

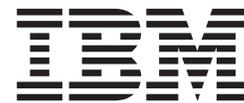
eNetwork Communications Server
Versão 6.0
para Windows NT



Guia de Administração de Rede

Versão 6.0

eNetwork Communications Server
Versão 6.0
para Windows NT



Guia de Administração de Rede

Versão 6.0

Nota

Antes de utilizar estas informações e o produto a que elas se referem, leia as informações gerais no “Apêndice B. Observações” na página 217.

Primeira Edição (Julho de 1998)

Esta edição se aplica à Versão 6.0 do IBM eNetwork Communications Server para Windows NT e a todos os releases e modificações subsequentes a menos que seja indicado em novas edições.

© Copyright International Business Machines Corporation 1989, 1996. Todos os direitos reservados.

Índice

Figuras	vii	Ativar por Pedido	36
Tabelas	ix	Repetição Automática de Ligação	37
Sobre Este Manual	xi	Máximo de Tentativas de Ativação	38
Como Utilizar este Manual	xi	Reativação Solicitada pelo Usuário	38
Convenções Utilizadas neste Manual	xii	Parâmetros de Desativação da Ligação	39
Convenções de Textos	xii	Tempo de Espera de Inatividade	39
Convenções de Números	xii	Recurso Limitado	39
Onde Encontrar Mais Informações	xiii	Redes de Conexão	40
Parte 1. Visão Geral e Conceitos	1	Outros Parâmetros de Ligação	41
Capítulo 1. Introdução às Funções do Communications Server	3	Tipo de Nó Adjacente	41
Funções Suportadas	3	Servidor do Nó da Rede Preferido	41
Suporte às Comunicações de SNA	4	Solicitar Sessões SSCP	42
APPC/APPN	4	Serviços de Diretório	42
Advanced Peer-to-Peer Networking (APPN)	8	Serviços de Topologia e Seleção de Rota	44
Interfaces de Programação	9	Banco de Dados de Topologia	45
High Performance Routing	10	Modos	46
Compactação de Dados de SNA	10	Classe de Serviço	47
Descoberta de Fornecedores de Serviço	10	Prioridade de Transmissão do SNA	47
Solicitador da LU Dependente (DLUR)	11	Seleção de Rota	48
SNA Gateway	11	Seleção de Rota para Usuários do VTAM	48
Suporte AnyNet	12	Encaminhamento de Sessão Intermediária	49
Servidor TN3270E	14	Suporte ao High Performance Routing (HPR)	49
Servidor TN5250	15	Rapid Transport Protocol (RTP)	50
Acesso aos Dados já Existentes	16	Automatic Network Routing (ANR)	52
Suporte ao Cliente do Communications Server	17	Suporte à LU	52
Suporte à Configuração e Administração	18	Suporte à SDDL	53
Balanceamento de Carga	19	Suporte ao Dependent Logical Unit Requester	53
Segurança de Dados	20	Sessões LU-LU	55
Suporte a Placas	20	LU 6.2	56
Suporte ao Data Link Control (DLC)	20	Outras LUs	57
Suporte MIB de APPN	21	Nó da Rede APPN e Suporte a T2.1	57
Sistema de Reserva Ligado	21	Compactação de Dados	57
Funções do Emulador de Nível de Entrada	21	Arquitetura da Compactação no Nível de Sessão do SNA	58
Capítulo 2. Communications Server e SNA	23	Compactação de Dados do Communications Server	59
Visão Geral das Funções de SNA	23	Criptografia no Nível de Sessão do SNA	60
Perfis de Data Link Control	24	Serviços de Gerenciamento	61
Advanced Peer-to-Peer Networking	25	Pontos Focais, Pontos de Serviço e Pontos de Entrada	61
Tipos de Nós do APPN	25	Níveis da Arquitetura dos Serviços de Gerenciamento do SNA	62
Pontos de Controle	27	Controle de Fluxo	63
Extensor de Ramificação	29	Controle de Velocidade do Nível de Sessão	63
Funções Suportadas	33	Controle de Velocidade BIND Adaptável	64
Data Link Control (DLC)	34	Segmento e Montagem	64
Conexões	34	Controle de Velocidade do High Performance Routing	64
Tipos de Ligações	35	Controle de Velocidade Fixo	64
Parâmetros de Definição e Ativação da Ligação	36	Como Particionar LUs entre os Sistemas Centrais	64
Ativar na Inicialização	36	Suporte SNA Gateway	65
		Parte 2. Planejamento e Instalação	69

Capítulo 3. Como Planejar o Suporte AnyNet 71

Como Configurar AnyNet SNA sobre TCP/IP	71
Como Mapear os Recursos do SNA para Endereços IP	71
Considerações sobre o SNA Gateway sobre TCP/IP	73
Considerações da Função de Nó do Acesso do SNA sobre TCP/IP	77
Exemplos de Configuração do AnyNet SNA sobre TCP/IP	78
Exemplo 1. Como Executar Aplicações APPC ou CPI-C sobre uma Rede TCP/IP	78
Exemplo 2. Emulação 3270 através do DLUR sobre uma Rede TCP/IP	79
Exemplo 3. Como Utilizar um SNA Gateway para Permitir Emulação 3270 entre as Redes SNA e TCP/IP	80
Exemplo 4. Como Utilizar um SNA Gateway para Emulação 3270 sobre uma Rede TCP/IP	81
Exemplo 5. Emulação 3270 de Duas Estações de Trabalho do Windows NT em Redes IP Diferentes	82
Dicas Úteis	83
Como Configurar AnyNet Sockets sobre SNA	84
Como Funciona o Sockets sobre SNA?	84
Suporte do Programa Aplicativo Fornecido pelo Sockets sobre SNA	86
Como Planejar o Sockets sobre SNA	86
Como Rotear e Mapear a Visão Geral	87

Capítulo 4. Como Planejar a Comunicação Cliente/Servidor 93

Cientes API de SNA.	93
Instalação e Configuração	93
Lightweight Directory Access Protocol	93
Cliente API Comum para Communications Server para Windows NT e IntranetWare para SAA	94
Como Atribuir uma LU Local Padrão	95
Como Atribuir uma LU Parceira Padrão	95
Como Atribuir um Nome de Sessão LUA Padrão	96
Criptografia de Dados do Cliente/Servidor.	96
Segurança do Client Server	96
Cientes Novell IntranetWare para SAA	97

Capítulo 5. Como Planejar o Legacy Data Access 99

Provedor OLE DB do AS/400	99
Servidor de Pasta Compartilhada do AS/400.	100
Host Publisher	101
Processamento de Página na Web	101
Configurações do Host Publisher	102
Acesso de Clientes aos Sistemas Centrais do CICS	103
Acesso de Clientes aos Sistemas Centrais do MQSeries	104
Acesso de Clientes aos Sistemas Centrais do DB2	105

Capítulo 6. Como Planejar o HPR 107

Características de Ligação HPR	107
Considerações HPR	108
Considerações para Sintonização de Parâmetros em DLCs da Rede Local	109
Processamento de Comutação de Caminhos do HPR	110

Capítulo 7. Como Planejar o SNA Gateway 113

Conexões Suportadas para Estações de Trabalho	113
Conexões SDLC de Estações de Trabalho	114
Conexões da Estação de Trabalho X.25	114
Conexões Suportadas para Estações de Trabalho	114
Considerações sobre o Sistema Central	115
Configuração de Endereços de Destino na Rede Local	116
Como Planejar as Definições Gateway LU	116
Como Utilizar Conexões Explícitas e Implícitas	118
Desempenho do SNA Gateway	119
Considerações da DLUR	119

Capítulo 8. Como Planejar o Servidor TN3270E 121

Estações de Trabalho de Cliente Suportadas no Servidor TN3270E	123
Destaques	123
Como Alterar o Número da Porta Padrão	123
Como Gerenciar o Tráfego do Sistema.	124
Filtragem de IP	125
Suporte ao Secure Sockets Layer (SSL)	125
Como Configurar Conexões SNA	125
Como Agrupar	125
Balanceamento de Carga de Servidores TN3270E	126

Capítulo 9. Como Planejar o Servidor TN5250 127

Estações de Trabalho de Cliente Suportadas no Servidor TN5250	129
Destaques	129
Como Alterar o Número da Porta Padrão	129
Como Gerenciar o Tráfego do Sistema.	129
Como Especificar Acesso aos AS/400s com Várias Portas	130
Filtragem de IP	130
Suporte ao Secure Sockets Layer (SSL)	130
Como Configurar a Rede SNA	131
Balanceamento de Carga de Servidores TN5250	131

Capítulo 10. Como Planejar a Segurança baseada em Secure Sockets Layer 133

Como Funciona a Segurança do SSL	133
Suporte ao SSL do Communications Server	134
Como Configurar a Segurança do SSL.	134
Utilitário de Gerenciamento do Conjunto de Chaves	135
Como Alterar a Senha	135

Etapa 6. Como Selecionar Recursos do Communications Server.	195
Etapa 6.1 Como Planejar Programas Aplicativos	197
Etapa 7. Como Criar Configurações e Como Instalar	197
Como Utilizar a Configuração e a Instalação do Arquivo de Resposta	197
Etapa 8. Como Criar Materiais do Usuário	197
Como Preparar a Documentação	198
Materiais e Procedimentos do Communications Server	198
Como Preparar os Procedimentos de Cópia de Segurança	199
Etapa 9. Como Manter a Rede	199

Parte 3. Como Controlar e Manter uma Rede.201

Capítulo 16. Recursos de Gerenciamento de Sistema.	203
Recursos Comuns de Gerenciamento de Sistema	203
Operações do Nó SNA	204
Administração Remota	204
Programas da Linha de Comandos	205
Administração Com Base na Web	205
Controle ActiveX de Operações do Nó SNA	206

Módulo Tivoli Plus	206
Suporte MIB de APPN	206
S/390 Remote Operations Support (ROPS) para o Programa NetView	207

Apêndice A. Como Planejar o Communications Server209

Hardware Compatível	209
Placas de Comunicação	209
Modems	209
Placas de Criptografia de Nível de Sessão	210
Software do Emulador	210
Considerações sobre a Compactação de Dados	210
Como Planejar a Conexão ao Sistema Central/VTAM	210
Como Planejar a Compactação de Dados do AS/400	213
Considerações sobre Desempenho	214

Apêndice B. Observações217

Marcas	218
------------------	-----

Índice Remissivo221

Comentários do Leitor.225

Figuras

1. Uma Sessão entre Duas LUs (LU-LU)	7
2. Conversação de Programas de Transação Ocorrendo através de uma Sessão	8
3. Sessões Paralelas entre LUs.	8
4. Exemplo de Conexões do SNA Gateway	12
5. Gateway SNA sobre TCP/IP	13
6. Gateway Sockets sobre SNA	14
7. Conexões do Servidor TN3270E	15
8. Conexões do Servidor TN5250.	16
9. Uma Parte de Um Exemplo de Rede APPN	26
10. Visão Geral Conceitual das Ligações Superiores e Inferiores da Ramificação	29
11. O Extensor de Ramificação em uma Rede	31
12. Uma Exemplo de Rede de Conexão	41
13. Diretório do Nó LEN.	43
14. Diretório do Nó Final.	43
15. Diretório do Nó da Rede	44
16. Banco de Dados de Configuração Local e Banco de Dados de Topologia da Rede em Nós da Rede.	46
17. Conexão do DLUR a um Sistema Central através de um Gateway do Communications Server	55
18. Sessões Múltiplas e Paralelas	56
19. Exemplo de Configuração do SNA Gateway	66

Tabelas

1. Conexões APPC Suportadas	4	20. Referência Cruzada de Parâmetros PC/Sistema Central: Conexões NPSI sobre X.25	169
2. Banco de Dados de Configuração do NN Local	45	21. Referência Cruzada de Parâmetros PC/Sistema Central: X.25 (VTAM/NCP) . . .	170
3. Banco de Dados de Topologia da Rede do NN Local.	46	22. Referência Cruzada de Parâmetros PC/Sistema Central: APPC em uma Rede Token-Ring IBM Utilizando X.25 para um Sistema Central.	171
4. Resumo do SNA Gateway	67	23. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Definição de Linha de Programa do Sistema Central OS/400.	172
5. Máscaras de Endereço IP Suportadas pelo Sockets sobre SNA.	87	24. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Parâmetros do Controlador	173
6. Comandos Equivalentes	123	25. Referência Cruzada dos Parâmetros do Communications Server com AS/400: Parâmetros do Dispositivo	174
7. Referência Cruzada de Parâmetros PC/Sistema Central: Definição de NTRI de Rede Token-Ring IBM	157	26. Referência Cruzada dos Parâmetros Sistema Central/PC: Descrição de Linha	175
8. Referência Cruzada de Parâmetros PC/Sistema Central: Rede IBM Token-Ring com Rede Comutada VTAM	158	27. Referência Cruzada dos Parâmetros do Sistema Central/PC: Descrição do Controlador	175
9. Referência Cruzada de Parâmetros PC/Sistema Central: Rede IBM Token-Ring 9370 de Rede Local VTAM	159	28. Referência Cruzada dos Parâmetros do Sistema Central/PC: Descrição do Controlador	176
10. Correspondência de Parâmetro entre uma Token Ring 3174 e o Communications Server	159	29. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Definição de Linha de Programa do Sistema Central OS/400 (X.25)	176
11. Referência Cruzada de Parâmetros PC/Sistema Central: PU de VTAM do controlador 3174 da Rede IBM Token-Ring e o Communications Server	159	30. Referência Cruzada de Parâmetros PVX X.25 do Communications Server com o AS/400: Parâmetros do Controlador	177
12. Referência Cruzada de Parâmetros PC/Sistema Central: Rede Comutada VTAM com Rede Ethernet	160	31. Referência Cruzada de Parâmetros SVC X.25 do Communications Server com o AS/400: Parâmetros do Controlador	178
13. Referência Cruzada de Parâmetros PC/Sistema Central: SDLC	161	32. Capacidade de Memória.	182
14. Referência Cruzada de Parâmetros PC/Sistema Central: APPC	164	33. Classes de Endereço IP Suportadas pelo Communications Server	189
15. Referência Cruzada de Parâmetros IOCP/HCD: MPC	165	34. Recursos do Servidor de Comunicações para Ações de Gerenciamento.	203
16. Referência Cruzada de Parâmetros VTAM: MPC	165		
17. Referência Cruzada de Parâmetros PC/Sistema Central: Sistema de Informação 9370 através do SDLC	166		
18. Referência Cruzada do Parâmetro do Communications Server VTAM: Utilizando DLUR	168		
19. Parâmetro DLUR do Communications Server VTAM que corresponde à Conexão do Sistema Central com a Estação de Trabalho	168		

Sobre Este Manual

IBM eNetwork Communications Server para Windows NT (referido neste manual como *Communications Server*) é uma plataforma de serviços de comunicação pública. Esta plataforma fornece uma ampla faixa de serviços para Windows NT estações de trabalho que se comunicam com computadores centrais e com outras estações de trabalho. Os usuários do Communications Server podem escolher entre várias opções de conectividade remota.

O *Guia de Administração de Rede* é fornecido como fonte de planejamento e administração para quem está utilizando ou planejando utilizar o Communications Server. O pessoal da administração, de suporte técnico e de serviço, os coordenadores de serviço, os funcionários da IBM, assim como qualquer um que tenha responsabilidade de tomar decisões em sistemas de informações considerarão útil este manual. Ele fornece uma visão geral do Communications Server, suas funções e as etapas necessárias para criar as configurações do Communications Server para as estações de trabalho que você suporta.

Supõe-se que você esteja utilizando o Windows NT 4.0 Server como o seu sistema operacional de base.

Como Utilizar este Manual

O *Guia de Administração de Rede* auxilia no planejamento necessário para instalar e configurar uma rede de estações de trabalho. Este manual o ajuda a:

- Planejar a rede
- Escolher a configuração e as ferramentas de instalação
- Criar um arquivo de configuração de gabarito
- Implementar o plano da rede
- Manter a rede

A configuração de uma rede de estações de trabalho requer um planejamento cuidadoso e completo. Ao criar uma rede, você precisa saber o seguinte:

- Os nomes das estações de trabalho, os nomes dos perfis, os nomes dos arquivos de configuração e outros nomes em sua rede
- Onde está localizado o ponto focal para enviar alertas
- As estações de trabalho que você já tem e que pode continuar a utilizá-las e de quantas mais estações de trabalho novas que você precisa
- A função que você deseja que cada estação de trabalho tenha na rede
- O pacote a ser instalado em cada estação da trabalho de forma que possa cumprir a função atribuída a ela
- Os recursos de hardware e software que você já tem que deseja manter ou atualizar
- Os novos recursos de hardware e software que você precisa antes que possa implementar o planejamento da rede
- O método para manter sua rede e seus recursos em hora extra
- O número e o tipo de conexões do sistema central e quais estações de trabalho devem ser anexadas aos sistemas centrais através do gateway e da definição do gateway

As etapas de “Capítulo 15. Como Implementar Configurações do Communications Server” na página 181 fornecem um procedimento para determinar estas informações para sua rede. Se você já possui um procedimento adequado, deverá querer preservá-lo, mas você deverá compará-lo com o capítulo antes de tomar qualquer decisão.

Convenções Utilizadas neste Manual

As seguintes convenções são utilizadas neste manual.

Convenções de Textos

Negrito	O tipo em negrito indica: <ul style="list-style-type: none">• Verbos, funções, palavras-chave e parâmetros que você pode utilizar em um programa ou em um prompt de comandos. Esses valores consideram maiúsculas e minúsculas e devem ser digitados exatamente como aparecem no texto.• Os nomes de controles de janelas, por exemplo listas, quadros de opções, campos de entrada, botões de comando e opções de menu.
<i>Itálico</i>	O tipo em itálico indica: <ul style="list-style-type: none">• Uma variável à qual é fornecida um valor.• Títulos de manuais.• Uma letra é usada como uma letra ou uma palavra é usada como uma palavra. Exemplo: Se você vir uma letra <i>a</i>, certifique-se de que não se trata de <i>uma</i>.
<i>Itálico e negrito</i>	O tipo em itálico e negrito é utilizado para enfatizar uma palavra.
MAIÚSCULA	A letra maiúscula indica constantes, nomes de arquivos e opções que você pode utilizar em um programa ou em um prompt de comandos. Você pode digitar esses valores em letra maiúscula ou em minúscula.
Aspas	As aspas indicam mensagens que você vê em uma janela. Um exemplo disso seriam as mensagens que aparecem na área de informações para o operador (OIA) de uma sessão do emulador.
Tipo de exemplo	O tipo de exemplo indica informações que você é instruído a digitar em um prompt de comandos ou em uma janela.

Convenções de Números

Números binários	Representados como B'xxxx xxxx' ou B'x', exceto em certas ocorrências onde são representados com texto (“Um valor binário xxxx xxxx é...”).
Posições de bits	Começam com 0 na posição mais à direita (bit menos significativo).
Números decimais	Os números decimais com mais de 4 dígitos são representados em estilo métrico. Um espaço é utilizado em vez de uma vírgula para separar grupos de 3 dígitos. Por exemplo, o número dezesseis mil cento e quarenta e sete é escrito 16 147.
Números hexadecimais	Representados no texto como hexadecimal xxxx ou X'xxxx' (“O endereço do nó adjacente é o hexadecimal 5D, que é especificado como X'5D'.”)

Onde Encontrar Mais Informações

Para obter maiores informações, consulte *Iniciação Rápida* que contém uma descrição completa da biblioteca do Communications Server e das publicações relacionadas.

A home page do Communications Server na Internet possui informações gerais sobre o produto, bem como informações sobre os serviços de APARs e correções. Há duas maneiras de acessar a home page:

1. No Communications Server, selecione o ícone **Acessar Home Page**
2. Ao utilizar o navegador Internet, vá para a seguinte URL:
<http://www.software.ibm.com/enetwork/commsserver/about/csnt.html>

Parte 1. Visão Geral e Conceitos

Capítulo 1. Introdução às Funções do Communications Server

Este capítulo fornece uma visão geral das funções de comunicações suportadas pelo Communications Server e dos métodos que podem ser utilizados para configurar seus sistemas para a execução destas funções. Os capítulos posteriores neste manual descrevem as funções e os métodos de configuração com maiores detalhes.

Funções Suportadas

Esta seção descreve as seguintes funções do Communications Server:

- Suporte à comunicação de SNA
- Advanced Program-to-Program Communications (APPC), que inclui Advanced Peer-to-Peer Networking (APPN)
- Interfaces de programação de aplicações (APIs) de 32 bits
- High performance routing (HPR)
- Compactação de dados de SNA
- Descoberta de fornecedores de serviço
- Aplicação da LU convencional (LUA)
- Solicitador de unidade lógica dependente (DLUR)
- SNA Gateway
- Suporte AnyNet
 - AnyNet SNA sobre TCP/IP (nó de acesso e gateway)
 - AnyNet Sockets sobre SNA (nó de acesso e gateway)
- Servidor TN3270E
- Servidor TN5250
- Acesso aos dados já existentes
 - Provedor OLE DB do AS/400
 - Host Publisher
 - Servidor de pasta compartilhada do AS/400
- Suporte ao cliente API de SNA
- Suporte ao cliente Novell IntranetWare para SAA
- Suporte à configuração e administração
- Balanceamento de carga
- Segurança de dados
- Suporte a placas
- Suporte ao Data Link Control (DLC)
- Suporte MIB de APPN
- Sistema de reserva ligado
- Funções do emulador de nível de entrada

Suporte às Comunicações de SNA

O Communications Server pode atuar como um nó do Systems Network Architecture (SNA) tipo 2.0 e um nó SNA tipo 2.1. Este suporte permite gravar programas para a comunicação com muitos outros produtos IBM SNA.

APPC/APPN

O Communications Server fornece nó final Advanced Peer-to-Peer Networking (APPN) e suporte ao nó da rede para estações de trabalho, permitindo que se comuniquem de forma mais flexível com outros sistemas na rede. Além disso, uma função extensora de ramificação permite isolar ramificações para evitar o tráfego desnecessário CP-CP.

O Communications Server fornece suporte ao advanced program-to-program communications (APPC) para suportar comunicações entre programas de processamento distribuído, chamados programas de transação (TPs). Os TPs podem estar localizados em qualquer nó na rede que forneça o APPC. O APPC utiliza o protocolo LU 6.2 para troca de dados entre programas localizados em unidades lógicas diferentes (LUs). Além disso, o APPC suporta várias ligações concorrentes e sessões paralelas. A segurança de conversação ou sessão entre os programas em comunicação também é suportada através do APPC.

O Communications Server fornece uma taxa de rendimento de APPC em ambientes de Rede Local críticos em desempenho. O Communications Server suporta as seguintes conectividades:

Tabela 1. Conexões APPC Suportadas

Protocolos	Conexão	Tipo de Conexão
Canal	<ul style="list-style-type: none">• CDLC (OEM)• MPC	
Rede Local (802.2)	<ul style="list-style-type: none">• Token-Ring• Ethernet• Retransmissão de Estrutura• Emulação de Rede Local ATM	
SDLC	<ul style="list-style-type: none">• Síncrono• Sincronização automática• Modems	<ul style="list-style-type: none">• Discado automaticamente, DTR discado, Permanente• Discado automaticamente• Discado automaticamente, Permanente• Discado automaticamente
X.25	<ul style="list-style-type: none">• Síncrono• Hayes** AutoSync• Rede X.25	<ul style="list-style-type: none">• Discado automaticamente, Semipermanente• Discado automaticamente, Permanente• Discado automaticamente
IP	SNA sobre IP	Conexões fornecidas por IP

Introdução às Funções do Communications Server

Tabela 1. Conexões APPC Suportadas (continuação)

Protocolos	Conexão	Tipo de Conexão
IP	HPR sobre IP	Conexões fornecidas por IP

Nota: O APPC/APPN também possui o recurso de compactação de dados. Consulte “Compactação de Dados” na página 57 para obter mais informações sobre a compactação de dados. Consulte também “Criptografia no Nível de Sessão do SNA” na página 60 para obter informações sobre criptografia.

Suporte à LU SNA Tipo 6.2

A LU 6.2 é uma arquitetura para o program-to-program communications. O Communications Server suporta os seguintes recursos opcionais da LU SNA 6.2:

- Conversações básicas e mapeadas
- Nível de sincronização de confirmação
- Suporte de segurança em níveis de sessão e de conversação
- Múltiplas LUs
- Sessões paralelas, incluindo a capacidade de utilizar um sistema remoto para alterar o número de sessões
- Transações em um modo simultâneo em uma ou em duas direções
- Várias ligações simultâneas com sessões SSCP-PU e cada uma pode ser conectada a uma rede de subárea

Consulte *Communications Server Programming Guide and Reference* para obter uma lista completa de recursos.

Avanços da Configuração do APPC

A configuração do nó final básico requer no mínimo quatro parâmetros: ID da rede, nome do nó local, tipo de ligação e endereço de destino. A definição do sistema é reduzida por:

- Modos fornecidos pela IBM
- Criação implícita de definições de LU parceira e de modo durante a alocação de uma conversação
- Inicialização implícita de limites de sessões (a função CNOS), que remove o requisito para inicializar explicitamente os limites de sessões antes da alocação de conversações
- Remoção de limites de sessões para LUs locais e parceiras, que permite maior liberdade na configuração e inicialização dos limites de sessões de modos
- Padrões para nomes de programas de transação, operação e tipo, que removem o requisito para configurar definições do programa de transação para programas aplicáveis
- Atualizações dinâmicas de configuração
- Definições implícitas de estações de trabalho do SNA Gateway
- Capacidade de editar um arquivo .ACG contendo parâmetros de configuração
- Capacidade de encontrar informações sobre a definição do sistema com a Descoberta

Como a configuração do SNA está armazenada como um arquivo de texto, é possível modificar o arquivo de forma rápida e fácil utilizando um editor ou um

Introdução às Funções do Communications Server

programa gravado por um usuário. É possível atualizar dinamicamente uma configuração ativa (sem encerrar o Communications Server).

Agora é possível configurar conexões com vários sistemas centrais e várias conexões do sistema central podem ficar ativas ao mesmo tempo. As conexões podem ser definidas para início por pedido ou como resultado da falha de um sistema de reserva ligado.

O suporte de Descoberta do Communications Server permite que um nó encontre dinamicamente o nome do ponto de controle, o endereço do controle de acesso ao meio de transmissão (MAC) e o endereço do ponto de acesso do serviço (SAP) de outro servidor do nó da rede do Communications Server em uma Rede Local Token-Ring ou Ethernet. Isto significa que o usuário não precisa saber o nome do ponto de controle, o endereço MAC e SAP de uma máquina parceira antes de conseguir definir uma conexão com ele. Atualmente, os usuários do Client Access/400 e do Personal Communications podem utilizar este recurso.

Conceitos Fundamentais do APPC

Esta seção apresenta os conceitos e termos do APPC.

Programas de Transação: *Programa de transação* (TP) é um program, ou parte de um programa aplicativo, que utiliza as funções de comunicações do APPC. Os programas aplicativos utilizam essas funções para se comunicarem com programas aplicativos em outros sistemas que suportam o APPC.

O Communications Server fornece a API de APPC e suporta chamadas do IBM Systems Application Architecture (SAA) Common Programming Interface for Communications (CPI-C) para programas de transação.

Os programas de transação emitem parâmetros de APPC para chamar funções de APPC. **Parâmetro** é um pedido formatado emitido por um programa de transação e executado pelo APPC. Um programa utiliza as seqüências de parâmetros do APPC para se comunicar com outro programa. Dois programas que comunicam entre si podem estar localizados em sistemas diferentes ou no mesmo sistema. A API de APPC é a mesma em ambos os casos.

Quando um programa de transação troca dados com outro programa de transação, o outro programa de transação é chamado de programa de transação **parceiro**.

Os programas de transação podem emitir chamadas de CPI-C. Estas chamadas permitem que os programas aplicativos aproveitem a compatibilidade fornecida pelo SAA.

Unidades Lógicas: Cada programa de transação obtém acesso a uma rede SNA através de uma **unidade lógica** (LU). LU é um software de SNA que aceita parâmetros de seus programas e atua nestes parâmetros. Um programa de transação emite parâmetros de APPC para sua LU. Estes parâmetros fazem com que os comandos e dados fluam através da rede para uma LU parceira. Uma LU também atua como uma intermediária entre programas de transação e a rede para gerenciar a troca de dados entre os programas de transação. Uma única LU pode fornecer serviços para vários programas de transação. Várias LUs podem ficar ativas simultaneamente no nó.

Introdução às Funções do Communications Server

Tipos de LU: O Communications Server suporta os tipos de LU 0, 1, 2, 3 e 6.2. Os tipos de LU 0, 1, 2 e 3 suportam comunicação entre programas aplicativos do sistema central e tipos diferentes de dispositivos, tais como, terminais e impressoras.

A LU 6.2 suporta comunicações entre dois programas localizados em nós de subárea tipo 5, nós periféricos tipo 2.1, ou ambos, e entre programas e dispositivos. O APPC é uma implementação da arquitetura da LU 6.2.

Sessões de LU: Antes que os programas de transação possam se comunicar, suas LUs devem estar conectadas em uma relação mútua chamada **sessão**. Uma sessão conecta duas LUs, por isso é chamada de sessão **LU-LU**. A Figura 1 ilustra essa relação de comunicação.



Figura 1. Uma Sessão entre Duas LUs (LU-LU)

As sessões atuam como um canal que gerencia o movimento de dados entre um par de LUs em uma rede SNA. Especificamente, as sessões lidam com situações, tais como, quantidade de dados transmitidos, segurança dos dados, roteamento da rede e congestionamento do tráfego.

As sessões são mantidas por LUs. Normalmente, os programas de transação não funcionam com características da sessão. Você define as características da sessão quando:

- Configura seu sistema
- Utiliza **Operações do Nó SNA**
- Utiliza parâmetros de gerenciamento

Conversações de Programas de Transação: A comunicação entre programas de transação é chamada de **conversação**. Como uma conversação telefônica, um programa de transação chama outro e eles se “comunicam”, um programa de transação de cada vez, até que o programa de transação encerre a conversação. Uma conversação é iniciada quando um programa de transação emite um parâmetro de APPC ou uma chamada de CPI-C que aloca uma conversação. As conversações ocorrem através de sessões LU-LU.

A alocação de uma conversação para uma sessão estabelece uma relação de envio-recepção entre os programas de transação conectados à conversação. Um programa de transação emite parâmetros para enviar dados. O outro programa de transação emite parâmetros para receber dados. Quando o programa de transação de envio encerra o envio de dados, ele pode transferir o controle de envio da conversação para o programa de transação de recepção. As conversações podem trocar informações e dados de controle e de dados.

Introdução às Funções do Communications Server

A Figura 2 mostra uma conversação entre dois programas de transação ocorrendo através de uma sessão.



Figura 2. Conversação de Programas de Transação Ocorrendo através de uma Sessão

Uma sessão pode suportar somente uma conversa de cada vez, mas pode suportar muitas conversações em seqüência. Como várias conversações podem reutilizar as sessões, uma sessão é uma conexão de longa duração, comparada a uma conversa. Quando um programa aloca uma conversa e todas as sessões aplicáveis estão em uso, a LU coloca a conexão de entrada (pedido de alocação) em uma fila. Ele conclui a alocação quando uma sessão se torna disponível.

Duas LUs também podem estabelecer sessões paralelas uma com a outra para suportar várias conversações simultâneas. Uma sessão paralela ocorre quando um programa de transação aloca uma conversa e existe uma sessão, mas está sendo utilizada por uma conversa. A LU pode solicitar uma nova sessão para atender a alocação.

A Figura 3 mostra três sessões paralelas entre duas LUs; cada sessão mantém uma conversa.

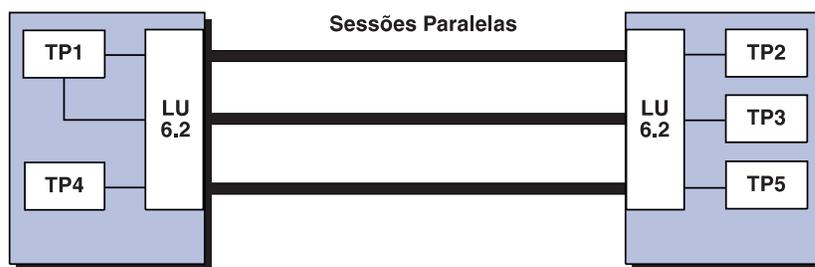


Figura 3. Sessões Paralelas entre LUs

Advanced Peer-to-Peer Networking (APPN)

O Advanced peer-to-peer networking (APPN) é um conjunto de funções, formatos e protocolos que melhoram muito o gerenciamento de uma rede SNA e a funcionalidade das aplicações do APPC em execução na rede. O APPN faz isto através de requisitos de configuração reduzidos, pesquisas dinâmicas de diretórios, recursos de cálculos de roteamento e roteamento de sessão intermediária.

Com o APPN, é possível gravar programas sem saber os detalhes da rede principal. Tudo que você precisa saber é o nome da LU parceira; você não precisa saber sua localização. O SNA determina a localização da LU parceira e o melhor caminho para o roteamento dos dados. Uma alteração na rede principal, como por

Introdução às Funções do Communications Server

exemplo, uma alteração no endereço físico, a inclusão de uma nova placa ou a relocação de uma máquina não afeta os programas de APPC.

O Communications Server fornece suporte ao nó final APPN e ao nó da rede para as estações de trabalho, permitindo que se comuniquem de forma mais flexível com os outros sistemas na rede. Além disso, uma função extensora de ramificação permite isolar ramificações para evitar o tráfego desnecessário CP-CP.

- O recurso do nó final fornece os seguintes serviços:
 - Conexão do nó local com um nó da rede de serviço para serviços de diretório e de roteamento
 - Reativação automática de sessões CP-CP quando um nó final perde seu servidor do nó da rede.
- O recurso do nó da rede fornece os seguintes serviços:
 - Serviços de seleção de roteamento que calculam a melhor rota para uma sessão através de uma rede APPN
 - Roteamento de sessão intermediária que permite que duas LUs em nós não adjacentes estejam em sessão uma com a outra, onde a sessão percorre um ou mais nós intermediários
 - Serviços de diretório que fornecem o recurso de aprender as localizações de LUs parceiras dinamicamente
 - Serviços de rede de conexão para a Rede Local que fornece o recurso de aprender os endereços de destino da Rede Local sem ter que configurá-los. Este recurso permite que um nó estabeleça uma ligação diretamente com outro nó com o endereço de destino da Rede Local configurado
 - Suporte extensor de ramificação que permite interconectar de forma eficaz uma filial com Redes Locais, nós finais e nós finais inferiores com LUs dependentes e independentes e PUs, como por exemplo, caixas eletrônicas, a uma ou várias Redes Amplas. Isto permite que mais nós da rede funcionem como gateways para filiais. Em cada filial, uma Rede Local pode ser configurada como uma rede de conexão.

Interfaces de Programação

O Communications Server suporta uma ampla faixa de interfaces de programação de aplicações (APIs) de 32 bit em um servidor para o desenvolvedor do programa aplicativo. Estas APIs fornecem maneiras convenientes para que os programas aplicativos acessem as funções do Communications Server e permitem que as aplicações enderecem as necessidades de comunicação de conexão para computadores IBM e outros. Além disso, as interfaces fornecidas suportam os protocolos SNA para que a padronização seja assegurada.

As APIs suportadas incluem:

- Comunicação Avançada Programa a Programa (APPC)
- Common Programming Interface for Communications (CPI-C)
- RUI e SLI da Interface de Aplicação da LU Convencional (LUA)
- Bibliotecas de Classes de Acesso ao Sistema Central (HAACL)
- Java CPI-C (JCPI-C)
- WinSock (juntamente com o AnyNet Sockets sobre SNA)
- Recurso do Operador da Rede
- Serviços de Gerenciamento
- Serviços Comuns

Introdução às Funções do Communications Server

Nos clientes, a API de APPC Avançada (EHNAPPC) também é fornecida.

O Communications Server Software Developers Tool Kit (que pode ser instalado separadamente a partir do CD-ROM do Communications Server) também está disponível para utilização pelos desenvolvedores da aplicação. Este conjunto de ferramentas contém amostras, arquivos de cabeçalho, arquivos de biblioteca e manuais online para cada uma das APIs.

Para obter maiores informações sobre interfaces de programação do Communications Server, consulte *Client/Server Communications Programming e System Management Programming*.

High Performance Routing

O high performance routing (HPR) é um avanço ao APPN que aumenta o desempenho e confiabilidade do roteamento de dados e estabelece uma ligação virtual entre os nós do protocolo de transporte rápido (RTP). O HPR substitui o roteamento de sessões intermediárias, que é a técnica de roteamento utilizada em APPN.

O HPR fornece transmissão mais rápida em nós intermediários, sessões de novos roteamentos ininterruptas em nós e ligações com falha e regula o fluxo do tráfego prevenindo e reduzindo o congestionamento na rede.

O Communications Server suporta conexões HPR sobre Enterprise Extender (IP), controle de ligação síncrona de dados (SDLC), LAN, WAN, canal, Multi-Path Channel (MPC) e conexões X.25.

Compactação de Dados de SNA

A compactação de dados no nível de sessão aumenta a taxa de rendimento para grandes quantidades de dados através de ligações de comunicação, resultando nos seguintes benefícios:

- Taxa de rendimento de dados avançada em linhas de baixa velocidade
- Custos reduzidos em linhas de alto custo
- Tempos de resposta mais rápidos, resultando em melhoras da produtividade

A compactação de dados de SNA é compatível com as implementações do S/390 e do AS/400 e pode ser utilizada com todos os tipos de LUs.

Descoberta de Fornecedores de Serviço

Trata-se de um protocolo de resolução de endereço da Rede Local que pode ser utilizado por um nó na Rede Local para encontrar outro nó que corresponda a um determinado critério de pesquisa. Ajustando o parâmetro de pesquisa, um nó pode pesquisar os nós da rede APPN, nós que fornecem a função limite do SNA, AS/400s, gateways SNA ou classes de servidor definidas pelo usuário. Um servidor Communications Server para Windows NT pode responder aos pedidos dos clientes como um servidor de nó da rede, um gateway PU 2.0 ou como uma classe de servidor definida pelo usuário. Um Communications Server pode também utilizar a descoberta para encontrar os nós do APPN e os gateways SNA.

Solicitador da LU Dependente (DLUR)

O Communications Server fornece suporte ao solicitador da LU dependente (DLUR) e ao nó final e nó da rede para estações de trabalho, permitindo que tirem vantagem do suporte ao ponto de controle de serviços avançados do sistema (SSCP) fornecido por um servidor de LU dependente (DLUS). O DLUS é suportado pelo VTAM V4R2 e posterior. Com este suporte, as LUs dependentes tradicionais de SNA, tais como, emuladores e até mesmo impressoras, podem obter muitas vantagens de uma rede APPN.

Alguns destes benefícios incluem:

- Permitir que LUs dependentes residam em nós que não são adjacentes ao sistema central
- Utilizar a lógica de pesquisa do APPN para fornecer o melhor caminho para sessões LU-LU

Consulte “Suporte ao Dependent Logical Unit Requester” na página 53 para obter mais informações sobre o DLUR.

SNA Gateway

Um gateway permite comunicação entre sistemas centrais que suportam estações de trabalho de PU 2.0 e estações de trabalho que utilizam tipos diferentes de DLC. Um SNA Gateway pode:

- Permitir que estações de trabalho compartilhem a mesma ligação ao sistema central
- Fornecer várias conectividades do sistema central com estações de trabalho que não possuem o recurso de várias PUs.
- Atuar como um conjunto da PU para estações de trabalho downstream de PU dedicada
- Atuar como um conversor de protocolo entre estações de trabalho que utilizam DLCs em suas ligações que são diferentes do DLC utilizado na ligação ao sistema central
- Reduzir a quantidade de definição do sistema no sistema central e em estações de trabalho
- Permitir a alteração dinâmica das definições da rede e incluir estações de trabalho
- Reduzir recursos do sistema central e reduzir o número de conexões do sistema central através da utilização de LUs agrupadas e do encerramento automático de sessões que não são utilizadas por um longo período de tempo especificado pelo usuário.
- Melhorar a confiabilidade fornecendo uma ligação de reserva ao sistema central

O SNA Gateway permite que um sistema central da família S/390 suporte estações de trabalho que implementam LU 0, 1, 2, 3 ou LU 6.2 dependente (APPC). O SNA Gateway também suporta LU 0, 1, 2 ou 3 em um sistema central AS/400. O sistema central AS/400 transmite os dados através de um sistema central da família S/390.

Cada sistema central visualiza o SNA Gateway como um nó PU 2.0 do SNA, suportando uma ou mais LUs por estação de trabalho. No que diz respeito ao sistema central, todas as LUs pertencem à PU do SNA Gateway. O SNA Gateway pode ter várias conexões do sistema central simultaneamente e direcionar

Introdução às Funções do Communications Server

diferentes sessões de estação de trabalho para sistemas centrais especificados. Entretanto, somente um sistema central (e deve ser em uma ligação com uma PU do CP) pode atuar como o ponto focal e o nome do ponto de controle é anexado a todos os transportes de vetores do gerenciamento de rede (NMVTs) roteados através do gateway.

Para as estações de trabalho suportadas, o SNA Gateway parece um controlador de comunicações da PU 4 de SNA e envia mensagens do sistema central como BIND e UNBIND. As LUs da rede não detectam o SNA Gateway. O SNA Gateway, contudo, está ciente de todas as LUs nas estações de trabalho.

Na verdade, o SNA Gateway é um tipo especial de PU 2.0. Contanto que uma estação de trabalho dependente esteja inativa, o SNA Gateway implementa as funções da LU para a estação de trabalho, exatamente como um PU 2.0 real faria. Entretanto, logo que uma estação de trabalho se torna online para o sistema central, o SNA Gateway permite que a estação de trabalho implemente funções da LU e simplesmente transmite os dados entre estações de trabalho e o sistema central.

Um SNA Gateway permite que as aplicações da estação de trabalho suportada acesse as aplicações remotas suportadas em uma rede de subárea sem necessitar de uma conexão direta separada para cada sistema central em cada estação de trabalho. Do ponto de vista de um sistema central, o sistema central possui uma única conexão com o gateway.

Consulte “Capítulo 7. Como Planejar o SNA Gateway” na página 113 para obter mais informações sobre como utilizar um SNA Gateway.

A Figura 4 mostra um exemplo de uma conexão utilizando um SNA Gateway.

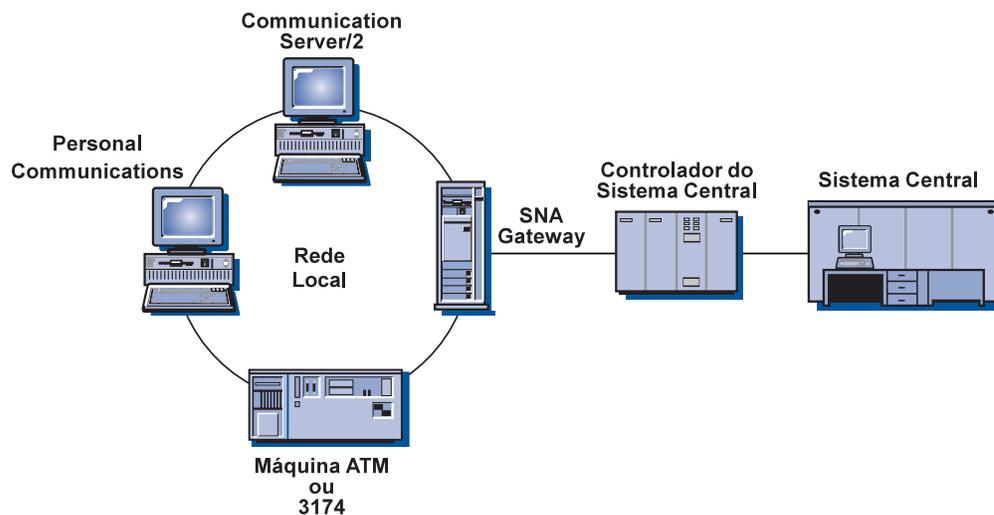
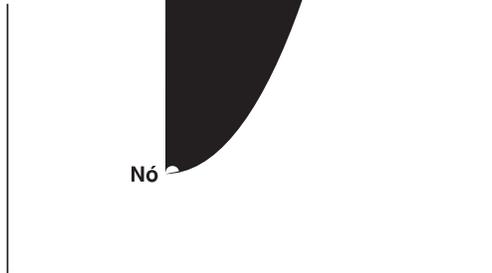


Figura 4. Exemplo de Conexões do SNA Gateway

Suporte AnyNet

O Communications Server incorpora as funções SNA sobre TCP/IP e Sockets sobre SNA a partir da família de produtos AnyNet. Este suporte permite estender e

Nó A: OS/2 / Win32



Servidor TN3270E

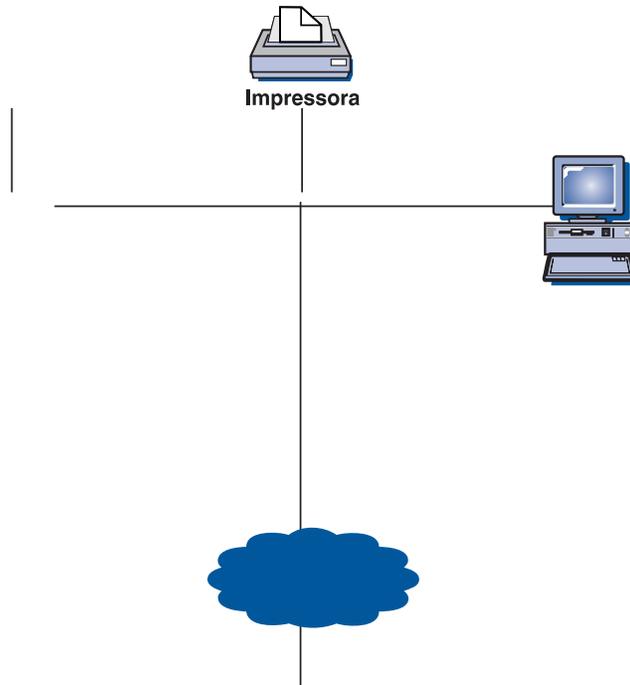
A função do servidor TN3270E permite que usuários do TCP/IP acessem aplicações através de uma máquina do sistema central em uma rede SNA. Qualquer estação de trabalho cliente TN3270 ou TN3270E padrão industrial pode se conectar ao servidor TN3270E para acessar redes SNA. O servidor TN3270E suporta o uso das teclas ATTN e SYSREQ e permite que usuários imprimam de aplicações do sistema central em impressoras conectadas à estação de trabalho. Essas impressoras podem estar conectadas localmente ou conectadas à rede.

O Communications Server suporta o balanceamento de carga para conexões de cliente do servidor TN3270E que se conectam aos mesmos recursos do sistema central, se o cliente estiver ativado para o balanceamento de carga.

O servidor TN3270E suporta a filtragem de IP e do nome do sistema central, que permite o acesso controlado às LUs sem modificar as configurações do cliente.

O servidor TN3270E também suporta a autenticação e criptografia de Secure Sockets Layer (SSL), fornecendo acesso seguro na rede TCP/IP. Se a segurança for especificada, o servidor deverá ter um certificado autenticado fornecido por uma autoridade de certificação, como por exemplo, Verisign. O Communications Server fornece um utilitário que gera e gerencia chaves e certificados utilizados pelo SSL Versão 3.

A Figura 7 mostra um exemplo de conexões do servidor TN3270E.



Servidor TN5250

A função do servidor TN5250 permite que usuários do TCP/IP acessem publicações através de um AS/400 em uma rede SNA. Qualquer estação de trabalho cliente TN5250 padrão industrial pode se conectar ao servidor TN5250 para acessar redes SNA.

O Communications Server suporta o balanceamento de carga para conexões de cliente dos servidores TN5250 que se conectam aos mesmos AS/400s, se o cliente estiver ativado para o balanceamento de carga.

O servidor TN5250 suporta a filtragem de IP e do nome do sistema central, que permite a administração central de acesso de clientes ao servidor, bem como o direcionamento de clientes aos AS/400s específicos.

O servidor TN5250 também suporta a autenticação e criptografia de Secure Sockets Layer (SSL), fornecendo acesso seguro na rede TCP/IP. Se a segurança for especificada, o servidor deverá ter um certificado autenticado fornecido por uma autoridade de certificação, como por exemplo, Verisign. O Communications Server fornece um utilitário que gera e gerencia chaves e certificados utilizados pelo SSL Versão 3.

A Figura 8 mostra um exemplo de conexões do servidor TN5250.

Introdução às Funções do Communications Server

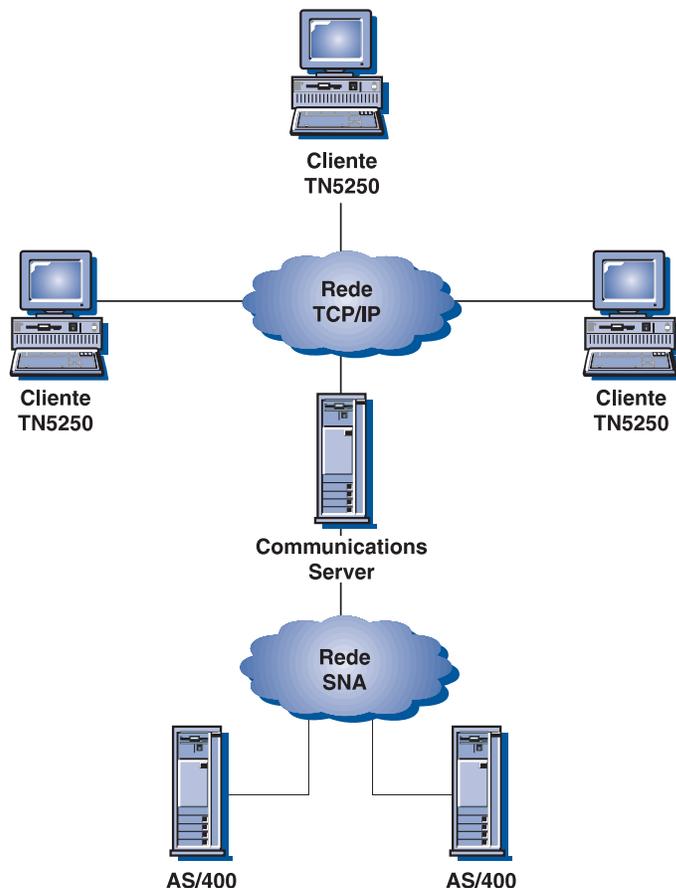


Figura 8. Conexões do Servidor TN5250

Acesso aos Dados já Existentes

O Communications Server fornece acesso aos dados através de máquinas do sistema central, AS/400s e estações de trabalho em redes SNA por meio das seguintes funções:

- Provedor OLE DB do AS/400
- Host Publisher
- Servidor de Pasta Compartilhada do AS/400

Provedor OLE DB do AS/400

As aplicações que utilizam OLE DB ou ActiveX podem se comunicar através do Communications Server para obter acesso ao nível de registro em arquivos do AS/400. A documentação para essa função, bem como informações sobre o desenvolvimento dessas aplicações que utilizam o Client Access, é fornecida no diretório `csnt\sdk\as400_oledb`.

Host Publisher

O Host Publisher fornece acesso através da Web a sites na Web de alto volume com conteúdo dinâmico. Você pode utilizar o Host Publisher, para acessar dados em sistemas centrais S/390 ou AS/400 e para publicá-los em páginas na Web criadas dinamicamente a partir do projeto.

Servidor de Pasta Compartilhada do AS/400

O sistema AS/400 utiliza uma estrutura chamada pasta para armazenar e organizar documentos, correspondência e outros objetos relacionados. O Communications Server permite criar unidades de disco no servidor que se comunica com pastas do AS/400 através do AS/400 Integrated File System (IFS). Além disso, se o servidor compartilhar essas unidades de disco, os clientes poderão utilizar NET USE para elas. Vários clientes podem se conectar às pastas no sistema AS/400 como se elas fossem unidades em suas estações de trabalho.

Você pode utilizar pastas compartilhadas para:

- Utilizar a segurança do AS/400 para limitar o acesso aos arquivos da estação de trabalho
- Compartilhar dados com vários usuários ao mesmo tempo
- Fazer cópia de segurança de arquivos da estação de trabalho em uma pasta do AS/400

Suporte ao Cliente do Communications Server

O Communications Server fornece suporte para clientes API de SNA (disponível em CD-ROM) e para clientes do Novell IntranetWare para SAA.

Suporte ao Cliente API do SNA

O suporte ao cliente API de SNA do Communications Server permite que clientes conectados ao TCP/IP e ao IPX acessem APIs de SNA sem requerer que os protocolos SNA fluam entre os clientes e o servidor. Isto permite que a maioria das configurações do SNA ocorram no servidor central.

O Communications Server suporta clientes API de SNA no Windows 95, Windows NT, Windows 3.1 e no OS/2.

Os clientes SNA fornecem suporte às interfaces CPI-C APPC, EHNAPPC, RUI de LUA, JCPI-C e API de HACL, enquanto fornecem o processamento real de SNA no servidor. Estes clientes são fornecidos como parte do servidor, mas, na realidade, estão instalados e configurados no cliente.

Os clientes de 32 bits do Windows e do OS/2 possuem avanços adicionais:

- Criptografia entre o cliente e o servidor
- Uma formatação mais detalhada de rastreamento que pode ajudar a depurar os problemas mais rapidamente
- Capacidade de iniciar e encerrar o rastreamento enquanto o cliente está em execução
- Capacidade para reinstalar o cliente sem desinstalá-lo

Os clientes do Windows NT e do Windows 95 são executados a partir do mesmo programa executável. Este programa executável pode ser instalado em uma unidade compartilhada; as correções se aplicam aos dois clientes. O novo cliente de 32 bits do Windows pode se comunicar com servidores Communications Servers, ou Novell IntranetWare ou NetWare para SAA.

Para obter mais informações sobre os clientes API no Communications Server, consulte “Capítulo 4. Como Planejar a Comunicação Cliente/Servidor” na página 93 .

Introdução às Funções do Communications Server

Suporte ao Cliente Novell IntranetWare para SAA

O Communications Server suporta clientes conectados ao IPX ou TCP/IP que executam pacotes de software do emulador, que implementam a arquitetura Queue Element/Message Unit (QEL/MU) da Novell para emulação 3270, permitindo que os clientes acessem dados do sistema central mainframe. Isto inclui o suporte aos recursos comuns do cliente, incluindo categorias de LUs dedicadas, agrupadas e públicas (às vezes referidos como tipos de recurso).

O Communications Server suporta clientes Novell IntranetWare para SAA no Windows 95, Windows NT, Windows 3.1 e OS/2.

Consulte o *Novell NetWare for SAA 3270 Client Interface Guide and Reference P/N 100-002018-001* para obter mais informações sobre como desenvolver estes clientes.

Balanceamento de Carga

Agora o Communications Server suporta o balanceamento de carga para todos os tipos de clientes. O balanceamento de carga permite distribuir sessões de LU 0 a 3 e LU 6.2 através dos servidores Communications Server e IntranetWare para SAA. O servidor informa os serviços, incluindo fatores de carregamento, que podem ser reunidos e organizados pelos clientes ou servidores para selecionar um servidor.

Exploração do Diretório

Você pode configurar múltiplos clientes a partir de uma localização central, utilizando o Lightweight Directory Access Protocol (LDAP) para simplificar o processo de configuração.

Para obter informações sobre a utilização da exploração do diretório, consulte “Capítulo 4. Como Planejar a Comunicação Cliente/Servidor” na página 93.

Suporte à Configuração e Administração

O Communications Server fornece recursos para a configuração e administração de recursos.

Configuração do Communications Server

Esta seção fornece uma visão geral dos componentes de configuração do Communications Server e dos métodos utilizados para criá-los ou alterá-los. A configuração é composta de um único arquivo (ACG) armazenado no subdiretório PRIVATE do diretório onde o produto foi instalado (por exemplo, C:\IBMCS\PRIVATE). O arquivo ACG pode ser criado ou modificado pela **Configuração do Nó** ou utilizando um editor ASCII. Existe um programa de verificação disponível para verificar a validade do arquivo ACG antes da utilização.

Você pode utilizar os seguintes métodos para criar ou alterar uma configuração do Communications Server:

- **Configuração do Nó**
- Configuração do arquivo de resposta

Configuração do Nó: O Communications Server fornece a aplicação **Configuração do Nó** (PCSCFG) que permite configurar as funções do Communications Server, utilizando uma interface gráfica e fornece padrões que facilitam a configuração

Introdução às Funções do Communications Server

delas através da utilização de um número mínimo de parâmetros. Quando a configuração for concluída, uma etapa de verificação automática examina a configuração criada e, se não existir conflitos, cria os arquivos de configuração necessários. Se existirem conflitos, os erros serão relatados para que você possa corrigi-los na configuração.

A configuração local é suportada a nível do cliente e do servidor. A configuração remota do servidor é suportada a partir de clientes do Windows NT e Windows 95.

A maioria das configurações pode ser criada utilizando a **Configuração do Nó**. Entretanto, algumas palavras-chave e parâmetros de palavra-chave não são suportados pela **Configuração do Nó**.

Configuração do Arquivo de Resposta: A configuração do arquivo de resposta permite personalizar um arquivo de configuração do gabarito de acordo com as necessidades de usuários específicos. Para obter mais informações sobre como utilizar os arquivos de resposta para configuração, consulte “Configuração com Arquivos de Gabarito e de Resposta” na página 191.

Operações do Nó SNA: As **Operações do Nó SNA** fornecem o recurso de criar e modificar recursos de seleção.

Administração do Communications Server

O Communications Server fornece os seguintes recursos para a administração de recursos.

- **Operações do Nó SNA**
- Utilitários da linha de comandos
- Administração baseada na Web
- Módulo Tivoli Plus

Para obter mais informações sobre as capacidades destes recursos, consulte o “Capítulo 16. Recursos de Gerenciamento de Sistema” na página 203.

Balanceamento de Carga

Balanceamento de carga é uma função do Communications Server que equilibra dinamicamente sessões de LU dependente (sistema central para estação de trabalho) e sessões de LU 6.2 independente, distribuindo-as ao communications server com o menor carregamento. O Communications Server executa o balanceamento de carga para programas de API do Communications Server e emuladores 3270 de outros fabricantes que se conectam através de protocolos TCP/IP ou emuladores TN3270 e TN5250 de outros fabricantes. Os recursos através dos quais ocorre o equilíbrio dependem do tipo de sessão:

- Para sessões de LU dependente, o carregamento é distribuído através de servidores em um conjunto da LU especificado e um escopo especificado.
- Para sessões de LU 6.2, o carregamento é distribuído através de todos os servidores disponíveis em um escopo especificado ou através dos servidores selecionados em uma lista de servidores especificados.

Os recursos do balanceamento de carga do Communications Server são criados nas APIs de cliente SNA. O balanceamento de carga é configurado para os clientes que utilizam a **Configuração do Cliente SNA**.

Introdução às Funções do Communications Server

Para sessões de LU dependente, os emuladores que utilizam as APIs de cliente SNA podem participar do balanceamento de carga. Caso contrário, será necessário adquirir o software do emulador 3270, TN3270 ou TN5250 de outro fabricante que suporte o balanceamento de carga.

Para sessões LU 6.2, a conexão inicial estabelecida por um cliente API de SNA determina o servidor que gerencia todas as sessões subseqüentes da LU 6.2.

Para obter mais informações sobre o balanceamento de carga, consulte “Capítulo 11. Como Planejar o Balanceamento de Carga” na página 141.

Segurança de Dados

O Communications Server fornece suporte de segurança básico ou avançado aos níveis de sessão e conversação. Há segurança na limitação de quais usuários do Windows NT podem acessar os recursos do SNA através dos clientes API do SNA. A segurança da conversação inclui suporte para substituição de senha. Há também segurança de LU-LU avançada.

O Communications Server fornece suporte à segurança baseada em Secure Sockets Layer (baseada em SSL) em conexões entre clientes TN e os servidores TN3270E ou TN5250. Essa segurança utiliza SSL Versão 3 para fornecer criptografia de dados e autenticação do servidor, utilizando certificados aprovados.

Suporte a Placas

O Communications Server fornece uma interface aberta para que os fabricantes de placas criem soluções de conectividade. É fornecida uma interface de placa superficial (não programável) para que os fabricantes de placas trabalhem com a pilha de protocolo SDLC e X.25 do Communications Server. É fornecida uma interface de placa profunda (programável) para que os fabricantes de placas criem soluções de conectividade utilizando os controles de ligação de dados fornecidos pelo fabricante.

Suporte ao Data Link Control (DLC)

O Communications Server permite comunicações através dos seguintes DLCs:

- AnyNet (SNA sobre TCP/IP)
- Biaxial (somente upstream)
- Rede Local (Toda placa de rede compatível com NDIS**)
- X.25 SDLC (síncrono, assíncrono e AutoSync)
- OEM (suporte a placas de outros fabricantes)
- Canal (somente upstream)
- Multi-Path Channel (somente HPR)
- Enterprise Extender

DLC AnyNet (SNA sobre TCP/IP)

Para obter mais informações sobre as capacidades destes recursos, consulte “SNA sobre TCP/IP” na página 13.

DLC do IBM Multi-Path Channel

O DLC do Multi-Path Channel (MPC) fornece conexões de fibra de grande capacidade e grande disponibilidade com um ou mais sistemas centrais compatíveis com MPC do S/390 sob a placa adaptadora do canal ESCON (P/N 9663 001). As conexões do MPC fornecem altas taxas de transmissão de dados com cópia de segurança transparente quando as conexões físicas são interrompidas ou se tornam temporariamente indisponíveis. Essa conexão canal a canal permite que clientes da rede local fiquem habilitados para acessarem recursos e serviços S/390.

DLC do Enterprise Extender

O Communications Server agora fornece conexões HPR em redes IP, utilizando pacotes UDP/IP. Para a rede HPR, a rede principal IP parece ser uma ligação lógica. Para a rede IP, o tráfego de SNA parece ser datagramas de UDP. Estes datagramas são roteados sem alterações na rede principal IP. Como não existe transformação de protocolo e a compactação ocorre no nível de roteamento sem a sobrecarga de níveis de transporte adicionais, isto resulta na utilização eficaz da infra-estrutura da intranet para clientes IP que acessam dados baseados em SNA (por exemplo, clientes TN3270 ou navegadores da Web que utilizam o IBM Host on Demand), bem como para clientes SNA.

Suporte MIB de APPN

O Communications Server suporta pedidos do simple network management protocol (SNMP) para informações sobre o gerenciamento de APPN a partir de qualquer sistema de gerenciamento do SNMP.

Sistema de Reserva Ligado

No Communications Server, você pode configurar determinadas ligações ao sistema central para ativar automaticamente se um servidor crítico especificado falhar. As conexões configuradas para um sistema central podem continuar a funcionar pela ativação de conexões alternativas em um servidor de reserva. Esta função é conhecida como sistema de reserva ligado.

As conexões especificadas na configuração de um servidor crítico no servidor de reserva são ativadas quando o servidor de reserva detecta uma perda de contato com o servidor crítico e as cargas de permissão para o servidor crítico são gerenciadas no servidor de reserva.

Nota: O recurso sistema de reserva ligado fornece somente a ativação de conexões do sistema central em um servidor de reserva e depende da utilização do software do emulador que suporta o roteamento alternativo para o servidor de reserva quando um servidor crítico se torna inativo.

Para obter mais informações sobre como utilizar o sistema de reserva ligado para conexões de reserva, consulte “Capítulo 12. Como Planejar as Conexões ao Sistema Central de Reserva” na página 145.

Funções do Emulador de Nível de Entrada

O Communications Server inclui uma versão de nível de entrada do emulador popular 3270 e 5250 do Personal Communications para objetivos administrativos. Este emulador fornece suporte básico 5250 e 3270 no servidor que contém um

Introdução às Funções do Communications Server

subconjunto de recursos e funções que estão na família de emuladores de função completa do IBM Personal Communications.

As funções de emulação de nível de entrada fornecidas incluem:

- Mapeamento de cores
- Transferência de linha de comando (apenas para 3270)
- Conjunto completo de fontes
- Tamanhos de telas modelo 2-5
- Duas sessões

Embora o remapeamento gráfico do teclado não seja suportado para o emulador de nível de entrada, você poderá utilizar os arquivos de remapeamento gerados pelo emulador de função completa.

Capítulo 2. Communications Server e SNA

Este capítulo discute as funções da rede SNA fornecidas pelo Communications Server e inclui os seguintes tópicos:

- Visão geral das funções de SNA
- Definições de controle de ligação de dados (DLC)
- Sistema Avançado de Rede Ponto a Ponto (APPN)
- High Performance Routing (HPR)
- Suporte à LU
- Compactação de dados
- Criptografia
- Serviços de gerenciamento (MS)
- Controle de fluxo
- Suporte ao SNA Gateway

Visão Geral das Funções de SNA

Esta seção fornece uma visão geral de como o Communications Server implementa o SNA em uma estação de trabalho. Não é uma discussão abrangente das funções de SNA. Para obter informações mais detalhadas sobre SNA, consulte os seguintes manuais:

- *Systems Network Architecture Concepts and Products*
- *Visão Geral Técnica do Systems Network Architecture*
- *Formatos de Produtos de Rede Systems Network Architecture* (disponível online na lista de documentações do Communications Server)
- *Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic for LU Type 6.2*

O SNA define os padrões, protocolos e funções utilizados por dispositivos na rede (desde mainframes até terminais) para comunicação entre os mesmos. Esta comunicação permite que estes dispositivos compartilhem informações e recursos de processo de forma transparente. Em outras palavras, um usuário em uma estação de trabalho não precisa saber o que acontece no plano de fundo para acessar informações em um sistema central ou para se comunicar com outro usuário.

Uma rede SNA é organizada como um sistema de nós e ligações. É importante lembrar que essa organização é lógica. O SNA classifica os nós de acordo com seus recursos e com a quantidade de controle que eles têm sobre outros nós na rede. O tipo de nó não está necessariamente associado a um tipo específico de hardware. Os recursos de um nó podem ser executados por diferentes dispositivos. Uma estação de trabalho que age como um gateway pode executar as mesmas funções que um controlador de comunicações. É até possível que um único dispositivo contenha mais de um nó.

A rede SNA é responsável por mover os dados entre dois usuários finais, de uma maneira eficiente, ordenada e confiável. Por exemplo, quando um usuário em uma estação de trabalho envia uma mensagem a outra estação de trabalho, o SNA executa as seguintes funções:

Communications Server e SNA

- Compacta a mensagem de uma forma que pode ser utilizada no tipo de ligação
- Endereça o pacote
- Seleciona uma rota para a mensagem
- Supervisiona a comunicação para assegurar que a mensagem chegue no destino
- Converte a mensagem de volta a um formato que pode ser utilizado no destino

Estas tarefas são definidas no SNA como camadas funcionais separadas. Estas camadas não são discutidas aqui, mas é importante lembrar que todas as camadas do SNA fazem parte de uma ligação lógica.

Conforme mencionado anteriormente, os nós SNA classificam-se de acordo com seus recursos de comunicações e com a quantidade de controle que o nó tem sobre outros nós na rede. Os nós SNA são amplamente classificados como nós de subárea e nós periféricos. Os nós de subárea são como hubs e podem se comunicar com os nós periféricos e com outros nós de subárea. Os nós de subárea ativam e controlam recursos nos nós periféricos. Os nós de subárea também são classificados como nós tipo 4 ou tipo 5. Os nós tipo 5 contêm um ponto de controle de serviços do sistema (SSCP) que fornece um ponto de controle central para os nós tipo 4 conectados ao mesmo. Um nó tipo 5 às vezes é chamado de nó do sistema central. Um nó periférico só pode se comunicar diretamente com o nó de subárea ao qual está conectado. Entretanto, um nó periférico pode controlar dispositivos aos quais está conectado. Por exemplo, um controlador de agrupamento de dispositivos que age como um nó periférico pode suportar os terminais conectados a ele. Os nós periféricos também são chamados de nós tipo 2 ou tipo 2.1.

Cada nó contém unidades acessíveis da rede (NAUs) que executam funções de controle e comunicação. Uma dessas NAUs é uma unidade física (PU). A PU gerencia os recursos físicos do nó. Outras NAUs chamadas unidades lógicas (LUs) fornecem pontos de acesso à rede lógicos que permitem a comunicação entre os usuários e as aplicações em cada nó. A comunicação entre as unidades lógicas é chamada de sessão. As sessões não só suportam a comunicação entre os usuários e as aplicações como também suportam a comunicação entre as aplicações, para compartilhar recursos de processamento. A comunicação entre as aplicações é conhecida como advanced program-to-program communication (APPC). APPC é um conjunto de convenções e protocolos de programação que implementam a LU 6.2. (APPC é o nome dado ao recurso LU 6.2 em produtos que implementam este tipo de LU.)

Perfis de Data Link Control

O controle de ligação de dados (DLC) permite trocas de dados ordenadas entre dois nós através de uma ligação lógica. O DLC fornece os protocolos necessários à entrega confiável de unidades básicas de transmissão (BTUs) entre um par de nós na rede SNA. Você deve configurar os perfis de DLC apropriados do Communications Server para que uma estação de trabalho acesse uma rede SNA.

Consulte o *Tutorial* online para obter mais informações sobre como configurar os perfis de DLC apropriados.

Advanced Peer-to-Peer Networking

Advanced Peer-to-Peer Networking (APPN) é uma extensão do SNA que inclui funções de comunicações além daquelas descritas nas seções anteriores. Seus componentes básicos incluem:

- Tipos de nós do APPN
- Pontos de controle
- Extensor de ramificação
- Controle de ligação de dados
- Ligações lógicas
- Serviços de Diretório
- Serviços de topologia e seleção de rotas

Tipos de Nós do APPN

Esta seção discute os três tipos de nós implementados pelo Communications Server, que podem participar de uma rede APPN:

- Nó da rede
- Nó final
- Nó da rede de entrada (LEN)

Além disso, o extensor de ramificação é uma extensão para um nó da rede. Embora forneça serviços aos nós finais como um nó da rede, ele aparece na rede como um nó final conectado a outros nós da rede.

Cada nó distingue-se dos outros na rede através de um nome exclusivo que consiste em duas partes — um ID da rede e um nome de nó local (também conhecido como um nome de ponto de controle [CP]). O nome identifica cada nó para todos os outros nós na rede. Além disso, o nó pode ter múltiplos nomes de PUs para acesso simultâneo a vários sistemas centrais T4/5 da PU.

Um nó pode ser configurado para ser um nó final ou um nó da rede, mas quando um nó final não tem sessões CP a CP (consulte “Sessões CP a CP” na página 28) para um nó de rede APPN, ele age como um nó LEN. Um nó LEN não suporta funções do APPN.

Os tipos de nós são descritos com mais detalhes nas seções seguintes. A Figura 9 na página 26 ilustra um exemplo de rede APPN que inclui todos estes tipos de nós.

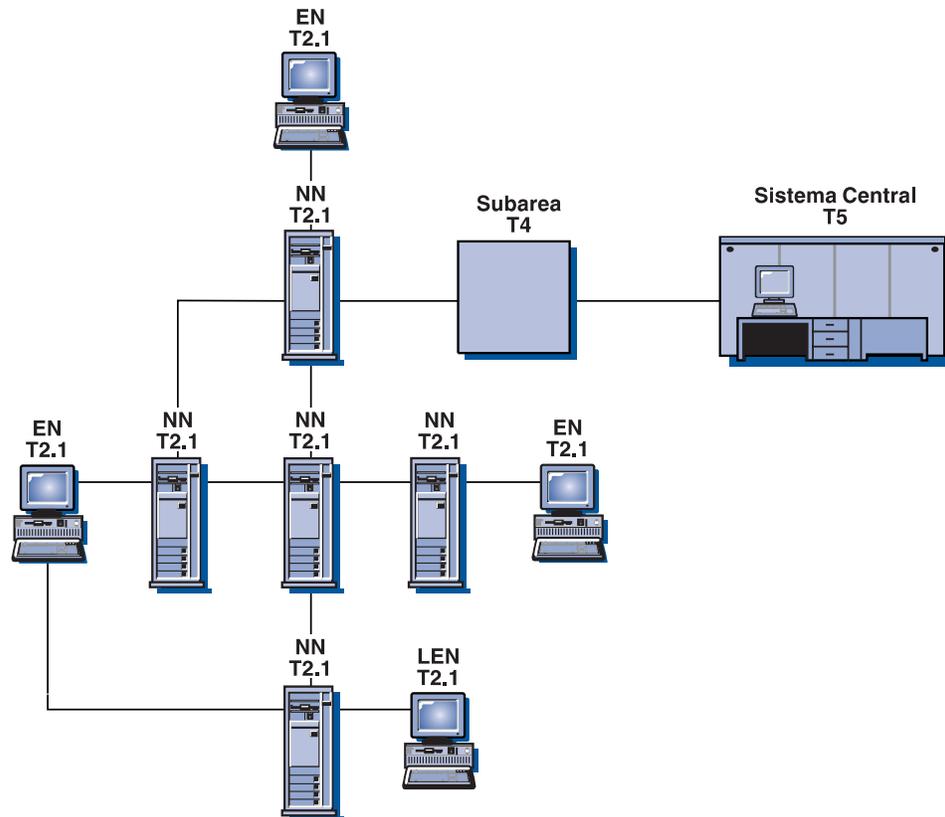


Figura 9. Uma Parte de Um Exemplo de Rede APPN. Essa visualização da topologia da rede mostra cinco nós da rede (NNs). Três nós finais (ENs) estão conectados, bem como um nó LEN e subárea. Os programas aplicativos de APPC escritos para qualquer nó nessa rede podem se comunicar com qualquer outro.

Nó da Rede

Um nó da rede suporta seus próprios usuários finais, fornece serviços de diretório, seleção de rota e gerenciamento aos nós finais e executa o roteamento intermediário de dados em sessões que o atravessam. O nó da rede executa pesquisas distribuídas da rede para localizar LUs parceiras e calcula a melhor rota do nó de origem até o nó de destino, com base em critérios especificados pelo usuário.

Um servidor do nó da rede consulta a função de um nó da rede ao agir como ponto de entrada da rede para nós finais específicos conectados a ele. Estes nós finais são definidos como se estivessem em seu domínio. Por exemplo, todos os pedidos do diretório relativos a recursos (como LUs) nestes nós finais (bem como seus próprios recursos) passam pelos serviços de diretório no servidor do nó da rede. Os nós da rede conseguem coletar e controlar informações de diretório que passam para a rede APPN.

Um nó da rede fornece o seguinte:

- Serviços de sessão LU-LU para suas LUs residentes locais
- Roteamento de sessão intermediária
- Funções do servidor de rede (para executar pesquisas de diretório da rede e seleção de rota) para nós finais ou nós LEN conectados (bem como para suas próprias LUs residentes localmente)

- Recurso de roteamento de serviços de gerenciamento (MS) para expedição de dados de serviços de gerenciamento (como alertas) entre um nó final servido e um ponto focal (FP) de serviços de gerenciamento.

Nó Final

Um nó final opera em um ambiente do mesmo nível para sessões LU-LU (utilizando protocolos de LU 6.2) enquanto fornece funções adicionais do APPN. Um nó final fornece aos usuários finais as funções de APPN, como serviços de diretório e serviços de seleção de rota, no seu próprio nó. Ele pode participar da rede APPN através da utilização dos serviços de um servidor do nó da rede conectado para pedidos de sessão que envolvem nós que não estão conectados diretamente. Ele faz isso trocando pedidos e respostas de serviços de diretório com um nó da rede adjacente (seu servidor) com a utilização de sessões CP a CP.

Os nós finais APPN podem registrar as LUs locais no servidor de nó de rede. Registrando os nós finais, o operador da rede no servidor do nó da rede não precisa predefinir os nomes de LUs para as LUs em todos os nós finais conectados para os quais o nó da rede fornece serviços.

Um nó final APPN pode ser conectado a múltiplos nós da rede, mas só pode ter sessões CP a CP ativas com um nó da rede de cada vez — o seu servidor do nó da rede. Os outros nós da rede podem ser utilizados para fornecer roteamento de sessão intermediária para o nó final ou podem ser utilizados como um servidor do nó da rede substituto se o servidor do nó da rede principal ficar indisponível. As sessões CP a CP nunca são estabelecidas entre dois nós finais.

Nó LEN

Nó LEN é um nó que implementa os protocolos T2.1 básicos sem os avanços do APPN. Em um nó LEN, todas as conexões potenciais às LUs parceiras são predefinidas antes do início das sessões para elas. Um nó LEN conectado a um nó da rede APPN adjacente utiliza as funções avançadas do APPN, predefinindo conexões potenciais a LUs parceiras como se elas existissem neste nó da rede. Por sua vez, o nó da rede pode agir automaticamente como o servidor do nó da rede do nó LEN, localizar o destino real da LU parceira e selecionar a melhor rota para o mesmo. Passando por um nó da rede, o nó LEN pode participar de uma rede APPN sem conexões diretas a todos os nós.

Pontos de Controle

O ponto de controle (CP) é responsável por gerenciar o nó e seus recursos. Para obter serviços de rede APPN, o ponto de controle em um nó final APPN deve se comunicar com o ponto de controle em um nó da rede adjacente. Além disso, para gerenciar a rede, o ponto de controle em um nó da rede APPN deve se comunicar com os pontos de controle em nós da rede adjacentes. O ponto de controle direciona essas funções como ativação e desativação da placa e ativação e desativação da ligação, e fornece assistência às LUs no início e término da sessão.

Ao configurar uma estação de trabalho, você deve definir o nome do ponto de controle (também conhecido como nome do nó local). O ponto de controle também é uma LU e você pode optar por ter a LU do ponto de controle como a única LU definida na estação de trabalho.

Sessões CP a CP

Para executar serviços de diretório e topologia e serviços de seleção de rota, os nós adjacentes em toda a rede APPN utilizam um par de sessões CP a CP paralelas para troca de informações da rede. Os nós da rede utilizam sessões CP a CP para supervisionar nós em uma ligação de rede, bem como para rastrear serviços de diretório e sessão. Um nó da rede estabelece duas sessões paralelas com cada nó adjacente da rede e com cada nó final servido. Um nó final APPN estabelece duas sessões paralelas com um único nó da rede adjacente, agindo como o seu servidor atual. Os nós LEN não suportam sessões CP a CP.

Após o estabelecimento da conexão, os nós trocam identificadores de troca (XID). Em seguida, as sessões CP a CP são iniciadas entre os pontos de controle nos nós conectados diretamente. As sessões CP a CP utilizam protocolos LU 6.2 e ambas as sessões de um determinado par devem estar ativas para que os pontos de controle parceiros iniciem e sustentem suas interações. Todas as sessões CP a CP são utilizadas para conduzir pesquisas de diretório.

Após o estabelecimento das sessões CP a CP, os dois nós trocam mensagens de recursos do ponto de controle que informam a cada nó sobre os recursos do outro. Quando ambos os nós são nós da rede, eles trocam mensagens de atualização do banco de dados de topologia (TDU). As mensagens de TDU contêm informações de identificação, características do nó e da ligação, e números de seqüência dos recursos para identificar as atualizações mais recentes de cada um dos recursos descritos na TDU.

Ativação da Conexão CP a CP

Quando o Communications Server é iniciado, ele tenta ativar a conexão ao servidor NN preferido primeiro. O Communications Server tenta ativar todas as outras conexões definidas como **ativar na inicialização**. Se existir uma ligação paralela alternativa à conexão ao servidor NN preferido, em vez de aguardar os resultados da tentativa de ativação para a conexão ao servidor NN preferido antes de tentar uma ligação alternativa, o Communications Server tenta ativar sessões CP a CP na ligação alternativa.

Nota: Se a conexão foi desativada a pedido do operador a partir do nó local, as sessões CP a CP não são redirecionadas. Se a conexão foi desativada a pedido do operador a partir do nó remoto, as sessões CP a CP são redirecionadas no nó local. Para ligações entre nós NN, apenas as ligações ativadas por demanda (ligações com o CPName adjacente especificado e que não estejam definidas como **ativar na inicialização**) são ativadas.

Reativação da Conexão CP a CP

O Communications Server fornece suporte à reativação da conexão CP a CP. A perda de sessões CP a CP entre um nó final e seu servidor do nó da rede, e entre nós da rede adjacentes pode interferir na operação de uma rede APPN. O suporte à reativação da conexão CP a CP melhora a confiabilidade de uma rede APPN através do restabelecimento dessas sessões importantes quando elas são encerradas devido a falhas ou desativação da conexão.

A tentativa de reativação da conexão CP a CP é iniciada pela ativação de uma ligação CP a CP, por uma falha na sessão CP a CP ou pela expiração do temporizador de repetição de CP a CP. As sessões CP a CP são iniciadas pelo Communications Server com a primeira ocorrência dos itens a seguir:

1. A sessão CP a CP do servidor preferido (se não tiver sido tentada anteriormente).
2. Se o DLUR estiver configurado, utilize um CP adjacente que suporte registro do DLUR.
3. A última (mais recente) ativação de NNs que não foi tentada, para a qual existe uma conexão ativa.
4. O primeiro de qualquer NN de nível superior para o extensor de ramificação

Nota: Se as conexões CP a CP foram terminadas devido a uma falha na ligação, o Communications Server não reativará a ligação. Você pode configurar uma conexão como **reativar automaticamente** (repetição infinita) para manter conexões importantes ativas.

Extensor de Ramificação

O extensor de ramificação é um subconjunto de nós intermediadores projetado para interconectar uma filial a uma rede principal da Rede Ampla APPN. As redes interconectadas podem ser nativas (isto é, têm o mesmo ID da rede) ou não-nativas. Um nó que suporta o extensor de ramificação é um nó de ramificação da rede que geralmente possui interfaces com Rede Local e Rede Ampla e também pode incluir DLUR e HPR.

As ligações em um nó, que suportam o extensor de ramificação, são definidas como **ligações superiores da ramificação** ou **ligações inferiores da ramificação**. A Figura 10 fornece um exemplo da forma como um nó de ramificação da rede funciona em uma rede. Nesta figura, o nó no centro é um nó de ramificação da rede. Geralmente o CP adjacente (nó de ligação superior da ramificação) será o servidor do nó da rede (NNS) para o nó de ramificação da rede, que se parece com um nó final para o nó de ligação superior da ramificação.

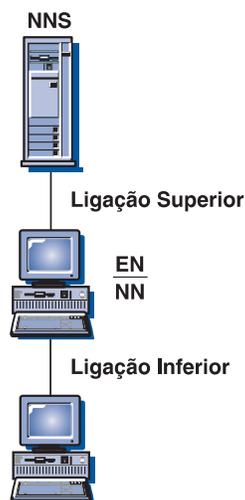


Figura 10. Visão Geral Conceitual das Ligações Superiores e Inferiores da Ramificação

As ligações superiores da ramificação são definidas no nó de ramificação da rede como upstream, para a rede principal. Você pode considerar que um nó com uma ligação superior é conectado de maneira periférica à rede principal.

As ligações inferiores da ramificação são definidas a partir do nó de ramificação da rede como downstream. O nó vê as ligações inferiores como conexões aos nós

Communications Server e SNA

finais (pontos de controle) no domínio. As ligações inferiores da ramificação são tipicamente ligações de Rede Local (mas não precisam ser). Você pode considerar os nós finais conectados através de ligações inferiores da ramificação como recursos locais. O nó de ramificação da rede é o servidor do nó da rede para esses nós finais. Nas ligações inferiores da ramificação, ele fornece serviços de nó da rede para nós finais do domínio, nós finais LEN, nós T2.0 dependentes e nós T2.1, e LUs e PUs locais.

Um nó de ramificação da rede funciona como um servidor do nó da rede para seu domínio. Ele mantém informações topológicas sobre todos os seus nós de ligação inferior da ramificação, mas não mantém informações completas sobre toda a rede de ligações superiores. Se as informações que o nó possui não forem suficientes, ele transmitirá o pedido LOCATE ao seu servidor do nó da rede da ligação superior, que pode ser outro nó de ramificação da rede ou um nó de rede APPN.

O extensor de ramificação otimiza o ambiente de comunicação ponto a ponto para os administradores que desejam conectar ramificações baseadas em Rede Local a uma Rede Ampla grande, baseada principalmente em uma rede comutada. O extensor de ramificação melhora o desempenho em grandes redes APPN. Especificamente, ele:

- Reduz o número de nós da rede em grandes redes APPN, permitindo que você inclua ramificações adicionais da rede
- Oculta informações sobre topologia da ramificação
- Permite a comunicação ponto a ponto entre as ramificações conectadas à mesma rede de conexão APPN
- Permite a coexistência com servidores de gateway de PU
- Reduz o tráfego de sessões CP a CP da ligação superior (tráfego da Rede Ampla)
- Isola a rede de ramificações da sobrecarga de tráfego da Rede Ampla principal

Communications Server e SNA

- Para evitar loop na pesquisa, os nós finais da ligação inferior devem ser nós finais reais e não nós que apresentam uma imagem do nó final.
- Um nó não pode ter sessões CP a CP com o nó de ramificação da rede através de ligações superiores e inferiores da ramificação, simultaneamente.
- O nó de ramificação da rede pode ter sessões CP a CP através de apenas uma ligação superior da ramificação de cada vez. Isto é, ele pode ter sessões CP a CP com no máximo um servidor do nó da rede.
- O extensor de ramificação não fornece suporte a Twinax.
- Um nó do extensor de ramificação não pode ter sessões DLUR downstream.

Configuração do Extensor de Ramificação

Para configurar o extensor de ramificação, você deve primeiro configurar um nó de ramificação da rede. Em seguida, você deve configurar um DLC (para uma ligação implícita) ou um nó de ramificação da rede. Uma ligação configurada para suportar o extensor de ramificação é uma ligação superior da ramificação. Em um nó de ramificação da rede, as ligações que não são configuradas para suportar o dispositivo são ligações inferiores da ramificação.

Se os nós de ramificação da rede tiverem ligações definidas entre si, eles deverão ser definidos como conexões **ponto a ponto**, o que lhes concede um tipo de ligação **LEARN** no arquivo ACG. Alternativamente, você pode definir a ligação como **ACTIVATE_AT_STARTUP=1**, assim a ligação estará sempre ativa. Quando os nós da ramificação forem conectados uns aos outros, ocorrerão loops na topologia. Isto é aceitável, contanto que as ligações estejam sempre ativas ou que fiquem conhecidas à medida que forem ativadas. Se forem definidas ligações entre os nós de ramificação da rede como ligações de **END_NODE** ou **NETWORK_NODE**, a topologia informada na direção oposta ao fluxo poderá interpretar as ligações inadequadamente e causar falhas na alocação.

Você também pode utilizar um arquivo ACG para configurar o extensor de ramificação.

Administração do Extensor de Ramificação

As seções seguintes descrevem como verificar uma configuração e as restrições à forma como você configura a rede.

Como Verificar a Configuração: Você pode utilizar as **Operações do Nó SNA** em um nó que suporta o extensor de ramificação, para determinar se uma ramificação local foi configurada de forma bem-sucedida. No tempo de execução, uma exibição da topologia a partir do nó nunca deve ter mais de dois nós da rede, ele mesmo e o servidor do nó da rede de ligação superior.

Nota: Apenas uma ligação superior está disponível para CP a CP. Cada estação de trabalho deve ser configurada como um nó final com o nó de ramificação da rede definido como seu servidor do nó da rede preferido.

Você pode utilizar as **Operações do Nó SNA** para verificar se o DLC ou a ligação foram configurados para suportarem corretamente o extensor de ramificação. Você também pode utilizar **Operações do Nó SNA** para determinar se uma ligação ativa é uma ligação superior ou inferior da ramificação. Os nós finais downstream registrados com a utilização do AnyNet não registrarão seus recursos.

Funções Suportadas

O Communications Server suporta todas as funções de base (tanto de nó final quanto de nó da rede) do APPN Versão 2. Adicionalmente, as seguintes opções são suportadas:

- Nó Final

Conjunto de Funções	Opção
162	EN da Esfera de Controle (SOC) do MS_CAPS Be
171	Dados de Diagnóstico de Problemas no Alerta
177	Alerta da Rede Local
178	Alerta do LLC de SDLC/Rede Local
181	Alerta X.25
182	Alerta Mantido para CPMS
1002	Nome da Estação de Ligação Adjacente
1007	TGs Paralelos
1011	Múltiplas LUs Independentes Locais
1012	CP=LU
1018	Eliminar Recursos de EN Antes de Registrar
1067	Solicitador da LU Dependente
1070	Criptografia de Sessão
1107	Registro de Recurso Central (das LUs)
1116	Registro de LU Servido por DLUS
1200	Armazenamento de Árvore e TC em Cache
1400	Base HPR (ANR)
1401	Rapid Transport Protocol
1402	Fluxos de Controle sobre RTP
1520	Serviços de Operações Comuns

- Nó da Rede

Conjunto de Funções	Opção
164	MS_CAPS Possui um Ponto Focal de Subárea
171	Dados de Diagnóstico de Problemas no Alerta
177	Alerta da Rede Local
178	Alerta do LLC de SDLC/Rede Local
181	Alerta X.25
182	Alerta Mantido para CPMS
1002	Nome da Estação de Ligação Adjacente
1007	TGs Paralelos
1011	Múltiplas LUs Independentes Locais

Communications Server e SNA

1012	CP=LU
1018	Eliminar Recursos de EN Antes de Registrar
1067	Solicitador da LU Dependente
1070	Criptografia de Sessão
1100	Armazenamento Seguro da Cache do Diretório
1101	Carregar Previamente a Cache do Diretório
1107	Registro de Recurso Central (das LUs)
1116	Registro de LU Servido por DLUS
1118	Registro de Vetor TG do EN
1121	Função do Extensor de Ramificação
1200	Armazenamento de Árvore e TC em Cache
1203	Deteção e Eliminação de Avisos de TDU
1301	Tráfego de Sessão Intermediária Não-Espaçado
1400	Base HPR (ANR)
1401	Rapid Transport Protocol
1402	Fluxos de Controle sobre RTP
1520	Serviços de Operações Comuns

Data Link Control (DLC)

O DLC fornece os protocolos necessários para a entrega confiável de unidades básicas de transmissão (BTUs) entre um par de nós na rede APPN e mantendo as conexões lógicas entre os nós.

Conexões

Uma conexão liga um par de nós adjacentes através do DLC fundamental.

Ligações Paralelas

O nó local pode ter múltiplas ligações a um nó adjacente. Essas associações chamam-se **ligações paralelas**. Um número exclusivo (número do grupo de transmissão) é designado a cada uma das ligações paralelas e elas podem ter diferentes características de ligação atribuídas a elas. Para que haja duas ligações paralelas entre dois nós, as estações de ligação das ligações podem estar em uma única placa em um dos nós, mas devem estar em placas separadas no outro nó. Isto é, a combinação de número da placa e endereço da estação de ligação adjacente (ou de destino) deve ser exclusiva para cada ligação.

Ativação da Ligação

A unidade de mensagem utilizada para transportar as características do nó e da ligação até um nó adjacente chama-se **Identificador de Troca (XID)**. Se **USE_PU_NAME_IN_XID=1**, o nome da PU será utilizado no campo CPName do XID. Caso contrário, o nome do ponto de controle será utilizado neste campo. Os XIDs são trocados entre os nós antes e durante a ativação da ligação, para estabelecer e negociar as características da ligação e do nó, e após a ativação da ligação para comunicar alterações nessas características.

Os nós do APPN trocam o formato 3 do XID (XID3) com outros nós T2.1 ou nós limite para executar a negociação de funções. Para conexões da PU 2.0, você utiliza a palavra-chave **LINK_STATION** para especificar um nome de PU e um ID de nó que são trocados no XID3. Se **USE_PU_NAME_IN_XID=1**, o nome da PU será utilizado no campo nome do XID. Caso contrário, o nome do ponto de controle será utilizado neste campo. As informações sobre as características do nó remetente estão contidas no XID3, incluindo a função da estação de ligação (principal, secundária ou negociável), o número de TG, o tipo de nó, o número da ligação lógica, o tamanho máximo da unidade de transmissão básica que pode ser recebida, o ID do nó e o nome da PU. Normalmente, o nome da PU é o nome do ponto de controle, mas pode-se especificar um nome de PU e um ID de nó alternativos na palavra-chave **LINK_STATION**, para suportar conexões simultâneas de PU 2.0.

Tipos de Ligações

Os seis tipos de ligações a seguir geralmente são definidos nos nós do Communications Server:

- Acesso principal à rede, inicialmente ativado (APPN ou sistema central)
- Acesso principal à rede, ligação ao sistema central
- Acesso principal à rede, utilizado em tempo integral (utilize quando necessário)
- Acesso secundário à rede, ligação de recepção (características de ligação predefinidas)
- Acesso secundário à rede, utilização limitada (também chamado de ligação limitada ao recurso)

A configuração do Communications Server fornece uma maneira de definir e controlar a utilização desses tipos de ligações. Esta seção descreve os parâmetros de configuração do nó, DLC e ligação utilizados, bem como os relacionamentos e as dependências existentes entre esses parâmetros. As seguintes categorias são descritas:

- Parâmetros de definição e ativação da ligação
- Parâmetros de desativação da ligação
- Outros parâmetros da ligação

Os seguintes parâmetros são descritos:

- **Parâmetros de definição e ativação**
 - Ativar na inicialização
 - Ativar por pedido
 - Repetição automática da ligação
 - Máximo de tentativas de ativação
 - Reativação solicitada pelo usuário
- **Parâmetros de desativação**
 - Tempo de espera de inatividade
 - Recurso limitado
- **Outros parâmetros da ligação**
 - Rede de conexão
 - Suporte à sessão CP a CP
 - Suporte ao high performance routing (HPR)
 - Tipo de nó adjacente

Communications Server e SNA

- Servidor do nó da rede preferido
- Solicitar sessões SSCP
- Nome da PU (ao solicitar sessões SSCP é 1)

Nota: Estes parâmetros estão no arquivo ACG e podem não estar disponíveis nos painéis (através da **Configuração do Nó**).

Parâmetros de Definição e Ativação da Ligação

Esta seção descreve os parâmetros de definição e ativação.

Ativar na Inicialização

Uma ligação do tipo **ativar na inicialização** geralmente é utilizada para ligações de acesso principal à rede, que são ativadas inicialmente quando você inicia o Communications Server. A ligação é ativada quando o Communications Server é iniciado na máquina e permanece ativa enquanto o Communications Server está sendo executado.

Para definir uma ligação para que ela seja ativada na inicialização, especifique **ACTIVATE_AT_STARTUP = 1** na palavra-chave **LINK_STATION** do Arquivo ACG. As ligações geralmente são configuradas para serem ativadas na inicialização quando são importantes para a conectividade da rede. Uma ligação importante também pode ser configurada para repetição automática da ligação (consulte “Repetição Automática de Ligação” na página 37).

A ligação de um nó final (EN) do APPN ao seu servidor do nó da rede (NN) preferido é um exemplo deste tipo de ligação.

Exemplos de ligações do tipo não ativar na inicialização, codificadas como **ACTIVATE_AT_STARTUP = 0**, poderiam ser uma ligação ao sistema central que não é necessária imediatamente quando o Communications Server é iniciado, uma ligação de recepção cujas características de ligação um nó desejaria controlar ou uma ligação que pode ser muito cara para ficar ativa o tempo todo. Essas ligações são definidas como ligações do tipo não ativar na inicialização e são ativadas quando os recursos de ligação são solicitados por uma aplicação (consulte “Ativar por Pedido”) ou pelo parceiro.

Ativar por Pedido

Uma ligação do tipo **ativar por pedido** (também chamada de “ativação automática”) geralmente é utilizada para acesso a uma LU parceira que requer ativação dinâmica da ligação. Quando o Communications Server é iniciado, a ligação permanece inativa. Entretanto, ela será colocada na topologia como uma ligação disponível se um nome de CP adjacente for especificado. A ligação é ativada quando um programa de transação (TP) solicita uma conexão a uma LU remota que requer que a ligação esteja ativa. O Communications Server utiliza o nome completo da LU parceira definido para ativar a ligação.

Para definir uma ligação como uma ligação do tipo ativar por pedido, **ACTIVATE_AT_STARTUP = 0** e **FQ_ADJACENT_CP_NAME=(netid.cpname)** devem ser configurados na palavra-chave **LINK_STATION**, no arquivo ACG do nó de origem. Se a parceira não for o **FQ_ADJACENT_CP_NAME**, configure a palavra-chave **PARTNER_LU**.

Freqüentemente, uma ligação do tipo ativar por pedido também é configurada como um recurso limitado (consulte “Recurso Limitado” na página 39) ou com um tempo de espera de inatividade (consulte “Tempo de Espera de Inatividade” na página 39) para que seja desativada quando não for mais necessária.

Um exemplo de ligação do tipo ativar por pedido é a que define uma conexão para uma parceira que precisa estar ativa por um tempo limitado. Para permanecer ativa o tempo todo, a ligação pode custar mais do que o desejado. Por exemplo, você pode ter uma coleção de um ou mais computadores se comunicando em uma base regular. No final de cada dia, é necessário que uma das máquinas ative uma ligação a alguma máquina remota, para enviar os resultados diários ou fazer uma cópia de segurança dos dados.

Outro exemplo pode ser quando você tem conexões a um servidor de dados ou um servidor de impressão. A conexão exige recursos do servidor. Para evitar limitações no número máximo de estações de ligação e sessões no servidor, configure uma ligação do tipo ativar por pedido para liberar os recursos no servidor de dados após a conclusão dos pedidos através da ligação do tipo ativar por pedido.

Uma ligação do tipo ativar por pedido não é necessariamente uma ligação de recurso limitado, mas pode ser definida dessa forma através da inclusão do parâmetro **LIMITED_RESOURCE = 1** na palavra-chave **LINK_STATION** (consulte “Recurso Limitado” na página 39).

Repetição Automática de Ligação

A repetição automática de ligação é uma função de recuperação de erros que melhora a disponibilidade de uma ligação que falhou. Se uma ligação precisar ser reativada (sem a intervenção do usuário) após uma falha, a repetição automática de ligação poderá ser utilizada. A repetição automática de ligação fará com que sejam feitas tentativas de reativação automática da ligação se os seguintes parâmetros forem especificados na palavra-chave **LINK_STATION** ou **PORT**:

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

Se um destes parâmetros for especificado na palavra-chave **PORT**, os valores serão utilizados pela palavra-chave **LINK_STATION** se o parâmetro **INHERIT_PORT_RETRY_PARMs** tiver sido especificado.

Após uma ativação bem-sucedida, o temporizador de intervalo é redefinido para 0.

É bom utilizar a repetição automática dos seguintes tipos de ligações:

- Uma ligação a um NN que é ativada na inicialização. Se a ligação falhar, apenas uma ligação ao servidor do nó da rede (NN) será reativada.
- Ligação ao sistema central
- A ligação principal que possui uma cópia de segurança (também definida normalmente como uma ligação do tipo ativar na inicialização)
- Qualquer ligação que precisa permanecer ativa o tempo todo.

Máximo de Tentativas de Ativação

Máximo de tentativas de ativação é um parâmetro de ativação da ligação que fornece um mecanismo para impedir que o tráfego do sistema central da LU dependente (por exemplo, LUA, 3270, um gateway de LU 2 e/ou DLUR tente ativar uma ligação ao sistema central para uma aplicação downstream). O parâmetro do número máximo de tentativas de ativação, **INHERIT_PORT_RETRY_PARMS**, representa o número de vezes que um pedido de ativação da ligação é tentado. Após este número de tentativas, os pedidos seguintes serão rejeitados, até que o número de tentativas seja redefinido. Os pedidos de ativação de ligação à LU dependente emitidos após o máximo de tentativas de ativação serão imediatamente rejeitados sem uma tentativa real de ativação da ligação. Neste caso, é retornado um código de retorno principal X'0003' e um código secundário X'00000005', repetição de DLC, com um código de detecção X'00000000'. Os pedidos de ativação da ligação à LU independente emitidos após o máximo de tentativas de ativação são tentados, mas juntamente com o código de retorno principal X'0003' e o código de retorno secundário X'00000005' um código de detecção 081C0001 é retornado para indicar que o limite máximo de tentativas de ativação foi atingido.

Nota: Se um TP, como uma aplicação LUA, estiver em um loop tentando ativar uma sessão para o mesmo sistema central da aplicação da LU dependente, o TP fará com que o número máximo de tentativas de ativação seja excedido antes que a aplicação dependente possa fazer seu primeiro pedido.

O número máximo de tentativas de ativação é redefinido da seguinte forma:

- Quando um TP independente ativa a ligação. É responsabilidade dos TPs verificar o código de detecção e implementar um protocolo razoável para ativação da ligação, que não repita infinitamente a ativação.
- Quando o usuário ativa a ligação utilizando **Operações do Nó SNA**.
- Quando a ligação é ativada a partir de outra direção (por exemplo, pelo parceiro).

Se as **Operações do Nó SNA** estiverem tentando uma ativação da ligação, o número máximo de tentativas de ativação será diminuído em 1 e o resultado será ignorado. Se o limite for excedido em uma ligação ao sistema central de gateway, a ativação da ligação será tentada após 30 minutos se uma ligação à estação de trabalho se tornar ativa. Isto permite que as repetições cessem, embora elas sejam reiniciadas mais tarde quando as estações de trabalho forem reinicializadas. Quando o gateway, LUA ou as **Operações do Nó SNA** ativam uma ligação com êxito, o número máximo de tentativas de ativação é definido para 0.

Para configurar o máximo de tentativas de ativação em uma ligação, o parâmetro **MAX_ACTIVATION_ATTEMPTS= n** é configurado na palavra-chave **LINK_STATION**, onde n é o número de tentativas de -1 a 127. Um -1 indica que o valor na palavra-chave **PORT** deve ser utilizado e 0 indica repetições infinitas.

Reativação Solicitada pelo Usuário

Reativação solicitada pelo usuário é quando o usuário solicita a reativação de uma ligação a partir de **Operações do Nó SNA** ou da linha de comandos utilizando, por exemplo, o Communications Server.

Parâmetros de Desativação da Ligação

As seções seguintes descrevem os parâmetros de desativação.

Tempo de Espera de Inatividade

Tempo de espera de inatividade é um parâmetro de desativação da ligação SDLC que controla quando as ligações são desativadas. O valor do tempo de espera de inatividade especifica o tempo (em segundos) que uma ligação pode ficar inativa antes de ser desativada. É semelhante ao **LINK_DEACT_TIMER** na palavra-chave **LINK_STATION**. A diferença é que o **LINK_DEACT_TIMER** aguarda até que todas as sessões sejam encerradas (a contagem de sessões atinge 0) antes de disparar a desativação da ligação. O **INACTIVITY_TIMER** ignora a contagem de sessões e dispara a desativação após a ligação ficar inativa durante o período de tempo especificado.

A função de tempo de espera de inatividade foi implementada para tratar a situação em que uma sessão de emulador, LUA, 3270 ou uma conexão LEN é acidentalmente deixada inativa por longos períodos de tempo. Quando o nó não detecta nenhuma atividade através desse tipo de conexão durante o tempo de duração do **INACTIVITY_TIMER**, a ligação é desativada automaticamente, independente de existirem sessões e conversações na ligação. Por definição, o **LINK_DEACT_TIMER** é considerado não-interruptor, mas o **INACTIVITY_TIMER** é considerado interruptor.

Notas:

1. O tempo de espera de inatividade pode ser utilizado em ligações de recursos limitados ou não-limitados. Se uma ligação for definida como recurso limitado e as conversações permanecerem ativas, o tempo de espera do recurso limitado não expirará e a ligação será desativada quando expirar o tempo de espera de inatividade. Se uma ligação for definida como recurso não-limitado, o tempo de espera de inatividade será utilizado para desativar a ligação para liberar recursos na extremidade remota.
2. Atualmente, com o HPR, o tempo de espera de inatividade é ignorado. Isto ocorre porque o HPR não pode distinguir o tipo de tráfego que está na ligação e o protocolo de manutenção da atividade do HPR gera tráfego suficiente para que a ligação nunca fique inativa.

Para configurar o tempo de espera de inatividade em uma conexão SDLC, o parâmetro **INACTIVITY_TIMER= n** é codificado no parâmetro **LINK_STATION_SDLC_SPECIFIC_DATA** da palavra-chave **LINK_STATION**, no arquivo ACG, onde n é 40-160. Para configurar o tempo de espera de inatividade em uma ligação, o parâmetro **LINK_DEACT_TIMER= n** é codificado na palavra-chave **LINK_STATION**, no arquivo ACG, onde n é 0—1000. O 0 indica nenhum tempo de espera (a ligação permanecerá ativa). O padrão do SDLC é 80 e o padrão para a ligação é 10.

Recurso Limitado

Uma ligação de recurso limitado geralmente é utilizada para ligações de acesso principal à rede, de uso limitado, e para ligações de acesso secundário à rede. Uma ligação de recurso limitado é uma ligação que é desativada automaticamente quando sua contagem de sessões atinge 0. A ligação de recurso limitado pode ser definida como **ACTIVATE_AT_STARTUP=1** ou **ACTIVATE_AT_STARTUP=0**. Se a ligação for **ACTIVATE_AT_STARTUP=1**, ela será iniciada quando o

Communications Server e SNA

Communications Server for iniciado. Se a ligação for **ACTIVATE_AT_STARTUP=0**, ela será colocada na topologia quando o Communications Server for iniciado, se o CPName adjacente for especificado, e será ativada quando os serviços forem solicitados.

Nota: As ligações do tipo ativar na inicialização não são colocadas na topologia, a menos que estejam ativas.

Para configurar uma ligação de recurso limitado, **LIMITED_RESOURCE = 1** é especificado na palavra-chave **LINK_STATION** do arquivo ACG. O **LINK_DEACT_TIMER= n** é especificado na palavra-chave **LINK_STATION** e o parâmetro **ADJACENT_NODE_TYPE=LEARN** deve ser especificado.

Nota: Se **CP_CP_SESSION_SUPPORT=1**, a ligação não será uma ligação de recurso limitado. A verificação da configuração sinalizará isso como um aviso. As seções CP a CP ativas evitarão que a ligação seja desativada.

Redes de Conexão

As redes de conexão permitem que os nós APPN em uma Rede Local tenham ligações diretas entre si, sem a necessidade de definições de ligações lógicas em cada nó. Este dispositivo reduz bastante a definição do sistema sem adicionar a carga de desempenho do roteamento de todas as sessões através de um nó da rede. Também permite que os novos nós, que são incluídos na Rede Local, participem completamente das conversações de APPC sem a necessidade de alterações na definição em nós intercalados.

Um nó da rede de conexão assume que todos os nós em uma rede de conexão podem ter ligações diretamente entre um e outro. Ao calcular a rota para uma sessão, o nó da rede considera a ligação direta e normalmente seleciona a mesma como a rota ideal. Após calcular a rota direta, o nó da rede simplesmente envia ao nó final o endereço do parceiro a ser utilizado para ativação da ligação.

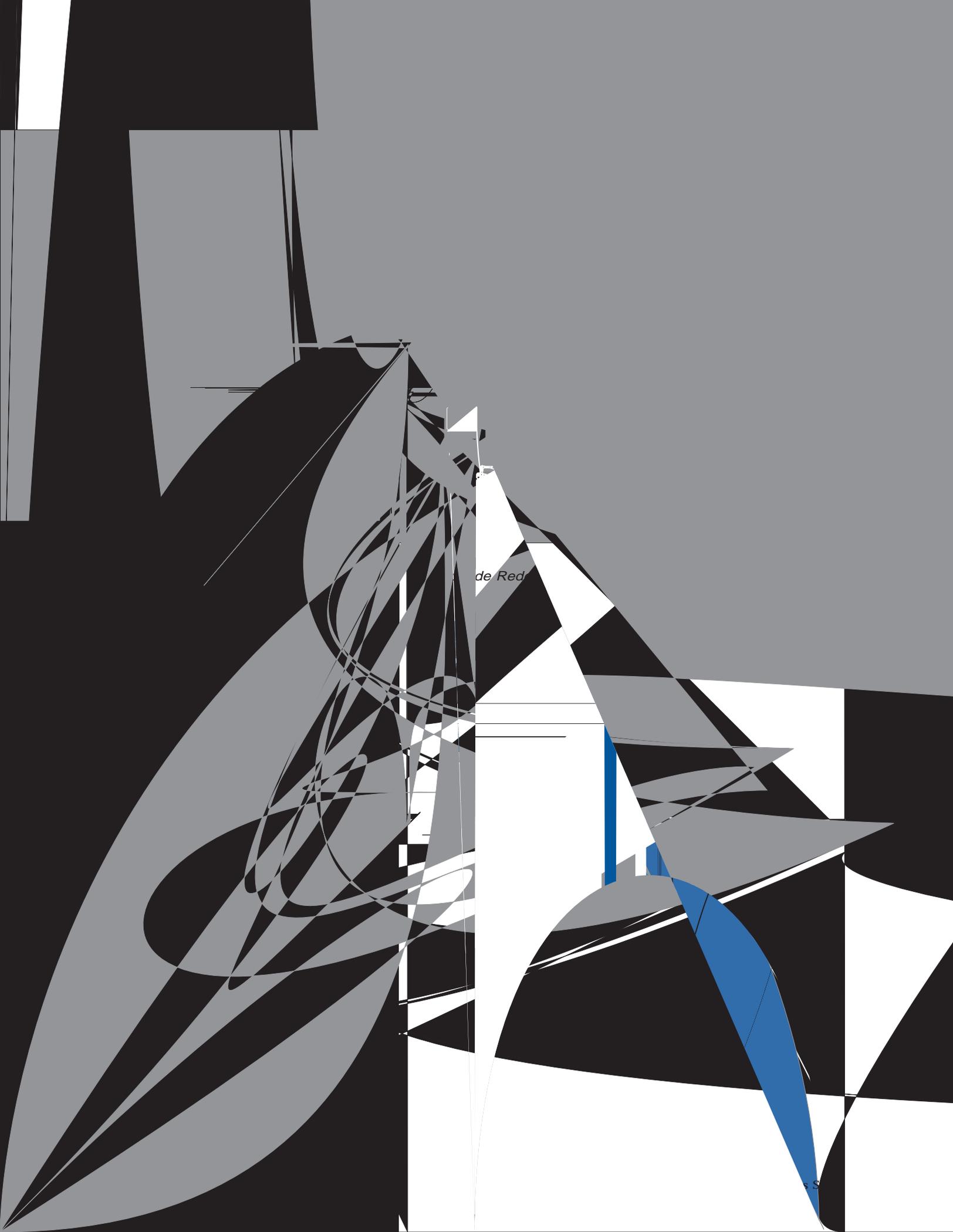
É possível que a rota da rede de conexão não seja seguida quando a segurança da rede de conexão for menor do que a necessária. Se o DLC da rede de conexão não for seguro e um modo como o **#BATCHSC** for utilizado no parâmetro **MODE_NAME**, o nó da rede tentará encontrar uma rota segura, ignorando a rede de conexão.

Se estiverem sendo utilizadas pontes de Rede Local, o APPN visualizará toda a Rede Local com pontes como uma única rede lógica. Como as ligações podem ser ativadas entre quaisquer dois sistemas na Rede Local, apenas uma rede de conexão será necessária. A rede de conexão deve ser definida em todos os sistemas APPN na Rede Local.

Um nó da rede absorve informações sobre a rede de conexão durante o registro do EN e as pesquisas de diretório do APPN. O servidor do nó da rede então possui informações suficientes para calcular uma conexão direta entre os nós terminais da sessão sem que a rota passe por nós intermediários.

Apenas os nós finais e os nós da rede podem se beneficiar da rede de conexão. As ligações aos nós LEN ainda devem ser definidas explicitamente.

A Figura 12 na página 41 ilustra um exemplo de rede de conexão. Esta visualização de uma Rede Local mostra uma rede de conexão com o nome LOCALNET.IBMLAN. Com esse tipo de definição, qualquer EN pode se conectar



de Red

s S

Solicitar Sessões SSCP

A opção solicitar sessões SSCP especifica se as sessões SSCP-PU são solicitadas ao sistema central através da ligação que está sendo definida.

Serviços de Diretório

Um nó da rede fornece serviços de diretório às LUs localizadas no nó da rede e às LUs localizadas nos nós finais que o nó da rede serve. O nó da rede também auxilia nos serviços de diretório fornecido por outros nó da redes na rede, respondendo positivamente para pedidos de procura de diretório recebido quando o recurso nomeado é encontrado no diretório local. O diretório local mapeia um nome de LU para o nome do ponto de controle do nó onde essa LU está localizada. Se o ponto de controle de destino for um nó LEN ou final, o diretório incluirá o nome do nó da rede que está servindo.

O componente dos serviços de diretório reside em todos os nós. Entretanto o seu escopo e as suas funções variam dependendo do nível de suporte ao diretório no nó.

Um nó final mantém um diretório local que contém entradas para LUs residentes localmente. Além disso, o nó final mantém entradas de diretório para LUs em nós adjacentes com as quais o nó final esteve em sessão. Para uma sessão LU-LU com um nó adjacente do mesmo nível, uma pesquisa do diretório local retorna o ponto de controle de destino apropriado, associado à LU procurada, permitindo que a ligação lógica adequada seja selecionada.

Em um nó LEN, todas as LUs parceiras são digitadas no diretório, como mostra o exemplo da Figura 13 na página 43. As que não estiverem em um nó final adjacente do mesmo nível mas estiverem fora, na rede APPN, serão associadas ao servidor do nó da rede designado, em seu diretório. O nó LEN envia o pedido de ativação de sessão LU-LU (BIND) ao seu servidor do nó da rede para qualquer LU associada ao servidor em seu diretório. O servidor automaticamente localiza a LU de destino para o mesmo e encaminha o BIND apropriadamente. O nó da rede pode enviar uma pesquisa Localizar, aguardar uma resposta e, em seguida, enviar o BIND.

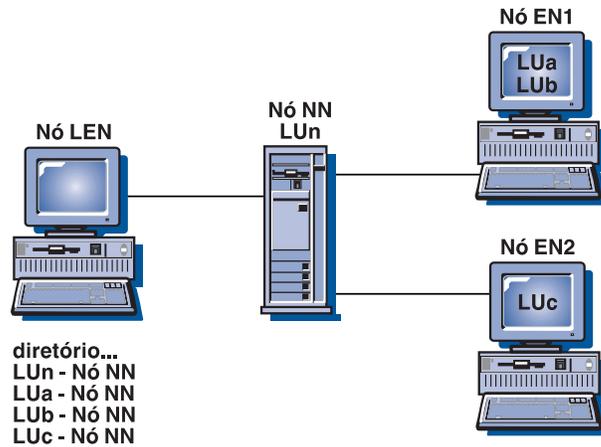
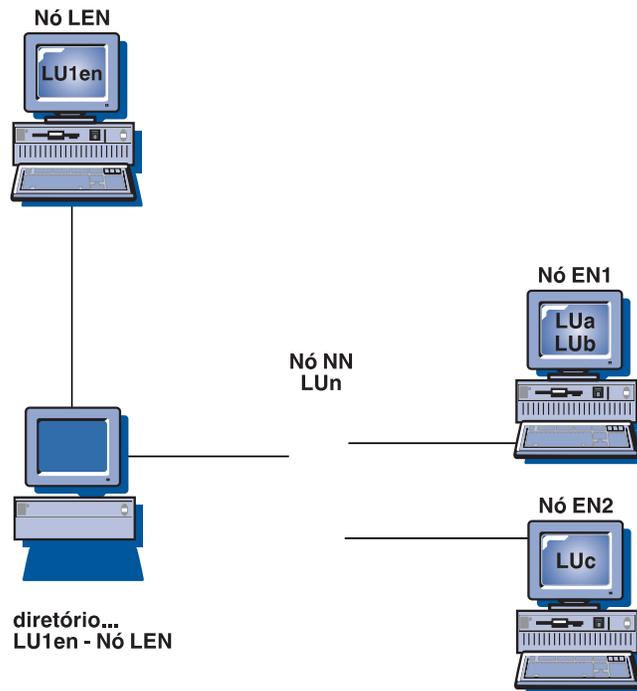


Figura 13. *Diretório do Nó LEN.* O diretório do nó LEN deve conter todas as LUs com as quais ele se comunica. Como o nó da rede (NN) adjacente serve o nó LEN mesmo sem sessões CP-CP, o nó LEN deve definir o ponto de controle do nó da rede como o “ponto de controle proprietário” de todas as LUs, incluindo as LUs localizadas nos nós finais (ENs).

Quando uma LU não é representada em um diretório do nó final, o nó final inicia uma pesquisa Localizar para encontrar a LU desejada. Para ativar a pesquisa, o nó final chama os serviços do seu servidor do nó da rede. A Figura 14 mostra um exemplo de um diretório do nó final.



Um nó da rede fornece serviços de diretório distribuídos aos seus nós finais servidos, em cooperação com todos os outros nós da rede na rede APPN. O nó da rede de origem recebe o nome de uma LU de destino em um pedido de pesquisa Localizar a partir de um nó final servido ou o nome de uma LU secundária em um BIND a partir de um nó LEN. O nó da rede verificará a localização atual da LU se

Communications Server e SNA

for representada no diretório do nó da rede (mas não no próprio nó da rede). A verificação é feita através do envio de uma pesquisa direcionada ao servidor do nó da rede de destino.

Se a LU não estiver no diretório do nó da rede de origem, o nó da rede iniciará uma pesquisa na rede. A pesquisa é iniciada pelo envio de uma pesquisa de difusão a todos os nó da rede adjacentes, cada um dos quais, por sua vez, propaga a difusão e retorna respostas indicando êxito ou falha. Para suas necessidades futuras, um nó da rede armazena em cache as informações obtidas nas pesquisas de difusão bem-sucedidas.

Um nó final APPN também pode receber (e responder) pedidos de pesquisa Localizar do seu servidor do nó da rede para pesquisar ou assegurar a presença contínua de LUs específicas no nó final.

Cada nó final pode registrar suas LUs em seu servidor do nó da rede através do envio de uma mensagem de registro ao nó da rede. Se o nó final for registrado no servidor do nó da rede, o nó da rede manterá as informações sobre o diretório atual, referentes aos nós finais do seu domínio.

A Figura 15 mostra um exemplo de um diretório do nó da rede.

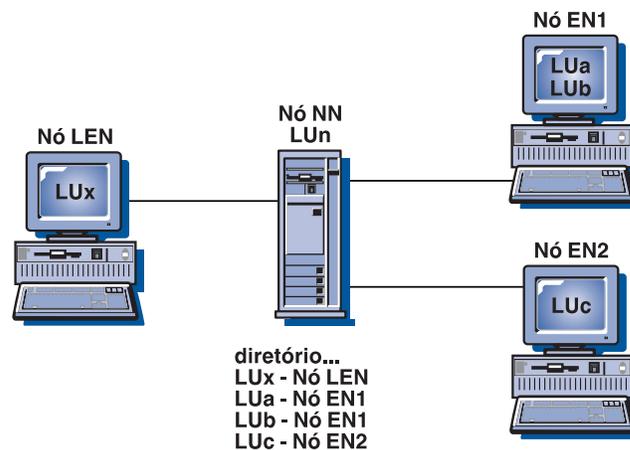


Figura 15. Diretório do Nó da Rede. O diretório do nó da rede (NN) contém todas as LUs que ele serve. Os nós finais (ENs) registram suas LUs. A LU do nó LEN deve ser configurada.

Serviços de Topologia e Seleção de Rota

Um nó da rede fornece serviços de seleção de rota para si mesmo e para os nós finais que ele serve. Ele mantém um banco de dados interno de topologia da rede que possui informações completas e atuais sobre a rede. Estas informações sobre topologia consistem em características de todos os nós de rede na rede e de todas as ligações entre nó da redes. Todos os nós da rede contêm uma cópia do banco de dados de topologia.

Um nó da rede utiliza o banco de dados de topologia da rede para computar rotas para sessões originadas em LUs nele mesmo e nos nós finais que ele serve. Cada rota que um nó da rede computa é a rota de menor peso, desde o nó que contém a LU de origem até o nó que contém a LU de destino. Para fornecer um caminho apropriado através da rede, o algoritmo utilizado para selecionar a rota primeiro designa pesos às ligações e nós. Com base no significado relativo das

características para a classe de serviço solicitada, o algoritmo de peso computa um valor escalar para cada nó e ligação lógica.

Banco de Dados de Topologia

O banco de dados de topologia da rede em um nó da rede contém informações sobre todos os nós da rede e todos os grupos de transmissão que os interconectam. É um banco de dados totalmente replicado, compartilhado por todos os nós da rede e utilizado para seleção de rota. A manutenção do banco de dados requer atualizações na difusão entre todos os nós da rede. As atualizações são realizadas através de mensagens de atualização do banco de dados de topologia (TDU), que contém informações que identificam o nó, características do nó e da ligação e números de seqüência das atualizações para identificar as alterações mais recentes para cada um dos recursos descritos em uma TDU.

Um banco de dados de topologia local em um nó final só contém informações sobre si mesmo e sobre os nós conectados diretamente.

O componente dos serviços de topologia e roteamento utiliza sessões CP a CP entre nós da rede para troca de informações, para criar e manter um banco de dados de topologia. Este banco de dados de topologia, nos nós da rede, é mantido em dia através das atualizações transmitidas entre todos os nós da rede sempre que um recurso (nó ou ligação) é ativado ou desativado ou sempre que as características de um recurso existente são alteradas.

Um banco de dados de configuração local e um banco de dados de topologia da rede são mantidos em cada nó da rede, conforme ilustrado na Figura 16 na página 46 . O banco de dados de configuração local é exclusivo do nó, enquanto o banco de dados de topologia da rede é replicado em todos os nós da rede.

A Tabela 2 mostra as informações contidas no banco de dados de configuração, no nó da rede local.

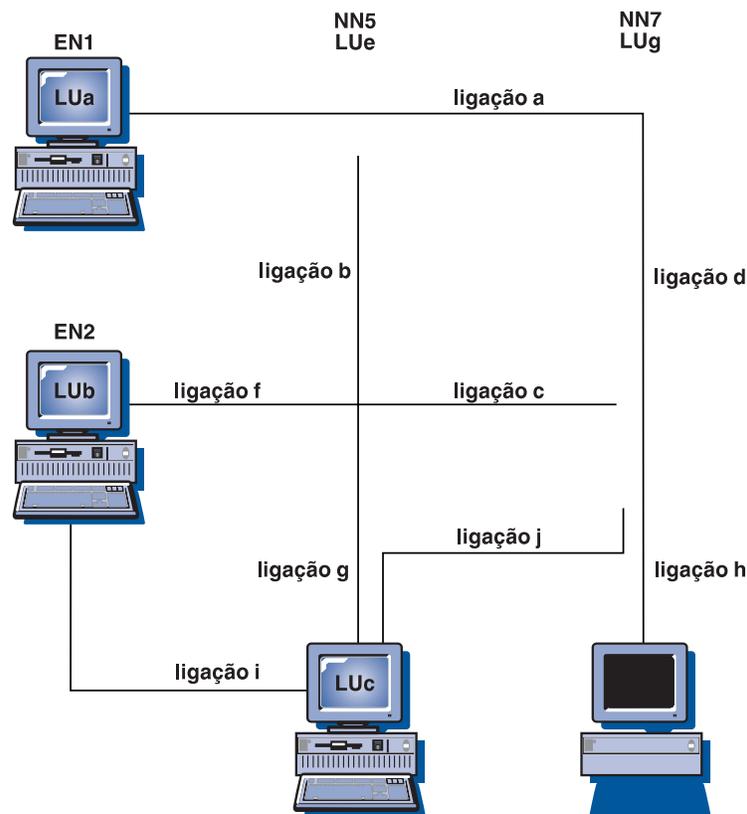
Tabela 2. Banco de Dados de Configuração do NN Local

Nó	Ligações	Conexão
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

A Tabela 3 mostra as informações contidas no banco de dados de topologia da rede, no nó da rede local.

Tabela 3. Banco de Dados de Topologia da Rede do NN Local

Nó	Ligações	Conexão
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



Modos

O modo determina os valores para as características da sessão e o número de sessões entre os parceiros da sessão. Por exemplo, o tamanho da maior unidade de pedido (RU) a ser trocada em uma sessão (isto é, o *tamanho máximo da RU*) é uma das características de um modo. O modo também especifica uma classe de serviço, que é utilizada para selecionar a rota para a sessão.

Classe de Serviço

No início da sessão, o BIND especifica um nome de modo. Este nome de modo é associado a uma definição de classe de serviço (COS) utilizada para determinar a rota mais desejável entre os nós de origem e de destino da sessão. As definições da COS especificam as características que os nós e as ligações devem possuir, a serem incluídas na rota selecionada para a sessão. Essa especificação permite que o algoritmo de seleção da rota determine se um nó ou ligação é aceitável. A partir do conjunto aceitável, o algoritmo calcula a melhor rota para a sessão.

Como as definições de COSs podem variar, as sessões diferentes podem utilizar diferentes rotas entre a mesma origem e os nós de destino, dependendo do nome do modo especificado. Cada nó da rede consegue computar a rota de menor peso (a mais desejável) para qualquer destino.

Quando uma sessão passa por uma rede APPN e uma rede de subárea, ela utiliza duas classes de serviço:

- Na rede APPN, a sessão utiliza a classe de serviço (COS) definida para o modo utilizado pelo programa de transação. Essa definição está na configuração ativa da estação de trabalho. Essa COS é utilizada para encaminhar a sessão na rede APPN.

Se você utilizar o modo em branco padrão, a COS associada será #CONNECT.

- Na rede de subárea, o nome da COS pode ser escrito na tabela de modos de início de sessão, na entrada para o nome do modo utilizado pela sessão. Este nome de COS é utilizado pelo programa VTAM para encaminhar a sessão através da rede de subárea.

Se você utilizar o modo em branco padrão ou se não definir nenhuma COS em uma entrada da tabela de modos de início de sessão, a COS assumirá o padrão da entrada em branco na tabela ISTSDCOS.

Em ambos os casos, cada rede utiliza o nome do modo para encontrar o nome da COS, mas os dois nomes de COSs não são necessariamente os mesmos.

Prioridade de Transmissão do SNA

A prioridade de transmissão é um valor especificado na classe de serviço. A prioridade de transmissão é enviada no BIND, no vetor de controle de Classe de Serviço/Prioridade de Transporte (COS/TPF). Após o estabelecimento da sessão, o fluxo dos dados da sessão seguinte seguirá a prioridade de transmissão especificada no vetor de controle de COS/TPF.

O fluxo de dados em sessões que utilizam uma classe de serviço com alta prioridade pode transmitir dados em sessões com prioridade mais baixa. Você deve dar prioridade mais alta às sessões com tráfego interativo onde o tempo de resposta é importante. Por exemplo, sessões de emulador. As sessões com grandes volumes de dados, por exemplo, transferências de arquivos para o NetView Distribution Manager, devem ter prioridade mais baixa. O suporte à prioridade de transmissão ajuda a impedir que as sessões com grandes volumes bloqueiem o tráfego nas sessões interativas.

As quatro prioridades de transmissão são: rede, alta, média e baixa. A rede é a prioridade utilizada para dados de controle da rede, como serviços de topologia e diretório. As outras prioridades são utilizadas para dados do usuário.

Communications Server e SNA

O Communications Server suporta a prioridade de transmissão para ligações de Rede Local, SDLC e X.25. O benefício é mais aparente quando a rede contém ligações de baixa velocidade congestionadas.

Seleção de Rota

Após o servidor do nó da rede receber uma resposta da sua pesquisa de localização, o componente dos serviços de topologia e roteamento calcula a melhor rota desde o nó de origem até o nó de destino, para a COS solicitada. Como o componente dos serviços de topologia e roteamento envia e recebe atualizações do banco de dados de topologia como características de qualquer alteração de recurso, cada rota é calculada com as informações mais atuais.

Seleção de Rota para Usuários do VTAM

Para encaminhar o tráfego de APPC através de uma subárea, as estações de trabalho conectadas à subárea devem ser definidas como nós da rede no Communications Server. Em cada nó da rede é definida uma ligação que conecta o nó à subárea. Do ponto de vista do nó da rede, as LUs parceiras do outro lado da subárea são definidas como se estivessem localizadas no sistema central (um nó LEN). Do ponto de vista do sistema central, cada nó da rede conectado à subárea deve ser definido para o programa VTAM com uma macro de PU. Todas as unidades lógicas da LU 6.2 de destino na rede APPN para uma determinada conexão são definidas na PU (nó da rede) como se estivessem realmente localizadas na PU. Entretanto, as LUs na realidade podem estar localizadas em outros nós na rede APPN conectada ao nó da rede. O sistema central só vê a PU do nó da rede. A PU do nó da rede também pode ser uma PU de gateway. O tráfego de SETN (**CP_CP_SESS_SUPPORT=NO**) não é permitido quando o parâmetro é definido para YES no NCP e não existe nenhuma sessão da PU ou do ponto de controle.

Se o nome da PU na definição do VTAM for igual ao nome do ponto de controle definido no Communications Server, saiba que você não poderá definir o ponto de controle como uma LU nas definições do VTAM. Os nomes devem ser exclusivos no programa VTAM, sejam eles nomes de PUs ou de LUs.

A macro da PU deve conter **XID=YES** para utilizar uma troca de XID durante a ativação da PU. Este parâmetro é codificado no nó principal do NCP. Ele não deve estar na instrução da PU de um nó principal comutado.

Para dispositivos SNA comutados, você pode utilizar um novo parâmetro na macro da PU: **CPNAME=ccccccc**. Ele especifica o nome do ponto de controle do nó da rede conectado à subárea. É necessário especificar **CPNAME** ou **IDBLK** e **IDNUM** em uma instrução de definição da PU comutada. Ambos podem ser especificados. O nó da rede fornece seu nome de ponto de controle ao programa VTAM na troca de XIDs durante a seqüência da conexão. O programa VTAM utiliza o nome do ponto de controle para localizar a macro da PU correspondente. Se não houver nenhuma macro da PU com o nome do ponto de controle correspondente, o programa VTAM utilizará **IDNUM** e **IDBLK** para localizar a macro da PU.

Para encaminhar o tráfego de APPC de uma rede APPN através da subárea e para outra parte da rede APPN, o nome da rede (**NETID**) do VTAM proprietário deve

estar de acordo com o ID da rede APPN. No Communications Server, o ID da rede (do nó da rede conectado à subárea) pode ser encontrado com a utilização do perfil de características do nó local SNA.

Encaminhamento de Sessão Intermediária

O encaminhamento de sessão intermediária é uma função executada por um nó da rede. Este recurso permite que um nó da rede receba e encaminhe dados destinados a outro nó. A origem e o destino dos dados pode ser um nó final, um nó da rede ou um nó LEN. A parte da sessão entre dois nós adjacentes chama-se estágio da sessão.

Suporte ao High Performance Routing (HPR)

O Communications Server suporta high performance routing (HPR) sobre Enterprise Extender (IP), controle de ligação síncrona de dados (SDLC), LAN, WAN, canal, Multi-Path Channel (MPC) e conexões X.25.

O automatic network routing (ANR) do HPR minimiza os requisitos de memória e processamento nos nós intermediários, o que é uma solução melhor do que o roteamento de sessão intermediária (ISR) do APPN para redes de alta velocidade com baixas taxas de erro.

O HPR melhora o roteamento do SNA com estes recursos principais:

- Nós intermediários sem estado

Os nós intermediários sem estado não têm nenhum conhecimento das conexões que passam por eles.

Um nó intermediário de HPR não precisa de nenhum bloco de controle ou área de buffers para suportar as conexões que passam por ele. Também não precisa de tabelas de roteamento porque as informações sobre roteamento são transportadas em cada pacote. Utilizando ANR, um nó intermediário de HPR simplesmente recebe um pacote, examina seu cabeçalho para encontrar um identificador para a ligação lógica ao nó seguinte e envia o pacote para essa ligação.

- Um nó intermediário de HPR:

- Não recupera pacotes porque os pontos finais da conexão de HPR detectarão e recuperarão pacotes perdidos utilizando o protocolo de transporte rápido (RTP).

Se a Rede Local tiver altas taxas de erros, você também poderá selecionar o suporte ao protocolo de recuperação de erros (ERP) do nível de ligação. Entretanto, isso não deve ser necessário em ligações com baixas taxas de erros.

- Não monta novamente os pacotes segmentados para depois segmentá-los outra vez, porque os nós de extremidade da conexão HPR automaticamente selecionarão um tamanho de pacote suportado por todos os nós intermediários na rota.
- Não gerencia ativamente os buffers nem impede o congestionamento porque os nós de extremidade da conexão HPR empregam algoritmos de controle de fluxo que impedem o congestionamento nos nós intermediários.
- Não determina a rota de um pacote através de uma pesquisa de tabela porque os nós de extremidade da conexão HPR executam o roteamento de origem e criam as informações sobre roteamento do pacote utilizando etiquetas selecionadas pelos nós intermediários para desempenho ótimo.

Communications Server e SNA

Para atingir os nós intermediários sem estado:

- Os nós de extremidade da rota devem ter capacidades de buffer que reflitam a combinação de atraso na rota e produtividade da aplicação, um valor que depende na configuração da rede.
- As ligações de dados devem suportar campos I de tamanho suficiente para conter os cabeçalhos do HPR e ainda transportar eficientemente os dados da aplicação.
- As ligações de dados devem ser muito confiáveis porque uma alta taxa de erros afetará desfavoravelmente a produtividade do HPR.

Para configurações onde essas condições não podem ser conseguidas, o APPN sem HPR ainda é uma opção de implementação válida. A tecnologia do HPR é uma opção do APPN e o APPN sem HPR ainda está disponível e é suportado.

- **Impedimento do congestionamento**

Uma rede HPR pode atingir taxas de utilização de ligações muito altas.

Utilizando uma técnica chamada controle de fluxo baseado em taxa automática (ARB), os nós de extremidade da conexão HPR detectam automaticamente o congestionamento da rede e reduzem a carga da transmissão. Isso evita os pacotes perdidos que, em outros algoritmos de roteamento, podem ser causados pela falta de buffers disponíveis nos nós intermediários.

- **Novo roteamento sem interrupção**

Quando um nó de extremidade da conexão HPR detecta que uma rota falhou, ele automaticamente computa uma nova rota, restabelece a conexão e recupera os pacotes perdidos devido à falha. Como os nós intermediários do HPR são sem estado (isto é, não têm conhecimento das conexões que passam por eles), eles não participam deste protocolo de recuperação. Como nenhum pacote será perdido se a rota for alternada com êxito, as aplicações que utilizam a rota não são interrompidas pela falha.

- **Software compatível com o hardware existente**

O HPR é uma extensão de software do APPN. Você pode utilizar o HPR nas placas de Rede Local ou Rede Ampla existentes e nas ligações de retransmissão de estrutura. Como o HPR não tenta fornecer largura de banda dedicada e transporte em tempo real garantido (deixando este nível de função para os Serviços de Rede de Banda Larga), as restrições ao desempenho nos atrasos de envio de pacotes são os mesmos para o APPN sem HPR. Os protocolos de ponto de controle utilizados pelo HPR são aqueles do APPN de base com inclusões mínimas, portanto os nós HPR podem ser instalados de forma incremental em uma rede APPN existente, sem planejamento prévio ou coordenação.

Rapid Transport Protocol (RTP)

O RTP é um conjunto de formatos de mensagens e protocolos projetado para utilizar um meio de comunicação de dados moderno, minimizar a sobrecarga nos nós intermediários e comutar automaticamente os caminhos quando uma ligação no caminho falha.

As conexões RTP são estabelecidas em uma **sub-rede HPR** e são utilizadas para transportar o tráfego da sessão. Uma sub-rede HPR é a parte de uma rede APPN capaz de estabelecer conexões RTP e transportar o tráfego da sessão HPR. As conexões RTP podem ser consideradas **canais de transporte** através dos quais as sessões são transportadas. Essas conexões podem transportar dados a velocidades muito altas, utilizando roteamento intermediário de nível inferior e podem

minimizar o tráfego através das ligações para recuperação de erros e controle do fluxo. Esses fluxos são gerenciados pelos pontos extremos de conexão RTP.

O caminho físico de uma conexão RTP pode ser alternado automaticamente para encaminhar novamente os dados, contornando um nó ou ligação com falha, sem interromper as sessões. Na ocasião da falha, os dados na rede são recuperados automaticamente.

O RTP executa a recuperação de erros de extremidade a extremidade, em vez de fazê-lo no nível da ligação. O desempenho é melhorado através da redução do número de fluxos necessários para a recuperação de erros. Os protocolos de recuperação de erros (ERPs) do nível da ligação também são suportados para todas as conexões. O ERP é um método que detecta um pacote perdido em uma extremidade de uma ligação e recupera o mesmo fazendo um pedido de retransmissão do pacote à outra extremidade. Se o ERP for utilizado, os pacotes HPR serão enviados como estruturas de informação numeradas (I-FRAMES). Quando uma estrutura é perdida, o DLC detecta a perda e o remetente retransmite a estrutura. Se o ERP não for utilizado, os pacotes HPR serão enviados como estruturas de informação não-numeradas (UI-FRAMES). Quando uma estrutura é perdida, o DLC não pode detectar a perda e o protocolo de transporte rápido (RTP) do HPR deve detectar e recuperar os pacotes perdidos nos nós de extremidade da conexão.

Em qualquer um dos casos, o RTP sempre detecta e recupera os pacotes perdidos nos nós de extremidade da conexão. Para qualquer conexão determinada, não existe nenhuma restrição no número de ligações que utilizam ERP ou não utilizam ERP.

O ERP pode ser ativado ou desativado ligação por ligação. Como o RTP detecta e recupera os pacotes perdidos nos nós de extremidade da conexão, você pode utilizar ligações ERP ou não-ERP ao construir a rede. Isto permite que você especifique o ERP no nível de ligação em ligações com uma alta taxa de perda de pacotes e maximize o rendimento em outras ligações, especificando que elas não utilizem ERP no nível de ligação. Em geral, a utilização do ERP não é recomendada em Redes Locais.

Nota: O ERP está sempre ativado em um ambiente de rede ampla (WAN).

Os controles de fluxo e de congestionamento também são feitos pelo RTP de extremidade a extremidade. O RTP utiliza uma técnica chamada controle de fluxo baseado em taxa automática (ARB) para utilizar completamente a largura de banda da rede, quando possível. Quando a rede suporta essa taxa de envio aumentada, o RTP aumenta a taxa na qual os pacotes são enviados. O congestionamento é reconhecido automaticamente e a taxa de envio será diminuída de acordo, quando ocorrer congestionamento. As capacidades efetivas configuradas das ligações no caminho de conexão são utilizadas para determinar a taxa de envio inicial e o incremento na taxa de envio.

O suporte aos fluxos de controle (CF) através das conexões RTP agora está disponível com o HPR no Communications Server. Anteriormente, os fluxos de controle, incluindo sessões CP a CP e mensagens de configuração de rota, utilizavam conexões APPN enquanto os fluxos de dados utilizavam conexões HPR. Agora, ambos tanto os fluxos de controle quanto os fluxos de dados podem utilizar conexões RTP. Os benefícios deste suporte incluem a comutação automática de caminhos para sessões CP a CP.

Communications Server e SNA

Os fluxos de controle passam automaticamente pelo RTP nos dois nós de extremidade da conexão que suporta essa função.

Automatic Network Routing (ANR)

O automatic network routing (ANR) é uma técnica de roteamento sem estado ativada por RTP, onde uma mensagem chega com uma etiqueta que identifica exclusivamente o próximo salto no caminho. Devido à sua simplicidade, o ANR pode ser executado em um nível baixo, sem nenhum conhecimento das conexões que utilizam o caminho. O ANR minimiza os ciclos e os requisitos de memória para roteamento de pacotes através dos nós intermediários.

A função de comutação rápida de pacotes do ANR melhora o desempenho nos nós intermediários através do roteamento em um nível inferior ao do APPN e da recuperação de erros, segmentação, controle de fluxo e controle de congestionamento no nó final, em vez do nó intermediário.

Os nós ANR intermediários não estão cientes das sessões do SNA ou das conexões RTP. As informações sobre roteamento para cada pacote são transportadas em um cabeçalho da rede com o pacote. Cada nó retira as informações que utilizou no cabeçalho antes de encaminhar o pacote, assim o nó seguinte pode encontrar suas informações sobre roteamento em um local fixo do cabeçalho. Não há necessidade de manter tabelas de roteamento para conectores de sessão como no APPN de base, portanto a comutação de pacotes através dos nós pode ser feita mais rapidamente.

Suporte à LU

O SNA define os tipos de LUs 0, 1, 2, 3, 4, 6.0, 6.1, 6.2 e 7. Os tipos de LUs 0, 1, 2, 3, 4 e 7 suportam comunicações entre programas aplicativos e diferentes tipos de estações de trabalho. As LUs tipos 6.0 e 6.1 fornecem comunicações entre programas localizados em nós de subárea tipo 5. A LU tipo 6.2 suporta comunicações entre dois programas localizados em nós de subárea tipo 5 ou nós periféricos tipo 2.1, ou ambos, e entre programas e dispositivos.

O Communications Server suporta LUs tipos 0, 1, 2 e 3, que suportam comunicações com aplicações do sistema central que suportam dispositivos como:

LU tipo 0 Terminais financeiros 3650 e 4700

LU tipo 1 Impressoras 3270

LU tipo 2 Telas interativas 3270

LU tipo 3 Impressoras 3270

A comunicação ocorre apenas entre as LUs do mesmo tipo. Por exemplo, uma LU 2 se comunica com outra LU 2. Ela não se comunica com uma LU 3. O Communications Server também suporta a LU tipo 6.2 ou APPC.

As funções SNA do Communications Server permitem que as aplicações utilizem a interface de programação de aplicações (API) de APPC para fornecer uma capacidade de processamento de transação distribuída na qual dois ou mais programas cooperam para executar uma função de processamento. Essa capacidade envolve a comunicação entre os dois programas, assim eles podem compartilhar recursos locais como ciclos do processador, bancos de dados, filas de trabalho e interfaces físicas como teclados e monitores.

O Communications Server suporta APPC através das APIs de APPC. Consulte as seguintes publicações para obter mais informações:

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

As seguintes funções do Communications Server suportam uma faixa de tipos de LUs:

- SNA Gateway

O SNA Gateway permite que sistemas centrais IBM System/370 (S/370) ou computadores centrais de arquitetura System/390 (S/390), ou ambos, suportem estações de trabalho conectadas à Rede Local que utilizam LUs tipos 0, 1, 2, 3 ou 6.2 para comunicação através de uma estação de trabalho de SNA Gateway.

O SNA Gateway também suporta LUs tipos 1, 2 ou 3 para computadores centrais AS/400, que podem processar os dados ou transmiti-los a computadores centrais de arquitetura S/370 ou S/390.

- Aplicação da LU Convencional (LUA)

A LUA consiste no software do sistema que fornece rotinas de serviço para suportar LUs 0, 1, 2 e 3.

Suporte à SDDL U

O suporte à LU dependente de autodefinição (SDDL U) permite definir dinamicamente e ativar uma LU dependente no sistema central (VTAM). No VTAM, isto é conhecido como definição dinâmica de LUs dependentes (DDDL U). A SDDL U é ativada no Communications Server através da codificação de uma instrução LU_MODEL em uma definição da LU.

Para ativar a função DDDL U no VTAM, codifique o operando LUGROUP na instrução de definição da PU e codifique um nó principal do grupo de LUs. Para utilizar a rotina de saída da SDDL U fornecida pela IBM, que gera os nomes de LUs para você, é preciso codificar também o operando LUSEED na instrução da PU.

O operando LUGROUP especifica o nome do grupo modelo de definições de LUs que o VTAM utilizará quando definir dinamicamente as LUs para essa PU. O nó principal do grupo de LUs contém as instruções de definição do modelo. As definições dinâmicas para as LUs são construídas com a utilização das definições de LUs do modelo, contidas nesse nó principal.

O operando LUSEED fornece um nome de padrão que é utilizado com a rotina de saída da SDDL U para criar um nome para a LU criada dinamicamente. Após a inclusão das instruções corretas na instrução da PU e a codificação do nó principal do grupo de LUs, estes nós principais precisam ser ativados para que a função SDDL U seja ativada.

Suporte ao Dependent Logical Unit Requester

O Dependent Logical Unit Requester (DLUR) é uma arquitetura destinada a fornecer suporte à LU dependente em um rede APPN. O Communications Server suporta todas as funções de base do DLUR e as seguintes funções opcionais:

- Suporte à LU dependente de autodefinição (SDDL U)

Communications Server e SNA

Utilizando suporte à SDDL, as LUs suportadas por DLUR podem ser definidas dinamicamente para o VTAM, eliminando assim necessidade de serem predefinidas.

- Suporte a TakeOver/GiveBack

Este suporte permite que as sessões LU-LU permaneçam ativas mesmo quando a conexão entre o DLUR e os nós do DLUS falhar. A conexão pode ser restabelecida com o mesmo DLUS ou com outro, sem que as sessões LU-LU sejam interrompidas.

- Suporte a MultiSubnet

Este suporte permite que o nó DLUR, o nó DLUS e o nó que contém a aplicação estejam em sub-redes diferentes.

- Registro de LU servida pelo DLUS

Um DLUR de nó final registra suas LUs para que o nó da rede possa localizá-las sem precisar transmitir os pedidos de localização ao DLUR.

- Suporte ao DLUS de Reserva

Quando a conexão ao DLUS principal falhar ou não ficar ativa, o Communications Server tentará automaticamente estabelecer uma conexão ao DLUS de reserva.

Como Utilizar o DLUR

Para utilizar a função DLUR, você configura uma definição **DLUR_DEFAULTS** e utiliza o nome da ligação dessa definição como as definições de ligação ao sistema central para LUA, LU dependente 6.2 ou gateway. O Communications Server envia o PUNAME, CPNAME e o NODEID para o DLUS. O PUNAME é enviado como parte das informações de sinalização (CV X'0E').

- Se o DLUS for de nível superior (suporta a verificação do CV X'0E' em REQACTPU), ele utilizará o PUNAME no seu algoritmo de pesquisa. Isto está disponível no VTAM 4.3 com PTF ou superior.
- Se o DLUS for de nível inferior, ele ignorará o CV X'0E'.
- Se não houver correspondência no PUNAME ou o DLUS for de nível inferior, o DLUS tentará localizar uma PU com nome de CP ou NODEID (IDBLK/IDNUM) correspondente, predefinida em um nó principal de comutação do VTAM ou criada dinamicamente utilizando a saída ISTECCS.

As conexões à rede, que utilizam a sua opção de conectividade (Token Ring, SDLC, AnyNet, etc.), devem ser configuradas e ativadas antes que a conexão DLUR a DLUS possa ser estabelecida. Existindo uma conexão APPN entre o DLUR e o DLUS, um par de sessões de controle é estabelecido entre o DLUR e o DLUS que estão utilizando um modo especial, CPSVRMGR. Este par de sessões de controle também é chamado de canal CP-SVR e aparece como uma ligação para o Communications Server. Portanto, ele pode ser ativado, desativado e exibido com a utilização das **Operações do Nó SNA**.

Após a ativação do canal, o suporte a SSCP para PU e SSCP para LU pode ser fornecido a PUs e LUs que definiram o canal como sua ligação ao sistema central. As sessões LU-LU não utilizam o canal, mas utilizarão o melhor caminho disponível através da rede.

No ambiente DLUR, qualquer número de PUs dedicadas pode ser definido nas sessões de LU 6.2. Isto permite que o gateway forneça às estações de trabalho downstream o acesso ao gerenciamento da rede através da PU dedicada, sem precisar de várias ligações físicas aos sistemas centrais.

... podem iniciar sessões e responder a ...
... inicia e responde os pedidos de acordo com ...
... independente.

... ativar uma sessão LU-LU (isto é, enviar um ...
... SSCP. Portanto, ela não tem uma sessão SSCP ...
... enviar e receber BINDs. A remetente do BIND ...
... receptora do BIND chama-se LU secundária (S ...

... LU 6.2 pode ser uma LU independente. O Com ...
... protocolos da LU independente para outros n ...
... de subárea tipo 5 do nível LEN.

... LU independentes podem ter sessões paralel ...
... podem ter várias sessões entre uma LU e dive ...
... sessões são estabelecidos com base no nom ...

A Figura 18 na página 56 mostra como ...
estabelecidas por uma LU independ ...
LUy e uma única sessão com a LU ...
relacionamento LU-SLU. A LU ...
uma das sessões com a LU ...
sessões paralelas com ...

Chave

representa uma ligação entre os nós

representa uma sessão entre LUs
(a seta aponta para

LU Dependente

LU dependente é uma LU controlada por um sistema central SNA. Para ativar uma sessão LU-LU, uma LU dependente requer a assistência de um SSCP. É necessária uma sessão SSCP-LU para enviar um BIND. Os protocolos da LU dependente são suportados pelo Communications Server, mas apenas para os nós de subárea tipo 5 que estão utilizando protocolos tipo 2.0, não para outros nós periféricos tipo 2.1. As LUs dependentes agem apenas como SLUs e têm um limite de 1 sessão LU-LU. Entretanto, o suporte múltiplo à PU no Communications Server permite estabelecer várias sessões SSCP-PU simultâneas com sessões da LU dependente.

A função dependent LU requester (DLUR) permite que o Communications Server se beneficie do suporte avançado ao SSCP, fornecido por um dependent LU server (DLUS). Alguns dos benefícios dessa função são:

- As LUs dependentes podem residir em nós que não são adjacentes ao sistema central.
- A lógica da pesquisa do APPN encontra o melhor caminho para sessões LU-LU.
- As LUs dependentes do SNA podem obter as vantagens de uma rede APPN.

Para utilizar este DLUR, configure um parâmetro

DEFINE_DEPENDENT_LU_SERVER e utilize o nome da ligação dessa definição para as definições de LUA, LU dependente 6.2 ou gateway.

LU 6.2

As LUs independentes são definidas para o programa VTAM através da codificação LOCADDR=0. Podem existir tantas LUs definidas com LOCADDR=0 quantas você desejar. Entretanto, observe que nem todas as LUs 6.2 são LUs independentes.

Ao definir as LUs de uma parte da rede APPN para o programa VTAM, você deve defini-las como se estivessem no nó da rede que conecta essa parte da rede APPN à rede de subárea. Após a definição da PU desse nó da rede, defina cada LU que você deseja atingir a partir da outra parte da rede APPN. Não se esqueça de que os pontos de controle são LUs. **Figura 185 Sessões Múltiplas e Paralelas Communications Server e S**

Uma LU deverá ser definida no VTAM para estabelecer uma sessão com outra LU se essa sessão passar pela rede de subárea. Não existe uma forma eficaz de contorná-la (como os caracteres curinga do APPN). O VTAM deve saber o nome de cada LU de destino.

Como uma rede APPN é alterada facilmente, você deve definir as LUs da rede APPN em um nó principal especial sempre que for possível. Você também pode definir, no VTAM, as LUs que ainda não existem.

Outras LUs

Se o nó da rede utilizar sua conexão à rede de subárea para emulação 3270, as LUs do tipo 2 da emulação 3270 serão definidas na mesma macro da PU como as LUs do tipo 6.2 da rede APPN. A ligação também será utilizada para a conexão entre a emulação 3270 e o sistema central.

Nó da Rede APPN e Suporte a T2.1

O APPN é um avanço da arquitetura SNA e do nó tipo 2.1 (T2.1) da IBM. O APPN permite a interconexão de sistemas de tamanhos amplamente diferentes em redes com uma topologia dinâmica. Uma rede APPN é mais fácil de utilizar, mais confiável e fornece mais flexibilidade do que as redes SNA tradicionais.

Consulte o *3174 APPN Implementation Guide* para obter informações adicionais sobre nós da rede APPN.

Compactação de Dados

A compactação de dados é o processo de compactação de bytes repetidos ou cadeias de dados repetidas para diminuir o comprimento dos registros ou blocos. Isto reduz o tempo de transferência necessário para as comunicações. Reduzindo a quantidade de dados transferidos entre as sessões do sistema central e da estação de trabalho, você pode aumentar o rendimento em linhas de baixa velocidade e diminuir o custo por bit nas linhas caras.

O ganho no desempenho, medido pelo número de bytes transferidos, que você pode esperar com a utilização da compactação de dados é freqüentemente uma relação de cerca de 2:1. Isto significa que, com a compactação de dados ativada, você economiza um em cada dois bytes nos buffers necessários para conversão de protocolo de nível inferior.

A compactação de dados é benéfica para aqueles que precisam:

- Melhorar os tempos de resposta, especialmente em linhas de baixa velocidade
- Reduzir custos nas linhas onde as tarifas baseiam-se no volume de dados
- Menos linhas dedicadas

Entretanto, a compactação de dados não deve ser aplicada a cada sessão que você está executando, uma vez que existem desvantagens que você deve considerar:

- A compactação e a descompactação precisam de ciclos de CPU adicionais
- Será necessário maior armazenamento de dados (32 bytes a 9,0 KB)
- A compactação de dados requer uma ligação segura, conforme definido na tabela de classe de serviço (COS) do APPN.

Communications Server e SNA

- Pode ser necessário ajustar o tamanho da RU para obter o melhor desempenho. Cada RU é compactada e enviada. Se os pacotes estiverem sendo enviados, uma RU de tamanho maior no modo permitirá que mais pacotes completos sejam enviados.

Nota: A quantidade de memória aumentada depende do algoritmo de compactação que você utiliza. Este aumento é adicional à memória necessária para a mensagem.

Para obter descrições detalhadas e técnicas dos diferentes algoritmos de compactação, consulte as seguintes publicações:

- *SNA Formats*
- *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*

As seções seguintes descrevem a compactação no nível do SNA e a implementação do Communications Server.

Arquitetura da Compactação no Nível de Sessão do SNA

A compactação em nível de sessão do SNA implementa a compactação de dados na meia-sessão LU-LU. Com o Communications Server, ela está disponível para todos os tipos de LUs suportados, isto é: LUs tipos 0, 1, 2, 3 e 6.2. A compactação de dados no nível de seção fornece estas vantagens:

- É mais eficiente para compactar dados antes de criptografá-los
- Os diferentes algoritmos são mais eficazes para os diferentes tipos de dados
- Os programas aplicativos não precisam fornecer sua própria lógica de compactação

Geralmente são definidos dois algoritmos para a compactação no nível de sessão do SNA, Codificação do comprimento de processamento (RLE) e uma forma de Lempel-Ziv (LZ). O Communications Server suporta a compactação no nível de sessão do SNA, utilizando os seguintes algoritmos:

- NENHUMA compactação.
- Compactação RLE. RLE é o algoritmo mais simples e amplamente conhecido, substituindo cadeias de bytes idênticos por cadeias codificadas mais curtas.
- Compactação LZ9. LZ9 é um algoritmo de compactação dinâmica que compacta cadeias vistas anteriormente (em RUs atuais ou anteriores) para um código de 9 bits que representa o índice de origem zero de uma entrada na tabela de compactação/descompactação. As entradas da tabela armazenam cadeias vistas anteriormente.
- Compactação LZ10. O LZ10 é um algoritmo de compactação dinâmica que compacta cadeias vistas anteriormente (em RUs atuais ou anteriores) para um código de 10 bits que representa o índice de origem zero de uma entrada na tabela de compactação/descompactação. As entradas da tabela armazenam cadeias vistas anteriormente.

Geralmente o LZ compacta dados melhor do que o RLE, mas a um custo maior de memória e função da CPU.

A compactação no nível de sessão do SNA visualiza a sessão em duas direções, PLU-SLU e SLU-PLU. A unidade lógica principal (PLU) é a LU responsável pela ativação da sessão. A unidade lógica secundária (SLU) é a LU que responde. A PLU ativa uma sessão enviando um pedido de Sessão Bind (BIND) à SLU, que responde com um BIND. Isto significa que os diferentes algoritmos de compactação podem ser utilizados nas direções PLU-SLU e SLU-PLU. Isto é executado através da negociação BIND dos níveis de compactação. A LU 6.2 pode utilizar qualquer combinação de níveis de compactação para uma sessão (por exemplo, a PLU pode utilizar RLE e a SLU-PLU pode utilizar LZ9). Todos os outros tipos de LUs têm compactação ativada ou desativada. Quando ativado, o nível de compactação PLU-SLU é LZ9 e o SLU-PLU é RLE.

Compactação de Dados do Communications Server

O Communications Server suporta compactação de dados no nível de sessão do SNA com os algoritmos de compactação RLE, LZ9 e LZ10. Com o Communications Server, você pode especificar a utilização de compactação de dados para comunicações através de sessões da CPI-C (por meio de sessões de APPC), sessões de APPC (LU 6.2) e sessões de LUA (LU 0, LU 1, LU 2 e LU 3).

Uma configuração de duas partes é utilizada para permitir a compactação de dados. O nó do Communications Server deve ser ativado para compactação de dados e a LU (APPC e LUA) deve ser ativada primeiro. Os dois campos de compactação de nó (nível e sinais) estão na janela de características do nó local (palavra-chave **NODE** no arquivo .ACG).

O campo nível de compactação define o nível máximo com o qual qualquer sessão pode ser iniciada: NONE, RLE, LZ9 ou LZ10. Este campo tem precedência sobre todos os níveis de compactação configurados ou tentados (a única exceção é o DFT independente, que não requer a definição de nó). Se estiver configurando uma sessão utilizando LUA (LU 0, LU 1, LU 2 e LU 3) para suportar emulação 3270 ou impressoras, o LZ9 será necessário para compactação de dados. Os outros níveis de compactação não permitem a compactação de dados para estes tipos de LUs.

O tamanho da unidade de pedido padrão para os modos compactados é duas vezes o tamanho da unidade básica de transmissão (BTU) da conexão. Se estiver utilizando comutação de pacotes, você não poderá utilizar este tamanho padrão. Em vez disso, utilize um tamanho maior e segmente os pacotes.

A compactação da LU 6.2 pode ser ativada pela:

- Utilização de modos fornecidos com o Communications Server
 - #INTERC
 - #BATCHC
 - #BATCHCS
 - #INTERCS
- Alteração ou inclusão de modos com a compactação ativada

No painel Definição de Modo (palavra-chave **MODE**, no arquivo .ACG), são exibidos três campos de modo de compactação: compactação necessária, nível de compactação PLU->SLU e nível de compactação SLU->PLU.

A necessidade de compactação pode ter dois valores.

Proibida

Nenhuma compactação.

Communications Server e SNA

Necessária

Utilize esta opção para solicitar a compactação de dados com os valores definidos no nível de compactação PLU->SLU e no nível de compactação SLU->PLU. O nível solicitado pode não ser obtido pelas seguintes razões:

- As definições do nó limitaram o nível permitido
- A SLU negociou os níveis para baixo

A SLU segue os níveis de compactação solicitados pela PLU, a menos que seja limitada pelas definições de compactação do nó.

Para obter mais informações sobre a compactação do Communications Server, consulte o texto do auxílio online do produto ou o *ASCII Configuration Reference*.

Criptografia no Nível de Sessão do SNA

A criptografia no nível de sessão do SNA permite criptografar todos os dados ou dados selecionados que são transferidos entre a estação de trabalho e o sistema central. Se desejar proteger quaisquer dados da estação de trabalho utilizando criptografia, o sistema central também deverá ser configurado para utilizá-la.

Uma placa IBM SecureWay 4758 PCI Cryptographic Coprocessor (chamada IBM 4758) deve ser instalada no servidor, para permitir a confidencialidade dos dados. Essa placa deve ser inicializada seguindo-se as instruções fornecidas com a mesma.

No Communications Server, a criptografia no nível de sessão da LU 6.2 é configurada com base na descrição do modo utilizado para um determinado programa de transação. Existem dois níveis de criptografia:

- Nível de sessão de APPC

Estritamente entre duas LUs, nenhum ponto de controle é envolvido na conversão das chaves

- Conversão de chave de sessão do APPN

O ponto de controle da LU de origem (EN ou NN) e possivelmente seu servidor do NN convertem as chaves além da LU de origem.

Para configurar um modo para criptografia, abra a janela Recursos do SNA e selecione **MODOS**. Em seguida, na janela Definição do Modo, selecione **Configuração...** A janela Suporte à Compactação e Criptografia no Nível de Sessão aparece. Os parâmetros para configuração da criptografia estão em duas partes:

- Para criptografia no nível de sessão, você pode especificar se a criptografia é opcional (as LUs negociam) ou obrigatória (a criptografia deve ser utilizada).

Nota: A criptografia do Communications Server para um sistema central é sempre obrigatória.

- Para conversão de chave de sessão do APPN, você pode especificar que apenas a LU converte a chave, que apenas o nó final converte a chave da sessão ou que o nó final e o seu nó da rede convertem a chave.

O Communications Server requer outros produtos para armazenamento e conversão da chave. Um produto common cryptographic architecture (CCA) é necessário para armazenamento da chave, gerenciado pelos utilitários fornecidos com a placa IBM 4758. O Communications Server chama um produto CCA, que interage com a placa IBM 4758 para obter as chaves e criptografar os dados.

Usuários do VTAM:

O Communications Server não criptografa a sessão SNASVCMG. Você deve especificar ENCR=OPT na instrução APPL da definição da aplicação VTAM. Ao trabalhar com VTAM, você deve especificar a criptografia na instrução MODEENT. Por exemplo:

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

Para utilizar a função de criptografia do VTAM, o IBM Programmed Cryptographic Facility (PCF) deve ser iniciado antes do VTAM.

Começando com o VTAM V3R4.1, o VTAM utiliza uma nova interface com o Integrated Cryptographic Service Facility/MVS (ICSF/MVS) para serviços de criptografia, como o fornecimento de criptografia no nível de sessão. Essa interface está de acordo com a Common Cryptographic Architecture (CCA) implementada pelo ICSF/MVS. Com este suporte, você pode iniciar e encerrar o serviço criptográfico após o VTAM ser iniciado e pode alterar a chave mestra sem interromper o VTAM ou as sessões LU-LU ativas.

Para obter mais informações sobre como definir a criptografia de dados, consulte o *OS/390 eNetwork Communications Server: SNA Network Implementation*.

Serviços de Gerenciamento

Os serviços de gerenciamento (MS) do Communications Server são funções distribuídas entre os componentes da rede para operar, gerenciar e controlar a rede. Este recurso é baseado na arquitetura de serviços de gerenciamento do SNA documentado no *Systems Network Architecture Management Services Reference*.

Pontos Focais, Pontos de Serviço e Pontos de Entrada

O Communications Server fornece suporte à programação que permite a instalação das aplicações do ponto focal (FP), ponto de serviço (SP) e ponto de entrada (EP) dos serviços de gerenciamento. As aplicações do SP dos serviços de gerenciamento são apenas uma variação das aplicações do EP dos serviços de gerenciamento e diferem apenas nos tipos de funções que fornecem. Caso contrário, elas interagem com um ponto focal dos serviços de gerenciamento como aplicações do EP dos serviços de gerenciamento.

Ponto Focal

Um ponto focal dos serviços de gerenciamento é um ponto central de controle para gerenciamento de uma rede. A partir de uma aplicação do SP ou do EP dos serviços de gerenciamento, o ponto focal dos serviços de gerenciamento pode solicitar certos dados relativos à operação de uma rede, como dados de problemas e desempenho ou identificação do produto.

O ponto focal dos serviços de gerenciamento também pode aceitar dos nós que ele gerencia certos dados dos serviços de gerenciamento não solicitados, com base na categoria dos dados dos serviços de gerenciamento. Um exemplo de categoria dos serviços de gerenciamento são os seus alertas. Um ponto focal dos serviços de gerenciamento pode gerenciar uma ou mais categorias de dados dos serviços de gerenciamento

Communications Server e SNA

e pode existir um ou mais pontos focais dos serviços de gerenciamento em uma rede. O IBM Communications Server, o programa IBM NetView e o sistema operacional IBM OS/400 são exemplos de produtos que fornecem o recurso do ponto focal dos serviços de gerenciamento.

Ponto de Serviço

Um SP dos serviços de gerenciamento é a função, em um nó, que pode solicitar e capturar dados dos dispositivos que, por si próprios, não podem servir como EPs dos serviços de gerenciamento, como os dispositivos conectados por protocolos de Rede Local (mas não protocolos do SNA de nível superior) para o nó do SP dos serviços de gerenciamento. Além de coletar dados não-locais, um SP dos serviços de gerenciamento funciona como um EP dos serviços de gerenciamento na sua relação com o ponto focal dos serviços de gerenciamento. Os programas sob licença IBM NetView/PC e IBM LAN Network Manager são exemplos de aplicações do EP dos serviços de gerenciamento que fornecem funções do SP e do EP dos serviços de gerenciamento.

Ponto de Entrada

Um EP dos serviços de gerenciamento é a função, em um nó, que captura os dados locais dos serviços de gerenciamento e envia os mesmos a um ponto focal dos serviços de gerenciamento para processamento, solicitado ou não. O Communications Server fornece a função do EP dos serviços de gerenciamento para envio de alertas ao ponto focal dos serviços de gerenciamento de alertas. Estes alertas podem se originar no Communications Server ou nos DLCs que ele utiliza. O Communications Server também fornece suporte à programação para aplicações, como os programas sob licença IBM NetView/PC e IBM LAN Network Manager, através do fornecimento de alertas a serem enviados ao ponto focal dos serviços de gerenciamento de alertas.

Níveis da Arquitetura dos Serviços de Gerenciamento do SNA

Um produto SNA implementa um determinado nível (ou geração) da arquitetura dos Serviços de Gerenciamento do SNA e alguns produtos suportam vários níveis da arquitetura. O Communications Server pode enviar e receber dados dos serviços de gerenciamento dos produtos SNA que implementam qualquer um dos três níveis da arquitetura dos serviços de gerenciamento. Estes níveis são:

Nível Multiple Domain Support (MDS)

Um produto SNA que implementa o nível MDS da arquitetura dos serviços de gerenciamento, como o Communications Server e o IBM NetView Versão 2 Release 2 (ou posterior). Ele pode enviar e receber unidades de mensagem MDS (MDS-MUs). O IBM NetView Versão 2 Release 2 fornece o nível MDS como uma LU de subárea, não um ponto de controle (CP) e utiliza sessões do modo SNASVCMG para transporte MDS-MUs. Como um ponto focal, ele suporta relacionamentos FP-EP explícitos, implícitos (principais) e implícitos (reserva). O NetView Versão 2 Release 2 também continua a suportar o relacionamento FP-EP do sistema central para produtos do EP que não possuem suporte no nível de MDS.

Nível Migration

Um produto SNA que implementa o nível anterior da arquitetura dos serviços de gerenciamento, como o Nível de Modificação 0 do IBM OS/400 Versão 1 Release 3 (ou anterior). Um produto do nível Migration pode suportar relacionamentos explícitos, padrão e FP-EP do domínio. O relacionamento FP-EP do domínio é indicado quando as sessões CP a CP são ativadas para um nó do nível Migration. Um nó da rede (NN) servidor

do nível Migration não envia Recursos de MS para Notificação do FP aos seus nós finais (ENs) servidos, e um EN servido do nível Migration não aceita Recursos de MS para Notificação do FP do seu NN servidor. Ele pode enviar e receber CP-MSUs mas não MDS-MUs. Como um ponto focal, ele suporta apenas a categoria de MS de alertas.

Nível de Network Management Vector Transport (NMVT)

Um produto SNA que implementa o nível de NMVT da arquitetura dos serviços de gerenciamento do SNA, como o IBM NetView Versão 2 Release 1 (ou posterior). O NMVT é uma unidade de pedido (RU) cujo fluxo passa através de uma sessão ativa entre os serviços de gerenciamento da PU e os serviços de gerenciamento do ponto de controle. Se um NMVT for encaminhado a partir de uma estação através de um gateway, o gateway incluirá o nome do seu ponto de controle no NMVT.

Controle de Fluxo

Para gerenciar o fluxo de dados através de uma rede, o Communications Server utiliza controle de velocidade adaptável do nível de sessão. O controle de velocidade ocorre entre cada par de nós adjacentes que fazem parte da rota da sessão. O controle de velocidade entre dois nós adjacentes não depende do controle de velocidade utilizado entre outros nós adjacentes da rota.

Controle de Velocidade do Nível de Sessão

O controle de velocidade adaptável do nível de sessão utiliza um esquema baseado em janelas, onde um remetente pode enviar apenas um número limitado ou *janela*, de unidades de pedido por concessão explícita de permissão para continuar. O tamanho da janela pode ser alterado com base nas condições do receptor. Essa função permite que um nó controle a quantidade de dados que é enviada e recebida durante a operação normal da sessão. O controle da janela permite que o nó receptor gerencie sua taxa para receber dados nos seus buffers de sessão. O controle de velocidade adaptável do nível de sessão fornece a um nó que suporta muitas sessões um meio dinâmico de alocar recursos para uma sessão que apresenta uma rajada de atividade e para regenerar recursos não utilizados das sessões que não apresentam nenhuma atividade. O controle de velocidade adaptável do nível de sessão permite que o nó receptor utilize eficazmente os recursos do seu buffer disponível.

Como cada estágio da sessão entre os pontos extremos tem sua velocidade controlada independentemente, tanto os nós terminais quanto os nós intermediários podem adaptar o controle de velocidade para as sessões que manipulam, de acordo com suas próprias condições de congestionamento locais. Essa ação é a base do controle de fluxo global e do gerenciamento do congestionamento em redes APPN.

Entretanto, se uma sessão interativa e uma sessão que está transferindo um arquivo grande compartilharem uma ligação, os dados da sessão interativa deverão ser transmitidos o mais rapidamente possível. Isto pode ser feito de duas formas:

1. Atribua uma prioridade mais baixa à sessão de transferência de arquivos. #BATCH utiliza prioridade baixa.
2. Utilize o controle de velocidade fixo com um tamanho de janela pequeno para a sessão de transferência de arquivos para ativar os dados da sessão interativa para utilizar a ligação quando a sessão de transferência de arquivos estiver aguardando a resposta do controle de velocidade. Se estiver conectado

Communications Server e SNA

diretamente a um sistema central NCP, o controle de velocidade fixo nos dois sentidos da janela poderá ser utilizado para definir o controle de velocidade em ambas as direções para a janela de recepção no modo definido.

Controle de Velocidade BIND Adaptável

O tráfego de BINDs pode ocorrer em rajadas, principalmente na inicialização do nó ou da rede. Portanto, o controle de velocidade adaptável do BIND existe para controlar o fluxo de BINDs entre dois nós adjacentes. O mesmo algoritmo da janela utilizado para o controle de velocidade do nível de sessão é empregado.

Segmento e Montagem

Para transmitir RUs com tamanho acima do tamanho máximo permitido por uma determinada ligação, o Communications Server suporta a segmentação e a remontagem de dados. Estes segmentos são remontados para formarem RUs inteiras no nó parceiro. Essa ação permite que o tamanho da RU definido para uma sessão seja independente da ligação que é utilizado para a rota.

Controle de Velocidade do High Performance Routing

O high performance routing (HPR) fornece um novo método de controle de fluxo chamado controle de congestionamento adaptável baseado em taxa (ARB). O ARB regula o fluxo de tráfego através da previsão de congestionamento na rede e da redução da taxa de envio de um nó para a rede, impedindo o congestionamento em vez de reagir ao mesmo.

Controle de Velocidade Fixo

O controle de velocidade fixo permite compartilhar uma conexão física entre duas sessões. Sem o controle de velocidade fixo, os dados a serem transmitidos são colocados em uma fila de controle de ligação de dados (DLC) comum e os dados interativos seguem os dados previamente enfileirados. O controle de velocidade fixo também reduz a quantidade de memória que pode ser utilizada para colocar os dados na fila do DLC. O controle de velocidade fixo nos dois sentidos pode ser utilizado com um NCP para evitar a definição do controle de velocidade fixo do sistema central. Entretanto, em geral o controle de velocidade adaptável é o método mais eficaz de transferência de dados entre os nós.

A prioridade de transmissão, como o controle de velocidade fixo, permite o compartilhamento de uma ligação física entre sessões. Entretanto, ela bloqueará a memória à medida que os dados forem colocados nas filas do DLC, mas não exigirá as respostas de controle de velocidade adicionais necessárias para o controle de velocidade fixo.

Como Particionar LUs entre os Sistemas Centrais

Quando você define múltiplas conexões ao sistema central de subárea, é necessário que o tráfego do domínio de um determinado sistema central só entre em uma ligação lógica. Observe que as conexões de discagem manual parecem ser uma única ligação. Você deve definir uma PU diferente para suportar cada sistema central diferente. Apenas as ligações ao sistema central definidas no ponto de controle podem ter sessões CP a CP e participar da rede APPN. As ligações com `USE_PU_NAME_IN_XID=1` não podem ter sessões CP a CP. Caso contrário, as

ligações ao sistema central podem ter sessões CP a CP e também podem participar da comunicação do APPN. A palavra-chave **LINK_STATION** especifica o nome da PU e a ligação lógica a ser utilizada para a PU. Se forem necessárias ligações paralelas (em situações onde existem mais de 254 LUs dependentes), uma das ligações deverá ter o suporte à sessão CP a CP definido para Não.

Cada LU dependente pode ser definida como associada a apenas uma PU. A palavra-chave **LOCAL_LU** especifica o nome da ligação ao sistema central utilizado para uma LU dependente tipo 6.2. A palavra-chave **LU_0_TO_3** especifica o nome da ligação ao sistema central para a LUA e o perfil 3270 especifica a ligação ao sistema central para cada sessão de emulação 3270.

O ponto de controle define automaticamente uma PU com o mesmo nome do ponto de controle. As LUs dependentes definidas em um SSCP da subárea podem ser associadas à PU do ponto de controle (de fato, a LU definida automaticamente para o ponto de controle também pode ser especificada como dependente). Cada PU 2.0 adicional para um sistema central de subárea diferente requer uma ligação e definição de PU separada. Uma PU é definida através da sua especificação em uma palavra-chave **LINK_STATION**. Isto não será necessário se todas as LUs forem independentes.

Se a sessão SSCP-PU for enviar alertas ao sistema central, defina a ligação ao ponto focal com a palavra-chave **NODE** no arquivo .ACG. Se um sistema central deve receber os alertas, especifique uma ligação lógica para o ponto de controle ao sistema central. Se a ligação a este sistema central não estiver disponível, o Communications Server registrará os alertas. Os únicos pedidos de gerenciamento de rede aceitos de um sistema central da PU 2.0 são aqueles para a PU do ponto de controle. As respostas são enviadas ao mesmo sistema central com a utilização da PU do ponto de controle.

Cada unidade lógica dependente deve ter um endereço local configurado que é o mesmo configurado no sistema central. Entretanto, a utilização do SNA Gateway permite uma conversão do endereço de gateway. Uma LU dependente 6.2 pode agir como uma LU independente para um nó do mesmo nível, isto é, ela só é dependente para a subárea. Essa LU não deve fazer parte de uma rede APPN com qualquer outra conexão à mesma subárea, isto é, a subárea que contém o SSCP controlador. Apenas uma conexão à subárea é permitida para uma rede APPN, a menos que as subáreas sejam independentes. Embora um gateway possa ter ligações paralelas à mesma subárea, apenas um pode ter sessões CP a CP e tráfego de APPN.

Um SSCP na rede de subárea ativa as LUs dependentes que ele controla após o estabelecimento da ligação com ele. Até que seja ativada, a LU não pode iniciar uma sessão. Quando o APPC é removido, a desconexão é solicitada a cada sistema central ativo em sessão com uma PU no nó. Cada sistema central libera a ligação após desativar primeiro as LUs e, em seguida, a PU na sessão SSCP-PU.

Suporte SNA Gateway

O Communications Server fornece um gateway de Systems Network Architecture (SNA) de função completa. O gateway permite que várias estações de trabalho conectadas à Rede Local acessem os sistemas centrais System/370 ou System/390 através de uma ou mais conexões físicas com um ou mais sistemas centrais. Isto

Communications Server e SNA

auxilia na redução de custo por estação de trabalho das conexões do sistema central.

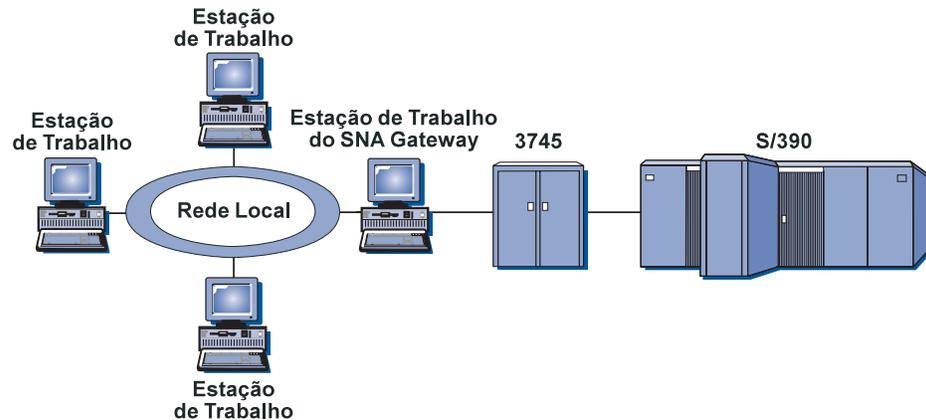


Figura 19. Exemplo de Configuração do SNA Gateway

O gateway do Communications Server suporta os protocolos do SNA LU 0, 1, 2, 3 e LU 6.2 (APPC) dependente. Com a função AnyNet SNA sobre TCP/IP, as estações de trabalho downstream agora podem se comunicar com o SNA Gateway sobre uma rede IP. O gateway também suporta LU 0, 1, 2 ou 3 para um sistema central AS/400 utilizando o pass-through do SNA. O sistema central AS/400 transmite dados através de um sistema central System/390.

Um gateway pode funcionar também como um conversor de protocolo entre as estações de trabalho conectadas à uma linha do sistema central da Rede Local e da Rede Ampla.

As LUs definidas no gateway podem ser dedicadas à uma estação de trabalho particular ou associadas a várias estações de trabalho. O controle permite que as estações de trabalho compartilhem as LUs comuns, que aumentam a eficiência das LUs e reduz os requisitos de configuração e inicialização para o sistema central. Você também pode definir vários grupos da LU, cada grupo associada à uma aplicação específica. E você pode definir grupos comuns que são associados aos vários sistemas centrais. Quando um cliente se conecta ao gateway, este recupera uma LU do conjunto para estabelecer uma sessão. A LU retorna ao grupo para ser acessada por outras estações de trabalho quando a sessão é encerrada.

Além disso, um SNA Gateway pode suportar a remessa de transporte de vetor de gerenciamento de rede (NMVTs) entre as estações de trabalho e o sistema central.

Cada sistema central visualiza o SNA Gateway como um nó PU 2.0 do SNA, suportando uma ou mais LUs por estação de trabalho. No que diz respeito ao sistema central, todas as LUs pertencem ao PU do SNA Gateway. O SNA Gateway pode ter várias conexões com o sistema central simultaneamente e pode direcionar diferentes sessões de estação de trabalho para sistemas centrais específicos.

Para as estações de trabalho suportadas, o SNA Gateway parece um controlador de comunicações PU 4 do SNA e envia os pedidos do sistema central como BIND e UNBIND. As LUs da estação de trabalho não ficam cientes do SNA Gateway. O SNA Gateway, contudo, está ciente de todas as LUs nas estações de trabalho.

As aplicações downstream, utilizando os protocolos padrão de conectividade do SNA para LU 0, 1, 2 e 3 e 6.2 dependente e comunicando-se através de um

gateway com um sistema central, são suportadas pelo Communications Server. A Tabela 4 resume os dispositivos do SNA Gateway.

Tabela 4. Resumo do SNA Gateway

Dispositivo	Descrição
Estações de Trabalho Ativas	254 (Rede Local) por placa 128 (X.25)
DLCs	AnyNet (SNA sobre TCP/IP) biaxial (apenas upstream) Rede Local (Toda placa de rede compatível com NDIS**) X.25 SDLC (síncronos, assíncronos e Sincronização Automática) Canal OEM (somente upstream) Canal MPC (somente upstream, requer DLUR) Enterprise Extender
Estações de Trabalho downstream	Todo produto que suporta os protocolos padrão de conectividade do SNA para LU 0, 1, 2, 3 e 6.2.
Inclusões e alterações dinâmicas	Sim
Suporte de estação de trabalho implícita	Sim
Associação da LU	Sim
Número Máximo de LUs	254 por PU; número de PUs ilimitado
Modo de operação	Várias Pus downstream (não aparentes ao sistema central) PUs não visíveis ao sistema central (exceto através do DLUR)
Vários suportes PU	Sim
Suporte de segmentação	Sim
Tipos suportados de LU	LU 0, 1, 2, 3 e 6.2 dependente

Communications Server e SNA

Parte 2. Planejamento e Instalação

Capítulo 3. Como Planejar o Suporte AnyNet

O Communications Server permite dois tipos de suporte AnyNet:

- Nó de Acesso e Gateway AnyNet SNA sobre TCP/IP
- Nó de Acesso e Gateway AnyNet Sockets sobre SNA

A função AnyNet SNA sobre TCP/IP no Communications Server permite que as aplicações SNA se comuniquem através das redes IP e SNA interconectadas.

A função de nó de acesso do SNA sobre TCP/IP permite que as aplicações SNA residentes em uma rede IP se comuniquem. Esta função suporta LU6.2 independente e LU 0, 1, 2, 3 ou 6.2 dependente com ou sem solicitador de LU dependente (DLUR). Além disso, o nó de acesso do SNA sobre TCP/IP pode ser utilizado em conjunto com o SNA Gateway para permitir sessões do SNA Gateway sobre TCP/IP.

A função SNA Gateway sobre TCP/IP amplia o alcance das aplicações SNA permitindo que as aplicações SNA em uma rede SNA se comuniquem com as aplicações SNA em uma rede IP. O SNA Gateway sobre TCP/IP suporta sessões de LU 6.2 independentes.

Para obter mais informações sobre como configurar o AnyNet SNA sobre TCP/IP, consulte o “Como Configurar AnyNet SNA sobre TCP/IP”.

A função nó de acesso do Sockets sobre SNA permite que os programas aplicativos TCP/IP utilizando a interface de soquete WinSock 1.1 e WinSock 2.0 se comuniquem através de uma rede SNA.

A função gateway do Sockets sobre SNA permite que as aplicações de soquetes em redes SNA e TCP/IP se comuniquem. Os gateways Sockets sobre SNA geralmente são utilizados para conectar redes TCP/IP isoladas, utilizando uma rede principal SNA.

Consulte “Como Configurar AnyNet Sockets sobre SNA” na página 84 para obter mais informações sobre a configuração do Sockets over SNA.

Como Configurar AnyNet SNA sobre TCP/IP

Esta seção contém informações detalhadas sobre a configuração do AnyNet SNA sobre TCP/IP.

Como Mapear os Recursos do SNA para Endereços IP

Uma das etapas mais importantes para permitir a comunicação do SNA sobre TCP/IP não é executada através dos painéis do Communication Server. Antes das sessões ou conexões do SNA serem estabelecidas, o SNA sobre TCP/IP deverá determinar o endereço IP do parceiro. Ele é obtido mapeando o identificador do SNA do parceiro para um endereço IP utilizando as seguintes etapas:

1. O SNA sobre TCP/IP recebe o identificador do SNA do Communications Server em um dos seguintes formatos:

AnyNet SNA sobre TCP/IP

- Para nomes da LU, `netid.luname`
 - Para nomes de CP, `netid.cpname`
 - Para valores IDBLK e IDNUM, configurados como ID do nó adjacente, com dois campos: ID do bloco e ID da unidade física.
2. O SNA sobre TCP/IP obtém o identificador e gera um nome de domínio:
- Para nomes da LU, `luname.netid.snasuffix`
 - Para nomes de CP, `cpname.netid.snasuffix`
 - Para valores de IDBLK e IDNUM, `bbnnnnn.snasuffix`

Nota: O valor padrão para `snasuffix` é **SNA.IBM.COM**. Para obter informações adicionais sobre o sufixo do nome de domínio do SNA, consulte o auxílio online.

A Figura 20 apresenta exemplos de nomes de domínio gerados pelo SNA sobre TCP/IP.

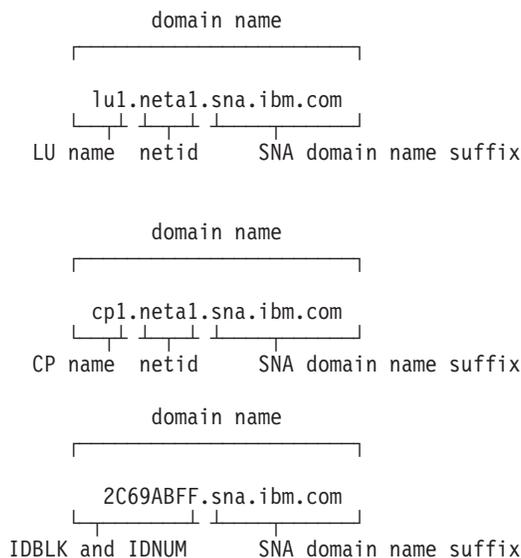


Figura 20. Formatos de Nomes de Domínio que o SNA Sobre TCP/IP Constrói

3. O SNA sobre TCP/IP pede que o nome de domínio seja convertido para um endereço IP.
4. O TCP/IP utiliza o arquivo HOSTS ou o servidor do nome de domínio para converter o nome de domínio em um endereço IP (por exemplo, 9.67.192.28).

Quando a rede IP inclui os gateways SNA sobre TCP/IP, considere as seguintes emissões de mapeamento de endereço adicional:

- Se a LU parceira for alcançada através de um gateway, o nome do domínio do parceiro deve ser mapeado para o endereço IP do gateway. Se houver gateways paralelos, o nome do domínio deverá ser mapeado para cada endereço IP de gateway.
- Para minimizar as informações de mapeamento de endereço necessárias para o AnyNet, utilize uma convenção de denominação na qual seu nome da LU seja o mesmo do nome do sistema central TCP/IP. Por exemplo, suponha que o nome do sistema central de seu computador seja `PATR.ANYNET.OURCORP.COM`. Se

you utilize the name of the LU PATR and the ID of the network ANYNET and, subsequently, define the suffix of the domain name of the SNA for OURCORP.COM, the AnyNet will request that the TCP/IP resolve the name PATR.ANYNET.OURCORP.COM. This name must already be in your domain name server.

Como Definir Nome de Domínio e Endereços IP

This section describes the function of name resolution of the TCP/IP, used by AnyNet to map SNA resources to IP addresses. This function consults the local HOSTS file and all domain name servers to convert a domain name (for example, lu1.neta1.sna.ibm.com) to an IP address (for example, 10.1.1.1).

Arquivo HOSTS

You will be able to use the HOSTS TCP/IP files to map domain names to IP addresses of your network. However, as the network grows and the maintenance of the HOSTS file in each workstation of the users becomes more time-consuming, it is recommended that you use a domain name server.

The HOSTS file (in the subdirectory drivers\etc of your system directory Windows NT) lists:

- IP Address
- Domain Name
- Other aliases for the domain name

For example, if your IP address is 10.1.1.1, the network ID is NETA1, the resource name is LUA1 and the suffix of the domain name of the SNA is the standard (sna.ibm.com), enter the following in your HOSTS file:

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

Servidor de Nome de Domínio

Domain names and IP addresses can also be defined in the domain name server database.

Each SNA identifier is mapped to an IP address corresponding to a domain name server. The location of these servers is configured in the Network section of the Control Panel.

For more information about the HOSTS files and domain name servers, consult the TCP/IP documentation. If your workstation is using TCP/IP support in Windows NT, consult the TCP/IP online documentation that accompanies the Windows NT product.

Considerações sobre o SNA Gateway sobre TCP/IP

The following information refers to gateways but not to node access functions.

Como Definir Nomes de CP e Nomes de Rede de Conexão

For configurations that have two or more SNA gateways over TCP/IP that connect a SNA network to two or more IP networks, you will need to define a unique control point (CP) name of the SNA and a unique network name of the SNA for each IP network.

AnyNet SNA sobre TCP/IP

Todas as LUs que residem em nós de acesso na rede IP parecem residir em um nó com este nome de CP.

Utilize o arquivo de dados reversos do servidor de nome de domínio ou o arquivo HOSTS para definir o nome de CP e de rede de conexão para uma determinada rede IP. Mapeie o endereço IP 127.0.0.3 para o nome de CP e o endereço IP 127.0.0.4 para o nome de rede de conexão.

O exemplo a seguir apresenta entradas no arquivo de dados reversos. Para uma rede IP com ID de rede do SNA NETA, o CPName MYCPNAME e o nome da rede de conexão MYCNET, será necessário definir as seguintes entradas:

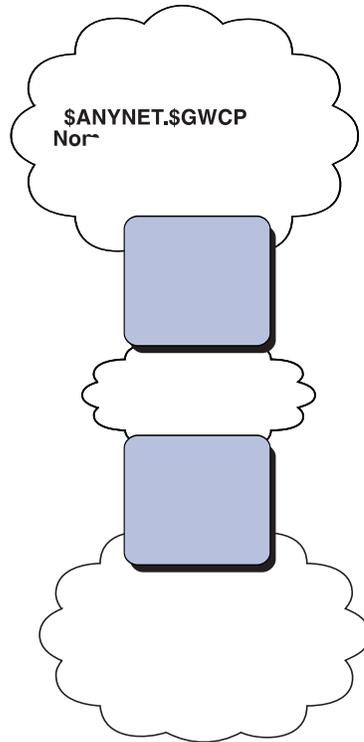
```
127.0.0.3      NETA.MYCPNAME.  
127.0.0.4      NETA.MYCNET.
```

Notas:

1. É necessário colocar um ponto depois do nome somente se a definição estiver no arquivo de dados reversos DNS. Não são utilizados pontos nas definições do arquivo HOSTS.
2. Não inclua o sufixo do nome de domínio do SNA.

A função AnyNet SNA sobre TCP/IP do Communications Server fornece um nome de CP padrão (\$ANYNET.\$GWCP) e um nome de rede de conexão padrão (\$ANYNET.\$GWCNET). Nas configurações com uma rede IP, você poderá utilizar o padrão se não definir um nome de CP ou um nome de rede de conexão. Nas configurações com gateways múltiplos que estejam conectados a múltiplas redes IP, uma delas poderá utilizar o padrão. Você deverá, portanto, definir um nome exclusivo de CP e de rede de conexão para todas as outras redes IP.

A Figura 21 na página 75 mostra como definir o CPName e o nome da rede de conexão para uma configuração com duas redes IP.



Como Utilizar a Entrada de Caractere Curinga para Reduzir as Definições do Servidor de Nome de Domínio

Se estiver utilizando o SNA sobre TCP/IP e a sua configuração encontrar as seguintes restrições de nomenclatura, você poderá reduzir o número de entradas do servidor de nome de domínio definindo uma entrada de nome de domínio para cada ID da rede SNA que possa ser acessada através de um ou mais gateways SNA sobre TCP/IP.

- Todas as redes do SNA deverão ter um ID exclusivo para cada uma delas.
- Todas as redes do IP deverão ter um ID exclusivo para cada uma delas.
- Uma rede SNA e IP poderá ter o mesmo ID de rede SNA.

Ao codificar uma entrada de nome de domínio único para cada ID de rede SNA, não é necessário definir uma entrada de nome de domínio para cada LU na rede SNA que você deseja comunicar através da rede IP. Você pode utilizar uma entrada de caractere curinga (*) para especificar o nome de LU de todas as LUs que possuam o mesmo ID de rede SNA. Ao substituir uma entrada de caractere curinga para o *luname* na entrada, você define uma entrada do servidor de nome de domínio que representa todas as LUs naquela determinada rede.

Nota: Se você utilizar a entrada de caractere curinga, é necessário utilizar o caractere curinga completo. Caracteres curingas parciais, como LUA*, não são válidos.

A entrada de caractere curinga é mapeada para o endereço IP do primeiro SNA Gateway sobre TCP/IP utilizado para alcançar a rede com aquele ID de rede SNA. Como mostra a Figura 22 na página 76, as unidades lógicas SNAAPPL1, APPC1, APPC2 e LU5 residem na rede NETB e podem ser alcançadas a partir da rede IP através de um

AnyNet SNA sobre TCP/IP

SNA Gateway sobre TCP/IP com endereço IP IPgwg. Se o sufixo do nome de domínio do SNA for SNA.IBM.COM, você irá definir a seguinte entrada no servidor de nome de domínio:

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

Esta entrada é utilizada para as quatro unidades lógicas.

Nota: Você tem a opção de definir cada unidade lógica individualmente.

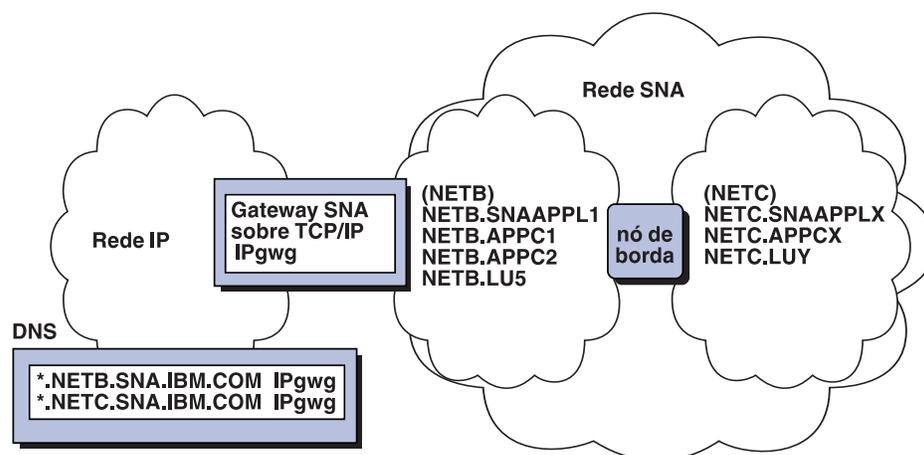


Figura 22. Definições do Servidor de Nome de Domínio para um Gateway Exclusivo Conectado a uma Rede SNA com dois IDs de Rede

Cada rede SNA deve ter uma única entrada. Como mostra a Figura 22, se você também tiver SNAAPPLX, APPCX e LUY na rede NETC, que poderá ser alcançada somente através do SNA Gateway sobre TCP/IP com endereço IP IPgwg, as entradas do servidor de nome de domínio serão as seguintes:

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

Além disso, cada gateway deverá ter uma única entrada. Se você incluir um SNA Gateway sobre TCP/IP paralelo, como mostra a Figura 23 na página 77, com endereço IP IPgwh para o exemplo anterior, as entradas do servidor de nome de domínio serão as seguintes:

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

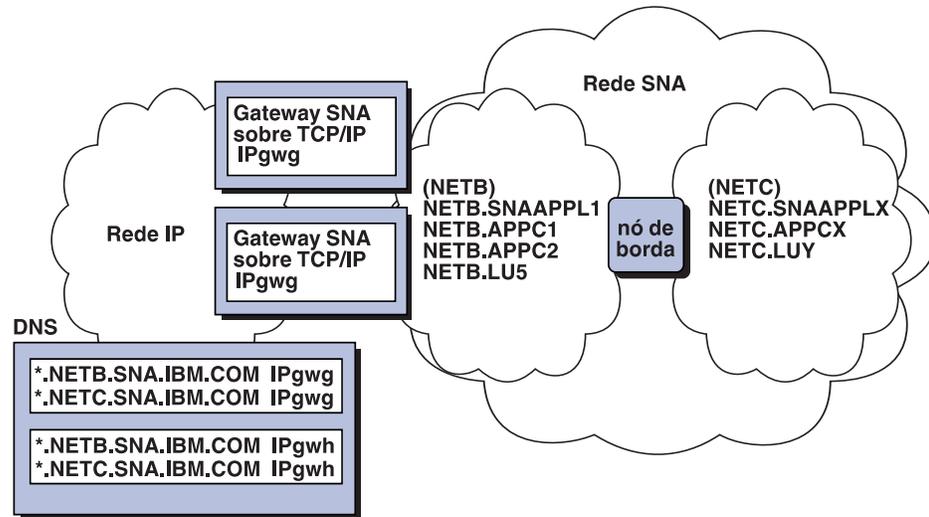


Figura 23. Definições do Servidor de Nome de Domínio para Gateways Paralelos Conectados a uma Rede SNA com Dois IDs de Rede

Considerações da Função de Nó do Acesso do SNA sobre TCP/IP

As informações a seguir referem-se apenas aos nós de acesso e não aos gateways.

Como Rotear as Sessões SNA através do AnyNet SNA sobre TCP/IP

Quando uma aplicação SNA inicia uma sessão, o Communications Server deve primeiro determinar qual transporte utilizar - o SNA, o IP ou uma combinação dos dois.

Você configura o transporte que preferir, definindo a preferência de roteamento. A preferência de roteamento pode ser definida como um nó completo através da preferência de roteamento padrão no dispositivo AnyNet sobre TCP/IP ou uma base por LU na definição das LUs parceiras.

A tabela de preferência de roteamento é utilizada somente para novas sessões. Previamente, as sessões existentes utilizam o mesmo transporte; elas não têm continuidade e não são roteadas novamente se a tabela de preferência de roteamento for alterada.

Nota: A preferência de roteamento de um nó apenas controla sessões que foram iniciadas a partir do nó (sessões de nó de acesso). As sessões que efetuam um nó não são afetadas pela preferência de roteamento.

Você pode definir ou modificar a preferência de roteamento padrão para um dos seguintes:

Nativo primeiro

Os pedidos são roteados através do SNA. Se nenhum roteamento do SNA estiver disponível, os pedidos serão roteados através do TCP/IP.

Não-nativo primeiro

Os pedidos são roteados através do TCP/IP. Se nenhum roteamento do TCP/IP estiver disponível, os pedidos serão roteados através do SNA.

AnyNet SNA sobre TCP/IP

Apenas Nativo

Os pedidos são roteados somente através do SNA. Se nenhum roteamento do SNA estiver disponível, a conexão falhará.

Apenas Não-nativo

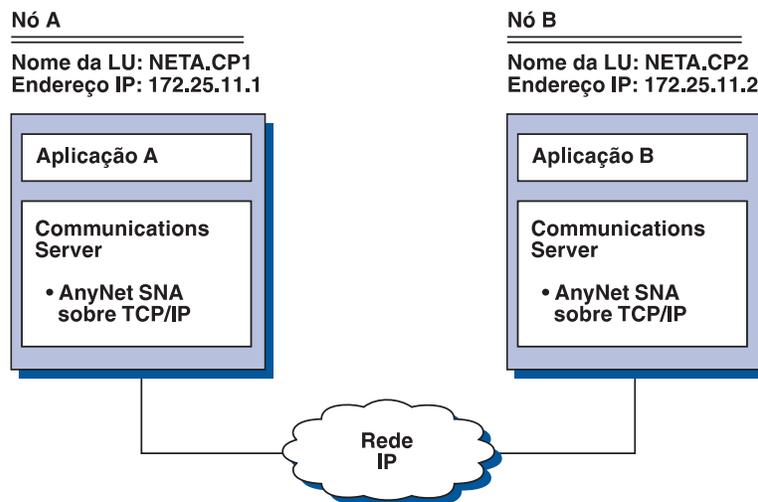
Os pedidos são roteados somente através do TCP/IP. Se nenhum roteamento do TCP/IP estiver disponível, a conexão falhará.

Exemplos de Configuração do AnyNet SNA sobre TCP/IP

Esta seção inclui exemplos do AnyNet que ativam o SNA através de comunicação IP. As seguintes instruções de configuração são completas somente no sistema operacional do Windows NT. Em todos os exemplos, o sufixo do nome de domínio do SNA é SNA.IBM.COM.

Para obter maiores informações sobre como configurar o AnyNet em quaisquer outras plataformas mencionadas nesta seção (como VTAM ou AS/400), consulte a documentação apropriada do produto.

Exemplo 1. Como Executar Aplicações APPC ou CPI-C sobre uma Rede TCP/IP



Etapas

Siga estas etapas para estabelecer comunicações entre os dois nós do Windows NT. Observe que neste exemplo os nomes de CP são utilizados como nomes de LU.

Para o Nó A, faça o seguinte:

1. Inclua a seguinte entrada no arquivo HOSTS local:
172.25.11.2 CP2.NETA.SNA.IBM.COM
2. Utilize **NETA.CP1** como o nome do ponto de controle durante a configuração do nó. Certifique-se de que a preferência de roteamento esteja definida para rotear as sessões sobre TCP/IP. Consulte os painéis de auxílio **Configuração do Nó** para obter mais informações.

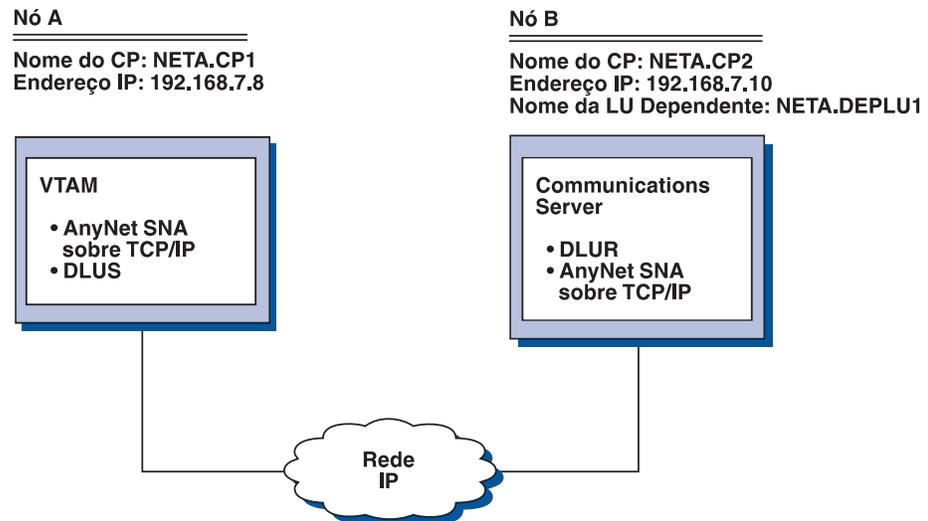
Para o Nó B, faça o seguinte:

1. Inclua a seguinte entrada no arquivo HOSTS local:

172.25.11.1 CP1.NETA.SNA.IBM.COM

- Utilize **NETA.CP2** como o nome do ponto de controle durante a configuração do nó. Certifique-se de que a preferência de roteamento esteja definida para rotear as sessões sobre TCP/IP. Consulte os painéis de auxílio **Configuração do Nó** para obter mais informações.

Exemplo 2. Emulação 3270 através do DLUR sobre uma Rede TCP/IP



Etapas

Siga estas etapas para estabelecer comunicações entre o Nó A e o Nó B.

Para o Nó B, faça o seguinte:

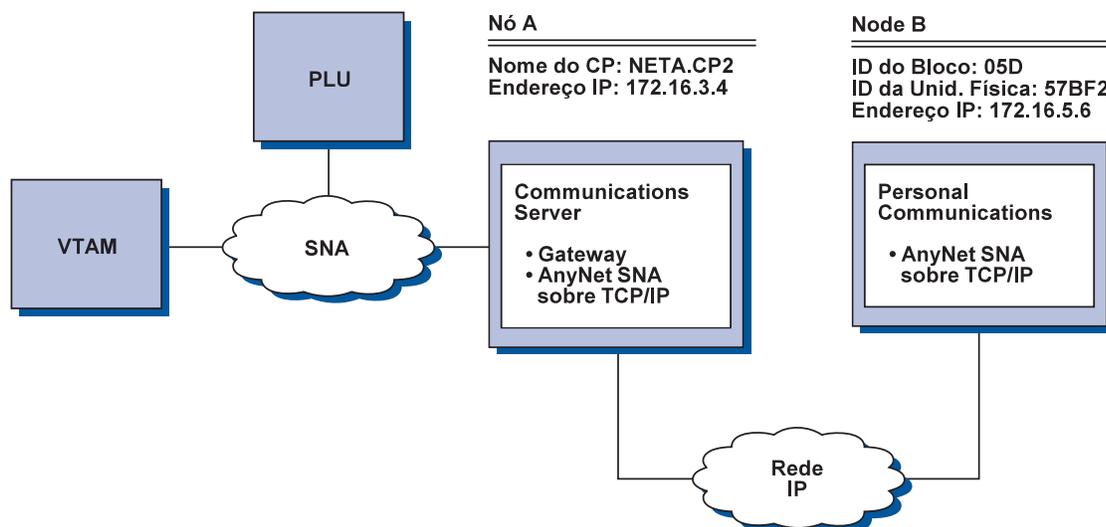
- Inclua a seguinte entrada no arquivo HOSTS local:
192.168.7.8 CP1.NETA.SNA.IBM.COM
- Utilize **NETA.CP2** como o nome do ponto de controle durante a configuração do nó e **NETA.CP1** como nome de DLUS quando estiver configurando PUs do DLUR. Certifique-se de que a preferência de roteamento esteja definida para rotear as sessões sobre TCP/IP. Consulte os painéis de auxílio **Configuração do Nó** para obter mais informações.

Para o Nó A, inclua as seguintes entradas no arquivo HOSTS:

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

Observe que MVS AnyNet SNA sobre TCP/IP atualmente requer DLUS/DLUR para comunicação da LU dependente.

Exemplo 3. Como Utilizar um SNA Gateway para Permitir Emulação 3270 entre as Redes SNA e TCP/IP



Etapas

Siga estas etapas para estabelecer comunicações entre o Nó B e o sistema central VTAM.

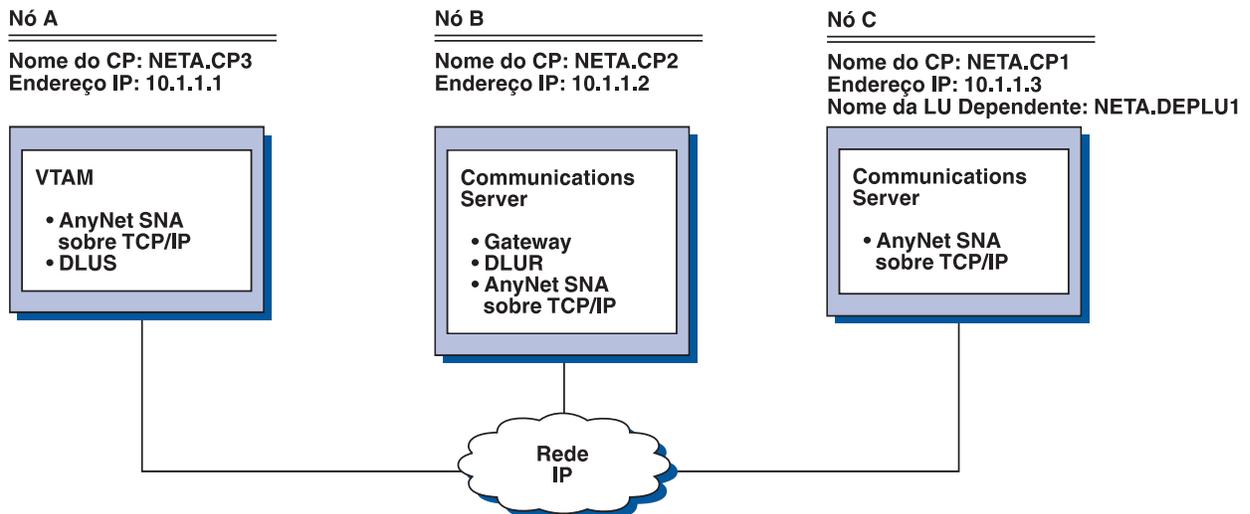
Para o Nó A, faça o seguinte:

1. Inclua a seguinte entrada no arquivo HOSTS local:
172.16.5.6 05D57BF2.SNA.IBM.COM
2. Utilize **NETA.CP2** como nome do ponto de controle durante a configuração do nó e o dispositivo ANYNET para designar os gabaritos implícitos quando estiver definindo clientes. Consulte os painéis de auxílio **Configuração do Nó** para obter mais informações.

Para o Nó B, inclua o seguinte no arquivo HOSTS local:

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

Exemplo 4. Como Utilizar um SNA Gateway para Emulação 3270 sobre uma Rede TCP/IP



Etapas

Siga estas etapas para estabelecer comunicações entre o Nó C e o Nó A.

Para o Nó B, faça o seguinte:

1. Inclua a seguinte entrada no arquivo HOSTS local:
 10.1.1.3 CP1.NETA.SNA.IBM.COM
2. Utilize **NETA.CP2** como o nome do ponto de controle durante a configuração do nó, **NETA.CP1** como o nome de CP adjacente quando estiver definindo a conexão AnyNet SNA sobre TCP/IP e **NETA.CP3** como o nome DLUS quando estiver atribuindo o DLUS a um gabarito de cliente. Certifique-se de que a preferência de roteamento esteja definida como não nativo para NETA.CP3. Consulte os painéis de auxílio **Configuração do Nó** para obter mais informações.

Para o Nó C, faça o seguinte:

1. Inclua a seguinte entrada no arquivo HOSTS:
 10.1.1.2 CP2.NETA.SNA.IBM.COM
2. Utilize **NETA.CP1** como o nome do ponto de controle durante a configuração do nó e **NETA.CP2** como o nome de CP adjacente quando estiver definido a conexão AnyNet SNA sobre TCP/IP. Consulte os painéis de auxílio **Configuração do Nó** para obter mais informações.

Para Nó A, inclua as seguintes entradas no arquivo HOSTS:

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

E.

çuração
do PUs
B.CP5
uração

Para Nó B, inclua as seguintes entradas no arquivo HOSTS:

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

Para Nó C, inclua as seguintes entradas no arquivo HOSTS:

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

Para o Nó D, faça o seguinte:

1. Inclua a seguinte entrada no arquivo HOSTS local:

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

2. Utilize **NETC.CP4** como o nome do ponto de controle durante a configuração do nó e **NETB.CP5** como o nome de DLUS quando estiver configurando PUs do DLUR. Certifique-se de que a preferência de roteamento para NETB.CP5 esteja definida como não-nativo. Consulte os painéis de auxílio **Configuração do Nó** para obter mais informações.

Dicas Úteis

Esta seção contém dicas úteis sobre ajuste, conectividade TCP/IP via SLIP ou PPP e endereços IP dinâmicos.

Ajuste

Se você puder acessar uma LU através de vários gateways SNA sobre TCP/IP e mapeou este nome da LU para vários endereços IP, aumente os parâmetros **CONN_RETRY_SECS** e **CONNWAIT_SECS** da palavra-chave **ANYNET_COMMON_PARAMETERS** quando estiver configurando os parâmetros básicos do AnyNet. Isto garante que as conexões TCP façam uma tentativa em todas as placas e gateways possíveis. Pode levar 90 segundos para que uma conexão TCP falhe em um endereço IP inativo.

Endereços IP Dinâmicos

Geralmente, o AnyNet SNA sobre TCP/IP depende dos recursos SNA (por exemplo, nomes da LU, nomes do CP ou idblk/num) que estão sendo mapeados estaticamente para os endereços IP. Entretanto, dependendo de sua configuração e de como suas conexões foram iniciadas, provavelmente você poderá utilizar AnyNet SNA sobre TCP/IP em ambientes onde os endereços IP estejam atribuídos dinamicamente (por exemplo, DHCP).

Aplicações APPC ou CPIC: Um nó de acesso SNA sobre TCP/IP com endereços IP atribuídos dinamicamente podem sempre iniciar sessões para outro nó de acesso ou SNA Gateway sobre TCP/IP com um endereço IP estático.

A única maneira que um nó de acesso ou SNA Gateway sobre TCP/IP com um endereço IP estático (nó A) pode iniciar uma sessão para um parceiro com um endereço IP dinâmico (nó B) é:

1. O nó B iniciou primeiro uma sessão para ou através do nó A.

AnyNet SNA sobre TCP/IP

2. A sessão iniciada na Etapa 1 ainda está ativa.

Aplicações da LU Dependente:

Nota: As informações nesta seção aplicam-se às aplicações LU 0, 1, 2, 3 ou 6.2 dependente.

Os nós de acesso SNA sobre TCP/IP com endereços IP atribuídos dinamicamente podem suportar comunicações de LU dependente se os seguintes critérios forem atendidos:

- A comunicação da LU dependente está ocorrendo através de um SNA Gateway através de um dos seguintes:
 - Communications Server/2 4.1 com APAR JR10461 aplicado
 - Communications Server/2 V5
 - Communications Server para Windows NT 5.01 ou superior
- O nó de acesso SNA sobre TCP/IP com endereço IP atribuído dinamicamente inicia conexões para um SNA Gateway com um endereço IP estático.

A comunicação da LU dependente através de DLUS/DLUR sobre AnyNet SNA sobre TCP/IP não é suportada se o nó DLUR tiver um endereço IP atribuído dinamicamente.

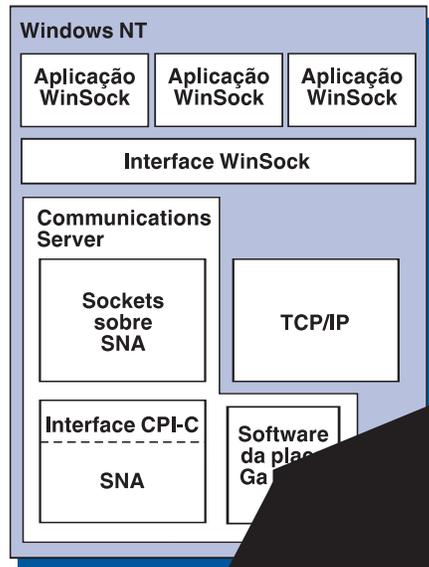
Como Configurar AnyNet Sockets sobre SNA

Esta seção contém mais informações sobre como configurar Sockets sobre SNA.

A função nó de acesso do Sockets sobre SNA do Communication Server permite que as aplicações compatíveis com WinSock se comuniquem sobre redes SNA. A função gateway Sockets sobre SNA permite que as aplicações de soquete se comuniquem nas redes SNA e IP.

Como Funciona o Sockets sobre SNA?

A Figura 24 na página 85 mostra a estrutura de um nó Windows NT executando o Sockets sobre SNA e ilustra como os programas aplicativos de soquetes e o Sockets sobre SNA operam em um nó Windows NT.



O Win

em u

O Winsock vai permitir que as aplicações em rede se comuniquem com as aplicações em rede IP se comunicarem com as aplicações em rede SNA. Isto é realizado através do uso de Sockets sobre SNA. Isto é realizado através da transformação dos pacotes de rede SNA e IP e da transformação dos pacotes de rede SNA e IP. O gateway AnyNet auxilia no estabelecimento de uma conexão entre as redes TCP/IP e SNA, e o código do Sockets sobre SNA permite a comunicação entre os dois protocolos.

a interface SNA permite

da rede SNA

Como Gerar uma Chamada da LU 6.2 a partir de uma Chamada de Socket

Para permitir que as informações formatadas para o protocolo TCP/IP façam parte de uma chamada LU 6.2 para a rede SNA, o Sockets sobre SNA mapeia endereços IP para nomes de LU 6.2 na rede SNA. Quando um programa aplicativo chama o Socket para estabelecer uma conexão com outro programa na rede SNA estabelece duas conversações semidúplex de LU 6.2.

O Sockets sobre SNA estabelece uma conversação de datagramas enviados para um único endereço de destino. Os datagramas de datagrama serão desalocados, se não forem especificados. Figura 247 Estrutura

Como Mapear um Endereço IP para um Nome Qualificado pela Rede SNA

Quando um programa aplicativo chama um Sockets sobre SNA para se comunicar com outro programa aplicativo, ele fornece o endereço IP do nó de destino. O Sockets sobre SNA deve mapear o endereço IP para um endereço SNA para que seja emitida uma chamada de LU 6.2 apropriada. Para cada endereço IP que identifica um nó, haverá um nome qualificado pela rede SNA correspondente.

“Como Rotear e Mapear a Visão Geral” na página 87 explica como o mapeamento de endereços funciona e fornece instruções e requisitos para a configuração do mapeamento de endereço IP-LU.

Como Rotear e Mapear Dados sobre as Redes SNA e IP

Os gateways Sockets sobre SNA permitem a comunicação entre programas aplicativos de soquetes em redes IP e SNA, através da combinação da função de roteamento de TCP/IP com a conversão de protocolos e recursos de mapeamento de endereços de Sockets sobre SNA.

A conversão de protocolos e o mapeamento de endereços serão necessários quando os dados forem roteados entre nós que utilizam protocolos de transporte diferentes. O gateway Sockets sobre SNA executa automaticamente a conversão de protocolos depois de determinar o tipo de transporte associado ao endereço IP de destino. Para obter um resumo do processo de roteamento e mapeamento, consulte “Como o Gateway Sockets sobre SNA Faz Roteamentos e Mapeia Dados” na página 89 .

Suporte do Programa Aplicativo Fornecido pelo Sockets sobre SNA

O Sockets sobre SNA suporta aplicações WinSock 1.1 e WinSock 2.0 (somente Windows NT 4.0) que utilizam soquetes AF_INET.

O Sockets sobre SNA não suporta aplicações que utilizam difusão.

Se pretende utilizar o gateway Sockets sobre SNA para rotear informações de e para um nó MVS/ESA configurado com a função VTAM V3R4.2 Sockets sobre SNA, primeiro você deverá instalar a função de roteamento no nó MVS/ESA. Para instalar a função de roteamento no MVS/ESA, instale a correção temporária de programa (PTF) UW03567. É possível obter PTFs através de qualquer uma das seguintes fontes:

- Acesso às Informações
- SoftwareXcel Estendido
- IBMLink (ServiceLink)

Se você não possuir acesso a estas fontes, entre em contato com o IBM Support Center.

Como Planejar o Sockets sobre SNA

Esta seção descreve o que o planejador de rede deve considerar antes de configurar uma rede com Sockets sobre SNA.

Como Rotear e Mapear a Visão Geral

Esta seção explica os conceitos básicos do endereçamento da Internet e como estes conceitos se relacionam com roteamento e mapeamento. Ela inclui as seguintes informações:

- “Endereçamento da Internet”
- “Tabela de Roteamentos IP” na página 88
- “ID de Rede SNA Utilizado pelo Sockets sobre SNA” na página 88
- “Como um Endereço IP É Mapeado para um Nome de LU” na página 88
- “Como o Gateway Sockets sobre SNA Faz Roteamentos e Mapeia Dados” na página 89

Endereçamento da Internet

A cada sistema central é atribuído, no mínimo, um endereço IP (Internet Protocol) exclusivo que é utilizado para rotear dados através da rede.

Nota: No conjunto IP de protocolos, o *sistema central* refere-se a um sistema final e pode ser qualquer estação de trabalho; não precisa ser um mainframe.

O endereço IP atribuído ao sistema central não define um sistema central na rede; ele define uma interface de rede naquele sistema central para uma rede. Por exemplo, o endereço da interface de rede SNA identifica uma conexão de nó com a rede SNA.

Um sistema central de gateway possui um endereço IP exclusivo para cada interface de rede. Como o gateway Sockets sobre SNA faz roteamento dos dados de SNA e TCP/IP, você deve configurar endereços IP exclusivos para interfaces TCP/IP e SNA.

A seção a seguir descreve o formato do endereço IP, classes de endereço e máscaras de rede. Para obter informações mais detalhadas, consulte a documentação do TCP/IP.

Formato e Classes do Endereço IP: Um endereço IP consiste em um campo de endereço 2-partes, 32-bits:

- A primeira parte do campo de endereço contém o endereço de rede; a segunda parte contém o endereço do sistema central.
- O número de bits utilizados para as partes de rede e de sistema central de um endereço IP é variável, dependendo da classe de endereços do endereço IP.
- Uma máscara de rede permite que você utilize um segmento da parte referente ao sistema central do endereço IP como um endereço de sub-rede.

As máscaras de rede padrão são mostradas em Tabela 5.

Tabela 5. Máscaras de Endereço IP Suportadas pelo Sockets sobre SNA

Para um endereço IP decimal pontilhado na forma de <i>a.b.c.d</i> , a faixa de valores para <i>a</i> é:	Máscara de Rede Padrão
1 a 127	255.0.0.0
128 a 191	255.255.0.0
192 a 223	255.255.255.0

AnyNet Sockets sobre SNA

Máscaras Utilizadas pelo Sockets sobre SNA: O Sockets sobre SNA utiliza dois tipos de máscara:

- **Máscara de sub-rede**

A máscara de sub-rede é utilizada no roteamento e é especificada durante a configuração do nó local e dos roteamentos. Você pode aceitar a máscara de subrede padrão ou especificar um valor diferente do padrão para definir os endereços de subrede.

- **Máscara de endereço**

A máscara de endereço é utilizada para mapeamentos de endereços IP-LU gerados e especificada durante a configuração.

Tabela de Roteamentos IP

Cada sistema central possui uma tabela de roteamentos IP que armazena informações sobre destinos possíveis e como alcançá-los. As entradas do roteamento estão incluídas quando:

- O endereço IP local está definido. Para obter mais informações, consulte o auxílio online.
- As instruções de roteamento são definidos a partir da janela **Configuração do Nó**. Dê um clique sobre **Configurar AnyNet Sockets** e, em seguida, dê um clique sobre **Roteamentos**. Para obter mais informações, consulte o auxílio online.
- É encontrado um roteamento com menos saltos. Isto ocorre quando o gateway Sockets sobre SNA recebe um redirecionamento ICMP ou uma mensagem RIP. Para obter mais informações, consulte “Função de Descoberta de Roteamento” na página 90.

Para um exemplo de uma tabela de roteamento, consulte Figura 25 na página 89.

ID de Rede SNA Utilizado pelo Sockets sobre SNA

Para cada roteamento definido através da interface SNA (sna0), deve haver um ID de rede SNA correspondente para o qual o endereço de rede IP é mapeado. O número de IDs de rede SNA definidos depende da maneira que você deseja mapear a rede IP para a rede SNA.

Por exemplo, se as aplicações de soquete que utilizam o SNA estiverem configuradas para utilizar as sub-redes IP 9.67.0.0 e 9.77.0.0, você poderá definir um ID de rede SNA que corresponda a cada sub-rede IP ou poderá definir um ID de rede SNA que corresponda às duas sub-redes. O Sockets sobre SNA não requer um mapeamento exclusivo um a um entre um endereço de rede IP e um ID de rede SNA.

Como um Endereço IP É Mapeado para um Nome de LU

É possível utilizar mapeamento gerado ou explícito para mapear os endereços IP para nomes SNA LU:

- No mapeamento explícito, todos os nomes de LU são definidos, e você atribui cada endereço de sistema central IP a um nome de LU SNA específico durante a configuração.
- No mapeamento gerado, os nomes de LU são gerados automaticamente. Durante a configuração, você especifica um endereço IP da rede, uma máscara de endereço, um ID de rede e um valor de gabarito da LU.

AnyNet Sockets sobre SNA

O Sockets sobre SNA utiliza a máscara de endereço para mapear a parte da rede do endereço IP para o ID da rede SNA e a parte do sistema central para o nome de LU SNA. O valor de gabarito da LU é utilizado para determinar os caracteres e as posições dos caracteres utilizados no nome de LU.

Você pode exibir o nome de LU gerado para um determinado endereço IP utilizando o utilitário da linha de comandos **sxmap**. A sintaxe para este utilitário é:

```
sxmap convert <IP address> <address mask> <LU template>
```

Como o Gateway Sockets sobre SNA Faz Roteamentos e Mapeia Dados

As etapas seguintes descrevem de maneira breve como o Gateway Sockets sobre SNA determina se é necessário rotear dados sobre SNA ou TCP/IP e como o mapeamento de endereços é controlado.

1. O Sockets sobre SNA pesquisa sua própria tabela de roteamentos para encontrar uma rota que permita que os dados cheguem ao endereço IP de destino. Se o Sockets sobre SNA não encontrar um roteamento correspondente, o pedido de conexão será enviado para a pilha TCP/IP nativa.
2. Se os Sockets sobre SNA encontrar uma rota correspondente, a entrada da rota indica como se pode chegar a esse destino:
 - a. Se o endereço do roteador for o endereço de uma interface de rede local, como `sna0`, a rede, a sub-rede ou o endereço do sistema central de destino poderá ser alcançado diretamente.
 - b. Se o endereço do roteador for o endereço de um gateway ou de um roteador, o destino poderá ser alcançado somente através do gateway ou do roteador intermediário.

A Figura 25 mostra um exemplo de uma tabela de roteamentos IP.

Endereço IP de Destino	Máscara de Dest.	End. IP do Gateway	Total de Utilização
1.2.3.4	255.255.255.255	199.245.253.1	10
10.0.0.0	255.0.0.0	199.245.253.2	0
10.11.0.0	255.255.0.0	199.245.253.113	37
127.0.0.1	255.255.255.255	127.0.0.1	8
128.1.0.0	255.255.0.0	199.245.253.3	0
199.245.253.0	255.255.255.0	199.245.253.113	368

Figura 25. Exemplo de um Painel de Roteamento IP

3. Se nenhum roteamento for encontrado na tabela de roteamentos do Sockets sobre SNA, o Sockets sobre SNA assumirá que o destino do TCP/IP poderá ser acessado através de uma rede IP nativa. Consulte a documentação do TCP/IP para obter mais informações sobre como o TCP/IP faz o roteamento dos dados.
4. Se a rota escolhida indica que os dados deverão passar pela interface SNA (`sna0`), o Sockets sobre SNA procura o próximo endereço de salto na tabela de mapeamento IP-LU :
 - a. Se o Sockets sobre SNA encontrar uma entrada correspondente, será estabelecida uma conexão de LU 6.2.
 - b. Se o Sockets sobre SNA não encontrar uma entrada correspondente, a tentativa de conexão falhará.
 - c. O Sockets sobre SNA transmite o endereço de destino e os dados para o Communications Server.



Se a rede ou a sub-rede for conhecida no Gateway 1 e um caminho mais direto estiver disponível, o Gateway 1 retornará uma mensagem de redirecionamento do ICMP ao solicitador indicando o caminho a ser utilizado no futuro. Esta mensagem de redirecionamento do ICMP atualiza a tabela de roteamentos do solicitador. Portanto, os Gateways 2 e 3 criam dinamicamente suas tabelas de roteamentos para redes e sub-redes remotas, conforme forem necessárias.

- Se novos gateways forem incluídos, atualize a tabela de roteamentos permanente do Gateway 1. Nenhuma instrução explícita de roteamento é necessária para os Gateways 2 e 3.

Como Definir Modos de Sockets sobre SNA

Sockets sobre SNA utilizam conversações da LU 6.2 para ativar a comunicação entre os programas aplicativos do soquete. Quando uma conversação de LU 6.2 é estabelecida, o Sockets sobre SNA define o modo e as características de sessão associadas da conexão. O Communications Server utiliza o nome do modo para identificar as características da conexão entre os dois nós de Sockets sobre SNA.

O modo padrão de Sockets sobre SNA é BLANK. Você pode utilizar o modo padrão para Sockets sobre SNA ou definir o seu próprio. Para alterar o modo Sockets sobre SNA padrão, a partir da janela **Configuração de Nó**, dê um clique em **Configurar AnyNet Sockets sobre SNA** e depois dê um clique **Modos**. Você pode definir outro modo padrão para todo o tráfego do TCP/IP e atribuir um modo específico a uma porta TCP/IP específica.

Se for especificado um modo alternativo que não esteja definido pelo Communications Server, será necessário definir as características de sessão associadas a esse modo para o Communications Server.

Como Alterar o Intervalo de Tempo de Espera de Inatividade

A opção início de tempo de espera de inatividade permite ajustar o número de segundos de inatividade antes que o Sockets sobre SNA desaloca a conversação do datagrama. Este intervalo permite equilibrar o uso de recursos para manter uma conversação existente do datagrama e a demorar a reestabelecer uma nova conversação do datagrama. Por exemplo, se este valor for definido para menor, as conversações de datagrama não utilizadas serão encerradas de maneira mais rápida, mas levará mais tempo para ser enviado o próximo datagrama. O intervalo de tempo de espera de inatividade padrão é de 90 segundos.

Para modificar a opção de início, a partir da janela **Configuração de Nó**, dê um clique sobre **Configurar AnyNet Sockets sobre SNA**, e depois dê um clique sobre **Visualizar/Alterar/Incluir**, dê um clique sobre o separador **Avançado** e selecione um novo valor para esta opção.

Capítulo 4. Como Planejar a Comunicação Cliente/Servidor

Este capítulo contém informações sobre o planejamento de clientes API de SNA para o Communications Server e Novell IntranetWare para SAA.

Clientes API de SNA

Essa seção contém informações específicas para clientes API de SNA.

Instalação e Configuração

Para obter informações sobre a instalação e configuração de clientes API de SNA do Communications Server, consulte o manual *Iniciação Rápida*.

Lightweight Directory Access Protocol

O Lightweight Directory Access Protocol (LDAP) fornece uma forma padrão para acessar serviços de diretório. O LDAP permite que você leia, pesquise, inclua e remova informações de bancos de dados centralizados ou remotos. O LDAP é semelhante ao Directory Access Protocol (DAP) X.500 mais antigo, mas sem algumas sobrecargas (como camadas de OSI de sessão e de apresentação). Você pode utilizar a **Configuração do Cliente LDAP** para configurar informações sobre o cliente API de SNA e armazená-las em um servidor LDAP.

A **Configuração do Cliente LDAP** mostra a organização lógica e a relação entre os clientes e suas configurações.

Para obter maiores informações sobre a utilização dessas áreas principais, consulte os painéis de auxílio da **Configuração do Cliente LDAP**.

Árvore de Informações de Diretório

A Árvore de Informações de Diretório (DIT) conecta todos os Agentes de Serviço de Diretório (DSAs) em um modelo predefinido. O modelo é uma estrutura hierárquica extensa que consiste em um número de objetos base. Um DIT de LDAP típico teria uma raiz, na qual **países** (c) são definidos. Abaixo dos países geralmente encontram-se **organizações** (o), e abaixo da organização encontram-se **pessoas**, ((cn) ou (uid)) ou **unidades organizacionais** (ou). Por exemplo, uma entrada LDAP completamente distinta seria especificada como:

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

Hierarquia do Cliente

A hierarquia do cliente é relativa ao DIT do LDAP onde a sessão foi iniciada. Você pode incluir usuários ou unidades organizacionais na hierarquia do cliente ou eliminar usuários ou unidades organizacionais da hierarquia do cliente.

Como Planejar a Comunicação Cliente e Servidor

Hierarquia de Configuração

A hierarquia de configuração é mostrada logicamente, através de exibição em árvore gráfica, configuração do cliente e de todas as relações entre as definições de configuração. A hierarquia de configuração permite que você crie, modifique ou remova definições.

Cliente API Comum para Communications Server para Windows NT e IntranetWare para SAA

O cliente fornecido com o Communications Server permite aos clientes localizar e acessar os servidores IBM Communications Servers e IntranetWare para SAA (IWSAA) na rede.

Opções de Instalação para a Localização de Configuração

Durante a instalação do cliente, o usuário pode escolher a localização da configuração do cliente. Há três opções:

- Configuração do arquivo INI, que é o método utilizado com as versões anteriores do Communications Server e é o método padrão ao instalar o cliente API de SNA incluído no Communications Server
- Netware Directory Services (NDS), que é o método utilizado com as versões anteriores do IWSAA e é o método padrão ao instalar o cliente API de SNA incluído no IntranetWare for SAA
- Lightweight Directory Access Protocol (LDAP)

A localização da configuração contém listas do servidor, nomes de usuário e todas as outras informações de configuração do cliente.

Localizações de Configuração

Como as informações de configuração são independentes do tipo de servidor (Communication Server para Windows NT ou IntranetWare para SAA), as informações podem ser armazenadas no NDS, INI ou LDAP. Por exemplo, os nomes e endereços do Communication Servers podem ser armazenados no NDS, INI ou LDAP para o cliente API. Como os programas de administração NDS são fornecidos somente com o IntranetWare para SAA, as informações de configuração do cliente API de SNA exigem que o produto IntranetWare para SAA esteja na rede. O recurso Cliente de API de SNA permite que você integre facilmente diferentes tipos de servidor na mesma rede.

Utilitário de Configuração

Use o utilitário **Definir Opções de Configuração**, para alterar a localização da configuração do cliente (INI, NDS ou LDAP) após a instalação.

Como Localizar Servidores

O cliente permite que o usuário localize e acesse os servidores IBM Communications Servers e IWSAA utilizando os protocolos de transporte TCP/IP e SPX.

TCP/IP: O método utilizado para localizar servidores através do protocolo de transporte TCP/IP é idêntico. O administrador da rede pode controlar o acesso aos servidores através da configuração do servidor. Consulte "Planejamento para Escopos TCP/IP" na página 142 para obter mais informações.

Como Planejar a Comunicação Cliente e Servidor

SPX: Os métodos utilizados para localizar servidores através do protocolo de transporte SPX são diferentes. Localizar servidores IBM Communications Servers e IWSAA leva mais tempo do que localizar somente servidores IBM Communications Servers ou IWSAA.

O cliente API de SNA do Communications Server tenta localizar os servidores IBM Communication Servers primeiro e, em seguida, os servidores IWSAA. Se não houver nenhum servidor IWSAA na rede ou se não puderem ser acessados, o usuário poderá definir uma variável de ambiente para evitar a localização de servidores IWSAA. Definir a variável melhora o desempenho em um ambiente em que somente IBM Communication Servers são acessados pelo protocolo de transporte SPX. A variável de ambiente é `SNA_API_CLIENT_NO_CC`. A definição da variável não afeta a localização do servidor utilizando o protocolo de transporte TCP/IP.

Como Atribuir uma LU Local Padrão

Você pode atribuir um alias de LU local padrão para cada usuário através da configuração do arquivo INI ou da configuração LDAP para clientes API de SNA do Windows de 32 bits.

Os programas APPC podem utilizar um alias de LU local padrão, em vez de especificarem um diretamente. Quando um programa APPC emite um verbo `TP_START` com o campo alias de LU local definido como zeros binários ou todos os espaços em branco do ASCII, a API do APPC utiliza o alias de LU local padrão configurado.

Os programas EHNAPPC podem utilizar um alias de LU local padrão, em vez de especificar um diretamente. Quando o campo de LU local no painel de configuração do AS/400 é deixado em branco, o alias de LU local padrão configurado é utilizado.

Os programas CPI-C podem utilizar um alias de LU local padrão, em vez de especificarem um diretamente. Quando o campo de alias de LU local no registro do lado CPI-C é deixado em branco e nenhum valor for definido utilizando a variável de ambiente `APPCLLU`, a API do CPI-C utiliza o alias de LU local padrão configurado ao iniciar uma comunicação.

Os programas Attach Manager podem utilizar um alias de LU local padrão, em vez de especificarem um diretamente. Quando o campo de alias de LU local no registro do gerenciador de fixação é deixado em branco, o Attach Manager utiliza o alias de LU local padrão configurado ao processar pedidos de entrada de conversação.

Como Atribuir uma LU Parceira Padrão

Você pode atribuir um alias de LU parceira padrão para cada usuário através da configuração do arquivo INI ou da configuração LDAP para clientes API de SNA do Windows de 32 bits.

Os programas APPC podem utilizar um alias de LU parceira padrão, em vez de especificarem um diretamente. Quando um programa APPC emite um verbo `ALLOCATE` com o campo de alias de LU parceira e o campo de LU parceira

Como Planejar a Comunicação Cliente e Servidor

completamente qualificado definido como zeros binários ou todos os espaços em branco do ASCII, a API do APPC utiliza o alias de LU parceira padrão configurado.

Os programas CPI-C podem utilizar um alias de LU parceira padrão, em vez de especificarem um diretamente. Quando o campo de alias de LU parceira no registro do gerenciador do lado do CPI-C é deixado em branco, a API do CPI-C utiliza o alias de LU parceira padrão configurado ao inicializar uma conversa.

Como Atribuir um Nome de Sessão LUA Padrão

Você pode atribuir um alias de LU parceira padrão para cada usuário através da configuração do arquivo INI ou da configuração LDAP para clientes API de SNA do Windows de 32 bits.

Os programas LUA, como emuladores 3270, podem utilizar um nome de sessão LUA padrão em vez de especificarem um diretamente. Quando um programa LUA emite um verbo RUI_INIT ou SLI_OPEN com o campo de nome de LU de LUA definido como zeros binários ou todos os espaços em branco ASCII, a API de RUI/SLI utiliza o nome da sessão LUA padrão configurado.

Criptografia de Dados do Cliente/Servidor

A criptografia de dados do cliente/servidor permite que o cliente solicite a criptografia de dados da aplicação em comunicações entre o cliente API de SNA e o Communications Server.

A criptografia de dados pode ser ativada, desativada ou opcional. A criptografia de dados opcional significa que a criptografia é utilizada se for suportada pelo servidor.

Segurança do Client Server

O Communications Server permite que clientes API de SNA do Windows 95 e do Windows NT utilizem a segurança de domínio do Windows NT, para autenticar a conexão do cliente como servidor sem digitar novamente o ID do usuário e a senha. O cliente deve ser parte de um domínio do Windows NT, pela participação em um domínio do Communications Server ou pela iniciação de sessão localmente com um ID de usuário e senha sincronizados.

Os usuários do cliente API de SNA fora do domínio do Windows NT são requeridos para fornecerem o ID de usuário e senha, através de um prompt ou através do armazenamento de valores no arquivo de configuração do cliente.

Os usuários autorizados do servidor cliente são mantidos no grupo local IBMCSADMIN, que está localizado diretamente no Communications Server ou no controlador de domínio onde participa o Communications Server. Esse grupo de usuário é criado durante a instalação e pode ser administrado utilizando o aplicativo Gerenciador de Usuário do Windows NT.

Você pode determinar se o ID do usuário e senha são requeridos para a conexão ao servidor através da alteração da entrada de valor **LogonControl** no servidor para zero (0), que remove a necessidade de especificação de ID de usuário e senha pelo cliente.

Como Planejar a Comunicação Cliente e Servidor

Os registros de trilha de auditoria de conexões do cliente ao servidor são rastreados no Registro de Eventos do Windows NT. Você pode visualizar os registros utilizando o Visualizador de Eventos do Windows NT no registro **Aplicação**. Se você não desejar rastrear conexões do cliente com o servidor, você poderá alterar a entrada de valor **AuditTrail** no servidor para zero (0).

Você pode acessar as entradas de valor **LogonControl** e **AuditTrail** através do Editor de Registros do Windows NT na chave:
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/IBM SNA Client Services.

Clientes Novell IntranetWare para SAA

O Communications Server suporta clientes conectados ao IPX ou TCP/IP que executam pacotes de software do emulador, que implementam a arquitetura Queue Element/Message Unit (QEL/MU) da Novell para emulação 3270, permitindo que os clientes acessem dados do sistema central mainframe. Isto inclui o suporte aos recursos comuns do cliente, incluindo categorias de LUs dedicadas, agrupadas e públicas (às vezes referidos como tipos de recurso).

O Communications Server suporta clientes Novell IntranetWare para SAA no Windows 95, Windows NT, Windows 3.1 e OS/2.

TCP/IP, IPX/SPX ou ambos são requeridos para clientes Novell IntranetWare para SAA comunicarem-se com o Communications Server. Se você estiver executando o IPX, também precisará ativar os seguintes softwares no servidor:

- Gateway Service para Netware
- Agente SAP
- NWLink IPX/SPX ou transporte compatível

Se o Communications Server estiver sendo executado em um controlador principal ou de reserva, devem ser concedidos aos usuários direitos no grupo IBMCSAPI, para iniciarem sessão localmente no servidor.

Capítulo 5. Como Planejar o Legacy Data Access

Este capítulo contém informações sobre as funções dentro do Communications Server que permitem acessar informações do sistema central.

Provedor OLE DB do AS/400

As aplicações que utilizam OLE DB ou ActiveX, podem se comunicar através do Communications Server para obter acesso ao nível de registro em arquivos do AS/400. O acesso a arquivos do AS/400 requer que você defina o AS/400 remoto, onde os arquivos são armazenados, como uma LU parceira.

O Provedor AS/400 OLE DB pode ser instalado como um componente do Communications Server ou como um componente do cliente API do SNA para Windows 95. Ele também pode ser instalado como um componente do cliente API do SNA para Windows NT. Portanto, ele requer Estação de Trabalho do Windows NT ou Servidor 4.0 ou posterior. Se você não tiver o Microsoft Data Access Components (MDAC) Versão 1.5 instalado, o Communications Server irá instalá-lo, quando você instalar esse componente.

Se o Provedor AS/400 OLE DB foi instalado em uma máquina que já possui o Client Access Versão 3 Release 2 MD (ou inferior) instalado, alguma função do Client Access será desativada, incluindo suporte a programas ActiveX e OLE DB que utilizam o Client Access para obter acesso a filas de dados do AS/400, comandos remotos, chamadas de programas remotos, procedimentos armazenados e instruções SQL.

Se quiser continuar utilizando essas funções através do Client Access, não instale o componente do Provedor AS/400 OLE DB durante a instalação do Communications Server. Se você instalar o componente do Provedor AS/400 OLE DB durante a instalação do Communications Server e se desejar recuperar as funções do Client Access, será preciso reinstalar o Client Access. Entretanto, se reinstalar o Client Access, você não poderá utilizar o Provedor AS/400 OLE DB com o Communications Server.

Quando Client Access é instalado após o Communications Server, as informações sobre registros são sobrepostas. Se desejar utilizar o Provedor AS/400 OLE DB com o Communications Server após o Client Access ser instalado, você poderá executar a ferramenta REGSVR32.EXE contra os arquivos cwbzzodb.dll e cwbzzidx.dll para restaurar as informações de registros do Provedor AS/400 OLE DB.

Você pode utilizar o Provedor AS/400 OLE DB para conectar clientes Windows 95 e Windows NT 4.0 através do Communications Server a um ou mais AS/400s, conforme mostrado na Figura 27 na página 100. Essa configuração concede acesso a clientes que têm o Provedor AS/400 OLE DB instalado, a registros específicos aos arquivos do AS/400.

Como Planejar o Legacy Data Access

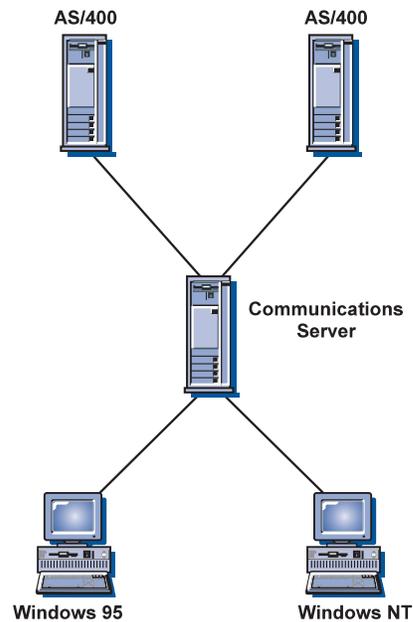


Figura 27. Provedor AS/400 OLE DB

Nessa figura, ambos os clientes têm o Provedor AS/400 OLE DB instalado. Alternativamente, você pode instalar e utilizar a função do servidor.

A documentação para essa função, bem como as informações o desenvolvimento dessas aplicações OLE DB e ActiveX que utilizam o Client Access, é fornecida no diretório `csnt\sdk\as400_oladb`.

Servidor de Pasta Compartilhada do AS/400

Você pode criar unidades de disco no servidor que se comunicam com pastas do AS/400 através do AS/400 Integrated File System (IFS). Se o servidor compartilhar essas unidades de disco, os clientes poderão conectar e utilizar essas unidades para obterem acesso às unidades do AS/400 sem configuração adicional ou instalação de código na máquina cliente. Vários clientes podem se conectar às pastas do sistema AS/400 como se elas fossem unidades em suas estações de trabalho.

Pode-se ativar o suporte da pasta compartilhada através da aplicação **Nó de Configuração**. Quando um dispositivo de disco estiver disponível para o usuário, ele age como uma unidade de disco suportado pelo sistema. Utilize as interfaces fornecidos pelo Windows NT para controlar o dispositivo. O usuários podem compartilhar a unidade pela rede, porém mantendo os direitos de acesso individuais.

O servidor de pasta compartilhada do AS/400 requer OS/400 Versão 3.1 ou superior.

Host Publisher

O Host Publisher fornece acesso através da Web a sites na Web de alto volume com conteúdo dinâmico. Você pode utilizar o Host Publisher, para acessar dados em sistemas centrais S/390 ou AS/400 e para publicá-los em páginas na Web criadas dinamicamente a partir do projeto.

O Host Publisher é composto de vários componentes. Para obter detalhes dos componentes e informações sobre instalação do Host Publisher, consulte *Iniciação Rápida* online.

Três valores de registros ativam o controle baseado em registro sobre a utilização de qualquer JIT atual e um caminho de classe específico para o Host Publisher. Implementações de Java, potencialmente incompatíveis podem existir na mesma máquina que o Host Publisher.

JITCompiler

Esse valor indica o nome do compilador JIT a ser utilizado no exemplo do Host Publisher do VM. Ele define a propriedade do sistema **java.compiler** que orienta a forma como o VM carrega e utiliza os JITs.

EnableJIT

Esse valor Booleano indica se o JIT especificado pelo **JITCompiler** é utilizado.

Classpath

Esse valor indica o caminho da classe especificado para o VM. Se o valor não for especificado ou, se for nulo, a variável de ambiente do sistema é utilizada.

Você pode acessar as entradas de valor **JITCompiler**, **EnableJIT** e **Classpath** através do Editor de Registros do Windows NT na chave:
HKEY_LOCAL_MACHINE/Software/IBM/Host Publisher/Config.

Se o Java VM for iniciado na inicialização do Host Publisher, o PageServer e o Integrator devem ser reinicializados para que as alterações nos registros se efetivem.

Processamento de Página na Web

Após criar uma biblioteca da Web utilizando o **Integrator**, você deve implementar a biblioteca para que clientes possam utilizar um navegador Web para visualizar a biblioteca na Web.

Quando um cliente dá um clique sobre um botão na sua página da Web, um pedido é enviado do sistema do cliente para um servidor Web. O servidor Web entra em contato com a **Placa**, que identifica se o pedido está associado a uma página na Web dinâmica, existente como um arquivo da biblioteca da Web em uma máquina de rede que contém um **PageServer**.

O **Despachador** determina qual **PageServer** deve atender o pedido e a **Placa** direciona o pedido para o **PageServer** recomendado.

O **PageServer** localiza a página em uma das bibliotecas e começa a processá-la. Ele varre o arquivo procurando por marcações DYNA.

Como Planejar o Legacy Data Access

- Se as marcações DYNA forem encontradas, o **PageServer** procura a biblioteca da Web para identificar a localização de objetos de integração associados às marcações DYNA e processa os comandos para extrair o conteúdo dinâmico. O **PageServer** resolve quaisquer scripts do lado do servidor encontrados na página, substitui as marcações DYNA por marcações HTML que incluem as informações extraídas da origem e retorna a página para a **Placa**.
- Se nenhuma marcação DYNA for encontrada, o **PageServer** cria um arquivo e o envia à **Placa**.

A **Placa** envia a página para o servidor Web, que encaminha a página para a máquina do cliente.

Configurações do Host Publisher

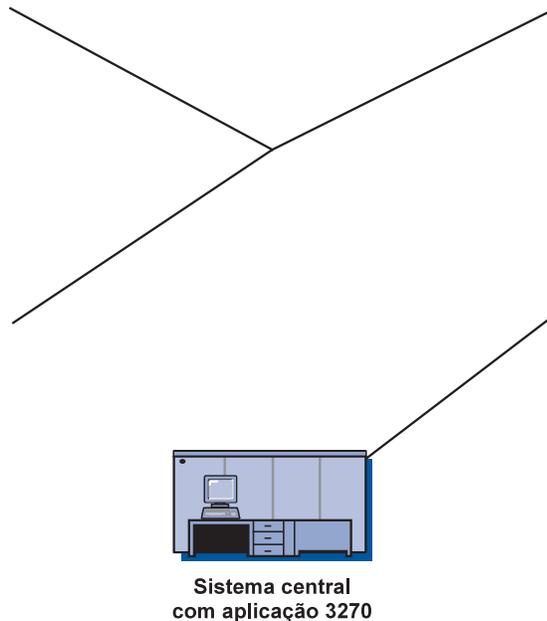
Você pode instalar várias configurações do Host Publisher, dependendo de fatores como a energia das máquinas e o desempenho de acesso à origem dos dados.

Para obter uma configuração básica, o servidor Web, **PageServer**, **Placa**, **Despachador** encontram-se todos na mesma máquina.

Para obter uma configuração estendida, você deve ter um servidor Web independente, múltiplos **PageServers** independentes e o **Despachador** deve estar na mesma máquina que o **PageServer** ou o servidor Web.

Para obter uma configuração excelente, você deve ter um servidor Web independente, múltiplos **PageServers** independentes, um **Despachador** principal independente e um **Despachador** secundário independente.

A Figura 28 na página 103 mostra um exemplo de como utilizar um navegador Web com o Host Publisher, para acessar informações de uma aplicação 3270 em um sistema central.



Configuração para Aplicações de Alta Disponibilidade

Você poderá facilmente estender seu site na Web, se o volume de atividade aumentar. Para garantir que clientes trabalhem em um ambiente tolerante à falha, o Host Publisher permite que você configure o **Despachador** para continuar operando com componentes de reserva.

O **Despachador** pode ser configurado para ter as instâncias principais e secundárias. Se o **Despachador** principal falhar por qualquer motivo, a **Placa** e os **PageServers** tentam imediatamente conectar-se ao **Despachador** secundário. Cada **Despachador** pode suportar múltiplos servidores Web.

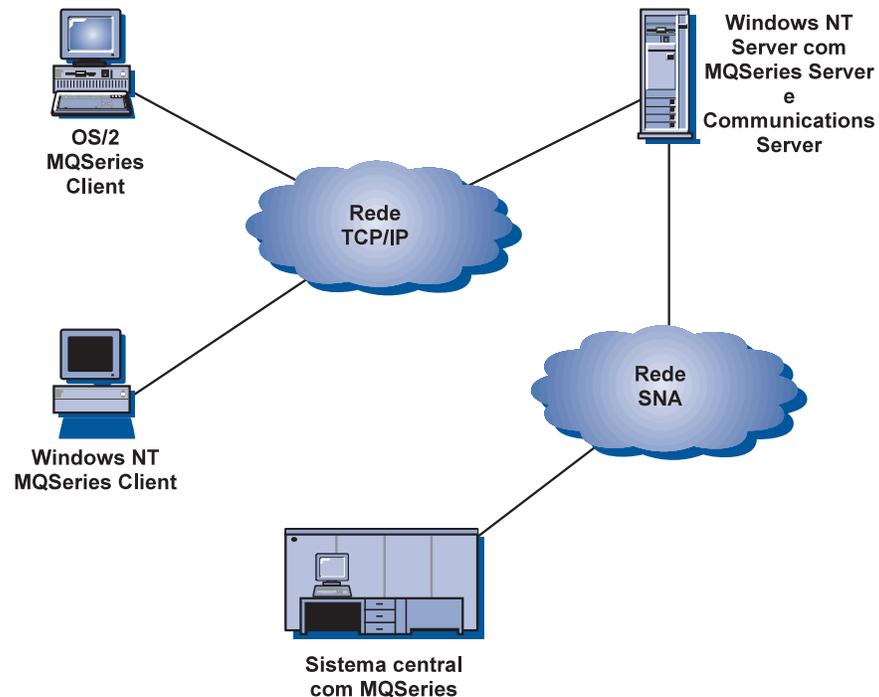
Você pode replicar as bibliotecas do Host Publisher em múltiplos **PageServers**. O **Despachador** funciona com os **PageServers** para executar o balanceamento de carga e alocação de recursos. Os pedidos do cliente são enviados para o **PageServer** com a maioria dos recursos disponíveis. Os **PageServers** adicionais podem ser iniciados com o aumento de pedidos de clientes.

Acesso de Clientes aos Sistemas Centrais do CICS

O software CICS client para Windows NT é fornecido com o Communications Server, permitindo que clientes conectem-se aos sistemas centrais do CICS através do Communications Server.

A Figura 29 na página 104 mostra um exemplo de como configurar um cliente CICS, para acessar informações em um banco de dados do CICS em um sistema central.





Para obter maiores informações sobre a configuração de clientes MQ, consulte *MQSeries Intercommunication Administration*. Esse manual encontra-se disponível na seguinte localização na Internet:

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

Acesso de Clientes aos Sistemas Centrais do DB2

O Communications Server inclui o software “try and buy” para DB2 Connect Enterprise Edition, um produto de conectividade de múltiplos usuários ao sistema central. Você pode instalar o DB2 Connect Enterprise Edition em um servidor Windows NT.

O Communications Server também inclui o DB2 Client Application Enabler (CAE), que possibilita acesso do cliente ao sistema central. Você pode instalar o CAE do DB2 em uma máquina cliente que executa o Windows 3.1, Windows 95, Windows NT ou OS/2.

A Figura 31 na página 106 mostra um exemplo de como você pode configurar o DB2 Connect Enterprise Edition para acessar informações em um banco de dados DB2 em um sistema central.

Como Planejar o Legacy Data Access

Figura 31. Ambiente do DB2 Connect Enterprise Edition

Capítulo 6. Como Planejar o HPR

O Communications Server suporta high performance routing (HPR) sobre Enterprise Extender (IP), controle de ligação síncrona de dados (SDLC), LAN, WAN, canal, Multi-Path Channel (MPC) e conexões X.25.

O roteamento de rede automático (ANR) HPR minimiza os requisitos de armazenamento e processamento nos nós intermediários, que é uma melhoria sobre o roteamento intermediária de sessões (ISR) para redes de alta velocidade com pouca margem de erro.

O suporte do Communications Server HPR inclui suporte para o protocolo de transporte rápido (RTP) e roteamento de rede automático (ANR).

Características de Ligação HPR

Para oferecer os benefícios listados acima, o HPR assume que as ligações de dados oferecem baixos índices de quadros perdidos. O HPR recupera-se de condições que causam quadros perdidos, mas se as condições persistem por períodos longos, o HPR assume que a congestão da rede está muito alta e a taxa de rendimento do HPR é reduzida. Um boa taxa de rendimento do HPR em uma dada ligação envolve uma configuração adequada do nó remetente, os recursos que constituem a ligação entre os dois nós, e o nó de recepção.

Nota: Talvez queira definir os valores ERP em casos onde os recursos da linha da rede local que tenham um alto índice de perda de estrutura.

Nó Remetente

Placas típicas utilizadas com o HPR enviam quadros na linha com baixos índices de falha. Para Ethernets, o comportamento do HPR será degradado caso a rede ampla estiver excessivamente carregada com muitas colisões (por exemplo, se a carga for maior do que aproximadamente 30% a 40% da velocidade nominal Ethernet). Para retransmissão de quadros, os recursos devem ser configurados de maneira que as conexões individuais possam estourar a taxa da linha de acesso sem provocar condições de congestionamento na rede de transmissão de quadros.

Recursos de Linha

Os recursos de rede ampla que têm uma substancial complexidade oculta, desde grandes números de estações compartilhando um único segmento da rede ampla a pontes entre segmentos da rede ampla, talvez com ligações ocultas de velocidade reduzida, a segmentos de rede ampla simulados que operem através de sub-redes complexas. O pressuposto da baixa perda de estrutura deverá ser atendido. Por exemplo, as ligações WAN entre pontes divididas deverão utilizar recursos com baixos índices de erro ou deverão compensar utilizando recuperação de erro ao nível de ligação entre as pontes. Como outro exemplo, as condições que provocam a sobreexecução dos buffers de ponte (tempestades de difusão ou grandes rajadas de quadros difundidos) deverão ser evitadas

Como Planejar o HPR

Nó Receptor

Placas típicas utilizadas com o HPR receberão quadros da linha com um baixo índice de falhas. Algumas placas, no entanto, não irão conseguir receber quadros quando quadros consecutivos chegarem muito rapidamente. O melhor desempenho é realizado quando a placa de recepção pode comportar seu tráfego sem perder quadros de entrada.

Se sua rede tiver um alto índice de erro, os administradores de sistemas podem perceber taxas de rendimento menores do que o esperado em conexões HPR.

Considerações HPR

Os dispositivos HPR são obtidos incluindo informações adicionais nos cabeçalhos dos quadros. Caso não precisar dos dispositivos HPR, a sobrecarga adicional poderá reduzir o desempenho da sua rede. Os recursos HPR são uma vantagem toda vez que houver nós intermediários e rotas alternativas. Entretanto, caso precisar alto desempenho entre dois nós conectados por uma única ligação sem recuperação sem interrupção durante uma falha na ligação, o HPR deverá ser desativado quando a ligação for configurada.

fila de prioridades dos implementos HPR. Em geral, o tráfego interativo passa rede mais rapidamente do que tráfego em lote de prioridade menor. Placas que colocam quadros em fila o fazem sem considerar a prioridade e podem interferir com a fila de prioridade do HPR. Talvez seja necessário reduzir o comprimento da fila da placa para evitar que o tráfego de baixa prioridade atrase o tráfego de alta prioridade. (Consulte a documentação da placa para instruções sobre como definir o comprimento da fila da placa).

Muitos PCs têm hoje recursos de gerenciamento avançado de energia que irão suspender a energia para dispositivos (como unidades de disco) e reduzir de forma significativa a taxa de clock em uma CPU para poupar energia caso o teclado ou o mouse não estiverem sendo utilizados. Em uma estação de trabalho, isto é um bom recurso, mas em uma plataforma de servidor, isto pode ocorrer enquanto estiver roteando dados de uma placa para outra (e nenhuma atividade de disco estiver ocorrendo). Para o Communications Server, desative o gerenciamento avançado de energia e o gerenciamento de energia de hardware digitando a configuração BIOS durante a inicialização (normalmente pressionando F1 ao inicializar o hardware) e desative estas opções.

O HPR irá utilizar mais memória da placa da rede ampla devido ao aumento de desempenho e da fila. Muitas placas RAM compartilhadas reverterem para o padrão de 8 kilobytes de memória compartilhada RAM. É necessário que o tamanho do RAM compartilhado seja 16 kilobytes. Para ajustar esta configuração, consulte o manual de configuração da placa. Esta definição está localizada na sua máquina BIOS, ou nas definições do comutador da placa.

Nota: Caso não seja aumentado o RAM compartilhado para 16 kilobytes, o desempenho da rede fica comprometido.

Não ajuste o valor RAM compartilhado acima de 16 kilobytes, que é a definição ótima para a memória da placa.

Caso as ligações HPR estejam falhando sob tráfego pesado, pode-se definir os temporizadores de recepção para um valor maior. Isto dá mais tempo para que as ligações possam receber um reconhecimento para quadros enviados.

Para ligações SDLC, esta é o Temporizador de Recepção Primário. O temporizador de recepção pode ser definido por DLC ou por uma instrução de ligação lógica.

Para calcular o valor mínimo do temporizador de recepção em décimos de segundo, utilize a seguinte fórmula:

$$[(\text{enviar_contagem_janela} * \text{tam_max_campo_i} * 8) / \text{velocidade linha atual}] * 10$$

Considerações para Sintonização de Parâmetros em DLCs da Rede Local

Pode-se especificar cinco parâmetros que afetam a velocidade com a qual o Communications Server lida com a recuperação e falhas nas ligações da Rede Local. Talvez seja preciso ajustar esses parâmetros para obter os melhores resultados caso esteja utilizando ligações lentas, HPR ou conexões ao sistema central de reserva.

Você deve considerar os seguintes parâmetros, ao definir um dispositivo de rede local na **Configuração do Nó**:

No separador **Avançado**:

Intervalo de repetição de teste

O intervalo de repetição do teste especifica o tempo entre as tentativas para encontrar a estação de ligação adjacente da rede local (LAN). O número de tentativas feitas baseia-se no valor especificado para o limite de repetição do teste.

O valor padrão é 8.

Limite de repetição do teste

O limite de repetição do teste especifica o número máximo de tentativas para encontrar a estação de ligação adjacente da rede local (LAN), sem receber uma confirmação no tempo definido pelo valor do intervalo de repetição do teste.

O valor padrão é 5.

Tamanho máximo de PIU

O tamanho máximo da unidade de informações de caminho (PIU) é o número máximo de bytes que estão contidos no buffer de dados utilizado em sessões SNA para essa ligação. Se o valor do tamanho máximo da PIU exceder o tamanho da estrutura suportado pelo controlador de dispositivo local, o valor será reduzido para corresponder ao tamanho da estrutura.

O valor padrão é 65535.

No separador **Desempenho**:

Tempo de espera inativo

O tempo de espera inativo especifica o tempo que o controlador de dispositivo da rede local aguarda, para que uma estrutura seja recebida antes de confirmar que a ligação está inativa.

O valor padrão é 30 segundos.

Como Planejar o HPR

Atraso na confirmação

O atraso na confirmação especifica o tempo que o dispositivo da rede local retém uma resposta para uma estrutura recebida, para permitir que mais estruturas sejam recebidas e confirmadas com o mesmo Pronto para Receber (RR).

O valor padrão é 100 milissegundos.

Tempo de espera da resposta de chamada seletiva

O tempo de espera de resposta da chamada seletiva especifica o tempo que o dispositivo da rede local aguarda por uma resposta a uma estrutura enviada com o conjunto de bits POLL.

O valor padrão é 8000 milissegundos.

Transmissões pendentes antecipadas

As transmissões pendentes antecipadas especificam o número máximo de estruturas enfileiradas pelo dispositivo da rede local, para uma estação de ligação antes de enviar um Não Está Pronto para Receber (RNR) para a estação de ligação adjacente.

O valor padrão é 16 estruturas.

Contagem do buffer de recepção

A contagem de buffers de recepção especifica o número de buffers reservados na memória, para reter dados recebidos do sistema central até que possam ser processados. Cada buffer é do tamanho da PIU.

O valor padrão é 32 buffers.

Processamento de Comutação de Caminhos do HPR

O HPR fornece uma comutação de caminhos sem interrupção para uma conexão diferente se uma conexão falhar. Uma repetição da conexão falha é tentada antes que ocorra uma comutação de caminhos. Segue-se uma explicação dos parâmetros envolvidos na determinação da falha da conexão e o tempo para iniciar uma comutação de caminhos.

Quando o valor especificado para **Tempo de espera inativo** é atingido, uma estrutura "manter ativo" é enviada. O padrão para **Tempo de espera inativo** é 30 segundos.

O valor especificado para **Tempo de espera de resposta de chamada seletiva** determina o tempo que o dispositivo aguarda uma resposta para a estrutura "manter ativo". O padrão para **Tempo de espera de resposta de chamada seletiva** é de oito segundos (8 000 milissegundos). Uma estrutura "manter ativo" é repetida 10 vezes. Esse número de repetições não pode ser alterado.

Se não houver resposta para a estrutura "manter ativo", os comandos TEST serão enviados para o sistema parceiro. O valor especificado para **Intervalo de repetição de teste** determina o tempo entre tentativas do comando TEST e o valor especificado para **Limite de repetição do teste** determina o número máximo de tentativas do comando TEST. O padrão para **Intervalo de repetição do teste** é de 8 segundos e o padrão para **Limite de repetição do teste** é de cinco tentativas.

O cálculo a seguir indica o tempo necessário para determinar se uma conexão falhou e inicia uma comutação de caminhos:

$$(\text{Tempo de espera inativo}) + (\text{Tempo de espera de resposta de chamada seletiva} * 10 \text{ repetições}) + (\text{Intervalo de repetição do teste} * \text{Limite de repetição do teste}) + 1$$

Como Planejar o HPR

Ao utilizar os padrões para os parâmetros, o tempo requerido para determinar uma falha de conexão e iniciar uma comutação de caminhos pode ter até 151 segundos.

$$(30 \text{ segundos}) + (8 \text{ segundos} * 10 \text{ repetições}) + (8 \text{ segundos} * 5 \text{ tentativas}) + 1 = 151 \text{ segundos}$$

Caso estiver tendo tempos longos de comutação de caminhos (ou falhas) com o HPR quando falhar uma ligação, você pode reduzir o tempo diminuindo os valores dos parâmetros no cálculo.

Capítulo 7. Como Planejar o SNA Gateway

O SNA Gateway suporta:

- Diversos protocolos SNA
- Diversas estações de trabalho downstream
- Diversos tipos de ligação entre o gateway e o sistema central
- Conjuntos de LUs (sessões) no gateway
- Definição de estações de trabalho implícitas
- Alteração ou inclusão dinâmica de definições para estações de trabalho não-ativas
- Sistemas centrais múltiplos simultaneamente
- Diversos tipos de ligação (que podem ser combinadas) entre as estações de trabalho e o gateway

Consulte o *Iniciação Rápida* para instruções sobre como configurar o SNA Gateway utilizando a **Configuração de Nós**.

Conexões Suportadas para Estações de Trabalho

O SNA Gateway suporta estações de trabalho conectadas por:

- Conectividades rede local
 - Token ring
 - Ethernet
 - ATM (Emulação rede local)
- Retransmissão de estruturas
- SDLC
 - Assíncrono
 - Síncrono
 - Síncrono Automático Hayes
 - Multiponto Principal
- Rede X.25
- AnyNet TCP/IP (para conectividades suportadas pelo Microsoft TCP/IP)
- Conexões ISDN

O SNA Gateway pode suportar até 254 LUs para cada PU definida. Você pode definir uma PU diferente para cada uma das conexões do sistema central. As LUs são utilizadas por estações de trabalho downstream, para conectarem-se ao sistema central. O número de estações de trabalho downstream suportado depende de vários fatores, incluindo o tipo de conectividade e o número de placas no gateway. Por exemplo, se você tiver uma placa de rede local no gateway, uma ligação do sistema central com 254 LUs poderá ser utilizada por 253 estações de trabalho downstream simultaneamente. Com duas placas, você pode duplicar o número de estações de trabalho downstream.

Conexões SDLC de Estações de Trabalho

Pode-se optar por conectar utilizando o SDLC em configurações ponto a ponto e Multiponto. Após a conclusão da configuração, nenhuma consideração especial é necessária para executar o SDLC entre a estação de trabalho e o gateway.

Ao definir estações de trabalho secundários multiponto, considere os diversos fatores que controlam o tempo de resposta de chamada seletiva. Existem limitações físicas que afetam a rapidez em que o principal pode chamar seletivamente o secundário mais distante. A definição de todas as estações secundárias utilizando os mesmos parâmetros simplificará o cálculo a seguir.

Para calcular o tempo de inatividade mínima em segundos, utilize esta fórmula:

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

onde:

NS = Número de estações
SW = Tamanho da janela de envio
RW = Tamanho da janela de recepção
IS = Tamanho do campo-I
LS = Velocidade de impressão da linha (bps)

Se estes valores não forem iguais para todas as estações secundárias, um cálculo separado deverá ser feito para cada grupo ou estação de trabalho e estes devem ser somados para encontrar o valor correto para o temporizador de inatividade.

Por exemplo, para uma ligação multiponto com 16 estações de trabalho a 14,4 Kbps, com cada estação de trabalho definido para um tamanho de janela de envio de 7, um tamanho de janela de recepção de 7, um tamanho de campo-I de 521, o cálculo para o temporizador de inatividade seria:

$$16 * (7 + 7) * (521 + 2) / (14400 / 8) = 65,1 \text{ segundos}$$

Nota: Sempre adicionar alguns segundos a mais como buffer.

Conexões da Estação de Trabalho X.25

Se você configurar o SNA Gateway para utilizar somente conexões do circuito virtual permanente (PVC) X.25 entre o gateway e as estações de trabalho, recomenda-se configurar todas as estações de trabalho e gateway PVCs com funções de estação de ligação negociáveis. Se os PVCs do gateway e das estações de trabalho não forem configuradas com funções de estação de ligação negociáveis, as estações de trabalho talvez não consigam estabelecer as ligações PVC X.25 até o gateway.

Consulte o Capítulo 13. Como Planejar para X.25 para obter maiores informações sobre conexões PVC e sobre a configuração.

Conexões Suportadas para Estações de Trabalho

O SNA Gateway suporta as seguintes conexões a um sistema central:

- Conectividades rede local
 - Token ring
 - Ethernet
 - ATM (Emulação rede local)
- Retransmissão de estruturas

- SDLC
 - Síncrono
 - Síncrono Automático Hayes
- rede X.25
- Biaxial (para o AS/400)
- AnyNet TCP/IP (para conectividades suportadas pelo Microsoft TCP/IP)
- Enterprise Extender IP (para conectividades suportadas pelo Microsoft IP)
- Canal (CDLC)
- Canal (MPC) com uma conexão DLUR
- Conexões ISDN

Se existirem conexões para múltiplos sistemas centrais do gateway que está sendo utilizado pelo tráfego de LU dependente, somente a ligação do sistema central com o nome de PU do ponto de controle poderá executar os seguintes itens:

- Agir como ponto focal do sistema central
- Ter sessões CP-CP com o sistema central
- Ser utilizada para funções APPN

As ligações que estão definidas com um nome de PU que não seja igual ao nome do ponto de contato, podem ser utilizadas somente para conexões de LU dependente adicional para um sistema central.

Se uma ligação do sistema central gateway estiver definida como um ligação de recursos limitados, ela enviará uma solicitação de descontato ao sistema central após a desativação da última sessão LU-LU. Em seguida, o gateway passa os DACTLUs para a estação de trabalho e um DACTPU para a estação de trabalho que tenha sessões somente com essa ligação de sistema central. Quando a estação de trabalho conectada ao gateway é definida como um recurso limitado, a ligação da estação de trabalho será desconectada se não houver nenhuma outra sessão. No Communications Server você pode designar uma estação de trabalho como um recurso limitado, ao definir a conexão do cliente explícita.

Entretanto, se a estação de trabalho tiver uma aplicação (ou emulador) que reative automaticamente a ligação do sistema central, o gateway irá reativar a ligação do gateway para o sistema central, quando a estação de trabalho ativar sua ligação para o gateway. Isto significa que as definições de estação de trabalho incompatíveis certamente inibirá a função de recurso limitado no gateway.

Considerações sobre o Sistema Central

Considere os seguintes itens ao planejar a conexão do sistema central:

- Se seu ambiente utiliza um ponto de controle de rede (NCP), o valor da macro 37xx NCPGEN, **LINE**, **MAXLU** deverá ser pelo menos tão grande quanto o número das LUs no Communications Server.
- Os usuário do VTAM podem controlar o intervalo de tempo durante o qual o VTAM irá colocar os dados em buffer antes de enviá-los para o controlador (coattailing). Quando o parâmetro coattailing do VTAM **DELAY = 0** estiver especificado em qualquer definição PU, isto poderá dar um tempo de resposta de envio do sistema central maior exigindo mais trabalho para o processador do sistema central.

Quando um valor diferente de zero para DELAY for especificado, isto poupa instruções do processador do sistema central às custas do aumento do tempo de resposta de recepção na Communications Server estação de trabalho.

Para coattailing, comece com um valor padrão de 0,2. Um atraso de 0,2 segundos tem um efeito moderado no tempo de resposta, mas se taxa for aproximadamente uma transação por segundo ou maior, ocorre o coattailing.

- Embora cada estação de trabalho SNA downstream na Rede Local implemente uma PU com seu próprio conjunto de LUs, o SNA Gateway é implementado para que o sistema central veja somente a PU do gateway. Portanto, somente uma definição de PU é codificada no sistema central. Essa definição de PU contém as LUs para **todas** as estações na Rede Local que irá se conectar ao sistema central através desse gateway.

Se o VTAM do sistema central suportar as LUs dependentes de auto-definição (SDDL), você poderá tirar proveito da função. Ao configurar as LUs do sistema central, especifique um tipo de modelo de LU ou forneça um nome de modelo de LU que corresponda ao valor do operando LUSEED definido no nó principal comutado VTAM e utilizado pela rotina de saída do VTAM SDDL.

Configuração de Endereços de Destino na Rede Local

É necessário fornecer um endereço de destino se for utilizar uma das conexões de rede local suportadas entre o gateway e o sistema central ou entre o gateway e as estações de trabalho definidas explicitamente. Ao determinar o endereço de destino correto para digitar em cada perfil, lembre-se de que a perspectiva apropriada para ambos os endereços é visualizar o destino a partir do SNA Gateway. Figura 32 exibe este modo.

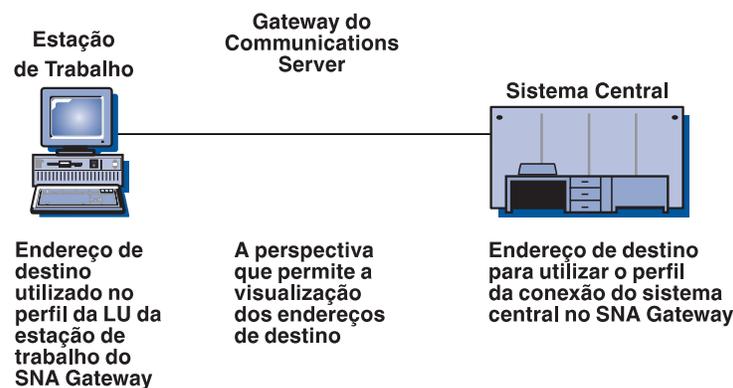


Figura 32. Perspectiva a ser Utilizada para Entradas de Endere" o de DestinoPlanejamento para o SNA Gatev

Como Planejar as Definições Gateway LU

O SNA Gateway suporta ambos as LUs de sistemas centrais **em conjunto** e LUs de sistemas centrais **dedicados**. Quando as LUs são configuradas para cada conexão do sistema central no SNA Gateway, elas podem ser agrupadas nos conjuntos. Frequentemente, a criação de conjuntos é benéfica pelas seguintes razões:

- Se todas as sessões em todas as estações de trabalho não precisarem se comunicar com o sistema central ao mesmo tempo, o conjunto poderá conservar recursos do sistema. As sessões de estação de trabalho na rede local podem compartilhar as mesmas LUs, mas não ao mesmo tempo. Esta função permite que o número de LUs configurado no SNA Gateway para sessões de estação de

Planejamento para o SNA Gateway

trabalho seja maior do que o número de LUs configurado entre o sistema central e o gateway, reduzindo os requisitos de recursos do sistema central, reduzindo a definição da estação de trabalho do sistema central e acelerando os reinícios.

- Os conjuntos são mais fáceis de administrar e configurar. Você pode ajustar o tamanho do conjunto incluindo mais LUs nele ou eliminando LUs dele, sem afetar outras definições.

As LUs em conjunto não são dedicadas a nenhuma estação de trabalho específica, nem precisam ser dedicadas para uso somente por usuários do gateway downstream. Um único conjunto pode ser compartilhado por usuários do TN3270 downstream e por estações de trabalho do SNA Gateway, bem como clientes API de SNA e por sessões do emulador local. Se desejar configurar um conjunto (por exemplo, PUBLIC) para todas as utilizações de LUs dependentes, você não precisará saber como os usuários serão distribuídos através desses tipos.

- Os conjuntos poderão fornecer melhor disponibilidade para as estações de trabalho downstream, se você definir LUs de múltiplas conexões no mesmo conjunto. Se uma das conexões estiver ativada e a outra não, os usuários poderão acessar as LUs na ligação ativa.

Considere os seguintes cenários:

- O Communications Server possui duas conexões do sistema central com 100 LUs definidas em cada conexão, todas pertencendo ao conjunto A. A primeira ligação é configurada como *ativar na inicialização* e é operacional. Todas as estações de trabalho estão utilizando essa ligação com as LUs. A segunda ligação está configurada como *auto-ativar*. Essa combinação de conjuntos com a configuração de ligação pode fornecer melhor disponibilidade de duas formas. Se a primeira ligação falhar, as sessões dependentes de recuperação ativarão automaticamente a segunda ligação. Se a primeira ligação esvaziar as LUs definidas, a ligação de reserva será automaticamente ativada quando a próxima LU (a 101ª) for requerida.
- Você também pode utilizar a combinação de conjuntos e configuração de ligação para fornecer o balanceamento de carga para estações de trabalho downstream através de conexões do sistema central disponíveis. Um exemplo disso é para o Communications Server que tem duas conexões do sistema central com 100 LUs definidas em cada conexão, todas pertencentes ao conjunto A. Ambas as ligações são configuradas como *ativar na inicialização* e são operacionais. As estações de trabalho que são mapeadas para o conjunto de LUs, serão distribuídas através de ambas conexões para compartilharem a carga através delas.

O SNA Gateway atribui LUs em conjunto a sessões da estação de trabalho, quando a estação de trabalho downstream conecta-se ao gateway. As sessões da estação de trabalho podem ser definidas para utilizarem LUs em sistemas centrais diferentes em LUs dedicadas ou em conjunto.

As LUs dedicadas não pertencem a um conjunto. Uma LU dedicada pode ser configurada para uso por um cliente definido explicitamente.

A Figura 33 na página 118 mostra uma configuração simples com estações de trabalho utilizando LUs dedicadas, LUs em conjunto ou ambos. (As linhas interligadas representam as LUs.)

Planejamento para o SNA Gateway

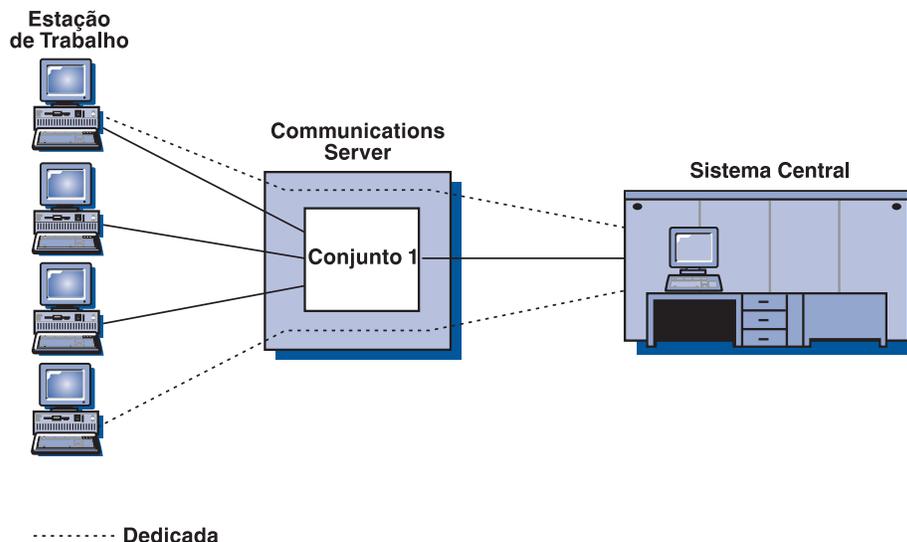


Figura 33. Um Cenário Simples Utilizando LUs Dedicadas e em Conjunto

Como Utilizar Conexões Explícitas e Implícitas

Existem dois tipos de estações de trabalho downstream suportados pelo gateway: explícita e implícita. Estações de trabalho explícitas são aquelas que têm endereços de destino definidos para um tipo específico de DLC (por exemplo, uma rede token-ring e SDLC). Para configurar estações de trabalho explícitas, deverão ser conhecidos o endereço de destino ou o nome do ponto de controle adjacente plenamente qualificado ou o ID do nó adjacente de cada estação de trabalho e também definir uma ligação lógica para o gateway para cada estação de trabalho. As LUs definidas para estações de trabalho explícitas podem ser agrupadas ou dedicadas.

As estações de trabalho implícitas são mais fáceis de configurar, mas só podem utilizar LUs em conjunto. Ao invés de definir uma ligação para cada estação de trabalho utilizando o gateway, defina um conjunto de LUs do sistema central (ou conjuntos) e configure os dispositivos (DLCs) utilizados pelas conexões à estação de trabalho. Configure um gabarito de cliente implícito a ser utilizado como um modelo para a definição de LU para cada estação de trabalho que é conectada ao gateway e que não corresponde a uma definição explícita. Por exemplo, se cada estação de trabalho em uma rede local Ethernet possuir duas sessões 3270 configuradas com endereços NAU 2 e 3, você irá configurar um gabarito de cliente com duas LUs (uma para o endereço 2 e uma para o endereço 3). Se ambos os endereços forem utilizados para um único sistema central, mapeie ambos os endereços para o mesmo conjunto de sistemas centrais. Entretanto, se o endereço 2 for utilizado para ir para o HOST_A e o endereço 3 for utilizado para ir para o HOST_B, mapeie cada um para o conjunto de sistemas centrais apropriados. Neste exemplo, toda vez que uma estação de trabalho que se conecta ao gateway através da Ethernet, a qual não corresponde a uma definição explícita, uma ligação será criada dinamicamente e as duas LUs para a NAU 2 e 3 serão alocadas no(s) conjunto(s) do sistema central.

Para estações de trabalho implícitas, os usuários conectando ao gateway necessitam saber que somente o endereço da placa do gateway DLC que estiver configurada

Planejamento para o SNA Gateway

para as estações de trabalho implícitas e quais valores NAU foram definidos no gateway. Eles deverão utilizar estes valores NAU ao definir suas sessões 3270 e impressoras lógicas.

Uma estação de trabalho downstream do Personal Communications que se conecta ao Communications Server pode utilizar a descoberta da rede local, pesquisando o nome do grupo IG02HOST, para localizar o endereço da placa.

Desempenho do SNA Gateway

O desempenho por qualquer gateway depende de muitos fatores, entre eles:

- A configuração do gateway
- A conexão ao sistema ou sistemas centrais
- Demanda geral de processamento para cada sistema central
- Conexões para as estações de trabalho suportadas
- Configurações das estações de trabalho suportadas
- Número de estações de trabalho suportadas
- Número de sessões com cada estação de trabalho
- prioridade de transmissão do SNA
- Controle do Fluxo
- Janela de controle de velocidade para todas as sessões
- Tráfego em sessões não-gateway

A utilização de uma estação de trabalho que implemente um gateway de software para outras funções pode comprometer o desempenho do gateway.

Se nenhum dos fatores mencionados anteriormente estiver causando um impacto negativo no desempenho, uma estação de trabalho individual utilizando protocolos suportados pela SNA não deverão sofrer qualquer diferença de desempenho notável entre uma conexão direta para o sistema central e uma conexão indireta por meio de uma rede local através de um SNA Gateway conectada ao sistema central. De fato, se as ligações do sistema central estiverem ativas no gateway, ativação da estação de trabalho poderá melhorar com a remoção do atraso da sobrecarga do sistema central. Entretanto, por causa das muitas variáveis envolvidas, talvez queira efetuar testes de desempenho em seu ambiente operacional para que se possa atingir o equilíbrio desejado entre função e desempenho.

Considerações da DLUR

Ao utilizar a DLUR para a conexão ao sistema central, você obtém flexibilidade de colocação do SNA Gateway. A conexão ao sistema central pode cruzar qualquer rede APPN e não é restrita por estar adjacente a um HOST/NCP. Um canal DLUR a DLUS é criado para o VTAM do DLUS que é utilizado para fluxos de controle de sessão dependentes.

A configuração recomendada para uma conexão do DLUR ao sistema central é definir o gateway para ser um nó de rede e configurar as informações sobre DLUS. Durante a configuração de clientes explícitos e implícitos, mapeie-os para a DLUS. Essa configuração é mais fácil porque ela não requer conhecimento das LUs downstream no gateway além de fornecer a visibilidade mais alta dos dispositivos downstream para VTAM, visto que o VTAM está ciente da PU.

Planejamento para o SNA Gateway

Se não desejar que o VTAM fique ciente das PUs downstream, você poderá configurar uma PU interna no gateway (em vez de uma conexão ao sistema central) e mapear as estações de trabalho downstream para essa PU interna.

Se uma estação de trabalho downstream, como Personal Communications, for sujeita a DLUR, você irá desejar que a estação de trabalho se direcione através do Communications Server utilizando o recurso de nó de rede em vez da função do SNA Gateway.

Capítulo 8. Como Planejar o Servidor TN3270E

A função do servidor TN3270E permite configurar sua rede conforme mostrado na Figura 34 ou Figura 35 na página 122.

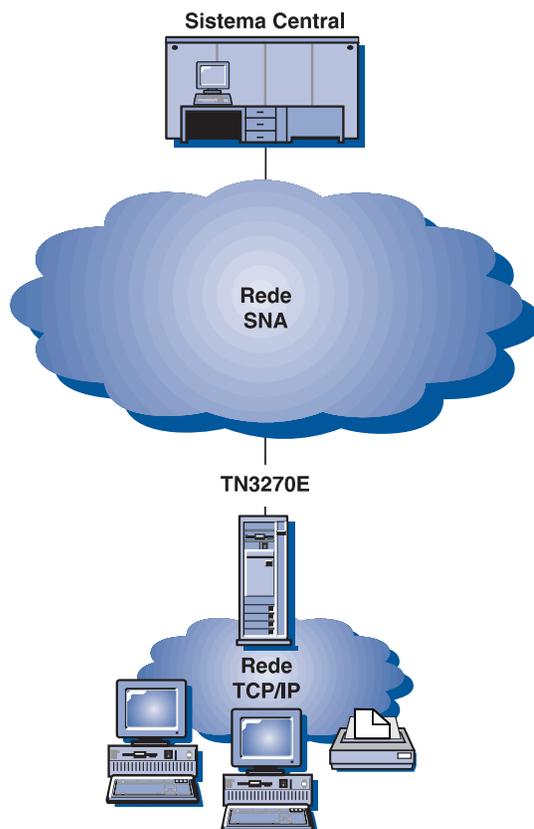
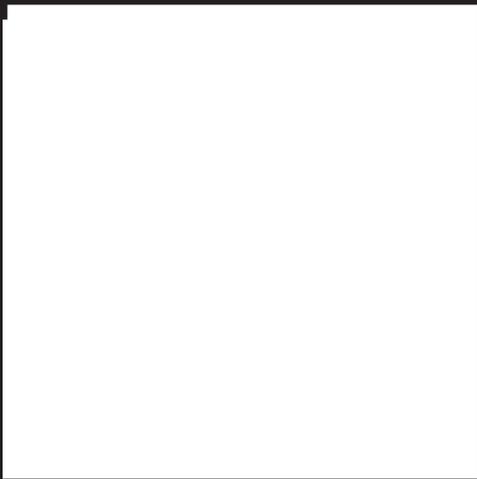


Figura 34. Communications Server configurado como um Servidor TN3270E com a Rede Ampla SNA



Como Planejar o Servidor TN3270E

permissão para se conectarem no servidor TN3270E e na especificação dos nomes de LU e conjuntos que podem ser acessados pelos clientes.

- Manuseio de respostas

Os clientes permitidos por TN3270E podem enviar respostas positivas e negativas, que o servidor TN3270E envia para o sistema central. O servidor TN3270E gera respostas de pedidos para clientes TN3270 padrão.

- Manuseio da Chave ATTN e SYSREQ

O servidor TN3270E pode converter e enviar informações para o sistema central quando o cliente envia uma tecla ATTN ou SYSREQ. Embora os clientes não permitidos pelo TN3270E não possuam definição explícita para ATTN e SYSREQ, o servidor TN3270E utiliza os seguintes comandos Telnet para implementar estas funções:

Tabela 6. Comandos Equivalentes

Telnet	TN3270E	TN3270 Padrão
IP	ATTN	SYSREQ
AO	SYSREQ	SYSREQ
BREAK	N/A	ATTN

- Classes de LU

O Communications Server classifica a conexão do usuário com as classes de LU. As classes consistem em LUs configuradas com características comuns, aquelas que requerem uma conexão específica ao sistema central, por exemplo. Isto simplifica o acesso do usuário, agrupa usuários por necessidades de aplicação e maximiza os recursos do sistema central.

- Segurança baseada em SSL (baseada em Secure Sockets Layer)

AS conexões entre clientes TN e o servidor TN3270E utiliza a Versão 3 do SSL para fornecer criptografia de dados e autenticação do servidor utilizando certificados assinados.

Consulte *Iniciação Rápida* para obter instruções sobre como configurar um servidor TN3270E.

Estações de Trabalho de Cliente Suportadas no Servidor TN3270E

O servidor TN3270E suporta qualquer cliente TN3270E ou TN3270 que esteja totalmente de acordo com o RFC 1576, 1646 ou o 1647.

Destaques

Esta seção fornece mais informações sobre alguns dos recursos que podem ser configurados para o servidor TN3270E.

Como Alterar o Número da Porta Padrão

Você pode configurar o número da porta utilizada pelo servidor, para novas conexões a partir da janela Opções do TN3270E. O número da porta padrão é 23, mas outras aplicações Telnet, como por exemplo, o suporte ao servidor TN5250, também podem utilizar esta porta. Se outras aplicações Telnet estiverem utilizando a porta 23, você deverá utilizar outra porta.

Como Planejar o Servidor TN3270E

Se você alterar o número da porta, evite números que são utilizados por outras aplicações. Se duas aplicações utilizam o mesmo número de porta, uma das aplicações vai falhar.

Se você alterar o número da porta, utilize um número maior que 1 024. Os números menores que 1 024 são reservados. Para obter mais informações sobre números de porta reservados, consulte o seguinte local na Internet:

<http://www.ds1.internic.net>

No momento da publicação deste documento, o RCF mais recente para números atribuídos era o RFC1700.

Notifique os usuários do cliente TN3270E quando alterar o número da porta, porque eles vão ter que configurar suas aplicações de emuladores para que sejam correspondentes.

Como Gerenciar o Tráfego do Sistema

Existem duas maneiras de controlar a frequência com que as conexões não utilizadas são desconectadas: processamento "manter ativo" e encerramento de sessão automático.

Por padrão, o servidor TN3270E não utiliza o processamento "manter ativo". Se você utilizar o processamento "manter ativo", pode escolher entre NOP ou marca de sincronização.

- O processamento de NOP envia um comando NOP do Telnet após uma frequência "manter ativo" especificada. Isto faz com que os dados sejam transmitidos durante a conexão, que faz com que o TCP/IP detecte que a conexão foi interrompida. O servidor não espera uma resposta do cliente. Pode demorar um tempo indeterminado para que o TCP/IP detecte a interrupção da conexão.
- O processamento de marca de sincronização envia um comando de marca de sincronização para o cliente. Se o cliente não responder dentro do período especificado, a conexão será encerrada.

O processamento de marca de sincronização gera mais tráfego no sistema do que o processamento de NOP mas libera conexões não utilizadas mais rapidamente.

Se você escolher o encerramento de sessão automático, o servidor vai desconectar qualquer sessão que esteja sem tráfego durante o período especificado. O tráfego do processamento "manter ativo" não mantém a conexão aberta; os dados devem ser enviados para ou a partir do sistema central. As sessões de impressoras não são encerradas automaticamente.

Se os emuladores de cliente estiverem configurados para executarem o processamento "manter ativo", você poderá desativá-lo no servidor e se o processamento "manter ativo" for encerrado no servidor, você poderá desativá-lo no cliente para reduzir o tráfego na rede.

Filtragem de IP

O Communications Server permite configurar filtros TN3270E para especificar quais clientes TCP/IP que podem se conectar no servidor. Os clientes podem ser especificados utilizando endereços IP individuais, sub-redes de IP ou nomes de domínio ou de sistema central TCP/IP.

Suporte ao Secure Sockets Layer (SSL)

Você pode configurar um número de porta segura utilizado pelo servidor para conexões seguras a partir da janela **Parâmetros do Servidor TN3270E** ou a partir de um arquivo de resposta.

Para permitir a segurança, o Communications Server fornece um utilitário **Gerenciamento do Conjunto de Chaves** para gerar o certificado e as chaves requeridas pelo SSL. Consulte o “Capítulo 10. Como Planejar a Segurança baseada em Secure Sockets Layer” na página 133 para obter maiores informações.

Quando tiver configurado e ativado a segurança, os clientes TN3270E que suportam o SSL Versão 3 podem se conectar em um número de porta segura e estabelecer conexões seguras.

Como Configurar Conexões SNA

É necessário configurar a conexão e as LUs do sistema central antes de utilizar a função do servidor TN3270E. Para obter uma tabela que descreve e explica os parâmetros do sistema central, consulte *Iniciação Rápida*.

Como Agrupar

Existem quatro classes de definições de LU específicas do servidor TN3270E: estação de trabalho implícita, estação de trabalho explícita, impressora implícita e impressora explícita. Essas classes correspondem às classes genéricas de terminal, específicas do terminal, genéricas da impressora, e específicas da impressora estabelecidas no RFC 1647.

As definições da **estação de trabalho implícita** são estabelecidas em um conjunto utilizado pelo servidor TN3270E para atender os pedidos para conexões. O conjunto padrão pode ser configurado para atender os pedidos em que o cliente não especifica um nome de LU ou de conjunto. Todos os outros conjuntos devem ser especificados pelo nome.

Você também pode definir um conjunto de definições de LU utilizados para atender pedidos de um nome de LU específico. Estas definições da **estação de trabalho explícita** garantem que um dispositivo de terminal solicitado por uma aplicação do sistema central não seja atribuído a um cliente que não fez a solicitação explicitamente.

De forma semelhante, você pode definir um conjunto de definições de impressora que será utilizado para atender pedidos de conexões que não requerem nomes de LU específicos (**impressora implícita**) e um conjunto utilizado para atender pedidos de um nome de LU específico (**impressora explícita**).

Como Planejar o Servidor TN3270E

As definições de impressoras implícita e explícita podem ter impressoras que estejam associadas a elas. Cada definição de terminal pode ter uma impressora que esteja atribuída a ela e cada impressora pode ter uma definição de terminal associada. Estas impressoras não estão incluídas nas definições de impressoras explícitas ou implícitas.

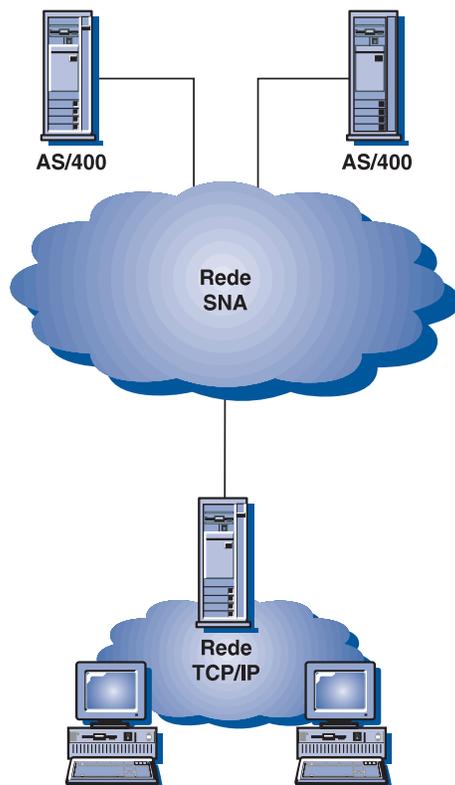
As definições da *impressora associada* só podem ser acessadas através da consulta ao nome da LU do terminal. Elas podem reduzir a quantidade de informações de que o usuário cliente precisa, porque ele ou ela precisa saber o nome da LU do terminal para se conectar às sessões de terminal e de impressora.

Balanceamento de Carga de Servidores TN3270E

O Communications Server também suporta o balanceamento de carga de clientes TN3270 através de vários servidores TN3270E. Consulte “Capítulo 11. Como Planejar o Balanceamento de Carga” na página 141 para obter mais informações.

Capítulo 9. Como Planejar o Servidor TN5250

A função do servidor TN5250 permite configurar sua rede conforme mostrado na Figura 36 ou Figura 37 na página 128.



Como Planejar o Servidor TN5250

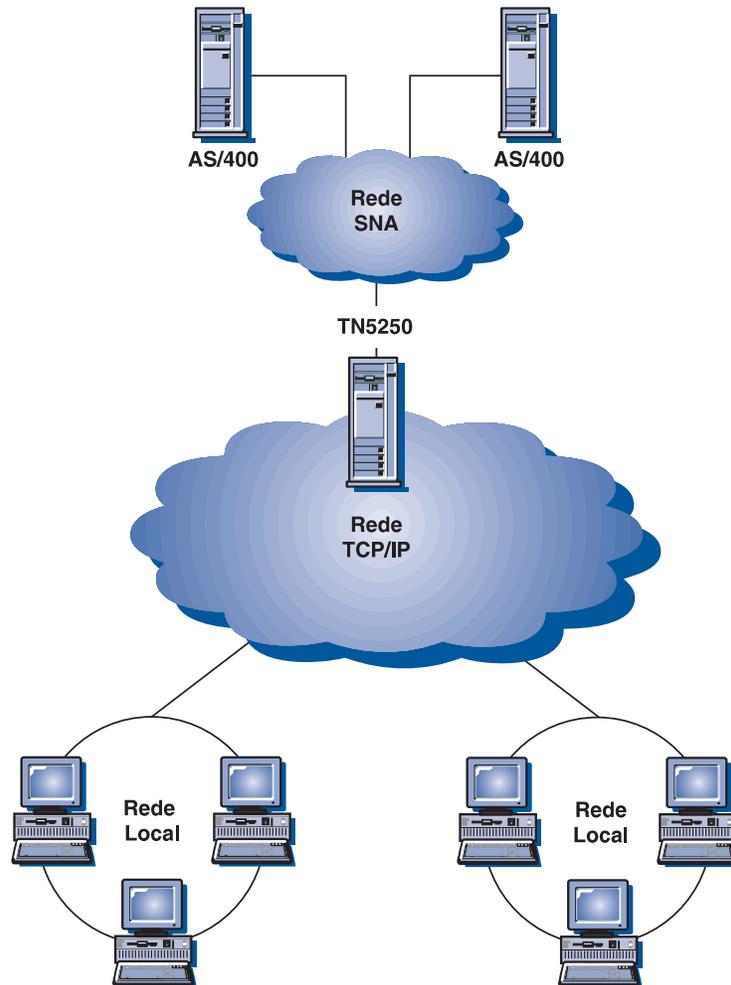


Figura 37. Communications Server configurado como um Servidor TN5250 com a Rede Ampla TCP/IP

A função do servidor TN5250 suporta:

- Conexão de clientes TN5250 com fluxo de dados da estação de trabalho 5250
Na implementação os protocolos descritos no RFC 1205, o servidor transmite dados da estação de trabalho 5250 para e a partir de um cliente TCP/IP que esteja emulando uma estação de trabalho IBM 5250. Geralmente, este cliente é conhecido como um cliente TN5250.
- Acesso a um ou mais AS/400s em uma rede SNA
O servidor se conecta aos sistemas centrais AS/400 utilizando um protocolo de LU 6.2 SNA. O suporte é fornecido para acessar um ou mais AS/400s a partir de estações de trabalho de cliente iguais ou diferentes.
- Filtragem de IP
O Communications Server permite a especificação de filtros do cliente TCP/IP, utilizando endereços IP, sub-redes, nomes de sistemas centrais e nomes de domínios. Esta função permite a administração central dos clientes com permissão para se conectarem no servidor e também o suporte ao direcionamento de clientes para AS/400s específicos.
- Segurança baseada em Secure Sockets Layer (baseada em SSL)

As conexões entre clientes TN e o servidor TN3270E utiliza a Versão 3 do SSL para fornecer criptografia de dados e autenticação do servidor utilizando certificados assinados.

Consulte *Iniciação Rápida* para obter instruções sobre como configurar um servidor TN5250.

Estações de Trabalho de Cliente Suportadas no Servidor TN5250

O servidor TN5250 suporta qualquer cliente TN5250 que esteja totalmente de acordo com o RFC 1205.

Destaques

Esta seção fornece mais informações sobre alguns dos recursos que podem ser configurados para o servidor TN5250.

Como Alterar o Número da Porta Padrão

Quando você configura o suporte ao servidor TN5250, é definida uma porta padrão com o número 23, mas outras aplicações Telnet, como por exemplo, o suporte ao servidor TN3270E, também podem utilizar esta porta. Se outras aplicações Telnet em execução estiverem utilizando a porta 23, você deverá utilizar outra porta.

Se você alterar o número da porta, evite números que são utilizados por outras aplicações. Se duas aplicações utilizam o mesmo número de porta, uma das aplicações vai falhar.

Se você alterar o número da porta, utilize um número maior que 1 024. Os números menores que 1 024 são reservados. Para obter mais informações sobre números de porta reservados, consulte o seguinte local na Internet:

<http://www.ds1.internic.net>

No momento da publicação deste documento, o RCF mais recente para números atribuídos era o RFC1700.

Notifique os usuários do cliente TN5250 quando alterar o número da porta porque eles terão que configurar suas aplicações de emuladores para que sejam correspondentes.

Como Gerenciar o Tráfego do Sistema

Existem duas maneiras de controlar a frequência com que as conexões não utilizadas são desconectadas: processamento "manter ativo" e encerramento de sessão automático.

Por padrão, o servidor TN5250 não utiliza o processamento "manter ativo". Se você utilizar o processamento "manter ativo", pode escolher entre NOP ou marca de sincronização.

- O processamento de NOP envia um comando NOP do Telnet após uma frequência "manter ativo" especificada. Isto faz com que os dados sejam transmitidos durante a conexão, que faz com que o TCP/IP detecte que a

Como Planejar o Servidor TN5250

conexão foi interrompida. O servidor não espera uma resposta do cliente. Pode demorar um tempo indeterminado para que o TCP/IP detecte a interrupção da conexão.

- O processamento de marca de sincronização envia um comando de marca de sincronização para o cliente. Se o cliente não responder dentro do período especificado, a conexão será encerrada.

O processamento de marca de sincronização gera mais tráfego no sistema do que o processamento de NOP mas libera conexões não utilizadas mais rapidamente.

Se você escolher o encerramento de sessão automático, o servidor vai desconectar qualquer sessão que esteja sem tráfego durante o período especificado. O tráfego do processamento "manter ativo" não mantém a conexão aberta; os dados devem ser enviados para ou a partir do sistema central.

Se os emuladores de cliente estiverem configurados para executarem o processamento "manter ativo", você poderá desativá-lo no servidor e se o processamento "manter ativo" for encerrado no servidor, você poderá desativá-lo no cliente para reduzir o tráfego na rede.

Como Especificar Acesso aos AS/400s com Várias Portas

O Communications Server permite configurar mais de um AS/400 e mais de uma porta para que o servidor TN5250 receba conexões de entrada. Quando você configura uma nova porta do servidor TN5250, é possível especificar o AS/400 que será associado à porta. As conexões TCP/IP de entrada recebidas nessa porta pelo servidor TN5250 vão acessar o AS/400 associado a essa porta.

Notifique os usuários do cliente TN5250 sobre as portas que devem ser configuradas para que suas aplicações de emuladores se conectem aos AS/400s específicos.

Filtragem de IP

O Communications Server permite configurar filtros TN5250 para especificar os clientes TCP/IP que podem se conectar no servidor. Os clientes podem ser especificados utilizando endereços IP individuais, sub-redes de IP ou nomes de domínio ou de sistema central TCP/IP.

Você também pode configurar um AS/400 com um filtro para especificar um AS/400 diferente do associado à porta. Isto pode ser utilizado para direcionar os clientes associados a um filtro para um AS/400 específico.

Pode ser especificado mais de um AS/400 em um filtro. Se a tentativa de conexão de um cliente com o primeiro AS/400 especificado não for bem-sucedida, serão tentadas conexões com outros AS/400s especificados no filtro.

Suporte ao Secure Sockets Layer (SSL)

Quando você configura uma nova porta do servidor TN5250, é possível especificar que a porta será utilizada para conexões seguras. Mais de uma porta pode ser especificada como segura.

Para permitir a segurança, o Communications Server fornece um utilitário **Gerenciamento do Conjunto de Chaves** para gerar o certificado e as chaves

Como Planejar o Servidor TN5250

requeridas pelo SSL. Consulte “Capítulo 10. Como Planejar a Segurança baseada em Secure Sockets Layer” na página 133 para obter maiores informações.

Quando tiver configurado e ativado a segurança, os clientes TN5250 que suportam o SSL Versão 3 podem se conectar em um número de porta segura e estabelecer conexões seguras.

Como Configurar a Rede SNA

É necessário configurar a rede SNA para permitir que o servidor TN5250 se conecte aos AS/400s. Consulte *Iniciação Rápida* para obter informações sobre como configurar a rede SNA para o servidor TN5250.

Balanceamento de Carga de Servidores TN5250

O Communications Server também suporta o balanceamento de carga de clientes TN5250 através de vários servidores TN5250. Consulte o “Capítulo 11. Como Planejar o Balanceamento de Carga” na página 141 para obter mais informações.

Capítulo 10. Como Planejar a Segurança baseada em Secure Sockets Layer

Você pode utilizar a segurança baseada em Secure Sockets Layer (baseada em SSL) em conexões entre clientes TN e o servidor TN3270E ou TN5250. Essa segurança utiliza SSL Versão 3 para fornecer criptografia de dados e autenticação do servidor, utilizando certificados.

Você pode configurar portas específicas para suportar a segurança baseada em SSL. Se a segurança for especificada, o servidor deverá ter um certificado autenticado fornecido por uma autoridade de certificação (CA). O Communications Server fornece um utilitário que gera e gerencia chaves e certificados utilizados pelo SSL Versão 3.

Este capítulo fornece uma visão geral do planejamento da segurança baseada em Secure Sockets Layer (baseada em SSL). A segurança baseada em SSL é fornecida como uma opção ao configurar o servidor TN3270E e TN5250.

Como Funciona a Segurança do SSL

Secure sockets layer (SSL) é um protocolo padrão industrial que utiliza tecnologia de criptografia de chave simétrica ou pública. A criptografia de chave simétrica utiliza a mesma chave para criptografar e decifrar mensagens. A criptografia de chave pública utiliza um par de chaves, uma chave pública e uma chave particular. A chave pública de cada servidor é publicada sendo que a chave particular é mantida em segredo. Para enviar uma mensagem segura para o servidor, o cliente criptografa a mensagem utilizando a chave pública do servidor. Quando o servidor recebe a mensagem, ele a decifra utilizando a chave particular.

O SSL fornece três serviços de segurança básicos:

- Exclusividade da mensagem

A exclusividade da mensagem é obtida através de uma combinação de criptografia da chave pública e da chave simétrica. Todos os tráfegos entre um cliente SSL e um servidor SSL são criptografados, utilizando uma chave e um algoritmo de criptografia negociado durante a configuração da sessão.

- Integridade da mensagem

O serviço de integridade da mensagem garante que o tráfego da sessão SSL não é alterado no percurso para seu destino final. O SSL utiliza uma combinação de chaves públicas/particulares e funções hash, para garantir a integridade da mensagem.

- Autenticação

A autenticação é o processo pelo qual o cliente e o servidor convencem um ao outro de suas identidades. As identidades do cliente e do servidor são codificadas em certificados de chave pública. Um certificado de chave pública contém os seguintes componentes:

- Nome específico do assunto
- Nome específico do emissor
- Chave pública do assunto
- Assinatura do emissor

Segurança baseada em SSL

- Período de validade
- Número de série

Nota: O Communications Server suporta autenticação do lado do servidor. Somente o servidor seguro requer autenticação de autoridade de certificado (CA), para permitir o estabelecimento de uma conexão TN3270E ou TN5250.

Suporte ao SSL do Communications Server

O Communications Server suporta os seguintes componentes de segurança do SSL:

- Sessões SSL seguras entre o servidor TN3270E e todos os clientes TN3270 e TN3270E que suportam o SSL Versão 3
- Sessões SSL seguras entre o servidor TN5250 e todos os clientes TN5250 que suportam o SSL Versão 3
- SSL Versão 3
- Exclusividade e integridade de mensagem
- Autenticação do lado do servidor

Como Configurar a Segurança do SSL

Durante a configuração do servidor TN3270E e TN5250, especifique quais portas irão utilizar a segurança do SSL para suas conexões. Consulte o “Capítulo 8. Como Planejar o Servidor TN3270E” na página 121 e o “Capítulo 9. Como Planejar o Servidor TN5250” na página 127 para obter maiores informações sobre a configuração de portas seguras.

Para ativar a segurança do SSL com a autenticação do servidor, um conjunto de chaves públicas/particulares e um certificado de chave pública autenticado associado é requerido. O Communications Server fornece um utilitário **Gerenciamento do Conjunto de Chaves** para criar, gerenciar e armazenar chaves públicas/particulares e certificados requeridos pelo SSL.

Ao utilizar o utilitário **Gerenciamento do Conjunto de Chaves**, você deve executar um dos seguintes itens:

- Crie um par de chaves públicas/particulares e obtenha um certificado de uma das autoridades de certificado (CAs) (reconhecida) predefinidas.
Esse procedimento requer menos configuração, porque o arquivo do banco de dados do conjunto de chaves é pré-configurado com os certificados de raiz CA requeridos, para identificar as CAs de quem o certificado é emitido.
- Crie um par de chaves públicas/particulares, defina um CA desconhecido através da obtenção e armazenamento do certificado raiz do CA no arquivo do banco de dados do conjunto de chaves, e obtenha e armazene um certificado do CA desconhecido.
- Crie um certificado assinado por você mesmo e armazene-o no arquivo do banco de dados do conjunto de chaves.

Nota: Para garantir segurança adequada para seu site, um certificado assinado por você mesmo deve ser utilizado somente para objetivos de teste controlados.

Utilitário de Gerenciamento do Conjunto de Chaves

O utilitário **Gerenciamento do Conjunto de Chaves** do Communications Server permite que você crie, gerencie e armazene chaves públicas/particulares e certificados requeridos para comunicações SSL entre o Communications Server e o cliente. Antes de começar a configurar as comunicações SSL, você deve abrir o arquivo do banco de dados do conjunto de chaves do Communications Server. Utilize as seguintes etapas para abrir o arquivo:

1. Selecione **Arquivo do Banco de Dados Chave** a partir do menu principal e selecione **Abrir** para abrir um banco de dados do conjunto de chaves existente.
2. Da janela **Abrir**, selecione o subdiretório **particular** do diretório onde você instalou o produto (por exemplo, C:\IBMCS\PRIVATE).
3. Selecione **ibmcs.kdb** como o banco de dados do conjunto de chaves
4. No prompt de senha, digite sua senha.

Nota: A senha é inicialmente definida como **ibmcs**. Para obter segurança adequada, é **mandatório** alterar a senha antes de executar qualquer uma das tarefas de **Gerenciamento do Conjunto de Chaves**.

Como Alterar a Senha

Utilize as etapas a seguir para alterar a senha do banco de dados atual:

1. Selecione **Arquivo do Banco de Dados Chave** do menu e selecione **Alterar Senha** para alterar a senha do banco de dados do conjunto de chaves do banco de dados atual. O diálogo de arquivo **Alterar Senha** aparece.
2. Digite a nova senha que deseja utilizar.
3. Digite a mesma senha novamente para confirmar.
4. Se desejar que a senha tenha uma data de expiração, dê um clique sobre **Definir data de expiração**. Para garantir a segurança adequada, a senha deve ter uma data de expiração.
5. Se você selecionar para permitir que a senha seja expirada, especifique o número de dias até que a senha expire.
6. Dê um clique sobre **Armazenar a senha** para armazenar a senha do banco de dados atual.

Como Configurar o SSL Utilizando um CA de Confiança Reconhecido

Siga os procedimentos nessa seção, para configurar a segurança do SSL utilizando um certificado emitido pelo CA reconhecido. Os certificados do signatário do CA a seguir já estão armazenados no banco de dados do conjunto de chaves e marcados como certificados de confiança:

- Integriion Certification Authority Root
- IBM World Registry Certification Authority
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA RSA secure server CA (também obtido do VeriSign)
- CA principal e público classe 4 de VeriSign
- CA principal e público classe 3 de VeriSign

Segurança baseada em SSL

- CA principal e público classe 2 de VeriSign
- CA principal e público classe 1 de VeriSign

Para configurar a segurança do SSL utilizando um CA reconhecido, os seguintes procedimentos são necessários:

- Crie uma chave e um pedido de certificado
- Submeta um pedido de certificado ao CA
- Obtenha e armazene um certificado no banco de dados do conjunto de chaves do servidor

Como Criar uma Chave e um Pedido de Certificado

Utilize as etapas a seguir no utilitário **Gerenciamento do Conjunto de Chaves**, para criar as chaves públicas/particulares e o pedido de certificado:

1. Selecione **Pedidos de Certificados Pessoais** da lista sobreposta do menu principal e dê um clique sobre **Novo** para criar um novo par de chaves e pedido de certificado. O diálogo **Criar Nova Chave e Pedido de Certificado** aparece.
2. Digite o nome (etiqueta) que é utilizado para identificar a chave e o certificado dentro do banco de dados.
3. Digite o número do tamanho da chave que deseja utilizar. A seleção do tamanho da chave maior resulta em segurança mais forte, mas requer mais processamento no cliente e no servidor para estabelecer uma conexão.
4. Digite o nome do sistema central do TCP/IP do communications server como o nome comum (por exemplo, wtr05306.raleigh.ibm.com).
5. Digite um nome de organização.
6. Digite uma unidade organizacional (opcional).
7. Digite uma cidade ou localidade (opcional).
8. Digite um estado ou província (opcional).
9. Digite um código de endereçamento postal (opcional).
10. Digite o código do país. Você deve especificar pelo menos 2 caracteres (por exemplo, E.U.).
11. Digite um nome de arquivo do pedido de certificado ou utilize o nome do arquivo padrão.

Ao dar um clique sobre **OK**, as informações fornecidas são processadas. Dois arquivos são produzidos:

ibmcs.rdb	Arquivo da chave particular do conjunto de chaves
certreq.arm	Esse é o nome padrão do arquivo de pedido de certificado. Se você atribuiu um nome de arquivo, um arquivo com esse nome será criado. O arquivo de pedido de certificado é um arquivo do tipo PKCS 10 em 64 formatos protegidos.

Não tente editar ou mover esses arquivos. Se o arquivo **ibmcs.rdb** não puder ser encontrado ou se foi danificado ao tentar digitar o certificado no banco de dados do conjunto de chaves, você terá que resubmeter o pedido de certificado para o CA.

Como Submeter um Pedido de Certificado

Inicie um navegador Web e acesse a página na Web para o CA. Siga as instruções fornecidas para submeter o pedido de certificado. A seguir encontram-se as URLs de alguns CAs reconhecidos:

- VeriSign: <http://www.verisign.com/>
- Thawte: <http://www.thawte.com/>

Dependendo do CA que você seleciona, o correio eletrônico que o pedido de certificado gerou pelo utilitário **Gerenciamento do Conjunto de Chaves** ou incorporar o pedido de certificado no formulário ou arquivo fornecido pelo CA.

Após submeter um pedido de certificado para um CA, você pode ativar a segurança do SSL através da criação e armazenamento de um certificado assinado por você mesmo. Um certificado assinado por você mesmo deve ser utilizado somente para objetivos de teste controlados. Consulte “Como Criar um Certificado Assinado por Você Mesmo” na página 139 para obter maiores informações.

Como Armazenar um Certificado no Banco de Dados do Conjunto de Chaves

Quando você receber um certificado de um CA, utilize o utilitário **Gerenciamento do Conjunto de Chaves** para colocar o certificado no arquivo do conjunto de chaves, **ibmcs.kdb**, localizado no servidor.

1. Selecione **Certificados Pessoais** da lista sobreposta do utilitário **Gerenciamento do Conjunto de Chaves** e dê um clique sobre **Receber** para receber o par de chaves e o pedido de certificado. O diálogo **Receber Certificado de um Arquivo** aparece.
2. Certifique-se de que o tipo de dados seja **Dados ASCII protegidos BASE64** (64 formatos protegidos).
3. Digite o nome do arquivo do certificado.
4. Digite a localização (nome do caminho) do certificado. Dê um clique sobre **OK**. O certificado armazenado é exibido como o primeiro item.
5. Destaque o certificado armazenado e dê um clique sobre **Visualizar/Editar**. O diálogo **Informações sobre chave** aparece.
6. Dê um clique sobre **Definir o certificado como o padrão**. A chave selecionada torna-se o padrão.

Como Configurar o SSL Utilizando um CA Desconhecido

Para configurar a segurança do SSL utilizando um CA desconhecido (ainda não definido no banco de dados), os seguintes procedimentos são necessários:

- Crie uma chave e um pedido de certificado
- Submeta um pedido de certificado ao CA
- Obtenha o certificado raiz do CA e seu certificado, e armazene-os no banco de dados do conjunto de chaves do servidor

Como Criar uma Chave e um Pedido de Certificado

Utilize as etapas a seguir no utilitário **Gerenciamento do Conjunto de Chaves**, para criar as chaves públicas/particulares e o pedido de certificado:

Segurança baseada em SSL

1. Selecione **Pedidos de Certificados Pessoais** da lista sobreposta do menu principal e dê um clique sobre **Novo** para criar um novo par de chaves e pedido de certificado. O diálogo **Criar Nova Chave e Pedido de Certificado** aparece.
2. Digite o nome (etiqueta) que é utilizado para identificar a chave e o certificado dentro do banco de dados.
3. Digite o número do tamanho da chave que deseja utilizar. A seleção do tamanho da chave maior resulta em segurança mais forte, mas requer mais processamento no cliente e no servidor para estabelecer uma conexão.
4. Digite o nome do sistema central do TCP/IP do communications server como o nome comum (por exemplo, wtr05306.raleigh.ibm.com).
5. Digite um nome de organização.
6. Digite uma unidade organizacional (opcional).
7. Digite uma cidade ou localidade (opcional).
8. Digite um estado ou província (opcional).
9. Digite um código de endereçamento postal (opcional).
10. Digite o código do país. Você deve especificar pelo menos 2 caracteres (por exemplo, E.U.).
11. Digite um nome de arquivo do pedido de certificado ou utilize o nome do arquivo padrão.

Ao dar um clique sobre **OK**, as informações fornecidas são processadas. Dois arquivos são produzidos:

ibmcs.rdb	Arquivo da chave particular do conjunto de chaves
certreq.arm	Esse é o nome padrão do arquivo de pedido de certificado. Se você atribuiu um nome de arquivo, um arquivo com esse nome será criado. O arquivo de pedido de certificado é um arquivo do tipo PKCS 10 em 64 formatos protegidos.

Não tente editar ou mover esses arquivos. Se o arquivo **ibmcs.rdb** não puder ser encontrado ou se foi danificado ao tentar digitar o certificado no banco de dados do conjunto de chaves, você terá que resubmeter o pedido de certificado para o CA.

Como Submeter um Pedido de Certificado

Siga os procedimentos do CA desconhecido, para submeter o pedido do certificado.

Dependendo do CA selecionado, envie por correio eletrônico o pedido de certificado gerado pelo utilitário **Gerenciamento do Conjunto de Chaves** ou anexe o pedido de certificado ao formulário ou arquivo fornecido pelo CA.

Após submeter um pedido de certificado para um CA, você pode ativar a segurança do SSL através da criação e armazenamento de um certificado assinado por você mesmo. Um certificado assinado por você mesmo deve ser utilizado somente para objetivos de teste controlados. Consulte "Como Criar um Certificado Assinado por Você Mesmo" na página 139 para obter maiores informações.

Como Armazenar um Certificado no Banco de Dados do Conjunto de Chaves

Quando você receber um certificado de um CA, entre em contato com o CA para obter o certificado raiz do CA. Você deve armazenar o certificado raiz do CA no banco de dados do conjunto de chaves, antes de armazenar o certificado que você aplicou. O certificado raiz do CA valida o certificado que você submeteu. Utilize o utilitário **Gerenciamento do Conjunto de Chaves** para armazenar o certificado raiz do CA.

1. Selecione **Certificados do Signatário** da lista sobreposta e dê um clique sobre **Receber** para receber o par de chaves e o pedido de certificado. O diálogo **Receber Certificado de um Arquivo** aparece.
2. Certifique-se de que o tipo de dados seja **Dados ASCII protegidos BASE64** (64 formatos protegidos).
3. Digite o nome do arquivo do certificado.
4. Digite a localização (nome do caminho) do certificado. Dê um clique sobre **OK**. O arquivo é marcado como **confiável** e é armazenado.

Para armazenar o certificado que você submeteu, utilize o utilitário **Gerenciamento do Conjunto de Chaves** para colocar o certificado no arquivo do conjunto de chaves, **ibmcs.kdb**, localizado no servidor.

1. Selecione **Certificados Pessoais** da lista sobreposta do menu principal e dê um clique sobre **Receber** para receber o par de chaves e o pedido de certificado. O diálogo **Receber Certificado de um Arquivo** aparece.
2. Certifique-se de que o tipo de dados seja **Dados ASCII protegidos BASE64** (64 formatos protegidos).
3. Digite o nome do arquivo do certificado.
4. Digite a localização (nome do caminho) do certificado. Dê um clique sobre **OK**. O certificado armazenado é exibido como o primeiro item.
5. Destaque o certificado armazenado e dê um clique sobre **Visualizar/Editar**. O diálogo **Informações sobre chave** aparece.
6. Dê um clique sobre **Definir o certificado como o padrão**. A chave selecionada torna-se o padrão.

Como Criar um Certificado Assinado por Você Mesmo

O recibo de um certificado de um CA de confiança reconhecido pode demorar três semanas. Até que você receba o certificado do servidor público, é possível criar um certificado assinado por você mesmo para ativar sessões SSL entre clientes e o servidor. Um certificado assinado por você mesmo deve ser utilizado somente para objetivos de teste controlados. Para garantir segurança adequada para seu site, um certificado assinado por você mesmo não deve ser utilizado em um ambiente de produção. Para configurar o site para a utilização de um certificado assinado por você mesmo usando o utilitário **Gerenciamento do Conjunto de Chaves**, siga essas etapas:

1. Selecione **Novo Certificado Assinado por Você Mesmo** da opção de menu **Criar** para criar um novo certificado assinado por você mesmo. O diálogo **Criar Novo Certificado Assinado por Você Mesmo** aparece.
2. Digite o nome (etiqueta) que é utilizado para identificar a chave e o certificado dentro do banco de dados. Selecione **X509 V3** como a versão do certificado.

Segurança baseada em SSL

3. Digite o número do tamanho da chave que deseja utilizar. A seleção do tamanho da chave maior resulta em segurança mais forte, mas requer mais processamento no cliente e no servidor para estabelecer uma conexão.
4. Digite o nome do sistema central do TCP/IP do communications server como o nome comum (por exemplo, wtr05306.raleigh.ibm.com).
5. Digite um nome de organização.
6. Digite uma unidade organizacional (opcional).
7. Digite uma cidade ou localidade (opcional).
8. Digite um estado ou província (opcional).
9. Digite um código de endereçamento postal (opcional).
10. Digite o código do país. Você deve especificar pelo menos 2 caracteres (por exemplo, E.U.).
11. Digite o número de dias que o certificado assinado por você mesmo deve ficar válido.
12. Dê um clique sobre **OK**.
13. Dê um clique sobre **Sim** para definir a chave como a chave padrão no banco de dados da chave.

Se você estiver utilizando o IBM eNetwork Host On-Demand ou algum outro cliente SSL que requer a designação do certificado assinado por você mesmo, utilize o utilitário **Gerenciamento do Conjunto de Chaves** e siga essas etapas:

1. Selecione **Certificados Pessoais** a partir da lista sobreposta, destaque o certificado assinado por você mesmo e dê um clique sobre **Extrair Certificado**. O diálogo **Extrair Certificado de um Arquivo** aparece.
2. Selecione **Dados DER binários** como o tipo de dados.
3. Digite o nome do arquivo do certificado. O arquivo deve ter um tipo de arquivo **crt** (por exemplo, ibmcs.crt).
4. Digite a localização (nome do caminho) do certificado.
5. Dê um clique sobre **OK**.

O arquivo de certificado deve ser fornecido para cada cliente autorizado a conectar-se ao servidor. Consulte a documentação do cliente, para obter instruções sobre o armazenamento do certificado assinado por você mesmo como um certificado raiz de CA no arquivo de classe do cliente ou no banco de dados do conjunto de chaves.

Capítulo 11. Como Planejar o Balanceamento de Carga

Este capítulo fornece uma visão geral do planejamento para balanceamento de carga. Descreve o planejamento para o balanceamento de carga LU e LU 6.2 dependentes.

Balanceamento de Carga de LU Dependente

O balanceamento de carga permite balancear sessões do sistema central dependentes através dos servidores. O balanceamento de carga é suportado por aplicações API LUX através de clientes API de SNA, emuladores 3270 e emuladores TN3270.

Quando o Communications Server responde a pedidos do cliente, ordena os servidores que suportam o conjunto solicitado por carga.

A carga para LUs dependentes representa uma porcentagem de recursos disponíveis de um determinado servidor. A porcentagem de carga é calculada dividindo-se o número de conexões de aplicações ativas pelo número total de LUs (0 a 3) disponíveis.

Você pode influenciar a carga calculada especificando um fator de carga LU0 a 3 (fator de carga da sessão do sistema central) para compensar as diferenças entre dois servidores, tais como memória disponível, velocidade do processador e utilização da CPU. Você pode também utilizar o fator de carga LU0 a 3 para balancear as cargas entre Communications Servers e servidores Novell IntranetWare para SAA.

Notas:

1. Os servidores participantes do balanceamento de carga são determinados pela associação do conjunto de LUs e pela associação do escopo. Todos os Communications Servers com LUs em conjuntos do mesmo nome estão sujeitos ao balanceamento de carga.
2. Os clientes que utilizam o protocolo TCP/IP podem participar do balanceamento de carga. Contudo, os clientes TCP/IP podem balancear a carga somente entre IBM Communications Servers. O balanceamento de carga é determinado pelos escopos configurados.

No Communications Server, se conjuntos de LUs em diferentes servidores tiverem o mesmo nome, eles funcionarão como um conjunto para o balanceamento de carga. Ao atribuir LUs a um conjunto de LUs, selecione entre ligações do sistema central em um servidor e atribua LUs a partir da ligação de sistema central selecionada ao conjunto de LUs. Estas LUs não precisam ser do mesmo tipo de LU. Além disso, o conjunto resultante pode conter LUs de ligações múltiplas.

Balanceamento de Carga de LU 6.2

O balanceamento de carga permite balancear sessões LU 6.2 independentes distribuindo-as pelos múltiplos servidores. O balanceamento de carga é suportado por aplicações API do APPC através de clientes API de SNA e emuladores TN5250.

Como Planejar o Balanceamento de Carga

A carga para LU6.2 representa uma porcentagem de recursos disponíveis de um determinado servidor. A porcentagem da carga é calculada dividindo-se o número total de conversações sobre todas as LUs locais em um determinado servidor pelo limite máximo de sessões cumulativas para todas as LUs locais. O limite máximo de sessões é o limite de sessões LU 6.2 especificado durante a configuração. Se o limite máximo de sessões for especificado como zero (0), indicando que não há limite de sessões, o limite máximo de sessões LU locais padrão de 512 por LU local será utilizado quando a carga for calculada. O limite máximo de sessões LU locais poderá também ser especificado durante a configuração.

Você pode influenciar a carga calculada especificando um fator de carga LU6.2 (fator de carga de sessão APPC) para compensar as diferenças entre dois servidores, tais como memória disponível, velocidade do processador e utilização da CPU. Você pode também utilizar o fator de carga LU6.2 para balancear as cargas entre Communications Servers e servidores Novell IntranetWare para SAA.

Nota: Os clientes que utilizam o protocolo TCP/IP podem participar do balanceamento de carga LU 6.2.

Planejamento para Escopos TCP/IP

Escopo é o parâmetro utilizado para controlar e gerenciar o acesso de cliente TCP/IP a servidores em uma rede. Ocorre o mesmo com o escopo do protocolo de localização de serviço (SLP) conforme referido em RFC 2165. O SLP é utilizado pelo Communications Server para implementar o balanceamento de carga baseado em TCP/IP.

O escopo de controle fornecido é necessário por dois motivos:

- Conforme sua rede e o número de clientes e de servidores crescem, torna-se necessário fornecer acesso a estes servidores pelo número crescente de clientes para reduzir o tráfego integral na rede.
- O escopo de controle permite que administradores organizem usuários e servidores em grupos administrativos.

O significado dos valores de escopo são definidos pelo administrador da rede. Estes valores podem representar qualquer entidade. Normalmente, são dispostos em linhas departamentais, geográficas ou organizacionais.

Uma vez configurados, os clientes podem atingir a rede SNA através de servidores configurados com o mesmo escopo ou que não tenham nenhum escopo associado (serviços ou servidores **sem escopo**).

Nota: Se um servidor for configurado como sem escopo, ele responderá a pedidos que têm e que não têm escopo do SLP. Se o cliente API de SNA for configurado para conectar-se a servidores sem escopo, somente os servidores sem escopo irão responder.

Escopos e Segurança do Client Server

O Communications Server permite que clientes Novell IntranetWare para clientes SAA utilizem a segurança de domínio do Windows NT, para autenticar a conexão do cliente como servidor sem digitar novamente o ID do usuário e a senha. O

Como Planejar o Balanceamento de Carga

cliente deve ser parte de um domínio do Windows NT, pela participação em um domínio do Communications Server ou pela iniciação de sessão localmente com um ID de usuário e senha sincronizados.

Os usuários autorizados do servidor cliente são mantidos no grupo local IBMCSADMIN, que está localizado diretamente no Communications Server ou no controlador de domínio onde participa o Communications Server. Esse grupo de usuário é criado durante a instalação e pode ser administrado utilizando o aplicativo Gerenciador de Usuário do Windows NT.

Os usuários do cliente Novell IntranetWare para SAA, fora do domínio do Windows NT, devem replicar o ID do usuário e senha através de todos os servidores configurados com o mesmo escopo.

Onde o Escopo É Configurado

Cada servidor é atribuído a um escopo ou escopos através da **Configuração de Nó**. Os clientes que utilizam estes servidores devem estar configurados para conectarem-se a servidores dentro de um único escopo específico ou a servidores que não tem escopo. Para obter mais informações sobre como configurar clientes, consulte *Client/Server Communications Programming*.

Como o Escopo Está Relacionado ao SLP

O escopo do Communications Server está relacionado diretamente com o escopo do protocolo de localização de serviço (SLP). Portanto, os agentes do diretório SLP podem estar localizados na rede que suporte os escopos configurados do Communications Server. Se estiver planejando permitir que clientes localizem serviços do Communications Server com base em escopos, considere a maneira pela qual o escopo se relaciona com a rede como um todo. Se houver serviços sem escopo em uma rede em que escopos também são utilizados, os serviços sem escopo são candidatos a satisfazer qualquer pedido com escopo, o que pode teoricamente sobrecarregar estes agentes de serviço e de diretório que suportam serviços sem escopo.

Nota: Se o cliente API de SNA for configurado para conectar-se a servidores sem escopo, somente os servidores sem escopo irão responder.

Se os agentes de diretório forem utilizados na mesma rede do site (para ajuste de escala ascendente), deverão ser configurados para tratar dos mesmos escopos da forma como são configurados para o Communications Server. Além disso, se serviços sem escopo forem utilizados em redes com agentes de diretório, pelo menos um agente de diretório sem escopo deverá ser configurado.

O Communications Server contém um agente de serviço SLP instalado em cada servidor em que o Communications Server está instalado. Nenhum suporte SLP adicional precisa ser instalado na rede para que o balanceamento de carga do TCP/IP e o recurso de busca do Communications Server funcionem adequadamente.

Como Rastrear a Carga Atual

Você pode rastrear a carga atual da LU 6.2 e de LUs dependentes, utilizando o Supervisor de Desempenho do Windows NT. Você pode iniciar o supervisor de desempenho da seleção **Ferramentas Administrativas (Comuns)** do menu **Programas**.

Na tela do supervisor de desempenho, selecione **Incluir no Gráfico** do menu pendente **Editar**. No campo **Objeto**, selecione **Balanceamento de Carga do IBM SNA**. Os dois contadores listados são:

Carga LU0/LU3

Utilize esse contador para rastrear a carga de LUs dependentes.

Carga LU6.2

Utilize esse contador para rastrear a carga de LUs da LU 6.2.

Os resultados do rastreamento de carga são salvos para referência futura.

Capítulo 12. Como Planejar as Conexões ao Sistema Central de Reserva

Para ambientes onde pode é importante fornecer conexões ao sistema central de reserva para as conexões principais utilizadas por sessões do emulador da estação de trabalho, o Communications Server fornece opções que permitem a configuração das conexões ao sistema central, que são ativadas em resposta às condições de falha. As opções que você pode utilizar dependem do nível de reserva que deseja fornecer:

- Para ativar a reserva do sistema completo entre os nós do servidor que suportam sessões do emulador da estação de trabalho IP ou IPX baseada em Rede Local, inclua o sistema de reserva quente no seu ambiente.
- Para ativar a reserva do sistema completo entre os nós do servidor que suportam sessões do emulador da estação de trabalho IP ou IPX que não sejam baseadas em Rede Local, não inclua o sistema de reserva quente no seu ambiente. Configure uma instalação duplicada do Communications Server no sistema de reserva.
- Para ativar a reserva em um nó do servidor, não utilize o sistema de reserva quente. Utilize as opções normais nas definições das conexões no ambiente de reserva.

Essas opções são explicadas nas seções seguintes.

Como Planejar as Conexões de Reserva Entre os Servidores que Utilizam Sistema de Reserva Quente

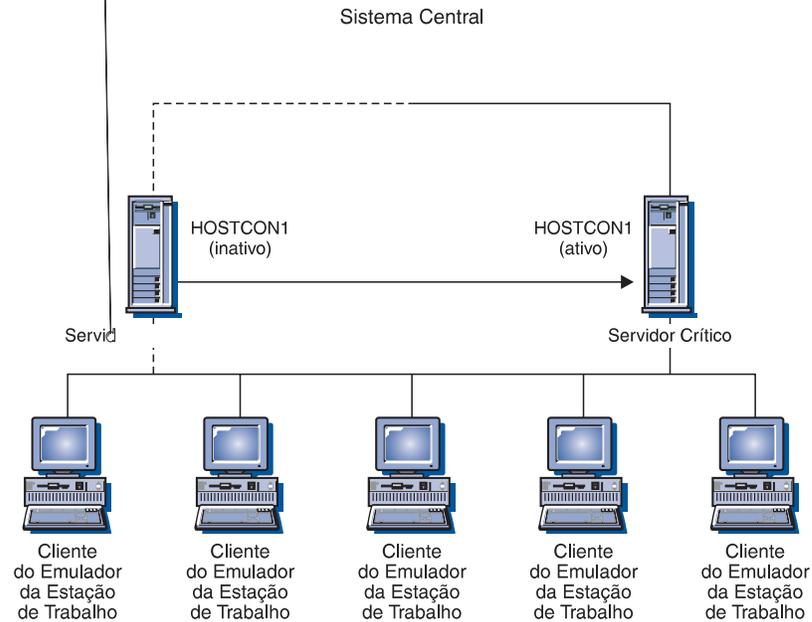
No Communications Server, você pode configurar ligações ao sistema central para serem ativadas automaticamente se um servidor crítico falhar. As conexões a um sistema central configuradas podem continuar funcionando através da ativação das conexões alternativas em um servidor de reserva. Essa função é conhecida como sistema de reserva quente.

Para o usuário de uma sessão do emulador da estação de trabalho com uma máquina central cuja conexão inicial falha devido a uma falha do Communications Server, o sistema de reserva quente permite uma tentativa posterior de reestabelecimento da conexão à máquina central, encaminhando automaticamente através de um Communications Server alternativo. O servidor inicial que está fornecendo a conexão é conhecido como **servidor crítico**. O servidor alternativo que fornece uma conexão à máquina central após a falha do servidor crítico é conhecido como **servidor de reserva**. O servidor de reserva fornece conexões que são iniciadas automaticamente em resposta à detecção de uma falha no servidor crítico e as cargas de licenciamento referentes à conectividade ao sistema central do servidor crítico são automaticamente gerenciadas no servidor de reserva.

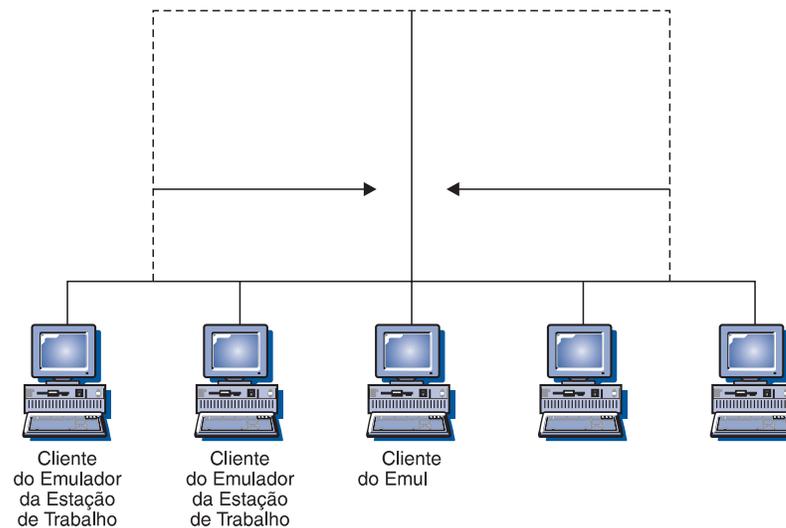
Um servidor pode ser crítico e de reserva ao mesmo tempo. Os servidores podem funcionar como servidores de reserva recíprocos.

O sistema de reserva quente permite que o servidor de reserva suporte sessões do emulador IP ou IPX baseadas em Rede Local. O sistema de reserva quente não fornece suporte ao servidor de reserva para o ambiente SNA.

Na Figura 38, o servidor de reserva está configurado com uma conexão de reserva completa ao HOSTCON1, o que fornece a conectividade ao sistema central principal no servidor crítico. As linhas pontilhadas entre o servidor de reserva e os clientes do emulador das estações de trabalho não estarão ativas enquanto o servidor crítico estiver em operação.



Na Figura 39 na página 147, cada um dos servidores de reserva está configurado com uma conexão de reserva parcial ao HOSTCON1, o que fornece a conectividade ao sistema central principal no servidor crítico. A combinação dos dois servidores fornece uma reserva completa para o HOSTCON1. As linhas pontilhadas entre os servidores de reserva e os clientes do emulador das estações de trabalho não estarão ativas enquanto o servidor crítico estiver em operação.



Se o servidor crítico falhar, a recuperação ocorrerá da seguinte forma:

1. O servidor de reserva, o sistema central e o software emulador da estação de trabalho na estação de trabalho detectam a falha aproximadamente no mesmo momento.
2. As conexões nomeadas na configuração do servidor crítico do servidor de reserva são ativadas automaticamente e sua conectividade à máquina central é estabelecida.
3. A estação de trabalho estabelece uma nova sessão com o servidor de reserva que acabou de ativar suas conexões ao servidor crítico.
4. A estação de trabalho entra em contato com a máquina central e exibe um prompt de início de sessão para o usuário.

Nota: Quando o servidor crítico é ativado novamente, as conexões ao servidor de reserva ativadas para o mesmo não são desativadas automaticamente. Você deve desativar as conexões ao servidor de reserva manualmente.

Como Utilizar Um Servidor de Reserva de Produção ou Dedicado para Sistema de Reserva Quente

Você não pode instalar as mesmas licenças do Communications Server em mais de um servidor que está sendo executado na mesma rede. Instale o Communications Server em vários servidores, adquirindo um pacote adicional do Communications Server para cada servidor adicional.

Antes de configurar o Communications Server para sistema de reserva quente, decida se o Communications Server deve ser executado tanto como um servidor de produção quanto um servidor de reserva ou como um servidor de reserva dedicado.

Como Planejar as Conexões ao Sistema Central de Reserva

Como Utilizar um Servidor de Produção

Um *servidor de produção* é um Communications Server que cuida das suas necessidades diárias de comunicação. Esse ambiente configura o Communications Server com conexões ao sistema central, que são ativadas fora de um cenário de falha do servidor crítico. A ativação e utilização dessas conexões requer a aquisição de licenças adequadas para as mesmas. Você não pode instalar as mesmas licenças do Communications Server em mais de um servidor. Para instalar o Communications Server para ser utilizado como um servidor de produção em vários sistemas, você deve adquirir um pacote adicional do Communications Server para instalação de cada servidor adicional.

Ao utilizar um Communications Server tanto como servidor de produção quanto como servidor de reserva, não existe nenhuma consideração de licença especial. Você instala o Communications Server e as licenças adquiridas para utilização do Communications Server como servidor de produção.

A função do Communications Server como servidor de reserva não requer nenhum licenciamento adicional além do licenciamento de base adquirido para os servidores críticos que ele está configurado para supervisionar. Você não precisa de nenhuma consideração sobre licença especial no servidor de reserva. Quando o servidor de reserva detecta uma falha de um servidor crítico, ele automaticamente ativa as conexões configuradas para o servidor crítico e ajusta as licenças do servidor de reserva baseadas naquelas em vigor para o servidor crítico. O Communications Server gerencia o licenciamento do sistema de reserva quente sem a sua intervenção.

Entretanto, se as conexões configuradas para o servidor crítico já tiverem sido ativadas fora de um cenário de falha do servidor crítico, o ajuste do servidor de reserva para as licenças do servidor crítico não será executado e será necessário licenciamento separado no servidor de reserva.

Como Utilizar um Servidor Dedicado

Um servidor de reserva *dedicado* não funciona como um servidor de produção e não ativa conexões fora de um cenário de falha do servidor crítico. Nenhuma conexão pode ser ativada no mesmo na inicialização nem pode ser ativada manualmente. Sua função é supervisionar um ou mais servidores críticos.

Um servidor de reserva dedicado não requer nenhum licenciamento adicional além do licenciamento de base adquirido para os servidores críticos que ele está configurado para supervisionar. O Communications Server gerencia o licenciamento do sistema de reserva quente sem a sua intervenção.

Planejamento do Ambiente do Sistema de Reserva Quente Completo

Os cenários para utilização do sistema de reserva quente envolvem cenários funcionais normais do Communications Server para suporte a clientes do emulador baseado em Rede Local através de IP ou IPX, com algumas operações específicas do sistema de reserva quente.

Para configurar um ambiente de sistema de reserva quente, existem duas dependências básicas:

Como Planejar as Conexões ao Sistema Central de Reserva

- Dois ou mais servidores de comunicações devem ser configurados para fornecerem conexões compatíveis a uma máquina central. O servidor utilizado como reserva deve ter uma configuração de servidor crítico para o servidor que fornece a conectividade principal à máquina central.
- O software cliente emulador da estação de trabalho utilizado para conectar através do servidor para fornecer aos usuários as sessões do emulador na máquina central deve suportar alguns meios de efetuar roteamento alternativo para o servidor de reserva caso ocorra uma falha no servidor crítico.

Alguns clientes do emulador podem não fornecer o roteamento alternativo. O planejamento de um ambiente de sistema de reserva quente requer a avaliação cuidadosa do software emulador e do tipo de conectividade utilizado entre o cliente e o servidor. A seguir estão algumas opções de roteamento alternativo:

- **Substituição quente** - Refere-se ao suporte em um cliente do emulador, para configuração de vários servidores nomeados a serem contatados, em uma determinada ordem, para estabelecer uma conexão através do servidor à máquina central para uma sessão do emulador. A substituição quente permite configurar o servidor de reserva para que seja contatado quando as tentativas de contatar o servidor crítico não tiverem êxito. Quando o servidor crítico falhar e os recursos no servidor de reserva forem ativados, o cliente do emulador entrará em contato com o servidor de reserva e estabelecerá uma rota alternativa através do mesmo para conexão à máquina central.
- **Conjunto de LUs** - Refere-se ao suporte em um cliente do emulador para estabelecer dinamicamente a conexão à máquina central para uma sessão do emulador através do servidor que atualmente está respondendo as consultas de LUs de um conjunto nomeado disponíveis. O suporte aos conjuntos de LUs permite que o servidor de reserva e os servidores críticos forneçam LUs ao mesmo conjunto. Inicialmente o servidor de reserva está definido mas não ativo. Quando o servidor crítico falha e os recursos do servidor de reserva são ativados, o servidor de reserva responde aos pedidos de LUs do conjunto, feitos pelo cliente do emulador, e estabelece uma rota alternativa através do mesmo para conexão à máquina central. Os conjuntos de LUs incluem os seguintes tipos de suporte ao cliente para conjuntos de LUs:
 - Suporte pré-SLP: Antes do suporte de SLP do Communications Server, o acesso do cliente aos conjuntos de LUs era aleatório ou em uma ordem de servidores especificada.
 - Suporte SLP: O suporte a SLP do Communications Server fornece ao cliente o acesso aos conjuntos de LUs, balanceado a carga da sessão através dos servidores que contribuem com o conjunto.
- **Múltiplas sessões do emulador** - Refere-se ao suporte, em um cliente do emulador, para configuração de múltiplas sessões do emulador, permitindo que o usuário configure sessões separadas utilizando o servidor de reserva e os servidores críticos para conexão à máquina central. A utilização de múltiplas sessões do emulador não é tão fácil quanto a substituição quente ou o suporte ao conjunto de LUs, porque requer intervenção manual pelo usuário do emulador para ajudar no roteamento alternativo quando ocorrer uma falha. Quando a conexão ao servidor crítico falha, o usuário inicia manualmente a sessão configurada para utilizar o servidor de reserva, para restabelecer a conexão à máquina central.

O suporte do IBM Personal Communications aos clientes do emulador TN3270E, TN5250, API ou QEL/MU fornece opções de roteamento alternativo através de

Como Planejar as Conexões ao Sistema Central de Reserva

uma ou mais das opções de substituição quente, conjuntos de LUs ou múltiplas sessões do emulador. Os clientes do emulador de alguns fornecedores fornecem opções de roteamento alternativo.

Como Configurar o Sistema de Reserva Quente no Servidor de Reserva

No painel avançado **Configuração do Nó**, utilize a opção de configuração **Configurar Servidores Críticos do Sistema de Reserva Quente** para configurar o sistema de reserva quente no servidor de reserva.

Não é necessário executar nenhuma configuração do sistema de reserva quente no servidor crítico, mas o servidor de reserva requer configuração do sistema de reserva quente. Utilizando a opção avançada **Configuração do Nó**, configure o servidor de reserva com as definições do servidor crítico. Uma definição de servidor crítico especifica o nome do servidor crítico supervisionado pelo servidor de reserva e os nomes das conexões ativadas quando o servidor crítico falha. É possível configurar múltiplas definições de servidores críticos, permitindo que um servidor de reserva supervise e forneça reserva para múltiplos servidores críticos. Após configurar as definições do servidor crítico no servidor de reserva, reinicie o nó do servidor de reserva para que as alterações sejam efetivadas. Para obter informações detalhadas sobre a configuração do sistema de reserva quente, consulte o auxílio online para **Configuração do Nó**.

Configuração de um Ambiente de Sistema de Reserva Quente

Siga estas etapas para configurar um ambiente de sistema de reserva quente:

1. **Configure o Servidor Crítico:** O servidor crítico é configurado sem nenhuma configuração relativa ao sistema de reserva quente. Configure a conectividade ao sistema central para que corresponda à opção de roteamento alternativa utilizada com os clientes do emulador.
2. **Configure o Servidor de Reserva:** A configuração do servidor de reserva envolve dois conceitos importantes:
 - a. A configuração da conectividade ao sistema central no servidor de reserva é semelhante ao servidor crítico, exceto que as conexões ao sistema central são configuradas para iniciação manual.
 - b. A configuração do servidor crítico no servidor de reserva para definir as conexões ao sistema central iniciadas quando é detectada uma falha no servidor crítico.
3. **Configure os clientes do emulador:** Os clientes do emulador da estação de trabalho são configurados para corresponderem a uma opção de roteamento alternativa para a conectividade que está sendo fornecida pelos servidores.
4. **Inicie os Nós do Servidor Crítico e do Servidor de Reserva:** Inicie os nós normalmente. As **Operações do Nó SNA** podem verificar o status de reserva quente nos servidores críticos e de reserva.
5. **Falha do Servidor Crítico:** Quando o servidor crítico falha, a recuperação ocorre da seguinte forma:
 - a. O servidor de reserva, o sistema central e o software emulador da estação de trabalho, no cliente, detectam a falha aproximadamente no mesmo momento.
 - b. As conexões nomeadas na configuração do servidor crítico, no servidor de reserva, são ativadas e a conectividade à máquina central é estabelecida.

Como Planejar as Conexões ao Sistema Central de Reserva

- c. O cliente do emulador da estação de trabalho estabelece uma nova sessão com o servidor de reserva. O servidor de reserva encaminha sessões à máquina central através da conexão que foi ativada no servidor de reserva quando o servidor crítico falhou.
 - d. A estação de trabalho entra em contato com a máquina central e exibe um prompt de início de sessão para o usuário.
6. **Servidor Crítico online novamente:** Quando o servidor crítico fica ativo novamente, as novas sessões do emulador da estação de trabalho utilizam a conectividade ao sistema central do servidor crítico. As sessões do emulador da estação de trabalho existentes, encaminhadas através do servidor de reserva, continuam operando até serem fechadas.

Você deve desativar manualmente as conexões ao sistema central do servidor de reserva. A desativação manual das conexões ao servidor de reserva devem ser executadas fora do horário de expediente. Você deve avisar os usuários de sessões do emulador da estação de trabalho com o servidor de reserva antes da desativação das conexões.

Como Planejar as Conexões de Reserva Entre Servidores sem Utilização do Sistema de Reserva Quente

Como o sistema de reserva quente limita-se aos ambientes que suportam sessões do emulador da estação de trabalho IP ou IPX baseadas em Rede Local, alguns ambientes não podem utilizar o sistema de reserva quente para conectividade de reserva. Muitas considerações para o planejamento de um ambiente de reserva sem o sistema de reserva quente são semelhantes ao planejamento de reserva com a utilização do sistema de reserva quente. Siga estas etapas para configurar um ambiente de reserva sem utilizar o sistema de reserva quente:

1. No servidor de reserva, instale um pacote do Communications Server adquirido separadamente com as licenças adequadas para fornecer conexões ao sistema central de reserva para o servidor principal.
2. No servidor de reserva, configure as conexões ao sistema central utilizadas como reservas para ativar sob demanda.
3. Configure os clientes do emulador da estação de trabalho para fornecerem roteamento automático aos recursos do servidor de reserva quando o servidor principal falhar. Entretanto, o roteamento deve restringir-se ao acesso ao servidor de reserva somente se for detectada uma falha do servidor principal.
4. Ambos os nós são iniciados mas, a princípio, apenas o nó principal com suas conexões upstream ativas fornecem conectividade ao sistema central.
5. Quando o servidor principal falha, os clientes do emulador da estação de trabalho tentam conexões posteriores através do servidor de reserva. As conexões do sistema central no servidor de reserva são ativadas.
6. O licenciamento duplicado instalado no servidor de reserva fornece a disponibilidade do servidor de reserva aos clientes anteriormente encaminhados através do servidor principal.
7. Quando o servidor principal estiver ativo novamente, as conexões no servidor de reserva serão desativadas manualmente.

Como Planejar as Conexões de Reserva em um Único Servidor

Você não pode utilizar o sistema de reserva quente para conectividade de reserva em um único servidor, porque o sistema de reserva quente só se aplica aos ambientes com conexões de reserva entre os servidores. Entretanto, algumas considerações para planejamento de um ambiente de reserva em um único servidor são semelhantes ao planejamento de reserva com a utilização do sistema de reserva quente. As diferenças estão resumidas nas etapas a seguir, para conexões de reserva em um único servidor:

1. No servidor que funciona como o gateway para o sistema central, configure as conexões principal e de reserva que fornecem LUs ao mesmo conjunto de LUs, mas com a conexão de reserva configurada para ser ativada sob demanda.
2. Configure os clientes do emulador da estação de trabalho para conexão através do conjunto de LUs.
3. Quando a conexão principal falhar ou as LUs do conjunto forem esgotadas, uma tentativa de conexão ao conjunto iniciará a ativação da conexão de reserva.
4. Quando o servidor principal estiver ativo novamente, as conexões no servidor de reserva serão desativadas manualmente.

Capítulo 13. Como Planejar para X.25

Você precisa planejar cuidadosamente a configuração do X.25. É preciso considerar o seguinte:

- Para utilizar um PSDN público, você precisa solicitar uma subscrição de rede para cada linha (ligação) necessária. Pode levar algum tempo para que uma linha seja fornecida, desta forma, verifique a negociação com o provedor de rede X.25.
- Quais funções estão disponíveis na rede X.25 e quais são necessárias. O provedor de rede geralmente fornece um guia técnico da rede, o qual deve ser obtido e consultado.
- Colete informações em canais lógicos que você requer para PVCs e SVCs.
 - Podem ser definidos até 16 grupos de 256 canais lógicos.
 - O número do grupo varia de 0 a 15.
 - O número do canal lógico dentro do grupo varia de 0 a 255.

Multiplicando o número do grupo por 256 e adicionando o número do canal lógico fornecerá um número no intervalo de 0 a 4095, que identifica exclusivamente um canal lógico. Esta combinação é, algumas vezes, referida como o número do canal lógico.

Notas:

1. Se você especificar o CCITT como 1984 ou 1988, o número máximo de canais lógicos será 4095.
 2. Se você especificar o CCITT como 1980, o número máximo de canais lógicos será 1024.
- Os grupos de canais lógicos podem ser somente de entrada (reservado para chamadas de outros DTEs), somente de saída (reservado para chamadas de outros DTEs), ou dos dois modos.
 - Quantos circuitos virtuais o uso de SNA requer
 - Quais PVCs você requer
 - A associação de canais lógicos somente de entrada, somente de saída e dos dois modos
 - O tamanho máximo do pacote que você requer e qual é suportado pela rede X.25.
 - Detalhes de quais recursos opcionais do X.25 seus programas aplicativos X.25 utilizarão.

As recomendações do X.25 CCITT definem um número de recursos opcionais que sua rede pode suportar.

Alguns recursos possuem parâmetros que podem ser especificados ou negociados por um programa aplicativo durante a configuração de chamada e limpeza utilizando os campos de recursos no pedido de chamada, aceitação de chamada e limpar pacotes de pedidos.

A conexão X.25 pode ser configurada para suportar os seguintes recursos durante a configuração de chamada:

- Grupo Fechado de Usuários
- Identificação do usuário da rede
- Negociação do tamanho da janela e pacote
- Cobrança no destinatário

Como Planejar para X.25

Defina os recursos durante a configuração do DLC X.25.

- Detalhes de quaisquer requisitos especiais para estrutura e parâmetros de pacotes. Os valores padrões para estes parâmetros de configuração foram escolhidos cuidadosamente para se adequarem à maioria das situações. Entretanto, seu provedor de rede pode requerer ou recomendar alguns valores.

Para evitar problemas, seus parâmetros de configuração devem corresponder aos detalhes de sua subscrição da rede. Por exemplo, se você configurou 20 canais lógicos SVC mas subscreveu apenas 10, o DCE detectaria uma condição de erro quando fosse tentar utilizar o 11º canal lógico.

Conexões X.25 Possíveis

A Figura 40 mostra como uma rede X.25 pode fornecer uma conexão a partir de um SNA gateway para um sistema central.

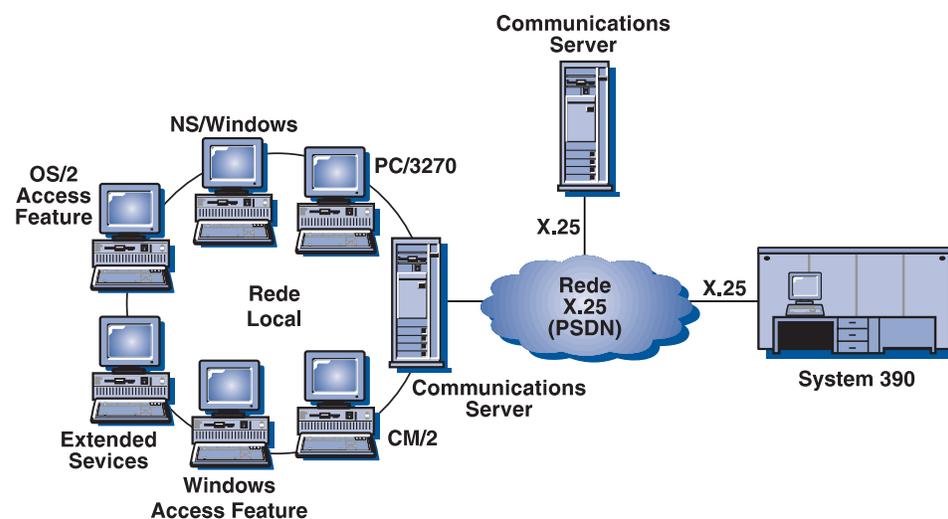


Figura 40. Conectividade X.25 e SNA Gateway

Custos da Rede X.25

Os custos reais dependem dos processos de cobrança do provedor da rede X.25, mas os custos geralmente consistem em alguns ou todos os seguintes elementos:

- Custo de instalação
Um custo de instalação única quando subscreve pela primeira vez para a rede X.25.
- Custo de aluguel periódico
Este custo depende dos recursos fornecidos pelo provedor da rede. Por exemplo, você pode pagar um preço para cada recurso opcional da rede ao qual se subscreveu. Pode também pagar um preço para cada canal lógico disponível. Os PVCs geralmente custam mais do que os SVCs pois requerem recursos da rede dedicados.
- Custo de Utilização
Este custo depende do período de tempo em que você está conectado logicamente à rede, possivelmente sujeito a um custo mínimo.
- Custo do volume

Este custo está relacionado à quantidade de dados transmitidos sobre a rede durante um período de cobrança.

Como Planejar para X.25

Capítulo 14. Como Configurar Conectividade do Sistema Central

Você pode conectar estações de trabalho em execução no Communications Server para System/390 (incluindo System/370) ou sistemas centrais AS/400. Muitos dos valores que você especifica para a configuração do Communications Server também são utilizados na configuração do sistema central. Este capítulo descreve o mapeamento entre os parâmetros de configuração especificados durante a configuração do Communications Server e os parâmetros especificados nos sistemas centrais. Contém também tabelas que listam os parâmetros que podem ser utilizados para eliminar os parâmetros comuns em cada macro a ser emitida entre o Communications Server e o sistema central.

Nota: Muitos parâmetros NCP emitidos a partir de macros LINE, PU e LU podem ser especificados na macro GROUP para possibilitar a leitura e facilitar a codificação. Esta correspondência de parâmetros elimina a necessidade de incluir parâmetros comuns em cada macro subsequente e permite ainda o recurso de substituir, quando apropriado.

NCP Token Ring (NTRI) com VTAM e o Communications Server

A Tabela 7 compara os parâmetros do sistema central aos parâmetros do Communications Server para conexões de Rede Token-Ring IBM.

Tabela 7. Referência Cruzada de Parâmetros PC/Sistema Central: Definição de NTRI de Rede Token-Ring IBM

NTRI/NCP	Perfil/Parâmetros do Communications Server	Comentários
GROUP ECLTYPE = PHY	Tipo de DLC: Rede Local	
LINE LOCADDR	Conexões de Configuração Rede Local Endereço de destino	O conjunto de valores para este parâmetro sob o Communications Server deve ser o endereço da placa da Rede Token-Ring IBM no controlador do sistema central.

Token Ring com Rede Comutada VTAM e o Communications Server

A Tabela 8 na página 158 compara os parâmetros do sistema central com os parâmetros do Communications Server para conexões de Rede IBM Token-Ring utilizando uma rede comutada VTAM.

Como Configurar Conectividade do Sistema Central

Tabela 8. Referência Cruzada de Parâmetros PC/Sistema Central: Rede IBM Token-Ring com Rede Comutada VTAM

VTAM	Perfil/Parâmetros do Communications Server	Comentários
IDBLK=	Configurar Nó ID de nó local ID de Bloco	O sistema central IDBLK deve corresponder aos 3 primeiros caracteres hexadecimais do ID de nó local , que o assume como X'05D' para Communications Server. Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
IDNUM=	Configurar Nó ID de Nó Local ID de Unidade Física	O IDNUM de sistema central deve corresponder aos 5 últimos caracteres hexadecimais do ID de nó local . Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
CPNAME=	Definição de Nó Configurar Nó Nome completo do CP (segundo campo)	Especifique este parâmetro ao utilizar linhas discadas ou omita ao utilizar IDBLK= e IDNUM=.
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Estes parâmetros devem ter o mesmo valor. Para LUs independentes, o VTAM recomenda criar uma definição CDRSC ou utilizar o operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições de codificação do CDRSC para LUs independentes, consulte <i>VTAM Network Implementation Guide</i> . Nenhuma definição de sistema central será requerida para LUs dependentes, se a definição dinâmica ou SDDLU for utilizada para LUs independentes em VTAM 3.4 ou posterior.
MAXDATA	Configurar Dispositivo de Rede Local Tamanho máximo de PIU (265–65535)	Este valores não precisam corresponder.
MAXOUT	Configurar Dispositivo de Rede Local Contagem do buffer de recepção (2–64)	A contagem do buffer de recepção no Communications Server deve ser igual ao parâmetro MAXOUT no sistema central.

Placa de Rede IBM Token-Ring 9370 e o Communications Server

A Tabela 9 na página 159 compara os parâmetros de sistema central 9370 aos parâmetros do Communications Server para conexões de Rede IBM Token-Ring.

Como Configurar Conectividade do Sistema Central

Tabela 9. Referência Cruzada de Parâmetros PC/Sistema Central: Rede IBM Token-Ring 9370 de Rede Local VTAM

VTAM	Perfil/Parâmetros do Communications Server	Comentários
VBUILD TYPE = Rede Local	Tipo de DLC: Rede Local	
PORT MACADDR=	Configurar Conexão Rede Local Endereço de destino	O endereço de destino especificado na personalização do Communications Server deve ser o endereço da placa Token-Ring IBM 9370.
PORT SAPADDR=04	Configurar Conexão Rede Local SAP Remoto	Estes valores devem corresponder.
ADDR=04 (somente de saída)	Configurar Conexão Rede Local SAP Local	Estes valores devem corresponder.

Controlador 3174 e o Communications Server

A Tabela 10 compara os parâmetros do controlador 3174 para Communications Server para conexões Token-Ring IBM.

Tabela 10. Correspondência de Parâmetro entre uma Token Ring 3174 e o Communications Server

3174	Perfil/Parâmetros do Communications Server	Comentários
O endereço do limite superior é maior que 104: CUA	Tipo de DLC: Rede Local	
Endereço Token-Ring para gateway	Conexões de Configuração Rede Local Endereço de destino	Estes valores devem corresponder.
Definição de transmissão do anel. W= window max out, F=0, W = 1-7, F=1, W = 1-7, F=2, W = 1-4, F=3, W = 1-2	Configurar Dispositivos Rede Local Contagem de buffer de recepção (1-8)	A Contagem de buffer de recepção do Communications Server deve ser igual a 3174 W.

PU de VTAM do Controlador 3174 e o Communications Server

A Tabela 11 compara os parâmetros PU do VTAM do controlador 3174 ao Communications Server para conexões Token-Ring IBM.

Tabela 11. Referência Cruzada de Parâmetros PC/Sistema Central: PU de VTAM do controlador 3174 da Rede IBM Token-Ring e o Communications Server

VTAM	Perfil/Parâmetros do Communications Server	Comentários
CUADDR (local) ou ADDR (remoto)	(nenhum)	Mapeado pelo controlador 3174 para endereço Token-Ring IBM

Como Configurar Conectividade do Sistema Central

Tabela 11. Referência Cruzada de Parâmetros PC/Sistema Central: PU de VTAM do controlador 3174 da Rede IBM Token-Ring e o Communications Server (continuação)

VTAM	Perfil/Parâmetros do Communications Server	Comentários
MAXDATA (somente remoto)	Configurar Dispositivos Rede Local Tamanho máximo de PIU (99-65535)	O valor do tamanho Máximo de PIU definido na estação de trabalho do Communications Server deve corresponder ao valor definido no sistema central.
MAXOUT (somente remoto)	Configurar Dispositivos Rede Local Contagem de buffer de Recepção (2-64)	A contagem do buffer de recepção do Communications Server deve ser igual à MAXOUT.
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Estes parâmetros devem ter o mesmo valor. Para LUs independentes, o VTAM recomenda criar uma definição CDRSC ou utilizar o operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições de codificação do CDRSC para LUs independentes, consulte <i>VTAM Network Implementation Guide</i> Nenhuma definição de sistema central será requerida para LUs dependentes, se a definição dinâmica ou SDDLU for utilizada para LUs independentes em VTAM 3.4 ou posterior.

Ethernet com Rede Comutada VTAM e o Communications Server

A Tabela 12 compara os parâmetros do sistema central do Communications Server para as conexões de Rede Ethernet utilizando uma rede conectada VTAM.

Tabela 12. Referência Cruzada de Parâmetros PC/Sistema Central: Rede Comutada VTAM com Rede Ethernet

VTAM	Perfil/Parâmetros do Communications Server	Comentários
IDBLK=	Configurar Nó ID de nó local ID de Bloco	O sistema central IDBLK deve corresponder aos 3 primeiros caracteres hexadecimais do ID de nó local , que o assume como X'05D' para Communications Server. Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
IDNUM=	Configurar Nó ID de Nó Local ID de Unidade Física	O IDNUM de sistema central deve corresponder aos 5 últimos caracteres hexadecimais do ID de nó local . Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.

Como Configurar Conectividade do Sistema Central

Tabela 12. Referência Cruzada de Parâmetros PC/Sistema Central: Rede Comutada VTAM com Rede Ethernet (continuação)

VTAM	Perfil/Parâmetros do Communications Server	Comentários
CPNAME=	Definição de Nó Configurar Nó Nome completo do CP (segundo campo)	Especifique este parâmetro ao utilizar linhas discadas ou omita ao utilizar IDBLK= e IDNUM=.
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Estes parâmetros devem ter o mesmo valor. Para LUs independentes, o VTAM recomenda criar uma definição CDRSC ou utilizar o operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições de codificação do CDRSC para LUs independentes, consulte <i>VTAM Network Implementation Guide</i> Nenhuma definição de sistema central será requerida para LUs dependentes, se a definição dinâmica ou SDDLU for utilizada para LUs independentes em VTAM 3.4 ou posterior.
MAXDATA	Configurar Dispositivo de Rede Local Tamanho de PIU máximo (265–65535)	Este valores não precisam corresponder.
MAXOUT	Configurar Dispositivo de Rede Local Contagem de buffer de recepção (2–64)	A contagem do buffer de recepção no Communications Server deve ser igual ao parâmetro MAXOUT no sistema central.

VTAM/NCP e o Communications Server (SDLC)

A Tabela 13 compara os parâmetros do sistema central VTAM/NCP a parâmetros do Communications Server para conexões SDLC.

Tabela 13. Referência Cruzada de Parâmetros PC/Sistema Central: SDLC

VTAM/NCP	Perfil/Parâmetros do Communications Server	Comentários
NETID=	Configurar Nó Nome completo do CP (primeiro campo)	Este parâmetro pode ser utilizado para linhas discadas e dedicadas. Este parâmetro identifica a rede SNA a qual você conecta utilizando o Communications Server.
NAME PU		Sempre utilize um NAME PU. Este nome de PU deve ser um nome que não seja o mesmo que o nome de CP local, portanto você pode definir uma LU para o ponto de controle.

Como Configurar Conectividade do Sistema Central

Tabela 13. Referência Cruzada de Parâmetros PC/Sistema Central: SDLC (continuação)

VTAM/NCP	Perfil/Parâmetros do Communications Server	Comentários
IDBLK=	Configurar Nó ID de nó local ID de Bloco	O sistema central IDBLK deve corresponder aos 3 primeiros caracteres hexadecimais do ID de nó local , que o assume como X'05D' para Communications Server. Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
IDNUM=	Configurar Nó ID de Nó Local ID de Unidade Física	O IDNUM de sistema central deve corresponder aos 5 últimos caracteres hexadecimais do ID de nó local . Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
CPNAME=	Definição de Nó Configurar Nó Nome completo do CP (segundo campo)	Especifique este parâmetro ao utilizar linhas discadas ou omita ao utilizar IDBLK= e IDNUM=.
LNCTL=SDLC	Tipo de DLC: SDLC-WAC, SDLC-MPA, COM Port (depende do hardware utilizado)	O SDLC deve ser selecionado aqui. Este parâmetro é utilizado para linhas discadas e dedicadas.
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Estes parâmetros devem ter o mesmo valor. Para LUs independentes, o VTAM recomenda criar uma definição CDRSC ou utilizar o operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições de codificação do CDRSC para LUs independentes, consulte <i>VTAM Network Implementation Guide</i> Nenhuma definição de sistema central será requerida para LUs dependentes, se a definição dinâmica ou SDDLU for utilizada para LUs independentes em VTAM 3.4 ou posterior.

Como Configurar Conectividade do Sistema Central

Tabela 13. Referência Cruzada de Parâmetros PC/Sistema Central: SDLC (continuação)

VTAM/NCP	Perfil/Parâmetros do Communications Server	Comentários
NRZI=YES/NO	Conexões de Configuração SDLC-WAC, SDLC-MPA, Porta COM Codificação NRZI	<p>O Communications Server utiliza USE_NRZI_ENCODING=0 e USE_NRZI_ENCODING=1.</p> <p>Este parâmetro é encontrado apenas em PCMs para o Tipo de Modem: Comutado Síncrono, Não-Comutado Síncrono e Sincronização Automática.</p> <p>O esquema de codificação, NRZI ou NRZ, deve ser configurado da mesma maneira nas duas extremidades de uma conexão. Se os esquemas de codificação não forem correspondentes, os modems vão se conectar, mas a transferência de dados não vai ser bem-sucedida e a conexão será desfeita pelo Communications Server após um tempo de espera de nível de ligação (geralmente 40 segundos)</p> <p>É recomendado o esquema de codificação NRZ ao conectar a uma rede X.25 utilizando um IBM Wide Area Connector.</p>
DUPLEX= FULL/HALF	Conexões de Configuração SDLC-WAC e Somente Porta COM Comunicação Full-duplex	O conjunto de valores em cada lado deve ser coerente com o tipo de modem e a configuração. Este parâmetro é utilizado para linhas discadas e dedicadas.
(TRANSFER * BFRS) -47	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Tamanho máximo de PIU (265-4105)	O valor máximo do tamanho do campo I deve ser menor ou igual ao (TRANSFER * BFRS) - 47 indicado no sistema central. Este parâmetro é utilizado para linhas discadas e dedicadas.
MAXDATA=	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Tamanho máximo de PIU (265-4105)	Este valores não precisam corresponder. Este parâmetro é utilizado para linhas discadas e dedicadas. Será utilizado o valor inferior.
MAXOUT=	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Contagem de janelas de recepção (1-30)	A Contagem da janela de recepção no Communications Server deve ser igual ao parâmetro MAXOUT no sistema central. Este parâmetro é utilizado para linhas discadas e dedicadas.

Como Configurar Conectividade do Sistema Central

Tabela 13. Referência Cruzada de Parâmetros PC/Sistema Central: SDLC (continuação)

VTAM/NCP	Perfil/Parâmetros do Communications Server	Comentários
ADDR=	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Endereço de estação de ligação (01-FE)	Estes parâmetros devem ter o mesmo valor. Ele é codificado de forma decimal para o Communications Server e VTAM/NCP. Este parâmetro é utilizado para linhas discadas e dedicadas.

VTAM e o Communications Server (APPC)

A Tabela 14 compara parâmetros de sistema central VTAM aos parâmetros do Communications Server para conexões APPC.

Tabela 14. Referência Cruzada de Parâmetros PC/Sistema Central: APPC

VTAM	Perfil/Parâmetros do Communications Server	Comentários
LU NAME	Configurar LU do Sistema Central Nome de LU local ou: Configurar Nó Nome completo do CP (segundo campo)	
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Estes parâmetros devem ter o mesmo valor. Para LUs independentes, o VTAM recomenda criar uma definição CDRSC ou utilizar o operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições de codificação do CDRSC para LUs independentes, consulte <i>VTAM Network Implementation Guide</i> Nenhuma definição de sistema central será requerida para LUs dependentes, se a definição dinâmica ou SDDLU for utilizada para LUs independentes em VTAM 3.4 ou posterior.
NETID APPL	Configurar LU Parceira 6.2 Nome de LU parceira	
VTAM Interpret Table	Configurar LU Parceira 6.2 Nome de LU parceira	Somente para LUs dependentes.
LOGMODE Table LOGMODE=	Configurar Modo Nome do modo	Estes parâmetros devem corresponder.
LOGMODE Table RUSIZES=	Configurar Modo Tamanho de RU Máximo (256-32767)	Os valores finais são negociados.

VTAM e o Communications Server (MPC)

A Tabela 15 e a Tabela 16 comparam os parâmetros do sistema central IOCP/HCD e VTAM com parâmetros do Communications Server para conexões Multi-Path Channel (MPC).

Tabela 15. Referência Cruzada de Parâmetros IOCP/HCD: MPC

IOCP/HCD	Perfil/Parâmetros do Communications Server	Comentários
IOCP IODEVICE UNIT=SCTC	Tipo de DLC: IBM-MPC	
HCD Tipo de Dispositivo SCTC	Tipo de DLC: IBM-MPC	

Tabela 16. Referência Cruzada de Parâmetros VTAM: MPC

Instrução de Definição de VTAM	Operando	Perfil/Parâmetros do Communications Server	Comentários
VBUILD,TYPE=TRL	LNCTL=MPC	Tipo de DLC: IBM-MPC	
	MPCLEVEL=HPDT		Conexões IBM-MPC do Communications Server requerem HPR/HPDT
	MAXBFRU	Configurar DLC do MPC Tamanho de PIU máximo	Pode afetar o desempenho e/ou utilização da memória VTAM
	MAXREADS	Configurar DLC do MPC Contagem de Buffer de Recepção	Pode afetar o desempenho e/ou utilização da memória VTAM
	READ	Configurar DLC do MPC	A lista de endereços VTAM READ IODEVICE deve corresponder à lista de DLCs do MPC do Communications Server de subcanais READ
WRITE	Configurar DLC do MPC	A lista de endereços VTAM WRITE IODEVICE deve corresponder à lista de DLCs do MPC do Communications Server de subcanais WRITE	

Como Configurar Conectividade do Sistema Central

Tabela 16. Referência Cruzada de Parâmetros VTAM: MPC (continuação)

Instrução de Definição de VTAM	Operando	Perfil/Parâmetros do Communications Server	Comentários
VBUILD,TYPE=LOCAL	CONNTYPE=APPN	Conexões de Configuração IBM-MPC Suporte APPN	A conexão IBM-MPC do Communications Manager requer APPN.
	XID=YES	Conexões de Configuração IBM-MPC Suporte APPN	A conexão IBM-MPC do Communications Manager requer PU2.1.
	CPCP=YES	Conexões de Configuração IBM-MPC Suporte APPN	A conexão IBM-MPC do Communications Manager requer APPN.
	HPR=YES	Conexões de Configuração IBM-MPC Suporte HPR	A conexão IBM-MPC do Communications Manager requer HPR.
	NN	Configurar Nó Tipo de nó	O tipo de nó de PU do VTAM deve corresponder à definição do Communications Server.
	DELAY		Pode afetar o desempenho e/ou utilização da CPU de VTAM

ES/9000 e o Communications Server (SDLC)

A Tabela 17 compara os parâmetros do Sistema de Informações 9370 aos parâmetros do Communications Server para conexões SDLC.

Tabela 17. Referência Cruzada de Parâmetros PC/Sistema Central: Sistema de Informação 9370 através do SDLC

9370/VTAM	Perfil/Parâmetros do Communications Server	Comentários
QFI: Non-return -to-zero inverted (microcode configuration)	Conexões de Configuração SDLC-WAC, SDLC-MPA, Porta COM Codificação NRZI	Estes parâmetros devem corresponder. Este parâmetro é utilizado para linhas discadas e dedicadas. O Communications Server utiliza USE_NRZI_ENCODING=0 e USE_NRZI_ENCODING=1. Este é o fluxo de dados síncrono.
QFI: Protocol (microcode configuration) VTAM: GROUP LNCTL = SDLC	Tipo de DLC SDLC-WAC, SDLC-MPA Porta COM	Os parâmetros VTAM e do microcódigo devem corresponder. Este parâmetro é utilizado para linhas discadas e dedicadas.
MAXDATA	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Tamanho Máximo de PIU (265–4105)	Este valores não precisam corresponder. Este parâmetro é utilizado para linhas discadas e dedicadas.

Como Configurar Conectividade do Sistema Central

Tabela 17. Referência Cruzada de Parâmetros PC/Sistema Central: Sistema de Informação 9370 através do SDLC (continuação)

9370/VTAM	Perfil/Parâmetros do Communications Server	Comentários
MAXBFRU * IOBUF size	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Tamanho de PIU Máximo (265–4105)	O valor máximo do tamanho do campo deve ser menor ou igual ao tamanho IOBUF vezes MAXBFRU indicado no sistema central. Este parâmetro é utilizado para linhas discadas e dedicadas.
MAXOUT=	Configurar Dispositivos Contagem de janelas de recepção (1–30)	A Contagem da janela de recepção no Communications Server deve ser igual ao parâmetro MAXOUT no sistema central. Este parâmetro é utilizado para linhas discadas e dedicadas.
ADDR=	Configurar Dispositivos Endereço da estação de ligação (01–FE)	O conjunto de valores para estes parâmetros devem corresponder. Este parâmetro é utilizado para linhas discadas e dedicadas.
IDBLK=	Configurar Nó ID de Nó local ID de Bloco	O sistema central IDBLK deve corresponder aos primeiros 3 caracteres hexadecimais do ID de nó local , que o assume como 'X'05D' para Communications Server. Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
IDNUM=	Configurar Nó ID de nó local ID de unidade física	O IDNUM de sistema central deve corresponder aos 5 últimos caracteres hexadecimais do ID de nó local . Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
CPNAME=	Configurar Nó Nome completo do CP (segundo campo)	Especifique este valor ao utilizar linhas discadas ou omita ao utilizar IDBLK= ou IDNUM=.
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Os parâmetros LOCADDR e NAU devem ter o mesmo valor. Para LUs independentes, o VTAM recomenda criar uma definição de CDRSC ou utilizar o operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições da codificação CDRSC para LUs independentes, consulte o <i>VTAM Network Implementation Guide</i> . Este parâmetro é utilizado para linhas discadas e dedicadas.

Como Configurar Conectividade do Sistema Central

Sistema Central e o Communications Server (DLUR)

A Tabela 18 compara parâmetros do Communications Server e do sistema central para conexões VTAM sobre DLUR.

Tabela 18. Referência Cruzada do Parâmetro do Communications Server VTAM: Utilizando DLUR

VTAM	Communications Server	Comentários
IDBLK=	Configurar PUs do DLUR ID de Bloco	O IDBLK deve corresponder aos 3 primeiros caracteres hexadecimais do ID de Nó, que assume como padrão X'05D' para o Communications Server. Especifique este parâmetro quando NÃO estiver utilizando o CPNAME=.
IDNUM=	Configurar PUs do DLUR ID de unidade física	O IDBLK deve corresponder aos 5 últimos caracteres hexadecimais do ID de Nó. Especifique este parâmetro quando NÃO estiver utilizando o CPNAME=.
CPNAME=	Configurar PUs do DLUR Nome de PU	O CPNAME deve corresponder ao nome de PU local. Especifique este parâmetro quando NÃO estiver utilizando IDNUM= e IDBLK=.

A Tabela 19 lista os seguintes parâmetros na instrução PATH, que são utilizados no estabelecimento de uma conexão do sistema central com a estação de trabalho.

Tabela 19. Parâmetro DLUR do Communications Server VTAM que corresponde à Conexão do Sistema Central com a Estação de Trabalho

VTAM	Communications Server	Comentários
DLURNAME=	Configurar Nó Nome completo do CP (segundo campo)	O DLURNAME fornece o nome do nó DLUR que possui a PU do DLUR. Para o Communications Server, este é nome completo do CP.
DLCADDR= (1,C,INTPU)		Obrigatório. Este parâmetro informa ao DLUR que a conexão é destinada a uma PU interna.
DLCADDR= (2,X,zzzzzzzz)	Configurar PUs do DLUR ID de Bloco e ID de unidade física	O zzzzzzzz em DLCADDR=(2,X,zzzzzzzz) deve corresponder ao ID de Nó. Especifique este parâmetro quando NÃO estiver utilizando o DLCADDR=(3,C,puname).
DLCADDR= (3,C,puname)	Configurar PUs do DLUR Nome de PU	O nome de PU no DLCADDR=(3,C,puname) deve corresponder ao nome de PU Local. Especifique este parâmetro quando NÃO estiver utilizando DLCADDR=(2,X,zzzzzzzz).

NPSI e o Communications Server (X.25)

O suporte X.25 do Communications Server permite a transmissão de estruturas SNA através de uma rede X.25. O X.25 considera estruturas SNA como dados brutos e os transmite como pacotes de dados dentro de dados. Os dois nós de rede não estão conectados diretamente, mas estão conectados a um intermediário chamado: rede de dados de comutação de pacotes (PSDN). A rede X.25 pode compreender quaisquer das conectividades X.25.

O software que interage com o PSDN e que agrupa os dados SNA dentro de pacotes e os extrai intactos é uma parte integral do Communications Server. No sistema central S/370, as funções X.25 são controladas através um produto de software separado chamado X.25 Network Control Program Packet Switching Interface (NPSI). As definições de NPSI são geradas juntamente com o NCP e o software NPSI é executado em harmonia com o NCP no mesmo controlador 3705, 3725, 3720 ou 3745.

A maioria dos parâmetros X.25 especificados no Communications Server e no NPSI tem valores que estão de acordo com você e o provedor da rede X.25 em vez de entre os dois nós. Por exemplo, com uma conexão SDLC em uma linha não discada, o controlador de sistema central (NCP) é configurado para chamar seletivamente um determinado endereço secundário. O Communications Server é configurado para responder àquele endereço em uma ligação física entre a estação de trabalho Communications Server e o sistema central.

Conexões NPSI sobre X.25

A Tabela 20 compara parâmetros do Communications Server e do sistema central para conexões NPSI sobre X.25.

Tabela 20. Referência Cruzada de Parâmetros PC/Sistema Central: Conexões NPSI sobre X.25

NPSI	Perfil/Parâmetros do Communications Server	Comentários
X25.LINE TYPE=	Tipo de DLC Porta COM X.25, X.25-WAC	Especifique TYPE=P para PVCs e TYPE=S para SVCs para definição de linha NPSI X.25.
CALL= (somente para o tipo = S)	Configurar Dispositivos Porta COM X.25, X.25-WAC Intervalo de circuito virtual	As faixas de circuito virtual devem corresponder às subscrição de rede X.25.
MAXDATA=	Configurar Dispositivos Porta COM X.25, X.25-WAC Tamanho máximo de PIU (256-4105)	Este valores não precisam corresponder.
VWINDOW	Configurar Dispositivos Porta COM X.25, X.25-WAC Tamanho de janela (1-7)	O tamanho de janela SVC/PVC deve corresponder às subscrições X.25.

Como Configurar Conectividade do Sistema Central

Tabela 20. Referência Cruzada de Parâmetros PC/Sistema Central: Conexões NPSI sobre X.25 (continuação)

NPSI	Perfil/Parâmetros do Communications Server	Comentários
MWINDOW	Configurar Dispositivos Porta COM X.25, X.25-WAC Valores de estrutura Tamanho de janela (1-7)	
FRMLGTH	Configurar Dispositivos Porta COM X.25, X.25-WAC Seqüência de estrutura Módulo	O valor FRMLGTH do sistema central deve ser no mínimo MAXPKT +3 ao executar o Módulo 8 ou MAXPKT +4, ao executar o Módulo 128. O tamanho do Módulo do Communications Server e sistema central e os tamanhos de pacotes devem corresponder à subscrição X.25.
MAXPKTL	Configurar Dispositivos Porta COM X.25, X.25-WAC Tamanho de pacote	Os tamanhos de pacote SVC/PVC do sistema central devem corresponder ao valor de subscrição X.25.

VTAM/NCP e o Communications Server (X.25)

A Tabela 21 compara parâmetros do Communications Server e sistema central para X.25 (VTAM/NCP).

Tabela 21. Referência Cruzada de Parâmetros PC/Sistema Central: X.25 (VTAM/NCP)

VTAM/NCP	Perfil/Parâmetros do Communications Server	Comentários
NETID=	Configurar Nó Nome completo do CP (primeiro campo)	Isto identifica a rede SNA à qual você se conecta utilizando o Communications Server.
NOME PU		Utilize sempre um nome de PU. Este nome de PU não deve ser o mesmo que o CPName local, portanto defina uma LU para o ponto de controle.
IDBLK=	Configurar Nó ID de nó local ID de Bloco	Os 3 primeiros dígitos hexadecimais do ID de nó local , que assumem como padrão X'05D' para o Communications Server. Especifique este parâmetro utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.
IDNUM=	Configurar Nó ID de nó local ID de unidade física	O IDNUM do sistema central deve corresponder aos últimos 5 caracteres hexadecimais do ID de nó local . Especifique este parâmetro quando estiver utilizando as linhas discadas ou omita-o, se utilizar o CPNAME=.

Como Configurar Conectividade do Sistema Central

Tabela 21. Referência Cruzada de Parâmetros PC/Sistema Central: X.25 (VTAM/NCP) (continuação)

VTAM/NCP	Perfil/Parâmetros do Communications Server	Comentários
CPNAME=	Configurar Nó Nome completo do CP (segundo campo)	Especifique este parâmetro ao utilizar linhas discadas ou omita ao utilizar IDBLK= e IDNUM=.
(TRANSFR * BFRS) - 47	Configurar Dispositivos Porta COM X.25, X.25-WAC Tamanho máximo de PIU (265-4105)	O Tamanho máximo de PIU deve ser igual ao valor definido no sistema central.
MAXDATA=	Configurar Dispositivos Porta COM X.25, X.25-WAC Tamanho máximo de PIU (265-4105)	Estes valores não precisam corresponder.
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Estes parâmetros devem ter o mesmo valor. Para LUs independentes, o VTAM recomenda criar uma definição CDRSC ou utilizar o operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições de codificação do CDRSC para LUs independentes, consulte <i>VTAM Network Implementation Guide</i> Nenhuma definição de sistema central será requerida para LUs dependentes, se a definição dinâmica ou SDDLU for utilizada para LUs independentes em VTAM 3.4 ou posterior.

APPC sobre X.25

A Tabela 22 corresponde aos parâmetros para uma estação de trabalho do Communications Server executando o advanced program-to-program communications (APPC) que se conecta a um sistema central através do X.25.

Tabela 22. Referência Cruzada de Parâmetros PC/Sistema Central: APPC em uma Rede Token-Ring IBM Utilizando X.25 para um Sistema Central

NCP	Perfil/Parâmetros do Communications Server	Comentários
LU NAME	Configurar LU Local 6.2 Nome de LU local ou: Configurar Nó Nome completo do CP (segundo campo)	

Como Configurar Conectividade do Sistema Central

Tabela 22. Referência Cruzada de Parâmetros PC/Sistema Central: APPC em uma Rede Token-Ring IBM Utilizando X.25 para um Sistema Central (continuação)

NCP	Perfil/Parâmetros do Communications Server	Comentários
LOCADDR	Configurar LUs do Sistema Central Endereço da NAU	Estes parâmetros <i>devem</i> ter o mesmo valor. Para LUs independentes, o VTAM recomenda a criação de uma definição CDRSC ou a utilização do operando DYNLU em vez da codificação LOCADDR=0. Para obter mais informações sobre as definições de codificação CDRSC para LUs independentes, consulte o <i>VTAM Network Implementation Guide</i> Nenhuma definição de sistema central será requerida para LUs dependentes, se a definição dinâmica ou SDDLUF for utilizada para LUs independentes em VTAM 3.4 ou posterior.
NETID APPL	Configurar LU Parceira 6.2 Nome de LU parceira	
VTAM Interpret Table	Configurar Parceira LU 6.2 Nome de LU parceira	Somente para LUs dependentes.
LOGMODE Table LOGMODE=	Configurar Modo Nome do modo	Estes parâmetros <i>devem</i> corresponder.
LOGMODE Table RUSIZES=	Configurar Modo Tamanho de RU Máximo (256–32767)	Estes valores devem corresponder.

Definições de Linha do Sistema Central AS/400

As definições de linha do sistema central AS/400 incluem parâmetros de sistema central OS/400 correspondentes com os parâmetros do Communications Server. A Tabela 23 contém os parâmetros de linha SDLC.

Tabela 23. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Definição de Linha de Programa do Sistema Central OS/400

OS/400	Perfil/Parâmetros do Communications Server	Comentários
NRZI= Codificação de Dados	Conexões de Configuração SDLC-WAC, SDLC-MPA, Porta COM Codificação NRZI	O Communications Server utiliza USE_NRZI_ENCODING=0 e USE_NRZI_ENCODING=1. Este parâmetro é encontrado apenas em PCMs para o Tipo de Modem: Comutado Síncrono, Não-Comutado Síncrono e Sincronização Automática.
Seleção da velocidade de transmissão	Configurar Dispositivos Somente Porta COM Configurar modem	Os parâmetros nos dois sistemas para os tipos de conexão de modem, assíncronos comutado, devem corresponder.

Como Configurar Conectividade do Sistema Central

Tabela 23. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Definição de Linha de Programa do Sistema Central OS/400 (continuação)

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Tamanho de estrutura máximo (MAXFRAME)	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Contagem de janelas de recepção (1-30)	Valores assíncronos não-comutado não precisam corresponder.
Estruturas pendentes máximas (MAXOUT)	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Contagem de janelas de recepção (1-30)	A Contagem de janela de recepção no Communications Server deve ser igual ao parâmetro MAXOUT no sistema central AS/400.

Definições do Controlador do Sistema Central AS/400

A definição do controlador de sistema central AS/400 inclui parâmetros de programa de sistema central OS/400 com parâmetros do Communications Server correspondentes.

A Tabela 24 mostra os parâmetros do programa do sistema central OS/400.

Tabela 24. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Parâmetros do Controlador

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Linktype: *SDLC	Tipo de DLC SDLC-WAC, SDLC-MPA Porta COM	O tipo de ligação nos dois sistemas deve corresponder. Este parâmetro está na descrição da linha, mas incluída para complementação.
Linha Não-Discada Conectada	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Linha Discada	Este parâmetro é para conexões não-discadas. Este valor deve corresponder a uma definição de linha de sistema central definida anteriormente.
Lista de Linhas Discadas	(nenhum)	Este parâmetro é para conexões discadas. Este valor deve corresponder a uma definição de linha de sistema central definida anteriormente.
Tamanho Máximo da Estrutura	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Tamanho de PIU Máximo (265-4105)	Este valores não precisam corresponder.
Identificador da rede remota	Configurar Nó Nome completo do CP (primeiro campo)	Estes valores devem corresponder.
Nome do ponto de controle remoto	Configurar Nó Nome completo do CP (segundo campo)	Estes valores devem corresponder.

Como Configurar Conectividade do Sistema Central

Tabela 24. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Parâmetros do Controlador (continuação)

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Função da ligação de dados:	Conexões de Configuração SDLC-WAC, SDLC-MPA, Porta COM Função da estação de ligação	Os parâmetros nos dois sistemas são complementares. Se a função do sistema central for principal, a estação de trabalho do Communications Server deverá ser configurada como secundária ou negociável. A não ser que o multiponto (*MP) seja utilizado, é melhor definir a função de ligação de dados como negociável (*NEG).
Endereço de estação	Configurar Dispositivos SDLC-WAC, SDLC-MPA, Porta COM Endereço da estação de ligação (01-FE)	Estes valores devem corresponder.
Suporte de sessão CP APPN: (Sim/Não)	Conexões de Configuração SDLC-WAC, SDLC-MPA, Porta COM Suporte APPN	Devem corresponder se forem desejadas as sessões CP-CP.
tipo do nó APPN:	Conexões de Configuração SDLC-WAC, SDLC-MPA, Porta COM Tipo de CP Adjacente	Estes valores devem corresponder.

Definições de Dispositivo do Sistema Central AS/400

O sistema central AS/400 pode criar uma definição de dispositivo quando a estação de trabalho do Communications Server for conectada sem uma definição de dispositivo definida anteriormente.

A Tabela 25 contém os parâmetros de dispositivo do programa do sistema central OS/400.

Tabela 25. Referência Cruzada dos Parâmetros do Communications Server com AS/400: Parâmetros do Dispositivo

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Nome da localização remota	Configurar LU local 6.2 Nome de LU local ou: Configurar Nó Nome completo do CP (segundo campo)	Estes valores devem corresponder.
Controlador conectado	(nenhum)	Este parâmetro é para conexões não-discadas. Este valor deve corresponder a uma definição de linha de sistema central definida anteriormente.
Nome da localização local		Utilize o padrão fornecido.

Como Configurar Conectividade do Sistema Central

Tabela 25. Referência Cruzada dos Parâmetros do Communications Server com AS/400: Parâmetros do Dispositivo (continuação)

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Identificador da rede remota	Configurar Nó Nome completo do CP (primeiro campo)	Utilize o padrão fornecido.
Modo	Configurar Modo Nome do modo	Utilize o padrão fornecido.

Descrição de Linha do Sistema Central AS/400 e o Communications Server

A Tabela 26 contém a descrição da linha do programa do sistema central AS/400.

Tabela 26. Referência Cruzada dos Parâmetros Sistema Central/PC: Descrição de Linha

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Endereço da placa local:	Conexões de Configuração Endereço de Destino da Rede Local	Os dois endereços devem corresponder para se comunicarem.

Descrição do Controlador do Sistema Central AS/400 e o Communications Server

A Tabela 27 contém a descrição do controlador de programa do sistema central OS/400.

Tabela 27. Referência Cruzada dos Parâmetros do Sistema Central/PC: Descrição do Controlador

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Linha discada ativa	(nenhum)	Este parâmetro é para conexões não-discadas. Este valor deve corresponder a uma definição de linha de sistema central definida anteriormente.
Ponto de controle remoto	Configurar Nó Nome completo do CP (segundo campo)	Os nomes devem corresponder.
Identificador da rede remota	Configurar Nó Nome completo do CP (primeiro campo)	Utilize o padrão ou combine os parâmetros se forem diferentes do ID da rede local do AS/400.
Descrição do controlador de modelo		Este parâmetro deve ser YES, se o AS/400 utilizar uma rede de conexão.
ID da rede de conexão e CPName da rede de conexão	Configurar Redes de Conexão Nome da rede de conexão	Estes valores devem corresponder para todos os nós que estiverem participando de uma rede de conexão.

Como Configurar Conectividade do Sistema Central

Descrições Biaxiais do AS/400

A Tabela 28 contém a descrição biaxial do AS/400.

Tabela 28. Referência Cruzada dos Parâmetros do Sistema Central/PC: Descrição do Controlador

AS/400	Perfil/Parâmetros do Communications Server	Comentários
Linha não-discada ligada	(nenhum)	Este parâmetro é para conexões não-comutadas. Este valor deve corresponder a uma definição de linha de sistema central determinada anteriormente.
Ponto de controle remoto	Configurar Nó Nome completo do CP (segundo campo)	Os nomes devem corresponder.
Identificador da rede remota	Configurar Nó Nome completo do CP (primeiro campo)	Utilize o padrão ou combine os parâmetros se forem diferentes do ID da rede local do AS/400.
Função da ligação de dados=*SEC:	Conexões de Configuração SDLC-WAC, SDLC-MPA Porta COM Função de estação de ligação	Os parâmetros nos dois sistemas são complementares. Se a função do sistema central for principal, a estação de trabalho do Communications Server deve ser configurada como secundária ou negociável. A não ser que o multiponto (*MP) seja utilizado, é melhor definir a função de ligação de dados como negociável (*NEG).

Definições de Linha do Sistema Central AS/400 (X.25)

As definições de linha do sistema central AS/400 incluem parâmetros de sistema central OS/400 correspondentes com os parâmetros do Communications Server. A Tabela 29 contém os parâmetros de linha X.25.

Tabela 29. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Definição de Linha de Programa do Sistema Central OS/400 (X.25)

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Endereço de Rede Local	Configurar Dispositivos Endereço Local	Ambos os endereços geralmente são determinados pelo provedor da rede.
Tipo de Conexão	Configurar Dispositivos Porta X.25-COM X.25-WAC Linha Discada	O Tipo de Conexão em ambos os sistemas deve corresponder.
Suporte ao DCE X.25	N/A	Deverá ser definido para SIM, se a conexão entre os dois sistemas for ponto a ponto, sem passar por uma rede X.25.

Como Configurar Conectividade do Sistema Central

Tabela 29. Referência Cruzada dos Parâmetros do Communications Server com o AS/400: Definição de Linha de Programa do Sistema Central OS/400 (X.25) (continuação)

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Tamanho Máximo da Estrutura	Configurar Dispositivos Porta X.25-COM X.25-WAC Tamanho Máximo da PIU	O Tamanho Máximo da estrutura em ambos os sistemas deve corresponder.
Tamanho do Pacote Padrão	Configurar Dispositivos Porta X.25-COM X.25-WAC Tamanho do Pacote	Esse valor é determinado pelo provedor de rede e é o mesmo para Transmissão e Recepção.
Tamanho Máximo do Pacote	N/A	Esse valor é determinado pelo provedor da rede.
Módulo	Configurar Dispositivos Porta X.25-COM X.25-WAC Seqüência	Esse valor é determinado pelo provedor da rede.
Tamanho da Janela Padrão	Configurar Dispositivos Porta X.25-COM X.25-WAC Tamanho da Janela	Esse valor é determinado pelo provedor de rede e é o mesmo para Transmissão e Recepção.
Inserir Endereço da Rede	Configurar Dispositivos Porta X.25-COM X.25-WAC	Esse valor é determinado pelo provedor de rede e deve ser o mesmo para ambos os sistemas.
Entradas do Canal Lógico	Configurar Dispositivos Porta X.25-COM X.25-WAC Circuito Virtual Intervalos	Esses valores são determinados pelo provedor de rede e pelo tipo de circuito virtual X.25.

Definições do Controlador do Sistema Central AS/400 (X.25 PVC)

A definição do controlador de sistema central AS/400 inclui parâmetros de programa de sistema central OS/400 com parâmetros do Communications Server correspondentes.

A Tabela 30 mostra os parâmetros do programa do sistema central do OS/400 para o PVC X.25.

Tabela 30. Referência Cruzada de Parâmetros PVX X.25 do Communications Server com o AS/400: Parâmetros do Controlador

OS/400	Perfil/Parâmetros do Communications Server	Comentários
ID de canal lógico X.25	Conexões de Configuração Porta COM X.25, X.25-WAC Número do Canal Lógico	Esses valores são determinados pelo provedor de rede.
Tipo de ligação: *X25	Conexões de Configuração	O Tipo de Ligação em ambos os sistemas deve corresponder.
Conexão Comutada: *NO		Todos os PVCs não são comutados.

Tabela 30. Referência Cruzada de Parâmetros PVX X.25 do Communications Server com o AS/400: Parâmetros do Controlador (continuação)

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Tamanho Máximo da Estrutura	Configurar Dispositivos Porta X.25-COM X.25-WAC Tamanho Máximo da PIU	Os valores do Tamanho Máximo da Estrutura não precisam corresponder.
Função da Ligação de Dados	Configurar Dispositivos Porta X.25-COM X.25-WAC Função da Estação de Ligação	Os parâmetros nos dois sistemas são complementares. Se a função do sistema central for principal, a estação de trabalho do Communications Server deve ser configurada como secundária ou negociável.
Nível de Rede X.25	Configurar Dispositivos Porta X.25-COM X.25-WAC Conformidade CCITT	Esses valores são determinados pelo provedor de rede.
Protocolo de Nível de Ligação X.25: *QLLC		Esse valor deve ser QLLC.

Definições do Controlador do Sistema Central AS/400 (X.25 SVC)

A definição do controlador de sistema central AS/400 inclui parâmetros de programa de sistema central OS/400 com parâmetros do Communications Server correspondentes.

A Tabela 31 mostra os parâmetros do programa do sistema central do OS/400 para o SVC X.25.

Como Configurar Conectividade do Sistema Central

Tabela 31. Referência Cruzada de Parâmetros SVC X.25 do Communications Server com o AS/400: Parâmetros do Controlador (continuação)

OS/400	Perfil/Parâmetros do Communications Server	Comentários
Nível de Rede X.25	Configurar Dispositivos Porta X.25-COM X.25-WAC Conformidade CCITT	Esses valores são determinados pelo provedor de rede.
Protocolo de Nível de Ligação X.25: *QLLC		Esse valor deve ser QLLC.

Como Configurar Conectividade do Sistema Central

Capítulo 15. Como Implementar Configurações do Communications Server

A seguir, é apresentado um procedimento sugerido para instalar e configurar o software para sua rede:

1. Planejar o hardware.
2. Planejar as aplicações de software.
3. Criar suas convenções de nomenclatura.
4. Definir endereços de rede.
5. Selecionar ferramentas de configuração e instalação.
6. Definir a configuração do gabarito.
7. Criar configurações e instalar.
8. Criar materiais do usuário.
9. Manter sua rede.

Este capítulo fornece as informações necessárias para a conclusão do procedimento sugerido.

Introdução

Uma configuração de gabarito define as informações sobre configuração comuns a um grupo de servidores. Você pode criar uma ou mais configurações de gabaritos. Cada arquivo de configuração do servidor começa com a configuração do gabarito e pode conter os parâmetros mínimos necessários para personalizar a configuração para esse servidor. Isto resulta em uma configuração de servidor simplificada.

A configuração do gabarito também pode ser utilizada para especificar opções de configuração que não podem ser especificadas utilizando arquivos de resposta.

Para obter informações sobre como utilizar arquivos de resposta e arquivos de gabaritos para configuração e instalação, consulte "Configuração com Arquivos de Gabarito e de Resposta" na página 191.

Lembre-se de somar os totais de requisitos de RAM e de espaço em disco rígido para cada estação de trabalho à medida que coleta informações nas etapas seguintes. Dessa forma, você pode garantir que tem o hardware adequado para seus usuários quando eles começarem a utilizar o software escolhido.

Etapa 1. Como Planejar o Hardware

Se você já tiver determinado que pode utilizar servidores existentes, será necessário certificar-se de que o hardware existente tenha memória e espaço em disco rígido adequados. O hardware existente também deve ter unidades de sistema, monitores, impressoras, teclados, placas, modems e cabos corretos para o software que será instalado.

Se você for adquirir novos servidores, registre o hardware nas planilhas preparadas para os usuários.

Como Desenvolver Configurações do Communications Server

Memória

Consulte *Iniciação Rápida* para obter os requisitos de memória para o Communications Server.

Capacidade de Memória

Quando planejar o hardware para execução no Communications Server, é importante analisar como o servidor será utilizado em termos de capacidade. Determine o tipo de sessões que serão suportadas pelo Communications Server. Elas incluem, mas não estão limitadas a sessões TN3270E, sessões do cliente API de SNA e sessões tradicionais do SNA em um sistema central. Com base neste número, é possível calcular a carga média no servidor e determinar a quantidade correta de memória para ele.

Nota: Estas estimativas são adicionais aos requisitos do sistema operacional básico (Windows NT Server) e de outras aplicações simultaneamente em execução no mesmo sistema.

Utilize a tabela a seguir para determinar a carga média no servidor:

Tabela 32. Capacidade de Memória

Tipo de Sessão do Cliente	Utilização de Memória por Sessão
SNA Gateway (tradicional)	29,9 KB
Cliente API de SNA	25,2 KB
TN3270E	15,8 KB

O consumo de memória estimado de um Communications Server ativo sem ligações ou sessões ativas é de 21 MB. Para minimizar a perda de desempenho, é melhor reduzir a quantidade de paginação (troca de segmentos da memória para o disco) que ocorre. Tente obter a maior quantidade de memória real disponível necessária pelo software em execução, deixando de 5 a 10 MB adicionais como um buffer. Por exemplo, uma instalação do Communications Server que suporta 1000 sessões de cliente TN3270E vai requerer as seguintes quantidades de memória (com base nos valores na Tabela 32).

Sistema operacional Microsoft Windows NT Server	19,0 MB (estimado)
Communications Server para Windows NT	21,0 MB
Sessões TN3270E (1 000 X 15,8 KB)	15,8 MB
Contingência	10,0 MB
Memória Total Recomendada	65,8 MB

Nota: 65.8 MB não é uma quantidade de memória necessária para sessões TN3270E 1000. Recomenda-se para melhor desempenho.

Velocidade da CPU

Quando determinar a velocidade mínima necessária do processador, é preciso saber o número médio de transações que serão processadas pelo servidor a cada

Como Desenvolver Configurações do Communications Server

minuto. Uma transação é qualquer troca de informações entre o cliente e o sistema central através do servidor, quer seja uma atualização de tela ou uma entrada do banco de dados solicitada.

Quando calcular a carga média da CPU, multiplique o número médio de sessões pelo número médio de transações por minuto por sessão e o fator de escala da tabela a seguir (com base no tipo de sessão).

Tipo de Sessão do Cliente	Fator de Carga da CPU (100 Mhz)	Fator de Carga da CPU (166 Mhz)
SNA Gateway (tradicional)	.004	.002
Cliente API de SNA	.021	.011
TN3270E	.011	.006

Por exemplo, para suportar 1000 sessões TN3270E simultâneas, com uma média de 6,7 transações por minuto, a carga média na CPU de 166 Mhz seria de $1 \times 6,7 \times .006$ ou de 40,2%. O desempenho é reduzido rapidamente quando a utilização da CPU excede 80%. Uma CPU mais rápida melhoraria o desempenho do Communications Server e do sistema. Mais usuários e transações conseguiriam tirar vantagem do servidor simultaneamente. Enquanto não existir velocidade máxima da CPU suportada pelo Communications Server, 100 Mhz é o mínimo recomendado.

Etapa 2. Como Planejar Aplicações de Software

As aplicações de software possuem requisitos além dos requisitos do Communications Server. Para obter mais informações, consulte a documentação da aplicação de software.

Etapa 3. Como Criar Convenções de Nomenclatura

As redes criadas com o Communications Server requerem a criação e utilização de diversos nomes para vários objetos na rede. Alguns destes nomes podem ser iguais de servidor para servidor, mas os outros nomes devem ser exclusivos na rede para evitar conflitos entre os servidores que tentam acessar recursos da rede.

Por exemplo, duas Redes Locais podem ter alguns dos mesmos nomes de domínio definidos. Desde que estas Redes Locais não estejam conectadas, não ocorrerão conflitos. Entretanto, se elas tiverem que ser conectadas posteriormente a uma Rede Local principal, seus nomes entrarão em conflito na Rede Local.

Isto significa que você deve criar convenções de nomenclatura. As convenções de nomenclatura são regras e padrões utilizados para atribuir nomes aos vários recursos da rede.

As seções a seguir listam as convenções de nomenclatura que você precisa planejar. Se já souber as convenções de nomenclatura que serão utilizadas no planejamento, registre-as enquanto planeja sua rede.

Critérios de Nomenclatura

Quando estiver criando convenções de nomenclatura, será necessário determinar:

- Os critérios a serem utilizados para criar nomes e endereços para a rede

Como Desenvolver Configurações do Communications Server

- Como será mantida a compatibilidade desses nomes e endereços e, onde necessário, exclusivos na rede

Por exemplo, se estiver conectando um servidor a uma rede do computador central, você descobrirá que a maioria dos nomes que devem ser utilizados na rede são escolhidos pela equipe do sistema central. Neste caso, para as unidades físicas e lógicas requeridas pelo sistema central, você deve registrar os nomes fornecidos para os arquivos de configuração do servidor.

Como outro exemplo, você pode selecionar a nomeação dos servidores da rede após os nomes das pessoas que os utilizam. Para uma rede pequena, isto pode ser viável, desde que o número de nomes seja pequeno e você consiga mantê-los exclusivos. Entretanto, isto não funcionaria em uma rede grande porque os nomes das pessoas geralmente não são exclusivos. É necessário criar uma outra convenção para os nomes de estações de trabalho em uma rede grande.

Independente dos critérios escolhidos para os nomes, certifique-se de que os tenha registrado. Dessa forma, você pode consultar as informações apropriadas a qualquer momento que incluir novos recursos na rede.

Tipos de Nomes e suas Restrições

A maioria dos nomes devem ser exclusivos na rede em que você os utiliza. As seções a seguir listam os tipos de nomes que podem ser encontrados durante o planejamento, instalação e configuração de uma rede. Você deve rever estes nomes antes de começar a planejar sua rede para familiarizar-se com eles.

Para cada nome são fornecidas as seguintes informações:

- Uma definição
- Se o nome deve ser exclusivo em uma rede
- Restrições de nomenclatura

Nomes Utilizados por mais de um Componente

Os nomes utilizados por mais de um componente são:

- IDs da rede
- Senhas
- IDs do usuário
- Nomes da unidade endereçável da rede (NAU)

IDs da Rede: IDs da rede são os nomes fornecidos às redes e utilizados por todos os servidores e estações de trabalho (nós) na rede específica para manter uma identidade exclusiva em todas as redes conectadas. O ID da rede também é utilizado em registros de erros e em alertas de gerenciamento de rede associados aos erros de sistema da rede.

Existem duas formas de consultas em redes. Uma forma é como uma rede física que consiste em uma “linha” em um ambiente token-ring ou em uma “cadeia” em um ambiente Ethernet ou rede de PC. A outra forma é como uma rede lógica que pode não ser igual à rede física. Duas ou mais redes físicas (por exemplo, duas token rings e uma cadeia Ethernet) podem ser conectadas com a intenção de mantê-las na mesma rede lógica.

Como Desenvolver Configurações do Communications Server

Os IDs da rede são exclusivos entre as redes lógicas, caso contrário, as redes seriam logicamente a mesma rede. Em uma rede lógica, os nomes de LU devem ser exclusivos para evitar conflitos de nomenclatura. Entre as redes lógicas, o ID da rede garante nomes exclusivos. Um nome de LU pode ser o mesmo em duas redes lógicas; entretanto, o ID da rede para cada rede lógica torna exclusivos os nomes completos das LUs. Mesmo que as redes não estejam conectadas no momento, os IDs da rede devem ser exclusivos se você planejar unir as redes no futuro.

Você deve registrar os IDs da rede com a IBM. Isto garante que as redes SNA podem ser interconectadas posteriormente sem gerar conflitos. Entre em contato com uma Filial IBM para obter mais informações sobre como registrar os IDs da rede.

As restrições para os IDs da rede são:

- **Comprimento:** De 1 a 8 caracteres
- **Caracteres permitidos:** A a Z, 0 a 9, \$, @, #

Senhas: Senhas são funções de segurança requeridas por aplicações e serviços configurados apropriadamente para proteger os dados e restringir acesso aos recursos.

As senhas não precisam ser exclusivas na rede. Elas são específicas dos usuários.

As restrições para as senhas LU-LU são:

- **Comprimento:** De 1 a 8 caracteres
- **Caracteres permitidos:** Qualquer cadeia hexadecimal

As restrições para outras senhas, como por exemplo, nas conexões CPI-C e AS/400 são:

- **Comprimento:** De 1 a 10 caracteres
- **Caracteres permitidos:** Qualquer cadeia ASCII

IDs do Usuário: IDs do usuário são nomes de identificação exclusivos fornecidos aos usuários dos recursos da rede para que possam acessar recursos do banco de dados, da Rede Local ou do sistema central com emulação.

Os IDs do usuário devem ser exclusivos na rede.

As restrições para os IDs do usuário são:

- **Comprimento:** De 1 a 8 caracteres
- **Caracteres permitidos:** A a Z, a a z, 0 a 9, \$, @, #

Nomes da Unidade Endereçável da Rede (NAU)

Os tipos de nomes que você pode ter que especificar no Communications Server são:

- Nomes do ponto de controle (CP) (nomes de nós locais)
- Nomes da unidade lógica (LU)

Nomes do Ponto de Controle (CP) (Nomes de Nós Locais): O ponto de controle (CP) é responsável pelo gerenciamento do nó e de seus recursos. Em um nó final APPN, o ponto de controle deve se comunicar com o ponto de controle em um nó da rede adjacente para obter serviços da rede APPN. Em um nó da rede APPN, o ponto de controle deve se comunicar com os pontos de controle em nó da rede

Como Desenvolver Configurações do Communications Server

para gerenciar a rede. O ponto de controle direciona determinadas funções como, ativação e desativação da placa, ativação e desativação da ligação e ajuda as LUs no início e término da sessão.

O nome do ponto de controle é a segunda metade do nome completo do CP na definição do NÓ do Communications Server.

Os nomes do ponto de controle devem ser exclusivos em uma rede. Entretanto, um nó pode ter vários nomes de PU que são estabelecidos na definição de conexão (**LINK_STATION**) e trocados no XID3 para sistemas centrais diferentes. Estes vários nomes de PU devem ser exclusivos no nó e no sistema central que está sendo conectado.

A PU e o ponto de controle não são iguais para o VTAM da subárea. É definido um nome de PU para cada nó periférico em um domínio VTAM nesse VTAM e representa a visualização que o VTAM tem dos nós periféricos. No VTAM, os nomes da PU não são conhecidos pelos nós periféricos; ou seja, o VTAM não envia os nomes da PU para os nós periféricos. Se desejar que o nome da PU em um nó periférico seja igual ao que foi definido no VTAM, você deverá coordená-lo. É recomendável que faça isto, mas para o SNA não é necessário.

Para o VTAM, o ponto de controle é uma LU utilizada para ativar sessões de LU 6.2 entre o ponto de controle e uma LU do VTAM (por exemplo, CICS). O nome do ponto de controle definido no nó periférico deve corresponder a uma definição de LU no VTAM se o VTAM iniciar sessões de LU 6.2 no ponto de controle. Caso contrário, o VTAM saberá o nome do ponto de controle quando o nó periférico iniciar uma sessão em uma LU do VTAM.

Para o Communications Server, o nome do ponto de controle (não incluindo o ID da rede) é considerado como o nome do ponto de controle do nó local e seu nome de PU. O único fluxo que contém o nome da PU do nó periférico é um alerta. Entretanto, quando o Communications Server (APPC/APPN) envia um alerta, ele inclui o nome do ponto de controle (o tipo de recurso é o CP) no alerta, não o nome de uma PU. Se os emuladores enviarem o nome de uma PU nos alertas, o nome será igual ao nome do ponto de controle (novamente, porque o Communications Server utiliza o nome do ponto de controle como o nome da PU do nó). O ponto focal do sistema central pode ser definido somente em uma ligação onde o nome da PU é igual ao nome do ponto de controle. Além disso, as ligações ao sistema central com um nome de PU diferente do nome do ponto de controle não podem ter sessões CP-CP com o sistema central ou rotear o tráfego do APPN através da ligação. Todos os alertas incluem o nome do ponto de controle mesmo que o alerta seja causado por uma condição em uma ligação que esteja utilizando outra PU.

As restrições para os nomes de nós locais são:

- **Comprimento:** De 1 a 8 caracteres
- **Caracteres permitidos:** A a Z, 0 a 9, \$, @, #
- **Primeiro caractere:** A a Z, \$, @, #

Nomes da Unidade Lógica (LU): Os nomes da unidade lógica (LU) são nomes fornecidos às entidades lógicas do SNA em um nó que fornece funções de suporte para o processamento de transações. Isto permite que elas se comuniquem com outras LUs na rede, incluindo aplicações do sistema central.

As restrições para nomes de LU são:

Como Desenvolver Configurações do Communications Server

- **Comprimento:** De 1 a 8 caracteres
- **Caracteres permitidos:** A a Z, 0 a 9, \$, @, #

Nomes de LU Sockets sobre SNA: O Sockets sobre SNA Gateway deve ter um nome de LU configurado para que o Gateway seja inicializado com êxito. O Sockets sobre SNA Gateway vai definir dinamicamente o nome da LU configurado para o Communications Server durante a inicialização.

A utilização da convenção de nomenclatura predefinida para os nomes de LU do Sockets sobre SNA pode ajudá-lo a:

- Controlar quais os nomes de LUs do Sockets sobre SNA Gateway e os nomes que representam outras LUs na rede.
- Analisar e corrigir erros de mapeamento e roteamento se ocorrerem.
- Permitir que o mapeamento algorítmico seja utilizado durante o mapeamento de endereços IP para nomes de LU do Sockets sobre SNA.

Para obter mais informações sobre o mapeamento de endereços IP para nomes de LU, consulte “Como Configurar AnyNet Sockets sobre SNA” na página 84.

Etapa 4. Como Definir Endereços da Rede

Garanta a compatibilidade e exclusividade dos endereços em sua rede. Cada endereço deve ser exclusivo. Os endereços que forem definidos vão depender de como a rede foi configurada. As seções a seguir descrevem os endereços para:

- Rede Loc.
- SDLC
- X.25

Registre os endereços que utiliza para certificar-se, quando necessário, de que os endereços não estejam em conflito e de que sejam compatível com as convenções de nomenclatura que foram escolhidas.

Endereços da Placa de Rede Local

Os endereços de placa da Rede Local são números hexadecimais com 12 caracteres codificados na placa adaptadora pelo fabricante (endereço de placa universalmente administrado) ou atribuídos pelo administrador da rede (endereço localmente administrado). Cada placa adaptadora de rede na estação de trabalho que está sendo configurada para comunicações da Rede Local deve ter um endereço exclusivo.

Você pode utilizar endereços universalmente administrados, também chamados de “endereços registrados”, para suas placas adaptadoras de rede ou pode atribuir endereços localmente administrados. Os endereços da placa de rede local devem ser exclusivos na rede. Se você utilizar endereços localmente administrados, certifique-se de que eles sejam exclusivos na rede.

Os endereços localmente administrados oferecem uma vantagem significativa no caso de uma falha da placa que exija a substituição dela. Você pode transferir o endereço existente para a placa substituta e evitar a alteração das configurações referentes a esse endereço. Se utilizar endereços universalmente administrados, é

Como Desenvolver Configurações do Communications Server

necessário alterar o endereço da placa adaptadora de rede de todas as estações de trabalho que acessam a placa adaptadora defeituosa.

As limitações para a configuração dos endereços da placa de rede local são:

- **Comprimento:** 12 caracteres
- **Caracteres permitidos:** A, B, C, D, E, F, 0-9
- **Faixa:** X'400000000000' a X'7FFF FFFF FFFF'

Na Rede Local, você pode optar por utilizar endereços localmente administrados da placa de rede local. Dessa forma, estará atribuindo números hexadecimais como os endereços da placa de rede local a cada uma das placas de rede local, em vez de utilizar os endereços universais da placa de rede local criados nas placas de rede local. Você pode optar por utilizar uma convenção com os seguintes critérios:

- Os primeiros 4 dígitos são sempre X'4000'
- Os próximos 3 dígitos são sempre X'268' para representar seu departamento
- Os dígitos finais estão na faixa de X'01000' a X'FFFFFF' para representar as estações de trabalho individuais de sua rede

Os endereços universalmente administrados na Ethernet estão no formato Ethernet. Você pode especificar o tipo de formato (Ethernet ou Token-ring) quando utilizar endereços localmente administrados. Quando configurar o endereço de destino em conexões SNA, certifique-se de que o formato do endereço seja igual ao especificado no remoto. Com a ponte, é possível estar em um token-ring localmente e ter a estação remota em uma Ethernet e utilizar um endereço com formato Ethernet (trocado por bytes).

Endereços da Estação Secundária de SDLC

Os endereços da estação são utilizados para identificar uma estação secundária na rede.

Os endereços da estação secundária devem ser exclusivos em uma rede. A estação principal vai se comunicar com uma estação secundária utilizando o endereço da estação secundária. A secundária vai se comunicar com a principal utilizando seu próprio endereço.

Para conexões ponto a ponto, se a estação secundária suportar o endereço de difusão X'FF', a principal vai saber o endereço da secundária remota. A secundária pode especificar qualquer valor entre X'01' e X'FE'.

Para principais que não suportam o endereço de difusão, a estação secundária deverá ser definida como o mesmo valor definido na principal. O valor deve estar entre X'01' e X'FE'.

Nota: A maioria das estações suportará o endereço de difusão; portanto, o endereço da estação secundária na principal deverá utilizar X'FF'.

As estações negociáveis possuem endereços de estação secundária local configurados entre X'01' e X'FE'. Será utilizado o endereço secundário da estação negociada para a secundária.

Para secundárias em uma conexão multiponto, o endereço deve corresponder ao valor especificado no nó que está fornecendo a função do servidor principal multiponto. O endereço estará na faixa de X'01' a X'FE'.

Endereços X.25

Os endereços X.25 são utilizados para identificar recursos que se comunicam em redes X.25. As redes X.25 implementam a recomendação CCITT que define a interface entre o equipamento terminal de dados e as redes de comutação de pacotes. Os endereços X.25 devem ser exclusivos em uma rede. Você pode obter estes endereços com o provedor da rede X.25.

Endereços Internet

Os endereços do Internet Protocol (IP) são utilizados para rotear dados através da rede. Cada sistema central TCP/IP está atribuído a pelo menos um endereço IP exclusivo. O endereço IP atribuído ao sistema central não define um sistema central na rede; ele define uma interface de rede naquele sistema central para uma rede.

Um nó do Communications Server deve ter um endereço IP exclusivo para cada interface de rede que faz o roteamento de dados do TCP/IP através do nó. Por exemplo, um nó do Communications Server que está roteando o tráfego do TCP/IP através de uma rede SNA (utilizando a função Sockets sobre SNA Gateway) precisa de endereços IP exclusivos tanto para a rede SNA como para a rede TCP/IP. O endereço IP da interface TCP/IP identifica a conexão do Gateway Sockets sobre SNA com a rede IP enquanto o endereço IP identifica a conexão com a rede SNA, que é semelhante a uma rede TCP/IP "virtual" para o sistema.

Um endereço IP consiste em um campo de endereço de 2 partes e 32 bits:

- A primeira parte do campo de endereço contém o endereço de rede; a segunda parte contém o endereço do sistema central.
- O número de bits utilizados para as partes de rede e de sistema central de um endereço IP é variável, dependendo da classe de endereços do endereço IP.
- Uma máscara de rede permite que você utilize um segmento da parte referente ao sistema central do endereço IP como um endereço de sub-rede.

A classe do endereço IP é determinada pela leitura dos 3 primeiros bits (superiores) do endereço. Conforme mostrado na Tabela 33, o Communications Server suporta as classes de endereço A, B e C. Para obter mais informações, consulte *Guide to Sockets over SNA*.

Tabela 33. Classes de Endereço IP Suportadas pelo Communications Server

Endereço Endereço	Máscara de Rede Máscara	Distribuição de Bits para Endereços de Rede e de Sistema Central	Para um endereço IP decimal pontilhado no formato <i>a.b.c.d</i> , a faixa de valores para <i>a</i> é de:
A	255.0.0.0	endereço de rede de 8 bits; endereço de sistema central com 24 bits	1 a 127 Por exemplo, 9.0.0.0 é um endereço de rede IP Classe A.
B	255.255.0.0	endereço de rede de 16 bits; endereço de sistema central de 16 bits	128 a 191 Por exemplo, 132.11.0.0 é um endereço de rede IP Classe B.

Como Desenvolver Configurações do Communications Server

Tabela 33. Classes de Endereço IP Suportadas pelo Communications Server (continuação)

Endereço Endereço	Máscara de Rede Máscara	Distribuição de Bits para Endereços de Rede e de Sistema Central	Para um endereço IP decimal pontilhado no formato <i>a.b.c.d</i> , a faixa de valores para <i>a</i> é de:
C	255.255.255.0	endereço de rede de 24 bits; endereço de sistema central de 8 bits	192 a 223 Por exemplo, 220.11.44.0 é um endereço de rede IP Classe C.

Etapa 5. Como Selecionar Ferramentas de Configuração e Instalação

O Communications Server utiliza as ferramentas de configuração explicadas nas seções a seguir. Consulte *Iniciação Rápida* para obter mais informações sobre estas ferramentas.

Aplicação de Configuração do Nó

A aplicação de **Configuração do Nó** é uma aplicação da janela de gráficos que permite gerenciar informações sobre a configuração do SNA. A aplicação utiliza uma exibição em árvore para organizar os dados de configuração do SNA para mostrar as relações entre as definições. O usuário recebe assistência para as tarefas quando cria uma configuração através de uma lista de tarefas integradas, do *Tutorial* online e do auxílio dependente de contexto. A aplicação é responsável por criar arquivos de configuração para o usuário e por verificar os dados fornecidos.

Configuração Remota

A **Configuração do Nó** também pode ser utilizada para se conectar a um Communications Server remoto e configurar diretamente seus recursos. O usuário consegue gerenciar remotamente a configuração para um Communications Server em qualquer lugar na rede.

Um cliente de administração remota instala somente aplicações administrativas em um cliente, incluindo a **Configuração do Nó**. A partir deste cliente, um usuário consegue administrar e configurar completamente qualquer Communications Server na rede.

Os clientes de administração remotos do Windows 95 e Windows NT utilizam a segurança de domínio do Windows NT, para autenticar a conexão do cliente como servidor sem digitar novamente o ID do usuário e a senha. O cliente deve ser parte de um domínio do Windows NT, pela participação em um domínio do Communications Server ou pela iniciação de sessão localmente com um ID de usuário e senha sincronizados.

Os usuários do cliente de administração remoto fora do domínio do Windows NT são solicitados a fornecerem o ID de usuário e senha, através de um prompt ou através do armazenamento de valores no arquivo de configuração do cliente.

Os usuários autorizados de clientes de administração remotos são mantidos no grupo local IBMCSADMIN, que está localizado diretamente no Communications Server ou no controlador de domínio onde está localizado o Communications Server. Esse grupo de usuário é criado durante a instalação e pode ser

Como Desenvolver Configurações do Communications Server

administrado utilizando o aplicativo Gerenciador de Usuários do Windows NT. Devem ser concedidos aos usuários do cliente de administração remoto direitos no grupo IBMCSADMIN para iniciarem sessão localmente no servidor.

Arquivo de Configuração ASCII

A **Configuração do Nó** do Communications Server armazena seus dados de configuração em um arquivo de configuração ASCII legível por seres humanos. Isto permite que o usuário modifique arquivos de configuração sem utilizar a **Configuração do Nó**. (Consulte *Configuration File Reference* para obter mais informações sobre este arquivo e sua sintaxe). Utilizando esse arquivo, um administrador da rede pode rapidamente fazer alterações na configuração utilizando tarefas automatizadas, como por exemplo, serviços de script ou de distribuição de software, tais como, o Tivoli TME10 ou o Microsoft System Management Server.

Durante a criação de configurações para um grande número de servidores a serem implementados, o administrador da rede pode criar um arquivo de configuração de gabarito que representa os elementos comuns da configuração para todos os servidores. Utilizando o arquivo de resposta somente com as alterações necessárias para cada servidor, o administrador pode distribuir o gabarito e o arquivo de resposta e mesclar os dois para criar a configuração de destino. Para obter informações detalhadas sobre como utilizar arquivos de gabarito e de resposta para configuração e instalação, consulte “Configuração com Arquivos de Gabarito e de Resposta”.

Web Administration

Através do Web administration, um usuário consegue modificar um arquivo de configuração do Communications Server, carregando o arquivo em uma janela de edição. As alterações são enviadas ao servidor, verificadas e salvas para utilização imediata. O usuário pode encerrar e reiniciar o servidor utilizando as alterações feitas ou aplicar as alterações da configuração em um sistema em execução.

Configuração com Arquivos de Gabarito e de Resposta

Os arquivos de gabarito e de resposta do Communications Server permitem criar ou modificar uma configuração utilizando um editor. Você pode configurar todas as palavras-chave e parâmetros de configuração do Communications Server com arquivos de resposta. Tanto os arquivos de gabarito como os de resposta possuem o mesmo formato que os arquivos de configuração (.ACG) do Communication Server.

Nota: O formato dos arquivos .ACG está documentado no arquivo OCDNTS50.DAT contido no diretório de instalação do Communications Server (por exemplo, C:\IBMCS). Consulte *Configuration File Reference* para obter mais informações sobre as palavras-chave e parâmetros utilizados nos arquivos .ACG.

Os arquivos de gabarito podem facilitar a distribuição em massa de configurações para servidores remotos. Um arquivo de gabarito pode especificar as palavras-chave que são mais comuns a vários servidores. Por exemplo, se você tiver vários servidores a serem configurados como SNA Gateways com suporte implícito ao cliente, muitas das palavras-chave serão idênticas. Você pode criar um arquivo de configuração de gabarito que reflita essas palavras-chave comuns.

Como Desenvolver Configurações do Communications Server

Pode utilizar arquivos de resposta para incluir, modificar ou eliminar palavras-chave em um arquivo de gabarito. O arquivo original de configuração de gabarito permanece inalterado. Um arquivo de resposta é mesclado em um arquivo de resposta especificando a palavra-chave INCLUDE no final do arquivo de gabarito. Por exemplo, se um arquivo de resposta chama-se *myconfig.rsp*, a última linha do arquivo de gabarito que utilizará o arquivo de resposta será INCLUDE = myconfig.rsp. Quando o arquivo de gabarito e o arquivo de resposta são intercalados, você pode nomear o arquivo de configuração resultante com a extensão .ACG que o diferencia dos outros arquivos .ACG.

Quando você cria configurações utilizando arquivos de gabarito e de resposta, o utilitário de verificação pesquisa diretórios na seguinte ordem:

1. O diretório local onde o utilitário de verificação está sendo chamado
2. O subdiretório PRIVATE no diretório de instalação do Communications Server.

Para garantir que o utilitário de verificação pode localizar os arquivos de gabarito e de resposta, você deve armazená-los no subdiretório PRIVATE. O subdiretório PRIVATE também é o local onde os arquivos de configuração (.ACG) estão armazenados.

Campos-chave

Campo-chave é o parâmetro em uma palavra-chave que nomeia a palavra-chave e a identifica exclusivamente das outras palavras-chave do mesmo tipo. O parâmetro @KEY_NAME especifica o campo-chave para a palavra-chave.

O campo-chave é sempre o primeiro parâmetro em uma palavra-chave que possui um campo-chave (por exemplo, **MODE_NAME** na palavra-chave **MODE**).

Algumas palavras-chave não possuem campos-chave porque podem ser especificadas somente uma vez em um arquivo de configuração. Um exemplo de palavra-chave que pode ser especificada somente uma vez é **TN3270E_DEF**.

Como Incluir Palavras-chave em um Arquivo de Gabarito

Quando utilizar um arquivo de resposta para incluir a definição de uma nova palavra-chave, deve ser fornecida a palavra-chave inteira. O campo-chave deve ser fornecido juntamente com um valor exclusivo. Se forem omitidos subcampos da palavra-chave, serão utilizados os padrões para esses campos. Por exemplo, para incluir uma palavra-chave **MODE** na configuração, o arquivo de resposta pode conter a seguinte palavra-chave:

```
MODE=(
  MODE_NAME=MYMODE
  COS_NAME=#INTER
  CRYPTOGRAPHY=NONE
  DEFAULT_RU_SIZE=1
  MAX_NEGOTIABLE_SESSION_LIMIT=8192
  MAX_RU_SIZE_UPPER_BOUND=4096
  MIN_CONWINNERS_SOURCE=4096
)
```

O conteúdo do arquivo de resposta assume que uma palavra-chave **MODE** com o parâmetro de **MODE_NAME=MYMODE** não existe no gabarito. Se existir, isto indica que os parâmetros foram atualizados com os valores fornecidos no arquivo de resposta.

Se o parâmetro **MODE_NAME** foi omitido do arquivo de resposta, pode ter ocorrido um erro durante a verificação da configuração porque o parâmetro **MODE_NAME** não

Como Desenvolver Configurações do Communications Server

pôde ser identificado exclusivamente. Nem todos os parâmetros disponíveis para a palavra-chave **MODE** foram especificados no arquivo de resposta. Os parâmetros restantes utilizam os padrões atribuídos pelo arquivo OCDSNT50.DAT. A inclusão resultante na configuração seria parecida com esta:

```
MODE=(
  MODE_NAME=MYMODE
  AUTO_ACT=0
  COMPRESSION=PROHIBITED
  COS_NAME=#INTER
  CRYPTOGRAPHY=NONE
  DEFAULT_RU_SIZE=1
  MAX_NEGOTIABLE_SESSION_LIMIT=8192
  MAX_RU_SIZE_UPPER_BOUND=4096
  MIN_CONWINNERS_SOURCE=4096
  PLU_MODE_SESSION_LIMIT=8192
  RECEIVE_PACING_WINDOW=20
)
```

Como Modificar uma Palavra-chave em um Arquivo de Gabarito

Quando utilizar o arquivo de resposta para modificar a definição de uma palavra-chave existente, a palavra-chave original deve existir no arquivo de gabarito. Se ela não existir no arquivo de gabarito, o arquivo de resposta vai incluir uma entrada na nova configuração. O parâmetro-chave deve ser especificado no arquivo de resposta para identificar a palavra-chave de destino. Somente os parâmetros especificados na palavra-chave do arquivo de resposta serão atualizados na palavra-chave do arquivo de gabarito. Os parâmetros não especificados no arquivo de resposta permanecem inalterados. Por exemplo, se a seguinte palavra-chave **MODE** estiver no arquivo de gabarito:

```
MODE=(
  MODE_NAME=#INTER
  AUTO_ACT=0
  COMPRESSION=PROHIBITED
  COS_NAME=#INTER
  CRYPTOGRAPHY=NONE
  DEFAULT_RU_SIZE=1
  MAX_NEGOTIABLE_SESSION_LIMIT=8192
  MAX_RU_SIZE_UPPER_BOUND=4096
  MIN_CONWINNERS_SOURCE=4096
  PLU_MODE_SESSION_LIMIT=8192
  RECEIVE_PACING_WINDOW=20 )
```

e se a seguinte palavra-chave estiver especificada no arquivo de resposta:

```
MODE=(
  MODE_NAME=#INTER
  AUTO_ACT=10
)
```

a configuração resultante terá a seguinte definição de palavra-chave **MODE**.

```
MODE=(
  MODE_NAME=#INTER
  AUTO_ACT=10
  COMPRESSION=PROHIBITED
  COS_NAME=#INTER
  CRYPTOGRAPHY=NONE
  DEFAULT_RU_SIZE=1
  MAX_NEGOTIABLE_SESSION_LIMIT=8192
  MAX_RU_SIZE_UPPER_BOUND=4096
  MIN_CONWINNERS_SOURCE=4096
  PLU_MODE_SESSION_LIMIT=8192
  RECEIVE_PACING_WINDOW=20
)
```

Como Desenvolver Configurações do Communications Server

Como Eliminar uma Palavra-chave de um Arquivo de Gabarito

Quando utilizar o arquivo de resposta para eliminar uma palavra-chave do gabarito, o parâmetro-chave e o valor que identificam a palavra-chave devem ser especificados juntamente com a palavra-chave DELETE. Por exemplo, se o arquivo de gabarito especificar a seguinte palavra-chave:

```
MODE=(
  MODE_NAME=#INTER
  AUTO_ACT=0
  COMPRESSION=PROHIBITED
  COS_NAME=#INTER
  CRYPTOGRAPHY=NONE
  DEFAULT_RU_SIZE=1
  MAX_NEGOTIABLE_SESSION_LIMIT=8192
  MAX_RU_SIZE_UPPER_BOUND=4096
  MIN_CONWINNERS_SOURCE=4096
  PLU_MODE_SESSION_LIMIT=8192
  RECEIVE_PACING_WINDOW=20
)
```

e se o arquivo de resposta contiver a seguinte palavra-chave:

```
MODE=(
  MODE_NAME=#INTER
  DELETE
)
```

o configuração resultante não conterá a definição do modo #INTER.

A palavra-chave **DELETE** pode aparecer depois de uma especificação *parâmetro=valor* isolada em uma linha ou precedendo ou seguindo o parâmetro. Por exemplo, são válidas as seguintes utilizações da palavra-chave **DELETE**:

```
MODE=(
  MODE_NAME=#INTER
  DELETE
)
MODE=(
DELETE
  MODE_NAME=#INTER
)
MODE=(
  MODE_NAME=#INTER DELETE
)
```

A palavra-chave **DELETE** pode **não** aparecer na frente de uma especificação *parâmetro=valor* na mesma linha. Por exemplo, não é válida a seguinte utilização da palavra-chave **DELETE**:

```
MODE=(
  DELETE MODE_NAME=#INTER
)
```

Para eliminar todas as palavras-chave de um determinado tipo ou eliminar uma palavra-chave que não possui um campo-chave, são necessárias somente a palavra-chave e a palavra-chave **DELETE**. Por exemplo,

```
TN3270E_DEF=(
DELETE
)
```

Etapa 6. Como Selecionar Recursos do Communications Server

Os recursos suportados pelo Communications Server estão descritos a seguir. Algumas ou todas essas funções podem ser suportadas para o seu tipo de conexão:

Configuração do SNA Gateway

Configurando um SNA Gateway, você pode trocar dados entre estações de trabalho de cliente downstream e um computador central mainframe de Systems Network Architecture (SNA). O gateway executa a função de um concentrador, tornando disponíveis os recursos da LU de um ou mais sistemas centrais e de PUs do sistema central para estações de trabalho do cliente SNA downstream através de meios de comunicações suportados pelo Communications Server.

Configuração do Servidor TN3270E

Configurando um servidor TN3270E, você pode trocar dados entre estações de trabalho do cliente TCP/IP downstream que estejam executando aplicações TN3270E (ou TN3270) e um computador central mainframe de Systems Network Architecture (SNA). O servidor executa a função de um concentrador, tornando disponíveis os recursos da LU de um ou mais sistemas centrais e de PUs de sistema central para sessões TN3270E downstream (ou TN3270) através de meios de comunicações suportados pelo Communications Server.

Configuração do Servidor TN5250

Configurando um servidor TN5250, você pode trocar dados entre estações de trabalho de cliente downstream em uma rede TCP/IP que esteja executando aplicações TN5250 e um AS/400 em uma rede SNA. O servidor executa a função de um gateway, tornando disponíveis as sessões de monitor do AS/400 para os clientes TN5250 downstream através dos meios de comunicações suportados pelo Communications Server.

Configuração do Nó da Rede APPN

Os nós de rede são responsáveis pela manutenção e roteamento de informações através de uma rede APPN. Eles mantêm um diretório de todos os recursos (LUs) disponíveis nos nós finais diretamente acoplados e também mantêm uma topologia de todos os nós de rede na rede APPN. Quando uma sessão de LU 6.2 independente é solicitada por um nó na rede, o nó da rede é responsável pela localização do recurso remoto solicitado pela sessão e pelo estabelecimento e roteamento da sessão entre os dois nós.

Configuração do DLUR/DLUS

O Communications Server suporta sessões de LU dependente através de redes APPN. Isto requer que o Communications Server funcione com um solicitador de LU dependente (DLUR) que solicita serviços de roteamento de um servidor de LU dependente LU (DLUS), que reside em um sistema central.

O Communications Server suporta DLUR para sessões e dispositivos locais, e também sessões e dispositivos downstream. Em qualquer um dos casos, o nó local deve ser configurado para se conectar em uma rede APPN.

Configuração do Gateway AnyNet SNA sobre TCP/IP

O SNA sobre TCP/IP gateway faz o roteamento do tráfego do SNA (LU 6.2 independente) entre as redes TCP/IP e SNA. Por exemplo, o SNA sobre TCP/IP gateway permite que aplicações APPC ou CPI-C em execução em

Como Desenvolver Configurações do Communications Server

outro nó de acesso AnyNet SNA sobre TCP/IP se comuniquem com nós SNA ponto a ponto em uma rede SNA.

O Gateway AnyNet SNA sobre TCP/IP deve ser configurado como um nó da rede APPN. Isto permitirá que sessões APPC sejam roteadas para os nós SNA ponto a ponto apropriados.

Configuração do AnyNet Sockets sobre SNA

Existem dois tipos de nós AnyNet Sockets sobre SNA: nós de acesso e nós de gateway. Os nós de acesso permitem que aplicações de soquetes do TCP/IP sejam executadas localmente e se comuniquem com outros nós de acesso ou gateways em algum lugar na rede SNA. O AnyNet Sockets sobre SNA Gateway serve como um conversor de protocolo, permitindo que aplicações em uma rede TCP/IP se comuniquem com aplicações de soquete que estejam sendo executadas em um nó de acesso na rede SNA. Utilizando dois gateways, redes TCP/IP separadas podem ser conectadas através de uma rede SNA.

Configuração do Cliente API de SNA

Os clientes API de SNA são máquinas separadas do Communications Server que têm a capacidade de executar aplicações SNA enquanto estão utilizando o código SNA no nó do Communications Server para gerenciar realmente a sessão. O Communications Server simplesmente estabelece e gerencia uma sessão como se a origem fosse o nó local, mas envia os dados da aplicação para o cliente API de SNA em vez de para suas próprias APIs de aplicação.

Os clientes API de SNA permitem que você execute aplicações SNA sem ter que instalar uma pilha de comunicações SNA, como o Communications Server para Windows NT, V5.0, na mesma máquina. Máquinas menores, menos potentes podem, assim, ser utilizadas para executar as aplicações SNA enquanto uma máquina centralizada, mais potente pode ser dedicada como o servidor SNA para estes clientes API de SNA.

Os clientes API de SNA suportam dois tipos de aplicações: aplicações APPC (LU 6.2 independente) e aplicações API de LUA, como emuladores 3270.

Configuração de CPI-C ou APPC

O Communications Server suporta aplicações CPI-C ou APPC (por exemplo, emulação APPC3270 ou 5250 para um sistema AS/400). A rede APPC é muito flexível e versátil e, contudo, ela pode ser complexa. A complexidade desta configuração depende de como você irá utilizar o Communications Server e de quanto trabalho sua aplicação fará para você.

Sessões de LU 6.2 Dependente para um Sistema Central

O Communications Server suporta sessões de LU 6.2 dependentes com uma PU do sistema central.

Configuração 3270

O Communications Server suporta sessões 3270 com um sistema central.

Configuração do Ponto Focal

O Communications Server suporta localizações do ponto focal remoto para rotear informações sobre o alerta para aplicações de serviços de gerenciamento específicos. O nó local vai localizar pontos focais remotos através de uma rede APPN.

Configuração de Pastas Compartilhadas do AS/400

O Communications Server permite criar unidades de disco no servidor que se comunica com pastas do AS/400 através do AS/400 Integrated File

Como Desenvolver Configurações do Communications Server

System (IFS). Se o servidor compartilhar essas unidades de disco, os clientes poderão utilizar NET USE para elas. Vários clientes podem se conectar às pastas no sistema AS/400 como se elas fossem unidades em suas estações de trabalho.

Etapa 6.1 Como Planejar Programas Aplicativos

Reveja suas aplicações para garantir que esteja de acordo com os requisitos que elas possuem. Especificamente, verifique os requisitos para:

- Modos
- Programas de transação (TPs)
- Definições de LU (sistema central, LU 6.2)
- LUs Parceiras

Etapa 7. Como Criar Configurações e Como Instalar

Você precisa determinar como o Communications Server será configurado e instalado nos servidores dos usuários. Você pode:

- Fornecer instruções aos usuários sobre como instalar e configurar o Communications Server. Você pode preparar suas próprias instruções ou imprimir cópias do *Iniciação Rápida*. Deve também fornecer informações específicas sobre cada servidor, como o ID da rede, o nome do ponto de controle e o endereço da rede.
- Você deve fornecer aos usuários instruções sobre como instalar o Communications Server com uma configuração existente ou um arquivo de gabaritos. Deve também fornecer um arquivo de resposta adaptado para cada servidor, além dos CDs do Communications Server ou o acesso às imagens do CD.
- Configurar e instalar você mesmo o Communications Server nos servidores do usuário. A menos que o grupo de usuário seja muito pequeno, você poderá tentar a utilização de um produto que auxilie na configuração, instalação e distribuição do software para várias estações de trabalho. Exemplos deste tipo de produto incluem o IBM NetView Distribution Manager/2 (NVDM/2), Tivoli TME-10 e Microsoft System Management Server (SMS).

Como Utilizar a Configuração e a Instalação do Arquivo de Resposta

Se você optar por utilizar a configuração e a instalação do arquivo de resposta, consulte “Configuração com Arquivos de Gabarito e de Resposta” na página 191.

Etapa 8. Como Criar Materiais do Usuário

Após ter feito o planejamento para a rede e determinado como irá implementar o seu plano, você precisará criar materiais do usuário. Isso significa que você deve preparar a documentação para instalação, configuração e uso diário, além de preparar procedimentos de cópia de segurança.

Como Desenvolver Configurações do Communications Server

Como Preparar a Documentação

Prepare um conjunto de documentação personalizado para auxiliar os usuários na instalação, configuração e utilização do Communications Server e de aplicações locais para suas necessidades específicas. As seções a seguir contêm sugestões para o tipo de informação que você deve incluir.

Materiais e Procedimentos de Configuração e Instalação

Iniciação Rápida e os auxílios de instalação online estão disponíveis para auxiliar os usuários na instalação do Communications Server. Suas instruções devem informar ao usuário quais das seguintes etapas devem ser executadas durante a instalação do software:

- Quando deve ser feita cópia de segurança dos arquivos de configuração
- Se devem ser aceitos os padrões para criar um arquivo de configuração do Communications Server
Poderá ser necessário fornecer informações da rede, como endereços da placa de rede local, nomes de rede e assim por diante.
- Quando fazer a instalação com um arquivo de resposta fornecido por você
- Quando fazer a instalação com um arquivo de configuração personalizado fornecido por você

Se necessário, forneça a documentação apropriada aos usuários.

Materiais e Procedimentos do Communications Server

Os seguintes materiais são recomendados para a utilização das funções e APIs do Communications Server:

- *Iniciação Rápida*
- Programas escritos pelo usuário para as APIs do Communications Server selecionadas

Como Iniciar e Encerrar o Communications Server

Para obter o procedimento sobre como iniciar ou encerrar o Communications Server, consulte *Iniciação Rápida*.

Se tiver instruções diferentes para iniciar ou encerrar, forneça tais instruções aos usuários.

- O nome do telefone de auxílio do sistema central para determinação de problemas (entre em contato com a assistência técnica do sistema central)
- Os procedimentos de início de sessão para sistemas centrais ou aplicações
- O procedimento para encerrar a aplicação do sistema central
Entre em contato com a assistência técnica de seu sistema central.

- Os procedimentos de encerramento de sessão

Suas instruções devem incluir todos os requisitos especiais para encerramento de sessão nos sistemas ou aplicações. Estas informações podem ser obtidas junto à assistência técnica do sistema central.

Materiais e Procedimentos para Programas Aplicativos

Você deve fornecer aos usuários os procedimentos e outras informações sobre os programas aplicativos que podem ser utilizados na rede. Geralmente, você deve fornecer:

- Os procedimentos para iniciar programas aplicativos
- Os procedimentos para executar programas aplicativos
- Os procedimentos para responder as mensagens geradas pelo programa aplicativo
- Os procedimentos para determinação de problemas
- Se necessário, os procedimentos para encerrar o programa aplicativo

Entre em contato com o programador de aplicativos para obter as informações anteriores.

Materiais e Procedimentos para Determinação de Problemas

Para obter os procedimentos sobre determinação de problemas e relatório, consulte *Iniciação Rápida*.

Como Preparar os Procedimentos de Cópia de Segurança

Ocasionalmente, os usuários podem apagar ou alterar os arquivos de configuração, o registro, o sistema de arquivos, os programas aplicativos e outros programas ou arquivos criados localmente. Além disso, os servidores podem também apagar itens ou executar alterações inaceitáveis, especialmente quando muitos usuários estiverem acessando as estações de trabalho do servidor durante o expediente.

Por esse motivo, será necessário preparar e documentar os procedimentos de cópia de segurança para a rede. Também poderá ser necessário alterar os atributos dos arquivos selecionados nos servidores para Somente de Leitura, de modo que os usuários não possam alterá-los.

Etapa 9. Como Manter a Rede

Quando tiver concluído o planejamento, a instalação e a configuração da rede, e ela estiver sendo executada diariamente, a tarefa restante será a manutenção. Você deve planejar a inclusão, alteração ou eliminação de recursos e usuários na rede e o planejamento para solução de problemas.

Você precisa executar etapas de planejamento e instalação com o mesmo nível para as alterações em sua rede que foram executadas para a configuração inicial. Deve seguir as mesmas etapas para as alterações na rede que foram utilizadas para o planejamento, a instalação e configuração iniciais.

O Communications Server fornece essas ferramentas para ajudá-lo a supervisionar o desempenho diário da rede:

- **Operações do Nó SNA**
- Utilitários da linha de comando
- Administrador Web
- Cliente de Administração Remota
- API de Gerenciamento do Sistema

Como Desenvolver Configurações do Communications Server

- Sub-agente SNMP
- Supervisor de Desempenho do NT

Os produtos a seguir também podem ajudá-lo na administração diária da rede:

- IBM NetView
- IBM LAN Network Manager
- Tivoli TME-10

Parte 3. Como Controlar e Manter uma Rede

Capítulo 16. Recursos de Gerenciamento de Sistema

Este capítulo fornece uma visão geral dos recursos de gerenciamento de sistema Communications Server e descreve os recursos comuns a cada função. Cada recurso também tem algumas funções exclusivas, as quais são descritas em cada recurso.

Os recursos de gerenciamento de sistema permitem supervisionar e controlar os recursos de comunicação em Communications Server. Eles também permitem ajustar estes recursos para melhorar a eficiência dos serviços de comunicação de SNA ou supervisionar e testar estes serviços durante a determinação do problema.

Consulte *Iniciação Rápida* para obter uma lista de recursos que você pode gerenciar.

É possível gerenciar o Communications Server com os seguintes recursos:

- **Operações do Nó SNA**
- Administração remota
- Utilitários da linha de comando
- Administração com base na Web
- Controle ActiveX de Operações do Nó SNA
- Módulo Tivoli Plus
- Suporte MIB de APPN
- S/390 Remote Operations Support (ROPS)

Você poderá utilizar qualquer combinação de recursos para o gerenciamento do Communications Server.

Recursos Comuns de Gerenciamento de Sistema

Cada recurso de gerenciamento de sistema pode executar as seguintes funções:

- Exibir informações sobre o recurso
- Iniciar recursos
- Encerrar recursos
- Eliminar recursos
- Iniciar interruptores de caminho

É possível executar um subconjunto destas ações para cada recurso, como mostrado em Tabela 34.

Tabela 34. Recursos do Servidor de Comunicações para Ações de Gerenciamento

Recurso	Exibir	Iniciar	Encerrar	Eliminar	Interruptor de Caminho
Conexões	X	X	X	X	
Informação secundária de CPI-C	X			X	
Dispositivos	X	X	X	X	
PU's do DLUR	X	X	X		

Recursos de Gerenciamento de Sistema

Tabela 34. Recursos do Servidor de Comunicações para Ações de Gerenciamento (continuação)

Recurso	Exibir	Iniciar	Encerrar	Eliminar	Interruptor de Caminho
LU local 0 a 3	X			X	
LU local 6.2	X			X	
Sessões LU 6.2	X		X		
Gateway PU 2.0/DLUR	X			X	
Conexões RTP	X				X
Sessões TN3270E	X		X		
Sessões TN5250	X		X		

Operações do Nó SNA

O recurso **Operações do Nó SNA** é um recurso online para supervisionar e controlar os recursos de comunicação mantidos pelo Communications Server. **As Operações do Nó SNA** permitem encerrar, iniciar e supervisionar recursos em sua rede.

Você pode utilizar **Operações do Nó SNA** para gerenciar os recursos em sua rede. Os recursos de programação de gerenciamento do sistemas do Communications Server possibilitam que você configure e gerencie os nós dentro de sua rede SNA. **As Operações do Nó SNA** fornecem um diagrama de exibição em árvore de sua configuração o que possibilita a seleção e modificação dos recursos em uma interface gráfica hierárquica.

É possível gerenciar janela múltiplas dentro da janela principal **Operações do Nó SNA**.

Você também pode definir mais de uma configuração do Communications Server e comutar entre as configurações de acordo com suas necessidades. Ao iniciar o Communications Server, a configuração padrão é oferecida como a primeira opção para configuração do nó ou operação do nó, a menos que você especifique uma outra configuração. Após concluir uma nova configuração, você poderá substituir a configuração padrão pela sua própria configuração. Utilize **Operações do Nó SNA** para aplicar sua nova configuração e garantir que a parte relevante do produto seja executada conforme você a configurou.

As Operações do Nó SNA possibilitam que você dispare outros programas Communications Server, como **Visualizador de Registro**, **Recurso de Rastreamento** ou **Configuração do Nó**.

Administração Remota

A **Configuração do Nó SNA** também pode ser utilizada para se conectar a um Communications Server remoto e configurar diretamente seus recursos. O usuário consegue gerenciar remotamente os recursos para um Communications Server em qualquer lugar na rede.

Um cliente de administração remota instala somente aplicações administrativas em um cliente, incluindo a **Configuração do Nó SNA**. A partir deste cliente, um usuário consegue administrar completamente qualquer Communications Server na rede.

Os clientes de administração remotos do Windows 95 e Windows NT utilizam a segurança de domínio do Windows NT, para autenticar a conexão do cliente como servidor sem digitar novamente o ID do usuário e a senha. O cliente deve ser parte de um domínio do Windows NT, pela participação em um domínio do Communications Server ou pela iniciação de sessão localmente com um ID de usuário e senha sincronizados.

Os usuários do cliente de administração remoto fora do domínio do Windows NT são requeridos para fornecerem o ID de usuário e senha, através de um prompt ou através do armazenamento de valores no arquivo de configuração do cliente.

Os usuários autorizados de clientes de administração remotos são mantidos no grupo local IBMCSADMIN, que está localizado diretamente no Communications Server ou no controlador de domínio onde participa o Communications Server. Esse grupo de usuário é criado durante a instalação e pode ser administrado utilizando o aplicativo Gerenciador de Usuário do Windows NT. Devem ser concedidos aos usuários do cliente de administração remoto direitos no grupo IBMCSADMIN, para iniciarem sessão localmente no servidor.

Programas da Linha de Comandos

Os programas da linha de comando possibilita a emissão de comandos a partir de uma janela do prompt do Windows NT. A saída dos comandos é exibida na tela, mas a saída pode ser redirecionada a um arquivo.

Consulte *Iniciação Rápida* para obter uma lista de programas da linha de comandos que você pode utilizar.

Administração Com Base na Web

A função de administração com base na Web do Communications Server permite que você gerencie o servidor em uma intranet de qualquer sistema que possua um navegador Web instalado. Para utilizar o recurso de administração da Web, um servidor Web deve estar sendo executado na mesma máquina que o Communications Server. Você pode gerenciar múltiplos Communications Servers, mas é possível acessar somente um servidor de cada vez. Os usuários devem iniciar sessão na administração da Web como um membro do grupo IBMCSADMIN, na máquina Windows NT que está executando o Communications Server para desenvolver funções administrativas.

Essa função recurso pode ser instalada a partir do CD-ROM do Communications Server. A maioria das funções das **Operações do Nó SNA** estão disponíveis através de um navegador Web. Você pode pesquisar o status do nó, obter informações sobre recursos, modificar recursos, exibir e editar arquivos de configuração, exibir registros de mensagens e executar outras tarefas administrativas. O recurso de administração da Web também permite que você edite arquivos de configuração e visualize o arquivo de registro. As etapas requeridas para utilizarem essas funções estão documentadas na página **Bem-Vindo ao Communications Server Web Administration** na Web.

Controle ActiveX de Operações do Nó SNA

Existe uma versão de controle ActiveX de **Operações do Nó SNA**. Esse controle permite que você incorpore **Operações de Nó SNA** em qualquer aplicação que permita controles incorporados como o Microsoft Management Console (MMC). O nome do controle é CSNCTX e ele está localizado no diretório de instalação do produto. Esse controle possui todas as funções de **Operações de Nó SNA** e fornece o benefício de incorporar **Operações de Nó SNA** em outras aplicações, permitindo o gerenciamento do produto cruzado.

Módulo Tivoli Plus

Se você utilizar o Tivoli Management Environment (TME) para gerenciar centralmente os dispositivos e aplicações na rede, o módulo Tivoli Plus do Communications Manager permite que você também gerencie o Communications Server do TME. O módulo Tivoli Plus do Communications Manager pode ser instalado no servidor TME. Uma imagem instalável do TME encontra-se no diretório do TME do CD-ROM do Communications Server. Para acessar as funções do TME Plus instaladas, dê um clique duplo sobre o ícone TivoliPlus que foi incluído no painel **Ambiente de Trabalho do Administrador** do TME. Ao dar um clique duplo sobre o ícone IBM CSPlus, você pode utilizar os ícones do painel para executar as seguintes ações:

- Distribuir, instalar e remover a instalação do Communications Server
- Iniciar, encerrar e pesquisar o servidor
- Exibir e modificar os recursos do servidor
- Listar arquivos de configuração
- Percorrer mensagens de erro a partir do Communications Server para um Tivoli Enterprise Console
- Estabelecer supervisores e limiares para a tecla atributos do Communications Server

Ao dar um clique duplo sobre qualquer ícone no painel IBM CSPlus, digite as informações nos campos da caixa de diálogo apresentada. O auxílio está disponível para os campos na caixa de diálogo.

Suporte MIB de APPN

Communications Server suporta pedidos simples do protocolo do gerenciamento de rede (SNMP) para informações de gerenciamento APPN a partir de qualquer sistema de gerenciamento SNMP.

O serviço SNMP está instalado a partir do marcador **Serviços** no menu pendente **Rede** do painel de controle do Windows NT. Depois que o software de Serviços SNMP esteja instalado em seu computador, você deverá configurá-lo com uma informação válida para que o SNMP possa operar.

Você deverá estar registrado como membro do grupo Administrador para o computador local para configurar o SNMP.

As informações sobre a configuração SNMP identificam comunidades e desvios de destino.

S/390 Remote Operations Support (ROPS) para o Programa NetView

Quando o RUNCMD é emitido a partir do NetView, o valor do parâmetro para o APPL tem de ser especificado como APPL=CSRCMDS.

Quando o comando RUNCMD é emitido, todas as informações, inclusive o ID e a senha, são transmitidas abertamente, não sendo guardadas de forma alguma, a menos que o caractere de supressão NetView seja utilizado durante a emissão. Estas informações são exibidas na tela e digitada no registro NetView. Se as senhas forem transmitidas para o serviço ROPS, o usuário será responsável pela segurança do terminal NetView e dos registros NetView de forma que tais dados não estejam comprometidos.

Apêndice A. Como Planejar o Communications Server

Este apêndice fornece as informações de que você precisa saber para planejar o ambiente do Communications Server.

Hardware Compatível

Esta seção descreve o hardware da IBM que suporta o Communications Server. Estas descrições incluem informações sobre:

- Placas de Comunicação
- Modems
- Placas de Criptografia de Nível de Sessão

Placas de Comunicação

Para obter uma lista de placas adaptadoras suportadas pelo Communications Server, consulte a seguinte URL na Internet:

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

Modems

O Communications Server suporta os seguintes tipos de modems:

- Modems assíncronos:
 - Modems 100% compatíveis com o conjunto de comandos AT Hayes**
 - Modems IBM que estão em conformidade com os padrões de interface ITU-T (CCITT) V.24/V.28 (EIA RS-232-D) e V.35
 - Os modems assíncronos não-IBM também são suportados, bem como a função base do equipamento terminal de dados padrão ITU-T (CCITT) V.24 (EIA RS-232-D) para a interface do equipamento terminal do circuito de dados (DCE) para comunicações assíncronas
 - Modems que estão em conformidade com o DTE padrão RS-232-D para a interface DCE
- Modems síncronos e unidades CSU/DSU que suportam o conjunto de comandos V.24bis
- Modems 100% compatíveis com o protocolo Hayes AutoSync

Os usuários de X.25 requerem um modem síncrono e unidades CSU/DSU que suportam o conjunto de comandos V.24bis ou um modem compatível com o protocolo Hayes AutoSync. Consulte o fornecedor da rede para obter o tipo de conexão e modem recomendados.

Para obter uma lista de modems suportados pelo Communications Server, consulte a seguinte URL na Internet:

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

Como Planejar o Communications Server

Placas de Criptografia de Nível de Sessão

Para utilizar a criptografia de nível de sessão, você deve ter o programa Programmed Cryptographic Facility e uma das seguintes placas:

- A placa IBM SecureWay 4758 PCI Cryptographic Coprocessor
- Outras placas compatíveis com a IBM Common Cryptographic Architecture

Nota: Se você utilizar uma placa diferente da IBM 4758, precisará utilizar os verbos de API criptográficos em substituição. Consulte o *Communications Server Programming Guide and Reference* para obter mais informações.

Software do Emulador

Para obter uma lista de softwares de emuladores suportados pelo Communications Server, consulte a seguinte URL na Internet:

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

Considerações sobre a Compactação de Dados

Antes de utilizar a compactação de dados do SNA, devem ser executadas diversas etapas de configuração nos sistemas envolvidos. A compactação de dados do SNA é suportada em:

- VTAM V3R4.1 ou superior
- OS/400 V2R3 ou superior

Quando a compactação termina, cada RU é compactada de forma independente e é incluído um cabeçalho de compactação na RU. O TH e o RH não são compactados. Nenhuma compactação é executada quando a RU é menor que 20 bytes ou maior que 64K bytes ou, somente no caso de RLE, se o tamanho dos dados compactados, incluindo o cabeçalho de compactação for maior que os dados originais.

Antes de começar a configurar os recursos apropriados do Communications Server para a compactação de dados, certifique-se de que o sistema parceiro seja capaz e esteja preparado para suportar a compactação de dados.

Como Planejar a Conexão ao Sistema Central/VTAM

Antes de solicitar a compactação de dados em uma sessão para um sistema central S/370 ou S/390* com a emulação 3270 ou comunicações do tipo LU 6.2, o VTAM Versão 3 Release 4.1 (VTAM V3R4.1) deve ser instalado e configurado para negociar estes pedidos.

Seu programador do sistema VTAM do sistema central deve fornecer-lhe as definições de VTAM apropriadas necessárias para a compactação de dados. A seguir, há uma lista resumida das definições necessárias. Os exemplos delas são fornecidos após a lista.

- As opções de inicialização do VTAM devem conter o parâmetro **CMPVTAM=x**
- É necessária uma entrada LOGMODE com o parâmetro **COMPRES=**
- Essa entrada LOGMODE deve estar na tabela Mode que está sendo utilizada
- Deve haver uma instrução APPL de VTAM com os parâmetros **CMPAPPLI=** e **CMPAPPLO=** para a aplicação que será utilizada

Como Planejar o Communications Server

- A definição da LU do VTAM para sua sessão deve especificar LOGMODE e a tabela Mode que foram definidas para a compactação.

CMPVTAM

Este é o parâmetro das opções de inicialização do VTAM que indica o nível máximo de compactação permitido para qualquer sessão conectada a este sistema central. A sintaxe deste parâmetro é:

CMPVTAM=n

em que n representa o nível de compactação permitido para um pedido, na faixa de 0 a 4. O valor recomendado é 4, que permite que todos os níveis da compactação de dados sejam utilizados.

COMPRES

Esta é a entrada da tabela MODEENT de VTAM na definição LOGMODE que será utilizada pela LU. A sintaxe é:

COMPRES=valor

em que valor representa SYSTEM, REQUESTED ou PROHIBITED. SYSTEM deve ser codificado para todos os tipos de LU suportados.

CMPAPPLO

Este é o parâmetro de definição (APPL) da aplicação VTAM que define o nível de compactação solicitado para os dados da Unidade de Pedido/Resposta (RU) de saída. A sintaxe é:

CMPAPPLO=n

em que "n" representa o nível solicitado da compactação de dados para a direção do fluxo de dados de PLU -> SLU, também chamado de dados de saída. Para sessões de todos os tipos de LU suportados pelo Communications Server, o valor de "n" pode ser igual a 0, 1 ou 2, representando a compactação de dados nos níveis 0, 1 e 2. Entretanto, para os tipos de LU 0, 1, 2 e, o Communications Server sempre reserva recursos de compactação no nível 2.

CMPAPPLI

Este é o parâmetro de definição (APPL) da aplicação VTAM que define o nível de compactação solicitado para os dados da Unidade de Pedido/Resposta de entrada. A sintaxe é:

CMPAPPLI=m

em que "m" representa o nível de compactação de dados solicitado para o fluxo de dados de SLU -> PLU, também chamado de dados de entrada. O valor para m depende do tipo de LU utilizado para a sessão:

- Para sessões do tipo de LU 3270, "m" pode ter o valor igual a 0 ou 1.
- Em sessões do tipo LU 6.2, "m" pode ter os valores 0, 1 ou 2.

Nota: O VTAM sempre representa a LU principal (PLU) e o Communications Server representa a LU secundária (SLU) para os tipos de LU 0, 1, 2 e 3.

A seguir estão exemplos codificados, que foram extraídos das listagens originais do VTAM, indicando a utilização e colocação dos parâmetros discutidos acima. Preste atenção especialmente nas linhas destacadas.

Como Planejar o Communications Server

```

*****
SSCPID=20,HOSTSA=20,XNETALS=YES, X
GWSSCP=YES, X
NODELST=NODES1, X
CMPVTAM=4, X
CONFIG=K0,SUPP=NOSUP, X
NETID=USIBMRA,HOSTPU=ISTPUS20,HOSTSA=20,SSCPNAME=RAK, X
SSCPDYN=YES,SSCPORD=PRIORITY, X
ASYDE=TERM, X
NOTRACE,TYPE=VTAM,IOINT=0, X
NOTRACE,TYPE=SMS,ID=VTAMBUF, X
PPOLOG=YES, X
NODETYPE=NN, X
CPCP=YES, X
CSALIMIT=0, X
NOTNSTAT,DYNLU=YES, X
IOBUF=(3500,256,3,,1,58), X
LPBUF=(1100,,2,,1,4), X
LFBUF=(100,,,1,1), X
CRPLBUF=(2400,,,1,4), X
SFBUF=(60,,,1,1) X
*****

```

Figura 41. Parâmetro de Inicialização do VTAM. É permitido até o nível de compactação 4 neste VTAM.

```

*****
* LOGMODE FOR COMPRESSION TEST - BASED ON D4C32XX3 *
*****
*
*          3274 MODEL 1C (REMOTE SNA)                @0Y02946*
*          PRIMARY SCREEN 24 X 80 (1920)
*          ALTERNATE SCREEN TO BE DETERMINED BY APPLICATION
*
*****
D4C3COMP MODEENT LOGMODE=D4C3COMP, *
                FMPROF=X'03', *
                TSPROF=X'03', *
                PRIPROT=X'B1', *
                SECPROT=X'90', *
                COMPROT=X'3080', *
                RUSIZES=X'87F8', *
                PSERVIC=X'028000000000000000000000300', *
                APPNCOS=#CONNECT, *
                COMPRES=REQD

```

Figura 42. Tabela Logmode do VTAM. A macro MODEENT configurada com a compactação de dados solicitada.

```

VBUILD TYPE=APPL
*****
* VTAM APPL STATEMENTS FOR CICS/MVS* 3.3 *
*****
RAKAC001 APPL ACBNAME=RAKAC001, *
          MODETAB=MTAPPC, *
          EAS=20, *
          SONSCIP=YES, *
          AUTH=(ACQ,VPACE,PASS), *
          PARSESS=YES, *
          VPACING=5, *
          CMPAPPLI=1 *
          CMPAPPLO=2

```

Figura 43. Instrução da Aplicação VTAM. Controla os níveis máximos suportados para esta sessão.

```

WTCC1102 PU ADDR=13,
          IDBLK=05D,
          IDNUM=32289,
          etc.
          DLOGMOD=D4C3COMP
          MODETAB=AMODETAB
          etc.

RACC1102 LU LOCADDR=2, DLOGMOD=D4C3COMP, MODETAB=AMODETAB
LU
          etc.

```

Figura 44. Definições da PU e da LU do VTAM. A LU RACC1102 o modo de início de sessão D4C3COMP, que está na tabela de modo AMODETAB.

Como Planejar a Compactação de Dados do AS/400

Quando se conectar a um sistema AS/400, é necessário o OS/400 V2R3 para a utilização da compactação de dados. Tudo isso realmente é necessário para assegurar que você tem uma definição MODE que especifica o suporte da compactação. São necessários três parâmetros no perfil “Criar Descrição de Modo” obtido através do comando CRTMODD ou através dos menus. Os três parâmetros são:

DTACPR

Este parâmetro controla a utilização da compactação de dados. Os parâmetros válidos são mostrados a seguir:

NETATR

Utilize o valor de rede em todo o sistema para este parâmetro.

NONE

Não é permitida a compactação de dados.

ALLOW

Se o sistema remoto solicitar a compactação de dados, o sistema local vai permitir que a sessão seja estabelecida.

REQUEST

O sistema local solicita a compactação de dados.

Como Planejar o Communications Server

REQUIRE

É necessária a compactação de dados. Se um dos sistemas não conseguir executar a compactação de dados no nível solicitado, a sessão não será estabelecida.

Sempre que a compactação de dados for permitida e solicitada, os dois sistemas vão negociar o nível de compactação de dados a ser utilizado nessa sessão, de acordo com as definições dos parâmetros **INDTACPR** e **OUTDTACPR**.

INDTACPR

Este valor representa o nível máximo de compactação utilizado para os dados de entrada.

OUTDTACPR

Este valor representa o nível máximo de compactação utilizado para os dados de saída.

Para sessões de LU 6.2, os níveis de compactação de dados 0, 1 e 2 são suportados nas duas direções, ou seja, para o fluxo de dados de saída e de entrada.

Para obter informações sobre como ativar o Communications Server para a compactação de dados, consulte *Iniciação Rápida*.

Considerações sobre Desempenho

O desempenho das comunicações de computadores em geral e do Communications Server em particular, está sujeito a um grande número de variáveis. O propósito das informações a seguir é apresentar alguns dos fatores que influenciam o desempenho das comunicações em um ambiente do Communications Server.

O desempenho das comunicações é afetado pela velocidade da linha de comunicações. Essa velocidade geralmente é expressa como o número de bits por segundo (bps) que podem ser transmitidos através da linha. Geralmente, quanto mais rápido o bps, maior será o desempenho das comunicações que pode ser alcançado na linha.

Além da velocidade de transmissão, vários outros fatores relacionados à linha podem afetar o desempenho das comunicações. Por exemplo, algumas linhas só podem transportar dados em uma direção de cada vez. Para alterar a direção das comunicações (que pode enviar), a estação gera um **pedido para enviar** (RTS) e aguarda a emissão de **disponível para enviar** (CTS). Isto requer tempo adicional para esta **inversão do fluxo de transmissão** (que é dependente do modem). Outro fator é a qualidade de transmissão da linha de comunicações. Quando ocorrer um erro na linha, a maioria dos protocolos vai detectá-lo e reenviar os dados. Uma linha que tiver menos erros de transmissão vai ter uma taxa de rendimento maior.

Também pode ser atingida uma taxa de rendimento maior se os protocolos operarem em um modo de transmissão de dados **duplex**, em que o protocolo pode receber e transmitir simultaneamente. A rede Local e X.25 são protocolos duplex. O SDLC pode operar em modo duplex ou semiduplex.

Para utilizar o modo duplex para o SDLC, você deve utilizar uma placa apropriada (a placa MPA não suporta o modo duplex). A estação remota também suporta o modo duplex.

Como Planejar o Communications Server

Conforme aumenta a velocidade da linha, a capacidade da velocidade de transmissão fica com menos limitação em desempenho. Em vez disso, a limitação fica relacionada aos atrasos nos dispositivos que estão utilizando a linha de comunicação (modems, unidades de controle ou limitações internas do computador). Em velocidades muito altas, esses atrasos podem prejudicar o desempenho da comunicação mais que a capacidade da velocidade de transmissão da linha.

A análise dessas situações dá um pouco de trabalho. Por exemplo, os atrasos de comunicação esperados podem ser causados por qualquer um dos seguintes fatores:

- Uma linha de comunicação sobrecarregada
- Um sistema central sobrecarregado
- Uma unidade de controle 3X74 sobrecarregada
- Um controlador de rede 37xx sobrecarregado
- Definição VTAM ou NCP menos ótima
- Projeto de rede ou gerenciamento de rede inadequado
- Memória cheia e troca do sistema operacional

Em um ambiente de comunicação de alta velocidade, como por exemplo, uma rede local, a velocidade de transmissão da linha de comunicação é menos significativa porque a capacidade de comunicação é amplamente determinada pela velocidade dos dispositivos de comunicação. Muitas vezes, um melhor desempenho de comunicação pode ser atingido aumentando-se a força de processamento da estação de trabalho, do sistema central ou de outros componentes da rede. Isso não significa que a velocidade de transmissão de uma rede da rede local nunca será limitada; certamente pode requerer a execução de vários computadores em sua capacidade de comunicação antes que o desempenho da rede local seja reduzido de forma significativa.

Resumindo, em muitos casos, o desempenho do Communications Server é amplamente determinado por fatores que estão relacionados à rede de comunicação que está sendo utilizada. O fornecimento do desempenho de comunicações a um custo razoável envolve um conhecimento da rede como um todo e a análise de seus componentes individuais.

Apêndice B. Observações

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. A IBM pode não oferecer os produtos, serviços ou recursos abordados nesse documento em outros países. Consulte seu Representante IBM local para obter informações sobre os produtos e serviços atualmente disponível em sua região. Qualquer referência a um produto, programa ou serviço IBM não significa que apenas os produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito poderá ser utilizado. Contudo, é de inteira responsabilidade do Cliente avaliar e verificar a operação de qualquer produto, programa ou serviço que não sejam IBM.

A IBM pode ter patentes ou solicitações de patentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, à:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
CEP 22290-240
Rio de Janeiro - RJ

O parágrafo a seguir não se aplica ao Reino Unido e a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO “COMO ESTÁ” SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO LIMITADO AS GARANTIAS DE NÃO-INFRAÇÃO, MERCADO OU ADEQUAÇÃO A UM DETERMINADO OBJETIVO. Alguns países não permitem exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Esta publicação pode conter imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, sem aviso prévio, aperfeiçoar e/ou alterar o(s) produto(s) ou programa(s) descritos (s) nesta publicação.

Todas as referências nessa publicação a sites na Web não-IBM são fornecidas somente para conveniência e de qualquer maneira não servem como endosso daqueles sites na Web. Os materiais nesses sites na Web não são parte dos materiais desse produto IBM e a utilização desses sites na Web sites é de seu próprio risco.

Os possuidores de licença deste programa que pretendam obter mais informações sobre o mesmo com o objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com a:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
CEP 22290-240
Rio de Janeiro - RJ

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, Contrato de Licença de Programação Internacional ou qualquer contrato equivalente entre a IBM e o Cliente.

Quaisquer dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar de maneira significativa. Algumas avaliações podem ter sido realizadas em sistemas em nível de desenvolvimento, sendo que não há garantias que estas avaliações permanecerão as mesmas nos sistemas disponíveis. Além disso, algumas avaliações podem ter sido estimadas através de extrapolação. Os resultados reais podem variar. Os usuários deste documento deverão verificar os dados aplicáveis a seu ambiente específico.

As informações referente a produtos que não sejam IBM foram obtidas a partir de fornecedores destes produtos, de suas publicações ou de outros recursos disponíveis publicamente. A IBM não testou tais produtos, não podendo confirmar a exatidão do desempenho, compatibilidade ou quaisquer outras afirmações relacionadas a produtos não-IBM. As perguntas a respeito dos recursos dos produtos não-IBM devem ser endereçadas diretamente aos fornecedores de tais produtos.

Marcas

Os termos a seguir são marcas da IBM Corporation nos Estados Unidos e/ou em outros países:

Advanced Peer-to-Peer Networking	IMS
AIX	Micro Channel
AnyNet	NetView
APPN	OS/2
AS/400	OS/400
AT	Personal System/2
BookManager	Portmaster
CICS	Presentation Manager
DB2/2	PS/2
eNetwork	System/370
Enterprise System/9000	System/390
ESCON	SystemView
ES/9000	S/370
FFST/2	S/390
First Failure Support Technology/2	TalkLink
Global Network	VTAM
IBM	WebExplorer
IBMLink	

Outros nomes de empresas, produtos e serviços podem ser marcas ou marcas de serviços de terceiros.

C-bus é uma marca da Corollary, Inc.

Java e HotJava são marcas da Sun Microsystems, Inc.

Microsoft, Windows e o logotipo Windows 95 são marcas registradas da Microsoft Corporation.

PC Direct é uma marca da Ziff Communications Company e é utilizada pela IBM Corporation sob licença.

ActionMedia, LANDesk, MMX, Pentium e ProShare são marcas ou marcas registradas da Intel Corporation nos Estados Unidos e outros países.

Para obter uma lista completa das marcas da Intel veja www.intel.com/tradmarx.htm.

UNIX é uma marca registrada nos Estados Unidos e outros países licenciada exclusivamente pela X/Open Company Limited.

Índice Remissivo

Numéricos

9370

- parâmetros de sistema central do Communications Server 158
- parâmetros de sistema central SDLC 166

A

- acesso aos dados existentes
 - descrição 16
 - planejamento para 99
- administração, extensor de ramificação 32
- ANR 52
- AnyNet
 - Como definir nomes de CP e de rede de conexão exclusivos 73
 - como mapear os recursos de SNA para endereço IP 71
 - Como rotear as sessões SNA através do AnyNet SNA sobre TCP/IP 77
 - Exemplos de AnyNet 78
- aplicações de rede de subárea 66
- aplicações de software, planejamento 183
- APPC
 - conceitos fundamentais 6
 - conectividades 4
 - parâmetros de sistema central VTAM 164
 - parâmetros de sistema central X.25 171
- APPN
 - definido 8
 - discussão geral 4, 23
 - ponto de controle (CP)
 - controle de ligação de dados 34
 - discussão geral 27
 - ligações lógicas 34
 - sessões CP-CP 28
 - redes de conexão 40
 - serviços de diretório 42
 - serviços de topologia e seleção de rota
 - banco de dados de topologia 45
 - classe de serviço 47
 - discussão geral 44
 - modos 46
 - roteamento de sessão intermediária 49
 - seleção de rota 48
 - tipos de nós
 - discussão geral 25
 - fim 27
 - LEN 27
 - rede 26
 - unidades lógicas (LUs) 6

- arquivo de gabarito, instalar e configurar
 - criar configurações e instalar
 - configuração e instalação do arquivo de resposta 197
 - discussão geral 197
 - criar convenções de nomenclatura
 - critérios 183
 - discussão geral 183
 - nomes de NAU 185
 - tipos e restrições 184
 - tipos utilizados por múltiplos componentes 184
 - criar materiais do usuário
 - materiais e procedimentos do Communications Server 198
 - preparar documentação 198
 - preparar procedimentos de cópia de segurança 199
 - definir a configuração do gabarito
 - plano para programas aplicativos 197
 - selecionar recursos 195
 - definir endereços de rede
 - discussão geral 187
 - estação SDLC 188
 - placa de rede 187
 - X.25 189
 - manter sua rede 199
 - plano para aplicações de software 183
 - plano para hardware 181
 - selecionar ferramentas de configuração e instalação
 - configuração 190
- AS/400
 - parâmetros de sistema central (Communications Server) da linha de sistema central 175
 - parâmetros de sistema central (Communications Server) do controlador de sistema central 175
 - parâmetros de sistema central biaxiais 176
 - parâmetros de sistema central de linha do sistema central 172
 - parâmetros de sistema central de linha do sistema central (X.25) 176
 - parâmetros de sistema central do controlador de sistema central 173
 - parâmetros de sistema central do dispositivo de sistema central 174
 - parâmetros do sistema central do controlador do sistema central (X.25 PVC) 177
 - parâmetros do sistema central do controlador do sistema central (X.25 SVC) 178
- ativar na inicialização 36
- ativar por pedido 36

B

- Balanceamento de carga 141

C

- cabeçalho de compactação 210
- características de ligação, HPR 107
- carga de instalação 154
- carga de volume 154
- cargas de rede, X.25 154
- CMSETUP 18
- cobrança de aluguel periódico 154
- Communications Server
 - funções suportadas 3
 - interfaces de programação de aplicações (APIs)
 - conversações 7
 - nomes de NAU 185
 - recursos, como selecionar 195
 - visão geral da configuração 3
- Communications Server e SNA Gateway
 - configuração do endereço de destino de Rede Local 116
 - desempenho do SNA Gateway 119
 - discussão geral 113
 - ligações suportadas para estações de trabalho 113
 - ligações suportadas para sistemas centrais 114
- como configurar o extensor de ramificação 32
- como configurar um arquivo de gabarito
 - criar configurações e instalar
 - configuração e instalação do arquivo de resposta 197
 - discussão geral 197
 - criar convenções de nomenclatura
 - critérios 183
 - discussão geral 183
 - nomes de NAU 185
 - tipos e restrições 184
 - tipos utilizados por múltiplos componentes 184
 - criar materiais do usuário
 - materiais e procedimentos do Communications Server 198
 - preparar documentação 198
 - preparar procedimentos de cópia de segurança 199
 - definir a configuração do gabarito
 - plano para programas aplicativos 197
 - selecionar recursos 195
 - definir endereços de rede
 - discussão geral 187
 - estação SDLC 188
 - placa de rede 187
 - X.25 189
 - manter sua rede 199
 - plano para aplicações de software 183
 - plano para hardware 181
 - selecionar ferramentas de configuração e instalação
 - configuração 190

- como instalar o extensor de ramificação 32
- como instalar um arquivo de gabarito
 - criar configurações e instalar configuração e instalação do arquivo de resposta 197
 - discussão geral 197
 - criar convenções de nomenclatura critérios 183
 - discussão geral 183
 - nomes de NAU 185
 - tipos e restrições 184
 - tipos utilizados por múltiplos componentes 184
- criar materiais do usuário
 - materiais e procedimentos do Communications Server 198
 - preparar documentação 198
 - preparar procedimentos de cópia de segurança 199
- definir a configuração do gabarito
 - plano para programas aplicativos 197
 - selecionar recursos 195
- definir endereços de rede
 - discussão geral 187
 - estação SDLC 188
 - placa de rede 187
 - X.25 189
- manter sua rede 199
- plano para aplicações de software 183
- plano para hardware 181
- selecionar ferramentas de configuração e instalação
 - configuração 190
- compactação de dados 57
- compactação de dados, SNA 10
- compactação de dados do AS/400 213
- compactação de RU 210
- Conexão de sistema central de rede
 - comutada VTAM
 - Ethernet 160
 - Token-Ring 157
- conexão de sistema central SDLC
 - 9370 166
 - VTAM/NCP 161
- Conexão de sistema central Token-Ring
 - NCP com VTAM 157
 - placa de rede 9370 158
 - Rede comutada VTAM 157
- conexões, X.25 154
- conexões de estações de trabalho X.25 114
- configuração
 - como criar 197
 - janelas, como utilizar o CMSETUP 18
 - métodos 18
 - para um arquivo de gabarito 190
 - parâmetros de sistema central 157
 - processo 18
- configuração, suporte local e remoto 18
- configuração de gabarito, como definir 181
- configuração do endereço de destino de Rede Local 116

- Configurações do AnyNet 71
- configurações do SNA sobre TCP/IP 71
- conjuntos de LUs 66
- considerações, HPR 108
- considerações HPR 108
- considerações sobre desempenho 214
- Controlador 3174
 - parâmetros de sistema central do Communications Server 159
 - Parâmetros de sistema central PU VTAM 159
- controle de fluxo 63
- controle de fluxo da sessão
 - controle de velocidade BIND adaptável 64
 - controle de velocidade do nível de sessão adaptável 63
 - segmentação e remontagem 64
- controle de ligação de dados
 - definições 24
 - perfis 24
- controle de velocidade 63
- controle de velocidade adaptável do BIND 64
- controle de velocidade BIND adaptável 64
- controle de velocidade do nível de sessão 63
- controle de velocidade do nível de sessão adaptável 63
- controle de velocidade fixo 64
- convenções de nomenclatura 183
- conversações, programa de transação 7
- conversor de protocolo 66
- CP (ponto de controle)
 - controle de ligação de dados 34
 - discussão geral 27
 - ligações lógicas
 - ativação da ligação 34
 - ligações paralelas 34
 - nomes 185
 - sessões CP-CP 28
- criptografia 60
- criptografia de nível de sessão
 - placas 210
- criptografia de nível de sessão SNA 60
- critérios para nomeação 183

- D**
- DDDLU 53
- definição dinâmica de LU dependente 53
- definições de terminal e impressora
 - explícitas 125
- definições de terminal e impressora implícitas 125
- Dependent Logical Unit Requester 53
- descoberta de fornecedores de serviço 10
- Descrição de Modo 213
- DLUR 53
 - parâmetros de sistema central 168
- documentação, como preparar 198

- E**
- emulador
 - funções de nível de entrada 21

- emulador de nível de entrada 21
- encaminhamento de sessão intermediária 49
- endereços
 - como definir a rede 187
 - estação SDLC 188
 - placa de rede 187
 - X.25 189
- endereços da placa, rede 187
- endereços de rede, como definir 187
- endereços internet 189
- endereços IP 189
- estações de trabalho explícitas 118
- estações de trabalho implícitas 118
- estações de trabalho secundários multiponto 114
- extensor de ramificação 29

- F**
- fila de prioridades, HPR 108
- função de descoberta de roteamento 90

- G**
- gateway
 - Sockets sobre SNA 71
- Gerenciador de Rede Local 66

- H**
- hardware, planejamento 181
- high performance routing (HPR) 107
 - controle de velocidade 64
 - planejamento 107
 - suporte 49
 - visão geral 10, 49
- Host Publisher
 - configurações 102
 - descrição 16
 - processamento de página na Web 101

- I**
- instalação, arquivo de resposta 197

- J**
- janelas, configuração, como utilizar o CMSETUP 18

- L**
- LDAP 93
- ligações a estações de trabalho 113
- ligações a sistemas centrais 114
- ligações lógicas
 - ativação da ligação 34
 - paralelo 34
- ligações suportadas para estações de trabalho 113
- ligações suportadas para sistemas centrais 114

Lightweight Directory Access Protocol (LDAP) 93
limitações
 O System/390 ROPS é compatível com NetView 207
LU 6.2 56
LU dependente 56
LU dependente de autodefinição 53
LU dependente do SSCP 56
LU independente 55
LU independente de SSCP 55
LUs agrupadas
 discussão geral 116
LUs dedicadas
 discussão geral 116
LUs suportadas
 dependente de SSCP 56
 discussão geral 52
 independente de SSCP 55

M

materiais do usuário, como criar 197
materiais e procedimentos
 Communications Server 198
 como criar um usuário 197
 determinação de problemas 199
 programas aplicativos 199
máximo de tentativas de ativação 38
modems, suportados 209
MPC
 parâmetros IOCP/HCD 165
 parâmetros VTAM 165
 suporte DLC 21
Multi-Path Channel
 suporte DLC 21
múltiplas PUs
 como particionar LUs entre sistemas centrais 64

N

NCP (NTRI)
 parâmetros de sistema central do Communications Server 157
NetView
 Suporte RUNCMD 207
nível de suporte de domínio múltiplo (MDS) 62
nível de transporte de vetor de gerenciamento de rede (NMVT) 63
nível Migration para serviços de gerenciamento de SNA 62
NMVTs 66
nó da rede
 definição e descrição 26
 recurso através de APPN 9
nó de acesso
 Sockets sobre SNA 71
nó final
 definição e descrição 27
 recurso através de APPN 9
nomes
 NAU 185
 tipos e restrições 184

nomes (*continuação*)
 utilizados por múltiplos componentes 184
nomes de LU
 sockets sobre SNA 187
Nós LEN 27
número da porta
 como alterar para servidor TN3270E 123
 como alterar para servidor TN5250 129

O

Observações 217

P

parâmetros
 conexão de sistema central 157
parâmetros de ativação 36
parâmetros de conexão de sistema central ES/9000 166
parâmetros de conexão do sistema central 157
parâmetros de definição 36
Parâmetros de sistema central (VTAM)
 Token-Ring 157
parâmetros de sistema central biaxiais 176
parâmetros de sistema central de suporte SDDLU 168
Parâmetros de sistema central Ethernet (VTAM) 160
Parâmetros de sistema central NPSI 169
Parâmetros de sistema central VTAM (APPC) 164
parâmetros VTAM (MPC) 165
placas
 comunicação 209
 criptografia de nível de sessão 210
planejamento
 aplicações de software 183
 configuração X.25 153
 hardware 181
 para SNA 113
 programas aplicativos 197
PLU 211
ponto de controle (CP)
 controle de ligação de dados 34
 discussão geral 27
 ligações lógicas
 ativação da ligação 34
 ligações paralelas 34
 nomes 185
 sessões CP-CP 28
ponto de entrada 62
ponto de serviço 62
ponto focal 61
preparar procedimentos de cópia de segurança 199
prioridade de transmissão 47
processamento de manutenção de atividade
 servidor TN3270E 124
 servidor TN5250 129
programa de transação (TP) 6

programas aplicativos, planejamento 197
provedor de serviços, descoberta de 10
Provedor OLE DB do AS/400
 descrição 16

R

Rapid Transport Protocol (RTP) 50
rede, como manter 199
redes X.25
 cargas da rede 154
 conexões possíveis 154
 endereços 189
 planejamento 153
remontagem, segmentação e 64
repetição automática de ligação 37
restrições, extensor de ramificação 31
RFC 1205 129
RFC 1576 123
RFC 1646 123
RFC 1647 123
Roteamento Automático da Rede (ANR) 52
RTP 50

S

SDDLU 53
SDLC (Synchronous Data Link Control)
 conexões de estações de trabalho comutadas 114
 endereços da estação de ligação 188
segmentação e remontagem 64
segurança
 conversação 4
 sessão 4
 visão geral 20
segurança baseada em secure sockets layer
 TN3270E 14
 TN5250 15
segurança dos dados 20
seleção de rota
 banco de dados de topologia 45
 classe de serviço 47
 discussão geral 44
 modos 46
 roteamento de sessão intermediária 49
 usuários do VTAM 48
serviços de diretório 42
serviços de gerenciamento
 controle de fluxo da sessão 63
 níveis da arquitetura de serviços de gerenciamento SNA 62
 pontos focais, pontos de serviço e pontos de entrada 61
Servidor de pasta compartilhada do AS/400
 configuração 100
 descrição 17
Servidor TN3270E
 como alterar o número da porta 123, 129
 descrição 14
 filtragem de IP 125
 planejamento para 121, 127

- Servidor TN3270E (*continuação*)
 - processamento de manutenção de atividade 124
- Servidor TN5250
 - acesso múltiplo de porta do AS/400 130
 - descrição 15
 - filtragem de IP 130
 - processamento de manutenção de atividade 129
- sessões LU-LU 55
- SLU 211
- SNA
 - arquitetura de serviços de gerenciamento, níveis de 62
 - com Communications Server 23
 - Communications Server e X.25
 - conexões X.25 possíveis 154
 - planejamento para configuração X.25 153
 - compactação de dados 10
 - conexões de estações de trabalho comutadas de SDLC 114
 - confidencialidade de dados de nível de sessão 60
 - definição 53
 - desempenho 119
 - funções
 - API de APPC 52
 - definições de controle de ligação de dados 24
 - LU dependente de SSCP 56
 - sessões LU-LU 55
 - suporte à LU 52
 - visão geral 23
 - gateways 65
 - configuração do endereço de destino de Rede Local 116
 - discussão geral 113
 - ligações suportadas para estações de trabalho 113
 - ligações suportadas para sistemas centrais 114
 - prioridade de transmissão 47
 - processo de configuração
 - controle de fluxo da sessão 63
 - discussão geral 18
 - janelas de configuração (CMSETUP) 18
 - serviços de gerenciamento 61
 - suporte
 - LUs agrupadas e dedicadas 116
 - suporte ao cliente API 17
 - visão geral de 119
- SNA (Systems Network Architecture)
 - definido 8
 - discussão geral 4, 23
 - ponto de controle (CP)
 - controle de ligação de dados 34
 - discussão geral 27
 - ligações lógicas 34
 - sessões CP-CP 28
 - redes de conexão 40
 - serviços de diretório 42
 - serviços de topologia e seleção de rota
 - banco de dados de topologia 45
 - classe de serviço 47

- SNA (Systems Network Architecture) (*continuação*)
 - serviços de topologia e seleção de rota (*continuação*)
 - discussão geral 44
 - modos 46
 - roteamento de sessão intermediária 49
 - seleção de rota 48
 - tipos de nós
 - discussão geral 25
 - fim 27
 - LEN 27
 - rede 26
 - unidades lógicas (LUs) 6
- SNA Gateway e Communications Server
 - configuração do endereço de destino de Rede Local 116
 - desempenho do SNA Gateway 119
 - discussão geral 113
 - ligações suportadas para estações de trabalho 113
 - ligações suportadas para sistemas centrais 114
- Sockets sobre SNA
 - descrição 71
- sockets sobre SNA
 - Nomes de LU 187
 - software do emulador 210
- Solicitador da LU Dependente (DLUR) 56
 - suporte 53
 - visão geral 11
- soquetes sobre SNA
 - como utilizar gateway de soquetes sobre SNA 13, 71
 - função de descoberta de roteamento 90
- suporte à administração 19
- suporte à configuração local 18
- suporte à configuração remota 18
- suporte à programação 9
- suporte ao cliente
 - API de SNA 17
 - Novell IntranetWare para SAA 18
- Suporte ao cliente Novell IntranetWare para SAA 18
- suporte ao gateway
 - aplicações em uma rede de subárea 66
 - comandos do NetView 66
 - como um conversor de protocolo 66
 - descrição 65
 - LAN Network Manager 66
 - tabela de dispositivos 67
 - transmissão de NMVTs 66
- suporte gateway
 - resumo dos dispositivos 67
- Suporte RUNCMD 207
- Suporte SNA Gateway
 - descrição 65

- T**
 - taxa de utilização 154
 - tipos de ligações 35

- tipos de nós
 - discussão geral 25
 - nó da rede 26
 - nó final 27
 - Nós LEN 27
- topologia
 - banco de dados de topologia 45
 - classe de serviço 47
 - discussão geral 44
 - modos 46
 - roteamento de sessão intermediária 49
 - seleção de rota 48
- transporte de vetor de gerenciamento de rede (NMVTs) 66

- U**
 - Unidade de Pedido (RU) 211
 - unidades lógicas (LUs)
 - discussão geral 6
 - nomes 186
 - suporte 52

- V**
 - VTAM/NCP
 - parâmetros de sistema central NTRI 157
 - parâmetros de sistema central SDLC 161
 - parâmetros de sistema central X.25 170

- W**
 - WinSock 84, 85

- X**
 - X.25
 - Parâmetros de conexão do sistema central APPC 171
 - Parâmetros de conexão do sistema central NPSI 169
 - Parâmetros de conexão sistema central VTAM/NCP 170

Comentários do Leitor

eNetwork Communications Server
Versão 6.0
para Windows NT
Guia de Administração de Rede
Versão 6.0

Publicação N&ous. S517-1394-00

Neste formulário, faça-nos saber sua opinião sobre este manual. Utilize-o se encontrar algum erro, ou se quiser externar qualquer opinião a respeito (tal como organização, assunto, aparência ...) ou fazer sugestões para melhorá-lo.

Para pedir publicações extras, fazer perguntas ou tecer comentários sobre as funções de produtos ou sistemas da IBM, fale com o seu representante IBM.

Quando você envia seus comentários, concede direitos, não exclusivos, à IBM para usá-los ou distribuí-los da maneira que achar conveniente, sem que isso implique em qualquer compromisso ou obrigação para com você.

Não se esqueça de preencher seu nome e seu endereço abaixo, se desejar resposta.

Nome

Endereço

Companhia ou Empresa

Telefone

Comentários do Leitor
S517-1394-00



Corte ou
dobre
ao longo
da linha

Dobre e cole com fita

Não grampeie

Dobre e cole com fita

COLE
SELO
POSTAL
AQUI

Centro Industrial IBM Brasil
Centro de Traduções
Caixa Postal 71
CEP 13001-970 Campinas, SP
BRASIL 27709-9990

Dobre e cole com fita

Não grampeie

Dobre e cole com fita

S517-1394-00

Corte ou
dobre
ao longo
da linha



Impresso na Dinamarca

S517-1394-00

