System i

Utilização em rede de encaminhamento de TCP/IP e equilíbrio de volume de trabalho

Versão 6 Edição 1

System i

Utilização em rede de encaminhamento de TCP/IP e equilíbrio de volume de trabalho

Versão 6 Edição 1

Nota

Antes de usar estas informações e o produto a que se referem, leia as informações em "Avisos", na página 43.

Esta edição aplica-se à versão 6, edição 1, modificação 0 do IBM i5/OS (número de produto 5761-SS1) e a todas as edições e modificações subsequentes até indicação em contrário em novas edições. Esta edição não é executada em todos os modelos reduced instruction set computer (RISC) nem é executada em modelos CISC.

Índice

Encaminhamento e equilíbrio do volume de trabalho do TCP/IP

Pode encaminhar e equilibrar o tráfego de TCP/IP do sistema utilizando as respectivas capacidades integradas de encaminhamento para eliminar a necessidade de um encaminhador externo.

Os métodos de encaminhamento e de equilíbrio do volume de trabalho, bem como as informações de segundo plano irão ajudar a compreender as opções disponíveis para utilização no sistema. Cada método é descrito através de uma imagem, por forma a que seja possível visualizar como as ligações são efectuadas. Estes métodos não incluem instruções sobre como configurar as técnicas de encaminhamento. Esta colecção de tópico incide principalmente sobre os princípios e os conceitos de encaminhamento que são necessários saber para que possa tirar o melhor rendimento do sistema.

Porque estes métodos são importantes para o utilizador

As técnicas utilizadas nestes métodos podem reduzir os custos globais das ligações, pois pode utilizar menos encaminhadores e servidores externos. Ao utilizar estes métodos de encaminhamento poderá libertar endereços de IP, pois irá geri-los de uma forma mais eficaz. Ao ler os métodos de equilíbrio do volume de trabalho, terá um melhor rendimento global do sistema, equilibrando o volume de trabalho das comunicações no sistema.

Novidade da V6R1

Inteire-se de informações novas ou significativamente alteradas relativas à colecção do tópico Encaminhamento e equilíbrio de volume de trabalho de TCP/IP.

Novo protocolo de encaminhamento suportado

O sistema operativo i5/OS foi expandido para suportar o protocolo de encaminhamento Open Shortest Path First - Abrir primeiro caminho mais curto (OSPF). *Open Shortest Path First - Abrir primeiro caminho mais curto* (OSPF) constitui um protocolo de encaminhamento de estados de ligação no qual encaminhadores ou sistemas dentro da mesma área mantêm uma base de dados de estados de ligação idêntica que descreve a topologia da área.

Melhorias de IP virtual

As melhorias de IP virtual que afectam a colecção do tópico Encaminhamento e equilíbrio de volume de trabalho de TCP/IP são as seguintes:

- Foi expandido o suporte de endereços de IP virtual para incluir endereços de IPv6.
- Uma interface de Point-to-Point Protocol (PPP) ou uma interface de Layer Two Tunneling Protocol (L2TP) podem utilizar um endereço de IP virtual como endereço de IP local para facultar tolerância de falhas a ligações remotas.
- Pode configurar um ARP de proxy de IP virtual enquanto a interface de IP virtual estiver activa.

Estas melhorias de IPv6 são descritas nos tópicos “Encaminhamento com IP virtual” na página 20 e “Tolerância a falhas” na página 22.

Novo método de equilíbrio de volume documentado

Apesar da utilização do IP virtual e do ARP de proxy como método de equilíbrio de volume não seja uma novidade em V6R1, este método de equilíbrio de volume não estava documentado neste manual. Foi

adicionado um tópico “Equilíbrio de volume utilizando o IP virtual e o ARP de proxy” na página 34 para apresentar este método de equilíbrio de volume.

Como ver as novidades ou as alterações

Para ajudar o utilizador a ver onde foram introduzidas alterações técnicas, o centro de informações utiliza:

- A imagem » para assinalar onde começam informações novas ou alteradas.
- A imagem « para assinalar onde acabam informações novas ou alteradas.

Em ficheiros PDF, poderá ver barras verticais de revisão (|) na margem esquerda de informações novas ou alteradas.

Para localizar outras informações sobre novidades ou alterações desta edição, consulte o Memorando para utilizadores.

Ficheiro PDF para encaminhamento e equilíbrio do volume de trabalho do TCP/IP

Pode ver e imprimir um ficheiro PDF destas informações.

Para ver ou descarregar uma versão em PDF deste documento, seleccione Encaminhamento e equilíbrio do volume de trabalho de TCP/IP (cerca de 1,40 MB).

Guardar ficheiros PDF

Para guardar um ficheiro PDF na estação de trabalho para visualizá-lo ou imprimi-lo:

1. Faça clique com o botão direito do rato na ligação do PDF no navegador.
2. Faça clique na opção que guarda localmente o PDF.
3. Navegue para o directório no qual pretende guardar o PDF.
4. Faça clique em **Guardar**.

Descarregar o Adobe Reader

Necessita de ter o Adobe Reader instalado no sistema para ver e imprimir estes PDFs. Pode descarregar uma cópia grátis no sítio da Web da Adobe (www.adobe.com/products/acrobat/readstep.html) .

Referências relacionadas

“Informações relacionadas sobre o encaminhamento e equilíbrio do volume de trabalho do TCP/IP” na página 40
Outras colecções de tópicos do centro de informações contêm informações relacionadas com a colecção do tópico Encaminhamento e equilíbrio do volume de trabalho do TCP/IP.

Funções de encaminhamento do TCP/IP por edição

Antes de pensar utilizar uma função de encaminhamento, o utilizador deve certificar-se de que dispõe da edição correcta do sistema para suportar a função que pretende executar.

V3R1: Reenvio de pacotes baseado no encaminhamento estático.

V3R7/V3R2: Serial Line Internet Protocol (SLIP), encaminhamento do Address Resolution Protocol (ARP) de proxy e suporte de rede com ligação não numerada

V4R1: Dynamic Routing Information Protocol Versão 1 (RIPv1).

V4R2: Dynamic Routing Information Protocol Versão 2 (RIPv2), criação de sub-redes transparentes e equilíbrio de volume baseado no encaminhamento duplicado

V4R3: Endereços de IP virtuais, criação de máscaras de endereços de IP, conversão de endereços de rede (NAT) e Encaminhamento Entre-Domínios sem Classes (CIDR)

V4R4: IP no OptiConnect

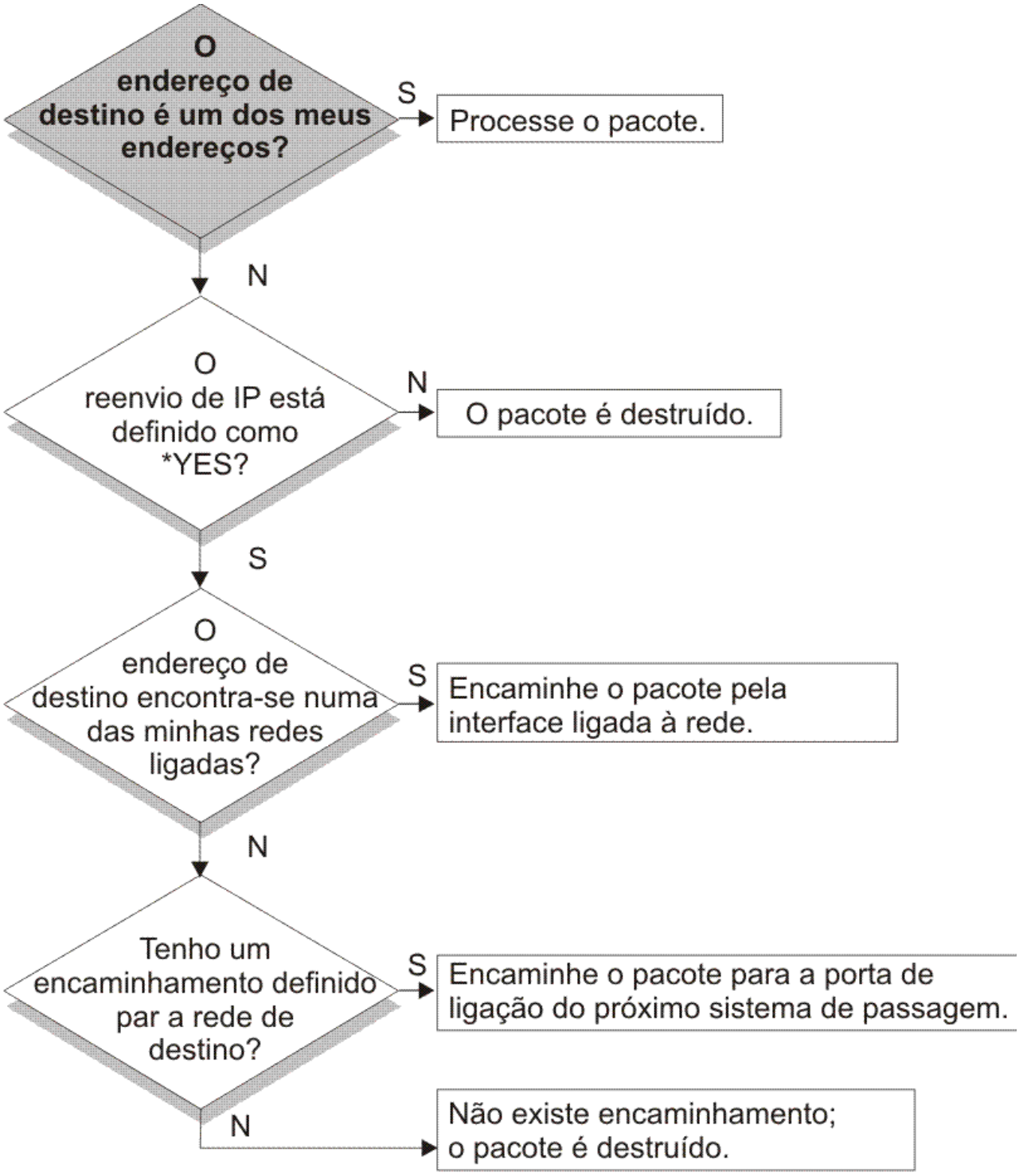
V5R4: Lista de interfaces preferenciais

| **V6R1:** Suporte de protocolo de encaminhamento Open Shortest Path First - Abrir primeiro o caminho
| mais curto (OSPF) e de endereço de IP virtual para endereços de IPv6

Processamento de pacotes

Ter uma boa compreensão do processamento de pacotes ajuda a decidir a forma como implementar as funções de encaminhamento.

O seguinte fluxograma simplificado mostra o processo lógico que ocorre quando um pacote IP (datagrama) chega a sistema operativo i5/OS. O fluxo real poderá ser diferente, mas o resultado deverá ser o mesmo. O processo lógico seguinte descreve apenas as situações de processamento de pacotes assumidas. Se forem utilizadas técnicas de encaminhamento avançadas, o processamento de pacotes poderá ser ligeiramente diferente.



Primeiro, o endereço de destino no cabeçalho IP é comparado com todos os endereços definidos no sistema. Se for determinado que o pacote é destinado ao sistema, o pacote passa da pilha IP para um nível de software superior, tal como o TCP, e depois para a aplicação que faz a recepção na porta de destino.

Se o pacote não for aceite localmente, a verificação seguinte é efectuada ao atributo de encaminhamento IP. Se o encaminhamento IP estiver definido para *YES, então o sistema está configurado para encaminhar pacotes como um encaminhador. Se o atributo estiver definido para *NO nos atributos TCP/IP ou no perfil PPP, o pacote é destruído.

O endereço de destino do pacote é comparado com todos os encaminhamentos *DIRECT conhecidos pelo sistema. Esta comparação é realizada através da inclusão do endereço de destino do pacote na máscara de sub-rede especificada nas entradas de encaminhamento *DIRECT das interfaces definidas, para determinar se o pacote está destinado a uma rede directamente ligada a este sistema. A verificação é realizada a partir dos encaminhamentos mais específicos até aos menos específicos.

Em seguida, se o i5/OS não estiver directamente ligado ao sistema central remoto, é verificada a tabela de encaminhamento. Esta verificação é realizada a partir do sistema central mais específico (máscara de sub-rede 255.255.255.255) até ao encaminhamento menos específico (máscara de sub-rede 0.0.0.0). Se for encontrado um encaminhamento, o pacote é reencaminhado para a porta de ligação do sistema de passagem seguinte.

O último ponto do fluxograma mostra que, se não for encontrada uma entrada de encaminhamento correspondente, o pacote é destruído.

Regras gerais de encaminhamento

Estas regras aplicam-se a TCP/IP em geral e a TCP/IP no sistema operativo i5/OS.

Para gerir pacotes no sistema, deverá ter em conta estas regras à medida que implementa funções de encaminhamento no sistema. Estas regras podem ajudá-lo a saber o que acontece aos pacotes dentro do sistema e para onde é que poderão estar a ir. Como acontece com a maior parte das regras, existem algumas excepções.

- O sistema não possui um endereço de IP; apenas as interfaces possuem endereços de IP.

  Nota: Os endereços IP Virtuais (sem ligação) são atribuídos ao sistema.
- Geralmente, se o endereço de IP destino estiver definido no sistema, este irá processá-lo independentemente da interface em que vier um pacote.

  A excepção a esta situação acontece quando um endereço estiver associado a uma interface sem número ou se estiverem activas uma NAT de IP ou uma filtragem, podendo o pacote ser encaminhado ou rejeitado.
- O endereço de IP e a máscara definem o endereço da rede ligada.
- O encaminhamento para fora de um sistema é seleccionado com base no endereço de rede ligado a uma interface. A selecção de um encaminhamento tem como base os seguintes itens:
  - Ordem de procura do grupo de encaminhamentos: encaminhamentos directos, encaminhamentos de sub-rede e, por fim, encaminhamentos assumidos.
  - Dentro de um grupo, é escolhido o encaminhamento com a máscara de sub-rede mais específica.
  - Os encaminhamentos com a mesma especificação ficam sujeitos à ordem da lista ou às técnicas de equilíbrio de volume.
  - Os encaminhamentos podem ser adicionados manual ou dinamicamente pelo sistema.

Métodos de conectividade de encaminhamento

O encaminhamento está relacionado com o caminho que o tráfego de rede segue, desde a origem até ao destino, e com a forma como o referido caminho está ligado.

Encaminhamento com ligações ponto a ponto

Utilizando as ligações ponto a ponto, pode enviar dados do sistema local para um sistema remoto ou de uma rede local para uma rede remota.

De modo geral, as ligações ponto a ponto são utilizadas para ligar dois sistemas numa rede alargada (WAN). É possível utilizar uma ligação ponto a ponto para deslocar dados do sistema local para um sistema remoto ou para deslocar dados de uma rede local para uma rede remota. Não se deve confundir ligações ponto a ponto com o Point-to-Point Protocol. O Point-to-Point Protocol (PPP) é um tipo de ligação ponto a ponto, geralmente utilizado para ligar um computador à Internet. Consulte Ligações PPP para obter mais informações sobre como configurar e gerir ligações PPP.

É possível utilizar ligações ponto a ponto em linhas de acesso de marcação, linhas não comutadas e outros tipos de redes, tais como retransmissão de estruturas. Existem duas formas de configurar os endereços de IP para uma ligação ponto a ponto: uma ligação numerada e uma ligação não numerada. Como as designações deixam entender, uma ligação numerada possui um endereço de IP exclusivo definido para cada interface. Uma ligação não numerada não utiliza endereços de IP adicionais para uma ligação.

Ligações à rede numeradas:

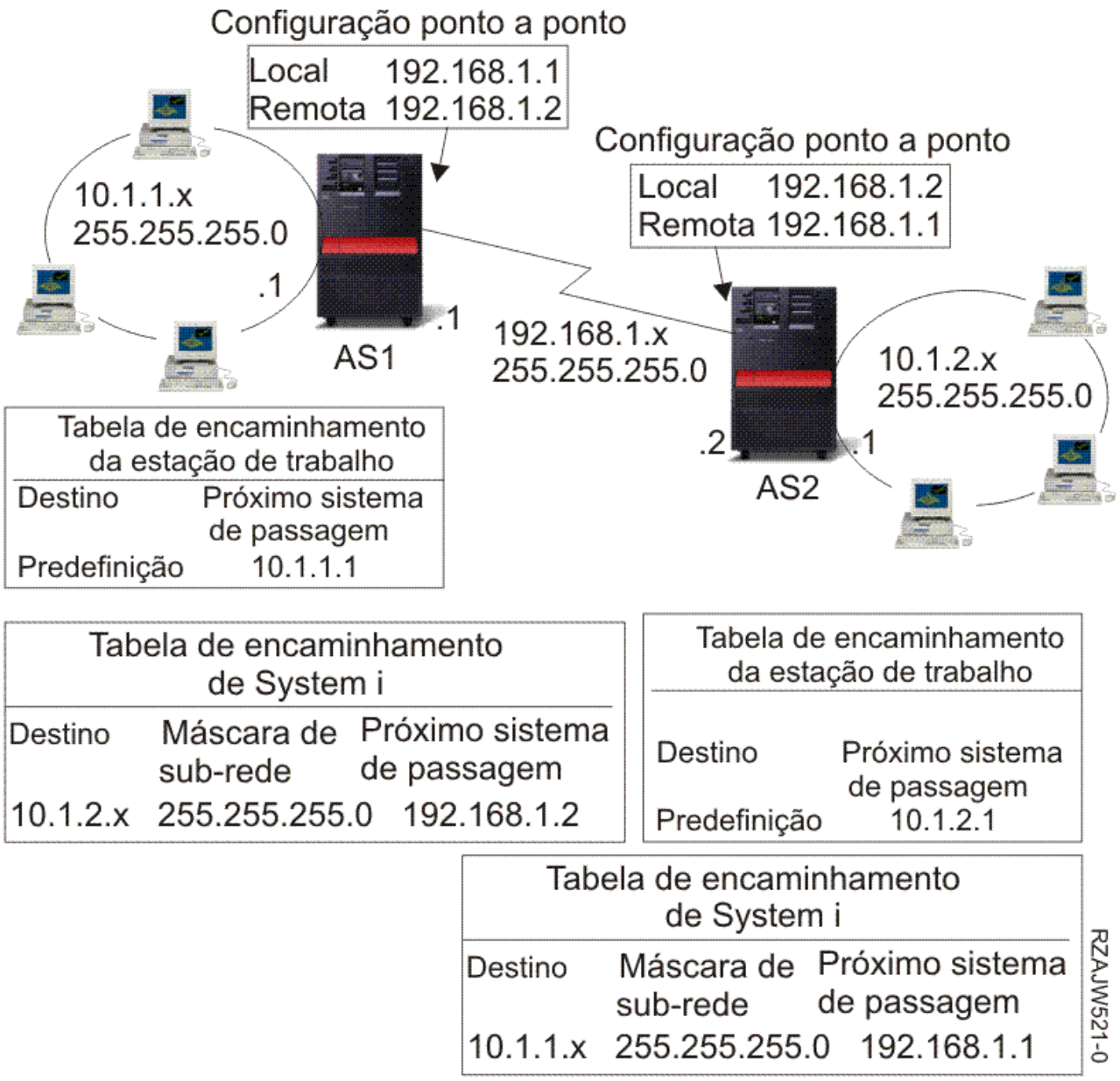
À primeira vista, parece que a forma mais simples de configurar uma ligação ponto a ponto é através da utilização de uma ligação numerada. Uma ligação numerada é uma definição ponto a ponto que possui um endereço de IP exclusivo definido em cada um dos extremos da ligação.

Seguem-se alguns dos pontos a ter em conta para a utilização de uma ligação ponto a ponto numerada:

- Cada um dos extremos da ligação possui um endereço de IP exclusivo.
- Devem ser adicionadas instruções de encaminhamento ao sistema, para fazer fluir o tráfego para o sistema remoto.
- Os endereços da ligação ponto a ponto devem ser geridos pelo administrador da rede.
- Os endereços são apenas utilizados para ligar dois sistemas.

Quando cada ligação ponto a ponto estiver definida no sistema, deve ser criada uma entrada de encaminhamento em cada extremo, para descrever a forma como chegar a qualquer rede do outro extremo da ligação. O processo de selecção de encaminhamento no sistema depende da existência de um endereço de IP para cada interface. Estes endereços e encaminhamentos devem ser geridos pelo administrador da rede. Numa rede de pequenas dimensões, estes endereços são facilmente controlados e não utilizam muitos endereços adicionais. Contudo, numa rede de maiores dimensões, poderá ser necessária uma sub-rede de endereços inteira, apenas para definir uma interface em cada extremo.

A figura seguinte mostra uma ligação de rede numerada entre duas plataformas System i. Não é necessária uma entrada de encaminhamento, se apenas pretender comunicar do AS1 para o AS2. Se pretender comunicar com sistemas da rede remota (10.1.2.x), a entrada de encaminhamento incluída na imagem deve ser adicionada a cada sistema. Esta necessidade advém do facto de a rede remota, 10.1.2.x, fazer parte da ligação 192.168.1.x.



Ligações de rede não numeradas

Uma ligação não numerada é um método mais complexo de definir uma ligação ponto a ponto do que uma ligação numerada. No entanto, a ligação não numerada poderá ser considerada uma forma mais simples e melhor de gerir uma rede.

O processo de selecção de encaminhamento no i5/OS depende da existência de um endereço de IP para cada interface. Numa ligação não numerada, a interface ponto a ponto não possui um endereço exclusivo. O endereço de IP da interface do sistema para uma ligação não numerada é, na verdade, o endereço de IP do sistema remoto.

Seguem-se alguns dos pontos a ter em conta para a utilização de uma ligação não numerada:

- A interface ponto a ponto possui um endereço que parece estar na rede remota.
- Não são necessárias instruções de encaminhamento neste sistema.
- A administração da rede é simplificada pela não utilização de endereços de IP para a ligação.

No exemplo seguinte, o AS1 parece ter uma interface na rede 10.1.4.x e o AS2 parece ter uma interface na rede 10.1.3.x. O AS1 está ligado à rede LAN 10.1.3.x com um endereço de 10.1.3.1. Isto permite ao AS1 comunicar, de forma directa, com qualquer sistema da rede 10.1.3.x.

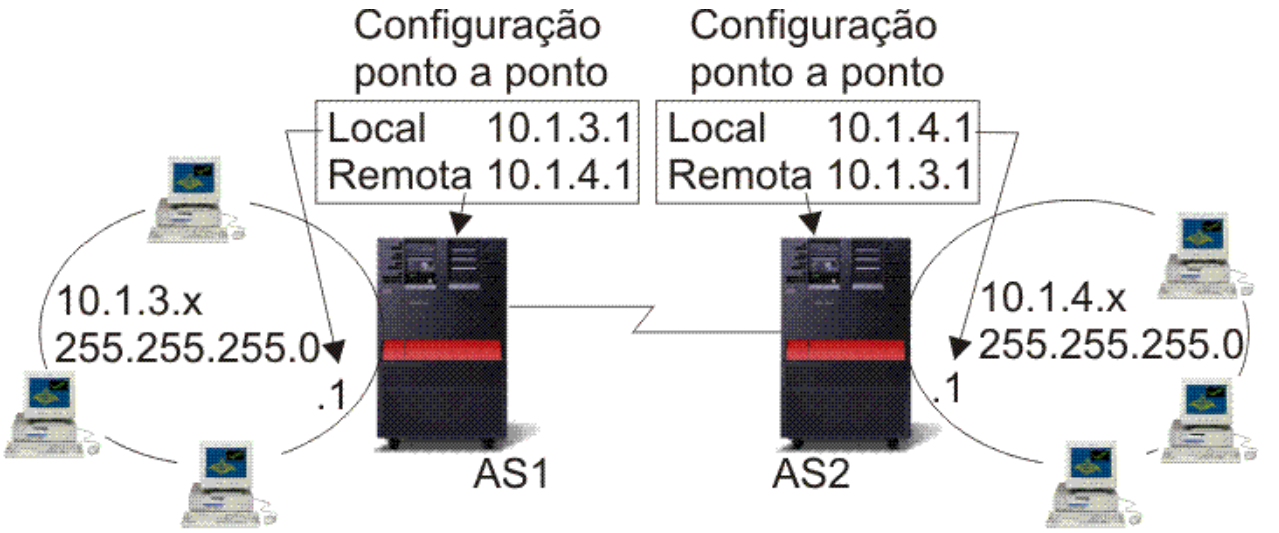


Tabela de encaminhamento da estação de trabalho	
Destino	Próximo sistema de passagem
Predefinição	10.1.3.1

Tabela de encaminhamento da estação de trabalho	
Destino	Próximo sistema de passagem
Predefinição	10.1.3.1

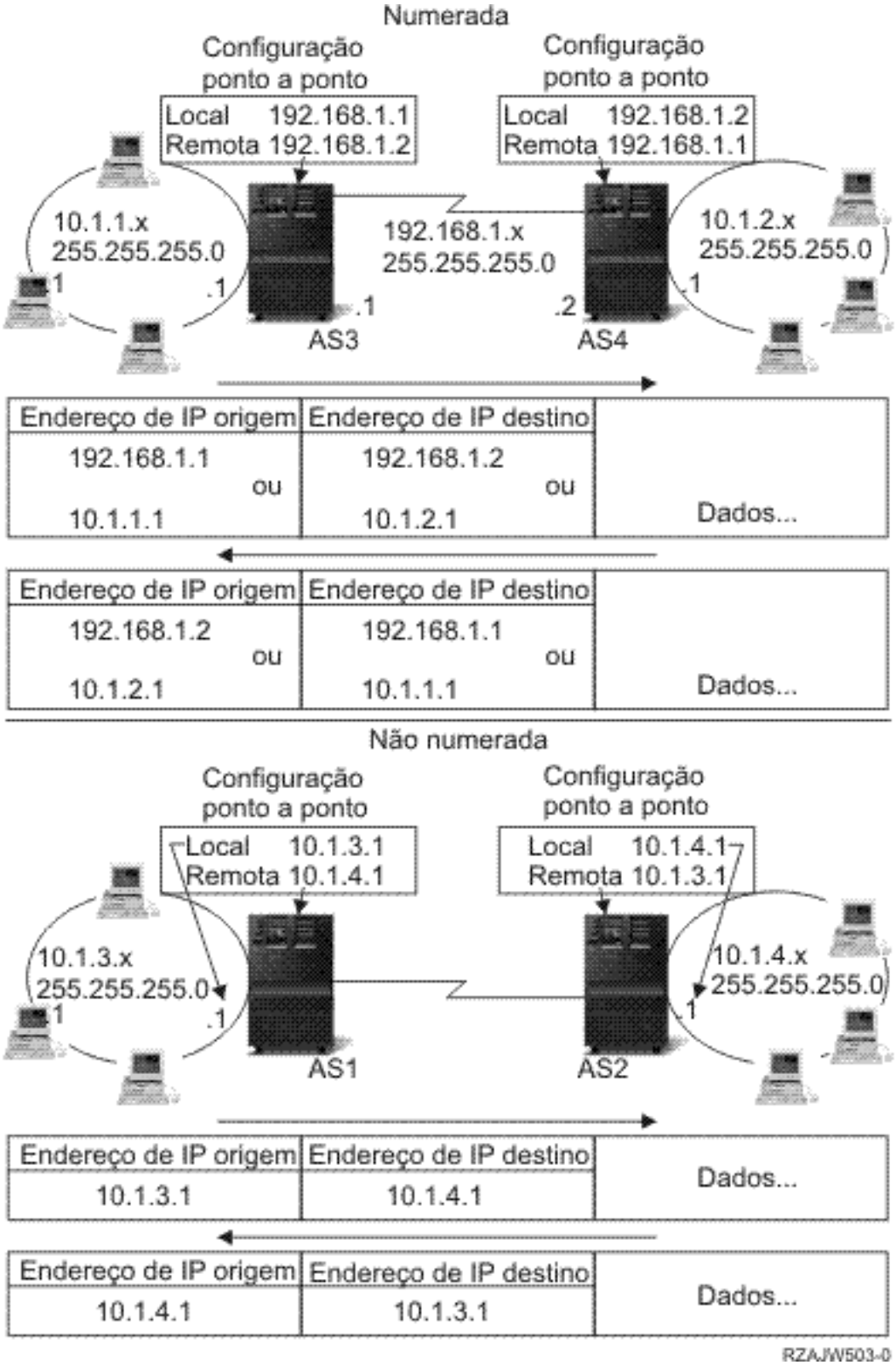
RZAJW502-0

O AS2 também é mostrado no exemplo. O AS2 está ligado à rede LAN 10.1.4.x com um endereço de 10.1.4.1. Isto permite ao AS2 comunicar, de forma directa, com qualquer sistema da rede 10.1.4.x. Cada um dos sistemas (AS1 e AS2) adiciona o endereço remoto à respectiva tabela de encaminhamento como uma interface local. O endereço é tratado de forma especial, de modo a que os pacotes destinados a esse endereço não sejam processados localmente. Os pacotes para o endereço remoto serão colocados na interface e transportados para o outro extremo da ligação. Quando o pacote chega ao outro extremo da ligação, é utilizado um processamento de pacotes normal.

Agora, é necessário ligar o AS1 à rede 10.1.4.x e o AS2 à rede 10.1.3.x. Se estes dois sistemas estivessem na mesma sala, poderia adicionar um adaptador de rede local (LAN) a cada sistema e ligar a nova interface à rede local correcta. Se esta acção fosse efectuada, não seria necessário adicionar entradas de encaminhamento ao AS1 e ao AS2. Neste exemplo, porém, os sistemas estão em cidades diferentes, pelo que deve ser utilizada uma ligação ponto a ponto. Apesar de ser utilizada uma ligação ponto a ponto, será melhor evitar adicionar entradas de encaminhamento. Ao ser definida a ligação do Point-to-Point Protocol (PPP) como uma ligação não numerada, são alcançados os mesmos resultados que seriam obtidos se utilizasse adaptadores de redelocal, sem adicionar quaisquer entradas de encaminhamento ao sistema. Para fazê-lo, cada sistema pede emprestado o endereço de IP do sistema remoto para utilizar com a resolução de encaminhamento.

Carregamento de dados na ligação numerada em comparação com a ligação não numerada

A figura seguinte mostra os endereços que serão utilizados em ligações ponto a ponto numeradas e não numeradas. A parte superior da imagem mostra que, com a ligação numerada, o endereço de 192.168.1.2 ou 10.1.2.1 do sistema remoto poderia ser utilizado para atingir o sistema remoto. Isto acontece porque existe uma entrada de encaminhamento no AS3 que dirige os pacotes do 10.1.2.1 para o 192.168.1.2, como o próximo sistema de passagem. Os endereços utilizados no pacote de retorno são baseados no pacote recebido. A parte inferior da imagem mostra os endereços utilizados com uma ligação não numerada. O pacote de envio tem uma origem de 10.1.3.1 e um destino de 10.1.4.1. Não são necessárias entradas de encaminhamento em qualquer dos sistemas, pois estes possuem uma interface directa para a rede remota, através da utilização do endereço do sistema remoto da ligação ponto a ponto.



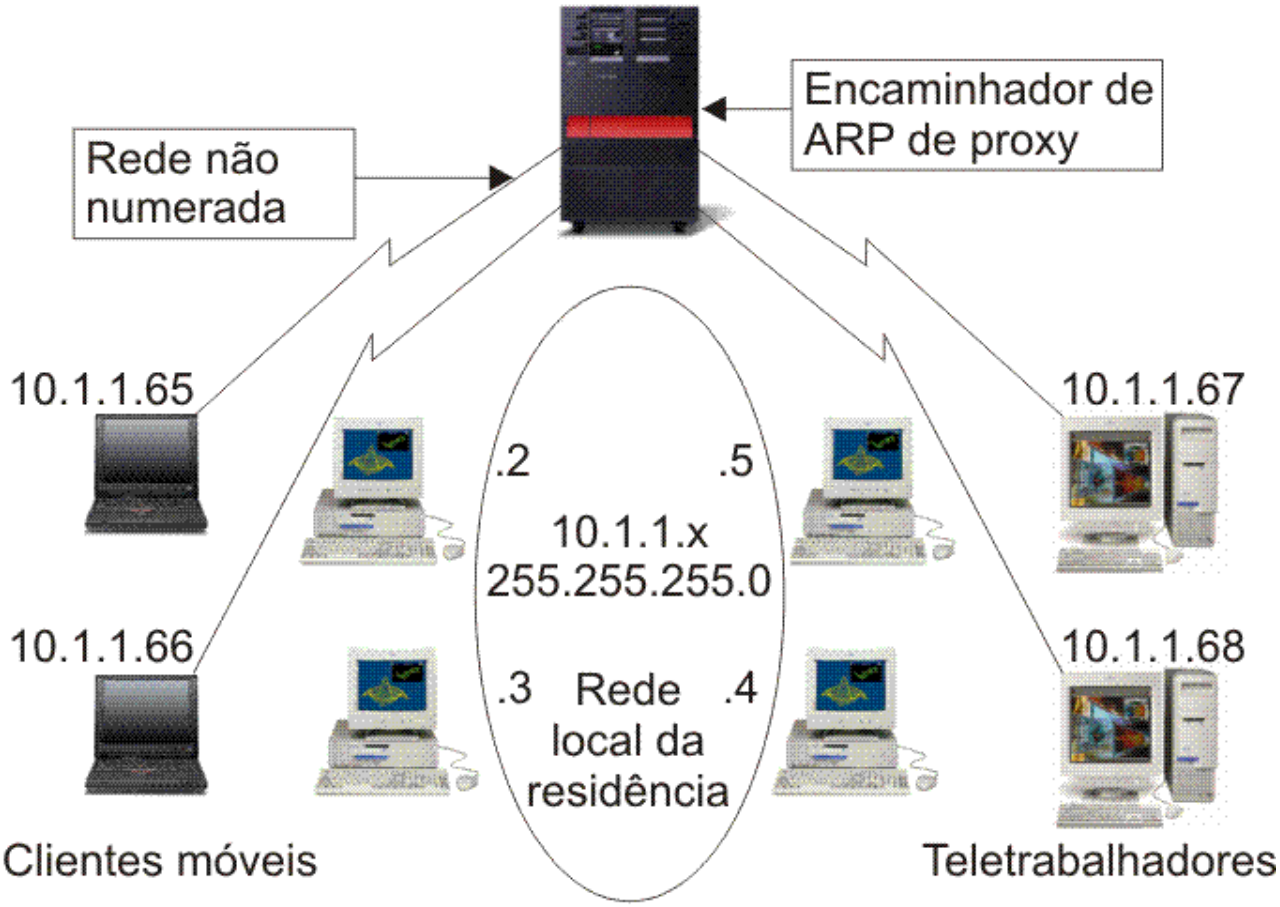
Conceitos relacionados

Ligações de PPP

Encaminhamento do Address Resolution Protocol de proxy

O Address Resolution Protocol (ARP) do proxy proporciona conectividade entre redes fisicamente separadas sem a criação de quaisquer redes lógicas novas e sem a actualização de quaisquer tabelas de encaminhamento. Este tópico contém uma descrição de sub-redes transparentes, que são uma extensão da técnica de encaminhamento de ARP do proxy.

O encaminhamento do ARP de proxy permite que redes separadas e fisicamente diferentes pareçam ser uma única rede lógica. Permite que sistemas que não estejam directamente ligados à rede local sejam apresentados a outros sistemas da rede local como se estivessem ligados. Isto é útil em situações de ligação por acesso telefónico, para fornecer ligações a toda a rede a partir de uma interface de acesso telefónico. A imagem seguinte apresenta uma situação possível. A ligação 10.1.1.x é a LAN da residência e as ligações de 10.1.1.65 a 10.1.1.68 são os sistemas remotos.



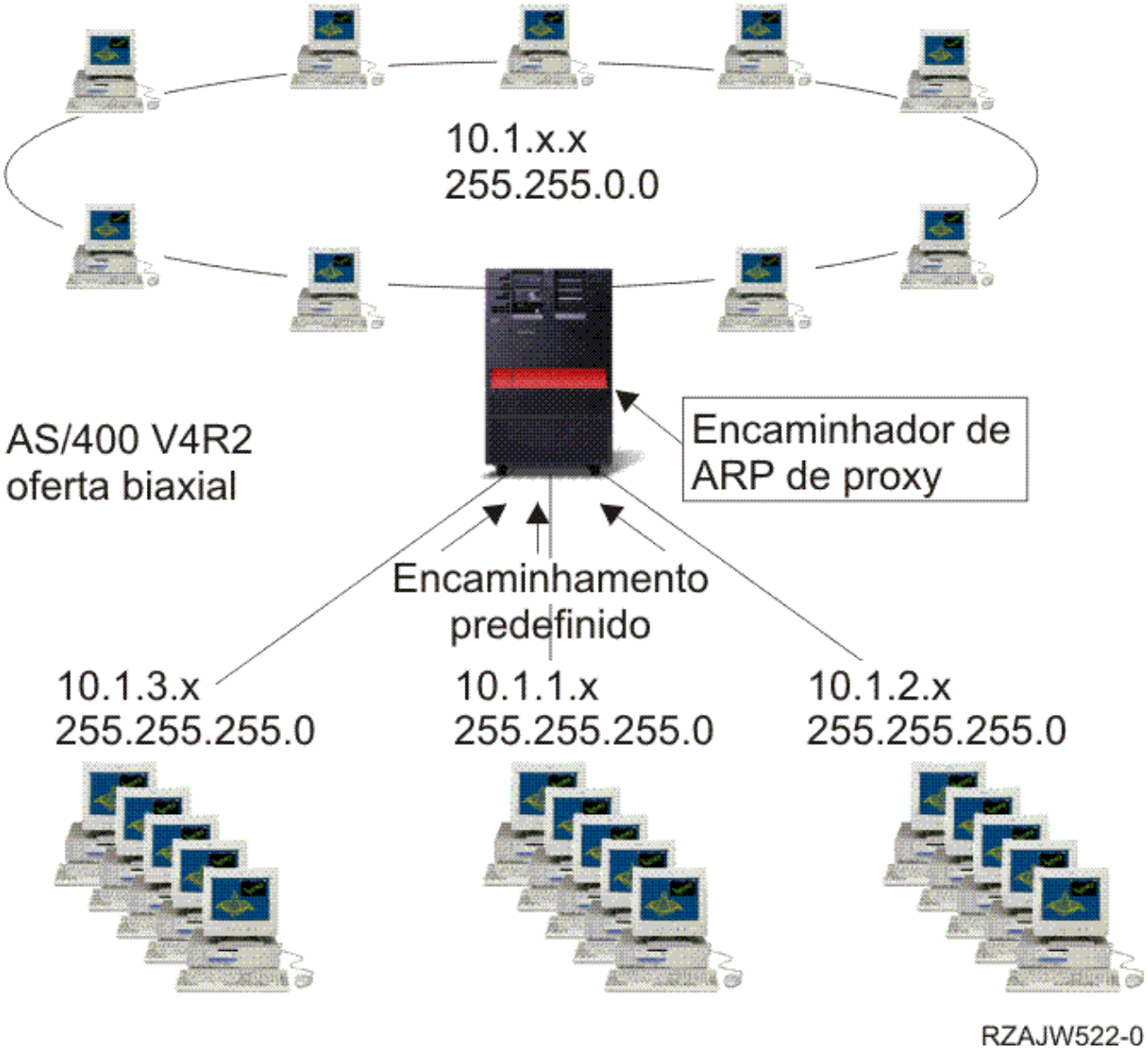
RZAJW500-0

Quando um sistema da LAN da residência (10.1.1.x) pretende enviar dados para um dos sistemas remotos, fará primeiro um pedido ARP. Trata-se de uma difusão efectuada para todos os sistemas ligados ao segmento da LAN para pedir o endereço do sistema de destino. Um sistema remotamente ligado não vê a difusão. Mas com o ARP de proxy, o sistema sabe quais os sistemas que estão remotamente ligados. Se o sistema receber um pedido ARP para um dos sistemas remotamente ligados, irá responder-lhe utilizando o respectivo endereço. O sistema recebe, então, os dados e reencaminha-os para o sistema remoto. Para que o reencaminhamento tenha lugar, o reencaminhamento IP deve estar definido para *YES. Se o sistema remoto não estiver ligado, o sistema não poderá responder ao pedido ARP e o sistema solicitador não poderá enviar os dados.

Sub-redes transparentes

As sub-redes podem ser utilizadas como forma de expandir o conceito de ARP de proxy. Pode utilizar sub-redes transparentes como um proxy para uma sub-rede completa ou intervalo de sistemas centrais. A criação de sub-redes visíveis permite que sejam atribuídos endereços do espaço de endereços da rede primária a redes intermédias.

As sub-redes visíveis funcionam para um único sistema central, de modo a que seja possível ligar a uma sub-rede inteira ou a um intervalo de sistemas centrais. Na figura seguinte, é possível ver que as sub-redes (10.1.1.x a 10.1.3.x) são endereços atribuídos que fazem parte do espaço de endereços da rede principal (10.1.x.x).



A função de sub-rede visível pode ser alargada para gerir as LANs reais localizadas remotamente. A criação de sub-redes visíveis em WANs faz com que as sub-redes remotas pareçam estar ligadas à rede local. Na figura anterior, três redes estão ligadas à rede local 10.1.x.x através da plataforma System i. Estas redes estão todas definidas utilizando uma máscara de sub-rede que as torna visíveis à rede local. O ARP do proxy responde a qualquer pedido ARP da rede local efectuado para sistemas nas sub-redes 10.1.1.x, 10.1.2.x e 10.1.3.x. Esta acção faz com que o tráfego da rede local seja encaminhado automaticamente para o sistema da rede local. Por sua vez, este sistema encaminha os dados para o sistema remoto correcto. O sistema remoto pode, então, processar os dados ou reencaminhá-los para o

sistema correcto da rede local remota. As estações de trabalho da LAN remota devem ter um encaminhamento assumido que aponte para o sistema remoto da respectiva rede como a primeira porta de ligação do sistema de passagem. As estações de trabalho da LAN local não necessitam de quaisquer entradas de encaminhamento adicionais, pois não são criadas redes lógicas novas.

Encaminhamento dinâmico

O encaminhamento dinâmico é um método de baixa manutenção que reconfigura automaticamente as tabelas de encaminhamento quando a rede é alterada.

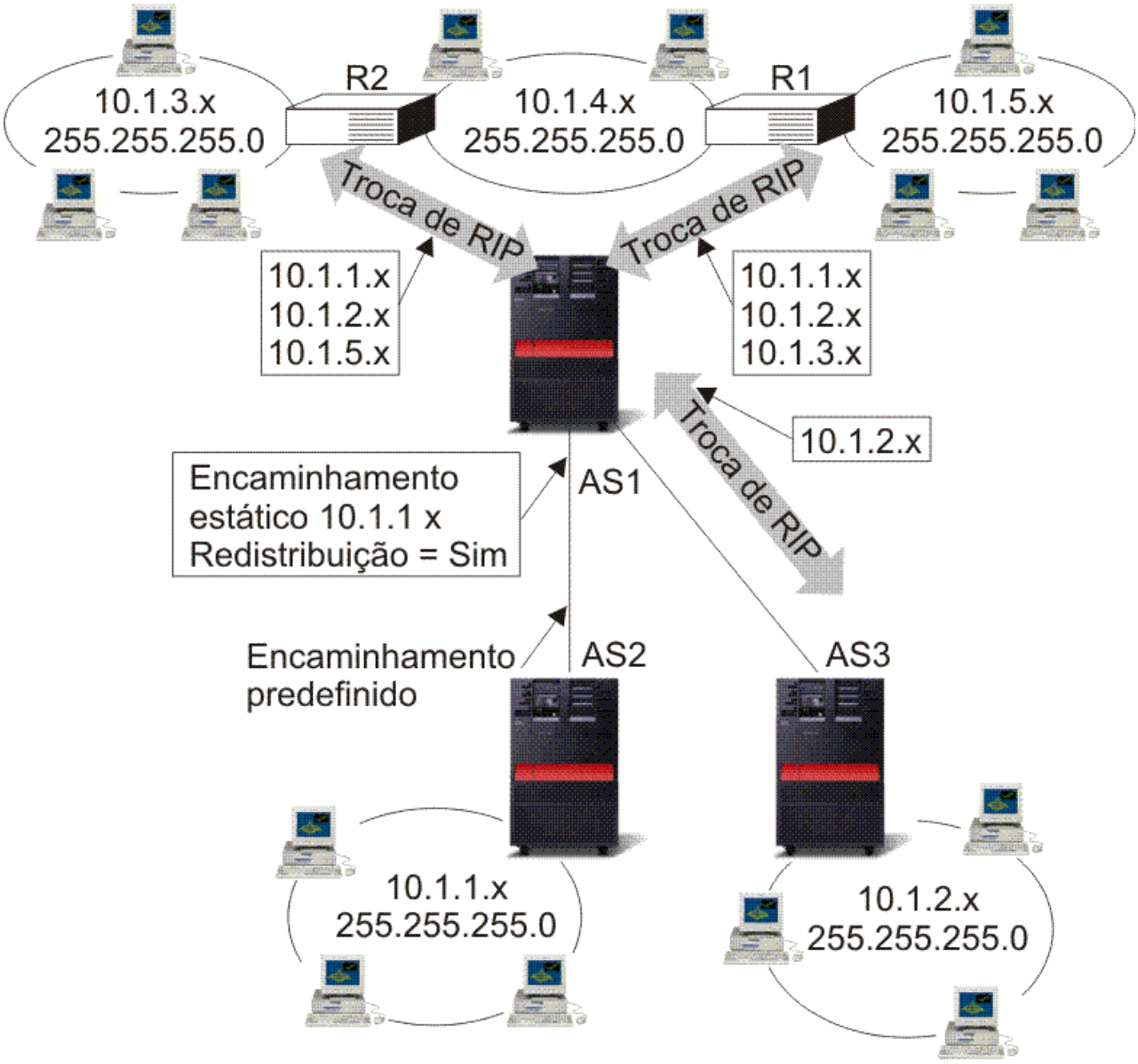
O encaminhamento dinâmico é fornecido pelos Interior Gateway Protocols (IGPs). O Protocolo de Informação de Encaminhamento (RIP) e o protocolo Open Shortest Path First - Abrir primeiro o caminho mais curto (OSPF) são os dois IGPs suportados pelo sistema operativo i5/OS.

Protocolo de Informação de Encaminhamento

O *Protocolo de Informação de Encaminhamento* (RIP) é um protocolo de encaminhamento baseado em vector de distância. Os encaminhadores que executem o protocolo baseado em vector de distância enviam todas ou uma parte das suas tabelas de encaminhamento em mensagens de actualização de encaminhamento aos sistemas vizinhos.

Pode utilizar o RIP para configurar os sistemas centrais como parte de uma rede de RIP. Este tipo de encaminhamento exige pouca manutenção, para além de reconfigurar automaticamente as tabelas de encaminhamento quando a rede é alterada ou pára. O RIPv2 foi adicionado ao produto System i, de modo a que seja possível enviar ou receber pacotes RIP para actualizar encaminhamentos em toda a rede.

Na figura seguinte, um encaminhamento estático é adicionado ao sistema central (AS1) que descreve a ligação à rede 10.1.1.x por intermédio de AS2. Trata-se de um encaminhamento estático (adicionado pelo administrador de rede) com a redistribuição de encaminhamentos definida para sim. Esta definição faz com que este encaminhamento seja partilhado por outros encaminhadores e sistemas, de modo a que, quando tiverem tráfego para 10.1.1.x, o encaminhem para a plataforma System i central (AS1). O AS2 tem o sistema encaminhado iniciado, de modo a que envie e receba informações RIP. Neste exemplo, o AS1 envia a mensagem referindo que o AS2 tem uma ligação directa ao 10.1.2.x.



O processo seguinte descreve o encaminhamento de tráfego da figura anterior.

- O AS1 recebe este pacote RIP do AS2 e processa-o. Se o AS1 não possuir um encaminhamento para 10.1.2.x, irá armazenar este encaminhamento. Se possuir um caminho para 10.1.2.x que possua um número igual ou inferior de sistemas de passagem, irá rejeitar estas novas informações do encaminhamento. Neste exemplo, o AS1 mantém os dados do encaminhamento.
- O AS1 recebe informações do R1 com informações do encaminhamento para 10.1.5.x. O AS1 mantém estas informações do encaminhamento.
- AS1 recebe informações do R2 com informações do encaminhamento para 10.1.3.x. O AS1 mantém estas informações do encaminhamento.
- Da próxima vez que o AS1 enviar mensagens RIP, irá enviar informações ao R1 que descrevem todas as ligações conhecidas pelo AS1 que o R1 talvez não conheça. O AS1 envia informações sobre o 10.1.1.x, o 10.1.2.x e o 10.1.3.x. O AS1 não envia informações sobre o 10.1.4.x ao R1, pois o AS1 tem conhecimento de que o R1 está ligado ao 10.1.4.x e não necessita de um encaminhamento. Informações semelhantes são enviadas ao R2 e ao AS3.

Open Shortest Path First - Abrir primeiro o caminho mais curto

Open Shortest Path First - Abrir primeiro o caminho mais curto (OSPF) é um protocolo de encaminhamento de estado de ligação desenvolvido para rede de IP e se baseia no algoritmo Shortest Path First (SPF). OSPF é um Interior Gateway Protocol (IGP).

Numa rede de OSPF, os encaminhadores ou sistemas na mesma área mantêm uma base de dados de estados de ligação idêntica que descreve a topologia da área. Cada encaminhador ou sistema da área gera a sua base de dados de estados de ligação a partir dos avisos de estado de ligação (LSAs) que recebe de todos os outros encaminhadores ou sistemas na mesma área e a partir dos LSAs que ele próprio gera. Um LSA é um pacote que contém informações acerca de sistemas vizinhos e custos de caminhos. De acordo com a base de dados de estados de ligação, cada encaminhador ou sistema calcula a árvore geradora de caminho mais curto, sendo a raiz o próprio encaminhador ou sistema, utilizando o algoritmo SPF.

OSPF possui as seguintes vantagens essenciais:

- Comparado com protocolos de encaminhamento com base em vector de distância como, por exemplo, o Protocolo de Informação de Encaminhamento (RIP), OSPF é mais adequado para funcionar com redes interligadas heterogéneas e de grande dimensão. O OSPF pode recalcular os encaminhamentos num curto período de tempo quando a topologia da rede é alterada.
- Com OSPF, pode dividir um Sistema Autónomo (AS) em áreas e separar topologias de área para diminuir o tráfego de encaminhamento de OSPF e a dimensão da base de dados de estados de ligação de cada área.
- O OSPF faculta encaminhamento para vários caminhos a um custo igual. Pode adicionar encaminhamentos duplicados à pilha de TCP utilizando sistemas de passagem seguintes diferentes.

Protocolo Hello e troca de bases de dados de estados de ligação de OSPF

Após os encaminhadores ou sistemas numa rede de OSPF se certificarem de que as suas interfaces estão operacionais, primeiro enviam pacotes Hello, utilizando o protocolo Hello pelas interfaces de OSPF, de modo a detectar vizinhos. Vizinhos são encaminhadores ou sistemas que possuem interfaces numa rede comum. De seguida, os encaminhadores ou sistemas vizinhos trocam as bases de estados de ligação para estabelecer contiguidades.

A figura seguinte ilustra o processo de localização de vizinhos e o estabelecimento de contiguidades em dois sistemas na sub-rede 9.7.85.0. Cada sistema possui uma interface de OSPF para a sub-rede comum 9.7.85.0 (interface 9.7.85.1 para o sistema A e interface 9.7.85.2 para o sistema B). A sub-rede 9.7.85.0 pertence à área 1.1.1.1.

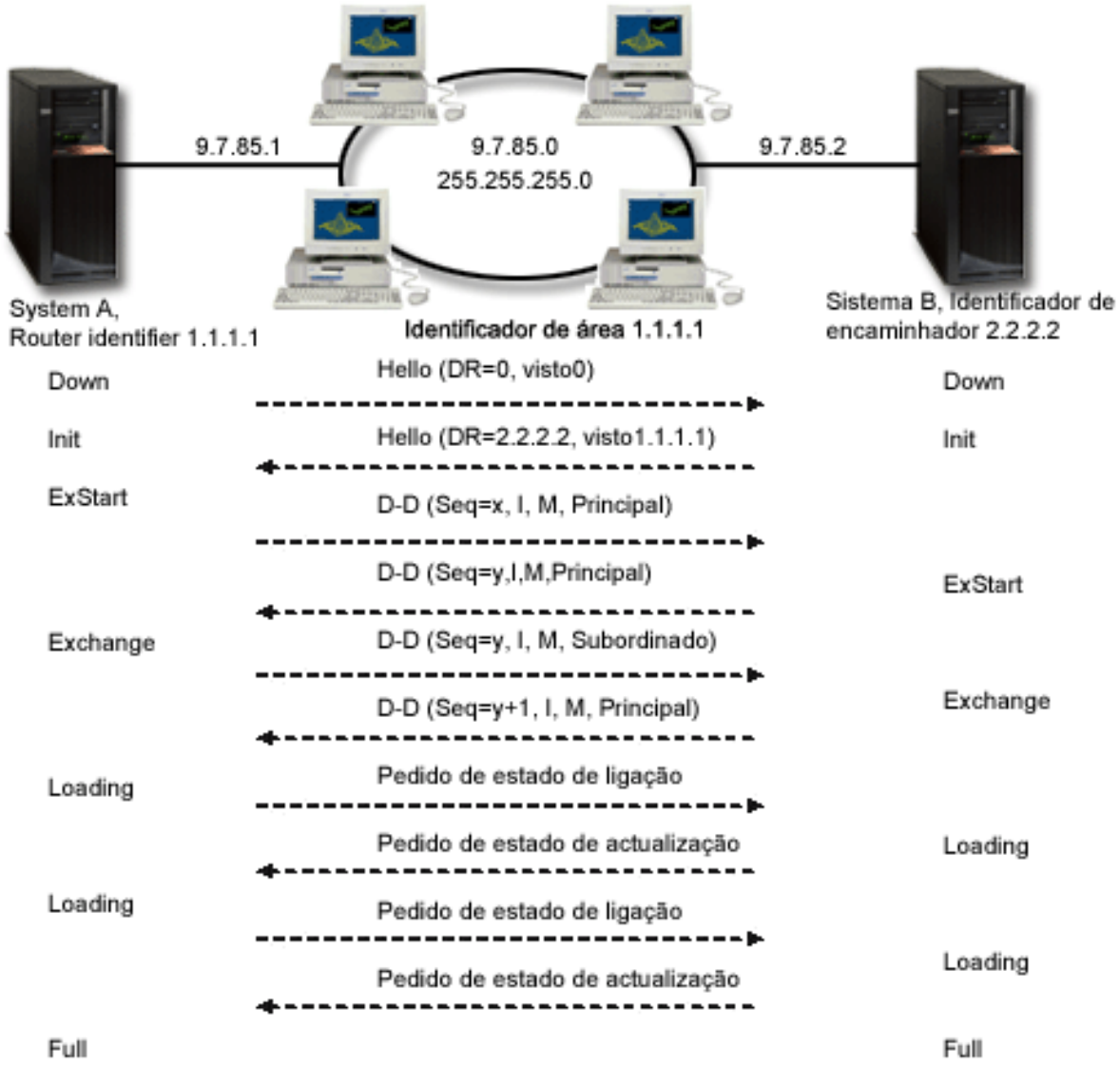


Figura 1. Protocolo Hello e troca de bases de dados de OSPF

Fase EXSTART
Este constitui o primeiro passo da troca de bases de dados de estados de ligação. Os dois sistemas negoceiam qual é o sistema principal e o sistema subordinado.

Fase EXCHANGE
Os dois sistemas trocam pacotes de Descrição de Base de Dados para averiguar quais os LSAs que a base de dados de estados de ligação de cada sistema não inclui. Cada sistema armazena os LSAs não incluídos na respectiva base de dados de estados de ligação na lista de retransmissão.

Fase LOADING
Cada sistema envia pacotes de Pedido de Estado de Ligação para pedir ao sistema vizinho (o outro sistema deste exemplo) que envie todos os LSAs que foram armazenados na lista de retransmissão durante a fase EXCHANGE. O sistema vizinho responde ao pedido com os LSAs em pacotes de Actualização de Estado de Ligação.

Fase FULL
Quando os dois sistemas terminam a troca de LSAs e as suas bases de dados de estados de ligação estão sincronizadas, a contiguidade é estabelecida entre os dois sistemas.

Após estabelecer contiguidades entre todos os encaminhadores ou sistemas na área, cada encaminhador ou sistema da área envia periodicamente um LSA para partilhar as suas contiguidades ou para comunicar a alteração do seu estado. Ao comparar as contiguidades estabelecidas com LSAs, os encaminhadores ou sistemas da área podem identificar as alterações à topologia da área e actualizar as suas bases de dados de estados de ligação de acordo com as mesmas.

Encaminhador designado e encaminhador designado de segurança

Numa rede de OSPF de vários acessos com pelo menos dois encaminhadores ligados, estes fixam um encaminhador designado e um encaminhador designado de segurança utilizando o protocolo Hello. (Uma rede de vários acessos é uma rede na qual vários dispositivos podem estabelecer ligação e comunicar em simultâneo.)

O encaminhador designado gera LSAs para toda a rede de vários acessos, escoa os LSAs para outros encaminhadores da rede e determina quais os encaminhadores que deverão ser contíguos. Todos os outros encaminhadores da rede são contíguos ao encaminhador designado. O encaminhador designado reduz o tráfego da rede e o tamanho da base de dados de estados de ligação desta rede.

O encaminhador designado de segurança não difere em nada de outros encaminhadores, excepto no facto de necessitar de estabelecer contiguidades com todos os encaminhadores da rede (incluindo o encaminhador designado). O encaminhador designado de segurança é promovido a encaminhador designado quando o actual encaminhador designado falha.

Na Figura 1, a sub-rede 9.7.85.0 é uma rede de difusão. Consequentemente, os encaminhadores da sub-rede 9.7.85.0 fixam um encaminhador designado e um encaminhador designado de segurança utilizando o protocolo Hello. Neste exemplo, o sistema A é fixado como o encaminhador designado e o sistema B é fixado como o encaminhador designado de segurança.

Dividir um AS de OSPF em áreas

Ao contrário de RIP, o OSPF pode funcionar dentro de uma hierarquia. A maior entidade dentro da hierarquia é o AS. Um AS é um grupo de redes sob uma administração comum que partilham uma estratégia de encaminhamento comum. Um AS pode ser dividido em áreas, ligadas entre si por encaminhadores. Uma área é formada por grupos de redes contíguas e sistemas centrais ligados. A topologia de uma área é invisível a entidades fora da área. Os encaminhadores dentro da mesma área possuem uma base de dados de estados de ligação idêntica. As topologias de área diferentes permitem um menor tráfego de encaminhamento e uma base de dados de estados de ligação menor para cada área.

Um encaminhador localizado no limite das áreas de OSPF e que liga estas áreas à rede principal denomina-se Encaminhador de Limite de Área. Um Encaminhador de Limite de Área possui várias interfaces para várias áreas e mantém bases de dados de estados de ligação distintas para cada área.

Na seguinte figura, estão configuradas duas áreas (área 1.1.1.1 e área 2.2.2.2). O sistema B é um Encaminhador de Limite de Área, com a interface 9.7.85.2 ligada à área 1.1.1.1 e a interface 9.5.104.241 ligada à área 2.2.2.2. O sistema B possui duas bases de dados de estados de ligação, uma para cada área. O sistema B estabelece contiguidades ao sistema A e ao encaminhador C na área 1.1.1.1, por intermédio da interface 9.7.85.2, e estabelece contiguidade ao sistema D na área 2.2.2.2, por intermédio da interface 9.5.104.241.

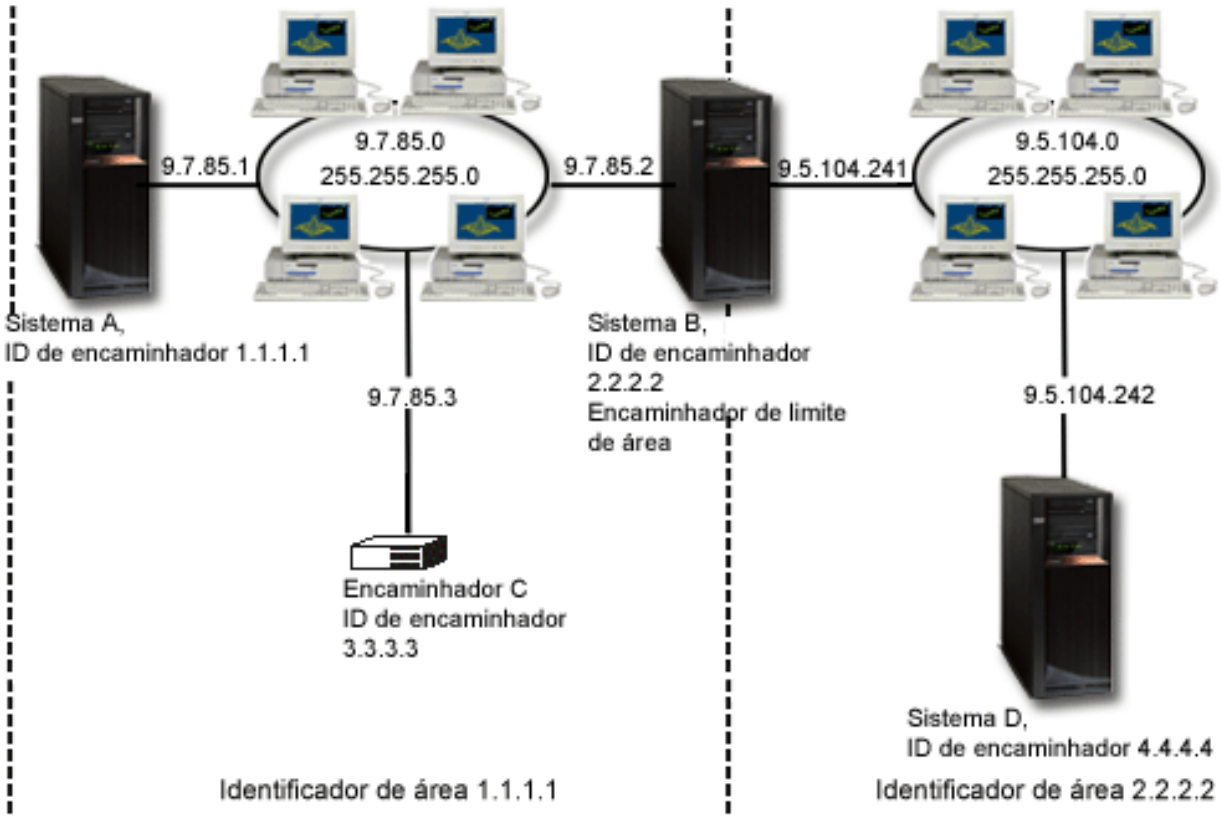


Figura 2. Dividir um AS de OSPF em áreas

Conceitos relacionados

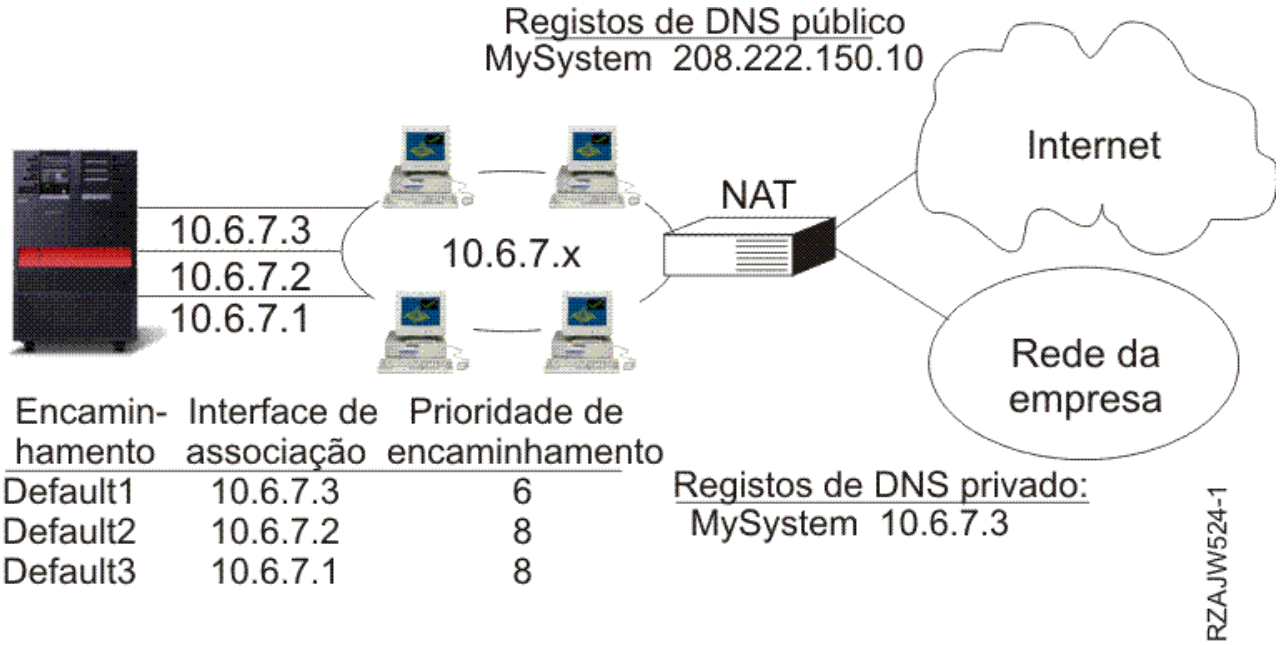
Open Shortest Path First - Abrir primeiro o caminho mais curto (OSPF)

Associação de encaminhamento

A associação de encaminhamento proporciona controlo sobre a interface a utilizar para enviar pacotes de informações de resposta.

Antes de existir a associação de encaminhamento preferencial, não era possível ter o controlo completo sobre qual a interface utilizada para enviar pacotes de informações de resposta. A Interface de Associação de Encaminhamento Preferencial, adicionada à função de adicionar encaminhamentos, proporciona um maior controlo sobre qual a interface utilizada para enviar pacotes, permitindo ao utilizador ligar explicitamente os encaminhamentos às interfaces.

Na figura seguinte existem três interfaces ligadas à mesma rede. Para garantir que, independentemente da interface que recebe o pedido de recepção, a resposta possa ser enviada de volta à mesma interface, tem de adicionar os encaminhamentos duplicados a cada interface. Neste exemplo, são adicionados três encaminhamentos predefinidos, cada um explicitamente associado a uma interface diferente. Esta ligação não é alterada, independentemente da ordem pela qual as interfaces são iniciadas ou terminadas.



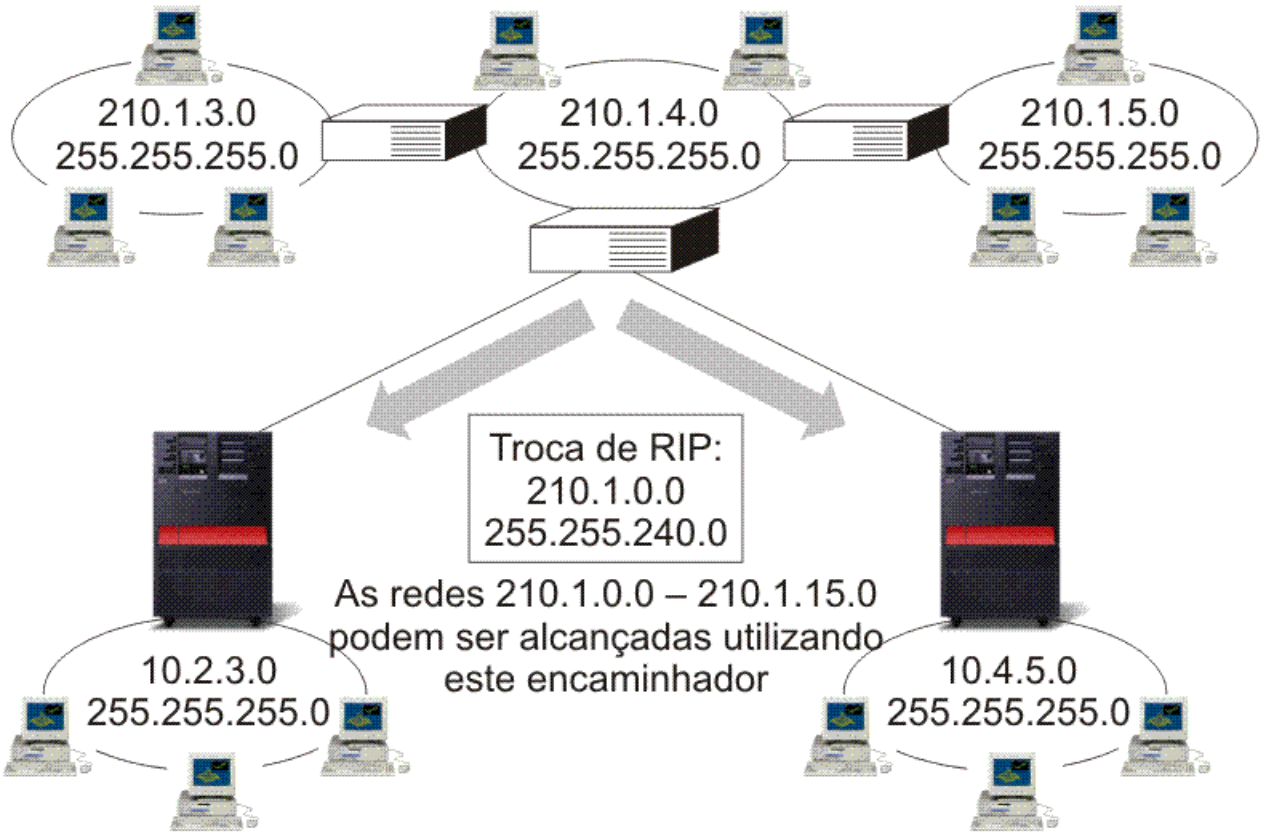
Encaminhamento Entre-Domínios sem Classes

O Encaminhamento Entre-Domínios sem Classes pode reduzir a dimensão das tabelas de encaminhamento e disponibilizar mais endereços de IP para a empresa.

O Encaminhamento Entre-Domínios sem Classes (CIDR ou criação de supernetting) é uma forma de combinar diversos intervalos de endereços da classe C em redes ou encaminhamentos individuais. Este método de encaminhamento adiciona endereços de Internet Protocol (IP) da classe C. Estes endereços são fornecidos por fornecedores de serviços da Internet (ISPs) para serem utilizados pelos respectivos clientes. Os endereços CIDR podem reduzir o tamanho das tabelas de encaminhamento e disponibilizar mais endereços de IP dentro de uma empresa.

No passado, era necessário introduzir uma máscara de sub-rede igual ou superior à máscara exigida pela classe de rede. Para os endereços da classe C, isto significava que uma sub-rede de 255.255.255.0 era a maior (253 sistemas centrais) que podia ser especificada. Para manter endereços de IP, quando uma empresa necessitava de mais de 253 sistemas centrais numa rede, a Internet emitia diversos endereços da classe C. Esta situação tornou difícil a configuração de encaminhadores e outros.

Actualmente, o CIDR permite que estes endereços da classe C adjacentes sejam combinados em intervalos de endereços de rede individuais, utilizando uma máscara de sub-rede. Por exemplo, se atribuir quatro endereços de rede da classe C (208.222.148.0, 208.222.149.0, 208.222.150.0 e 208.222.151.0 com uma máscara de sub-rede de 255.255.255.0), é possível solicitar ao ISP que os transforme numa supernetting, utilizando a máscara de sub-rede 255.255.252.0. Esta máscara combina as quatro redes numa só, para efeitos de encaminhamento. O CIDR é um benefício, pois reduz o número de endereço de IP atribuídos, mas desnecessários.

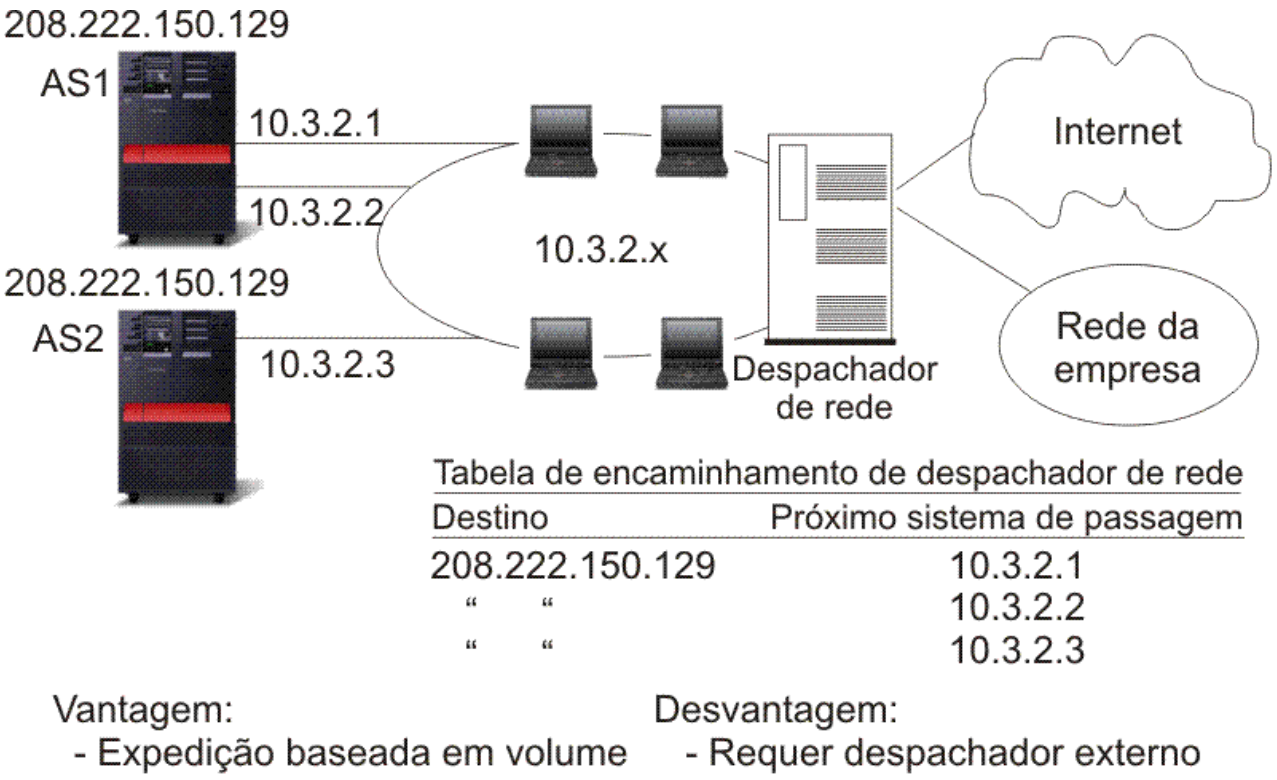


Neste exemplo, o encaminhador é configurado para enviar uma mensagem RIP com o endereço de rede 210.1.0.0 e uma máscara de sub-rede 255.255.240.0. Estes números indicam ao sistema para receber mensagens RIP das redes 210.1.0.0 a 210.1.15.0 através deste encaminhador. Esta indicação faz enviar uma mensagem em vez das 16 necessárias para transmitir as mesmas informações, se o CIDR não estivesse disponível.

Encaminhamento com IP virtual

O IP virtual, também denominado uma interface sem circuito ou de circuito fechado, é uma função extremamente útil que proporciona uma forma de atribuir um ou mais endereços ao sistema sem a necessidade de associar os endereços a uma interface física.

Esta função pode ser utilizada quando pretende executar várias ocorrências de um sistema associado a diferentes endereços ou quando pretende executar outros serviços que necessitem de ser associados a portas predefinidas. A maioria dos ambientes onde se pretenderá utilizar o IP virtual são casos em que se pretende fornecer vários caminhos entre a porta de ligação local e a plataforma System i como, por exemplo, o equilíbrio de volume e a tolerância às falhas. Neste contexto, cada caminho implica uma interface individual e, consequentemente, um endereço de IP adicional, não virtual no sistema, tal como mostra a figura seguinte.



RZAJW510-0

A existência destas várias interfaces apenas deveria ser visível na rede local. Não deve permitir que os clientes remotos tenham conhecimento dos vários endereços de IP do sistema. O ideal seria permitir que vissem o sistema como um endereço de IP individual. A forma como o pacote de recepção é encaminhado através da porta de ligação, na rede local, até ao sistema deveria ser invisível ao cliente remoto. Para fazê-lo, deve utilizar-se o IP virtual. Os clientes locais devem comunicar com o sistema através de qualquer um dos endereços de IP físicos, enquanto os clientes remotos devem ver apenas a interface IP virtual.

O ambiente IP virtual é para o sistema que actua como servidor para clientes ligados remotamente. Mais importante ainda, o endereço de IP virtual está numa sub-rede diferente daquela das interfaces físicas. Além disso, o endereço de IP virtual faz com que o sistema seja apresentado como um sistema central individual e não necessariamente como um ligado a uma rede ou sub-rede de grandes dimensões. Desta forma, a máscara de sub-rede da interface IP virtual deve ser, de modo geral, definida para 255.255.255.255.

| Dado que o endereço de IP virtual não está associado a uma única interface física, o sistema nunca
| responde a um pedido de Address Resolution Protocol (ARP) efectuado ao endereço de IP virtual. Por
| outras palavras, ao activar o ARP de proxy, uma interface local pode responder aos pedidos de ARP em
| nome do endereço de IP virtual. Caso contrário, os sistemas remotos têm de ter um encaminhamento
| definido para alcançar o endereço. O utilizador já pode configurar o ARP de proxy de IP virtual para
| uma interface de IP virtual enquanto está activa.

No exemplo anterior, todas as estações de trabalho apontam para uma das interfaces 10.3.2 do sistema, como respectiva porta de ligação do sistema de passagem seguinte. Quando chega um pacote ao sistema, passa pelo processamento de pacotes. Se o endereço de destino corresponder a qualquer um dos endereços definidos no sistema (incluindo os endereços de IP virtuais), o sistema processa o pacote.

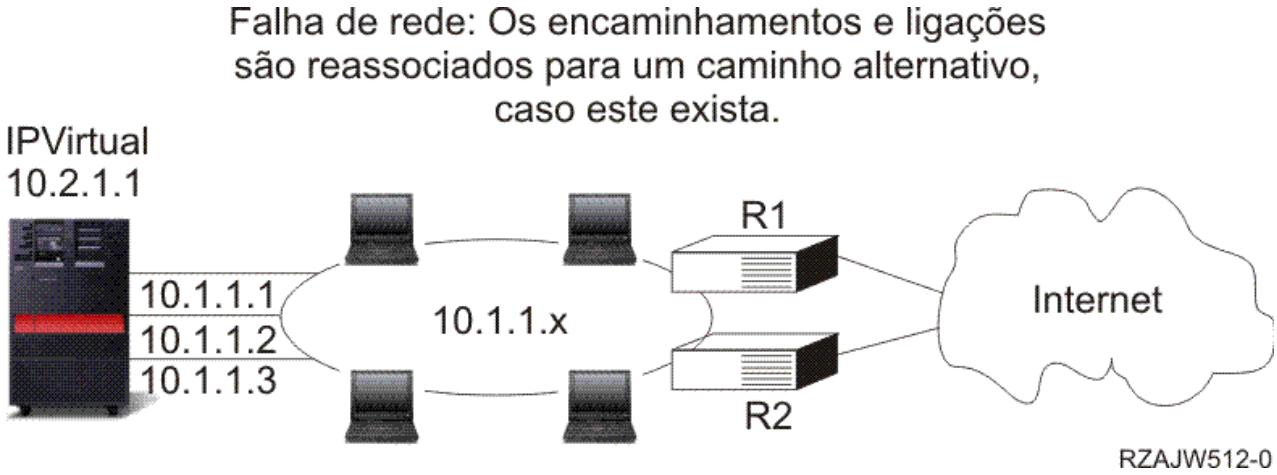
Os servidores Domain Name System (DNS) utilizam os endereços do sistema solicitado. Neste caso, todos os endereços representam o mesmo sistema. Pode utilizar a função de IP virtual ao consolidar vários sistemas num único sistema de grandes dimensões.

| O suporte de endereço de IP virtual passa a incluir endereços de IPv6.

Tolerância a falhas

Outra utilização para os endereços de IP virtuais é proteger contra falhas de encaminhador. A tolerância a falhas mostra diversas formas diferentes de como um encaminhamento pode ser recuperado após uma desactivação.

Este exemplo mostra diversas formas diferentes de como um encaminhamento pode ser recuperado após uma desactivação. A ligação mais fiável é aquela em que um endereço de IP virtual é definido no sistema. Com o suporte do IP virtual, mesmo se uma interface falhar, a sessão pode continuar a comunicar utilizando outras interfaces.



O que acontece se o encaminhador R1 falhar

- As ligações efectuadas através do R1 são reencaminhadas através do R2.
- A porta de ligação em falha irá detectar a recuperação do R1, mas as ligações activas irão continuar a ser executadas através do R2.

O que acontece se a interface 10.1.1.1 falhar

- As ligações activas para a 10.1.1.1 são perdidas, mas outras ligações para 10.1.1.2, 10.1.1.3 e 10.2.1.1 mantêm-se.
- Reassociação de encaminhamento:
  - Anterior à V4R2: Os encaminhamentos indirectos são reassociados para 10.1.1.2 ou 10.1.1.3.
  - V4R2: Os encaminhamentos apenas são reassociados se a Interface de Ligação Preferencial estiver definida para NONE.
  - V4R3 e superior: É necessário definir 10.2.1.1 como endereço de IP virtual e endereço principal do sistema.
    - O endereço de IP principal permanece activo.
    - O sistema permanece acessível enquanto, pelo menos, uma interface física permanecer activa.

| Uma interface de Point-to-Point Protocol (PPP) ou uma interface de Layer Two Tunneling Protocol (L2TP)
| a partir de agora podem utilizar um endereço de IP virtual como endereço de IP local para facultar
| tolerância de falhas a ligações remotas.

Encaminhamento com a conversão de endereços de rede

O encaminhamento com a conversão de endereços de rede (NAT) permite o acesso a redes remotas como, por exemplo, a Internet, ao mesmo tempo que protege a rede privada, mascarando os endereços de IP utilizados na rede privada.

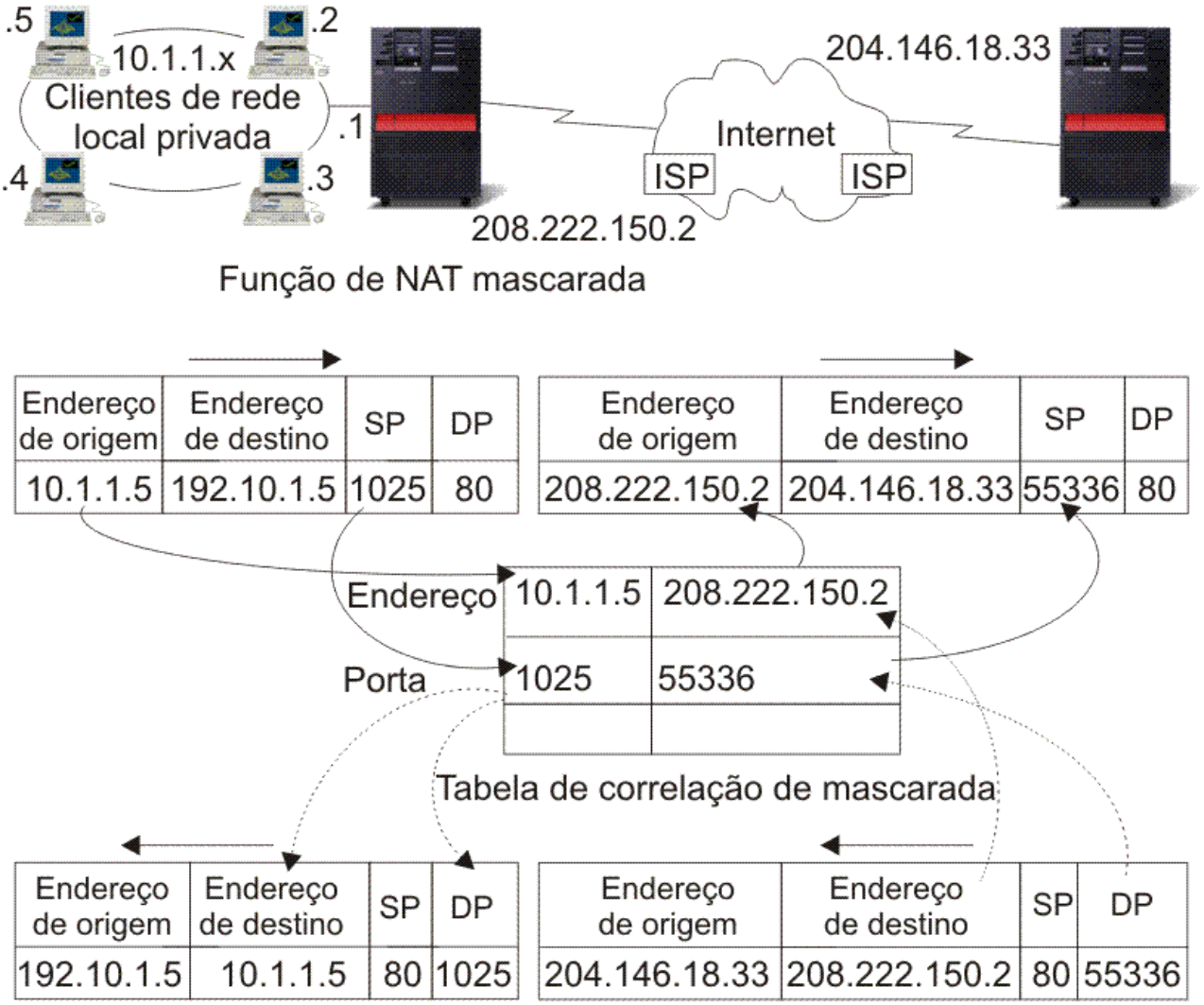
A NAT proporciona o acesso a uma rede remota, habitualmente a Internet, ao mesmo tempo que protege a rede privada, mascarando os endereços de IP utilizados dentro da firewall.

NAT mascarada

A NAT mascarada é utilizada para permitir que a rede privada seja ocultada, bem como representada, pelo endereço ligado à interface pública.

Em muitas situações, o endereço associado à interface pública é o endereço atribuído por um Fornecedor de Serviços da Internet (ISP) e o referido endereço pode ser dinâmico, no caso de uma ligação efectuada por intermédio do Point-to-Point Protocol (PPP). Este tipo de conversão apenas pode ser utilizado em ligações originadas na rede privada e destinadas à rede pública externa. Cada ligação de envio é mantida através da utilização de um número da porta de IP de origem diferente.

A NAT mascarada permite que as estações de trabalho com endereços de IP privados comuniquem com sistemas centrais na Internet através do sistema operativo i5/OS. O i5/OS possui um endereço de IP atribuído pelo ISP local como respectiva porta de ligação à Internet. A expressão *máquina ligada localmente* é utilizada para referir todos os sistemas de uma rede interna, independentemente do método de ligação (rede de área local ou rede alargada) e da distância da ligação. A expressão *sistemas internos* refere-se a sistemas localizados na Internet. A imagem seguinte ilustra a forma como a NAT mascarada funciona.



RZAJW507-0

Para a Internet, todas as estações de trabalho parecem estar contidas no sistema; ou seja, apenas um endereço de IP está associado tanto ao sistema como às estações de trabalho. Quando um encaminhador recebe um pacote dirigido à estação de trabalho, procura determinar qual o endereço da LAN interna que deve recebê-lo e envia-o para lá.

Cada estação de trabalho deve ser configurada de forma a que o i5/OS seja a respectiva porta de ligação e também o respectivo destino predefinido. A correspondência entre uma determinada ligação de comunicação (porta) e uma estação de trabalho é configurada quando uma das estações de trabalho envia um pacote ao i5/OS para que seja enviado para a Internet. A função NAT mascarada guarda o número da porta, de modo a que quando receba respostas para o pacote da estação de trabalho dessa ligação, possa enviar a resposta para a estação de trabalho certa.

Um registo das ligações de porta activas e do último tempo de acesso de ambos os extremos da ligação é criado e mantido pela NAT mascarada. Estes registos são periodicamente limpos de todas as ligações que ficam inactivas durante um período de tempo predeterminado, com base no pressuposto de que uma ligação que está inactiva já não está a ser utilizada.

Todas as comunicações entre a estação de trabalho e a Internet devem ser iniciadas por sistemas ligados localmente. Esta é uma firewall de segurança eficaz; a Internet ignora a existência das estações de trabalho e não consegue difundir os endereços através da Internet.

O ponto-chave para a implementação da NAT mascarada é a utilização de portas lógicas, emitidas pela NAT mascarada para distinguir entre as várias sequências de comunicação. O TCP contém um número da porta de origem e um número da porta de destino. A estas designações, a NAT adiciona um número da porta lógica.

Processamento da NAT mascarada de recepção (resposta e outras):

Este processo, associado do processamento de NAT mascarada de envio, abre a mensagem de envio correspondente para obter as informações correctas sobre a estação de trabalho origem.

A mensagem de recepção da figura anterior é um pacote enviado da Internet para a rede local privada. Para datagramas de recepção, o número da porta de destino é o número da porta local. (Para mensagens de recepção, o número da porta de origem é o número da porta externa. Para mensagens de envio, o número da porta de destino é o número da porta externa.)

As mensagens de resposta vindas da Internet destinadas a um sistema ligado localmente possuem um número da porta lógica atribuído pela máscara como número da porta de destino no cabeçalho do nível de transporte. Os passos do processamento de recepção da NAT mascarada são:

1. A NAT mascarada procura na respectiva base de dados este número da porta lógica (porta de origem). Se não for encontrado, presume-se que o pacote é um pacote não solicitado, sendo devolvido, inalterado, ao programa de chamada. Então, é tratado como um destino desconhecido normal.
2. Se for encontrado um número de porta lógica correspondente, é efectuada uma nova verificação para determinar se o endereço IP de origem corresponde ao endereço de IP de destino da entrada da tabela do número da porta lógica existente. Se corresponder, o número da porta original do sistema local substitui a porta de origem no cabeçalho IP. Se a verificação falhar, o pacote é enviado de volta, inalterado.
3. Os endereços de IP locais correspondentes são colocados no destino do pacote IP.
4. O pacote é depois processado, como habitualmente, pelo IP ou pelo TCP, e vai parar ao sistema correcto ligado localmente. Como a NAT mascarada exige um número da porta lógica para determinar os endereços das portas de origem e de destino correctos, não é capaz de tratar os datagramas não solicitados enviados pela Internet.

Processamento da NAT mascarada de envio:

Este processo substitui a porta origem de uma mensagem de envio com um número de porta lógica único quando a mensagem for enviada da rede local privada para a Internet.

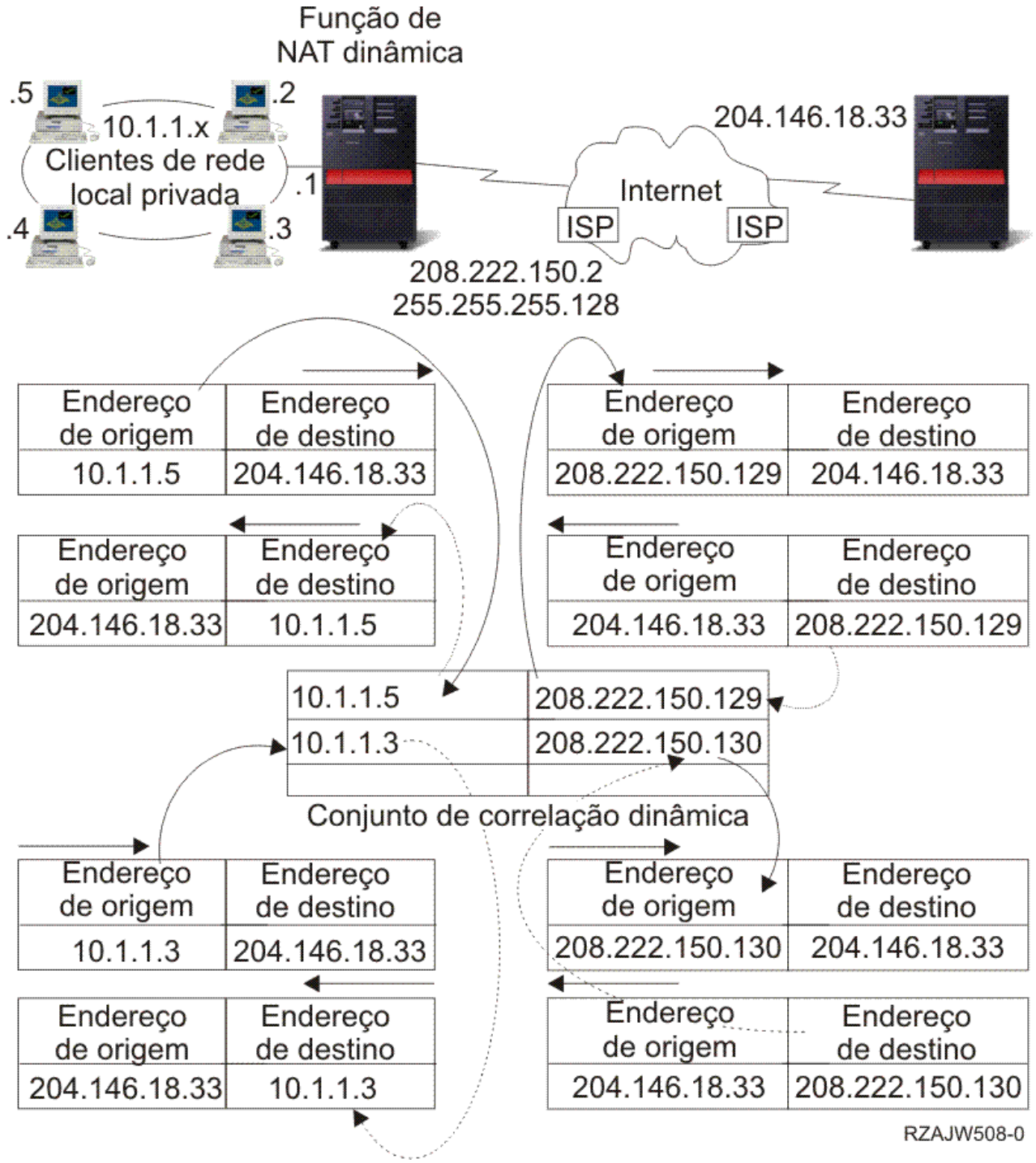
A mensagem de envio da figura anterior é um pacote enviado da rede local privada para a Internet. Uma mensagem de envio (da rede local para a externa) contém a porta de origem utilizada pela estação de trabalho de origem. A NAT guarda este número e substitui-o no cabeçalho de transporte por um número da porta lógica exclusivo. Para datagramas de envio, o número da porta de origem é o número da porta local. Os passos do processamento de envio da NAT mascarada são:

1. O processamento da NAT mascarada de envio parte do pressuposto de que todos os pacotes IP que recebe são destinados a endereços de IP externos e, por isso, não efectua uma verificação para determinar se um pacote deve ser encaminhado localmente.
2. O conjunto de números da porta lógica procura um correspondente no nível de transporte, bem como no endereço de IP origem e na porta de origem. Se encontrar, o número da porta lógica correspondente é substituído pela porta de origem. Se não for encontrado um número da porta correspondente, é criado outro e um novo número da porta lógica é seleccionado e substituído pela porta de origem.
3. O endereço de IP de origem é convertido.
4. O pacote é depois processado, como habitualmente, pelo IP e enviado para o sistema externo correcto.

NAT dinâmica

A NAT dinâmica apenas pode ser utilizada para estabelecer ligações a partir da rede privada para a rede pública.

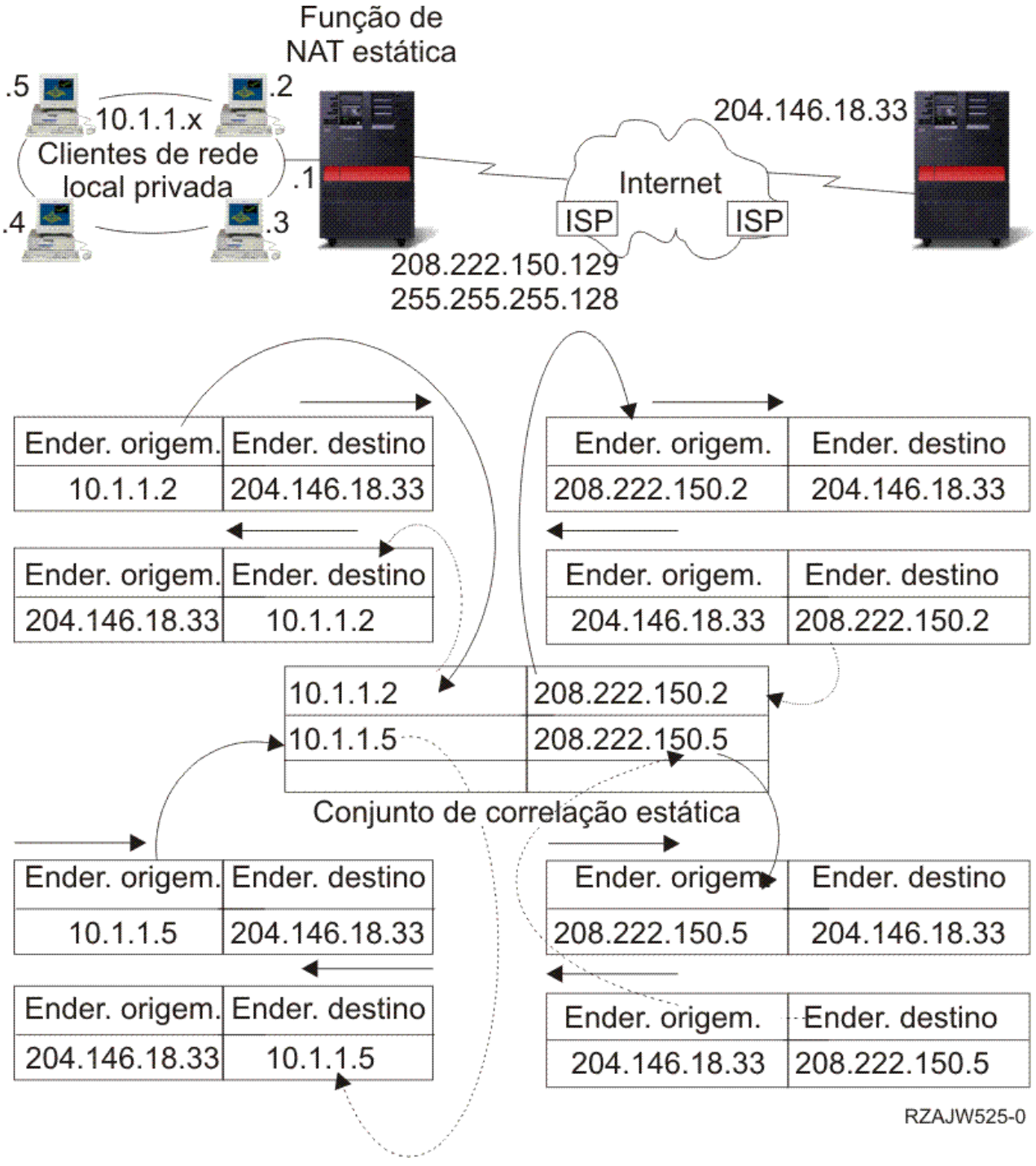
Um conjunto de endereços de rede é mantido e utilizado quando uma ligação de envio é efectuada. Cada ligação é atribuída a um endereço público exclusivo. O número máximo de ligações simultâneas é igual ao número de endereços públicos do conjunto. Este número é semelhante a uma correspondência de um para um entre endereços. A NAT dinâmica permite-lhe comunicar com a Internet através de um endereço NAT dinâmico. A imagem seguinte ilustra a NAT dinâmica.



NAT estática

A NAT estática pode utilizar ligações de recepção de uma rede pública para uma rede privada.

A NAT estática é uma correspondência de um para um simples entre endereços públicos e privados. Esta NAT é exigida para suportar ligações de recepção vindas da rede pública para a rede privada. Para cada endereço local definido, tem de haver um endereço globalmente exclusivo associado.



Conceitos relacionados

"Equilíbrio de volume baseado no DNS" na página 31
É possível utilizar o equilíbrio de volume baseado no DNS no volume de trabalho de recepção. Se for necessário o equilíbrio de volume para os clientes locais, utilize o equilíbrio de volume do DNS.

Encaminhamento com OptiConnect e partições lógicas

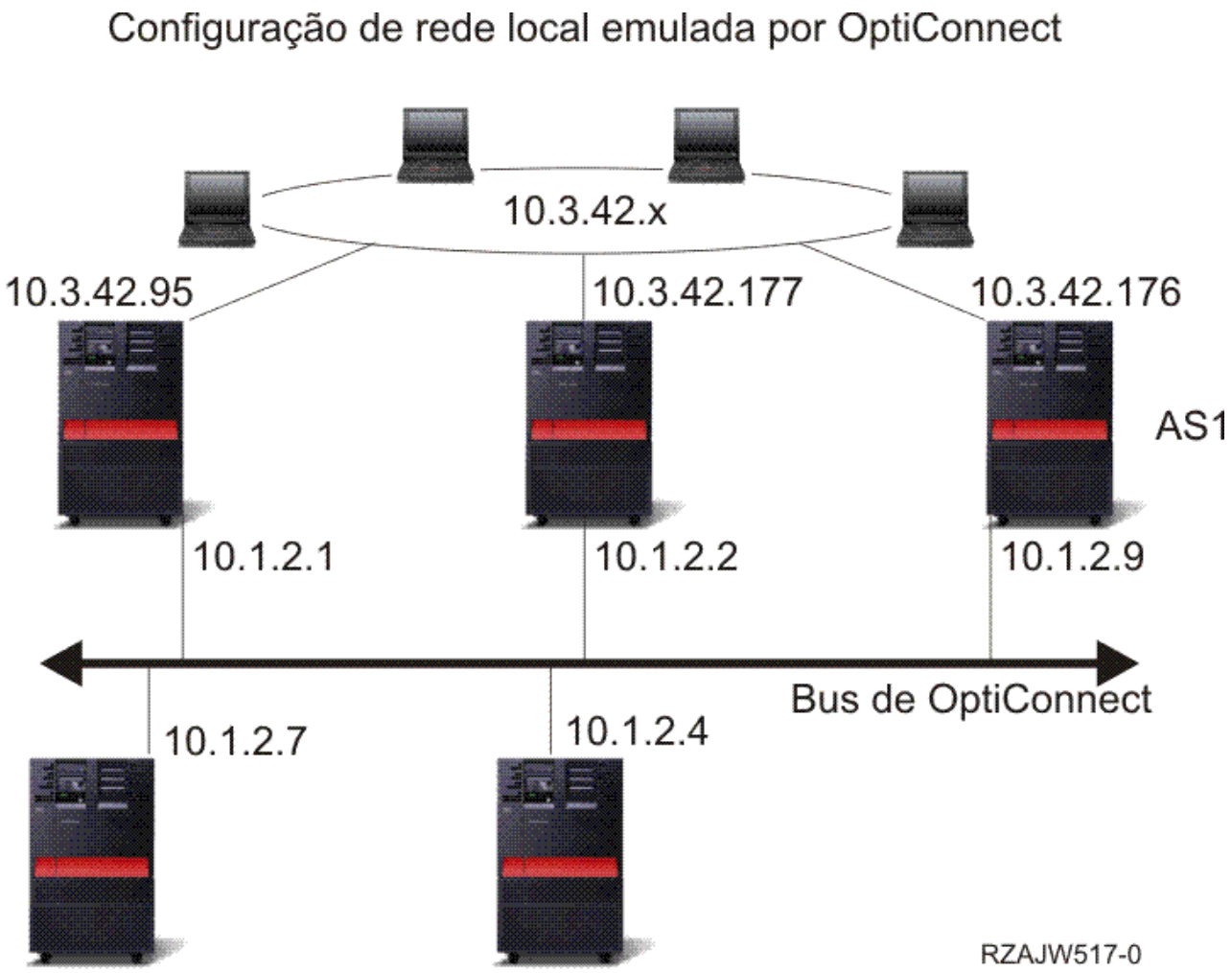
O OptiConnect pode ligar várias plataformas System i utilizando um bus de fibra óptica de alta velocidade. O OptiConnect e as partições lógicas proporcionam outros ambientes para utilizar as bases de encaminhamento de ARP do proxy, ponto a ponto e interfaces IP virtuais.

TCP/IP e OptiConnect

Pode definir ligações TCP/IP num bus OptiConnect. O TCP/IP no OptiConnect proporciona outro método para os elementos constituintes do encaminhamento como, por exemplo, o ARP do proxy, as redes ponto a ponto não numeradas e as interfaces de IP virtuais.

É possível efectuar esta configuração com uma configuração de rede local emulada por OptiConnect ou com uma configuração ponto a ponto OptiConnect.

Com uma **configuração LAN emulada por OptiConnect**, o bus OptiConnect é apresentado como uma rede local ao TCP/IP, tal como é mostrado na figura seguinte. É fácil de configurar, mas a conectividade OptiConnect da LAN não é automática, uma vez que exige o Routing Information Protocol (RIP) ou encaminhamentos estáticos.



A **configuração ponto a ponto OptiConnect** utiliza interfaces não numeradas ponto a ponto, que são configuradas para cada par de sistemas centrais OptiConnect. Não são criadas novas redes e, por isso, a conectividade OptiConnect da LAN é automática. Uma das vantagens desta configuração é que não são necessárias definições de encaminhamento adicionais. A conectividade entre um sistema central de uma rede e sistemas centrais de outra rede é automática. Outra vantagem é que, se duas redes estiverem activas, os dados enviados entre os sistemas circulam pelo bus OptiConnect, uma vez que estes

encaminhamentos possuem a máscara de sub-rede mais específica. Se o bus OptiConnect falhar, o tráfego é automaticamente comutado para a LAN token-ring.

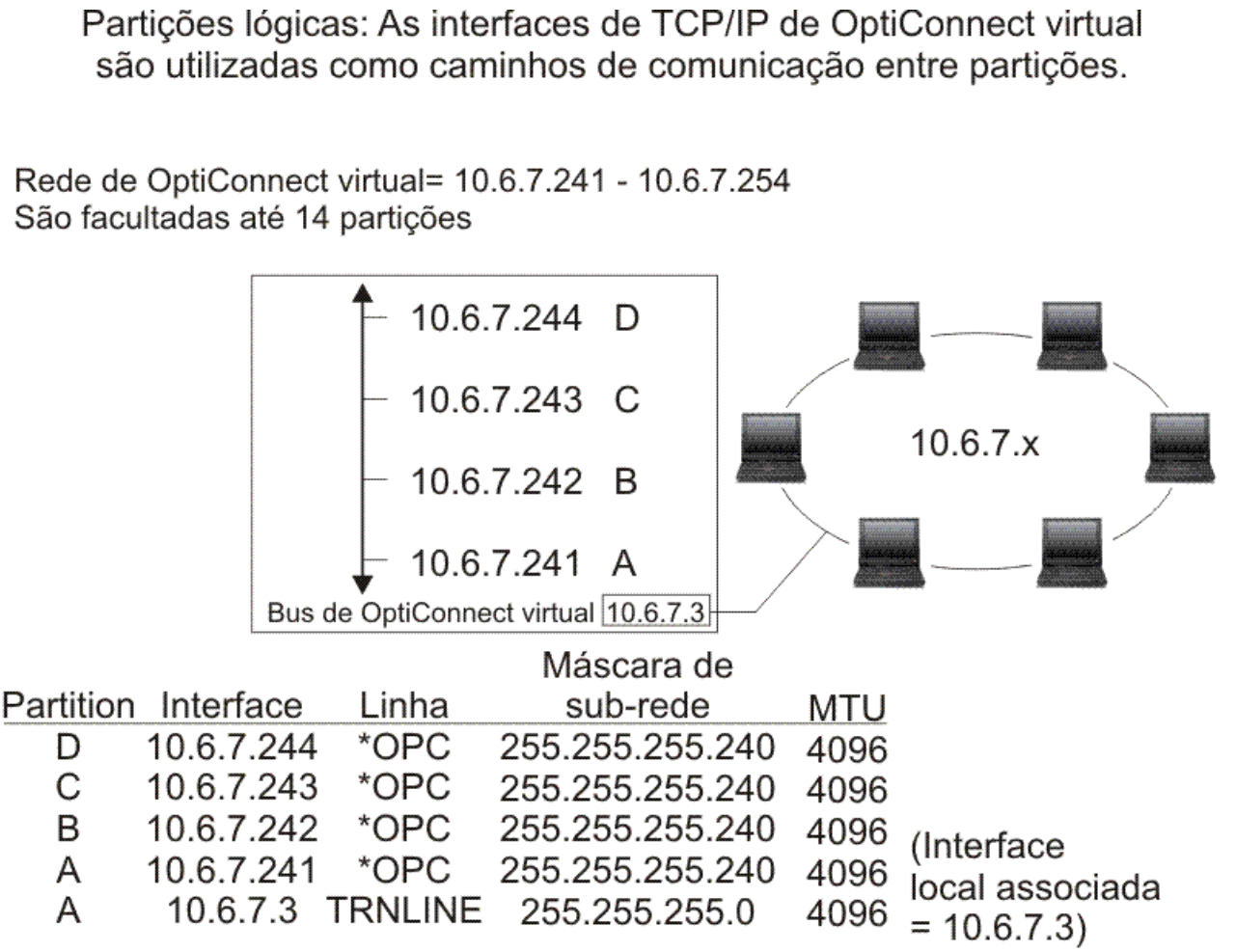
A **configuração ponto a ponto OptiConnect com IP virtual** é uma variação da configuração ponto a ponto não numerada. Sempre que forem utilizadas interfaces não numeradas ponto a ponto, cada interface tem de possuir uma interface local associada especificada. Este é o endereço de IP através do qual o sistema do extremo remoto da ligação ponto a ponto conhece o sistema local. Esta interface local associada poderá ser a interface de rede local principal do sistema, conforme mostrado na figura seguinte. Ou pode utilizar uma interface IP virtual como a interface local associada.

Nesta configuração ponto a ponto OptiConnect utilizando um IP virtual, utiliza-se o bus OptiConnect como um conjunto de ligações ponto a ponto. É definida uma ligação não numerada para cada par de sistemas centrais. Tal como a configuração ponto a ponto OptiConnect, não são necessárias definições de encaminhamento adicionais e a conectividade entre um sistema central de uma rede e os sistemas centrais de outra rede é automática. Uma das vantagens desta configuração é que, se qualquer das redes estiver activa, existe um caminho para chegar a qualquer sistema em execução no sistema operativo i5/OS.

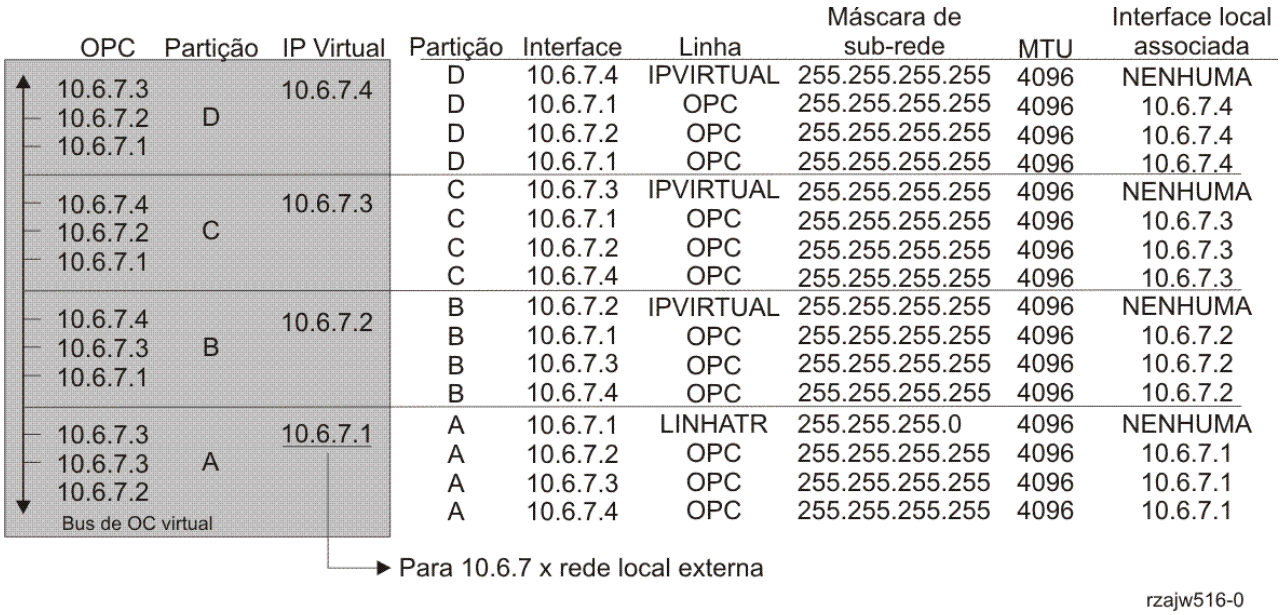
Encaminhamento com OptiConnect virtual e partições lógicas

Com partições lógicas, um único sistema é dividido, de forma lógica, em vários sistemas virtuais. As interfaces OptiConnect virtuais do TCP/IP são utilizadas como caminhos de comunicação entre partições.

Cada partição possui um espaço de endereço próprio, uma ocorrência de TCP/IP própria e poderá ter adaptadores de I/O dedicados próprios. Para o TCP/IP, cada partição é apresentada como um sistema diferente. A comunicação TCP/IP entre as diferentes partições é efectuada utilizando um bus OptiConnect virtual. O código de encaminhamento TCP/IP não utiliza o caminho para outra partição de uma forma diferente de um caminho para outro sistema ligado por um bus OptiConnect físico.



Nestes exemplos, apenas é instalado um adaptador de LAN no sistema. Este adaptador é atribuído à partição A. Os clientes da LAN necessitam de comunicar com as outras partições definidas no sistema. Para fazê-lo, deve definir uma sub-rede visível no bus OptiConnect virtual. A LAN possui um endereço de rede 10.6.7.x. Como pretende planear partições adicionais, são necessários endereços de IP. Para obter 12 endereços, deve utilizar uma máscara de sub-rede de 255.255.255.240. Esta acção proporciona-lhe os endereços de 10.6.7.241 a 10.6.7.254, um total de 14 endereços utilizáveis. É fundamental garantir que estes endereços ainda não estão a ser utilizados na LAN. Depois de obter os endereços, deve atribuir um a cada partição. Adicione uma interface a cada partição e defina o endereço no bus OptiConnect virtual.



A criação de sub-redes visíveis é activada automaticamente quando as seguintes instruções são verdadeiras. Primeiro, o bus OptiConnect virtual é menor ou igual ao tamanho da MTU da interface LAN real. Segundo, a sub-rede do bus OptiConnect é uma sub-rede do endereço de rede da LAN. Se ambas as instruções forem verdadeiras, então a criação de sub-redes visíveis é activada automaticamente. A interface 10.6.7.3 efectua um proxy a todas as interfaces definidas nas partições. Isto permite que os clientes da LAN fiquem ligados às partições.

Métodos de equilíbrio do volume de trabalho do TCP/IP

O *equilíbrio do volume de trabalho* é a redistribuição do tráfego e do volume de trabalho da rede suportados por sistemas que processam uma grande quantidade de acessos em vários processadores, adaptadores de interface ou servidores de sistemas centrais.

Para obter o máximo rendimento possível do sistema operativo i5/OS, é necessário distribuir o volume de trabalho de comunicações por várias partes do sistema.

Podem ser utilizados vários métodos de encaminhamento do TCP/IP para equilibrar o volume de trabalho do sistema.

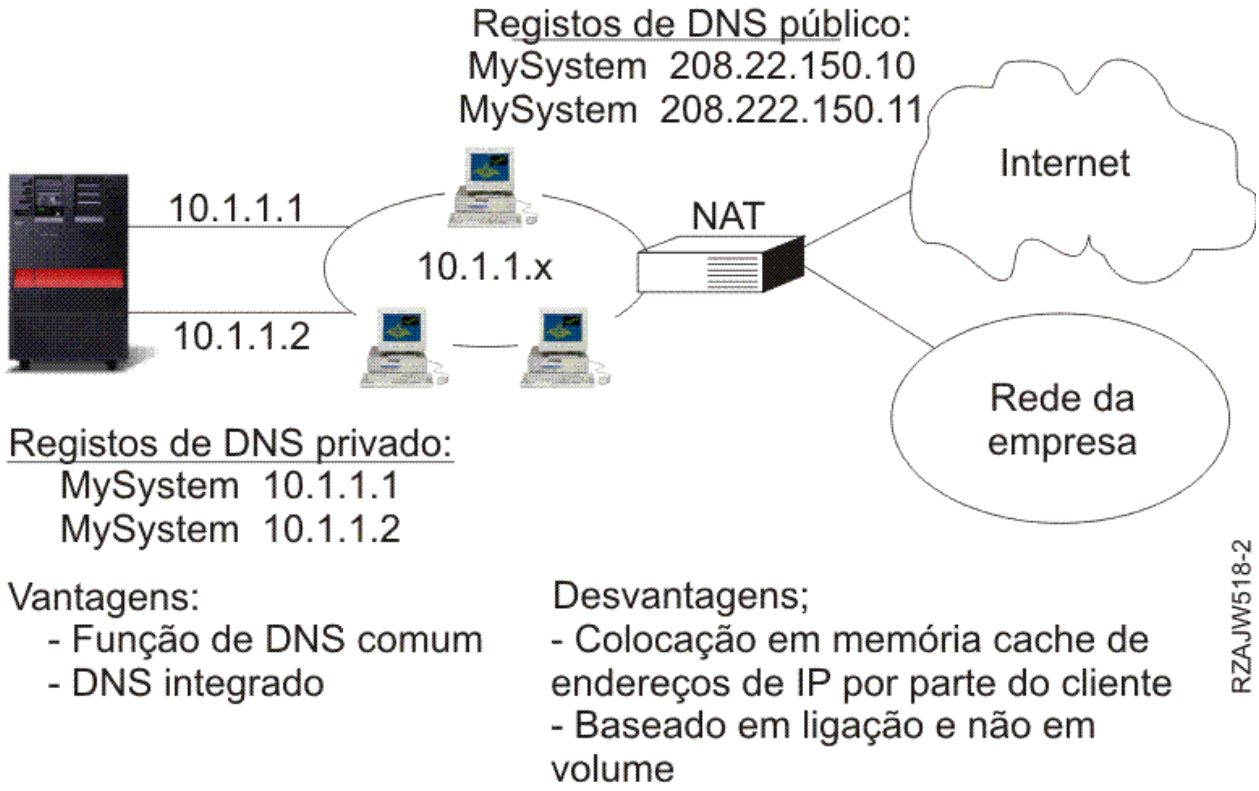
Equilíbrio de volume baseado no DNS

É possível utilizar o equilíbrio de volume baseado no DNS no volume de trabalho de recepção. Se for necessário o equilíbrio de volume para os clientes locais, utilize o equilíbrio de volume do DNS.

O equilíbrio de volume baseado no DNS é utilizado para o equilíbrio do carregamento de recepção. Estão configurados vários endereços de IP de sistemas centrais no DNS para um único nome de sistema central. O DNS alterna o endereço de IP de sistema central devolvido a um pedido de resolução do nome de sistema central cliente bem sucedido. Uma vantagem deste tipo de equilíbrio de volume é que se trata de uma função comum do DNS. As desvantagens desta solução consistem no facto de os endereços de IP poderem ser colocados na memória cache por um cliente e de ser uma solução baseada na ligação e não uma solução baseada no carregamento.

A primeira forma de alcançar o equilíbrio de volume é utilizando uma função do DNS para distribuir vários endereços para o mesmo nome do sistema. O DNS irá indicar um endereço de IP diferente de cada vez que for efectuado um pedido ao registo de endereços do nome do sistema. No exemplo seguinte, cada endereço corresponde a um sistema diferente. Isto permite-lhe proporcionar equilíbrio de volume a

dois sistemas diferentes. No caso de clientes de redes privadas, estes recebem um endereço diferente para cada pedido. Esta é uma função comum do DNS. Note que o DNS público também possui duas entradas de endereço. Estes endereços são convertidos utilizando a NAT estática, por forma a que, se estiver na Internet, possa alcançar os dois sistemas.



Se os programas dependerem no alcançar um sistema específico ou no regresso ao mesmo sistema depois da ligação inicial, os sítios e as páginas da Web devem ser codificados para enviar um nome do sistema diferente, depois de ser efectuado o primeiro contacto. Podem ser adicionadas entradas do DNS adicionais ao MyServer1 208.222.150.10 e ao MyServer2 208.222.150.11. Ao fazê-lo, os sítios da Web, por exemplo, podem apontar para o MyServer2, depois do primeiro contacto. Este tipo de equilíbrio de volume proporciona equilíbrio pelo pedido de ligação. Na maioria dos casos, após o utilizador ter processado o endereço, o cliente coloca o endereço na memória cache e não volta a perguntá-lo. Este tipo de equilíbrio de volume não considera a quantidade de tráfego que vai para cada sistema. De notar que este tipo de equilíbrio de volume apenas considera o tráfego de recepção e que é possível possuir dois adaptadores num sistema e não um adaptador em dois sistemas.

Conceitos relacionados

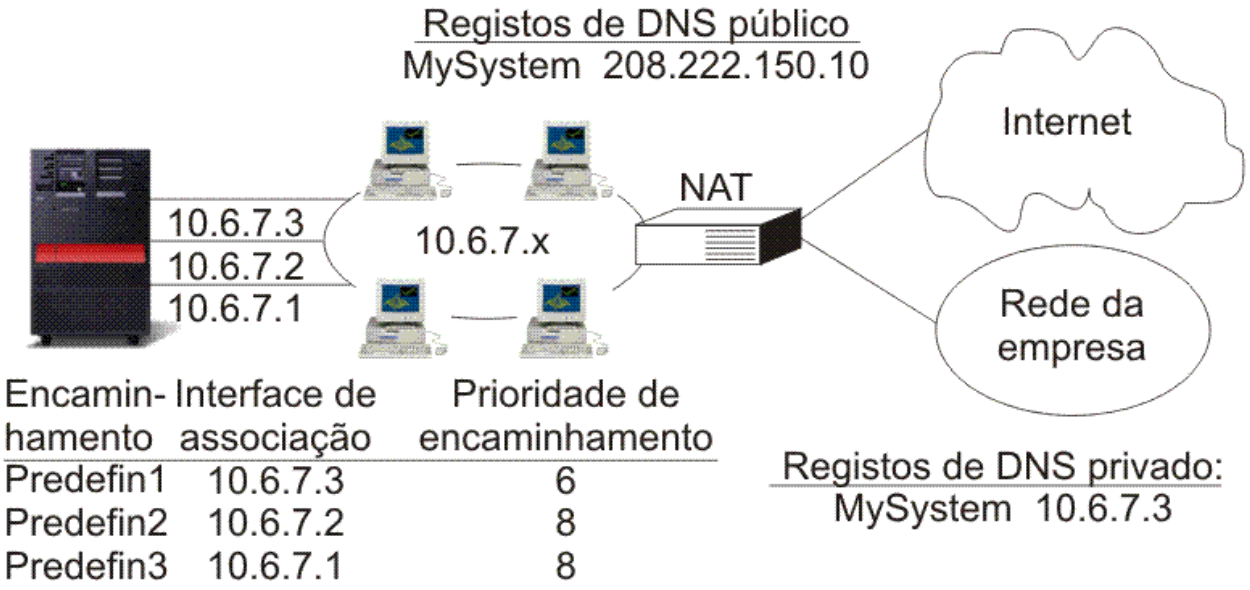
"NAT estática" na página 27
A NAT estática pode utilizar ligações de recepção de uma rede pública para uma rede privada.

Equilíbrio de volume baseado em encaminhamento duplicado

É possível utilizar o equilíbrio de volume baseado em encaminhamento duplicado para o equilíbrio do volume de trabalho de envio através de interfaces múltiplas.

Esta é uma solução baseada na ligação com uma maior flexibilidade do que o equilíbrio de volume baseado no DNS, mas não está activa para clientes locais. As vantagens na utilização deste tipo de equilíbrio de volume consistem no facto de ser uma solução completa do i5/OS, de ter maior flexibilidade do que o DNS e de ser ideal para aplicações em que a maior parte do tráfego é de envio, como HTTP e Telnet. As desvantagens consistem no facto de ser uma solução baseada na ligação (e não uma solução baseada no carregamento), de não estar activa para clientes locais e de não ter qualquer efeito em pedidos de recepção.

No exemplo seguinte, três adaptadores do sistema estão ligados ao mesmo segmento LAN. É necessário configurar um dos adaptadores apenas como linha de recepção e configurar os outros dois adaptadores como de envio. Os clientes locais continuam a funcionar da mesma forma que anteriormente. Quer isto dizer que a interface de envio é a mesma que a interface de recepção. Lembre-se de que o sistema local é qualquer sistema que não exija um encaminhador para atingi-lo. Pode ser uma rede de grandes dimensões, se fossem utilizados comutadores em vez de encaminhadores.



Os encaminhamentos duplicados e indirectos com uma predefinição >(5) serão seleccionados de acordo com a prioridade de encaminhamento

Vantagens:
- Mais flexibilidade do que DNS
- Adequado para HTTP, Telnet

Desvantagens:
- Baseado em ligação e não em volume
- Não está activo para clientes locais
- Não afecta pedidos de recepção

RZAJW511-2

Pode configurar o equilíbrio de volume baseado no encaminhamento duplicado com o comando Add TCP/IP Route (ADDTCPRTE) ou com a interface System i Navigator. A configuração é realizada definindo a prioridade de encaminhamento duplicado ou a interface de associação preferencial. Se o valor da prioridade de encaminhamento duplicado for mantido conforme o valor predefinido de 5, nada acontece. Se for definido um valor superior a 5, as ligações são distribuídas entre os encaminhamentos com a mesma prioridade. A interface de associação preferencial é utilizada para associar um encaminhamento a uma interface específica através do endereço de IP.

No exemplo anterior, existe um adaptador ″de recepção″ (10.6.7.3) com uma prioridade de encaminhamento duplicado de 6. Os outros dois adaptadores estão configurados com uma prioridade de encaminhamento de 8. Como a prioridade de encaminhamento num adaptador é 6, não será seleccionada para uma ligação de envio, a menos que todas as interfaces de prioridade de encaminhamento individual de 8 estejam em baixo.

Todas as interfaces de envio devem ser colocadas à mesma prioridade. Se algumas tiverem um valor e outras outro valor, apenas as interfaces com maior valor serão utilizadas.

Tenha em atenção que o DNS aponta para a interface 10.6.7.3, tornando-a a interface de recepção. Mesmo que decida não utilizar a prioridade de encaminhamento duplicado, deve sempre definir um encaminhamento assumido para fora do sistema em cada interface, utilizando o parâmetro interface de ligação preferencial.

Equilíbrio de volume utilizando o IP virtual e o ARP de proxy

Pode utilizar o IP virtual e o ARP de proxy para efectuar equilíbrio de volume em várias interfaces. Este método de equilíbrio de volume de trabalho suporta volumes de trabalhos de recepção e de envio.

As vantagens da utilização do IP virtual e do ARP de proxy como método de equilíbrio de volume de trabalho são as seguintes:

- Suporta volumes de trabalho de recepção e de envio.
- Suporta clientes locais.
- Faculta mais flexibilidade do que os métodos de equilíbrio de volume baseado em encaminhamento duplicado e de equilíbrio de volume baseado em DNS.

A desvantagem deste método de equilíbrio de volume de trabalho consiste em ser uma solução baseada em ligações e não uma solução baseada em volume. O volume de cada interface não é considerado. Parte-se do princípio que o volume de tráfego é idêntico em todas as ligações.

O exemplo seguinte tira o máximo partido da utilização de endereços de IP virtual. Para além de associar um único endereço de IP virtual a cada aplicação, este exemplo faculta equilíbrio de ligações de recepção e de envio e um determinado nível de tolerância a falhas.

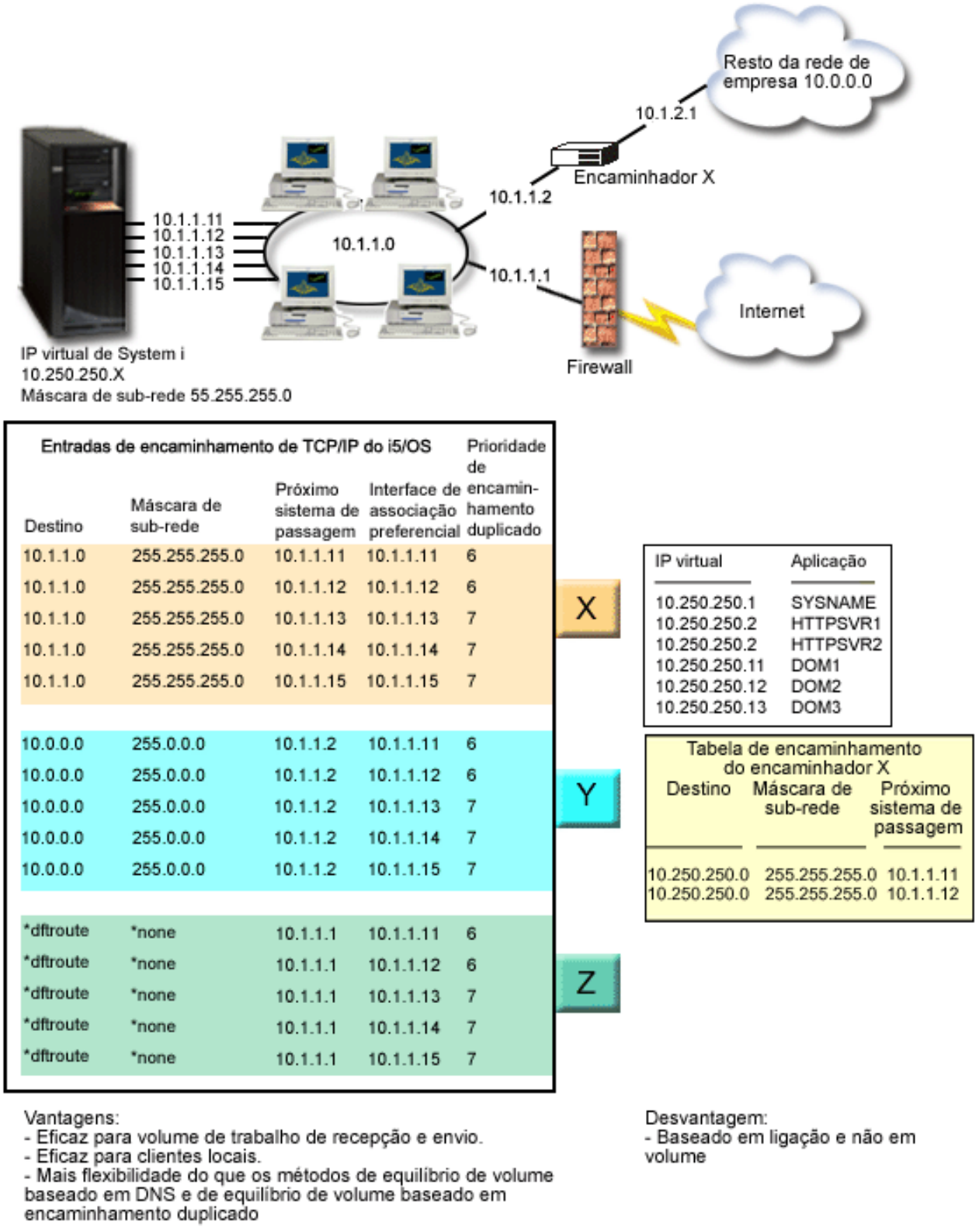


Figura 3. Equilíbrio de volume utilizando o IP virtual e o ARP de proxy

Neste exemplo, o equilíbrio de ligação de recepção é conseguido utilizando endereços de IP virtual definidos no sistema e utilizando o encaminhador, a firewall e o comutador externos que consigam executar encaminhamento de nível três (nível de rede). O equilíbrio de ligação de recepção é conseguido

utilizando os parâmetros de interface de associação preferencial e de prioridade de encaminhamento duplicado nas entradas de encaminhamento de TCP/IP do i5/OS. As ligações de envio são distribuídas sequencialmente por todas as interfaces na mesma prioridade de encaminhamento duplicado quando o valor desta prioridade estiver definido acima do valor predefinido de 5. Se todas as interfaces de valor um ficaram indisponíveis, o sistema comuta para as interfaces do próximo valor mais baixo.

Segundo as directivas de encaminhamento configuradas no encaminhador X, as interfaces 0.1.1.11 e 10.1.1.12 estão configuradas como as interfaces de recepção principais. As ligações de recepção são distribuídas sequencialmente pelas interfaces 10.1.1.11 e 10.1.1.12, função esta que é facultada pela maioria dos encaminhadores.

Segundo as entradas de encaminhamento de TCP/IP do i5/OS, as interfaces 10.1.1.13, 10.1.1.14 e 10.1.1.15 com uma prioridade de encaminhamento duplicado de 7 são configuradas como as interfaces de envio principais. As ligações de envio são distribuídas sequencialmente pelas interfaces 10.1.1.13, 10.1.1.14 e 10.1.1.15. Caso estas três interfaces estejam todas desactivadas, as interfaces 10.1.1.11 e 10.1.1.12 com uma prioridade de encaminhamento duplicado de 6 são utilizadas para as ligações de envio e recepção.

Neste exemplo, as entradas de encaminhamento de TCP/P do i5/OS são formadas por três grupos. O grupo X faculta equilíbrio de ligações de envio ao segmento local da rede empresarial (10.1.1.0). O grupo Y faculta equilíbrio de ligações de envio ao resto da rede empresarial (10.0.0.0) através do encaminhador. O grupo Z faculta equilíbrio de ligações de envio à Internet através da firewall.

Conceitos relacionados

"Cenário: Mudança de recurso de adaptador utilizando o IP virtual e o ARP de proxy"
Os endereços de IP virtuais permitem-lhe atribuir um endereço ao sistema, em vez de atribui-lo a uma interface específica. Pode definir o mesmo endereço para vários sistemas, o que permite muitas novas opções para o equilíbrio de volume.

Cenário: Mudança de recurso de adaptador utilizando o IP virtual e o ARP de proxy

Os endereços de IP virtuais permitem-lhe atribuir um endereço ao sistema, em vez de atribui-lo a uma interface específica. Pode definir o mesmo endereço para vários sistemas, o que permite muitas novas opções para o equilíbrio de volume.

Nota: Este cenário de mudança de recurso refere-se a um único adaptador e não a uma grande interrupção do sistema que seria resolvida pela criação de um conjunto de unidades. Esta solução requer a existência de um sistema de equilíbrio de volume externo.

Situação

O seu sistema de produção trata a entrada de dados quer a partir do cliente remoto, quer a partir do cliente de rede local. Tem a aplicação crítica da empresa incluída. À medida que a empresa se foi desenvolvendo, também aumentaram as respectivas exigências sobre o hardware System i e sobre a rede. Devido a este crescimento, tornou-se imperativo que este sistema estivesse disponível na rede sem tempos de inactividade imprevistos. Se, por qualquer motivo, um adaptador de rede ficar indisponível, outros adaptadores de rede no sistema deverão tomar o lugar do primeiro, de modo a que os clientes da rede não se apercebam de quaisquer falhas.

Objectivos

O conceito de disponibilidade tem muitos aspectos diferentes de redundância e cópia de segurança relativamente a componentes em falha. Neste cenário, o objectivo consiste em providenciar a disponibilidade da rede no sistema para os respectivos clientes, em caso de falha do adaptador.

Detalhes

Uma forma de resolver a situação anterior é estabelecer várias ligações físicas à rede local a partir da plataforma System i. Considere a figura que se segue.

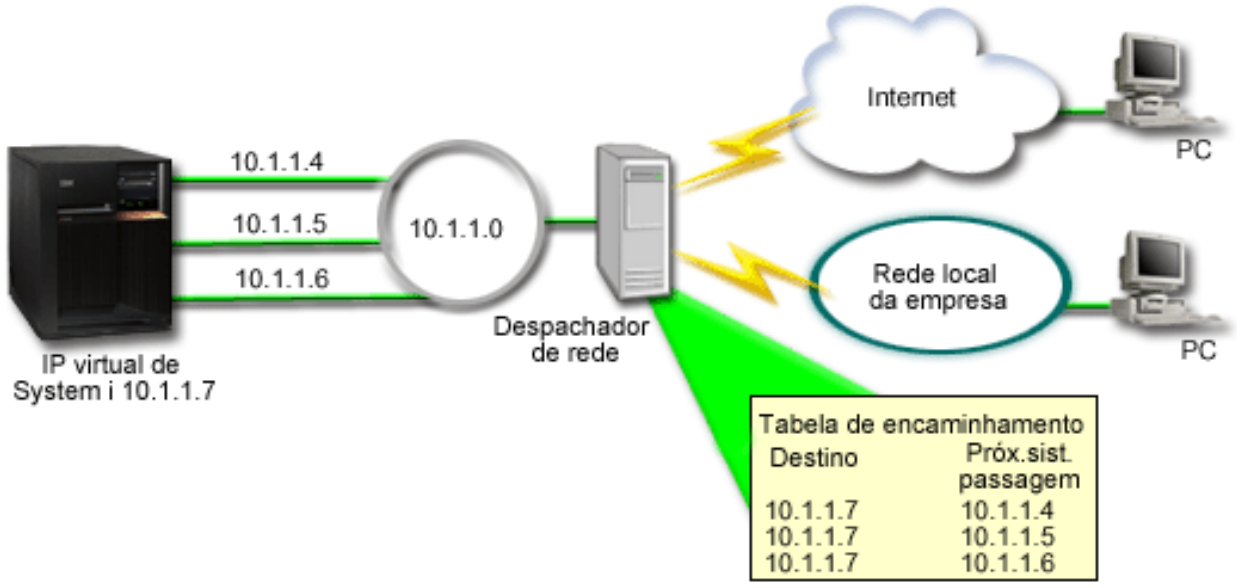


Figura 4. Mudança de recurso de adaptador sem clientes locais

Cada ligação física possui um endereço de IP diferente. Em seguida, poder-se-ia atribuir um endereço de IP virtual ao sistema. Este endereço de IP virtual é o endereço de IP pelo qual todos os respectivos clientes o reconhecem. Todos os clientes remotos (clientes que não estão fisicamente ligados à mesma rede local que a plataforma System i) comunicam com o sistema através de um servidor de equilíbrio de volume externo como, por exemplo, um despachador de rede. Quando os pedidos de IP provenientes dos clientes remotos passam pelo despachador de rede, este encaminha os endereços de IP virtuais para um dos adaptadores de rede no sistema.

Se a rede local à qual está ligado o sistema tiver clientes, estes clientes não utilizarão o despachador de rede para direccionar o respectivo tráfego localmente associado porque isso sobrecarrega desnecessariamente o despachador de rede. Pode criar entradas de encaminhamento em cada cliente semelhantes às tabelas de encaminhamento no despachador de rede. Todavia, não é prático a rede local ter um vasto número de clientes locais. Esta situação é ilustrada na figura que se segue.

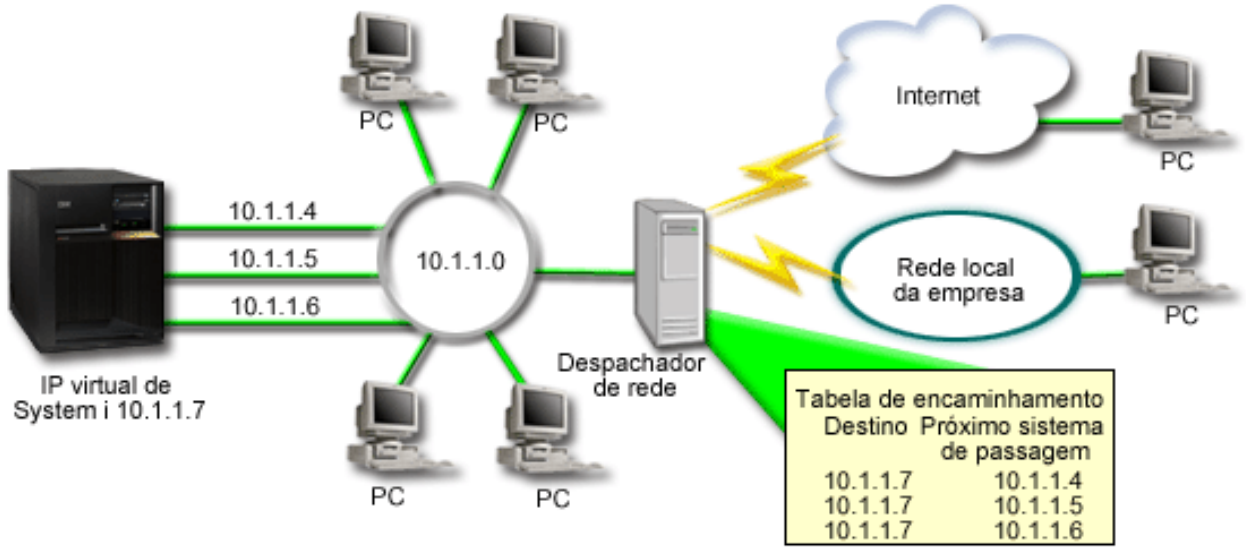


Figura 5. Mudança de recurso de adaptador sem clientes locais

Os clientes locais (clientes ligados à mesma rede local do sistema) podem estabelecer ligação do endereço de IP virtual do sistema por intermédio de ARP. Isto permite que os clientes locais disponham igualmente de uma solução de mudança de recurso de adaptador.

Em cada um dos casos, nem os clientes locais nem os remotos estão a par da mudança de recurso quando esta ocorre. O sistema escolhe os adaptadores e endereços de IP que constituem a interface preferencial para a selecção de agente de Protocolo de Resolução de Endereços de Proxy (ARP) do endereço de IP virtual (VIPA).

Pode seleccionar manualmente quais os adaptadores e endereços de IP que deverão constituir a interface preferencial da selecção de agente de ARP de proxy do VIPA. Pode seleccionar a interface a utilizar criando uma lista de interface preferenciais, caso ocorra uma falha do adaptador. Uma lista de interfaces preferenciais é uma lista ordenada dos endereços de interfaces que substituem os adaptadores falhados. Pode utilizar o System i Navigator ou a interface de programação de aplicações (API) Change TCP/IP IPv4 Interface (QTOCC4IF) para configurar uma lista de interfaces preferenciais. A lista de interfaces preferenciais também é configurável para interfaces de Ethernet virtual e de endereço de IP virtual.

Utilizando a Figura 2 como exemplo, os clientes remotos comunicam com o sistema local recorrendo ao endereço de IP virtual 10.1.1.7. Parta do princípio que 10.1.1.4 é o adaptador local inicial utilizado nesta comunicação e que pretende que 10.1.1.5 substitua o 10.1.1.4, caso este falhe. Também pretende que a interface 10.1.1.6 substitua os adaptadores de 10.1.1.4 e10.1.1.5, caso estes falhem. Para controlar a ordem pela qual estas interfaces são utilizadas numa situação de mudança de recursos, pode definir uma lista de interfaces preferenciais para o endereço de IP virtual 10.1.1.7. Neste caso, trata-se de uma lista ordenada de endereços de interfaces formada por 10.1.1.4, 10.1.1.5 e 10.1.1.6.

A solução também pode envolver a utilização de duas ou mais plataformas System i que se suportem mutuamente. Caso um dos sistemas ficar indisponível, o segundo sistema pode funcionar como mudança de recurso. A figura que se segue mostra a mesma configuração utilizando dois sistemas.

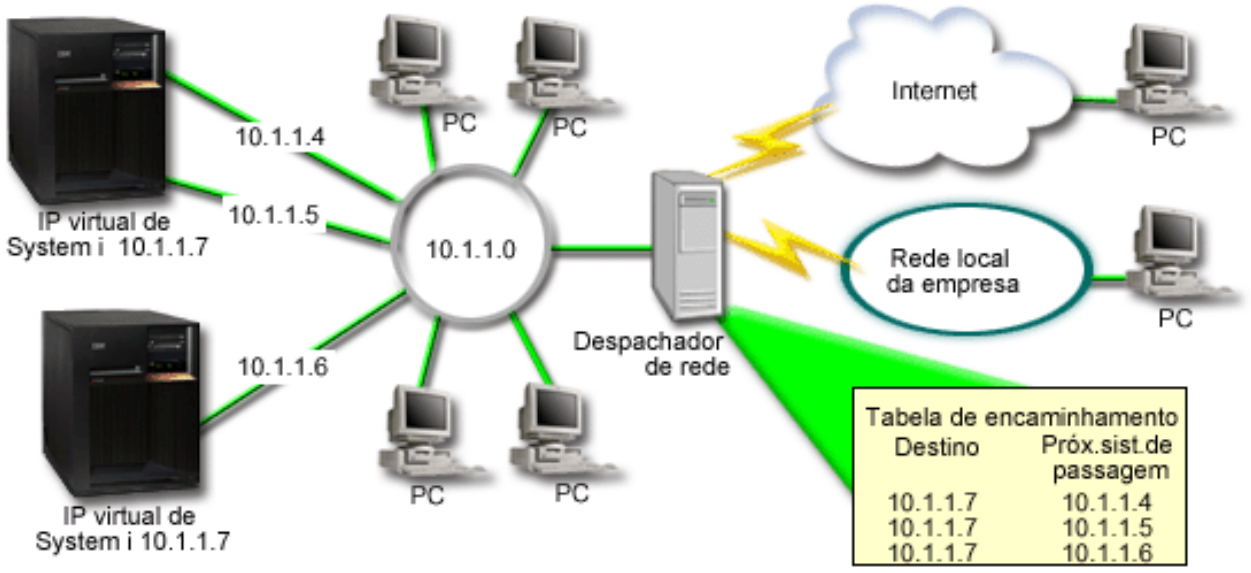


Figura 6. Mudança de recurso de adaptador com várias plataformas System i e clientes locais

O encaminhamento de pacotes é igual ao encaminhamento para um único sistema e para os respectivos clientes remotos; no entanto, existe uma diferença distinta quanto aos clientes locais. Se tiver vários sistemas a utilizar o mesmo endereço IP virtual, só poderá utilizar proxy para um dos sistemas. Neste caso, pretende que o sistema com as duas ligações de rede local funcione como proxy.

Passos de configuração

A configuração do equilíbrio de volume utilizando o IP virtual e o ARP de proxy é muito semelhante às configurações padrão de TCP/IP, com a adição de uma interface de TCP/IP virtual.

Conceitos relacionados

"Equilíbrio de volume utilizando o IP virtual e o ARP de proxy" na página 34
Pode utilizar o IP virtual e o ARP de proxy para efectuar equilíbrio de volume em várias interfaces. Este método de equilíbrio de volume de trabalho suporta volumes de trabalhos de recepção e de envio.

Mudança de recurso utilizando a selecção automática de interfaces

Utilize estes passos para configurar o IP virtual e o ARP de proxy em situações de mudança de recurso de adaptador neste cenário.

Utilizando a Figura 2 como exemplo, os passos de configuração geral seriam:

1. Configure uma interface de TCP/IP virtual.

   Utilizando o System i Navigator, crie uma interface de TCP/IP virtual. Poderá encontrar o assistente de Novas Interfaces de IP Virtuais em: **Rede** → **Configuração de TCP/IP** → **IPv4** → **Interfaces**. De seguida, faça clique com o botão direito do rato em **Interfaces** e seleccione **Nova interface** → **Virtual IP**.

   Para o nosso exemplo, introduza um endereço de IP 10.1.1.7 com uma máscara de sub-rede 255.255.255.255. Após criar a interface virtual, faça clique com o botão direito do rato na interface e seleccione **Propriedades**. Faça clique sobre o separador **Avançadas** e seleccione a caixa de verificação **Activar ARP de proxy**.
2. Crie interfaces de TCP/IP para todas as suas ligações físicas à rede local.

   Utilize o assistente de Criação de Interface de TCP/IP para criar as suas interfaces de TCP/IP. O assistente encontra-se em System i Navigator e pode ser acedido por intermédio de: **Rede** →

Configuração de TCP/IP → IPv4 → Interfaces. De seguida, faça clique com o botão direito do rato em **Interfaces** e seleccione **Nova interface → Rede de área local**. Conclua o assistente para cada uma das suas ligações à rede local.

Para este exemplo, o assistente deve ser executado três vezes para introduzir os endereços de IP10.1.1.4, 10.1.1.5 e 10.1.1.6 com uma máscara de sub-rede 255.255.255.0. Após concluir cada interface, faça clique com o botão direito do rato na interface e seleccione **Propriedades**. Faça clique no separador **Avançadas** e seleccione a caixa de verificação **Interface local associada** para associar a interface à interface de IP virtual criada no passo 1.

Mudança de recurso utilizando uma lista de interfaces preferenciais

Pode criar uma lista de interfaces preferenciais para controlar a ordem pela qual as interfaces locais são utilizadas quando ocorre uma falha de adaptador.

Para criar uma lista de interfaces preferenciais, siga estes passos:

1. Em System i Navigator, expanda **Rede → Configuração de TCP/IP → IPv4**.
2. Faça clique em **Interfaces**.
3. Das listas de interfaces apresentadas, seleccione uma para o endereço de IP virtual ou para a Ethernet virtual para a qual pretende criar a lista de interfaces preferenciais.

   Utilizando a Figura 2 como exemplo, seleccione o endereço de IP virtual 10.1.1.7.
4. Faça clique com o botão direito do rato na interface e, de seguida, seleccione **Propriedades**.
5. Faça clique no separador **Avançados**.
6. No painel, seleccione os endereços de interfaces na lista Interfaces disponíveis e faça clique em **Adicionar**.

   Utilizando a Figura 2 como exemplo, seleccione as interfaces 10.1.1.4, 10.1.1.5 e 10.1.1.6, e adicione-as à lista de interfaces preferenciais uma à uma.

   Também pode remover a interface da lista de interfaces preferenciais na área de janela direita utilizando o botão **Remover** ou mova uma interface para cima e para baixo na lista para alterar a ordem utilizando os botões **Mover para cima** e **Mover para baixo**.
7. Seleccione a caixa de verificação **Activar ARP de proxy** por cima da lista de Interfaces disponíveis para activar a lista.
8. Faça clique em **OK** para guardar a lista de interfaces preferenciais que acabou de criar.

Nota: Só pode incluir 10 interfaces na lista de interfaces preferenciais. Caso configure mais de 10, a lista é truncada às primeiras 10.

Informações relacionadas sobre o encaminhamento e equilíbrio do volume de trabalho do TCP/IP

Outras colecções de tópicos do centro de informações contêm informações relacionadas com a colecção do tópico Encaminhamento e equilíbrio do volume de trabalho do TCP/IP.

Outras informações

- Domain Name System

  DNS é um sistema avançado para gerir nomes do sistema central que estão associados a endereços Internet Protocol (IP) em redes TCP/IP. É aqui que encontra os conceitos e procedimentos básicos necessários para saber como configurar e administrar o DNS.
- Partições lógicas

  Esta colecção de tópico faculta mais informações de fundo e detalhes.
- Filtragem de IP e conversão de endereços de rede

As informações desta colecção de tópico ajudam o utilizador a gerir as regras de filtragem. Algumas das funções incluem adicionar comentários, editar e visualizar.

- OptiConnect

  Esta colecção de tópico faculta mais informações sobre o encaminhamento OptiConnect.

- Serviços de Acesso Remoto: Ligações PPP

  Point-to-Point Protocol (PPP) é habitualmente utilizado para ligar um computador à Internet. PPP é um padrão da Internet e constitui o protocolo de ligação mais utilizado entre os fornecedores de serviços de Internet (ISPs).

Referências relacionadas

"Ficheiro PDF para encaminhamento e equilíbrio do volume de trabalho do TCP/IP" na página 2
Pode ver e imprimir um ficheiro PDF destas informações.

Apêndice. Avisos

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

É possível que a IBM não disponibilize, nos restantes países, os produtos, serviços ou módulos mencionados neste manual. Para obter informações sobre os produtos e serviços actualmente disponíveis na sua área, contacte um representante local IBM. Quaisquer referências nesta publicação a produtos, programas ou serviços IBM, não significam que apenas esses produtos, programas ou serviços IBM possam ser utilizados. Qualquer outro produto, programa ou serviço funcionalmente equivalente, poderá ser utilizado em substituição daqueles, desde que não infrinja qualquer dos direitos de propriedade intelectual da IBM. A avaliação e verificação do funcionamento de qualquer produto, programa ou serviço não IBM é da inteira responsabilidade do utilizador.

Nesta publicação podem ser feitas referências a patentes ou a pedidos de patente pendentes. O facto deste documento ser disponibilizado ao utilizador não confere quaisquer licenças sobre essas patentes. Todos os pedidos de informação sobre licenças deverão ser endereçados a:

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

Os pedidos de informação sobre licenças relacionados com informações de duplo-byte (DBCS), devem ser endereçados ao IBM Intellectual Property Department no seu país ou enviados, 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. Alguns Estados não permitem a exclusão de garantias, quer explícitas quer implícitas, em determinadas transacções; esta declaração pode, portanto não se aplicar ao seu caso.

Esta publicação pode conter imprecisões técnicas ou erros de tipografia. A IBM permite-se fazer alterações periódicas às informações aqui contidas; essas alterações serão incluídas nas posteriores edições desta publicação. Em qualquer altura, a IBM pode efectuar melhoramentos e/ou alterações no(s) produto(s) e/ou no(s) programa(s) descrito(s) nesta publicação, 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 da licença deste programa que pretendam informações sobre o mesmo com o objectivo de possibilitar: (i) a troca de informações entre programas criados de forma independente e outros programas (incluindo este) e (ii) a utilização mútua da informação que foi trocada, devem contactar:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Tal informação pode encontrar-se disponível e sujeita a termos e condições adequados, incluindo, nalguns casos, o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível para o mesmo é fornecido pela IBM nos termos do IBM Customer Agreement, IBM International Program License Agreement ou de qualquer acordo existente entre as partes.

Quaisquer dados de desempenho aqui contidos foram determinados num ambiente controlado. Assim sendo, os resultados obtidos noutros ambientes operativos podem variar significativamente. Algumas medições podem ter sido efectuadas em sistemas ao nível do desenvolvimento, pelo que não existem garantias de que estas medições sejam iguais nos sistemas disponíveis habitualmente. Para além disso, algumas medições podem ter sido calculadas por extrapolação. Os resultados reais podem variar. Os utilizadores deste documento devem verificar os dados aplicáveis ao seu ambiente específico.

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 declarações 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 comerciais diárias. Para ilustrá-los o melhor possível, os exemplos incluem nomes de indivíduos, firmas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e moradas reais é mera coincidência.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicações exemplo em linguagem de origem, a qual pretende ilustrar técnicas de programação em diversas plataformas operativas. Poderá copiar, modificar e distribuir estes programas exemplo sem qualquer encargo para com a IBM, no intuito de desenvolver, utilizar, comercializar ou distribuir programas de aplicação conformes à interface de programação de aplicações relativa à plataforma operativa para a qual tais programas exemplo foram escritos. Estes exemplos não foram testados exaustivamente e sob todas as condições. A IBM, por isso, não pode garantir ou sugerir acessibilidade, funcionalidade ou funcionamento destes programas.

Cada cópia ou parte destes programas exemplo ou de trabalho deles derivada deverá incluir um aviso de direitos de autor como se segue:

© (nome da empresa) (ano). Existem partes deste código derivadas de Programas Exemplo da IBM Corp.
© Copyright IBM Corp. _introduza o(s) ano(s)_. Todos os direitos reservados.

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

Informações sobre interfaces de programação

Estes documentos de publicação sobre encaminhamento e equilíbrio de volume de trabalho de TCP/IP destinam-se a Interfaces de Programação que permitem ao cliente escrever programas para utilizar os serviços do i5/OS da IBM.

Marcas Comerciais

Os termos seguintes são marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou noutros:

i5/OS
IBM
IBM (logótipo)
System i

Adobe, o logótipo Adobe, PostScript e o logótipo PostScript são marcas comerciais registadas ou marcas comerciais de Adobe Systems Incorporated nos Estados e/ou outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de outros fabricantes.

Termos e condições

As permissões de utilização destas publicações são concedidas sujeitas aos termos e condições seguintes.

Utilização pessoal: Pode reproduzir estas publicações para uso pessoal e não comercial, desde que mantenha todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas publicações, nem reproduzir, distribuir ou apresentar qualquer parte das mesmas, sem o expresso consentimento do fabricante.

Utilização comercial: Pode reproduzir, distribuir e apresentar estas publicações exclusivamente no âmbito da sua empresa, desde que mantenha todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas publicações, nem reproduzir, distribuir ou apresentar estas publicações, ou qualquer parte das mesmas fora das instalações da empresa, sem o expresso consentimento do fabricante.

À excepção das concessões expressas nesta permissão, não são concedidos outros direitos, permissões ou licenças, quer explícitos, quer implícitos, sobre as publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contidos nesta publicação.

O fabricante reserva-se o direito de retirar as permissões concedidas nesta publicação sempre que considerar que a utilização das publicações pode ser prejudicial aos seus interesses ou, tal como determinado pelo fabricante, sempre que as instruções acima referidas não estejam a ser devidamente cumpridas.

Não pode descarregar, exportar ou reexportar estas informações, excepto quando em total conformidade com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação em vigor nos E.U.A.

O FABRICANTE NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS ″TAL COMO ESTÃO″ (AS IS) E SEM GARANTIAS DE QUALQUER ESPÉCIE, QUER EXPLÍCITAS, QUER IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRACÇÃO E ADEQUAÇÃO A UM DETERMINADO FIM.