ネットワーク用語集

Part No: E62686
2016 年 11 月

Part No: E62686

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 ネットワークに関連して使用される一般的なネットワーク用語と頭字語の定義を示します。
- **対象読者** – システム管理者。
- **前提知識** - ネットワーク管理の基本的なスキルと一部の高度なスキル。

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 Oracle Solaris ネットワーク用語

この用語集では、ホワイトペーパー、仕様、およびユーザーやトレーニング用のドキュメントの執筆の手助けとなり、確実に一貫性を持って使用できるよう、Oracle Solaris でよく使われるネットワーク用語と頭字語を定義します。この用語集には、すべてのネットワークに広く適用される用語を完全に網羅したリストが含まれているわけではありません。また、この用語集の用語の多くは、Oracle Solaris ネットワーク技術に固有の用語です。

用語集

3DES Triple-Data Encryption Standard の略。Data Encryption Standard (DES) 暗号アルゴリズムを適用してデータを 3 回暗号化する対称鍵暗号化方法。3DES では鍵の長さとして 168 ビットが必要です。3DES は Triple-DES とも呼ばれます。

6to4 IPv4 ネットワーク上で IPv6 パケットを転送する自動トンネルメカニズム。6to4 トンネルを使用すると、分離された IPv6 サイトが、明示的なトンネルを構成しなくても IPv4 上で自動トンネルを介して通信できます。

アイデンティティーアソシエーション IA を参照してください。

アイデンティティーアソシエーション識別子 IAID を参照してください。

アップリンクポート Oracle Solaris EVS 機能を使用するときに、VNIC が作成されるデータリンク。

アドレス解決プロトコル ARP を参照してください。

インターネットセキュリティーアソシエーションおよび鍵管理プロトコル ISAKMP を参照してください。

インターネットブートストラッププロトコル BOOTP を参照してください。

インターネットプロトコルのバージョン 4 IPv4 を参照してください。

インターネットプロトコルのバージョン 6 IPv6 を参照してください。

インターネットプロトコルバージョン 6 制御プロトコル IPCP を参照してください。

インターネットプロトコル制御プロトコル IPCP を参照してください。

インターネットレジストリ IR を参照してください。

インターネット鍵交換 IKE を参照してください。

インターネット制御メッセージプロトコル ICMP を参照してください。

エッジ仮想ブリッジング EVB を参照してください。

エニーキャストアドレス 通常は別のノードに属する、インタフェースグループに割り当てられる IPv6 アドレス。エニーキャストアドレスに送られたパケットは、そのアドレスを持つ、プロトコルに基づき「もっとも近い」インタフェースに配送されます。パケットのルートは、ルーティングプロトコルの距離測定に応じて決定されます。

エニーキャストグループ 同じエニーキャスト IPv6 アドレスからなるインタフェースグループ。IPv6 の Oracle Solaris 実装は、エニーキャストアドレスやグループの作成をサポートしていません。ただし、Oracle Solaris IPv6 ノードはトラフィックをエニーキャストグループに送信できます。

エラスティック仮想スイッチ EVS を参照してください。

カプセル化 パケットがネットワークプロトコルスタックを通過するとき、各層のプロトコルは、基本ヘッダーにフィールドを追加したり、そこからフィールドを削除したりします。送信側ホストのプロトコルがパケットヘッダーにデータを追加する場合、そのプロセスをデータのカプセル化と呼びます。

カプセル化セキュリティーペイロード ESP を参照してください。

キーストア 暗号化鍵が格納されるディスクまたはカード上の場所。

キーストア名 管理者がキーストアに付ける名前。暗号化フレームワークでは、キーストア名は 'トークン' または 'トークン ID' とも呼ばれます。

コールバック制御プロトコル CBCP を参照してください。

コミュニティー VLAN セカンダリ VLAN のタイプ。コミュニティー VLAN に関連付けられたポートは、同じコミュニティー VLAN 内にあるプライマリ VLAN とその他のポートと通信できます。プライマリ VLAN ドメイン内に複数のコミュニティー VLAN を作成できます。

サーバーメッセージブロック SMB を参照してください。

サービス管理機能 SMF を参照してください。

サービス拒否攻撃 意図的または不注意により、受信ネットワークパケットがサーバーに押し寄せる攻撃。サーバーのスループットが多大な影響を受けたり、サーバーが過負荷になり機能しなくなったりする可能性があります。

サブネット それぞれのネットマスクを含む、サブネット番号と IP アドレススキームによってシステムを接続する IP ネットワークを論理的に分割したもの。

シングルルート I/O 仮想化 SR-IOV を参照してください。

スタンバイインタフェース グループ内のほかの物理インタフェースに障害が発生した場合だけデータの伝送に使用される物理インタフェース。

ステートフルパケットフィルタ アクティブな接続の状態をモニターし、そこから得た情報を使ってパケットフィルタを通過させるネットワークパケットを決めるファイアウォール。要求と応答を追跡、照合することによって、ステートフルパケットフィルタは、要求と一致しない応答を選別できます。

ステートレス自動構成 ホストがそれ自身の IPv6 アドレスを生成する処理。その生成は、ホスト自身の MAC アドレスと、ローカル IPv6 ルーターによって表明される IPv6 接頭辞を結合することによって行われます。

ストリーム制御転送プロトコル SCTP を参照してください。

スパニングツリープロトコル STP を参照してください。

スプーフィング コンピュータに不正にアクセスするために、メッセージが、信頼されるホストから来たかのように見える IP アドレスを使ってコンピュータにメッセージを送信すること。IP のなりすましを行うために、送信者はまず、さまざまなテクニックを使って、信頼されるホストの IP アドレスを見つけ、次にパケットヘッダーを変更します。それによって、パケットは、そのホストから来たかのように見えます。

セカンダリ VLAN プライマリ VLAN のサブ VLAN。

セキュア RPC セキュアリモート手続き呼び出し (Secure Remote Procedure Call)。認証メカニズムを使用してリモート手続きを保護する方式。Diffie-Hellman 認証メカニズムは、サービスを要求するホストとユーザーを認証します。認証メカニズムでは DES 暗号化を使用します。Secure RPC を使用するアプリケーションには、NFS と NIS ネームサービスが含まれます。

セキュアハッシュアルゴリズム SHA-1 を参照してください。

セキュアリモート手続き呼び出し セキュア RPC を参照してください。

セキュリティーアソシエーション SA を参照してください。

セキュリティーアソシエーションデータベース SADB を参照してください。

セキュリティーパラメータインデックス SPI を参照してください。

セキュリティーポリシーデータベース SPD を参照してください。

セレクタ IPQoS では、ネットワークストリームからトラフィックを選択するために、特定クラスのパケットに適用される条件を具体的に定義する要素。セレクタは、IPQoS 構成ファイル内のフィルタ句に定義します。

ダイアルアウトマシン ダイアルアップリンクを確立するための呼び出しを開始するピア。構成後は、ダイアルアウトマシンは任意の台数のダイアルインサーバーを呼び出すことができます。一般に、ダイアルアップリンクを確立するには、ダイアルアウトマシンが認証資格を提供する必要があります。

ダイアルアップ PPP リンク 電話回線または ISDN が提供する媒体など、通信媒体の一方の端にピアとモデムが使用されている PPP 接続。「ダイアルアップ」という用語は、ローカルモデムがリモートピアの電話番号を使用してダイアルアップする場合のリンクネゴシエーションにおけるシーケンスを指します。ダイアルアップリンクは最も広く使用され、最小コストの PPP 構成です。

ダイアルインサーバー ダイアルアウトマシンから呼び出しを受け、ダイアルアップ PPP リンクの受け取り側をネゴシエーションし、確立するピア。「ダイアルインサーバー」という用語が一般に使用されていますが、クライアントサーバーという形では動作しません。形としては、ピアがダイアル

アップリンクの設定要求に応答するだけです。構成後は、ダイアルインサーバーは任意の台数のダイアルアウトマシンからの呼び出しを受信できます。

ダイレクトメモリーアクセス DMA を参照してください。

チャネルサービスユニット CSU を参照してください。

チャレンジハンドシェーク認証プロトコル CHAP を参照してください。

データアドレス データの発信元アドレスまたは宛先アドレスとして使用できる IP アドレス。データアドレスは IPMP グループの一部であり、グループ内の任意のインタフェース上でトラフィックの送受信に使用できます。さらに、IPMP グループ内の 1 つのインタフェースが機能している場合は、IPMP グループのデータアドレスのセットを継続的に使用することができます。

データサービスユニット DSU を参照してください。

データセンターブリッジング DCB を参照してください。

データセンターブリッジング交換プロトコル DCBX を参照してください。

データリンクマルチパスアグリゲーション DLMP アグリゲーションを参照してください。

データ暗号化規格 DES を参照してください。

デジタル署名 送信側を一意に識別する、電子的に転送されたメッセージに添付されるデジタルコード。

テナント エラスティック仮想スイッチとそのリソースが含まれている論理グループ。リソースは、テナントの名前空間の外部からは見えません。

デュアルスタック IPv4 プロトコルと IPv6 プロトコルの両方が同じネットワークインフラストラクチャーでトンネルメカニズムを使用せずに動作できるようにする TCP/IP プロトコルスタック。Oracle Solaris のネットワークはデュアルスタックです。このデュアルスタック技術はホストとルーターの両方でサポートされています。

ドメインネームシステム DNS を参照してください。

トランクアグリゲーション IEEE 802.3ad 標準に基づくリンクアグリゲーション。トランクアグリゲーションは、複数のトラフィックのフローを集約されたポートのセットに分散できるようにすることで機能します。IEEE 802.3ad はスイッチ構成を必要とし、複数のスイッチ全体で機能させるためには、スイッチのベンダー独自の拡張機能も必要です。

ネットワークアカウンティング 追跡、プロビジョニング、統合、または請求のためにログファイル内のネットワークトラフィックに関する統計情報を取り込むために使用される方法。

ネットワークアドレス変換 NAT を参照してください。

ネットワークインタフェースカード NIC を参照してください。

ネットワークファイルシステム NFS を参照してください。

ネットワーク構成プロファイル NCP を参照してください。

ネットワーク構成ユニット NCU を参照してください。

ネットワーク情報サービス NIS を参照してください。

ノード コンピュータネットワークでは、ノードはデータの送信用の接続ポイントまたはエンドポイントです。

パケット 通信回線上で、1 単位として送られる情報の集合。MAC ヘッダーとペイロードが含まれ、場合によっては IP ヘッダーも含まれています。

パケットフィルタ 指定するパケットのファイアウォールの通過を許可するようにも許可しないようにも構成できるファイアウォール機能。

パケットヘッダー IP ヘッダーを参照してください。

パスワード認証プロトコル PAP を参照してください。

バックアップルーター アクティブであってもマスター状態ではない VRID の VRRP インスタンスは、バックアップルーターと呼ばれます。1 つの VRID に対して任意の数のバックアップルーターが存在できます。現在のマスタールーターで障害が発生した場合は、バックアップルーターがそのマスタールーターの役割になれます。VRRP および VRID も参照してください。

ハッシュベースメッセージ認証符号 HMAC を参照してください。

ファイアウォール 組織のプライベートネットワークやイントラネットをインターネットから切り離し、外部からの進入を防止するためのハードウェアまたはソフトウェア。ファイアウォールには、フィルタリングや、プロキシサーバー、NAT などを組み込むことができます。

フィルタ クラスの特性を IPQoS 構成ファイル内に定義するための規則セット。IPQoS システムでは、IPQoS 構成ファイル内に定義されたフィルタに適合するトラフィックフローを選択して処理します。パケットフィルタを参照してください。

プライベート VLAN PVLAN を参照してください。

プライベートアドレス インターネット経由でルーティングできない IP アドレス。プライベートアドレスは、インターネット接続を必要としない社内ネットワークのホストで使用できます。IPv4 プライベートアドレスについての詳細は、RFC 1918 (`https://tools.ietf.org/html/rfc1918`) を参照してください。IPv6 プライベートアドレスについての詳細は、RFC 4193 (`http://www.ietf.org/rfc/rfc4193.txt`) を参照してください。

プライベート仮想ネットワーク システム上のほかの仮想ネットワークと外部ネットワークの両方から切り離された仮想ネットワーク。プライベート仮想ネットワークは etherstub 上に構成されます。

プライマリ MAC クライアント NIC または PV NIC を表し、独自のアドレスと L2 (MAC) および L3 (IP) レイヤーのその他の属性を持つ MAC クライアント。

プライマリ VLAN 標準の (IEEE 802.1Q) VLAN。

フラットネットワーク エラスティック仮想スイッチの実装に使用されます。すべての VM インスタンスを VLAN または VXLAN なしで同じセグメント上に配置できます。VLAN タグ付けまたはほかのタイプのネットワークセグメント化はありません。

フロー 単一の属性または属性の組み合わせに基づいてネットワークパケットを分類するためのカスタマイズされた方法。フローを作成するための基盤として機能する属性は、ネットワークパケットのヘッダー内の情報から引き出されます。フローは SLA に関連付けることができ、可観測性に使用できます。

フローアカウンティング IPQoS でのトラフィックフローに関する情報の蓄積および記録のプロセス。フローアカウンティングは、IPQoS 構成ファイルの `flowacct` モジュールにパラメータを定義することによって確立できます。

ブロードキャスト ネットワークにおいて、サブネット上の送信側を除くすべてのシステムにパケットを同時に送信するために使用される方法。通常はブロードキャストパケットがサブネットを超えてルーティングされることはありません。

フローの優先順位 フローに属するパケットが処理される優先順位。フローの `priority` プロパティーが `high` に設定されている場合は、そのフローに属するすべてのパケットが、同じデータリンク上のほかのパケットの前に処理されます。このプロパティーは、待機時間の影響を受けやすいアプリケーションのフローを作成するために使用されます。

フロー属性 ネットワークパケットのヘッダー内の情報から引き出され、フローを作成するための基盤として機能する属性。属性には、トランスポートプロトコル名、IP アドレス、アプリケーションポート番号、および DS フィールドを含めることができます。

プロキシサーバー クライアントと別のサーバーの間の中継サーバー。キャッシュサービス、管理、およびセキュリティーを提供します。たとえば、プロキシサーバーを使用して、特定の Web サイトにアクセスできないようにします。

プロミスキャストランクポート 分離された VLAN とコミュニティー VLAN の両方と通信できる最上位のスイッチアップリンクポートで構成されたポート。

ペイロード パケットで伝送されるデータ。ペイロードには、パケットを宛先に送るために必要なヘッダー情報は含まれません。

ポイントツーポイントプロトコル PPP を参照してください。

ポート VLAN 識別子 PVID を参照してください。

ホスト ネットワークホストは、任意のデバイス、またはコンピュータネットワークに接続されているコンピュータです。ネットワークホストは、サービス、情報リソース、およびアプリケーションをネットワークのユーザーやほかのノードに提供します。

ホップ 2 つのホストを分離するルーターの数を判別するための手段。たとえば、始点ホストと終点ホストが 3 つのルーターで分離されている場合、ホストは互いに 4 ホップ離れています。

ホップ単位動作 PHB を参照してください。

マーカー パケットの転送方法を指示する値をパケットに付ける diffserv アーキテクチャーのモジュールの 1 つ。

マスタールーター ある瞬間に仮想ルーターの経路制御機能を実行する VRRP インスタンス。ある特定の VRID である瞬間にアクティブになっているマスタールーターは、1 つだけです。マスタールーターが、仮想ルーターに関連付けられた 1 つまたは複数の IPv4 または IPv6 アドレスを制御します。仮想ルーターは、マスタールーターの IP アドレスに送信されたパケットを転送します。VRRP および VRID も参照してください。

マルチキャスト ネットワーク層手順。IP ネットワーク上の複数システムにデータグラムパケットを送信するのに使用されます。ブロードキャストルーティングとは異なり、パケットはすべてのシステムによって処理されるわけではありません。マルチキャストでは、ルーターを Distance Vector Multicast Routing Protocol (DVMRP) などの特定のルーティングプロトコルで構成するルーターが必要です。DVMRP についての詳細は、RFC 1075 (`http://tools.ietf.org/rfc/rfc1075.txt`) を参照してください。

マルチキャストアドレス インタフェースのグループを識別する IPv4 または IPv6 アドレス。マルチキャストアドレスに送信されるパケットは、グループにあるすべてのインタフェースに配信されます。

マルチホームホスト 複数のインタフェースを持ち、パケット転送を行わないシステム。マルチホームホストではルーティングプロトコルを実行できます。

メーター 特定クラスのトラフィックフローの速度を測定する diffserv アーキテクチャーのモジュール。IPQoS 実装には、`tokenmt` および `tswtclmt` という 2 つのメーターがあります。

ユーザーデータグラムプロトコル UDP を参照してください。

ユーザー優先順位 サービスクラス (CoS) マークを実装する 3 ビット値。CoS は、VLAN デバイスのネットワーク上での Ethernet データグラムの転送方法を定義します。

ユニキャストアドレス IPv6 が有効なノードの単一インタフェースを識別する IPv6 アドレス。ユニキャストアドレスは、サイト接頭辞や、サブネット ID、インタフェース ID などからなります。

ラージレシーブオフロード LRO を参照してください。

リアクティブネットワーク構成モード 手動の再構成を必要とせずに、システムが自動的にネットワーク状況の変化に適応するネットワーク構成モード。

リダイレクト 特定の終点に到達するために、ホストに対して最適な最初のホップノードを、ルーターが通知すること。

リンクアグリゲーション ネットワークトラフィックのスループットを向上させて、高可用性を実現するために、システム上の複数のリンクを単一の論理ユニットにリンクする方法。リンクアグリゲーションは、DLMP アグリゲーションとトランクアグリゲーションを含む L2 エンティティーです。

リンクアグリゲーション制御プロトコル LACP を参照してください。

リンクローカルアドレス IPv6 で自動アドレス構成などのために、単一リンク上でアドレスを指定するために使用される指定。デフォルトでは、リンク - ローカル・アドレスはシステムの MAC アドレスから作成されます。

リンク制御プロトコル LCP を参照してください。

リンク層検出プロトコル LLDP を参照してください。

ルーター 複数のインタフェースを持ち、ルーティングプロトコルを実行し、コンピュータネットワーク間でデータパケットを転送するシステム。ルーターはトラフィックをインターネット上に向けて、さまざまなネットワークからの複数のデータ回線を接続します。ルーターは、パケットがその宛先に到達するまで、ネットワークを介してルーターから別のルーターへとデータパケットを転送します。

ルーター広告 ルーターが、各種のリンクパラメータおよびインターネットパラメータと共に、その存在を定期的にあるいはルーター要請メッセージに応じて通知すること。

ルーター発見 ホストが、接続されているリンク上にあるルーターを特定すること。

ルーター要請 ホストがルーターに対し、次に予定されている時間ではなく、ただちにルーター広告メッセージを送信するように要求すること。

ルーティングテーブル パケットのルーティング情報が含まれているテーブルであり、その宛先に到達するためのパケットの最適なパスを決定するために役立ちます。

ルーティング情報プロトコル RIP を参照してください。

ローカル使用アドレス ローカルのルーティング可能な範囲だけを対象とするユニキャストアドレス (サブネット内またはネットワーク内)。また、ローカルまたはグローバルな一意の範囲を対象とすることもできます。

圧縮制御プロトコル CCP を参照してください。

仮想 IP アドレス VRIP を参照してください。

仮想 LAN デバイス VLAN デバイスを参照してください。

仮想スイッチ 仮想マシン間の通信を容易にするエンティティー。仮想スイッチは、物理マシン内の仮想マシン (VM 間トラフィック) 間のトラフィックをループし、このトラフィックを外部ネットワークには送信しません。VNIC が作成されて、EVS によって管理されると、仮想スイッチが自動的にインスタンス化されます。

仮想ステーションインスタンス VSI を参照してください。

仮想ネットワーク 物理ネットワークをエミュレートし、ハードウェアとソフトウェアのネットワークリソースの組み合わせであるネットワーク。

仮想ネットワークインタフェースカード VNIC を参照してください。

仮想ネットワーク識別子 VNI を参照してください。

仮想プライベートネットワーク VPN を参照してください。

仮想ポート VNIC とエラスティック仮想スイッチの間の接続ポイント。仮想ポートは、仮想ポートに接続すると VNIC に継承される、さまざまなネットワーク構成パラメータをカプセル化します。

仮想ルーター ID VRID を参照してください。

仮想ルーター冗長プロトコル VRRP を参照してください。

仮想ローカルエリアネットワーク VLAN を参照してください。

仮想拡張ローカルエリアネットワーク VXLAN を参照してください。

仮想機能 VF を参照してください。

解釈ドメイン DOI を参照してください。

回復検出 障害の発生後、NIC や NIC からレイヤー 3 デバイスへの経路が、正しく動作し始めたことを検出する処理。

外部ネットワーク修飾子 ENM を参照してください。

拡張アカウンティング タスク、プロセス、フロー、またはネットワークコンポーネントに関するリソース消費統計情報を記録できる方法。一定期間にわたるデータリンクとフローの統計情報をログファイルに定期的に記録できます。このデータは、あとで分析のために取得できます。

タスク、プロセス、フロー、またはネットワークコンポーネントに関するリソース消費統計情報の記録を可能にします。データリンクとフローの統計情報は、あとで分析のために取得できるように、一定期間にわたって定期的にログファイルに記録できます。

ネットワークアカウンティングも参照してください。

拡張サービスセット識別子 ESSID を参照してください。

拡張伝送選択 ETS を参照してください。

逆アドレス解決プロトコル RARP を参照してください。

近傍検索 接続されているリンク上にあるほかのホストをホストが特定できるようにするための IP メカニズム。

近傍通知 近傍要請メッセージに対する応答、またはデータリンク層アドレスの変更を通知するために、ノードが自発的に近傍通知メッセージを送ること。

近傍要請 近傍のリンク層アドレスを決定するために、ノードによって送信される要請。また、キャッシュされたリンク層アドレスによって近傍が到達可能であるかを確認します。

結果 (outcome) IPQoS では、トラフィックの計測結果に基づいて実行されるアクション。IPQoS メーターは、赤、黄、および緑の 3 つの結果があります。結果は IPQoS 構成ファイル内に定義します。

検査用アドレス IPMP グループ内の IP アドレスで、検査信号用の発信元アドレスまたは宛先アドレスとして使用する必要があり、データトラフィック用の発信元アドレスまたは宛先アドレスとして使用してはならないもの。

鍵管理 暗号化鍵の管理。この管理には、ユーザー間またはシステム間の、ユーザーレベルでの鍵の生成、交換、格納、使用、および置換が含まれます。

固定ネットワーク構成モード ネットワーク状況が変化したかどうかにかかわらず、システムのインスタンス化された構成が変更されないネットワーク構成モード。このような、インタフェースの追加などの変化が発生した場合は、新しい環境に適応させるためにシステムのネットワークを再構成する必要があります。

公開鍵インフラストラクチャー PKI を参照してください。

公開鍵暗号化 数学的に関連付けられた 2 つの異なる鍵を必要とする暗号化アルゴリズム。公開鍵はだれでも使用できます。非公開鍵は、メッセージの受信者だけが知っています。公開鍵暗号化は非対称暗号化とも呼ばれます。

再実行攻撃 データ送信中に侵入者によってパケットが捕捉されるネットワーク攻撃。捕捉されたパケットは、不正なパケットに置き換えられるか、あとで繰り返されます。そのような攻撃を防止するために、パケットを

保護している秘密鍵が存在している間、値が増加を続けるフィールドをパケットに含めることができます。

最小カプセル化 ホームエージェント、外来エージェント、およびモバイルノードによってサポートされる任意の形態の IPv4 内 IPv4 トンネリング。最小カプセル化は、IP 内 IP カプセル化よりも 8 ないし 12 バイト少ないオーバーヘッドしか持ちません。

最大転送単位 MTU を参照してください。

次世代のルーティング情報プロトコル RIPng を参照してください。

自動ネゴシエーション 接続済みの 2 つのデバイスが、速度、デュプレックスモード、フロー制御などの伝送パラメータに関する機能を共有する Ethernet プロシージャー。接続済みのデバイスは、サポートするもっとも高いパフォーマンス伝送モードを使用します。

自律システム 複数のルーターとネットワークがあるサイトのネットワークトポロジの管理に使用される、単一のルーティングドメイン。このルーティングドメインは 1 つ以上の IP 接頭辞の接続グループであり、単一の明確に定義されたルーティングポリシーを持ちます。詳細は、RFC 1930 (`http://tools.ietf.org/html/rfc1930`) を参照してください。

識別名 DN を参照してください。

準仮想化 NIC PV NIC を参照してください。

証明書失効リスト CRL を参照してください。

障害管理リソース識別子 FMRI を参照してください。

障害検出 インタフェースや、インタフェースからインターネット層デバイスまでのパスが動作していないことを検出する処理。IP ネットワークマルチパス (IPMP) とデータリンクマルチパス (DLMP) には、障害検出のタイプとして、リンクベース (デフォルト) と検証ベース (オプション) があります。

障害検出時間 FDT を参照してください。

信頼できる呼び出し元 PPP において、ダイアルインサーバーがアクセスを許可するリモートピア。リモートピアのセキュリティー資格をダイアルインサーバーの PAP または CHAP シークレットデータベースに追加することによりアクセスを許可します。

静的ルーティング システムネットワーク管理者がルートを手動でルーティングテーブルに追加できるプロセス。

専用回線 PPP リンク ホストと、プロバイダからリースした同期ネットワーク媒体に接続された CSU/DSU からなる PPP 接続。Optical Carrier 3 (OC3) と T キャリア (T1) は、専用回線媒体の一般的な例です。管理は簡単ですが、専用回線リンクはダイアルアップ PPP リンクよりも費用がかかることから、広くは使われていません。

双方向トンネル 双方向にパケットを送信するトンネル。

対称鍵暗号化 メッセージの送信側と受信側が 1 つの共通鍵を共有する暗号化システム。この共通鍵は、メッセージを暗号化および復号化するために使用されます。Advanced Encryption Standard は、対称鍵の一例です。

帯域幅共有 同じデータリンク上のほかの VNIC との競合が発生した場合に VNIC が取得する帯域幅の最小共有。

帯域幅制御 アプリケーションごと、ポートごと、プロトコルごと、およびアドレスごとに物理 NIC の使用可能な帯域幅を制御できます。

帯域幅遅延積 ネットワークを介して送信されるデータの量を測定します。このデータは、使用可能なネットワーク帯域幅と接続の待機時間またはラウンドトリップ時間の積です。

盗聴 コンピュータネットワーク上で盗聴すること。普通のテキストによるパスワードなどの情報をネットワークから自動的に選別するプログラムの一部としてしばしば使用されます。

等コストマルチパス ECMP を参照してください。

動的パケットフィルタ ステートフルパケットフィルタとも呼ばれます。

動的ホスト構成プロトコル DHCP を参照してください。

動的ルーティング IPv4 ネットワーク用の RIP や IPv6 ネットワーク用の RIPng などのルーティングプロトコルを使用することによって、システムが自動的にルーティングテーブルを更新するというルーティングのタイプ。動的ルーティングは、多数のホストがある大規模なネットワークでの使用が最適です。

動的再構成 DR を参照してください。

同期 PPP 同期デジタル回線上の PPP の形式。生のビットを連続ストリームとして転送します。専用回線 PPP リンクは同期 PPP を使用します。

認証 プログラムなどのエンティティーまたはリモートユーザーがネットワークを通して提供する識別情報の検証作業。

認証ヘッダー IP データグラムに対し認証と完全性を提供する拡張ヘッダー。機密性は提供されません。

認証局 CA を参照してください。

反射型リレー 外部スイッチによってループバックされる通信で VM 間トラフィックを送信するオプションを提供し、複数のホストを共有ホスト上の複数の VM またはゾーンに統合できようにする EVB の機能。

非対称ルーティング パケットがパス内のソースから宛先に移動しても、ソースに戻る際に別のパスをとるときに発生します。一般的にはレイヤー 3 (ネットワーク層) ルーティングネットワークで見られます。

非対称鍵暗号化 メッセージの送受信側で異なる鍵を使用してメッセージの暗号化および暗号解除を行う暗号化システム。非対称鍵を使用すると、対称鍵暗号に対するセキュアなチャネルを作成できます。Diffie-Hellman プロトコルは、非対称鍵プロトコルの例です。

非同期 PPP 非同期シリアル回線上の PPP の形式。同時に 1 文字ずつデータ転送します。最も一般的な PPP の形式であるダイアルアップリンクでは、非同期 PPP 通信が使用されています。

非武装ゾーン DMZ を参照してください。

負荷分散 インバウンドまたはアウトバウンドのトラフィックを一連のインタフェースに分散する処理。負荷分散を使用すると、より高いスループットを達成できます。ただし、負荷分散が行われるのは、データが複数の接続を経由して複数の標識に送信される場合だけです。負荷分散には、インバウンドトラフィック用のインバウンド負荷分散とアウトバウンドトラフィック用のアウトバウンド負荷分散の 2 種類があります。

物理インタフェース リンクへのシステムの接続。この接続は、しばしばデバイスドライバおよび NIC として実装されます。NIC によっては、`igb` のように複数の接続点を持つものもあります。

物理機能 PF を参照してください。

分離された VLAN セカンダリ VLAN のタイプ。このタイプの VLAN に関連付けられたポートはプライマリ VLAN とのみ通信でき、ほかのどのセカンダリ VLAN とも通信できません。1 つの分離された VLAN のみをプライマリ VLAN ドメイン内に作成できます。

優先順位ベースのフロー制御 PFC を参照してください。

予期-送信 (expect-send) PPP chat スクリプトや UUCP chat スクリプトで使用されるスクリプト記述形式。chat スクリプトは、リモートピアからの受け取りを期待する *(expect)* テキストまたは手順で始まります。次の行には、リモートピアから期待どおりの文字列を受信した後にローカルホストが送信する *(send)* 応答が記述されます。その後に続く行では、通信確立に必要な手順が正常にネゴシエーションされるまで、ローカルホストとリモートピア間の予期-送信 (expect-send) 手順が繰り返されます。

Advanced Encryption Standard AES を参照してください。

AES Advanced Encryption Standard の略。対称 128 ビットブロックのデータ暗号技術。AES は米国政府の暗号化標準です。

anet リソース Oracle Solaris ゾーンの `zonecfg` コマンドを使用することで構成され、ゾーンのブート時にインスタンス化される、VNIC または IPoIB パーティションデータリンク。VNIC も参照してください。

ARP アドレス解決プロトコル (Address Resolution Protocol)。IP アドレスと Ethernet アドレスの間で動的マッピングを行うプロトコル。ARP は IPv4 ネットワークでのみ使用されます。IPv6 ネットワークはプロトコルアドレスを変換するために近傍検索プロトコルを使用します。詳細は、RFC 826 (`http://tools.ietf.org/html/rfc826`) を参照してください。

BGP Border Gateway Protocol の略。自律システムの間でルーティング情報を交換するプロトコル。詳細は、RFC 4271 (`http://www.ietf.org/rfc/rfc4271.txt`) を参照してください。

Blowfish 32 ビットから 448 ビットまでの可変長鍵の対称ブロックの暗号化アルゴリズム。その作成者である Bruce Schneier 氏は、鍵を頻繁に変更しないアプリケーションに効果的であると述べています。

BOOTP インターネットブートストラッププロトコル (Internet Bootstrap Protocol)。ネットワーククライアントがサーバーから IP アドレスを取得するために使用するプロトコル。

Border Gateway Protocol BGP を参照してください。

CA 認証局 (Certificate Authority)。デジタル証明書を発行する信頼できる第三者機関または企業。デジタル証明書はデジタル署名および公開鍵

/非公開鍵ペアを作成するために使用されます。CA は、一意のデジタル証明書を付与された個人がこの人物であることを保証します。

CBCP コールバック制御プロトコル (Callback Control Protocol)。コールバックセッションのネゴシエーションを行うために使用される、Microsoft 独自の PPP 拡張機能。Solaris PPP 4.0 は、このプロトコルのクライアント (最初の呼び出し元) 側のみをサポートします。

CCP 圧縮制御プロトコル (Compression Control Protocol)。PPP のサブプロトコル。リンク上でのデータ圧縮の使用についてネゴシエーションします。ヘッダー圧縮とは異なり、CCP はリンク上に送信されたパケット内のすべてのデータを圧縮します。

CHAP チャレンジハンドシェーク認証プロトコル (Challenge Handshake Authentication Protocol)。PPP リンク上の呼び出し元の識別情報の検証に使用できる認証プロトコル。CHAP 認証では、「チャレンジ」と「応答」の概念を使用します。呼び出しを受信したシステムが呼び出し側にチャレンジを送信してその識別情報を確認します。

パスワード認証プロトコルも参照してください。

CHAP シークレット 識別目的で使用される ASCII またはバイナリ文字列。PPP リンク上の両ピアにより認識されます。CHAP シークレットはシステムの `/etc/ppp/chap-secrets` ファイル内に平文のまま保存されますが、PPP リンク上には、たとえ暗号化された形であっても、決して送信されることはありません。CHAP プロトコルは、呼び出し元が使用する CHAP シークレットのハッシュと、受け取り側の `/etc/ppp/chap-secrets` ファイルに設定されている呼び出し元の CHAP シークレットエントリのハッシュが一致することを検証します。

chat スクリプト モデムとリモートピアの間の通信リンクを確立する方法を、モデムに指示する手順。PPP プロトコルと UUCP プロトコルは、ともにダイアルアップリンク確立とダイアルバック呼び出しに chat スクリプトを使用します。

CRL 証明書失効リスト (Certificate Revocation List)。CA が無効にした公開鍵証明書のリスト。CRL は、IKE を使用して管理される CRL データベースに格納されます。

CSU チャネルサービスユニット (Channel Service Unit)。専用通信回線へのローカルインタフェースを提供し、その回線を終端する同期通信装置。米国内では、CSU は T1 回線を終端し、DS1 インタフェースまたは DSX インタフェースを提供します。国際的には、電話会社プロバイダが CSU を所有するのが一般的です。

DCB データセンターブリッジング (Data Center Bridging)。ネットワークとストレージのプロトコル間でデータリンクを共有するときなどに、

同じネットワークリンクを共有する複数のトラフィックタイプの帯域幅、相対的な優先順位、およびフロー制御の管理に使用される L2 テクノロジ。

DCBX データセンターブリッジング交換プロトコル (Data Center Bridging Exchange Protocol)。ホスト間の通信でデータセンターブリッジング機能に関する構成情報を交換できるようにするプロトコル。

DefaultFixed NCP ネットワーク構成がインスタンス化されていてもモニターされない、システムの唯一の固定 NCP。

DEPRECATED アドレス IPMP グループ内でデータの発信元アドレスとして使用することのできない IP アドレス。通常、IPMP の検査用 IP アドレスは DEPRECATED です。ただし、任意のアドレスに DEPRECATED のマークを付けて、そのアドレスが発信元アドレスとして使用されることを防止できます。

DES データ暗号化規格 (Data Encryption Standard)。ANSI で ANSI X. 3.92 として標準化された対称鍵 64 ビットのブロックデータ暗号化方法。DES では 56 ビットの鍵を使用します。

DHCP 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)。クライアント/サーバーメカニズムを使用することによって、TCP/IP ネットワーク内のホストの自動ネットワーク構成を可能にするプロトコル。このプロトコルによって、TCP/IP ネットワーク上のホストは IP アドレスを要求し、割り当てられた IP アドレスを取得し、さらに接続先のネットワークに関する情報を検出できます。IPv4 用の DHCP についての詳細は RFC 2131 (http://www.ietf.org/rfc/rfc2131.txt)、IPv6 用の DHCP についての詳細は RFC 3315 (http://www.ietf.org/rfc/rfc3315.txt) を参照してください。

DHCP 一意識別子 DUID を参照してください。

Diffie-Hellman プロトコル セキュアでない通信媒体で、2 人のユーザーが事前の情報がなくても秘密鍵を交換できる、非対称暗号鍵協定プロトコル。非対称暗号化鍵協定は公開鍵の暗号化の基準です。

diffserv モデル IP ネットワークで差別化サービスを実装するための IETF (Internet Engineering Task Force) のアーキテクチャー標準。IP ネットワークでは、Diffserv モデルは、ネットワークトラフィックを分類および管理し、IPQoS を提供するための、シンプルでスケーラブルなメカニズムを提供します。主なモジュールとして、クラシファイア、メーター、マーカー、スケジューラ、およびドロッパがあります。IPQoS では、クラシファイア、メーター、およびマーカーの各モジュールを実装します。詳細は、RFC 2475 (http://www.ietf.org/rfc/rfc2475.txt) を参照してください。

Direct Server Return DSR を参照してください。

DLMP アグリゲーション データリンクマルチパスアグリゲーション (Datalink Multipathing aggregation)。複数のスイッチをサポートし、そのデータリンクへの継続的な接続を提供する、リンクアグリゲーションのタイプ。スイッチに障害が発生すると、アグリゲーションはほかのスイッチを使用して、そのデータリンクへの接続を引き続き提供します。このタイプのリンクアグリゲーションはスイッチ構成を必要としません。DLMP アグリゲーションは 1 つのスイッチ上に作成することもできます。

DMA ダイレクトメモリーアクセス (Direct Memory Access)。一部のデバイスは、CPU の助けを借りずに、メインメモリーなどのデバイスを必要とするデータ転送を行うことができます。このタイプのデータ転送は、ダイレクトメモリーアクセス (DMA) とも呼ばれます。

DMZ 非武装ゾーン (Demilitarized Zone)。組織のプライベートネットワークへの公開アクセスを防止するように設定されている分離されたネットワーク。分離されたネットワークには、Web サーバー、匿名 (anonymous) ftp サーバー、データベースなど、会社が一般に公開するリソースを含めることができます。

DN 識別名 (Distinguished Name)。一般的な文字列を使用して共有情報を表す、標準化された手法。DN は LDAP や X. 509 証明書などのテクノロジで使用されます。

DNS ドメインネームシステム (Domain Name System)。ドメイン名とマシン名をインターネットアドレスなどの企業外部のアドレスにマッピングする場合のネーミングポリシーとメカニズムを提供するサービス。すなわち DNS は、ドメイン名とマシン名をインターネットなどの企業外部のアドレスにマッピングする場合のネーミングポリシーとメカニズムを提供する。詳細は、RFC 1034 (`http://tools.ietf.org/html/rfc1034`) を参照してください。

DOI 解釈ドメイン (Domain Of Interpretation)。データ形式や、ネットワークトラフィック交換タイプ、セキュリティー関連情報の命名規約を定義します。セキュリティー関連情報の例としては、セキュリティーポリシーや、暗号化アルゴリズム、暗号化モードなどがあります。

DR 動的再構成 (Dynamic Reconfiguration)。システムを実行しながらシステムハードウェアを再構成するために使用されるオペレーティングシステムの機能。DR を使用することで、通常のシステムの動作をほとんど、あるいはまったく中断せずに、ハードウェアリソースを追加または交換できます。Oracle の Sun プラットフォームの一部は、DR をサポートしていません。プラットフォームの一部は、NIC など特定のタイプのハードウェアの DR だけをサポートする場合があります。

DS コードポイント DSCP を参照してください。

DSCP DS コードポイント (DS codepoint)。パケットヘッダーの差別化サービス (DS) フィールドに含まれる 6 ビット値。DSCP は、パケットをどのように転送する必要があるかを示します。詳細は、RFC 2474 (https://www.rfc-editor.org/rfc/rfc2474.txt) を参照してください。

DSR Direct Server Return の略。統合ロードバランサが受信リクエストをバックエンドサーバーに分散できるようにするが、サーバーからクライアントへの戻りトラフィックは統合ロードバランサをバイパスさせるモード。

DSU データサービスユニット (Data Service Unit)。専用回線 PPP リンク上で使用する同期通信装置。DSU は通信回線上で使用されるデータフレーミング形式間の変換を行い、標準データ通信インタフェースを提供します。

DUID DHCP 一意識別子 (DHCP Unique Identifier)。DHCPv6 対応システムのクライアントシステムを識別するために使用される識別子。

ECMP 等コストマルチパス (equal-cost multi-path)。等コストの複数のパスに沿ってパケットをルーティングするルーティング技術。転送エンジンはネクストホップによってパスを識別します。パケットを転送するときは、使用するネクストホップ (パス) をルーターが決定する必要があります。詳細は、RFC 2992 (http://tools.ietf.org/html/rfc2992) を参照してください。

ENM 外部ネットワーク修飾子 (External Network Modifier)。リアクティブネットワーク構成の外部にあるが、ネットワーク構成を変更および修正できるアプリケーション用に作成されるプロファイル。ENM には、アプリケーションまたはスクリプト (たとえば、VPN アプリケーション) が NCP および場所プロファイルで指定された構成の外部で独自のネットワーク構成を行う必要があるタイミングを指定する機能があります。

ESP カプセル化セキュリティーペイロード (Encapsulating Security Payload)。IP データグラムに整合性、機密性、リプレー保護を提供する拡張ヘッダー。

ESSID 拡張サービスセット識別子 (Extended Service Set Identifier)。コンピュータやネットワークデバイスがインターネットに接続してアクセスするための識別情報およびアドレスとして機能する、電子マーカーまたは識別子。これは、すべての 802.11 無線ネットワークを識別する名前です。

Ethernet 多数のコンピュータシステムを接続してローカルエリアネットワークを構築するために使用されるシステム。Ethernet は、プロトコルを使用して、情報の受け渡しを制御したり、2 つ以上のシステムによる同時送信を回避したりできます。

etherstub Oracle Solaris ネットワークスタックのデータリンク層 (L2) に構成される仮想 Ethernet スイッチ。システム上のほかの仮想ネットワークや外部ネットワークからも切り離されたプライベート仮想ネットワークを構築するために、物理リンクではなく etherstub 上に VNIC を作成できます。

ETS 拡張伝送選択 (Enhanced Transmission Selection)。NIC 上の帯域幅を DCB 優先順位に基づいてアプリケーションに割り当てる DCB 機能。

EVB エッジ仮想ブリッジング (Edge Virtual Bridging)。ホストが外部スイッチと仮想リンク情報を交換できるようにする L2 テクノロジ。EVB はスイッチにトラフィックの SLA の適用をオフロードします。

EVS エラスティック仮想スイッチ (Elastic Virtual Switch)。Oracle Solaris のソフトウェア仮想スイッチであり、複数のサーバーをつなぐことができるため、エラスティック仮想スイッチに接続された複数のサーバー上の仮想マシン間のネットワーク接続を提供できます。

EVS クライアント エラスティック仮想スイッチを管理する EVS コンポーネント。

EVS コントローラ 複数のノードにまたがるエラスティック仮想スイッチの構成とステータスを保持する EVS コンポーネント。

EVS ノード VNIC がエラスティック仮想スイッチに接続するホスト。

EVS マネージャー EVS コントローラと通信するエンティティーで、L2 ネットワークトポロジと、これらの L2 ネットワークで使用する必要のある IP アドレスを定義します。

FCoE Fibre Channel over Ethernet の略。カプセル化されたファイバチャネルフレームを拡張された Ethernet 上で転送する T11 標準。FCoE は、大規模な配備におけるネットワークコンバージェンスとコスト効果の高いストレージエリアネットワーク (SAN) 拡張を可能にします。

FDT 障害検出時間 (Failure Detection Time)。インタフェースからインターネット層デバイスへのインタフェースまたはパスが動作しなくなっているかどうかを検出するために必要な時間。

Fibre Channel over Ethernet FCoE を参照してください。

FMRI 障害管理リソース識別子 (Fault Management Resource Identifier)。Oracle Solaris の各サービス、ハードウェアリソース、またはソフトウェアパッケージの識別子。パッケージの場合、FMRI には、パッケージパブリッシャー、パッケージ名、およびソフトウェアパッケージのバージョンが含まれています。

GARP VLAN 登録プロトコル GVRP を参照してください。

GLDv3 Generic LAN Driver version 3 の略。GLDv3 フレームワークは、MAC プラグインと、MAC ドライバサービスのルーチンおよび構造体に対する、関数呼び出しベースのインタフェースです。GLDv3 フレームワークは、必要な STREAMS エントリポイントを GLDv3 準拠ドライバに代わって実装し、DLPI との互換性を実現します。

GVRP General Attribute Registration Protocol の略。クライアントシステムで接続されているスイッチに VLAN ID を自動的に登録するために使用されるプロトコル。

HMAC ハッシュベースメッセージ認証符号 (Hash-based Message Authentication Code)。メッセージ認証を行うための鍵付きハッシュ方法。HMAC は、SHA-1 などの繰り返し暗号化のハッシュ関数で、秘密共有鍵と組み合わせて使用される秘密鍵認証アルゴリズムです。HMAC の暗号の強さは、基になるハッシュ関数のプロパティーによって異なります。

IA アイデンティティーアソシエーション (Identity Association)。サーバーとクライアントで関連する一連の IPv6 アドレスの識別、グループ化、および管理に使用される方法。

IAID アイデンティティーアソシエーション識別子 (Identity Association Identifier)。DHCPv6 対応システムのクライアントシステム上のインタフェースを識別するために使用される識別子。

IANA Internet Assigned Numbers Authority の略。登録された IP アドレスを世界中のインターネットレジストリに委託する組織。詳細は、`http://www.internetassignednumbersauthority.org/` を参照してください。

ICMP インターネット制御メッセージプロトコル (Internet Control Message Protocol)。ネットワークでエラーを検出して報告するために使用されるプロトコル。詳細は、RFC 792 (`https://tools.ietf.org/html/rfc792`) および RFC 4443 (`https://tools.ietf.org/html/rfc4443`) を参照してください。

ICMP エコー要求パケット 応答を促すためにインターネット上のシステムに送信されるパケット。そのようなパケットは一般に "ping" パケットと呼ばれ、IP ネットワーク上のホストの到達可能性をテストするために使用されます。

IKE Internet Key Exchange の略。IKE は IPsec セキュリティーアソシエーション (SA) 用の認証された鍵情報の供給を自動化します。詳細は、RFC 2409 (`https://www.rfc-editor.org/rfc/rfc2409.txt`) および RFC 7296 (`https://tools.ietf.org/html/rfc7296`) を参照してください。

ILB Oracle Solaris 統合ロードバランサ (Oracle Solaris Integrated Load Balancer)。システムが使用可能なリソース間でネットワーク処理の負荷を分散できるようにする、L3 および L4 テクノロジ。ILB を使用して、信頼性とスケーラビリティーを向上させたり、ネットワークサービスの応答時間を最小化したりできます。

InfiniBand スイッチ式ファブリックに基づく入出力テクノロジ。この技術により、入出力デバイスとホストとの接続やホスト間の通信で、帯域幅が広く応答時間の短い相互接続が提供されます。InfiniBand は高パフォーマンスのコンピューティングと企業のデータセンターで使用されます。

Integrated Services Digital Network 端末アダプタ ISDN TA を参照してください。

Internet Assigned Numbers Authority IANA を参照してください。

IP サービス品質 IPQoS を参照してください。

IP セキュリティー IPsec を参照してください。

IP ヘッダー インターネットパケットを固有に識別するデータ。ヘッダーには、パケットの送信元と送信先のアドレスが含まれています。ヘッダー内のオプションによって、バイトをさらに追加できます。IPv4 ヘッダーには 20 バイトのデータが含まれ、IPv6 ヘッダーには 40 バイトのデータが含まれます。

IP マルチパス IPMP を参照してください。

IP 内 IP カプセル化 IP パケット内で IP パケットをカプセル化するためのメカニズム。カプセル化を参照してください。

IPCP インターネットプロトコル制御プロトコル (Internet Protocol Control Protocol)。PPP のサブプロトコル。リンク上のピアの IP アドレスについてネゴシエーションします。また、リンクのヘッダー圧縮をネゴシエーションし、ネットワーク層プロトコルを使用可能にします。

IPMP IP マルチパス (IP Multipathing)。システムがネットワークに常にアクセスできるようにする、レイヤー 3 (L3) テクノロジ。IPMP を使用して、複数の IP インタフェースを 1 つの IPMP グループに構成します。

IPMP グループ IP マルチパスグループは、ネットワークの可用性と利用率を向上させるために相互に入れ替え可能なものとしてシステムで扱われる、一連のネットワークインタフェースと一連のデータアドレスで構成されます。IPMP グループは、そのすべての IP インタフェースとデータアドレスも含めて、IPMP インタフェースによって表されます。

IPnet エラスティック仮想スイッチに関連付けられた、IPv4 または IPv6 アドレスのブロック。IPv4 または IPv6 アドレスのブロックはブロックのデフォルトルーターと同じサブネット上に存在し、Oracle Solaris エラスティック仮想スイッチ機能で使用されます。

IPoIB VNIC IB 接続経由での IP パケットの移送を可能にする VNIC のタイプ。この VNIC の作成時にパーティションキーを指定する必要があります。

IPQoS IP サービス品質 (IP Quality of Service)。diffserv モデル標準に加えて、仮想 LAN に対するフローアカウンティングや 802.1D マーカーの実装を行うソフトウェア機能。IPQoS を使用することで、顧客やアプリケーションにさまざまなレベルのネットワークサービスの提供できます。

IPsec IP セキュリティー (IP security)。IP パケットの認証および暗号化によって IP 通信の保護を提供する、セキュリティーアーキテクチャー。

IPv4 インターネットプロトコルのバージョン 4 (Internet Protocol, version 4)。32 ビット アドレス空間をサポートするインターネットプロトコルのバージョン。IPv4 は単に IP と呼ばれることもあります。詳細は、RFC 791 (`http://www.ietf.org/rfc/rfc791.txt`) を参照してください。

IPv4 ブロードキャストアドレス アドレスのホスト部分のビットにすべてゼロ (10.50.0.0) またはすべて 1 (10.50.255.255) が含まれる IPv4 ネットワークアドレス。ローカルネットワーク上のシステムからブロードキャストアドレスに送信されたパケットは、同じネットワーク上のすべてのシステムに配信されます。

IPv6 インターネットプロトコルのバージョン 6 (Internet Protocol, version 6)。128 ビットのアドレス空間をサポートするインターネットプロトコルのバージョン。詳細は、RFC 2460 (http://www.ietf.org/rfc/rfc2460.txt) を参照してください。

IPv6 自動構成 ホストが、サイト接頭辞とローカル MAC アドレスからその IPv6 アドレスを自動的に構成する処理。

IR インターネットレジストリ (Internet Registry)。IP アドレスと自律システム (AS) 番号を含むインターネット番号の登録情報が含まれるレジストリ。

ISAKMP インターネットセキュリティーアソシエーションと鍵管理プロトコル (Internet Security Association and Key Management Protocol)。SA 属性の形式を設定したり、SA のネゴシエーション、変更、および削除を行なったりするための、一般的なフレームワーク。ISAKMP は、IKE 交換を処理するための IETF 標準です。

ISDN TA ISDN 端末アダプタ (Integrated Services Digital Network terminal adaptor)。ISDN 上のダイアルアップ PPP リンクのモデムに似たインタフェースを提供する、信号対応デバイス。標準のモデムとして使用されるときに ISDN TA を構成するには、Solaris PPP 4.0 構成ファイルを使用します。

KMF Oracle Solaris 鍵管理フレームワーク (Key Management Framework)。X.509 証明書と公開鍵/非公開鍵ペアを含む公開鍵オブジェクトを管理するためのツールとプログラミングインタフェースを提供するフレームワーク。また、KMF では、アプリケーションによる X.509 証明書の使用方法を定義したポリシーを管理するためのツールも提供されます。

LACP リンクアグリゲーション制御プロトコル (Link Aggregation Control Protocol)。リンクアグリゲーショングループ内のシステム間でネットワーク構成情報を動的に交換するための IEEE 802.3ad 標準。このプロトコルは、リンクアグリゲーショングループの自動的な構成と保守に役立ちます。

LCP リンク制御プロトコル (Link Control Protocol)。PPP のサブプロトコル。ピア間リンクパラメータの初期セットのネゴシエーションに使用されます。LCP は、リンクされているデバイスの識別情報をチェックし、リンク構成のエラーを検索し、送信の許容可能なパケットサイズを決定します。

LDAP Lightweight Directory Access Protocol の略。IP ネットワーク上のディレクトリ情報の管理に使用されるクライアント/サーバープロトコル。LDAP は、情報の格納、検索、および配布の単一点の管理を可能にします。LDAP は、クライアントとサーバーが LDAP ネームサービスを

使用して互いに通信できるようにします。詳細は、RFC 4511 (https://tools.ietf.org/rfc/rfc4511.txt) を参照してください。

Lightweight Directory Access Protocol — LDAP を参照してください。

LLDP — リンク層検出プロトコル (Link Layer Discovery Protocol)。ネットワークデバイスが IEEE 802 ローカルエリアネットワーク (LAN) 上のほかのネットワークデバイスに機能、識別情報、および現在のステータスを通知できるようにする、リンク層プロトコル。

LRO — ラージレシーブオフロード (large receive offload)。連続した着信パケットを IP レイヤーに配信される前に単一のパケットにマージするテクノロジ。着信パケットは、同じトランスポートプロトコル、ローカルまたはリモートの IP アドレス、およびポート番号を共有する必要があります。この属性セットは 5 タプルとも呼ばれます。

MAC アドレス — メディアアクセス制御アドレス (Media Access Control address)。ネットワークインタフェースに割り当てられた一意のアドレス。MAC アドレスは物理ネットワークセグメント上の通信に使用されます。

Microsoft CHAP — MS-CHAP を参照してください。

MS-CHAP — Microsoft CHAP の略。独自の PPP 用 Microsoft 認証プロトコル。Solaris PPP 4.0 では、クライアントモードとサーバーモードの両方において、このプロトコルの version 1 と 2 をサポートします。

MTU — 最大伝送単位 (Maximum Transmission Unit)。リンク上で送信できる、オクテットで指定されるデータの最大単位のサイズ。

NAT — ネットワークアドレス変換 (Network Address Translation)。あるネットワークで使用されている IP アドレスを、別のネットワークで認識されている異なる IP アドレスに変換すること。必要となる大域 IP アドレスの数を抑えるために使用されます。

NCP — ネットワーク構成プロファイル (Network Configuration Profile)。Oracle Solaris でシステムのネットワーク構成を管理するプロファイル。システム上で一度にアクティブになることができる NCP は 1 つだけです。

NCU — ネットワーク構成ユニット (Network Configuration Unit)。NCP を定義するプロパティーがすべて含まれている、個別の構成オブジェクト。各 NCU は、物理リンクまたはインタフェースを表し、そのリンクまたはインタフェースの構成を定義するプロパティーを含んでいます。

Network Time Protocol (NTP) NTP を参照してください。

NFS ネットワークファイルシステム (Network File System)。ネットワークを介して共有ファイルにリモートからアクセスするために使用されるファイルシステムプロトコル。Oracle Solaris では、NFSv2、NFSv3、NFSv4、および NFSv4.1 バージョンがサポートされます。NFS バージョンの詳細は、それぞれ RFC 1094、RFC 1831、および RFC 5661 を参照してください。

NIC ネットワークインタフェースカード (Network Interface Card)。コンピュータをネットワークに接続するネットワークアダプタカード。NIC によっては、`igb` カードなど複数の物理インタフェースを装備できるものもあります。

NIC リング NIC 上にある受信 (Rx) リングと送信 (Tx) リングはそれぞれ、システムがネットワークパケットの受信と送信を行うために使用するハードウェアリソースです。

NIS ネットワーク情報サービス (Network Information Service)。ネットワーク上のシステムとユーザーに関する重要な情報が収められている分散型ネットワークデータベース。

NTP Network Time Protocol の略。システム時間の設定および維持に使用されるプロトコル。NTP ソフトウェアは、RFC 5905 (`https://tools.ietf.org/html/rfc5905`) で定義されているバージョン 4 標準の完全な実装である、`ntpd` デーモンとして実装されます。

Open Systems Interconnection モデル OSI モデルを参照してください。

Oracle Solaris 鍵管理フレームワーク KMF を参照してください。

Oracle Solaris 統合ロードバランサ ILB を参照してください。

OSI モデル Open Systems Interconnection モデル。国際標準化機構 (ISO) により策定された、ネットワーク上でデータをどのように送信する必要があるかを記述する標準モデル。

PAP パスワード認証プロトコル (Password Authentication Protocol)。PPP リンク上の呼び出し元の識別情報の検証に使用できる認証プロトコル。PAP は平文パスワードを使用し、このパスワードはリンク上に送信さ

れるので、パスワードを端点のシステムの中の 1 つに保存できます。たとえば、呼び出しを受信するシステム上の UNIX `password` データベース内のログインとパスワードエントリを使用して、呼び出し元の識別情報を検証できます。

PCIe Peripheral Component Interconnect Express の略。コンピュータをその周辺機器と接続するシリアル I/O バス。

Perfect Forward Secrecy PFS を参照してください。

Peripheral Component Interconnect Express PCIe を参照してください。

PF 物理機能 (Physical Function)。SR-IOV 仕様に規定された SR-IOV 機能をサポートする PCI 機能。PF は SR-IOV 機能構造を含んでおり、SR-IOV の機能を管理するために使用されます。PF は完全な機能を備えた PCIe 機能であり、他の PCIe デバイスと同様に発見、管理、および操作を行えます。PF は完全な構成リソースを備えているため、PCIe デバイスの構成や制御に使用できます。

PFC 優先順位ベースのフロー制御 (Priority-based Flow Control)。データリンクレベルのフロー制御メカニズム。PFC では、IEEE 802.1p サービスクラス (CoS) 値を含むように標準 PAUSE フレームが拡張されます。PFC では、データリンク上のすべてのトラフィックを停止する代わりに、PFC フレームで有効になっている CoS 値に対してのみ、選択的にトラフィックを一時停止します。

PFS Perfect Forward Secrecy の略。PFS では、データ伝送を保護するために使用される鍵が、追加の鍵を導き出すために使用されることはありません。さらに、データ伝送を保護するために使用される鍵のソースが、追加の鍵を導き出すために使用されることはありません。PFS は IKE の認証された鍵交換に適用されます。

PHB ホップ単位動作 (Per-Hop Behavior)。パケットのトラフィッククラスに割り当てられている、ホップを追跡する際の優先順位。

PKI 公開鍵インフラストラクチャー (Public Key Infrastructure)。インターネットトランザクションに関係する各関係者の有効性を確認および承認する、デジタル署名、CA、ほかの登録機関のシステム。

PPP ポイントツーポイントプロトコル (Point-to-Point Protocol)。ポイントツーポイント媒体上でデータグラムを転送する標準方法を提供するリンク層プロトコル。PPP 構成はピアと呼ばれる 2 台の端点コンピュー

タ、およびピアが通信に使用する電話回線または双方向リンクから構成されます。2 台のピア間のハードウェアおよびソフトウェア接続が *PPP* リンクであると考えられます。

PPP は、PAP、CHAP、LCP、CCP などの複数のサブプロトコルから構成されます。

PPP over Ethernet PPPoE を参照してください。

PPPoE PPP over Ethernet の略。ホストが Ethernet リンクを介して PPP セッションを実行できるようにするプロトコル。PPPoE は通常デジタル加入者回線 (DSL) サービスで使用されます。

Precision Time Protocol PTP を参照してください。

PTP Precision Time Protocol の略。ブロードキャストドメイン内の複数のシステム間でシステムクロックの同期に使用される IEEE プロトコル。PTP ソフトウェアは、IEEE 規格 1588-2008 で定義されている PTP バージョン 2 の実装である、`ptpd` デーモンとして実装されます。

PV NIC ゲストオペレーティングシステムのハイパーバイザ内にあり、ホスト内の物理 NIC と同等のエンティティー。たとえば、カーネルゾーン内の `zvnet`。

PVID ポート VLAN 識別子 (port VLAN identifier)。リンクとの間で送受信されるタグなしパケットとして設定されるデフォルトの VLAN ID。

PVLAN プライベート VLAN (private VLAN)。ネットワークトラフィックを分離するために VLAN を分割したもの。PVLAN は VLAN をパーティション分割し、単一のブロードキャストドメインをより小さなサブドメインにします。

PVLAN セカンダリトランクポート PVLAN トラフィックを複数のスイッチにまたがることができるように中間スイッチで構成されているポート。

RARP 逆アドレス解決プロトコル (Reverse Address Resolution Protocol)。インターネットプロトコル (IP) アドレスと Ethernet アドレスの間で動的にマッピングを行うプロトコル。RARP は MAC アドレスをローカルエリアネットワーク上の IP アドレスに解決するために使用されます。詳細は、RFC 903 (`http://tools.ietf.org/rfc/rfc903.txt`) を参照してください。

RCM Reconfiguration Coordination Manager の略。システムコンポーネントの動的な除去を管理し、システムリソースを順番に登録および解放するために役立つフレームワーク。

Reconfiguration Coordination Manager RCM を参照してください。

RIP ルーティング情報プロトコル (Routing Information Protocol)。IPv4 パケットをルーティングし、LAN 上のすべてのホストのルーティングテーブルを保持する、内部ゲートウェイプロトコル。詳細は、RFC 2453 (`https://tools.ietf.org/html/rfc2453`) を参照してください。

RIPng 次世代のルーティング情報プロトコル (Routing Information Protocol next generation)。IPv6 パケットをルーティングし、LAN 上のすべてのホストのルーティングテーブルを保持する、内部ゲートウェイプロトコル。詳細は、RFC 2080 (`http://tools.ietf.org/rfc/rfc2080.txt`) を参照してください。

RSA デジタル署名と公開鍵暗号化システムを取得するための方法。

SA セキュリティーアソシエーション (Security Association)。1 つのホストから 2 つめのホストにセキュリティー属性を指定するアソシエーション。IKE は IPsec SA 用の認証された鍵情報の供給を自動化します。

SADB セキュリティーアソシエーションデータベース (Security Associations Database)。暗号化鍵と暗号化アルゴリズムを指定する、SA のテーブル。鍵とアルゴリズムは、安全なデータ転送で使用されます。

SCTP ストリーム制御転送プロトコル (Stream Control Transport Protocol)。TCP と似た方法で接続指向の通信を行うトランスポートレイヤープロトコル。さらに、このプロトコルは、接続のエンドポイントの 1 つが複数の IP アドレスをもつことができる複数ホーム機能をサポートします。詳細は、RFC 4960 (`http://tools.ietf.org/html/rfc4960`) を参照してください。

Secure Socket Layer SSL を参照してください。

`sendmail` メール転送エージェントとして機能し、構成ファイルを使用して、別名処理、転送、ネットワークゲートウェイへの自動ルーティング、および柔軟な構成を提供するプログラム。

SHA-1 セキュアハッシュアルゴリズム (Secure Hashing Algorithm)。このアルゴリズムは、長さが 2^{64} 未満の入力に対して演算を行い、メッセージダイジェストを生成します。SHA-1 アルゴリズムは DSA に入力されます。

SHA-2 ブロックサイズが異なるハッシュアルゴリズムのセット。たとえば、SHA-256 や SHA-512。

SMB サーバーメッセージブロック (Server Message Block)。クライアントがネットワーク上のサーバーのファイルにアクセスして、サービスを要求できるようにするプロトコル。

SMF サービス管理機能 (Service Management Facility)。アプリケーション間またはサービス間の関係を定義して、依存するサービスを必要なときに自動的に再起動できるようにするための機能。

smurf 攻撃 リモートロケーションから IP ブロードキャストアドレスまたは複数のブロードキャストアドレスに向けられた ICMP エコー要求パケットを使用して、深刻なネットワークの輻輳や中断を引き起こすプロセス。

SNMP SNMP を参照してください。

SNMP Simple Network Management Protocol の略。IP ネットワークに接続されているデバイスを照会、モニター、および管理するための一般的な方法を提供するプロトコル。

SPD セキュリティーポリシーデータベース (Security Policy Database)。IPsec でパケットにどのレベルの保護を適用するかを指定するデータベース。SPD は、IP トラフィックをフィルタして、パケットの破棄、ネットワーク上での送信、IPsec での保護が必要かどうかを決めます。

SPI セキュリティーパラメータインデックス (Security Parameter Index)。受信側が受信したパケットを復号化するために使用する、SADB 内の行を特定する整数値。

SR-IOV シングルルート I/O 仮想化 (Single Root I/O Virtualization)。仮想マシン間での Peripheral Component Interconnect Express (PCIe) デバイスの効率的な共有を可能にし、ハードウェアに実装される標準。SR-IOV 仕様により、仮想マシンを I/O デバイスに直接接続できます。

SSL Secure Sockets Layer の略。HTTP や FTP のようなプロトコルで使用される、セキュアな低レベル暗号化の形態。SSL プロトコルには、サーバー認証のプロビジョニング、送信中のデータの暗号化、およびオプションのクライアント認証が含まれます。

SSL カーネルプロキシ 構成可能なプロキシをカーネルで実行して、Secure Sockets Layer (SSL) によって保護された Web サーバー通信を高速化します。SSL カーネルプロキシは KSSL とも呼ばれます。

STP スパニングツリープロトコル (Spanning Tree Protocol)。サブネットが使用不可になるネットワークループを回避するために、ブリッジネットワークで使用されるデフォルトのプロトコル。

TFTP Trivial File Transfer Protocol の略。ネットワーク構成サーバーとネットワーククライアントの間でファイルを転送するために使用されるファイル転送プロトコル。TFTP は、一般に、ローカルネットワーク内のシステム間での構成またはブートファイルの自動転送に使用されます。詳細は、RFC 1350 (http://www.ietf.org/rfc/rfc1350.txt) を参照してください。

Transparent Interconnection of Lots of Links TRILL を参照してください。

TRILL Transparent Interconnection of Lots of Links の略。リンクを無効にせずにネットワークループを回避するために、ブリッジネットワークで使用されるプロトコル。TRILL はネットワーク内の TRILL ノードごとに最短パス情報を計算し、その情報を使用して個々の宛先にパケットを転送します。TRILL は、宛先への複数のパス間のトラフィックを負荷分散するために役立ちます。

Triple-Data Encryption Standard 3DES を参照してください。

Trivial File Transfer Protocol TFTP を参照してください。

UDP ユーザーデータグラムプロトコル (User Datagram Protocol)。コンピュータが特殊な送信チャネルやデータパスを設定せずに IP ネットワーク上のほかのコンピュータにデータグラムを送信するために使用するプロトコル。詳細は、RFC 768 (http://www.ietf.org/rfc/rfc768.txt) を参照してください。

Uniform Resource Indicator URI を参照してください。

Uniform Resource Locator URL を参照してください。

UNIX-to-UNIX Copy Program UUCP を参照してください。

URI Uniform Resource Indicator の略。インターネットやプライベートイントラネット上のリソースを識別するアドレス指定技術。

URL Uniform Resource Locator の略。インターネットやプライベートイントラネット上のリソースを識別する文字列。

UUCP UNIX-to-UNIX Copy Program の略。コンピュータ間で相互にファイルの転送とメールの交換を行えるプログラム。また、UUCP を使用して Usenet のような大規模なネットワークにコンピュータを接続することもできます。

VDP VSI Discovery and Configuration Protocol の略。VSI (Virtual Switch Interface) に関する情報を交換するために EVB で使用されるプロトコル。

VF 仮想機能 (Virtual Function)。物理機能に関連付けられた SR-IOV 機能。VF は軽量な PCIe 機能であり、物理機能やその PF に関連付けられたほかの VF と、1 つ以上の物理リソースを共有します。VF が持つことを許可されている構成リソースは、自身の動作に対するものだけです。

VLAN 仮想ローカルエリアネットワーク (Virtual Local Area Network)。ローカルエリアネットワークをプロトコルスタックのデータリンク層で分割したもの。

VLAN デバイス 仮想 LAN デバイス (Virtual LAN device)。IP プロトコルスタックの Ethernet (データリンク) レベルでトラフィック転送を行うネットワークインタフェース。

VNI 仮想ネットワーク識別子 (Virtual Network Identifier)。VXLAN は VXLAN セグメント ID (VNI とも呼ばれます) を使用して識別されます。すべての VXLAN データリンクは VNI に関連付けられています。

VNIC 仮想ネットワークインタフェースカード (Virtual Network Interface Card)。構成されている場合は物理 NIC と同様に動作する L2 エンティティー、つまり仮想ネットワークデバイス。複数のゾーンまたは仮想マシン (VM) の間で共有したり、エラスティック仮想スイッチに VNIC を接続するには、ベースとなるデータリンク上に VNIC を構成します。

VPN 仮想プライベートネットワーク (Virtual Private Network)。インターネットのような公共ネットワーク内でトンネルを利用する、単独の、セキュアで論理的なネットワーク。

VRID 仮想ルーター ID (Virtual Router ID)。特定のネットワークセグメント上の仮想ルーターを識別するために使用される一意の番号。VRID は LAN 内の仮想ルーターを識別します。

VRIP 仮想 IP アドレス (Virtual IP address)。VRID に関連付けられる IP アドレス。ほかのホストはそこからネットワークサービスを取得できま

	す。VRIP は、VRID に属する VRRP インスタンスによって管理されます。
VRRP	仮想ルーター冗長プロトコル (Virtual Router Redundancy Protocol)。ルーターやロードバランサに使用されるものなどの、IP アドレスの高可用性を提供するプロトコル。詳細は、RFC 5798 (https://tools.ietf.org/html/rfc5798) を参照してください。
VSI	仮想ステーションインスタンス (Virtual Station Instance)。VSI は、ステーション上に構成されている VNIC を指します。
VSI Discovery and Configuration Protocol	VDP を参照してください。
VXLAN	仮想拡張可能ローカルエリアネットワーク (Virtual eXtensible Local Area Network)。IP (L3) ネットワークの最上位にデータリンク (L2) ネットワークをオーバーレイすることによって機能する、L2 および L3 テクノロジ。VXLAN は VLAN を使用する際に課せられる 4K の制限に対処します。通常、VXLAN は、複数の仮想ネットワークを分離するためにクラウドインフラストラクチャーで使用されます。
VXLAN セグメント ID	VNI も参照してください。
WAP	Wireless Application Protocol の略。モバイル無線ネットワーク上の情報にアクセスするための標準プロトコル。
WEP 鍵	Wired Equivalent Privacy 鍵 (Wired Equivalent Privacy key)。セキュアな Wi-Fi ネットワークとの接続を確立する鍵。
Wired Equivalent Privacy 鍵	WEP 鍵を参照してください。
Wireless Application Protocol	WAP を参照してください。