データシート

ArubaOS 8

今日のモバイル・ワークプレイスのためのスマートなオペレーティング・システム

概要

モバイル・デバイス、IoT、ビジネス・クリティカル・アプリケーションはモバイル・ワーカーの生産性と効率を向上させていますが、同時にネットワークに対する需要も拡大しています。

ArubaOSは、Arubaモビリティ・コントローラー、仮想モビリティ・コントローラー、モビリティ・マスター、コントローラー管理による無線アクセス・ポイントのすべてを対象としたオペレーティング・システムです。広範なテクノロジーと機能を装備したArubaOS 8は、有線/無線の統合アクセス、シームレスなローミング、エンタープライズグレードのセキュリティ、常時稼働ネットワーク、高密度環境のサポートに必要なパフォーマンス、ユーザー・エクスペリエンス、信頼性を提供します。

Arubaアーキテクチャの新しいコンポーネントであるモビリティ・マスターは、お客様が一元的な管理やモバイルおよびIoTデバイス向けの需要拡大に対するネットワーク拡張が必要となった際に、高度な機能を活用し対応することができます。また、これまでマスター・コントローラーが備えていた機能を置き換え、仮想アプライアンスまたはx86ハードウェア・アプライアンスのいずれかとして配備できます。モビリティ・マスターは、自動的なRF最適化を提供し、コントローラーの停止という不測の事態ではヒットレス・フェイルオーバーを可能にします。

Arubaモビリティ・コントローラーを現在ご利用のお客様は、ArubaOSのバージョンを6から8にアップグレードすることで、いくつかの新機能のメリットをすぐに利用できます。サードパーティとの統合などの高度な機能を利用するには、モビリティ・マスターを追加する必要があります。ArubaOS 8の機能の詳細なリストについては、こちらのリリースノートをご覧ください。

モビリティ・マスターでサポートされるArubaOS 8のテクノロジー

機能	メリット
AirMatch	ArubaはAirMatchによってARM (Adaptive Radio Management)テクノロジーをさらに強化します。AirMatchは、動的な機械学習インテリジェンスを利用してWLANネットワーク全体の最適ビューを自動的に生成し、チャネル最適化、送信出力調整、チャネル幅調整を自動的に行う新しいシステムです。
ライブ・アップグレード※	新しいオペレーティング・システムへのアップグレードには、通常はネットワーク全体のダウンタイムが伴います。しかし、ネットワーク上にはミッションクリティカルなデータが絶えず行き交っており、メンテナンスのための時間枠を確保することは日に日に難しくなっています。「ライブ・アップグレード」を利用することで、ネットワーク全体をリアルタイムかつダウンタイムなしで最新のオペレーティング・システムにアップグレードできます。ユーザーに影響が生じることもありません。
コントローラー・クラスタリング	コントローラー・クラスタリングは、コントローラーの故障という不測の事態が生じた場合のヒットレス・フェイルオーバーを可能にします。音声通話、ビデオ、データ転送は、大きな影響を受けることなくすべて継続されます。どのユーザーに対しても単一障害点が生じることがないように、ユーザー・セッションの情報はクラスタ内のコントローラー間で共有されます。
MultiZone	モビリティ・マスターの新しいMultiZone機能を利用することで、IT部門は物理的に同じ場所にある同じAPを使用しながら、複数の異なるセキュア・ネットワークを維持できます。
NBAPI	モビリティ・マスターには、ネットワークに対する深い可視性を実現する完全なノースバウンドAPIセットが用意されています。NBAPIは、RF正常性に関するメトリクス、アプリ使用率、デバイス・タイプ、ユーザー・データを簡単に統合できる形式で提供します。サードパーティ製アプリケーションは、コントローラーから情報を受け取り、これらすべてのメトリクスを分析することで可視性と監視の向上を図ります。
インサービス・モジュール・アップグレード	モビリティ・マスターは、システム全体を再起動することなく、モビリティ・マスターに常駐している個々のサービス・モジュール（AppRF、AirGroup、ARM、AirMatch、NBAPI、UCM、WebCC、IP分類）を動的に更新する機能を備えています。
トンネル・ノード	トンネル・ノードにより、無線のポリシーを有線にまで拡張できるため、ユーザーの接続方法に関係なくユーザー単位の統一ポリシーを利用できます。
マルチOSのサポート	新しいOSリリースへのアップグレード時に生じるネットワーク・ダウンタイムを最小限に抑えるために、IT管理者はこの新しいテクノロジーを利用することで、新規ソフトウェア更新のテストと試行を特定の領域(コントローラー・クラスタ)で行くことができます。ネットワーク全体に影響を生じることはありません。これは、新しいイノベーションを最小限のリスクで採用するための段階的移行ツールとして利用できます。

※この機能を利用できるのはArubaOS 8.1以降のバージョンです。

Arubaオペレーティング・システムのコアとなるテクノロジー	
機能	**メリット**
ClientMatch	Arubaの特許技術であるClientMatchテクノロジーは、クライアントを最適なアクセス・ポイントにアソシエートさせることでスティッキー・クライアント状態を解消し、Wi-Fiのパフォーマンスを向上させます。また、複数MU-MIMOクライアントのグループ化によって複数デバイスに対して同時に送信を行うことで、WLANの全体的なキャパシティを向上させます。
AppRF	オプションのAruba PEF (Policy Enforcement Firewall)モジュールの一部であるAppRFテクノロジーは、WLANにアプリケーションの認識をもたらします。これを利用することで、IT部門は各ユーザーのアプリケーションに優先順位を付け、BYODトランザクションとデバイス密度を計ることができます。
AirGroupテクノロジー	AirGroupを利用することで、Apple TV、Google Chromecast、その他のDNSアドバタイズ・デバイスをサブネット上で簡単に共有できます。シンプルな構成オプションによってすべてのデバイスが相互に認識できるようにし、高度なオプションによって物理的な場所、時間帯、ロール、自分で設定する共有エリアに基づいて共有の範囲を狭めることができます。
ARM (Adaptive Radio Management)	ARM (Adaptive Radio Management)は、RF環境を動的に調整することでWi-Fiの安定性と予測可能性を最大化し、すべてのクライアントとアプリケーションの最適なパフォーマンスを引き出します。Microsoft Skype for Businessの音声、ビデオ、デスクトップ共有、チャット・フローも対象となります。
RFProtectモジュール	ネットワーク・リソースを無線の脅威から保護し、ネットワーク・パフォーマンスを最適化するために、ArubaOS 8にはRFProtectモジュールという業界をリードする不正AP分類および封じ込めソリューションが統合されています。 RFProtectモジュールはネットワーク・インフラストラクチャに無線セキュリティを統合し、RFセンサーやセキュリティ・アプライアンスの個別システムを使用せずに政府レベルの無線侵入防御を実現します。 注： これはオプションのライセンシング対象機能です。
高度な暗号化機能	ArubaOS ACR (Advanced Cryptography)モジュールは、軍用レベルのSuite B暗号化機能をArubaモビリティ・コントローラーに提供し、重要性の高い機密情報や非公開情報を扱うネットワークへのセキュアなアクセスとユーザー・モビリティを実現します。 米国国家安全保障局(NSA)によって認定されたSuite Bは、パフォーマンスを向上させ、扱いにくいワークフローと厳密な取り扱い要件を排除します。
VIA（Virtual Intranet Access）クライアント	無償のハイブリッドIPsec/SSL VPNであるVIAは、企業ネットワークへの最もセキュアな接続を自動的にスキャンして選択します。従来のVPNソフトウェアとは異なり、VIAではクライアント端末のWLAN設定はゼロタッチで自動的に行われます。VIAは完全なWi-Fi Awareです。
Clarity	IT部門は、RF以外のメトリック(RADIUS、DHCP、DNSサーバー)に対する可視性を得ることができます。これにより、無線のユーザー・エクスペリエンスに対するエンドツーエンドの可視性が得られるだけでなく、ユーザーに影響が生じる前に接続性の問題を予測することもできます。 Clarityは、ネットワーク上を流れる実際のトラフィックに対する可視性を提供するだけでなく、WLAN管理者がトラフィックをシミュレーションし、ユーザーに影響が生じる前にサービス停止やパフォーマンスの問題を特定できるようにします。 これにより、何千ものロケーションを対象としたオンデマンドまたはスケジュールによるプロアクティブなワークフローが実現します。 注： これはオプションのライセンシング対象機能です。

合理化されたオペレーション

グローバル構成とローカル構成が含まれるフラットな構成モデルで動作するArubaOS 6とは対照的に、ArubaOS 8は一元的かつ重層的なアーキテクチャを採用しており、管理、制御、転送の各機能が明確に分離された新しいUIを備えています。モビリティ・マスターと管理対象デバイスの全体的な構成は、どちらも一元的な場所から行われるため、可視性と監視能力がより良くなります。また、構成プロセスが合理化され、繰り返しが最小限に抑えられます。

ArubaOS 8の新しいUIは先進的な外観と、シンプルに使用できるクイック・ワークフローを備えています。ネットワーク・オペレーションを合理化するArubaOS 8の機能は次のとおりです。

プールによる一元的ライセンシング：IT部門は、モビリティ・マスターまたはマスター・コントローラーのいずれかからの一元的ライセンシングを使用して、すべてのライセンスを一元的な場所から管理できます。新しいArubaOS 8ではこの機能が拡張され、プールによる一元的ライセンシングが含まれるようになりました。社内のグループごとに予算が異なるお客様のために、ライセンスをグループに割り当てることでグループごとにライセンスを管理、使用するオプションも用意されています。

ゼロタッチ・プロビジョニング（ZTP）：ZTPは、APと管理対象デバイスの配備を自動化します。プラグアンドプレイによって配備の迅速化と簡略化およびオペレーションの合理化を図り、コストを削減してプロビジョニング・エラーを限定します。ZTPは7xxxモビリティ・コントローラーに搭載された機能です。この機能が拡張され、ArubaOS8では72xxモビリティ・コントローラで利用できるようにしました。モビリティ・コントローラーは、マスター・コントローラーまたはモビリティ・マスターからローカル構成、グローバル構成、ライセンス制限を受信すると、自動的にプロビジョニングします。

統合アクセスの実現

Arubaは、ユーザーが所在地に関係なく、また、有線、無線を問わずにエンタープライズ・ネットワークにセキュアにアクセスできるようにし、常にアクセス可能で、高い顧客満足度を実現します。ユーザーには、本社、ブランチ・オフィス、ホーム・オフィス、外出先で均一なセキュリティおよびアクセス・ポリシーが適用されます。ユーザーとデバイスは、モビリティ・コントローラーにセキュアかつ自動的に接続するシンプルな軽量アクセス・デバイスまたはソフトウェアを使用してネットワークに接続します。

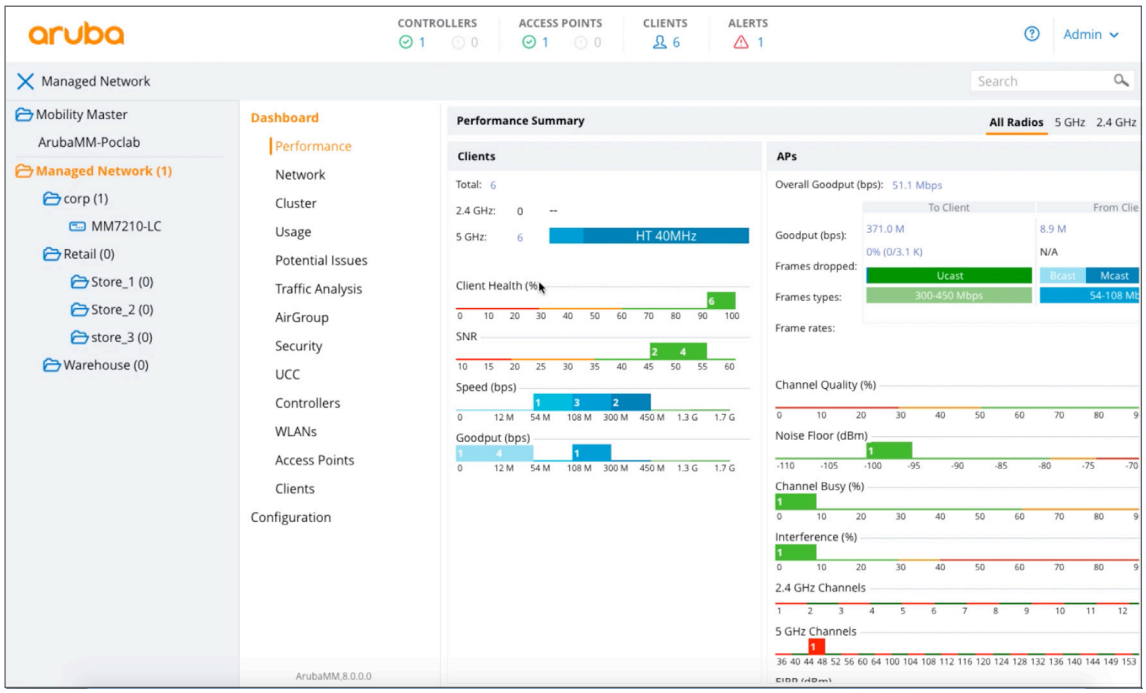


図1：ArubaOS 8の新しいUI

統合アクセス・フレームワーク	
ユーザーの接続方式	• セキュアなエンタープライズグレードWi-Fi • 有線Ethernet • VPNリモート・アクセス
APの接続方式	• プライベート/パブリックIPクラウド - Ethernet - 無線WAN (EVDO、HSDPA) • Wi-Fiメッシュ(ポイントツーポイント、ポイントツーマルチポイント)
トラフィックの転送	• 一元的 – すべてのユーザー・トラフィックはモビリティ・コントローラーを経由します • ポリシーベースのルーティング – ユーザー・トラフィックはトラフィック・タイプとポリシーに応じて選択的にモビリティ・コントローラーを経由するか、ローカルにブリッジングされます
Wi-Fi暗号化	• 一元的 – トラフィックはデバイスとモビリティ・コントローラーの間で暗号化されます • 分散 – トラフィックはデバイスとAPの間で暗号化されます • オープン – 暗号化なし
既存ネットワークとの統合	• レイヤー2/3統合 – モビリティ・コントローラーはVLANベースでトラフィックをスイッチング/ルーティングできます • ラピッド・スパニング・ツリー – 高速レイヤー2コンバージェンスを可能にします • OSPF – 既存のルーティング・トポロジーとのシンプルな統合

ArubaOS 8を搭載したモビリティ・コントローラーは、Arubaアクセス・デバイスとアクセス・ソフトウェアを管理します。また、ソフトウェア・イメージ、構成、ユーザーの接続状態の管理とポリシーの適用も行います。有線/無線のインフラストラクチャ全体の制御は、Aruba AirWaveによって一元的に行われるため、IT部門は複数世代のマルチベンダー・ネットワーク全体でアプリケーションとデバイスを管理できます。AirWaveでは、無線とモビリティのSLA（サービスレベル・アグリーメント）に影響するすべての要素を可視化できるため、ヘルプデスク・チケットを受け取る前に、キャパシティ・プランニング、クライアント・パフォーマンスの可視化、アプリケーションのトラブルシューティングをプロアクティブに行うことができます。

シームレスなモビリティを実現する設計

エンタープライズ・ユーザーは、移動中もネットワーク・アクセスを必要とすることが多くなっています。ArubaOSは、Wi-Fiネットワーク向けにユーザーの移動中もネットワーク全体のシームレスな接続性を提供します。ローミング・ハンドオフ時間は2～3ミリ秒であるため、音声やビデオのように遅延が重視される持続的なアプリケーションでも中断が生じることはありません。

ArubaOSにはプロキシ・モバイルIPとプロキシDHCPの機能が統合されているため、ユーザーは特別なクライアント・ソフトウェアを使わずにサブネット、ポート、AP、コントローラー間をローミングできます。これにより、ユーザーが仕事中にネットワーク上を移動しながら最初に接続したAPから遠く離れた場所に移ったとしても、シームレスなパフォーマンスが維持されます。

VLANプーリングは、ネットワーク設計を合理化するもう1つの強力なアクセス・エッジ機能です。VLANをネットワーク・エッジまで引き出す代わりに、モビリティ・コントローラー内に一元化してAPへのトンネルを設定します。これには、ネットワーク構成の複雑さの軽減やスパニング・ツリーの直径縮小などの大きなメリットがあります。大人数のユーザー・グループがネットワーク上を移動する際は、VLANのユーザー・メンバーシップを負荷分散することで最適なネットワーク・パフォーマンスを維持します。

Arubaのユニファイド・アクセス・アプローチは、プライベートWANを介して、または公共のインターネットを利用してエンタープライズをリモート・ロケーションにまで拡張し、場所に関係なくユーザーに同じアクセスを提供します。エンタープライズ・ネットワーク・インフラストラクチャから離れた場所にいるユーザーを接続するために、モビリティ・コントローラーは標準VPNコンセントレーターとして機能し、他のエンタープライズ・ユーザーと同じアクセスおよびセキュリティ・フレームワークでリモート・ユーザーを接続します。

モビリティ・マスターを利用している場合は、コントローラーのクラスタリングによって大規模キャンパス内でのシームレスなローミングが実現されます。大規模キャンパス内を移動しながらSkype for Businessなどのミッション・クリティカル・アプリケーションを使用しても、ユーザーが遅延を感じることはありません。クラスタ内のすべてのコントローラーが連携してユーザーを管理します。ユーザーが10,000台のAPの間をローミングしても、新しいIPアドレスの取得、再認証、ファイアウォール状態情報の損失が生じることはありません。

ネットワーク全体の無線セキュリティ

ArubaOS 8は、エンタープライズ・ネットワークの保護のためにユーザーとデバイスの認証、アクセス制御、暗号化を行います。Arubaのアーキテクチャでは認証は標準であり、有線、無線ネットワーク用に実装できます。無線では、WPA2および802.11iプロトコルの1つのコンポーネントである802.1Xが最先端のWi-Fiセキュリティとして広く知られています。

ArubaOSは独自の方法でAAA FastConnectをサポートします。これにより、802.1X認証情報の交換の暗号化部分をモビリティ・コントローラー上で終端させることができ、RADIUSやLDAPなどの異なるIDストアとの間で連合させることができます。AAA FastConnectは、PEAP-MSCHAPv2、PEAP-GTC、EAP-TLSをサポートしているため、外部認証サーバーを802.1X対応にする必要はありません。

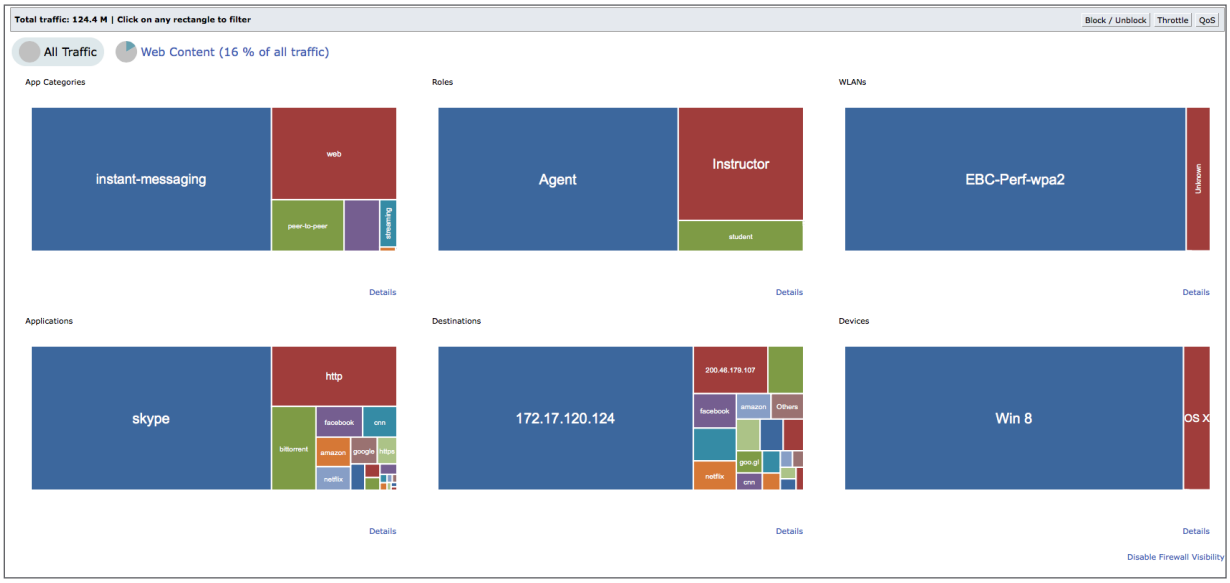
WPA、VPN、その他のセキュリティ・ソフトウェアを持たないクライアントのために、Arubaはブラウザーベースのセキュアな認証を提供するキャプティブ・ポータルを提供します。キャプティブ・ポータル認証はSSLによって暗号化され、ログイン名とパスワードを持つ登録ユーザーとメール・アドレスのみを入力するゲスト・ユーザーの両方に対応します。

未承認無線デバイスからの防御のために、システムはネットワークに接続して脅威となっている不正APと、干渉が生じている近隣APをArubaの不正AP分類アルゴリズムによって正確に区別します。不正デバイスとして分類されたAPは、有線/無線ネットワークを通じて自動的に無効化できます。不正APの分類と封じ込めはArubaOSの基本機能として利用できるため、モビリティ・コントローラーの追加ライセンシングは必要ありません。

Webは不可欠でありながら危険な場所でもあるため、ユーザーがアクセスするサイトのタイプを迅速に特定し、それらのサイトがネットワークやユーザーにもたらす相対的脅威を評価する機能が求められます。それを最新の方法で、できるだけ正確に行うために、ArubaOS 8にはオプション・サブスクリプションとしてURLフィルタリング、IPレピュテーション、ジオロケーションのためのWebコンテンツ・ポリシーおよびレピュテーションが用意されています。これを利用することで、適切なポリシーによってブロックとレート制限を行うことができます。現時点では、AOS 8はURLフィルタリングとURLレピュテーションのみに対応しています。

総合的な無線侵入防御機能を提供するモビリティ・コントローラーのRFProtectモジュールは、アドホック・ネットワーク、中間者攻撃、DoS（サービス拒否）などの多数の脅威に対する防御を実現し、無線侵入シグネチャーの検出に対応します。

ArubaOS 8のエンタープライズ・セキュリティ・フレームワーク	
認証タイプ	• IEEE 802.1X (EAP、LEAP、PEAP、EAP-TLS、EAP-TTLS、EAP-FAST、EAP-SIM、EAP-POTP、EAP-GTC、EAP-TLV、EAP-AKA、EAP-Experimental、EAP-MD5) • RFC 2548 Microsoft vendor-specific RADIUS attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS authentication • RFC 3579 RADIUS support for EAP • RFC 3580 IEEE 802.1X RADIUS guidelines • RFC 3748 extensible authentication protocol • MACアドレス認証 • Webベース・キャプティブ・ポータル認証
認証サーバー	• 内部データベース • LDAP/SSLセキュアLDAP • RADIUS • TACACS+ • 互換性を検証済みの認証サーバー： - Microsoft Active Directory (AD) - Microsoft IASおよびNPS RADIUSサーバー - Cisco ACS、ISEサーバー - Juniper Steel Belted RADIUS、Unified Accessサーバー - RSA ACE/Server - Infoblox - Interlink RADIUS Server - FreeRADIUS
暗号化プロトコル	• CCMP/AES • WEP 64/128ビット • TKIP • SSLとTLS： - RC4 128ビット - RSA 1024ビット - RSA 2048ビット • L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
プログラミング可能な暗号化エンジン	ソフトウェア更新によって将来の暗号化標準に対応できます
Webベース・キャプティブ・ポータル(SSL)	認証方式の柔軟性が得られます
統合型ゲスト・アクセス管理	セキュアなゲスト・アクセス・オプションを提供します
Site-to-Site VPN	モビリティ・コントローラーとIPsecデバイスの間にIPsecトンネルを確立します。X.509 PKI、IKEv2、IKE PSK、IKEアグレッシブ・モードの認証をサポートします。



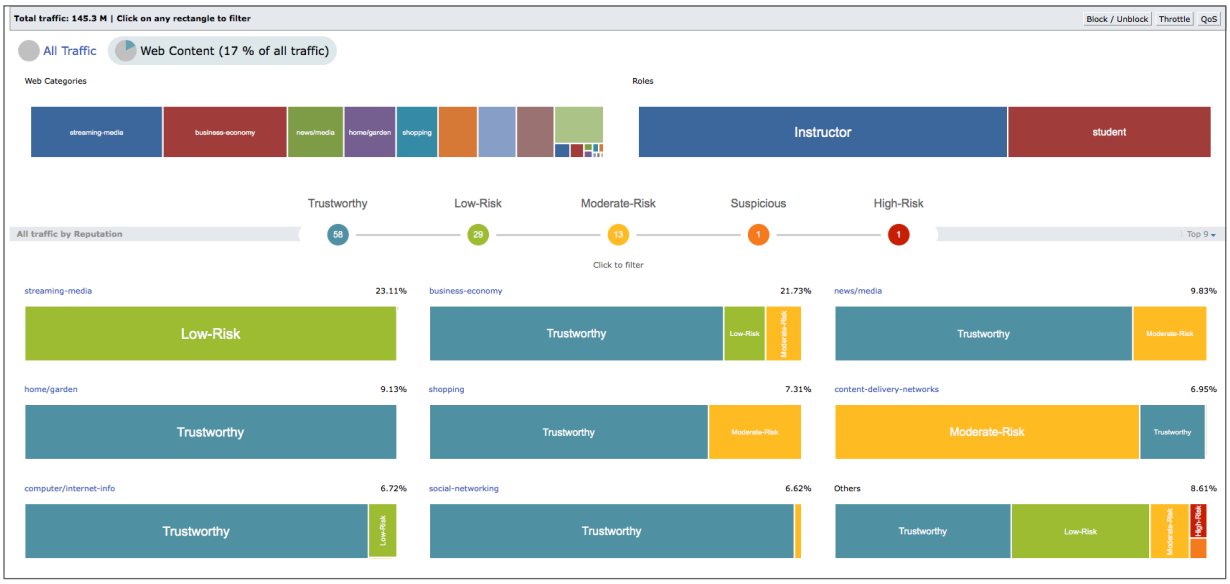


図2: WebCCダッシュボード

アプリケーション・アウェアな可視性とロールベースのセキュリティ

ArubaOS PEFライセンスは、ユーザーセントリックなセキュリティ、アプリケーションの可視性、制御を強化し、ほとんどのユーザー・トラフィックがネットワークに最初に接触する無線エッジに次世代モビリティ・ファイアウォールの性能を提供します。DPI（ディープ・パケット・インスペクション）によってトラフィックを分類、最適化し、シンプルなダッシュボードを通じてトラフィックの完全な可視性を提供します。

PEFは、完全なIDベースのセキュリティと、無線エッジにおいてユーザーベースで適用される統合型ファイアウォール制御機能を追加することでアクセス・セキュリティを強化、合理化します。これにより、ArubaOSは各ユーザー/デバイスの周囲にセキュリティ境界を作成し、そのユーザー/デバイスがエンタープライズ・ネットワーク・リソースにアクセスする方法を詳細に制御できます。

PEFライセンスの一部であるAppRFは、アプリケーションの認識と制御をWLANに提供します。AppRFは、Wi-Fiネットワークを流れるトラフィックのタイプに対する可視性を提供することで、どのユーザー・トラフィックが貴重なエア・リソースを使用しているかを管理者が把握できるようにします。AppRFはトラフィックに対する高度なコントロールも提供し、柔軟かつ強力な制御を実現します。管理者は、2,500種類以上のアプリケーションに対し、どのユーザー、どの優先度のトラフィックに伝送を許可するかを指定できます。

ArubaOS 8ではAppRFの機能が拡張され、お客様がカスタム・アプリケーションとアプリケーション・カテゴリを定義する機能（AppRFカスタマイズ）が追加されます。これにより、お客様はArubaが将来のソフトウェア・リリースでカスタマイズ機能を実装するのを待たずにカスタム・カテゴリとそのカテゴリに関連するすべてのアプリケーションに関するポリシーを適用し、カスタム・アプリケーション・トラフィックへの優先度の適用によってより優れたユーザー・エクスペリエンスを得ることができます。

UCC（UNIFIED COMMUNICATIONS AND COLLABORATION）のユーザー・エクスペリエンスの強化

今日の従業員は、モバイルUCCによる自由とコラボレーションを好みます。Aruba UCCソリューションは次のアプリケーションのネットワーク品質を自動的に分類、監視することで優れたユーザー・エクスペリエンスを提供します： Apple FaceTime、Alcatel Lucent New Office Environment（NOE）、Microsoft Lync/Skype for Business、Cisco Jabber、Cisco Skinny Call Control Protocol（SCCP）、Spectralink Voice Priority（SVP）、SIP、H.323、Vocera、Cellular Wi-Fi Calling。

Aruba Skype for Businessソリューションは、予測可能なUnified Communicationsエクスペリエンスを確保するために、Microsoft Skype for BusinessおよびAppRFテクノロジーとのSDN統合を利用してQoS（サービス品質）を適用し、優れた可視性を実現します。ArubaOS 8ではUCCソリューションがさらに強化され、次のUCC機能が提供されます。

- Cisco Jabberのサポートは、Cisco Jabberクライアントの非暗号化バージョンを使って行われる音声、ビデオ通話、デスクトップ共有セッションのQoSと可視性を提供します。
- マルチアプリケーション・レイヤー・ゲートウェイ（ALG）のサポートは、同一クライアント・デバイス上で同時に実行される複数のアプリケーションの特定と優先順位付けを可能にします。クライアント・デバイス上で同時に実行される最大10アプリケーションに対応しています。

Wi-Fi通話の利用が増加しているため、社内Wi-Fiネットワークの設計、ハンドオフ、QoS、RFカバレッジの目標を準備および再評価する必要があります。ArubaOS 8は屋内Wi-Fiカバレッジを改善し、QoSの適用、通話のブロック/抑制、クライアント正常性に関する可視性の提供を行い、お客様にキャリアグレードの音声エクスペリエンスを提供します。Arubaは、高品質なサービスの強化に加え、ユーザー、デバイス、キャリアベースでのWi-Fi通話に対する可視性も提供します。

アプリケーション・アウェアな可視性とロールベースのセキュリティ

機能	メリット
グローバルまたはロールベースのポリシー	単一コマンドですべてのユーザー・トラフィックを制御するシンプルさ、どのユーザーがどのアプリを実行できるかを正確に制御する柔軟性
2,500種類以上のアプリケーション	細分性の高い可視性と制御
19のアプリケーション・カテゴリ	タイプが異なるトラフィックの制御を合理化します
QoS (サービス品質)タグの適用	他のアプリケーションに対して特定のアプリケーションを優先します
望ましくないアプリケーションのブロック	帯域幅を節約し、望ましくないアクティビティを停止します
アプリケーションまたはアプリケーション・カテゴリのレート制限	ミッション・クリティカル・アプリケーションに負担が生じないように、重要性の低いトラフィックを制限します

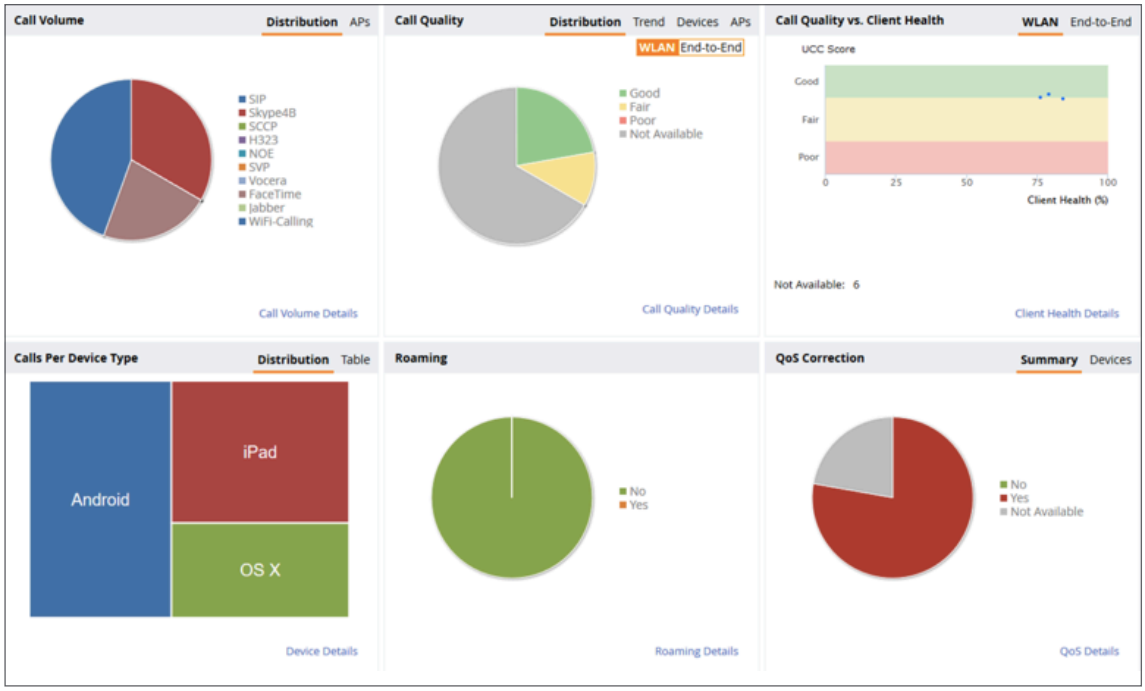


図3：ArubaOS 8のUCCダッシュボード

エンタープライズグレードのアダプティブWLAN

今日のビジネス世界では、いつ、どこにいてもモバイル・デバイスとアプリケーションを利用できることが必須要件となっています。そのアクセスを確実に提供するには、ダイナミックなモバイル環境自体に合わせて無線周波数（RF）スペクトラムをアクティブに管理できるWLANが必要です。

ARM（Adaptive Radio Management）テクノロジーはインフラストラクチャ・ベースの自動制御によってRFスペクトラム全体を管理する、定評のある特許技術です。ARMは、RF環境を動的に調整することでWi-Fiの安定性と予測可能性を最大化し、すべてのクライアントとアプリケーションの最適なパフォーマンスを引き出します。これには、Microsoft Skype for Businessの音声、ビデオ、デスクトップ共有、チャットの個々のフローの可視化と制御も含まれます。ARMを利用することで、ユーザーはIT部門の助けを借りずに常に満足できるエクスペリエンスを得ることができます。

ArubaOS 8では、ARM（Adaptive Radio Management）テクノロジーをさらに強化するために、新しいRF最適化システムであるAirMatchが追加されます。

モビリティ・マスター内のAirMatchは、最先端のRF環境を前提に設計されています。AirMatchは、ノイズが多く、クリーンで自由な空間が少ない高密度環境に合わせて調整されています。過去24時間のRF統計情報を収集し、それに基づいて翌日のネットワークをプロアクティブに最適化します。AirMatchはチャネル、チャネル幅、送信出力を自動的に最適化することで均等なチャネル使用を実現し、干渉の緩和とシステム・キャパシティの最大化に貢献します。

AirMatchのメリット	
均等なチャネル割り当て	利用可能チャネル間でラジオを均等に分散させ、干渉の緩和とシステム・キャパシティの最大化を実現します。
動的なチャネル幅調整	環境の密度に合わせて20、40、80MHzの間で動的に調整します。
送信出力の自動調整	WLANカバレッジ全体を調べてAPの送信出力を自動的に調整することで最高のカバレッジとユーザー・エクスペリエンスを実現します。

信頼性とユーザー・エクスペリエンスの向上

ネットワークには、モバイル・デバイス、IoT、クリティカル・アプリケーションから大量のトラフィックが流れています。コントローラーに障害が発生しても、大規模キャンパス内を移動していても、ユーザーはモバイル・エクスペリエンスの中断を想定していません。ArubaOS 8は、コントローラーに障害が発生した場合のダウンタイムを最小限に抑えられるように設計された強力な高可用性機能を提供します。

モビリティ・マスターで行われるコントローラー・クラスタリングは、キャンパスWLAN内の最大12台のコントローラーをクラスタ化することでヒットレス・フェイルオーバーを提供します。たとえコントローラーに障害が発生したとしても、ユーザーがそれに気付くことはありません。音声通話、ビデオ、データ転送は、大きな影響を受けることなくすべて継続されます。どのユーザーに対しても単一障害点が生じることがないように、ユーザー・セッションの情報はクラスタ内のコントローラー間で共有されます。

ブランチおよびホーム・オフィス向けのリモート・ネットワーキング

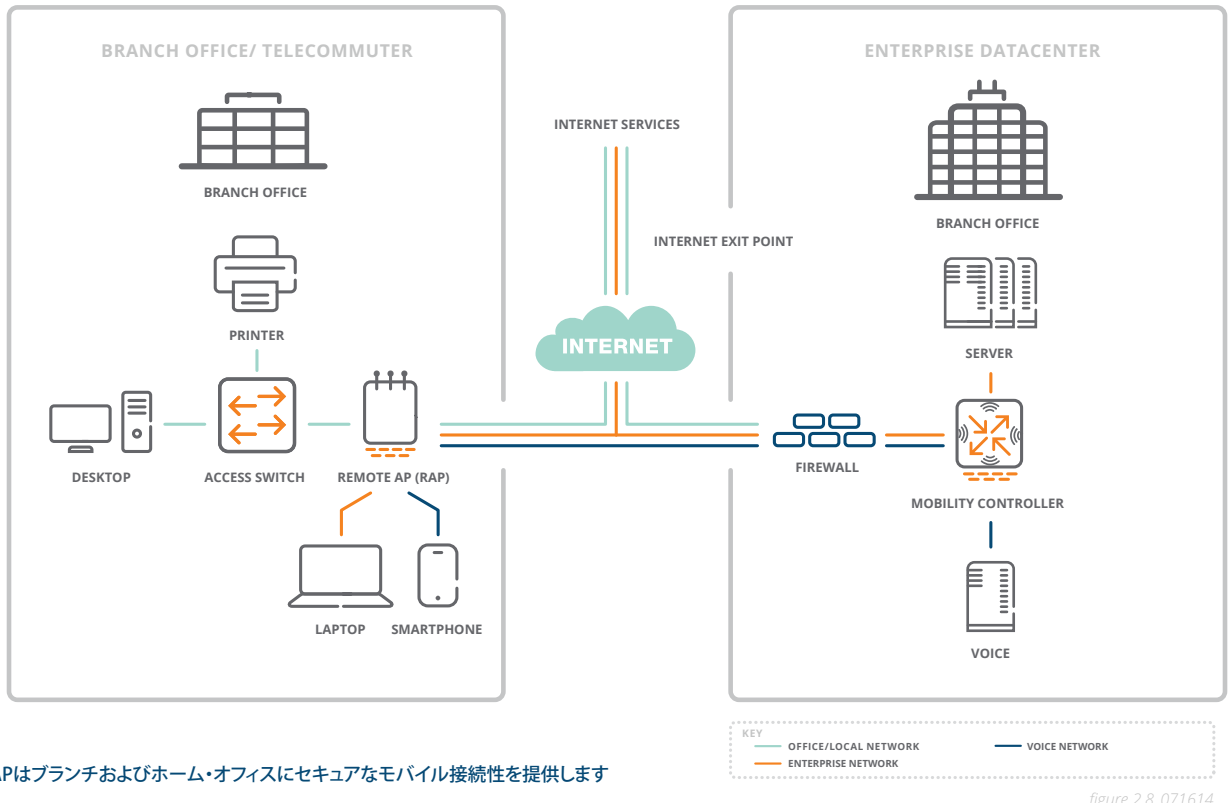
Arubaのリモートおよびブランチ・ネットワーキング・ソリューションは、企業ネットワークをオフィス、病院、店舗、SOHOにまで拡張するシンプル、セキュア、高コスト効率な方法を提供します。ArubaOSは、キャンパスまたはデータセンター内のモビリティ・コントローラーでのVPNの終端、ブランチ・ゲートウェイとしてモビリティ・コントローラーに配備されるWANサービスなど、ブランチ専用機能をモビリティ・コントローラーに統合します。

キャンパス内のモビリティ・コントローラーは、複雑な構成、管理、ソフトウェア更新、認証、侵入検出、リモート・サイト終端タスクをすべて処理します。ブランチに配備されるモビリティ・コントローラーは、ポリシーベースのルーティング、圧縮、ローカル・ネットワーク機能などのゲートウェイ・タスクを処理します。小規模ブランチまたはリモートのユースケースでは、手頃な価格のRAP（リモート・アクセス・ポイント）を使用して、または屋外ではAruba VIA（Virtual Intranet Access）VPNサービスを使用して企業ネットワークを拡張できます。

高可用性導入モード	
アクティブ/アクティブ(1:1)	各モビリティ・コントローラーは、通常は定格キャパシティの50%で動作します。第1コントローラーは第2コントローラーが管理するAPのスタンバイとして、またはその反対として動作します。コントローラーに障害が発生すると、APをもう一方のコントローラーにフェイルオーバーさせることで、すべてのAPの高可用性を実現します。
アクティブ/スタンバイ(1+1)	すべてのAPは1台のモビリティ・コントローラーで終端し、他のコントローラーはスタンバイとして機能します。プライマリ・コントローラーが停止すると、APはスタンバイ・コントローラーに移行します。
N+1	アクティブな複数のモビリティ・コントローラーを1台のスタンバイ・コントローラーでバックアップします。

機能	メリット
APがアクティブ/スタンバイ両方のモビリティ・コントローラーを使って同時通信チャネルを確立する	第1モビリティ・コントローラーに障害が発生した場合は、冗長コントローラーへと瞬時にフェイルオーバーします。
APはフェイルオーバー中にラジオのオン/オフを切り替えない	SSIDを常に使用できます。
ソリューションはレイヤー3ネットワークにまたがって機能する	特別なトポロジーは必要ありません。
クライアント状態の同期	資格情報はキャッシュされるため、再認証が不要となり、RADIUSサーバーに余分な負荷がかかりません。
N+1オーバーサブスクリプション	構成を単純化し、必要なモビリティ・コントローラーの台数を削減します。

在宅勤務者のリモート・アクセス・ポイントの使用	
ゼロタッチ・プロビジョニング	管理者は、事前設定なしでRAPを配備できるので、それをエンド・ユーザーに発送するだけで済みます。
有線と無線	ユーザーは、Ethernet、Wi-Fi、または両方を使ってRAPに接続します。
柔軟な認証	802.1X、キャプティブ・ポータル、ポート単位・ユーザー単位のMACアドレス認証。
一元管理	構成と管理はモビリティ・コントローラーによって行われ、APのローカル構成は行われません。
3G/4G LTE WAN接続	RAPは、プライマリ/バックアップ・インターネット接続用のUSB無線WANアダプター(EV-DO、HSDPA)に対応しています。
FlexForwardトラフィック転送	• 一元的 – すべてのユーザー・トラフィックはモビリティ・コントローラーを経由します。 • ローカル・ブリッジング – すべてのユーザー・トラフィックはアクセス・デバイスによってローカルLANセグメントにブリッジングされます。 • ポリシーベースのルーティング – ユーザー・トラフィックはトラフィック・タイプとポリシーに応じて選択的にモビリティ・コントローラーを経由するか、ローカルにブリッジングされます(PEFライセンスが必要)。
エンタープライズ・グレードのセキュリティ	モビリティ・コントローラーへのRAPの認証にはX.509証明書が使用され、認証が完了すると、セキュアなIPsecトンネルが確立されます。
アップリンク帯域幅の予約	音声のように損失が重視されるアプリケーション・プロトコル向けに予約帯域幅を定義します。
ローカル診断	ヘルプデスクへの連絡が必要になった場合に、ローカル・ユーザーは事前に設定されたURLにアクセスすることでRAP診断をフルに利用できます。
リモート・メッシュ・ポータル	RAPはダウンストリームAPに無線リンクを提供するメッシュ・ポータルとしても機能します。
サポートされるAP	AP-90シリーズ、AP-100シリーズ、AP-110シリーズ、AP130シリーズ、AP-170シリーズ、AP-200シリーズ、AP-210シリーズ、AP-220シリーズ、AP-270シリーズ、AP-300シリーズ、AP-310シリーズ、AP-320シリーズ、AP-330シリーズ、AP-360シリーズ、RAP-155、RAP-100シリーズ、RAP-3
必要最低リンク速度	64kbps (SSIDあたり)
暗号化プロトコル(RAPからモビリティ・コントローラー)	AES-CBC-256 (IPsec ESP内)



Aruba RAPはブランチおよびホーム・オフィスにセキュアなモバイル接続性を提供します

figure 2.8_071614

出張者向けのシンプルでセキュアな接続

オフィスから離れた場所からエンタープライズ・リソースにアクセスしなければならないユーザーは、通常はエンタープライズDMZ内に配備されたVPNコンセントレーターに接続するVPNクライアント・ソフトウェアを使用します。

Arubaの場合、モビリティ・コントローラーがVPNコンセントレーターとして機能するため、リモートVPNユーザーは他のすべてのユーザーと同様に扱われます。本社でも、ブランチ・オフィスのRAP配備でも、同じアクセス・ポリシーとサービス定義が使用されます。

ArubaOSは、いくつかの一般的なVPNクライアント、および主要クライアント・オペレーティング・システムに組み込まれているVPNクライアントとの互換性を持っています。また、Android、iOS、Mac OS X、Windowsデバイスにインストールできるオプションの VIAクライアントも提供します。

アクセス・ネットワークのマージによってポリシーとアクセス構成が統合され、ユーザー・エクスペリエンスが向上します。これにより、ヘルプデスクへの問い合わせとIT部門のコストは削減されます。

リモート・アクセスのためのセキュアな接続	
サポートを検証済みのクライアント	• Windows、Mac OS、Android、iOS、Linux上のAruba VIAクライアント • CiscoとNortelのVPNクライアント • OpenVPN、Apple/Windowsネイティブ・クライアント
VPNプロトコル	• L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
認証	• ユーザー名とパスワード • X.509 PKI • RSA SecurID • ICカード • 多要素

セキュア・エンタープライズ・メッシュ

Arubaのセキュア・エンタープライズ・メッシュ・ソリューションは、屋内、屋外を問わずに必要な場所にAPを配備できるようにするための、ケーブルが不要な柔軟な設計を提供します。ファイバーやケーブルを使用せずに実行されるため、ネットワーク設置コストが抑えられ、必要なEthernetポートも少なくて済みます。

このソリューションはArubaのユニファイド・アクセス・フレームワークと完全に統合され、ユーザーがどこでもローミングできる単一のエンタープライズネットワークが実現されます。セキュア・エンタープライズ・メッシュはプログラミング可能なソフトウェアをベースとしており、特別なハードウェアは必要ありません。Arubaの屋内用または高耐久化された屋外用802.11n/802.11ac APであれば、どれでもメッシュAPとして利用できます。

セキュア・エンタープライズ・メッシュは、Wi-Fiアクセス、同時無線侵入防御、無線バックホール、LANのブリッジング、ポイントツーマルチポイント接続など、企業のあらゆる無線ニーズに1つの共通インフラストラクチャで対応できます。

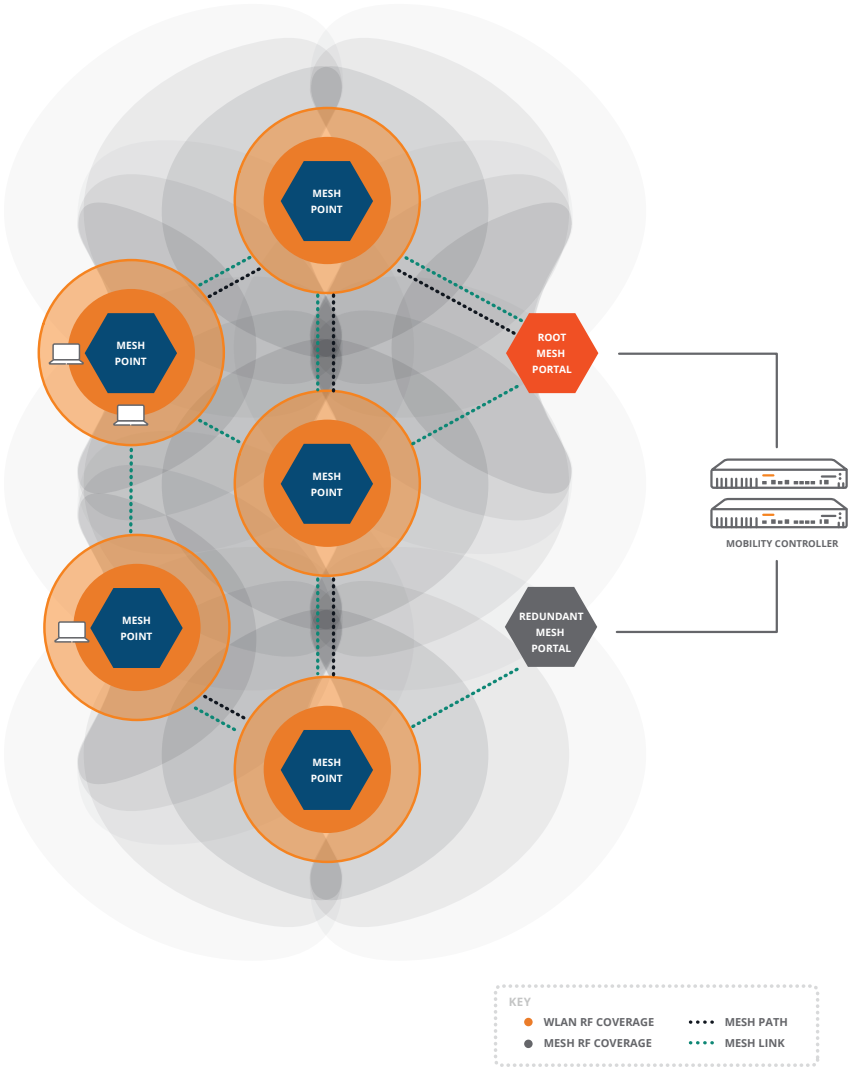
これは、建物間の接続性、屋外キャンパス・モビリティ、ケーブルレス・オフィス、有線バックアップなどのアプリケーションの接続性だけでなく、ビデオと音声の監視、アラームと強制信号、産業用アプリケーションとセンサーのネットワークなどのセキュリティ・アプリケーション向けとしても卓越したソリューションです。

Arubaは、協調制御テクノロジーであるインテリジェント・リンク管理アルゴリズムによってトラフィック・パスとリンクを最適化します。

メッシュAPは近隣APと通信し、RFとリンクの多数の属性（リンク・コスト、パス・コスト、ノード・コスト、負荷など）をアドバタイズします。これにより、アプリケーション用の最適パスをインテリジェントに選択できます。

高負荷または干渉が生じると、メッシュ・パスとリンクは自動的に調整されます。さらに、音声/ビデオ・トラフィック用のアプリケーション・タグを共有することで、他のデータに対してレイテンシが重視されるトラフィックを優先します。

協調制御テクノロジーは、パスがブロックされたり、APに障害が生じた場合のメッシュ・ネットワークの自己修復機能も提供します。



Arubaセキュア・エンタープライズ・メッシュ・ソリューション

Arubaセキュア・エンタープライズ・メッシュ・ソリューション	
広範なアプリケーションのサポート	Wi-Fiアクセス、同時無線侵入防御、無線バックホール、LANのブリッジング、ポイントツーマルチポイント接続。
ユニファイド・ネットワーク・アクセス	メッシュ・ネットワークとキャンパス/ブランチ・オフィスのWLANを統合します。ユーザーはキャンパス/ブランチのWi-Fiとメッシュ・ネットワークの間をシームレスにローミングできます。
協調制御	インテリジェントRFリンク管理によって最適パフォーマンスのパスを特定し、ネットワーク編成を自動的に行えるようにします。
自己修復機能	耐障害性に優れた自己修復メッシュにより、パスの破損やAPの障害を克服します。
メッシュ・クラスタリング	大規模メッシュを高可用性クラスタに分割できるようにすることで拡張性が増します。
一元的な暗号化	クライアントからコアへのデータはエンドツーエンドで暗号化されます。メッシュAPが盗難にあってもネットワークは保護されます。
一元管理	すべてのメッシュ・ノードはモビリティ・コントローラーによって一元的に構成、制御されます。ローカル管理は必要ありません。
多様なグラフィカル・サポート・ツール	ネットワークの完全な可視化には、カバレッジ・ヒート・マップ、リンク・バジェット自動計算、フロア・プラン、ネットワーク・トポロジーを備えたマップが含まれます。
標準ベースの設計	セキュア・エンタープライズ・メッシュは、IEEE 802.11sの設計原則に基づいています。

管理、構成、トラブルシューティング

モビリティ・コントローラーの構成、管理、トラブルシューティングには、すべてのネットワーク管理者にとって使いやすいブラウザーベースのGUIとコマンドライン・インターフェースを使用します。

ArubaOSはAirWaveとも統合し、プランニングと配備から監視、分析、トラブルシューティングに至るWLANライフサイクルのすべての段階で管理が容易になります。AirWaveは、長期傾向分析機能、ヘルプデスク統合ツール、カスタマイズ可能なレポートも提供します。

すべてのAPとモビリティ・コントローラーは、ブランチや支社に配備されているものも含め、単一コンソールから一元的に構成、管理できます。一般的なタスクを簡単に構成できるように、プロセスのすべてのステップをネットワーク管理者に示すタスクベースの直感的なウィザードが用意されています。

モビリティ・コントローラはデータセンター冗長をサポートし、1:1および1:NのVRRPベースの冗長構成で配備できます。レイヤー3トポロジーで配備する場合は、OSPFルーティング・プロトコルで自動的にルート学習・ルート配信をすることで、高速なコンバージェンスを可能にします。

無線ネットワークの管理と構成	
Webベースの構成	管理者が標準のWebブラウザーを使用してシステムを管理できるようにします。
コマンドライン	コンソール、SSH
Syslog	複数サーバー、複数レベル、複数施設をサポートします。
SNMP v2c	対応
SNMP v3	標準のSNMPを暗号化セキュリティで強化します。
モビリティ・コントローラーの一元構成	指定したマスター・モビリティ・コントローラーが複数のローカル・コントローラーを構成、管理できます。
VRRP	複数モビリティ・コントローラー間の高可用性をサポートします。
データセンター冗長のサポート	対応 – アクセス・デバイスにバックアップ・コントローラーのIPアドレスを構成できます。
OSPF	対応 – アップストリーム・ルーターへのデフォルト・ルートの学習や、ローカル・ルートの差し込みのためのスタブ・モードに対応しています。
ラピッド・スパニング・ツリー・プロトコル	対応 – 高速レイヤー2コンバージェンスを提供します。

ARUBAOSのIPV6のサポート

使用可能IPv4アドレスの枯渇により、組織はネットワークへのIPv6の導入を計画している、またはすでに開始しています。

IPv4とIPv6は、どちらもネットワーク上のデータの伝送方法を定義しますが、IPv6はIPv4よりずっと大きなアドレス空間を持ち、数十億ものユニークIPアドレスをサポートできます。

組織がIPv4からIPv6に移行する際に、ネットワーク機器はIPv4ネットワーク上でのIPv6とのデュアルスタック相互運用性、または純粋なIPv6環境への完全導入をサポートする必要があります。

ArubaOSは、今日のIPv6およびデュアルスタック環境へのモビリティ・コントローラーとAPの配備を促進します。管理、監視、ファイアウォールのあらゆる機能は、完全にIPv6アウェアです。

IPv6のサポート	
IPV6 IPsec	対応
IPv6による管理	GRE、SSH、Telnet、SCP、Web UI、FTP、TFTP、Syslog、SNMP
IPv6 DHCPサーバー	対応
IPv6によるキャプティブ・ポータル	対応
モビリティ・コントローラーでのIPv6 VLANインターフェース・アドレスのサポート	対応
APとモビリティ・コントローラーの間のIPv6による通信のサポート	対応
USGv6認定ファイアウォール	対応

コンテキスト・アウェアな制御

遅延が重視されるアプリケーションの無線サービス品質は、802.11eとWMM（Wi-Fi Multimedia）のサポートによってWMMタグと内部ハードウェア・キューをマッピングすることで確保されます。

モビリティ・コントローラーは、802.1pおよびIP DiffServタグとハードウェア・キューのマッピングによって有線側のQoSを確保し、特定の802.1pおよびIP DiffServタグを異なるアプリケーションに適用するように指定できます。

Aruba PEFモジュールが追加されたことで、Lync、SIP（Session Initiation Protocol）、SVP（Spectralink Voice Priority）、Alcatel NOE（New Office Environment）、Vocera、SCCP（Skinny Call Control Protocol）は、Arubaモビリティ・コントローラー内で実行されます。また、Arubaのアプリケーション・フィンガープリンティング・テクノロジーにより、モビリティ・コントローラーは暗号化された信号プロトコルは、Arubaモビリティ・コントローラー内で実行されます。

これらのストリームが特定されると、無線チャネルでの配信と音声関連機能のトリガーのために、Aruba WLANはそれぞれに優先順位を付けます。

これらの音声関連機能には、通話時間のARMスキャニングを延期するコマンドや、アクティブ通話でエンゲージされたクライアントのローミングに優先順位を付けるためのコマンドを含めることができます。これは、Wi-Fiを利用したエンタープライズ音声コミュニケーションの大規模な配備を実現する上で重要です。

さらに、ArubaOSにはデバイス・フィンガープリンティング・テクノロジーも搭載されました。ネットワーク管理者は、アプリケーションやユーザーだけでなく、デバイス・タイプに基づくネットワーク・ポリシーも割り当てることができます。デバイス・フィンガープリンティングは、ネットワーク・アクセスが許可されるデバイスと、それらのデバイスの使用方法に対するコントロールを提供します。

ArubaOSは、Apple iPad、iPhone、iPodなどのモバイル・デバイスや、AndroidまたはBlackBerryオペレーティング・システムを実行しているデバイスを正確に特定、分類できます。この情報は、ロケーションやモバイル・デバイスを問わない、すべてのネットワーク・ユーザーのネットワーク可視性を高めるためにAirWaveと共有されます。

コンテキスト・アウェアな制御ネットワーク	
T-SPEC/TCLAS	対応
WMM	対応
WMM優先度マッピング	対応
U-APSD (Unscheduled Automatic Power-Save Delivery)	対応
効率的なマルチキャスト配信のための IGMPスヌーピング	対応
アプリケーションとデバイスのフィンガープリンティング	対応

認定

- Wi-Fi Alliance認定（802.11a/b/g/n/d/h/ac、WPA™ Personal、WPA™ Enterprise、WPA2™ Personal、WPA2™ Enterprise、WMM™、WMM Power Save）
- FIPS 140-2検証（FIPSモード実行時）
- Common Criteria EAL-2
- RSA認定
- Polycom/Spectralink VIEW認定
- USGv6ファイアウォール

対応している規格

一般的なスイッチングとルーティング

- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2236 IGMPv2
- RFC 2328 OSPFv2

- RFC 2338 VRRP
- RFC 2460 Internet Protocol version 6 (IPv6)
- RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
- RFC 3220 IP Mobility Support for IPv4 (部分的サポート)
- RFC 4541 IGMP and MLD Snooping
- IEEE 802.1D-2004 – MAC Bridges
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.1w – Rapid Spanning Tree Protocol

QoSとポリシー

- IEEE 802.1D – 2004 (802.1p) Packet Priority
- IEEE 802.11e – QoS Enhancements
- RFC 2474 Differentiated Services

無線

- IEEE 802.11a/b/g/n/ac 5 GHz、2.4 GHz
- IEEE 802.11d Additional Regulatory Domains
- IEEE 802.11e QoS
- IEEE 802.11h Spectrum and TX Power Extensions for 5 GHz in Europe
- IEEE 802.11i MAC Security Enhancements
- IEEE 802.11k Radio Resource Management
- IEEE 802.11ac Enhancements for Very High Throughput
- IEEE 802.11n Enhancements for Higher Throughput
- IEEE 802.11v Wireless Network Management (部分的サポート)

管理とトラフィック分析

- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 854 Telnet client and server
- RFC 783 TFTP Protocol (リビジョン2)
- RFC 951 Bootstrap Protocol (BOOTP)
- RFC-1542 Clarifications and Extensions for the Bootstrap Protocol
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 1591 DNS (クライアント・オペレーション)
- RFC 1155 Structure of Management Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212 Concise MIB definitions.
- RFC 1213 MIB Base for Network Management of TCP/IP-based internets - MIB-II
- RFC 1215 Convention for defining traps for use with the SNMP
- RFC 1286 Bridge MIB
- RFC 3414 User-based Security Model (USM) for v.3 of the Simple Network Management
- RFC 1573 Evolution of Interface
- RFC 2011 SNMPv2 Management Information Base for the Internet Protocol using SMIv2
- RFC 2012 SNMPv2 Management Information
- RFC 2013 SNMPv2 Management Information
- RFC 2578 Structure of Management Information Version 2 (SMIv2)
- RFC 2579 Textual Conventions for SMIv2
- RFC 2863 The Interfaces Group MIB
- RFC 3418 Management Information Base (MIB) for SNMP
- RFC 959 File Transfer Protocol (FTP)
- RFC 2660 Secure HyperText Transfer Protocol (HTTPS)
- RFC 1901 1908 SNMP v2c SMIv2 and Revised MIB-II
- RFC 2570, 2575 SNMPv3 user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2233 Interface MIB
- RFC 2251 Lightweight Directory Access Protocol (v3)
- RFC 1492 An Access Control Protocol, TACACS+
- RFC 2865 Remote Access Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 3576 Dynamic Authorization Extensions to remote RADIUS
- RFC 3579 RADUIS Support For Extensible Authentication Protocol (EAP)
- RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
- RFC 2548 Microsoft RADUIS Attributes
- RFC 1350 The TFTP Protocol (リビジョン2)
- RFC 3164 BSD System Logging Protocol (syslog)
- RFC 2819 Remote Network Monitoring (RMON) MIB

セキュリティと暗号化

- IEEE 802.1X Port-Based Network Access Control
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 2104 Keyed-Hashing for Message Authentication (HMAC)
- RFC 2246 The TLS Protocol (SSL)
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 ESP DES-CBC cipher algorithm with explicit IV
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2407 IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 Internet Key Exchange (IKE) v1
- RFC 2451 The ESP CBC-Mode Cipher Algorithms

- RFC 2661 Layer Two Tunneling Protocol “L2TP”
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 3079 Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)
- RFC 3162 Radius over IPv6
- RFC 3193 Securing L2TP using IPsec
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3706 Dead Peer Detection (DPD)
- RFC 3736 DHCP Services for IPv6
- RFC 3748, 5247 Extensible Authentication Protocol (EAP)
- RFC 3947 Negotiation of NAT-Traversal in the IKE
- RFC 3948 UDP encapsulation of IPsec packets
- RFC 4017 EAP Method Requirements for Wireless LANs
- RFC 4106 GCM for IPSEC
- RFC 4137 State Machines for EAP Peer and Authenticator
- RFC 4306 Internet Key Exchange (IKE) v2
- RFC 4793 EAP-POTP
- RFC 5246 TLS1.2
- RFC 5247 EAP Key Management Framework
- RFC 5281 EAP-TTLS v0
- RFC 5430 Suite-B profile for TLS
- RFC 6106 IPv6 Router Advertisement Options for DNS Configuration
- IETF Draft RadSec – TLS encryption for RADIUS

a Hewlett Packard Enterprise company

日本ヒューレット・パッカード 株式会社　〒136-8711　東京都江東区大島 2丁目2番1号
1.844.473.2782 |電話：(03) 5749-8372|（カスタマーインフォメーションセンター）

www.arubanetworks.com/ja/