA.SNA.IBM.COM
   ```

2. Utilisez **RESA.CP1** comme nom de point de contrôle lors de la configuration des nœuds. Assurez-vous que la préférence de routage est définie de manière à acheminer les sessions sur TCP/IP. Pour plus de détails, consultez les panneaux d'aide de l'utilitaire **Configuration du nœud**.

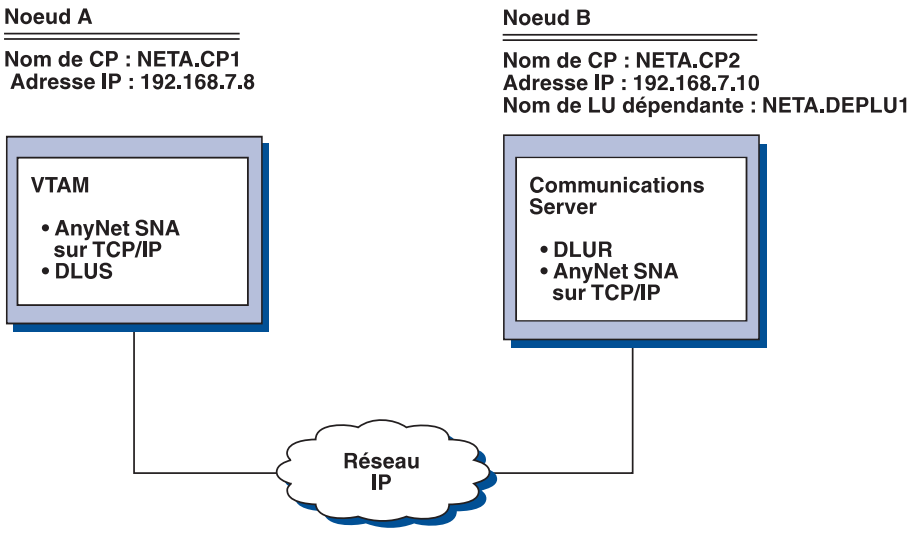
Pour le nœud B, procédez comme suit :

1. Ajoutez l'entrée suivante dans le fichier HOSTS local :

   ```
   172.25.11.1  CP1.RESA.SNA.IBM.COM
   ```

2. Utilisez **RESA.CP2** comme nom de point de contrôle lors de la configuration des nœuds. Assurez-vous que la préférence de routage est définie de manière à acheminer les sessions sur TCP/IP. Pour plus de détails, consultez les panneaux d'aide de l'utilitaire **Configuration du nœud**.

Exemple 2. Émulation 3270 via DLUR sur un réseau TCP/IP



Étapes

Suivez les étapes ci-après pour établir des communications entre le nœud A et le nœud B.

Pour le nœud B, procédez comme suit :

1. Ajoutez l'entrée suivante dans le fichier HOSTS local :

```
192.168.7.8    CP1.RESA.SNA.IBM.COM
```

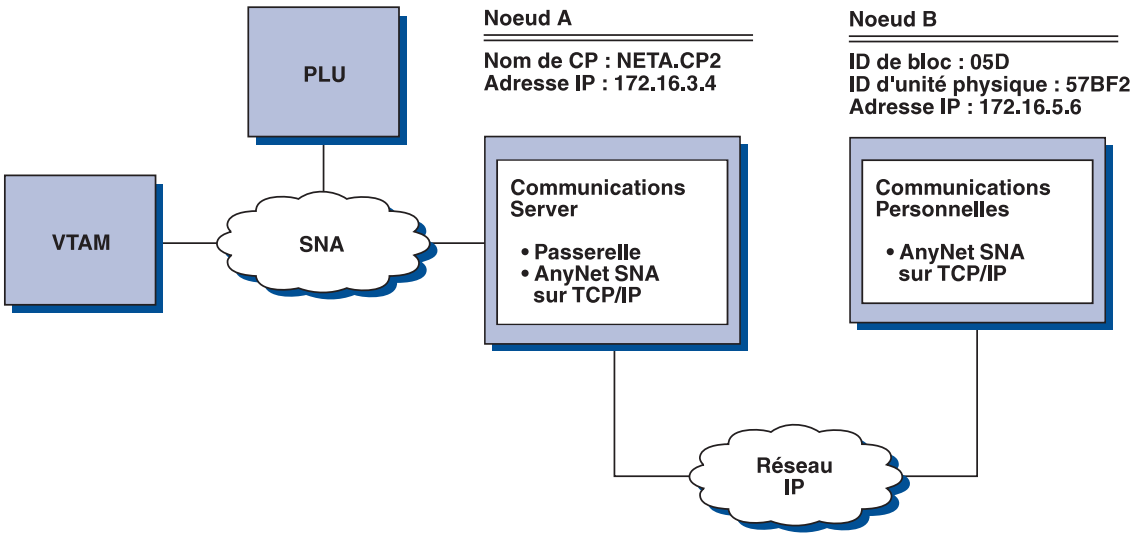
2. Utilisez **RESA.CP2** comme nom de point de contrôle lors de la configuration des nœuds, puis **RESA.CP1** comme nom de DLUS lors de la configuration des PU DLUR. Assurez-vous que la préférence de routage est définie de manière à acheminer les sessions sur TCP/IP. Pour plus de détails, consultez les panneaux d'aide de l'utilitaire **Configuration du nœud**.

Pour le nœud A, ajoutez les entrées suivantes dans le fichier HOSTS :

```
192.168.7.1□    CP2.RESA.SNA.IBM.COM
192.168.7.1□    DEPLU1.RESA.SNA.IBM.COM
```

Il est à noter que MVS AnyNet SNA sur TCP/IP requiert actuellement DLUS/DLUR pour les communications des LU dépendantes.

Exemple 3. Utilisation d'une passerelle SNA pour l'activation de l'émulation 3270 entre les réseaux SNA et TCP/IP



Étapes

Suivez les étapes ci-après pour établir des communications entre le nœud B et l'hôte VTAM.

Pour le nœud A, procédez comme suit :

1. Ajoutez l'entrée suivante dans le fichier HOSTS local :

   ```
   172.16.5.6 ▫5D57BF2.SNA.IBM.COM
   ```

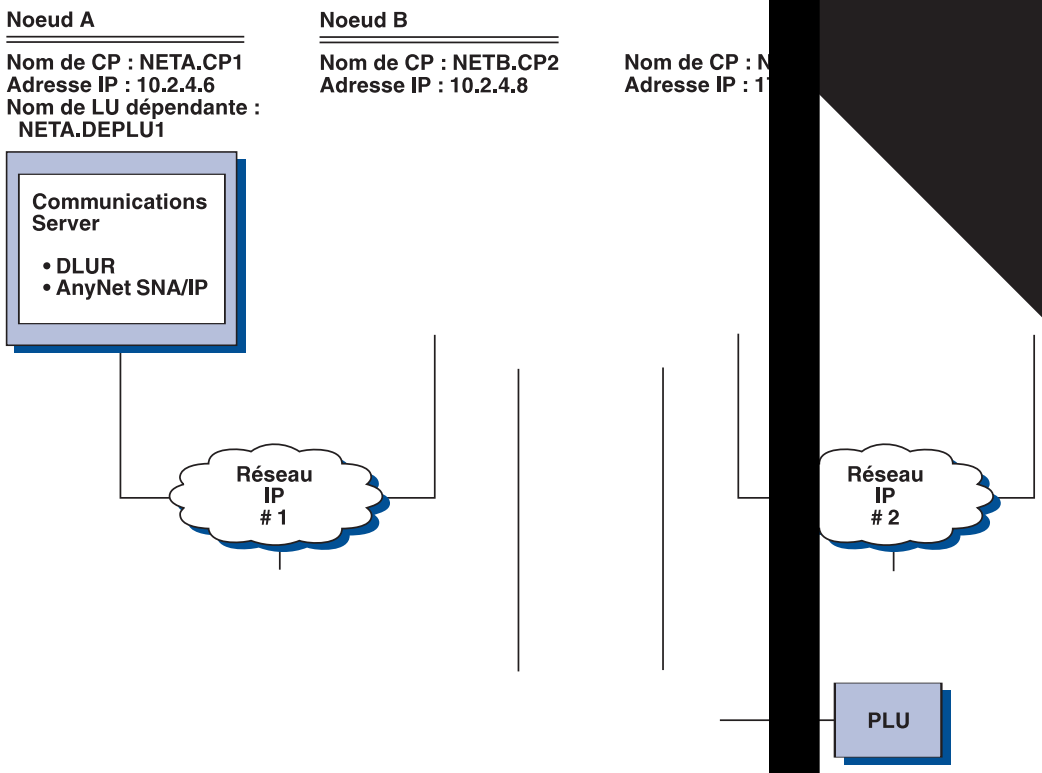
2. Indiquez **RESA.CP2** comme nom de point de contrôle lors de la configuration du nœud, puis utilisez le périphérique ANYNET pour affecter des modèles implicites lors de la définition des clients. Pour plus de détails, consultez les panneaux d'aide de l'utilitaire **Configuration du nœud**.

Pour le nœud B, ajoutez l'entrée suivante dans le fichier HOSTS local :

```
172.16.3.4  CP2.RESA.SNA.IBM.COM
```


Communications
Server
• Passerelle
• DLUR
• AnyNet SNA
sur TCP/IP

Exemple 5. Émulation 3270 à partir de deux
NT sur des réseaux IP différent



2. Utilisez **RESA.CP1** comme nom de point de contrôle lors de la configuration des nœuds, puis **NETB.CP5** comme nom de DLUS lors de la configuration des PU DLUR. Assurez-vous que la préférence de routage de NETB.CP5 a pour valeur Non natif. Pour plus de détails, consultez les panneaux d'aide de l'utilitaire **Configuration du nœud**.

Pour le nœud B, ajoutez les entrées suivantes dans le fichier HOSTS :

```
1□.2.4.6     CP1.RESA.SNA.IBM.COM
127.□.□.2    DEPLU1.RESA.SNA.IBM.COM
1□.2.4.6     DEPLU1.RESA.SNA.IBM.COM
127.□.□.4    IPNET1.GWCNET
127.□.□.3    IPNET1.CP1
```

Pour le nœud C, ajoutez les entrées suivantes dans le fichier HOSTS :

```
172.2□.1.2   CP4.NETC.SNA.IBM.COM
127.□.□.2    DEPLU2.NETC.SNA.IBM.COM
172.2□.1.2   DEPLU2.NETC.SNA.IBM.COM
127.□.□.4    IPNET2.GWCNET
127.□.□.3    IPNET2.CP2
```

Pour le nœud D, procédez comme suit :

1. Ajoutez l'entrée suivante dans le fichier HOSTS local :

```
172.2□.1.1   CP5.NETB.SNA.IBM.COM
127.□.□.4    IPNET2.GWCNET
127.□.□.3    IPNET2.CP2
```

2. Utilisez **NETC.CP4** comme nom de point de contrôle lors de la configuration des nœuds, puis **NETB.CP5** comme nom de DLUS lors de la configuration des PU DLUR. Assurez-vous que la préférence de routage de NETB.CP5 a pour valeur Non natif. Pour plus de détails, consultez les panneaux d'aide de l'utilitaire **Configuration du nœud**.

Conseils utiles

La présente section contient des conseils utiles sur les mises au point, sur la connectivité TCP/IP via SLIP ou PPP et sur les adresses IP dynamiques.

Mise au point

Si vous pouvez accéder à une LU via plusieurs passerelles SNA sur TCP/IP et que vous avez mappé ce nom de LU à plusieurs adresses IP, augmentez les paramètres **CONN_RETRY_SECS** et **CONNWAIT_SECS** du mot clé **ANYNET_COMMOM_PARAMETERS** lors de la configuration des paramètres de base d'AnyNet. Ainsi, des tentatives de connexions TCP à toutes les cartes et passerelles possibles sont assurées. Une connexion TCP à une adresse IP inactive peut échouer dans un délai maximal de 90 secondes.

Adresses IP dynamiques

En général, AnyNet SNA sur TCP/IP est fonction des ressources SNA (par exemple, noms de LU, noms de CP ou idblk/num) qui sont en cours de mappage statique à des adresses IP. Cependant, en fonction de votre configuration et du mode d'activation des connexions, vous pouvez utilisez AnyNet SNA sur TCP/IP dans les environnements où les adresses IP sont affectées de façon dynamique (par exemple, DHCP).

Applications APPC ou CPIC : Il se peut qu'un nœud d'accès SNA sur TCP/IP dont l'adresse IP est affectée de façon dynamique établisse systématiquement des sessions avec un autre nœud d'accès ou une autre passerelle SNA sur TCP/IP comportant une adresse IP statique.

Un nœud d'accès ou une passerelle SNA sur TCP/IP comportant une adresse IP statique (nœud A) ne peut établir une session avec un partenaire comportant une adresse IP dynamique (nœud B) que de la manière suivante :

1. Le nœud B a établi en premier une session avec ou via le nœud A.
2. La session établie à l'étape 1 est toujours active.

Applications de LU dépendantes

Remarque : Les informations de la présente section s'appliquent aux applications LU 0, 1, 2, 3 ou 6.2 dépendante.

Les nœuds d'accès SNA sur TCP/IP dont les adresses IP sont affectées de manière dynamique peuvent prendre en charge les communications des LU dépendantes si les critères suivants sont remplis :

- Les LU dépendantes communiquent à travers une passerelle SNA via :
  - Communications Server/2 4.1, l'APAR JR10461 étant appliquée ;
  - Communications Server/2 V5 ; ou
  - Communications Server pour Windows NT 5.01 ou version ultérieure.
- Le nœud d'accès SNA sur TCP/IP dont l'adresse IP est affectée de manière dynamique active des connexions à une passerelle SNA comportant une adresse IP statique.

Les communications de LU dépendantes via DLUS/DLUR sur AnyNet SNA sur TCP/IP ne sont pas prises en charge si l'adresse IP du nœud DLUR est affectée de façon dynamique.

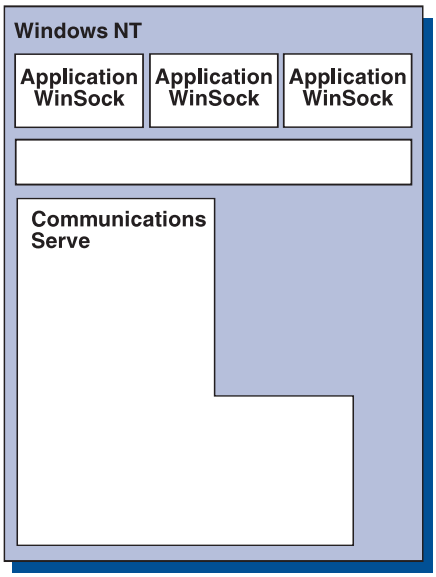
Configuration d'AnyNet Sockets sur SNA

La présente section explique comment configurer Sockets sur SNA.

La fonction de nœud d'accès Sockets sur SNA de Communications Server permet aux applications conformes à WinSock de communiquer sur des réseaux SNA. La fonction de passerelle Sockets sur SNA permet à des applications sockets des réseaux SNA et IP de communiquer.

Fonctionnement de Sockets sur SNA

La figure 24, à la page 91, présente la structure d'un nœud Windows NT qui exécute Sockets sur SNA, et illustre le mode de fonctionnement des programmes d'application socket et de Sockets sur SNA sur un nœud Windows NT.



WinSock est une API qui permet l'exécution des applications socket dans un envi-

Génération d'un appel LU 6.2 à partir d'un appel Socket

Pour permettre le routage des informations au format TCP/IP via SNA, Sockets sur

Mappage d'une adresse IP à un nom qualifié par le réseau SNA

Lorsqu'un programme d'application fait appel à Sockets sur SNA pour communiquer avec un autre programme d'application, il fournit l'adresse IP du nœud de destination. Sockets sur SNA doit mapper l'adresse IP à une adresse SNA afin d'émettre un appel LU 6.2 approprié. À chaque adresse IP identifiant un nœud correspond un nom qualifié par le réseau SNA.

La section «Présentation du routage et du mappage», à la page 93 explique la procédure de mappage d'adresses et fournit les directives et exigences relatives à la configuration du mappage d'adresses IP-LU.

Routage et mappage de données sur les réseaux SNA et IP

Les passerelles Sockets sur SNA permettent une communication entre les programmes d'application socket des réseaux IP et SNA grâce à l'association de la fonction de routage de TCP/IP aux fonctions de conversion de protocole et de mappage d'adresse de Sockets sur SNA.

Les fonctions de conversion de protocole et de mappage d'adresse sont requises lors de l'acheminement des données entre les nœuds qui utilisent des protocoles de transport différents. La passerelle Sockets sur SNA effectue automatiquement la conversion de protocole après avoir déterminé le type de transport associé à l'adresse IP de destination. Un récapitulatif du processus de routage et de mappage figure dans la section «Mode de routage et de mappage de données par la passerelle Sockets sur SNA», à la page 95.

Support de programme d'application fourni par Sockets sur SNA

Sockets sur SNA prend en charge les applications WinSock 1.1 et WinSock 2.0 (Windows NT 4.0 uniquement) qui utilisent les sockets AF_INET.

Sockets sur SNA ne prend pas en charge les applications qui utilisent la diffusion.

Si vous envisagez d'utiliser la passerelle Sockets sur SNA pour acheminer des informations à destination et en provenance d'un nœud MVS/ESA configuré à l'aide de la fonction Sockets sur SNA de VTAM version 3, édition 4.2, vous devez au préalable installer la fonction `d'acheminement` sur le nœud MVS/ESA. Pour ce faire, installez la PTF (modification provisoire du logiciel) UW03567. Vous pouvez vous procurer des PTF auprès de l'une des sources suivantes :

- Information Access
- SoftwareXcel Extended
- IBMLink (ServiceLink)

Si vous n'avez pas accès à ces sources, prenez contact avec le centre de support IBM.

Planification de Sockets sur SNA

La présente section décrit les aspects à prendre en considération par le planificateur de réseau avant la configuration d'un réseau avec Sockets sur SNA.

Présentation du routage et du mappage

La présente section décrit les concepts de base de l'adressage Internet et explique la relation entre ces concepts et les fonctions de routage et de mappage. Voici les informations incluses dans cette section :

Adressage Internet

Au moins une adresse IP unique servant à acheminer des données via le réseau est affectée à chaque hôte.

Remarque : Dans la série de protocoles IP, le terme ***hôte*** désigne un système terminal et peut correspondre à n'importe quel poste de travail ; il ne doit pas nécessairement s'agir d'un ordinateur central.

L'adresse IP affectée à l'hôte ne définit pas ce dernier sur le réseau ; elle permet à un réseau d'identifier l'interface de réseau de cet hôte. Par exemple, l'adresse de l'interface de réseau SNA permet au réseau SNA d'identifier la connexion d'un nœud.

Un hôte passerelle comporte une adresse IP unique pour chaque interface de réseau. Dans la mesure où la passerelle Sockets sur SNA achemine des données SNA et TCP/IP, des adresses IP uniques doivent être configurées pour les interfaces TCP/IP et SNA.

La section suivante décrit le format d'adresse IP, les classes d'adresse et les masques de réseau. Pour plus de détails, consultez la documentation TCP/IP.

Format et classes d'adresses IP : Une adresse IP est constituée de deux zones d'adresses 32 bits :

- La première partie contient l'adresse du réseau et la deuxième l'adresse de l'hôte.
- Le nombre de bits utilisés pour les zones réseau et hôte d'une adresse IP varie en fonction de la classe de l'adresse IP.
- Un masque de réseau permet d'utiliser une partie de la zones hôte de l'adresse IP sous forme d'adresse de sous-réseau.

Les masques de réseau par défaut sont présentés dans le tableau 5.

Tableau 5. Masques d'adresse IP pris en charge par Sockets sur SNA

Pour une adresse IP en notation décimale au format *a.b.c.d*, la plage des valeurs de *a* est la suivante :	**Masque de réseau par défaut**
1 à 127	255.0.0.0
128 à 191	255.255.0.0
192 à 223	255.255.255.0

Masques utilisés par Sockets sur SNA : Sockets sur SNA utilise les deux types de masques suivants :

- **Masque de sous-réseau**

  Le masque de sous-réseau est utilisé dans le cadre du routage et indiqué lors de la configuration du nœud local et des chemins. Vous pouvez accepter le masque de sous-réseau par défaut ou indiquer une autre valeur pour définir des adresses de sous-réseau.

- **Masque d'adresse**

  Le masque d'adresse est utilisé pour le mappage d'adresses IP-LU généré ; il est indiqué lors de la configuration.

Table de routage IP

Chaque hôte est doté d'une table de routage IP qui stocke des informations relatives aux destinations possibles et au mode d'accès à celles-ci. Des entrées de chemin sont ajoutées lorsque :

- l'adresse IP locale est définie. Pour plus de détails, consultez l'aide en ligne ;
- des instructions d'acheminement sont définies à partir de la fenêtre **Configuration du nœud**. Cliquez sur **AnyNet Sockets**, puis sur **Chemins**. Pour plus de détails, consultez l'aide en ligne ;
- un chemin comportant moins de segments est trouvé. Ce cas se produit lorsque la passerelle Sockets sur SNA reçoit un message RIP ou de réacheminement ICMP. Pour plus de détails, reportez-vous à la section «Fonction de découverte de chemin», à la page 96.

Un exemple de table de routage est présenté dans la figure 25, à la page 95.

ID réseau SNA utilisés par Sockets sur SNA

À chaque chemin défini via l'interface SNA (sna0) doit correspondre un ID réseau SNA auquel l'adresse de réseau IP est mappée. Le nombre d'ID réseau SNA défini est fonction de la façon dont vous souhaitez mapper le réseau IP au réseau SNA.

Par exemple, si les applications socket utilisant SNA sont configurées pour faire appel aux sous-réseaux IP 9.67.0.0 et 9.77.0.0, vous pouvez définir un ID réseau SNA qui correspond à chaque sous-réseau IP, ou un seul ID réseau correspondant aux deux sous-réseaux. Sockets sur SNA ne requiert pas un mappage bi-univoque unique entre une adresse de réseau IP et un ID réseau SNA.

Mode de mappage d'une adresse IP à un nom de LU

Vous pouvez utiliser le mappage explicite ou généré pour mapper les adresses IP aux noms LU SNA :

- Le mappage explicite consiste à définir tous les noms de LU et à associer chaque adresse IP de l'hôte à un nom de LU SNA spécifique, au moment de la configuration.
- Avec le mappage généré, les noms de LU sont automatiquement créés pour vous. Au moment de la configuration, vous indiquez une adresse IP de réseau, un masque d'adresse, un ID réseau et une valeur de modèle de LU.

  Sockets sur SNA utilise le masque d'adresse pour associer la partie réseau de l'adresse IP à l'ID réseau SNA, et la partie hôte au nom de la LU SNA.

La valeur du modèle de LU sert à déterminer le nombre de caractères utilisés dans le nom de la LU, et leur position.

Vous pouvez afficher le nom de LU généré pour une adresse IP données, à l'aide de l'utilitaire **sxmap** de la ligne de commande. Voici la syntaxe de cet utilitaire :

```
sxmap convert <adresse IP> <masque d'adresse> <modèle de LU>
```

Mode de routage et de mappage de données par la passerelle Sockets sur SNA

Les étapes suivantes expliquent brièvement comment la passerelle Sockets sur SNA détermine si les données doivent être acheminées via SNA ou via TCP/IP, et décrivent le mode de traitement du mappage d'adresse :

1. Sockets sur SNA recherche dans sa table de routage un chemin permettant aux données d'accéder à l'adresse IP de destination. Si Sockets sur SNA ne trouve pas de chemins concordants, la demande de connexion est transmise à la pile TCP/IP native.
2. Dans le cas contraire, l'entrée de chemin indique le mode d'accès à la destination :
   a. Si l'adresse du routeur correspond à celle d'une interface de réseau local, par exemple, sna0, l'adresse du réseau de destination, du sous-réseau ou de l'hôte est directement accessible.
   b. Si l'adresse du routeur correspond à celle d'une passerelle ou d'un routeur, la destination n'est accessible que via la passerelle ou le routeur intermédiaire.

   La figure 25 illustre un exemple de table de routage IP.

```
Adresse IP de destination Masque de destination Adresse IP de passerelle  Nbre d'utilisations
-------------------------------------------------------------------------------
1.2.3.4                   255.255.255.255     199.245.253.1        1▫
1▫.▫.▫.▫                  255.▫.▫.▫           199.245.253.2        ▫
1▫.11.▫.▫                 255.255.▫.▫         199.245.253.113      37
127.▫.▫.1                 255.255.255.255     127.▫.▫.1            8
128.1.▫.▫                 255.255.▫.▫         199.245.253.3        ▫
199.245.253.▫             255.255.255.▫       199.245.253.113      368
```

Figure 25. Exemple de table de routage IP

3. Si aucun chemin n'est trouvé dans la table de routage de Sockets sur SNA, ce dernier considère que la destination TCP/IP est accessible via un réseau IP natif. Pour plus de détails sur le mode de routage de données par TCP/IP, consultez la documentation TCP/IP.
4. Si le chemin choisi indique que le transfert de données doit se faire via l'interface SNA (sna0), Sockets sur SNA recherche l'adresse du prochain segment dans la table de mappage IP-LU :
   a. Si Sockets sur SNA trouve une entrée concordante, une connexion LU 6.2 est établie.
   b. Sinon, la tentative de connexion échoue.
   c. Sockets sur SNA transmet les données et l'adresse de destination à Communications Server.

5. Tous les chemins définis pour Sockets sur SNA sont dupliqués dans la pile TCP/IP native afin de permettre l'acheminement de paquets IP via SNA.

Fonction de découverte de chemin : Cette fonction fournie par la passerelle Sockets sur SNA permet un acheminement plus efficace du trafic TCP/IP et la réduction du nombre des instructions de chemin explicitement définies de votre réseau. Il n'est pas nécessaire de sélectionner ou de configurer cette fonction.

Un des problèmes rencontrés au niveau des grands réseaux correspond à la façon dont l'ajout de nouveaux réseaux ou sous-réseaux doit être détecté, et au type de routeur à utiliser pour accéder à ces nouveaux réseaux ou sous-réseaux. Sockets sur SNA résout ce problème en demandant à tous les nœuds d'utiliser au début un routeur par défaut qui notifie aux autres nœuds le moment de détection d'un chemin plus direct. Cela est plus efficace que la solution TCP/IP type qui consiste à diffuser des informations de routage.

Remarque : Pour utiliser efficacement cette fonction, vous devez utiliser le mappage algorithmique des adresses IP aux noms de LU, ainsi qu'un réseau fédérateur APPN. Sinon, les nœuds doivent définir de manière explicite des noms de LU et des adresses IP pour tous les nœuds éloignés avec lesquels ils communiquent.

La figure 26, illustre un exemple de configuration.

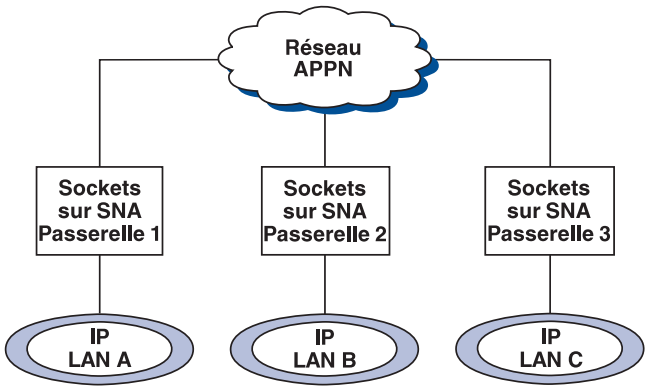


Figure 26. Exemple de réseau utilisant la fonction de découverte de Sockets sur SNA

Dans cet exemple :

- Les passerelles 1, 2 et 3 correspondent à des passerelles Sockets sur SNA connectées à des réseaux locaux IP. Ces passerelles permettent la connexion des réseaux locaux IP à un réseau fédérateur APPN.
- La passerelle 1 est la seule dans laquelle une table de routage complète et permanente est maintenue.

  Les passerelles 2 et 3 définissent la passerelle 1 en tant que leur routeur par défaut. Si un réseau ou un sous-réseau éloigné est identifié par la passerelle 1, il n'est pas nécessaire que les passerelles 2 et 3 définissent ces chemins de façon explicite.
- Lorsque les passerelles 2 et 3 acheminent des données vers des réseaux ou des sous-réseaux non définis, ces requêtes sont envoyées à leur routeur par défaut, la passerelle 1.

Si le réseau ou le sous-réseau est identifié par la passerelle 1 et qu'un chemin plus direct est disponible, la passerelle 1 renvoie un message de réacheminement ICMP au demandeur en indiquant le chemin à utiliser dans l'avenir. Ce message permet la mise à jour de la table de routage du demandeur. Par conséquent, les passerelles 2 et 3 créent leurs tables de routage de façon dynamique pour les réseaux ou sous-réseaux éloignés, selon la demande.

- Si de nouvelles passerelles sont ajoutées, la table de routage permanente de la passerelle 1 doit être mise à jour. Aucune instruction de chemin explicite n'est requise pour les passerelles 2 et 3.

Définition des modes de Sockets sur SNA

Sockets sur SNA utilise des conversations LU 6.2 pour permettre une communication entre les programmes d'application socket. Lorsqu'une conversation LU 6.2 est établie, Sockets sur SNA définit le mode et les caractéristiques de session associées de la connexion. Communications Server utilise le nom de mode pour identifier les caractéristiques de la connexion entre les deux nœuds Sockets sur SNA.

Le mode Sockets sur SNA par défaut est BLANK. Vous pouvez utiliser ce ce dernier ou définir votre propre mode. Pour modifier le mode Sockets sur SNA par défaut, cliquez, dans la fenêtre **Configuration du nœud**, sur **AnyNet Sockets sur SNA**, puis sur **Modes**. Vous pouvez définir un autre mode par défaut pour l'ensemble du trafic TCP/IP et affecter un mode particulier à un port TCP/IP spécifique.

Si vous indiquez un autre mode qui n'est pas défini par Communications Server, vous devez définir pour Communications Server les caractéristiques de session associées à ce mode.

Modification du délai d'inactivité

L'option de démarrage du délai d'inactivité permet de contrôler le délai, en secondes, pendant lequel une conversation de datagramme reste inactive avant qu'elle ne soit désallouée par Sockets sur SNA. Ce délai permet de choisir d'utiliser les ressources système pour maintenir la conversation de datagramme existante ou d'attendre plus longtemps une nouvelle conversation de datagramme. Par exemple, si vous définissez une valeur faible, les conversations de datagramme inutilisées sont plus rapidement arrêtées, mais la transmission d'un nouveau datagramme est plus longue. Le délai d'inactivité par défaut est de 90 secondes.

Pour modifier l'option de démarrage, cliquez, dans la fenêtre **Configuration du nœud**, sur **AnyNet Sockets sur SNA**, puis sur **Visualiser/Modifier/Ajouter** ; cliquez ensuite sur l'onglet **Avancés**, puis sélectionnez une nouvelle valeur pour cette option.

Planification des communications client/serveur

Le présent chapitre décrit la planification des clients API SNA de Communications Server et de Novell IntranetWare pour SAA.

Clients API SNA

La présente section contient des informations spécifiques aux clients API SNA.

Installation et configuration

Pour plus de détails sur l'installation et la configuration des clients API SNA de Communications Server, consultez *Guide d'utilisation*.

Protocole LDAP

Le protocole LDAP (Lightweight Directory Access Protocol) permet d'accéder aux services de répertoire. Il permet de lire, de rechercher, d'ajouter et de supprimer des informations dans des bases de données centralisées ou réparties. Il est similaire à l'ancien protocole DAP (X.500 Directory Access Protocol) mais il est moins surchargé en données (par exemple, les couches OSI de présentation et de session ont, par exemple, été supprimées). Vous pouvez utiliser le panneau **Configuration du client LDAP** pour configurer les informations du client d'API SNA et les conserver sur un serveur LDAP.

Le panneau **Configuration du client LDAP** présente l'organisation logique et les relations existant entre les clients et leurs configurations.

Pour plus de détails sur l'utilisation de ces sections principales, consultez les panneaux d'aide de **Configuration du client LDAP**.

Arborescence des informations de répertoire

L'arborescence des informations de répertoire (DIT) connecte l'ensemble des agents de services de répertoire (DSA) d'un modèle prédéfini. Un modèle est une structure hiérarchique extensible comprenant un certain nombre d'objets de base. Une arborescence d'informations de répertoire LDAP est composée d'une racine sous laquelle les ***pays*** (c) sont définis. Sous ces pays se trouvent généralement des ***organisations*** (o), et sous ces dernières des ***individus*** ((cn) ou (uid)) ou des ***unités organisationnelles*** (ou). Par exemple, une entrée LDAP distinctive se présente de la manière suivante :

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

Hiérarchie client

La hiérarchie client affiche l'arborescence des informations de répertoire LDAP à laquelle vous vous êtres connecté. Vous pouvez ajouter ou supprimer des utilisateurs ou des unités organisationnelles dans la hiérarchie client.

Hiérarchie des configurations

La section Hiérarchie des configurations présente de manière logique la configuration client et l'ensemble des relations existant entre les définitions de la configuration. Elle permet de créer, de modifier ou de supprimer des définitions.

Client API commun pour Communications Server pour Windows NT et IntranetWare pour SAA

Le client livré avec Communications Server permet aux clients de localiser des serveurs IBM Communications Server et IntranetWare for SAA (IWSAA) dans le réseau, et d'y accéder.

Installation des options de localisation des configurations

Lors de l'installation du client, l'utilisateur peut choisir l'une des trois options de localisation de configuration client suivantes :

- Configuration du fichier INI : méthode utilisée avec les versions précédentes de Communications Server ; il s'agit de la méthode par défaut utilisée lors de l'installation du client API SNA inclus dans Communications Server.
- Services de répertoire NetWare (NDS) : méthode utilisée avec les versions précédentes d'IWSAA il s'agit de la méthode par défaut utilisée lors de l'installation du client API SNA inclus dans IntranetWare pour SAA.
- Protocole LDAP (Lightweight Directory Access Protocol)

L'emplacement de la configuration contient des listes de serveurs, des noms utilisateur et toutes les autres informations relatives à la configuration client.

Emplacements de la configuration

Dans la mesure où les informations de configuration sont indépendantes du type de serveur (Communication Server pour Windows NT ou IntranetWare pour SAA), elles peuvent être stockées dans NDS, INI ou LDAP. Par exemple, les noms et adresses de Communication Server peuvent être stockés dans NDS, INI ou LDAP du client API. Dans la mesure où les programmes d'administration NDS ne sont livrés qu'avec IntranetWare pour SAA, la configuration des informations client API SNA dans NDS requiert l'existence du produit IntranetWare pour SAA sur le réseau. Le client API SNA commun permet l'intégration aidée de différents types de serveurs sur le même réseau.

Utilitaire de configuration

Faites appel à l'utilitaire **Définition des options de configuration** pour modifier l'emplacement de la configuration client (INI, NDS ou LDAP) à la suite de l'installation.

Localisation des serveurs

Le client permet à l'utilisateur de localiser des serveurs IBM Communications Server et IWSAA et d'y accéder à l'aide des deux protocoles de transport TCP/IP et SPX.

TCP/IP : La méthode de localisation de serveurs utilisant le protocole de transport TCP/IP est identique. L'administrateur de réseau peut contrôler l'accès aux serveurs via la configuration de serveur. Pour plus de détails, reportez-vous à la section «Planification des secteurs TCP/IP», à la page 148.

SPX : Les méthodes de localisation de serveurs utilisant le protocole de transport SPX sont identiques. Le délai de localisation des deux serveurs IBM Communications Server et IWSAA est supérieur à celui de chaque serveur séparément.

Le client API SNA de Communications Server tente de localiser en les serveurs IBM Communication Server en premier, puis les serveurs IWSAA. Si le serveur IWSAA ne figure pas dans le réseau ou qu'il n'est pas accessible, l'utilisateur peut définir une variable d'environnement empêchant la localisation des serveurs IWSAA. La définition de la variable améliore les performances dans un environnement où seuls les serveurs IBM Communication Server sont accessibles au protocole de transport SPX. Il s'agit de la variable d'environnement **SNA_API_CLIENT_NO_CC**. Celle-ci n'a aucune incidence sur l'emplacement de serveur via le protocole de transport TCP/IP.

Affectation d'une LU locale par défaut

Vous pouvez affecter un alias de LU locale par défaut pour chaque utilisateur, à l'aide de la configuration de fichier INI ou de la configuration LDAP pour les clients API SNA Windows 32 bits.

Les programmes APPC peuvent utiliser un alias de LU locale par défaut au lieu d'en indiquer un directement. Lorsqu'un programme APPC émet une instruction TP_START, la zone d'alias de LU locale contenant des zéros binaires ou uniquement des blancs ASCII, l'API APPC utilise l'alias de LU locale par défaut qui est configuré.

Les programmes EHNAPPC peuvent utiliser un alias de LU locale par défaut au lieu d'en indiquer un directement. Lorsque la zone de LU locale du panneau de configuration AS/400 est laissée en blanc, l'alias de LU locale par défaut configuré est utilisé.

Les programmes CPI-C peuvent utiliser un alias de LU locale par défaut au lieu d'en indiquer un directement. Lorsque la zone d'alias de LU locale de l'enregistrement annexe CPI-C est laissée en blanc et qu'aucune valeur n'a été définie à l'aide de la variable d'environnement APPCLLU, l'API CPI-C utilise l'alias de LU locale par défaut lors de l'activation d'une conversation.

Les programmes démarrés par Attach Manager peuvent utiliser un alias de LU locale par défaut au lieu d'en indiquer un directement. Lorsque la zone d'alias de LU locale de l'enregistrement d'Attach Manager est laissée en blanc, celui-ci utilise l'alias de LU locale par défaut lors du traitement des demandes de conversation entrantes.

Affectation d'une LU partenaire par défaut

Vous pouvez affecter un alias de LU partenaire par défaut pour chaque utilisateur, à l'aide de la configuration de fichier INI ou de la configuration LDAP pour les clients API SNA Windows 32 bits.

Les programmes APPC peuvent utiliser un alias de LU partenaire par défaut au lieu d'en indiquer un directement. Lorsqu'un programme APPC émet une instruction ALLOCATE, la zone de nom de LU partenaire qualifié contenant des zéros binaires ou uniquement des blancs ASCII, l'API APPC utilise l'alias de LU partenaire par défaut qui est configuré.

Les programmes CPI-C peuvent utiliser un alias de LU partenaire par défaut au lieu d'en indiquer un directement. Lorsque la zone d'alias de LU partenaire de l'enregistrement annexe CPI-CI est laissée en blanc, L'API CPI-C utilise l'alias de LU partenaire par défaut lors de l'activation d'une conversation.

Affectation d'un nom de session LUA par défaut

Vous pouvez affecter un alias de LU partenaire par défaut pour chaque utilisateur, à l'aide de la configuration de fichier INI ou de la configuration LDAP pour les clients API SNA Windows 32 bits.

Les programmes LUA tels que les émulateurs 3270 peuvent utiliser un nom de session LUA par défaut au lieu d'en indiquer un directement. Lorsqu'un programme LUA émet une instruction RUI_INIT ou SLI_OPEN, la zone de nom de LU LUA contenant des zéros binaires ou uniquement des blancs ASCII, l'API RUI/SLI utilise le nom de session LUA par défaut qui est configuré.

Chiffrement des données client/serveur

Cette fonction permet au client de demander le chiffrement des données d'application lors des communications entre le client API SNA et Communications Server.

Le chiffrement de données peut être activé, désactivé ou facultatif. Le chiffrement de données facultatif signifie que le chiffrement est utilisé s'il est pris en charge par le serveur.

Sécurité client/serveur

Communications Server permet aux clients API SNA Windows 95 et Windows NT d'utiliser la sécurité de domaine Windows NT pour authentifier la connexion du client au serveur sans que l'ID utilisateur et le mot de passe soient ré-entrés. Le client doit faire partie d'un domaine Windows NT en participant dans un domaine de Communications Server ou à l'aide d'une connexion locale à un ID utilisateur et un ot de passe synchronisés.

Les utilisateurs du client API SNA situés à l'extérieur du domaine Windows NT sont tenus de fournir l'ID utilisateur et le mot de passe par le biais d'une invite ou en stockant de ces valeurs dans le fichier de configuration client.

Les utilisateurs autorisés du serveur client sont maintenus dans le groupe local IBMCSAPI qui est situé directement sur Communications Server ou sur le contrôleur de domaine dans lequel Communications Server participe. Ce groupe d'utilisateurs est créé lors de l'installation et peut être administré à l'aide de l'application Gestionnaire d'utilisateurs Windows NT.

Vous pouvez déterminer si l'ID utilisateur et le mot de passe sont requis aux fins de connexion au serveur, en remplaçant la valeur **LogonControl** définie au niveau du serveur par zéro (0) ; ainsi, le client n'est plus tenu d'indiquer l'ID utilisateur et le mot de passe.

Les enregistrements de trace de contrôle des connexions client au serveur sont consignées dans le journal d'événements de Windows NT. Vous pouvez visualiser ces enregistrements à l'aide de l'afficheur d'événements de Windows NT dans le journal **Application**. Si vous ne souhaitez pas suivre les connexions client au serveur, vous pouvez remplacer la valeur **AuditTrail** au niveau du serveur par zéro (0).

Pour accéder aux entrées **LogonControl** et **AuditTrail**, utilisez l'Editeur du registre de Windows NT sous la clé `HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/IBM SNA Client Services`.

Clients Novell IntranetWare pour SAA

Communications Server prend en charge les clients connectés via IPX ou TCP/IP qui exécutent des progiciels d'émulation mettant en œuvre l'architecture QEL/MU (Queue Element/Message Unit) de Novell pour l'émulation 3270, afin de permettre aux clients d'accéder aux données hôte de l'ordinateur central. Le support des fonctions client courantes y est inclus, notamment les catégories de LU spécifiques, de groupe et publiques (parfois désignées par types de ressources).

Communications Server prend en charge les clients Novell IntranetWare pour SAA sous Windows 95, Windows NT, Windows 3.1 et OS/2.

TCP/IP et/ou IPX/SPX sont requis pour les communications des clients Novell IntranetWare pour SAA avec Communications Server. Si IPX est en cours d'exécution, les logiciels suivants doivent être également activés sur le serveur :

- Gateway Service pour NetWare
- Agent SAP
- NWLink IPX/SPX ou un transport compatible

Si Communications Server est en cours d'exécution sur un contrôleur principal ou secondaire, les utilisateurs doivent disposer de droits d'accès au groupe IBMCSAPI pour se connecter en local au serveur.

Planification de l'accès aux données existantes

Le présent chapitre décrit les fonctions de Communications Server qui permettent d'accéder aux informations de l'hôte.

AS/400 OLE DB Provider

Les applications qui utilisent OLE DB ou ActiveX peuvent communiquer via Communications Server pour l'accès de niveau enregistrement aux fichiers des systèmes AS/400. Pour accéder aux fichiers AS/400, vous devez définir, sous forme de LU partenaire, l'AS/400 éloigné qui contient les fichiers.

L'AS/400 OLE DB Provider peut être installé sous la forme d'un composant de Communications Server ou d'un composant du client API SNA pour Windows 95. Il peut également être installé sous forme de composant du client API SNA pour Windows NT cependant, il requiert Windows NT Workstation ou Server 4.0, ou une version ultérieure. Si le produit Microsoft Data Access Components (MDAC) version 1.5 n'est pas installé, celui-ci sera installé automatiquement par Communications Server lors de l'installation de ce composant.

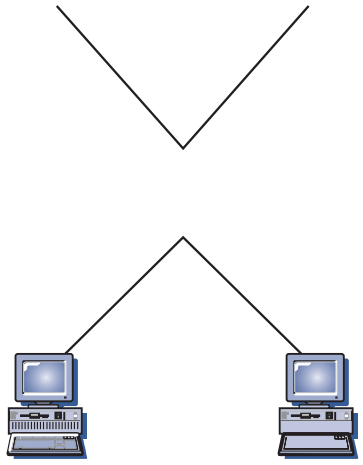
Si l'AS/400 OLE DB Provider est installé sur une machine déjà équipée de Client Access version 3 édition 2 MD (ou antérieure), certaines fonctions de Client Access seront désactivées, notamment le support des programmes ActiveX et OLE DB qui utilisent Client Access pour accéder aux files d'attente de données, aux commandes éloignées, aux appels de programmes répartis, aux procédures stockées et aux instructions SQL du système AS/400.

Pour continuer d'utiliser ces fonctions via Client Access, n'installez pas le composant AS/400 OLE DB Provider lors de l'installation de Communications Server. Sinon, vous pouvez réinstaller Client Access pour récupérer également les fonctions de ce dernier. Cependant, si vous réinstallez Client Access, vous ne pouvez pas utiliser AS/400 OLE DB Provider via Communications Server.

Lorsque Client Access est installé après Communications Server, les informations du registre sont remplacées. Pour utiliser AS/400 OLE DB Provider via Communications Server après l'installation de Client Access, vous pouvez exécuter l'outil REGSVR32.EXE avec les fichiers cwbzzodb.dll et cwbzzidx.dll pour restaurer les informations du registre AS/400 OLE DB Provider.

Vous pouvez utiliser AS/400 OLE DB Provider pour connecter des clients Windows 95 et Windows NT 4.0 via Communications Server à un ou plusieurs systèmes AS/400, selon l'illustration de la figure 27, à la page 106. Cette configuration permet aux clients sur lesquels AS/400 OLE DB Provider est installé d'accéder à des enregistrements spécifiques dans des fichiers de l'AS/400.

Planification de l'accès aux données existantes



Host Publisher

Host Publisher permet d'accéder aux sites Web à grand volume Web ayant un contenu dynamique. Vous pouvez utiliser Host Publisher pour accéder aux données d'hôtes IBM 390 ou AS/400 et pour les publier sur des pages Web créées de façon dynamique à partir de votre modèle.

Host Publisher est constitué de plusieurs composants. Pour plus de détails sur les composants et sur l'installation de Host Publisher, consultez le *Guide d'utilisation* en ligne.

Trois valeurs de registre permettent de contrôler sur la base du registre l'utilisation de tout JIT présent et d'un CLASSPATH spécifique à Host Publisher. Des mises en œuvre de Java potentiellement incompatibles peuvent figurer sur la même machine que Host Publisher.

JITCompiler Cette valeur indique le nom du compilateur JIT à utiliser pour l'instanciation Host Publisher du VM. Elle définit la propriété système **java.compiler** qui régit le mode de chargement et d'utilisation des JIT par le VM.

EnableJIT Cette valeur booléenne indique si le JIT indiqué par **JITCompiler** est utilisé.

Classpath Cette valeur indique le CLASSPATH indiqué pour le VM. Si la valeur n'est pas indiquée ou qu'elle est nulle, la variable d'environnement système est utilisée.

Pour accéder aux entrées de valeurs **JITCompiler**, **EnableJIT** et**Classpath**, utilisez l'Editeur du registre de Windows NT sous la clé `HKEY_LOCAL_MACHINE/Software/IBM/Host Publisher/Config`.

Dans la mesure où le VM Java est initialisé lors de l'initialisation de Host Publisher, les modules PageServer et Integrator doivent être redémarrés avant que les modifications apportées au registre prennent effet.

Traitement de pages Web

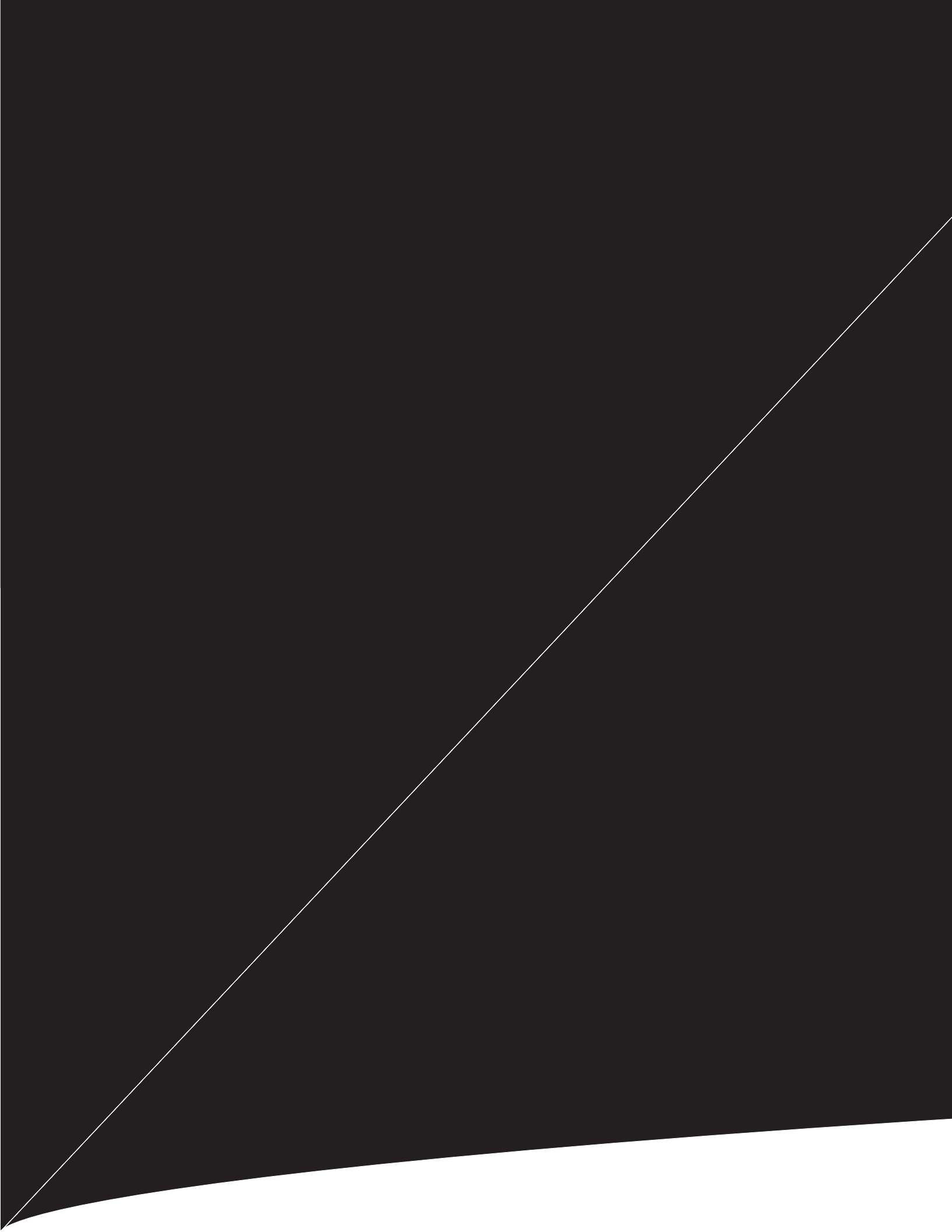
Une fois que vous avez créé une bibliothèque Web à l'aide de **l'Integrator**, vous devez la déployer afin que les clients puissent consulter les pages avec un navigateur Web.

Lorsqu'un client clique sur un bouton de votre page Web, une demande est envoyée par le système client à un serveur Web. Ce dernier appelle l'**Adapter** qui détermine que la demande est associée à une page Web dynamique se trouvant dans un fichier de bibliothèque Web d'une machine de réseau sur laquelle réside un **PageServer**.

Le **Dispatcher** détermine quel **PageServer** doit servir la demande et l'**Adapter** achemine la demande au **PageServer** recommandé

Le **PageServer** repère la page dans l'une de ses bibliothèques et commence à la traiter. Il cherche dans le fichier les éventuels codes DYNA.

- S'il en trouve, il consulte la bibliothèque Web pour localiser les objets d'intégration associés aux codes DYNA et traite les commandes nécessaires pour obtenir le contenu dynamique.



Configuration destinée aux applications à disponibilité élevée

Vous pouvez aisément agrandir votre site Web si le volume des activités augmente. Pour assurer que les clients travaillent dans un environnement à tolérance de panne, Host Publisher vous permet de configurer le **Dispatcher** de sorte que ce dernier continue de fonctionner avec des composants de secours.

Le **Dispatcher** peut être configuré en double (module principal et module secondaire). En cas de défaillance du **Dispatcher** principal pour une raison quelconque, l'**Adapter** et les **PageServer** essaient immédiatement de se connecter au **Dispatcher** secondaire. Chaque **Dispatcher** peut prendre en charge plusieurs serveurs Web.

Vous pouvez installer des répliques des bibliothèques Host Publisher sur plusieurs **PageServer**. Le **Dispatcher** collabore avec les **PageServer** pour effectuer un équilibrage de charge et une allocation de ressources. Les demandes des clients sont transmises au **PageServer** dont les ressources sont les plus disponibles. D'autres **PageServer** peuvent être lancés à mesure que le nombre des demandes des clients augmente.

Connexion de Client Access aux hôtes CICS

Le logiciel client CICS pour Windows NT est livré avec Communications Server pour permettre aux clients de se connecter à des hôtes CICS via Communications Server.

La figure 29 illustre un exemple de configuration d'un client CICS permettant d'accéder aux informations d'un hôte ou d'une base de données CICS.

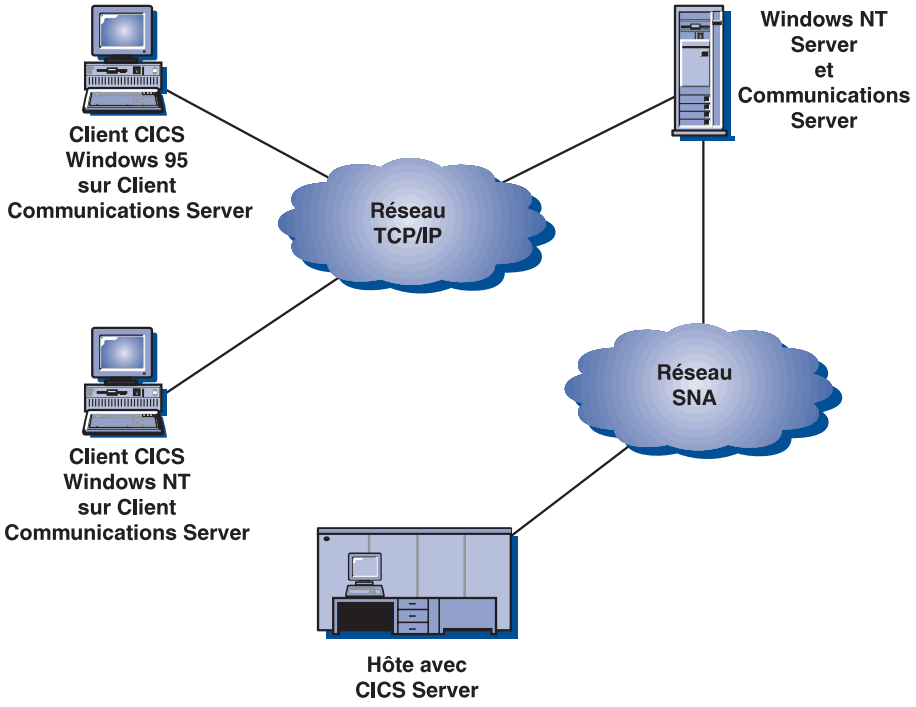


Figure 29. Environnement de client CICS

Pour plus de détails sur la configuration des clients CICS, consultez le manuel *CICS Clients Administration*.

Ce manuel est disponible sur le site Internet suivant :

http://www.software.ibm.com/ts/cics/library

Connexion de Client Access aux hôtes MQSeries

Le logiciel client MQSeries pour Windows NT est livré avec Communications Server pour permettre aux clients de se connecter à des hôtes MQ via Communications Server.

La figure 30, illustre un exemple de configuration d'un client MQSeries permettant d'accéder aux informations d'un hôte ou d'une base de données MQSeries.

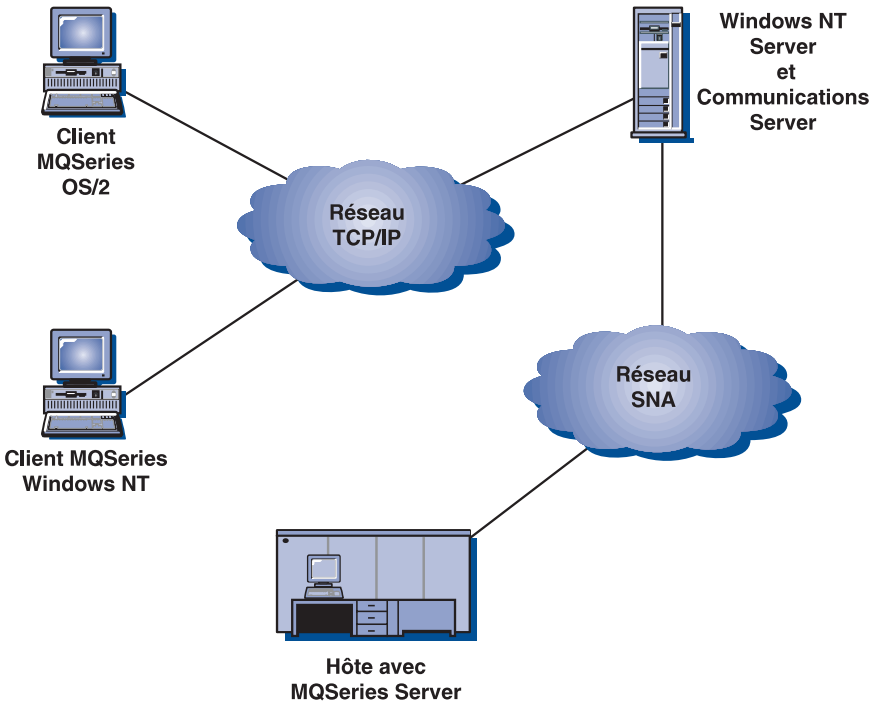


Figure 30. Environnement de client MQSeries

Pour plus de détails sur la configuration des clients MQ, consultez le manuel *MQSeries Intercommunication*. Ce manuel est disponible sur le site Internet suivant :

http://www.software.ibm.com/ts/mqseries/library

Connexion de Client Access aux hôtes DB2

Communications Server comporte un logiciel «à l'essai» pour DB2 Connect Enterprise Edition, un produit permettant la connexion de plusieurs utilisateurs à l'hôte. Vous pouvez installer DB2 Connect Enterprise Edition sur un serveur Windows NT.

Communications Server comporte également DB2 Client Application Enabler (CAE) qui permet l'accès client à l'hôte. Vous pouvez installer DB2 CAE sur une machine client exécutant Windows 3.1, Windows 95, Windows NT ou OS/2.

La figure 31, à la page 111, illustre un exemple de configuration de DB2 Connect Enterprise Edition permettant d'accéder aux informations d'une base de données DB2 sur un hôte.

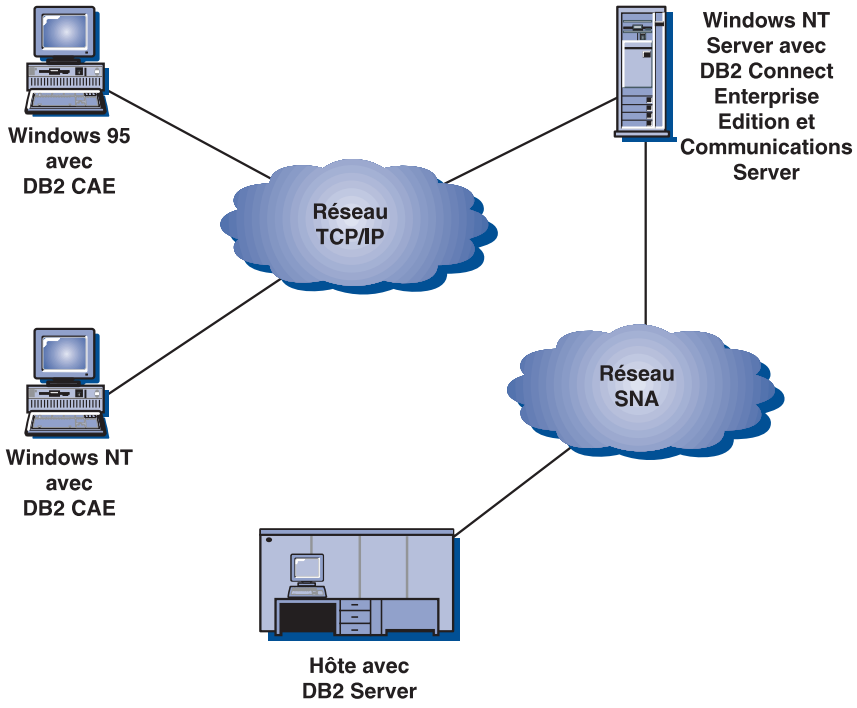


Figure 31. Environnement DB2 Connect Enterprise Edition

Pour plus de détails sur la configuration de Communications Server pour un hôte exécutant DB2, accédez à l'URL suivant sur Internet :

http://www.networking.ibm.com/cms/tips/csncfgdb2.htm

Planification du routage hautes performances

Communications Server prend en charge le routage hautes performances (HPR) via des connexions Enterprise Extender (IP), SDLC (commande de liaison de donnée synchrones), par réseau local, par réseau longue distance, par canal, MPC (Multi-Path Channel) et X.25.

Le routage ANR (Automatic Network Routing) HPR minimise la mémoire et le traitement requis dans les nœuds intermédiaires, ce qui constitue une amélioration par rapport au routage de session intermédiaire (ISR) APPN destiné aux réseaux rapides dont les taux d'erreur sont faibles.

Le support HPR de Communications Server comporte le support de protocole RTP (Rapid Transport Protocol) et le routage ANR (Automatic Network Routing).

Caractéristiques de liaison HPR

Pour fournir les avantages répertoriés ci-dessus, HPR considère que les liaisons de données fournissent de faibles taux de trames perdues. HPR procède à une reprise à la suite des conditions qui occasionnent une perte de trames mais, si ces conditions persistent longtemps, HPR considère que l'encombrement du réseau est trop élevé et que le débit HPR est réduit. Pour obtenir un débit HPR approprié sur une liaison donnée, il est nécessaire de configurer correctement lu nœud émetteur, les fonctions constituant la liaison entre les deux nœuds, et le nœud récepteur.

Remarque : Vous pouvez définir des valeurs ERP dans les cas où les fonctions de connexion de réseau local ont un taux de perte de trames élevé.

Nœud émetteur

Des cartes types utilisées avec HPR envoient des trames sur la liaison avec de faibles taux de défaillance. Pour les réseaux Ethernet, le comportement HPR est dégradé si le réseau local est fortement chargé de collisions (par exemple, si la charge dépasse environ 30 à 40% de la vitesse Ethernet nominale. Pour Frame Relay, des fonctions doivent être configurées pour permettre des connexions individuelles en rafales à la vitesse de transmission d'accès sans occasionner des conditions d'encombrement sur le réseau Frame Relay.

Fonctions de connexion

Les fonctions de réseau local peuvent présenter une grande complexité cachée, par exemple, en présence d'un grand nombre de postes partageant un seul segment de réseau local ou des ponts entre des segments de réseau local, éventuellement des liaisons plus lentes cachées ou des segments de réseau local qui fonctionnent sur des sous-réseaux complexes. L'hypothèse d'une faible perte de trames doit être assurée. Par exemple, les liaisons de réseau longue distance entre les ponts découpés doivent utiliser des fonctions à faible taux d'erreur ou doivent compenser en utilisant la reprise sur incident au niveau de la liaison entre les ponts.

À titre d'exemple supplémentaire, les conditions qui occasionnent le débordement des tampons de pont (orages de diffusion ou importantes rafales de trames de diffusion) doivent être évitées.

Nœud récepteur

Des cartes types utilisées avec HPR reçoivent des trames sur la liaison avec de faibles taux de défaillance. Cependant, certaines cartes ne parviennent pas à recevoir des trames lorsque des trames consécutives arrivent trop rapidement. Les meilleures performances HPR sont réalisées lorsque la carte réceptrice peut traiter son trafic sans perdre des trames entrantes.

Si le taux d'erreur de votre réseau est élevé, il se peut que les administrateurs système constatent sur les connexions HPR un débit inférieur à celui est prévu.

Remarques relatives au routage HPR

Vous pouvez obtenir les caractéristiques HPR en ajoutant des informations supplémentaire dans les en-têtes de trames. Si les caractéristiques HPR ne sont pas requises, il se peut que les surcharges de données réduisent les performances de votre réseau. Les caractéristiques HPR présentent un avantage en présence de nœuds intermédiaires ou de chemins secondaires. Cependant, si des performances élevées sont requises entre deux nœuds connectés via une seule liaison dont la reprise est perturbatrice lors d'un incident de liaison, HPR doit être désactivé lors de la configuration de cette liaison.

HPR met en œuvre la mise en file d'attente prioritaire. En général, le trafic interactif traverse le réseau plus rapidement que le trafic par lots prioritaire. Les cartes qui mettent des trames en file d'attente procèdent ainsi sans tenir compte de la priorité et perturbent peut-être la mise en file d'attente prioritaire de HPR. Il est peut-être nécessaire de réduire la taille de la file d'attente de la carte pour empêcher qu'un trafic à faible priorité retarde le trafic à priorité élevée. Pour plus de détails sur la définition de la taille de file d'attente de la carte, consultez la documentation de la carte.)

La plupart des PC sont désormais dotées de fonctions de gestion d'alimentation avancées qui coupent l'alimentation aux périphériques (par exemple, les unités de disques) et réduisent considérablement la vitesse d'horloge d'un processeur aux fins d'économie d'énergie, si le clavier ou la souris n'est pas utilisé. Sur un poste de travail, il s'agit d'une fonction appropriée ; cependant, sur une plate-forme de serveur, cette coupure peut avoir lieu lors de l'acheminement des données d'une carte à une autre (sans aucune activité du disque). Pour Communications Server, désactivez les fonctions de gestion d'alimentation avancée et matérielle en entrant la configuration du BIOS lors du démarrage (en général, il est nécessaire d'appuyer sur F1 lors de l'initialisation du matériel), puis désactivez ces options.

HPR utiliser un espace mémoire plus important de la carte de réseau local, en raison de l'augmentation des performances et de la mise en file d'attente. La plupart des cartes RAM partagées utilisent par défaut 8 ko de mémoire RAM partagée. La taille de la mémoire RAM partagée requise est de 16 ko. Pour ajuster cette configuration, consultez le manuel de configuration de la carte.

Cette valeur figure sur le BIOS de votre machine ou sur les paramètres de commutateur de la carte.

Remarque : Si vous n'augmentez pas la mémoire RAM partagée à 16 ko, les performances du réseau se dégradent.

N'affectez pas à la mémoire RAM partagée une valeur supérieure à 16 ko (valeur optimale de la mémoire de la carte).

En cas de défaillance des liaisons HPR dans des circonstances à fort trafic, une valeur plus élevée peut être affectée aux horloges de réception. Ainsi, les liaisons disposent d'un délai plus long afin de recevoir un accusé de réception pour les trames envoyées.

Pour les liaisons SDLC, il s'agit du délai de réception principal. Ce délai peut être paramétré sur le DLC ou sur une instruction de liaison logique.

Pour calculer la valeur minimale du délai de réception en dixièmes de secondes, utilisez la formule suivante :

```
[(nbre_fenêtre_émission ▫ taille_zone_i_max ▫ 8) /vitesse transmission effective]▫ 1▫
```

Remarques relatives au paramètres de réglage des DLC de réseau local

Vous pouvez indiquer huit paramètres permettant de modifier la façon dont Communications Server traite la reprise et les incidents liés aux liaisons de réseau local. Il est peut-être nécessaire d'ajuster ces paramètres pour obtenir les meilleurs résultats, si des liaisons lentes, le routage HPR ou des connexions hôte de secours sont utilisées,

Vous devez prendre en considération les paramètres suivants lors de la définition d'un périphérique de réseau local à l'aide de l'application **Configuration du nœud** :

Sous l'onglet **Avancés** :

Délai entre tentatives de test Il s'agit du délai entre les tentatives de recherche du poste de liaison adjacent sur le réseau local. Le nombre de tentatives dépend du du nombre maximal de tentatives de test.

Valeur par défaut : 8.

Nombre maximal de tentatives de test Il s'agit du nombre maximal de tentatives visant à rechercher le poste de liaison adjacent sur le réseau local sans qu'un accusé de réception ne soit délivré dans le laps de temps défini par le délai entre tentatives de test.

Valeur par défaut : 5.

Taille maximale de la PIU La taille maximale de l'unité d'information d'acheminement (PIU) correspond au nombre maximal d'octets contenus dans la mémoire tampon de données que les sessions SNA utilisent pour cette liaison. Si la valeur de la taille maximale de la PIU dépasse la taille de trame prise en charge par votre pilote de périphérique local, la valeur sera réduite pour correspondre à la taille de la trame.

Valeur par défaut : 65535.

Sous l'onglet **Performance** :

Délai d'inactivité Il s'agit de la période à l'issue de laquelle le pilote de périphérique de réseau local déclare la liaison inactive, s'il n'a reçu aucune trame.

Valeur par défaut : 30 secondes.

Retard d'accusé de réception Il s'agit du temps passé par l'unité de réseau local à retenir une réponse à une trame reçue, afin de permettre la réception et la confirmation de trames supplémentaires à l'aide du même message Demande prête (DP).

Valeur par défaut : 100 millisecondes.

Délai de réponse POLL

Il s'agit de la période durant laquelle l'unité de réseau local attend une réponse à une trame envoyée avec le bit POLL.

Valeur par défaut : 8000 millisecondes.

Nombre anticipé de transmissions en suspens Le nombre anticipé de transmissions en suspens correspond au nombre maximal de trames mises en file d'attente par l'unité de réseau local sur un poste de liaison, avant d'envoyer un message Réception non prête (RNP) au poste adjacent.

Valeur par défaut : 16 trames.

Nombre de mémoires tampon de réception Il s'agit du nombre de mémoires tampon réservées au stockage des données en attente de traitement, provenant du système hôte. La taille de chaque mémoire tampon est égale à celle de la PIU.

Valeur par défaut : 32 mémoires tampon.

Changement de chemin HPR

En cas d'échec d'une connexion, HPR assure la commutation non perturbatrice du chemin sur une autre connexion. Une tentative de réactivation de la connexion échouée a lieu avant le changement de chemin. Vous trouverez ci-après une explication des paramètres permettant de déterminer si une connexion a échoué, et du délai d'activation d'un chemin.

Lorsque la valeur indiquée au paramètre **Délai d'inactivité** est atteinte, une trame de repos est envoyée. La valeur par défaut du **Délai d'inactivité** est de 30 secondes.

La valeur indiquée au paramètre **Délai de réponse POLL** détermine le temps pendant lequel l'unité attend une réponse à la trame de repos. La valeur par défaut du paramètre **Délai de réponse POLL** est de huit secondes (8000 millisecondes). 10 tentatives de réactivation d'une trame de repos ont lieu. Ce nombre ne peut pas être modifié.

En l'absence de réponse à la trame de repos, des commandes TEST sont envoyées au système partenaire. La valeur indiquée au paramètre **Délai entre tentatives de test** détermine le délai entre les tentatives de commandes TEST, et la valeur du paramètre **Nombre maximal de tentatives de test** détermine le nombre maximal de tentatives de commandes TEST. La valeur par défaut du **Délai entre tentatives de test** est de 8 secondes et celle du **Nombre maximal de tentatives de test** est de cinq.

Le calcul suivant indique le délai requis pour déterminer si une connexion a échoué et pour activer un changement de chemin :

```
(Délai d'inactivité) + (Délai de réponse POLL ▫ 1▫ tentatives) +
          (Délai entre tentatives de test ▫ Nbre maxi tentatives de test) + 1
```

L'utilisation des valeurs par défaut des paramètres permet d'affecter la valeur de 151 secondes au temps requis pour déterminer un échec de connexion et pour activer un changement de chemin.

```
(3▫ secondes) + (8 secondes ▫ 1▫ tentatives) +
          (8 secondes ▫ 5 tentatives) + 1 = 151 secondes
```

Si, en cas d'échec d'une connexion, vous constatez que les temps de changement de chemin (ou incidents) avec HPR sont longs, vous pouvez les réduire en diminuant les valeurs des paramètres utilisés dans le calcul.

Planification de la passerelle SNA

La passerelle SNA prend en charge :

- Plusieurs protocoles SNA
- Divers postes de travail en aval
- Divers types de liaison entre la passerelle et l'hôte
- Le regroupement des LU (sessions) au niveau de la passerelle
- La définition des postes de travail implicites
- La modification ou l'ajout dynamique des définitions relatives aux postes de travail non actifs
- Plusieurs hôtes simultanément
- Divers types de liaison (pouvant être combinés) entre les postes de travail et la passerelle

Pour plus de détails sur la configuration de la passerelle SNA à l'aide de l'application **Configuration du nœud**, consultez le manuel *Guide d'utilisation*.

Connexions aux postes de travail

La passerelle SNA prend en charge les postes de travail connectés via les éléments suivants :

- Connectivités de réseau local
  - Token ring
  - Ethernet
  - ATM (Émulation de réseau local)
- Frame Relay
- SDLC
  - Asynchrone
  - Synchrone
  - Hayes Autosync
  - Principal multipoint
- Réseau X.25
- AnyNet TCP/IP (pour les connectivités prises en charge via Microsoft TCP/IP)
- Connexions RNIS

La passerelle SNA peut prendre en charge jusqu'à 254 LU pour chaque PU définie. Vous pouvez définir une PU différente pour chacune de vos connexions hôte. Les LU sont utilisées par les postes de travail en aval pour la connexion à l'hôte. Le nombre de postes de travail en aval pris en charge est fonction de plusieurs facteurs, notamment le type de connectivité et le nombre de cartes de la passerelle. Par exemple, si une carte de réseau local réside sur la passerelle, une seule liaison hôte comportant 254 LU peut être utilisée simultanément par 253 postes de travail en aval. Vous pouvez utiliser deux cartes pour doubler ce nombre.

Connexions aux postes de travail SDLC

Vous pouvez choisir de vous connecter via SDLC dans des configurations point à point et multipoint. Une fois la configuration terminée, aucune considération particulière n'est nécessaire pour l'exécution de SDLC entre le poste de travail et la passerelle.

Lors de la configuration des postes de travail secondaires multipoint, prenez en considération les divers facteurs qui contrôlent le temps d'exécution d'appel. La rapidité d'appel du poste secondaire le plus loin par le poste principal est physiquement limitée. La définition de tous les postes de travail secondaires à l'aide des mêmes paramètres permet de simplifier le calcul suivant.

Pour calculer le délai d'inactivité minimal en secondes, utilisez la formule suivante :

```
     NS ▫ (SW + RW) ▫ (IS + 2) / (LS / 8)
où :
     NS  =  Nombre de postes
     SW  =  Taille de la fenêtre d'émission
     RW  =  Taille de la fenêtre de réception
     IS  =  Taille de la zone d'information
     LS  =  Vitesse de transmission (bps)
```

Si ces valeurs ne sont pas identiques pour tous les postes de travail, un calcul distinct doit être effectué pour chaque groupe ou poste de travail, puis additionné pour obtenir la valeur correcte du délai d'inactivité.

Par exemple, pour une liaison multipoint comportant 16 postes de travail à 14,4 kbps, chacun défini pour une taille de fenêtre d'émission de 7, une taille de fenêtre de réception de 7 et une taille de zone d'information de 521, le calcul du délai d'inactivité est le suivant :

```
16 ▫ (7 + 7) ▫ (521 + 2) / (144▫▫ / 8) = 65,1 secondes
```

Remarque : Ajoutez toujours quelques secondes supplémentaires pour une mémoire tampon.

Connexions aux postes de travail X.25

Si vous configurez la passerelle SNA pour utiliser uniquement des connexions PVC (Permanent Virtual Circuit) X.25 entre la passerelle et les postes de travail, il est conseillé de configurer toutes les PVC de poste de travail et de passerelle avec des rôles de poste de liaison négociables. Sinon, les postes de travail risquent de ne pas pouvoir établir les liaisons PVC X.25 avec la passerelle.

Pour plus de détails sur les connexions PVC et sur la configuration, reportez-vous à la section Planification de X.25.

Connexions aux hôtes

La passerelle SNA prend en charge les connexions suivantes à un hôte :

- Connectivités de réseau local
  - Token ring
  - Ethernet
  - ATM (Émulation de réseau local)

- Frame Relay
- SDLC
  - Synchrone
  - Hayes Autosync
- Réseau X.25
- Twinaxial (à l'AS/400)
- AnyNet TCP/IP (pour les connectivités prises en charge via Microsoft TCP/IP)
- Enterprise Extender IP (pour les connectivités prises en charge via Microsoft IP)
- Channel (CDLC)
- Channel (MPC) avec une connexion DLUR
- Connexions RNIS

Si des connexions sont établies à plusieurs hôtes à partir de la passerelle utilisée par le trafic de LU dépendantes, seule la liaison hôte au nom de PU de point de contrôle peut :

- servir de point focal hôte ;
- établir des sessions CP-CP avec l'hôte ;
- être utilisé pour les fonctions APPN.

Les liaisons qui sont définies à l'aide d'un nom de PU autre que le nom de point de contrôle ne peuvent être utilisées que pour d'autres connexions de LU dépendantes à un hôte.

Si une liaison de l'hôte à la passerelle est définie comme sous forme de liaison à ressources limitées, elle envoie une demande de déconnexion à l'hôte une fois que la dernière session LU-LU est arrêtée. La passerelle transmet ensuite les DACTLU au poste de travail et un DACTPU aux postes de travail ayant établi des sessions uniquement avec cette liaison hôte. Lorsque le poste de travail connecté à la passerelle est défini comme étant une ressource limitée, la liaison au poste de travail est déconnectée en l'absence d'autres session. Dans Communications Server, vous pouvez désigner un poste de travail par ressource limitée, lors de la définition de la connexion client explicite.

Cependant, si le poste de travail est doté d'une application (ou d'un émulateur) qui réactive automatiquement sa liaison à l'hôte, la passerelle réactive la liaison avec son hôte lorsque le poste de travail active sa liaison à la passerelle. Cela signifie que des définitions de postes de travail incompatibles annulent la fonction à ressource limitée au niveau de la passerelle.

Remarques relatives à l'hôte

Prenez en considération les remarques suivantes lors de la planification de la connexion hôte :

- Si votre environnement utilise un point de contrôle réseau (NCP), le paramètre 37*xx* NCPGEN, la macro **LINE**, la valeur **MAXLU** doivent être au moins équivalents au nombre de LU de Communications Server.

- Les utilisateurs VTAM peuvent contrôler le délai pendant lequel VTAM met les données en mémoire tampon avant de les envoyer au contrôleur. Lorsque le paramètre **DELAY=0** de VTAM est indiqué sur une définition de PU, le temps de réponse d'émission hôte risque d'être plus rapide au détriment d'un effort supplémentaire du processeur hôte.

  Une valeur autre que zéro affectée à DELAY permet d'économiser les instructions de processeur hôte au détriment d'une augmentation du temps de réponse de réception sur le poste de travail Communications Server.

  Pour le coattailing, commencez par affecter une valeur par défaut de 0,2. Un retard de 0,2 seconde a un effet modéré sur le temps de réponse mais, si la vitesse correspond à environ une transaction par seconde ou plus, un coattailing se produit.

- Bien que chaque poste de travail SNA en aval du réseau local mette en œuvre une PU avec son propre ensemble de LU, la passerelle SNA est mise en œuvre de sorte que l'hôte n'identifie que la PU de passerelle. Par conséquent, une seule définition de PU est codifiée au niveau de l'hôte. Cette définition de PU contient les LU de ***tous*** les postes du réseau local qui se connecteront à l'hôte via cette passerelle.

  Si le VTAM de l'hôte prend en charge les LU dépendantes à définition automatique (SDDLU), vous pouvez tirer parti de la fonction. Lors de la configuration des LU hôte, indiquez un type ou un nom de modèle de LU correspondant à la valeur de l'opérande LUSEED défini dans le nœud principal commuté VTAM et utilisé par l'exit SDDLU VTAM.

Configuration des adresses de destination de réseau local

Vous devez entrer une adresse de destination si vous utilisez une des connexions de réseau local prises en charge entre la passerelle et l'hôte ou entre la passerelle et un poste de travail défini de manière explicite. Lors de la détermination de l'adresse de destination correcte à entrer dans chaque profil, veillez à ce que l'image appropriée des deux adresses permette la visualisation de la destination à partir de la passerelle SNA (voir la figure 32).

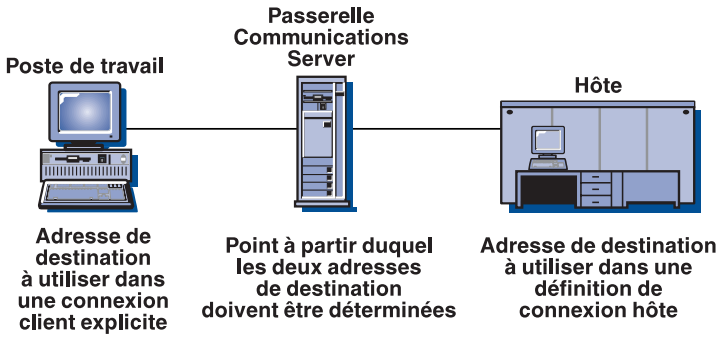


Figure 32. Image à utiliser pour les entrées d'adresse de destination

Planification des définitions de LU de passerelle

La passerelle SNA prend en charge les ***groupes*** de LU hôte et les LU hôte ***spécifique***. Lorsque des LU sont configurées pour chaque connexion hôte au niveau de la passerelle, elles peuvent être réunies dans des groupes. La création de groupes est généralement avantageuse pour les raisons suivantes :

- Si toutes les sessions de tous les postes de travail doivent communiquer simultanément avec l'hôte, le regroupement permet de conserver les ressources système. Les sessions de postes de travail du réseau local peuvent partager les mêmes LU mais non en même temps. Cette fonction permet au nombre de LU configurées au niveau de la passerelle SNA pour des sessions de poste de travail de dépasser le nombre de LU configurées entre l'hôte et la passerelle, ce qui réduit les ressources d'hôte requises et la définition de poste de travail, et accélère les redémarrages.
- Les groupes sont plus faciles à administrer et à configurer. Vous pouvez ajuster la taille du groupe en y ajoutant des LU supplémentaires ou en en supprimant des LU sans aucune incidence sur les autres définitions.

  Les LU de groupe ne sont pas affectées à un poste de travail particulier et ne doivent pas être réservées uniquement aux utilisateurs de passerelle en aval. Un seul groupe peut être partagé par des utilisateurs TN3270 en aval et par des postes de travail de passerelle SNA, ainsi que par des clients API SNA et des sessions d'émulation locales. Pour configurer un seul groupe (par exemple, PUBLIC) pour toutes les utilisations de LU dépendantes, il n'est pas nécessaire de savoir comment les utilisateurs sont répartis à travers ces types.
- Les groupes permettent une meilleure disponibilité des postes de travail en aval si des LU sont définies à partir de plusieurs connexions dans le même groupe. Si une seule des connexions est active, les utilisateurs peuvent accéder aux LU de la liaison active.

Prenez en considération les scénarios suivants :

- Communications Server est doté de deux connexions hôte, chacune comportant 100 LU, l'ensemble appartenant au groupe A. La première liaison est configurée comme faisant l'objet d'une *activation au démarrage* et est opérationnelle. Tous les postes de travail utilisent cette liaison et ses LU. La seconde liaison est configurée comme étant à *activation automatique*. Cette combinaison de groupes et de configuration de liaison peut assurer une meilleure disponibilité de deux manières. Si la première liaison échoue, les sessions dépendantes de reprise activent automatiquement la deuxième liaison. Si la première liaison réduit ses LU définies, la liaison de secours sera automatiquement activée lorsque la LU suivante (la 101e) est requise.
- Vous pouvez également utiliser la combinaison de groupes et de configuration de liaison afin de fournir un équilibrage de charge pour les postes de travail en aval à travers les connexions hôte disponibles. À titre d'exemple, Communications Server doit être doté de deux connexions hôte, chacune comportant 100 LU, l'ensemble appartenant au groupe A. Les deux liaisons sont configurées comme faisant l'objet d'une *activation au démarrage* et sont opérationnelles. Les postes de travail associés à la LU de groupe seront répartis entre les deux connexions afin de partager la charge à travers celles-ci.

La passerelle SNA attribue des LU de groupe aux sessions de postes de travail lors de la connexion du poste de travail en aval à la passerelle.

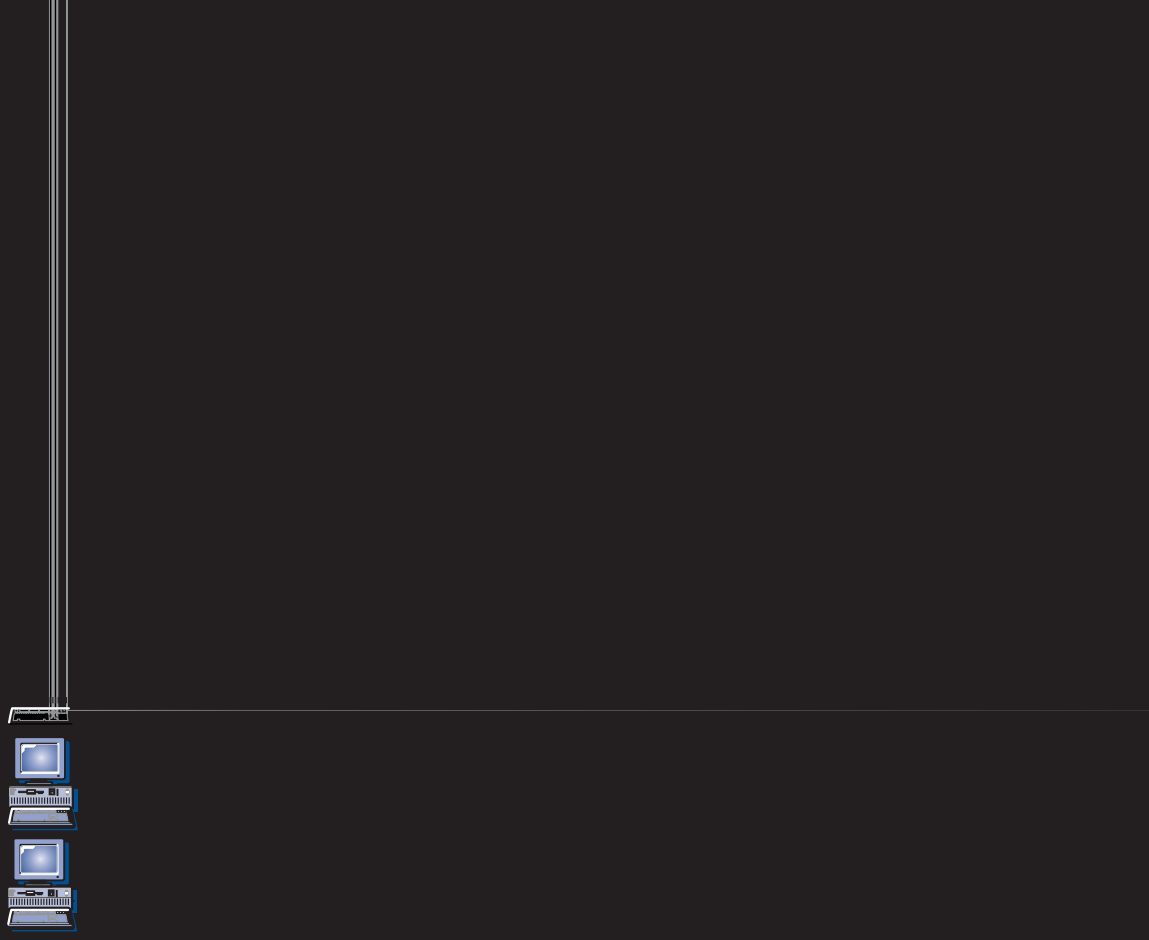


Figure 33. Scénario simple utilisant des LU de groupe et des LU spécifiques

Connexions explicites et implicites

Les deux types de postes de travail en aval suivants sont pris en charge par la passerelle : postes de travail explicites et postes de travail implicites. Les postes de travail explicites disposent d'adresses de destination définies sur un type de DLC particulier (par exemple, un réseau en anneau à jeton et SDLC). Pour configurer un poste de travail explicite, vous devez connaître l'adresse de destination, le nom qualifié du point de contrôle adjacent ou l'ID nœud adjacent de chaque poste de travail ; vous devez également définir une liaison logique à la passerelle pour chaque poste de travail. Vous pouvez définir des LU de groupe ou des LU spécifiques pour les postes de travail explicites.

Il est beaucoup plus facile de configurer un poste de travail implicite. En revanche, celui-ci ne peut utiliser que des LU de groupe. Au lieu de définir une liaison avec chaque poste de travail à l'aide de la passerelle, vous pouvez définir un ou plusieurs groupes sur l'hôte et configurer les unités (DLC) auxquelles se connecteront les postes de travail. Il suffit alors de configurer un modèle de client implicite pour la définition de LU de chaque poste de travail connecté à la passerelle et ne correspondant pas à une définition explicite. Par exemple, si chaque poste de travail d'un réseau Ethernet dispose de deux sessions 3270 configurées avec les adresses NAU 2 et 3, vous définirez un modèle de client avec deux LU (une pour l'adresse 2 et une pour l'adresse 3). Si les deux adresses sont utilisées pour les sessions établies avec un seul hôte, les deux doivent être associées au même groupe hôte. Si, cependant, l'adresse 2 est utilisée pour accéder à HOST_A et l'adresse 3 à HOST_B, chacune doit être associée au groupe hôte approprié.

Dans cet exemple, une liaison est créée de manière dynamique chaque fois qu'un poste de travail ne correspondant pas à une définition explicite se connecte à la passerelle via Ethernet, et les deux LU des NAU 2 et 3 sont allouées à partir du ou des groupes hôte.

Pour les postes de travail implicites, les utilisateurs qui se connectent à la passerelle doivent uniquement connaître l'adresse du DLC passerelle configurée sur la carte pour ces postes de travail, ainsi que les valeurs NAU qui ont été définies sur la passerelle. Ils doivent utiliser ces valeurs NAU lors de la définition de leurs imprimantes logiques et sessions 3270.

Un poste de travail Communications Personnelles en aval se connectant à Communications Server peut utiliser la fonction de découverte de réseau local pour rechercher, à l'aide du nom de groupe `IGO2HOST`, l'adresse de la carte.

Performances de la passerelle SNA

Les performances via une passerelle sont fonction de plusieurs facteurs :

- Configuration de la passerelle
- Connexion à l'hôte ou aux hôtes
- Demande de traitement global sur chaque hôte
- Connexions aux postes de travail pris en charge
- Configurations des postes de travail pris en charge
- Nombre de postes de travail pris en charge
- Nombre de sessions établies avec chaque poste de travail
- Priorité de transmission SNA
- Contrôle de flux
- Fenêtre de régulation pour toutes les sessions
- Trafic sur des sessions non passerelle

L'utilisation d'un poste de travail qui met en œuvre une passerelle logicielle pour d'autres fonctions peut également réduire les performances de la passerelle.

Si aucun des facteurs susmentionnés n'a une incidence négative sur les performances, un poste de travail individuel utilisant des protocoles SNA pris en charge ne doit rencontrer aucun écart de performances important entre une connexion directe à l'hôte et une connexion indirecte au moyen d'un réseau local via une passerelle SNA connectée à l'hôte. En effet, si les liaisons hôte sont actives au niveau de la passerelle, l'activation du poste de travail risque de s'améliorer grâce à la suppression du délai de surcharge de l'hôte. Cependant, en raison du grand nombre de variables utilisées, vous pouvez mener des tests de performances dans votre environnement d'exploitation de manière à obtenir l'équilibre souhaité entre les fonctions et les performances.

Remarques relatives au DLUR

L'utilisation du DLUR pour la connexion à l'hôte permet de bénéficier d'une souplesse dans l'éventuel emplacement de la passerelle SNA. La connexion à l'hôte peut traverser n'importe quel réseau APPN et ne doit pas nécessairement être adjacente à un HOST/NCP. Un canal de communication DLUR-DLUS est créé sur le VTAM DLUS, qui est utilisé pour les flux de contrôle de sessions indépendantes.

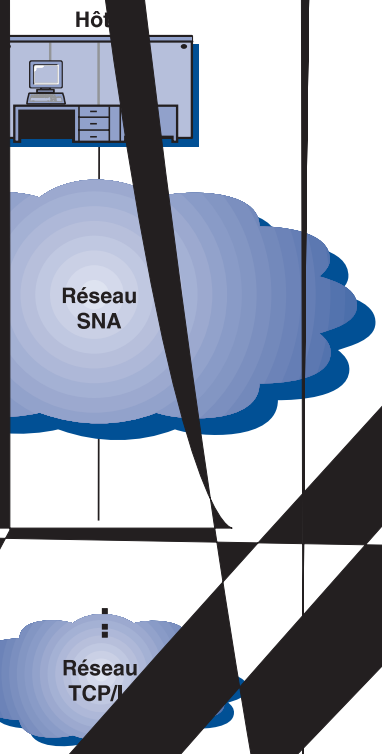
La configuration recommandée pour l'établissement d'une connexion DLUR à l'hôte doit définir la passerelle comme étant un nœud de réseau et configurer les informations DLUS. Lors de la configuration des clients explicites et implicites, ceux-ci doivent être associés au DLUS. Cette configuration est la plus simple car elle ne requiert aucune connaissance des LU en aval au niveau de la passerelle et elle fournit au VTAM un maximum de visibilité des périphériques en aval dans la mesure où VTAM est informé de la PU.

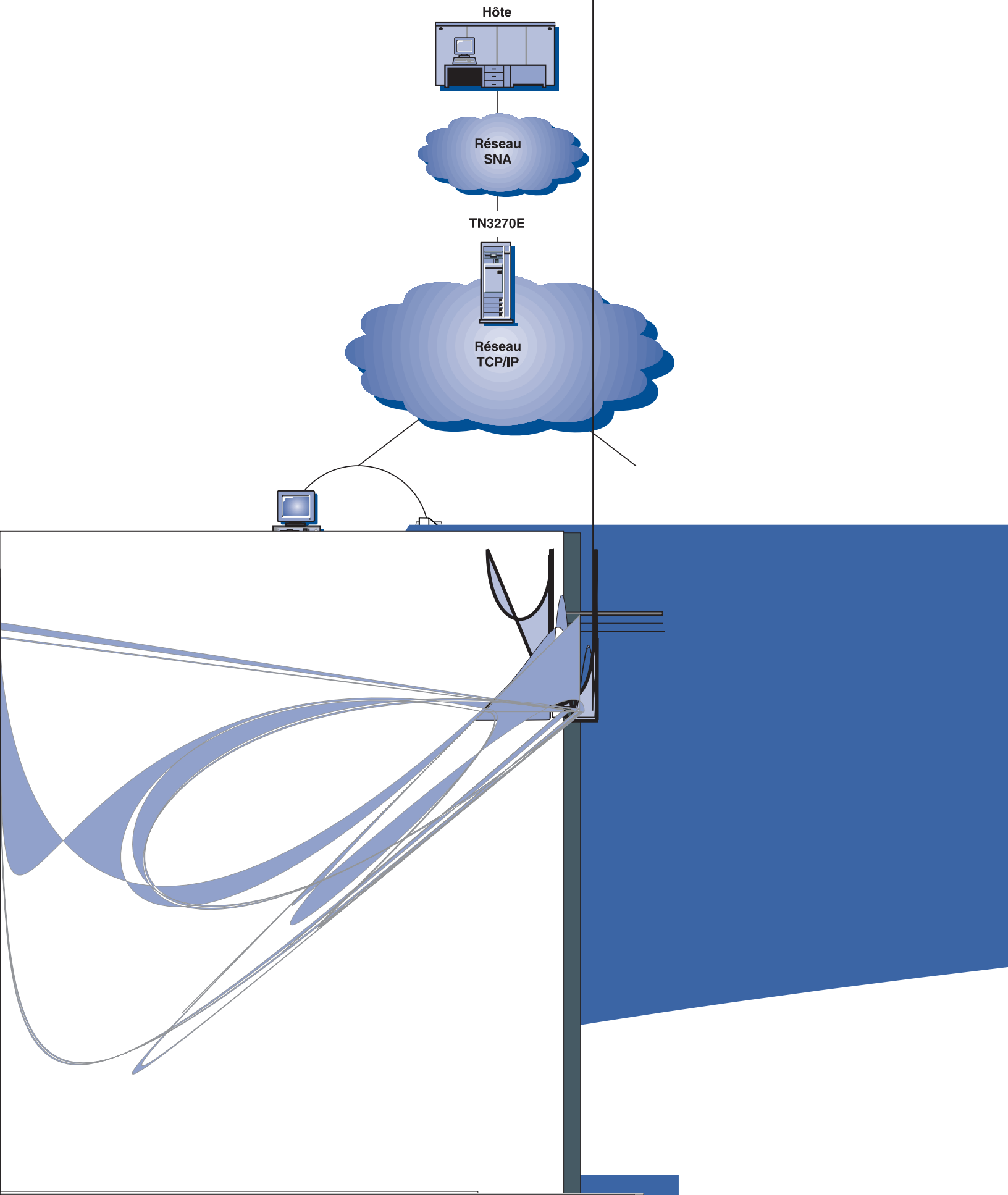
Si vous ne voulez pas que VTAM soit informé des PU en aval, vous pouvez configurer une PU interne au niveau de la passerelle (et non une connexion hôte), puis associer les postes de travail en aval à cette PU interne.

Si un poste de travail en aval tel que Communications Personnelles prend en charge le DLUR, vous pouvez choisir l'acheminement de ce poste de travail via Communications Server à l'aide de la fonction de nœud de réseau et non de la fonction de passerelle SNA.

ification du serve 3270E

La fonction Serveur T 270E permet de configurer le ré selon les illustrations de la figure , ou de figure 35, à la page 128.




Hôte
Réseau
SNA
TN3270E
Réseau
TCP/IP

Communications Server prend en charge la spécification des filtres client TCP/IP en utilisant des adresses IP, des sous-réseaux, des noms d'hôte ou des noms de domaine. Cette fonction permet l'administration centralisée des clients qui sont autorisés à se connecter au serveur TN3270E, ainsi que la spécification des noms et groupes de LU accessibles aux clients.

- Traitement des réponses

  Les clients prenant en charge TN3270E peuvent envoyer des réponses positives et négatives transmises à l'hôte par le serveur TN3270E. Ce dernier génère des réponses aux demandes des clients TN3270 standard.

- Gestion des touches ATTN et SYSREQ

  Le serveur TN3270E peut convertir et envoyer des informations à l'hôte lorsque le client appuie sur une touche ATTN ou SYSREQ. Bien que les clients qui ne prennent pas en charge TN3270E ne disposent pas de définition explicite relative aux fonctions ATTN et SYSREQ, ces dernières sont mises en œuvre par le serveur TN3270E à l'aide des commandes Telnet suivantes :

Tableau 6. Équivalents de commandes

Telnet	TN3270E	TN3270 standard
IP	ATTN	SYSREQ
AO	SYSREQ	SYSREQ
BREAK	Non applicable	ATTN

- Classes LU

  Communications Server attribue à la connexion utilisateur des classe de LU. Les classes sont constituées de LU configurées avec des caractéristiques courantes qui requièrent, par exemple, une connexion hôte spécifique. Cela simplifie l'accès des utilisateurs, regroupe les utilisateurs en fonction des besoins en application et maximise les ressources de l'hôte.

- Sécurité SSL (Secure Sockets Layer)

  Les connexions entre les clients TN et le serveur TN3270E utilisent SSL version 3 pour assurer le chiffrement de données et l'authentification du serveur à l'aide de certificats signés.

Pour plus de détails sur la configuration d'un serveur TN3270E, consultez le *Guide d'utilisation*.

Postes de travail client pris en charge sur le serveur TN3270E

Le serveur TN3270E prend en charge tout client TN3270E ou TN3270 qui est entièrement conforme aux documents RFC 1576, 1646 ou 1647.

Caractéristiques principales

La présente section fournit des informations complémentaires relatives à certaines fonctions que vous pouvez configurer pour le serveur TN3270E.

Modification du numéro de port par défaut

Vous pouvez configurer le numéro de port utilisé par le serveur pour les nouvelles connexions, à l'aide de la fenêtre Options TN3270E. Le numéro de port par défaut est 23 mais il se peut que celui-ci soit également utilisé par d'autres applications Telnet telles que le support de serveur TN5250. Si tel est le cas, vous devez utiliser un autre port.

Si vous modifiez le numéro de port, évitez les numéros qui sont utilisés par d'autres applications. Si deux applications utilisent le même numéro de port, l'une de ces applications n'aboutit pas.

Si vous modifiez le numéro de port, utilisez un numéro supérieur à 1024, les numéros inférieurs à ce chiffre étant réservés. Pour plus de détails sur les numéros de port réservés, accédez au site Internet suivant :

http://www.ds1.internic.net

Au moment de la publication du présent manuel, le document RFC le plus récent relatif aux numéros affectés est le RFC 1700.

Lorsque vous modifiez le numéro de port, informez les clients TN3270E car ces derniers devront configurer leurs applications d'émulation en conséquence.

Gestion du trafic système

La fréquence de désactivation des connexions peut être contrôlée selon les deux méthodes suivantes :traitement du repos et fin de session automatique

Par défaut, le serveur TN3270E n'utilise pas le traitement du repos. Si vous utilisez ce dernier, vous pouvez choisir l'option NOP ou la marque de synchronisation.

- Le traitement NOP envoie une commande NOP Telnet après une fréquence de repos indiquée. Il en résulte une transmission de données sur la connexion, ce qui permet à TCP/IP de détecter la désactivation de la connexion. Le serveur n'attend pas de réponse de la part du client. La détection par TCP/IP d'une interruption de connexion peut prendre un certain temps.
- Le traitement de marque de synchronisation envoie une commande de marque de synchronisation Telnet au client. Si ce dernier ne répond pas dans le délai indiqué, la connexion est libérée.

La marque de synchronisation permet sur le système un trafic plus important que le traitement NOP mais libère plus rapidement les connexions non utilisées.

Si l'option Fin de session automatique est choisie, le serveur déconnecte les sessions qui sont inactives pendant le délai indiqué. Le trafic résultant du traitement du repos ne permet pas de conserver la connexion ; des données doivent être envoyées à destination ou en provenance de l'hôte. Les sessions d'imprimante ne sont pas automatiquement fermées.

Si les émulateurs client sont configurés pour le traitement du repos, ce dernier peut être mis hors tension sur le serveur ; de même, si le traitement du repos est effectué au niveau du serveur, il est possible de le mettre hors tension au niveau du client afin de réduire le trafic sur le réseau.

Filtrage IP

Communications Server permet de configurer des filtres TN3270E pour préciser quels clients TCP/IP peuvent se connecter au serveur. Les clients peuvent être définis à l'aide d'adresses IP individuelles, de sous-réseaux IP, de noms d'hôte TCP/IP ou de noms de domaine.

Support SSL (Secure Sockets Layer)

Vous pouvez, dans la fenêtre **TN3270E Server Parameters** ou à partir d'un fichier réponses, configurer un numéro de port sécurisé utilisé par le serveur pour des connexions sécurisées.

Pour activer la sécurité, Communications Server fournit un utilitaire **Key-Ring Management** qui permet de générer le certificat et les clés requis par SSL. Pour plus de détails, reportez-vous à la section «Planification de la sécurité SSL», à la page 139.

Une fois la sécurité configurée et activée, les clients TN3270E prenant en charge SSL version 3 peuvent se connecter à un numéro de port sécurisé et établir des connexions sécurisées.

Configuration des connexions SNA

Vous devez configurer la connexion hôte et des LU hôte avant d'utiliser la fonction Serveur TN3270E. Pour consulter un tableau qui décrit et explique les paramètres hôte, consultez le *Guide d'utilisation*.

Groupe de LU

Voici les quatre classes de définitions de LU qui sont spécifiques au serveur TN3270E : poste de travail implicite, poste de travail explicite, imprimante implicite et imprimante explicite. Ces classes correspondent aux classes terminal générique, terminal spécifique, imprimante générique et imprimante spécifique indiquées dans le document RFC 1647.

Les définitions de ***poste de travail implicite*** sont définies dans un groupe utilisé par le serveur TN3270E pour répondre aux demandes de connexion. Le groupe par défaut peut être configuré pour répondre aux demandes dans lesquelles le client n'indique pas de nom de LU ou de groupe. Tous les autres groupes doivent être demandés à l'aide d'un nom.

Vous pouvez également définir un ensemble de définitions de LU servant à répondre aux demandes de nom de LU spécifique. Ces définitions de ***poste de travail explicite*** assurent qu'un terminal requis par une application hôte n'est pas affecté à un client qui n'en a pas expressément fait la demande.

De même, vous pouvez définir un groupe de définitions d'imprimante servant à répondre aux demandes de connexions qui ne requièrent pas de noms de LU spécifiques (***imprimante implicite***), ainsi qu'un ensemble permettant de répondre aux demandes de nom de LU spécifique (***imprimante explicite***).

Les définitions de poste de travail implicite et explicite peuvent être associées à des imprimantes. Chaque définition de terminal peut être associée à une imprimante et chaque imprimante à une définition de terminal. Ces imprimantes ne sont pas incluses dans les définitions d'imprimante explicite ou implicite.

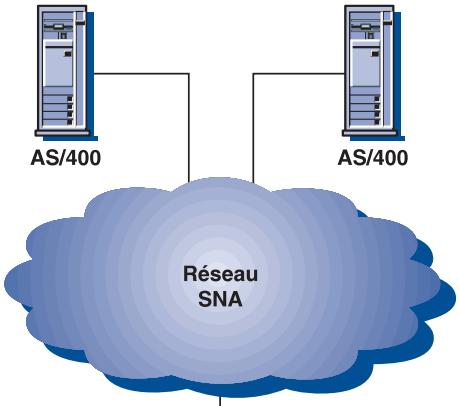
Les définitions d'***imprimante associée*** ne sont accessibles qu'à l'aide du nom de LU du terminal. Elles réduisent la quantité d'informations requises par le client car il suffit que ce dernier connaisse le nom de LU du terminal pour se connecter aux sessions d'imprimante et de terminal.

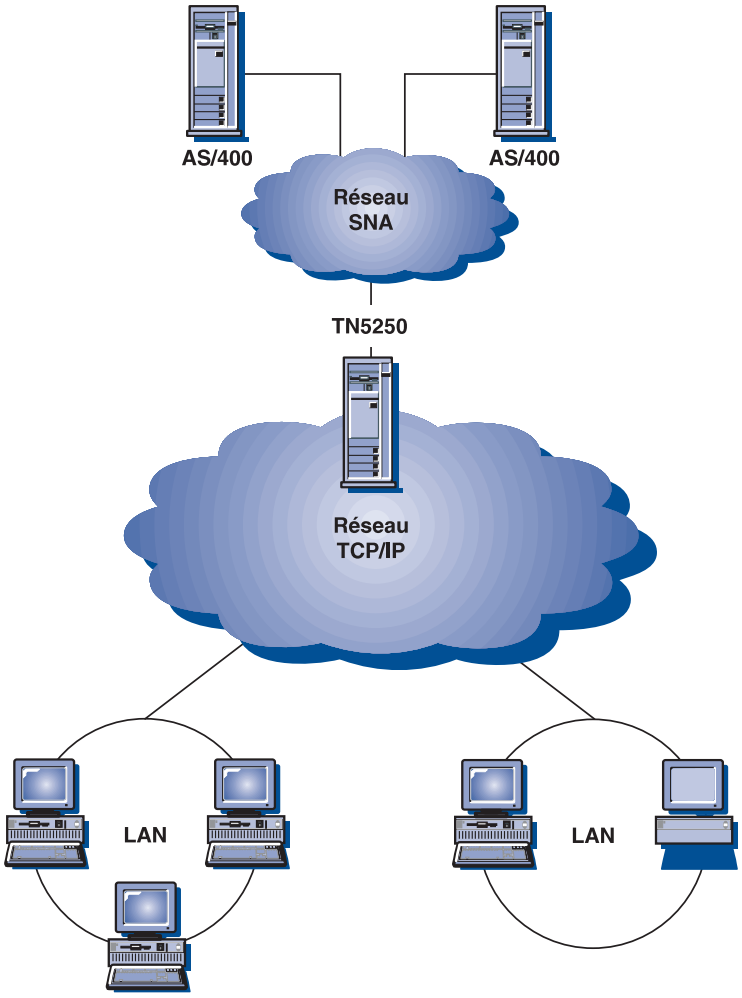
Équilibrage de charge des serveurs TN3270E

Communications Server prend également en charge l'équilibrage de charge des clients TN3270 sur plusieurs serveurs TN3270E. Pour plus de détails, reportez-vous à la section «Planification de l'équilibrage de charge», à la page 147.

Planification du serveur TN5250

La fonction Serveur TN5250 permet de configurer le réseau selon les illustrations de la figure 36, ou de la figure 37, à la page 134.




AS/400
AS/400
Réseau
SNA
TN5250
Réseau
TCP/IP
LAN
LAN

- Sécurité SSL (Secure Sockets Layer)

  Les connexions entre les clients TN et le serveur TN3270E utilisent SSL version 3 pour assurer le chiffrement de données et l'authentification du serveur à l'aide de certificats signés.

Pour plus de détails sur la configuration d'un serveur TN5250, consultez le *Guide d'utilisation*.

Postes de travail client pris en charge sur le serveur TN5250

Le serveur TN5250 prend en charge tout client 5250 entièrement conforme au document RFC 1205.

Caractéristiques principales

La présente section fournit des informations complémentaires relatives à certaines fonctions que vous pouvez configurer pour le serveur TN5250.

Modification du numéro de port par défaut

Lors de la configuration du support de serveur TN5250, un port par défaut portant le numéro 23 est défini mais il se peut que celui-ci soit également utilisé par d'autres applications Telnet telles que le support de serveur TN3270E. Si tel est le cas, vous devez utiliser un autre port.

Si vous modifiez le numéro de port, évitez les numéros qui sont utilisés par d'autres applications. Si deux applications utilisent le même numéro de port, l'une de ces applications n'aboutit pas.

Si vous modifiez le numéro de port, utilisez un numéro supérieur à 1024, les numéros inférieurs à ce chiffre étant réservés. Pour plus de détails sur les numéros de port réservés, accédez au site Internet suivant :

http://www.ds1.internic.net

Au moment de la publication du présent manuel, le document RFC le plus récent relatif aux numéros affectés est le RFC 1700.

Lorsque vous modifiez le numéro de port, informez les clients TN5250 car ces derniers devront configurer leurs applications d'émulation en conséquence.

Gestion du trafic système

La fréquence de désactivation des connexions peut être contrôlée selon les deux méthodes suivantes :traitement du repos et fin de session automatique

Par défaut, le serveur TN5250 n'utilise pas le traitement du repos. Si vous utilisez ce dernier, vous pouvez choisir l'option NOP ou la marque de synchronisation.

- Le traitement NOP envoie une commande NOP Telnet après une fréquence de repos indiquée. Il en résulte une transmission de données sur la connexion, ce qui permet à TCP/IP de détecter la désactivation de la connexion. Le serveur n'attend pas de réponse de la part du client. La détection par TCP/IP d'une interruption de connexion peut prendre un certain temps.

- Le traitement de marque de synchronisation envoie une commande de marque de synchronisation Telnet au client. Si ce dernier ne répond pas dans le délai indiqué, la connexion est libérée.

La marque de synchronisation permet sur le système un trafic plus important que le traitement NOP mais libère plus rapidement les connexions non utilisées.

Si l'option Fin de session automatique est choisie, le serveur déconnecte les sessions qui sont inactives pendant le délai indiqué. Le trafic résultant du traitement du repos ne permet pas de conserver la connexion ; des données doivent être envoyées à destination ou en provenance de l'hôte.

Si les émulateurs client sont configurés pour le traitement du repos, ce dernier peut être mis hors tension sur le serveur ; de même, si le traitement du repos est effectué au niveau du serveur, il est possible de le mettre hors tension au niveau du client afin de réduire le trafic sur le réseau.

Accès aux systèmes AS/400 via plusieurs ports

Communications Server permet de configurer plusieurs systèmes AS/400, ainsi que plusieurs ports destinés au serveur TN5250 pour recevoir les connexions entrantes. Lors de la configuration d'un nouveau port de serveur TN5250, vous pouvez indiquer l'AS/400 devant être associé à ce port. Les connexions TCP/IP entrantes reçues sur ce port par le serveur TN5250 accèdent au système AS/400 associé à ce port.

Notifiez aux clients TN5250 les numéros de port à configurer aux fins de connexion de leurs applications d'émulation à des systèmes AS/400 spécifiques.

Filtrage IP

Communications Server permet de configurer des filtres TN5250 pour préciser quels clients TCP/IP peuvent se connecter au serveur. Les clients peuvent être définis à l'aide d'adresses IP individuelles, de sous-réseaux IP, de noms d'hôte TCP/IP ou de noms de domaine.

Vous pouvez également configurer un AS/400 avec un filtre afin d'indiquer un système AS/400 autre que celui qui est associé au port. Cela permet de diriger les clients associés à un filtre vers un AS/400 spécifique.

Plusieurs systèmes AS/400 peuvent être indiqués dans un filtre. Si une tentative de connexion client au premier AS/400 indiqué n'aboutit pas, des tentatives de connexion à d'autres AS/400 indiqués dans le filtre sont faites.

Support SSL (Secure Sockets Layer)

Lors de la configuration d'un nouveau port de serveur TN5250, vous pouvez indiquer que le port sera utilisé pour des connexions sécurisées. Plusieurs ports peuvent être définis comme étant sécurisés.

Pour activer la sécurité, Communications Server fournit un utilitaire **Key-Ring Management** qui permet de générer le certificat et les clés requis par SSL. Pour plus de détails, reportez-vous à la section «Planification de la sécurité SSL», à la page 139.

Une fois la sécurité configurée et activée, les clients TN5250 prenant en charge SSL version 3 peuvent se connecter à un numéro de port sécurisé et établir des connexions sécurisées.

Configuration du réseau SNA

Il est nécessaire de configurer le réseau SNA de sorte que le serveur TN5250 se connecte aux systèmes AS/400. Pour plus de détails sur la configuration du réseau SNA pour le serveur TN5250, consultez le *Guide d'utilisation*.

Équilibrage de charge des serveurs TN5250

Communications Server prend également en charge l'équilibrage de charge des clients TN5250 sur plusieurs serveurs TN5250. Pour plus de détails, reportez-vous à la section «Planification de l'équilibrage de charge», à la page 147.

Planification de la sécurité SSL

Vous pouvez utiliser la fonction de sécurité SSL (Secure Sockets Layer) sur les connexions entre les clients TN et le serveur TN3270E ou TN5250. Cette sécurité utilise SSL version 3 pour fournir le chiffrement de données et l'authentification du serveur à l'aide de certificats signés.

Vous pouvez configurer des ports spécifiques prenant en charge la sécurité SSL. Si une sécurité est définie, le serveur doit disposer d'un certificat authentifié fourni par une autorité de certification (AC). Communications Server fournit un utilitaire qui génère et gère les clés et les certificats utilisés par SSL version 3.

Le présent chapitre donne un aperçu de la planification de la sécurité SSL (Secure Sockets Layer) qui est fournie en option lors de la configuration des serveurs TN3270E et TN5250.

Fonctionnement de la sécurité SSL

SSL (Secure Sockets Layer) est un protocole conforme aux normes de l'industrie, qui utilise la technologie de chiffrement à clé symétrique et à clé publique. Le chiffrement à clé symétrique utilise la même clé pour le chiffrement et le déchiffrement des messages. Le chiffrement à clé publique utilise une paire de clés, une clé publique et une clé privée. La clé publique de chaque serveur est publiée et la clé privée est confidentielle. Pour envoyer un message sécurisé au serveur, le client chiffre le message à l'aide de la clé publique du serveur. Lorsque ce dernier reçoit le message, il le déchiffre à l'aide de la clé privée.

SSL fournit les trois services de sécurité de base suivants :

- Confidentialité des messages

  Ce service est effectué grâce à une combinaison de chiffrements à clé publique et à clé symétrique. L'ensemble du trafic entre un client SSL et un serveur SSL est chiffré à l'aide d'une clé et d'un algorithme négocié lors de la configuration de session.

- Intégrité des messages

  Ce service assure que le trafic de session SSL ne change pas de chemin jusqu'à sa destination finale. SSL utilise une combinaison de clés publiques/privées et des fonctions de hachage pour assurer l'intégrité des messages.

- Authentification

  Il s'agit du processus permettant au client et au serveur de se convaincre de leurs identités. Ces dernières sont codées dans des certificats à clé publique. Un certificat à clé publique contient les composants suivants :

  – Nom distinctif de l'objet

  – Nom distinctif de l'émetteur

  – Clé publique de l'objet

  – Signature de l'émetteur

  – Période de validité

– Numéro de série

Remarque : Communications Server prend en charge l'authentification côté serveur. Seul le serveur sécurisé requiert une authentification d'AC pour permettre l'établissement d'une connexion TN3270E ou TN5250.

Support SSL de Communications

Communications Server prend en charge les composants suivants de la sécurité SSL :

- Sessions SSL sécurisées entre le serveur TN3270E et les clients TN3270 et TN3270E prenant en charge SSL version 3.
- Sessions SSL sécurisées entre le serveur TN5250 et les clients TN5250 et TN3270E prenant en charge SSL version 3.
- SSL version 3
- Confidentialité et intégrité des messages
- Authentification côté serveur

Configuration de la sécurité SSL

Lors de la configuration des serveurs TN3270E et TN5250, vous indiquez les ports qui utilisent la sécurité SSL pour leurs connexions. Pour plus de détails sur la confi-

Utilitaire Key-Ring Management

L'utilitaire **Key-Ring Management** de Communications Server permet de créer, de gérer et de stocker des clés publiques/privées et des certificats requis pour les communications SSL entre Communications Server et le client. Avant de commencer à configurer les communications SSL, vous devez ouvrir le fichier de base de données de clés de Communications Server. Pour ouvrir le fichier, effectuez les étapes suivantes :

1. Sélectionnez **Fichier de base de données de clés** dans le menu principal, puis **Ouvrir** pour ouvrir une base de données de clés existante.
2. Dans la fenêtre **Ouvrir**, choisissez le sous-répertoire **private** du répertoire d'installation du produit (par exemple, C:\IBMCS\PRIVATE).
3. Choisissez **ibmcs.kdb** comme base de données de clés .
4. À l'invite, entrez votre mot de passe.

   Remarque : **ibmcs** est le mot de passe par défaut. Pour des raisons de sécurité, vous ***devez*** modifier le mot de passe avant d'effectuer une des tâches de **Key-Ring Management**.

Modification du mot de passe

Pour modifier le mot de passe de la base de données en cours, procédez comme suit :

1. Sélectionnez **Fichier de base de données de clés** dans le menu, puis **Modifier le mot de passe** pour changer le mot de passe de la base de données de clés en cours. La boîte de dialogue **Modifier le mot de passe** s'affiche.
2. Entrez le nouveau mot de passe que vous voulez utiliser.
3. Tapez-le de nouveau pour vérifier.
4. Si vous voulez affecter une date d'expiration au mot de passe, cliquez sur **Définir date d'expiration**. Pour des raisons de sécurité, il est préférable que le mot de passe ait une date d'expiration.
5. Si vous voulez que le mot de passe ait une date d'expiration, précisez le délai (nombre de jours) d'expiration.
6. Cliquez sur **Stocker le mot de passe sur le système** pour stocker le mot de passe de la base de données en cours.

Configuration de SSL à l'aide d'une AC sécurisée connue

Les procédures décrites dans cette section permettent de configurer la sécurité SSL à l'aide d'un certificat émis par une AC connue. Les certificats signataires d'AC suivants sont déjà stockés dans la base de données de clés et indiqués en tant que certificats sécurisés :

- Integrion Certification Authority Root
- IBM World Registry Certification Authority
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA

- CA de serveur sécurisé Thawte Server CA RSA (également disponible auprès de VeriSign)
- AC principale publique de classe 4 VeriSign
- AC principale publique de classe 3 VeriSign
- AC principale publique de classe 2 VeriSign
- AC principale publique de classe 1 VeriSign

Pour configurer la sécurité SSL à l'aide d'une AC connue, procédez comme suit :

- Créez une clé et une demande de certificat.
- Soumettez la demande de certificat à l'AC.
- Procurez-vous un certificat et stockez-le dans la base de données de clés du serveur.

Création d'une clé et d'une demande de certificat

Pour créer les clés publique/privée et une demande de certificat, effectuez les étapes suivantes de l'utilitaire **Key-Ring Management** :

1. Sélectionnez **Demandes de certificats personnels** dans la liste déroulante du menu principal, puis cliquez sur **Nouveau** pour créer une paire de clés et une demande de certificat. La boîte de dialogue **Créer une clé et une demande de certificat** s'affiche.
2. Entrez le nom (label) servant à identifier la clé et le certificat dans la base de données.
3. Tapez le chiffre correspondant à la taille que vous voulez utiliser pour la clé. Plus la taille est importante, plus la sécurité est grande, mais cela nécessite davantage de traitements de la part du client et du serveur pour établir une connexion.
4. Entrez le nom d'hôte TCP/IP du serveur de communications en tant que nom courant (par exemple, wtr05306.raleigh.ibm.com).
5. Entrez un nom de société.
6. Entrez le nom d'un service de cette société (facultatif).
7. Entrez le nom d'une ville ou d'une localité (facultatif).
8. Entrez le nom d'un département (facultatif).
9. Entrez un code postal (facultatif).
10. Entrez le code d'un pays. Vous devez taper au moins deux caractères (FR, par exemple).
11. Entrez le nom d'un fichier de demande de certificat, ou utilisez le nom de fichier par défaut.

Lorsque vous cliquez sur **OK**, les informations que vous avez indiquées sont traitées et les deux fichiers suivants sont créés :

ibmcs.rdb Fichier de clé privée

certreq.arm Il s'agit du nom par défaut ou du nom que vous avez affecté au fichier de demande de certificat. Ce dernier est un fichier de type PKCS 10 au format 64 protégé.

N'essayez pas d'éditer ou de déplacer ces fichiers. Lorsque vous essayez d'entrer le certificat dans la base de données de clés , si le fichier **ibmcs.rdb** est introuvable ou endommagé, soumettez de nouveau la demande de certificat à l'AC.

Soumission d'une demande de certificat

Lancez un afficheur Web, puis accédez à la page Web de l'AC. Suivez les instructions concernant la soumission des demandes de certificat. La liste suivante fournit les URL de certaines AC connues :

- VeriSign : **http://www.verisign.com/**
- Thawte : **http://www.thawte.com/**

En fonction de l'AC que vous choisissez, envoyez par courrier électronique la demande de certificat générée à l'aide de l'utilitaire **Key-Ring Management**, ou envoyez la demande de certificat avec le formulaire ou le fichier fournis par l'AC.

Après avoir soumis une demande de certificat à une AC, vous pouvez activer la sécurité SSL en créant et stockant un certificat auto-signé. Ce certificat auto-signé doit être utilisé uniquement pour les tests contrôlés. Pour plus de détails, reportez-vous à la section «Création d'un certificat auto-signé», à la page 145.

Stockage d'un certificat dans la base de données de clés

Lorsque vous recevez un certificat d'une AC, utilisez **Key-Ring Management** pour placer le certificat dans le fichier de base de données de clés (**ibmcs.kdb**), qui se trouve sur le serveur.

1. Sélectionnez **Certificats personnels** dans la liste déroulante de l'utilitaire **Key-Ring Management**, puis cliquez sur **Recevoir** pour recevoir la paire de clés et la demande de certificat. La boîte de dialogue **Recevoir un certificat à partir d'un fichier** s'affiche.
2. Assurez-vous que les données sont du type **Données ASCII protégées en base 64** (format 64 protégé).
3. Entrez le nom de fichier du certificat.
4. Entrez l'emplacement (chemin d'accès) du certificat. Cliquez sur **OK**. Le certificat que vous venez de stocker est le premier élément qui s'affiche.
5. Mettez-le en évidence, puis cliquez sur **Visualiser/Editer**. La boîte de dialogue **Données de clés** apparaît.
6. Cliquez sur **Définir le certificat par défaut** pour définir la clé sélectionnée comme clé par défaut.

Configuration de SSL à l'aide d'une AC inconnue

Pour configurer la sécurité SSL à l'aide d'une AC inconnue (non encore définie dans la base de données), procédez comme suit :

- Créez une clé et une demande de certificat.
- Soumettez la demande de certificat à l'AC.
- Procurez-vous le certificat racine de l'AC ainsi que votre certificat et stockez-les dans la base de données de clés du serveur.

Création d'une clé et d'une demande de certificat

Pour créer les clés publique/privée et une demande de certificat, effectuez les étapes suivantes de l'utilitaire **Key-Ring Management** :

1. Sélectionnez **Demandes de certificats personnels** dans la liste déroulante du menu principal, puis cliquez sur **Nouveau** pour créer une paire de clés et une demande de certificat. La boîte de dialogue **Créer une clé et une demande de certificat** s'affiche.
2. Entrez le nom (label) servant à identifier la clé et le certificat dans la base de données.
3. Tapez le chiffre correspondant à la taille que vous voulez utiliser pour la clé. Plus la taille est importante, plus la sécurité est grande, mais cela nécessite davantage de traitements de la part du client et du serveur pour établir une connexion.
4. Entrez le nom d'hôte TCP/IP du serveur de communications en tant que nom courant (par exemple, wtr05306.raleigh.ibm.com).
5. Entrez un nom de société.
6. Entrez le nom d'un service de cette société (facultatif).
7. Entrez le nom d'une ville ou d'une localité (facultatif).
8. Entrez le nom d'un département (facultatif).
9. Entrez un code postal (facultatif).
10. Entrez le code d'un pays. Vous devez taper au moins deux caractères (FR, par exemple).
11. Entrez le nom d'un fichier de demande de certificat, ou utilisez le nom de fichier par défaut.

Lorsque vous cliquez sur **OK**, les informations que vous avez indiquées sont traitées et les deux fichiers suivants sont créés :

ibmcs.rdb Fichier de clé privée

certreq.arm Il s'agit du nom par défaut ou du nom que vous avez affecté au fichier de demande de certificat. Ce dernier est un fichier de type PKCS 10 au format 64 protégé.

N'essayez pas d'éditer ou de déplacer ces fichiers. Lorsque vous essayez d'entrer le certificat dans la base de données de clés , si le fichier **ibmcs.rdb** est introuvable ou endommagé, soumettez de nouveau la demande de certificat à l'AC.

Soumission d'une demande de certificat

Suivez les procédures de l'AC inconnue pour soumettre la demande de certificat.

En fonction de l'AC que vous choisissez, envoyez par courrier électronique la demande de certificat générée à l'aide de l'utilitaire **Key-Ring Management**, ou envoyez la demande de certificat avec le formulaire ou le fichier fournis par l'AC.

Après avoir soumis une demande de certificat à une AC, vous pouvez activer la sécurité SSL en créant et stockant un certificat auto-signé. Ce certificat auto-signé doit être utilisé uniquement pour les tests contrôlés. Pour plus de détails, reportez-vous à la section «Création d'un certificat auto-signé», à la page 145.

Stockage d'un certificat dans la base de données de clés

Lorsque vous recevez un certificat d'une AC, contactez cette dernière pour obtenir le certificat racine de l'AC. Vous devez stocker le certificat racine de l'AC dans la base de données de clés avant de stocker le certificat demandé. Le certificat racine de l'AC sert à valider le certificat demandé. Utilisez **Key-Ring Management** pour stocker le certificat racine de l'AC.

1. Sélectionnez **Certificats signataires** dans la liste déroulante, puis cliquez sur **Recevoir** pour recevoir la paire de clés et la demande de certificat. La boîte de dialogue **Recevoir un certificat à partir d'un fichier** s'affiche.
2. Assurez-vous que les données sont du type **Données ASCII protégées en base 64** (format 64 protégé).
3. Entrez le nom de fichier du certificat.
4. Entrez l'emplacement (chemin d'accès) du certificat. Cliquez sur **OK**. Le fichier est défini en tant que ***sécurisé*** et stocké.

Lorsque vous recevez un certificat d'une AC, utilisez **Key-Ring Management** pour placer le certificat dans le fichier de base de données de clés (**ibmcs.kdb**), qui se trouve sur le serveur.

1. Sélectionnez **Certificats personnels** dans la liste déroulante du menu principal, puis cliquez sur **Recevoir** pour recevoir la paire de clés et la demande de certificat. La boîte de dialogue **Recevoir un certificat à partir d'un fichier** s'affiche.
2. Assurez-vous que les données sont du type **Données ASCII protégées en base 64** (format 64 protégé).
3. Entrez le nom de fichier du certificat.
4. Entrez l'emplacement (chemin d'accès) du certificat. Cliquez sur **OK**. Le certificat que vous venez de stocker est le premier élément qui s'affiche.
5. Mettez-le en évidence, puis cliquez sur **Visualiser/Editer**. La boîte de dialogue **Données de clés** apparaît.
6. Cliquez sur **Définir le certificat par défaut** pour définir la clé sélectionnée comme clé par défaut.

Création d'un certificat auto-signé

Il faut généralement attendre deux à trois semaines avant de recevoir un certificat provenant d'une AC sécurisée connue. En attendant de recevoir le certificat de serveur public, vous pouvez créer un certificat auto-signé afin d'établir des sessions SSL entre les clients et le serveur. Ce certificat auto-signé doit être utilisé uniquement pour les tests contrôlés. Pour que votre site bénéficie d'une sécurité adéquate, il est fortement recommandé de ne pas utiliser de certificat auto-signé dans un environnement de production. Pour configurer votre site de sorte que celui-ci utilise un certificat auto-signé, procédez, à l'aide de l'utilitaire **Key-Ring Management**, comme suit :

1. Sélectionnez **Nouveau certificat auto-signé** dans l'option de menu **Créer** pour créer un certificat auto-signé. La boîte de dialogue **Créer un certificat auto-signé** apparaît.

2. Entrez le nom (label) servant à identifier la clé et le certificat dans la base de données. Sélectionnez **X509 V3** en tant que version du certificat.
3. Tapez le chiffre correspondant à la taille que vous voulez utiliser pour la clé. Plus la taille est importante, plus la sécurité est grande, mais cela nécessite davantage de traitements de la part du client et du serveur pour établir une connexion.
4. Entrez le nom d'hôte TCP/IP du serveur de communications en tant que nom courant (par exemple, wtr05306.raleigh.ibm.com).
5. Entrez un nom de société.
6. Entrez le nom d'un service de cette société (facultatif).
7. Entrez le nom d'une ville ou d'une localité (facultatif).
8. Entrez le nom d'un département (facultatif).
9. Entrez un code postal (facultatif).
10. Entrez le code d'un pays. Vous devez taper au moins deux caractères (FR, par exemple).
11. Entrez le nombre de jours pendant lesquels le certificat auto-signé sera valide.
12. Cliquez sur **OK**.
13. Cliquez sur **Oui** pour définir la clé sélectionnée comme clé par défaut dans la base de données de clés.

Si vous utilisez IBM eNetwork Host On-Demand ou tout autre client SSL nécessitant le certificat auto-signé désigné procédez, à l'aide de l'utilitaire **Key-Ring Management**, comme suit :

1. Sélectionnez **Certificats personnels** dans la liste déroulante, mettez votre certificat auto-signé en évidence, puis cliquez sur **Extraire un certificat**. La boîte de dialogue **Extraire un certificat vers un fichier** s'affiche.
2. Sélectionnez **Données DER binaires** comme type de données.
3. Entrez le nom de fichier du certificat. L'extension du fichier doit être du type **der** (par exemple, ibmcs.crt).).
4. Entrez l'emplacement (chemin d'accès) du certificat.
5. Cliquez sur **OK**.

Le fichier de certificat doit être fourni à tous les clients autorisés à se connecter au serveur. Pour les instructions concernant le stockage du certificat auto-signé en tant que certificat racine d'AC dans le fichier de classe ou la base de données de clés du client, consultez la documentation du client.

Planification de l'équilibrage de charge

Le présent chapitre décrit la planification de l'équilibrage de charge relatif aux LU dépendantes et aux LU 6.2.

Équilibrage de charge des LU dépendantes

L'équilibrage de charge permet d'équilibrer les sessions hôte dépendantes sur l'ensemble des serveurs. Il est pris en charge pour les applications API LUx via des clients API SNA et des émulateurs 3270 et TN3270.

Lorsque Communications Server répond aux demandes des clients, il trie, en fonction de la charge, les serveurs qui prennent en charge le groupe demandé.

La charge des LU dépendantes représente un pourcentage de ressources accessibles à partir d'un serveur particulier.
Le pourcentage de charge est calculé en divisant le nombre de connexions d'application actives par le nombre total de LU (0 à 3) disponibles.

Vous pouvez modifier la charge calculée, en indiquant un facteur de charge LU 0 à 3 (facteur de charge de session hôte) pour compenser les écarts entre deux serveurs, par exemple, la mémoire disponible, la vitesse du processeur et l'utilisation de l'unité centrale. Vous pouvez également utiliser le facteur de charge LU 0 à 3 pour équilibrer les charges entre les serveurs Communications Server et Novell IntranetWare pour SAA.

Remarques :

1. Les serveurs participant à l'équilibrage de charge sont déterminés par leur appartenance au groupe de LU et au secteur. Tous les serveurs Communications Server dont les LU figurent dans des groupes du même nom font l'objet d'un équilibrage de charge.
2. Les clients utilisant le protocole TCP/IP peuvent participer à l'équilibrage de charge. Cependant, les clients TCP/IP peuvent équilibrer la charge uniquement entre des serveurs IBM Communications Server. L'équilibrage de charge est déterminé par des secteurs configurés.

Dans Communications Server, si des groupes de LU ont le même nom sur différents serveurs, ils fonctionnent comme un seul et même groupe pour l'équilibrage de charge. Lorsque vous affectez des LU à un groupe de LU, sélectionnez une liaison hôte sur un serveur, puis affectez les LU de la liaison hôte sélectionnée au groupe de LU. Il n'est pas nécessaire que ces LU soient du même type. Le groupe ainsi obtenu peut contenir des LU provenant de plusieurs liaisons.

Équilibrage de charge des LU 6.2

L'équilibrage de charge vous permet d'équilibrer des sessions LU 6.2 indépendantes en les répartissant sur plusieurs serveurs. Il est pris en charge pour les applications API APPC via des clients API SNA et des émulateurs TN5250.

La charge des LU 6.2 représente un pourcentage de ressources accessibles à partir d'un serveur particulier.

Le pourcentage de charge est calculé en divisant le nombre total des conversations sur toutes les LU locales d'un serveur particulier par le nombre maximal cumulé des sessions de toutes les LU locales. Ce nombre correspond au nombre maximal de sessions LU 6.2 indiqué lors de la configuration. S'il a pour valeur zéro (0), c'est-à-dire aucune limite de session, le nombre maximal par défaut des sessions de LU locales de 512 par LU locale est utilisé lors du calcul de la charge. Ce nombre par défaut peut également être indiqué lors de la configuration.

Vous pouvez modifier la charge calculée, en indiquant un facteur de charge LU 6.2 (facteur de charge de session APPC) pour compenser les écarts entre deux serveurs, par exemple, la mémoire disponible, la vitesse du processeur et l'utilisation de l'unité centrale. Vous pouvez également utiliser le facteur de charge LU 6.2 pour équilibrer les charges entre les serveurs Communications Server et Novell IntranetWare pour SAA.

Remarque : Les clients utilisant le protocole TCP/IP peuvent participer à l'équilibrage de charge LU 6.2.

Planification des secteurs TCP/IP

Un ***secteur*** correspond à un paramètre servant à contrôler et à gérer l'accès des clients TCP/IP aux serveurs d'un réseau. Il est identique au secteur SLP (Service Location Protocol) référencé dans le document RFC 2165. Le protocole SLP est utilisé par Communications Server pour mettre en œuvre un équilibrage de charge basé sur TCP/IP.

Le secteur de contrôle fourni est nécessaire pour les deux raisons suivantes :

- Au fur et à mesure de l'évolution de votre réseau, du nombre des clients et du nombre des serveurs, il est nécessaire de partitionner l'accès du nombre croissant des clients à ces serveurs, afin de réduire le trafic global sur le réseau.
- Le secteur de contrôle permet aux administrateurs d'organiser les utilisateurs et les serveurs en groupes administratifs.

Les valeurs de secteur sont définies par l'administrateur du réseau. Elles peuvent représenter n'importe quelle entité. En général, elles s'alignent sur des liaisons départementales, géographiques ou organisationnelles.

Une fois configurés, les clients sont en mesure d'accéder au réseau SNA par le biais de serveurs configurés avec le même secteur ou non associés à aucun secteur (services ou serveurs ***non sectorisés***).

Remarque : Si un serveur est configuré comme étant non sectorisé, il répond aux demandes SLP sectorisées **et** non sectorisées. Si le client API SNA est configuré pour se connecter à des serveurs non sectorisés, seuls ces derniers envoient une réponse.

Secteurs et sécurité du serveur client

Communications Server permet aux clients Novell IntranetWare pour SAA d'utiliser la sécurité de domaine Windows NT pour authentifier la connexion du client au serveur sans que l'ID utilisateur et le mot de passe soient ré-entrés. Le client doit faire partie d'un domaine Windows NT en participant dans un domaine de Communications Server ou à l'aide d'une connexion locale à un ID utilisateur et un ot de passe synchronisés.

Les utilisateurs autorisés du serveur client sont maintenus dans le groupe local IBMCSAPI qui est situé directement sur Communications Server ou sur le contrôleur de domaine dans lequel Communications Server participe. Ce groupe d'utilisateurs est créé lors de l'installation et peut être administré à l'aide de l'application Gestionnaire d'utilisateurs Windows NT.

Les utilisateurs du client Novell IntranetWare pour SAA se trouvant à l'extérieur du domaine Windows NT doivent dupliquer l'ID utilisateur et le mot de passe sur l'ensemble des serveurs configurés avec le même secteur.

Emplacement de configuration des secteurs

Un ou plusieurs secteurs sont affectés à chaque serveur via l'application **Configuration du nœud**. Les clients utilisant ces serveurs doivent être configurés pour se connecter aux serveurs d'un seul secteur spécifique ou à des serveurs non sectorisés. Pour plus de détails sur la configuration des clients, consultez le manuel *Client/Server Communications Programming*.

Mode de rattachement d'un secteur au SLP

Le secteur de Communications Server est directement rattaché au secteur SLP (Service Location Protocol). Par conséquent, il se peut que les agents de répertoire SLP résident dans le réseau qui prend en charge les secteurs configurés de Communications Server. Si vous envisagez d'autoriser des clients à localiser les services de Communications Server en fonction des secteurs, prenez en considération la façon dont un secteur se rattache à l'ensemble du réseau. Si un réseau dans lequel des secteurs sont utilisés contient des services non sectorisés, ces derniers remplissent les conditions requises pour répondre aux demandes sectorisées, ce qui peut éventuellement représenter une lourde charge pour les agents de service et de répertoire qui prennent en charge les services non sectorisés.

Remarque : Si le client API SNA est configuré pour se connecter à des serveurs non sectorisés, seuls ces derniers envoient une réponse.

Si des agents de répertoire doivent être utilisés dans le réseau du site (pour une extension), ils doivent être configurés de sorte qu'ils traitent les mêmes secteurs que ceux configurés pour Communications Server. En plus, si des services non sectorisés doivent être utilisés dans des réseaux comportant des agents de répertoire, au moins un agent de répertoire non sectorisé doit être configuré.

Communications Server contient un agent de service SLP qui est installé sur tous les serveurs où Communications Server est installé. Aucun autre support SLP ne doit être installé sur le réseau pour le bon fonctionnement de l'équilibrage de charge TCP/IP et de la fonction de découverte de Communications Server.

Suivi de la charge en cours

Vous pouvez suivre la charge en cours des LU dépendantes et des LU 6.2 à l'aide du Moniteur de performances de Windows NT. Ce dernier peut être lancé à partir de l'option **Administrative Tools (Common)** du menu **Programs**.

Dans l'écran du moniteur de performances, sélectionnez **Add to Chart** à partir du menu déroulant **Edit**. Dans la zone **Object**, sélectionnez **IBM SNA Load Balancing**. Voici les deux compteurs répertoriés :

LU0/LU3 Load Ce compteur permet de suivre la charge des LU dépendantes.

LU6.2 Load Ce compteur permet de suivre la charge des LU 6.2.

Les résultats du suivi de charge peuvent être sauvegardés à titre de référence.

Planification des connexions hôte de secours

Pour les environnements dans lesquels il est peut-être important de fournit des connexions hôte de secours aux connexions principales utilisées par les sessions d'émulation de postes de travail, Communications Serveur offre des options qui permettent de configurer des connexions hôte activées en cas de défaillance. Ces options sont fonction du niveau de secours souhaité :

- Pour permettre la sauvegarde complète du système entre les nœuds de serveur prenant en charge des sessions d'émulation de poste de travail IP ou IPX de réseau local, installez la fonction de secours automatique dans votre environnement.
- Pour permettre la sauvegarde complète du système entre les nœuds de serveur prenant en charge des sessions autres que les sessions d'émulation de poste de travail IP ou IPX de réseau local, n'installez pas la fonction de secours automatique dans votre environnement. Configurez une installation Communications Server en double sur le système de secours.
- Pour assurer une sauvegarde dans un nœud de serveur, n'utilisez pas la fonction de secours automatique. Utilisez les options courantes des définitions de connexion de votre environnement de secours.

Ces options sont décrites dans les sections suivantes.

Planification des connexions de secours entre les serveurs utilisant la fonction de secours automatique

Communications Server permet de configurer des liaisons hôte de sorte que celles-ci s'activent automatiquement en cas de défaillance au niveau d'un serveur critique. Les connexions configurées à un hôte peuvent continuer de fonctionner grâce à l'activation de connexions secondaires sur un serveur de secours. Il s'agit de la fonction de secours automatique.

Pour l'utilisateur d'une session d'émulation de poste de travail avec une machine hôte dont la connexion initiale échoue en raison d'une défaillance de Communications Server, la fonction de secours automatique permet une tentative de réactivation de la connexion à la machine hôte, au moyen d'un routage automatique via un serveur Communications Server secondaire. Le serveur initial fournissant la connexion est désigné par ***serveur critique***. Le serveur secondaire fournissant une connexion à la machine hôte à la suite de la défaillance du serveur critique est désigné par ***serveur de secours***. Ce dernier fournit des connexions qui démarrent automatiquement une fois qu'une défaillance est détectée au niveau d'un serveur critique ; les frais de licence afférents à la connectivité hôte du serveur critique sont automatiquement gérés sur le serveur de secours.

Un serveur peut être à la fois un serveur critique et un serveur de secours. Les serveurs peuvent s'assurer mutuellement des fonctions de secours.

La fonction de secours automatique fournit un support de serveur de secours pour les sessions d'émulation IP ou IPX de réseau local. Il n'en fournit aucun pour l'environnement SNA.

Dans la figure 38, à la page 152, le serveur de secours est configuré avec une connexion de secours complète pour HOSTCON1, qui assure la connectivité hôte principale sur le serveur critique. Les liaisons indiquées en pointillé entre le serveur de secours et les clients d'émulation de poste de travail ne sont pas actives lors du fonctionnement du serveur critique.

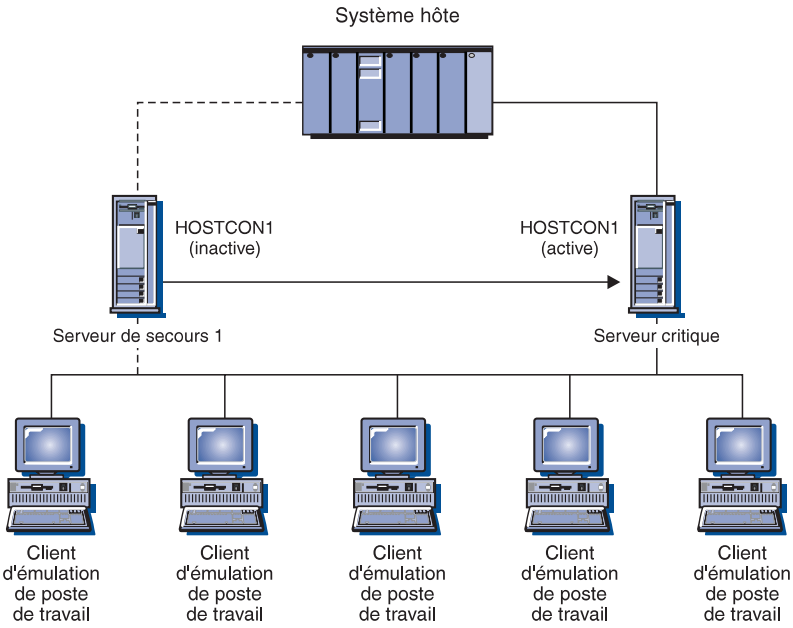
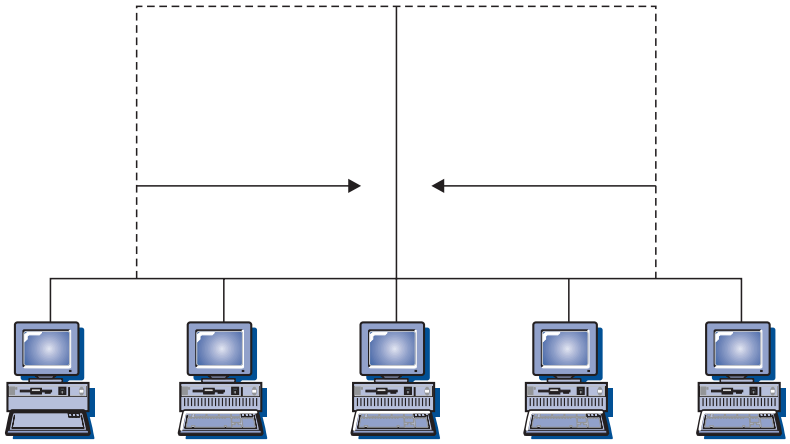


Figure 38. Serveur critique doté d'un seul serveur de secours

Dans la figure 39, à la page 153, chaque serveur de secours est configuré avec une connexion de secours partielle pour HOSTCON1, qui assure la connectivité hôte principale sur le serveur critique. La combinaison des deux serveurs de secours assure un secours complet pour HOSTCON1. Les liaisons indiquées en pointillé entre les serveurs de secours et les clients d'émulation de poste de travail ne sont pas actives lors du fonctionnement du serveur critique.



Utilisation d'un serveur de production

Un ***serveur de production*** est un Communications Server qui répond à vos besoins quotidiens en matière de communication. Cet environnement configure Communications Server avec des connexions hôte qui sont activées en dehors d'un cas de défaillance du serveur critique. L'activation et l'utilisation de ce type de connexions requièrent l'acquisition de licences appropriées. Vous ne pouvez pas installer les mêmes licences Communications Server sur plusieurs serveurs. Pour installer Communications Server en tant que serveur de production sur plusieurs serveurs, vous devez vous procurer un autre module Communications Server par installation de serveur supplémentaire.

Lorsque vous utilisez un serveur Communications Server à la fois comme serveur de production et comme serveur de secours, aucune condition de licence particulière ne s'applique. Vous installez Communications Server et les licences que vous avez acquises pour utiliser Communications Server comme serveur de production.

Le rôle de Communications Server comme serveur de secours ne requiert aucune licence autre que la licence de base acquise pour les serveurs critiques qu'il doit contrôler. Aucune condition de licence particulière n'est requise sur le serveur de secours.

Lorsque ce dernier détecte une défaillance au niveau d'un serveur critique, il active automatiquement les connexions configurées pour ce serveur critique, puis ajuste les licences du serveur de secours en fonction de celles en vigueur pour le serveur critique. Communications Server gère l'accord de licence de secours automatique sans votre intervention.

Cependant, si les connexions configurées pour le serveur critique ont déjà été activées en dehors d'un cas de défaillance de serveur critique, les licences du serveur critique ne sont pas ajustées et une licence distincte est requise sur le serveur de secours.

Utilisation d'un serveur spécifique

Un serveur de secours ***spécifique*** ne fonctionne pas comme serveur de production et n'active une connexion qu'en cas de défaillance du serveur critique. Aucune connexion ne peut être activée sur ce serveur au démarrage ou manuellement. Son rôle consiste à surveiller un ou plusieurs serveurs critiques.

Un serveur de secours spécifique ne requiert aucune licence autre que la licence de base acquise pour les serveurs critiques qu'il doit contrôler. Communications Server gère l'accord de licence de secours automatique sans votre intervention.

Planification de l'environnement de secours automatique complet

Les cas d'utilisation du secours automatique impliquent des scénarios de fonctionnement normal de Communications Server pour la prise en charge des clients d'émulation de réseau local via IP ou IPX, à l'aide de quelques opérations de secours automatique spécifiques.

Pour configurer un environnement de secours automatique, les deux dépendances de base suivantes sont disponibles :

- Au moins deux serveurs de communication doivent être configurés pour fournir des connexions compatibles à une machine hôte. Le serveur de secours doit être configuré avec une configuration de serveur critique fournissant la connexion principale à la machine hôte.
- Le logiciel de client émulateur de poste de travail permettant une connexion via le serveur pour fournir aux utilisateurs des sessions d'émulation sur la machine hôte doit prendre en charge d'autres moyens de routage vers le serveur de secours en cas de défaillance du serveur critique.

Il se peut que certains clients émulateurs n'assurent pas le routage secondaire. La planification d'un environnement de secours automatique requiert une évaluation minutieuse du logiciel d'émulation et du type de connectivité utilisé entre le client et le serveur. Voici quelques options de routage secondaire :k

- **Substitution à chaud** - Il s'agit, sur un client émulateur, d'un support de configuration de plusieurs serveurs à contacter, dans un ordre particulier, afin d'établir une connexion via le serveur à la machine hôte pour une session d'émulation. La fonction de substitution à chaud vous permet de configurer le serveur de secours qui doit être contacté lorsque les tentatives de connexion au serveur critique n'aboutissent pas. En cas de défaillance du serveur critique et lors de l'activation de ressources sur le serveur de secours, le client émulateur contacte le serveur de secours via lequel il établit ensuite un chemin secondaire pour la connexion à la machine hôte.

- **Groupes de LU** - Il s'agit, sur un client émulateur, d'un support d'établissement dynamique de la connexion à la machine hôte pour une session d'émulation via le serveur qui répond actuellement aux demandes de LU disponibles dans un groupe désigné. Le support de groupes de LU permet au serveur de secours et aux serveurs critiques de fournir des LU au même groupe. Le serveur de secours est défini à l'origine mais n'est pas actif. En cas de défaillance du serveur critique et lors de l'activation de ressources sur le serveur de secours, ce dernier répond aux demandes de LU de groupe du client émulateur via lequel il établit ensuite un chemin secondaire aux fins de connexion à la machine hôte. Les groupes de LU comportent les types suivants du support client correspondant :
  - Support pré-SLP : Avant le support de SLP de Communications Server, l'accès client des groupes de LU était aléatoire ou dans un ordre de serveur spécifique.
  - Support SLP : Le support SLP de Communications Server fournit l'accès client des groupes de LU pour équilibrer la charge de session à travers les serveurs qui contribuent au groupe.
- **Sessions d'émulation multiples** - Il s'agit du support de configuration de plusieurs sessions d'émulation dans un client émulateur, permettant à l'utilisateur de configurer des sessions distinctes à l'aide du serveur de secours et des serveurs critiques aux fins de connexion à la machine hôte. L'utilisation de plusieurs sessions d'émulation n'est pas aussi facile que la substitution à chaud ou le support de groupe de LU car elle requiert l'intervention de l'utilisateur de l'émulateur dans le routage secondaire lorsqu'un incident se produit. En cas de défai rsion eur Ø connexide du serve s crit , de l'utilisate° } ro 'utieær

Configuration d'un environnement de secours automatique

Pour configurer un environnement de secours automatique, effectuez les étapes suivantes :

1. **Configuration du serveur critique :** Le serveur critique est configuré sans aucune configuration liée à la fonction de secours automatique. Configurez la connectivité hôte de sorte qu'elle concorde avec l'option de routage secondaire utilisée avec les clients émulateurs.
2. **Configuration du serveur de secours :** Cette configuration implique les deux principaux concepts suivants :
   a. La configuration de la connectivité hôte sur le serveur de secours est similaire à celle du serveur critique à ceci près que les connexions hôte sont configurées pour être activées manuellement.
   b. Une configuration de serveur critique sur le serveur de secours, qui permet de définir les connexions hôte démarrées en cas de défaillance du serveur critique est détectée.
3. **Configuration des clients émulateurs :** Les clients émulateurs de poste de travail sont configurés de sorte que l'option de routage secondaire concorde avec la connectivité fournie par les serveurs.
4. **Démarrage du serveur critique et des nœuds de serveur de secours :** Démarrez les nœuds comme vous le faites normalement. L'application **Fonctionnement du nœud SNA** peut vérifier l'état de secours automatique du serveur critique et du serveur de secours.
5. **Défaillance du serveur critique :** En cas de défaillance du serveur critique, la reprise se déroule de la façon suivante :
   a. Le serveur de secours, l'hôte et le logiciel d'émulation du poste de travail du client détectent la défaillance à peu près en même temps.
   b. Les connexions définies dans la configuration du serveur critique sur le serveur de secours sont activées et une connexion à la machine hôte est établie.
   c. Le client émulateur de poste de travail établit une nouvelle session avec le serveur de secours. Ce dernier achemine des sessions vers la machine hôte via la connexion qui est activée sur le serveur de secours lors de la défaillance du serveur critique.
   d. Le poste de travail prend contact avec la machine hôte et affiche une invite d'ouverture de session destinée à l'utilisateur.
6. **Remise en fonction du serveur critique :** Lorsque le serveur critique est de nouveau actif, les nouvelles sessions d'émulation de poste de travail utilisent la connexion du serveur critique à l'hôte. Les sessions d'émulation de poste de travail existantes qui sont acheminées via le serveur de secours continuent de fonctionner jusqu'à la fermeture des sessions.

   Vous devez désactiver manuellement les connexions hôte du serveur de secours. Cette désactivation doit être effectuée pendant les heures creuses. Avant la désactivation des connexions, vous devez notifier les utilisateurs qui ont établi des sessions d'émulation de poste de travail avec le serveur de secours.

Planification des connexions de secours entre les serveurs sans la fonction de secours automatique

Dans la mesure où la fonction de secours automatique est limitée aux environnements qui prennent en charge les sessions d'émulation de poste de travail IP ou IPX de réseau local, elle ne peut pas être utilisée par certains environnements pour la connectivité de secours. La plupart des remarques relatives à la planification d'un environnement de secours sans la fonction de secours automatique sont similaires à celle d'un environnement de secours utilisant la fonction de secours automatique. Pour configurer un environnement de secours sans la fonction de secours automatique, effectuez les étapes suivantes :

1. Sur le serveur de secours, installez un module Communications Server acquis séparément et doté des licences appropriées pour les connexions hôte de secours au serveur principal.
2. Sur le serveur de secours, configurez des connexions hôte de secours à activer à la demande.
3. Configurez les émulateurs clients de poste de travail pour assurer un routage automatique vers les ressources du serveur de secours lors de la défaillance du serveur principal. Cependant, ce routage ne doit permettre l'accès au serveur de secours que si une défaillance du serveur principal est détectée.
4. Les deux nœuds sont démarrés mais seul le nœud principal dont les connexions en amont sont actives assure initialement une connectivité à l'hôte.
5. Lors de la défaillance du serveur principal, les clients émulateurs de poste de travail tentent les connexions suivantes via le serveur de secours. Les connexions hôte sur le serveur de secours sont activées.
6. La licence en double installée sur le serveur de secours permet aux clients précédemment acheminés via le serveur principal d'accéder au serveur de secours.
7. Lorsque le serveur principal est de nouveau actif, les connexions sur le serveur de secours sont désactivées manuellement.

Planification des connexions de secours sur un seul serveur

Vous ne pouvez pas utiliser la fonction de secours automatique pour fournir une connectivité de secours sur un seul serveur car cette fonction ne s'applique qu'aux environnements dotés de connexions de secours entre des serveurs. Cependant, certaines remarques relatives à la planification d'un environnement de secours sur un seul serveur sont similaires à celle d'un environnement de secours utilisant la fonction de secours automatique. Les différences sont récapitulées dans les étapes suivantes :

1. Sur le serveur qui sert de passerelle à l'hôte, configurez des connexions principale et de secours qui fournissent des LU au même groupe de LU cependant, la connexion de secours doit être configurée pour être activée à la demande.
2. Configurez les clients émulateurs de poste de travail de sorte qu'ils se connectent via le groupe de LU.
3. En cas de défaillance de la connexion principale ou lorsque les LU du groupe arrivent à épuisement, une tentative de connexion au groupe déclenche l'activation de la connexion de secours.

4. Lorsque le serveur principal est de nouveau actif, les connexions sur le serveur de secours sont désactivées manuellement.

Planification de X.25

Vous devez planifier la configuration X.25 avec soin. Il est nécessaire de prendre en considération les remarques suivantes :

- Pour utiliser un réseau de commutation de données par paquet (PSDN), vous devez demander un abonnement au réseau pour chaque ligne (liaison) requise. La mise à disposition d'une ligne risque de prendre un certain temps ; prenez donc contact bien à l'avance avec le fournisseur de réseau X.25.
- Pour plus de détails sur les fonctions disponibles sur le réseau X.25 et sur les fonctions requises, procurez-vous auprès du fournisseur de réseau un guide technique réseau.
- Rassemblez des informations sur les voies logiques qui sont requises pour les PVC et les SVC.
  - Jusqu'à 16 groupes de voies logiques peuvent être définis.
  - Le numéro du groupe peut être compris entre 0 et 15.
  - Le numéro de la voie logique dans le groupe peut être compris entre 0 et 255.

    La multiplication du numéro de groupe par 256 et l'ajout du numéro de voie logique donnent lieu à un numéro compris entre 0 et 4095, ce qui permet l'identification unique d'une voie logique. Cette combinaison est généralement désignée par numéro de voie logique.

    Remarques :

    1. Si vous indiquez CCITT 1984 ou 1988, le nombre maximal des voies logiques est égal à 4095.
    2. Si vous indiquez CCITT 1980, le nombre maximal des voies logiques est égal à 1024.
  - Les groupes de voies logiques peuvent être des groupes d'entrée uniquement (réservés aux appels provenant d'autres ETTD), de sortie uniquement (réservés aux appels à destination d'autres ETTD) ou bidirectionnels.
- Nombre de circuits virtuels requis pour SNA.
- Types de PVC requis.
- Combinaison des voies logiques d'entrée, de sortie et directionnels.
- Taille de paquet maximale requise et éléments pris en charge par le réseau X.25.
- Détails des fonctions X.25 facultatives utilisées par vos programmes d'application X.25.

  Les recommandations CCITT X.25 définissent un certain nombre de fonctions facultatives pouvant être prises en charge par votre réseau.

  Certaines fonctions comportent des paramètres qui peuvent être indiqués ou négociés par un programme d'application lors de l'établissement ou de la libération des appels à l'aide des zones de fonction des paquets de demande, d'acceptation et de libération d'appel.

La connexion X.25 peut être configurée pour la prise en charge des fonctions suivantes lors de l'établissement d'un appel :

- Groupe fermé d'utilisateurs
- Identification des utilisateurs du réseau
- Négociation de la taille des paquets et des fenêtres
- Appel en PCV

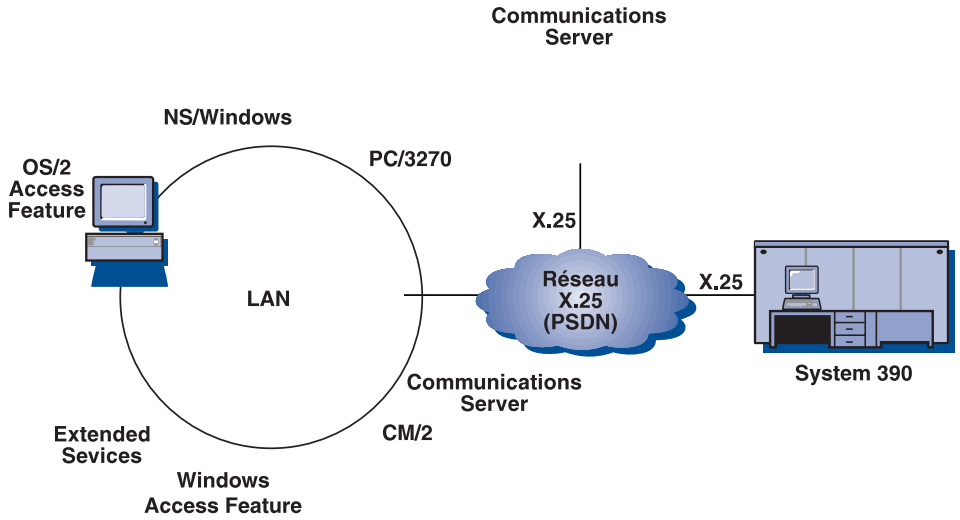
Définissez les fonctions lors de la configuration du DLC X.25.

- Détails des conditions spéciales applicables aux paramètres de trame et de paquet. Les valeurs par défaut de ces paramètres de configuration ont été choisies minutieusement de sorte qu'elles correspondent à la plupart des situations. Cependant, votre fournisseur de réseau peut imposer ou recommander certaines valeurs.

  Pour éviter des incidents, vos paramètres de configuration doivent correspondre à votre abonnement au réseau. Par exemple, si vous avez configuré 20 voies logiques SVC et que vous ne vous êtes abonné qu'à 10, l'ETCD détecte une condition d'erreur lors de la tentative d'utilisation de la onzième voie logique.

Connexions X.25 possibles

La figure 40 illustre comment un réseau X.25 peut fournir une connexion d'une passerelle SNA à un hôte.



Frais de réseau X.25

Les frais réels sont fonction des modes de facturation du fournisseur de réseau X.25 ; cependant, les frais sont généralement constitués de tout ou partie des éléments suivants :

- Frais d'installation

  Il s'agit de frais uniques facturés lors du premier abonnement au réseau X.25.

- Redevances de location périodiques

  Celles-ci dépendent des fonctions fournies par votre fournisseur de réseau. Par exemple, vous pouvez prévoir une redevance pour chaque fonction de réseau facultative à laquelle vous vous abonnez. Vous pouvez également prévoir une redevance pour chaque voie logique disponible. Le coût des PVC est généralement supérieur à celui des SVC car les premiers requièrent des ressources réseau spécifiques.

- Frais d'utilisation

  Ces frais sont fonction de la durée de connexion logique au réseau, sous réserve éventuellement d'une facturation minimale.

- Frais de volume

  Ces frais sont liés à la quantité de données transmises sur le réseau pendant une période de facturation.

Configuration de la connectivité hôte

Vous pouvez connecter les postes de travail exécutant Communications Server à des hôtes IBM 390 (y compris IBM 370) ou AS/400. La plupart des valeurs que vous indiquez pour la configuration de Communications Server sont également utilisées lors de la configuration de l'hôte. Le présent chapitre décrit le mappage entre les paramètres de configuration que vous indiquez lors de la configuration de Communications Server et les paramètres indiqués sur les hôtes. Il contient également des tableaux qui répertorient les paramètres permettant d'éliminer les paramètres courants de chaque macro à émettre entre Communications Server et l'hôte.

Remarque : La plupart des paramètres NCP émis à partir des macros LINE, PU et LU peuvent être indiqués dans la macro GROUP par soucis de lisibilité et de facilité de codification. Grâce à cette correspondance de paramètres, il n'est plus nécessaire d'entrer des paramètres courants dans chaque macro ultérieure et une annulation reste toutefois possible.

Anneau à jeton Ring NCP (NTRI) avec VTAM et Communications Server

Le tableau 7 compare les paramètres de l'hôte aux paramètres de Communications Server en ce qui concerne les connexions du réseau IBM Token-Ring.

Tableau 7. Références croisées des paramètres hôte/PC : Définition NTRI du réseau IBM Token-Ring

NTRI/NCP	Profil/paramètres Communications Server	Remarques
GROUP ECLTYPE = PHY	Type de DLC : Réseau local	
LINE LOCADDR	Configuration des connexions Réseau local **Adresse de destination**	La valeur définie pour ce paramètre sous Communications Server doit correspondre à l'adresse de la carte IBM Token-Ring Network du contrôleur hôte.

Token Ring avec réseau commuté VTAM et Communications Server

Le tableau 8 compare les paramètres de l'hôte aux paramètres de Communications Server en ce qui concerne les connexions Réseau IBM Token-Ring via un réseau commuté VTAM.

Tableau 8 (page 1 de 2). Références croisées des paramètres hôte/PC : Réseau commuté VTAM Réseau IBM Token-Ring

VTAM	Profil/paramètres Communications Server	Remarques
IDBLK=	Configuration du nœud ID nœud local **ID de bloc**	L'IDBLK hôte doit correspondre aux trois premiers caractères hexadécimaux de l'**ID nœud local** dont la valeur par défaut est X'05D' pour Communications Server. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.

Tableau 8 (page 2 de 2). Références croisées des paramètres hôte/PC : Réseau commuté VTAM Réseau IBM Token-Ring

VTAM	Profil/paramètres Communications Server	Remarques
IDNUM=	Configuration du nœud ID nœud local **ID d'unité physique**	L'IDNUM hôte doit correspondre aux 5 derniers caractères hexadécimaux de l'**ID nœud local**. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
CPNAME=	Définition du nœud Configuration du nœud **nom qualifié de CP** (seconde zone)	Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez IDBLK= et IDNUM=.
LOCADDR	Configuration des LU hôte **Adresse NAU**	Ces paramètres doivent comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC pour les LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Aucune définition hôte n'est requise pour les LU dépendantes si SDDLU ou une définition dynamique est utilisée pour les LU indépendantes sur VTAM version 3.4 ou ultérieure.
MAXDATA	Configuration des unités de réseau local **Taille maximale de la PIU** (265 à 65535)	Il n'est pas nécessaire que ces valeurs soient concordantes.
MAXOUT	Configuration des unités de réseau local **Nombre de mémoires tampon de réception** (2 à 64)	Le **nombre de mémoires tampon de réception** dans Communications Server doit être égal au paramètre MAXOUT sur l'hôte.

Carte Réseau IBM Token-Ring 9370 et Communications Server

Le tableau 9 compare les paramètres hôte 9370 aux paramètres de Communications Server en ce qui concerne les connexions Réseau IBM Token-Ring

Tableau 9 (page 1 de 2). Références croisées des paramètres hôte/PC : Réseau local VTAM 9370 Réseau IBM Token-Ring

VTAM	Profil/paramètres Communications Server	Remarques
VBUILD TYPE = LAN	Type de DLC : Réseau local	
PORT MACADDR=	Configuration des connexions Réseau local **Adresse de destination**	L'adresse de destination indiquée dans la personnalisation de Communications Server doit correspondre à l'adresse de la carte 9370 IBM Token-Ring.
PORT SAPADDR=04	Configuration des connexions Réseau local **SAP éloigné**	Ces valeurs doivent être concordantes.

Tableau 9 (page 2 de 2). Références croisées des paramètres hôte/PC : Réseau local VTAM 9370 Réseau IBM Token-Ring

VTAM	Profil/paramètres Communications Server	Remarques
ADDR=04 (de sortie uniquement)	Configuration des connexions Réseau local **SAP local**	Ces valeurs doivent être concordantes.

Contrôleur 3174 et Communications Server

Le tableau 10, compare les paramètres du contrôleur 3174 à Communications Server pour les connexions IBM Token-Ring.

Tableau 10. Correspondance de paramètres entre un 3174 Token Ring et Communications Server

3174	Profil/paramètres Communications Server	Remarques
Limite d'adresse maximale supérieure à 104 : CUA	Type de DLC : Réseau local	
Adresse Token-Ring pour la passerelle	Configuration des connexions Réseau local **Adresse de destination**	Ces valeurs doivent être concordantes.
Définition de transmission en anneau. W= fenêtre maxi sortie, F=0, W = 1-7, F=1, W = 1-7, F=2, W = 1-4, F=3, W = 1-2	Configuration des unités Réseau local **Nombre de mémoires tampon de réception** (1 à 8)	Le **nombre de mémoires tampon de réception** de Communications Server doit être égal à 3174 W.

PU VTAM de contrôleur 3174 et Communications Server

Le tableau 11, compare les paramètres de PU VTAM du contrôleur 3174 à Communications Server pour les connexions IBM Token-Ring.

Tableau 11 (page 1 de 2). Références croisées des paramètres hôte/PC : PU VTAM de contrôleur 3174 Réseau IBM Token-Ring et Communications Server

VTAM	Profil/paramètres Communications Server	Remarques
CUADDR (local) ou ADDR (éloigné)	(aucun)	Associé par le contrôleur 3174 à l'adresse IBM Token-Ring
MAXDATA (éloigné uniquement)	Configuration des unités Réseau local **Taille maximale de la PIU** (99 à 65535)	La taille maximale de la PIU définie sur le poste travail Communications Server doit correspondre à la valeur définie sur l'hôte.
MAXOUT (éloigné uniquement)	Configuration des unités Réseau local **Nombre de mémoires tampon de réception** (2 à 64)	Le **nombre de mémoires tampon de réception** de Communications Server doit être égal à MAXOUT.

Tableau 11 (page 2 de 2). Références croisées des paramètres hôte/PC : PU VTAM de contrôleur 3174 Réseau IBM Token-Ring et Communications Server

VTAM	Profil/paramètres Communications Server	Remarques
LOCADDR	Configuration des LU hôte **Adresse NAU**	Ces paramètres doivent comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC pour les LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Aucune définition hôte n'est requise pour les LU dépendantes si SDDLU ou une définition dynamique est utilisée pour les LU indépendantes sur VTAM version 3.4 ou ultérieure.

Ethernet avec réseau commuté VTAM et Communications Server

Le tableau 12 compare les paramètres de l'hôte aux paramètres de Communications Server en ce qui concerne les connexions du réseau Ethernet via un réseau commuté VTAM.

Tableau 12 (page 1 de 2). Références croisées de paramètres hôte/PC : Réseau Ethernet et réseau commuté VTAM

VTAM	Profil/paramètres Communications Server	Remarques
IDBLK=	Configuration du nœud ID nœud local **ID de bloc**	L'IDBLK hôte doit correspondre aux trois premiers caractères hexadécimaux de l'**ID nœud local** dont la valeur par défaut est X'05D' pour Communications Server. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
IDNUM=	Configuration du nœud ID nœud local **ID d'unité physique**	L'IDNUM hôte doit correspondre aux 5 derniers caractères hexadécimaux de l'**ID nœud local**. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
CPNAME=	Définition du nœud Configuration du nœud **nom qualifié de CP** (seconde zone)	Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez IDBLK= et IDNUM=.

Tableau 12 (page 2 de 2). Références croisées de paramètres hôte/PC : Réseau Ethernet et réseau commuté VTAM

VTAM	Profil/paramètres Communications Server	Remarques
LOCADDR	Configuration des LU hôte **Adresse NAU**	Ces paramètres doivent comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC pour les LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Aucune définition hôte n'est requise pour les LU dépendantes si SDDLU ou une définition dynamique est utilisée pour les LU indépendantes sur VTAM version 3.4 ou ultérieure.
MAXDATA	Configuration des unités de réseau local **Taille maximale de la PIU** (265 à 65535)	Il n'est pas nécessaire que ces valeurs soient concordantes.
MAXOUT	Configuration des unités de réseau local **Nombre de mémoires tampon de réception** (2 à 64)	Le **nombre de mémoires tampon de réception** dans Communications Server doit être égal au paramètre MAXOUT sur l'hôte.

VTAM/NCP et Communications Server (SDLC)

Le tableau 13 compare les paramètres hôte VTAM/NCP aux paramètres de Communications Server en ce qui concerne les connexions SDLC.

Tableau 13 (page 1 de 3). Références croisées des paramètres hôte/PC : SDLC

VTAM/NCP	Profil/paramètres Communications Server	Remarques
NETID=	Configuration du nœud **Nom qualifié de CP** (première zone)	Ce paramètre peut être utilisé pour les lignes spécialisées et les lignes commutées. Il identifie le réseau SNA auquel vous vous connectez à l'aide de Communications Server.
NAME PU		Utilisez systématiquement un nom de PU (NAME PU). Ce dernier doit être différent du nom de CP local de sorte que vous puissiez définir une LU pour le point de contrôle.
IDBLK=	Configuration du nœud ID nœud local **ID de bloc**	L'IDBLK hôte doit correspondre aux trois premiers caractères hexadécimaux de l'**ID nœud local** dont la valeur par défaut est X'05D' pour Communications Server. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.

Tableau 13 (page 2 de 3). Références croisées des paramètres hôte/PC : SDLC

VTAM/NCP	Profil/paramètres Communications Server	Remarques
IDNUM=	Configuration du nœud ID nœud local **ID d'unité physique**	L'IDNUM hôte doit correspondre aux 5 derniers caractères hexadécimaux de l'**ID nœud local**. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
CPNAME=	Définition du nœud Configuration du nœud **nom qualifié de CP** (seconde zone)	Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez IDBLK= et IDNUM=.
LNCTL=SDLC	Type de DLC : SDLC-WAC, SDLC-MPA, port COM (en fonction du matériel utilisé)	SDLC doit être sélectionné à ce stade. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.
LOCADDR	Configuration des LU hôte **Adresse NAU**	Ces paramètres doivent comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC pour les LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Aucune définition hôte n'est requise pour les LU dépendantes si SDDLU ou une définition dynamique est utilisée pour les LU indépendantes sur VTAM version 3.4 ou ultérieure.
NRZI=YES/NO	Configuration des connexions SDLC-WAC, SDLC-MPA, Port COM **Codage NRZI**	Communications Server utilise USE_NRZI_ENCODING=0 et USE_NRZI_ENCODING=1. Ce paramètre ne figure que sur des PCM pour le type de modem : commuté synchrone, non commuté synchrone et AutoSync. Le plan de codage, NRZI ou NRZ, doit être configuré de la même façon aux deux extrémités d'une connexion. Si le plan de codage ne concorde pas, les modems se connectent mais le transfert de données n'aboutit pas et la connexion est interrompue par Communications Server après un délai au niveau de la liaison (en général, 40 secondes). Nous vous conseillons d'utiliser le plan de codage NRZ lorsque vous vous connectez à un réseau X.25 à l'aide d'un connecteur WAC (Wide Area Connector) d'IBM.
DUPLEX= FULL/HALF	Configuration des connexions SDLC-WAC et Port COM uniquement **Communication en duplex intégral**	Les valeurs définies à chaque extrémité doivent être conformes au type et à la configuration du modem. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.

Tableau 13 (page 3 de 3). Références croisées des paramètres hôte/PC : SDLC

VTAM/NCP	Profil/paramètres Communications Server	Remarques
(TRANSFR * BFRS) –47	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Taille maximale de la PIU** (265 à 4105)	La valeur de la taille maximale de la zone d'information doit être inférieure ou égale à (TRANSFR * BFRS) - 47 indiqué sur l'hôte. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.
MAXDATA=	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Taille maximale de la PIU** (265 à 4105)	Il n'est pas nécessaire que ces valeurs soient concordantes. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées. La valeur minimale est utilisée.
MAXOUT=	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Fenêtre de trames de réception** (1 à 30)	La **fenêtre de trames de réception** dans Communications Server doit être égale au paramètre MAXOUT sur l'hôte. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.
ADDR=	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Adresse du poste de liaison** (01 à FE)	Ces paramètres doivent comporter la même valeur. Ils sont codifiés au format hexadécimal pour Communications Server et VTAM/NCP. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.

VTAM et Communications Server (APPC)

Le tableau 14 compare les paramètres hôte VTAM aux paramètres de Communications Server en ce qui concerne les connexions APPC.

Tableau 14 (page 1 de 2). Références croisées des paramètres hôte/PC : APPC

VTAM	Profil/paramètres Communications Server	Remarques
LU NAME	Configuration des LU hôte **Nom de LU locale** ou : Configuration du nœud **Nom qualifié de CP** (seconde zone)	
LOCADDR	Configuration des LU hôte **Adresse NAU**	Ces paramètres doivent comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC pour les LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Aucune définition hôte n'est requise pour les LU dépendantes si SDDLU ou une définition dynamique est utilisée pour les LU indépendantes sur VTAM version 3.4 ou ultérieure.
NETID APPL	Configuration des LU partenaires LU 6.2 **Nom de la LU partenaire**	

Tableau 14 (page 2 de 2). Références croisées des paramètres hôte/PC : APPC

VTAM	Profil/paramètres Communications Server	Remarques
Table d'interprétation VTAM	Configuration des LU partenaires LU 6.2 **Nom de la LU partenaire**	Réservé uniquement aux LU dépendantes.
Table LOGMODE LOGMODE=	Configuration du nœud **Nom du mode**	Ces paramètres doivent être concordants.
Table LOGMODE RUSIZES=	Configuration du nœud **Taille maximale de la RU** (256 à 32767)	Les valeurs définitives sont négociées.

VTAM et Communications Server (MPC)

Le tableau 15 et le tableau 16 comparent les paramètres hôte VTAM et IOCP/HCD aux paramètres de Communications Server en ce qui concerne les connexions MPC (Multi-Path Channel).

Tableau 15. Références croisées des paramètres IOCP/HCD : MPC

IOCP/HCD	Profil/paramètres Communications Server	Remarques
IOCP IODEVICE UNIT=SCTC	Type de DLC : IBM-MPC	
HCD Type d'unité SCTC	Type de DLC : IBM-MPC	

Tableau 16 (page 1 de 2). Références croisées des paramètres VTAM : MPC

Instruction de définition VTAM	Opérande	Profil/paramètres Communications Server	Remarques
VBUILD,TYPE=TRL	LNCTL=MPC	Type de DLC : IBM-MPC	
	MPCLEVEL=HPDT		Les connexions IBM-MPC de Communications Server requièrent HPR/HPDT
	MAXBFRU	Configuration de la fonction MPC DLC **Taille maximale de la PIU**	Peut avoir une incidence sur les performances et/ou sur la mémoire VTAM utilisée
	MAXREADS	Configuration de la fonction MPC DLC **Nombre de mémoires tampon de réception**	Peut avoir une incidence sur les performances et/ou sur la mémoire VTAM utilisée
	READ	Configuration de la fonction MPC DLC	La liste des adresses VTAM READ IODEVICE doit correspondre à la liste MPC DLC des sous-canaux READ de Communications Server.
	WRITE	Configuration de la fonction MPC DLC	La liste des adresses VTAM WRITE IODEVICE doit correspondre à la liste MPC DLC des sous-canaux WRITE de Communications Server.

Tableau 16 (page 2 de 2). Références croisées des paramètres VTAM : MPC

Instruction de définition VTAM	Opérande	Profil/paramètres Communications Server	Remarques
VBUILD,TYPE=LOCAL	CONNTYPE=APPN	Configuration des connexions IBM-MPC **Support APPN**	La connexion IBM-MPC de Communications Server requiert APPN.
	XID=YES	Configuration des connexions IBM-MPC **Support APPN**	La connexion IBM-MPC de Communications Server requiert PU2.1.
	CPCP=YES	Configuration des connexions IBM-MPC **Support APPN**	La connexion IBM-MPC de Communications Server requiert APPN.
	HPR=YES	Configuration des connexions IBM-MPC **Support HPR**	La connexion IBM-MPC de Communications Server requiert HPR.
	NN	Configuration du nœud **Type de nœud**	Le type de nœud de PU VTAM doit correspondre à la définition de Communications Server.
	DELAY		Peut avoir une incidence sur les performances et/ou sur l'unité centrale de VTAM

ES/9000 et Communications Server (SDLC)

Le tableau 17 compare les paramètres du système d'information 9370 aux paramètres de Communications Server en ce qui concerne les connexions SDLC.

Tableau 17 (page 1 de 2). Références croisées des paramètres hôte/PC : Système d'information 9370 via SDLC

9370/VTAM	Profil/paramètres Communications Server	Remarques
QFI : codage NRZI (configuration de microcode)	Configuration des connexions SDLC-WAC, SDLC-MPA, Port COM **Codage NRZI**	Ces paramètres doivent être concordants. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées. Communications Server utilise USE_NRZI_ENCODING=0 et USE_NRZI_ENCODING=1. Il s'agit du flot de données synchrone.
QFI : protocole (configuration de microcode) VTAM: GROUP LNCTL=SDLC	Type de DLC SDLC-WAC, SDLC-MPA Port COM	Les paramètres du microcode et de VTAM doivent être concordants. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.
MAXDATA	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Taille maximale de la PIU** (265 à 4105)	Il n'est pas nécessaire que ces valeurs soient concordantes. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.
Taille MAXBFRU * IOBUF	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Taille maximale de la PIU** (265 à 4105)	La valeur de la taille maximale de la zone d'information doit être inférieure ou égale à MAXBFRU multiplié par la taille IOBUF indiquée sur l'hôte. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.

Tableau 17 (page 2 de 2). Références croisées des paramètres hôte/PC : Système d'information 9370 via SDLC

9370/VTAM	Profil/paramètres Communications Server	Remarques
MAXOUT=	Configuration des unités **Fenêtre de trames de réception** (1 à 30)	La **fenêtre de trames de réception** dans Communications Server doit être égale au paramètre MAXOUT sur l'hôte. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.
ADDR=	Configuration des unités **Adresse du poste de liaison** (01 à FE)	Les valeurs définies pour ces paramètres doivent être concordantes. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.
IDBLK=	Configuration du nœud ID nœud local **ID de bloc**	L'IDBLK hôte doit correspondre aux trois premiers caractères hexadécimaux de l'**ID nœud local** dont la valeur par défaut est X'05D' pour Communications Server. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
IDNUM=	Configuration du nœud ID nœud local **ID d'unité physique**	L'IDNUM hôte doit correspondre aux 5 derniers caractères hexadécimaux de l'**ID nœud local**. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
CPNAME=	Configuration du nœud **Nom qualifié de CP** (seconde zone)	Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez IDBLK= ou IDNUM=.
LOCADDR	Configuration des LU hôte **Adresse NAU**	Les paramètres LOCADDR et NAU doivent comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC pour les LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Ce paramètre est utilisé pour les lignes spécialisées et les lignes commutées.

Hôte et Communications Server (DLUR)

Le tableau 18 compare les paramètres de l'hôte et de Communications Server pour les connexions VTAM via le DLUR.

Tableau 18 (page 1 de 2). Références croisées des paramètres Communications Server VTAM : utilisation du DLUR

VTAM	Communications Server	Remarques
IDBLK=	Configuration des PU DLUR **ID de bloc**	L'IDBLK doit correspondre aux 3 premiers caractères hexadécimaux de l'ID nœud dont la valeur par défaut est X'05D' pour Communications Server ; indiquez ce paramètre lorsque vous n'utilisez pas CPNAME=.

Tableau 18 (page 2 de 2). Références croisées des paramètres Communications Server VTAM : utilisation du DLUR

VTAM	Communications Server	Remarques
IDNUM=	Configuration des PU DLUR **ID d'unité physique**	L'IDNUM doit correspondre aux 5 derniers caractères hexadécimaux de l'ID nœud. Indiquez ce paramètre lorsque vous n'utilisez pas CPNAME=.
CPNAME=	Configuration des PU DLUR **Nom de PU**	Le CPNAME doit correspondre au nom de la PU locale. Indiquez ce paramètre lorsque vous n'utilisez pas IDNUM= et IDBLK=.

Le tableau 19, répertorie les paramètres suivants de l'instruction PATH, qui sont utilisés lors de l'établissement d'une connexion de l'hôte au poste de travail.

Tableau 19. Correspondance des paramètres DLUR Communications Server VTAM - Connexion de l'hôte au poste de travail

VTAM	Communications Server	Remarques
DLURNAME=	Configuration du nœud **Nom qualifié de CP** (seconde zone)	Le DLURNAME fournit le nom du nœud DLUR qui détient la PU DLUR. Pour Communications Server, il s'agit du nom qualifié de CP.
DLCADDR= (1,C,INTPU)		Obligatoire. Ce paramètre indique au DLUR que la connexion est destinée à une PU interne.
DLCADDR=(2,X,zzzzzzzz)	Configuration des PU DLUR **ID de bloc et** **ID d'unité physique**	Le zzzzzzzz de DLCADDR=(2,X,zzzzzzzzz) doit correspondre à l'ID nœud. Indiquez ce paramètre lorsque vous n'utilisez pas DLCADDR=(3,C,nompu).
DLCADDR= (3,C,nompu)	Configuration des PU DLUR **Nom de PU**	Le nom de PU de DLCADDR=(3,C,nompu) doit correspondre au nom de la PU locale. Indiquez ce paramètre lorsque vous n'utilisez pas DLCADDR=(2,X,zzzzzzzz).

NPSI et Communications Server (X.25)

Le support X.25 de Communications Server permet la transmission des trames SNA via un réseau X.25. X.25 traite les trames SNA comme des données brutes et les transmet sous forme de paquets de données dans des données. Les deux nœuds de réseau ne sont pas directement connectés mais ils sont connectés à un réseau intermédiaire appelé réseau de commutation de données par paquet (PSDN). Le réseau X.25 peut comprendre l'une des connectivités X.25.

Le logiciel qui assure l'interaction avec le réseau PSDN, qui conditionne les données SNA en paquets et qui extrait ces données telles quelles fait partie intégrante de Communications Server. Côté hôte IBM 370, les fonctions X.25 sont traitées par un produit logiciel distinct appelé interface NPSI (Network Control Program Packet Switching Interface) X.25. Les définitions NPSI sont générées conjointement avec le NCP, et le logiciel NPSI s'exécute en accord avec le NCP dans le même contrôleur 3705, 3725, 3720 ou 3745.

La plupart des paramètres X.25 indiqués dans Communications Server et NPSI prennent des valeurs qui sont convenues par vous-même et par le fournisseur de réseau X.25 et non entre les deux nœuds. Par exemple, dans le cas d'une connexion SDLC sur une ligne non commutée, le contrôleur hôte (NCP) est configuré pour appeler une adresse secondaire particulière. Communications Server est configuré pour répondre à cette adresse sur une liaison physique entre le poste de travail Communications Server et l'hôte.

Connexions NPSI sur X.25

Le tableau 20 compare les paramètres de l'hôte et de Communications Server pour les connexions NPSI sur X.25.

Tableau 20. Références croisées des paramètres hôte/PC : Connexions NPSI sur X.25

NPSI	Profil/paramètres Communications Server	Remarques
X25.LINE TYPE=	Type de DLC Port COM X.25, X.25-WAC	Indiquez **TYPE=P** pour les PVC et **TYPE=S** pour les SVC de la définition de liaison NPSI X.25.
CALL= (uniquement pour le type = S)	Configuration des unités Port COM X.25, X.25-WAC **Plages de circuits virtuels**	Les plages de circuits virtuels doivent correspondre à votre abonnement au réseau X.25.
MAXDATA=	Configuration des unités Port COM X.25, X.25-WAC **Taille maximale de la PIU** (256 à 4105)	Il n'est pas nécessaire que ces valeurs soient concordantes.
VWINDOW	Configuration des unités Port COM X.25, X.25-WAC **Taille de la fenêtre** (1 à 7)	La **taille de la fenêtre SVC/PVC** doit correspondre aux abonnements X.25.
MWINDOW	Configuration des unités Port COM X.25, X.25-WAC Valeurs de trame **Taille de la fenêtre** (1 à 7)	
FRMLGTH	Configuration des unités Port COM X.25, X.25-WAC Séquence de trame **Modulo**	La valeur du paramètre hôte **FRMLGTH** doit être au moins égale à MAXPKT +3 lors de l'exécution de Modulo 8, ou à MAXPKT +4 lors de l'exécution de Modulo 128. La taille Modulo de l'hôte et de Communications Server, ainsi que les tailles de paquets doivent correspondre à votre abonnement X.25.
MAXPKTL	Configuration des unités Port COM X.25, X.25-WAC **Taille du paquet**	Les **tailles de paquets SVC/PVC** de l'hôte doivent correspondre à la valeur de l'abonnement X.25.

VTAM/NCP et Communications Server (X.25)

Le tableau 21 compare les paramètres de l'hôte et de Communications Server pour les connexions X.25 (VTAM/NCP).

Tableau 21. Références croisées des paramètres hôte/PC : X.25 (VTAM/NCP)

VTAM/NCP	Profil/paramètres Communications Server	Remarques
NETID=	Configuration du nœud **Nom qualifié de CP** (première zone)	Ce paramètre identifie le réseau SNA auquel vous vous connectez à l'aide de Communications Server.
PU NAME		Utilisez systématiquement un nom de PU. Ce dernier ne doit pas être identique au nom de CP local de sorte que vous puissiez définir une LU pour le point de contrôle.
IDBLK=	Configuration du nœud ID nœud local **ID de bloc**	Les trois premiers chiffres hexadécimaux de l'**ID nœud local** dont la valeur par défaut est X'05D' pour Communications Server. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
IDNUM=	Configuration du nœud ID nœud local **ID d'unité physique**	L'IDNUM hôte doit correspondre aux 5 derniers caractères hexadécimaux de l'**ID nœud local**. Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez CPNAME=.
CPNAME=	Configuration du nœud **Nom qualifié de CP** (seconde zone)	Indiquez ce paramètre lors de l'utilisation de liaisons commutées, ou ne l'indiquez pas si vous utilisez IDBLK= et IDNUM=.
(TRANSFR * BFRS) - 47	Configuration des unités Port COM X.25, X.25-WAC **Taille maximale de la PIU** (265 à 4105)	La **taille maximale de la PIU** doit être égale à la valeur définie sur l'hôte.
MAXDATA=	Configuration des unités Port COM X.25, X.25-WAC **Taille maximale de la PIU** (265 à 4105)	Il n'est pas nécessaire que ces valeurs soient concordantes.
LOCADDR	Configuration des LU hôte **Adresse NAU**	Ces paramètres doivent comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC pour les LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Aucune définition hôte n'est requise pour les LU dépendantes si SDDLU ou une définition dynamique est utilisée pour les LU indépendantes sur VTAM version 3.4 ou ultérieure.

APPC sur X.25

Le tableau 22 établit la correspondance des paramètres d'un poste de travail Communications Server exécutant APPC, qui se connecte à un hôte via X.25.

Tableau 22. Références croisées des paramètres hôte/PC : APPC sur un réseau IBM Token-Ring se connectant à un hôte via X.25.

NCP	Profil/paramètres Communications Server	Remarques
LU NAME	Configuration de la LU 6.2 locale **Nom de LU locale** ou : Configuration du nœud **Nom qualifié de CP** (seconde zone)	
LOCADDR	Configuration des LU hôte **Adresse NAU**	Ces paramètres ***doivent*** comporter la même valeur. En ce qui concerne les LU indépendantes, VTAM recommande la création d'une définition CDRSC ou l'utilisation de l'opérande DYNLU à la place de la codification de LOCADDR=0. Pour plus de détails sur la codification des définitions CDRSC relatives aux LU indépendantes, consultez le manuel *VTAM Network Implementation Guide*. Aucune définition hôte n'est requise pour les LU dépendantes si SDDLU ou une définition dynamique est utilisée pour les LU indépendantes sur VTAM version 3.4 ou ultérieure.
NETID APPL	Configuration des LU partenaires LU 6.2 **Nom de la LU partenaire**	
Table d'interprétation VTAM	Configuration des LU partenaires LU 6.2 **Nom de la LU partenaire**	Réservé uniquement aux LU dépendantes.
Table LOGMODE LOGMODE=	Configuration du nœud **Nom du mode**	Ces paramètres ***doivent*** être concordants.
Table LOGMODE RUSIZES=	Configuration du nœud **Taille maximale de la RU** (256 à 32767)	Ces valeurs doivent être concordantes.

Définitions de liaison hôte AS/400

Les définitions de liaison hôte AS/400 comportent une correspondance entre les paramètres de programme hôte OS/400 et les paramètres de Communications Server. Le tableau 23, à la page 179 contient les paramètres de liaison SDLC.

Tableau 23. Références croisées des paramètres Communications Server AS/400 : Définition de ligne de programme hôte OS/400

OS/400	Profil/paramètres Communications Server	Remarques
NRZI= Codage de données	Configuration des connexions SDLC-WAC, SDLC-MPA, Port COM **Codage NRZI**	Communications Server utilise USE_NRZI_ENCODING=0 et USE_NRZI_ENCODING=1. Ce paramètre ne figure que sur des PCM pour le type de modem : commuté synchrone, non commuté synchrone et AutoSync.
Sélection du débit de données du modem	Configuration des unités Port COM uniquement **Configuration du modem**	Les paramètres relatifs à la connexion de type asynchrone commuté du modem doivent être concordants sur les deux systèmes.
Taille maximale de trame (MAXFRAME)	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Fenêtre de trames de réception** (1 à 30)	Il n'est pas nécessaire que les valeurs de connexion asynchrone non commutée soient concordantes.
Nombre maximal de trames en attente (MAXOUT)	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Fenêtre de trames de réception** (1 à 30)	La **fenêtre de trames de réception** dans Communications Server doit être égale au paramètre MAXOUT sur l'hôte AS/400.

Définitions de contrôleur hôte AS/400

La définition du contrôleur hôte AS/400 comporte une correspondance entre les paramètres de programme hôte OS/400 et les paramètres de Communications Server.

Le tableau 24 présente les paramètres du programme hôte OS/400.

Tableau 24 (page 1 de 2). Références croisées des paramètres Communications Server AS/400 : paramètres du contrôleur

OS/400	Profil/paramètres Communications Server	Remarques
Type de liaison : *SDLC	Type de DLC SDLC-WAC, SDLC-MPA Port COM	Le type de liaison des deux systèmes doit être concordant. Ce paramètre figure dans la description de ligne mais entrez-le pour compléter les informations.
Ligne non commutée connectée	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Ligne commutée**	Ce paramètre est destiné aux connexions non commutées. Cette valeur doit correspondre avec une définition de ligne hôte précédemment définie.
Liste de lignes commutées	(aucun)	Ce paramètre est destiné aux connexions commutées. Cette valeur doit correspondre avec une définition de ligne hôte précédemment définie.
Taille maximale de trame	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Taille maximale de la PIU** (265 à 4105)	Il n'est pas nécessaire que ces valeurs soient concordantes.

Tableau 24 (page 2 de 2). Références croisées des paramètres Communications Server AS/400 : paramètres du contrôleur

OS/400	Profil/paramètres Communications Server	Remarques
ID du réseau éloigné	Configuration du nœud **Nom qualifié de CP** (première zone)	Ces valeurs doivent être concordantes.
Nom du point de contrôle éloigné	Configuration du nœud **Nom qualifié de CP** (seconde zone)	Ces valeurs doivent être concordantes.
Rôle de liaison de données :	Configuration des connexions SDLC-WAC, SDLC-MPA, Port COM **Rôle du poste de liaison**	Les paramètres sur les deux systèmes sont complémentaires. Si le rôle du poste hôte est principal, le poste de travail Communications Server doit être configuré comme secondaire ou négociable. Il est préférable d'affecter au poste de liaison de données un rôle négociable (*NEG), sauf si une connexion multipoint (*MP) est utilisée.
Adresse du poste	Configuration des unités SDLC-WAC, SDLC-MPA, Port COM **Adresse du poste de liaison** (01 à FE)	Ces valeurs doivent être concordantes.
Support de session CP APPN : (Oui/Non)	Configuration des connexions SDLC-WAC, SDLC-MPA, Port COM **Support APPN**	Ces valeurs doivent être concordantes si des sessions CP-CP sont souhaitées.
Type de nœud APPN :	Configuration des connexions SDLC-WAC, SDLC-MPA, Port COM **Type du CP adjacent**	Ces valeurs doivent être concordantes.

Définitions d'unité hôte AS/400

Le hôte AS/400 peut créer une définition d'unité lorsque le poste Communications Server se connecte sans qu'une définition d'unité soit précédemment définie.

Le tableau 25 présente les paramètres des unités du programme hôte OS/400.

Tableau 25 (page 1 de 2). Références croisées des paramètres Communications Server AS/400 : paramètres d'unités

OS/400	Profil/paramètres Communications Server	Remarques
Nom d'emplacement éloigné	Configuration de la LU 6.2 locale **Nom de LU locale** ou : Configuration du nœud **Nom qualifié de CP** (seconde zone)	Ces valeurs doivent être concordantes.
Contrôleur connecté	(aucun)	Ce paramètre est destiné aux connexions non commutées. Cette valeur doit correspondre avec une définition de ligne hôte précédemment définie.
Nom d'emplacement local		Utilisez la valeur par défaut fournie.

Tableau 25 (page 2 de 2). Références croisées des paramètres Communications Server AS/400 : paramètres d'unités

OS/400	Profil/paramètres Communications Server	Remarques
ID du réseau éloigné	Configuration du nœud **Nom qualifié de CP** (première zone)	Utilisez la valeur par défaut fournie.
Mode	Configuration du nœud **Nom du mode**	Utilisez la valeur par défaut fournie.

Description de liaison hôte AS/400 et Communications Server

Le tableau 26 contient la description de ligne du programme hôte AS/400.

Tableau 26. Références croisées des paramètres hôte/PC : description de ligne

OS/400	Profil/paramètres Communications Server	Remarques
Adresse de la carte locale :	Configuration des connexions **Adresse de destination de réseau local**	Les deux adresses doivent être concordantes aux fins de communication.

Description de contrôleur hôte AS/400 et Communications Server

Le tableau 27 présente les paramètres de contrôleur du programme hôte OS/400.

Tableau 27. Références croisées des paramètres hôte/PC : description de contrôleur

OS/400	Profil/paramètres Communications Server	Remarques
Ligne commutée active	(aucun)	Ce paramètre est destiné aux connexions non commutées. Cette valeur doit correspondre avec une définition de ligne hôte précédemment définie.
Point de contrôle éloigné	Configuration du nœud **Nom qualifié de CP** (seconde zone)	Les noms doivent être concordants.
ID du réseau éloigné	Configuration du nœud **Nom qualifié de CP** (première zone)	Utilisez la valeur par défaut ou établissez une correspondance entre les paramètres s'ils sont différents de l'ID du réseau local AS/400.
Description du contrôleur modèle		Ce paramètre doit avoir pour valeur YES si l'AS/400 utilise un réseau de connexion.
ID du réseau de connexion et nom de CP du réseau de connexion	Configuration des réseaux de connexion **Nom du réseau de connexion**	Ces valeurs doivent être concordantes pour tous les nœuds participant dans un réseau de connexion.

Descriptions twinax AS/400

Le tableau 28 contient la description twinax AS/400.

Tableau 28. Références croisées des paramètres hôte/PC : description de contrôleur

AS/400	Profil/paramètres Communications Server	Remarques
Ligne non commutée connectée	(aucun)	Ce paramètre est destiné aux connexions non commutées. Cette valeur doit correspondre avec une définition de ligne hôte précédemment définie.
Point de contrôle éloigné	Configuration du nœud **Nom qualifié de CP** (seconde zone)	Les noms doivent être concordants.
ID du réseau éloigné	Configuration du nœud **Nom qualifié de CP** (première zone)	Utilisez la valeur par défaut ou établissez une correspondance entre les paramètres s'ils sont différents de l'ID du réseau local AS/400.
Rôle de liaison de données=*SEC:	Configuration des connexions SDLC-WAC, SDLC-MPA Port COM **Rôle du poste de liaison**	Les paramètres sur les deux systèmes sont complémentaires. Si le rôle du poste hôte est principal, le poste de travail Communications Server doit être configuré comme secondaire ou négociable. Il est préférable d'affecter au poste de liaison de données un rôle négociable (*NEG), sauf si une connexion multipoint (*MP) est utilisée.

Définitions de liaison hôte AS/400 (X.25)

Les définitions de liaison hôte AS/400 comportent une correspondance entre les paramètres de programme hôte OS/400 et les paramètres de Communications Server. Le tableau 29 contient les paramètres de liaison X.25.

Tableau 29 (page 1 de 2). Références croisées des paramètres Communications Server AS/400 : Définition de ligne de programme hôte OS/400 (X.25)

OS/400	Profil/paramètres Communications Server	Remarques
Adresse du réseau local	Configuration des unités **Adresse locale**	Les deux adresses sont généralement déterminées par votre fournisseur de réseau.
Type de connexion	Configuration des unités Port COM X.25 X.25-WAC **Ligne commutée**	Le Type de connexion des deux systèmes doit être concordant.
Support ETCD X.25	Non applicable	Doit avoir pour valeur YES si la connexion entre les deux systèmes est de type point à point sans traverser un réseau X.25.
Taille maximale de trame	Configuration des unités Port COM X.25 X.25-WAC **Taille maximale de la PIU**	La taille maximale de la PIU sur les deux systèmes doit être concordante.

Tableau 29 (page 2 de 2). Références croisées des paramètres Communications Server AS/400 : Définition de ligne de programme hôte OS/400 (X.25)

OS/400	Profil/paramètres Communications Server	Remarques
Taille de paquet par défaut	Configuration des unités Port COM X.25 X.25-WAC **Taille du paquet**	Cette valeur est déterminée par votre fournisseur de réseau ; elle est identique pour la transmission et la réception.
Taille maximale des paquets	Non applicable	Cette valeur est déterminée par votre fournisseur de réseau.
Modulus	Configuration des unités Port COM X.25 X.25-WAC **Classement**	Cette valeur est déterminée par votre fournisseur de réseau.
Taille de fenêtre par défaut	Configuration des unités Port COM X.25 X.25-WAC **Taille de la fenêtre**	Cette valeur est déterminée par votre fournisseur de réseau ; elle est identique pour la transmission et la réception.
Insertion de l'adresse de réseau	Configuration des unités Port COM X.25 X.25-WAC	Cette valeur est déterminée par votre fournisseur de réseau ; elle doit être identique pour les deux systèmes.
Entrées de voies logiques	Configuration des unités Port COM X.25 X.25-WAC **Plages de circuits virtuels**	Ces valeurs sont déterminées par votre fournisseur de réseau et par le type de circuit virtuel X.25 dont vous disposez.

Définitions du contrôleur hôte AS/400 (PVC X.25)

La définition du contrôleur hôte AS/400 comporte une correspondance entre les paramètres de programme hôte OS/400 et les paramètres de Communications Server.

Le tableau 30 présente les paramètres du programme hôte OS/400 pour la connexion PVC X.25.

Tableau 30 (page 1 de 2). Références croisées des paramètres PVC X.25 Communications Server-AS/400 : paramètres du contrôleur

OS/400	Profil/paramètres Communications Server	Remarques
ID voie logique X.25	Configuration des connexions Port COM X.25, X.25-WAC **Numéro de la voie logique**	Ces valeurs sont déterminées par votre fournisseur de réseau.
Type de liaison : *X25	Configuration des connexions	Les types de liaison des deux systèmes doivent être concordants.
Connexion commutée : *NO		Tous les PVC sont non commutés.
Taille maximale de trame	Configuration des unités Port COM X.25 X.25-WAC **Taille maximale de la PIU**	Il n'est pas nécessaire que les valeurs de taille maximale de trame soient concordantes.

Tableau 30 (page 2 de 2). Références croisées des paramètres PVC X.25 Communications Server-AS/400 : paramètres du contrôleur

OS/400	Profil/paramètres Communications Server	Remarques
Rôle de liaison de données	Configuration des unités Port COM X.25 X.25-WAC **Rôle du poste de liaison**	Les paramètres sur les deux systèmes sont complémentaires. Si le rôle du poste hôte est principal, le poste de travail Communications Server doit être configuré comme secondaire ou négociable.
Niveau de réseau X.25	Configuration des unités Port COM X.25 X.25-WAC **Conformité CCITT**	Ces valeurs sont déterminées par votre fournisseur de réseau.
Protocole de niveau de liaison X.25 : *QLLC		Cette valeur doit être QLLC.

Définitions du contrôleur hôte AS/400 (SVC X.25)

La définition du contrôleur hôte AS/400 comporte une correspondance entre les paramètres de programme hôte OS/400 et les paramètres de Communications Server.

Le tableau 31 présente les paramètres du programme hôte OS/400 pour la connexion SVC X.25.

Tableau 31. Références croisées des paramètres SVC X.25 Communications Server AS/400 : paramètres du contrôleur

OS/400	Profil/paramètres Communications Server	Remarques
Type de liaison : *X25	Configuration des connexions	Les types de liaison des deux systèmes doivent être concordants.
Connexion commutée : *YES		Tous les SVC sont commutés.
Taille maximale de trame	Configuration des unités Port COM X.25 X.25-WAC **Taille maximale de la PIU**	Il n'est pas nécessaire que les valeurs de taille maximale de trame soient concordantes.
Numéro de connexion	Configuration des unités Port COM X.25 X.25-WAC **Adresse ETTD local**	Cette valeur est déterminée par votre fournisseur de réseau.
Rôle de liaison de données	Configuration des unités Port COM X.25 X.25-WAC **Rôle du poste de liaison**	Les paramètres sur les deux systèmes sont complémentaires. Si le rôle du poste hôte est principal, le poste de travail Communications Server doit être configuré comme secondaire ou négociable.
Niveau de réseau X.25	Configuration des unités Port COM X.25 X.25-WAC **Conformité CCITT**	Ces valeurs sont déterminées par votre fournisseur de réseau.
Protocole de niveau de liaison X.25 : *QLLC		Cette valeur doit être QLLC.

Mise en œuvre des configurations de Communications Server

Voici une procédure recommandée pour l'installation et la configuration du logiciel de votre réseau :

1. Planification du matériel.
2. Planification des applications logicielles.
3. Création des conventions de dénomination.
4. Définition des adresses de réseau.
5. Choix des outils de configuration et d'installation.
6. Définition du modèle de configuration.
7. Création et installation des configurations.
8. Création des matériels utilisateur.
9. Maintenance du réseau.

Le présent chapitre décrit la procédure recommandée.

Introduction

Un modèle de configuration définit les informations de configuration communes à un groupe de serveurs. Vous pouvez créer un ou plusieurs modèles de configuration. Chaque fichier de configuration commence par le modèle de configuration et peut contenir les quelques paramètres requis pour la personnalisation de la configuration du serveur. Il en résulte une configuration simplifiée du serveur.

Le modèle de configuration permet également de définir des options de configuration qui ne peuvent pas être indiquées à l'aide de fichiers réponses.

Pour plus de détails sur l'utilisation des fichiers réponses et modèles destinés aux opérations de configuration et d'installation, reportez-vous à la section «Configuration à l'aide de fichiers modèles et réponses», à la page 196.

Veillez à cumuler les totaux de la mémoire RAM et de l'espace disque requis pour chaque poste de travail à mesure que vous rassemblez des informations dans les étapes suivantes. Vous pouvez ainsi vous assurer que le matériel que vous avez choisi pour les aux utilisateurs est adéquat.

Étape 1. Planification du matériel

Si vous avez déjà déterminé que vous pouvez utiliser des serveurs existants, vous devez vous assurer que la mémoire et l'espace disque du matériel existant sont suffisants. Ce matériel doit également être équipé d'unités système, d'écrans, d'imprimantes, de claviers, de cartes, de modems et de câbles pour le logiciel qui sera installé.

Si vous vous procurez de nouveaux serveurs, enregistrez le matériel sur les feuilles de travail que vous préparez pour ces utilisateurs.

Mémoire

Pour plus de détails sur l'espace mémoire requis pour Communications Server, consultez le *Guide d'utilisation*.

Capacité de mémoire

Lors de la planification du matériel d'exécution de Communications Server, il est important d'évaluer la façon dont le serveur sera utilisé en termes de capacité. Déterminez les types de sessions qui seront pris en charge par Communications Server, notamment, sans que cette liste soit limitative, les sessions TN3270E, les sessions de client API SNA et les sessions SNA traditionnelles avec un hôte. En fonction de ce nombre, vous pouvez calculer la charge moyenne sur le serveur, et déterminer l'espace mémoire approprié.

Remarque : Ces estimations s'ajoutent aux exigences du système d'exploitation de base (Windows NT Server) et des autres applications qui s'exécutent simultanément sur le même système.

Utilisez le tableau suivant pour déterminer la charge moyenne sur le serveur :

Tableau 32. Capacité de mémoire

Type de session client	Mémoire utilisée par session
Passerelle SNA (traditionnelle)	29,9 ko
Client API SNA	25,2 ko
TN3270E	15,8 ko

L'espace mémoire estimatif utilisé par un serveur Communications Server actif sans aucune liaison ou session active est de 21 Mo. Pour minimiser la perte de performances, il est préférable de réduire la quantité de pagination (permutation des segments de mémoire sur le disque) qui se produit. Il est recommandé que l'espace mémoire réellement disponible dans le système soit égal à celui qui est requis par le logiciel d'exécution avec 5 à 10 Mo supplémentaires réservés à une mémoire tampon. Par exemple, une installation de Communications Server prenant en charge 1000 sessions client TN3270E requiert les espaces mémoire suivants (en fonction des valeurs indiquées dans le tableau 32).

Système d'exploitation Microsoft Windows NT Server	19,0 Mo (estimation)
Communications Server pour Windows NT	21,0 Mo
Sessions TN3270E (1000 X 15,8 ko)	15,8 Mo
Réserve	10,0 Mo
Mémoire totale recommandée	65,8 Mo

Remarque : L'espace mémoire de 65,8 Mo n'est pas requis pour 1000 sessions TN3270E. Il s'agit d'une recommandation visant à optimiser les performances.

Vitesse du processeur

Lors de la détermination de la vitesse minimale requise pour le processeur, vous devez comprendre le nombre moyen des transactions par minute qui doivent être traitées par le serveur. Une transaction correspond à tout échange d'informations entre le client et l'hôte via le serveur, qu'il s'agisse d'une régénération d'écran ou d'une entrée de base de données demandée.

Lors du calcul de la charge moyenne du processeur, multipliez le nombre moyen des sessions par le nombre moyen des transactions par minute par session, et par le facteur d'échelle indiqué dans la table suivante (en fonction du type de session).

Type de session client	Facteur de charge du processeur (100 MHz)	Facteur de charge du processeur (166 MHz)
Passerelle SNA (traditionnelle)	0,004	0,002
Client API SNA	0,021	0,011
TN3270E	0,011	0,006

Par exemple, pour la prise en charge de 1000 sessions TN3270E simultanées, avec une moyenne de 6,7 transactions par minute, la charge moyenne sur le processeur 166 MHz est égale à 1000 X 6,7 X 0,006, soit 40.2%. Les performances se dégradent rapidement lorsque le processeur est utilisé à plus de 80%. Un processeur plus rapide permet d'améliorer les performances de Communications Server et du système. Un nombre plus élevé d'utilisateurs et de transactions seraient en mesure de tirer parti du serveur simultanément. Aucune valeur maximale n'est prise en charge par Communications Server pour la vitesse du processeur ; cependant, 100 MHz est la valeur minimale recommandée.

Étape 2. Planification des applications logicielles

Les exigences des applications logicielles s'ajoutent à celles de Communications Server. Pour plus de détails, consultez la documentation des applications logicielles.

Étape 3. Création de conventions de dénomination

Les réseaux créés à l'aide de Communications Server requièrent la création et l'utilisation de nombreux noms pour plusieurs objets du réseau. Certains de ces noms peuvent être identiques entre les serveurs mais d'autres doivent être uniques sur le réseau afin d'éviter des conflits entre les serveurs qui tentent d'accéder aux ressources du réseau.

Par exemple, il se peut que des noms de domaine identiques soient définis sur deux réseaux locaux. Aussi longtemps que ces derniers ne sont pas connectés, aucun conflit ne se produit. Cependant, s'ils sont connectés ultérieurement à un réseau local fédérateur, leurs noms sont en conflit sur le réseau local.

Cela signifie que vous devez créer des conventions de dénomination. Il s'agit de règles et de normes permettant d'attribuer des noms aux diverses ressources du réseau.

Les sections suivantes répertorient les conventions de dénomination dont la planification est requise. Si vous connaissez déjà les conventions de dénomination que vous êtes amené à utiliser dans le cadre de la planification, enregistrez-les lors de la planification du réseau.

Critères de dénomination

Lors de la création de conventions de dénomination, vous devez déterminer :

- les critères permettant de créer des noms et des adresses pour votre réseau ;
- la façon dont ces noms et adresses resteront cohérentes et, le cas échéant, uniques au sein du réseau.

En cas de connexion d'un serveur à un réseau d'ordinateurs hôte, par exemple, il se peut que la plupart des noms devant être utilisés sur le réseau soient choisis par le personnel hôte. Dans ce cas, en ce qui concerne les unités physiques et logiques requises par l'hôte, vous devez enregistrer ces noms pour vos fichiers de configuration de serveur.

Pour citer un autre exemple, vous pouvez choisir d'attribuer aux serveurs de votre réseau les noms de leurs utilisateurs. Cela est possible sur un petit réseau aussi longtemps que la quantité des noms est faible et qu'ils peuvent rester uniques. Cependant, cela ne fonctionne pas sur un grand réseau car les noms des utilisateurs ne sont généralement pas uniques. Vous devez créer une autre convention pour les noms de poste de travail d'un grand réseau.

Quels que soient les critères que vous choisissez pour les noms, veillez à les enregistrer. De cette manière, vous pouvez vous reporter aux informations appropriées chaque fois que vous ajouter de nouvelles ressources sur le réseau.

Types de noms et restrictions applicables

La plupart des noms doivent être uniques au réseau sur lequel vous les utilisez. Les sections suivantes répertorient les types de noms que vous pouvez rencontrer lors de la planification, de l'installation et de la configuration d'un réseau. Vous devez vous familiariser avec ces noms avant de commencer la planification du réseau.

Les informations suivantes sont fournies pour chaque nom :

- Une définition
- Caractère unique ou non du nom dans un réseau
- Restrictions de dénomination

Noms utilisés par plusieurs composants

- ID réseau
- Mots de passe
- ID utilisateur
- Noms d'unité adressable de réseau (NAU)

ID réseau : Il s'agit de noms attribués à des réseaux et utilisés par tous les serveurs et postes de travail (nœuds) du réseau spécifique afin de maintenir une identité sur l'ensemble des réseaux connectés. L'ID réseau est également utilisé

dans les journaux d'erreurs et dans les alertes de gestion de réseau associées aux erreurs système du réseau.

Les réseaux peuvent apparaître sous deux formes. La première correspond à un réseau physique constitué d'un “anneau” dans un environnement en anneau à jeton ou d'une “chaîne” dans un environnement de réseau Ethernet ou PC. La deuxième correspond à un réseau logique qui n'est peut-être pas identique au réseau physique. Vous pouvez connecter au moins deux réseaux physiques (par exemple, deux anneaux à jeton et un chaîne Ethernet) afin de les conserver dans le même réseau logique.

Les ID réseau sont uniques entre les réseaux logiques ; dans le cas contraire, les réseaux correspondraient logiquement au même réseau. Dans un réseau logique, les noms de LU doivent être uniques afin d'éviter les conflits de dénomination. L'ID réseau garantit des noms uniques entre les réseaux logiques. Un nom de LU peut le même sur deux réseaux logiques ; cependant, l'ID de chaque réseau logique rend uniques les noms de LU qualifiés. Même si les réseaux ne sont pas actuellement connectés, les ID réseau doivent être uniques si le pontage des réseaux est prévu dans l'avenir.

Vous devez enregistrer vos ID réseau auprès d'IBM. Cela garantit que des réseaux SNA peuvent être interconnectés ultérieurement sans aucun conflits d'adressage. Pour plus de détails sur l'enregistrement de vos ID réseau, prenez contact avec une agence IBM.

Voici les restrictions applicables aux ID réseau :

- **Longueur** : 1 à 8 caractères
- **Caractères admis** : A à Z, 0 à 9, $, @, #

Mots de passe : Il s'agit de fonctions requises par des applications et services configurés de façon appropriée afin de protéger les données et à limiter l'accès aux ressources.

Il n'est pas nécessaire que les mots de passe soient uniques au sein du réseau. Les mots de passes sont spécifiques aux utilisateurs.

Voici les restrictions applicables aux mots de passe LU-LU :

- **Longueur** : 1 à 8 caractères
- **Caractères admis** : toute chaîne hexadécimale

Voici les restrictions applicables aux autres mots de passe, par exemple, ceux des connexions CPI-C et AS/400 :

- **Longueur** : 1 à 10 caractères
- **Caractères admis** : toute chaîne ASCII

ID utilisateur : Les ID utilisateur sont uniques ; ils identifient les noms attribués aux utilisateurs des ressources de réseau de sorte qu'ils puissent accéder aux ressources de base de données, de réseau local, d'hôte qui sont dotées d'une émulation.

Les ID utilisateur doivent être uniques dans le réseau.

Voici les restrictions applicables aux ID utilisateur :

- **Longueur** : 1 à 8 caractères
- **Caractères admis** : A à Z, a à z, 0 à 9, $, @, #

Noms d'unité adressable de réseau (NAU)

Voici les types de noms que vous devez peut-être indiquer dans Communications Server :

- Noms de point de contrôle (noms des nœuds locaux)
- Noms d'unité logique (LU)

Noms de point de contrôle (noms des nœuds locaux) : Le point de contrôle (CP) est responsable de la gestion du nœud et des ressources de ce dernier. Dans un nœud d'extrémité APPN, le point de contrôle doit communiquer avec le point de contrôle d'un nœud de réseau adjacent pour accéder aux services de réseau APPN. Dans un nœud de réseau APPN, le point de contrôle doit communiquer avec les points de contrôle des nœuds de réseau adjacents afin de gérer le réseau. Le point de contrôle dirige des fonctions telles que l'activation et la désactivation des cartes et des liaisons, puis apporte son concours aux LU lors de l'établissement et de l'arrêt des sessions.

Le nom du point de contrôle correspond à la deuxième partie du nom de CP qualifié figurant dans la définition de nœud (NODE) de Communications Server.

Les noms de point de contrôle doivent être uniques dans un réseau. Cependant, un nœud peut comporter plusieurs noms de PU qui sont définis dans la définition de connexion (**LINK_STATION**) et échangés sur XID3 entre différents hôtes. Ces noms de PU multiples doivent être uniques sur le nœud et sur l'hôte qui est en cours de connexion.

La PU et le point de contrôle ne sont pas les mêmes pour un VTAM de secteur. Un nom de PU pour chaque nœud périphérique d'un domaine VTAM est défini au niveau de ce VTAM, et représente la perception des nœuds périphériques par VTAM. Les noms de PU au niveau du VTAM ne sont pas identifiés par les nœuds périphériques ; cela signifie que VTAM n'envoie pas les noms de PU aux nœuds périphériques. Si vous voulez que le nom de PU au niveau d'un nœud périphérique soit identique à celui qui est défini au niveau du VTAM, vous devez en assurer la coordination. Il est conseillé d'effectuer cette opération qui n'est toutefois pas requise pour SNA.

VTAM considère le point de contrôle comme une LU servant à activer des sessions LU 6.2 entre le point de contrôle et une LU VTAM (par exemple, CICS). Le nom de point de contrôle défini au niveau du nœud périphérique doit correspondre à une définition de LU au niveau du VTAM si ce dernier établit des sessions LU 6.2 avec le point de contrôle. Sinon, VTAM identifie le nom de point de contrôle lorsque le nœud périphérique établit une session avec une LU VTAM.

Pour Communications Server, le nom de point de contrôle (l'ID réseau non compris) est traité comme nom de point de contrôle du nœud local et comme son nom de PU. Le seul circuit qui contient le nom de PU du nœud périphérique est une alerte. Cependant, Communications Server (APPC/APPN) envoie une alerte, cette dernière comporte le nom de point de contrôle (le type de ressource est CP) et non un nom de PU. Si des émulateurs envoient un nom de PU dans les alertes,

le nom est identique au nom de point de contrôle (une fois encore car Communications Server utilise le nom de point de contrôle comme nom de PU du nœud). Le point focal hôte ne peut être défini que sur une liaison où le nom de PU est identique au nom de point de contrôle. Par ailleurs, les liaisons hôte dont le nom de PU est différent du nom de point de contrôle ne peuvent pas établir de sessions CP-CP avec l'hôte, ou acheminer un trafic APPN via la liaison. Toutes les alertes comportent le nom de point de contrôle même si l'alerte résulte d'un état sur une liaison qui utilise une autre PU.

Voici les restrictions applicables aux noms des nœuds locaux :

- **Longueur** : 1 à 8 caractères
- **Caractères admis** : A à Z, 0 à 9, $, @, #
- **Premier caractère** : A à Z, $, @, #

Noms d'unité logique (LU)s : Il s'agit de noms attribués aux entités logiques SNA d'un nœud, qui fournissent des fonctions de support pour le traitement de transaction. Elles peuvent ainsi communiquer avec d'autres LU du réseau, notamment avec des applications hôte.

Voici les restrictions applicables aux noms de LU :

- **Longueur** : 1 à 8 caractères
- **Caractères admis** : A à Z, 0 à 9, $, @, #

Noms de LU Sockets sur SNA : La passerelle Sockets sur SNA doit comporter un nom de LU qui est configuré de sorte que l'initialisation de la passerelle aboutisse. Une fois initialisée, la passerelle Sockets sur SNA définira de manière dynamique sur Communications Server le nom de LU configuré.

Une convention de dénomination prédéfinie pour la LU Sockets sur SNA permet aux noms :

- de contrôler quels noms correspondent aux LU de passerelle Sockets sur SNA, et quels noms qui représentent les autres LU de votre réseau ;
- d'analyser et de résoudre les erreurs de mappage et de routage, le cas échéant ;
- d'activer le mappage algorithmique lors du mappage des adresses IP aux noms de LU Sockets sur SNA.

Pour plus de détails sur le mappage des adresses IP aux noms de LU, reportez-vous à la section «Configuration d'AnyNet Sockets sur SNA», à la page 90.

Étape 4. Définition des adresses de réseau

Assurez-vous que l'adresse est cohérente et unique dans votre réseau. Chaque adresse doit être unique. Les adresses que vous définies sont fonction de la configuration du réseau. Les sections ci-après décrivent les adresses suivantes :

- Réseau local
- SDLC
- X.25

Enregistrez les adresses que vous utilisez pour vous assurer, le cas échéant, qu'aucune des adresses n'est en conflit et qu'elles sont conformes aux conventions de dénomination choisies.

Adresses de carte de réseau local

Il s'agit de nombres hexadécimaux à 12 caractères, codés dans la carte par le constructeur (adresse de carte administrée universellement), ou attribués par l'administrateur de réseau (adresse administrée en local). Chaque carte de réseau du poste de travail que vous configurez pour des communications de réseau local doit comporter une adresse unique.

Vous pouvez utiliser pour vos cartes de réseau les adresses administrées universellement, également désignées par «adresses gravées (burned-in)», ou vous pouvez attribuer des adresses administrées en local. Les adresses de carte de réseau local doivent être uniques au sein du réseau. Si vous utilisez des adresses administrées en local, assurez-vous qu'elles sont uniques au sein du réseau.

Les adresses administrées en local présentent un avantage important dans le cas d'une défaillance de carte nécessitant le remplacement de la carte. Vous pouvez transférer l'adresse existante vers la carte de remplacement, et éviter de modifier les configurations qui font référence à cette adresse. Si vous utilisez des adresses administrées universellement, vous devez modifier l'adresse de carte de réseau de tous les postes qui accèdent à la carte défectueuse.

Voici les restrictions applicables à la configuration des adresses de carte de réseau local :

- **Longueur** : 12 caractères
- **Caractères admis** : A, B, C, D, E, F, 0 à 9
- **Plage**: X'400000000000' à X'7FFF FFFF FFFF'

Sur le réseau local, vous pouvez choisir d'utiliser des adresses de carte de réseau local administrées en local. Ainsi, vous affectez des nombres hexadécimaux sous forme d'adresses de carte de réseau local à chacune des cartes de réseau local, au lieu d'utiliser les adresses de carte de réseau local universelles intégrées aux cartes de réseau local. Vous pouvez décider d'utiliser une convention dont les critères sont les suivants :

- Les quatre premiers chiffres sont toujours X'4000'
- Les 3 chiffres suivants sont toujours X'268', représentant votre département
- Les dernier chiffres sont compris entre X'01000' et X'FFFFF', représentant les postes de travail individuels de votre réseau

Les adresses administrées universellement sur Ethernet sont au format Ethernet. Vous pouvez indiquer le type de format (Ethernet ou Token-Ring) lors de l'utilisation des adresses administrées en local. Lors de la configuration de l'adresse de destination des connexions SNA, assurez-vous que le format d'adresse est identique à celui qui est indiqué à l'extrémité éloignée. Dans le cadre d'un pontage, le poste local peut être situé sur un anneau à jeton en local et le poste éloigné sur un Ethernet, tout en utilisant une adresse au format Ethernet (permutation d'octets).

Adresses de poste secondaire SDLC

Les adresses de poste servent à identifier un poste secondaire sur le réseau.

Les adresses de poste secondaire doivent être uniques au sein d'un réseau. Le poste principal communique avec un poste secondaire à l'aide de l'adresse de ce dernier. Le poste secondaire communique avec le poste principal à l'aide de sa propre adresse.

Pour les connexions point à point, si le poste secondaire prend en charge l'adresse de diffusion X'FF', le poste primaire identifie l'adresse du poste secondaire. Ce dernier peut indiquer n'importe quelle valeur comprise entre X'01' et X'FE'.

Pour les postes principaux qui ne prennent pas en charge l'adresse de diffusion, le poste secondaire doit comporter la même valeur que celle définie sur le poste principal. Cette valeur doit être comprise entre X'01' et X'FE'.

Remarque : La plupart des postes prennent en charge l'adresse de diffusion ; l'adresse de poste secondaire au niveau du poste principal doit donc utiliser X'FF'.

Les postes négociables comportent des adresses de poste secondaire locales configurées entre X'01' et X'FE'. L'adresse secondaire du poste négocié comme secondaire sera utilisée.

Pour les postes secondaires résidant sur une connexion multipoint, l'adresse doit correspondre à la valeur indiquée au niveau du nœud qui fournit la fonction de serveur principal multipoint. L'adresse sera comprise entre X'01' et X'FE'.

Adresses X.25

Les adresses X.25 servent à identifier les ressources communiquant sur des réseaux X.25. Ces derniers mettent en œuvre la recommandation CCITT définissant l'interface entre les équipements terminaux de données et les réseaux de commutation par paquets. Les adresses X.25 doivent être uniques au sein d'un réseau. Vous pouvez vous procurer ces adresses auprès de votre fournisseur de réseau X.25.

Adresses Internet

Les adresses IP (Internet Protocol) servent à acheminer des données via le réseau. Au moins une adresse IP unique est affectée à chaque hôte TCP/IP. L'adresse IP affectée à l'hôte ne définit pas ce dernier sur le réseau ; elle permet à un réseau d'identifier l'interface de réseau de cet hôte.

Un nœud Communications Server doit comporter une adresse IP unique pour chaque interface de réseau qui achemine des données TCP/IP via le nœud. Par exemple, un nœud Communications Server qui achemine le trafic TCP/IP sur un réseau SNA (à l'aide de la fonction de passerelle Sockets sur SNA) requiert des adresses IP uniques pour le réseau SNA et pour le réseau TCP/IP. L'adresse IP de l'interface TCP/IP identifie la connexion de passerelle Sockets sur SNA au réseau IP, alors que l'adresse IP identifie la connexion au réseau SNA qui apparaît, pour le système, comme un réseau TCP/IP "virtuel".

Une adresse IP est constituée de deux zones d'adresses 32 bits :

- La première partie contient l'adresse du réseau et la deuxième l'adresse de l'hôte.
- Le nombre de bits utilisés pour les zones réseau et hôte d'une adresse IP varie en fonction de la classe de l'adresse IP.
- Un masque de réseau permet d'utiliser une partie de la zones hôte de l'adresse IP sous forme d'adresse de sous-réseau.

La classe de l'adresse IP est déterminée à l'aide des 3 premiers bits (supérieurs) de l'adresse. Comme l'indique le tableau 33, Communications Server prend en charge les classes d'adresse A, B et C. Pour plus de détails, consultez le manuel *Guide to Sockets over SNA*.

Tableau 33. Classes d'adresse IP prises en charge par Communications Server

Classe d'adresse	**Masque de réseau par défaut**	**Répartition des bits pour les adresses réseau et hôte**	**Pour une adresse IP en notation décimale au format *a.b.c.d*, la plage de valeurs de *a* est :**
A	255.0.0.0	Adresse de réseau 8 bits ; Adresse hôte 24 bits	1 à 127 Par exemple, 9.0.0.0 est une adresse de réseau IP de classe A.
B	255.255.0.0	Adresse de réseau 16 bits ; Adresse hôte 16 bits	128 à 191 Par exemple, 132.11.0.0 est une adresse de réseau IP de classe B.
C	255.255.255.0	Adresse de réseau 24 bits ; Adresse hôte 24 bits	192 à 223 Par exemple, 220.11.44.0 est une adresse de réseau IP de classe C.

Étape 5. Choix des outils de configuration et d'installation

Communications Server utilise les outils de configuration décrits dans les sections suivantes. Pour plus de détails sur ces outils, consultez le *Guide d'utilisation*.

Application Configuration du nœud

L'application **Configuration du nœud** est une application de fenêtre graphique qui permet la gestion des informations de configuration SNA. L'application utilise une vue arborescente pour organiser les données de configuration SNA de sorte qu'elles montrent les relations entre les définitions. L'utilisateur reçoit une assistance lors de la création d'une configuration via une liste de tâches intégrées, le *Tutoriel* en ligne et l'aide contextuelle. L'application est responsable de la création des fichiers de configuration pour l'utilisateur, ainsi que de la vérification des données fournies.

Configuration éloignée

L'application **Configuration du nœud** permet également la connexion à un serveur Communications Server éloigné et la configuration directe des ressources de celui-ci. L'utilisateur peut gérer à distance la configuration d'un serveur Communications Server à n'importe quel endroit du réseau.

Un client d'administration éloignée n'installe que les applications administratives sur un poste client, notamment l'application **Configuration du nœud**. À partir de ce poste client, un utilisateur est en mesure d'administrer et de configurer en intégralité tout serveur Communications Server du réseau.

Les clients d'administration éloignée Windows 95 et Windows NT utilisent la sécurité de domaine Windows NT pour authentifier la connexion du client au serveur sans que l'ID utilisateur et le mot de passe soient ré-entrés. Le client doit faire partie d'un domaine Windows NT en participant dans un domaine de Communications Server ou à l'aide d'une connexion locale à un ID utilisateur et un ot de passe synchronisés.

Les clients d'administration éloignée situés à l'extérieur du domaine Windows NT sont tenus de fournir l'ID utilisateur et le mot de passe par le biais d'une invite ou en stockant ces valeurs dans le fichier de configuration client.

Les utilisateurs autorisés des clients d'administration éloignée sont maintenus dans le groupe local IBMCSADMIN qui est situé directement sur Communications Server ou sur le contrôleur de domaine dans lequel Communications Server participe. Ce groupe d'utilisateurs est créé lors de l'installation et peut être administré à l'aide de l'application Gestionnaire d'utilisateurs Windows NT. Les utilisateurs des clients d'administration éloignée doivent détenir de droits d'accès au groupe IBMCSADMIN pour se connecter en local au serveur.

Fichier de configuration ASCII

L'application **Configuration du nœud** de Communications Server stocke ses données de configuration dans un fichier de configuration ASCII lisible par l'utilisateur. Ce dernier peut ainsi modifier les fichiers de configuration sans utiliser l'application **Configuration du nœud**. (Pour plus de détails sur ce fichier et sur sa syntaxe, consultez le manuel *Configuration File Reference*.) Ce fichier permet à un administrateur de réseau d'apporter rapidement des modifications à la configuration à l'aide de tâches automatisées telles que les services de script ou de distribution logicielle, par exemple, Tivoli TME10 ou Microsoft System Management Server.

Lors de la création des configurations destinées à un grand nombre de serveurs, l'administrateur de réseau peut créer un modèle de fichier de configuration qui représente les éléments de configuration communs à tous les serveurs. L'administrateur peut, à l'aide d'un fichier réponses comportant uniquement les modifications nécessaires à chaque serveur, diffuser le fichier modèle et le fichier réponses, puis fusionner les deux pour créer la configuration cible. Pour plus de détails sur l'utilisation des fichiers modèles et réponses destinés aux opérations de configuration et d'installation, reportez-vous à la section «Configuration à l'aide de fichiers modèles et réponses», à la page 196.

Administration Web

L'administration Web permet à un utilisateur de modifier un fichier de configuration Communications Server en chargeant le fichier dans une fenêtre d'édition. Les modifications sont envoyées au serveur, vérifiées, et sauvegardées pour être utilisées immédiatement. L'utilisateur peut soit arrêter et relancer le serveur à l'aide des modifications apportées, soit appliquer les modifications de configuration à un système en cours d'exécution.

Configuration à l'aide de fichiers modèles et réponses

Les fichiers modèles et réponses de Communications Server permettent de créer ou de modifier une configuration à l'aide d'un éditeur. Vous pouvez configurer tous les mots clés et paramètres de configuration de Communications Server, à l'aide de fichiers réponses. Les fichiers modèles et réponses ont le même format que les fichiers de configuration (.ACG) de Communications Server.

Remarque : Le format des fichiers .ACG est documenté dans le fichier OCDNTS50.DAT qui se trouve dans le répertoire d'installation de Communications Server (par exemple, C:\IBMCS). Pour plus de détails sur les mots clés et les paramètres utilisés dans les fichiers .ACG, consultez le manuel *Configuration File Reference*.

Les modèles de fichier peut faciliter la diffusion en série des configuration aux serveurs éloignés. Un modèle de fichier peut indiquer les mots clés communs à plusieurs serveurs. Par exemple, si plusieurs serveurs doivent être configurés comme passerelles SNA avec un support client implicite, la plupart des mots clés seront identiques Vous pouvez créer un modèle de fichier de configuration qui reflète ces mots clés communs.

Les fichiers réponses permettent d'ajouter, de modifier ou de supprimer des mots clés dans un fichier modèle. Le fichier de configuration modèle reste inchangé. Un fichier réponses est fusionné dans un fichier modèle lorsque le mot clé INCLUDE est indiqué à la fin d'un fichier modèle. Par exemple, si un fichier réponses est intitulé *maconfig.rsp*, la dernière ligne du fichier modèle qui utilisera le fichier réponses est `INCLUDE = maconfig.rsp`. Lors de la fusion du fichier modèle et du fichier réponses, vous pouvez attribuer au fichier de configuration résultant un nom comportant le suffixe .ACG qui permet de distinguer ce fichier des autres autres fichiers .ACG.

Lors de la création de configurations à l'aide de fichiers modèles et réponses, l'utilitaire de vérification effectue une recherche dans les répertoires dans l'ordre suivant :

1. Le répertoire local dans lequel l'utilitaire de vérification est appelé.
2. Le sous-répertoire PRIVATE du répertoire d'installation de Communications.

Pour assurer que l'utilitaire de vérification peut localiser les fichiers modèle et réponse, vous devez stocker ces derniers dans le sous-répertoire PRIVATE. Celui-ci se trouve également dans l'emplacement des fichiers de configuration (.ACG).

Zones clés

La zone clé correspond au paramètre d'un mot clé, qui attribue à ce dernier un nom et qui permet de le distinguer des autres mots clés du même type. Le paramètre @KEY_NAME indique la zone clé du mot clé.

La zone clé correspond systématiquement au premier paramètre d'un mot clé comportant une zone clé (par exemple, **MODE_NAME** dans le mot clé **MODE**).

Certains mots clés ne comportent pas de zones clés car ils ne peuvent être indiqués qu'une seule fois dans un fichier de configuration, par exemple, le mot clé **TN3270E_DEF**.

Ajout de mots clés dans un fichier modèle

Lors de l'utilisation du fichier réponses pour l'ajout d'une nouvelle définition de mot clé, le mot clé doit être entré en intégralité. La zone clé doit être indiquée avec une valeur unique. Si des sous-zones sont omises dans le mot clé, les valeurs par défaut de ces zones sont utilisées. Par exemple, pour ajouter un mot clé **MODE** dans la configuration, il se peut que le fichier réponses contienne le mot clé suivant :

```
MODE=(
     MODE_NAME=MYMODE
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4␣96
     MIN_CONWINNERS_SOURCE=4␣96
)
```

Le contenu du fichier réponses laisse supposer que le modèle ne contient pas de mot clé **MODE** comportant le paramètre `MODE_NAME=MYMODE`. S'il en contient, les paramètres auraient été mis à jour à l'aide des valeurs fournies dans le fichier réponses.

Si le paramètre `MODE_NAME` a été omis dans le fichier réponses, une erreur se produit lors de la vérification de la configuration car le paramètre `MODE_NAME` ne peut pas être identifié de manière unique Tous les paramètres disponibles pour le mot clé **MODE** n'ont pas été indiqués dans le fichier réponses. Les paramètres restants utilisent les valeurs par défaut affectées par le fichier OCDSNT50.DAT. Voici le résultat des mots clés ajoutés dans la configuration :

```
MODE=(
     MODE_NAME=MYMODE
     AUTO_ACT=␣
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4␣96
     MIN_CONWINNERS_SOURCE=4␣96
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=2␣
)
```

Modification d'un mot clé dans un fichier modèle

Lors de l'utilisation du fichier réponses pour la modification d'une définition de mot clé existante, le fichier modèle doit contenir le mot clé d'origine. Sinon, le fichier réponses ajoute une entrée dans la nouvelle configuration. Le paramètre clé doit être indiqué dans le fichier réponses pour identifier le mot clé cible. Seuls les paramètres indiqués dans le mot clé du fichier réponses sont mis à jour dans le mot clé du fichier modèle. Les paramètres non indiqués dans le fichier réponses restent inchangés.

Par exemple, si le fichier modèle contient le mot clé **MODE** suivant :

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=▫
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4▫96
     MIN_CONWINNERS_SOURCE=4▫96
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=2▫ )
```

et que le mot clé suivant est indiqué dans le fichier réponses :

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=1▫
)
```

la configuration qui en résulte comporte la définition de mot clé **MODE** suivante :

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=1▫
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4▫96
     MIN_CONWINNERS_SOURCE=4▫96
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=2▫
)
```

Suppression d'un mot clé d'un fichier modèle

Lors de l'utilisation du fichier réponses pour la suppression d'un mot clé du modèle, la valeur et le paramètre clé qui identifient le mot clé doivent être indiqués, ainsi que le mot clé `DELETE`. Par exemple, si le fichier modèle indique le mot clé suivant :

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=▫
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4▫96
     MIN_CONWINNERS_SOURCE=4▫96
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=2▫
)
```

et que le fichier réponses contient le mot clé suivant :

```
MODE=(
     MODE_NAME=#INTER
     DELETE
)
```

la configuration qui en résulte ne contient pas la définition de mode `#INTER`.

Le mot clé **DELETE** peut apparaître après une spécification *paramètre=valeur* ou seul sur une ligne, précédant le paramètre ou venant à la suite de celui-ci. Par exemple, les utilisations suivantes du mot clé **DELETE** sont admises :

```
MODE=(
     MODE_NAME=#INTER
     DELETE
)
MODE=(
     DELETE
     MODE_NAME=#INTER
)
MODE=(
     MODE_NAME=#INTER DELETE
)
```

Le mot clé **DELETE ne peut pas** apparaître en regard d'une spécification *paramètre=valeur* sur la même ligne. Par exemple, l'utilisation suivante du mot clé **DELETE** est admise :

```
MODE=(
     DELETE MODE_NAME=#INTER
)
```

Pour supprimer tous les mots clés d'un type particulier ou pour supprimer un seul mot clé qui ne comporte pas de zone clé, seul ce mot clé et le mot clé **DELETE** sont nécessaires. Par exemple,

```
TN327␣E_DEF=(
            DELETE
)
```

Étape 6. Choix des fonctions de Communications Server

Les fonctions prises en charge pour Communications Server sont décrites ci-dessous. Il se peut que tout ou partie de ces fonctions soient prises en charge pour votre type de connexion :

Configuration de passerelle SNA La configuration d'une passerelle SNA permet d'échanger des données entre des postes de travail client en aval et un ordinateur hôte SNA (Systems Network Architecture). La passerelle sert de concentrateur pour rendre les ressources de LU d'un ou de plusieurs hôtes et PU hôte accessibles aux postes de travail client SNA en aval, par le biais des supports de communication pris en charge par Communications Server.

Configuration du serveur TN3270E La configuration d'un serveur TN3270E permet d'échanger des données entre des postes de travail client TCP/IP en aval exécutant des applications TN3270E (ou TN3270), et un ordinateur hôte SNA (Systems Network Architecture). Le serveur sert de concentrateur pour rendre les ressources de LU d'un ou de plusieurs

hôtes et PU hôte accessibles aux sessions TN3270E (ou TN3270) en aval, par le biais des supports de communication pris en charge par Communications Server.

Configuration du serveur TN5250 La configuration d'un serveur TN5250 permet d'échanger des données entre des postes de travail client en aval d'un réseau TCP/IP exécutant des applications TN5250, et un système AS/400 d'un réseau SNA. Le serveur sert de passerelle pour rendre les sessions d'écran AS/400 accessibles aux clients TN5250 en aval par le biais des supports de communication pris en charge par Communications Server.

Configuration du nœud de réseau APPN Les nœuds de réseau sont responsables du maintien et du routage des informations via un réseau APPN. Ils maintiennent un répertoire de toutes les ressources (LU) disponibles sur des nœuds d'extrémité connectés directement, ainsi qu'une topologie de tous les nœuds du réseau APPN. Lorsqu'une session LU 6.2 indépendante est demandée par un nœud sur le réseau, le nœud de réseau est chargé de localiser la ressource éloignée demandée par la session et d'établir et d'acheminer la session entre les deux .

Configuration DLUR/DLUS Communications Server prend en charge des sessions LU dépendantes via des réseaux APPN. À cet effet, Communications Server doit servir de DLUR (demandeur de LU dépendantes) demandant des services de routage à un serveur de LU dépendantes (DLUS) qui réside sur un hôte.

Communications Server prend en charge le DLUR pour les sessions et périphériques locaux, ainsi que pour les sessions et périphériques en aval. Dans l'un ou l'autre cas, le nœud local doit être configuré de sorte qu'il se connecte à un réseau APPN.

Configuration de la passerelle AnyNet SNA sur TCP/IP La passerelle SNA sur TCP/IP achemine le trafic SNA (LU 6.2 indépendante) entre des réseaux TCP/IP et SNA. La passerelle SNA sur TCP/IP permet, par exemple, aux applications APPC ou CPI-C qui s'exécutent sur un autre nœud d'accès AnyNet SNA sur TCP/IP de communiquer avec des nœuds d'égal à égal SNA sur un réseau SNA.

La passerelle AnyNet SNA sur TCP/IP doit être configurée sous forme de nœud de réseau APPN. Ainsi, des sessions APPC peuvent être acheminées à des nœuds d'égal à égal SNA appropriés.

Configuration d'AnyNet Sockets sur SNA Les deux types de nœuds AnyNet Sockets sur SNA sont disponibles : nœuds d'accès et nœuds de passerelle. Les nœuds d'accès permettent aux applications sockets TCP/IP d'être exécutées en local et de communiquer avec d'autres passerelles ou nœuds d'accès du réseau SNA. La passerelle AnyNet Sockets sur SNA sert de convertisseur de protocole, permettant à des applications d'un réseau TCP/IP de communiquer avec des applications sockets exécutées sur un nœud d'accès du réseau SNA. Deux passerelles permettent la connexion de réseaux TCP/IP distincts via un réseau SNA.

Configuration du client API SNA Les clients API SNA sont des machines distinctes du serveur Communications Server ; ils peuvent exécuter des applications SNA lors de l'utilisation du code SNA sur le nœud Communications Server, afin de gérer effectivement la session.

Communications Server établit simplement une session et gère cette dernière comme si l'origine était le nœud local ; cependant, il transmet les données d'application au client API SNA et non à ses propres API d'application.

Les clients API SNA permettent d'exécuter des applications SNA sans avoir à installer sur la même machine une pile de communication SNA telle que le serveur Communications Server pour Windows NT. De petites machines moins puissantes peuvent ainsi être utilisées pour exécuter les applications SNA alors qu'une machine centralisée plus puissante peut être dédiée comme serveur SNA à ces clients API SNA.

Les clients API SNA prennent en charge les deux types d'applications suivants : applications APPC (LU 6.2 indépendante) et applications API LUA, par exemple, les émulateurs 3270.

Configuration CPI-C ou APPC Communications Server prend en charge des applications CPI-C ou APPC (par exemple, l'émulation APPC3270 ou 5250 sur un système AS/400). La gestion de réseau APPC est très souple et polyvalente ; par conséquent, elle peut être compliquée. La complexité de cette configuration dépend de la façon dont vous êtes amené à utiliser Communications Server et de la quantité de travail effectuée pour vous par l'application.

Sessions LU 6.2 dépendantes avec un hôte Communications Server prend en charge des sessions LU 6.2 dépendantes avec une PU hôte.

Configuration 3270 Communications Server prend en charge des sessions 3270 avec un hôte.

Configuration des points focaux Communications Server prend en charge la localisation des points focaux éloignés aux fins de routage des infirmations d'alerte pour des applications de services de gestion spécifiques. Le nœud local repère des points focaux éloignés via un réseau APPN.

Configuration des dossiers partagés AS/400 Communications Server permet de créer sur le serveur des unités de disque communiquant avec des dossiers AS/400 via le système de fichiers intégré (IFS) AS/400. Si le serveur partage ces unités de disque, les clients peuvent se connecter à elles à l'aide de la commande NET USE. Plusieurs clients peuvent ainsi se connecter aux dossiers du système AS/400 comme s'il s'agissait d'unités sur leurs postes de travail.

Étape 6.1 - Planification des programmes d'application

Assurez-vous que vos applications remplissent les conditions requises, notamment pour le éléments suivants :

- Modes
- Programmes de transactions (TP)
- Définitions de LU (hôte, LU 6.2)
- LU partenaires

Étape 7. Création de configurations et installation

Vous devez déterminer la façon dont Communications Server sera configuré et installé sur les serveurs de l'utilisateur. Vous pouvez procéder comme suit :

- Fournissez aux utilisateurs des instructions d'installation et de configuration de Communications Server. Vous pouvez préparer vos propres instructions ou imprimer des exemplaires du *Guide d'utilisation*. Vous devez également fournir les informations spécifiques relatives à chaque serveur, par exemple, l'ID réseau, le nom de point de contrôle et l'adresse de réseau.
- Fournissez aux utilisateurs des instructions relatives à l'installation de Communications Server à l'aide d'un fichier modèle ou un fichier de configuration existant. Vous devez également fournir un fichier réponses pour chaque serveur, ainsi que des CD Communications Server ou l'image à des images de CD.
- Configurez et installez vous-même Communications Server sur des serveurs d'utilisateur. Sauf si vous disposez d'un petit groupe d'utilisateurs, vous pouvez envisager l'utilisation d'un produit d'aide à la configuration, à l'installation et à la distribution des logiciels sur plusieurs postes de travail. Il s'agit, par exemple, des produits suivants : IBM NetView Distribution Manager/2 (NVDM/2), Tivoli TME-10 et Microsoft System Management Server (SMS).

Configuration et installation d'un fichier réponses

Si vous choisissez d'utiliser la configuration et l'installation d'un fichier réponses, reportez-vous à la section «Configuration à l'aide de fichiers modèles et réponses», à la page 196.

Étape 8. Création de matériels utilisateur

Après avoir planifié le réseau et déterminé la façon dont vous mettez en œuvre le plan, vous devez créer des matériels utilisateur. Cela signifie que vous devez préparer la documentation relative à l'installation, à la configuration et à l'utilisation quotidienne, ainsi que des procédures de sauvegarde.

Préparation de la documentation

Préparez un jeu de documentation personnalisée pour aider les utilisateurs à installer, à configurer et à utiliser Communications Server et les applications locales répondant à leurs besoins particuliers. Les sections suivantes contiennent des recommandations concernant le type d'informations à inclure.

Matériels et procédures de configuration et d'installation

Le *Guide d'utilisation* et des aides en ligne permettent aux utilisateurs d'installer Communications Server. Les instructions que vous fournissez aux utilisateurs doivent permettre à ces derniers de choisir parmi les étapes suivantes lors de l'installation du logiciel :

- Moment de sauvegarde des fichiers de configuration
- Acceptation ou non des valeurs par défaut pour la création d'un fichier de configuration Communications Server

  Vous devez peut-être fournir des informations de réseau, par exemple, les adresses de carte de réseau local, les noms de réseau, etc.
- Moment d'installation à l'aide d'un fichier réponse que vous avez fourni

- Moment d'installation à l'aide d'un fichier de configuration personnalisé que vous avez fourni

Si nécessaire, fournissez aux utilisateurs la documentation appropriée.

Matériels et procédures de Communications Server

Les matériels suivants sont recommandés pour l'utilisation des API et fonctions de Communications Server :

- *Guide d'utilisation*
- Programmes écrits par l'utilisateur pour les API Communications Server choisis

Démarrage et arrêt de Communications Server

Pour plus de détails sur la procédure de démarrage ou d'arrêt de Communications Server, consultez le *Guide d'utilisation*.

Si des instructions de démarrage et d'arrêt différentes sont disponibles, celles-ci doivent être fournies aux utilisateurs.

- Numéro de téléphone d'aide hôte aux fins d'identification des incidents (prenez contact avec votre personnel hôte)
- Procédures d'ouverture de session relatives aux applications et systèmes hôte
- Procédure d'arrêt de l'application hôte

  Prise de contact avec le personnel hôte
- Procédures de fermeture de session

  Vos instructions doivent inclure les conditions particulières requises pour la déconnexion des systèmes ou applications. Vous pouvez vous procurer ces informations auprès du personnel hôte.

Matériels et procédures relatifs aux programmes d'application

Vous devez fournir aux utilisateurs des procédures et d'autres informations relatives aux programmes d'application que vous utilisez peut-être sur le réseau. En général, vous devez fournir les éléments suivants :

- Procédures de démarrage des programmes d'application
- Procédures d'exécution des programmes d'application
- Procédures de réponse aux messages générés par le programme d'application
- Procédures d'identification des incidents
- Si nécessaire, procédures d'arrêt du programme d'application

Pour obtenir les informations précédentes, prenez contact avec le programmeur d'application.

Matériels et procédures d'identification des incidents

Pour plus de détails sur les procédures d'identification et de signalisation des incidents, consultez le *Guide d'utilisation*.

Préparation des procédures de sauvegarde

Il se peut que les utilisateurs effacent ou modifient les fichiers de configuration, un registre, un système de fichiers, des programmes d'application et d'autres programmes ou fichiers créés en local. De même, les serveurs risquent d'être confrontés à des opérations d'effacement ou de modifications inacceptables, notamment lorsque de nombreux utilisateurs accèdent aux postes de travail du serveur tout au long de la journée de travail.

Pour cette raison, vous devez préparer et documenter les procédures de sauvegarde relatives à votre réseau. Vous pouvez également définir les attributs de certains fichiers de vos serveurs en lecture seule, de sorte que les utilisateurs ne puissent pas les modifier.

Étape 9. Maintenance du réseau

Une fois que la planification, l'installation et la configuration du réseau sont terminées et que celui-ci s'exécute sur une base quotidienne, il ne vous reste qu'à effectuer la tâche de maintenance. Vous devez planifier l'ajout, la modification ou la suppression des ressources et utilisateurs de votre réseau, ainsi que la résolution des incidents.

Vous devez effectuer le même niveau de planification et de mise en œuvre pour les modifications apportées au réseau dans le cadre de la configuration initiale. Pour ces modifications apportées au réseau, vous devez suivre les mêmes étapes utilisées lors des opérations de planification, d'installation et de configuration initiales.

Communications Server fournit ces outils pour vous permettre de surveiller les performances quotidiennes du réseau :

- **Fonctionnement du nœud SNA**
- Utilitaires de la ligne de commande
- Administrateur Web
- Client d'administration éloignée
- API de gestion système
- Sous-agent SNMP
- Moniteur de performances NT

Les produits suivants peuvent également vous aider dans la gestion quotidienne de votre réseau :

- IBM NetView
- IBM LAN Network Manager
- Tivoli TME-10

Contrôle et maintenance d'un réseau

Outils de gestion système

Le présent chapitre donne un aperçu des outils de gestion du système Communications Server et décrit les capacités communes à chaque outil. Chaque outil comporte également quelques fonctions uniques qui sont décrites pour chaque outil.

Les outils de gestion système permettent de surveiller et de contrôler les ressources de communication de Communications Server. Ils servent également à ajuster ces ressources pour améliorer l'efficacité des services de communication SNA ou pour surveiller et tester ces services lors de l'identification des incidents.

Pour obtenir une liste des ressources que vous pouvez gérer, consultez le *Guide d'utilisation*.

Vous pouvez gérer Communications Server à l'aide des outils suivants :

- **Fonctionnement du nœud SNA**
- Administration éloignée
- Utilitaires de la ligne de commande
- Administration basée sur le Web
- Contrôle ActiveX du Fonctionnement de nœud SNA
- Module Tivoli Plus
- Support MIB APPN
- Support ROPS (Remote Operations Support) IBM 390

Vous pouvez utiliser toute combinaison de ces outils pour la gestion de Communications Server.

Fonctions communes des outils de gestion système

Chaque outil de gestion système peut effectuer les actions suivantes destinées aux ressources :

- Affichage des informations relatives aux ressources
- Démarrage des ressources
- Arrêt des ressources
- Suppression de ressources
- Activation des changements de chemin

Vous pouvez effectuer un sous-ensemble de ces actions pour chaque ressource, comme indiqué dans le tableau 34, à la page 208.

Tableau 34. Actions de gestion des ressources de Communications Server

Ressource	Affichage	Démarrage	Arrêt	Suppression	Changement de chemin
Connexions	X	X	X	X	
Informations annexes CPI-C	X			X	
Périphériques	X	X	X	X	
PU DLUR	X	X	X		
LU 0 à 3 locales	X			X	
LU 6.2 locale	X			X	
Sessions LU 6.2	X		X		
Passerelle PU 2.0/DLUR	X			X	
Connexions RTP	X				X
Sessions TN3270E	X		X		
Sessions TN5250	X		X		

Fonctionnement du nœud SNA

Fonctionnement du nœud SNA est un utilitaire en ligne permettant la surveillance et le contrôle des ressources de communication maintenues par Communications Server. Il permet d'arrêter, de démarrer et de surveiller les ressources de votre réseau.

Vous pouvez utiliser l'utilitaire **Fonctionnement du nœud SNA** pour gérer les ressources de votre réseau. Les fonctions de programmation de gestion système de Communications Server vous permettent de configurer et de gérer les nœuds de votre réseau SNA. L'utilitaire **Fonctionnement du nœud SNA** fournit une vue arborescente de votre configuration, permettant de sélectionner et de modifier des ressources dans une interface graphique hiérarchique.

Vous pouvez gérer plusieurs fenêtres dans la fenêtre principale de **Fonctionnement du nœud SNA**.

Vous pouvez définir plusieurs configurations de Communications Server et passer d'une configuration à l'autre en fonction de vos besoins. Lors du démarrage de Communications Server, la configuration par défaut correspond au premier choix de configuration ou de fonctionnement du nœud, sauf si vous indiquez une autre configuration. Une fois qu'une une nouvelle configuration a été effectuée, celle-ci peut remplacer la configuration par défaut. Utilisez l'utilitaire **Fonctionnement du nœud SNA** pour appliquer la nouvelle configuration et pour vous assurer que la partie correspondante du produit s'exécute comme vous l'avez configurée.

L'utilitaire **Fonctionnement du nœud SNA** permet de lancer d'autres programmes de Communications Server tels que **Afficheur de journaux**, **Utilitaire de trace** ou **Configuration du nœud**.

Administration éloignée

L'utilitaire **Fonctionnement du nœud SNA** permet également la connexion à un serveur Communications Server éloigné et l'administration directe des ressources de celui-ci. L'utilisateur peut gérer à distance les ressources d'un serveur Communications Server à n'importe quel endroit du réseau.

Un client d'administration éloignée n'installe que les applications administratives sur un poste client, notamment l'utilitaire **Fonctionnement du nœud SNA**. À partir de ce poste client, un utilisateur est en mesure d'administrer en intégralité tout serveur Communications Server du réseau.

Les clients d'administration éloignée Windows 95 et Windows NT utilisent la sécurité de domaine Windows NT pour authentifier la connexion du client au serveur sans que l'ID utilisateur et le mot de passe soient ré-entrés. Le client doit faire partie d'un domaine Windows NT en participant dans un domaine de Communications Server ou à l'aide d'une connexion locale à un ID utilisateur et un ot de passe synchronisés.

Les clients d'administration éloignée situés à l'extérieur du domaine Windows NT sont tenus de fournir l'ID utilisateur et le mot de passe par le biais d'une invite ou en stockant ces valeurs dans le fichier de configuration client.

Les utilisateurs autorisés des clients d'administration éloignée sont maintenus dans le groupe local IBMCSADMIN qui est situé directement sur Communications Server ou sur le contrôleur de domaine dans lequel Communications Server participe. Ce groupe d'utilisateurs est créé lors de l'installation et peut être administré à l'aide de l'application Gestionnaire d'utilisateurs Windows NT. Les utilisateurs des clients d'administration éloignée doivent détenir de droits d'accès au groupe IBMCSADMIN pour se connecter en local au serveur.

Programmes de la ligne de commande

Les programmes de la ligne de commande permettent d'émettre des commandes à partir d'une invite Windows NT. La sortie des commandes s'affiche mais elle peut être redirigée vers un fichier.

Pour obtenir une liste des programmes de ligne de commande que vous pouvez utiliser, consultez le *Guide d'utilisation*.

Administration Web

Cette fonction de Communications Server permet de gérer le serveur sur un réseau Intranet à partir de tout système sur lequel un navigateur Web est installé. Pour utiliser la fonction d'administration Web, un serveur Web doit être en cours d'exécution sur la même machine que Communications Server. Vous pouvez gérer plusieurs serveurs Communications Server, mais vous ne pouvez accéder qu'à un seul serveur à la fois. Pour effectuer des fonctions administratives, les utilisateurs doivent se connecter à la fonction d'administration Web en tant que membre du groupe IBMCSADMIN sur la machine Windows NT qui exécute Communications Server.

Cette fonction peut être installée à partir du CD-ROM de Communications Server. La plupart des fonctions de l'utilitaire **Fonctionnement du nœud SNA** sont disponibles via un navigateur Web. Vous pouvez interroger l'état du nœud, accéder aux informations relatives aux ressources, modifier ces dernières, afficher et éditer des fichiers de configuration, afficher des journaux de messages et effectuer d'autres tâches administratives. La fonction d'administration Web permet également d'éditer des fichiers de configuration et de visualiser le fichier journal. Les étapes requises pour l'utilisation de ces fonctions sont documentées sur la page Web **Bienvenue dans le programme Web Administration de Communications Server**.

Contrôle ActiveX du Fonctionnement du nœud SNA

Une version de contrôle ActiveX de l'utilitaire **Fonctionnement du nœud SNA** est disponible. Ce contrôle permet d'inclure **Fonctionnement du nœud SNA** dans toute application permettant des contrôles intégrés, par exemple, Microsoft Management Console (MMC). Le contrôle est intitulé CSNTACTX et situé dans le répertoire d'installation du produit. Ce contrôle est doté de toutes les fonctions de l'utilitaire **Fonctionnement du nœud SNA** et permet d'intégrer ce dernier dans d'autres applications, afin de permettre une gestion croisée des produits.

Module Tivoli Plus

Si TME (Tivoli Management Environment) est utilisé pour la gestion centralisée des périphériques et applications du réseau, le module Tivoli Plus de Communications Server permet de gérer ce dernier également à partir de TME. Le module Tivoli Plus de Communications Server peut être installé sur le serveur TME. Une image installable de TME figure dans le répertoire TME du CD-ROM Communications Server. Pour accéder aux fonctions TME Plus installées, cliquez deux fois sur l'icône TivoliPlus qui a été ajoutée dans le panneau **Bureau pour l'administrateur**. Lorsque vous cliquez deux fois sur l'icône IBM CSPlus, vous pouvez utiliser les icônes du panneau pour effectuer les opérations suivantes :

- Distribution, installation et désinstallation e Communications Server
- Démarrage, arrêt et interrogation du serveur
- Affichage et modification des ressources du serveur
- Affichage de la liste des fichiers de configuration
- Acheminement des messages d'erreur à partir de Communications Server vers un système Tivoli Enterprise Console
- Établissement de moniteurs et de seuils pour les attributs clés de Communications Server

Lorsque vous cliquez deux fois sur une icône du panneau IBM CSPlus, complétez les zones de la boîte de dialogue affichée. Une aide est disponible pour les zones de la boîte de dialogue.

Support MIB APPN

Communications Server prend en charge les demandes SNMP (Simple Network Management Protocol) relatives aux informations de gestion APPN de tout système de gestion SNMP.

Le service SNMP est installé à partir de l'onglet **Services** dans le menu déroulant **Réseau** du panneau de configuration de Windows NT. Après avoir installé le service SNMP sur votre ordinateur, vous devez le configurer à l'aide des informations valides pour que SNMP fonctionne.

Pour configurer SNMP, vous devez être connecté en tant que membre du groupe administrateur de l'ordinateur local.

Les informations de configuration SNMP identifient les communautés et les destinations de trappe.

Support ROPS IBM 390 destiné au programme NetView

Lorsque la commande RUNCMD est émise à partir de NetView, la valeur du paramètre APPL doit être spécifiée comme suit : APPL=CSRCMDS.

Lorsque la commande RUNCMD est émise, toutes les informations, y compris l'ID et le mot de passe, sont transmises en clair et ne sont en aucun cas sécurisées, sauf si le caractère de suppression NetView est utilisé lors de l'émission de la commande RUNCMD. Ces informations s'affichent et sont entrées dans le journal NetView. Si des mots de passe sont transmis au service ROPS, l'utilisateur est chargé de sécuriser le terminal NetView et ses journaux NetView de sorte que les données confidentielles ne soient pas compromises.

Annexes

Annexe A. Planification de Communications Server

La présente annexe fournit les informations nécessaires à la planification de l'environnement Communications Server.

Matériel compatible

La présente section décrit le matériel IBM qui prend en charge Communications Server. Ces descriptions comportent les informations suivantes :

- Cartes de communication
- Modems
- Cartes de chiffrement au niveau des sessions

Cartes de communication

Pour obtenir la liste des cartes de communication prises en charge par Communications Server, accédez à l'URL suivant sur Internet :

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Modems

Communications Server prend en charge les types de modems suivants :

- Modems asynchrones :
  - Modems 100% compatibles avec le jeu de commandes Hayes** AT
  - Modems IBM conformes aux normes d'interface V.35 et V.24/V.28 (EIA RS-232-D) ITU-T (CCITT)
  - Les modems asynchrones non IBM sont également pris en charge, ainsi que la fonction de base de l'interface entre ETTD et ETCD conforme à la norme V.24 (EIA RS-232-D) ITU-T (CCITT) pour les communications asynchrones
  - Modems conformes à l'interface entre ETTD et ETCD de la norme RS-232-D
- Modems synchrones et unités CSU/DSU prenant en charge le jeu de commandes V.24bis
- Modems 100% compatibles avec le protocole Hayes AutoSync

Les utilisateurs X.25 requièrent un modem synchrone et des unités CSU/DSU qui prennent en charge le jeu de commandes V.24bis ou un modem compatible avec le protocole Hayes AutoSync. Pour plus de détails sur le modem et le type de connexion recommandés, adressez-vous à votre fournisseur de réseau.

Pour obtenir la liste des modems pris en charge par Communications Server, accédez à l'URL suivant sur Internet :

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Cartes de chiffrement au niveau des sessions

Pour utiliser le chiffrement au niveau des sessions, vous devez disposer de l'utilitaire de chiffrement programmé (Programmed Cryptographic Facility) et de l'une des cartes suivantes :

- La carte IBM SecureWay 4758 PCI Cryptographic Coprocessor Adapter
- D'autres cartes conformes à l'IBM Common Cryptographic Architecture

Remarque : Si vous utilisez une carte autre que l'IBM 4758, vous devez utiliser des instructions API de chiffrement. Pour plus de détails, consultez le manuel *Communications Server Programming Guide and Reference*.

Logiciels d'émulation

Pour obtenir la liste des logiciels d'émulation pris en charge par Communications Server, accédez à l'URL suivant sur Internet :

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Remarques relatives à la compression de données

Avant d'utiliser la compression de données SNA, plusieurs étapes de configuration doivent être mises au point sur les systèmes impliqués. La compression de données SNA est prise en charge sur :

- VTAM version 3, édition 4.1 ou suivante
- OS/400 version 2, édition 3 ou suivante

Une fois la compression effectuée, chaque RU est comprimée indépendamment et un en-tête de compression est ajouté dans la RU. Les TH et RH ne sont pas comprimés. Aucune compression n'est effectuée lorsque la RU est inférieure à 20 octets ou supérieure à 64 octets ou, dans le cas de RLE uniquement, si la taille des données comprimées, y compris l'en-tête de compression, est supérieure aux données d'origine.

Avant de commencer la configuration des fonctions de Communications Server appropriées pour la compression de données, assurez-vous que le système partenaire est apte et prêt à prendre en charge la compression de données.

Planification de la connexion hôte/VTAM

Avant de demander une compression de données lors d'une session avec un hôte IBM 370 et IBM 390* doté de l'émulation 3270 ou de communications de type LU 6.2, VTAM version 3, édition 4.1 (VTAM V3R4.1) doit être installé et configuré de manière à négocier de telles demandes.

Votre programmeur de système VTAM hôte doit vous fournir les définitions VTAM appropriées pour la compression de données. Voici une liste récapitulative des définitions requises. Des exemples de définitions sont fournis à la suite de la liste.

- Les options de lancement VTAM doivent contenir le paramètre **CMPVTAM**=x
- Une entrée LOGMODE comportant le paramètre **COMPRES=** est requise

- Cette entrée LOGMODE doit figurer dans la table Mode qui est en cours d'utilisation
- Une instruction VTAM APPL comportant les paramètres **CMPAPPLI=** et **CMPAPPLO=** doit exister pour l'application que vous êtes amené à utiliser
- La définition de LU VTAM relative à votre session doit indiquer l'entrée LOGMODE et la table Mode qui ont été définies pour la compression

CMPVTAM Il s'agit du paramètre d'options de lancement VTAM indiquant le niveau de compression maximal autorisé pour toute session connectée à cet hôte. La syntaxe de ce paramètre est la suivante :

```
CMPVTAM=n
```

où n représente le niveau de compression autorisé pour une demande (valeur comprise entre 0 et 4). La valeur recommandée est de 4, ce qui permet l'utilisation de tous les niveaux de compression de données.

COMPRES Il s'agit de l'entrée de table MODEENT de VTAM de la définition LOGMODE qui sera utilisée par votre LU. La syntaxe est la suivante :

```
COMPRES=valeur
```

où valeur représente SYSTEM, REQUESTED ou PROHIBITED. La valeur SYSTEM doit être codifiée pour tous les types de LU pris en charge.

CMPAPPLO Il s'agit du paramètre de définition d'application VTAM (APPL) qui définit le niveau de compression demandé pour les données d'unités de requête/réponse (RU) sortantes. La syntaxe est la suivante :

```
CMPAPPLO=n
```

où "n" représente le niveau de compression de données demandé pour le sens PLU -> SLU du flux de données, également désigné par données sortantes. Pour toutes les sessions de type LU prises en charge par Communications Server, la valeur de "n" doit être égale à 0, 1 ou 2, ce qui représente les niveaux de compression de données 0, 1 et 2. Cependant, pour les LU de type 0, 1, 2 et 3, Communications Server réserve systématiquement les ressources de compression au niveau 2.

CMPAPPLI Il s'agit du paramètre de définition d'application VTAM (APPL) qui définit le niveau de compression demandé pour les données d'unités de requête/réponse (RU) entrantes. La syntaxe est la suivante :

```
CMPAPPLI=m
```

où "m" représente le niveau de compression de données demandé pour le sens SLU -> PLU du flux de données, également désigné par données entrantes. La valeur de m est fonction du type de LU utilisé pour la session :

- Pour les sessions de type LU 3270, "m" peut avoir pour valeur 0 ou 1.
- Pour les sessions de type LU 6.2, "m" peut avoir pour valeur 0, 1 ou 2.

Remarque : VTAM représente toujours la LU principale (PLU) et Communications Server la LU secondaire (SLU) pour les LU de types 0, 1, 2 et 3.

Voici des exemples codifiés qui ont été extraits des listings VTAM d'origine ; ils soulignent l'utilisation et la position des paramètres susmentionnés. Accordez une attention particulière aux lignes mises en évidence.

```
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
SSCPID=2□,HOSTSA=2□,XNETALS=YES,                                      X
GWSSCP=YES,                                                           X
NODELST=NODES1,                                                       X
CMPVTAM=4,                                                            X
CONFIG=K□,SUPP=NOSUP,                                                 X
NETID=USIBMRA,HOSTPU=ISTPUS2□,HOSTSA=2□,SSCPNAME=RAK,                 X
SSCPDYN=YES,SSCPORD=PRIORITY,                                         X
ASYDE=TERM,                                                           X
NOTRACE,TYPE=VTAM,IOINT=□,                                            X
NOTRACE,TYPE=SMS,ID=VTAMBUF,                                          X
PPOLOG=YES,                                                           X
NODETYPE=NN,                                                          X
CPCP=YES,                                                             X
CSALIMIT=□,                                                           X
NOTNSTAT,DYNLU=YES,                                                   X
IOBUF=(35□□,256,3,,1,58),                                             X
LPBUF=(11□□,,2,,1,4),                                                 X
LFBUF=(1□□,,,,1,1),                                                   X
CRPLBUF=(24□□,,,,1,4),                                                X
SFBUF=(6□,,,,1,1)
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

Figure 41. Paramètre de lancement VTAM. Un niveau de compression maximal de 4 est autorisé dans ce VTAM.

```
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□ LOGMODE FOR COMPRESSION TEST - BASED ON D4C32XX3                     □
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□                                                                      □
□              3274 MODEL 1C (REMOTE SNA)                     @OY□2946□
□              PRIMARY SCREEN 24 X 8□ (192□)                           □
□              ALTERNATE SCREEN TO BE DETERMINED BY APPLICATION        □
□                                                                      □
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
D4C3COMP MODEENT LOGMODE=D4C3COMP,                                     □
                 FMPROF=X'□3',                                         □
                 TSPROF=X'□3',                                         □
                 PRIPROT=X'B1',                                        □
                 SECPROT=X'9□',                                        □
                 COMPROT=X'3□8□',                                      □
                 RUSIZES=X'87F8',                                      □
                 PSERVIC=X'□28□□□□□□□□□□□□□□□□□□3□□',                  □
                 APPNCOS=#CONNECT,                                     □
                 COMPRES=REQD
```

Figure 42. Table LOGMODE de VTAM. Macro MODEENT configurée lorsque la compression de données est demandée.

```
   VBUILD TYPE=APPL
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□ VTAM APPL STATEMENTS FOR CICS/MVS* 3.3                              □
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
RAKAC□□1 APPL ACBNAME=RAKAC□□1,                                      □
              MODETAB=MTAPPC,                                        □
              EAS=2□,                                                □
              SONSCIP=YES,                                           □
              AUTH=(ACQ,VPACE,PASS),                                 □
              PARSESS=YES,                                           □
              VPACING=5,                                             □
              CMPAPPLI=1                                  □
              CMPAPPLO=2
```

Figure 43. Instruction d'application VTAM. Elle contrôle les niveaux maximum pris en charge pour cette session.

```
WTCC11□2   PU   ADDR=13,
                IDBLK=□5D,
                IDNUM=32289,
                etc.
                DLOGMOD=D4C3COMP
                MODETAB=AMODETAB
                etc.

RACC11□2   LU   LOCADDR=2,DLOGMOD=D4C3COMP,MODETAB=AMODETAB
           LU
           etc.
```

Figure 44. Définitions de PU et de LU VTAM. La LU RACC1102 utilise le mode de connexion D4C3COMP qui figure dans la table de modes AMODETAB.

Planification de la compression de données AS/400

Lorsque vous êtes connecté à un système AS/400, vous avez besoin d'OS/400 version 2, édition 3 pour utiliser la compression de données. Il suffit de vous assurer qu'une définition MODE indique le support de compression. Les trois paramètres suivants sont requis sur le profil de «création d'une description de mode» accessible via la commande CRTMODD ou à l'aide des menus :

DTACPR Ce paramètre contrôle l'utilisation de la compression de données. Voici les paramètres admis :

- **NETATR** Utilisez la valeur de réseau indiquée sur l'ensemble du système pour ce paramètre.
- **NONE** Aucune compression de données n'est utilisée.
- **ALLOW** Si le système éloigné demande une compression de données, le système local autorise l'établissement de la session.
- **REQUEST** Le système local demande une compression de données.
- **REQUIRE** L'utilisation de la compression de données est obligatoire. Si un des systèmes n'est pas en mesure d'effectuer la compression de données au niveau demandé, la session n'est pas établie.

Chaque fois qu'une compression de données est autorisée et demandée, les deux systèmes négocient le niveau de compression de données à utiliser sur cette session en fonction des valeurs des des paramètres **INDTACPR** et **OUTDTACPR**.

INDTACPR Cette valeur représente le niveau de compression maximal utilisé pour les données entrantes.

OUTDTACPR Cette valeur représente le niveau de compression maximal utilisé pour les données sortantes.

Pour les sessions LU 6.2, les niveaux de compression de données 0, 1 et 2 sont pris en charge dans les deux sens, c'est-à-dire pour le flux de données sortant et entrant.

Pour plus de détails sur l'activation de Communications Server aux fins de compression de données, consultez le *Guide d'utilisation*.

Remarques relatives aux performances

Les performances des communications d'ordinateurs en général et de Communications Server en particulier font l'objet d'un grand nombre de variables. Les informations suivantes ont pour objet de présenter certains des facteurs qui ont une incidence sur les performances des communications dans un environnement Communications Server.

Les performances des communications sont affectées par la vitesse de la ligne de communication. Cette vitesse est généralement exprimée en nombre de bits par secondes (bps) pouvant être transmis sur la ligne. En général, plus le nombre de bits par secondes est élevé, plus les performances de communications obtenues sur la ligne sont importantes.

En plus du débit binaire, plusieurs autres facteurs liés à la ligne peuvent avoir une incidence sur les performances des communications. Par exemple, certaines lignes ne peuvent acheminer les données que dans un seul sens. Pour modifier le sens des communications (l'émetteur), le poste envoie une ***demande pour émettre*** (DPE) et attend l'émission d'un signal ***prêt à émettre*** (PAE). Un délai supplémentaire est requis pour cette ***inversion du sens de transmission*** (qui est fonction du modem). La qualité de transmission de la ligne de communication représente un autre facteur à prendre en considération. Lorsqu'une erreur de ligne se produit, la plupart des protocoles détectent cette erreur et retransmettent les données. Une ligne à faible taux d'erreurs de transmission produit un débit plus élevé.

Un débit plus élevé peut également être obtenu si les protocoles fonctionnent en mode de transmission de données ***duplex*** permettant une réception et une transmission simultanées. Le réseau local et X.25 correspondent aux protocoles duplex. SDLC peut fonctionner en mode duplex ou semi-duplex.

Afin d'utiliser le mode duplex pour SDLC, vous devez installer une carte appropriée (la carte MPA ne peut pas prendre en charge le mode duplex). Le poste éloigné peut également prendre en charge le mode duplex.

À mesure que la vitesse de transmission augmente, la capacité de débit binaire de la ligne représente une contrainte moins importante en matière de performances.

En revanche, la contrainte est désormais liée aux délais à l'intérieur des périphériques qui utilisent la ligne de communication (modems, unités de contrôle ou contraintes internes aux ordinateurs). À des vitesses très élevées, l'impact de ces délais sur les performances des communications peut être supérieur à celui de la capacité de débit binaire de la ligne.

L'analyse de ces situations demande un certain effort. Par exemple, des délais de communication plus longs que prévu peuvent être occasionnés par l'un des éléments suivants :

- Une ligne de communication surchargée
- Un système hôte surchargé
- Une unité de contrôle 3X74 surchargée
- Un contrôleur de réseau 37*xx* surchargé
- Définition VTAM ou NCP non optimale
- Conception ou gestion de réseau inadéquate
- Engagement excessif et permutation de la mémoire du système d'exploitation

Dans un environnement de communication à grande vitesse, par exemple, un réseau local, le débit binaire de la ligne de communication est moins important car la capacité de communication est largement déterminée par la vitesse des périphériques de communication. De meilleures performances de communication peuvent généralement être réalisées grâce à l'augmentation de la puissance de traitement du poste de travail, de l'hôte ou d'autres composants de réseau. Cela ne signifie pas que le débit binaire d'un réseau local ne représente jamais une contrainte ; plus exactement, il peut nécessiter le fonctionnement de plusieurs ordinateurs à leur capacité de communication avant une dégradation considérable des performances du réseau local.

En résumé, dans la plupart des cas, les performances de Communications Server sont largement déterminées par des facteurs liés au réseau de communication utilisé. Le fait de fournir des performances de communications à un coût raisonnable implique une compréhension du réseau dans son ensemble, ainsi que l'analyse de chacun de ses composants.

Annexe B. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Cela ne signifie pas qu'IBM ait l'intention de les y annoncer. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM.

Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM.

Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Le présent document peut également contenir des programmes réduits fournis par IBM à titre de simple exemple et d'illustration. Ces programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE OU D'ADAPTATION À VOS BESOINS SONT EXPRESSÉMENT EXCLUES.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document.

La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense CEDEX
France

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Marques

Les termes qui suivent sont des marques d'International Business Corporation dans certains pays :

AIX
AnyNet
APPN
AS/400
AT
BookManager
CICS
DB2/2
eNetwork
Enterprise System/9000
ESCON
ES/9000
FFST/2
First Failure Support Technology/2
Global Network
IBM
IBMLink
IMS
Micro Channel
NetView
OS/2
OS/400
Personal System/2
Portmaster
Presentation Manager
PS/2
IBM 370
System/390
SystemView
S/370
S/390
TalkLink
VTAM
WebExplorer

Les termes qui suivent sont des marques d'autres sociétés :

C-bus est une marque de Corollary, Inc.

Java et HotJava sont des marques de Microsystems, Inc.

Microsoft, Windows et le logo Windows 95 sont des marques de Microsoft Corporation.

PC Direct est une marque de Ziff Communications Company utilisée sous licence par IBM Corporation.

ActionMedia, LANDesk, MMX, Pentium et ProShare sont des marques d'Intel Corporation dans certains pays.

Pour obtenir la liste complète des marques d'Intel, connectez-vous sur www.intel.com/tradmarx.htm.

UNIX est une marque dans certains pays, dont seule la société X/Open Company Limited peut concéder la licence.

Remarque : D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

Index

Nombres

A

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W

X

REMARQUES DU LECTEUR

Réf. : SC11-1493-00

Titre : eNetwork Communications Server Version 6.0 pour Windows NT

Guide d'administration réseau

Vos commentaires nous permettent d'améliorer la qualité de nos documents : ils jouent un rôle important lors de leur mise à jour.

Si vous avez des observations sur le(s) document(s) ci-joint(s), nous vous serions reconnaissants de nous en faire part en les faisant précéder, au besoin, des rubriques ou des numéros de pages et de lignes concernés. Elles seront étudiées avec le plus grand soin par les responsables du Centre de francisation.

Par ailleurs, nous vous rappelons que pour toute question technique ou pour toute demande de document, vous devez vous adresser à votre partenaire commercial IBM.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie de ces informations que, de votre côté, vous pourrez évidemment continuer à exploiter.

Envoyez vos remarques à :

Pour la France	Pour le Canada
IBM FRANCE	**IBM CANADA Ltée**
Centre de francisation	**Services linguistiques**
4, avenue Montaigne	**1250, boul. René-Levesque ouest**
93881 Noisy-le-Grand Cedex	**Montréal (Québec) H3B 4W2**

Si vous désirez une réponse, n'oubliez pas de mentionner vos nom et adresse.

Merci de votre collaboration.

MODIFICATIONS OU ÉCLAIRCISSEMENTS DEMANDÉS :

Page ou rubrique *Commentaires*

Compagnie IBM France
Tour Septentrion
20, avenue André Prothin
La Défense 4
92400 Courbevoie

Document réalisé et composé par le Centre de francisation

à Noisy-le-Grand

Juin 1998

Imprimé au Danemark par IBM Danmark A/S.

SC11-1493-□□