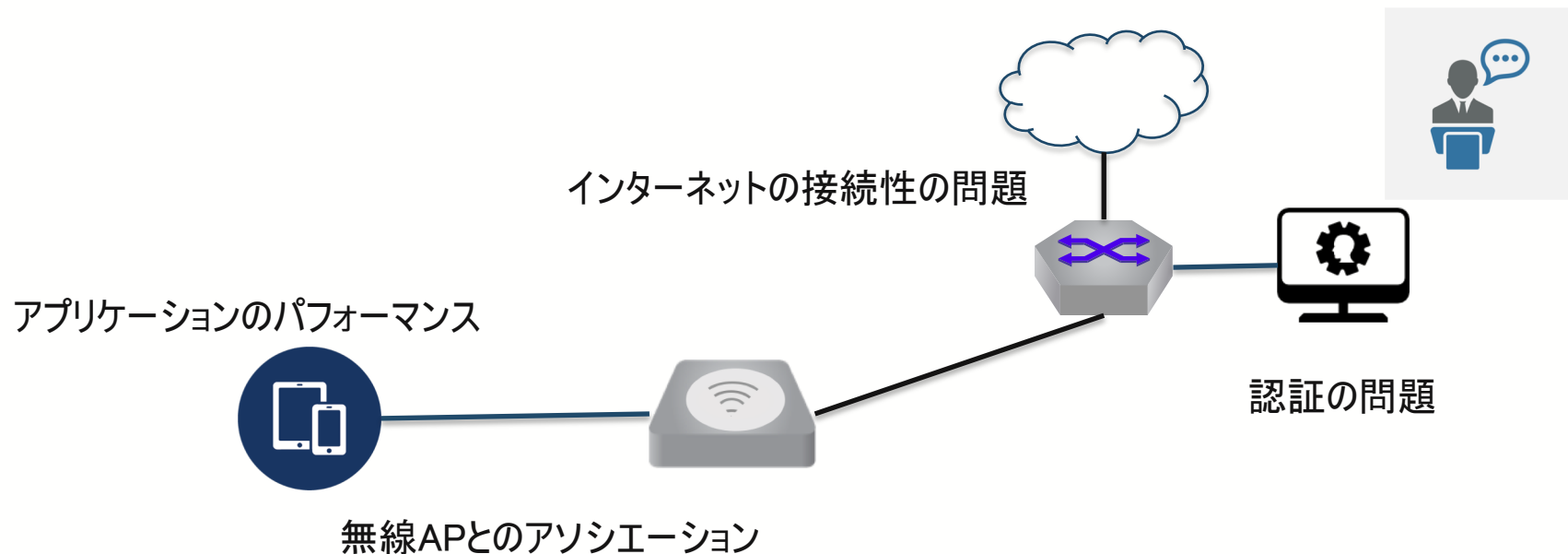


WiFiのトラブルシューティングをどうやるのか？ -How to resolve WiFi Trouble-

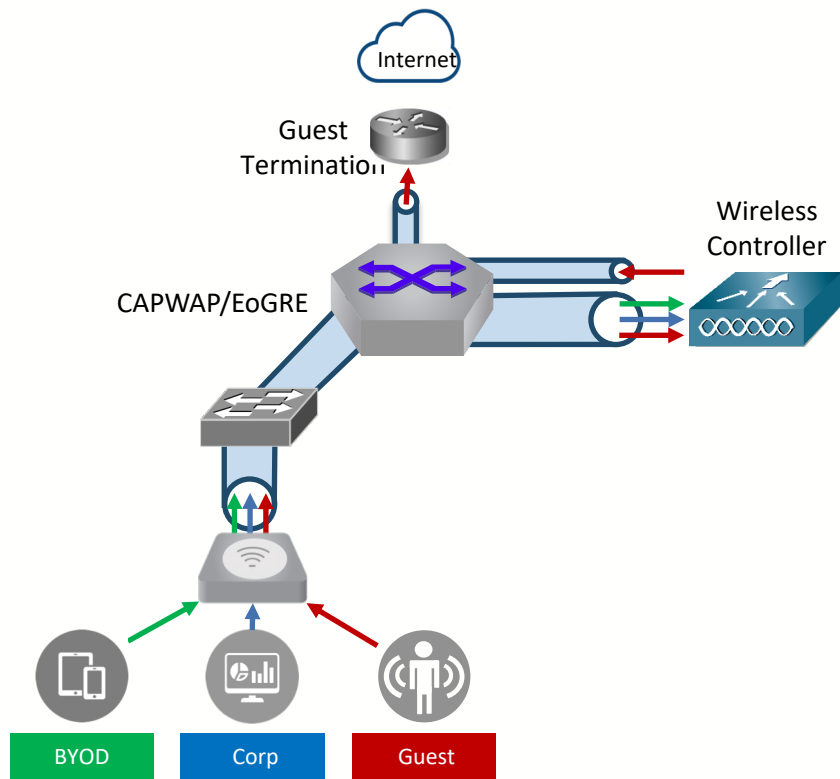
Shishio Tsuchiya
shtsuchi@arista.com

WiFiでつながらない！ときに何が考えられるか？



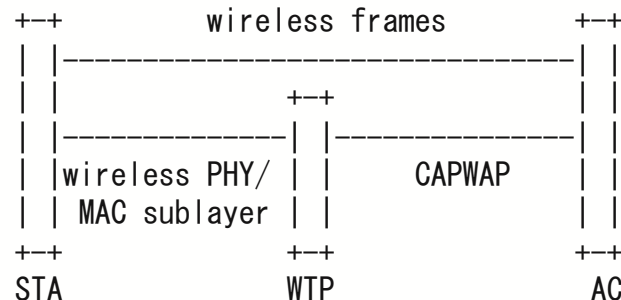
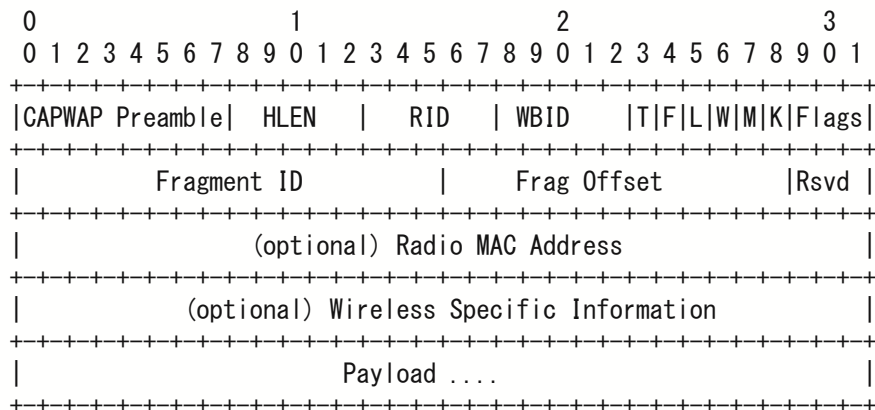
- 非常に普及をしているので、繋がらない!!にも色々の種類が
- トラブルシューティングも大変

典型的なWiFiネットワーク



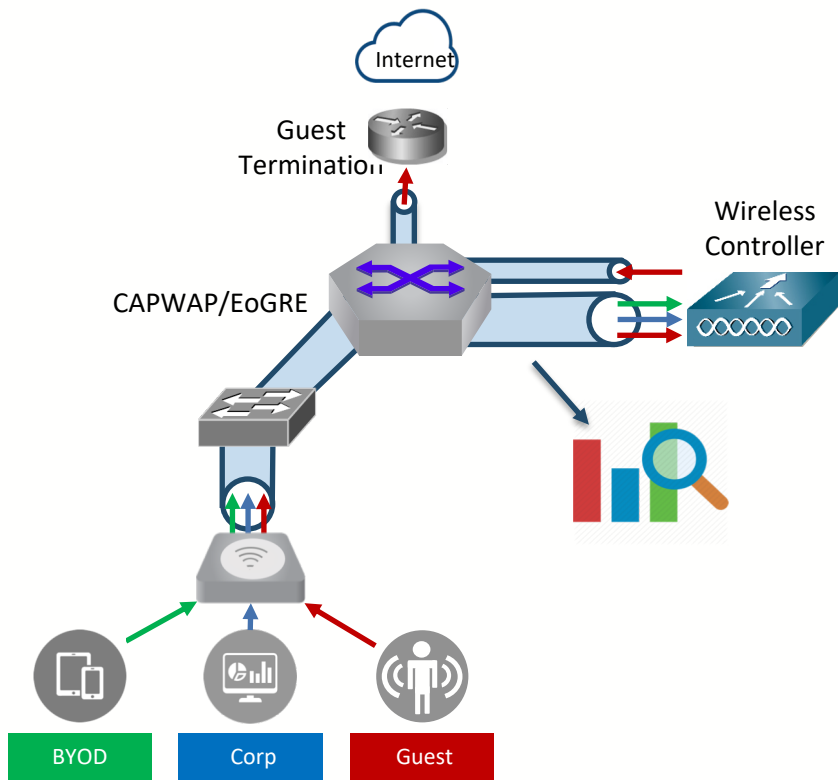
- APからワイヤレスコントローラーまでトンネルプロトコル(EoGRE/CAPWAP)が使用され、イーサネットフレームを運ぶ
- 解析に特化させる為にはそれなりのコストも必要

CAPWAP(Control And Provisioning of Wireless Access Points)Protocol



- CAPWAPはRFC5415でプロトコル仕様を定義
- しかしLWAPP(RFC5412)やEoGREなど未サポートベンダー/バージョンでの展開も多い
- 独自のコントローラーとAPのサポートになるため、コスト増が大きい

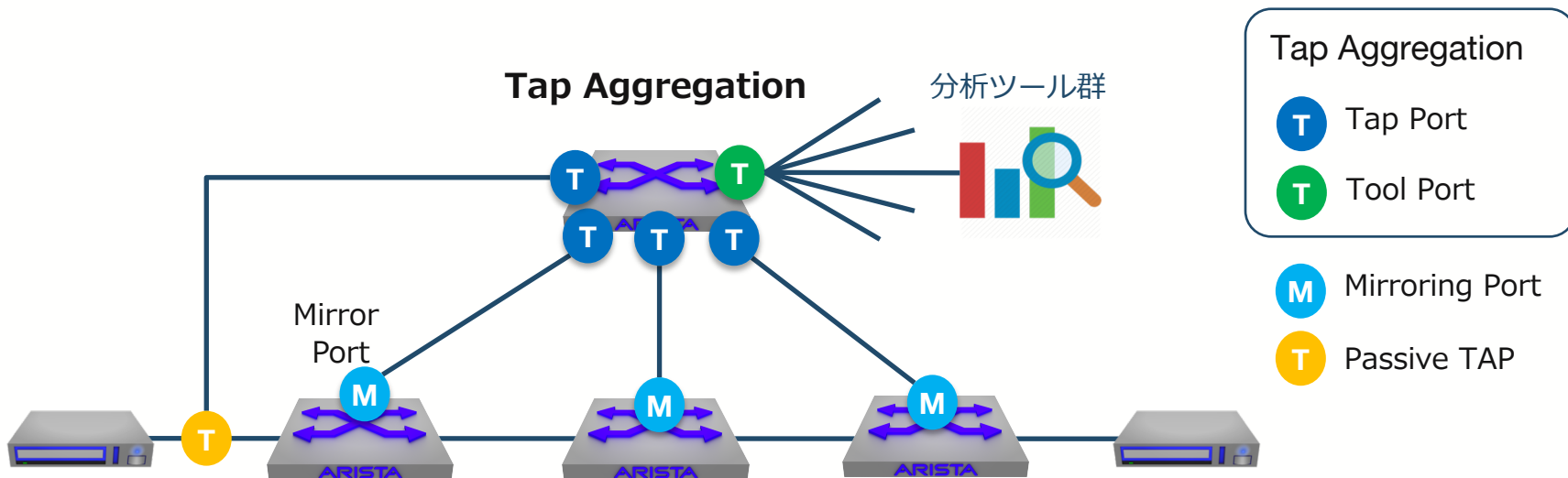
Packet Monitoring for WiFi Access



- 高精度のモニタリング装置に実データを転送するためには各カプセリングプロトコルを理解して、その後続くパケット毎にステアリングする様な機能が必要

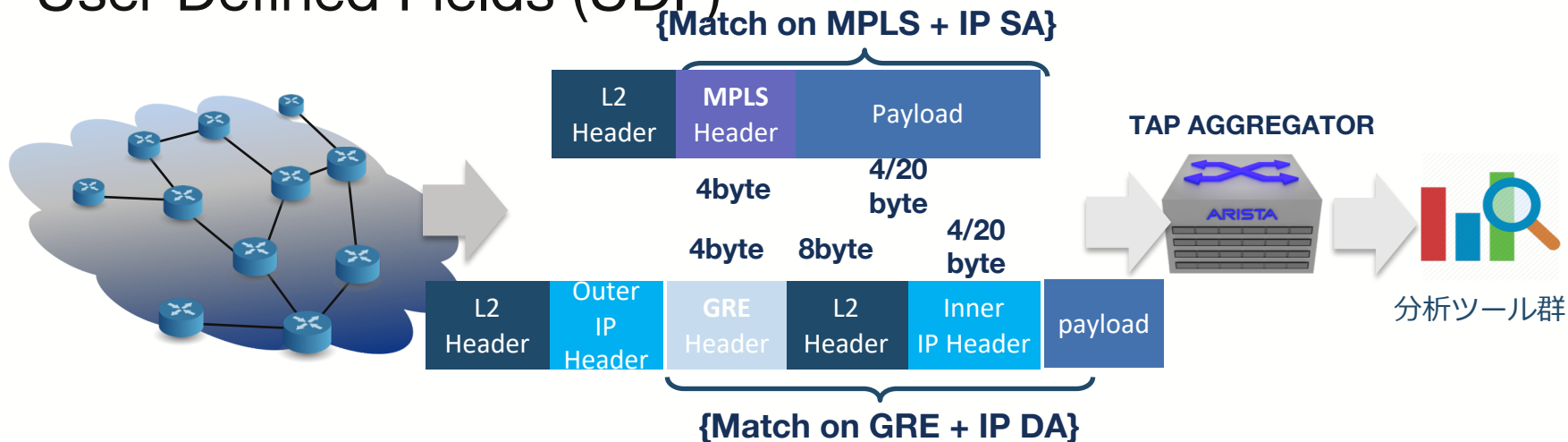
Tap Aggregation

- タップまたはミラーリングされたデータの集約と分析ツールへのデータ転送
- 分析ツールへの投資を最小限に



DPIを利用したトラフィックステアリング

User Defined Fields (UDF)



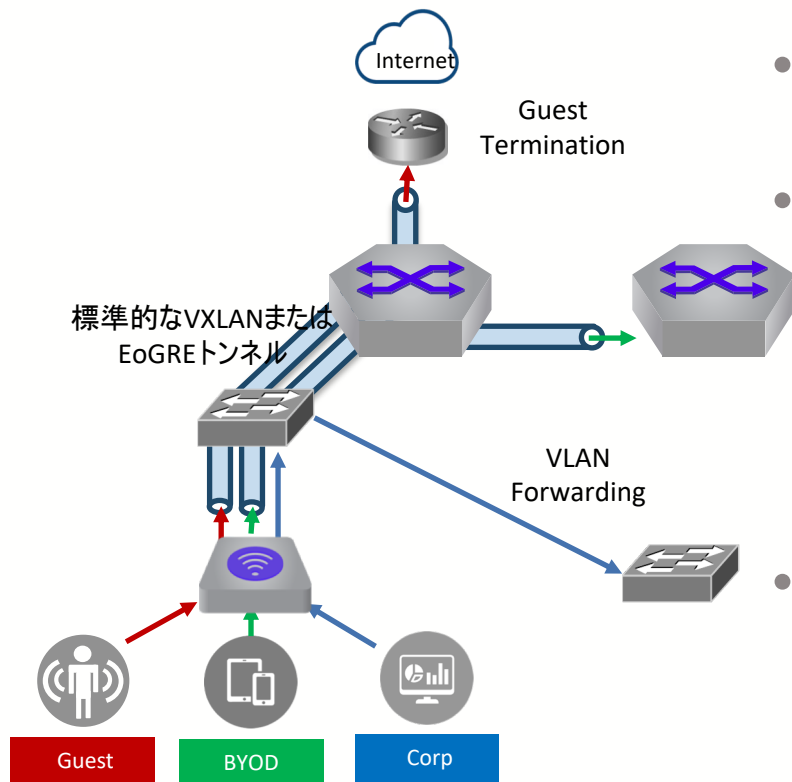
課題

- サービスプロバイダネットワークでは、任意のヘッダオフセットを利用したステアリングが期待される
- たとえば、MPLSやGREでカプセルリングされたパケットのヘッダ情報を削除することなくステアリング

ソリューション

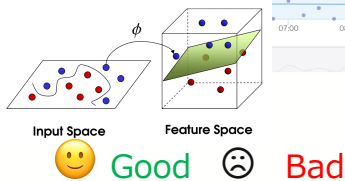
- Ethernet/IPヘッダ以降の任意のバイトにマッチするパケットを処理対象可能
- MPLS、VXLANやGREにカプセルリングされたパケットの内部ヘッダのマッチング
- MAC/IP ACLで4byteおき、128byte目までのフィールドをチェック可能

コントローラーレスのWiFiネットワーク



- それぞれのAPが自律的にネットワークを構成し、トンネルレスで動作する
- ゲストアクセスなど制限したネットワークアクセスはワイヤレスに特化させずに、標準的なVXLANやEoGREで集中させれば良いが、基本的には分散されたトラフィックになり、管理がしにくくなる
- =>各APがモニターシステムにPush型で通知するTelemetryタイプのアーキテクチャーが必要

コントローラーレスの解析



- APから集積したテレメトリデータを解析
- アソシエーション/認証/プロトコル/アプリケーション/端末レベルでのエラー表示
- マシンラーニングによるアノマリ検知

データ	周期/間隔
300以上の KPI	間隔 (15mins)
詳細なクライアントのログ	リアルタイム
アプリケーション分析	間隔 (15mins)
端末に関する分析	端末がAPから接続解除時
端末の可視化分析	1分単位のRSSIサンプル
APイベントログ	リアルタイム
AP デバッグログ	オンデマンド

まとめ

- WiFiトラブル解析の手法に関して共有
 - TapAggを使ったコントローラー型のDPIステアリング
 - コントローラーレスWiFiのテレメトリー型解析



Thank You

www.arista.com