

パフォーマンス管理：：ベスト プラクティスの ホワイト ペーパー

目次

[概要](#)

[背景説明](#)

[重要な成功要因](#)

[パフォーマンス管理のインジケータ](#)

[パフォーマンス管理のプロセス フロー](#)

[ネットワーク管理の運用コンセプトの作成](#)

[パフォーマンスの測定](#)

[予防的な障害分析の実行](#)

[パフォーマンス管理のインジケータ](#)

[ネットワーク管理のビジネス目標の文書化](#)

[サービス レベル契約の文書化](#)

[ベースラインのための変数のリストの作成](#)

[ベースラインとトレンド分析のレビュー](#)

[What-if 分析の方法論の文書化](#)

[ネットワーク パフォーマンスを向上させるために使用する方法論の文書化](#)

[要約](#)

[関連情報](#)

概要

パフォーマンス管理には、ネットワーク サービスの応答時間の最適化および個々のネットワーク サービスやネットワーク サービス全体の一貫性と品質の管理があります。最も重要なサービスは、ユーザやアプリケーションの応答時間を測定する必要性です。ほとんどのユーザにとって、応答時間がパフォーマンスにおける重要な成功要因となります。この要素により、お客様のユーザとアプリケーション管理者の両者が、ネットワークの成功を認識できます。

背景説明

キャパシティ計画は、将来見込まれるネットワーク リソース要件を判断して、ビジネス クリティカルなアプリケーションに対するパフォーマンスやアベイラビリティの影響を回避するためのプロセスです。キャパシティ計画の分野では、ネットワークのベースライン（CPU、メモリ、バッファ、入出力オクテットなど）応答時間に影響を与える可能性があります。そのため、パフォーマンスの問題は、キャパシティに関連していることが多いことに注意してください。ネットワークでは、これは一般的に、帯域幅とネットワーク上に送信される前にキューで待機する必要があるデータを指します。音声アプリケーションでは、この待機時間はほぼ確実にユーザへの影響があります。これは、遅延やジッタなどの要素が音声コールの品質に影響を与えるためです。

パフォーマンス管理を複雑にしているもう1つの大きな問題は、大企業やサービスプロバイダーのネットワークの双方にとってネットワークの高いアベイラビリティが不可欠となっているにもかかわらず、長期的には高いコストが発生する（多くの場合は予期しないほど）リスクを抱えながら短期的な収益を追求する傾向があることです。ネットワーク管理者とプロジェクトの実装担当者は、各予算周期ごとに、パフォーマンスと迅速な実装との間にバランスを見いだすというジレンマに直面します。さらに、ネットワーク管理者は、短い市場投入の時期に合わせるための迅速な製品開発、複雑な技術、ビジネスの統合、競合する市場、予定外のダウンタイム、専門技術の欠如、そして頻繁にツールが不十分であるなどの困難に直面します。

これらの問題の観点から、ネットワーク管理のフレームワークにパフォーマンスはどのように適合するのでしょうか。理想的なネットワーク管理システムの主な機能は、ネットワークの運用に関する機能を最適化することです。これをネットワーク管理の最終的な目標として受け入れたならば、ネットワーク管理の焦点は最高のパフォーマンスでネットワークの動作を維持することになります。

理想的なネットワーク管理システムは、基本的に次のような機能を備えています。

- パフォーマンスが低下しそうなことをオペレータに通知する。
- パフォーマンスの低下や障害の発生時には、容易な代替ルートや回避策を提示する。
- パフォーマンスの低下や障害の原因を特定するためのツールを提供する。
- ネットワークの復元力と耐久性を実現するための中核として機能する。
- パフォーマンスについてリアルタイムで報告する。

この理想的なシステムについての定義に基づけば、パフォーマンス管理がネットワーク管理に不可欠になります。パフォーマンス管理に関する重要な課題を次に示します。

- ユーザのパフォーマンス
- アプリケーションのパフォーマンス
- キャパシティプランニング
- 予防的な障害管理

音声やビデオなどの新しいアプリケーションを使用に際しては、パフォーマンスが成功のための重要な要素であり、一定したパフォーマンスが達成できないときには、そのサービスは低品質で役に立たないという評価に繋がってしまうことに注意することが大切です。また別のケースでは、アプリケーションの断続的なタイムアウトでパフォーマンスが安定しないために生産性やお客様満足度が低下するという現象にユーザが悩まされている場合があります。

このドキュメントでは、成功のための重要な要素、主要なパフォーマンスインジケータ、パフォーマンス管理のための高レベルのプロセスマップなど、パフォーマンス管理の最も重要な課題について詳しく説明します。また、アベイラビリティ、応答時間、精度、利用率、キャパシティ計画のコンセプトについても取り上げ、パフォーマンス管理と理想的なネットワーク管理システムにおける予防的な障害分析の役割についても簡単に説明します。

重要な成功要因

重要な成功要因では、ベストプラクティスを実装するための要件が明確にされます。重要な成功要因として認められるには、そのプロセスや手順によってアベイラビリティが向上するか、あるいはそのプロセスや手順を活用しないとアベイラビリティが低下することが必要条件となります。また、重要な成功要因は測定できる必要があり、これによって組織は成功の程度を判断できません。

注: [詳細については、" Performance Managementのインジケータ](#)を参照してください。

パフォーマンス管理に関する重要な成功要因は次のとおりです。

- ネットワークとアプリケーションのデータの両方に対するベースラインを収集する。
- 使用しているネットワークやアプリケーションに対して what-if 分析を行う。
- キャパシティの問題に対して例外報告を行う。
- 提示されているかまたは潜在的なあらゆるネットワーク管理サービスに対するネットワーク管理のオーバーヘッドを判断する。
- キャパシティ情報を分析する。
- ネットワークとアプリケーション両方に対するキャパシティ情報や、ベースラインおよび例外を定期的にレビューする。
- アップグレードやチューニングの手順を定めて、対処的および長期的なキャパシティの問題に対応する。

パフォーマンス管理のインジケータ

パフォーマンス インジケータは、重要な成功要因を測定するための仕組みを提供します。パフォーマンス計画に対するパフォーマンス インジケータには、次のものがあります。

- ネットワーク管理のビジネス目標を文書化する。これはネットワーク管理を運用するための公式なコンセプト、あるいは必要な機能や目標に関する非公式な要件となることがあります。
- 詳細な測定可能サービス レベル目標を設定する。
- サービス レベル契約を図やグラフを添えて文書化し、これらの契約への適合の可否を経時的に示します。
- ポーリングの間隔、発生するネットワーク管理のオーバーヘッド、適切なトリガーのしきい値、変数をトラップのトリガーとして使用できるかどうか、各変数に使用するトレンド分析など、ベースラインとしての変数のリストを作ります。
- 定期的に会議を開き、ベースラインとトレンドの分析をレビューします。
- what-if 分析の方法論を文書化します。これには、適用できる場合はモデリングと検証が含まれます。
- しきい値を超過した場合には、ネットワーク リソースを増やすための方法論を文書化します。文書化する項目には、WAN の帯域幅を増やすために必要なタイム ラインやコスト テーブルがあります。

パフォーマンス管理のプロセス フロー

パフォーマンス管理の高度なプロセス フローのステップは次のとおりです。

1. [ネットワーク管理の運用コンセプトの作成](#)[必要な機能の定義](#)： [サービス、スケーラビリティ、アベイラビリティの目標](#)[アベイラビリティとネットワーク管理の目標の定義](#)[パフォーマンスの SLA とメトリックの定義](#)[SNR の定義](#)
2. [パフォーマンスの測定](#)[ネットワークのベースライン データの収集](#)[アベイラビリティの測定](#)[応答時間の測定](#)[精度を測定します](#)[使用率の測定](#)[キャパシティ計画](#)
3. [予防的な障害分析の実行](#)[予防的な障害管理にしきい値を使用する](#)[ネットワーク管理の実装](#)[ネットワークの運用メトリック](#)

ネットワーク管理の運用コンセプトの作成

ネットワークについての詳細なパフォーマンスとキャパシティの変数を定義する前に、組織でのネットワーク管理の運用コンセプト全体を見ておく必要があります。全体のコンセプトを定義することは、使用しているネットワークに必要な機能を正確に定義するためのビジネス基盤を提供します。ネットワーク管理の運用コンセプトの作成に失敗すると、目標を見失ったり、顧客の要求によって目標が常に変化してしまいます。

通常は、ネットワーク管理プログラムのシステム定義フェーズの最初のステップとして、ネットワーク管理の運用コンセプトを確立します。この目的は、必要とされるシステムの特徴の全体像を、運用の観点から記述することです。このドキュメントを使用して、ネットワークの運用、エンジニアリング、設計、他のビジネス単位、およびエンドユーザなどの全体的なビジネス（数量化できない）目標を組み合わせます。このドキュメントの焦点は、ネットワーク管理と運用についての長期的な運用計画アクティビティを構築することです。また、サービスレベル契約など、この後に続く定義文書を作成するガイドラインにもなります。この一連の初期定義は、管理特有のネットワーク問題に限定して絞り込みすぎないようにして、組織全体に重要度を主張できる項目で、管理する必要のあるコストにも関連するようにします。目標には次のものがあります。

- ネットワーク インフラストラクチャを効率的に使用するために不可欠な特性を識別する。
- ネットワークをサポートするサービスやアプリケーションを識別する。
- エンドツーエンドのサービス管理を開始する。
- サービス全体を向上させるパフォーマンス ベースのメトリックを開始する。
- パフォーマンス管理情報を収集し、配布する。
- ユーザからのフィードバックでネットワークの戦略的な評価を行う。

別の言い方をすれば、ネットワーク管理の運用コンセプトでは、組織全体の目標や、その目標を達成するための方針に焦点を当てる必要があります。主な構成要素としては、任務の高度なレベルでの定義、任務の目的、システムの目標、組織の関与、および全体の運用方針があります。

ネットワーク管理者は、一貫性を欠くことが多いユーザからのパフォーマンスへの期待を取りまとめるという立場にあります。たとえば、ネットワークに対する主要要件が、大きなファイルのある場所から別の場所に転送することである場合は、高いスループットと対話式のユーザへの応答時間が短くなることに重点を置きたくなります。しかし、さまざまな問題を考慮しないまま、パフォーマンスに対する観点を限定しないよう注意してください。たとえば、ネットワークをテストするときには、利用されている負荷レベルに注目します。よくあることですが、負荷が非常に小さなパケットに基づいていながら、スループットは非常に大きなパケットに基づいていることがあります。これらのパフォーマンステストから非常によい結果を得られたとしても、ネットワークによっては、トラフィックの負荷がパフォーマンスの実際の現象を表していない場合があります。使用しているネットワークのパフォーマンスを考えられる限りのワークロードで調査し、そのパフォーマンスについて文書化します。

また、多くのネットワーク管理組織において、デバイスの障害を技術者に通知するために、効率的なアラーム技術が使用されています。しかし、エンドツーエンドのアプリケーションのパフォーマンスを評価するプロセスを定義および実装することは、これよりも遥かに困難です。したがって、Network Operations Center (NOC; ネットワーク オペレーション センター) がダウンしたルータやスイッチに迅速に対応する一方で、ネットワークのパフォーマンスを徐々に悪化させたり、ユーザの使用感に影響を与えたりするようなネットワークの状態が気づかれぬまま、実際に使用感が悪くなるまで容易に進行する可能性があります。しかし難しいとはいえ、この2番目のプロセスは、ビジネス組織とネットワーク管理の双方に非常に大きな利点をもたらします。

最後に、ネットワーク パフォーマンスに対して非現実的な期待を抱かないようにします。非現実的な期待は通常はネットワーク プロトコルやアプリケーションの詳細を誘導すると作成されます。ネットワーク障害が原因でパフォーマンスが悪いのではなく、アプリケーションの設計が悪いことが原因になる場合もよくあります。アプリケーションのパフォーマンスを文書化および測定する唯一の方法は、アプリケーションをインストールする前にネットワーク パフォーマンスのベ

ースラインを記録しておくことです。

必要な機能の定義： サービス、スケーラビリティ、アベイラビリティの目標

Performance Management、継続的なキャパシティプランニング、ネットワーク設計の最初に必要な機能やサービスを定義することです。このステップでは、アプリケーション、基本的なトラフィックフロー、ユーザとサイトの数、および必要なネットワークサービスについて理解することが必要です。この情報を最初に使用するのは、組織の目標に対するアプリケーションの重要性を判断するときです。また、これらの情報は、論理設計での使用に関するナレッジベースを作成し、帯域幅、インターフェイス、接続性、設定、および物理デバイスなどの要件を理解する上で役立ちます。この最初のステップによって、ネットワーク設計者がネットワークのモデルを作成できるようになります。

ソリューションのスケーラビリティに関する目標を設定すると、ネットワークの設計に将来の拡張要件を盛り込むことができます。また、予測どおりにネットワークが拡張する限り、提案された設計においてリソースの制約が発生しないことを確約できます。リソースの制約には次のものがあります。

- 全体のトラフィック
- ボリューム
- 方路数
- バーチャルサーキットの数
- ネイバーの数
- ブロードキャストドメイン
- デバイスのスループット
- メディアのキャパシティ

ネットワークの設計者は、必要な設計寿命、予測される拡張範囲またはサイト（設計寿命を通じての予測が必要）、新規ユーザの数、および予測されるトラフィック量または変化について決定する必要があります。これによって、提案されたソリューションが、設計の計画されている期間内での拡張要件を満たすようにすることができます。

ソリューションのスケーラビリティを調査していないと、事後対応型の大きな設計変更を迫られる可能性があります。この階層設計変更により、メディアのアップグレード、ハードウェアのアップグレードを含めることができます。大きなハードウェアの購入に非常に厳密な予算サイクルを必要とする組織では、こうした変更が全体の成功に対する大きな阻害要因になることがあります。アベイラビリティの面では、ネットワークが予期しないリソースの限界に遭遇して、利用不可能な期間が生じ、事後対応的な手段をとらざるを得ない場合もあります。

相互運用性と相互運用性テストは、新規ソリューションの導入を成功させるうえで非常に重要です。相互運用性の意味には、異なるハードウェアベンダーだけでなく、ネットワークの実装中または実装後に接続しなければならない、異なるトポロジまたはソリューションが含まれます。相互運用性の問題には、プロトコルスタックからルーティングに至るハードウェアシグナリングや、トランスポートの問題などがあります。相互運用性の問題は、ネットワークソリューションの移行前、移行中、移行後に発生する可能性があります。相互運用性計画には、異なるデバイス間の接続性や、移行中に発生する可能性のあるトポロジの問題を含める必要があります。

ソリューションの比較とは、他のソリューションでの要件の実現方法に対して、考えられるさまざまな設計を比較していくことです。これにより、計画中のソリューションが特定の環境に最も適合していることが確認され、設計プロセスが個人的な先入観によって推進されることがなくなります。比較には、コスト、復元力、アベイラビリティ、リスク、相互運用性、管理性、スケーラビリティ、およびパフォーマンスなどのさまざまな要素が含まれます。これらの要素はすべて

、設計が実装された後、ネットワーク全体のアベイラビリティに大きな影響を及ぼします。また、メディア、階層、冗長性、ルーティングプロトコル、および同様の機能の能力についても比較できます。X 軸を要素、Y 軸を考えられるソリューションとする表を作成して、ソリューションの比較結果をまとめます。また、ラボ環境でソリューションを詳細に比較すれば、さまざまな比較要素について新規ソリューションと新機能を客観的に調査できます。

ネットワーク管理の運用コンセプトの一環として、ネットワークとサポートされているサービスの目標を、すべてのユーザが理解できるように定義することは不可欠です。運用コンセプトの文書化後のアクティビティは、このドキュメントの品質に大きく影響されます。

これらは標準パフォーマンス目標です:

- 応答所要時間
- 使用率の向上
- スループット
- キャパシティ (最大スループット比率)

これらの計測結果は、単純な LAN の場合は大したものではない場合もありますが、スイッチドキャンパス ネットワークやマルチベンダーによる企業ネットワークでは非常に複雑になる場合があります。よく考えられた運用計画のコンセプトを採用すれば、それぞれのパフォーマンスの目標が測定可能な方法で定義されます。たとえば、アプリケーション「x」に対する応答時間を、業務時間内のピーク時で 500 ミリ秒以下とします。これによって、変数、その測定方法、およびネットワーク管理アプリケーションで焦点を当てる 1 日のうちの時間帯を判別するための情報が定義されます。

アベイラビリティとネットワーク管理の目標の定義

アベイラビリティの目標では、ネットワーク サービスについてのサービス レベルまたはサービス レベルの要件を定義します。これによって、ソリューションが末端のアベイラビリティ要件を満たすようにすることができます。特定の組織に対して異なるサービス クラスを定義し、アベイラビリティ要件に対応する各クラスのネットワーク要件を詳述します。また、ネットワークの領域ごとに異なるレベルのアベイラビリティが必要となる場合があります。アベイラビリティの目標を高く設定すると、強化された冗長性とサポート手順が必要になる可能性があります。特定のネットワーク サービスに対してアベイラビリティの目標を定義し、そのアベイラビリティを測定することにより、目標の SLA を達成するために必要なコンポーネントとサービス レベルを把握できます。

全体的な Network Management は制御機能が備わっていないことを確認するために Manageability の目標を定義します。Manageability の目標を設定するには、構成のサポート プロセスおよび関連 Network Management ツールを理解します。管理性の目標には、考えられる相違点や新規要件との関連の中で、新規ソリューションが既存のサポートおよびツール モデルにどのように適合するかについての知識が含まれます。新規ソリューションをサポートする能力は、展開を成功させ、アベイラビリティの目標を満たすために最も重要であるため、このことはネットワークのアベイラビリティには不可欠です。

管理性の目標においては、想定されるネットワークのサポートに必要なすべての重要な MIB またはネットワーク ツールに関する情報、新しいネットワーク サービスのサポートに必要なトレーニング、新しいサービスや他のサポート要件のための要員計画モデルを明確にする必要があります。この情報が導入の前に明確になっておらず、新しいネットワーク設計をサポートするために割り当てるリソースが足りず、全体のアベイラビリティを満たせないこともよくあります。

パフォーマンスの SLA とメトリックの定義

パフォーマンスの SLA とメトリックは、新しいネットワーク ソリューションのパフォーマンスを定義および測定して、パフォーマンス要件を満たすのに役立ちます。提案されたソリューションのパフォーマンスは、パフォーマンス監視ツールを使用して測定したり、提案されているネットワーク インフラストラクチャ上で単に ping を実行することで測定したりする場合があります。パフォーマンス SLA には、予想されるトラフィック量の平均、トラフィック量のピーク、平均応答時間、および許容される最大の応答時間を含める必要があります。その後、この情報はソリューションの検証セクションで使用され、最終的にはネットワークに必要なパフォーマンスとアベイラビリティの決定に役立ちます。

[SNR の定義](#)

ネットワーク設計の重要な面は、ユーザや顧客に対するサービスを定義することです。企業はこれらをサービス レベル契約と呼び、サービス プロバイダーはサービス レベル管理と呼びます。サービス レベル管理には通常、問題のタイプと重大度の定義や、ヘルプデスクの責務（報告経路、各層のサポート レベルでの報告までの時間、問題の処理に取りかかるまでの時間、優先順位に基づいて対象をクローズするまでの時間など）が含まれます。他に検討すべき重要な要素としては、キャパシティ計画の領域で提供されるサービスのタイプ、予防的な障害管理、変更管理通知、しきい値、アップグレード基準、およびハードウェアの交換があります。

組織でサービス レベルが明確に定義されていないと、後日明らかになるリソース要件を向上したり、追加することが困難になります。また、ネットワークのサポートに役立てるために、どのようなリソースを追加すべきか理解することも困難になります。多くの場合、これらのリソースは問題が明らかになってからようやく追加されることになります。

[パフォーマンスの測定](#)

パフォーマンスの管理は、異なるパフォーマンス領域の設定および測定を組み入れた包括的な用語です。このセクションでは、パフォーマンス管理における 6 つのコンセプトについて説明します。

- [ネットワークのベースライン データの収集](#)
- [アベイラビリティの測定](#)
- [応答時間の測定](#)
- [精度を測定します](#)
- [使用率の測定](#)
- [キャパシティ計画](#)

[ネットワークのベースライン データの収集](#)

ほとんどの企業のイントラネットでは、十分な帯域幅が用意されています。しかし、データが適切でなければ、低いアプリケーション パフォーマンスの要因であるネットワークの輻輳を排除できない可能性があります。輻輳やエラーが発生していることの手がかりの 1 つは、パフォーマンスの低下が断続的にあるいは時間帯によって起きていないかどうかを調べることです。この状況の例としては、パフォーマンスが夜間には適切であるが、午前中や業務時間帯のピーク時には非常に遅くなることが挙げられます。

ネットワーク管理の運用コンセプトを定義し、必要な実装データを定義した後は、このデータを時間をかけて収集することが必要です。このタイプの収集作業は、ネットワークのベースラインの基盤となります。

新しいソリューション（アプリケーションや IOS の変更）を導入する前と後に、現在のネットワ

ークのベースラインを確認し、新しいソリューションのための予想値を算定します。このベースラインは、ソリューションがパフォーマンスやアベイラビリティの目標やベンチマークキャパシティを満たしているかどうかの判断に役立ちます。一般的なルータやスイッチのベースラインレポートには、CPU、メモリ、バッファ管理、リンクやメディアの使用率、およびスループットに関連するキャパシティの問題が含まれます。また、運用コンセプトで定義されている目標に基づき、別の種類のベースラインデータを含めることもあります。たとえば、アベイラビリティのベースラインは、ネットワーク環境の安定性やアベイラビリティの向上を示します。新旧の環境でのベースラインを比較して、ソリューション要件を検証します。

もう1つの特別なベースラインは、アプリケーションのネットワーク要件の傾向を調べるときに重要アプリケーションのベースラインです。この情報は、アップグレードサイクルにおいて課金や予算編成の目的に使用することもできます。アプリケーション別の望ましいサービスやサービス品質などに関連するアプリケーションのアベイラビリティの分野でも、アプリケーションのベースラインが重要になることがあります。アプリケーションのベースライン情報は、時間帯ごとにアプリケーションによって使用される帯域幅で主に構成されています。一部のネットワーク管理アプリケーションでは、アプリケーションのパフォーマンスをベースラインとすることができます。トラフィックのタイプ (Telnet または FTP) の詳細を調べることも、計画において重要な場合があります。組織によっては、より重要なリソースが制限されたネットワークの領域を重要な指標として監視します。ネットワークマネージャはネットワークを割り当てるか、計画や調整するには、この情報を使用できます。ネットワークを調整すると、ネットワークサービスまたはアプリケーションのQoSキューまたはパラメータを変更できます。

アベイラビリティの測定

ネットワーク管理者が使用する主要なメトリックの1つにアベイラビリティがあります。アベイラビリティとは、ユーザがネットワークシステムまたはアプリケーションを使用できる時間の指標です。ネットワークの観点から見ると、アベイラビリティはネットワーク上の個々のコンポーネントの信頼性を表します。

たとえば、アベイラビリティを測定するには、マネージドデバイスから集められた統計情報のヘルプデスクの電話を調整できます。しかし、アベイラビリティツールでは、障害のすべての理由を判断することはできません。

ネットワークの冗長性は、アベイラビリティを測定するときに考慮するもう1つの要素です。冗長性がない場合、全体的なネットワークに障害が生じるというよりも、サービスの低下を示します。その結果として応答時間が長くなり、パケットのドロップによってデータの損失が生じます。また、使用率や応答時間など、別のパフォーマンス測定値の分野で影響が生じる場合もあります。

最後に対してSLAにパスすると、予定されている休止を考慮する必要があります。停止の理由としては、移動、追加、変更、設備の休止、あるいは必ずしも報告したくないようなその他のイベントが考えられます。これは困難な業務で、さらに、手作業になる可能性もあります。

応答時間の測定

ネットワークの応答時間とは、トラフィックが2つのポイント間を移動するのに必要な時間のことです。応答時間が通常より長くなることは、ベースラインの比較やしきい値の超過などから分かりますが、これは輻輳の発生がネットワークの障害を示している可能性があります。

応答時間は、顧客のネットワークの使用の最適な指標であり、ネットワークの効率の評価にも役立ちます。応答が低下したことの原因が何であっても、トラフィックが遅延すればユーザはストレスを感じます。分散ネットワーク環境では、次のような多くの要素が応答時間に影響します。

- ネットワークの輻輳
- 宛先への望ましいルートが得られない (あるいはルートがまったくない)
- ネットワーク デバイスの動力不足
- ブロードキャスト ストームなどのネットワーク障害
- ノイズまたは CRC エラー

QoS 関連のキューイングを実行しているネットワークでは、適切なタイプのトラフィックが期待どおりにネットワーク上を通過しているかどうかを確認するために、応答時間の測定が重要になります。たとえば、IP ネットワーク上で音声トラフィックを実装している場合、適切な音声品質を維持するには、音声パケットが一定レートで時間どおりに搬送される必要があります。音声トラフィックとして分類されるトラフィックを生成すると、ユーザが受け取ると同時にトラフィックの応答時間を測定できます。

アプリケーション サーバとネットワーク マネージャ間の論争の解決には応答時間を測定できます。アプリケーションやサーバの速度が低下したときには、ネットワーク管理者が責任を感じるものがよくあります。するとネットワーク管理者は、ネットワークに問題がないことを証明する必要があります。応答時間のデータを収集することは、ネットワークがアプリケーションのトラブルの原因であることを証明または反証できる、明白な手段となります。

可能であればいつでも、ユーザが受け取る応答時間を計測する必要があります。ユーザは応答を、Enter キーを押したときかボタンをクリックしたときから画面に表示されるまでの時間として認識します。この経過時間には、各ネットワーク デバイス、ユーザのワークステーション、および宛先サーバのトラフィックを処理するために必要な時間が含まれます。

残念ながら、このレベルでの計測は、ユーザ数の問題やツールがないことから、ほぼ不可能です。さらに、将来のネットワークの成長を判断したり、ネットワークの問題のトラブルシューティングを行う際には、ユーザやサーバの応答時間を組み込んでもあまり価値はありません。

応答時間の計測には、ネットワーク デバイスやサーバを使用できます。また、ICMP などのツールを使用してトランザクションを計測することもできますが、上位のレイヤが処理しているときにシステムに生じる遅延は考慮されません。このアプローチは、ネットワーク パフォーマンスに関する問題を解決します。

最も簡単なレベルとしては、ネットワーク管理ステーションから、メインフレームのインターフェイスやサービス プロバイダーの接続のエンド ポイント、あるいは主要なユーザの IP アドレスなどのネットワークの重要ポイントに対して ping を送信し、その応答を計測することで応答時間を測定することができます。この方法を使用する上での問題は、ユーザのマシンと宛先マシンとの間でユーザが実感する応答時間が、この測定値では正確に反映されないことです。この方法では、ネットワーク管理ステーションの観点から単に情報を収集し、応答時間を報告しているだけです。また、この方法では、ネットワーク全体のホップごとの応答時間の問題を覆い隠してしまいます。

サーバ中心のポーリングに代わる方法としては、計測用にシミュレートしたい発信元と宛先のより近くにエフォートを分散させる方法があります。分散型ネットワーク管理ポラーを使用し、Cisco IOS Service Assurance Agent (SAA; サービス保証エージェント) 機能を実装します。ルータで SAA をイネーブルにして、ルータと、サーバや他のルータなどの宛先デバイスとの間の応答時間を計測できます。また、TCP ポートまたは UDP ポートを指定し、それによってトラフィックを強制的に、シミュレートしているトラフィックと同じ方法で転送および誘導することもできます。

マルチサービス ネットワーク上で音声、ビデオ、データを統合した状態では、顧客はネットワーク内に QoS のプライオリティ設定を行っています。異なるアプリケーションは別々のプライオリティを与えられているため、単純な ICMP や UDP による測定では応答時間が正しく反映され

ません。また、タグスイッチングを行っている、個々のパケットに含まれているアプリケーションのタイプによって、トラフィックルーティングが変動することがあります。したがって ICMP の ping では、各ルータでその ping がどのように処理されるかによって異なるプライオリティを与えられ、別の効率の劣るルートを与えられることもあります。

この場合、応答時間を測定する唯一の方法は、特定のアプリケーションや対象とするテクノロジーに類似したトラフィックを生成することです。これによって、ネットワークデバイスが、実際のトラフィックに対して行う処理と同様の方法でこのトラフィックを処理するようになります。このレベルの処理は、SAA、またはサードパーティのアプリケーションを意識したプローブを使用して実行できる場合もあります。

精度を測定します

精度とは、エラーが発生していないインターフェイストラフィックの指標であり、一定時間内の全体のパケットの比率に対する成功率を比較するパーセンテージで表すことができます。最初に、エラー率を測定する必要があります。たとえば、100 パケットごとにエラーが 2 つ発生した場合、エラー率は 2 % となり、精度率は 98 % となります。

以前のネットワーク技術では、特に大規模ネットワークの場合には、ある程度のエラーは受容されていました。しかし、高速のネットワークおよび現在の WAN サービスでは、伝送は非常に正確になり、実際に問題がない限りエラー率はゼロに近づいています。一般的なインターフェイスのエラーには、次のような原因があります。

- 仕様外の配線
- 電気的な干渉
- ハードウェアまたはソフトウェアの障害

詳しい調査を開始するには、低い精度率を使用します。ある特定のインターフェイスが問題を呈していて、そのエラーは受容できるものであると判定できる場合もあります。この場合は、このインターフェイスに対する精度のしきい値を調整して、受容できないエラー率を反映させるようにします。受容できないエラー率は、それより前のベースラインで報告されている可能性もあります。

この表に記載されている変数は、精度とエラー率の式で使用されます：

表記	説明
$\Delta \text{ifInErrors}$	snmp ifInErrors オブジェクトを収集する 2 つのポール サイクル間のデルタ (または差異)。これはエラーが発生した着信パケットの数を示します。
$\Delta \text{ifInUcastPkts}$	snmp ifInUcastPkts オブジェクトを収集する 2 つのポール サイクル間のデルタ。これは着信したユニキャスト パケットの数を示します。
$\Delta \text{ifInNUcastPkts}$	snmp ifInNUcastPkts オブジェクトを収集する 2 つのポール サイクル間のデルタ。これは着信した非ユニキャスト パケット (マルチキャストおよびブロードキャスト) の数を示します。

エラー率を計算する式は、通常はパーセンテージで表現します。

$$\text{エラー率} = (\Delta \text{ifInErrors}) * 100$$

($\Delta \text{InUcastPkts} + (\Delta \text{InNUcastPkts})$)

エラー率や精度の式では、発信エラーは対象とされていないことに注意してください。これは、デバイスがエラーを含むパケットを故意にネットワーク上に送信することは決してなく、発信インターフェイスのエラー率が増加することは考えられないためです。したがって、着信トラフィックとエラーだけが、インターフェイスのエラーと精度を測定する対象となります。

精度を計算する式では、100 からエラー率を減算します (この式ではパーセンテージを使用します) 。

精度 = $100 - (\Delta \text{InErrors}) * 100$

($\Delta \text{InUcastPkts} + (\Delta \text{InNUcastPkts})$)

これらの式は、MIB II インターフェイス (RFC 2233) の Generic カウンタでのエラーと精度が反映されます。結果は、送信された全体のパケット数とエラーを比較したパーセンテージで表されます。結果として得られたエラー率を 100 から減算すると、精度率になります。100 % の精度率は、完全であることを意味します。

MIB II の変数はカウンタに保存されるため、2 つのポール サイクルを使用して、この 2 つの値の差を計算します (そのため、この式でデルタが使用されています) 。

使用率の測定

使用率は、特定のリソースの一定時間内の使用度を測定します。この測定値はリソースの使用量を最大運用可能キャパシティに比較したもので、パーセンテージで表されます。使用率の測定値から、ネットワーク全体の輻輳 (または発生する可能性のある輻輳) の状態を判断できます。また、使用率の低いリソースを見つけ出すこともできます。

使用率は、ネットワークのパイプ (リンク) がどの程度いっぱいかを判断するための基本的な指標です。CPU、インターフェイス、キューイング、およびその他のシステムに関連するキャパシティを測定して、ネットワークシステムのリソースが消費されている程度を判断します。

使用率が高いことは、必ずしも悪いことではありません。使用率が低いことは、トラフィックが予期していない場所を流れていることを示している場合もあります。回線が使用過多の状態になると、その影響は大きなものになります。使用過多の状態は、インターフェイスに送られるトラフィックが、処理できる限界以上にキューイングされたときに生じます。リソースの使用率の突然の増加は、障害を示している可能性があります。

インターフェイスが輻輳し始めると、ネットワーク デバイスはパケットをキューに入れるか、廃棄せざるをえません。ルータがパケットを満杯のキューに入れようとする、そのパケットはドロップされます。トラフィックは高速のインターフェイスから低速のインターフェイスへの転送時に廃棄されたパケット結果。これは $Q = u / (1-u)$ という式で表されます。ここで u は使用率、 Q は平均的なキューの深さ (ランダムなトラフィックを仮定) です。したがって、リンク上での使用率のレベルが高いと、平均的なキューの深さも深くなり、パケットのサイズが分かれば、遅延を予測できます。ネットワーク レポート関連のベンダーの中には、より小さな帯域幅を指定して、WAN のコストを削減するように示唆するものもあります。ただし、遅延の影響は 95% の使用率で WAN リンクを実行すると表示されます。さらに、ネットワークを VoIP に移行す

るときには、ネットワーク管理者はポリシーを変更して、WAN リンクを日常的に 50 % 程度の使用率で運用する必要があります。

パケットがドロップされると、上位レイヤのプロトコルから強制的にパケットの再送信が行われます。複数のパケットが廃棄されると、過剰なリトライトラフィックが生じる可能性があります。このような動作によってデバイス上でバックアップが行われて、回線が低下する可能性があります。この問題を解決するには、異なるレベルのしきい値を設定できます。

ネットワーク使用率の測定のうち最も一般的なものは、インターフェイスの使用率です。測定する接続が半二重方式か全二重方式かに応じて、次の表で説明する式を使用します。

表記	説明
Δ ifInOctets	snmp ifInOctets オブジェクトを収集する 2 つのポーリングサイクル間のデルタ (または差異)。これはトラフィックの着信オクテットの数を示します。
Δ ifOutOctets	snmp ifOutOctets オブジェクトを収集する 2 つのポーリングサイクル間のデルタ。これはトラフィックの発信オクテットの数を示します。
ifSpeed	snmp ifSpeed オブジェクトで報告されるインターフェイスのスピード。ifSpeed は、WAN インターフェイスのスピードを正確に反映しない場合があることに注意してください。

コンテンションを検出するために、デバイスによるリスニングが送信前に必要なため、共有 LAN 接続では半二重方式がよく使用されます。WAN 接続がポイントツーポイントであるため、通常は全二重です; 両方のデバイスで送信し、確認するために、同時に受信されるので、接続を共有する 1 つのそのほかのデバイスです。

MIB II の変数はカウンタに保存されるため、2 つのポーリングサイクルを使用して、この 2 つの値の差を計算します (そのため、この式でデルタが使用されています)。

半二重方式のメディアの場合は、インターフェイスの使用率の計算に次の式を使用します。

$$(\Delta\text{ifInOctets} + \Delta\text{ifOutOctets}) * 8 * 100$$

$$(\Delta \text{ 内の秒数}) * \text{ifSpeed}$$

全二重メディア用に、使用率の計算は複雑です。たとえば、全二重 T-1 シリアル接続では、回線速度は 1.544 Mbps です。これは、T-1 インターフェイスでは送受信の両方を 1.544 Mbps で行うことができ、全体としての帯域幅は 3.088 Mbps になることを意味します。

全二重方式接続の場合にインターフェイスの帯域幅を計算するときには、次の式を使用します。ここでは、in と out の値の大きい方を使用して、使用率をパーセンテージで求めます。

$$\text{最大} (\Delta\text{ifInOctets} (\Delta\text{ifOutOctets}) * 8 * 100$$

$$(\Delta \text{ 内の秒数}) * \text{ifSpeed}$$

しかし、この方式では、小さい値の方向の使用率が隠されており、結果の精度はやや低くなります。これよりも正確な方法は、次のように、入力側の使用率と出力側の使用率を別々に計測する方法です。

$$\text{入力側の使用率} = \Delta \text{ifInOctets} * 8 * 100$$

$$(\Delta \text{内の秒数}) * \text{ifSpeed}$$

および

$$\text{出力側の使用率} = \Delta \text{ifOutOctets} * 8 * 100$$

$$(\Delta \text{内の秒数}) * \text{ifSpeed}$$

これらの式はやや単純化されており、特定のプロトコルに関するオーバーヘッドは考慮されていません。より正確な式は、各プロトコルの機能処理を考慮します。たとえば、RFC 1757 ではイーサネットの使用率についての式が定義されており、パケットオーバーヘッドが考慮されています。しかし、高可用性の組織で、ほとんどの場合、LAN インターフェイスと WAN インターフェイスの両方に対してここで示した一般的な式を使用でき、信頼性も問題ないことが判明しています。

キャパシティ計画

前述したように、キャパシティ計画は、将来見込まれるネットワークリソース要件を判断して、ビジネスクリティカルなアプリケーションに対するパフォーマンスや可用性の影響を回避するためのプロセスです。キャパシティおよびパフォーマンスの[Management](#)を参照してください: [このトピック](#)の詳細についてのベストプラクティスホワイトペーパー。

予防的な障害分析の実行

予防的な障害分析は、パフォーマンス管理に不可欠な要素です。予防的な障害分析では、パフォーマンス管理用に収集されたものと同じタイプのデータを使用できます。しかし、予防的な障害管理とパフォーマンス管理では、このデータを取得するタイミングと使用方法が異なります。

予防的な障害管理は、理想的なネットワーク管理システムが設定した目標に到達するための方法です。パフォーマンス管理との関係は、ベースラインを使用することと、使用するデータの変数です。プロアクティブなFault Managementはカスタマイズされたイベント、イベント関連エンジン、チケット問題を統合してベースラインデータの統計分析に結びつけるために、理想的で効果的なNetwork Management SystemのパフォーマンスとChange Management障害が報告されます。

パフォーマンスデータに対するポーリングは、通常は10分、15分、場合によっては30分ごとに行われますが、障害状態の把握はもっと短い時間間隔で行われる必要があります。予防的な障害管理の1つの方法は、RMONアラームとイベントグループを使用することです。外部デバイスからポーリングされないデバイス上にしきい値を設定することで、しきい値をさらに短くすることができます。このドキュメントでは説明しませんが、別の方法として、分散管理システムを使用するという方法があります。分散管理システムでは、Manager of Managers (MoM) でデータを集約してローカルレベルでポーリングを実行できます。

予防的な障害管理にしきい値を使用する

しきい値とは、特定のデータ ストリーム内での対象とするポイントを定義し、しきい値を超えたときにはイベントを発生させるプロセスのことです。ネットワークのパフォーマンスに関するデータを使用して、しきい値を設定します。

しきい値には異なるタイプがいくつかありますが、データのタイプごとに適したしきい値があります。しきい値は数値的なデータにだけ適用可能なため、元のデータは離散数値に変換されます。あるオブジェクトに対するテキスト文字列をすべて理解していなくても、「対象の」文字列を列挙して、その他のすべての文字列を設定値として割り当てることができます。

数値データの2つのクラスのしきい値の2つのクラスがあります: *継続的*、*独立した*。連続的なしきい値は、SNMP カウンタやゲージに記録される連続的あるいは時系列的なデータに適用します。離散しきい値は、列挙型のオブジェクトや離散的な数値データに適用します。ブール型のオブジェクトは、2つの値を持つ列挙型の値で、true または false の値をとります。離散データは、イベント データとも呼ばれます。これはイベントによってある値から別の値への移行が行われるためです。

連続的なしきい値は、時系列のオブジェクトの値が指定したしきい値を越えたときにイベントをトリガーします。オブジェクトの値は、しきい値を上回ると、またはその下に表示されます。また、上昇および下降しきい値を別々に設定することもできます。この技術はヒステリシス メカニズムと呼ばれ、このデータのクラスから生成されるイベントの数を減らすのに役立ちます。ヒステリシス メカニズムは、急速に変化する時系列データのしきい値から生成されるイベントの量を減らします。このメカニズムは、時系列データのあらゆるしきい値の手法と合わせて使用できます。

イベントの量は、オブジェクトの値を追跡するために生成されるアラームを使用して減らすことができます。このアラームには、上昇しきい値と下降しきい値を割り当てます。アラームは、データの値が上昇しきい値を上回ったときにだけトリガーされます。しきい値をいったん越えると、上昇アラームは下降しきい値を下回るまで再度生成されることはありません。同じ機能が上昇しきい値を下回るまで再度下限しきい値の生成を防止します。このメカニズムを使用すると、障害が発生しているかどうかを判断するために必要な情報を減らすことなく、イベントの量を大幅に減らすことができます。

時系列のデータは、カウンタまたはゲージとして表されます。カウンタの場合は、新しいデータのポイントがそれまでのデータのポイントの合計に追加されます。ゲージの場合は、時間間隔内の比率としてデータが表現されます。各データ タイプに該当する継続的なしきい値の2つの形式があります: *絶対値*による連続的しきい値と*相対値*による連続的しきい値。絶対値による連続的しきい値はゲージに対して、相対値による連続的しきい値はカウンタに対して使用します。

ネットワークのしきい値を決定するには、次の手順を実行してください:

1. オブジェクトを選択します。
2. デバイスとインターフェイスを選択します。
3. 各オブジェクトのしきい値を指定または反対する/インターフェイスのタイプ。
4. 各しきい値によって生成されるイベントの重大度を決定します。

やや多いのはどのオブジェクトで特定するために必要です (またはデバイスおよびインターフェイス) に使用するしきい値を。幸いにも、パフォーマンス データのベースラインが収集してあれば、この作業の大部分が処理済みということになります。また、NSA および High Availability Service (HAS) プログラムを使用すると、オブジェクトの設定と範囲の作成に関する推奨事項が提示されます。しかし、この推奨事項を使用している特定のネットワークに合わせる必要があります。

ネットワークに関するパフォーマンス データを収集済みであるときには、HAS プログラムからインターフェイスをカテゴリ別にグループ化することが推奨されます。これによって、各デバイスやデバイス上のオブジェクトごとにしきい値を設定するのではなく、各カテゴリのメディア タイプ別にしきい値を設定すればよいため、設定が簡単になります。たとえば、イーサネット ネットワークと FDDI ネットワークに別々のしきい値を設定するとします。一般的には、イーサネット セグメントを共有するよりも、FDDI ネットワークを 100 % に近い使用率で実行した方がよいと考えられています。しかし、全二重方式のイーサネットでは、コリジョンが生じないため、100 % に近い使用率で実行できます。全二重方式のリンクではコリジョンが見られないため、このリンクのコリジョンに対しては非常に低いしきい値を設定することになると思われます。

また、インターフェイスの重要性および、しきい値のタイプのカテゴリや重要度の組み合わせを考慮することもできます。これらの要素を使用してイベントに優先順位を設定し、その結果、イベントの重要性とネットワークの運用スタッフからの注目度を設定します。

ネットワーク デバイスとインターフェイスのグループ化およびカテゴリ化には、十分に注意を払っても払いすぎるということはありません。グループ化とカテゴリ化が可能になればなるほど、ネットワーク管理プラットフォームに対してしきい値のイベントを統合できるようになります。この情報に対しては、ベースラインを基本的なリソースとして使用します。キャパシティおよびパフォーマンスの [Management](#) "を参照してください: [ベスト プラクティスのホワイト ペーパー](#)" を参照してください。

ネットワーク管理の実装

組織ではネットワーク管理システムを実装して、定義したしきい値を検出し、指定した時間内の値をレポートする必要があります。RMON ネットワーク管理システムを使用すると、しきい値のメッセージを日常的なレビュー、あるいは完全なデータベース ソリューション用にログ ファイルに蓄積できます。これを使用して、あるパラメータについてのしきい値の例外を検索することができます。この情報は、ネットワークの運用スタッフおよび管理者が、継続的に使用できるようにする必要があります。ネットワーク管理の実装には、ソフトウェアやハードウェアのクラッシュまたはトレースバック、インターフェイスの信頼性、CPU、リンクの使用率、キューまたはバッファの失敗、ブロードキャストの量、キャリアの移行、インターフェイスのリセットなどを検出する機能を持たせる必要があります。

ネットワークの運用メトリック

予防的な障害管理の最後の部分は、パフォーマンス管理と重複しますが、ネットワークの運用メトリックです。これらのメトリックによって、障害管理プロセスを向上させるための有効なデータを提供します。少なくとも、これらのメトリックには、ある時間内に発生したすべての問題を分類したものを含める必要があります。この分類には、次のような情報が含まれている必要があります。

- コール優先度ごとに発生した問題の数
- 各優先度におけるクローズまでの最小、最大、平均時間
- 問題のタイプごとの分類 (ハードウェア、ソフトウェア クラッシュ、設定、電源、ユーザによるエラー)
- 各問題のタイプがクローズするまでの時間の内訳
- アベイラビリティ グループまたは SLA ごとのアベイラビリティ
- どのくらいの頻度で SLA 要件に適合、または適合しないか

ヘルプ デスクでは、多くの場合、メトリックやレポートを作成できる機能を備えたレポートイングシステムが備えられています。このデータを収集する別の方法は、アベイラビリティ監視ツールを使用することです。全体のメトリックは、月単位をベースとして入手できるようにします。

ディスカッションに基づいたプロセスの向上を行って、抜けていたサービスレベル契約の要件を改善したり、特定の問題のタイプの処理を向上させたりするようにします。

パフォーマンス管理のインジケータ

パフォーマンス指標は、重要な成功要因を測定するための仕組みを提供します。

ネットワーク管理のビジネス目標の文書化

このドキュメントはネットワーク管理を運用するための公式なコンセプト、あるいは必要な機能や目標に関する非公式な声明となることがあります。ただし、このドキュメントは、成功を評価する際にネットワーク マネージャをまとめました。

このドキュメントは組織におけるネットワーク管理の戦略であり、ネットワークの運用、エンジニアリング、設計、他のビジネス単位、およびエンド ユーザなどから構成される全体的なビジネス (数量化できない) 目標を組み合わせる必要があります。この点に注目することにより、組織におけるネットワーク管理と運用についての長期のアクティビティ計画を行えるようになります。これには、予算編成のプロセスも含まれます。また、ネットワーク管理の目標を達成するために必要な、SLA などのツールや統合パスを入手するためのガイドラインも提供します。

この戦略的なドキュメントは、管理特有のネットワーク問題に限定して絞り込みすぎず、予算問題などの組織全体にとって重要な項目にも重点を置くようにします。次に、例を示します。

- 到達可能な目標を備えた包括的な計画を明確にする。
- ネットワークのサポートに必要な各ビジネス サービスやアプリケーションを明確にする。
- サービスの測定に必要なパフォーマンス ベースのメトリックを明確にする。
- パフォーマンス メトリック データの収集や配布を計画する。
- ネットワークの評価やユーザのフィードバックに必要なサポートを明確にする。
- 測定可能なサービス レベルの目標を詳細に定め、文書化する。

サービス レベル契約の文書化

SLA を正しく文書化するには、サービス レベル目標のメトリックを完全に定義する必要があります。このドキュメントは、ユーザが評価を行う際に使用できるようにします。これによってフィードバックのループができ、ネットワーク管理の組織がサービス契約のレベルを維持するために必要な変数を測定し続けることができます。

SLA は「生きている」ドキュメントといえます。これはビジネス環境とネットワークは本質的に変化し続けるものであるためです。今日、SLA の測定に使用しているものは、明日には旧式のものになる可能性があります。ユーザからのフィードバックのループを設置し、その情報に基づいて行動するだけで、ネットワークの運用において組織に必要とされる高いアベイラビリティの数値を維持できるようになります。

ベースラインのための変数のリストの作成

このリストには、ポーリングの間隔、発生するネットワーク管理のオーバーヘッド、適切なトリガーのしきい値、変数をトラップのトリガーとして使用できるかどうか、各変数に使用するトレンド分析などの項目が含まれます。

これらの変数は、前述したサービス レベルの目標に必要なメトリックに限定されるものではありません。

ません。少なくとも、これらの変数を含める必要があります: ルータの状態、スイッチヘルス、ルーティング情報、技術的データ、使用率と遅延。これらの変数は定期的にポーリングされ、データベースに保存されます。その後、このデータに対してレポートを作成します。これらのレポートは、ネットワーク管理の運用や計画を行うスタッフにとって、次のような面で役に立ちます。

- 事後対処的な問題を履歴データベースを使用して迅速に解決する。
- パフォーマンスレポートやキャパシティ計画はこのタイプのデータを必要とする。
- このレポートに照らし合わせてサービスレベルの目標を測定する。

ベースラインとトレンド分析のレビュー

ネットワーク管理の担当者は、定期的にミーティングを開催して、具体的なレポートを検討する必要があります。このミーティングにより、新たなフィードバックを行うほか、ネットワーク上の潜在的な問題に対する予防的なアプローチを行うことができます。

これらのミーティングには、運用と計画の両方の担当者が加わる必要があります。計画担当者にとっては、ベースラインやトレンドを示すデータを運用面から分析した結果を入手する機会となります。また、このミーティングによって、運用スタッフが計画分析のための「メンバーの一員」となります。

これらのミーティングに加えるもう1つの項目は、サービスレベルの目標です。目標のしきい値に近づいたときは、ネットワーク管理の担当者は目標到達の失敗を回避するための行動を取ることができます。場合によっては、このデータを一部の予算の正当化のために使用することもできます。正しい測定が行われていない場合は、このデータから、サービスレベルの目標がどの時点から破綻し始めたかを示すことができます。また、これらの目標はビジネスサービスとアプリケーションによって明確にされているため、財政基盤に対する正当化を容易に行うことができます。

このようなレビューを2週間ごとに行って、さらに徹底的な分析のためのミーティングを6週間から12週間に1度行います。これらのミーティングにより、短期および長期にわたる問題を解決できるようになります。

What-if 分析の方法論の文書化

what-if 分析には、ソリューションのモデリングと検証が含まれます。新しいソリューション(新しいアプリケーションか Cisco IOS リリースの変更)をネットワークに追加する前に、代替案をいくつか文書化しておく必要があります。

この分析のためのドキュメントには、主な疑問点、方法論、データセット、設定ファイルなどが含まれます。主なポイントは、what-if 分析が、このドキュメントに記述された情報を基にして他のだれかが再実行できる実験であることです。

ネットワークパフォーマンスを向上させるために使用する方法論の文書化

このドキュメントには、特定のタイプのリンクの帯域幅を拡張するために、追加の WAN 帯域幅とコストテーブルが含まれます。この情報によって、組織が帯域幅の拡張にかかる時間と費用を実感できるようになります。公式な文書化を行うことにより、パフォーマンスとキャパシティの専門家が、パフォーマンスが向上した方法とタイミングを特定でき、さらにこの成果にかかったタイムラインやコストを特定できるようになります。

このドキュメントを定期的にレビューして、最新状態を保つようにします。可能であれば、四半期ごとのパフォーマンス レビューの一環として行います。

要約

理想的なネットワーク管理システムの目標を達成するための唯一の方法は、パフォーマンス管理のためのコンポーネントを積極的にシステムに組み込んでいくことです。これには、しきい値を超過したときに通知するシステムと統合されたアベイラビリティや応答時間のメトリックを使用することが含まれます。また、キャパシティ計画のためのベースラインの使用も組み込む必要があります。これはプロビジョニングと例外レポートのための発見的なモデルとリンクします。さらに、組み込み型のモデリングまたはシミュレーション エンジンを含める場合もあります。これによってモデルをリアルタイムで更新し、ソフトウェアシミュレーションによって計画とトラブルシューティングの両方のレベルを提供します。

このようなシステムのほとんどは、実現不可能な理想上のものに思われるかもしれませんが、各コンポーネントは現在使用可能です。さらに、これらのコンポーネントを統合するためのツールも、MicroMuse のようなプログラムがすでに存在しています。この理想が今までになく現実的になった今、私たちはこの理想に到達するための努力を続けて行かなくてはなりません。

関連情報

- [高可用性テクノロジーのホワイト ペーパー](#)
- [キャパシティとパフォーマンス管理 White Paper](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)