Oracle® Solaris 11.3 でのネットワーク管理のトラブルシューティング

Part No: E62591
2016 年 11 月

Part No: E62591

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。

目次

このドキュメントの使用法

- **概要** – Oracle Solaris オペレーティングシステム (OS) でのネットワーク構成に関する問題をトラブルシューティングするためのタスクについて説明します。
- **対象読者** – システム管理者。
- **前提知識** – 基本的および高度なネットワーク管理の概念と実践に関する理解。

製品ドキュメントライブラリ

この製品および関連製品のドキュメントとリソースは http://www.oracle.com/pls/topic/lookup?ctx=E62101-01 で入手可能です。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

♦ ♦ ♦ 第 1 章

1 ネットワーク管理の問題のトラブルシューティング

この章では、ネットワーク構成、ネットワーク接続、および各種のエラー状態に関する問題を含む、ネットワーク上で発生する可能性のあるさまざまな問題をトラブルシューティングする方法について説明します。

Oracle Solaris 10 から Oracle Solaris 11 に移行している場合は、このリリースでのネットワーク管理の詳細について『Oracle Solaris 10 から Oracle Solaris 11.3 への移行』 の第 7 章,「ネットワーク構成の管理」を参照してください。

この章の内容は、次のとおりです。

ネットワーク管理に関する一般的な質問への答え

ネットワーク管理の固定モードを使用している場合は、次のトラブルシューティング情報を参照してください。リアクティブモードを使用している場合のネットワーク管理の問題のトラブルシューティングについては、67 ページの「プロファイルベースのネットワーク構成に関する一般的な質問への答え」を参照してください。詳細は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「ネットワーク構成モードについて」を参照してください。

質問: インストール後にシステムで使用されているネットワークモードを確認するにはどうしたらよいでしょうか。

回答: ネットワークモードは、インストール中にアクティブにされるプロファイルで確認します。`DefaultFixed` プロファイルがアクティブにされている場合は、固定モードになっています。`Automatic` プロファイルがアクティブにされている場合は、リアクティブモードになっています。現在システム上でアクティブになっているモードを確認するには、`netadm list` コマンドを次のように使用します。

```
# netadm list
```

質問: インストール後にシステムがデフォルトでリアクティブモードになります。この問題はどのようにして修正できますか。

回答: `DefaultFixed` プロファイルを有効にすることによって、固定モードに切り替える必要があります。アクティブなプロファイルを切り替えるには、`netadm` コマンドを次のように使用します。

```
# netadm enable -p ncp DefaultFixed
```

質問: インストール中にシステムを手動で構成し、`netadm list` では固定モードを使用していることが示されますが、システムのネットワークが依然として正しく構成されていません。どうしたらよいでしょうか。

回答: その答えは、どのネットワークコンポーネントが正しく構成されていないかによって異なります。固定モードでは、`dladm` および `ipadm` コマンドを使用してネットワークを構成します。インストール時に設定できる構成パラメータのタイプを考慮すると、もっとも可能性が高いのは IP インタフェースまたはアドレスが正しく構成されていないことです。

どのネットワークコンポーネントを再構成する必要があるかを特定するには、まず現在のネットワーク構成を次のように表示します。

```
# ipadm
```

IP アドレスが正しくない場合は、そのアドレスを削除してから正しい IP アドレス (静的 IP アドレスや DHCP アドレスなど) を作成する必要があります。

次の例は、IP 構成の IPv6 `addrconf` 部分を削除する方法を示しています。この例では、`ipadm` コマンドを実行することによって IPv6 `addrconf` アドレスが特定されています。

```
# ipadm
NAME              CLASS/TYPE STATE        UNDER      ADDR
lo0               loopback   ok           --         --
lo0/v4            static     ok           --         127.0.0.1/8
lo0/v6            static     ok           --         ::1/128
net0              ip         ok           --         --
net0/v4           dhcp       ok           --         10.1.1.10/24
net0/v6           addrconf   ok           --         fe80::8:20ff:fe90:10df/10
# ipadm delete-addr net2/v6
```

```
# ipadm
NAME              CLASS/TYPE STATE        UNDER      ADDR
lo0               loopback   ok           --         --
lo0/v4            static     ok           --         127.0.0.1/8
lo0/v6            static     ok           --         ::1/128
net0              ip         ok           --         --
net0/v4           dhcp       ok           --         10.1.1.10/24
```

次に、ほかの既存の IP 構成を削除せずに、ネットマスクプロパティーだけを次のように設定します。

```
# ipadm set-addrprop -p prefixlen=len  addrobj-name
```

完全な手順については、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 第 3 章, 「Oracle Solaris での IP インタフェースとアドレスの構成および管理」を参照してください。

質問: システム上で永続的なデフォルトルートを構成するにはどうしたらよいでしょうか。

回答: `/etc/defaultrouter` ファイルは Oracle Solaris 11 では非推奨であるため、このファイルの編集によってデフォルトルートを管理することはできなくなりました。また、新規インストールのあと、このファイルをチェックしてシステムのデフォルトルートを確認することもできなくなりました。

ルート (デフォルトまたはそれ以外) を次のように表示および構成します。

- 永続的に作成されたルートを次のように表示します。

  ```
  # route -p show
  ```

- 永続的なデフォルトルートを次のように追加します。

  ```
  # route -p add default ip-address
  ```

- システム上の現在アクティブなルートを次のように表示します。

  ```
  # netstat -rn
  ```

『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の「永続的 (静的) ルートの作成」を参照してください。

質問: システムの MAC アドレスを表示するにはどうしたらよいでしょうか。

回答: システム内の物理リンクの MAC アドレスは次のように表示します。

```
# dladm show-phys -m
```

Oracle Solaris 10 では、同様の情報を表示するために `ifconfig` コマンドが使用されます。`ifconfig(5)` のマニュアルページを参照してください。

システム内のすべてのリンク (物理および物理以外) の MAC アドレスは次のように表示します。

```
# dladm show-linkprop -p mac-address
```

質問: `dladm show-dev` コマンドを使用してシステム内の物理リンクを表示することができなくなりました。現在はどのようなコマンドを使用したらよいでしょうか。

回答: `dladm show-phys` コマンドを次のように使用します。

```
# dladm show-phys
LINK              MEDIA               STATE      SPEED  DUPLEX    DEVICE
net0              Ethernet            up         0      unknown   vnet0
```

質問: システム上のリンク名、デバイス、および場所の間のマッピングを表示するにはどうしたらよいでしょうか。

回答: 次のように、`-L` オプションを指定して `dladm show-phys` コマンドを使用します。

```
# dladm show-phys -L
LINK         DEVICE       LOCATION
net0         e1000g0      MB
net1         e1000g1      MB
net2         e1000g2      MB
net3         e1000g3      MB
net4         ibp0         MB/RISER0/PCIE0/PORT1
net5         ibp1         MB/RISER0/PCIE0/PORT2
net6         eoib2        MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
net7         eoib4        MB/RISER0/PCIE0/PORT2/cloud-nm2gw-2/1A-ETH-2
```

質問: システムでサポートされている MTU の範囲を確認するには、どのようなコマンドを使用したらよいでしょうか。

回答: 次の例に示すように、この情報を確認するには `ipadm show-ifprop` コマンドを使用します。最後の列に、サポートされる MTU の範囲が表示されます。

```
# ipadm show-ifprop -p mtu interface
```

質問: インストール後にシステム上のネームサービスの設定が失われているか、または正しく構成されていない場合はどうなるでしょうか。

回答: 固定モードを使用している場合、ネームサービスの構成は、インストール中に指定された内容になるはずです。このリリースでは、ネームサービスはサービス管理機能 (SMF) によって構成されます。ネームサービスを構成する方法、およびインストール後にクライアントシステムにネームサービス構成をインポートする方法については、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 第 4 章, 「Oracle Solaris クライアントでのネームサービスとディレクトリサービスの管理」を参照してください。

注記 - リアクティブモードを使用している場合は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「場所の作成」を参照してください。

質問: 最初からやり直してシステムのすべてのネットワーク設定を再構成するにはどうしたらよいでしょうか。

回答: Oracle Solaris インスタンス (ネットワーク設定を含む) を構成解除して再構成するには、次のようにします。

```
# sysconfig unconfigure -g network,naming_services
```

質問: `dladm create-vlan` コマンドを使用した仮想 LAN (VLAN) の作成と、`dladm create-vnic -v VID ...` コマンドを使用した仮想 NIC (VNIC) の作成の違いは何ですか。また、もう一方のコマンドよりそのコマンドを使用することが必要になる、両方のコマンドの固有の機能とは何ですか。

回答: これらの各機能は、ネットワークのニーズや、実現しようとしている内容に応じて異なる目的に使用されます。

VLAN は、ネットワークスタックのデータリンク層 (L2) での LAN の分割です。VLAN を使用すると、ネットワークを、物理ネットワーク環境に追加することなくサブネットワークに分割できます。そのため、サブネットワークは仮想的であり、同じ物理ネットワークリソースを共有します。VLAN では、保守しやすい小さなグループが使用されるため、ネットワーク管理が容易になります。

VNIC は、物理ネットワークインタフェースカード (NIC) と同じデータリンクインタフェースを使用する仮想ネットワークデバイスです。VNIC は、ベースとなるデータリンク上に構成します。構成された VNIC は、物理 NIC のように動作します。使用されているネットワークインタフェースに応じて、デフォルトアドレス以外の VNIC に MAC アドレスを明示的に割り当てることができます。

どのネットワーク管理方法を使用すべきかについての詳細は、『Oracle Solaris 11.3 でのネットワーク管理の計画』 の 第 1 章,「Oracle Solaris ネットワーク管理のサマリー」を参照してください。

ネットワーク接続および構成に関する問題のトラブルシューティング

ネットワーク接続および構成に関する問題をトラブルシューティングするための一般的なガイドラインを次に示します。

ネットワーク上の問題の最初の兆候の 1 つは、1 つまたは複数のホストでの通信の損失です。システムがはじめてネットワークに追加されたときに動作しない場合は、障害のある NIC の問題か、または SMF によって管理されているネットワークデーモンに関する問題である可能性があります。

以前にネットワークに接続された単一システムで突然ネットワークの問題が発生した場合は、システムのネットワークインタフェース構成の問題である可能性がありま

す。ネットワーク上のシステムが互いに通信できるが、ほかのネットワークと通信できない場合は、ルーターの問題である可能性があります。ほかのネットワークにも別の問題が考えられます。

基本的なネットワーク構成チェックの実行

`dladm` および `ipadm` コマンドを使用して、1 つのシステムでのネットワーク構成の問題をトラブルシューティングできます。これらの 2 つのコマンドは、オプションなしで使用された場合、現在のネットワーク構成に関する役立つ情報を提供します。

これらのコマンドを使用して構成に関する問題をトラブルシューティングするための方法のいくつかを次に示します。

- `dladm` コマンドを使用して、システム上のすべてのデータリンクに関する一般的な情報を表示します。

```
# dladm
LINK        CLASS     MTU     STATE     OVER
net0        phys      1500    up        --
```

- データリンク、その汎用名、および対応するネットワークデバイスインスタンスの間のマッピングに関する情報を次のように表示します。

```
# dladm show-phys
LINK     MEDIA        STATE     SPEED     DUPLEX     DEVICE
net0     Ethernet     up        1000      full       e1000g0
```

- `ipadm` コマンドを使用して、システム上のすべての IP インタフェースに関する一般的な情報を表示します。

```
# ipadm
NAME         CLASS/TYPE STATE     UNDER  ADDR
lo0          loopback   ok        --     --
 lo0/v4       static    ok        --     127.0.0.1/8
 lo0/v6       static    ok        --     ::1/128
net0         ip         ok        --     --
 net0/v4      static    ok        --     10.132.146.233/24
```

- `ipadm show-` *interface* コマンドを使用して、特定の IP インタフェースに関する情報を表示します。

```
# ipadm show-if net0
IFNAME     CLASS    STATE    ACTIVE OVER
net0       ip       ok       yes    --
```

- システム上のすべてのインタフェースに関する情報を次のように表示します。

```
# ipadm show-if
IFNAME       CLASS        STATE     ACTIVE     OVER
```

```
lo0          loopback     ok        yes        --
net0         ip           ok        yes        --
```

- システム上のすべての IP アドレスに関する情報を次のように表示します。

```
# ipadm show-addr
ADDROBJ           TYPE       STATE     ADDR
lo0/v4            static     ok        127.0.0.1/8
net0/v4           static     ok        192.168.84.3/24
```

- `ipadm show-addr` *interface* コマンドを使用して、特定のインタフェースの IP アドレスに関する情報を表示します。

```
# ipadm show-addr net0
ADDROBJ           TYPE     STATE        ADDR
net0/v4           dhcp     ok           10.153.123.225/24
```

- 特定の IP アドレスのプロパティーを次のように表示します。

```
# ipadm show-addrprop net1/v4
ADDROBJ           PROPERTY   PERM CURRENT         PERSISTENT      DEFAULT   POSSIBLE
net0/v4           broadcast  r-   10.153.123.255  --              10.255.255.255  --
net0/v4           deprecated rw   off             --              off   on,off
net0/v4           prefixlen  rw   24              --              8   1-30,32
net0/v4           private    rw   off             --              off   on,off
net0/v4           reqhost    r-   --              --              --   --
net0/v4           transmit   rw   on              --              on   on,off
net0/v4           zone       rw   global          --              global
```

詳細は、ipadm(1M) のマニュアルページを参照してください。

ネットワークサービスおよびデーモンが実行されていることの確認

ネットワーク接続に関する問題のトラブルシューティングにおける重要なステップは、システム上で実行されているすべての SMF ネットワークサービスの現在のステータスを確認することです。

システム上で実行されているすべての SMF ネットワークサービスの現在のステータスは、次のように確認できます。

```
$ svcs svc:/network/*
```

コマンド出力によって、あるサービスが無効になっているか、または保守状態にあることが示される場合は、その特定のサービスに関する詳細情報を次のように取得できます。

```
$ svcs -xv service-name
```

たとえば、svc:/network/loopback:default SMF ネットワークサービスに関する詳細情報は、次のように取得します。

```
$ svcs -xv svc:/network/loopback:default
svc:/network/loopback:default (loopback network interface)
 State: online since Thu Dec 05 19:30:54 2013
   See: man -M /usr/share/man -s 1M ifconfig
   See: /system/volatile/network-loopback:default.log
Impact: None.
```

基本的なネットワーク診断チェックの実行

ネットワークの問題の原因で表には見えにくいものに、ネットワークパフォーマンスの低下があります。ネットワークで問題が発生している場合は、基本的な問題を診断して修正するために一連のソフトウェアチェックを実行できます。たとえば、ping コマンドを使用すると、システムでのパケットの損失などの問題を定量化できます。または、netstat コマンドを使用して、ルーティングテーブルやプロトコルの統計情報を表示できます。これらのタイプのネットワークの問題をトラブルシューティングするために使用できる各種の方法の詳細は、25 ページの「TCP/IP ネットワーク上の問題をモニターおよび検出するためのリソース」を参照してください。

ネットワークモニターユーティリティーを使用したネットワーク診断の実行については、第5章「network-monitor トランスポートモジュールユーティリティーを使用したネットワーク診断の実行」を参照してください。

サードパーティーのネットワーク診断プログラムにも、ネットワークの問題をトラブルシューティングするためのいくつかのツールが用意されています。詳細は、サードパーティー製品のドキュメントを参照してください。

▼ 基本的なネットワークソフトウェアチェックの実行方法

1. **netstat コマンドを使用して、ネットワーク情報を表示します。**

   netstat コマンドは、ネットワーク接続の問題のトラブルシューティングに役立つさまざまな情報を表示します。表示される情報の種類は、使用するオプションによって異なります。『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「netstat コマンドによるネットワークステータスのモニタリング」および netstat(1M) のマニュアルページを参照してください。

2. **hosts データベースをチェックして、すべてのエントリが正しく、かつ最新の状態になっていることを確認します。**

   /etc/inet/hosts データベースの詳細は、hosts(4) のマニュアルページを参照してください。

3. **telnet コマンドを使用して、ローカルシステムに接続してみます。**

   詳細は、telnet(1) のマニュアルページを参照してください。

4. **inetd ネットワークデーモンが実行されていることを確認します。**

```
# /usr/bin/pgrep inetd
883
```

   前の出力は、inetd デーモンがプロセス ID 883 でシステム上で実行されていることを示しています。

5. **ネットワーク上で IPv6 が有効になっている場合は、in.ndpd デーモンが実行されていることを確認します。**

```
# /usr/bin/pgrep in.ndpd
822
```

   前の出力は、inetd デーモンがプロセス ID 882 でシステム上で実行されていることを示しています。

6. **システムのルーターとルーティング情報を確認します。**

   - **システムの永続的なルートを次のように表示します。**

```
# route -p show
```

     19 ページの「永続的なルートを追加するときの問題のトラブルシューティング」を参照してください。

   - **ルーティングテーブル内の構成を次のように表示します。**

```
# netstat -nr
```

永続的なルートを追加するときの問題のトラブルシューティング

route コマンドは、ネットワークルーティングテーブルを管理するために使用されます。ネットワークルーティングテーブルへのすべての変更がシステムのリブートのあとも確実に永続されるようにするには、-p オプションを使用します。

注記 - 永続的なルートを追加するときは、追加されるすべてのルートが既存の永続的な構成と競合しないように十分に注意することが重要です。

永続的な構成の中にルートがすでに存在するかどうかを次のように確認します。

```
# route -p show
persistent: route add default 10.153.123.1 -ifp net0
```

永続的な構成の中にルートがすでに存在する場合は、永続的な構成ではないネットワークルーティングテーブル内の情報が、永続的な構成とは異なる可能性があります。

次の例は、この点をさらに詳細に示しています。この例では、net1 に永続的なルートを追加しようとしています。ただし、前の例の出力に従って net0 の永続的なルートがすでに存在するため、このコマンドは失敗します。

```
# route -p add default 10.153.123.1 -ifp net1
add net default: gateway 10.153.123.1
add persistent net default: gateway 10.153.123.1: entry exists
Warning: persistent route might not be consistent with routing table.
```

route -p show コマンドを再度実行すると、次の出力に示すように、永続的なルートは変更されずに引き続き net0 用に構成されていることがわかります。

```
# route -p show
persistent: route add default 10.153.123.1 -ifp net0
```

ただし、次の出力に示すように、このコマンドにより、カーネル内のルーティングテーブルは net1 を使用するように変更されました。

```
# netstat -nr

Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use Interface
-------------------- -------------------- ----- ----- ---------- ---------
default              10.153.123.1         UG        2          1 net1
10.153.123.0         10.153.123.78        U         3          0 net1
127.0.0.1            127.0.0.1            UH        2        466 lo0
.
.
.
```

そのため、新しいルートの追加を構成する前に、既存の永続的なルートをすべて削除することが常に最善です。詳細は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「永続的 (静的) ルートの作成」を参照してください。

インタフェース構成のエラー状態のトラブルシューティング

このセクションには、次のトピックが含まれています。

ipadm create-addr コマンドを使用して IP アドレスを割り当てることができない

Oracle Solaris 10 内のネットワーク構成に使用される従来の `ifconfig` コマンドでは、1 つのコマンドを使用して IP アドレスの plumb と割り当てを行うことができます。Oracle Solaris 11 では、`ipadm` コマンドを使用して IP インタフェースおよびアドレスを構成します。

次の例では、インタフェースに静的 IP アドレスが割り当てられることを前提にしています。このプロセスには、次の 2 つの手順が必要です。最初に、`ipadm create-ip` コマンドを使用して IP インタフェースを作成または plumb します。次に、`ipadm create-addr` コマンドを使用して、そのインタフェースに IP アドレスを割り当てます。

```
# ipadm create-ip interface
# ipadm create-addr -T addr-type -a address addrobj
```

IP アドレスの構成中に cannot create address object: Invalid argument provided というエラーメッセージが表示される

アドレスオブジェクトは、IP インタフェースにバインドされた特定の IP アドレスを識別します。アドレスオブジェクトは、IP インタフェース上の IP アドレスごとの一意の識別子です。同じ IP インタフェースに割り当てる 2 番目の IP アドレスを識別するには、別のアドレスオブジェクトを指定する必要があります。同じアドレスオブジェクト名を使用する場合は、最初のアドレスオブジェクトインスタンスを削除してから別の IP アドレスに割り当てる必要があります。

次のいずれかの方法を使用します。

- 次のように、別のアドレスオブジェクトを指定して 2 番目の IP アドレスを識別します。

```
# ipadm show-addr
ADDROBJ   TYPE     STATE   ADR
lo0       static   ok      127.0.0.1/10
net0/v4   static   ok      192.168.10.1

# ipadm create-addr -T static -a 192.168.10.5 net0/v4b
# ipadm show-addr
ADDROBJ   TYPE     STATE   ADR
lo0       static   ok      127.0.0.1/10
net0/v4   static   ok      192.168.10.1
net0/v4b  static   ok      192.168.10.5
```

- 次のように、そのアドレスオブジェクトの最初のインスタンスを削除してから、同じアドレスオブジェクトを別の IP アドレスに割り当てます。

```
# ipadm show-addr
ADDROBJ   TYPE     STATE   ADR
lo0       static   ok      127.0.0.1/10
net0/v4   static   ok      192.168.10.1
# ipadm delete-addr net0/v4
# ipadm create-addr -T static -a 192.168.10.5 net0/v4
# ipadm show-addr
ADDROBJ   TYPE     STATE   ADR
lo0       static   ok      127.0.0.1/10
net0/v4   static   ok      192.168.10.5
```

IP インタフェースの構成中に cannot create address: Persistent operation on temporary object というエラーメッセージが表示される

デフォルトでは、ipadm コマンドは永続的なネットワーク構成を作成します。構成している IP インタフェースが一時的なインタフェースとして作成された場合は、ipadm コマンドを使用して、そのインタフェース上に永続的な設定を構成することはできません。構成しているインタフェースが一時的であることを確認したら、そのインタフェースを削除し、それを永続的に再作成します。そのあと、次のように、インタフェースの構成を再開できます。

```
# ipadm show-if -o all
IFNAME    CLASS      STATE   ACTIVE   CURRENT        PERSISTENT   OVER
lo0       loopback   ok      yes      -m46-v------   46--         --
net0      ip         ok      yes      bm4---------   ----         --
```

PERSISTENT フィールドに IPv4 構成のときの 4 フラグまたは IPv6 構成のときの 6 フラグが存在しない場合は、net0 が一時的なインタフェースとして作成されたことを示します。

```
# ipadm delete-ip net0
# ipadm create-ip net0
# ipadm create-addr -T static -a 192.168.1.10 net0/v4
ipadm: cannot create address: Persistent operation on temporary object
```

IPv6 配備に関する問題のトラブルシューティング

サイトで IPv6 を計画または配備しているときに問題が発生した場合は、次の情報を参照してください。具体的な計画タスクについては、『Oracle Solaris 11.3 でのネットワーク配備の計画』 の 第 2 章,「IPv6 アドレスの使用の計画」を参照してください。

IPv6 インタフェースが正しく構成されていない

IPv6 インタフェースが存在したとしても、必ずしもシステムで IPv6 が使用されているわけではありません。そのインタフェース上で IPv6 アドレスを実際に構成するまでインタフェースは起動されません。

たとえば、`ifconfig` コマンドの次の出力は、`inet6` `net0` インタフェースが `UP` としてマークされておらず、`::/0` のアドレスを持っていること、つまり IPv6 インタフェースが構成されていないことを示しています。

```
# ifconfig net0 inet6
net0:
flags=120002000840<RUNNING,MULTICAST,IPv6,PHYSRUNNING> mtu 1500 index 2 inet6 ::/0
```

`in.ndpd` デーモンは引き続きシステム上で実行されていますが、`addrconf` アドレスが構成されていない IP インタフェース上では動作しません。

IPv4 ルーターを IPv6 にアップグレードできない

既存の装置をアップグレードできない場合は、IPv6 に対応した装置を購入することが必要になる可能性があります。製造元のドキュメントを調べて、IPv6 をサポートするために実行する必要のある装置固有の手順がないかどうかを確認してください。

特定の IPv4 ルーターは IPv6 サポート用にアップグレードできません。使用しているトポロジでこの状況が発生する場合は、代わりの方法として、IPv6 ルーターを IPv4 ルーターの次に物理的に接続できます。このようにすれば、IPv6 ルーターから IPv4 ルーター経由でトンネルできます。IP トンネルを構成する手順については、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 第 5 章, 「IP トンネルの管理」を参照してください。

サービスを IPv6 サポート用にアップグレードしているときに問題が発生する

サービスを IPv6 サポート用に準備しているときに、次の問題が発生する場合があります。

- 特定のアプリケーションは、IPv6 に移植されたあとであっても、デフォルトでは IPv6 サポートを有効にしません。このようなアプリケーションは、IPv6 が有効になるように構成する必要があります。
- 複数のサービス (一部のサービスは IPv4 のみ、ほかは IPv4 と IPv6 の両方) を実行するサーバーでは、問題が発生する場合があります。クライアントによっては両方のタイプのサービスを使用することが必要になり、これがサーバー側の混乱をもたらす場合があります。

現在の ISP が IPv6 をサポートしない

IPv6 を配備したいが、現在のインターネットサービスプロバイダ (ISP) によって IPv6 アドレス指定が提供されていない場合は、次の代わりの方法を考慮してください。

- サイトからの IPv6 通信用に 2 番目の回線を提供している別の ISP を採用します。この解決方法には、高い費用がかかります。
- 仮想 ISP を取得します。仮想 *ISP* はサイトに IPv6 接続を提供しますが、リンクは提供しません。その代わりに、サイトから IPv4 ISP 経由で仮想 ISP に到達するトンネルを作成します。
- 自分のサイトから ISP 経由でほかの IPv6 サイトに到達する 6to4 トンネルを使用します。アドレスとしては、6to4 ルーターの登録済みの IPv4 アドレスを IPv6 アドレスのパブリックトポロジの部分として使用できます。詳細は、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「6to4 トンネルを構成する方法」を参照してください。

6to4 リレールーターへのトンネルを作成するときのセキュリティー問題

本来、6to4 ルーターと 6to4 リレールーター間のトンネルは安全ではありません。次のタイプのセキュリティーの問題は、このようなトンネルに固有のものです。

- 6to4 リレールーターはパケットのカプセル化とカプセル化の解除を行いますが、パケット内に含まれるデータのチェックは行いません。
- アドレスのスプーフィングは、6to4 リレールーターとの間で構築されるトンネルにおける際立った問題です。着信トラックについては、6to4 ルーターはリレールーターの IPv4 アドレスを送信元の IPv6 アドレスと対応させることができないという問題があります。このため、IPv6 システムのアドレスは簡単にスプーフィングされかねません。6to4 リレールーターのアドレスもスプーフィングの可能性があります。
- デフォルトでは、6to4 ルーターと 6to4 リレールーターの間に信頼できるメカニズムは存在しません。そのため、6to4 ルーターは 6to4 リレールーターが信頼できるものであるかどうかや、場合によっては、それが正規の 6to4 リレールーターであるかどうかさえ識別できません。6to4 サイトと IPv6 宛先の間に信頼できる関係が存在する必要があります。そうでない場合は、両方のサイトが、可能性のある攻撃に無防備なままになります。

これらの問題や 6to4 リレールーターに固有のその他のセキュリティーの問題は、RFC 3964, Security Considerations for 6to4 (`http://www.rfc-editor.org/rfc/rfc3964.txt`) で説明されています。6to4 の使用に関する更新された情報については、RFC 6343, Advisory Guidelines for 6to4 Deployment (`http://www.rfc-editor.org/rfc/rfc6343.txt`) も参照してください。

一般には、6to4 リレールーターのサポートは次のような場合だけ検討してください。

- 信頼できるプライベートな IPv6 ネットワークとの間で 6to4 サイトが通信を行う場合。たとえば、独立した 6to4 サイトとネイティブ IPv6 サイトから構成されるキャンパスネットワーク上などでこのサポートを有効にすると便利かもしれません。
- ビジネス上の理由で、6to4 サイトと特定のネイティブ IPv6 システムとの通信を避けることができない場合。
- 6to4 に関するセキュリティー上の考慮事項 (`http://www.ietf.org/rfc/rfc3964.txt`) および6to4 配備に関するアドバイザリガイドライン (`http://www.ietf.org/rfc/rfc6343.txt`) で推奨されているチェックおよび信頼モデルを実装している場合。

TCP/IP ネットワーク上の問題をモニターおよび検出するためのリソース

次の表では、TCP/IP ネットワーク上の問題をモニターおよび検出するためのタスクについて説明しています。完全な手順については、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』を参照してください。

表 1 TCP/IP ネットワークをモニターするためのタスク

タスク	コマンドまたは説明	タスク情報
Oracle Solaris ネットワークプロトコルスタックのさまざまなレイヤーで構成されている機能のネットワークトラフィック使用状況をモニターします。	機能や、その機能がネットワークプロトコルのどのレイヤーで構成されているかに応じて、さまざまな可観測性ツールを使用して統計を収集したり、ネットワークトラフィック使用状況をモニターしたりできます。	33 ページの「ネットワーク構成およびトラフィック使用状況の監視」
すべての着信 TCP 接続の IP アドレスをログに記録します。	トランスポート層プロトコルは通常、正しく動作するために介入を必要としません。ただし、状況によっては、トランスポート層プロトコル経由で動作するサービスをログ記録または変更することが必要になる場合があります。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「すべての着信 TCP 接続の IP アドレスをロギングする方法」
リモートシステムが動作しているかどうかを確認します。	`ping` コマンドを使用して、リモートシステムのステータスを確認します。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「リモートシステムが到達可能かどうかの確認」
システムでパケットが破棄されているかどうかを検出します。	`ping` コマンドの `-s` オプションを使用して、リモートシステムが動作しているにもかかわらず、パケットを破棄しているかどうかを確認します。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「システムとリモートシステム間でパケッ

タスク	コマンドまたは説明	タスク情報
		トが失われているかどうかの確認」
プロトコルごとのネットワークの統計情報を表示します。	`netstat` コマンドを使用して、TCP、Stream Control Transmission Protocol (SCTP)、およびユーザーデータグラムプロトコル (UDP) エンドポイントに対するプロトコルごとの統計情報を表形式で表示します。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「netstat コマンドによるネットワークステータスのモニタリング」
TCP および UDP 管理を実行します。	`netcat` (または `nc`) ユーティリティーを使用して、TCP 接続の確立、UDP パケットの送信、すべての TCP および UDP ポート上での待機、ポートスキャンの実行などを行います。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「netcat ユーティリティーを使用した TCP と UDP の管理の実行」
IPv4 ルーティングデーモンのアクション (すべてのパケット転送を含む) を追跡します。	`routed` デーモンの誤動作が疑われる場合は、デーモンのアクティビティーを追跡するログを開始できます。`routed` デーモンを起動すると、このログにはすべてのパケット転送が記録されます。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「IPv4 ルーティングデーモンのアクションのロギング」
リモートシステムへのルートを検出します。	`traceroute` コマンドを使用して、リモートシステムへのルートを検出します。この出力には、パケットがたどるパス内のホップの数が表示されます。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「リモートホストまでのルートの発見」
IPv4 サーバーとクライアントの間のパケットを確認します。	仲介するトラフィックを確認するために、IPv4 クライアントまたはサーバーのどちらかに接続されている、ハブから離れたスヌープシステムを確立します。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「IPv4 サーバー/クライアント間のパケットを確認する方法」
パケット転送プロセスをモニターします。	`snoop` コマンドを使用して、パッケージ (データ) 転送の状態をモニターします。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「snoop コマンドによるパケット転送のモニタリング」
ネットワークトラフィックを分析します。	TShark コマンド行インタフェース (CLI) または Wireshark グラフィカルユーザーインタフェース (GUI) を使用して、ネットワークトラフィックを分析します。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「TShark および Wireshark を使用したネットワークトラフィックの解析」
サーバー上のネットワークトラフィックをモニターします。	`ipstat` および `tcpstat` コマンドを使用して、サーバー上のネットワークトラフィックをモニターします。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「ipstat および tcpstat コマンドを使用したネットワークトラフィックの監視」
IPv6 ネットワーク上のネットワークトラフィックをモニターします。	`snoop ip6` コマンドを使用して、ネットワークノードの IPv6 パケットのみを表示します。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「IPv6 ネッ

タスク	コマンドまたは説明	タスク情報
		トワークトラフィックのモニタリング」
システム上の IPMP のステータスをモニターします。	`ipmpstat` コマンドを使用して、IPMP のステータスに関するさまざまな種類の情報を収集します。また、このコマンドを使用すると、各 IPMP グループのベースとなる IP インタフェースや、各グループで構成されているデータおよびテストアドレスに関する情報を表示することもできます。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「IPMP 情報のモニタリング」
`ping`、`netstat`、および `traceroute` コマンドの出力を制御します。	IPv6 関連コマンドの表示出力を制御するファイル内にある `DEFAULT_IP` 変数を設定する `inet_type` という名前のファイルを作成します。	『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「IP 関連コマンドの表示出力を制御する方法」

IPMP 構成のトラブルシューティング

このセクションには、次のトピックが含まれています。

注記 - IP ネットワークマルチパス (IPMP) を構成するためのコマンドおよびタスクが変更されました。IPMP の構成や管理には、`ifconfig` コマンドの代わりに `ipadm` コマンドが使用されるようになりました。これらの 2 つのコマンドが互いにどのように対応するかについては、『Oracle Solaris 10 から Oracle Solaris 11.3 への移行』 の 「ifconfig コマンドと ipadm コマンドの比較」を参照してください。`ifconfig(5)` のマニュアルページも参照してください。

IPMP での障害検出

トラフィックを送受信するネットワークの継続的な可用性を保証するために、IPMP は、IPMP グループのベースとなる IP インタフェース上で障害検出を実行します。故障したインタフェースは、修復されるまで使用不可能なままになります。残りのアク

ティブインタフェースはすべて、必要に応じて、既存のどのスタンバイインタフェースが配備されている間も引き続き機能します。

in.mpathdデーモンは次の種類の障害検出を処理します。

- プローブベースの障害検出:
  - テストアドレスは構成されていない (推移的プローブ)
  - テストアドレスが構成されている
- リンクベースの障害検出 (NIC ドライバがサポートしている場合)

詳細は、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「IPMP での障害検出」を参照してください。

リンクベースの IPMP 構成でのアウトバウンド負荷分散の無効化

リンクベースの IPMP でアウトバウンド負荷分散を無効にすることができます。あるインタフェースをスタンバイとしてマークすると、リンクベースまたはプローブベースのどちらの障害検出が使用されているかには関係なく、そのインタフェースはアクティブインタフェースに障害が発生するまで使用されません。リンクベースの障害検出は、in.mpathd デーモンによって常に有効化されています。

ipadm コマンドを次のように使用します。

```
# ipadm set-ifprop -m ip -p standby=on interface
```

リンクベースの IPMP でインバウンドおよびアウトバウンド負荷分散がどのように機能するかについては、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「IPMP を使用する利点」を参照してください。

IPMP グループの作成中に *ipadm: cannot add net0 to ipmp0: Underlying interface has addresses managed by dhcpagent(1M)* というエラーメッセージが表示される

IPMP グループを追加しようとすると、次のエラーメッセージが表示される場合があります。

```
*ipadm: cannot add net0 to ipmp0: Underlying interface has addresses managed by dhcpagent
(1M)*
```

このメッセージは、アドレスが dhcpagent によって管理されている IP インタフェースを IPMP グループに追加できないために表示されます。回避方法として、net0 上の

DHCP またはステートフルアドレス構成、あるいはその両方を無効にしてからそれを IPMP グループに追加します。

VRRP と Oracle Solaris バンドル版 IP フィルタに関する問題のトラブルシューティング

Virtual Router Redundancy Protocol (VRRP) は、ルーターやロードバランサなどに使用される IP アドレスの高可用性を提供します。Oracle Solaris では、L2 VRRP と L3 VRRP の両方がサポートされます。詳細は、『ルーターまたはロードバランサとしての Oracle Solaris 11.3 システムの構成』 の 第 3 章,「仮想ルーター冗長プロトコルの使用」を参照してください。

標準の VRRP マルチキャストアドレス (224.0.0.18/32) は、VRRP が正しく機能することを保証するために使用されます。詳細については、http://www.rfc-editor.org/rfc/rfc5798.txt を参照してください。VRRP を Oracle Solaris バンドル版 IP フィルタで使用する場合は、マルチキャストアドレスに対して発信または着信 IP トラフィックが許可されているかどうかを明示的に確認する必要があります。

この情報を確認するには、`ipfstat -io` コマンドを次のように使用します。

```
# ipfstat -io
empty list for ipfilter(out)
empty list for ipfilter(in)
```

このコマンドの出力で、標準のマルチキャストアドレスに対してトラフィックが許可されていないことが示されている場合は、各 VRRP ルーターの IP フィルタ構成に次の規則を追加する必要があります。

```
# echo "pass out quick on VRRP VIP Interface from VRRP VIP/32 to 224.0.0.18/32 \
pass in quick on VRRP VIP Interface from VRRP IP/32 to 224.0.0.18/32" | ipf -f
```

IP フィルタ規則セットを構成する方法の詳細は、『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 「アクティブなパケットフィルタリング規則セットに規則を追加する方法」を参照してください。

♦ ♦ ♦ 第 2 章

2 可観測性ツールを使用したネットワークトラフィック使用状況のモニタリング

この章では、Oracle Solaris ネットワーク可観測性ツールを使用して構成情報を表示したり、Oracle Solaris ネットワークプロトコルスタックの各レイヤーでのネットワークトラフィック使用状況をモニターしたりする方法について説明します。

この章の内容は、次のとおりです。

この章には、選択されたネットワーク機能および特定のネットワーク構成シナリオの例が含まれています。Oracle Solaris リリースでネットワーク機能を管理する方法の詳細は、次の追加のリソースを参照してください。

- 『Oracle Solaris 11.3 でのネットワークデータリンクの管理』
- 『Oracle Solaris 11.3 での仮想ネットワークとネットワークリソースの管理』
- 『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』

ネットワークのトラブルシューティングと可観測性について

次の表では、レイヤーごとにグループ化された Oracle Solaris ネットワークプロトコルスタックの主な機能について説明しています。また、ネットワークトラフィック使用状況を監視およびモニターしたり、これらの各機能の構成を表示したりするために使用するツールに関する情報も提供されています。さまざまなネットワーク機能を管理および監視するために使用するツール (`dladm` コマンドや `dlstat` コマンドなど) の場合は、各機能に固有のサブコマンドも提供されています。

表 2 レイヤーごとにグループ化された Oracle Solaris ネットワークプロトコルスタックのネットワーク機能

ネットワークプロトコルスタックレイヤー	機能	機能領域	管理インタフェース
ハードウェアレイヤー			

ネットワークプロトコルスタックレイヤー	機能	機能領域	管理インタフェース
	物理ネットワークインタフェースカード (NIC)	ハードウェア接続	`dladm show-phys`、`dlstat show-phys`
	ドライバ構成	ドライバ接続	`driver.conf` ファイルおよび `dladm` プロパティー (`dladm show-linkprop`) を使用して管理される
データリンクレイヤー (L2)			
	アグリゲーション (DLMP およびトランキング)	高可用性	`dladm show-aggr` および `dlstat show-aggr`
	ブリッジングプロトコル: ■ STP ■ TRILL	高可用性、ネットワーク仮想化	`dladm show-bridge` および `dlstat show-bridge`
	データセンターブリッジング (DCB)	ネットワークストレージ、パフォーマンス	`lldpadm`、`dladm`
	Etherstub	ネットワーク仮想化	`dladm show-etherstub`
	エッジ仮想ブリッジング (EVB)	ネットワーク仮想化	`dladm`
	エラスティック仮想スイッチ (EVS)	ネットワーク仮想化	`evsadm`、`evsstat`、`dladm`
	フロー	可観測性、リソース管理、セキュリティー	`flowadm` および `flowstat`
	IP トンネル	IP 接続	`dladm show-iptun`、`ipadm`
	Link Layer Datalink Protocol (LLDP)	可観測性、ネットワークストレージ、ネットワーク仮想化	`lldpadm`
	仮想ローカルエリアネットワーク (VLAN)	ネットワーク仮想化	`dladm show-vlan`、`dlstat`
	仮想ネットワークインタフェースカード (VNIC)	ネットワーク仮想化	`dladm show-vnic`、`dlstat`
	Virtual eXtensible area network (VXLAN)	ネットワーク仮想化	`dladm show-vxlan`、`dlstat`
ネットワークレイヤー (L3)			
	エラスティック仮想スイッチ (EVS)	ネットワーク仮想化	`evsadm`、`evsstat`、`dladm`
	ファイアウォール	セキュリティー	`ipf` および `ipnat` によるパケットフィルタリング
	フロー	可観測性、リソース管理、セキュリティー	`flowadm`、`flowstat`
	統合ロードバランサ (ILB)	パフォーマンス	`ilbadm`、`ilbadm show-server`、`ilbadm show-servergroup`

ネットワークプロトコルスタックレイヤー	機能	機能領域	管理インタフェース
	IPMP	高可用性	`ipadm`
	IP トンネル	IP 接続	`ipadm show-iptun`
	ルーティング	IP 接続	`route -p display`、`netstat`、`routeadm`
	VNI	IP 接続	`ipadm`
	VNIC	ネットワーク仮想化	`dladm show-vnic` および `dlstat`
	VRRP	高可用性	`dladm`、`vrrpadm`
	VXLAN	ネットワーク仮想化	`dladm show-vxlan` および `dlstat`
トランスポートレイヤー (L4)			
	ファイアウォール	セキュリティー	`ipf` および `ipnat` によるパケットフィルタリング
	フロー	可観測性、リソース管理、セキュリティー	`flowadm` および `flowstat`
	プラガブル輻輳制御	パフォーマンス	`ipadm`
	ソケットフィルタリング	セキュリティー	`soconfig (-F)`

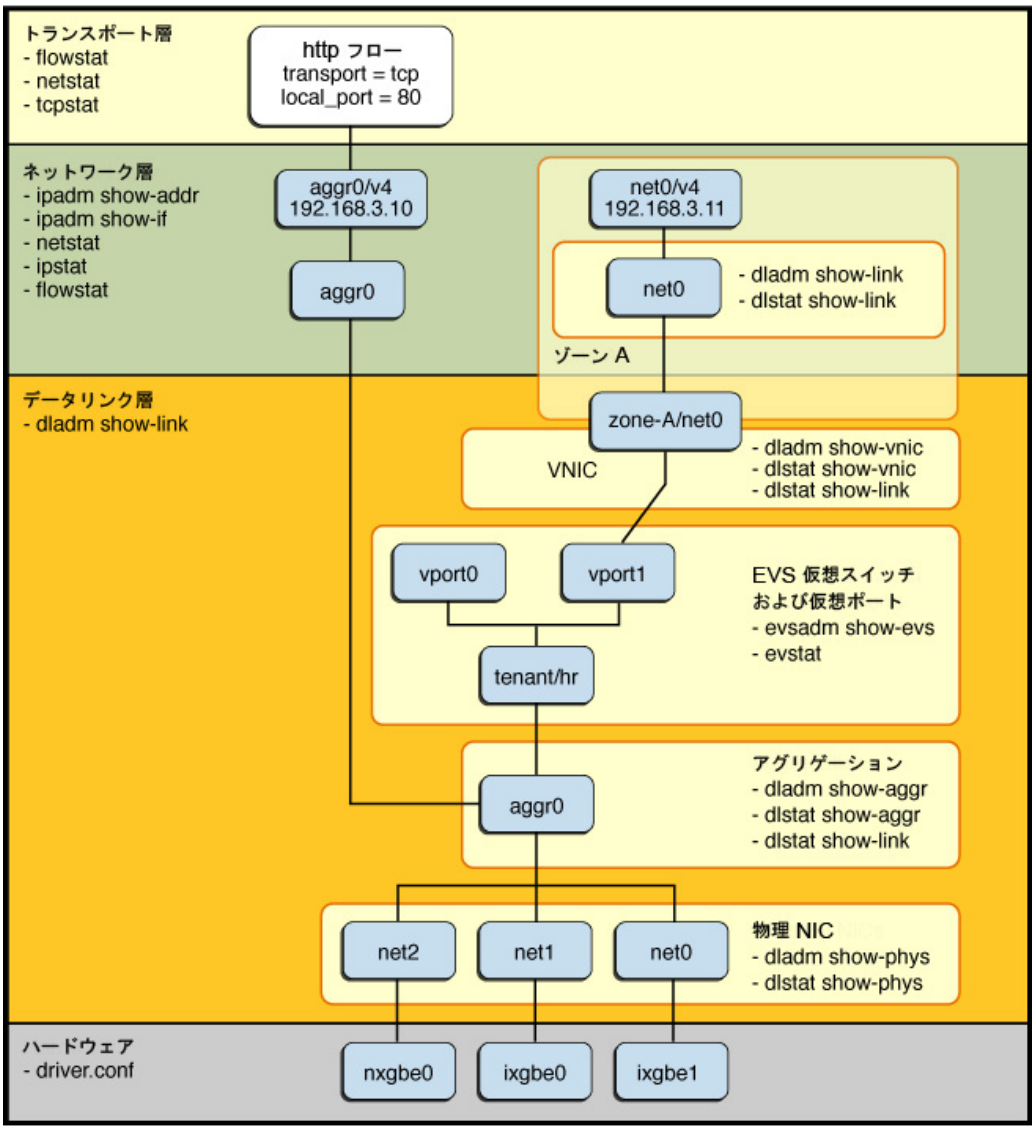
ネットワーク構成およびトラフィック使用状況の監視

次の情報は、表2で説明されている可観測性ツールを使用する方法を示しています。

次の図は、Oracle Solaris ネットワークプロトコルスタックのさまざまなレイヤーで構成されているネットワーク機能のうちのいくつかから成る一般的な仮定のネットワーク構成を示しています。例としてのみ提供されているこの図のあとには、実際に Oracle Solaris ツールを使用して、関連するさまざまなコンポーネントに関する統計を監視および収集する方法を示す一連のコマンド例が示されています。

注記 - この図に、構成可能なすべてのタイプのデータリンクが含まれているわけではありません。ネットワークプロトコルスタックの各レイヤーで構成可能なすべての機能の詳細は、『Oracle Solaris 11.3 でのネットワーク管理の計画』 の 第 1 章, 「Oracle Solaris ネットワーク管理のサマリー」を参照してください。

図 1 Oracle Solaris ネットワークプロトコルスタック内のネットワーク構成



この図は、ネットワークプロトコルスタックのさまざまなレイヤーでいくつかの Oracle Solaris 機能を組み合わせる方法を示す次の構成を表しています。

- ネットワークスタックの物理レイヤーには、3 つの物理 NIC `nxgbe0`、`ixgbe0`、および `ixgbe1` がシステム内に存在し、それぞれ物理データリンクインスタンス `net2`、`net1`、および `net0` として表示されます。
- 次に、これらの物理 NIC が `aggr0` と呼ばれるリンクアグリゲーションにグループ化されます。
- このリンクアグリゲーションデータリンクが次に、IP アドレス (`aggr0/v4`) で直接構成されると同時に、エラスティック仮想スイッチとして構成されている、`tenant/hr` と呼ばれる仮想スイッチのアップリンクとしても使用されます。この仮想スイッチには、`vport0` と `vport1` の 2 つの仮想ポートがあります。
- Oracle Solaris ゾーン (`zone-A`) には、これらの仮想ポートの 1 つに接続されている、`zone-A/net0` と呼ばれる VNIC が存在します。そのゾーン自体の中では、この VNIC は、IP アドレス (`net0/v4`) で構成されているデータリンク (`net0`) として表示されます。
- HTTP トラフィックのフローもアグリゲーション (`aggr0`) 上に作成されます。

次の例では、Oracle Solaris で提供されているツールを使用して、これらのコンポーネントに関する構成情報を取得したり、さまざまなネットワーク機能のネットワークトラフィック使用状況を監視したりする方法についてさらに詳細に説明しています。

ネットワーク構成およびトラフィック使用状況を監視するためのツール

データリンクは、`dladm` コマンドを使用して構成および管理します。データリンクのネットワークトラフィック使用状況に関する統計を取得するには、`dlstat` コマンドを使用します。たとえば、リンクごとのインバウンドおよびアウトバウンドトラフィック統計は、次のコマンドのいずれかを使用して表示します。

```
# dlstat link
```

```
# dlstat show-link link
```

物理ネットワークデバイスごとのインバウンドおよびアウトバウンドトラフィックの統計情報は次のように表示します。

```
# dlstat show-phys link
```

ポートごと、およびリンクアグリゲーションごとのインバウンドおよびアウトバウンドトラフィック統計は次のように表示します。

```
# dlstat show-aggr link
```

詳細は、dlstat(1M) のマニュアルページを参照してください。

フローは、`flowadm` コマンドを使用して構成および管理します。フローのネットワークトラフィック使用状況に関する統計を取得するには、`flowstat` コマンドを使用し

ます。図1に示すように、指定した属性に応じて、フローを使用して、ネットワークスタックのさまざまなレイヤーでのネットワークトラフィックの使用状況を監視できます。

```
# flowstat
```

詳細は、flowstat(1M) のマニュアルページを参照してください。

次の例は、ネットワーク構成情報を表示したり、機能ごと、および Oracle Solaris ネットワークプロトコルスタックのレイヤーごとのネットワークトラフィック統計を監視したりする方法を示しています。ネットワークトラフィック使用状況のモニタリングの詳細は、『Oracle Solaris 11.3 での仮想ネットワークとネットワークリソースの管理』 の 第 8 章,「ネットワークトラフィックとリソース使用状況のモニタリング」を参照してください。

ハードウェアレイヤーでのネットワーク構成およびトラフィック使用状況の監視

ネットワークプロトコルスタックのハードウェアレイヤーでのネットワーク構成やパフォーマンスの問題のトラブルシューティングには、次の監視が必要になることがあります。

- 物理 NIC ごとに存在するリングの数と、それらのリングを通して転送されているパケットの数。
- 発生しているパケット破棄の数。
  - 物理 NIC ごと
  - 物理リングごと
- 役立つ可能性のある NIC 固有のカウンタ。
- 物理 NIC ごとに構成されているリングの数と記述子の数。

物理デバイスの場合は、`dladm show-phys` および `dlstat show-phys` コマンドを使用するとネットワークトラフィック使用状況を監視できます。これらの 2 つのコマンドは、取得する情報のタイプによって異なる出力を表示します。

たとえば、システム上のすべての物理リンクの物理デバイスと属性を表示するには、`dladm show-phys` コマンドをオプションなしで使用します。

```
# dladm show-phys
LINK MEDIA    STATE   SPEED DUPLEX   DEVICE
net1 Ethernet unknown 0     unknown  bge0
net0 Ethernet up      1000  full     nge0
```

詳細および例については、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 第 2 章,「Oracle Solaris でのデータリンク構成の管理」および dladm(1M) のマニュアルページを参照してください。

dlstat show-phys コマンドは、物理デバイスごとの送受信されたパケット数とバイト数に関する統計を表示します。このサブコマンドは、ネットワークスタックのデバイスレイヤーにあるハードウェアリングに対して動作します。

次の例では、システム上のすべての物理リンクに関する統計を表示します。この出力は、システム上の各リンクに関する受信トラフィックと送信トラフィックの両方の統計を表示します。また、パケットの数とパケットごとのバイトサイズも表示されます。

```
# dlstat show-phys
LINK    IPKTS   RBYTES    OPKTS   OBYTES
net1        0        0        0        0
net0    1.95M  137.83M   37.95K    3.39M
```

-r オプションを使用すると、データリンクデバイスの各ハードウェアリングに関する受信側の統計を表示できます。このコマンドの出力には、そのデータリンクデバイスで受信されたバイト数とパケット数や、ハードウェアとソフトウェアでの破棄数などが含まれます。この例は、net4 に、次の出力の INDEX フィールドで識別される 8 つのリングが存在することを示しています。

```
# dlstat show-phys -r net4
LINK TYPE INDEX IPKTS RBYTES
net4 rx   0     701   42.06K
net4 rx   1     0     0
net4 rx   2     0  0
net4 rx   3     0  0
net4 rx   4     0  0
net4 rx   5     0  0
net4 rx   6     0  0
net4 rx   7     0  0
```

転送されたトラフィックに関する同様の情報を取得するには、-t オプションを使用します。

次の例では、物理リンクごとの破棄されたインバウンドパケットの数を表示します。

```
dlstat show-phys -o idrops
IDROPS
0
871.14K
```

-o *field*[,...] オプションは、表示する出力フィールドの大文字と小文字が区別されないコンマ区切りリストを指定するために使用されます。

次の例では、物理リンクごとの破棄されたインバウンドおよびアウトバウンドパケット数とバイト数が表示されます。

```
# dlstat show-phys -o idrops,idropbytes,odrops,odropbytes
IDROPS    IDROPBYTES ODROPS ODROPBYTES
0         0          0      0
871.14K   0          0      0
```

dlstat show-phys -o コマンドでは idrops と idropbytes の両方のオプションを指定することをお勧めします。IDROPS フィールドが 0 以外であるのに対して、IDROBYTES フィールドは 0 である前の出力に示すように、システムのハードウェ

ア機能によっては、これらの値のどちらかが 0 になる場合があることに注意してください。

ドライバ構成の場合は、`driver.conf` ファイルだけでなく、`dladm` プロパティーでも特定のドライバのプロパティー値を管理できます。ドライバ構成ファイルを使用すると、そのデバイス自体によって提供されるデフォルト値をオーバーライドするデバイスのプロパティー値を指定できます。`driver.conf` ファイルを使用して情報を管理する方法の詳細は、`driver.conf(4)` のマニュアルページを参照してください。

データリンクレイヤーでのネットワーク構成およびトラフィック使用状況の監視

ネットワークプロトコルスタックのデータリンクレイヤー (L2) では、いくつかのネットワーク機能が構成されます。これらの機能には、物理データリンクと仮想データリンクの両方が含まれます。スタックのこのレイヤーでのネットワークトラフィック使用状況を監視するために使用する特定のコマンドは汎用であるため、構成されているすべてのタイプのデータリンクに使用できます。その他のサブコマンドはその機能自体に固有であるため、その機能の構成に関する追加情報を表示するために使用できます。

スタックのこのレイヤーで使用するコマンドはまた、監視する情報のタイプによっても異なります。たとえば、スタックのデータリンクレイヤーでは、ファンアウトの統計またはリンクごとの統計を表示することがあります。各タイプの情報を取得するには、異なるコマンドを使用します。

データリンクに関する基本情報を取得するには、`dladm show-link` を使用します。このコマンドは、次の出力に示すように、システム上のすべてのデータリンクまたは指定されたデータリンクのリンク構成情報を表示します。

```
# dladm show-link
LINK CLASS MTU STATE   OVER
net1 phys 1500 unknown --
net0 phys 1500 up      --
```

前の出力は、このシステムに、それぞれ対応する物理 NIC に直接関連付けられた 2 つのデータリンクが存在することを示しています。システム上に特殊なデータリンク (アグリゲーションや VNIC など) は存在しません。これらのタイプの L2 エンティティーは、`phys` クラスの下の物理データリンク上に構成されます。

データリンクレイヤーでのネットワークトラフィック使用状況を監視するには、`dlstat show-link` コマンドを使用します。`show-link` サブコマンドは、ネットワークプロトコルスタックのデータリンクレイヤーで動作し、物理リンク上に構成されているレーンに関する統計を提供します。

次の出力は、リンクごとのインバウンドおよびアウトバウンドトラフィック統計を示しています。

```
# dlstat show-link
LINK   IPKTS  RBYTES  OPKTS  OBYTES
net1   0      0         0         0
net0   1.96M  137.97M   38.40K    3.29M
```

次の例では、net4 デバイスの受信側のトラフィック統計が報告されます。また、INTRS および POLLS カウンタの統計も表示されます。これらの統計は、割り込みコンテキストとポーリングモードのそれぞれで受信されたパケットの数を報告します。IDROPS カウンタは、ネットワークスタックのデータリンクレイヤーで破棄されたパケットの数を示しています。

```
# dlstat show-link -r net4
LINK TYPE   ID    INDEX    IPKTS  RBYTES    INTRS    POLLS   IDROPS
net4 rx    local  --        0      0        0        0       0
net4 rx    other  --        0      0        0        0       0
net4 rx    hw     0     7.46M  1.06G    5.62M    1.84M       0
net4 rx    hw     1        0      0        0        0       0
net4 rx    hw     2        0      0        0        0       0
net4 rx    hw     3        0      0        0        0       0
net4 rx    hw     4        2    196        2        0       0
net4 rx    hw     5        0      0        0        0       0
net4 rx    hw     6        0      0        0        0       0
net4 rx    hw     7        0      0        0        0       0
```

前の出力では、指定されたリンク、物理デバイス (show-phys サブコマンドの場合)、またはアグリゲーション (show-aggr サブコマンドの場合) の統計のみが表示されます。このコマンドで *link* が指定されていない場合は、すべてのリンク、デバイス、およびアグリゲーションの統計が出力に表示されます。

この例では、ID フィールドに表示される情報は次のように解釈されます。

- local – ネットワークスタックのレイヤー 2 (L2) 上の対応するループバックトラフィックを示します。
- other – ブロードキャストおよびマルチキャストトラフィックが含まれます。

  データリンクの有効期間を通して、そのデータリンクに関連付けられたハードウェアリソースは、リソース使用率、リンク構成、または物理 NIC のリンクアグリゲーションへの割り当てによって異なる可能性があります。show-link -r コマンドの出力に示されている rx エントリは、現在そのリンクに割り当てられているハードウェアリソースに対応します。other 行の出力には、そのデータリンクにはすでに割り当てられていないハードウェアリソースのトラフィックが含まれています。
- hw – ハードウェアレーンを示します。
- sw – ソフトウェアレーンを示します (次の例を参照してください)。

ハードウェアレーンとソフトウェアレーンの区別は、リング割り当てをサポートする NIC の能力に基づいています。ハードウェアレーン上では、リングは、それらのレーンを使用するパケット専用になります。これに対して、ソフトウェアレーン上のリングはデータリンクの間で共有されます。

次の出力は、net1 によって使用されているリング上のアウトバウンドパケットに関する統計を報告します。

```
# dlstat show-link -t net1
LINK  TYPE       ID  INDEX    OPKTS   OBYTES   ODROPS
net4    tx    local     --        0        0        0
net4    tx    other     --        0        0        0
net4    tx       hw      0      372   15.67K        0
net4    tx       hw      1        1       98        0
net4    tx       hw      2        0        0        0
net4    tx       hw      3        0        0        0
net4    tx       hw      4        0        0        0
net4    tx       hw      5        0        0        0
net4    tx       hw      6        1       98        0
net4    tx       hw      7        0        0        0
```

アグリゲーションのネットワーク構成およびトラフィック使用状況の監視

アグリゲーションもまた、ネットワークプロトコルスタックのデータリンクレイヤー (L2) で構成されます。取得する情報のタイプ (物理 NIC 間のトラフィックの全体的な分布やアグリゲーションの統計など) に応じて、次のコマンドを使用します。

`dladm show-aggr`	すべてのアグリゲーションまたは指定されたアグリゲーションのアグリゲーション構成 (デフォルト)、LACP 情報、または DLMP プローブベースの障害および回復検出ステータスを表示します。 アグリゲーションの詳細なアグリゲーションごとの情報を表示するには、-x オプションを指定します。
`dlstat show-aggr`	アグリゲーションで送受信されたパケット数とバイト数に関するポートごとの統計を表示します。
`dlstat show-link`	アグリゲーション (データリンクであるアグリゲーション) で送受信されたパケット数とバイト数に関する統計を表示します。

`dlstat show-aggr` コマンドと `dlstat show-link` コマンドの 1 つの違いは、`dlstat show-aggr` コマンドがポートごとの統計を表示するのに対して、`dlstat show-link` コマンドはリンクごとの統計を提供することです。これらの 2 つのコマンドのもう 1 つの重要な違いとして、`dlstat show-aggr` コマンドは、アグリゲーション全体に関する全体的な統計を表示します。これに対して、`dlstat show-link` コマンドは、アグリゲーションのプライマリクライアント (IP など) に関する統計のみを表示します。

そのため、アグリゲーション上に VNIC を作成した場合、`dlstat show-aggr` コマンドはすべての VNIC にわたるパケットの総数に加え、プライマリクライアント (IP) に関する統計を報告します。この出力は、`show-link` サブコマンドと比較した場合の `show-phys` サブコマンドに似ています。この場合、`show-phys` が全体的なトラフィック使用状況を表示するのに対して、`show-link` はプライマリデータリンクのトラフィック使用状況のみを表示します。

次の例は、アグリゲーションのネットワークトラフィック使用状況を監視する方法を示しています。アグリゲーションの管理の詳細は、『Oracle Solaris 11.3 でのネット

ワークコンポーネントの構成と管理』 の 第 2 章, 「Oracle Solaris でのデータリンク構成の管理」を参照してください。

例 1 アグリゲーション構成情報の表示

次の出力例では、システム上に構成されている既存のアグリゲーションのステータスを報告します。

```
# dladm show-aggr -x
LINK  PORT SPEED    DUPLEX  STATE  ADDRESS          PORTSTATE
aggr1 --   1000Mb   full    up     0:14:4f:29:d1:9d --
net1       1000Mb   full    up     0:14:4f:29:d1:9d attached
net3       0Mb      unknown down   0:14:4f:29:d1:9f standby
```

例 2 アグリゲーションのポートごとの統計の表示

`dlstat show-aggr` コマンドの次の出力例では、アグリゲーションのポートごとの統計を報告します。アグリゲーションで送受信されたパケット数とバイト数の両方が表示されます。

```
# dlstat show-aggr
LINK            PORT    IPKTS      RBYTES    OPKTS   OBYTES
aggr1             --      99 1      2.18K     23       966
aggr1            net4     25        1.50K      8       336
aggr1            net5     74        10.68K    15       630
```

例 3 アグリゲーションのリンクごとの統計の表示

`dlstat show-link` コマンドの次の出力例では、アグリゲーションのリンクごとの統計を報告します。アグリゲーションで送受信されたパケット数とバイト数の両方が表示されます。この例と前の例の違いは、`show-aggr` サブコマンドがポートごとの統計を報告するのに対して、`show-link` サブコマンドはリンクごとの統計を報告することです。

```
# dlstat show-link
LINK    IPKTS     RBYTES    OPKTS   OBYTES
net5        0          0        0        0
net2        0          0    5.60K    1.49M
net4        0          0        0        0
net6    4.43K      1.32M    6.39K    1.56M
net1    4.43K      1.32M    6.39K    1.56M
net0  387.10K     99.42M   59.43K    7.67M
net3        0          0    5.61K    1.50M
aggr1     150     18.65K        30   1.26K
```

例 4 アグリゲーションのハードウェアリングに関する受信側のトラフィック統計の表示

次の例では、アグリゲーション (`aggr1`) のハードウェアリングに関する受信側の統計を報告します。

```
# dlstat show-phys -r aggr1
```

```
LINK TYPE INDEX   IPKTS  RBYTES
aggr1   rx     0     723  43.38K
aggr1   rx     1       0       0
aggr1   rx     2       0       0
aggr1   rx     3       0       0
aggr1   rx     4       0       0
aggr1   rx     5       0       0
aggr1   rx     6       0       0
aggr1   rx     7       0       0
aggr1   rx     8  22.20K   1.33M
aggr1   rx     9     692  63.66K
aggr1   rx    10       0       0
aggr1   rx    11       0       0
aggr1   rx    12       0       0
aggr1   rx    13  12.99K   4.44M
aggr1   rx    14       0       0
aggr1   rx    15  10.39K 623.34K
```

例 5 アグリゲーションのハードウェアレーンに関する受信側のトラフィック統計の表示

次の例では、アグリゲーション (aggr1) の各ハードウェアレーンに関する受信側のトラフィック統計を報告します。報告される統計が、アグリゲーションのプライマリクライアントのトラフィック (そのアグリゲーション上の IP トラフィックなど) にのみ関連していることに注意してください。この出力には、そのアグリゲーション上に構成されているほかのクライアント (VNIC など) に関するトラフィック統計は含まれていません。アグリゲーションのすべてのクライアントのトラフィック使用状況を表示するには、例1「アグリゲーション構成情報の表示」および 例4「アグリゲーションのハードウェアリングに関する受信側のトラフィック統計の表示」に示すように、`dlstat show-aggr` および `dlstat show-phys` を使用します。

```
# dlstat show-link -r aggr1
LINK   TYPE    ID    INDEX    IPKTS   RBYTES    INTRS   POLLS  IDROPS
aggr1   rx   local     --       0       0        0       0      0
aggr1   rx   other     --       0       0        0       0      0
aggr1   rx      hw      0     721   43.26K     721       0      0
aggr1   rx      hw      1       0       0        0       0      0
aggr1   rx      hw      2       0       0        0       0      0
aggr1   rx      hw      3       0       0        0       0      0
aggr1   rx      hw      4       0       0        0       0      0
aggr1   rx      hw      5       0       0        0       0      0
aggr1   rx      hw      6       0       0        0       0      0
aggr1   rx      hw      7       0       0        0       0      0
aggr1   rx      hw      8  22.23K   1.33M   22.23K       0      1
aggr1   rx      hw      9     693  63.76K      693       0      0
aggr1   rx      hw     10       0       0        0       0      0
aggr1   rx      hw     11       0       0        0       0      0
aggr1   rx      hw     12       0       0        0       0      0
aggr1   rx      hw     13  13.00K   4.45M    13.00K      0      2
aggr1   rx      hw     14       0       0        0       0      0
aggr1   rx      hw     15  10.40K 624.06K   10.40K       0      0
```

EVS スイッチのネットワーク構成およびトラフィック使用状況の監視

Oracle Solaris のエラスティック仮想スイッチ (EVS) 機能は、ネットワークプロトコルスタックのデータリンクレイヤーで構成および管理します。表示する情報のタイプに応じて、次のコマンドを使用します。

`evsadm`	EVS スイッチとそのリソースである IP ネットワーク (*IPnet*) および仮想ポート (*VPort*) を作成および管理します。 EVS コントローラによって管理されているすべての EVS スイッチまたは指定された EVS スイッチの情報を表示するには、`show-evs` サブコマンドを使用します。
`evsstat`	大規模な配置のすべての VPort または指定されたエラスティック仮想スイッチのすべての VPort のネットワークトラフィック統計を表示します。このコマンドはまた、その VPort に関連付けられたすべての VNIC の統計も報告します。
`dladm show-vnic -c`	EVS スイッチに接続されている VNIC に関する情報を表示します。その VNIC が接続されている VPort と EVS スイッチは、EVS スイッチによって決定されます。

次の例は、エラスティック仮想スイッチの構成情報を表示したり、EVS 構成のネットワークトラフィック使用状況やその他の統計を監視したりする方法を示しています。EVS 機能の管理の詳細は、『Oracle Solaris 11.3 での仮想ネットワークとネットワークリソースの管理』 の 第 6 章,「エラスティック仮想スイッチの管理」を参照してください。

例 6 EVS 構成に関する情報の表示

次の例では、`evsadm` コマンドを使用して EVS 構成に関する基本情報を表示します。

```
# evsadm
NAME          TENANT        STATUS  VNIC    IP          HOST
evs0          sys-global    busy    --      ipnet0      sysabc-02
sys-vport0    --            used    vnic0   10.0.0.2/24 sysabc-02
```

例 7 EVS スイッチに接続されている VPort のインバウンドおよびアウトバウンドトラフィック使用状況の表示

次の例では、`evsstat` コマンドを使用して、EVS スイッチに接続されている VPort のみの受信および送信ネットワークトラフィック統計を表示します。

```
# evsstat
VPORT       EVS   TENANT      IPKTS    RBYTES   OPKTS  OBYTES
sys-vport0  evs0  sys-tenant  101.88K  32.86M  40.16K  4.37M
sys-vport1  evs0  sys-tenant    4.50M   6.78G   1.38M  90.90M
```

例 8 EVS スイッチに接続されている VNIC に関する情報の表示

VNIC には、ベースとなるリンク上に作成するものと、EVS スイッチに接続されているものの 2 つのタイプがあります。EVS スイッチに接続されている VNIC に関する情報を取得するには、次の例に示すように、`dladm show-vnic` コマンドを `-c` オプションとともに使用します。

```
# dladm show-vnic -c
LINK        TENANT        EVS     VPORT       OVER   MACADDRESS        IDS
vnic0       sys-global    evs0    sys-vport0  net    12:8:20:f2:46:22  VID:200
```

VNIC のネットワーク構成およびトラフィック使用状況の監視

VNIC は、ネットワークプロトコルスタックのデータリンクレイヤー (L2) で構成されます。これらの L2 エンティティーに関する構成情報を表示したり、ネットワークトラフィック使用状況を監視したりするには、次のコマンドを使用します。

`dladm show-vnic`	システム上のすべての VNIC、リンク上のすべての VNIC、または指定された `vnic-link` の VNIC 構成情報を表示します。
`dlstat`	VNIC ごとの送受信されたパケット数とバイト数に関する統計を表示します。

次の例は、VNIC のネットワークトラフィック使用状況を監視する方法を示しています。VNIC の管理の詳細は、『Oracle Solaris 11.3 での仮想ネットワークとネットワークリソースの管理』 の 「VNIC の管理」を参照してください。

例 9 VNIC 構成情報の表示

次の例では、システム上の 1 つの既存の VNIC (`vnic0`) の VNIC 構成情報を表示します。

```
# dladm show-vnic
LINK        OVER        SPEED  MACADDRESS       MACADDRTYPE IDS
vnic0       net1        1000   2:8:20:f2:46:22  fixed       VID:200
```

例 10 VNIC のネットワークトラフィック統計の表示

次の例では、`dlstat` コマンドを使用して、特定の VNIC (`vnic0`) によって送受信されたパケット数とバイト数に関する統計を表示します。

```
# dlstat vnic0
LINK    IPKTS   RBYTES    OPKTS    OBYTES
vnic0   1.53M   158.18M   154.22K  32.84M
```

IP レイヤーでのネットワーク構成およびトラフィック使用状況の監視

ネットワークプロトコルスタックの IP レイヤー (L3) でのネットワークトラフィック使用状況は、いくつかの異なるコマンドを使用して監視します。表示する情報のタイプに応じて、次のコマンドを使用します。

`flowstat`	ネットワークプロトコルスタックの IP レイヤーで構成されているさまざまな IP アドレスまたはサブネットに対して作成するフローに関する統計を表示します。
`ipadm`	IP インタフェースおよびアドレスに関する一般的な構成情報を表示します。
`ipadm show-addr`	指定されたアドレスオブジェクト (`addrobj`)、または指定されたインタフェース上に構成されているすべてのアドレスオブジェクト (永続的な構成だけに存在するものも含む) の IP アドレス情報を表示します。
`ipadm show-if`	システム上に構成されているすべてのネットワークインタフェース (永続的な構成だけに存在するものも含む)、または指定されたインタフェースのネットワークインタフェース構成情報を表示します。
`ipstat`	選択された出力モードとソート順序に基づいて、IP トラフィックに関する統計を表示します。
`netstat`	ネットワークに関連した特定のデータ構造の内容をさまざまな形式で表示します。

次の例は、ネットワークプロトコルスタックの IP レイヤーで構成されているネットワーク機能に関するネットワークトラフィック使用状況を監視したり、統計を収集したりする方法を示しています。IP 構成の管理の詳細は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「IP インタフェースとアドレスのモニタリング」を参照してください。`ipstat(1M)` および `netstat(1M)` のマニュアルページも参照してください。

例 11 IP 構成に関する一般的な情報の表示

IP 構成に関する一般的な情報を表示するには、`ipadm` コマンドを使用します。次の例は、システム上に構成されているすべての IP インタフェースおよびアドレスに関する情報を表示する方法を示しています。

```
# ipadm
NAME              CLASS/TYPE STATE        UNDER      ADDR
lo0               loopback   ok           --         --
```

```
   lo0/v4        static     ok           --         127.0.0.1/8
   lo0/v6        static     ok           --         ::1/128
net0             ip         ok           --         --
   net0/v4       static     ok           --         10.134.67.140/24
```

例 12 構成されている IP インタフェースに関する情報の表示

システム上に構成されている IP インタフェースに関する情報を表示するには、次の例に示すように、`ipadm` コマンドを `show-if` サブコマンドとともに使用します。

```
# ipadm show-if
IFNAME   CLASS      STATE   ACTIVE   OVER
lo0      loopback   ok       yes     ---
net0     ip         ok       yes     ---
```

例 13 構成されている IP アドレスオブジェクトに関する情報の表示

次の例は、`ipadm` コマンドを `show-addr` サブコマンドとともに使用して、システム上に構成されている IP アドレスオブジェクトに関する情報を表示する方法を示しています。

```
# ipadm show-addr
ADDROBJ       TYPE       STATE   ADDR
lo0/v4        static     ok      127.0.0.1/8
```

例 14 `ipstat` コマンドを使用した IP トラフィックに関する統計の表示

次の例は、`ipstat` コマンドを使用して IP トラフィックに関する統計を表示する方法を示しています。このコマンドには、指定された発信元または宛先アドレス、インタフェース、および上位レイヤープロトコルに一致する IP トラフィックに関する統計を報告するためのオプションが用意されています。

```
# ipstat
SOURCE               DEST                 PROTO   INT   RATE
abc11example-02      dhcp-sys.example     TCP     net0  145.6
dns1.example.com     abc11example-02      UDP     net0  66.0
abc11example-02      dns1.example.com     UDP     net0  10.4
dhcp-sys.example     abc11example-02      TCP     net0  4.0
foo1.example.com     all-sys.mcast.net    ICMP    net0  3.2
```

詳細は、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「ipstat および tcpstat コマンドを使用したネットワークトラフィックの監視」を参照してください。

例 15 `netstat` コマンドを使用した接続されたソケットの表示

`netstat` コマンドは、ネットワークステータスやプロトコル統計を表示します。TCP、SCTP、および UDP の各エンドポイントのステータスは表形式で表示できます。また、このコマンドを使用して、ルーティングテーブルやインタフェース情報を表示することもできます。報告されるさまざまなタイプのネットワークデータは、指定するコマンド行オプションによって異なります。

次の例では、netstat コマンドをオプションなしで使用して、プロトコルごとのアクティブなソケットのリストを表示します。

```
# netstat
 TCP: IPv4
   Local Address        Remote Address          Swind  Send-Q  Rwind   Recv-Q  State
  ------------------     -----------------    -------  ------  -------- ------  --------
   localsys.local.port1  remotesys1            65535   0      128592   0      ESTABLISHED
   localsys.local.port2  localsys.local.port5   130880  0      139264   0      ESTABLISHED
   localsys.local.port3  localsys.local.port6   139060  0      130880   0      ESTABLISHED
   localsys.local.port4  remotesys2.remote.port2 65572  63     128480   0      ESTABLISHED
```

次の例に示すように、適用可能なソケットのみの統計または状態の表示を特定のプロトコルに制限するには、netstat -P *protocol* コマンドを次のように使用します。

```
# netstat -P tcp
TCP: IPv4
Local Address Remote Address               Swind  Send-Q  Rwind  Recv-Q    State
------------ --------------------          ------ ------ ------- ------  --------
sys3.48962   foo.com.ldaps                 49232   0   128872    0    ESTABLISHED
sys3.ssh     dhcp1-10-132-146-210.foo.com  64292  63   128480    0    ESTABLISHED
```

protocol は、ip、ipv6、icmp、icmpv6、igmp、udp、tcp、rawip のいずれかとして指定できます。

次の簡略化された例は、netstat -s コマンドを使用してプロトコルごとの統計を表示する方法を示しています。

```
# netstat -s
RAWIP   rawipInDatagrams    =     2    rawipInErrors   =  0
        rawipInCksumErrs    =     0
        rawipOutDatagrams   =     2
        rawipOutErrors      =     0

UDP     udpInDatagrams      =   1023   udpInErrors    =   0
        udpOutDatagrams     =   1023
        udpOutErrors        =      0

TCP     tcpRtoAlgorithm     =      4    tcpRtoMin     =   200
        tcpRtoMax           =  60000
        tcpMaxConn          =     -1
        tcpActiveOpens      =    382
        tcpPassiveOpens     =     83
        tcpAttemptFails     =     81
        tcpEstabResets      =      1
        tcpCurrEstab        =      2
        tcpOutSegs          =   6598
        tcpOutDataSegs      =   5653
        tcpOutDataBytes     = 836393
        tcpRetransSegs      =     16
. . .
```

例 16 ネットワークスタックの IP レイヤーで構成されているフローに関する統計の表示

次の例に示すように、ネットワークプロトコルスタックの IP レイヤーで構成されている目的とするさまざまな IP アドレスまたはサブネットのフローを作成できます。

次に、flowstat コマンドを使用すると、これらのフローに関する統計を表示できます。

```
# flowadm add-flow -l net0 -a transport=tcp tcpflow1
# flowadm add-flow -l net4 -a transport=tcp tcpflow2

# flowstat
FLOW      IPKTS   RBYTES   IDROPS    OPKTS   OBYTES   ODROPS
tcpflow2      0       0        0        0        0        0
tcpflow1     53   5.62K        0       45    5.52K        0
```

特定のデータリンクデバイスのフロー情報を表示するには、-l オプションを指定します。

```
# flowstat -l net0
FLOW      IPKTS   RBYTES  IDROPS   OPKTS  OBYTES ODROPS
tcpflow1    108   11.19K       0     86   10.45K      0
```

例 17 特定の IP アドレスのフローの作成および監視

flowadm add-flow コマンドで local_ip および remote_ip 属性を使用しすると、特定の IP アドレスのフローを作成できます。次の例に示すように、次に flowstat コマンドを使用すると、これらのフローに関する統計を表示できます。

```
# flowadm add-flow -l net0 -a local_ip=10.10.12.45 flow1
# flowadm add-flow -l net4 -a remote_ip=10.134.64.0/24 flow2
# flowstat
FLOW      IPKTS     RBYTES   IDROPS    OPKTS  OBYTES   ODROPS
flow2   528.54K    787.39M        0  179.39K  11.85M        0
flow1   742.81K      1.10G        0        0       0        0
```

トランスポートレイヤーでのネットワーク構成およびトラフィック使用状況の監視

ネットワークプロトコルスタックのトランスポートレイヤー (L4) で構成および管理されている機能のネットワークトラフィックは、次のコマンドを使用して監視します。

flowstat	ユーザー定義のフローに関する実行時統計を報告します。flowstat コマンドで指定するフロー名を確認するには、flowadm show-flow コマンドを使用します。 フローは、帯域幅制御のためだけではなく、(たとえば、特定のサービスが消費するトラフィックの量を測定するための) 可観測性ツールとしても使用できます。
netstat	ネットワークに関連した特定のデータ構造の内容をさまざまな形式で表示します。引数なしの netstat コマンドは、-f オプションを使用して変更されないかぎり、PF_INET、PF_INET6、および PF_UNIX の接続されたソケットを表示します。

`tcpstat` コマンド構文で指定されている選択された出力モードとソート順序に基づいて、サーバー上の TCP および UDP トラフィックに関する統計を報告します。

次の例は、ネットワークプロトコルスタックのトランスポートレイヤーで構成されている機能に関するネットワークトラフィック使用状況を監視したり、統計を収集したりする方法を示しています。

`netstat` および `tcpstat` コマンドを使用した TCP/IP ネットワークの管理の詳細は、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 第 1 章, 「TCP/IP ネットワークの管理」を参照してください。

`flowstat` コマンドの詳細は、『Oracle Solaris 11.3 での仮想ネットワークとネットワークリソースの管理』 の 「フロー上のネットワークトラフィックの統計情報の表示」および `flowstat(1M)` のマニュアルページを参照してください。

例 18 `flowstat` コマンドを使用したフローに関する実行時統計の表示

次の出力例は、システム上の構成されているすべてのフローに関するトラフィック情報の静的な表示を示しています。`flowadm` コマンドは、フローの名前を確認するために使用されます。

```
# flowadm
FLOW         LINK     PROTO LADDR   LPORT RADDR  RPORT DIR
tcpflow1     net1     tcp   --      --    --     --    bi
tcpflow0     net0     tcp   --      --    --     --    bi
udpflow0     net0     udp   --      --    --     --    bi

# flowstat
FLOW       IPKTS   RBYTES  IDROPS    OPKTS   OBYTES   ODROPS
tcpflow1       0        0       0        0        0        0
tcpflow0   1.39K  117.86K       0     2.16K  260.77K        0
udpflow0       5    1.43K       0        0        0        0
```

次の 2 つの例の出力に示すように、`flowstat` コマンドを `-l` オプションとともに使用して、指定されたリンクのすべてのフローに関する統計または指定されたフローに関する統計を表示することもできます。

```
# flowstat -l net0
FLOW       IPKTS   RBYTES   IDROPS    OPKTS    OBYTES   ODROPS
tcpflow0   1.51K  126.85K        0    2.43K   292.85K        0
udpflow0       9    2.80K        0        0         0        0

# flowstat -l net0 tcpflow0
FLOW       IPKTS    RBYTES   IDROPS     OPKTS   OBYTES  ODROPS
tcpflow0   1.66K   137.11K        0     2.69K  324.42K       0
```

例 19 `netstat` コマンドを使用したトランスポートレイヤーのデータ構造に関する情報の表示

`netstat` コマンドを使用すると、ネットワークプロトコルスタックのトランスポートレイヤー (L4) のデータ構造 (TCP や UDP など) に関する情報を表示できます。次の例

では、netstat -P *transport-protocol* コマンドを使用して TCP に関する情報を表示します。

```
# netstat -p tcp
TCP: IPv4
  Local Address      Remote Address   Swind   Send-Q  Rwind  Recv-Q  State
  ----------------  ---------------  ------- ------ ------- ------ -----------
  localsys.ssh     remotesys1.port4   65380     63     128480   0    ESTABLISHED
  localsys.port1   remotesys2.ldaps   65535      0     128592   0    ESTABLISHED
  localsys.port2   localsys.port5    130880     0      139264   0    ESTABLISHED
  localsys.port3   localsys.port6    139060     0      130880   0    ESTABLISHED
```

例 20 tcpstat コマンドを使用した TCP および UDP トラフィックに関する統計の表示

ネットワークプロトコルスタックのトランスポートレイヤーのネットワークトラフィック (特に TCP および UDP) を監視するには、tcpstat コマンドを使用します。発信元および宛先 IP アドレスに加えて、発信元および宛先 TCP または UDP ポート、トラフィックを送信または受信しているプロセスの PID、およびそのプロセスが動作している大域ゾーンの名前を監視できます。

次の例は、tcpstat コマンドを -c オプションとともに使用したときに報告される情報のタイプを示しています。-c オプションは、新しいレポートを前のレポートのあとに、前のレポートを上書きすることなく出力するように指定します。

```
# tcpstat -c 3
ZONE         PID PROTO  SADDR             SPORT DADDR             DPORT   BYTES
global    100680 UDP    antares           62763 agamemnon          1023   76.0
global    100680 UDP    antares             775 agamemnon          1023   38.0
global    100680 UDP    antares             776 agamemnon          1023   37.0
global    100680 UDP    agamemnon          1023 antares           62763   26.0
global    104289 UDP    zucchini          48655 antares            6767   16.0
global    104289 UDP    clytemnestra      51823 antares            6767   16.0
global    104289 UDP    antares            6767 zucchini         48655   16.0
global    104289 UDP    antares            6767 clytemnestra     51823   16.0
global    100680 UDP    agamemnon          1023 antares             776   13.0
global    100680 UDP    agamemnon          1023 antares             775   13.0
global    104288 TCP    zucchini          33547 antares            6868    8.0
global    104288 TCP    clytemnestra      49601 antares            6868    8.0
global    104288 TCP    antares            6868 zucchini         33547    8.0
global    104288 TCP    antares            6868 clytemnestra     49601    8.0
Total: bytes in: 101.0  bytes out: 200.0
```

次の出力では、tcpstat コマンドは、サーバーでもっともアクティブな 5 つの TCP トラフィックフローを報告します。

```
# tcpstat -l 5
ZONE           PID PROTO  SADDR            SPORT DADDR            DPORT   BYTES
global       28919 TCP    achilles.exampl  65398 aristotle.exampl   443   33.0
zone1         6940 TCP    ajax.example.com  6868 achilles.exampl  61318    8.0
zone1         6940 TCP    achilles.exampl  61318 ajax.example.com  6868    8.0
global        8350 TCP    ajax.example.com  6868 achilles.exampl  61318    8.0
global        8350 TCP    achilles.exampl  61318 ajax.example.com  6868    8.0
Total: bytes in: 16.0  bytes out: 49.0
```

詳細は、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「ipstat および tcpstat コマンドを使用したネットワークトラフィックの監視」および `tcpstat(1M)` のマニュアルページを参照してください。

♦ ♦ ♦ 第 3 章

3 ネームサービス構成の問題のトラブルシューティング

この章では、Oracle Solaris での基本的なネームサービスの構成と、ネットワークの正常な動作を妨げる可能性のある関連するさまざまな問題を管理およびトラブルシューティングする方法について説明します。

この章の内容は、次のとおりです。

ネームサービスの構成について

このリリースでは、ネームサービスの構成はサービス管理機能 (SMF) によって管理されます。この変更は、SMF リポジトリがすべてのネームサービスの構成のためのプライマリリポジトリになったため、ネームサービスの構成のために特定のファイルを変更する必要がなくなったことを示しています。この構成を永続的にするには、適切な SMF サービスを有効にするか、またはリフレッシュする必要があります。

インストール後にネットワーク構成が存在しない場合、ネームサービスはデフォルトで `nis files` ではなく、`files only` の動作になります。構成に関する潜在的な問題を回避するために、`svc:/system/name-service/cache` SMF サービスが常に有効になっていることを確認してください。詳細は、『Oracle Solaris 11.3 ディレクトリサービスとネームサービスでの作業: DNS と NIS』 の 第 1 章,「ネームサービスとディレクトリサービスについて」を参照してください。

DNS の問題のトラブルシューティング

次の手順について説明します。

▼ DNS クライアントの問題をトラブルシューティングする方法

Oracle Solaris 11 では、DNS クライアントへの永続的な変更を行うために `/etc/resolv.conf` ファイルを編集する必要がなくなりました。すべての DNS クライアント構成が `dns/client` SMF サービスによって管理されます。DNS クライアントを有効にする方法については、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「DNS クライアントを有効にする方法」を参照してください。

1. **DNS サービスのステータスを確認します。**

```
# svcs -xv dns/client:default
```

2. **DNS クライアントサービスのログを確認します。**

```
# more /var/svc/log/network-dns-client:default.log
```

3. **ネームサーバーの設定を確認します。**

```
# svcprop -p config/nameserver dns/client
```

4. **検索の設定を確認します。**

```
# svcprop -p config/search dns/client
```

5. **DNS のすべての設定を確認します。**

```
# svcprop -p config dns/client
```

▼ DNS サーバーの問題をトラブルシューティングする方法

1. **DNS サービスのステータスを確認します。**

```
# svcs -xv dns/server:default
```

2. **DNS サービスのログを確認します。**

```
# more /var/svc/log/network-dns-server:default.log
```

3. **syslog メッセージを確認します。**

```
# grep named /var/adm/messages
```

4. **named デーモンを起動します。**

```
# named -g
```

5. **問題を解決したら、DNS サービスをクリアします。**

```
# svcadm clear dns/server:default
```

6. **DNS サービスがオンラインに戻ったことを確認します。**

```
# svcs dns/server:default
```

NFS の問題のトラブルシューティング

次の手順について説明します。

- 55 ページの「NFS クライアントの接続の問題をトラブルシューティングする方法」
- 56 ページの「NFS サーバーをリモートで確認する方法」
- 56 ページの「サーバー上の NFS サービスに関する問題をトラブルシューティングする方法」

▼ NFS クライアントの接続の問題をトラブルシューティングする方法

NFS サーバーに接続しているクライアントに関する問題のトラブルシューティングには、根本原因に応じて、いくつかの手順が必要になる場合があります。次の手順は、NFS クライアントの接続の問題を解決するためにたどる可能性のある論理的順序に従っています。指定された手順を実行することによって問題を解決できない場合は、その問題が識別および修正されるまで、次の手順に進んでください。

1. **クライアントシステムから NFS サーバーに接続できることを確認します。**

```
# ping nfs-server
```

2. **クライアントからサーバーに接続できない場合は、ローカルのネームサービスが実行されていることを確認します。**

3. **ローカルのネームサービスが実行されている場合は、クライアントのホスト情報が正しいことを確認します。**

```
# getent hosts nfs-server
```

4. クライアント上のホスト情報が正しい場合は、別のクライアントから `ping` コマンドを実行することによって NSF サーバーへの接続を試みます。

5. 2 番目のクライアントから NFS サーバーに接続できる場合は、`ping` コマンドを使用して、最初のクライアントからローカルネットワーク上のほかのいずれかのシステムに接続できるかどうかを確認します。

   ```
   # ping other-client-system
   ```

6. ほかのクライアントに接続できない場合は、18 ページの「基本的なネットワーク診断チェックの実行」で説明されている手順に従います。

▼ NFS サーバーをリモートで確認する方法

次の手順では、NFS サーバーをリモートで確認するためにたどる論理的順序を説明しています。

1. NFS サーバー上で NFS サービスが開始されていることを確認します。

   ```
   # rpcinfo -s bee|egrep 'nfs|mountd`
   ```

2. クライアント上で次のコマンドを実行することによって、NFS サーバーの `nfsd` プロセスが応答していることを確認します。

   ```
   # rpcinfo -u nfs-server nfs
   ```

3. NFS サーバー上で `mountd` デーモンが実行されていることを確認します。

   ```
   # rpcinfo -u nfs-server mountd
   ```

4. ローカルの `autofs` サービスが使用されているかどうかを確認します。

   ```
   # cd /net/wasp
   ```

5. NFS サーバー上でファイルシステムが期待どおりに共有されていることを確認します。

   ```
   # showmount -e nfs-server
   ```

▼ サーバー上の NFS サービスに関する問題をトラブルシューティングする方法

次の手順では、サーバー上で NFS サービスが実行されているかどうかを確認するためにたどる論理的順序を説明しています。

1. **NFS サーバーがクライアントに到達できることを確認します。**

   ```
   # ping client
   ```

2. **クライアントに接続できない場合は、ローカルのネームサービスが実行されていることを確認します。**

3. **ネームサービスが実行されている場合は、サーバー上のネットワークソフトウェア構成 (`/etc/netmasks` ファイルや、`svc:/system/name-service/switch` SMF サービスに対して設定されているプロパティーなど) を確認します。**

4. **`rpcbind` デーモンが実行されているかどうかを確認します。**

   ```
   # rpcinfo -u localhost rpcbind
   ```

5. **`nfsd` デーモンが実行されているかどうかを確認します。**

   ```
   # rpcinfo -u localhost nfs
   # ps -ef | grep mountd
   ```

ネームサービスのスイッチファイルに関する問題のトラブルシューティング

ネームサービスのスイッチファイル (`/etc/nsswitch.conf`) の現在の構成を次のように確認します。

```
# svccfg -s name-service/switch listprop config
```

NIS の問題のトラブルシューティング

以降の情報では、ネットワーク情報サービス (NIS) (このガイドでは「niss」と呼びます) に関する問題をデバッグする方法について説明します。NIS サーバーまたはクライアントの問題をデバッグしようとする前に、『Oracle Solaris 11.3 ディレクトリサービスとネームサービスでの作業: DNS と NIS』 の 第 5 章,「ネットワーク情報サービスについて」を確認してください。

このセクションには、次のトピックが含まれています。

- 58 ページの「NIS のバインドに関する問題のトラブルシューティング」
- 58 ページの「単一の NIS クライアントに影響を与える問題のトラブルシューティング」
- 62 ページの「複数の NIS クライアントに影響を与える問題のトラブルシューティング」

NIS のバインドに関する問題のトラブルシューティング

NIS のバインドに関する問題の一般的な現象を次に示します。

- `ypbind` デーモンでサーバーが見つからないか、またはサーバーと通信できないというメッセージ。
- サーバーが応答していないというメッセージ。
- NIS が使用できないというメッセージ。
- クライアント上のコマンドがバックグラウンドモードでゆっくり実行されるか、または通常よりはるかに低速である。
- クライアント上のコマンドがハングアップする。システムが全体としては正常であり、新しいコマンドも実行できるにもかかわらず、コマンドがハングアップする場合がある。
- クライアント上のコマンドが不明瞭なメッセージで、または何もメッセージを表示せずにクラッシュする。

単一の NIS クライアントに影響を与える問題のトラブルシューティング

1 台か 2 台のクライアントだけで、NIS のバインドに関する問題を示す症状が発生している場合は、そのクライアントに問題があると考えられます。ただし、多数の NIS クライアントが正常にバインドできない場合は、1 台以上の NIS サーバーで問題が発生している可能性があります。62 ページの「複数の NIS クライアントに影響を与える問題のトラブルシューティング」を参照してください。

次に示すのは、単一クライアントに影響を与える一般的な NIS の問題です。

- **`ypbind` デーモンがクライアント上で実行されていない**

  あるクライアントに問題がありますが、同じサブネット上のその他のクライアントは正常に動作しています。問題のあるクライアント上で、そのクライアントの `/etc/passwd` ファイル内に存在しないファイルを含む、多数のユーザーによって所有されているファイルが含まれているディレクトリ (`/usr` など) で `ls -l` コマンドを実行します。その結果の表示に、ローカルの `/etc/passwd` ファイル内に存在しないファイルの所有者が名前ではなく、番号として含まれている場合は、そのクライアント上で NIS サービスは動作していません。

  これらの現象は通常、クライアントの `ypbind` プロセスが実行されていないことを示します。NIS クライアントサービスが実行されているかどうかを次のように確認します。

  ```
  client# svcs \*nis\*
  ```

```
STATE          STIME    FMRI
disabled       Sep_01   svc:/network/nis/domain:default
disabled       Sep_01   svc:/network/nis/client:default
```

これらのサービスが `disabled` 状態にある場合は、ログインして `root` 役割になり、NIS クライアントサービスを次のように開始します。

```
client# svcadm enable network/nis/domain
client# svcadm enable network/nis/client
```

- **ドメイン名がないか、または正しくない**

  あるクライアントに問題があり、その他のクライアントは正常に動作していますが、そのクライアント上で `ypbind` デーモンが実行されています。この場合は、そのクライアントでドメインが間違って設定されている可能性があります。

  そのクライアント上で `domainname` コマンドを実行して、どのドメイン名が設定されているかを確認します。

  ```
  client# domainname
  example.com
  ```

  その出力を、NIS マスターサーバー上の `/var/yp` ディレクトリ内の実際のドメイン名と比較します。次の例に示すように、実際の NIS ドメインは `/var/yp` ディレクトリ内のサブディレクトリとして表示されます。

  ```
  client# ls -l /var/yp
  -rwxr-xr-x 1 root Makefile
  drwxr-xr-x 2 root binding
  drwx------ 2 root example.com
  ```

  NIS クライアント上の `domainname` コマンドの出力に表示されたドメイン名が、`/var/yp` ディレクトリ内のサブディレクトリとして表示されたサーバードメイン名と同じでない場合は、`nis/domain` サービスの `config/domain` プロパティー内のドメイン名が正しくありません。NIS ドメイン名をリセットします。手順については、『Oracle Solaris 11.3 ディレクトリサービスとネームサービスでの作業: DNS と NIS』 の 「マシンの NIS ドメイン名を設定する方法」を参照してください。

注記 - NIS ドメイン名では大文字と小文字が区別されます。

- **NIS クライアントがサーバーにバインドされない**

  ドメイン名が正しく設定され、`ypbind` デーモンが実行されているにもかかわらず、依然としてコマンドがハングアップする場合は、`ypwhich` コマンドを実行することによって、クライアントがサーバーにバインドされていることを確認してください。直前に `ypbind` デーモンを起動した場合は、`ypwhich` コマンドを実行します。`ypwhich` コマンドを複数回実行することが必要になる場合があります。通常、このコマンドをはじめて実行した場合は、ドメインがバインドされていないこ

とが報告されます。このコマンドを 2 回目に実行すると、正常に処理が続行されるはずです。

- **NIS サーバーが使用できない**

  ドメイン名が正しく設定され、`ypbind` デーモンも実行されているが、NIS クライアントがサーバーと通信できないことを示すメッセージが表示される場合は、次のことを確認します。

  - このクライアントには、バインドするサーバーのリストを含む `/var/yp/binding/`*domainname*`/ypservers` ファイルが存在しますか。選択された NIS サーバーを表示するには、`svcprop -p config/ypservers nis/domain` コマンドを使用します。存在しない場合は、`ypinit -c` コマンドを実行して、このクライアントがバインドするサーバーを希望順に指定します。
  - クライアントに `/var/yp/binding/`*domainname*`/ypservers` ファイルが存在する場合は、1 または 2 台のサーバーが使用できなくなる事態に備えて、そのリストに十分な台数のサーバーが含まれていますか。選択された NIS サーバーを表示するには、`svcprop -p config/ypservers nis/domain` コマンドを使用します。含まれていない場合は、`ypinit -c` コマンドを実行することによって、リストにサーバーを追加します。
  - `/etc/inet/hosts` ファイル内に、選択された NIS サーバーのエントリがありますか。選択された NIS サーバーを表示するには、`svcprop -p config/ypservers nis/domain` コマンドを使用します。これらのシステムがローカルの `/etc/inet/hosts` ファイルに含まれていない場合は、`ypinit -c` または `ypinit -s` コマンドを実行することによって、`hosts` の NIS マップにサーバーを追加してマップを再構築します。詳細は、『Oracle Solaris 11.3 ディレクトリサービスとネームサービスでの作業: DNS と NIS』 の 「NIS マップに関する作業」を参照してください。
  - ネームサービススイッチが NIS に加えて、システムのローカルの `hosts` ファイルを確認するように設定されていますか。詳細は、『Oracle Solaris 11.3 ディレクトリサービスとネームサービスでの作業: DNS と NIS』 の 第 2 章, 「ネームサービススイッチについて」を参照してください。
  - ネームサービススイッチが最初に `services` の、次に `rpc` の `files` を確認するように設定されていますか。

- `ypwhich` **の表示に一貫性がない**

  `ypwhich` コマンドを同じクライアント上で複数回実行すると、NIS サーバーが変更されるため、その結果の表示は変化します。これは正常な動作です。NIS クライアントから NIS サーバーへのバインドは、ネットワークや NIS サーバーを使用中の場合は時間の経過に伴って変化します。ネットワークは、可能であれば常に、すべてのクライアントが NIS サーバーから受け入れ可能な応答時間を受信した時点で安定した状態になります。クライアントが NIS サービスを受けるかぎり、そのサービスがどこから来ているかは問題になりません。たとえば、ある NIS サーバーが、ネットワーク上の別の NIS サーバーから NIS サービスを受けることができます。

- **NIS サーバーのバインドが不可能な場合の対処**

ローカルサーバーのバインドが不可能な極端なケースでは、可能であれば、ypbind コマンドの ypset オプションを使用して、別のネットワークまたはサブネット上の別の NIS サーバーへのバインドを一時的に許可します。-ypset オプションを使用するには、-ypset または -ypsetme のどちらかのオプションを使用して ypbind デーモンを起動する必要があることに注意してください。詳細は、ypbind(1M) のマニュアルページを参照してください。

```
# /usr/lib/netsvc/yp/ypbind -ypset
```

別の方法については、『Oracle Solaris 11.3 ディレクトリサービスとネームサービスでの作業: DNS と NIS』 の 「特定の NIS サーバーへのバインド」を参照してください。

注意 - セキュリティー上の理由から、-ypset または -ypsetme オプションの使用はお勧めできません。これらのオプションは、制御された環境でのデバッグの目的にのみ使用してください。-ypset または -ypsetme オプションを使用すると、重大なセキュリティー侵害につながる場合があります。デーモンの実行中、だれでも NIS サーバーのバインドを変更できるため、これによって機密データへの不正なアクセスが許可される場合があります。このどちらかのオプションを使用して ypbind デーモンを起動する必要がある場合は、問題を修正したあとに ypbind プロセスを強制終了し、次にこれらのオプションを指定せずにデーモンを再起動してください。

ypbind デーモンを次のように再起動します。

```
# svcadm enable -r svc:/network/nis/client:default
```

ypset(1M) のマニュアルページを参照してください。

- **ypbind デーモンがクラッシュする**

  ypbind デーモンが起動のたびにほぼ即座にクラッシュする場合は、svc:/network/nis/client:default サービスログに問題が含まれていないかどうか調べてください。rpcbind デーモンの存在を次のように確認します。

  ```
  % ps -e |grep rpcbind
  ```

  rpcbind デーモンが存在しないか、安定しないか、または異常な動作を行う場合は、svc:/network/rpc/bind:default ログファイルを確認してください。詳細は、rpcbind(1M) および rpcinfo(1M) のマニュアルページを参照してください。

  正常に機能しているシステムから、問題のあるクライアント上の rpcbind デーモンと通信できる可能性があります。

  機能しているシステムから、次のコマンドを実行します。

  ```
  % rpcinfo client
  ```

  問題のあるシステム上の rpcbind デーモンが正常な場合は、次の出力が表示されます。

```
program version netid address service owner
...
100007    3    udp6      ::.191.161          ypbind     1
100007    3    tcp6      ::.135.200          ypbind     1
100007    3    udp       0.0.0.0.240.221     ypbind     1
100007    2    udp       0.0.0.0.240.221     ypbind     1
100007    1    udp       0.0.0.0.240.221     ypbind     1
100007    3    tcp       0.0.0.0.250.107     ypbind     1
100007    2    tcp       0.0.0.0.250.107     ypbind     1
100007    1    tcp       0.0.0.0.250.107     ypbind     1
100007    3    ticlts    2\000\000\000       ypbind     1
100007    2    ticlts    2\000\000\000       ypbind     1
100007    3    ticotsord 9\000\000\000       ypbind     1
100007    2    ticotsord 9\000\000\000       ypbind     1
100007    3    ticots    @\000\000\000       ypbind     1
...
```

アドレスが表示されない場合は (システムによってアドレスは異なります)、`ypbind` デーモンでそのサービスを登録できませんでした。システムをリブートし、`rpcinfo` コマンドを再度実行してください。`ypbind` プロセスがそこに存在し、NIS サービスを再起動しようとするたびに変更される場合は、`rpcbind` デーモンが実行されている場合でもシステムをリブートします。

複数の NIS クライアントに影響を与える問題のトラブルシューティング

1 台か 2 台のクライアントだけで、NIS のバインドに関する問題を示す症状が発生している場合は、そのクライアントに問題があると考えられます。58 ページの「単一の NIS クライアントに影響を与える問題のトラブルシューティング」を参照してください。ただし、複数の NIS クライアントが正常にバインドできない場合は、1 台以上の NIS サーバーで問題が発生している可能性がもっとも高くなります。

次に示すのは、複数のクライアントに影響を与える可能性のある一般的な NIS の問題です。

- **`rpc.yppasswdd` コマンドが `r` で始まる制限のないシェルを制限付きと見なしている**

  この問題を解決するには、次の手順を実行します。

  1. `"check_restricted_shell_name=1"` という特殊な文字列を含む `/etc/default/yppasswdd` ファイルを作成します。
  2. `"check_restricted_shell_name=1"` の文字列がコメントアウトされている場合、`r` の確認は実行されません。

- **ネットワークまたはサーバーに接続できない**

  ネットワークまたは NIS サーバーがあまりにも過負荷であるために、ypserv デーモンがクライアントの ypbind プロセスから返された応答をタイムアウト期間以内に受信できない場合は、NIS がハングアップすることがあります。NIS はまた、ネットワークがダウンしている場合にもハングアップすることがあります。

  このどちらの状況でも、ネットワーク上のすべてのクライアントで同じか、または同様の問題が発生します。ほとんどの場合、この状態は一時的です。これらのメッセージは通常、NIS サーバーが ypserv デーモンをリブートおよび再起動するか、NIS サーバー上またはネットワーク自体の負荷が減るか、またはネットワークが通常の動作を再開すると消えます。

- **NIS サーバーの誤動作**

  NIS サーバーが起動され、実行されていることを確認します。サーバーに物理的に近い場所にいない場合は、ping コマンドを使用して、サーバーに接続できるかどうかを確認します。

- **NIS デーモンが実行されていない**

  NIS サーバーが起動および実行されている場合は、正常に動作しているクライアントを見つけて、そのクライアント上で ypwhich コマンドを実行してみてください。ypwhich コマンドが応答しない場合は、強制終了します。次に、NIS サーバー上で root 役割になり、NIS プロセスが実行されているかどうかを次のように確認します。

```
# ptree |grep ypbind
100759 /usr/lib/netsvc/yp/ypbind -broadcast
527360 grep yp
```

  ypserv デーモン (NIS サーバー) も ypbind デーモン (NIS クライアント) デーモンも実行されていない場合は、これらのデーモンを次のように再起動します。

  NIS クライアントサービスを次のように再起動します。

```
# svcadm restart network/nis/client
```

  NIS サーバー上で ypserv プロセスと ypbind プロセスの両方が実行されている場合は、ypwhich コマンドを実行します。このコマンドが応答しない場合、ypserv デーモンはおそらくハングアップしているため、再起動してください。

  サーバー上で、NIS サービスを次のように再起動します。

```
# svcadm restart network/nis/server
```

- **サーバーに NIS マップの異なるバージョンが存在する**

  NIS はサーバー間でマップを伝播するため、ネットワーク上の各種の NIS サーバー上に同じマップの異なるバージョンが見つかる場合があります。このバージョンの不一致は、その違いがそれほど長く続かなければ正常であり、受け入れ可能です。

  マップの不一致のもっとも一般的な原因は、マップの正常な伝播が妨げられている場合です。たとえば、NIS サーバーまたは NIS サーバー間に配置されているルー

ターが停止している場合があります。すべての NIS サーバーおよび NIS サーバー間のルーターが実行されている場合、ypxfr コマンドは成功します。

サーバーおよびルーターが正常に機能している場合は、次のように処理を続行します。

- ypxfr のログ出力をチェックします。例21「ypxfr コマンドの出力のロギング」を参照してください。
- svc:/network/nis/xfr:default ログファイルにエラーが表示されていないかどうかをチェックします。
- 制御ファイル (crontab ファイルと yupxfr シェルスクリプト) を確認します。
- マスターサーバー上の ypservers マップをチェックします。

- **ypserv プロセスがクラッシュする**

  ypserv プロセスがほぼ即座にクラッシュし、起動を繰り返しても安定しない場合、デバッグプロセスは、ypbind のクラッシュに対するデバッグプロセスとほぼ同じです。

  まず、次のコマンドを実行して、何らかのエラーが報告されているかどうかを確認します。

  ```
  # svcs -vx nis/server
  ```

  rpcbind デーモンが存在するかどうかを、次のようにチェックします。

  ```
  # ptree |grep rpcbind
  ```

  デーモンが見つからない場合は、NIS サーバーをリブートします。このデーモンが実行されている場合は、次のコマンドを実行し、同様の出力を探してください。

  ```
  # rpcinfo -p ypserver


  program vers     proto port   service
  100000  4        tcp   111    portmapper
  100000  3        tcp   111    rtmapper
  100068 2        udp   32813  cmsd
  ...
  100007  1       tcp   34900 ypbind
  100004 2        udp   731    ypserv
  100004  1        udp   731    ypserv
  100004  1        tcp   732    ypserv
  100004  2        tcp   32772  ypserv
  ```

  前の例では、次の 4 つのエントリが ypserv プロセスを表しています。

  ```
  100004  2        udp   731    ypserv
  100004  1        udp   731    ypserv
  100004         tcp   732    ypserv
  ```

```
100004  2t       tcp   32772  ypserv
```

これらのエントリが存在せず、ypserv がそのサービスを rpcbind に登録できない場合は、システムをリブートします。エントリが存在する場合は、ypserv を再起動する前に rpcbind からこのサービスの登録を解除します。たとえば、次のようにして rpcbind からこのサービスの登録を解除します。

```
# rpcinfo -d number 1
# rpcinfo -d number 2
```

ここで、*number* は rpcinfo によって報告された ID 番号 (前の例では 100004) です。

例 21 ypxfr コマンドの出力のロギング

- 特定のスレーブサーバーでマップの更新に関する問題が発生している場合は、そのスレーブサーバーにログインし、ypxfr コマンドを対話的に実行します。

  このコマンドが失敗した場合は、失敗した原因に関するメッセージが表示され、その問題を修正できるようになります。このコマンドは成功するが、失敗した場合もあったと疑われる場合は、次のように、そのスレーブサーバー上にログファイルを作成してメッセージのロギングを有効にします。

  ```
  ypslave# cd /var/yp
  ypslave# touch ypxfr.log
  ```

  このログファイルの出力は、ypxfr コマンドを対話的に実行したときの出力に似ていますが、ログファイル内の各行にはタイムスタンプが記録される点が異なります。タイムスタンプの順序が異常なことに気付いた場合、それは、ログには ypxfr コマンドが実際に実行された各時間が示されているためです。ypxfr の複数のコピーが同時に実行されたが、その完了にかかった時間が異なる場合は、各コピーによって、そのコマンドが実行されたのとは異なる順序でサマリーステータス行がログファイルに書き込まれる可能性があります。断続的に発生するあらゆる種類の障害がログに記録されます。

  注記 - 問題を解決したら、ログファイルを削除することによってロギングを無効にします。削除し忘れた場合は、そのファイルが無制限に拡張し続けます。

- crontab ファイルと ypxfr シェルスクリプトを確認します。

  root crontab ファイルを検査し、そのファイルが起動した ypxfr シェルスクリプトを確認します。これらファイルにタイプミスがあると、伝播に関する問題が発生します。/var/spool/cron/crontabs/root ファイル内でシェルスクリプトを参照できない場合のほか、いずれかのシェルスクリプト内でマップを参照できない場合にもエラーが発生することがあります。

- ypservers マップを確認します。

また、NIS スレーブサーバーが、そのドメインのマスターサーバー上の ypservers マップに記載されていることも確認してください。記載されていない場合でも、スレーブサーバーは引き続きサーバーとして完全に動作しますが、yppush はマップの変更をそのスレーブサーバーに伝播しません。

- 壊れたスレーブサーバー上のマップを更新します。

  NIS スレーブサーバーの問題が明らかでない場合は、scp または ssh コマンドを使用して、問題のデバッグ中に回避方法を実行できます。これらのコマンドは、一貫性のないマップの最新バージョンをいずれかの正常な NIS サーバーからコピーします。

  次の例は、問題のあるマップを転送する方法を示しています。

  ```
  ypslave# scp ypmaster:/var/yp/mydomain/map.\* /var/yp/mydomain
  ```

  前の例では、* 文字がコマンド行でエスケープされ、それがローカルに ypslave でではなく、ypmaster で展開されるようにしています。

♦ ♦ ♦ 第 4 章

プロファイルベースのネットワーク管理の問題のトラブルシューティング

この章では、リアクティブプロファイルの構成および管理時に発生する可能性のある問題のトラブルシューティングについて説明します。リアクティブモードは、ノートブック PC に対して、およびネットワーク状態が頻繁に変化する状況で、もっとも一般的に使用されます。

プロファイルベースのネットワーク構成の詳細は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 第 5 章, 「Oracle Solaris でのプロファイルベースのネットワーク構成の管理について」を参照してください。

この章の内容は、次のとおりです。

プロファイルベースのネットワーク構成に関する一般的な質問への答え

ネットワーク管理のリアクティブモードを使用している場合は、次のトラブルシューティング情報を参照してください。固定モードを使用している場合のネットワーク管理の問題のトラブルシューティングについては、11 ページの「ネットワーク管理に関する一般的な質問への答え」を参照してください。詳細は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「ネットワーク構成モードについて」を参照してください。

質問: インストール後にシステムで使用されているネットワークモードを確認するにはどうしたらよいでしょうか。

回答: ネットワークモードは、インストール中にアクティブにされるプロファイルで確認します。`Automatic` プロファイルがアクティブにされている場合は、リアクティブモードになっています。`DefaultFixed` プロファイルがアクティブにされている場合は、固定モードになっています。現在システム上でアクティブになっているモードを確認するには、`netadm list` コマンドを次のように使用します。

```
# netadm list
```

質問: インストール後にシステムがデフォルトで固定モードになり、`DefaultFixed` プロファイルが現在アクティブになっています。リアクティブモードに切り替えるにはどうしたらよいでしょうか。

回答: リアクティブモードを有効にするには、`netadm enable` コマンドを使用して、`Automatic` プロファイルまたは別のリアクティブプロファイルに切り替える必要があります。たとえば、次のように `Automatic` プロファイルを有効にします。

```
# netadm enable -p ncp Automatic
```

質問: IPv6 を plumb しないようにするには、どのようなプロファイルを参照する必要がありますか。また、ネットワーク構成のこの側面は、Automated Installer (AI) の使用時またはインストール時にどのように管理されますか。

回答: IPv6 アドレスが構成されていない任意のプロファイルを作成できます。このプロファイルを有効にした場合、IPv6 は plumb されません。インストール時に AI マニフェストから新しいリアクティブプロファイルを作成することはできません。インストール後にリアクティブプロファイルを作成する場合は、`netcfg` コマンドを使用します。『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「プロファイルの構成」を参照してください。AI マニフェストを使用すると、インストールのあと、システムのリブート後にどのプロファイルをアクティブにするかを選択できることに注意してください。

質問: Oracle Solaris をインストールしたあと、システム上のネームサービスの設定が正しく設定されていません。どうしたらよいでしょうか。

回答: リアクティブモードの場合、ネームサービスの情報やその他のシステム全体の設定は、別の主なプロファイルの種類である `Location` プロファイルで指定されます。詳細は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「プロファイルタイプの説明」を参照してください。

次の例は、システム上のすべてのプロファイルとその状態を表示する方法を示しています。このコマンドを使用して、現在アクティブな `Location` プロファイルを確認します。この例の 2 番目の部分では、対話型の `netcfg` セッションを起動したあと、現在アクティブな `Location` を選択し、その構成情報を一覧表示する方法を示しています。

```
# netadm list
```

```
TYPE        PROFILE        STATE
ncp         DefaultFixed   disabled
ncp         Automatic      online
ncu:phys    net0           offline
ncu:ip      net0           offline
loc         Automatic      online
loc         NoNet          offline
loc         DefaultFixed   offline

# netcfg
netcfg> select loc myloc
netcfg:loc:myloc> list
loc:myloc
      activation-mode                manual
      enabled                        false
      nameservices                   dns
      nameservices-config-file       "/etc/nsswitch.dns"
      dns-nameservice-configsrc      dhcp
netcfg:loc:myloc>
```

前の例では、DNS が使用され、`/etc/nsswitch.dns` ファイルが参照されています。

次の例は、`myloc` という名前の `Location` の既存のネームサービスの構成を変更する方法を示しています。

```
# netadm list
TYPE        PROFILE        STATE
ncp         DefaultFixed   disabled
ncp         Automatic      online
ncu:phys    net0           offline
ncu:ip      net0           offline
loc         Automatic      offline
loc         NoNet          offline
loc         DefaultFixed   offline
loc         myloc          online

# netcfg
netcfg> select loc myloc
netcfg:loc:myloc> list
loc:myloc
activation-mode                manual
enabled                        false
nameservices                   nis
nameservices-config-file       "/etc/nsswitch.nis"
dns-nameservice-configsrc      dhcp
nfsv4-domain
netcfg:loc:myloc> set nameservices=dns
netcfg:loc:myloc> set nameservices-config-file="/etc/nsswitch.dns"
netcfg:loc:myloc> list
        activation-mode                system
        enabled                        false
        nameservices                   dns
        nameservices-config-file       "/etc/nsswitch.dns"
netcfg:loc:myloc> commit
Committed changes
netcfg:loc:myloc> exit
```

`Locations` の構成の詳細は、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「場所の作成」を参照してください。

質問: デスクトップからネットワーク管理 GUI (以前の NWAM) を起動できません。この GUI をコマンド行から起動できますか。

回答: この GUI をコマンド行から起動するには、次のコマンドを使用します。

```
% /usr/lib/nwam-manager
```

それでも GUI が起動しない場合は、デスクトップパネルの GNOME 通知領域にネットワーク管理 GUI のアイコンが表示されていることを確認してください。このアイコンが表示されていない場合は、マウスの右ボタンを押してデスクトップパネルの「パネルに追加...」オプションを選択したあと、パネルに通知領域を追加します。

質問: 通常のユーザーとしてコマンド行 (`/usr/lib/nwam-manager`) からネットワーク管理 GUI を起動したところ、次のメッセージが表示されました:「別のインスタンスが実行されています。このインスタンスは今すぐ終了します。」GUI は起動したようでしたが、そのアイコンがデスクトップ上に表示されていません。どのようにしたら GUI にアクセスできますか。

回答: デスクトップパネルにアイコンが表示されていない場合は、マウスの右ボタンを押してデスクトップパネルの「パネルに追加...」オプションを選択したあと、パネルに通知領域を追加します。

`netadm` コマンドを使用したプロファイル構成に関する問題のトラブルシューティング

システム上のプロファイルに関する情報を表示したり、プロファイルベースのネットワーク構成をトラブルシューティングしたりするには、`netadm list` コマンドを適切なオプションおよび引数とともに使用します。詳細は、netadm(1M) のマニュアルページを参照してください。

追加オプションなしで使用された場合、`netadm list` コマンドは、システム上のすべてのプロファイルとその現在の状態を表示します。

```
%  netadm list
TYPE         PROFILE        STATE
ncp          DefaultFixed   disabled
ncp          Automatic      online
ncu:phys     net0           online
ncu:ip       net0           online
loc          Automatic      online
loc          NoNet          offline
loc          DefaultFixed   offline
```

特定のプロファイルに関する情報を表示するには、次の例に示すように、プロファイルの名前を指定します。ここでは、`Automatic` プロファイルが指定されています。

```
% netadm list Automatic
```

```
TYPE         PROFILE        STATE
ncp          Automatic      online
ncu:ip       net1           offline
ncu:phys     net1           offline
ncu:ip       net0           online
ncu:phys     net0           online
loc          Automatic      online
```

システム上の特定のタイプのすべてのプロファイルに関する情報を表示するには、`netadm list` コマンドを `-p` オプションとともに使用します。たとえば、次のようにして、システム上のすべての `Location` プロファイルを表示します。

```
% netadm list -p loc
TYPE         PROFILE        STATE
loc          NoNet          offline
loc          Automatic      online
loc          DefaultFixed   offline
```

次の例では、`netadm list` コマンドを `-c` オプションとともに使用して、現在アクティブなプロファイルの構成の詳細を表示します。

```
% netadm list -c ip
TYPE         PROFILE         STATE
ncu:ip       net0            online
```

`netadm list -x` コマンドは、ネットワークインタフェースが正しく構成されない場合の原因を特定する際に役立ちます。このコマンドを使用すると、システム上の各種のプロファイル、その現在の状態、およびその状態にある理由が表示されます。

たとえば、ケーブルが抜けている場合は、`netadm list -x` コマンドを使用して、リンク状態がオフラインであるかどうかとその理由 (「link is down」など) を確認します。同様に、重複するアドレスの検出の場合、`netadm list -x` コマンドの出力では物理リンクがオンライン (起動中) であることが示されますが、IP インタフェースは保守状態にあります。この例では、表示される理由は「アドレスの重複が検出されました」です。

次の例は、`netadm list -x` コマンドを使用して取得できる情報の種類を示しています。

```
% netadm list -x
TYPE        PROFILE        STATE          AUXILIARY STATE
ncp         DefaultFixed   online         active
ncp         Automatic      disabled       disabled by administrator
loc         NoNet          offline        conditions for activation are unmet
loc         DefaultFixed   online         active
loc         Automatic      offline        conditions for activation are unmet
```

リンクまたはインタフェースがオフラインである理由を特定したら、問題の修正に進むことができます。IP アドレスが重複している場合は、`netcfg` コマンドを使用して、指定されたインタフェースに割り当てられた静的 IP アドレスを変更する必要があります。手順については、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「プロファイルのプロパティー値を設定する」を参照してください。変更を確定したら、`netadm list -x` コマンドを再度実行して、インタフェースが正しく構成され、その状態が `online` と表示されることを確認します。

インタフェースが正しく構成されていない理由の別の例として、既知の無線ローカルエリアネットワーク (WLAN) が使用できない場合があります。この場合、WiFi リンクの状態は「offline」と表示され、その理由は「need WiFi network selection」と表示されます。あるいは、最初に WiFi の選択が行われたが、鍵が必要な場合、その理由は「need WiFi key」と表示されます。

すべてのネットワーク接続の現在の状態をモニターする

ネットワーク管理デーモン `nwamd` によってモニターされているイベントを待機したり、表示したりするには、`netadm show-events` コマンドを使用します。このサブコマンドは、ネットワークプロファイルの構成プロセスに関連したイベントに関する役立つ情報を提供します。

```
% netadm show-events
EVENT                   DESCRIPTION
OBJECT_ACTION           ncp Automatic -> action enable
OBJECT_STATE            ncp Automatic -> state online, active
OBJECT_STATE            ncu link:net0 -> state offline*, (re)initialized but not config
OBJECT_STATE            ncu link:net0 -> state online, interface/link is up
OBJECT_STATE            ncu interface:net0 -> state offline*, (re)initialized but not c
OBJECT_STATE            ncu interface:net0 -> state offline*, waiting for IP address to
PRIORITY_GROUP          priority-group: 0
LINK_STATE              net0 -> state up
OBJECT_STATE            loc NoNet -> state offline*, method/service executing
OBJECT_STATE            loc Automatic -> state offline, conditions for activation are u
OBJECT_STATE            loc NoNet -> state online, active
IF_STATE                net0 -> state flags 1004843 addr 10.153.125.198/24
OBJECT_STATE            ncu interface:net0 -> state offline*, interface/link is up
OBJECT_STATE            ncu interface:net0 -> state online, interface/link is up
IF_STATE                net0 -> state flags 2080841 addr 2002:a99:7df0:1:221:28ff:fe3c:
IF_STATE                net0 -> state flags 2004841 addr 2001:db8:1:2::4ee7/128
OBJECT_STATE            loc Automatic -> state offline*, method/service executing
OBJECT_STATE            loc NoNet -> state offline, conditions for activation are unmet
OBJECT_STATE            loc Automatic -> state online, active
```

`netcfg walkprop` コマンドを使用したプロファイルプロパティーの表示および設定

プロファイルの個々のプロパティーや複数のプロパティーを対話的に表示または変更するには、`netcfg walkprop` コマンドを使用します。このコマンドを使用すると、プロファイルのさまざまなプロパティーを (1 回につき 1 つ) 表示し、必要に応じて各プロパティーを変更することができます。`walkprop` サブコマンドを使用する場合は、`set` サブコマンドを使用してプロパティー値を設定する必要はありません。

`walkprop` サブコマンドを使用してプロファイルの構成を表示または変更するには、正しい対話型のスコープ内にいる必要があることに注意してください。『Oracle

Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「プロファイルの構成」を参照してください。

手順および例については、『Oracle Solaris 11.3 でのネットワークコンポーネントの構成と管理』 の 「walkprop サブコマンドを使用してプロファイルのプロパティー値を設定する」を参照してください。

♦ ♦ ♦ 第 5 章

5 network-monitor トランスポートモジュールユーティリティーを使用したネットワーク診断の実行

この章では、ネットワーク診断モニタリングユーティリティーを使用して、Oracle Solaris システム上の誤って構成されたネットワークリソースやエラー状態を検出する方法について説明します。

この章の内容は、次のとおりです。

network-monitor トランスポートモジュールユーティリティーの概要

network-monitor (この章ではモニターとも呼びます) は、Oracle Solaris 11 システム上でネットワーク診断を実行するために使用される障害管理デーモン (fmd) トランスポートモジュールユーティリティーです。このユーティリティーはネットワークリソースをモニターし、ネットワーク機能の制限や縮退につながる可能性のある状態を報告します。モニターが異常なネットワーク条件を検出すると、レポート (*ireport* と呼ばれます) が生成されます。fmdump コマンドを使用して ireport を取得できます。77 ページの「network-monitor モジュールによって生成されたレポートの取得」を参照してください。このモニターによって、エラー状態のそれ以上の診断や、追加の復旧アクションが実行されることはありません。詳細は、network-diagnostics(4) のマニュアルページを参照してください。

このモニターは、svc:/network/diagnostics サービス管理機能 (SMF) サービス内に格納されているプロパティー値によって制御されます。詳細は、79 ページの「svc:/network/diagnostics SMF サービスによるプローブの使用の制御」を参照してください。

データリンクの MTU の不一致エラーが検出される方法

このエラー状態は、2 つのピアデータリンク間の最大転送単位 (MTU) に不一致が存在する場合に発生します。あるデータリンクがピアデータリンクで受信可能なサイズより大きいフレームを送信する可能性があるため、このタイプの不一致によってフレームが破棄される場合があります。このモニターは、MTU が大きすぎる、ローカルシステム上のすべてのデータリンクを検出しようとします。データリンクは、システムの起動時に検証されたあと、MTU の変更が発生したときに再度検証されます。

MTU の検証は、Link-Layer Discovery Protocol (LLDP) または Internet Control Message Protocol (ICMP) のどちらかのプローブ方法を使用して実行されます。LLDP サービスが有効になっているピアシステムは、情報交換に MTU の詳細を含めることができます。このユーティリティーは、ピアの MTU 情報を抽出することによって MTU の検証を実行します。LLDP 情報が使用できない場合、このモニターは、データリンクの MTU に達するまで一連の異なるサイズの ICMP プローブを転送することによって MTU を検証しようとします。このユーティリティーが、最大サイズのプローブを使用したターゲットへの接続に常に失敗する場合は、不一致のフラグが付けられます。

データリンクの VLAN ID の不一致エラーが検出される方法

仮想ローカルエリアネットワーク (VLAN) は、エンドシステムの各ホストを同じブロードキャストドメインにグループ化するために使用されます。VLAN 上の各ホストが同じ LAN 上には存在しない可能性がありますが、その場合でも、各ホストはレイヤー 2 (L2) プロトコルを使用して別のホストと通信できます。逆に、同じ LAN 上に存在しても、VLAN が異なるホストは L2 プロトコルを使用して通信することができません。VLAN 上に存在する各ホストは、ネットワークインタフェースを使用して VLAN 上のほかのホストと通信します。VLAN は、関連するネットワークインタフェースを経由して LLDP デーモンによって各ピアにエクスポートされる VLAN 識別子 (VID) で識別されます。これらのピアは通常、ネットワークデバイスであり、これには、VID を使用して対応するホストにデータパケットを転送するスイッチなどが含まれます。

関連するネットワークインタフェース上で VID が正しく構成されていない場合は、ホストが目的のパケットを受信できない可能性があります。VLAN ID 不一致モニター

は、VID 情報を VLAN 情報が変更されるたび、システムのブート時、さらに定期的に検証するため、このタイプの構成ミスを取り込むことができます。インタフェースの VID が変更された場合は、適切な ireport メッセージが生成されます。VLAN 情報は LLDP パケットを使用して検証されるため、ピアホストで LLDP サービスが有効になっている必要があります。『Oracle Solaris 11.3 でのネットワークデータリンクの管理』 の 第 6 章,「リンク層検出プロトコルによるネットワーク接続情報の交換」を参照してください。

network-monitor モジュールの管理

fmadm コマンドは、モニターの現在のステータスを報告し、次の例に示すように、障害モニタリングを実行しているときは active と表示されます。

```
# fmadm config

  MODULE                   VERSION STATUS  DESCRIPTION
  cpumem-retire            1.1     active  CPU/Memory Retire Agent
  disk-diagnosis           0.1     active  Disk Diagnosis engine
  ...
  network-monitor          1.0     active  Network monitor
```

/usr/lib/fm/fmd/plugins/network-monitor.conf 構成ファイルには、network-monitor の状態を制御する enable プロパティーがあります。モニターを有効にするには、次のように enable プロパティーを true に設定します。

```
# enable
#
# Enable/disable the network-monitor.
#
setprop enable true
```

モニターはリブート時にアクティブになります。

network-monitor モジュールによって生成されたレポートの取得

ネットワークに関する問題が発生した場合や、ネットワークパフォーマンスの縮退が疑われる場合は、fmdump コマンドを使用して、network-monitor によって生成された ireport を取得できます。これらのレポートには、潜在的な問題が検出されたデータリンクの名前が含まれています。

たとえば、次のコマンドを実行することによって ireport を取得できます。

```
# fmdump -IVp -c 'ireport.os.sunos.net.datalink.*'
```

-I　　情報レポートを取得することを指定します。

-v　　レポートの内容をダンプすることを指定します。

-p　　レポートを出力することを指定します。

-c *class*　　イベントのタイプを指定します。

-c *class* オプションを使用すると、特定のクラスに一致するイベントのみを出力できます。このモニターによって生成されたイベントには、'ireport.os.sunos.net.datalink' のクラス接頭辞が使用されます。

詳細は、fmdump(1M) のマニュアルページを参照してください。

次の例は、network-monitor によって送信された ireport の出力を示しています。

```
nvlist version: 0
     class = ireport.os.sunos.net.datalink.mtu_mismatch
     version = 0x0
     uuid = f3832064-e83b-6ce8-9545-8588db76493d
     pri = high
     detector = fmd:///module/network-monitor
     attr = (embedded nvlist)
     nvlist version: 0
  linkname = net0
  linkid = 0x3
  mtu = 0x1b58
     (end attr)
 __ttl = 0x1
 __tod = 0x513a4f2e 0x279ba218
```

この特定の ireport の出力には、次の情報が含まれています。

class　　エラー状態のタイプを指定します。network-monitor モジュールによって送信された ireport には、ireport.os.sunos.net.datalink の接頭辞が付けられます。前の例に示したように、この情報は -c オプションで指定されます。

linkname　　この状態が検出されたデータリンクの名前を指定します。

fmstat コマンドを使用した network-monitor モジュールの統計情報の表示

fmstat コマンドは、障害管理モジュールの統計情報を報告します。また、このコマンドを使用すると、network-monitor トランスポートモジュールユーティリティーを含む、現在障害管理に参加している診断エンジンやエージェントの統計情報を表示することもできます。

特定の障害管理モジュールによって保持されている統計情報を表示するには、次のコマンド構文を使用します。

```
# fmstat -m module
```

ここで、-m *module* は障害管理モジュールを指定します。

たとえば、network-monitor の統計情報は、次のように表示します。

```
# fmstat -m network-monitor
                NAME VALUE            DESCRIPTION
mtu-mismatch.allocerr 0               memory allocation errors
mtu-mismatch.enabled true             operating status for mtu-mismatch
mtu-mismatch.nprobes 7                number of transmitted ICMP probes
mtu-mismatch.procerr 0                errors processing datalinks
          sysev_drop 0                number of dropped sysevents
vlan-mismatch.enabled true            operating status for vlan-mismatch
```

fmstat コマンドの使用の詳細は、fmstat(1M) のマニュアルページを参照してください。

障害管理に参加しているモジュールのリストを取得するには、fmadm コマンドを使用します。fmadm(1M) のマニュアルページを参照してください。

svc:/network/diagnostics SMF サービスによるプローブの使用の制御

このモニターが実行する診断のタイプは、svc:/network/diagnostics SMF サービスの policy/allow_probes プロパティー内に格納されている値によって制御されます。このプロパティーによって、診断エージェントがネットワークに関する問題のモニタリングや報告の目的でプローブパケットを転送できるかどうかが決定されます。このプロパティーの値を設定または変更するには、svccfg コマンドを使用します。有効な値は true と false です。デフォルトでは、このプロパティーは true に設定されています。詳細は、svccfg(1M) および network-diagnostics(4) のマニュアルページを参照してください。

例 22 診断プローブの転送の無効化

次の例は、svc:/network/diagnostics SMF サービスの policy/allow_probes プロパティーを false に設定することによって診断プローブの転送を無効にする方法を示しています。変更を有効にするには、デフォルト値を変更したあとに SMF サービスをリフレッシュする必要があります。

```
# svccfg -s network/diagnostics setprop policy/allow_probes = boolean: false
# svccfg -s network/diagnostics refresh
```

索引

は

ま

ら

D

H

I

N