

株式会社トライアルカンパニー御中

次世代店舗ネットワーク設計 Phase1 経過報告

T.Kashiwagi <t.kashiwagi@parallel-networks.com>

改版履歴

2024/12/25 初版

2024/12/29 体制周辺記述

2024/12/31 実機による実験結果をもとに追記

2025/1/3 全体調整

契約期間・会議体

- 2024/10/01-2024/12/31
- 週次スプリントミーティング@オンライン
- 月次ミーティング@多の津
 - 宮若参加
- 参加メンバ

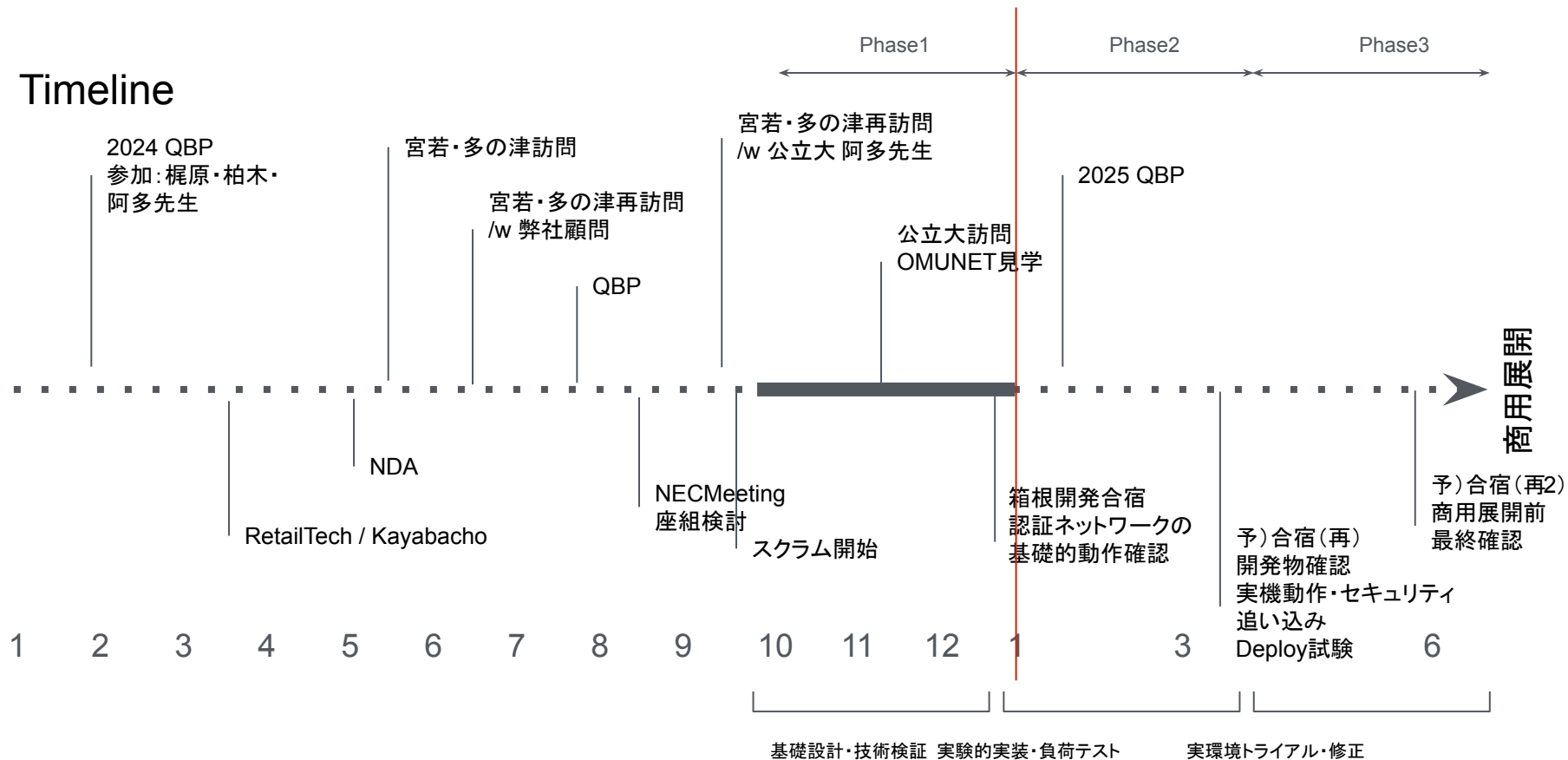
トライアル(以降 T社: 敬称略)

- 梶原
- 秋竹
- 高橋
- 渡邊

パラレルネットワークス(以降 P社: 同敬称略)

- 柏木
- 大阪公立大 阿多先生 連携
- 他非同期フォロワー3名(板橋・内田・眞鍋)
- 顧問(加納)への定期報告
- 関係各所調整(担当: 阿部)

Timeline



基礎設計概要 - これまでの意見召請と調査検討結果

-
- 店舗フォーマットごとに異なる目標値
 - 全体として 3000万デバイスへの対応
 - 見える化できていない
 - つながるべきでない端末がつながっていたことも散見される(SSID、PSKの漏洩、ポート接続ミス)
 - BCPを維持したい
 - ある地方や店舗で生じた問題を他サイトに影響させない
 - 店舗増大に対してスケールメリットのある構成
 - WiFi(Meraki)への強い依存、このままでスケールできない
 - 業務系、決済系、情報系それぞれの分離
 - DHCPの安定性が低い
 - 災害時のバックアップ通信路確保
 - これまでも分離はしていたがトラブル時の迅速さが必要
 - SSCの通信状態を可能な限りベストに維持したい
 - キットティングの負荷軽減
- 全端末を認証して接続するネットワーク。PSKは使用しない。
 - アプリケーションごとのネットワーク管理
 - 性能優先を定義する
 - LLDP/SNMP/nmapによる常時スキャン、監視
 - アドレスやVIDには意味を持たせない。状況をあとからでも「追える」ことを重視する
 - ソフトウェアによる自動設定、自動監視、自動運用。
 - ワイヤレフトフォワーディングが必要な部分以外ではアプライアンスを使用せず、OSSの組み合わせで性能や信頼性を担保する。
 - ソフトウェア化が可能ならば、中央集権しなくてよい。地理的なサイトに分離し、データのレプリケーションによってサイトごとに運用管理する。ログは中央にバックアップされ、分析される。
 - 小規模店舗は近隣の大規模基幹店舗の出先、場所の違う出張先商品棚、という扱いになる。コンピューティングは配置せず、ネットワーク機材のみで実現し、基幹店舗とL2接続する。これによりコスト最適化を図る

最初に解決すべき課題: スケーラビリティの確保

- T社店舗展開戦略においては、MEGAまたはSCを中心としてサテライトのGo(都市型または住宅地型)を展開する流れ
- 店舗展開のベロシティの確保が最大優先。
- 店舗それぞれごとに職人の手仕事でキッティングしては展開スケジュールに間に合わない。
- PowerONと同時に自動設定が行われる、本部キッティングもなしでDeployでいきなりZTPできることが必要。
 - ZTPはMACアドレスが判別できれば実現可能
- [NetworkCI/CD] ZTPが可能となることは、障害時対応も予備機を現地側で入れ替えるだけで済む、再起動時には毎度CIが実施されるのと同じであり、運用監視は継続的なテストとみなすことができる。
- スケールのため、小規模店舗はL2(VPN)運用、ネットワーク装置のみをDeployする。
- BCPを考慮してSCごとにL3を分離運用し互いの通信は行わず、センタAPとのみZeroTrustシステムとして通信する。
- 分散拠点のソフトウェア配信にはこれまでに大きな実績のあるRDBMSレプリケーションを用いることで極めて高いスケーラビリティを確保する。
- 回線開通は時間がかかることが多いため、SIM/StarlinkでDeploy開始してハンドオーバーさせる。クイックな回線業者を選定することも重要
 - Deploy初期段階はWiFiを使用してスピードを上げ、その後有線にできる部分を配線オフロードしていく

セキュリティ

- 業務用全端末は認証され、アプリケーションごとに分離されたネットワークに接続される。
- EAP可能な端末はEAPによる
 - EAP-PEAP
 - EAP-T/TLS
 - EAP-SIM
- モビリティ性向上、IoT収容のため、RADIUS Proxy によるMAC認証を組み合わせる
- 認証に使用するデータはすべて中央で管理されてサイトには準リアルタイムで配信される
 - 想定されない端末は接続できない
 - 同じくCI/CD
 - DBレプリカがよいか、gitなどのTextlによる差分系がよいか
- ログは逆にLogShipperを通じて中央側に準リアルタイムで同期され、分析、改善に供される
- SSC(決済)などリアルタイム系通信が必要なものは、PrivateLTE(1.9GHz)、6GHz、60GHzなどの綺麗な帯域を選択することが必要な場面がある

コストパフォーマンス

- OpenのswitchNOSはCumulus有力だったが残念ながら将来がない。
 - VXは現時点では提供されているが、いつなくなるかわからない。
 - 保守は必要ないが冗長化は必要
- 業界としてはSONiCになっているが、Cloudで使う方向に全振りしていて、エッジのDeployについては明らかに考慮されていない。
- OVSでLinuxのままvxlanオーバレイか、VyOSで収容しても大きなパフォーマンス問題にはならないとは思える
 - 性能、L3冗長化検証実施必要
 - https://qiita.com/hum_op/items/cb649d53ffd10c2ae3ab
 - VyOSはなくなることはないが、ローリングアップデートになったので、都度自動試験を回して投入可能性を検証必要
- WLANでなくてよいものは、有線に倒す。
 - Deploy初期段階ではWLANはスピードが出せるので良い
 - しかし装置は高い傾向なのと無線帯域が汚れていることが多いこと、DFSなど特有事情で、DHCPなどの失敗要因にもなっている。
 - FailSafeWLANは現時点ではなさそうだが、主計にうまく接続できなかった時のためのセカンダリのWLANを検討したい。
 - トラフィックが多いカメラなどについては徐々に有線PoEに移行するのが推奨
 - RPIなどWLANを持っていてかつ有線接続可能なものでAPを自製で作ってしまう方法もある
 - 電波は範囲を小さく、高密度に色分けすることが重要
 - <https://forums.raspberrypi.com/viewtopic.php?t=302174>
 - いろいろご意見はあるようですが、アンテナで調整するというハードモードでもあるにはある気はします。

Networking Software

- RADIUS
- RADIUS Proxy
- RDBMS Replication
- DNS/DHCP/NAT
- nmap/SNMP/LLDP
- rsyslog
- FileBeat/ElasticSearch
- Zabbix/Prometheus
- Ansible/git/GitLab CICD
- VyOS/OpenVSwitch
- Proxmox/Docker/LXC/LXD
- EventEngine: conductor/StackStorm

freeRADIUS



帰結 - 認証ネットワーク

認証されたデバイスが、機械的に、Codeやデータをもとに正しいネットワークに接続される
認証されないデバイスについても、優先度の低い通信として検疫ネットワークへの接続は許容する

正しく接続されたことがログから(機械的に)探索可能であるシステム

LLMでネットワークの正常性を検証し続けられるシステム (Stay SMALL Team)

基本骨格はOMUNETで実現されていることだが、コアの分散化、高速 Deploy、現代的冗長機能についての
開発・検証が必要

実験実施

12/18-20

大阪公立大協力のもと、箱根にて専用装置における
実験を行った。

実施構成:

RT NEC IX,

SW APRESIA GM200, NEC QX, YAMAHA SWX3k

FreeRADIUS/MariaDB/DHCP

実施結果:

YAMAHA SWX はMAC認証時にセキュリティ問題があると思われる。

QXは想定動作をしなかったが、原因は明らかでない。

APRESIA良好動作、ただしハンドオーバについては時間都合
で実施できなかった

IXのsyslog がFloodしていたが設定調整を行った

課題:

MAC認証がうまく動いていたかしっかり確認できなかった

ハンドオーバ実験の時間が足りなかった

ログを検討する時間が取れなかった

12E 時点進捗

- 今回試行した認証NWをソフトウェア含めて手元で再現する (TRIAL/PNL)
- OMU構成をリファレンスとしてRADIUS/DHCP/RDBを使用。
- PNLで実施したのは右構成
 - フィジビリティとして現時点ではRDB使用せず
 - 有線無線両系でハンドリングしやすいと思われるxAPとして RBD53iG-5HacD2HnDを選定した。
 - 4 Core ARM
 - 256Mメモリ
 - Docker対応 (radius/dhcpdくらいならenv可能)
 - DN/監視系 (Yellow) については既設線とし、全機材MGMT (Green) を設置
 - Syslog
 - NTP
 - SNMP/LLDP
 - SSH
 - RADIUS用ネットワーク (Red) を張り出し、それぞれ直結した。
 - Datapath (EAPoL) 用には専用のL2を設置 (Blue) し、VRFを分離した



RADIUS

user1 Cleartext-Password := "user1user1"

Tunnel-Type = 13,

Tunnel-Medium-Type = 6,

Tunnel-Private-Group-ID = "10",

Mikrotik-Wireless-VLANID = 10,

Mikrotik-Wireless-VLANID-type = 0

user2 Cleartext-Password := "user2user2"

Tunnel-Type = 13,

Tunnel-Medium-Type = 6,

Tunnel-Private-Group-ID = "20",

Mikrotik-Wireless-VLANID = 20,

Mikrotik-Wireless-VLANID-type = 0

user3 Cleartext-Password := "user3user3"

Tunnel-Type = 13,

Tunnel-Medium-Type = 6,

Tunnel-Private-Group-ID = "30",

Mikrotik-Wireless-VLANID = 30,

Mikrotik-Wireless-VLANID-type = 0

AP/wired Bridge

VID	GW/DHCP	AP/wired Bridge
10	10.64.10.254/24	-
20	10.64.20.254/24	-
30	10.64.30.254/24	-
RADIUS	-	10.90.9.116/24
1(MGMT)	10.64.88.253/24	10.64.88.254/24

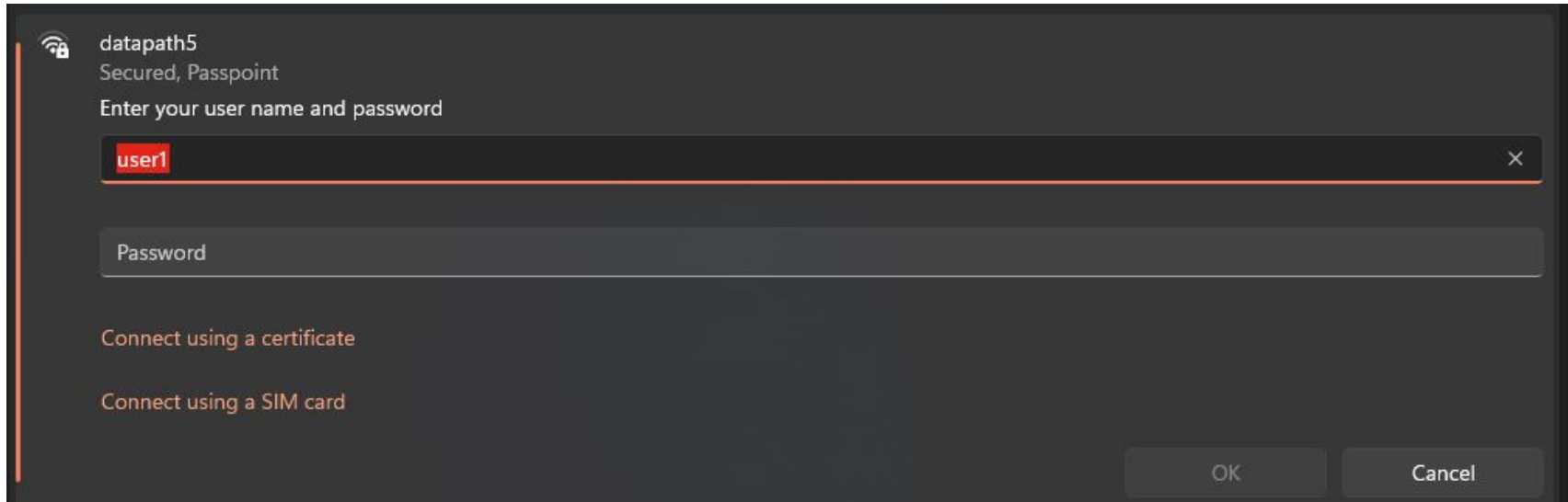
実施結果 - 大体よさそうな構成は判明した


DynamicVLAN(dot1X/ not MAC)	成功 (SVLANまで実施。並列接続は 3まで実施) MAC検証は実施必要あり	VIDがTrunkで動的に張り出される
WLAN+ DynamicVLAN	同上	VIDがTrunkで動的に張り出される
動的PortVLAN	未検証	
Windows直結	未実施	柏木PCのWindows WiredDriverがVLAN対応していない模様
認証失敗時	WLAN: 別のKnownWLANに接続される	LAN:EAPoL以外のパケット導通せず
検疫ネットワーク	未検証	
ログ分析	未検証	
DHCP/RADIUS/NAT/DNS他syslog突合	未検証	
VLANフィルタ	未検証	
Windows@WLAN	良好動作(ただし証明書系を無視している)	
Android@WLAN	良好動作(ただし証明書系を無視している)	
iOS@WLAN	うまくつながらない。OWEにもうまくつながらないので、AP側の設定かもしれない	おそらく証明書を綺麗に作らないと受け入れてくれない
macOS@WLAN	未検証	もっていない
ハンドオーバー検証	未検証	同じ機材が 2台無かった(箱根で大井君にあげてしまった)
優先制御	未検証	

動的なVID Trunk

```
Last login: Fri Jan 3 17:04:42 JST 2025 on pts/1
root@pve:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master vmbr0 state UP group default qlen 1000
    link/ether 00:90:0b:86:65:92 brd ff:ff:ff:ff:ff:ff
3: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master vmbr1 state UP group default qlen 1000
    link/ether 00:90:0b:86:65:93 brd ff:ff:ff:ff:ff:ff
4: enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:90:0b:86:65:94 brd ff:ff:ff:ff:ff:ff
5: vmbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:90:0b:86:65:92 brd ff:ff:ff:ff:ff:ff
    inet 10.90.9.9/24 scope global vmbr0
        valid_lft forever preferred_lft forever
6: vmbr1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:90:0b:86:65:93 brd ff:ff:ff:ff:ff:ff
7: veth102i0@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master vmbr0 state UP group default qlen 1000
    link/ether fe:b9:4d:8e:61:20 brd ff:ff:ff:ff:ff:ff link-netnsid 0
8: veth103i0@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master vmbr0 state UP group default qlen 1000
    link/ether fe:c8:cl:57:79:a5 brd ff:ff:ff:ff:ff:ff link-netnsid 1
9: enp4s0.10@enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:90:0b:86:65:94 brd ff:ff:ff:ff:ff:ff
    inet 10.64.10.251/24 brd 10.64.10.255 scope global dynamic noprefixroute enp4s0.10
        valid_lft 301sec preferred_lft 226sec
root@pve:~#
```

```
9: enp4s0.40@enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:90:0b:86:65:94 brd ff:ff:ff:ff:ff:ff
root@pve:~# dhcpcd enp4s0.40
dhcpcd-9.4.1 starting
DUID 00:04:03:00:02:00:04:00:05:00:06:00:07:00:08:00:09
enp4s0.40: IAID ff:00:00:28
enp4s0.40: adding address fe80::1093:1234:df7f:7e70
ipv6_addaddr1: Permission denied
enp4s0.40: soliciting an IPv6 router
enp4s0.40: soliciting a DHCP lease
enp4s0.40: offered 100.65.40.1 from 100.65.40.254
enp4s0.40: probing address 100.65.40.1/24
enp4s0.40: leased 100.65.40.1 for 600 seconds
enp4s0.40: adding route to 100.65.40.0/24
enp4s0.40: adding default route via 100.65.40.254
forked to background, child pid 8748
root@pve:~# ip r
default via 10.90.9.254 dev vmbr0 proto kernel onlink
default via 100.65.40.254 dev enp4s0.40 proto dhcp src 100.65.40.1 metric 1009
10.90.9.0/24 dev vmbr0 proto kernel scope link src 10.90.9.9
100.65.40.0/24 dev enp4s0.40 proto dhcp scope link src 100.65.40.1 metric 1009
root@pve:~#
```

 datapath5
Secured, Passpoint
Enter your user name and password

user1

Password

Connect using a certificate

Connect using a SIM card

OK Cancel

IP assignment:	Automatic (DHCP)
DNS server assignment:	Automatic (DHCP)
SSID:	datapath5
Protocol:	Wi-Fi 6 (802.11ax)
Security type:	WPA3-Enterprise
Manufacturer:	Intel Corporation
Description:	Intel(R) Wi-Fi 6E AX211 160MHz
Driver version:	23.100.0.4
Type of sign-in info:	Microsoft: Protected EAP (PEAP)
Network band (channel):	5 GHz (36)
Aggregated link speed (Receive/ Transmit):	360/544 (Mbps)
IPv4 address:	10.64.10.250
IPv4 default gateway:	10.64.10.254
IPv4 DNS servers:	10.64.10.254 (Unencrypted) 10.90.9.254 (Unencrypted) 8.8.8.8 (Unencrypted)
Physical address (MAC):	68-C6-AC-09-52-04

複数同時のVLANトラフィック

<input type="checkbox"/>	R	— 3E trunk-brid...	Bridge	1500	1598	259.9 Mbps	1884.4 kbps	22 097	2 888	259.1 Mbps	1884.1 kbps
<input type="checkbox"/>	R	↻ tv10	VLAN	1500	1594	227.8 Mbps	1077.9 kbps	19 405	1 605	227.2 Mbps	1077.9 kbps
<input type="checkbox"/>	R	↻ tv20	VLAN	1500	1594	1104 bps	0 bps	1	0	0 bps	0 bps
<input type="checkbox"/>	R	↻ tv30	VLAN	1500	1594	31.7 Mbps	721.3 kbps	2 719	1 296	31.5 Mbps	721.3 kbps
<input type="checkbox"/>	R	↻ v77	VLAN	1500	1594	0 bps	0 bps	0	0	0 bps	0 bps
<input type="checkbox"/>	X	3E wan1-brid...	Bridge			0 bps	0 bps	0	0	0 bps	0 bps

未検証だが早急に対処が必要と思われること

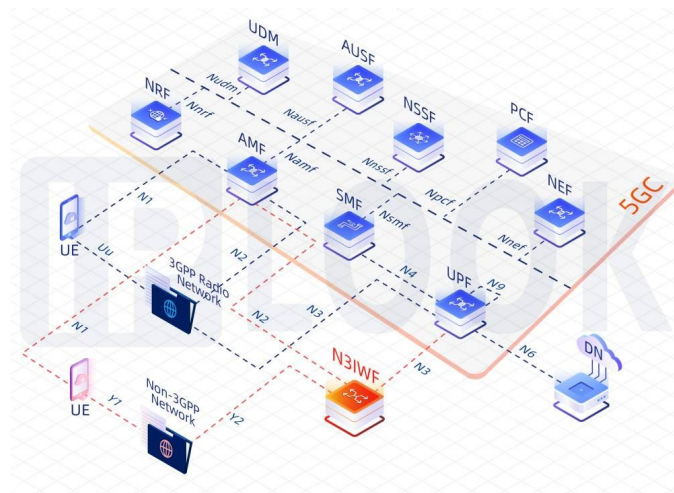
証明書系を今回投入していないが本来必要なので、真正な証明書を作成して投入実験が必要。
iOSがつかない問題の解消に必須と思われる。

参考:

https://www.marbacka.net/blog/freeradius_eap-tls_wi-fi/

5GC/N3IWF(柏木提案)

- これまでの技術では LANでエンドポイント認証し、特に通信制御はSTAを直接收容している多数の装置へ個別に実施する
- 通信要求に対してアンダレイネットワークが **充分に高速である** とき、RANに倣って、かつ non-3gpp(ETSI TS 124 502:別添参考物)收容を活用する手もある
 - モバイルネットワーク技術が、すべてのネットワークを飲み込むとき



一言でいえばクラウドネットワーキング→ 店舗では店舗内のマイクロクラウドネットワーキングにすればよい

従来ではキャリアによる閉域網回線ではできなかったことが3GPPによる5G(RAN/Core)のOpen化、およびセルラ網以外の收容性まで議論がされたこと、リファレンス実装も多数出たことによって、いまやローカルに構築できる。

(強力なポリシー) 網や端末の挙動、優先度を細かく制御することができる

キャリアの基地局は本当にただの無線局でパケット処理はしていない。パケットハンドリングはUPFおよび外側DNで実施

(強力な認証) SIMをベースとする認証管理が可能

(ハンドオーバ) AMFはN3IWFと連動する

注意: UEの実装については議論がある。時間が解決するかもしれないが、逆に言うところ研究として面白い。動作する 4G RAN/Coreは保持している。

昨年時点では末端のスイッチ内部に UE相当を配置し、必要に応じて OTA/OOBでSIMをプロビジョニングする方法を検討した。



**5G;
Access to the 3GPP 5G Core Network (5GCN)
via non-3GPP access networks
(3GPP TS 24.502 version 18.6.0 Release 18)**



How 5G & Wi-Fi Convergence Together - Introduction of ATSSS

Access Traffic Steering, Switching, and Splitting

In Release 15:

- 5GS support mobility between 3GPP & **untrusted non-3GPP access (#N3IWF)**.
- Each PDU Session is only active in one access at a given time. In other words, only one access type can be used, either 5G or untrusted Wi-Fi connection.

In Release 16:

- 5GS support **trusted** non-3GPP access & **wireline access (#TNGF, #TWIF, W-#AGF)**.
- Introduced **#ATSSS** enabling multi-connectivity simultaneously by using 3GPP access & non-3GPP access (trusted, untrusted, & wireline access).

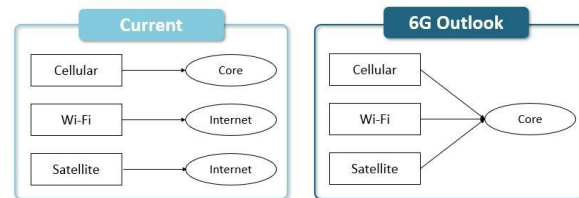
In Release 17:

- Enhanced **#ATSSS** (ATSSS_ph2) supporting (1). steering mode enhancement (2). MA PDU Session with a 3GPP access over EPC and a non-3GPP access via 5GC.

In Release 18:

- Enhanced **#ATSSS** (ATSSS_ph3) by studying key issues and investigating solutions: (1). support new higher-layer steering functionality (e.g., MPQUIC) for non-TCP traffic (e.g., UDP flow); (2). Support a redundant traffic steering to improve transmission reliability and reduce packet latency; (3). Support switch traffic of an MA PDU session between non-3GPP access paths; (4). Support MA PDU session with a non-3GPP access over EPC and a 3GPP access via 5GC.

Multi-Access Technologies Integration Into Single Mobile Core Network



[Source: CHT]

Non-3GPP Access Standardization Roadmap

		R15	R16	R17	R18
3GPP	5G supports non-3GPP access	Support untrusted non-3GPP access (#N3IWF)	Support trusted non-3GPP access (#TNGF, #TWIF) Support wireline access (#WAGF) Support ATSSS	Support ATSSS phase2	Support ATSSS phase3
	3GPP Reference Doc	TS 23.501 (v15)	TS 23.501, TS 23.502 (v16), TS 24.103 (v16), TR 23.793	TR 23.917, TS 23.502 (v17), TS 24.103 (v17), TR 23.790-95, SP-230591	TR 23.700-53, SP-231612, S2-23105753
ATSSS	Summary	NA	1 st introduce ATSSS enabling multiple data connectivity simultaneously (MA PDU Session) over 3GPP access & non-3GPP access	Specify the enhancement of ATSSS: • Steering mode enhancement • An MA PDU session with a 3GPP access path via EPC	Study key issues & investigate solutions: • new higher-layer steering functionality (MPQUIC) for non-TCP traffic (UDP flow) • redundant traffic steering • Switch traffic of an MA PDU Session between two non-3GPP access paths. • An MA PDU session with a non-3GPP access path via EPC
	Traffic Distribution	NA	MA PDU Session with: 1*3GPP access path via 5GC 1*non-3GPP access path via 5GC	MA PDU Session with: 1*3GPP access path via EPC 1*non-3GPP access path via 5GC	MA PDU Session with: 1*3GPP access path via 5GC 1*non-3GPP access path via EPC
	Steering Functionality	NA	• Higher-Layer steering functionality – MPICP for TCP traffic. • Lower-Layer steering functionality – ATSSS-LI for non-TCP traffic	NA	Higher-Layer steering functionality – MPQUIC for non-TCP traffic
	MA PDU Session Type	NA	• Support: IPv4, IPv6, IPv6 Ethernet type • Not Support: Unstructured type		?

知財候補？

(阿多先生ご提案: 柏木の検討が生煮え、まだ外に出せるレベルではない)

こちらはそもそも目標外だが、検討次第で成果にしたい目論見

DymanicVLAN可能な無線装置は高い、またはクラウドコントローラの系統→ 1X+MAC認証(W)LAN+DynamicVLAN Wired装置+自製Software

- a. クラウドコントローラではスケールしない(保守より予備機: 予備機のライセンスをずっと払い続けるのか?)
 - i. 監視自由度が低い(テレメトリが細かく取れない MISTでもどこにLogが出ているのかよくわかっていない)
 - ii. Logも想定したものが出ないことがある
- b. 詳細についてはこの先議論必要あり
 - i. 1X/MAC認証するがVLANをつけないWLAN装置はある。IPはFramedIPでアサイン可能?
 - ii. DyVLAN装置のポートにタグなしで到着したパケットのMACをもとに特定VLANへ再収容できるか?
(逆に言うと別VLANから来たパケットを別の特定VLANに混ぜながら再放流するというネットワーク的には美しい装置に見える。通常のネットワーク屋だとやらない気がする。探してみたがやはりなさそう) WLAN付け替え装置はある。AlaxalとかApresiaだとタグ変換のようだが、MACに頼って混ぜるとはやはり違う)
 - 1. そのような装置がいまなくとも作るのはできそう(研究&知財: どんな名前 DynamicMACVLANだと誤解しか生まない)
 - 2. 同時にスロットリングできてもいいだろう
 - iii. Wired区間を暗号化できないか?(暗号アルゴリズムを動的変更)
 - 1. 有線の暗号化トンネルなので、機器間でトンネル必要だが、通常のWired装置はそんなものは持たない
 - 2. hostapdを搭載しているSWなら可能性はあるがワイヤレート至上主義のdataplaneにそんな物載せる人はまずいない WLANのほうが誰でもものぞけるAirなので進んだということか、1暗号化だと光トランスポンダならば搭載例がある
 - 3. パスワードの必要ないOWEのような暗号化方式は取れないか?

Propose new Protocol for MACVLAN/tag mapping

- 世の中で一番MACVLANを使っているのはおそらくDocker
 - <https://docs.docker.com/engine/network/drivers/macvlan/>
 - <https://docs.docker.com/engine/network/tutorials/macvlan/>
- LXDでも同様
 - https://linuxcontainers.org/incus/docs/main/reference/network_macvlan/
- Uplinkにtagは投入できる
- セグメント間のトラフィックを混ぜる話は当然出てこない
- <https://suhu0426.github.io/Web/Presentation/20150203/index.html#macvlan>
- 上位L2のMACテーブルにかなり負荷がかかる。Linuxベースならばどうということもない
- ブロードキャスト問題
 - vxlanBUMトラフィックと同様の扱い
 - <https://www.infraexpert.com/study/virtual3.html>

通常のVLANさばき

MACをもとにVIDでカプセルして上位転送

認証したMACあてパケットの転送
ペイロードの暗号化

ブロードキャストについても
SrcMACを見て上位転送

no enc

New Tunnel

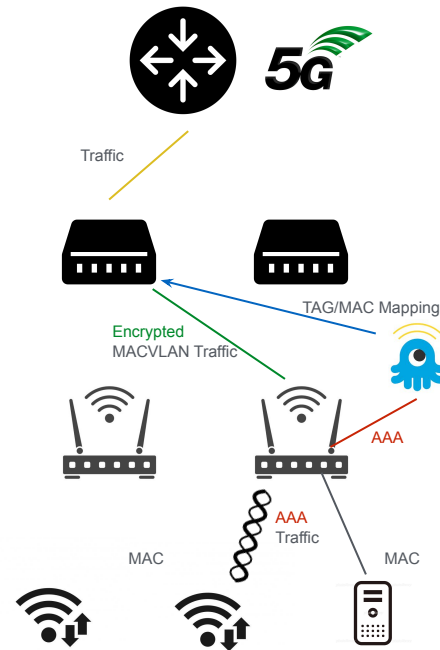
WPA3

manyTag/vxlan
| 5GC

1Seg/MACVLAN

1Seg/SSID

SimpleAuthBridge



AAA-ID	MAC	VID VNI PDU SessionID	PortID	Encryption Key	QueueID
--------	-----	---------------------------	--------	----------------	---------

今後の予定 - 商用に至るまで

3Eまで:現時点ではまだ確定していないパラメータを確定させる

- 12E未検証の項目をすべて検証し終わってしまう必要性→機材選定にかかわる
 - クリティカル。ここを早く終えないと次にいけない
- 店舗フォーマットに合わせたネットワーク構成のソフトウェア・ハードウェアの動作状態までもっていく(公立大と連携する)
- 無線の有り無しなども含める
(Goは無線LANは本当に要るか? :近い将来はPacerだけSIMでもなんとかなるという高橋意見がある。T社主導、我々チームで考える必要がある)
- 検疫ネットワーク、隔離方法の確定 トラブル時に使用できるHistory UI(阿多先生のUIが一番優れていると考えます)
- 機材選定:複数のIaC可能な機材を選定する(現時点ではApresia有力だが手元実績はまだない)
- クラウド管理系は本当に使用できるか? 災害時の挙動はどうなるか?
 - 基本的にはライセンス的考え方なので、多の津の意思には合わないのでは?
- セグメントの確定
- SSIDどれにするか、チャンネルはどこにするか。スイッチのポート実装ポリシー
- ログの調整:具体的に実施
LogStorage
- 監視項目の調整:具体的に実施

6Eまで:7月からの店舗展開開始までの予行

- 3E構成物のパイロット店舗での試行(問題があれば戻せる場所:粕屋、もう一つは宮田?)
- 運用設計
 - 通知
 - 対応確定
 - 連絡パス
- Deploy後の導通試験仕様の確定
- リモートサポートをどのように実施するか具体的に確定する
- DeploySpeedの向上:自動化
- MACアドレスのスキャン
- 既存の店舗にある既設の装置などのMACはどうやって収集するか?
 - 業者と直接話せるのがいいだろう
 - MACリストを納品物とすべき
 - CSVバルクローダの開発必要
- ケーブル色、太さ、タイプ仕様決め
- 実装ポリシーを確定する。サイクル化できるようにする

7月以降

月5店舗くらいのスピードで実装する必要がある。

毎週Deploy

初期段階は開発チームで実施する

トラブル時対応

共同研究 - 大阪公立大学

受入先: 阿多 信吾 教授

大阪公立大学 情報基盤センター センター長

大阪公立大学 学長補佐

大阪公立大学 大学院情報学研究科 副研究科長

研究分野 : 通信工学, 情報ネットワーク

ご連絡先: ata@omu.ac.jp

本件お問い合わせ先

support+trial@parallel-networks.com

office-admin@parallel-networks.com

Parallel Networks LLC.

203 Tensho-Takadanobaba bldg.

3-2 Takadanobaba

shinjuku-ku Tōkyō Japan

169-0075

+81-50-1742-2500

+81-70-9097-8007

EOF

