JUNIPER NETWORKS | Engineering Simplicity

eGuide

WANのトラブルシューティング：より迅速な解決のためのeGuide

始める

はじめに

WAN（広域ネットワーク）は、重要性を問わずさまざまなビジネストラフィックを伝送する複雑なクラウドです。

大部分のWANは、サービスプロバイダが運用し、基盤となるトランスポートタイプは複数あります。近年は、低コストでWANを構築および補完するために、専用インターネットアクセス（DIA）回線を使用しているプロバイダが増えています。

場合によっては、WANはインターネット回線上にオーバーレイまたはVPNとして完全に構築されています。その場合、トラフィックは、専用線接続を使用するのではなく、ローカルのインターネットブレークアウトとパスを共有します。

WAN（コンポーネントを含む）を監視することは、そこを流れているビジネストラフィックの信頼性、完全性、可用性を保証するうえで非常に重要です。

大部分のWANは、直接または間接的にダイナミックルーティングプロトコルを使用しています。このプロトコルは、基盤となる要素で生じる障害と、パスにおける後続の到達可能性にとって重要です。

障害は必ず起きることではありませんが、発生する可能性は高く、その原因は、デバイスの問題から、輻輳、ケーブルの短絡、ヒューマンエラーまで、ありとあらゆるものにわたります。

自動化の台頭と継続的な抽象化レベルに伴い、サービスを保証する能力を損なうロジックまたはルートを含む漏れに直面することがあります。

本ガイドでは、ネットワークで発生した問題をトラブルシューティングする際の具体的な手順とアプローチをいくつかご紹介します。

ネットワークに問題が発生した場合、サービスを復旧するアプローチはいくつかあります。

その目的は常に同じで、短時間で復旧し、故障の発生を最小限に抑えることです。

お使いのWANでは
リスクをどのように
分散していますか？

リスクをどのように
分類していますか？

障害や停滞を避けられ
ない場合、どのように
対処していますか？

トラブルシューティングのアプローチ

インターネット（IPネットワーク）は「ひと続きのチューブ」と説明されてきましたが、管理対象デバイスと非管理対象デバイス間で行われる一連のセッションやメッセージとして考えると分かりやすいです。

メッセージはステートレスである場合もありますが、セッションには常に「ステート（状態）」という概念が伴います。この両方の種類のトラフィックは、いずれも複数の依存関係を作り、持つことになります。

依存関係はリスクを生みます。

トラブルシューティングでは、調査と探索を実施します。トラブルシューティングの非常に効率的な方法の1つは、二分探索のように、継続的に問題の領域を確保することです。トラブルシューティングでは調査を行いますが、症状、問題の報告、監視では、必ずしも根本的な問題の状態が分かるわけではありません。

エンジニアは多くの場合、具体的な原因を絞り込みつつ、相関を使用してトラブルシューティングする必要があります。目標は、根本原因をできるだけ早く突き止め、問題に優先順位を付けて緩和し、再発**を防止する是正措置に取り組むことです。**

トラブルシューティングには、「トップダウン」または「ボトムアップ」というアプローチが用いられることがありますが、どちらの方法も効率が悪く、無駄な作業が発生し、時間がかかります。「ミドルアウト」というアプローチでは、最初の不明瞭な状況下でも、短時間で答えを出すことができます。

エンジニアまたはシステムが異常を示すトリガーが送信されると、通常、独自の検証または二次検証が必要となります。これは「信ぜよ、されど確認せよ」の実践です。トリガーまたはアラートの送信元が信頼されていたとしても、コストのかかるトラブルシューティングに着手すると、常に疑いが生じるものです。

自動化にはほとんどの検証段階でメリットがあります。たとえば、労力を削減し、その結果、時間が短縮され、オペレーターがより高次かつ複雑な仕事をするための時間を確保することができます。

ユーザーの監視

「測定できないものは管理できない」という格言は今でも当てはまります。ノイズを最小限に抑えるために受信したデータをフィルタリングしながら、アセットとサービスを可視化することが不可欠です。

あらゆることを測定して状態を把握することと、実施可能なアラートに短時間で優先順位をつけることのバランスをとることが大切です。

ユーザーのセッションを利用する

ユーザーは具体的なデータとセッションに関心があります。ユーザーは複雑なデバイスを操作し、一連のアプリケーションを実行しますが、トラブルシューティングは難しい場合があります。問題が発生すると、ユーザーにとってはネットワークが機能していないように見える場合がありますが、技術的な障害の場所を特定することはユーザーの責任ではありません。

ユーザーから障害の不正確な報告を受けることがありますが、それでもユーザーやマシンは問題がどこにあるかを示す指標として非常に役立ちます。ユーザーのセッションは、WANの本当の状態を明らかにするなど、根本原因をすぐに特定するのに役立つ場合があります。

ユーザーのセッションから制御グループを作成すれば、個別または複合したネットワーク問題を特定することができます。これまでは、追跡と計測には大きなコストが必要でした。

従来の手動によるトラブルシューティングがまだ使用されることもありますが、ジュニパーは、今までのように時間がかかり、間違えれば会社の存続にも関わるようなシナリオに対して、優れた診断ツールを開発しました。

今では、WANでの実際のユーザー監視を利用し、自動化された「ボトムアップ」のトラブルシューティングを行うことができます。これにより、WANの問題を診断して分類する時間を短縮し、より迅速なサービスの修復と復旧が可能になります。

ネットワークの監視

問題の原因が分かっているのなら、トラブルシューティングの必要はないはずです。その代わり、関連するコンポーネントまたは要素が望ましくない状態になっていないかを監視します。

ネットワーク全体をより良く観察できるほど、アウトプットからシステムの状態を推測する能力が高まり、より速く細かく問題領域を分割して、答えを見つけることができます。

プロトコル、信号方式、データグラム、パケットは、すべて明確に規定され、ルールに従っている必要があります。しかし、ネットワーク自体は複雑な分散システムです。1台のデバイスの設定によって、他のデバイスの状態が分かるようになっています。

従来のネットワーク監視は、ネットワーク要素の状態を主な監視対象にしていました。これは今でも非常に重要ですが、ユーザーの具体的なセッションデータをAからBに確実に転送できることを証明する必要があります。

つまり、より高度な基数データが必要になり、ユーザーの観点からの可用性だけでなく、パス内到達可能性を確認する負担はまだ運用チームにかかります。

システムが複雑化することで、依存関係や共有状態によって根本原因を簡単に見つけることができないと、今でもトラブルシューティングが必要になるのが現実です。

- システムや人間からのアウトプットは正しいかもしれませんが、バグやバイアスをもたらす可能性がある。
- 収集するデータの量が多すぎると負担が高まる。そのため、注目すべき場所を事前に把握していても、検証が不要になるわけではない。
- 監視は、問題のある既知の状態またはしきい値の測定に役立つが、多くの場合、根本原因を特定するには詳細に調べる必要がある。

一時的に未知の障害を検索するということは、その障害をまだ計測または監視できていないことです。この照会および検索はトラブルシューティングに不可欠です。

複雑化するにつれ、トラフィックに影響する変数の数が何倍にも増える。

ネットワークが正常に機能していることを実証することが重要な業務になる。

WANのトラブルシューティング

WANは、数々の種類のトポロジー、プロトコル、ベンダー、要素から成ります。

以下は、作業を促進するのに役立つ一般的なガイダンスの概要やポイントです。目標は、独自にカスタマイズしたトラブルシューティングのプロセスを運用可能にし、それをモデル化し、文書化して、より良い知識の共有と迅速な自動化を可能にすることです。

一般的な推奨事項

必ず**問題ステートメント**を定義し、継続的に更新する。

範囲と影響を分類する。範囲と影響は、ビジネスニーズと重要度に関係する。

できるだけ早急に機能に優先順位を付けて復旧する。根本原因が依然として不明の場合は、後で非の打ちどころのない事後分析を行う。

最新のデータと実証的証拠を確認するように依頼する。

作業内容を文書化する。すべてのデータ、スニペット、タイムスタンプ、レポートを入手し、認められている場合は共有する。

定期的に**第一原則を再考**し、問題点について議論する。

ほとんどの場合、必要以上に多くを仮定するべきでない。履歴も重要。**変更点を把握する。**

問題領域を区分化する際、共通点に加えて**相違点に焦点を当てる。**

目に見えないからといって、発生していない、というわけではない。

よりシンプルな設計ほど、トラブルシューティングが容易である。

前提条件

ネットワーク要素の監視は、デバイスレベルの状態診断（アグリゲート仮想デバイスを含む）に有効。

インターフェイスレベルの監視と傾向分析を実施（速度、しきい値、バッファ、またはキューイングに関する適切な統計を含む）。

ユーザーの位置またはサイトからのルートをトレースできる。

RIB（Routing Information Base）とFIB（Forwarding Information Base）へのアクセスが、ユーザーのデバイスを含め、関連する管理対象ネットワーク要素すべてで利用可能である（可能な場合）。

ログへの記録および照会を一元化。理想的にはUTCタイムスタンプに基づき、ミリ秒の粒度。

想定

1. ユーザーエンドポイントは、同じ問題（固有のホスト問題ではない）のあるデバイスグループの1つ。
2. ユーザーエンドポイントはトラフィックを他の送信先に正しく転送できる（WANを通らない）。
3. 収集したデータ（間接または直接）はすべて役立つが、記録のシステムで個別に検証またはチェックするまで、間違っている可能性がある。
4. WANの問題は持続的または断続的である場合がある。
5. （1）および（2）のとおり、問題はWANに存在する。クライアント側のホストルーティング、認証、クライアントVPNの問題などではない。
6. 全体を通じたIPv4スタック（デュアルスタックまたはIPv6のみに対して）。
7. ICMPエコーリクエスト（タイプ8）、エコー応答（タイプ0）、超過時間（タイプ11）が送信元から送信先へのパス上におけるネットワーク要素上のエンドツーエンドで有効。
8. 運用チームが管理対象トポロジーのレイアウトを把握している。文書化またはダイナミックマッピングが、すべての管理対象インフラストラクチャノードで最新である。
9. ネットワークの監視機能は、指定の期間内に影響を引き起こす未知の問題または関連問題を報告しない。

解決と到達可能性

1. クライアントのソースインターフェイスおよびリモートサービスまたは送信先の**実際の**IPアドレスを設定し、使用する。これには、名前付きリソースが使用されているかどうか、およびクライアントの観点からリソースがどのように解決されるかを確認することが含まれる。

2. **クライアントのデフォルトゲートウェイの送信元IPアドレスから送信先IPアドレスにICMPエコー（ping）を送信する**（DFビットを設定し、エンドツーエンドで転送可能と思われるパケットサイズを使用）。失敗した場合は...

3. **クライアントのデフォルトゲートウェイの送信元IPアドレスから送信先IPアドレスまでのルートをトレースする**（ICMPを使用するが、可能な場合はUDPまたはTCPの使用を検討する）。失敗した場合、または想定外のノードが関係している場合は...

4. **IP到達可能性が、想定したパスに従っていること**と、最後の既知の「良好な」ホップのRIBを確認する。

5. **該当するACL（アクセスコントロールリスト）、ファイアウォールポリシー、インターフェイスのMTU（最大送信単位）**を、最後の既知の「良好な」ホップと、1ホップ離れたパスで確認する。

6. **IPの到達可能性が証明されたら、ソースのサブネットから開始し、対象のサービスのTCPポートまたはUDPポートをテストする。**汎用コンピューティングデバイスへのアクセスに、telnet、tcptraceroute、tcping、curl、hping3、nmap、ncといったツールが必要になる場合がある（ネットワークデバイスに用意されていない場合）。

7. **ほとんどすべてのTCPサービスはSYNに応答する。**ただし、多くのUDPサービスは、対象のサービス向けにメッセージが適切に構成されていない限り、応答しない。

8. **リモートサービスが適切なポート（使用可能な場合）でリッスンしていることを個別に検証**し、リモートサブネットの観点から、（1）の手順を繰り返す。

テストを実行し、ユーザーを完全にエミュレーションするための、ソースエンドポイントの制御機能がない場合は、初期および最も近いレイヤー3インターフェイスを使用すること（通常はクライアントのデフォルトゲートウェイ）

ネットワーク要素には通常、コマンドラインで使用するトラブルシューティングツールのサブセットが付属している。ただし、インストール可能なパッケージとツールを備えた、十分な機能を有する 汎用コンピューティングエンドポイントで使用する機能ほど柔軟性があるとは限らない。

RUM（Real User Monitoring）を既知のサービスに追加して、セッションレベルでリアルタイムに監視することを検討する。

セッションおよびアプリケーションを意識する

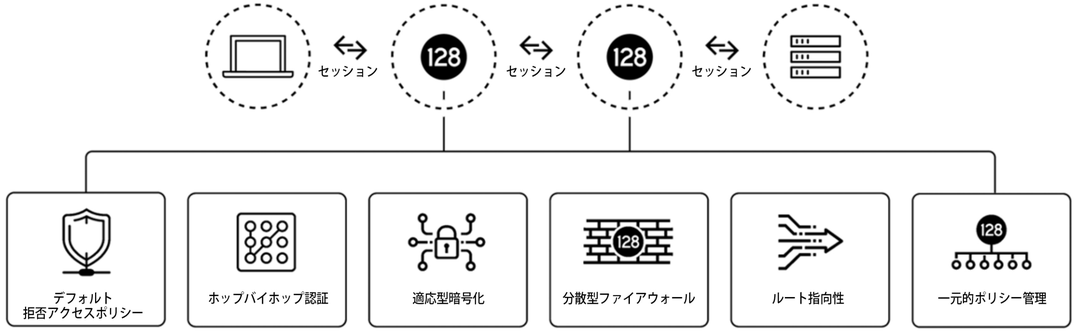
トラブルシューティングは状況認識を前提にしています。ルーターは従来、セッションまたはアプリケーションの実際の状態にかかわらず、転送の機能を実行してきました。ファイアウォールおよびロードバランサーは、状態を追跡して使用しますが、セッション指向はネットワーク全体にまだ浸透していません。よりスマートなルーティングおよびポリシー適用を実現するための、セッション指向およびアプリケーション指向の新しいルーターが誕生しました。

ジュニパーのSession Smart™ルーター（SSR）の仕様は、アプリケーション指向およびセッション指向です。

ユーザーエクスペリエンスを継続的に最適化し、サポートコストおよびMTTRが大幅に削減（30～40%）されます。セッションベースのこのネットワークモデルは、トンネリングを使用しないため高フォーマンスで拡張が容易です。

簡素化されたアクセスコントロールとハイパーセグメンテーションにより、SASE（Secure Access Service Edge）が最初から組み込まれています。

ファブリックに「ゼロトラスト」セキュリティ機能が組み込まれたことで、リスクが劇的に低減し、サービスの完全性が向上します。



ネットワークのファブリックにインテリジェンスを追加できるようになると、サポートコストの低減、可視性の向上、トラブルシューティングの簡素化などの多くのメリットがもたらされます。

Juniper Session Smart™

ジュニパーのソフトウェアベースのSession Smart™ソリューションは、迅速かつ簡単にホワイトボックスやハイパーバイザーを介してオンプレミスで導入することや、パブリッククラウドに導入することが可能です。

セッションベースのこのモデルにより、境界のないファブリックを構築し、遅延が最大60%、帯域幅コストが30～50%低減できます。柔軟な導入オプションにより、既存のインフラストラクチャすべてを有効活用し、WANのスマート化および簡素化によるメリット（ユーザー満足度向上、パフォーマンス向上、トラブルシューティング件数削減、セキュリティ強化）を得ることができます。

簡素化

トンネリングなし、オーバーレイなし、ハードウェア中心のネットワークから脱却

俊敏性

短時間で導入、応答性の向上、動的な最適化

セキュリティ

ゼロトラストモデル：
認証 + 暗号化 + セグメンテーション

パフォーマンス

間接費削減、拡張性向上、動的な最適化

コスト削減

帯域幅コストおよび接続コストを削減

Session Smart™ SD-WANのご紹介

オンラインセミナーを見る

AIドリブンSD-WANの実例をご紹介するジュニパーのTransformation Thursdayライブデモにご参加ください。

さらにご質問がある場合はその他のサポート情報およびトラブルシューティングガイドの詳細は、ジュニパーのナレッジベースをご覧ください。

PN：7400132-001-JP

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888.
JUNIPER（888.586.4737）
または+1.408.745.2000
FAX：+1.408.745.2100
www.juniper.net

APAC、EMEA本社
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.0.207.125.700
FAX：+31.0.207.125.701

日本
東京本社
ジュニパーネットワークス株式会社
〒163-1445 東京都新宿区西新宿3-20-2
東京オペラシティタワー45階
電話番号：03-5333-7400
FAX：03-5333-7401
西日本事務所
〒530-0001 大阪府大阪市北区梅田2-2-2
ヒルトンプラザウエストオフィスタワー18階
www.juniper.net/jp/jp