



@server

iSeries

Configuração de TCP/IP para Funcionamento em Rede

Versão 5 Edição 3





@server

iSeries

Configuração de TCP/IP para Funcionamento em Rede

Versão 5 Edição 3

Parte 1. Configuração de TCP/IP

O servidor chegou e o utilizador está preparado para o pôr a funcionar. Este tópico apresenta ferramentas e procedimentos de configuração de TCP/IP em OS/400. Por exemplo, poderá usar estas informações para criar uma descrição de linha, uma interface de TCP/IP e um encaminhamento. Ficarão também a saber como personalizar a configuração de TCP/IP com o iSeries Navigator e conhecerá diversas técnicas de TCP/IP que permitem direccionar os dados que entram e saem da sua rede.

Antes de utilizar estas informações de configuração de TCP/IP, consulte Instalação e utilização do hardware para se assegurar de que instalou todos os componentes de hardware necessários. Após a conclusão das tarefas iniciais de configuração de TCP/IP, estará preparado para expandir as capacidades do servidor com aplicações, protocolos e serviços de TCP/IP de modo a obviar a necessidades específicas.

Novidades da V5R3

Conheça funções de TCP/IP novas e alteradas.

Imprimir este tópico

Utilize este tópico para imprimir ou descarregar uma versão em PDF (Portable Document Format) da documentação sobre configuração de TCP/IP.

Internet Protocol versão 6 (IPv6)

O novo Internet Protocol, IPv6, desempenha uma função essencial no futuro da Internet e pode ser utilizado no servidor iSeries. Este tópico inclui informações gerais sobre o IPv6 e respectiva implementação no servidor iSeries.

Planear a configuração de TCP/IP

Este tópico ajuda-o a preparar-se para a instalação e configuração do TCP/IP no servidor iSeries. Inclui requisitos básicos para instalação e configuração para que disponha de todas as informações necessárias quando começar a configurar o TCP/IP. Inclui ainda referências a termos e conceitos relacionados.

Instalar TCP/IP

Este tópico acompanha a instalação de produtos que preparam o servidor iSeries para começar a funcionar.

Configurar TCP/IP

Este tópico mostra como preparar o iSeries e configurar TCP/IP. Além disso, consulte as instruções para configurar IPv6.

Personalizar TCP/IP com o iSeries Navigator

Este tópico inclui opções de personalização com a utilização do iSeries Navigator.

Técnicas de TCP/IP via Ethernet virtual

Conheça as vantagens da Ethernet virtual em OS/400.

Deteção e resolução de problemas de TCP/IP

Se deparar com problemas relativos a ligações ou tráfego de TCP/IP, consulte a secção Deteção e resolução de problemas de TCP/IP para saber as possíveis soluções. Este guia de deteção e resolução de problemas ajuda-o a resolver problemas relacionados com IPv4 e IPv6.

Informações relacionadas para configuração de TCP/IP

Este tópico responde à pergunta "Que mais posso fazer?" Encontre referências a serviços e aplicações que melhoram o rendimento do servidor.

Capítulo 1. Novidades da V5R3


Aperfeiçoamentos à configuração de TCP/IP

Se utilizar uma rede de Ethernet virtual para que as partições existentes comuniquem entre si, poderá necessitar de expandir essa comunicação a uma rede local (LAN) física externa. Consulte Técnicas de TCP/IP para ligar Ethernet virtual a redes locais externas para saber como ligar a rede Ethernet virtual a uma rede local externa. Use estas informações para rever exemplos que ilustram três métodos diferentes para fazer a ponte ao tráfego de rede entre a rede Ethernet virtual e uma rede local externa.

Para localizar outras informações sobre novidades ou alterações desta edição, consulte oMemorando para Utilizadores.

Como ver as novidades ou as alterações

Para ajudar a ver onde se encontram as alterações técnicas, estas informações usam a seguinte sinalética:

- A imagem  para assinalar onde começam as informações novas ou alteradas.
- A imagem  para assinalar onde terminam as informações novas ou alteradas.



Capítulo 2. Imprimir este tópico

Para ver ou transferir a versão deste documento em PDF, seleccione Configuração de TCP/IP (cerca de 362 Kb).



Outras informações

Poderá ainda ver ou imprimir os seguintes PDFs:

- Manuais:

- **TCP/IP Configuration and Reference**  (592 KB)
Este manual inclui informações sobre configuração de TCP/IP (Transmission Control Protocol/Internet Protocol), funcionamento e gestão da rede.
- **Tips and Tools for Securing your iSeries**  (1 MB)
Este manual inclui recomendações básicas sobre a utilização das funções de segurança do iSeries para proteger o servidor e as operações associadas.

- Redbooks:


- **TCP/IP Tutorial and Technical Overview**  (7 MB)
Este redbook fornece informações sobre os conceitos básicos de TCP/IP.
- **TCP/IP for AS/400: More Cool Things Than Ever**  (9 MB)
Este redbook inclui uma lista extensiva de aplicações e serviços comuns de TCP/IP.

Guardar ficheiros PDF

Para guardar um ficheiro PDF na estação de trabalho para posterior visualização ou impressão:

1. Faça clique com o botão direito do rato sobre o PDF no browser (faça clique com o botão direito do rato sobre a ligação acima).
2. Clique em **Save Target As...** se usar o Internet Explorer. Clique em **Save Link As...** se usar Netscape Communicator.
3. Seleccione o directório no qual deseja guardar o ficheiro PDF.
4. Faça clique sobre **Save**.

Transferir o Adobe Acrobat Reader

O Adobe Acrobat Reader é necessário para ver ou imprimir estes ficheiros PDF. Poderá transferir uma cópia do sítio na Web da Adobe (www.adobe.com/products/acrobat/readstep.html) .

Capítulo 3. Internet Protocol versão 6 (IPv6)

O Internet Protocol versão 6 (IPv6) é a versão actualizada do Internet Protocol versão 4 (IPv4) e tem vindo gradualmente a substituir o IPv4 como norma de Internet.

Poderá simplesmente saber como se processa a utilização do IPv6 para melhorar o e-business da sua empresa, ou poderá ser programador e pretender criar aplicações de IPv6 para que a mesma empresa possa beneficiar deste protocolo Internet aperfeiçoado. Leia estes tópicos para encontrar informações básicas sobre o IPv6 e como o utilizar no servidor iSeries:

O que é o IPv6?

Saiba por que razão o IPv6 veio substituir o IPv4 como norma da Internet e como pode utilizá-lo em benefício próprio.

Quais as funções do IPv6 disponíveis?

Saiba como o IPv6 está presentemente a ser implementado no servidor iSeries.

Cenários do IPv6

Veja exemplos que o ajudarão a compreender situações em que utilizaria o IPv6 na sua empresa.

Conceitos do IPv6

Aprenda conceitos básicos sobre o IPv6. Se não tem a certeza de quais as diferenças entre o IPv4 e o IPv6, consulte as comparações detalhadas, como por exemplo, em que medida os endereços de IPv4 e IPv6 se comparam entre si ou como os cabeçalhos de pacotes do IPv4 diferem dos cabeçalhos de pacotes do IPv6.

Configurar IPv6

Saiba onde encontrar requisitos de hardware e software e instruções para configurar o IPv6 no servidor.

Deteção e resolução de problemas do IPv6

Encontre soluções para problemas no IPv6.

Informações relacionadas com o IPv6

Saiba onde encontrar ligações a recursos que o ajudam a compreender o IPv6.

O que é o IPv6?

O Internet Protocol versão 6 (IPv6) é a evolução no futuro dos protocolos Internet. A maioria dos utilizadores da Internet utiliza actualmente o IPv4 e este protocolo provou ser fiável e resistente durante mais de 20 anos. No entanto, o IPv4 tem graves limitações que tendem a causar mais problemas com a expansão crescente da Internet.

Verifica-se especialmente uma carência cada vez maior de endereços de IPv4, os quais são necessários para todos os novos dispositivos adicionados à Internet. A chave para o aperfeiçoamento do IPv6 é a expansão do espaço de endereços de IP de 32 bits para 128 bits, o que permite endereços de IP praticamente ilimitados e exclusivos. O novo formato de texto de endereços do IPv6 é:

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

em que cada x é um dígito hexadecimal que representa 4 bits.

A capacidade de endereçamento expandida do IPv6 constitui uma solução para o problema da carência de endereços, o que assume particular relevância à medida que vai aumentando a utilização da

informática portátil, como telemóveis e computadores portáteis. A crescente procura por parte de utilizadores de aparelhos sem fios contribui para a falta de endereços IPv4. A capacidade expandida dos endereços de IP do IPv6 resolve este problema ao fornecer endereços de IP suficientes para o número crescente de dispositivos sem fios.

Além desta capacidade de endereçamento, o IPv6 fornece novas funções que simplificam as tarefas de configuração e gestão dos endereços existentes na rede. A configuração e manutenção de redes é uma actividade intensiva. O IPv6 reduz algum do volume de trabalho ao automatizar várias tarefas do administrador.

Se utiliza IPv6, não terá de voltar a numerar os endereços dos dispositivos quando mudar para um ISP (Internet Service Provider - fornecedor de serviços de Internet) diferente. Poderá manter estes endereços uma vez que são endereços globalmente exclusivos.

A função de configuração automática do IPv6 configura automaticamente endereços de interface e de encaminhador. Numa configuração automática sem estado, o IPv6 obtém o endereço MAC da máquina e um prefixo de rede fornecido por um nó local e combina estes dois endereços para criar um novo endereço de IPv6 exclusivo. Esta função elimina a necessidade de um servidor de DHCP, o que ajuda a poupar tempo ao administrador e dinheiro à empresa.

Para mais fontes de informação sobre IPv6, consulte a secção Informações relacionadas sobre IPv6

Consulte a secção Quais as funções do IPv6 disponíveis? para obter informações sobre o IPv6 relacionadas especificamente com o servidor iSeries.

Quais as funções do IPv6 disponíveis?

A IBM está a implementar o IPv6 para o servidor iSeries em várias edições de software. O IPv6 está actualmente implementado numa plataforma de desenvolvimento de aplicações com a finalidade de desenvolver e testar aplicações do IPv6. As funções do IPv6 são transparentes para as aplicações do TCP/IP existentes e coexistem com as funções do IPv4.

Seguem-se as funções principais do servidor iSeries que são afectadas pelo IPv6:

- **Configuração**

Tenha em atenção que o processo de configuração do IPv6 é diferente do processo do IPv4. Para utilizar a função do IPv6, terá de alterar a configuração de TCP/IP do servidor configurando uma linha para o IPv6. Pode configurar o IPv6 numa linha de Ethernet ou numa linha de túnel.

Se configurar uma linha de Ethernet para o tráfego do IPv6, enviará pacotes de IPv6 numa rede de IPv6. Consulte a secção Criar uma rede local (LAN) do IPv6 para ver um cenário que descreve uma situação de configuração de uma linha de Ethernet para o IPv6.

Se configurar linhas de túnel, enviará pacotes de IPv6 numa rede de IPv4 existente. Consulte as secções Enviar pacotes de IPv6 numa rede local (LAN) de IPv4 e Enviar pacotes de IPv6 numa rede alargada (WAN) de IPv4 para ver cenários que descrevem duas situações de criação de uma linha de túnel configurada para IPv6.

Consulte Configurar o IPv6 para configurar a sua rede para o IPv6.

- **Sockets**

Desenvolva e teste aplicações de sockets com APIs e ferramentas do IPv6. O IPv6 melhora os sockets de modo a que as aplicações possam utilizar o IPv6 com uma nova família de endereços: AF_INET6. Estes aperfeiçoamentos não afectam as aplicações de IPv4 existentes. Poderá criar aplicações que suportem o tráfego simultâneo de IPv4 e IPv6 ou tráfego só de IPv6. Consulte a secção Utilizar uma família de endereços de AF_INET6 para mais informações sobre o IPv6 para sockets.

- **DNS**
O Domain Name System (DNS) suporta endereços AAAA e um novo domínio para procuras invertidas: IP6.ARPA. Embora seja verdade que o DNS obtém informações de IPv6, o servidor tem de utilizar o IPv4 para comunicar com o DNS.
- **Detecção e resolução de problemas de TCP/IP**
Utilize ferramentas padrão de detecção e resolução de problemas, como os comandos PING e netstat, encaminhamento de rastreio e rastreio de comunicações para redes e túneis de IPv6. Estas ferramentas suportam agora o formato de endereços do IPv6. Consulte a secção Detecção e resolução de problemas de TCP/IP para resolver problemas relacionados com ambas as redes de IPv4 e IPv6.

Consulte a secção Informações relacionadas sobre IPv6 para ver recursos do IPv6.

Cenários: IPv6

Observe os seguintes cenários para saber por que razão deverá implementar o IPv6 e como configurar a sua rede numa das seguintes situações:

- Criar uma rede local (LAN) do IPv6
- Enviar pacotes de IPv6 numa rede local (LAN) do IPv4
- Enviar pacotes de IPv6 numa rede alargada (WAN) de IPv4

Nota: nos cenários, os endereços de IP 10.x.x.x representam endereços de IP públicos. Todos os endereços utilizados nestes cenários destinam-se apenas a fins exemplificativos.

Consulte a secção Configurar o IPv6 para configurar o servidor para IPv6.

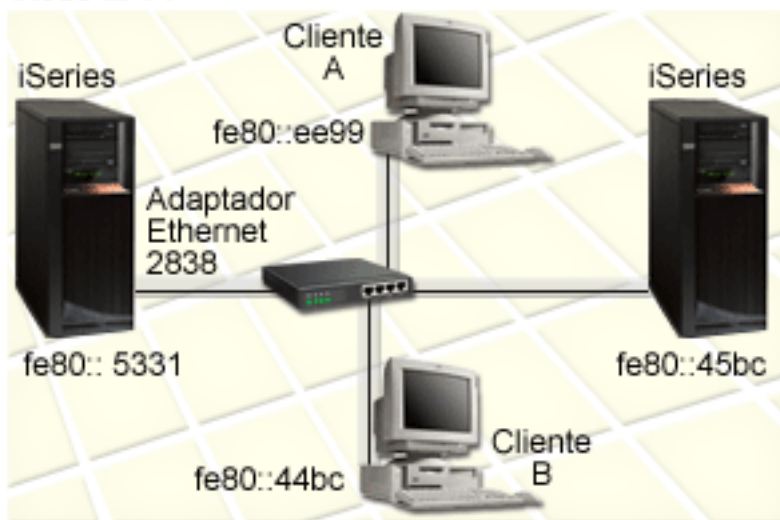
Consulte a secção Conceitos de IPv6 para ver definições de conceitos básicos do IPv6.

Criar uma rede local (LAN) de IPv6

Situação

O IPv6 tende a substituir o IPv4 como norma de Internet. Por conseguinte, a sua empresa decide implementar o IPv6 para as operações financeiras e adquire uma nova aplicação contabilística que utiliza IPv6 para fins de conectividade. A aplicação necessita de estabelecer ligação a outra instância da aplicação que se encontra num servidor diferente ligado à rede local (LAN) de Ethernet do local. O seu trabalho consiste em configurar o servidor para o IPv6 de modo a que a sua empresa possa começar a utilizar a aplicação contabilística. A figura que se segue ilustra a configuração da rede neste cenário.

Departamento de Contabilidade Rede IPv6



Solução

Para criar uma rede local de IPv6, terá de configurar uma descrição de linha de Ethernet para o IPv6. Os pacotes de IPv6 passam entre servidores e clientes do iSeries na rede à medida que os empregados utilizam a aplicação contabilística.

Os requisitos de configuração incluem:

- OS/400 Versão 5, Edição 2 ou posterior
- Adaptadores de Ethernet 2838 ou 2849, já que são os únicos tipos de recursos de hardware actualmente suportados em IPv6.
- iSeries Access for Windows and iSeries Navigator (componente de rede do iSeries Navigator)
- O servidor tem de ter uma interface física de IPv4 separada configurada antes de configurar a linha de Ethernet para o IPv6 porque o TCP/IP tem de estar em execução no servidor. Se não tiver configurado o servidor para IPv4, consulte a secção Configurar TCP/IP pela primeira vez antes de configurar a linha para o IPv6.

Configuração

Para configurar uma descrição de linha de Ethernet para o IPv6, tem de utilizar o assistente **IPv6 Configuration** no iSeries Navigator. O IPv6 só pode ser configurado a partir do iSeries Navigator e não pode ser configurado a partir da interface baseada em caracteres.

O assistente requer o nome do recurso de comunicações de hardware no servidor em que irá configurar o IPv6; por exemplo, CMN01. Este tem de ser um adaptador de Ethernet 2838 ou 2849 que não esteja configurado actualmente para IPv4.

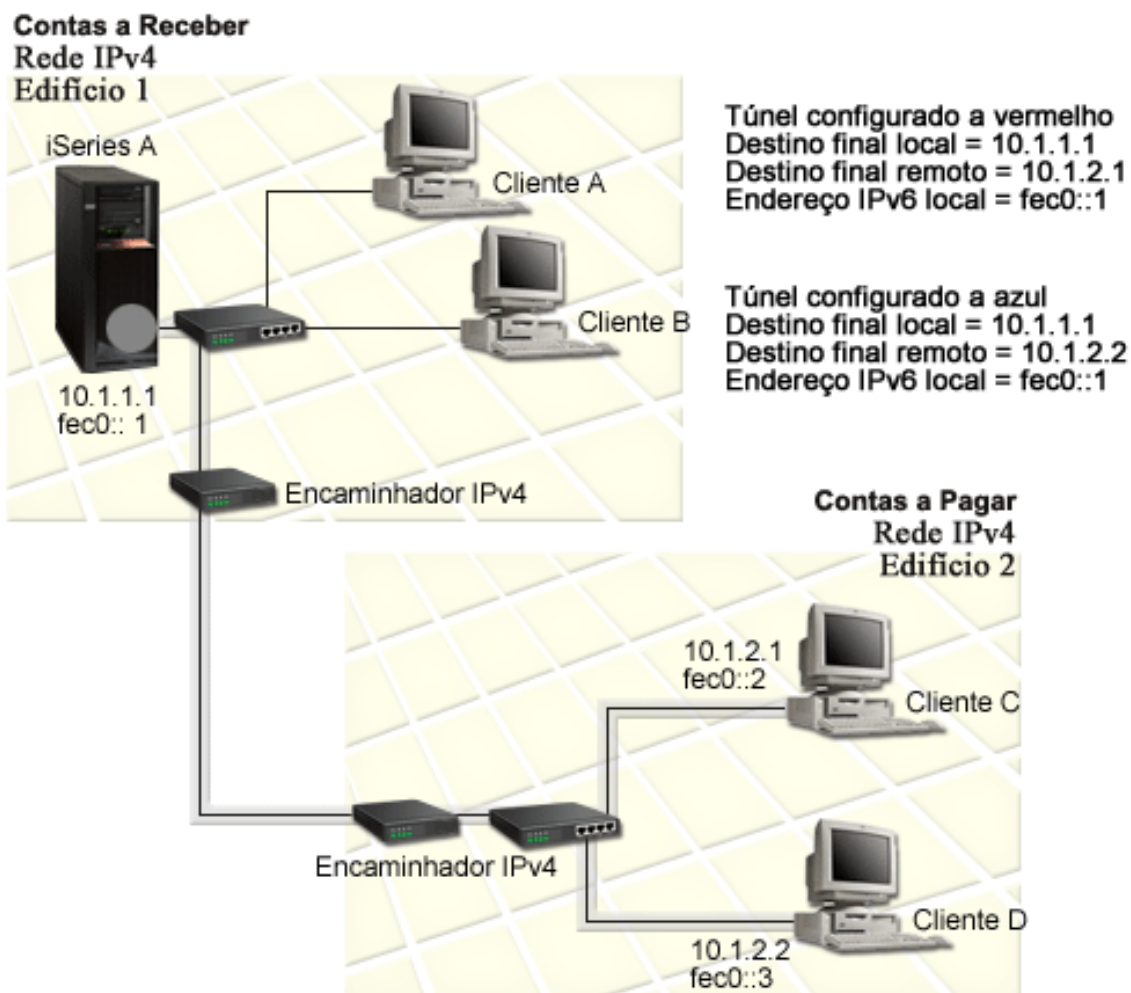
Para utilizar o assistente **IPv6 Configuration**, siga estes passos:

1. No iSeries Navigator, seleccione o seu **servidor** —> **Network** —> **TCP/IP Configuration**.
2. Faça clique com o botão direito do rato sobre **IPv6**, seleccione **IPv6 Configuration** e siga as instruções do assistente para configurar uma linha de Ethernet para o IPv6.

Enviar pacotes de IPv6 numa rede local (LAN) de IPv4

Situação

A sua empresa escreveu uma nova aplicação contabilística do IPv6. Trata-se de uma aplicação servidor-cliente que irá utilizar localmente. A aplicação comunica com outras instâncias de si própria que se encontram na mesma instalação, mas noutros edifícios e redes locais (LANs). Embora a sua empresa pretenda utilizar o IPv6 para esta aplicação, não está preparada para mudar toda a infra-estrutura do IPv4 para o IPv6. O seu trabalho é configurar linhas de túnel de IPv6 que permitam a transmissão de pacotes de IPv6 através das redes de IPv4 locais. A figura que se segue ilustra a configuração da rede neste cenário.



Solução

Para utilizar o IPv6 nestas redes locais de IPv4, terá de criar dois túneis configurados e vários encaminhamentos associados. Um túnel está assinalado a vermelho e o outro a azul, para fins exemplificativos.

Primeiro, considere o túnel a vermelho:

- O túnel a vermelho começa no iSeries A (ponto de terminação local 10.1.1.1) no Edifício 1 e termina no Cliente C (ponto de terminação remoto 10.1.2.1) no Edifício 2.
- O iSeries A encapsula um pacote de IPv6 num pacote de IPv4 e envia o pacote de IPv4 pelo túnel para o Cliente C, que retira o pacote de IPv6 do encapsulamento, de modo a poder ligar-se a outra instância da aplicação do IPv6.

A seguir, considere o túnel a azul:

- O túnel a azul começa em iSeries A (ponto de terminação local 10.1.1.1) no Edifício 1, tal como o túnel a vermelho; no entanto, o túnel a azul termina no Cliente D (ponto de terminação remoto 10.1.2.2) no Edifício 2.
- O iSeries A encapsula um pacote de IPv6 num pacote de IPv4 e envia o pacote de IPv4 pelo túnel para o Cliente D, que retira o pacote de IPv6 do encapsulamento de modo a poder ligar-se a outra instância da aplicação do IPv6.

Cada ligação de túnel é do tipo ponto a ponto, de modo que terá de definir um ponto de terminação remoto para cada túnel. Esta tarefa é realizada através da criação de dois encaminhamentos. Cada encaminhamento está associado à mesma linha de túnel, mas define um ponto de terminação remoto diferente como sistema de passagem seguinte. Por outras palavras, irá definir os pontos de terminação remotos de cada túnel à medida que criar os encaminhamentos.

Além da criação dos encaminhamentos iniciais que definem os pontos de terminação do túnel e permitem que os pacotes cheguem aos clientes no Edifício 2, terá de criar mais dois encaminhamentos para que os pacotes possam regressar ao servidor no Edifício 1.

Os requisitos de configuração incluem:

- OS/400 Versão 5, Edição 2 ou posterior
- iSeries Access for Windows and iSeries Navigator (componente de rede do iSeries Navigator)
- O TCP/IP (com IPv4) tem de ser configurado no servidor para poder criar a linha de túnel configurada. Se não tiver configurado o servidor para IPv4, consulte a secção Configurar TCP/IP pela primeira vez antes de configurar a linha de túnel para IPv6.

Configuração

Para criar uma linha de túnel configurada, tem de utilizar o assistente **IPv6 Configuration** e o assistente **New IPv6 Route** no iSeries Navigator. O IPv6 só pode ser configurado a partir do iSeries Navigator e não a partir da interface baseada em caracteres.

Para utilizar o assistente **IPv6 Configuration** para criar a linha de túnel a vermelho, siga estes passos:

1. No iSeries Navigator, seleccione o seu **servidor** → **Network** → **TCP/IP Configuration**.
2. Faça clique com o botão direito do rato sobre **IPv6**, seleccione o assistente **IPv6 Configuration** e siga as instruções do assistente para configurar uma linha de túnel para o IPv6. Após concluir o assistente **IPv6 Configuration**, este pedir-lhe-á que crie um novo encaminhamento para a linha de túnel configurada e será apresentada a caixa de diálogo **New IPv6 Route**. Terá de criar um novo encaminhamento para permitir que os pacotes de IPv6 passem pelo túnel a vermelho.
3. No assistente **New IPv6 Route**, crie um encaminhamento para o túnel a vermelho. Especifique o ponto de terminação remoto 10.1.2.1 como sistema de passagem seguinte e especifique fec0::2 como endereço destino.

Utilize de novo o assistente **New IPv6 Route** para criar um encaminhamento para o túnel a azul. Note que não é necessário criar o túnel a azul com o assistente **IPv6 Configuration**. O túnel a azul é criado quando definir o respectivo ponto de terminação remoto com o assistente **New IPv6 Route**. Para utilizar o assistente **New IPv6 Route**, siga estes passos:

1. No iSeries Navigator, seleccione o seu **servidor** → **Network** → **TCP/IP Configuration** → **IPv6**.

2. Faça clique com o botão direito do rato sobre **Routes**, seleccione **New Route** e siga as instruções do assistente para configurar um encaminhamento de IPv6 para o túnel a azul. Especifique o ponto de terminação remoto 10.1.2.2 como sistema de passagem seguinte e especifique fec0::3 como endereço destino.

Após criar as linhas de túnel configuradas e os encaminhamentos que definem os pontos de terminação do túnel, terá de criar um encaminhamento no Cliente C e outro no Cliente D que permita aos pacotes passarem de novo para o servidor no Edifício 1. Para cada um destes encaminhamentos, deverá especificar 10.1.1.1 como sistema de passagem seguinte e fec0::1 como endereço destino.

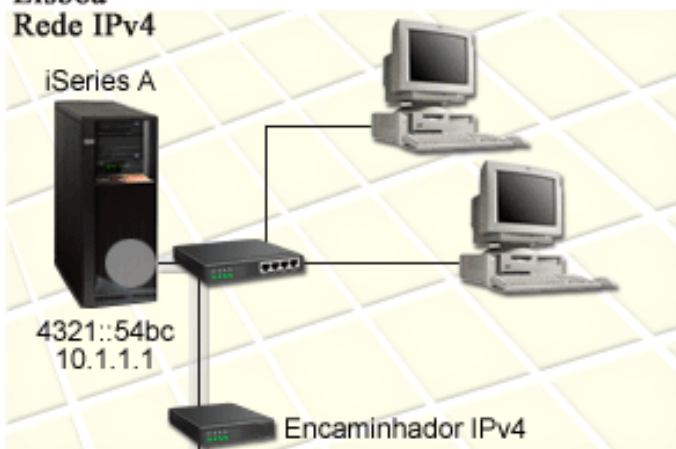
Enviar pacotes de IPv6 numa rede alargada (WAN) de IPv4

Situação

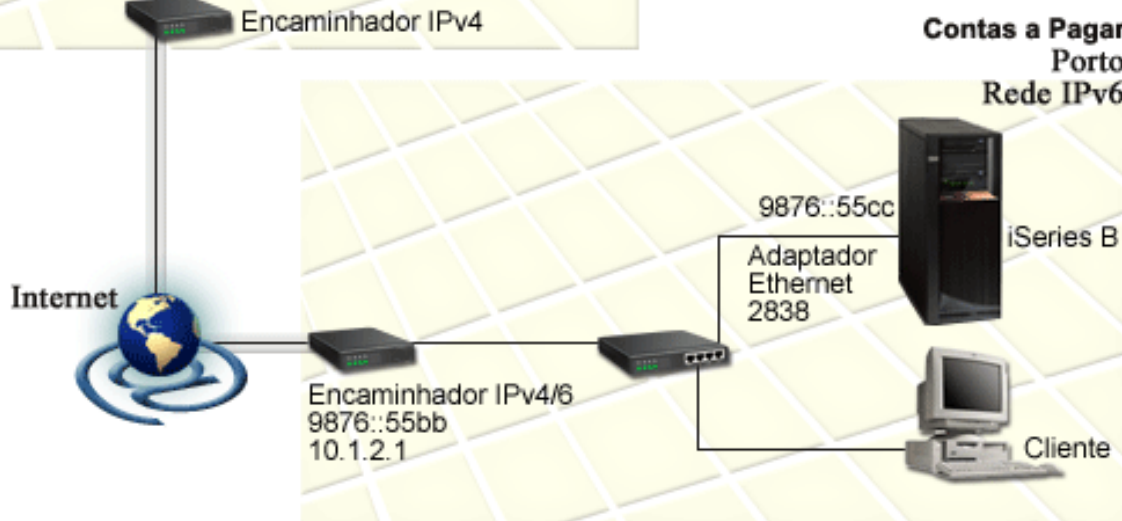
A sua empresa utiliza uma aplicação contabilística para contas a receber no servidor, na filial de Coimbra. Necessita de ligar a aplicação a um servidor na Filial do Porto. Esta aplicação utiliza o endereçamento de IPv6 nos servidores em ambas as cidades. Uma vez que o seu ISP não pode fornecer encaminhamentos de IPv6 entre os dois escritórios, tem de configurar um túnel entre os dois servidores. Os pacotes de aplicações passam pelo túnel através da rede alargada de IPv4 entre os dois servidores. A figura que se segue ilustra a configuração da rede neste cenário.

Nota: neste cenário, os endereços de IP 10.x.x.x representam endereços de IP públicos que podem ser globalmente encaminhados. Todos os endereços utilizados destinam-se apenas a fins exemplificativos.

Contas a Receber
Lisboa
Rede IPv4



Túnel configurado a verde
Destino final local = 10.1.1.1
Destino final remoto = 10.1.2.1
Endereço IPv6 local = 4321::54bc



Solução

Para utilizar o IPv6 numa rede alargada que consista numa infra-estrutura de IPv4, terá de criar uma linha de túnel configurada e vários encaminhamentos associados. Este esquema funciona do seguinte modo:

- O túnel começa em iSeries A (ponto de terminação local 10.1.1.1) em Coimbra e termina no encaminhador de IPv4/6 (ponto de terminação remoto 10.1.2.1) no Porto.
- A aplicação que reside no iSeries A necessita de estabelecer ligação com a aplicação que reside no iSeries B. O iSeries A encapsula o pacote de IPv6 no pacote de IPv4 e envia-o pelo túnel para o encaminhador de IPv4/6, que retira o pacote de IPv6 do encapsulamento e reencaminha o pacote de IPv6 para o iSeries B.
- O pacote regressa a Coimbra tomando o caminho inverso.

A ligação de túnel é do tipo ponto a ponto, de modo que terá de definir o ponto de terminação remoto do túnel. Esta acção é executada criando um encaminhamento que esteja associado a esta linha de túnel. O encaminhamento define o ponto de terminação remoto(10.1.2.1) como sistema de passagem seguinte. Por outras palavras, irá definir o ponto de terminação remoto à medida que criar o encaminhamento. Além disso, o encaminhamento define o endereço destino como 9876::55cc (o endereço de IPv6 associado ao iSeries B).

Além de criar o encaminhamento inicial que define o ponto de terminação do túnel e permite que o pacote passe para o iSeries B no Porto, terá de criar mais dois encaminhamentos para que o pacote possa regressar ao iSeries A em Coimbra.

Os requisitos de configuração incluem:

- OS/400 Versão 5, Edição 2 ou posterior
- iSeries Access for Windows and iSeries Navigator (componente de rede do iSeries Navigator)
- O TCP/IP (com IPv4) tem de ser configurado no servidor para poder criar a linha de túnel configurada. Se não tiver configurado o servidor para IPv4, consulte a secção Configurar TCP/IP pela primeira vez antes de configurar a linha de túnel para IPv6.

Configuração

Para criar uma linha de túnel configurada, tem de utilizar o assistente **IPv6 Configuration** e o assistente **New IPv6 Route** no iSeries Navigator. Os túneis configurados só podem ser configurados a partir do iSeries Navigator e não da interface baseada em caracteres.

Para utilizar o assistente **IPv6 Configuration** para criar a linha de túnel, siga estes passos:

1. No iSeries Navigator, seleccione o seu **servidor** —> **Network** —> **TCP/IP Configuration**.
2. Faça clique com o botão direito do rato sobre **IPv6**, seleccione **IPv6 Configuration** e siga as instruções do assistente para configurar uma linha de túnel para o IPv6. Após concluir o assistente **IPv6 Configuration**, este pedir-lhe-á que crie um novo encaminhamento para a linha de túnel configurada e será apresentada a caixa de diálogo **New IPv6 Route**. Terá de criar um novo encaminhamento para permitir que os pacotes de IPv6 passem pelo túnel.
3. No assistente **New IPv6 Route**, crie um encaminhamento de sistema central para o túnel. Especifique o ponto de terminação remoto 10.1.2.1 como sistema de passagem seguinte e especifique 9876::55cc como endereço destino.

Após criar a linha de túnel configurada e o encaminhamento que define o ponto de terminação do túnel, terá de criar encaminhamentos no iSeries B e no encaminhamento de IPv4/6 que permite que os pacotes regressem a Coimbra. Para o encaminhamento no iSeries B, deverá especificar 9876::55bb como sistema de passagem seguinte e 4321::54bc como endereço destino. Para o encaminhamento no encaminhador de IPv4/6, deverá especificar 10.1.1.1 como sistema de passagem seguinte e 4321::54bc como endereço destino.

Nota: o encaminhador de IPv4/6 no Porto deverá ter um encaminhamento directo para 9876::55cc, mas, uma vez que este encaminhamento é criado automaticamente, não é necessária nenhuma configuração manual.

Conceitos: IPv6

Leia as descrições destes conceitos de IPv6 para melhor compreender o modo de funcionamento do IPv6:

Comparar IPv4 e IPv6

Saiba como os atributos de IPv4 correspondem aos de IPv6. Esta tabela permite-lhe procurar rapidamente funções específicas e comparar a respectiva utilização em cada protocolo Internet.

Formatos de endereço de IPv6

Saiba qual o tamanho e formato do endereço de IPv6.

Tipos de endereço de IPv6

Conheça os novos tipos de endereços no âmbito do IPv6.

Direcionamento de IPv6

Saiba como o direcionamento do IPv6 permite que pacotes IPv6 passem numa rede IPv4.

Identificação de vizinhos

Saiba como a identificação de vizinhos permite que sistemas centrais e encaminhadores comuniquem entre si.

Configuração automática de endereços sem estado

Saiba como a configuração automática de endereços sem estado automatiza algumas das tarefas do administrador de rede.

Formatos de endereço de IPv6

O tamanho dos endereços de IPv6 é de 128 bits. A representação de endereços de IPv6 preferencial é: `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx` em que cada x é um dígito hexadecimal que representa 4 bits. Os endereços de IPv6 vão de `0000:0000:0000:0000:0000:0000:0000:0000` a `ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`.

Além deste formato preferencial, os endereços de IPv6 podem ser especificados em dois outros formatos abreviados:

- **Omitir zeros à esquerda**
Especifique endereços de IPv6 omitindo os zeros à esquerda. Por exemplo, o endereço IPv6 `1050:0000:0000:0000:0005:0600:300c:326b` pode ser escrito como `1050:0:0:0:5:600:300c:326b`.
- **Dois pontos duplos**
Especifique endereços de IPv6 utilizando dois pontos duplos (`::`) em vez de uma série de zeros. Por exemplo, o endereço de IPv6 `ff06:0:0:0:0:0:0:c3` pode ser escrito como `ff06::c3`. Os dois pontos duplos só podem ser utilizados uma vez num endereço de IP.

Um formato alternativo para os endereços de IPv6 combina os dois pontos e a notação decimal, de modo que o endereço de IPv4 pode ser incorporado no endereço de IPv6. São especificados valores hexadecimais para os 96 bits mais à esquerda e valores decimais para os 32 bits mais à direita que indicam o endereço de IPv4 incorporado. Este formato assegura a compatibilidade entre os nós de IPv6 e de IPv4 quando estiver a trabalhar num ambiente de rede misto.

Estes dois tipos de endereços de IPv6 utilizam o seguinte formato alternativo:

- **Endereço de IPv6 correlacionado com IPv4**
Este tipo de endereço é utilizado para representar nós de IPv4 como endereços de IPv6. Permite que aplicações de IPv6 comuniquem directamente com aplicações de IPv4. Por exemplo, `0:0:0:0:ffff:192.1.56.10` e `::ffff:192.1.56.10/96` (formato abreviado).
- **Endereço de IPv6 compatível com IPv4**
Este tipo de endereço é utilizado para direcionamento. Permite que os nós de IPv6 comuniquem através de uma infra-estrutura de IPv4. Por exemplo, `0:0:0:0:0:0:192.1.56.10` e `::192.1.56.10/96` (formato abreviado).

Todos estes formatos são formatos de endereço de IPv6 válidos. Especifique qualquer um destes formatos de endereço de IPv6 no iSeries Navigator.

Tipos de endereço de IPv6

Os endereços de IPv6 estão categorizados em três tipos básicos:

Endereço de unidifusão

O endereço de unidifusão especifica uma única interface. Um pacote enviado para um destino de endereço de unidifusão passa de qualquer sistema central para o sistema central destino.

Os três tipos de endereços de unidifusão incluem:

Endereço local de ligação

Os endereços locais de ligação destinam-se à utilização numa única ligação local (rede local). Os endereços locais de ligação são automaticamente configurados em todas as interfaces. O prefixo utilizado para um endereço local de ligação é fe80::/10. Os encaminhadores não reencaminham pacotes com um endereço destino ou origem que contenha um endereço local de ligação.

Endereço local de instalação

Os endereços locais de instalação destinam-se a ser utilizados numa instalação específica. O prefixo utilizado para um endereço local de instalação é fec0::/10. Os encaminhadores não reencaminham pacotes com um endereço origem que contenha um endereço local de instalação fora de uma instalação específica.

Endereço global

Os endereços globais destinam-se à utilização em qualquer rede. O prefixo utilizado para um endereço global começa com 001 binário.

Os dois tipos de endereços de unidifusão especiais incluem:

Endereço não especificado

O endereço não especificado é 0:0:0:0:0:0:0:0 ou pode ser abreviado com dois pontos duplos (::). O endereço não especificado indica a falta de um endereço e nunca pode ser atribuído a um sistema central. Pode ser utilizado por um sistema central de IPv6 que ainda não tenha um endereço atribuído. Por exemplo, quando o sistema central envia um pacote para identificar um endereço de outro nó, o sistema central utiliza o endereço não especificado como o respectivo endereço origem.

Endereço de reinício cíclico

O endereço de reinício cíclico é 0:0:0:0:0:0:0:1 ou pode ser abreviado como ::1. O endereço de reinício cíclico é utilizado por um nó para enviar um pacote para si próprio.

Endereço de difusão geral

O endereço de difusão geral especifica um conjunto de interfaces, possivelmente em diferentes localizações, que partilham um único endereço. Um pacote enviado para um endereço de difusão geral só se dirige para o membro mais próximo do grupo. O servidor iSeries não suporta presentemente endereçamento de difusão geral.

Endereço de multidifusão

O endereço de multidifusão especifica um conjunto de interfaces, possivelmente em múltiplas localizações. O prefixo utilizado para um endereço de multidifusão é ff. Se um pacote for enviado para um endereço de multidifusão, é enviada uma cópia do pacote para cada membro do grupo. O servidor iSeries fornece presentemente suporte base para endereços de multidifusão. A criação de interfaces de multidifusão e o suporte de aplicações não são presentemente suportados.

Direccionamento de IPv6

O direccionamento de IPv6 permite que o servidor iSeries seja ligado a nós de IPv6 (sistemas centrais e encaminhadores) em domínios de IPv4. O direccionamento permite que os nós ou as redes de IPv6 isolados comuniquem sem alterar a infra-estrutura de IPv4 subjacente. O direccionamento permite que os protocolos de IPv4 e IPv6 cooperem e faculta assim um modo de transição da implementação do IPv6 enquanto mantém a conectividade do IPv4.

Um túnel consiste em dois nós de pilha dupla (IPv4 e IPv6) numa rede de IPv4. Estes nós de pilha dupla suportam o processamento de comunicações quer de IPv4 quer de IPv6. Um dos nós de pilha dupla na extremidade da infra-estrutura de IPv6 insere um cabeçalho de IPv4 (encapsula) à frente de cada pacote de IPv6 que chega e envia-o tal como se se tratasse de tráfego normal de IPv4, através das ligações

existentes. Os encaminhadores de IPv4 continuam a reencaminhar este tráfego. Na outra extremidade do túnel, outro nó de pilha dupla remove o cabeçalho de IP extra do pacote de IPv6 (retira do encapsulamento) e encaminha-o para o último destino com o IPv6 padrão.

O direccionamento de IPv6 para o servidor iSeries passa através de linhas de túnel configuradas que são linhas virtuais. As linhas de túnel configuradas fornecem comunicações de IPv6 a qualquer nó com um endereço de IPv4 encaminhável que suporte túneis de IPv6. Estes nós podem existir em qualquer parte, ou seja, no domínio local do IPv4 ou num domínio remoto.

As ligações de túnel configuradas são do tipo ponto a ponto. Para configurar este tipo de linha de túnel, tem de especificar o ponto de terminação local do túnel (endereço de IPv4), como por exemplo, 124.10.10.150, e o endereço de IPv6 local, como por exemplo, 1080:0:0:0:8:800:200c:417a. Também terá de criar um encaminhamento de IPv6 para permitir que o tráfego passe pelo túnel. À medida que for criando o encaminhamento, definirá um dos pontos de terminação remotos do túnel (endereço de IPv4) como sistema de passagem seguinte do encaminhamento. Pode configurar um número ilimitado de pontos de terminação para um número ilimitado de túneis.

Consulte as secções Enviar pacotes de IPv6 numa rede local (LAN) de IPv4 e Enviar pacotes de IPv6 numa rede alargada (WAN) de IPv4 para ver cenários e figuras que demonstram o direccionamento de IPv6.

Identificação de vizinhos

As funções da identificação de vizinhos são utilizadas pelos nós de IPv6 (sistemas centrais ou encaminhadores) para identificar a presença de outros nós de IPv6, determinar endereços de nível de ligação de nós, localizar encaminhadores que suportem reencaminhamento de pacotes de IPv6 e manter uma memória cache de vizinhos de IPv6 activos. Os nós de IPv6 utilizam as seguintes cinco mensagens do Internet Control Message Protocol versão 6 (ICMPv6) para comunicar com outros nós:

Solicitação do encaminhador

Os sistemas centrais enviam estas mensagens para pedir aos encaminhadores que criem anúncios do encaminhador. Um sistema central envia uma solicitação de encaminhador inicial quando o sistema central fica disponível pela primeira vez na rede.

Anúncio do encaminhador

Os encaminhadores enviam estas mensagens periodicamente ou em resposta a uma solicitação de encaminhador. As informações fornecidas pelos anúncios de encaminhador são utilizadas pelos sistemas centrais para criar automaticamente interfaces locais de instalação, interfaces globais e encaminhamentos associados. Os anúncios de encaminhador também contêm outras informações de configuração utilizadas por um sistema central, tais como a unidade de transmissão máxima e o limite de sistemas de passagem.

Solicitação de vizinho

Os nós enviam estas mensagens para determinar o endereço de nível de ligação de um vizinho ou para verificar se um determinado vizinho ainda está contactável.

Anúncio de vizinho

Os nós enviam estas mensagens em resposta a uma solicitação de vizinho ou como mensagem não solicitada para anunciar uma alteração de endereço.

Redireccionar

Os encaminhadores utilizam estas mensagens para informar os sistemas centrais acerca de um primeiro sistema de passagem melhor para determinado destino.

Consulte o RFC 2461 para obter mais informações sobre identificação de vizinhos e identificação de encaminhadores. Para ver o RFC 2461, consulte o RFC Editor (<http://www.rfc-editor.org/rfcsearch.html>)



Configuração automática de endereços sem estado

A configuração automática de endereços sem estado é o processo que os nós de IPv6 (sistemas centrais ou encaminhadores) utilizam para configurar automaticamente endereços de IPv6 para interfaces. O nó constrói vários endereços de IPv6 combinando um prefixo de endereço com o endereço MAC do nó ou com um identificador de interface especificado pelo utilizador. Os prefixos incluem o prefixo do local de ligação (fe80::/10) e os prefixos de comprimento 64 anunciados por encaminhadores de IPv6 locais (se existir algum). A configuração automática de endereços sem estado também cria interfaces de multidifusão apropriadas quando o tipo de ligação suporta multidifusão.

O nó executa a detecção de endereços duplicados para verificar a exclusividade do endereço antes de atribuir a uma interface. O nó envia uma consulta de solicitação de vizinho para o novo endereço e fica a aguardar uma resposta. Se o nó não receber uma resposta, presume-se que o endereço é exclusivo. Se o nó receber uma resposta sob forma de um anúncio de vizinho, significa que o endereço já está a ser utilizado. Se um nó determinar que um endereço de IPv6 não é exclusivo, a configuração automática pára e é necessária a configuração manual da interface.

Comparar IPv4 e IPv6

A IBM está a implementar o IPv6 para o servidor iSeries em várias edições de software. O IPv6 está actualmente implementado numa plataforma de desenvolvimento de aplicações com a finalidade de desenvolver e testar aplicações do IPv6.

O utilizador poderá interrogar-se em que medida o IPv6 difere do IPv4. Esta tabela permite consultar rapidamente atributos conhecidos inerentes ao IPv4 e compará-los com atributos semelhantes do IPv6. Seleccione um atributo nesta lista para associar à comparação na tabela.

- “endereço” na página 20
- “atribuição de endereços” na página 20
- “duração do endereço” na página 21
- “máscara do endereço” na página 21
- “prefixo do endereço” na página 21
- “Address Resolution Protocol (ARP)” na página 21
- “âmbito do endereço” na página 21
- “tipos de endereço” na página 21
- “rastreamento de comunicações” na página 21
- “configuração” na página 21
- “Domain Name System (DNS)” na página 21
- “Dynamic Host Configuration Protocol (DHCP)” na página 21
- “File Transfer Protocol (FTP)” na página 22
- “fragmentos” na página 22
- “tabela de sistemas centrais” na página 22
- “interface” na página 22
- “Internet Control Message Protocol (ICMP)” na página 22
- “Internet Group Management Protocol (IGMP)” na página 22
- “cabeçalho de IP” na página 22
- “opções do cabeçalho de IP” na página 22
- “byte do protocolo de cabeçalho de IP” na página 22
- “byte do Tipo de Serviço (TOS) do cabeçalho de IP” na página 22
- “suporte do iSeries Navigator” na página 22
- “ligação de rede local (LAN)” na página 22
- “Layer 2 Tunnel Protocol (L2TP)” na página 22
- “endereço de reinício cíclico” na página 23
- “Unidade Máxima de Transmissão (MTU)” na página 23
- “netstat” na página 23
- “Network Address Translation (NAT)” na página 23
- “tabela de rede” na página 23
- “consulta de informações do nó” na página 23

- “filtragem de pacotes” na página 23
- “reencaminhamento de pacotes” na página 23
- “direcionamento de pacotes” na página 23
- “PING” na página 23
- “Point-to-Point Protocol (PPP)” na página 23
- “restrições de porta” na página 23
- “portas” na página 23
- “endereços privados e públicos” na página 24
- “tabela de protocolos” na página 24
- “Quality of Service (QOS)” na página 24
- “renumeração” na página 24
- “encaminhamento” na página 24
- “Routing Information Protocol (RIP)” na página 24
- “tabela de serviços” na página 24
- “Simple Network Management Protocol (SNMP)” na página 24
- “API de sockets” na página 25
- “selecção do endereço de origem” na página 25
- “iniciar e parar” na página 25
- “Telnet” na página 25
- “trace route” na página 25
- “níveis de transporte” na página 25
- “endereço não especificado” na página 25
- “virtual private networking (VPN)” na página 25

	IPv4	IPv6
endereço	<p>32 bits de comprimento (4 bytes). O endereço é composto por uma rede e uma parte do sistema central, que depende da classe de endereço. Estão definidas várias classes de endereços: A, B, C, D ou E, consoante os primeiros bits iniciais. O número total de endereços de IPv4 é 4 294 967 296.</p> <p>O formato de texto do endereço de IPv4 é nnn.nnn.nnn.nnn, em que $0 \leq n \leq 255$ e cada n é um dígito decimal. Os zeros à esquerda podem ser omitidos. O número máximo de caracteres de impressão é 15, não contando uma máscara.</p>	<p>128 bits de comprimento (16 bytes). A arquitectura base é de 64 bits para o número da rede e 64 bits para o número do sistema central. Regra geral, a parte relativa ao sistema central de um endereço de IPv6 (ou parte dele) é um endereço de MAC ou outro identificador de interface.</p> <p>Consoante o prefixo da sub-rede, o IPv6 terá uma arquitectura mais complicada do que o IPv4.</p> <p>O número de endereços de IPv6 é 10^{28} (79 228 162 514 264 337 593 543 950 336) vezes superior ao número de endereços de IPv4. O formato do texto do endereço IPv6 é</p> <p>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, em que cada x é um dígito hexadecimal que representa 4 bits. Os zeros à esquerda podem ser omitidos. Os dois pontos duplos (::) podem ser utilizados se estiverem no formato de texto de um endereço, para designar qualquer número de 0 bits. Por exemplo, ::ffff:10.120.78.40 é um endereço de IPv6 correlacionado com IPv4. (Consulte o RFC 2373 para obter detalhes. Para ver este RFC, consulte o RFC Editor (http://www.rfc-editor.org/rfcsearch.html).</p>
atribuição de endereços	<p>Originalmente, os endereços eram atribuídos por classe de rede. À medida que o espaço de endereços se vai esgotando, são criadas atribuições menores utilizando Classless Inter-Domain Routing (CIDR). A atribuição não foi equilibrada entre instituições e nações.</p>	<p>A atribuição ainda está numa primeira fase. A Internet Engineering Task Force (IETF) e a Internet Architecture Board (IAB) recomendam que seja atribuído, essencialmente, a todas as empresas, lares ou entidades um comprimento de prefixo de sub-rede de /48. Este valor deixaria 16 bits para a empresa proceder à criação de sub-redes. O espaço de endereço é suficientemente grande para conceder a cada utilizador no mundo inteiro o comprimento de prefixo de sub-rede de /48 que lhe compete.</p>

	IPv4	IPv6
duração do endereço	<p>Geralmente, não se trata de um conceito aplicável, excepto para os endereços atribuídos com a utilização de DHCP.</p>	<p>Os endereços de IPv6 têm duas durações: preferencial e válida, sendo a duração preferencial sempre <= válida.</p> <p>Após expirar a duração preferencial, o endereço não deverá ser utilizado como endereço de IP origem. Após expirar a duração válida, o endereço não é utilizado (reconhecido) como endereço de IP válido para pacotes que entram em rede.</p> <p>Alguns endereços de IPv6 têm, por definição, durações preferenciais e válidas infinitas; por exemplo, os do tipo local de ligação (consulte “âmbito do endereço”).</p>
máscara do endereço	Utilizada para designar a rede a partir da parte do sistema central.	Não utilizado (consulte “prefixo do endereço”).
prefixo do endereço	Por vezes, utilizado para designar a rede a partir da parte do sistema central. Por vezes, escrito como o sufixo /nn no formato de apresentação de endereço.	Utilizado para designar o prefixo de sub-rede de um endereço. Escrito como um sufixo /nnn (até 3 dígitos decimal, 0 <= nnn <= 128) após o formato de impressão. Um exemplo é fe80::982:2a5c/10, em que os primeiros 10 bits compreendem o prefixo de sub-rede.
Address Resolution Protocol (ARP)	O Address Resolution Protocol é utilizado pelo IPv4 para procurar um endereço físico, como o MAC ou o endereço de ligação, associado a um endereço de IPv4.	O IPv6 incorpora estas funções no próprio IP como parte dos algoritmos para configuração automática sem estado e a identificação de vizinhos com Internet Control Message Protocol versão 6 (ICMPv6). Assim, <u>não</u> existe nada semelhante a ARP6.
âmbito do endereço	Para endereços de unidifusão, o conceito não se aplica. Existem intervalos de endereços privados designados e reinício cíclico. Fora isso, presume-se que os endereços são globais.	<p>No IPv6, o âmbito de endereços faz parte da arquitectura. Os endereços de unidifusão têm 3 âmbitos definidos, incluindo os do local da ligação, os do local da instalação e os globais; os endereços de multidifusão têm 14 âmbitos. A selecção de endereços predefinida quer para a origem, quer para o destino, tem o âmbito em consideração.</p> <p>Uma zona de âmbito é uma instância de um âmbito numa rede em particular. Por conseguinte, os endereços de IPv6 por vezes têm de ser introduzidos ou associados a um ID de zona. A sintaxe é %zid, em que zid é um número (normalmente baixo) ou um nome. O ID da zona é escrito após o endereço e antes do prefixo. Por exemplo, 2ba::1:2:14e:9a9b:c%3/48.</p>
tipos de endereço	Unidifusão, multidifusão e difusão.	Unidifusão, multidifusão e difusão geral. Consulte Tipos de endereços de IPv6 para ver descrições.
rastreo de comunicações	Uma ferramenta para recolher um rastreo detalhado de pacotes de TCP/IP (e outros) que entram e saem de um servidor iSeries.	O mesmo acontece para IPv6, e este é suportado, incluindo pacotes de ICMPv6 e IPv6 com túneis definidos em IPv4.
configuração	A configuração tem de ser executada num sistema recém-instalado antes de poder comunicar; ou seja, têm de ser atribuídos endereços e encaminhamentos de IP.	A configuração é opcional, consoante as funções necessárias. Uma interface de Ethernet ou túnel apropriada tem de ser designada como interface de IPv6, no iSeries Navigator. Assim que esta operação for executada, as interfaces de IPv6 são de configuração automática. Assim, o sistema poderá comunicar com outros sistemas de IPv6 que sejam locais e remotos, dependendo do tipo de rede e do facto de existir ou não um encaminhador de IPv6.
Domain Name System (DNS)	<p>As aplicações aceitam nomes de sistemas centrais e, em seguida, utilizam o DNS para obter um endereço de IP, utilizando a API de socket gethostbyname().</p> <p>As aplicações também aceitam endereços de IP e, em seguida, utilizam o DNS para obter nomes de sistemas centrais com gethostbyaddr().</p> <p>Em IPv4, o domínio para procuras invertidas é in-addr.arpa.</p>	<p>O mesmo acontece em IPv6. O suporte para o IPv6 existe através da utilização do tipo de registo AAAA (A quádruplo) e da procura invertida (IP-para-nome). Uma aplicação pode optar por aceitar endereços de IPv6 a partir do DNS (ou não) e, em seguida, utilizar o IPv6 para comunicar (ou não).</p> <p>A API de socket gethostbyname() permanece inalterada em IPv6 e a API getaddrinfo() pode ser utilizada para obter (mediante escolha da aplicação) apenas endereços de IPv6 ou IPv4 e IPv6.</p> <p>Em IPv6, o domínio utilizado para pequenas procuras invertidas é ip6.arpa e, se não for encontrado, é ip6.int (consulte a API getnameinfo()).</p>
Dynamic Host Configuration Protocol (DHCP)	Utilizado para obter dinamicamente um endereço de IP e outras informações de configuração.	Presentemente, o DHCP não suporta IPv6.

	IPv4	IPv6
File Transfer Protocol (FTP)	O File Transfer Protocol permite enviar e receber ficheiros em redes.	Presentemente, o FTP não suporta IPv6.
fragmentos	Quando um pacote é grande demais para a ligação seguinte pela qual irá passar, poderá ser fragmentado pelo emissor (sistema central ou encaminhador).	No caso do IPv6, a fragmentação só pode ocorrer no nó origem, e a reassemblagem só é efectuada no nó destino. Actualmente, o cabeçalho de extensão de fragmentação não é suportado.
tabela de sistemas centrais	No iSeries Navigator, é uma tabela configurável que associa um endereço de Internet a um nome de sistema central; por exemplo, 127.0.0.1, reinício cíclico. Esta tabela é utilizada pela resolução de nomes de sockets, antes de uma procura de DNS ou após uma procura de DNS falhar (determinado pela prioridade da procura de nomes de sistemas centrais).	Presentemente, esta tabela não suporta o IPv6. Os clientes terão de configurar um registo AAAA num DNS para a resolução de domínios de IPv6. Pode executar o DNS localmente no mesmo sistema que a resolução ou pode executá-lo num sistema diferente.
interface	A entidade conceptual ou lógica utilizada pelo TCP/IP para enviar e receber pacotes e sempre fortemente associada a um endereço de IPv4, se não designada com um endereço de IPv4. Por vezes, referida como interface lógica. Pode ser iniciada e parada independentemente uma da outra e independentemente do TCP/IP utilizando os comandos STRTCPIFC e ENDTCPIFC e utilizando o iSeries Navigator.	O mesmo conceito que IPv4. Pode ser iniciada e parada independentemente uma da outra e independentemente do TCP/IP utilizando apenas o iSeries Navigator.
Internet Control Message Protocol (ICMP)	O ICMP é utilizado pelo IPv4 para comunicar informações da rede.	Utilizado de forma semelhante para o IPv6; no entanto, o Internet Control Message Protocol versão 6 (ICMPv6) fornece alguns novos atributos. Os tipos de erros básicos permanecem como, por exemplo, destino não alcançável e pedido e resposta de eco. São adicionados novos tipos e códigos para suportar a identificação de vizinhos e funções relacionadas.
Internet Group Management Protocol (IGMP)	O IGMP é utilizado por encaminhadores de IPv4 para procurar sistemas centrais que pretendem tráfego para um grupo de multidifusão em particular, e também utilizado por sistemas centrais de IPv4 para informar os encaminhadores de IPv4 de receptores de grupos de multidifusão existentes (no sistema central).	Substituído pelo protocolo MLD (identificação de receptores de multidifusão) para o IPv6. Executa essencialmente as mesmas funções que o IGMP para o IPv4, mas utiliza o ICMPv6 adicionando alguns valores de tipo ICMPv6 específicos de MLD.
cabeçalho de IP	Comprimento variável de 20-60 bytes, dependendo das opções de IP presentes.	Comprimento fixo de 40 bytes. Não existem opções de cabeçalho de IP. Geralmente, o cabeçalho de IPv6 é mais simples do que o cabeçalho de IPv4.
opções de cabeçalho de IP	Várias opções que podem acompanhar um cabeçalho de IP (antes de qualquer cabeçalho de transporte).	O cabeçalho de IPv6 não tem opções. Como alternativa, o IPv6 adiciona outros cabeçalhos de extensão (opcionais). Os cabeçalhos de extensão são AH e ESP (inalterados do IPv4), sistema de passagem por sistema de passagem, encaminhamento, fragmento e destino. Presentemente, o IPv6 não suporta cabeçalhos de extensão.
byte do protocolo de cabeçalhos de IP	O código de protocolo do nível de transporte ou débito de pacotes; por exemplo, ICMP.	O tipo de cabeçalho imediatamente a seguir ao cabeçalho de IPv6. utiliza o mesmo valor que o campo de protocolo de IPv4. Mas o efeito arquitectural consiste em permitir um intervalo presentemente definido de cabeçalhos seguintes e é facilmente expandido. O cabeçalho seguinte será um cabeçalho de transporte, um cabeçalho de extensão ou o ICMPv6.
byte do Tipo de Serviço (TOS) do cabeçalho de IP	Utilizado por QoS e serviços diferenciados para designar uma classe de tráfego.	Designa a classe de tráfego de IPv6, de forma semelhante ao IPv4. Utiliza códigos diferentes. Presentemente, o IPv6 não suporta o TOS.
suporte do iSeries Navigator	O iSeries Navigator fornece uma função de configuração completa para TCP/IP.	A configuração opcional do IPv6 é fornecida em pleno pelo iSeries Navigator, incluindo o assistente de Configuração de IPv6 .
ligação de rede local (LAN)	Utilizada por uma interface de IP para chegar à rede física. Existem muitos tipos; por exemplo, token ring, Ethernet e PPP. Por vezes, referida como interface física, ligação ou linha.	O IPv6 tem o mesmo conceito. Presentemente só são suportadas as placas de Ethernet 2838 e 2849 e linhas de túnel.
Layer 2 Tunnel Protocol (L2TP)	O L2TP pode ser considerado como um PPP virtual e funciona em qualquer tipo de linha suportado.	Presentemente, o L2TP não suporta o IPv6.

	IPv4	IPv6
endereço de reinício cíclico	Uma interface com o endereço 127.*.*.* (normalmente, 127.0.0.1) que só pode ser utilizada por um nó para enviar pacotes para si própria. A interface física (descrição de linha) chama-se *LOOPBACK.	O conceito é o mesmo que no IPv4, e o endereço de reinício cíclico exclusivo é 0000:0000:0000:0000:0000:0000:0000:0001 ou ::1 (versão abreviada). A interface física virtual chama-se*LOOPBACK6.
Unidade Máxima de Transmissão (MTU)	A unidade máxima de transmissão de uma ligação é o número máximo de bytes suportado por um tipo de linha em particular, tal como Ethernet ou modem. Para o IPv4, 576 é o mínimo normal.	O IPv6 tem um limite inferior arquitectado na MTU de 1280 bytes. Ou seja, o IPv6 não fragmentará pacotes abaixo deste limite. Para enviar o IPv6 numa ligação com menos de 1280 MTU, o nível de ligação tem de fragmentar e desfragmentar de forma transparente os pacotes de IPv6.
netstat	Uma ferramenta para observar o estado de ligações, interfaces ou encaminhamentos de TCP/IP. Disponível com a utilização do iSeries Navigator e 5250.	O mesmo acontece para IPv6, e o IPv6 é suportado para o 5250 e iSeries.
Conversão de Endereços de Rede (NAT)	Funções básicas de firewall integradas no TCP/IP, configuradas com a utilização do iSeries Navigator.	Presentemente, o NAT não suporta o IPv6. De uma forma mais geral, o IPv6 não requer o NAT. O espaço de endereço expandido do IPv6 elimina o problema da falta de espaço de endereços e facilita a renumeração.
tabela de rede	No iSeries Navigator, é uma tabela configurável que associa um nome de rede a um endereço de IP sem ser necessária uma máscara. Por exemplo, a Rede14 do sistema central e o endereço de IP 1.2.3.4.	Presentemente não são efectuadas alterações a esta tabela para o IPv6.
consulta de informações do nó	Não existe.	Uma ferramenta de rede simples e conveniente que deveria funcionar como o ping, excepto com conteúdo: um nó de IPv6 pode consultar outro nó de IPv6 quanto ao nome de DNS do destino, endereço de unidifusão de IPv6 ou endereço de IPv4. Presentemente, não é suportado.
filtragem de pacotes	Funções básicas de firewall integradas em TCP/IP, configuradas utilizando o iSeries Navigator.	Presentemente, a filtragem de pacotes não suporta IPv6. No entanto, a filtragem de IPv4 pode ser aplicada ao tráfego de IPv6 direccionado por túnel.
reencaminhamento de pacotes	O servidor iSeries pode ser configurado para reencaminhar pacotes de IP que recebe para endereços de IP não locais. Normalmente, a interface de entrada e a interface de saída estão ligadas a redes locais (LANs) diferentes.	Presentemente os pacotes de IPv6 não são reencaminhados.
direccionamento de pacotes	No IPv4, o direccionamento ocorre na VPN para ligações de VPN de modo de túnel (IPv4 direccionado no IPv4) e no LZTP.	Para o IPv6, o espera-se que o direccionamento em pacotes de IPv4 seja uma das partes principais da respectiva evolução. Actualmente, estão definidos por IETF, pelo menos, 5 tipos diferentes de direccionamentos de 6-em-4, cada um com atributos e vantagens diferentes. É suportado um tipo de direccionamento de IPv6 em IPv4 básico e flexível para permitir que os nós de IPv6 comuniquem através da Internet IPv4 existente. Chamado direccionamento configurado , ele fornece uma ligação ponto a ponto virtual entre dois nós de IPv6 e utiliza um novo tipo de linha de túnel chamado *TNLCFG64.
PING	Ferramenta base de TCP/IP para testar a capacidade de alcance. Disponível através da utilização do iSeries Navigator e 5250.	O mesmo acontece para IPv6, e o IPv6 é suportado para o 5250 e iSeries Navigator.
Point-to-Point Protocol (PPP)	O PPP suporta interfaces de marcação através de vários tipos de modems e linhas.	Presentemente, o PPP não suporta o IPv6.
restrições de porta	Estes painéis do iSeries permitem que um cliente configure um número de porta seleccionado ou intervalos de números de porta para TCP ou UDP para que fiquem disponíveis apenas para um perfil específico.	Não suportado para o IPv6. As restrições configuradas só se aplicam ao IPv4.
portas	O TCP e o UDP têm espaços de porta separados, cada qual identificado por números de porta compreendidos entre 1-65535.	Para o IPv6, as portas funcionam do mesmo modo que para o IPv4. Uma vez que estes se encontram numa nova família de endereços, existem agora quatro espaços de porta separados. Por exemplo, existem dois espaços de porta 80 de TCP ao qual uma aplicação pode ser ligada, um em AF_INET e o outro em AF_INET6.

	IPv4	IPv6
endereços privados e públicos	<p>Todos os endereços de IPv4 são públicos, excepto os três intervalos de endereços que foram designados como privados pelo RFC 1918 de IETF: 10.*.* (10/8), 172.16.0.0 a 172.31.255.255 (172.16/12) e 192.168.*.* (192.168/16). Os domínios de endereços privados são frequentemente utilizados nas empresas. Os endereços privados não podem ser encaminhados na Internet.</p>	<p>O IPv6 tem um conceito análogo, mas com diferenças importantes.</p> <p>Os endereços são públicos ou temporários, sendo anteriormente intitulados anónimos. Consulte o RFC 3041. Ao contrário dos endereços privados de IPv4, os endereços temporários podem ser globalmente encaminhados. A motivação também é diferente; os endereços temporários de IPv6 destinam-se a proteger a identidade de um cliente quando inicia a comunicação (uma questão de privacidade). Os endereços temporários têm uma duração limitada e não contêm um identificador de interface que seja um endereço de ligação (MAC). Em geral, não é possível distingui-los dos endereços públicos.</p> <p>O IPv6 tem a noção do âmbito de endereço limitado utilizando as respectivas designações de âmbito arquitectadas (consulte a secção “âmbito do endereço” na página 21).</p>
tabela de protocolos	<p>No iSeries Navigator, é uma tabela configurável que associa o nome de um protocolo ao respectivo número de protocolo atribuído; por exemplo, UDP, 17. O sistema é fornecido com um pequeno número de entradas: IP, TCP, UDP, ICMP.</p>	<p>A tabela suporta IPv6 sem alteração.</p>
Quality of service (QoS)	<p>Quality of service (Qualidade de serviço) permite-lhe pedir a prioridade de pacotes e largura de banda para aplicações de TCP/IP.</p>	<p>Presentemente, o QoS não suporta o IPv6. No entanto, quando o IPv6 é direccionado no IPv4, os serviços de QoS do iSeries podem ser aplicados ao tráfego de IPv4, que irá tratar, em seguida, de forma transparente, os débitos de IPv6.</p>
renumeração	<p>Executada pela reconfiguração manual, com a possível excepção de DHCP. Geralmente, para uma instalação ou organização, é um processo difícil e problemático a evitar sempre que possível.</p>	<p>É um elemento arquitectural importante do IPv6 e supõe-se que seja amplamente automático, especialmente com o prefixo /48.</p>
encaminhamento	<p>Em termos lógicos, é uma definição de um conjunto de endereços de IP (pode conter apenas 1) para uma interface física e um único endereço de IP de sistema de passagem seguinte. Os pacotes de IP cujo endereço destino esteja definido como parte do conjunto são reencaminhados para o sistema de passagem seguinte utilizando a linha. Os encaminhamentos de IPv4 estão associados a uma interface de IPv4 e, conseqüentemente, a um endereço de IPv4.</p> <p>O encaminhamento predefinido é *DFROUTE.</p>	<p>Conceptualmente, é o mesmo que para o IPv4. Uma diferença importante: os encaminhamentos de IPv6 estão associados (ligados) a uma interface física (uma ligação, tal como *TNLCFG64 ou ETH03), em vez de a uma interface. Existem várias razões para esta situação. Uma delas é o facto de a selecção de endereços origem funcionar de forma diferente para o IPv6 relativamente ao IPv4. Consulte a secção “selecção do endereço de origem” na página 25.</p> <p>Os encaminhamentos duplicados podem aumentar a robustez, mas são ignorados durante a procura de encaminhamentos.</p>
Routing Information Protocol (RIP)	<p>O RIP é um protocolo de encaminhamento suportado pelo daemon encaminhado.</p>	<p>Presentemente, o RIP não suporta o IPv6. O encaminhamento de IPv6 utiliza encaminhamentos estáticos.</p>
tabela de serviços	<p>No servidor iSeries, é uma tabela configurável que associa um nome de serviço a uma porta e protocolo; por exemplo, nome de serviço controlo de FTP, porta 21, TCP e UDP.</p> <p>A tabela de serviços contém um grande número de serviços conhecidos. Muitas aplicações utilizam esta tabela para determinar qual a porta a utilizar.</p>	<p>Não são efectuadas alterações a esta tabela para o IPv6.</p>
Simple Network Management Protocol (SNMP)	<p>O SNMP é um protocolo para gestão de sistemas.</p>	<p>Presentemente, o SNMP não suporta o IPv6. O encaminhamento de IPv6 utiliza encaminhamentos estáticos.</p>

	IPv4	IPv6
API de sockets	Estas APIs são a forma como as aplicações utilizam o TCP/IP. As aplicações que não necessitam do IPv6 não são afectadas pelas alterações aos sockets para suportar o IPv6.	<p>O IPv6 melhora os sockets de modo a que as aplicações possam utilizar agora o IPv6, através da utilização de uma nova família de endereços: AF_INET6.</p> <p>Os melhoramentos foram concebidos de modo a que as aplicações de IPv4 não sejam de todo afectadas pelas alterações ao IPv6 e às APIs. As aplicações que pretendam suportar o tráfego simultâneo de IPv4 e IPv6, ou o tráfego apenas de IPv6, são facilmente correlacionados com a utilização de endereços de IPv6 definidos com IPv4 no formato <code>::ffff:a.b.c.d</code>, em que <code>a.b.c.d</code> é o endereço de IPv4 do cliente.</p> <p>As novas APIs também incluem suporte para a conversão de endereços de IPv6 de texto para binário e de binário para texto.</p> <p>Consulte a secção Utilizar a família de endereços AF_INET6 para obter mais informações sobre os melhoramentos aos sockets no IPv6.</p>
selecção de endereços origem	Uma aplicação pode designar um IP origem (normalmente, utilizando <code>sockets bind()</code>). Se for ligado a INADDR_ANY, um IP origem é escolhido com base no encaminhamento.	Tal como com o IPv4, uma aplicação pode designar um endereço de IPv6 origem utilizando <code>bind()</code> . De modo semelhante ao IPv4, pode deixar o sistema escolher um endereço origem de IPv6 utilizando <code>in6addr_any</code> . Mas, uma vez que as linhas de IPv6 têm muitos endereços de IPv6, o método interno de escolha de um IP origem é diferente.
iniciar e parar	Utilize STRTCP e ENDTCP para iniciar ou parar o TCP/IP.	<p>O mesmo que para o IPv4. O IPv4 e IPv6 não são iniciados ou parados independentemente um do outro ou independentemente do TCP/IP. Ou seja, todo o TCP/IP é iniciado e parado, não apenas o IPv4 ou IPv6.</p> <p>Quaisquer interfaces de IPv6 são automaticamente iniciadas se o parâmetro AUTOSTART = *YES (predefinição). O IPv6 não pode ser utilizado ou configurado sem o IPv4 e o IPv6 tem de ter o reinício cíclico de IPv6 configurado (<code>:::1</code>).</p>
Telnet	O Telnet permite-lhe iniciar sessão e utilizar um computador remoto tal como se estivesse ligado a ele directamente.	Presentemente, o Telnet não suporta o IPv6.
trace route	Ferramenta base de TCP/IP para executar a determinação de caminho. Disponível através da utilização do iSeries Navigator e 5250.	O mesmo acontece para IPv6, e o IPv6 é suportado para o 5250 e iSeries.
níveis de transporte	TCP, UDP, RAW. Um novo transporte, Stream Control Transmission Protocol (SCTP), tem por objectivo fornecer as melhores funções do TCP e UDP, ou seja, uma comunicação sem ligações garantida. O SCTP está na primeira fase de utilização e não é suportado no iSeries.	Para o IPv6, existem os mesmos três transportes que não foram alterados em termos de funções.
endereço não especificado	Aparentemente não definido, como o próprio nome indica. A programação de sockets utiliza <code>0.0.0.0</code> como INADDR_ANY.	Definido como <code>::/128</code> (128 0 bits). É utilizado como IP origem em certos pacotes de identificação de vizinhos e em vários outros contextos, tais como sockets. A programação de sockets utiliza <code>::/128</code> como <code>in6addr_any</code> .
rede privada virtual (VPN)	A rede privada virtual (utilizando IPsec) permite-lhe alargar uma rede segura e privada a uma rede pública existente.	Presentemente, a VPN não suporta o IPv6. No entanto, quando o IPv6 é direccionado no IPv4, os serviços de VPN do iSeries existentes podem ser aplicados ao tráfego de IPv4, que, em seguida, irá tratar, de modo transparente, os débitos de IPv6.


Resolução de problemas do IPv6


Se tiver o IPv6 configurado no servidor, poderá utilizar várias das mesmas ferramentas de resolução de problemas que para o IPv4. Por exemplo, ferramentas como o encaminhamento de rastreios e o PING aceitam ambos os formatos de endereço de IPv4 e IPv6, de modo que pode utilizá-las para testar as ligações e os encaminhamentos para ambos os tipos de redes. Para além disso, pode utilizar a função rastreio de comunicações para rastrear os dados em ambas as linhas de comunicações de IPv4 e IPv6.

Consulte a secção Resolução de problemas de TCP/IP para obter instruções gerais de resolução de problemas que fornecem técnicas para resolver problemas relacionados com o IPv4 e IPv6.

Informações relacionadas com o IPv6

Para obter mais informações sobre o IPv6, consulte estas fontes de informação:

Internet Engineering Task Force (IETF) (<http://www.ietf.cnri.reston.va.us/>) 
Conheça o grupo de indivíduos que desenvolveu o protocolo Internet, incluindo o IPv6.

IP Versão 6 (IPv6) (<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 
Saiba onde encontrar especificações actuais do IPv6 e referências a várias fontes sobre o IPv6.

IPv6 Forum (<http://www.ipv6forum.com/>) 
Saiba onde encontrar artigos e acontecimentos noticiosos que abordam os desenvolvimentos mais recentes do IPv6.

Capítulo 4. Planear a configuração de TCP/IP

Antes de começar a instalar e a configurar o servidor iSeries, planeie cuidadosamente toda a operação. Consulte os tópicos a seguir para obter directrizes de planeamento. Estas directrizes de planeamento destinam-se a uma configuração de TCP/IP base com o IPv4. Se tenciona configurar o IPv6, consulte Configurar IPv6 para ver os requisitos de instalação e as instruções de configuração.

Requisitos de configuração de TCP/IP


Recolha e registe informações básicas necessárias à configuração do TCP/IP.

Considerações de segurança de TCP/IP

Considere as suas necessidades de segurança enquanto novo membro de uma rede.

Requisitos de configuração de TCP/IP

Imprima esta página e registe as informações de configuração sobre o servidor e a rede de TCP/IP com a qual está a estabelecer ligação. Necessitará de consultar esta informação mais tarde quando configurar o TCP/IP. Utilize as instruções a seguir à tabela para obter ajuda para determinar o valor das duas primeiras linhas. Se não estiver familiarizado com algum destes termos, consulte o redbook IBM TCP/IP

for AS/400: More Cool Things Than Ever , capítulo segundo, "TCP/IP: Basic Installation and Configuration."

Informação necessária	Para o sistema	Exemplo
O tipo de adaptador de comunicações instalado no sistema (consulte as instruções abaixo)		Ethernet
Nome do recurso		CMN01
Endereço de IP para o seu servidor iSeries		199.5.83.158
Máscara de sub-rede para o seu servidor iSeries		255.255.255.0
Endereço da porta de ligação		199.5.83.129
Nome de sistema central e nome de domínio para o sistema		sys400.xyz.empresa.com
Endereço de IP para o servidor de nomes de domínio		199.4.191.76

Para encontrar a informação do adaptador de comunicações, siga estes passos:

1. Na linha de comandos do servidor, escreva `go hardware` e prima **Enter**.
2. Para seleccionar Trabalhar com recursos de comunicação (Opção 1), escreva 1 e prima **Enter**.

Os recursos de comunicação serão listados por nome de recurso. Siga as instruções do ecrã se deseja trabalhar com os recursos ou visualizar mais detalhes.

Que fazer de seguida:

Instalar o TCP/IP

Considerações de segurança sobre o TCP/IP

Quando está a planear a sua configuração de TCP/IP, deve ter em consideração as suas necessidades de segurança. Esta estratégia pode ajudar a limitar a sua exposição com o TCP/IP:

- **Inicie apenas as aplicações TCP/IP de que necessita.**

Cada aplicação TCP/IP possui as suas próprias exposições de segurança. Não dependem de um encaminhamento para rejeitar pedidos para uma aplicação em particular. Como defesa secundária, defina os valores de arranque automático das aplicações que não forem necessárias como N0.

- **Limite as horas durante as quais as aplicações TCP/IP são executadas.**

Limite a sua exposição reduzindo as horas de funcionamento dos servidores. Se possível, desligue os servidores de TCP/IP tais como o FTP e o Telnet fora das horas de expediente.

- **Controle quem pode iniciar e alterar as aplicações de TCP/IP.**

Por predefinição, a autoridade *IOSYSCFG é necessária para alterar as definições de configuração de TCP/IP. Um utilizador sem a autoridade *IOSYSCFG necessita da autoridade *ALLOBJ ou autoridade explícita para os comandos de início de TCP/IP. Dar autoridades especiais a utilizadores representa uma exposição de segurança. Avalie a necessidade para quaisquer autoridades especiais para cada utilizador e mantenha as autoridades especiais ao mínimo essencial. Mantenha um controlo sobre quais utilizadores possuem autoridades especiais e reveja periodicamente os seus requisitos para a autoridade. Isto também limita a possibilidade de acesso ao servidor fora das horas de expediente.

- **Controle o encaminhamento de TCP/IP:**

- Desactive o reencaminhamento de IP de modo a que os piratas informáticos não possam utilizar o seu servidor da Web para atacar outros sistemas fidedignos.
- Defina apenas um encaminhamento no servidor público da Web: o encaminhamento predefinido para o seu Fornecedor de Serviços Internet.
- Não configure nomes de sistemas centrais e endereços de IP de sistemas seguros internos no seu servidor na tabela de sistemas centrais do servidor de TCP/IP da Web. Coloque apenas o nome de outros servidores públicos de que necessita para chegar a esta tabela.

- **Controle os servidores de TCP/IP concebidos para início de sessão interactiva remota.**

Aplicações como FTP e Telnet são mais vulneráveis a ataques vindos do exterior. Para mais detalhes sobre controlo de vulnerabilidade, leia o capítulo sobre sugestões de controlo de início de sessão

interactivo no manual *Tips and Tools for Securing Your iSeries*  .

Para mais informações sobre segurança e opções disponíveis, consulte *iSeries and Internet security*.

Capítulo 5. Instalar TCP/IP

O suporte base de TCP/IP acompanha o OS/400 e permite ligar um servidor iSeries a uma rede. No entanto, se pretender utilizar aplicações de TCP/IP, como por exemplo, Telnet, FTP e SMTP, também terá de instalar o TCP/IP Connectivity Utilities. Este é um produto licenciado instalável em separado, que está incluído no sistema operativo.

Para instalar TCP/IP Connectivity Utilities no servidor iSeries, siga estes passos:

1. Introduza o suporte de instalação do TCP/IP no servidor. Se o suporte de instalação for um CD-ROM, introduza-o no dispositivo óptico. Se o suporte de instalação for uma banda, introduza-o na unidade de bandas.
2. Na linha de comandos, escreva `GO LICPGM` e prima **Enter** para aceder ao ecrã *Trabalhar com Programas Licenciados*.
3. Seleccione a opção **11** (Instalar programas licenciados) no ecrã *Trabalhar com Programas Licenciados* para ver os programas licenciados e partes opcionais de programas licenciados.
4. Escreva **1** (Instalar) na coluna *Opção* junto a `57xxTC1` (TCP/IP Connectivity Utilities para iSeries). Prima **Enter**. O ecrã *Confirmar Programas Licenciados a Instalar* apresenta o programa licenciado que seleccionou para instalação. Prima **Enter** para confirmar.
5. Preencha as seguintes opções do ecrã *Opções de Instalação*:

Dispositivo de instalação	Escreva <code>Q0PT</code> , se estiver a instalar a partir de uma unidade de CD-ROM. Escreva <code>TAP01</code> , se estiver a instalar a partir de uma unidade de bandas.
Objectos a instalar	Esta opção permite-lhe instalar programas e objectos de idioma, apenas programas ou apenas objectos de idioma.
Reinício automático	Esta opção determina se o sistema será iniciado automaticamente quando o processo de instalação for concluído com êxito.

Quando o TCP/IP Connectivity Utilities for instalado com êxito, é apresentado o menu *Trabalhar com Programas Licenciados* ou o ecrã *Iniciar Sessão*.

6. Seleccione a opção **50** (*Apresentar registo de mensagens*) para verificar se instalou o programa licenciado com êxito.

Se ocorrer um erro, surgirá a mensagem *A função Trabalhar com Programa Licenciado não está completa na parte inferior do ecrã Trabalhar com Programas Licenciados*. Se ocorrer um problema, tente reinstalar o TCP/IP Connectivity Utilities. Se o problema não for resolvido, terá de contactar a assistência.

Nota:

Outros programas licenciados que pode pretender instalar incluem:

- *OiSeries Access for Windows 95/NT* (5769–XD1 V3R1M3 ou posterior) faculta suporte iSeries Navigator que se usa para configurar alguns dos componentes de TCP/IP.
- O *IBM HTTP Server for iSeries* (57xx–DG1) fornece suporte de servidor Web.
- Algumas aplicações de TCP/IP requerem a instalação adicional de programas licenciados. Para saber de que programas necessita, consulte as instruções de configuração da aplicação específica que pretende.

Capítulo 6. Configurar TCP/IP

Pode estar a configurar TCP/IP pela primeira vez ou a alterar uma configuração existente para utilizar a função IPv6. Este tópico fornece instruções para configurar TCP/IP em cada uma destas situações. Consulte as opções a seguir para obter instruções sobre a configuração de TCP/IP no servidor:

Configurar TCP/IP pela primeira vez

Utilize estas instruções se estiver a configurar um novo servidor. Irá estabelecer uma ligação e configurar TCP/IP pela primeira vez.

Configurar IPv6

Utilize estas instruções para configurar o servidor para a função IPv6. Irá beneficiar da capacidade de endereçamento melhorada e das funções robustas deste Internet Protocol. Se não estiver familiarizado com o IPv6, consulte o Internet Protocol versão 6 (IPv6) para ver uma descrição geral. Terá de ter TCP/IP configurado no servidor para poder configurar o IPv6.

Configurar TCP/IP quando o sistema operativo está em estado restrito

Use este método se necessitar de executar TCP/IP com o sistema operativo em estado restrito.

Configurar TCP/IP pela primeira vez

Selecione um dos seguintes métodos para configurar TCP/IP no seu novo servidor:

Configurar TCP/IP com o assistente EZ-Setup

Utilize este método preferencial se o PC estiver equipado para utilizar o assistente EZ-Setup. O assistente EZ-Setup é fornecido juntamente com o servidor iSeries.

Configurar TCP/IP com a interface baseada em caracteres

Recorra a este método se não conseguir utilizar o assistente EZ-Setup. Por exemplo, se quiser utilizar o iSeries Navigator num PC que necessite de configuração básica de TCP/IP antes de executar o iSeries Navigator, deverá utilizar este método.

Configurar TCP/IP com o assistente EZ-Setup

O iSeries Navigator é uma interface gráfica de utilizador que faculta caixas de diálogo e assistentes concisos para configurar TCP/IP. Para configuração inicial, use o assistente EZ-Setup do iSeries Navigator para estabelecer uma ligação e configurar TCP/IP pela primeira vez. Este é o método preferencial para trabalhar com o servidor, uma vez que a interface é fácil de utilizar. O CD-ROM que contém o assistente EZ-Setup é fornecido juntamente com o servidor iSeries.

Para configurar o servidor, siga estes passos:


1. Utilize o assistente EZ-Setup. Aceda ao assistente a partir do CD-ROM que acompanha o servidor. Siga as instruções do assistente para configurar TCP/IP.
2. Inicie o TCP/IP
 - a. No iSeries Navigator, expanda o **servidor** -> **Network**.
 - b. Faça clique com o botão direito do rato sobre **TCP/IP configuration** e seleccione **Start**. Todas as interfaces e servidores que foram definidos para início automático quando o TCP/IP é iniciado serão iniciados.

Terminou a configuração do TCP/IP no servidor. Utilize o iSeries Navigator para modificar a configuração consoante a evolução das necessidades de funcionamento em rede. Consulte a secção

Personalizar TCP/IP com o iSeries Navigator para adicionar encaminhamentos e interfaces ou Configurar IPv6 para utilizar o Internet Protocol versão 6 na sua rede.

Configurar TCP/IP com a interface baseada em caracteres

Se não conseguir utilizar o assistente EZ-Setup do iSeries Navigator, utilize a interface baseada em caracteres como alternativa. Por exemplo, se quiser utilizar o iSeries Navigator num PC que necessite de configuração básica de TCP/IP antes de executar o iSeries Navigator, deverá utilizar a interface baseada em caracteres para executar a configuração básica.

Para executar os passos de configuração explicados nesta secção, necessitará da autoridade especial *IOSYSCFG no seu perfil de utilizador. Para mais informações sobre este tipo de autoridade, consulte o capítulo sobre perfis de utilizador em iSeries Security Reference  .

Para configurar o TCP/IP com a interface baseada em caracteres, siga estes passos:

1. Na linha de comandos, escreva G0 TCPADM para ver o menu Administração de TCP/IP e prima Enter.
2. Especifique a opção 1 (Configurar TCP/IP) para ver o menu Configurar TCP/IP (CFGTCP) e prima Enter. Utilize este menu para seleccionar tarefas de configuração. Observe cuidadosamente o menu antes de começar a configurar o servidor.

Execute os passos que se seguem para configurar o TCP/IP no seu servidor.

1. Configurar uma descrição de linha
2. Activar reenvio de datagramas de IP
3. Configurar uma interface
4. Configurar um encaminhamento
5. Definir nomes de domínio local e de sistema central
6. Definir uma tabela de sistemas centrais
7. Iniciar TCP/IP

Configurar uma descrição de linha (Ethernet)

Estas instruções referem-se à configuração de TCP/IP num adaptador de comunicações de Ethernet. Contudo, se estiver a utilizar um tipo de adaptador diferente, como por exemplo, token-ring, consulte o TCP/IP Configuration and Reference, *Apêndice A*, para obter um comando inerente ao adaptador em questão.

Para configurar uma descrição de linha, siga estes passos:

1. Na linha de comandos escreva CRTLINETH para aceder ao menu Create Line Desc (Ethernet) (CRTLINETH) e prima Enter.
2. Especifique o nome da linha e prima Enter. (Utilize qualquer nome.)
3. Especifique o nome do recurso e prima Enter.

O que fazer em seguida:

Activar reenvio de datagramas de IP

Activar reenvio de datagramas de IP

Active o reenvio de datagramas de IP de modo a que os pacotes possam ser reenviados entre sub-redes diferentes.

Para activar reenvio de datagramas de IP, siga estes passos:

1. Na linha de comandos, introduza CHGTCPA e prima F4.
2. Ao pedido *IP datagram forwarding* responda com *YES.

O que fazer em seguida:

Configurar uma interface

Configurar uma interface

Para configurar uma interface, siga estes passos:

1. Na linha de comandos, escreva CFGTCP para aceder ao menu Configure TCP/IP e prima Enter.
2. Seleccione a opção 1 (Work with TCP/IP interfaces) no menu Configure TCP/IP e prima Enter.
3. Especifique a opção 1 (Add) para ver o ecrã Add TCP/IP Interface e prima Enter.
4. Especifique o valor de endereço que pretende para representar o servidor iSeries, o endereço de máscara de sub-rede e o nome da descrição de linha que definiu anteriormente e prima Enter.

Para iniciar a interface, especifique a opção 9 (Start) para a interface que configurou e prima Enter.

O que fazer em seguida:

Configurar um encaminhamento

Configurar um encaminhamento

Para alcançar redes remotas, é necessária, pelo menos uma entrada de encaminhamento. Se não tiver sido adicionada manualmente nenhuma entrada de encaminhamento, o servidor não poderá alcançar os sistemas que não se encontrem na mesma rede à qual está ligado. Também terá de adicionar entradas de encaminhamento para permitir que os clientes de TCP/IP que estejam a tentar chegar ao servidor a partir de uma rede remota funcionem correctamente.

Deverá ter a tabela de encaminhamento definida de modo a que exista sempre uma entrada para, pelo menos, um encaminhamento predefinido (*DFTRROUTE). Se não existir correspondência em nenhuma outra entrada da tabela de encaminhamento, os dados serão enviados para o encaminhador de IP especificado pela primeira entrada de encaminhamento predefinida disponível.

Para configurar um encaminhamento predefinido, siga estes passos:

1. Seleccione a opção 2 (Work with TCP/IP Routes) no menu Configure TCP/IP e prima Enter.
2. Especifique a opção 1 (Add) para ir para o ecrã Add TCP/IP Route (ADDTCPRTE) e prima Enter.
3. Especifique *DFTRROUTE para o destino de encaminhamento, especifique *NONE para a máscara de sub-rede, especifique o endereço de IP para o sistema de passagem seguinte e prima Enter.

O que fazer em seguida:

Definir nomes de domínio local e de sistema central

Definir nomes de domínio local e de sistema central

Para definir nomes de domínio local e de sistema central, siga estes passos:

1. Seleccione a opção 12 (Change TCP/IP domain) no menu Configure TCP/IP e prima Enter.
2. Especifique os nomes que seleccionou como o nome do sistema central local e o nome do domínio local, deixando os outros parâmetros nas respectivas predefinições e prima Enter.

O que fazer em seguida:

Definir uma tabela de sistemas centrais

Definir uma tabela de sistemas centrais

Para definir uma tabela de sistemas centrais, siga estes passos:

1. Seleccione a opção 10 (Work with TCP/IP Host Table Entries) no menu Configure TCP/IP e prima Enter.
2. Especifique a opção 1 (Add) para ir para o ecrã Add TCP/IP Host Table Entry e prima Enter.
3. Especifique o endereço de IP, o nome de sistema central local associado e o nome de sistema central totalmente qualificado e prima Enter.

4. Introduza um sinal de mais (+) para disponibilizar mais espaço para mais do que um nome de sistema central, se necessário.
5. Repita estes passos para cada um dos outros sistemas centrais da rede com os quais pretende comunicar por nome e adicione uma entrada para cada um.

O que fazer em seguida:

Iniciar TCP/IP

Iniciar TCP/IP

Os serviços de TCP/IP não ficam disponíveis enquanto não iniciar TCP/IP.

Para iniciar TCP/IP, escreva STRTCP na linha de comandos.

O comando Start TCP/IP (STRTCP) inicializa e activa o processamento de TCP/IP, inicia as interfaces de TCP/IP e inicia os trabalhos do servidor. Só as interfaces e os servidores de TCP/IP com AUTOSTART *YES são iniciados com o comando STRTCP.

Terminou a configuração do TCP/IP no servidor. Utilize o iSeries Navigator para modificar a configuração consoante a evolução das necessidades de funcionamento em rede. Consulte a secção Personalizar TCP/IP com o iSeries Navigator para adicionar encaminhamentos e interfaces ou Configurar IPv6 para utilizar o Internet Protocol versão 6 na sua rede.

Configurar IPv6

Está pronto para tirar partido da próxima geração da Internet utilizando o IPv6 na sua rede. Para utilizar a função IPv6, terá de alterar a configuração de TCP/IP configurando uma linha que esteja dedicada ao IPv6. Tem de configurar uma linha num adaptador de Ethernet 2838 ou 2849 ou numa linha de túnel configurada (linha virtual). Leia estes tópicos para obter instruções sobre a configuração de IPv6:

Requisitos de configuração

Este tópico lista os requisitos de hardware e software para configurar o servidor para usar IPv6.

Configurar o IPv6 com o assistente IPv6 Configuration

Consulte as instruções para utilizar o assistente **IPv6 Configuration** para configurar o IPv6 no servidor.

Requisitos de configuração

Determine qual destes dois tipos de configurações de IPv6 é mais apropriado para o seu caso. Se não tiver a certeza do tipo a escolher, consulte a secção Cenários de IPv6 para ver exemplos.

Será necessário cumprir estes requisitos para permitir que o IPv6 funcione no seu servidor:

Para configurar uma linha de Ethernet para o IPv6:

- OS/400 Versão 5, Edição 2 ou posterior
- iSeries Access for Windows e iSeries Navigator
 - Componente de rede do iSeries Navigator
- Adaptador de Ethernet 2838 ou 2849 a ser dedicado para o IPv6.
- O encaminhador que suporta o IPv6 só é necessário se pretender enviar tráfego de IPv6 para além da rede local (LAN) adjacente.
- O TCP/IP (com o IPv4) tem de ser configurado num adaptador físico separado, uma vez que tem de estar em execução no servidor. Se não tiver configurado o servidor para o IPv4, consulte a secção Configurar TCP/IP pela primeira vez antes de configurar a linha para o IPv4.

Para criar uma linha de túnel configurada (TNLCFG64):

- OS/400 Versão 5, Edição 2 ou posterior
- iSeries Access for Windows e iSeries Navigator
 - Componente de rede do iSeries Navigator
- O TCP/IP (com o IPv4) tem de ser configurado no servidor antes de poder configurar a linha de túnel para o IPv6. Se não tiver configurado o servidor para o IPv4, consulte a secção Configurar TCP/IP pela primeira vez.

Siga para Configurar IPv6 com o assistente IPv6 Configuration para obter instruções sobre acesso ao assistente.

Configurar o IPv6 com o assistente IPv6 Configuration

Para configurar o IPv6 no servidor, terá de alterar a configuração do mesmo com o assistente **IPv6 Configuration** no iSeries Navigator. O IPv6 só pode ser configurado a partir do iSeries Navigator e não a partir da interface baseada em caracteres.

Nota: pode configurar a descrição de linha de Ethernet do IPv6 com o comando Create Line Desc (Ethernet) CRTLINETH na interface baseada em caracteres; no entanto, terá de especificar o endereço de grupo de multidifusão hexadecimal 333300000001. Em seguida, terá de utilizar o assistente **IPv6 Configuration** para acabar de configurar o IPv6.

O assistente irá pedir as seguintes informações:

Para configurar uma linha de Ethernet para o IPv6:

Esta configuração permite enviar pacotes de IPv6 numa rede local (LAN) de IPv6. O assistente requer o nome do recurso de comunicações de hardware no servidor em que irá configurar o IPv6; por exemplo, CMN01. Este tem de ser um adaptador de Ethernet 2838 ou 2849 que não esteja actualmente configurado para o IPv4. Consulte a secção Criar uma rede local (LAN) de IPv6 para ver um cenário que mostra uma situação de configuração de uma linha de Ethernet para o IPv6.

Para criar uma linha de túnel configurada (TNLCFG64):

Esta configuração permite enviar pacotes de IPv6 em redes de IPv4. O assistente requer o endereço de IPv4 do ponto de terminação local e o endereço de IPv6 da interface local associada ao túnel. Consulte as secções Enviar pacotes de IPv6 numa rede local (LAN) de IPv4 e Enviar pacotes de IPv6 numa rede alargada (WAN) de IPv4 para ver cenários que mostram duas situações de criação de linhas de túnel configuradas para o IPv6.

Para utilizar o assistente **IPv6 Configuration**, siga estes passos:

1. No iSeries Navigator, expanda o **servidor** —> **Network** —> **TCP/IP Configuration**.
2. Faça clique com o botão direito do rato sobre **IPv6** e seleccione **IPv6 Configuration**.
3. Siga as instruções do assistente para configurar o IPv6 no seu servidor.

Configurar TCP/IP quando o sistema operativo está em estado restrito

Situação

Na qualidade de administrador de rede, terá de obter relatórios de estado de cópia de segurança do servidor. Ao executar procedimentos de cópia de segurança, o sistema operativo terá de estar em estado restrito para impedir que os utilizadores alterem quaisquer configurações. Visto que se encontra numa localização remota, o acesso aos relatórios de estado processa-se através de um dispositivo PDA (ou qualquer dispositivo de funcionamento em rede TCP/IP). O PDA usa uma aplicação activada para sockets que necessita de uma interface TCP/IP activa e disponível para comunicar com o servidor. Para estabelecer esta comunicação, deverá primeiro iniciar o TCP/IP com parâmetros especiais. Após o início de TCP/IP, terá de iniciar uma interface TCP/IP específica para permitir acesso ao sistema. As informações abaixo incluem mais detalhes.

Pré-requisitos

O servidor iSeries está em execução em OS/400(R) V5R2 ou superior.

Restrições

Aplicam-se as restrições que se seguem quando o sistema operativo está em estado restrito:

- Não é possível iniciar servidores de TCP/IP (comando CL: STRTCPSRV), dado que necessitam de subsistemas activos.
- Só é possível iniciar uma interface para um tipo de linha específico (Ethernet, token-ring, ou DDI) que não esteja ligada a uma descrição de servidor de rede (NWSD) nem a uma descrição de interface de rede (NWID).

Etapas de configuração

1. Iniciar TCP/IP com parâmetros especiais

Quando o sistema iSeries estiver em estado restrito, emita o seguinte comando na interface de linha de comandos: STRTCP STRSVR(*NO) STRIFC(*NO). Estes são os únicos parâmetros aceites quando o sistema operativo está em estado restrito. O comando acima irá iniciar o TCP/IP; todavia, não irá nem poderá iniciar servidores de aplicações TCP/IP nem interfaces de IP.

2. Iniciar uma interface TCP/IP específica

Uma vez iniciado o TCP/IP em estado restrito, poderá iniciar a interface específica necessária à aplicação activada para sockets de que dispõe.

- a. Verificar se a interface que pretende iniciar utiliza uma descrição de linha *ELAN, *TRLAN ou *DDI.

Para ver o tipo de linha da sua interface, introduza numa linha de comandos CFGTCP e seleccione a opção 1 - Work with TCP/IP interfaces.

- b. Verificar se a interface não está ligada a uma NWID ou NWSD. As outras tentativas que efectuar irão resultar numa mensagem de erro.

Para verificar se a interface não está ligada a uma NWID ou NWSD, introduza numa linha de comandos DSPLIND abc (em que abc é o nome da descrição de linha em questão). Verifique se o Nome de recurso (Resource name) não é *NWID ou *NWSD.

Nota: Se a interface estiver ligada a uma NWID ou NWSD, recomendamos que seleccione outra interface.

- c. Por fim, iniciar a interface. Numa linha de comandos, introduza o seguinte: STRTCPIFC INTNETADR('a.b.c.d'). Substitua a.b.c.d pelo endereço de IP da sua interface.

Nota: Verifique se STRTCPIFC INTNETADR(*AUTOSTART) não foi especificado.

3. Verificar se a interface está activa.

Emita o comando ping para a interface específica da sua aplicação. Existem muito poucos utilitários relativos a TCP/IP que funcionem em estado restrito. Todavia, poderá usar Ping e Netstat. Para mais informações sobre a utilização dos comandos ping e netstat, reveja a secção Ferramentas para verificar a estrutura da rede na Detecção e resolução de problemas de TCP/IP.

Capítulo 7. Personalizar TCP/IP com o iSeries Navigator

Assim que tiver configurado TCP/IP, poderá optar por personalizar a configuração. Ao longo da evolução da rede, poderá ter de alterar propriedades ou de adicionar interfaces ou encaminhamentos ao servidor. Poderá ter de configurar o servidor para IPv6 (Internet Protocol versão 6), de modo a utilizar aplicações de IPv6. Utilize os assistentes do iSeries Navigator para realizar rapidamente muitas destas tarefas.

Escolha qualquer um dos tópicos a seguir para personalizar a sua configuração com o iSeries Navigator. Estes tópicos fornecem um ponto de partida para a gestão da configuração de TCP/IP com o iSeries Navigator.

- Alterar definições de TCP/IP
- Configurar IPv6
- Adicionar interfaces de IPv4
- Adicionar interfaces de IPv6
- Adicionar encaminhamentos de IPv4
- Adicionar encaminhamentos de IPv6

Alterar definições de TCP/IP

Poderá ver e alterar as definições de TCP/IP com o iSeries Navigator. Por exemplo, poderá alterar as propriedades de nomes de sistema central ou de domínio, servidor de nomes, entradas da tabela de sistemas centrais, atributos de sistema, restrições de portas, servidores ou ligações ao cliente. Poderá alterar propriedades gerais ou propriedades que são específicas do IPv4 ou IPv6 como, por exemplo, transportes.

Para aceder à página de propriedades gerais de TCP/IP, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network**.
2. Faça clique com o botão direito do rato sobre **TCP/IP Configuration** e seleccione **Properties** para abrir a caixa de diálogo **TCP/IP Properties**.
3. Seleccione os separadores na parte superior da caixa de diálogo para ver e editar as informações de TCP/IP.

Para adicionar e alterar entradas da tabela de sistemas centrais, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network**.
2. Faça clique com o botão direito do rato sobre **TCP/IP Configuration** e seleccione **Host Table** para abrir a caixa de diálogo **Host Table**.
3. Utilize a caixa de diálogo **Host Table** para adicionar, editar ou remover entradas da tabela de sistemas centrais.

Para aceder às páginas de propriedades que são específicas do IPv4, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network**.
2. Faça clique com o botão direito do rato sobre **IPv4** e seleccione **Properties** para abrir a caixa de diálogo **IPv4 Properties**.
3. Seleccione os separadores na parte superior da caixa de diálogo para ver e editar as definições de propriedades de IPv4.

Para aceder às páginas de propriedades que são específicas do IPv6, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network**.

2. Faça clique com o botão direito do rato sobre **IPv6** e seleccione **Properties** para abrir a caixa de diálogo **IPv6 Properties**.
3. Seleccione os separadores na parte superior da caixa de diálogo para ver e editar as definições de propriedades de IPv6.

Configurar IPv6

Se não estiver familiarizado com o IPv6, consulte Internet Protocol versão 6 (IPv6) para ver uma descrição geral.

Para configurar o IPv6, terá de alterar a configuração do servidor com o assistente **IPv6 Configuration**. Antes de utilizar o assistente, consulte a a secção Configurar o IPv6 para ver instruções e requisitos especiais.

Adicionar interfaces de IPv4

Para criar uma nova interface de IPv4, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network** —> **TCP/IP Configuration**—> **IPv4**.
2. Faça clique com o botão direito do rato sobre **Interfaces**, seleccione **New Interface** e seleccione **Local Area Network, Wide Area Network** ou **Virtual IP**, para criar o tipo apropriado de interface de IPv4.
3. Siga as instruções do assistente para criar uma nova interface de IPv4.

Adicionar interfaces de IPv6

Para criar uma nova interface de IPv6, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network** —> **TCP/IP Configuration**—> **IPv6**.
2. Faça clique com o botão direito do rato sobre **Interfaces** e seleccione **New Interface**.
3. Siga as instruções do assistente para criar uma nova interface de IPv6.

Adicionar encaminhamentos de IPv4

As alterações que efectuar às informações de encaminhamento entram imediatamente em vigor.

Para configurar um novo encaminhamento de IPv4, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network** —> **TCP/IP Configuration**—> **IPv4**.
2. Faça clique com o botão direito do rato sobre **Routes** e seleccione **New Route**.
3. Siga as instruções do assistente para configurar um novo encaminhamento de IPv4.

Adicionar encaminhamentos de IPv6

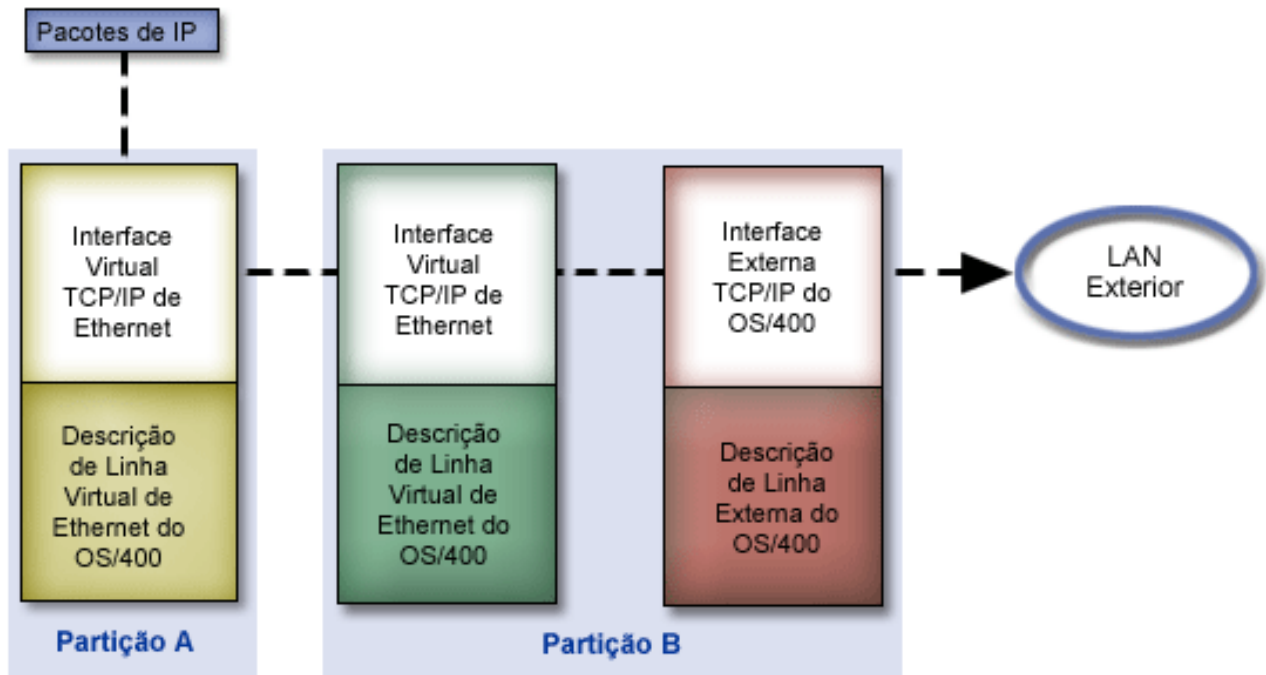
As alterações que efectuar às informações de encaminhamento entram imediatamente em vigor.

Para configurar um novo encaminhamento de IPv6, siga estes passos:

1. No iSeries Navigator, seleccione o **servidor** —> **Network** —> **TCP/IP Configuration**—> **IPv6**.
2. Faça clique com o botão direito do rato sobre **Routes** e seleccione **New Route**.
3. Siga as instruções do assistente para configurar um novo encaminhamento de IPv6.

Capítulo 8. Técnicas de TCP/IP para ligar Ethernet virtual a redes locais (LANs) externas

Se utilizar uma rede de Ethernet virtual para comunicação entre partições, poderá ter de activar estas partições para comunicarem com uma rede local física e externa. Existem várias formas de ligar a rede de Ethernet virtual a uma rede local externa com diversas técnicas de TCP/IP. Terá de permitir ao tráfego de TCP/IP a passagem entre a rede de Ethernet virtual e a rede local externa. Esta figura mostra uma transmissão lógica de pacotes de IP.



O tráfego de IP iniciado pela Partição A vai da respectiva interface de Ethernet virtual da Partição B. Ao implementar uma das três técnicas de TCP/IP abaixo mencionadas, poderá permitir que os pacotes de IP sigam para a interface externa em direcção ao seu destino.

Existem três métodos de ligação da Ethernet virtual à rede local externa. Cada um deles tem ligeiras diferenças que o tornam mais adequado aos conhecimentos de TCP/IP e ao ambiente do utilizador. Escolha um dos seguintes métodos:

- **ARP com proxy**

Este método usa uma colocação em sub-rede transparente para associar uma interface virtual de uma partição a uma interface externa. A função ARP com proxy está incorporada na pilha de TCP/IP. Se dispuser dos endereços de IP necessários, recomendamos esta abordagem.

- **Conversão de endereços de rede**


A filtragem de pacotes do OS/400 pode utilizar-se para encaminhar tráfego entre uma partição e a rede exterior.

- **Encaminhamento de TCP/IP**

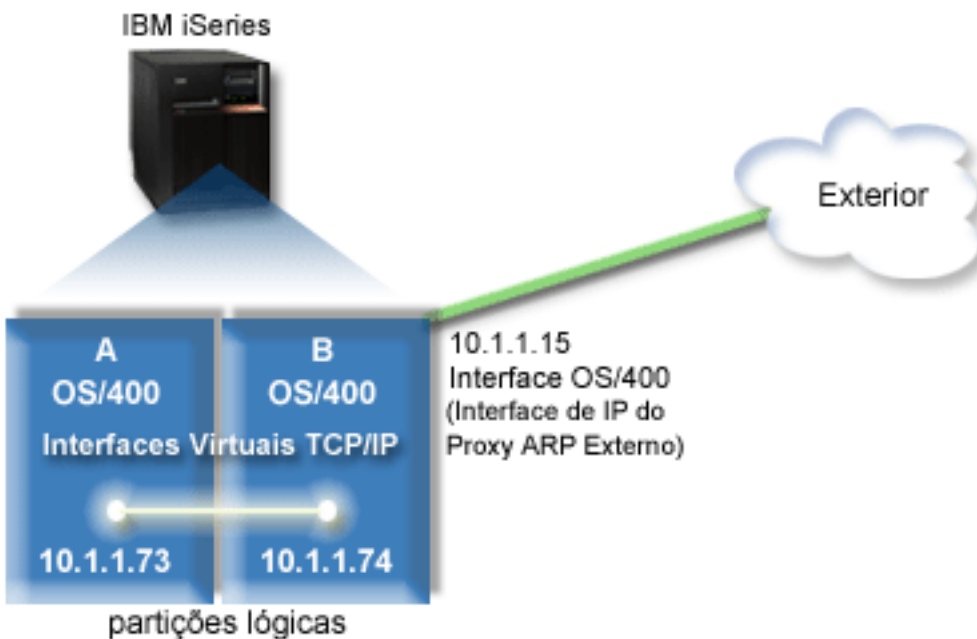
A norma de encaminhamento de TCP/IP usa-se para encaminhar tráfego para a rede Ethernet virtual da mesma forma em que se define encaminhamento para qualquer outra rede local (LAN). Para isto é necessário que actualize as informações de encaminhamento ao longo da sua rede.

Método do ARP de Proxy

O método ARP de proxy utiliza uma técnica conhecida como *colocação em sub-rede transparente*. Para saber mais sobre colocação em sub-rede transparente:

- V4 TCP/IP for AS/400: More Cool Things Than Ever 
Este redbook inclui cenários exemplo que demonstram soluções comuns com configurações ilustrativas. Além disso, ajuda a planejar, instalar, personalizar, configurar, detectar e resolver problemas de TCP/IP no servidor iSeries.
- Encaminhamento de TCP/IP e equilíbrio de volumes de trabalho
Este tópico inclui técnicas e instruções sobre encaminhamento e equilíbrio de volumes de trabalho.

Se tiver optado por usar o método ARP de proxy, terá de conhecer bem o funcionamento da colocação em sub-rede e de TCP/IP. Terá ainda de obter um bloco contíguo de endereços de IP que sejam encaminháveis pela sua rede. Irá colocar este bloco de endereços de IP em sub-rede. Neste exemplo utiliza-se um bloco contíguo de quatro endereços de IP (de 10.1.1.72 até 10.1.1.75). Dado que se trata de um bloco de quatro endereços de IP, a máscara de sub-rede destes será 255.255.255.252. Irá atribuir um a cada uma das interfaces de TCP/IP virtuais nas suas partições, como ilustra a figura.



Neste exemplo, o tráfego de TCP/IP da partição A passa pela Ethernet virtual para a interface 10.1.1.74 na partição B. Dado que 10.1.1.74 está associado à interface 10.1.1.15 de ARP de proxy externo, os pacotes saem da Ethernet virtual através da interface de ARP de proxy.

Para configurar uma Ethernet virtual para usar o método de ligação ARP com proxy, siga estas tarefas de configuração.

1. Activar partições lógicas para participarem numa Ethernet virtual
2. Criar as descrições de linha da Ethernet
3. Activar reenvio de datagramas de IP
4. Criar a interface para activar ARP com proxy
5. Criar a interface virtual de TCP/IP na partição A
6. Criar a interface virtual de TCP/IP na partição B
7. Criar o encaminhamento
8. Verificar comunicações de rede

Passo 1: Activar partições lógicas para participarem numa Ethernet virtual

Nota: Se utilizar outros servidores além dos modelos 270 and 8xx, terá de executar este passo com a HMC (Hardware Management Console) for eServer ao invés da partição principal. Consulte Ethernet virtual para mais pormenores.

Para activar a Ethernet virtual, siga estes passos:

1. Na linha de comandos da partição principal (partição A), introduza STRSST e prima Enter.
2. Introduza o ID de utilizador e a palavra-passe das ferramentas de serviço.
3. No ecrã das SST (System Service Tools), seleccione a opção 5 (Work with System Partitions).
4. No ecrã Work with System Partitions, seleccione a opção 3 (Work with partition configuration).
5. Prima F10 (Work with Virtual Ethernet).
6. Introduza 1 na coluna apropriada à partição A e à partição B para activar partições de modo a comunicarem entre si via Ethernet virtual.
7. Saia das SST (System Service Tools) para voltar à linha de comandos.

O que fazer em seguida

Criar as descrições de linha da Ethernet

Passo 2: Criar as descrições de linha da Ethernet

Terá de seguir este passo de uma de duas formas, consoante o modelo de servidor que utilizar. Escolha um destes métodos para criar as descrições de linha com base no modelo de servidor de que dispuser.

- Criar as descrições de linha Ethernet em servidores modelo 270 e 8xx
- Criar as descrições de linha Ethernet em servidores diferentes dos modelos 270 e 8xx

Criar as descrições de linha Ethernet em servidores modelo 270 e 8xx

Para configurar novas descrições de linha Ethernet que suportem a Ethernet virtual, siga estes passos:

1. Na linha de comandos na partição A, introduza WRKHDWRSC *CMN e prima Enter.
2. No ecrã Work with Communication Resources, seleccione a opção 7 (Display resource detail) junto à porta Ethernet virtual apropriada.
A porta Ethernet identificada como 268C é o recurso Ethernet virtual. Existirá uma para cada Ethernet virtual que esteja ligada à partição lógica.
3. No ecrã Display Resource Detail, desloque-se para baixo para localizar o endereço da porta. O endereço da porta corresponde à Ethernet virtual que tiver seleccionado durante a configuração da partição lógica.
4. No ecrã Work with Communication Resources, seleccione a opção 5 (Work with configuration descriptions) junto à porta Ethernet virtual apropriada e prima Enter.
5. No ecrã Work with Configuration Descriptions, seleccione a opção 1 (Create) e prima Enter para ver o ecrã Create Line Description Ethernet (CRTLINETH).
 - a. Ao pedido *Line description* responda com VETH0. O nome VETH0, embora arbitrário, corresponde à coluna numerada na página da Ethernet virtual onde activou as partições lógicas para comunicarem entre si. Se utilizar os mesmos nomes para as descrições de linha e respectiva Ethernet virtual associada, poderá ter sempre presentes as configurações da Ethernet virtual.
 - b. Ao pedido *Line speed* responda com 1G.
 - c. Ao pedido *Duplex* responda com *FULL e prima Enter.
 - d. Ao pedido *Maximum frame size* responda com 8996 e prima Enter. Ao alterar o tamanho das frames para 8996, irá melhorar a transferência de dados através da Ethernet virtual.
Será apresentada uma mensagem em como a descrição de linha foi criada.

- | 6. Active a descrição de linha. Introduza WRKCFGSTS *LIN e selecione a opção 1 (Vary on) para VETH0.
- | 7. Repita os passos de 1 a 6, mas a partir da linha de comandos da partição B, de modo a criar uma descrição de linha Ethernet para a partição B.
- | Embora os nomes das descrições de linha sejam arbitrários, será útil usar os mesmos para todas as descrições de linha associadas à Ethernet virtual. Neste cenário, todas as descrições de linha se chamam VETH0.

| O que fazer em seguida

| Activar reenvio de datagramas de IP

| Criar as descrições de linha Ethernet em servidores diferentes dos modelos 270 e 8xx

| Para configurar novas descrições de linha Ethernet que suportem a Ethernet virtual, siga estes passos:

- | 1. Na linha de comandos na partição A, introduza WRKHDWRSC *CMN e prima Enter.
- | 2. No ecrã Work with Communication Resources, selecione a opção 7 (Display resource detail) junto à porta Ethernet virtual apropriada.
| As portas Ethernet identificadas como 268C são os recursos Ethernet virtuais. Existirá uma para cada adaptador de Ethernet virtual. Cada uma das portas identificada como 268C tem um código de localização associado que é criado quando se cria o adaptador Ethernet virtual com a HMC (Passo 1).
- | 3. No ecrã Display Resource Detail, desloque-se para baixo para localizar o recurso 268C que está associado ao código de localização específico criado para esta Ethernet virtual.
- | 4. No ecrã Work with Communication Resources, selecione a opção 5 (Work with configuration descriptions) junto ao recurso Ethernet virtual apropriada e prima Enter.
- | 5. No ecrã Work with Configuration Descriptions, selecione a opção 1 (Create) e prima Enter para ver o ecrã Create Line Description Ethernet (CRTLINETH).
 - | a. Ao pedido *Line description* responda com VETH0. Se utilizar os mesmos nomes para as descrições de linha e respectiva Ethernet virtual associada, como por exemplo VETH0, poderá ter sempre presentes as configurações da Ethernet virtual.
 - | b. Ao pedido *Line speed* responda com 1G.
 - | c. Ao pedido *Duplex* responda com *FULL e prima Enter.
 - | d. Ao pedido *Maximum frame size* responda com 8996 e prima Enter. Ao alterar o tamanho das frames para 8996, irá melhorar a transferência de dados através da Ethernet virtual.
| Será apresentada uma mensagem em como a descrição de linha foi criada.
- | 6. Active a descrição de linha. Introduza WRKCFGSTS *LIN e selecione a opção 1 (Vary on) para VETH0.
- | 7. Repita os passos de 1 a 6, mas a partir da linha de comandos da partição B, de modo a criar uma descrição de linha Ethernet para a partição B.
- | Embora os nomes das descrições de linha sejam arbitrários, será útil usar os mesmos para todas as descrições de linha associadas à Ethernet virtual. Neste cenário, todas as descrições de linha se chamam VETH0.

| O que fazer em seguida

| Activar reenvio de datagramas de IP

| Passo 3: Activar reenvio de datagramas de IP

| Active o reenvio de datagramas de IP de modo a que os pacotes possam ser reenviados entre sub-redes diferentes.

| Para activar reenvio de datagramas de IP, siga estes passos:

- | 1. Na linha de comandos da partição A, introduza CHGTCPA e prima F4.

| 2. Ao pedido *IP datagram forwarding* responda com *YES.

| O que fazer em seguida

| Criar a interface para activar ARP com proxy

| **Passo 4: Criar a interface para activar ARP com proxy**

| Para criar a interface TCP/IP para activar ARP com proxy, siga estes passos:

- | 1. Obtenha um bloco contíguo de endereços de IP que sejam encaminháveis pela sua rede.
| Visto que dispõe de duas partições nesta Ethernet virtual, terá um bloco de quatro endereços. O quarto segmento do primeiro endereço de IP no bloco tem de ser divisível por quatro. O primeiro e último endereço de IP deste bloco são a sub-rede e os endereços de IP de difusão e são inutilizáveis. O segundo e terceiro endereços de IP podem utilizar-se para as interfaces TCP/IP para a Ethernet virtual na partição A e B. Nesse sentido, o bloco de endereços de IP será de 10.1.1.72 a 10.1.1.75 com uma máscara de sub-rede 255.255.255.252.
| É necessário ainda um único endereço de IP para o endereço de TCP/IP externo. Este endereço de IP não tem de pertencer ao bloco de endereços contíguos mas terá de se inserir na mesma máscara de sub-rede original 255.255.255.0. Neste procedimento, o endereço de IP externo é 10.1.1.15.
- | 2. Crie uma interface TCP/IP de OS/400 para a partição B. Esta interface é conhecida como interface de IP de ARP com proxy externa. Para criar a interface, siga estes passos:
 - | a. Na linha de comandos na partição B, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.
 - | b. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.
 - | c. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).
 - | d. Ao pedido *Internet address* responda com '10.1.1.15'.
 - | e. Ao pedido *Line description* responda com o nome da descrição de linha, como por exemplo, LINHAETH.
 - | f. Ao pedido *Subnet mask* responda com '255.255.255.0'.
- | 3. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.

| O que fazer em seguida

| Criar a interface virtual de TCP/IP na partição A

| **Passo 5: Criar a interface virtual de TCP/IP na partição A**

| Para criar a interface virtual, siga estes passos:

- | 1. Na linha de comandos na partição A, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.
- | 2. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.
- | 3. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).
- | 4. Ao pedido *Internet address* responda com '10.1.1.73'.
- | 5. Ao pedido *Line description* responda com o nome da descrição de linha, como por exemplo, LINHAETH.
- | 6. Ao pedido *Subnet mask* responda com '255.255.255.252'.
- | 7. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.

| O que fazer em seguida

| Criar a interface virtual de TCP/IP na partição B

| **Passo 6: Criar a interface virtual de TCP/IP na partição B**

| Para criar a interface virtual, siga estes passos:

- | 1. Na linha de comandos na partição B, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.
- | 2. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.
- | 3. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).
- | 4. Ao pedido *Internet address* responda com '10.1.1.74'.
- | 5. Ao pedido *Line description* responda com o nome da descrição de linha, como por exemplo, LINHAETH.
- | 6. Ao pedido *Subnet mask* responda com '255.255.255.252'.
- | 7. Ao pedido *Associated local interface* responda com '10.1.1.15'. Irá assim associar a interface virtual à interface externa e activar o ARP com proxy para reenviar pacotes entre a interface virtual 10.1.1.74 e a interface externa 10.1.1.15.
- | 8. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.

| **O que fazer em seguida**

| Criar o encaminhamento

| **Passo 7: Criar o encaminhamento**

| Para criar o encaminhamento predefinido de modo a permitir aos pacotes saírem da rede Ethernet virtual, siga estes passos:

- | 1. Na linha de comandos na partição A, introduza CFGTCP e prima Enter.
- | 2. Seleccione a opção 2 (Work with TCP/IP Routes) e prima Enter.
- | 3. Seleccione a opção 1 (Add) e prima Enter.
- | 4. Ao pedido *Route destination* responda com *DFTRROUTE.
- | 5. Ao pedido *Subnet mask* responda com *NONE.
- | 6. Ao pedido *Next hop* responda com '10.1.1.74'.
| Os pacotes da partição A passam pela Ethernet virtual e chegam à interface 10.1.1.74 por este encaminhamento predefinido. Dado que 10.1.1.74 está associado à interface 10.1.1.15 de ARP de proxy externo, os pacotes saem da Ethernet virtual através da interface ARP com proxy.

| **O que fazer em seguida**

| Verificar comunicações de rede

| **Passo 8: Verificar comunicações de rede**

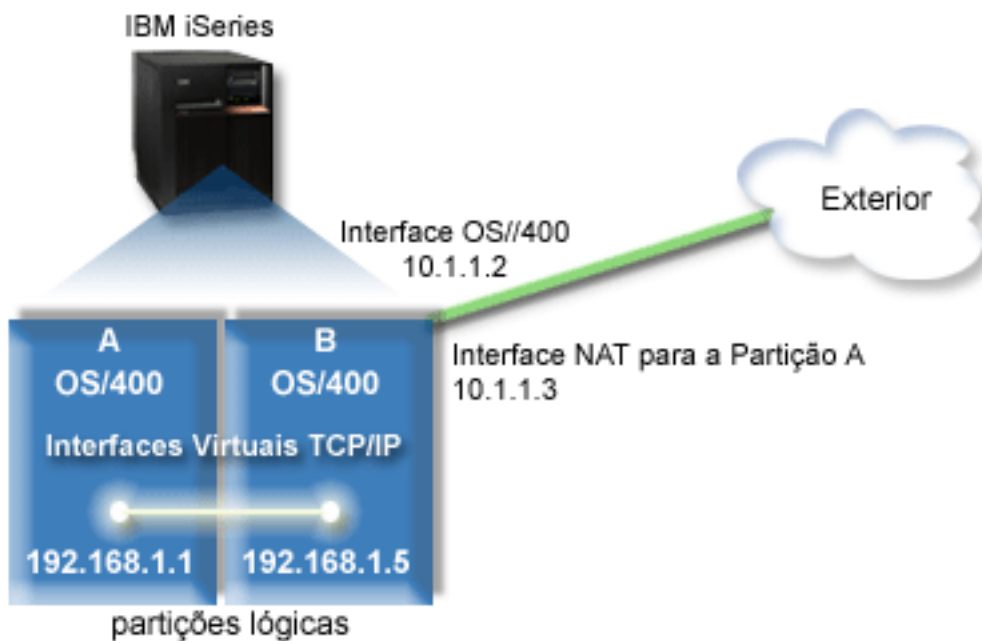
| Verifique as comunicações de rede com o comando ping:

- | • Na partição A, execute ping à interface Ethernet virtual 10.1.1.74 e a um sistema central externo.
- | • A partir de um sistema central OS/400 externo, execute ping às interfaces Ethernet 10.1.1.73 e 10.1.1.74.

| **Método de conversão de endereços de rede**

| A conversão de endereços de rede (NAT - network address translation) pode reencaminhar tráfego entre a rede Ethernet virtual e uma rede externa. A esta forma especial de NAT chama-se NAT estática, e esta permitirá tanto tráfego de entrada como de saída na rede Ethernet virtual. As outras formas de NAT, como a NAT de colocação em máscara, também funcionam se a rede Ethernet virtual não necessitar de receber tráfego iniciado por clientes externos. Tal como com os métodos de encaminhamento TCP/IP e ARP com proxy, poderá tirar partido da ligação de rede do OS/400 existente. Dado que irá usar regras de pacotes de IP, terá de usar o iSeries Navigator para criar e aplicar as suas regras.

| A figura que se segue exemplifica a utilização da NAT para ligar a rede Ethernet virtual a uma rede externa. A rede 10.1.1.x representa uma rede externa, enquanto que a rede 192.168.1.x representa a rede Ethernet virtual.



| Neste exemplo, o tráfego de TCP/IP existente para o servidor passa pela interface 10.1.1.2. Dado que se trata de um cenário de correlação estática, o tráfego de entrada é convertido da interface 10.1.1.3 na interface 192.168.1.5. Por seu turno, o tráfego de saída é convertido da interface 192.168.1.5 na interface 10.1.1.3 externa. A partição A e a partição B usam as respectivas interfaces virtuais 192.168.1.1 e 192.168.1.5 para comunicarem entre si.

| Para que a NAT estática funcione, terá de configurar primeiro as comunicações do OS/400 e do TCP/IP. Em seguida poderá criar e aplicar algumas regras de pacotes de IP. Para configurar uma Ethernet virtual para usar o método NAT, siga estas tarefas de configuração:

- | 1. Activar partições lógicas para participarem numa Ethernet virtual
- | 2. Criar as descrições de linha da Ethernet
- | 3. Activar reenvio de datagramas de IP
- | 4. Criar as interfaces
- | 5. Verificar comunicações de rede
- | 6. Criar regras de pacotes
- | 7. Verificar comunicações de rede

| **Passo 1: Activar partições lógicas para participarem numa Ethernet virtual**

| **Nota:** Se utilizar outros servidores além dos modelos 270 and 8xx, terá de executar este passo com a HMC (Hardware Management Console) for eServer ao invés da partição principal. Consulte Ethernet virtual para mais pormenores.

| Para activar a Ethernet virtual, siga estes passos:

- | 1. Na linha de comandos da partição principal (partição A), introduza STRSST e prima Enter.
- | 2. Introduza o ID de utilizador e a palavra-passe das ferramentas de serviço.
- | 3. No ecrã das SST (System Service Tools), seleccione a opção 5 (Work with System Partitions).

- | 4. No ecrã Work with System Partitions, seleccione a opção 3 (Work with partition configuration).
- | 5. Prima F10 (Work with Virtual Ethernet).
- | 6. Introduza 1 na coluna apropriada à partição A e à partição B para activar partições de modo a comunicarem entre si via Ethernet virtual.
- | 7. Saia das SST (System Service Tools) para voltar à linha de comandos.

| O que fazer em seguida

| Criar as descrições de linha da Ethernet

| Passo 2: Criar as descrições de linha da Ethernet

| Terá de seguir este passo de uma de duas formas, consoante o modelo de servidor que utilizar. Escolha um destes métodos para criar as descrições de linha com base no modelo de servidor de que dispuser.

- | • Criar as descrições de linha Ethernet em servidores modelo 270 e 8xx
- | • Criar as descrições de linha Ethernet em servidores diferentes dos modelos 270 e 8xx

| Criar as descrições de linha Ethernet em servidores modelo 270 e 8xx

| Para configurar novas descrições de linha Ethernet que suportem a Ethernet virtual, siga estes passos:

- | 1. Na linha de comandos na partição A, introduza WRKHDWRSC *CMN e prima Enter.
- | 2. No ecrã Work with Communication Resources, seleccione a opção 7 (Display resource detail) junto à porta Ethernet virtual apropriada.
| A porta Ethernet identificada como 268C é o recurso Ethernet virtual. Existirá uma para cada Ethernet virtual que esteja ligada à partição lógica.
- | 3. No ecrã Display Resource Detail, desloque-se para baixo para localizar o endereço da porta. O endereço da porta corresponde à Ethernet virtual que tiver seleccionado durante a configuração da partição lógica.
- | 4. No ecrã Work with Communication Resources, seleccione a opção 5 (Work with configuration descriptions) junto à porta Ethernet virtual apropriada e prima Enter.
- | 5. No ecrã Work with Configuration Descriptions, seleccione a opção 1 (Create) e prima Enter para ver o ecrã Create Line Description Ethernet (CRTLINETH).
 - | a. Ao pedido *Line description* responda com VETH0. O nome VETH0, embora arbitrário, corresponde à coluna numerada na página da Ethernet virtual onde activou as partições lógicas para comunicarem entre si. Se utilizar os mesmos nomes para as descrições de linha e respectiva Ethernet virtual associada, poderá ter sempre presentes as configurações da Ethernet virtual.
 - | b. Ao pedido *Line speed* responda com 1G.
 - | c. Ao pedido *Duplex* responda com *FULL e prima Enter.
 - | d. Ao pedido *Maximum frame size* responda com 8996 e prima Enter. Ao alterar o tamanho das frames para 8996, irá melhorar a transferência de dados através da Ethernet virtual.
| Será apresentada uma mensagem em como a descrição de linha foi criada.
- | 6. Active a descrição de linha. Introduza WRKCFGSTS *LIN e seleccione a opção 1 (Vary on) para VETH0.
- | 7. Repita os passos de 1 a 6, mas a partir da linha de comandos da partição B, de modo a criar uma descrição de linha Ethernet para a partição B.
| Embora os nomes das descrições de linha sejam arbitrários, será útil usar os mesmos para todas as descrições de linha associadas à Ethernet virtual. Neste cenário, todas as descrições de linha se chamam VETH0.

| O que fazer em seguida

| Activar reenvio de datagramas de IP

Criar as descrições de linha Ethernet em servidores diferentes dos modelos 270 e 8xx

Para configurar novas descrições de linha Ethernet que suportem a Ethernet virtual, siga estes passos:

1. Na linha de comandos na partição A, introduza WRKHDWRSC *CMN e prima Enter.
2. No ecrã Work with Communication Resources, seleccione a opção 7 (Display resource detail) junto à porta Ethernet virtual apropriada.
As portas Ethernet identificadas como 268C são os recursos Ethernet virtuais. Existirá uma para cada adaptador de Ethernet virtual. Cada uma das portas identificada como 268C tem um código de localização associado que é criado quando se cria o adaptador Ethernet virtual com a HMC (Passo 1).
3. No ecrã Display Resource Detail, desloque-se para baixo para localizar o recurso 268C que está associado ao código de localização específico criado para esta Ethernet virtual.
4. No ecrã Work with Communication Resources, seleccione a opção 5 (Work with configuration descriptions) junto ao recurso Ethernet virtual apropriada e prima Enter.
5. No ecrã Work with Configuration Descriptions, seleccione a opção 1 (Create) e prima Enter para ver o ecrã Create Line Description Ethernet (CRTLINETH).
 - a. Ao pedido *Line description* responda com VETH0. Se utilizar os mesmos nomes para as descrições de linha e respectiva Ethernet virtual associada, como por exemplo VETH0, poderá ter sempre presentes as configurações da Ethernet virtual.
 - b. Ao pedido *Line speed* responda com 1G.
 - c. Ao pedido *Duplex* responda com *FULL e prima Enter.
 - d. Ao pedido *Maximum frame size* responda com 8996 e prima Enter. Ao alterar o tamanho das frames para 8996, irá melhorar a transferência de dados através da Ethernet virtual.
Será apresentada uma mensagem em como a descrição de linha foi criada.
6. Active a descrição de linha. Introduza WRKCFGSTS *LIN e seleccione a opção 1 (Vary on) para VETH0.
7. Repita os passos de 1 a 6, mas a partir da linha de comandos da partição B, de modo a criar uma descrição de linha Ethernet para a partição B.
Embora os nomes das descrições de linha sejam arbitrários, será útil usar os mesmos para todas as descrições de linha associadas à Ethernet virtual. Neste cenário, todas as descrições de linha se chamam VETH0.

O que fazer em seguida

Activar reenvio de datagramas de IP

Passo 3: Activar reenvio de datagramas de IP

Active o reenvio de datagramas de IP de modo a que os pacotes possam ser reenviados entre sub-redes diferentes.

Para activar reenvio de datagramas de IP, siga estes passos:

1. Na linha de comandos da partição A, introduza CHGTCPA e prima F4.
2. Ao pedido *IP datagram forwarding* responda com *YES.

O que fazer em seguida

Criar as interfaces

Passo 4: Criar as interfaces

Para criar as interfaces TCP/IP, siga estes passos:

1. Crie e inicie uma interface de TCP/IP em OS/400 na partição B para comunicações genéricas de e para o servidor. Para criar a interface, siga estes passos:

- a. Na linha de comandos na partição B, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.
 - b. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.
 - c. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).
 - d. Ao pedido *Internet address* responda com '10.1.1.2'.
 - e. Ao pedido *Line description* responda com ETHLINE.
 - f. Ao pedido *Subnet mask* responda com '255.255.255.0'.
 - g. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.
2. Crie e inicie outra interface TCP/IP que se ligue a uma rede externa. Esta deverá usar a mesma descrição de linha que a interface TCP/IP existente. Esta interface irá efectuar a conversão de endereços relativa à sua partição. Para criar a interface, siga estes passos:
 - a. Na linha de comandos na partição B, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.
 - b. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.
 - c. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).
 - d. Ao pedido *Internet address* responda com '10.1.1.3'.
 - e. Ao pedido *Line description* responda com ETHLINE.
 - f. Ao pedido *Subnet mask* responda com '255.255.255.0'.
 - g. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.
3. Crie e inicie a interface de TCP/IP do OS/400 na partição A para a Ethernet virtual. Para criar a interface, siga estes passos:
 - a. Na linha de comandos na partição A, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.
 - b. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.
 - c. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).
 - d. Ao pedido *Internet address* responda com '192.168.1.1'.
 - e. Ao pedido *Line description* responda com VETH0.
 - f. Ao pedido *Subnet mask* responda com '255.255.255.0'.
 - g. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.
 4. Crie e inicie a interface de TCP/IP do OS/400 na partição B para a Ethernet virtual. Para criar a interface, siga estes passos:
 - a. Na linha de comandos na partição B, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.
 - b. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.
 - c. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).
 - d. Ao pedido *Internet address* responda com '192.168.1.5'.
 - e. Ao pedido *Line description* responda com VETH0.
 - f. Ao pedido *Subnet mask* responda com '255.255.255.0'.
 - g. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.

O que fazer em seguida

Verificar comunicações de rede

| **Passo 5: Verificar comunicações de rede**

| Verifique as comunicações de rede com o comando ping:

- | • Na partição A, execute ping à interface Ethernet virtual 192.168.1.5 e a um sistema central externo.
- | • A partir de um sistema central OS/400 externo, execute ping às interfaces Ethernet virtuais 192.168.1.1 e 192.168.1.5.

| **O que fazer em seguida**

| Criar regras de pacotes

| **Passo 6: Criar regras de pacotes**

| Use o assistente Address Translation no iSeries Navigator para criar as regras de pacotes que correlacionam o endereço privado na partição A com o endereço público na partição B.

| Para criar as regras de pacote, siga estes passos:

- | 1. No iSeries Navigator, expanda o servidor **iSeries** -> **Network** -> **IP Policies**.
- | 2. Clique com o botão direito do rato em **Packet Rules** e seleccione **Rules Editor**.
- | 3. Seleccione **Address Translation** no menu **Wizard**.
- | 4. Siga as instruções do assistente para criar as regras de pacote. Este procedimento usa as seguintes selecções:
 - | • Seleccione **Map address translation**
 - | • Introduza o endereço de IP privado 192.168.1.1
 - | • Introduza o endereço de IP público 10.1.1.3
 - | • Seleccione a linha em que as interfaces estão configuradas, por exemplo, LINHAETH.
- | 5. Seleccione **Activate Rules** no menu **File**.

| **O que fazer em seguida**

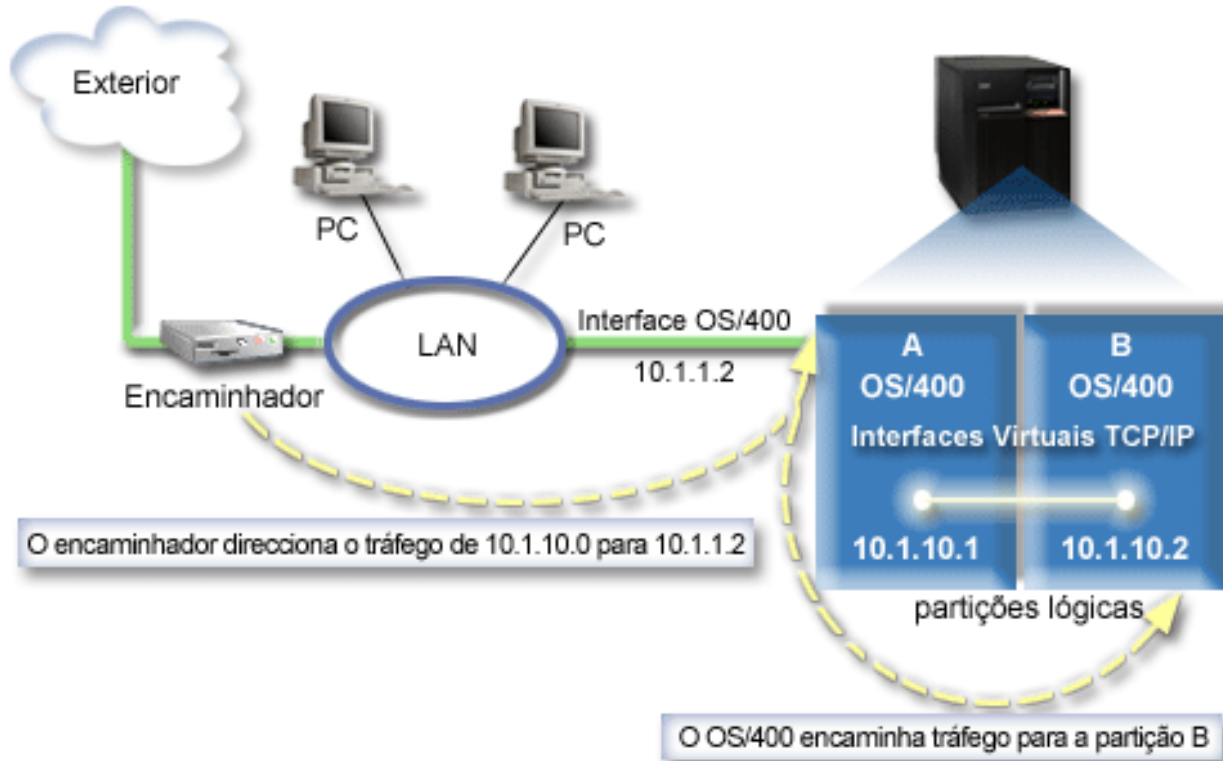
| Verificar comunicações de rede

| **Passo 7: Verificar comunicações de rede**

| Depois de criar as regras de pacote deverá verificar as comunicações da rede. Para testar comunicações de saída, execute o comando ping a um sistema central externo a partir da partição A. Em seguida, desse sistema central, execute o comando ping à partição A para testar as comunicações de entrada.

Método de encaminhamento de TCP/IP

Poderá também encaminhar tráfego para as partições através do servidor iSeries e com diversas técnicas de encaminhamento. Esta solução não é difícil de configurar no servidor mas, consoante a topologia da sua rede, poderá não ser prática de implementar. Considere a figura que se segue.



A interface TCP/IP existente (10.1.1.2) liga-se à rede local (LAN). A rede local está ligada a redes remotas através de um encaminhador. A interface TCP/IP virtual na partição B é endereçada como 10.1.10.2 e a interface TCP/IP virtual na partição A como 10.1.10.1. Em OS/400, se activar o reenvio de datagramas de IP, o OS/400 encaminhará os pacotes de IP de e para a partição B. Quando se define a ligação de TCP/IP para a partição B, o endereço do encaminhador tem de ser 10.1.10.1.

A dificuldade deste tipo de encaminhamento está em levar os pacotes de IP ao iSeries. Neste cenário, poderia definir um encaminhamento no encaminhador de modo a transmitir pacotes à interface 10.1.1.2 que eram destinados à rede 10.1.10.0. Isso funciona para clientes de rede remota, e funcionaria também para clientes da rede local (clientes ligados à mesma rede local do iSeries) se reconhecerem esse mesmo encaminhador como sistema de passagem seguinte. Se assim não for, cada cliente terá de ter um encaminhamento que direcione o tráfego de 10.1.10.0 para a interface 10.1.1.2 do OS/400, daí a dificuldade prática deste método. Se tiver muitos clientes de rede local terá de definir muitos encaminhamentos.

Para configurar uma Ethernet virtual para usar o método de encaminhamento TCP/IP, siga estas instruções:

1. Activar partições lógicas para participarem numa Ethernet virtual
2. Criar as descrições de linha da Ethernet
3. Activar reenvio de datagramas de IP
4. Criar as interfaces

Passo 1: Activar partições lógicas para participarem numa Ethernet virtual

Nota: Se utilizar outros servidores além dos modelos 270 and 8xx, terá de executar este passo com a HMC (Hardware Management Console) for eServer ao invés da partição principal. Consulte Ethernet virtual para mais pormenores.

Para activar a Ethernet virtual, siga estes passos:

1. Na linha de comandos da partição principal (partição A), introduza STRSST e prima Enter.
2. Introduza o ID de utilizador e a palavra-passe das ferramentas de serviço.
3. No ecrã das SST (System Service Tools), seleccione a opção 5 (Work with System Partitions).
4. No ecrã Work with System Partitions, seleccione a opção 3 (Work with partition configuration).
5. Prima F10 (Work with Virtual Ethernet).
6. Introduza 1 na coluna apropriada à partição A e à partição B para activar partições de modo a comunicarem entre si via Ethernet virtual.
7. Saia das SST (System Service Tools) para voltar à linha de comandos.

O que fazer em seguida

Criar descrições de linha da Ethernet

Passo 2: Criar as descrições de linha da Ethernet

Terá de seguir este passo de uma de duas formas, consoante o modelo de servidor que utilizar. Escolha um destes métodos para criar as descrições de linha com base no modelo de servidor de que dispuser.

- Criar as descrições de linha Ethernet em servidores modelo 270 e 8xx
- Criar as descrições de linha Ethernet em servidores diferentes dos modelos 270 e 8xx

Criar as descrições de linha Ethernet em servidores modelo 270 e 8xx

Para configurar novas descrições de linha Ethernet que suportem a Ethernet virtual, siga estes passos:

1. Na linha de comandos na partição A, introduza WRKHDWRSC *CMN e prima Enter.
2. No ecrã Work with Communication Resources, seleccione a opção 7 (Display resource detail) junto à porta Ethernet virtual apropriada.
A porta Ethernet identificada como 268C é o recurso Ethernet virtual. Existirá uma para cada Ethernet virtual que esteja ligada à partição lógica.
3. No ecrã Display Resource Detail, desloque-se para baixo para localizar o endereço da porta. O endereço da porta corresponde à Ethernet virtual que tiver seleccionado durante a configuração da partição lógica.
4. No ecrã Work with Communication Resources, seleccione a opção 5 (Work with configuration descriptions) junto à porta Ethernet virtual apropriada e prima Enter.
5. No ecrã Work with Configuration Descriptions, seleccione a opção 1 (Create) e prima Enter para ver o ecrã Create Line Description Ethernet (CRTLINETH).
 - a. Ao pedido *Line description* responda com VETH0. O nome VETH0, embora arbitrário, corresponde à coluna numerada na página da Ethernet virtual onde activou as partições lógicas para comunicarem entre si. Se utilizar os mesmos nomes para as descrições de linha e respectiva Ethernet virtual associada, poderá ter sempre presentes as configurações da Ethernet virtual.
 - b. Ao pedido *Line speed* responda com 1G.
 - c. Ao pedido *Duplex* responda com *FULL e prima Enter.
 - d. Ao pedido *Maximum frame size* responda com 8996 e prima Enter. Ao alterar o tamanho das frames para 8996, irá melhorar a transferência de dados através da Ethernet virtual.
Será apresentada uma mensagem em como a descrição de linha foi criada.

- | 6. Active a descrição de linha. Introduza WRKCFGSTS *LIN e selecione a opção 1 (Vary on) para VETH0.
 - | 7. Repita os passos de 1 a 6, mas a partir da linha de comandos da partição B, de modo a criar uma descrição de linha Ethernet para a partição B.
- | Embora os nomes das descrições de linha sejam arbitrários, será útil usar os mesmos para todas as descrições de linha associadas à Ethernet virtual. Neste cenário, todas as descrições de linha se chamam VETH0.

| O que fazer em seguida

| Activar reenvio de datagramas de IP

| Criar as descrições de linha Ethernet em servidores diferentes dos modelos 270 e 8xx

| Para configurar novas descrições de linha Ethernet que suportem a Ethernet virtual, siga estes passos:

- | 1. Na linha de comandos na partição A, introduza WRKHDWRSC *CMN e prima Enter.
- | 2. No ecrã Work with Communication Resources, selecione a opção 7 (Display resource detail) junto à porta Ethernet virtual apropriada.
| As portas Ethernet identificadas como 268C são os recursos Ethernet virtuais. Existirá uma para cada adaptador de Ethernet virtual. Cada uma das portas identificada como 268C tem um código de localização associado que é criado quando se cria o adaptador Ethernet virtual com a HMC (Passo 1).
- | 3. No ecrã Display Resource Detail, desloque-se para baixo para localizar o recurso 268C que está associado ao código de localização específico criado para esta Ethernet virtual.
- | 4. No ecrã Work with Communication Resources, selecione a opção 5 (Work with configuration descriptions) junto ao recurso Ethernet virtual apropriada e prima Enter.
- | 5. No ecrã Work with Configuration Descriptions, selecione a opção 1 (Create) e prima Enter para ver o ecrã Create Line Description Ethernet (CRTLINETH).
 - | a. Ao pedido *Line description* responda com VETH0. Se utilizar os mesmos nomes para as descrições de linha e respectiva Ethernet virtual associada, como por exemplo VETH0, poderá ter sempre presentes as configurações da Ethernet virtual.
 - | b. Ao pedido *Line speed* responda com 1G.
 - | c. Ao pedido *Duplex* responda com *FULL e prima Enter.
 - | d. Ao pedido *Maximum frame size* responda com 8996 e prima Enter. Ao alterar o tamanho das frames para 8996, irá melhorar a transferência de dados através da Ethernet virtual.
| Será apresentada uma mensagem em como a descrição de linha foi criada.
- | 6. Active a descrição de linha. Introduza WRKCFGSTS *LIN e selecione a opção 1 (Vary on) para VETH0.
- | 7. Repita os passos de 1 a 6, mas a partir da linha de comandos da partição B, de modo a criar uma descrição de linha Ethernet para a partição B.
| Embora os nomes das descrições de linha sejam arbitrários, será útil usar os mesmos para todas as descrições de linha associadas à Ethernet virtual. Neste cenário, todas as descrições de linha se chamam VETH0.

| O que fazer em seguida

| Activar reenvio de datagramas de IP

| Passo 3: Activar reenvio de datagramas de IP

| Active o reenvio de datagramas de IP de modo a que os pacotes possam ser reenviados entre sub-redes diferentes.

| Para activar reenvio de datagramas de IP, siga estes passos:

- | 1. Na linha de comandos da partição A, introduza CHGTCPA e prima F4.

| 2. Ao pedido *IP datagram forwarding* responda com *YES.

| O que fazer em seguida

| Criar as interfaces

| Passo 4: Criar as interfaces

| Para criar as interfaces TCP/IP, siga estes passos:

| 1. Crie uma interface TCP/IP de OS/400 na partição A. Para criar a interface, siga estes passos:

| a. Na linha de comandos na partição A, introduza CFGTCP e prima Enter para ver o ecrã Configure TCP/IP.

| b. Seleccione a opção 1 (Work with TCP/IP Interfaces) e prima Enter.

| c. Seleccione a opção 1 (Add) e prima Enter para ver o ecrã Add TCP/IP Interface (ADDTCPIFC).

| d. Ao pedido *Internet address* responda com '10.1.1.2'.

| e. Ao pedido *Line description* responda com o nome da descrição de linha, como por exemplo, LINHAETH.

| f. Ao pedido *Subnet mask* responda com '255.255.255.0'.

| 2. Inicie a interface. No ecrã Work with TCP/IP Interfaces, seleccione a opção 9 (Start) junto à interface.

| 3. Repita os passos 2 e 3 para criar e iniciar as interfaces de TCP/IP na partição A e na partição B.

| Estas interfaces são usadas para a Ethernet virtual. Use os endereços de IP 10.1.10.1 e 10.1.10.2 para estas interfaces e a máscara de sub-rede 255.255.255.0.

| Considerações de Ethernet virtual

| Pode usar a Ethernet virtual como alternativa à utilização de uma placa de rede para comunicação entre partições. Permite estabelecer comunicações de alta velocidade entre partições lógicas sem adquirir hardware adicional. Para cada uma das 16 portas activadas, o sistema cria uma porta de comunicações Ethernet virtual, como por exemplo CMNxx com um tipo de recurso 268C. As partições lógicas atribuídas à mesma rede local ficam depois disponíveis para comunicar através dessa ligação. Um sistema físico permite configurar até 16 redes locais virtuais diferentes. A Ethernet virtual faculta a mesma função que a utilização de um adaptador Ethernet de 1 Gb. As redes locais de token Ring ou de Ethernet de 10 Mbps e 100 Mbps não são suportadas com a Ethernet virtual.

| A Ethernet virtual é uma solução económica de funcionamento em rede que proporciona grandes benefícios:



- | • Económica: não é necessário hardware de funcionamento em rede adicional, em princípio. Pode adicionar partições ao servidor e comunicar com uma rede local externa sem instalar placas de rede local físicas adicionais. Se o actual servidor tiver poucas ranhuras de placa disponíveis onde instalar placas de rede local adicionais, a utilização da Ethernet virtual oferece a capacidade de trabalhar com partições anexas à rede local sem ser necessário actualizar o servidor.
- | • Flexível: é possível configurar um máximo de 16 ligações distintas, o que permite a configuração de caminhos de comunicação selectivos entre partições. Para maior flexibilidade, o modelo de configuração permite que as partições lógicas implementem tanto uma Ethernet virtual como uma ligação a uma rede local física. Trata-se de uma função desejável quando se usa uma partição Linux para servir de sistema central a uma aplicação com firewall.
- | • Rápida: a Ethernet virtual emula uma ligação Ethernet de 1 Gb e faculta um método de comunicação entre partições rápido e conveniente. Destaca-se assim a oportunidade de integrar aplicações separadas executadas em partições lógicas diferentes.
- | • Versátil: independentemente das partições serem executadas em OS/400 ou Linux, podem estar todas ligadas à mesma Ethernet virtual.
- | • Congestionamento reduzido: ao utilizar a Ethernet virtual para comunicação entre partições, o tráfego de comunicações fica reduzido na rede local externa. No caso da Ethernet, a qual é uma norma

- | baseada em colisão, esta vantagem ajudará certamente a impedir uma degradação da qualidade do
- | serviço para com os outros utilizadores da rede local.
- | <<



Capítulo 9. Informações relacionadas para a configuração de TCP/IP

Agora que o seu servidor está pronto para funcionar, poderá perguntar-se "Que mais posso fazer com o meu servidor?" Segue-se uma lista dos manuais e Redbooks da IBM (em formato PDF) e o tópico do Centro de Informações que está relacionado com o tópico de configuração de TCP/IP. Pode ver ou imprimir os ficheiros PDF. Utilize as seguintes referências para beneficiar ao máximo do TCP/IP no servidor iSeries:




Manuais

- **TCP/IP Configuration and Reference**  (592 KB)
Este manual inclui informações sobre configuração de TCP/IP (Transmission Control Protocol/Internet Protocol), funcionamento e gestão da rede.
- **Tips and Tools for Securing your iSeries**  (1 MB)
Este manual inclui recomendações básicas sobre a utilização das funções de segurança do iSeries para proteger o servidor e as operações associadas.

Redbooks

- **TCP/IP Tutorial and Technical Overview**  (7 MB)
Este redbook fornece informações sobre os conceitos básicos de TCP/IP.
- **TCP/IP for AS/400: More Cool Things Than Ever**  (9 MB)
Este redbook inclui uma lista extensiva de aplicações e serviços comuns de TCP/IP.

IPv6


- **The Internet Engineering Task Force (IETF)** (<http://www.ietf.cnri.reston.va.us/>) 
Conheça o grupo de indivíduos que desenvolveu o protocolo Internet, incluindo o IPv6.
- **IP Version 6 (IPv6)** (<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 
Saiba onde encontrar especificações actuais do IPv6 e referências a várias fontes sobre o IPv6.
- **IPv6 Forum**(<http://www.ipv6forum.com/>) 
Saiba onde encontrar artigos noticiosos e acontecimentos que comunicam os desenvolvimentos mais recentes do IPv6.

Outras informações

- **TCP/IP**
Este tópico contém informações sobre aplicações e serviços de TCP/IP para além do âmbito da configuração.

Para guardar um ficheiro PDF na estação de trabalho para posterior visualização ou impressão:

1. Faça clique com o botão direito do rato sobre o PDF no browser (faça clique com o botão direito do rato sobre a ligação acima).
2. Clique em **Save Target As...**
3. Selecciona o directório no qual deseja guardar o ficheiro PDF.
4. Clique em **Save**.

Se necessitar do Adobe Acrobat Reader para ver ou imprimir estes PDFs, pode descarregar uma cópia a partir do sítio na Web da Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Parte 2. Apêndices

Apêndice. Avisos

Estas informações foram desenvolvidas para produtos e serviços disponibilizados nos E.U.A.

A IBM poderá não disponibilizar os produtos, serviços ou funções mencionados neste documento em outros países. Consulte o representante local da IBM para informações sobre produtos e serviços actualmente disponíveis na sua área. As referências a um produto, programa ou serviço da IBM não implicam que só se deva utilizar esse produto, programa ou serviço da IBM. Qualquer produto, programa ou serviço funcionalmente equivalente e que não infrinja os direitos de propriedade intelectual da IBM poderá ser utilizado. Todavia, é da responsabilidade do utilizador avaliar e verificar o funcionamento de qualquer produto, programa ou serviço alheio à IBM.

A IBM poderá ter patentes ou pedidos de patente pendentes relativos a temáticas abordadas neste documento. O facto deste documento ser disponibilizado ao utilizador não implica quaisquer licenças sobre essas patentes. Poderá enviar pedidos de licença, por escrito, para:

- | IBM Director of Licensing
- | IBM Corporation
- | North Castle Drive
- | Armonk, NY 10504-1785
- | U.S.A.

Para pedidos de licença relativos a informações de duplo byte (DBCS), contacte o IBM Intellectual Property Department do seu país ou envie pedidos por escrito para:

- | IBM World Trade Asia Corporation
- | Licensing
- | 2-31 Roppongi 3-chome, Minato-ku
- | Tokyo 106-0032, Japan

O parágrafo seguinte não se aplica ao Reino Unido nem a qualquer outro país onde as respectivas cláusulas sejam incompatíveis com a lei local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FACULTA ESTA PUBLICAÇÃO “TAL COMO ESTÁ” SEM GARANTIAS DE QUALQUER TIPO, EXPRESSAS OU IMPLÍCITAS, INCLUINDO A TÍTULO MERAMENTE EXEMPLIFICATIVO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRACÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A DETERMINADO FIM. Existem estados que não permitem a renúncia de garantias expressas ou impressas em certas transacções, de modo que estas cláusulas podem não ser aplicáveis ao utilizador.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. Estas informações são alteradas periodicamente; estas alterações serão incluídas em novas edições da publicação. A IBM poderá introduzir melhorias e/ou alterações em produto(s) e/ou programa(s) idos nesta publicação em qualquer altura e sem aviso prévio.

As referências contidas nestas informações relativas a sítios na Web alheios à IBM são facultadas a título de conveniência e não constituem de modo algum aprovação desses sítios na Web. Os materiais mencionados nesses sítios na Web não fazem parte dos materiais da IBM relativos ao presente produto, de modo que a utilização desses sítios na Web é da inteira responsabilidade do utilizador.

- | A IBM poderá utilizar ou distribuir informações facultadas pelo utilizador, no todo ou em parte, da forma que entender apropriada sem incorrer em qualquer obrigação para com o utilizador.

Os titulares de licenças deste programa que pretendam obter informações acerca do mesmo no intuito de fomentar: (i) intercâmbio de informação entre programas criados independentemente e outros programas (incluindo o presente) e (ii) a utilização mútua da informação trocada, devem contactar:

- | IBM Corporation
- | Software Interoperability Coordinator, Department 49XA
- | 3605 Highway 52 N
- | Rochester, MN 55901
- | U.S.A.

As ditas informações poderão ser disponibilizadas, sujeitas a termos e condições, incluindo em alguns casos o pagamento de uma taxa.

- | O programa licenciado descrito nestas informações e todo o material licenciado disponível para o mesmo são facultados pela IBM nos termos do IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code ou qualquer acordo equivalente entre as partes.

Quaisquer dados sobre rendimento contidos neste documento foram determinados num ambiente controlado. Por conseguinte, os resultados obtidos noutros sistemas operativos podem variar de forma significativa. Algumas medições podem ter sido efectuadas em sistemas ao nível da programação e não existe qualquer garantia de que os resultados venham a ser os mesmos em sistemas disponíveis no geral. Além do mais, algumas medições podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os utilizadores deste documento devem verificar os dados que se aplicam ao ambiente específico com que trabalham.

As informações relativas a produtos alheios à IBM foram obtidas junto dos fornecedores desses produtos, dos anúncios de publicidade dos mesmos ou de outras fontes disponíveis publicamente. A IBM não testou tais produtos e não pode confirmar a exactidão do desempenho, a compatibilidade ou outras alegações relativas a produtos que lhe são alheios. Quaisquer perguntas sobre as capacidades de produtos alheios à IBM deverão ser endereçadas aos fornecedores desses produtos.

Todas as instruções relativas a projectos e intenções futuras da IBM estão sujeitas a alteração ou eliminação sem aviso prévio e representam meramente metas e objectivos.

Estas informações contêm exemplos de dados e relatórios utilizados em operações empresariais diárias. No intuito de as ilustrar o mais integralmente possível, os exemplos incluem nomes de pessoas, empresas, marcas e produtos. Todos estes nomes são fictícios, de modo que qualquer semelhança com nomes e moradas de empresas reais será mera coincidência.

Se consultar estas informações em formato electrónico, as fotografias e ilustrações a cores poderão não ser apresentadas.

Marcas Registadas

Os termos que se seguem são marcas registadas da International Business Machines Corporation nos Estados Unidos e/ou noutros países:

AS/400
e(logo)server
eServer
IBM
iSeries
OS/400
Redbooks

Microsoft, Windows, Windows NT e o logotipo Windows são marcas registadas da Microsoft Corporation nos Estados Unidos e/ou outros países.

Outros nomes de empresas, produtos e serviços podem ser marca registrada de terceiros.

Termos e condições para descarregar e imprimir publicações

- | As permissões para uso das informações seleccionadas para descarregamento são concedidas sujeitas aos seguintes termos e condições e à indicação de aceitação dos mesmos por parte do utilizador.
 - | **Uso Pessoal:** poderá reproduzir estas informações para uso pessoal e não comercial desde que todos os avisos de propriedade sejam preservados. Não poderá distribuir, exibir ou fazer trabalhos derivados destas informações, no todo ou em parte, sem o consentimento expresso da IBM.
 - | **Uso Comercial:** poderá reproduzir, distribuir e exibir estas informações somente na empresa a que pertencer e desde que todos os avisos de propriedade sejam preservados. Não poderá fazer trabalhos derivados destas informações, nem reproduzir, distribuir ou exibir estas informações, no todo ou em parte, fora da empresa a que pertencer, sem o consentimento expresso da IBM.
 - | Salvo no expressamente concedido nesta permissão, não se concedem outras permissões, licenças ou direitos, expressas ou implícitas, relativamente às informações ou quaisquer dados, software ou demais propriedade intelectual nela contida.
 - | A IBM reserva-se o direito de retirar as permissões concedidas neste documento sempre que, no seu entender, o uso das informações seja prejudicial aos seus interesses ou, conforme determinação da IBM, as instruções supra mencionadas não sejam devidamente respeitadas.
 - | Não tem autorização para descarregar, exportar ou reexportar estas informações salvo em conformidade com leis e regulamentos aplicáveis, incluindo leis e regulamentos sobre exportação dos Estados Unidos. A IBM NÃO GARANTE O CONTEÚDO DESTAS INFORMAÇÕES. AS INFORMAÇÕES SÃO DISPONIBILIZADAS "TAL COMO ESTÃO" E SEM GARANTIAS DE QUALQUER TIPO, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, A TÍTULO MERAMENTE EXEMPLIFICATIVO, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO FIM.
- Todos os materiais estão vinculados pelos direitos de autor da IBM Corporation.
- | Ao descarregar ou imprimir estas informações deste sítio, constitui aceitação destes termos e condições por parte do utilizador.



Impresso em Portugal