# **OpenWRTのVLANと複数SSID**

2024/11/1 作成者:sutinza

## 本資料の目的

昨今の在宅ワークの需要増加で家庭内においてもネットワークのセキュリティ確保を厳重に行う必要性が発生しつつある。 特に会社支給のPCというのは管理者であればほぼ自由に行えるがそのことが原因で各ユーザーのネットワークへの侵入も可能となっている。 企業の管理者側は大量の端末を管理しているので侵入されないとは思うが放置していても良いものではない。

RDPなどで会社の知らない人間に業務支給用PCを経由して自宅のNASやルータ、PCなどに接続されて気分のいい人間はまずいないだろうと思う。 「そんな暇あるかー!」という管理者たちの怒りや嘆きも聞こえてきそうだが、知らないうちに恨みなどを買ってしまうとそういかなくなるのが人間の性。

### 現状では企業の管理者の性善説に頼っているだけで保障は一切何もない。

その為、自宅内のネットワークでもセキュリティの向上化を行いプライベートな部分を保護する事とした。

いろいろな機能を希望すると民生品では出来ない事が多々出てくる。(業務用の機器を買えれば問題はないがランニングコストとか電力量増加とか・・・) 市販のワイヤレスルータのファームウェアではSSIDを1セグメントでしか利用できない。(そもそもVlanが利用できない) その為Vlan環境下ではセグメントごとにWiFi環境を提供しようとするとワイヤレスルータを複数台用意する必要が出てくる。 市販のワイヤレスルータのファームウェアでは無線LAN部分をPrivate用とGuest用で分割はできるもののあくまでもクライアント間通信無効は無線接続された機器間であり LAN内までは有効化されない。

以上のような背景からOpenWRTを利用しVIanでセグメメントを分割し複数のSSIDを利用する必要性が発生し本資料の作成に至った。

# 1. 現状の構成

現状の構成では各Vlan単位でアクセスポイントを 配置しSSIDを提供している。 1Vlanに物理の1アクセスポイントとなり無駄が多い。



# 1.1 目標の構成

OpenWRTを利用し各VLANと複数のSSIDを1台のアクセスポイントに集約する。 アクセスポイントからルータまではTrunkを行い物理配線を削減する。



# 2.検証環境の準備

検証機として余っていたNetgear社のWNDR4300を利用する。 Trunkの検証としてNetgear社のGS108Eを利用する。



図2-1 Netgear社のWNDR4300

検証環境として自宅で長年の間押し入れで眠っていた上記の2台を用意した。 WNDR4300にはOpenWRTをインストールしGS108EはVlanのTrunk検証を行う。 全体的なパラメーターは下記を利用する。

管理用セグメメント:	192.168.1.0/24
Vlan10 :	192.168.10.0/24
Vlan20 :	192.168.20.0/24
SSID : Private	Vlan10
SSID : Guest	Vlan20
Vlan10 Gateway :	192.168.10.254/24
Vlan20 Gateway :	192.168.20.254/24



図2-2 Netgear社のGS108E

# 2.1 検証用SWの設定

GS108Eに管理用IPを割り当てVlanとインターフェースの設定を行う

GS108Eのパラメーター ・ブートローダーバージョン: ・ファームウェアバージョン: ・管理用IPアドレス: ・管理用PCのIPアドレス: ・Vlan(VID): ・ポートメンバ:

V2.06.03 V2.06.24JP 192.168.10.243/24(Vlan10) 192.168.10.20/24 (Vlan10) Vlan1 Vlan10 Vlan20 ポート1 Trunk(UpLink用) ポート2 Trunk(アクセスポイント用) ポート3 Vlan10 ポート4 Vlan10 ポート5 Vlan10 ポート6 Vlan10 ポート7 Vlan20 ポート8 Vlan20 有効



・ループ検出

# 3. OpenWRTのアーキテクチャ

OpenWRTをインストールした直後のインターフェース構成は 図3-1のようになっている。 CPUとEthXは直結され **CPU内部にbr-lan(ブリッジデバイス)インターフェース** が存在する。 Switch0はEth0と接続され他のEthXには接続されていない。 Switch0には **仮想インターフェースLAN1~LAN4(物理デバイス数により変動)** が存在する。

各LAN1~LAN4は物理ポート(Port\_1~Port\_4)に接続されている。

Eth1は物理ポート(Port\_Wan)に接続されている。 Eht2はWiFi用で物理としては見えないがPort\_WiFiに接続されている。

この構成を把握していないとOpenWRTの設定はできない。 ※図3-1で示しているEthX名はメーカの設計などにより変動する。 またEth2のWiFiデバイス名はユーザ定義が可能である。



図3-1 インストール直後の基本的なOpenWRTの構造

# 3.1 OpenWRTのインストール

1.OpenWRTはファームウェアなのでTFTPを使いインストールする。 TFTPサーバソフトは各自で用意する。

2.Windows標準のTFTPクライアント機能の追加をしておく。 コントロールパネル→プログラムと機能→Windowsの機能の有効化または無効化 Windowsの機能で「TFTPクライアント」にチェックを入れ「OK」をクリックする。 これを行わないとTFTPコマンドをコマンドプロンプト上で実行できない。

3.OpenWRTのイメージファイルは公式サイトから入手する。 <u>https://openwrt.org/toh/netgear/wndr4300</u> openwrt-23.05.5-ath79-nand-netgear\_wndr4300-squashfs-factory.img

4.可能であれば念のためにメーカのファームウェアも確保。 https://www.netgear.com/support/product/wndr4300/#download WNDR4300-V1.0.2.104.img

5.OpenWRTイメージの転送準備 設定用PCのIPアドレスを「192.168.1.2/24」にしてWNDR4300背面の リセットボタン(RestoreFactorySettigs)を押しながら電源を投入する。 オレンジのLEDが点滅後グリーンのLEDで点滅を始めたらリセットボタンを離す。

グリーンのLEDが点滅中に下記のコマンドをコマンドプロンプトで実行する。 tftp -i 192.168.1.1 put openwrt-23.05.5-ath79-nand-netgear\_wndr4300-squashfs-factory.img 「正常に転送完了」 と表示されれば完了でWNDR4300が自動的に再起動する。

以上でファームウェアの書き換え作業は完了する。



### 図3.1-1 TFTPサーバソフトの設定画面



### 図3.1-2 TFTPクライアント機能の追加画面



図3.1-3 TFTPコマンドによるOpenWRTのインストール画面

# 3.2 OpenWRTの初期設定

※WNDR4300ではファームウェア書き換え直後はWiFiの5Gアダプタを見失っているので電源ケーブルを抜いて30秒程度待ってから再度起動する。

任意のブラウザで<u>http://192.168.1.1</u>へアクセスする。 ログインIDとパスワードは下記でログインする。 ユーザ:root パスワード: (空白)

ログインするとStatusページが表示され画面上部にパスワードを設定するダイアログが表示されるのでクリックしパスワードを設定する。 パスワード設定後は初期設定を行う。

System→System

Host name :	V
Description :	C
Timezone :	А

WNDR4300 OpenWRT Asia/Tokyo

「Save&Apply」をクリックして保存し反映させる。



### 図3.2-1 初回起動後は5Gインターフェースが存在しない

/NDR4300	Status 🗸	System - Network - Log out	REFRESHING UNSAVED CHANGES: 11
<b>ystem</b> ere you can config	gure the basic	c aspects of your device like its hostname or the timezone.	
ystem Prop	erties		
	Local Time	2024-11-19 21:51:26 Sync with browser Sync with NTP-Server	
	Hostname	WNDR4300	
	Description	OpenWRT  An optional, short description for this device	
	Notes	Optional, free-form notes about this device	
	Timezone	Asia/Tokyo	
		Save & Ap	pply T Save Reset

図3.2-2 ホスト名とタイムゾーンの設定

# 3.3 OpenWRTのデバイスの設定①

必要なデバイスを追加する。

Network→Interface で行う。 「Device」タブをクリックし「Add device configuration」をクリックする。 下記のようにパラメータを指定する。 Device type: VLAN(802.1q) Base device: Eth0

VLAN ID :10Enable IPv6 :Disabled「Save」をクリックする。

続いてブリッジデバイスの追加する。 「Add device configuration」をクリックし Private用のbr-privateを作成する。

Device type :Bridge deviceDevice name :br-privateBridge ports :Eth0.10Enable IPv6 :Disabled「Save」をクリックする。

# VLAN (802.1q): eth0.10 General device options Advanced device options Device type VLAN (802.1q) Base device # eth0 VLAN ID 10 Device name eth0.10 MTU 1500 MAC address 28:C6:8E:B2:3E:0F TX queue length 1000 Enable IPv6 disabled VIENS Save

### 図3.3-1 PrivateインターフェースのVLANデバイスの設定画面

Bridge device: br-p	rivate									
	Advanced dev	vice options	Bridge VLAN fil							
Device	e type Bridge									
Device	name br-priv									
Bridge	ports 🛛 🗺 eth	n0.10								
	Spe inter	ecifies the wire rface as netwo	d ports to attach ork in the wireles	to this s settin	bridge. In o gs.	order to attach	wireless net	works, choo	ose the assoc	iated
Bring up empty t	oridge									
	😢 Brin	ng up the bridg	e interface ever	n if no p	orts are atta	ached				
	MTU 1500									
MAC ad	dress DA:Al									
TX queue I	ength 1000									
Enable	IPv6 disabl	led								
									Dismiss	Save

図3.3-2 Privateインターフェースのブリッジデバイスの設定画面

# 3.3.1 デバイスの設定状況

ここまでの設定は図のようになる。 赤字部分を前述までに行った設定個所になる。 ・CPU内のbr-privateブリッジインターフェースの追加 ・Vlan10の追加



図3.3.1-1 設定後におけるWNDR4300のOpenWRTの構造

# 3.4 OpenWRTのデバイスの設定②

引き続き必要なデバイスを追加する。 Network→Interface で行う。 「Device」タブをクリックし「Add device configuration」をクリックする。 下記のようにパラメータを指定する。 Device type: VLAN(802.1q) Base device: Eth0 VLAN ID: 20 Enable IPv6: Disabled 「Save」をクリックする。

続いてブリッジデバイスの追加する。 「Add device configuration」をクリックし Guest用のbr-guestを作成する。

Device type :Bridge deviceDevice name :br-guestBridge ports :Eth0.20Enable IPv6 :Disabled「Save」をクリックする。

# VLAN (802.1q): eth0.20 General device options Advanced device options Device type VLAN (802.1q) Base device eth0 VLAN ID 20 Device name eth0.20 MTU 1500 MAC address 28:C6:8E:B2:3E:0F T× queue length 1000 Enable IPv6 disabled Dismiss Save

### 図3.4-1 GuestインターフェースのVLANデバイスの設定画面

snuge device. bi-gi	1621					
General device options	Advanced device options	Bridge VLAN filtering				
Device	type Bridge device					
Device r	br-guest					
Bridge	ports 🕎 eth0.20					
	Opecifies the wind interface as network a	red ports to attach to this work in the wireless setti	bridge. In order to attach ngs.	n wireless networks, choo	se the associate	d
Bring up empty b	ridge					
	Ø Bring up the brid	lge interface even if no p	orts are attached			
	MTU 1500					
MAC add	dress 28:C6:8E:B2:3E:0					
TX queue le	ength 1000					
Enable	IPv6 disabled					
					Dismiss	Save

図3.4-2 Guestインターフェースのブリッジデバイスの設定画面



ここまでの設定は図のようになる。 赤字部分を前述までに行った設定個所になる。 ・CPU内のbr-guestブリッジインターフェースの追加 ・Vlan20の追加



図3.4.1-1 設定後におけるWNDR4300のOpenWRTの構造

# 3.5 OpenWRTのインターフェースの設定①

### 次にインターフェースを追加する。

このインターフェースとはデバイスをグループ化するものになる。 インターフェースに各デバイスを所属させることでデバイス間が通信可能になる。

### Network→Interfaces で行う。 「Add new Interface」をクリックする。 下記のようにパラメータを指定する。 Name : Protocol : Device : 「インターフェースを作成」をクリックする。

Private(大文字と小文字の混在可能) Static address br-private

### 続いて表示されるインターフェースの設定をする。 General Settingsタブ

IPv4 address :	192.168.10.246				
IPv4 netmask :	255.255.255.0				
IPv4 gateway :	192.168.10.254				
Advanced Settingsタブ					
Use custom DNS server :	1.1.1.1				

以上で「Save」をクリックする。

Add new interface			
Name	Private		
Protocol	Static address ~		
Device	🔊 br-private 🔹		
		Cancel	Create interface

### 図3.5-1 Privateインターフェースの追加画面

Interfaces » Private							
General Settings Adv	anced Settings	Firewall Settings	DHCP Server				
	Status M R T)	evice: br-private AC: DA:AE:05:2A:6 X: 0 B (0 Pkts.) X: 0 B (0 Pkts.)	i1:AD				
Pr	otocol Static	address					
	Device 💵 br-	-private					
Disable this int	erface						
Bring up o	n boot 🗹						
IPv4 ad	ldress 192.1	68.10.246					
IPv4 ne	tmask 255.2	55.255.0					
IPv4 ga	teway 192.1	68.10.254					
IPv4 broa	adcast 192.1						
IPv6 ac	ddress Add II						
IPv6 ga	iteway						
IPv6 routed	prefix	11 fi i i ii					
	W Pub	nic prefix routed to t	his device for d	istribution to client	s		
						Dismiss	Save

図3.5-2 Privateインターフェースの設定画面



ここまでの設定は図のようになる。 赤字部分を前述までに行った設定個所になる。 ・Privateインターフェースを作成しbr-privateを所属させた。

先ほどの設定でBr-privateにはEth0.10が所属しているので 自動的にPrivateインターフェースに所属される。



図3.5.1-1 設定後におけるWNDR4300のOpenWRTの構造

# 3.6 OpenWRTのインターフェースの設定②

次にGuest用のインターフェースを追加する。

Network→Interface で行う。 「インターフェースを新規作成」をクリックする。 下記のようにパラメータを指定する。 Name: Guest (大文字と小文字の混在可能) Protocol: Static address Device: br-guest 「インターフェースを作成」をクリックする。

続いて表示されるインターフェースの設定をする。 **\* GatewayとDNSはPrivateで設定済みなので不要** IPv4 adress: 192.168.20.242 IPv4 netmask: 255.255.255.0

以上で「保存」をクリックする。

Add new interface					
Name					
Protocol	Static address				
Device	🔊 br-guest				
				Cancel	Create interface
		図3.6-1	Guestインターフ	エースの	追加画面

erfaces » Guest							
eneral Settings Advanced	I Settings	Firewall Settings	DHCP Server				
Statu	S P De Up MA RX TX IPv	vice: br-guest time: 21h 10m 1s .C: 28:C6:8E:B2:3t : 191.99 MB (1858 : 461.20 KB (5445 :4: 192.168.10.242	5:0F 939 Pkts.) Pkts.) /24				
Protoco	I Static a	address					
Devic	e 🔊 br-g	juest					
Disable this interface							
Bring up on boo							
IPv4 addres	s 192.16	8.20.242					
IPv4 netmas	k 255.25	5.255.0					
IPv4 gatewa	y 192.16	8.20.254					
IPv4 broadcas							
IPv6 addres							
IPv6 gatewa							
IPv6 routed prefi	x ? Publi	c prefix routed to th	nis device for dis	tribution to clients			
						Dismiss	Save

図3.6-2 Guestインターフェースの設定画面



ここまでの設定は図のようになる。 赤字部分を前述までに行った設定個所になる。 ・Guestインターフェースを作成しbr-guestを所属させた。

先ほどの設定でbr-guestにはEth0.20が所属しているので 自動的にGuestインターフェースに所属される。



図3.6.1-1 設定後におけるWNDR4300のOpenWRTの構造

# 3.7 OpenWRTのSwitch0の設定

次はSwitch0を設定する。 これにより内部ネットワークと物理ポートが接続される。 ネットワーク→スイッチ に移動する。 VLANを追加で下記を追加する。 VLANID : 3→10 VLANID : 4→20 まずはCPU(eth0)に先ほど作成したVLANを設定する。 VLAN10: tagged VLAN20: tagged 続いて物理ポートにVLANを割り当てる。 今回は下記のようにした。 物理ポート1は Trunkポート 物理ポート2は Vlan10 物理ポート3は Vlan20 物理ポート4は MGMTとする。 設定としては下記となる。 VLAN1 LAN1 off off LAN2 off LAN3 LAN4 untagge VLAN10 tagged LAN1 LAN2 untagged LAN3 off off LAN4 VLAN20 LAN1 tagged LAN2 off LAN3 untaggd LAN4 off 以上の設定を行うとネットワークに接続が開始される。

### Switch

The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0"							
Enable VLAN function	onality 🖌						
Enable mirroring of inc pa	oming 🗌 ackets						
Enable mirroring of ou pa	tgoing 🗌 ackets						
VLANs on "switc	h0"						
VLAN ID	Description	CPU (eth0)	LAN 1	LAN 2	LAN 3	LAN 4	WAN
Port status:		1000baseT full-duplex	j 1000baseT full-duplex	no link	no link	1000baseT full-duplex	no link
		tagged ~	off ~	off v	off ~	untaggei v	off ~ Delete
2		tagged ~	off ~	off v	off ~	off ~	untagç > Delete
10		tagged v	tagged ~	untagç v	off v	off ~	off v Delete
20		tagged ~	tagged ~	off ~	untagç ~	off ~	off ~ Delete
						Save &	Apply   Save Reset

図3.7-1 Switch0の設定後の画面



ここまでの設定は図のようになる。 赤字部分を前述までに行った設定個所になる。 Switch0のVlan10、20と各インターフェースの割り当て LAN1でTrunkインターフェース化 LAN4を管理用としEth0で接続



図3.7.1-1 設定後におけるWNDR4300のOpenWRTの構造

# 3.8 OpenWRTの日本語化とモジュールの更新

### インターネットまでの通信を確認する。

Network→Diagnostics

の診断画面でゲートウェイに向けてPing試験と名前解決試験を行ってパスするか確認する。 無事に確認できれば正常に接続されているのでOpenWRTのLuCIの日本語化を行う。

### System→Software

の画面でUpdateListをクリックしモジュールリストの最新化を行う。 更新が完了すると完了のメッセージが表示されるのでDissmissをクリックする。 4000件以上のモジュール一覧が表示され探すのに苦労するので「Filter:」に **luci-i18n-base-jp** と入力し「Install」をクリックする。 インストール後は自動で日本語化される。

Updatesタブをクリックしてパッケージの更新が山のようにあるはずなので全て更新を行う。

### ※補足

なお英語に戻すには システム→システム の言語とスタイルのタブで言語をEnglishにし保存と更新をクリックすれば英語に戻る。 図3.8-3を参照



### 図3.8-1 インターフェースの疎通試験



### 図3.8-2 GUIの日本語モジュールの追加

WNDR4300 秋雨・ システム・ ネットワーク・ ログアウト	更新中
システム ここではホストSやタイムソーンなどのデバイスの基本的な設定をすることができます。	
システムプロパティ	
一般設定 ロギング 時刻同期 言語とスタイル	
auto v	
$\vec{\tau} \cdot \vec{\tau} \cdot \vec{\tau} > Bootstrap $	
(4/78.00) • (4/7) (UE	

図3.8-3 言語設定の変更

# 3.9 WiFiの設定

### いよいよWiFiの設定を行う。 今回は2つのSSIDを追加する。 まずはデフォルトのOpenWRTのSSIDを削除する。

続いて各WiFiのインターフェースごとにSSIDを追加する。

### デバイス設定の詳細設定

国コード: JP-Japan ↑まずこれを必ず設定する。なぜなら他にしてしまうと電波法違反になる為。

### デバイス設定の一般設定

動作周波数: 帯域幅を40MHz

### インターフェース設定の一般設定タブ

モード:	アクセスポイント	
ESSID :	private	
ネットワーク:	Private	

### インターフェース設定の無線セキュリティタブ

暗号化:	WPA2-PSKなど
≠-:	お好みで

### インターフェース設定の詳細設定タブ

インターフェース名:	private_2g or private_5g
MACアドレス:	randomly generated

### 他詳細な設定は各自お好みで。 以上で保存するとWiFiが機能する。

無線ネットワークを編集	
デバイス設定	
一般設定詳細設定	
状態	▲ モード: Master   SSID: OpenWrt dBm 無線機器はまだ接続されていません
無線ネットワークは有効	
動作周波数	モード チャンネル 帯域幅 N v auto v 40 MHz v
レガシー802.11bレートを許可	
	♀レガシーまたは動作の悪いデバイスは、相互運用するためにレガシーな 802.11b レートを必要とする場合があります。これらを使用すると、通信時間の効率が大幅に低下する可能性があります。可能な限り 802.11b レートを許可しないことをお勧めします。
最大送信出力	ドライバーデフォルト 🗸 - 現在の出力: <i>不明</i>
インターフェース設定	
一般設定無線セキュリティ	MACフィルタ 詳細設定
	アクセスポイント・
ESSID	OpenWrt
ネットワーク	
<u>ESSID</u> を非表示	
	● ESSID が非表示の場合、クライアントがローミングに失敗し、通信時間の効率が大幅に低下する可能性があります。     す。
WMMモード	
	開じる 保存

図3.9-1 WiFi設定

# 3.9.1 インターフェースの設定状況



図3.9.1-1 設定後におけるWNDR4300のOpenWRTの構造