Hewlett Packard Enterprise

ビジネスホワイトペーパー

BYODのための ネットワーク再設計

目次

要旨

今日、個人が所有するモバイルデバイスを使用して、企業ネットワークにアクセスする従業員が増加していることにお気づきでしょうか。多くの従業員は、自分のスマートフォンやタブレットを職場で使用することにより、生産性を向上させています。

かつては、企業のIT部門がネットワークにアクセスできるモバイルデバイスの種類を制限していましたが、それも今では過去のものとなりました。私物デバイスのオフィスへの持ち込み（BYOD）ポリシーは、従業員の満足度と生産性を高める一方で、企業ネットワークに負荷をかけます。

キャンパスオフィスやブランチオフィスで幅広く使用されているレガシーネットワークは、とりわけ大きく制限されます。レガシーネットワークは柔軟性があまり高くないため、従業員はネットワークの使用方法をカスタマイズできません。また、ネットワーク設計者が想定していなかったモバイルデバイスをユーザーが接続することで、セキュリティのリスクも高まります。さらに、レガシーネットワークは複雑で人手を要します。新しいデバイスを接続できるようにするために手動で構成を変更しなくてはなりません。また、従来の3層アーキテクチャーで、無線ネットワークを使用したときは特に、最新のアプリケーションの動作が遅くなる可能性があります。

そこで、企業ネットワークを再設計しましょう。そうすれば、BYODのセキュリティ確保と管理が容易になります。次世代のネットワーク機器は速度低下への対策として有用であり、更新されたネットワークは高い柔軟性と拡張性を提供します。さらに、優れたネットワーク管理アプリケーションを使用すると、管理者は一元管理可能なプラットフォームから、ネットワーク上のデバイスの特定、アクセス対象、セキュリティ状況を把握できます。

このホワイトペーパーでは、レガシーネットワークの持つ制約、特にBYODのサポートについて重点的に説明します。これらの制約を理解することにより、キャンパスネットワークやブランチネットワークにおいて、BYOD管理ポリシーを正しく機能させることが可能になります。

レガシーネットワークが足かせになっていませんか

かつて、職場の有線ネットワークに接続するデバイスはすべて、IT部門が提供していました。現在では、各ユーザーがデバイスを複数台所有しており、これらのデバイスをIT部門が必ずしも提供または承認しているわけではありません。また、ユーザーは、これらのデバイスで無線ネットワークによるビデオのストリーミングや会話など、複雑なアプリケーションを使用したいと考えています。

無線ネットワーク利用の要求が複雑化し、サービスが変化するのに伴って、ネットワークも適応しなければなりません。しかし、従来のネットワークではこのような対応が困難です。レガシーネットワークは、以下の4つの点においてBYODの制約となります。

1. **柔軟性の欠如:** レガシーネットワークは、ITがユーザーと場所のタイプを管理できるように設計されています。従業員は、ネットワークの使い方をカスタマイズできないため、生産性の向上が阻害されます。また、ITスタッフはネットワーク上の各テクノロジー向けに異なる管理プラットフォームを使用しなければならず、その習得も必要となります。
2. **セキュリティの制約:** レガシーネットワークでは、境界が明確に定義されていました。しかし現在では、ネットワークが設計された当初には存在しなかったモバイルデバイスが接続されるため、セキュリティのリスクが高まっています。
3. **複雑性:** 無線ネットワーク構成の変更では、スクリプトを作成しコマンドラインインターフェイス (CLI) での変更が必要となるため、時間がかかり、手動で操作しなければなりません。ネットワークは複雑化し、データ、ビデオ、および音声を無線でも円滑に送信することが求められます。
4. **低速な3層ネットワーク:** 従来の3層ネットワークは、従業員の大部分がデスクトップコンピューターを使用し、無線ネットワークの利用が少数の幹部の特権であった時代に設計されたものです。2層ではなく3層の構造をとることによって、ネットワークが使用されるたびに追加のホップが必要となるため、ネットワークが減速します。

これらの問題について解説し、解決策について検討しましょう。

柔軟性の欠如

レガシーネットワークは、固定された構成により設計されていました。従業員はIT部門からコンピューターを提供され、機器は有線ネットワークに接続します。各オフィスにはネットワークドロップがあり、設定が変わることはありません。従業員がネットワークや接続するデバイスをカスタマイズすることができなかったため、ITは接続するデバイスを把握できました。また、帯域幅と容量は、各ユーザーがネットワーク上でデバイスを1台ずつ使用するという想定の下に計画されました。コストを抑制するためにも、ネットワークの構築に必要以上の容量が使用されることはなかったのです。

今日では、1人のユーザーがデスクトップコンピューター、ラップトップ、タブレット、スマートフォンを使用し、これらすべてを同時にネットワークに接続することもあります。ユーザーは、Wi-Fiでトレーニングビデオを視聴するときも、デスクトップコンピューターからSkype通話を実行するときも、同等のパフォーマンスを期待します。職場のモデルも変化し、会議室などの共有ワークスペースから従業員がネットワークに接続するようになりました。従来のネットワーク設計では、もはや十分な役割を果たすことができなくなっているのです。

セキュリティの制約

レガシーネットワークでは、厳密にセキュリティを管理できていました。ネットワーク管理者が許可するデバイスを定め、高度なファイアウォールが許可されないデバイスによる企業データへのアクセスを防止していたのです。アクセスを許可されるデバイスはすべて、ITが 購入して構築し、リモートサポートを提供していたので、許可されたデバイスであるかどうかは簡単に把握できました。

しかし、状況は一変しています。最善のファイアウォールでも、信頼できない未知のデバイスから完全に保護することはできません。一方で、BYODセキュリティポリシーは、本質的にこのようなのデバイスの接続をユーザーに勧めるものなのです。セキュリティは、ネットワークの境界を保護するだけでは十分ではなく、ユーザーがネットワークに接続するあらゆる場所を保護しなければならなくなっています。

今日のネットワーク管理者は、ネットワークに接続するデバイスについて、デバイスの種類、アクセス対象、消費する帯域幅の「見える化」を必要としています。新しいサービスが利用可能になったらすぐに提供できるように、ネットワークソリューションには柔軟性が求められています。このように、レガシーネットワークの制約により、このような変更やBYODのセキュリティには時間がかかります。

従来、レガシーネットワークの変更はCLIを介して手動で行われてきました。しかし、新しいデバイスは種類が多く、しかもネットワーク接続するすべての新しいデバイスについてユーザーが必ずしもIT部門に知らせるわけではないため、このような手動の変更は不可能です。

ネットワークのゲストユーザーは、さらなる問題を引き起こします。オフィスへの訪問者も、ネットワークに接続するつもりでタブレット、ラップトップ、スマートフォンを持参することが多いでしょう。キャンパスやブランチの施設への訪問者に無線LANへのアクセスを提供する場合でも、企業の機密データを安全に保護する必要があります。

さらに、従業員は無線アクセスを一層要求するようになっており、しかも高速なアクセスと信頼性を期待しています。

複雑さ

レガシーネットワークでは、ネットワーク上のデバイス数があまり変化しなかったため、IT管理者はこれらのデバイスを把握できていました。

ネットワークに追加する機能が増加すると、それに伴って管理も複雑になります。無線ネットワークが有線ネットワークに追加されることにより、突如として2セットのネットワーク、2セットの管理アプリケーション、2セットのセキュリティ実装が存在するようになります。

つまり、管理が何倍も複雑になるのです。未知のデバイスがネットワークとの接続/切断を実行し、同一ユーザーがラップトップからネットワークに1時間アクセスした後で、スマートフォンからもアクセスするような環境では、これらの通信をすべて管理できる統合システムを導入することが重要となります。CLIを使用してポリシーを定義および適用するのは、もはや現実的ではありません。

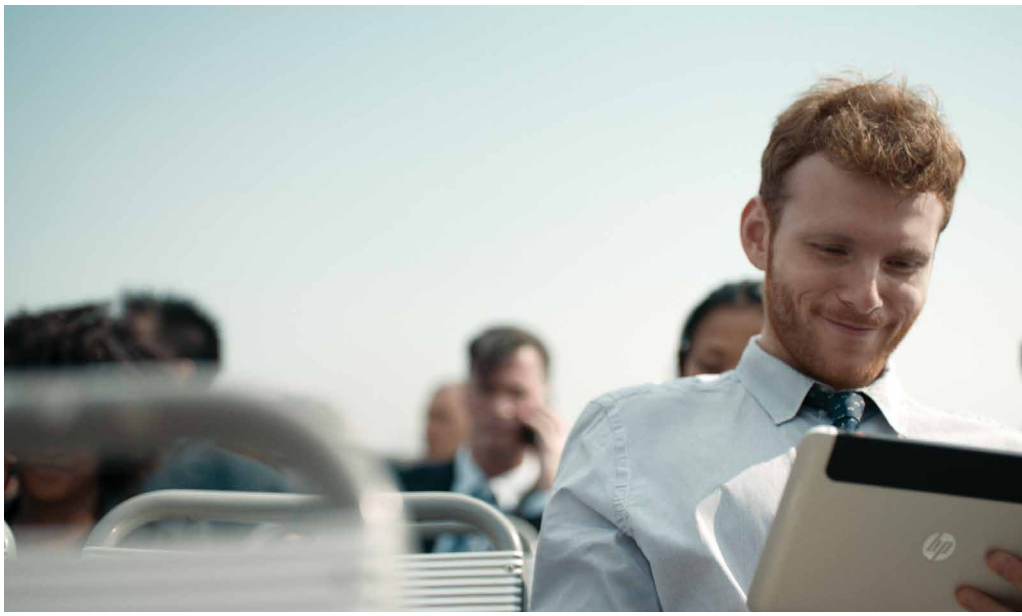
低速な3層ネットワーク
3層アーキテクチャーを擁するレガシーネットワークは、有線アクセス向けに設計されました。アクセススイッチはディストリビューションスイッチに接続され、ディストリビューションスイッチは高速バックボーンに接続されます。ネットワークが設計された当時は、すべてのアクセススイッチがコアネットワークに直接接続できたわけではないため、これでも合理的でした。クライアント/サーバーのアーキテクチャーでは、ネットワーク管理者がトラフィックを物理的に複数のサブネットに分割します。

しかし、現在では職場のテクノロジーは大きく異なります。仮想化、ビデオコラボレーション、VoIP、ワークグループコラボレーションのような高度に協調的なテクノロジーには、レイテンシの低いネットワークが必要です。たとえば、デスクトップ仮想化の場合、データとアプリケーションはクラウドに保存されます。これはつまり、ユーザーがアプリケーションを必要とするたびに、デバイスがクラウドベースのサーバーに接続しなくてはならないことを意味しています。従来の3層アーキテクチャーはネットワークで追加ホップを必要とするので、このプロセスを減速させることになります。

レガシーの無線ネットワークも、正しく接続するためにアクセスポイントの近くに位置しなければならない、低電力のモバイルデバイスをサポートするようには設計されていません。モバイルデバイスを適切にサポートするには、無線ネットワークを高密度（アクセスポイントの近くに位置する小さな領域内に多くのデバイスが存在する状態）向けに再設計する必要があります。

BYODのためのネットワーク再設計

BYOD無線ネットワークのためのベストプラクティス
BYODでネットワークが複雑化することにより動きが取れなくなってしまわないように、これを機にネットワークを簡素化してはいかがでしょうか。より大きな帯域幅とより高速なスループットを実現するために、ネットワークを2層に再設計することを検討してみてください。ソフトウェア定義ネットワーク（SDN）は、ユーザーの動的な変化に対応するためのネットワークの再構成を容易にします。



2層ネットワークは高速でレイテンシが低く、ビデオ会議などの際に円滑に動作します。新しいタイプのインフラストラクチャ（クラウドサービスなど）のサポートに十分な柔軟性を持ち、既存の投資やファイアウォール、ルーティング、およびアプリケーションデリバリの最適化ポリシーもサポートします。また、アプリケーションの使用からルーターのレイテンシまで、すべてを表示する一元的なインターフェイスにより、ITスタッフの効率性と効果が向上します。

また、柔軟性と拡張性の高いネットワークを使用することで、従業員が職場で複数のデバイスを使用できるようになります。新しいデバイスが追加され、新しいビジネスの要求が出されるのに伴い、ネットワークも拡張します。また、柔軟なネットワークにより、会議室、カフェテリアなど、ユーザーが集中しやすい高密度スペースでも、容易にアクセスポイントを追加できます。新しい世代のWLANコントローラーを使用すると、旧来のコントローラーに比べて数倍の数のアクセスポイントを管理できるので、BYODを円滑にサポートする上で欠かせません。

ネットワークのセキュリティ確保

ネットワークの再設計により、ユーザーが職場で生産性を高める方法は増え、同時にネットワークの安全性も保持できます。その方法は以下のとおりです。

- ネットワークを分割して、最も機密性の高い部分にゲストがアクセスできないようにします。
- ネットワークに接続するデバイスのタイプ、実行するオペレーティングシステム、および使用されるブラウザーを識別できるツールを配備します。
- 802.1X認証およびNetwork Access Control (NAC) をサポートできるように、ネットワークをアップグレードします。これにより、ネットワーク管理者はユーザー、デバイス、または場所に基づいて、企業リソースへのアクセスを制限できるようになります。

有線/無線ネットワークの統合はネットワークを簡素化し、デスクトップPCを使用してビジネスアプリケーションにアクセスしている場合でも、タブレットを使用している場合でも、一貫性のあるエクスペリエンスをユーザーに提供します。簡素化されたネットワークが自動化されると、各管理プラットフォームやすべてのネットワーク機器の構成を手動で変更する必要はありません。これまで投資してきたネットワークやセキュリティにも容易に統合できるので、単一プラットフォームからマルチベンダーインフラストラクチャを管理できます。

無線の簡素化

現在の従業員はモバイルを重視しており、いつでもどこでも接続できる環境がますます求められています。また、従業員は個人所有のデバイスを利用するようになっています。モバイル接続を常に可能にすることが求められているため、無線テクノロジーに対する観点もまた変わりつつあります。すでに有線ネットワークを単に補完するものではなくなっており、従業員の主要なアクセス手段としてとらえている企業も増加しています。

有線ネットワークと同じくらい高速でスムーズな無線アクセスへの要求がますます高まっています。ユニファイドコミュニケーション&コラボレーションソリューション (UCC) アプリケーションが、モバイルクライアントで広く使用されるようになっています。これらのタイプのアプリケーションでは、高品質で信頼性の高い音声とビデオを実現するために、優れた無線周波数 (RF) カバレッジが求められます。これらの高品質なサービスレベルを満たすためには、最新の802.11acアクセスポイントによる高パフォーマンスの無線LANが必要です。

現在の無線ネットワークが、IEEE 802.11nよりも古い標準を使用している場合、ネットワーク接続とアプリケーションのアクセスが低速になります。Wi-Fi接続のための新しい802.11acアクセスポイントは、優れたパフォーマンスとセキュリティを実現するため、無線接続に関する懸念は解消されます。新しい802.11acアクセスポイントは、簡単にセットアップでき、SMBの業務を高速化し合理化できるように設計された多くの機能を提供します。最新の802.11acテクノロジーを実装したアクセスポイントは、以前の標準と比較してパフォーマンスが最大で3倍高速になります。また、管理用のダッシュボードもあらかじめ組み込まれています。ユーザーが移動したり、無線周波数の条件が変わったりする場合に、新しいアクセスポイントテクノロジーは、クライアントのパフォーマンスを次のように最適化します。

- 最適なアクセスポイントを各モバイルデバイスに割り当てます。
- ユーザーが移動したり、無線周波数の条件が変わったりする場合にWi-Fiのパフォーマンスを動的に最適化します。
- 統合型の無線侵入防止機能によって、別途RFセンサーやセキュリティアプライアンスを導入しなくても、脅威から保護できます。
- Webページを迅速にロードして、高品質なビデオストリームを実現します。
- 高密度のモバイルデバイス環境もサポートします。

モバイルを利用する従業員や顧客が増加する中で、企業はモバイルデバイス向けの最新のアプリケーションを迅速かつ安全に提供していく必要に迫られています。新しい802.11acアクセスポイントによって、ミッションクリティカルアプリケーションをより信頼性の高い方法で配信できるようになり、顧客、従業員、そしてパートナーに優れた接続環境を提供できます。

まとめ

HPEのBYODソリューションには、従業員の満足度と生産性を向上させる大きな可能性があります。レガシーネットワークが障害とならないように、対策を打ちましょう。また、お客様のキャンパスまたはブランチオフィス向けのBYOD対応ネットワークの構築方法については、お客様の地域のビジネスパートナー、またはHPEの販売店にお問い合わせください。

詳細情報

hpe.com/networking/byod（英語）をご覧ください。

4AA4-3882JPN、2015年11月、Rev. 1

Hewlett Packard Enterprise