

Fujitsu Network SR-M コマンド設定事例集

V20

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
無線LANを使用した安全なネットワークを構築するために、本装置をご利用ください。

2020年12月 初版
2021年 6月 第2版
2021年12月 第3版
2022年 4月 第4版
2023年 1月 第5版
2023年10月 第6版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。
従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。
Microsoft Corporationのガイドラインに従って画面写真を使用しています。
Copyright Fujitsu Limited 2020-2023

目次

はじめに	2
本書の使いかた	4
本書の読者と前提知識	4
本書における商標の表記について	5
本装置のマニュアルの構成	6
1 無線 LAN 機能を使う (SR-M630AP1,610AP1)	7
1.1 無線 LAN を構築する (IEEE802.11ax)	7
1.2 無線 LAN を構築する (IEEE802.11ac)	9
1.3 無線 LAN を構築する (IEEE802.11n)	11
1.4 無線 LAN を構築する (IEEE802.11b/g)	13
1.5 仮想アクセスポイントにより複数の無線 LAN ネットワークを構築する	15
1.6 IEEE802.1X 認証および MAC アドレス認証により VLAN を管理する	20
1.7 同一 SSID の複数アクセスポイントを構築する	25
1.8 認証自動切替機能を使う	29
1.9 端末台数制限機能を使う	32
1.10 端末台数最低保証機能を使う	34
1.11 WDS ブリッジ機能を使う	36
1.12 VLAN ネットワークを WDS ブリッジ機能で接続する	42
1.13 MAC アドレスフィルタリング機能を使う	46
1.14 WMM 機能を使う	48
1.15 周辺アクセスポイント検出機能を使う	50
1.16 チャンネルボンディング機能を使う	52
1.17 バンドステアリング機能を使う	55
1.18 エアタイムフェアネス機能を使う	57
1.19 無線 LAN アクセスポイントを屋外で利用する	60
1.20 144ch のサポートを無効に設定する	63
1.21 空間再利用機能を使用する	66
1.22 Enhanced Open 認証を使う	68
1.23 パケットキャプチャ機能を使う	70
2 VLAN 機能を使う	73
2.1 ポート VLAN 機能を使う	73
2.2 タグ VLAN 機能を使う	74
3 リンクアグリゲーション機能を使う	75
3.1 LACP 機能を使う	76
4 リンクインテグリティ機能を使う	77
5 フィルタリング機能を使う	78
5.1 特定サービスへのアクセスだけを許可する	80
6 DHCP 機能を使う	82
6.1 DHCP クライアント機能を使う	82
7 SNMP エージェント機能を使う	84
8 システムログを採取する	87
9 スケジュール機能を使う	88
9.1 構成定義情報の切り替えを予約する	88
10 アプリケーションフィルタ機能を使う	89
11 端末可視化機能を使う	91
12 NXconcierge と連携する	93
13 装置を保護する	96
索引	98

本書の使いかた

本書では、ネットワークを構築するために、代表的な接続形態や本装置の機能を活用した接続形態について説明しています。

本書の読者と前提知識







本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

-  **ヒント** 本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。
- こんな事に気をつけて** 本装置をご使用になる際に、注意していただきたいことを説明しています。
-  **補足** 操作手順で説明しているもののほかに、補足情報を説明しています。
-  **参照** 操作方法など関連事項を説明している箇所を示します。
-  **適用機種** 本装置の機能を使用する際に、対象となる機種名を示します。
-  **警告** 製造物責任法 (PL) 関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
-  **注意** 製造物責任法 (PL) 関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

設定例の記述について

コマンド例では configure コマンドを実行して、構成定義モードに入ったあとのコマンドを記述しています。また、プロンプトは設定や機種によって変化するため、“#”に統一しています。

本書における商標の表記について

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® 10 Home 64ビット版	Windows 10 および Windows
Microsoft® Windows® 10 Pro 64ビット版	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
ご利用にあたって	本装置の設置方法やソフトウェアのインストール方法を説明しています。
コマンドユーザズガイド	構成定義コマンド、運用管理コマンド、およびその他のコマンドの項目やパラメタの詳細な情報を説明しています。
コマンドリファレンス	コマンドの項目やパラメタの詳細な情報を説明しています。
コマンド設定事例集 (本書)	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード/ソフトウェア仕様と MIB/Trap 一覧を説明しています。
Web ユーザズガイド	Web 画面を使用して、基本的な設定またはメンテナンスについて説明しています。

1 無線 LAN 機能を使う (SR-M630AP1,610AP1)

適用機種 SR-M630AP1,610AP1

1.1 無線 LAN を構築する (IEEE802.11ax)

適用機種 SR-M630AP1,610AP1

ここでは、既存の有線 LAN ネットワークを無線化する場合を例に説明します。

無線 LAN によるネットワークのワイヤレス化を行い、LAN ケーブルの配線なしに無線通信によるネットワークを構築することができます。

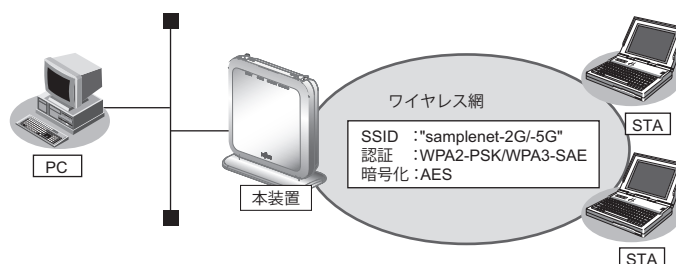
本装置は IEEE802.11ax 規格 (Wi-Fi6) に準拠しています。IEEE802.11ax を使用することにより、高速な無線通信が実現できます。IEEE802.11ax を使用する場合の無線 LAN 構築例を以下に記載します。

なお、IEEE802.11ax は、2.4GHz、5GHz 両方の周波数帯で同時に利用できます。

こんな事に気をつけて

- IEEE802.11ax で接続する場合、無線 LAN クライアントも IEEE802.11ax に対応している必要があります。
- 無線モジュール (2.4GHz 帯) は、11b/g/n/ax 共存または 11g/n/ax 共存の無線通信モードを設定してください。5GHz 帯に対してのみ有効なモードを定義した場合は、無効な設定となり無線 LAN インタフェースが使用できません。
- 無線モジュール (5GHz 帯) は、11a/n/ac/ax 共存の無線通信モードを設定してください。2.4GHz 帯に対してのみ有効なモードを定義した場合は、無効な設定となり無線 LAN インタフェースが使用できません。
- 本装置を IEEE802.11ax 固定の無線通信モード設定にすることはできません。
- IEEE802.11n 以降の無線通信モードでは、暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。
- 以下の認証モードを利用する場合、PMF 機能は有効 (必須) を設定してください。
wpa3, wpa3-sae, enhanced-open, open/enhanced-open_owe
- 以下の認証モードを利用する場合、PMF 機能は有効 (必須) または有効 (オプション) を設定してください。
wpa2/wpa3, wpa2-psk/wpa3-sae
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☞ 参照 マニュアル「ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール : ieee80211 1 (2.4GHz 帯) および ieee80211 2 (5GHz 帯)
- 利用する無線 LAN インタフェース : wlan 1 (2.4GHz 帯) および wlan 9 (5GHz 帯)
- 通信モード : IEEE802.11b/g/n/ax (2.4GHz 帯) および IEEE802.11a/n/ac/ax (5GHz 帯)

- チャンネル : 自動判別
- 無線 LAN インタフェース数 : 8
- SSID : samplenet-2G (2.4GHz帯) および samplenet-5G (5GHz帯)
- 認証モード : WPA2-PSK/WPA3-SAE 自動判別認証
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで“abcdefghijklmnopqrstuvwxy”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel any
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel any
```

無線LANインタフェース数を設定する

```
# wlan-conf wlan-num 8
```

無線LANインタフェースを設定する

```
# wlan 1 use on
# wlan 1 ssid samplenet-2G
# wlan 1 auth wpa2-psk/wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxy
# wlan 9 use on
# wlan 9 ssid samplenet-5G
# wlan 9 auth wpa2-psk/wpa3-sae
# wlan 9 wpa cipher aes
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxy
```

設定終了

```
# save
# commit
```


1.2 無線 LAN を構築する (IEEE802.11ac)

適用機種 SR-M630AP1,610AP1

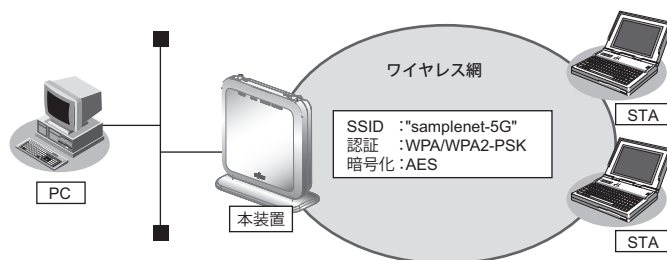
主に IEEE802.11ac (Wi-Fi5) とそれ以前の無線 LAN 通信規格を使用する場合の無線 LAN 構築例を以下に記載します。

なお、IEEE802.11ac は、5GHz の周波数帯で利用できます。

こんな事に気をつけて

- IEEE802.11ac で接続する場合、無線 LAN クライアントも IEEE802.11ac に対応している必要があります。
- 無線モジュール (5GHz 帯) は、11a/n/ac 共存の無線通信モードを設定してください。2.4GHz 帯に対してのみ有効なモードを定義した場合は、無効な設定となり無線 LAN インタフェースが使用できません。
- 本装置を IEEE802.11ac 固定の無線通信モード設定にすることはできません。
- IEEE802.11n 以降の無線通信モードでは、暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール : ieee80211 2 (5GHz 帯)
- 利用する無線 LAN インタフェース : wlan 9 (5GHz 帯)
- 通信モード : IEEE802.11a/n/ac
- チャンネル : 52
- 無線 LAN インタフェース数 : 8
- SSID : samplenet-5G (5GHz 帯)
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで“abcdefghijklmnopqrstuvwxyz”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線 LAN モジュールを設定する

```
# ieee80211 2 use on
```

```
# ieee80211 2 mode 11a/n/ac
```

```
# ieee80211 2 channel 52
```

無線 LAN インタフェース数を設定する

```
# wlan-conf wlan-num 8
```

無線 LAN インタフェースを設定する

```
# wlan 9 use on
```

```
# wlan 9 ssid samplenet-5G
```

```
# wlan 9 auth wpa/wpa2-psk
```

```
# wlan 9 wpa cipher aes
```

```
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz
```

設定終了

```
# save
```

```
# commit
```

1.3 無線 LAN を構築する (IEEE802.11n)

適用機種 SR-M630AP1,610AP1

主に IEEE802.11n (Wi-Fi4) とそれ以前の無線 LAN 通信規格を使用する場合の無線 LAN 構築例を以下に記載します。

なお、IEEE802.11n は、2.4GHz、5GHz 両方の周波数帯で同時に利用できます。

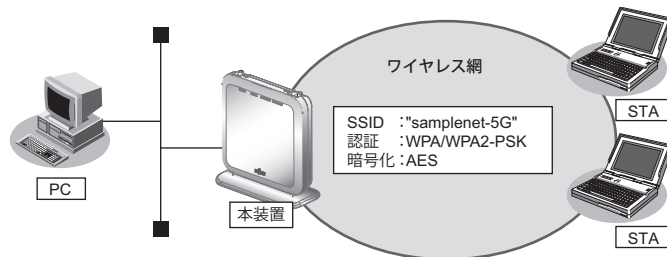
こんな事に気をつけて

- IEEE802.11n で接続する場合、無線 LAN クライアントが IEEE802.11n に対応している必要があります。
- IEEE802.11n 以降の無線通信モードでは、暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。
- IEEE802.11n 未対応の無線装置が同一チャンネルに存在している場合、スループットが低下する場合があります。

☛ 参照 マニュアル「機能説明書」

- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール : ieee80211 2 (5GHz 帯)
- 利用する無線 LAN インタフェース : wlan 9 (5GHz 帯)
- 通信モード : IEEE802.11a/n
- チャンネル : 52
- 無線 LAN インタフェース数 : 8
- SSID : samplenet-5G (5GHz 帯)
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで“abcdefghijklmnopqrstuvwxy”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線 LAN モジュールを設定する

```
# ieee80211 2 use on  
# ieee80211 2 mode 11a/n  
# ieee80211 2 channel 52
```

無線 LAN インタフェース数を設定する

```
# wlan-conf wlan-num 8
```

無線 LAN インタフェースを設定する

```
# wlan 9 use on  
# wlan 9 ssid samplenet-5G  
# wlan 9 auth wpa/wpa2-psk  
# wlan 9 wpa cipher aes  
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz
```

設定終了

```
# save  
# commit
```

1.4 無線 LAN を構築する (IEEE802.11b/g)

適用機種 SR-M630AP1,610AP1

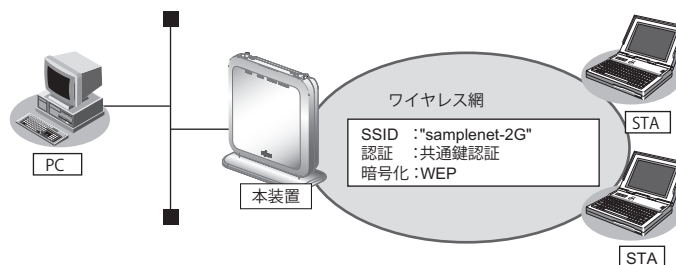
WEPのみをサポートする古い機器をお使いの場合など、無線通信モードを旧規格のIEEE802.11b/gに固定した構築例を以下に記載します。

なお、IEEE802.11b/gは、2.4GHzの周波数帯で利用できます。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- ・ 利用する無線 LAN モジュール : ieee80211 1 (2.4GHz 帯)
- ・ 利用する無線 LAN インタフェース : wlan 1 (2.4GHz 帯)
- ・ 通信モード : IEEE802.11b/g
- ・ チャンネル : 6
- ・ 無線 LAN インタフェース数 : 8
- ・ SSID : samplenet-2G
- ・ 認証モード : 共通鍵認証
- ・ 暗号化モード : WEP
- ・ WEP キー : テキストで“abcdefghijklm”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 6

無線LANインタフェース数を設定する
# wlan-conf wlan-num 8

アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet-2G
# wlan 1 auth shared
```

```
# wlan 1 wep mode enable  
# wlan 1 wep key 1 text abcdefghijklm  
# wlan 1 wep send 1
```

```
設定終了  
# save  
# commit
```

1.5 仮想アクセスポイントにより複数の無線LANネットワークを構築する

適用機種 SR-M630AP1,610AP1

仮想アクセスポイントを使用することで、1つの無線LANモジュールで複数の無線LANネットワークを構築することができます。それぞれの無線LANインタフェースにVLAN IDを割り当てることで、ネットワークのグループ化を行うことができます。

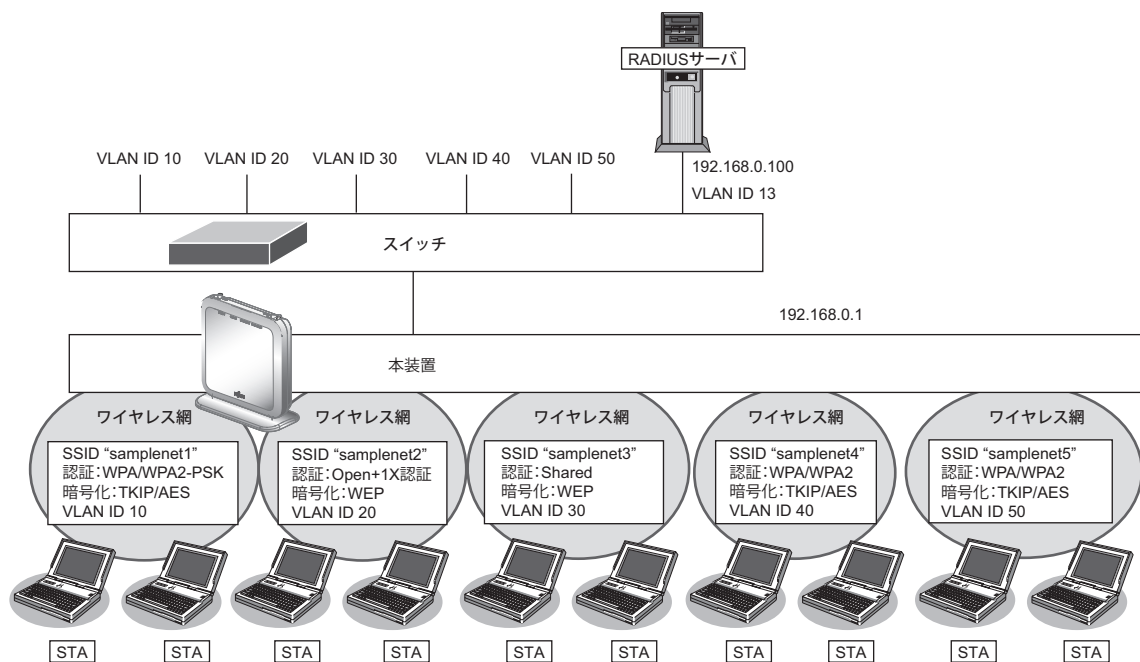
IEEE802.1X認証機能を使用すると、認証サーバを利用して、無線LANネットワークに接続する端末またはユーザが、ネットワークへのアクセス権を持っているかを認証することもできます。

同一の無線LANネットワークを2.4GHz帯および5GHz帯の両方で動作させるには、両方の無線LANデバイスに対する無線LANインタフェースに同じVLAN IDの定義を行ってください。

こんな事に気をつけて

- プライバシープロテクション機能は、同一仮想アクセスポイント内の端末どうしの通信を防止するものであり、同機能が有効な場合であっても同一のVLAN IDを指定した複数の無線LANインタフェース間の通信については可能です。
- OPEN認証、SHARED認証、Enhanced-OPEN認証、OPEN/Enhanced-OPEN認証またはOPEN/Enhanced-OPEN_OWE認証と、IEEE802.1X認証との併用はできません。IEEE802.1X認証が無効で動作します。
- OPEN認証、SHARED認証、OPEN/Enhanced-OPEN認証またはOPEN/Enhanced-OPEN_OWE認証と、MACアドレス認証と併用する場合は、認証サーバから通知されたVLANを割り当てる機能を無効 (wlan macauth vlan assign disable) にし、端末に割り当てるデフォルトVLAN ID 機能 (wlan macauth vid) を利用してください。
- WEP暗号とIEEE802.1X認証またはMACアドレス認証を併用する場合、すべての無線LANインタフェースで、認証サーバから通知されたVLANを割り当てる機能を無効 (wlan dot1x vlan assign disable / wlan macauth vlan assign disable) に設定し、端末に割り当てるデフォルトVLAN ID 機能 (wlan dot1x vid / wlan macauth vid) を利用してください。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

参照 マニュアル「ご利用にあたって」



● 設定条件**有線 LAN を使ってネットワークに接続する**

- 利用するポート : ether1
- IP アドレス : 192.168.0.1/24

無線 LAN を使用する (共通)

- 利用する無線 LAN モジュール : ieee80211 1 および ieee80211 2
- 通信モード : IEEE802.11b/g および IEEE802.11a
- チャネル : 10 (11b/g) および 52 (11a)

仮想アクセスポイント (SSID : samplenet1) を構築する

- 利用する無線 LAN インタフェース : wlan 1 および wlan 9
- SSID : samplenet1
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで "abcdefghijklmnopqrstuvwxy"
- VLAN ID : 10

仮想アクセスポイント (SSID : samplenet2) を構築する

- 利用する無線 LAN インタフェース : wlan 2 および wlan 10
- SSID : samplenet2
- 認証モード : オープン認証
- 暗号化モード : WEP
- WEP キー : テキストで "abcdefghijklm"
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (サーバ) : aaa1
- VLAN ID : 20

仮想アクセスポイント (SSID : samplenet3) を構築する

- 利用する無線 LAN インタフェース : wlan 3 および wlan 11
- SSID : samplenet3
- 認証モード : 共通鍵認証
- 暗号化モード : WEP
- WEP キー : テキストで "nopqrstuvwxyz"
- VLAN ID : 30

仮想アクセスポイント (SSID : samplenet4) を構築する

- 利用する無線 LAN インタフェース : wlan 4 および wlan 12
- SSID : samplenet4
- 認証モード : WPA/WPA2 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (サーバ) : aaa1
- VLAN ID : 40

仮想アクセスポイント (SSID:samplenet5) を構築する

- 利用する無線 LAN インタフェース : wlan 5 および wlan 13
- SSID : samplenet5
- 認証モード : WPA/WPA2 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (サーバ) : aaa1
- VLAN ID : 50

認証サーバを AAA 定義で指定する

- aaa 定義番号 : aaa1
- 認証サーバ IP アドレス : 192.168.0.100
- 認証サーバシークレットキー : passwd

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```

IEEE802.1X 認証を使用する
# dot1x use on

RADIUS サーバの VLAN を設定する
# lan 0 vlan 13
# lan 0 ip address 192.168.0.1/24 3

ETHER1 ポートを設定する
# ether 1 vlan tag 10,13,20,30,40,50

無線 LAN モジュールを設定する (IEEE802.11b/g)
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

無線 LAN モジュールを設定する (IEEE802.11a)
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 52

仮想アクセスポイント (SSID : samplenet1) を設定する
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 1 vlan untag 10
# wlan 9 use on
# wlan 9 ssid samplenet1
# wlan 9 auth wpa/wpa2-psk
# wlan 9 wpa cipher auto
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 9 vlan untag 10

仮想アクセスポイント (SSID : samplenet2) を設定する
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth open
# wlan 2 wep mode enable
# wlan 2 wep key 1 text abcdefghijklm

```

```
# wlan 2 wep send 1
# wlan 2 dot1x use on
# wlan 2 dot1x aaa 1
# wlan 2 dot1x vid 20
# wlan 2 dot1x vlan assign disable
# wlan 10 use on
# wlan 10 ssid samplenet2
# wlan 10 auth open
# wlan 10 wep mode enable
# wlan 10 wep key 1 text abcdefghijklm
# wlan 10 wep send 1
# wlan 10 dot1x use on
# wlan 10 dot1x aaa 1
# wlan 10 dot1x vid 20
# wlan 10 dot1x vlan assign disable

仮想アクセスポイント (SSID : samplenet3) を設定する
# wlan 3 use on
# wlan 3 ssid samplenet3
# wlan 3 auth shared
# wlan 3 wep mode enable
# wlan 3 wep key 1 text nopqrstuvwxyz
# wlan 3 wep send 1
# wlan 11 use on
# wlan 11 ssid samplenet3
# wlan 11 auth shared
# wlan 11 wep mode enable
# wlan 11 wep key 1 text nopqrstuvwxyz
# wlan 11 wep send 1

仮想アクセスポイント (SSID : samplenet4) を設定する
# wlan 4 use on
# wlan 4 ssid samplenet4
# wlan 4 auth wpa/wpa2
# wlan 4 wpa cipher auto
# wlan 4 dot1x use on
# wlan 4 dot1x aaa 1
# wlan 4 dot1x vid 40
# wlan 4 dot1x vlan assign disable
# wlan 12 use on
# wlan 12 ssid samplenet4
# wlan 12 auth wpa/wpa2
# wlan 12 wpa cipher auto
# wlan 12 dot1x use on
# wlan 12 dot1x aaa 1
# wlan 12 dot1x vid 40
# wlan 12 dot1x vlan assign disable

仮想アクセスポイント (SSID : samplenet5) を設定する
# wlan 5 use on
# wlan 5 ssid samplenet5
# wlan 5 auth wpa/wpa2
# wlan 5 wpa cipher auto
# wlan 5 dot1x use on
# wlan 5 dot1x aaa 1
# wlan 5 dot1x vid 50
# wlan 5 dot1x vlan assign disable
# wlan 13 use on
# wlan 13 ssid samplenet5
# wlan 13 auth wpa/wpa2
# wlan 13 wpa cipher auto
# wlan 13 dot1x use on
```

```
# wlan 13 dot1x aaa 1
# wlan 13 dot1x vid 50
# wlan 13 dot1x vlan assign disable

認証サーバを AAA 定義で指定する
# aaa 1 name aaasvr
# aaa 1 radius service client auth
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 192.168.0.100
# aaa 1 radius client server-info auth 0 source 192.168.0.1

設定終了
# save
# commit
```

1.6 IEEE802.1X 認証および MAC アドレス認証により VLAN を管理する

適用機種 SR-M630AP1,610AP1

IEEE802.1X 認証機能または MAC アドレス認証機能を使用した場合、認証データベースで、ユーザごとに所属する VLAN ID を設定すると、認証端末またはユーザが所属するネットワークを指定することができます。

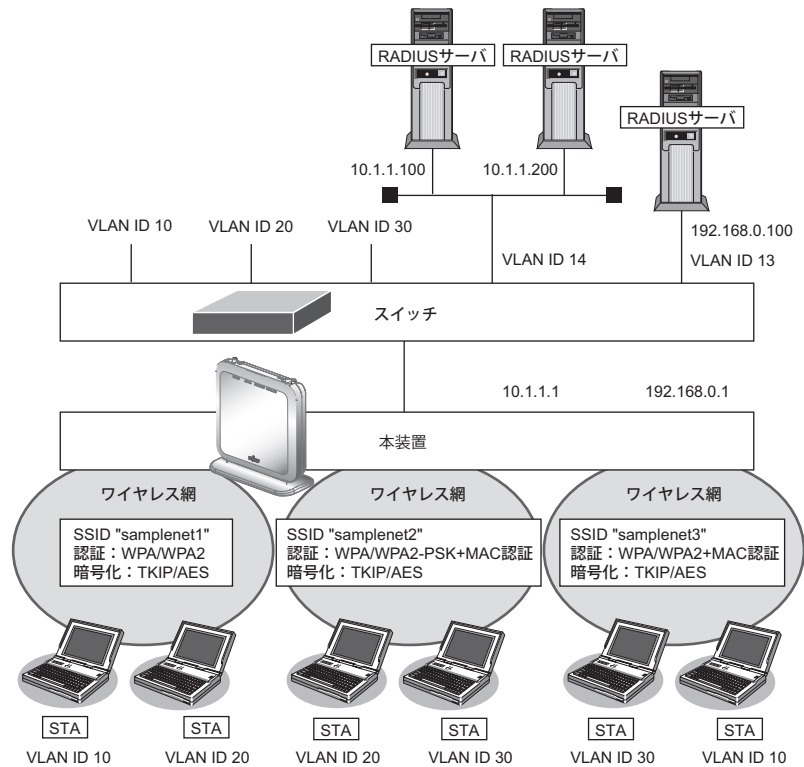
これにより、ネットワークへのアクセスを認証端末またはユーザごとに管理することができます。

☛ 参照 マニュアル「機能説明書」

こんな事に気をつけて

- IEEE802.1X 認証、MAC アドレス認証を利用する無線 LAN インタフェースでは事前に VLAN を設定できません。
- IEEE802.1X 認証、MAC アドレス認証で利用する AAA のグループ ID を正しく設定してください。
- 1つの無線 LAN インタフェースで IEEE802.1X 認証と MAC アドレス認証を併用する場合、同じ VLAN ID が割り当てられるよう以下のコマンドを同じ設定にする必要があります。
 - 1) wlan dot1x vlan assign コマンドと wlan macauth vlan assign コマンド
 - 2) wlan dot1x vid コマンドと wlan macauth vid コマンド
- 認証サーバに VLAN ID が設定されていない場合、wlan dot1x vid コマンド、および wlan macauth vid コマンドで設定された VLAN ID が使用されます。
- OPEN 認証、SHARED 認証、Enhanced-OPEN 認証、OPEN/Enhanced-OPEN 認証または OPEN/Enhanced-OPEN_OWE 認証と、IEEE802.1X 認証との併用はできません。IEEE802.1X 認証が無効で動作します。
- OPEN 認証、SHARED 認証、OPEN/Enhanced-OPEN 認証または OPEN/Enhanced-OPEN_OWE 認証と、MAC アドレス認証と併用する場合は、認証サーバから通知された VLAN を割り当てる機能を無効 (wlan macauth vlan assign disable) にし、端末に割り当てるデフォルト VLAN ID 機能 (wlan macauth vid) を利用してください。
- WEP 暗号と IEEE802.1X 認証または MAC アドレス認証を併用する場合、すべての無線 LAN インタフェースで、認証サーバから通知された VLAN を割り当てる機能を無効 (wlan dot1x vlan assign disable / wlan macauth vlan assign disable) に設定し、端末に割り当てるデフォルト VLAN ID 機能 (wlan dot1x vid / wlan macauth vid) を利用してください。
- プライバシープロテクション機能を有効にした場合でも、無線 LAN インタフェース間で同一の VLAN ID が割り当てられた端末どうしの通信は可能です。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「SR-M610AP1/SR-M630AP1 ご利用にあたって」



● 設定条件

有線LANを使ってネットワークに接続する

- ・ 利用するポート : ether1
- ・ IPアドレス : 192.168.0.1/24、10.1.1.1/24

無線LANを使用する (共通)

- ・ 利用する無線LAN モジュール : ieee80211 1 および ieee80211 2
- ・ 通信モード : IEEE802.11b/g および IEEE802.11a
- ・ チャンネル : 10 (11b/g) および 52 (11a)

仮想アクセスポイント (SSID : samplenet1) を構築する

- ・ 利用する無線LAN インタフェース : wlan 1 および wlan 9
- ・ SSID : samplenet1
- ・ 認証モード : WPA/WPA2 自動判別認証
- ・ 暗号化モード : TKIP/AES 自動判別
- ・ IEEE802.1X 認証 : 有効
- ・ IEEE802.1X 認証 (サーバ) : aaa1

仮想アクセスポイント (SSID : samplenet2) を構築する

- ・ 利用する無線LAN インタフェース : wlan 2 および wlan 10
- ・ SSID : samplenet2
- ・ 認証モード : WPA/WPA2-PSK 自動判別認証
- ・ 暗号化モード : TKIP/AES 自動判別
- ・ 事前共有キー (PSK) : テキストで "abcdefghijklmnopqrstuvwxyz"
- ・ MAC アドレス認証 : 有効
- ・ MAC アドレス認証 (サーバ) : aaa2

仮想アクセスポイント (SSID : samplenet3) を構築する

- 利用する無線 LAN インタフェース : wlan 3 および wlan 11
- SSID : samplenet3
- 認証モード : WPA/WPA2 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (サーバ) : aaa3
- MAC アドレス認証 : 有効
- MAC アドレス認証 (サーバ) : aaa3

認証 / 課金サーバを AAA 定義で指定する

- aaa 定義番号 : aaa1
- 認証サーバ (プライマリ) IP アドレス : 10.1.1.100
- 認証サーバ (プライマリ) シークレットキー : passwd
- 認証サーバ (セカンダリ) IP アドレス : 10.1.1.200
- 認証サーバ (セカンダリ) シークレットキー : passwd
- 課金サーバ (プライマリ) IP アドレス : 10.1.1.100
- 課金サーバ (プライマリ) シークレットキー : passwd
- 課金サーバ (セカンダリ) IP アドレス : 10.1.1.200
- 課金サーバ (セカンダリ) シークレットキー : passwd

- aaa 定義番号 : aaa2
- 認証サーバ (プライマリ) IP アドレス : 10.1.1.200
- 認証サーバ (プライマリ) シークレットキー : passwd
- 認証サーバ (セカンダリ) IP アドレス : 10.1.1.100
- 認証サーバ (セカンダリ) シークレットキー : passwd

- aaa 定義番号 : aaa3
- 認証サーバ IP アドレス : 192.168.0.100
- 認証サーバシークレットキー : passwd
- 課金サーバ IP アドレス : 192.168.0.100
- 課金サーバシークレットキー : passwd

こんな事に気をつけて

RADIUS サーバにはユーザに VLAN ID を割り当てるために、以下の属性を設定してください。
設定方法については、RADIUS サーバのマニュアルを参照してください。

名前	番号	属性値 (※)
Tunnel-Type	64	VLAN (13)
Tunnel-Media-Type	65	802 (6)
Tunnel-Private-Group-ID	81	VLAN ID (10 進数表記を ASCII コードでコーディング)

※) () 内の数字は属性として設定される 10 進数の値

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IEEE802.1X 認証を使用する
# dot1x use on

MAC アドレス認証を使用する
# macauth use on

RADIUS サーバの VLAN を設定する
# lan 0 vlan 13
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 14
# lan 1 ip address 10.1.1.1/24 3

ETHER1 ポートを設定する
# ether 1 vlan tag 10,13,14,20,30

無線 LAN モジュールを設定する (IEEE802.11b/g)
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

無線 LAN モジュールを設定する (IEEE802.11a)
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 52

仮想アクセスポイント (SSID : samplenet1) を設定する
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2
# wlan 1 wpa cipher auto
# wlan 1 dot1x use on
# wlan 1 dot1x aaa 1
# wlan 9 use on
# wlan 9 ssid samplenet1
# wlan 9 auth wpa/wpa2
# wlan 9 wpa cipher auto
# wlan 9 dot1x use on
# wlan 9 dot1x aaa 1

仮想アクセスポイント (SSID : samplenet2) を設定する
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth wpa/wpa2-psk
# wlan 2 wpa cipher auto
# wlan 2 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 2 macauth use on
# wlan 2 macauth aaa 2
# wlan 10 use on
# wlan 10 ssid samplenet2
# wlan 10 auth wpa/wpa2-psk
# wlan 10 wpa cipher auto
# wlan 10 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 10 macauth use on
# wlan 10 macauth aaa 2

仮想アクセスポイント (SSID : samplenet3) を設定する
# wlan 3 use on
# wlan 3 ssid samplenet3
```

```
# wlan 3 auth wpa/wpa2
# wlan 3 wpa cipher auto
# wlan 3 dot1x use on
# wlan 3 dot1x aaa 3
# wlan 3 macauth use on
# wlan 3 macauth aaa 3
# wlan 11 use on
# wlan 11 ssid samplenet3
# wlan 11 auth wpa/wpa2
# wlan 11 wpa cipher auto
# wlan 11 dot1x use on
# wlan 11 dot1x aaa 3
# wlan 11 macauth use on
# wlan 11 macauth aaa 3

認証／課金サーバを AAA 定義で指定する
# aaa 1 name aaasvr1
# aaa 1 radius service client both
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 10.1.1.100
# aaa 1 radius client server-info auth 0 source 10.1.1.1
# aaa 1 radius client server-info auth 1 secret passwd
# aaa 1 radius client server-info auth 1 address 10.1.1.200
# aaa 1 radius client server-info auth 1 priority 1
# aaa 1 radius client server-info auth 1 source 10.1.1.1
# aaa 1 radius client server-info accounting 0 secret passwd
# aaa 1 radius client server-info accounting 0 address 10.1.1.100
# aaa 1 radius client server-info accounting 0 source 10.1.1.1
# aaa 1 radius client server-info accounting 1 secret passwd
# aaa 1 radius client server-info accounting 1 address 10.1.1.200
# aaa 1 radius client server-info accounting 1 priority 1
# aaa 1 radius client server-info accounting 1 source 10.1.1.1
# aaa 2 name aaasvr2
# aaa 2 radius service client auth
# aaa 2 radius client server-info auth 0 secret passwd
# aaa 2 radius client server-info auth 0 address 10.1.1.200
# aaa 2 radius client server-info auth 0 source 10.1.1.1
# aaa 2 radius client server-info auth 1 secret passwd
# aaa 2 radius client server-info auth 1 address 10.1.1.100
# aaa 2 radius client server-info auth 1 priority 1
# aaa 2 radius client server-info auth 1 source 10.1.1.1
# aaa 3 name aaasvr3
# aaa 3 radius service client auth
# aaa 3 radius client server-info auth 0 secret passwd
# aaa 3 radius client server-info auth 0 address 192.168.0.100
# aaa 3 radius client server-info auth 0 source 192.168.0.1
# aaa 3 radius client server-info accounting 0 secret passwd
# aaa 3 radius client server-info accounting 0 address 192.168.0.100
# aaa 3 radius client server-info accounting 0 source 192.168.0.1

設定終了
# save
# commit
```


1.7 同一 SSID の複数アクセスポイントを構築する

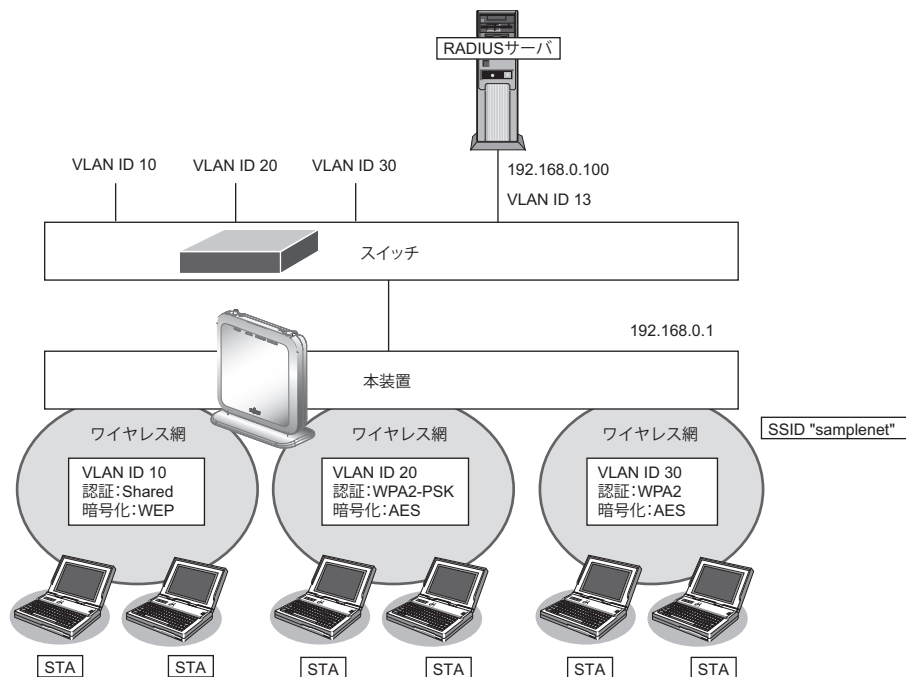
適用機種 SR-M630AP1,610AP1

同一 SSID の仮想アクセスポイントを構築することにより、接続の際の認証・暗号化方式によって端末が属するネットワークを分けることができます。

こんな事に気をつけて

- 同一の SSID かつ同一の認証・暗号化方式の仮想アクセスポイントを設定した場合、どちらの仮想アクセスポイントに接続されるかは不定となります。
- OPEN 認証、SHARED 認証、Enhanced-OPEN 認証、OPEN/Enhanced-OPEN 認証または OPEN/Enhanced-OPEN_OWE 認証と、IEEE802.1X 認証との併用はできません。IEEE802.1X 認証が無効で動作します。
- OPEN 認証、SHARED 認証、OPEN/Enhanced-OPEN 認証または OPEN/Enhanced-OPEN_OWE 認証と、MAC アドレス認証と併用する場合は、認証サーバから通知された VLAN を割り当てる機能を無効 (wlan macauth vlan assign disable) にし、端末に割り当てるデフォルト VLAN ID 機能 (wlan macauth vid) を利用してください。
- WEP 暗号と IEEE802.1X 認証または MAC アドレス認証を併用する場合、すべての無線 LAN インタフェースで、認証サーバから通知された VLAN を割り当てる機能を無効 (wlan dot1x vlan assign disable / wlan macauth vlan assign disable) に設定し、端末に割り当てるデフォルト VLAN ID 機能 (wlan dot1x vid / wlan macauth vid) を利用してください。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件

有線 LAN を使ってネットワークに接続する

- 利用するポート : ether1
- IP アドレス : 192.168.0.1/24

無線 LAN を使用する (共通)

- 利用する無線 LAN モジュール : ieee80211 1 および ieee80211 2
- 通信モード : IEEE802.11b/g および IEEE802.11a
- チャンネル : 10 (11b/g) および 52 (11a)

仮想アクセスポイント (共通鍵認証) を構築する

- 利用する無線 LAN インタフェース : wlan 1 および wlan 9
- SSID : samplenet
- 認証モード : 共通鍵認証
- 暗号化モード : WEP
- WEP キー : テキストで “abcdefghijklm”
- VLAN ID : 10

仮想アクセスポイント (WPA2-PSK) を構築する

- 利用する無線 LAN インタフェース : wlan 2 および wlan 10
- SSID : samplenet
- 認証モード : WPA2-PSK
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで “abcdefghijklmnopqrstuvwxyz”
- VLAN ID : 20

仮想アクセスポイント (WPA2) を構築する

- 利用する無線 LAN インタフェース : wlan 3 および wlan 11
- SSID : samplenet
- 認証モード : WPA2
- 暗号化モード : AES
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (サーバ) : aaa1
- VLAN ID : 30

認証 / 課金サーバを AAA 定義で指定する

- aaa 定義番号 : aaa1
- 認証サーバ IP アドレス : 192.168.0.100
- 認証サーバシークレットキー : passwd
- 課金サーバ IP アドレス : 192.168.0.100
- 課金サーバシークレットキー : passwd

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IEEE802.1X 認証を使用する
# dot1x use on

RADIUS サーバの VLAN を設定する
# lan 0 vlan 13
# lan 0 ip address 192.168.0.1/24 3

ETHER1 ポートを設定する
# ether 1 vlan tag 10,13,20,30
```

無線LANモジュールを設定する (IEEE802.11b/g)

```
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10
```

無線LANモジュールを設定する (IEEE802.11a)

```
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 52
```

仮想アクセスポイント (共通鍵認証) を設定する

```
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth shared
# wlan 1 wep mode enable
# wlan 1 wep key 1 text abcdefghijklm
# wlan 1 wep send 1
# wlan 1 vlan untag 10
# wlan 9 use on
# wlan 9 ssid samplenet
# wlan 9 auth shared
# wlan 9 wep mode enable
# wlan 9 wep key 1 text abcdefghijklm
# wlan 9 wep send 1
# wlan 9 vlan untag 10
```

仮想アクセスポイント (WPA2-PSK) を設定する

```
# wlan 2 use on
# wlan 2 ssid samplenet
# wlan 2 auth wpa2-psk
# wlan 2 wpa cipher aes
# wlan 2 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 2 vlan untag 20
# wlan 10 use on
# wlan 10 ssid samplenet
# wlan 10 auth wpa2-psk
# wlan 10 wpa cipher aes
# wlan 10 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 10 vlan untag 20
```

仮想アクセスポイント (WPA2) を設定する

```
# wlan 3 use on
# wlan 3 ssid samplenet
# wlan 3 auth wpa2
# wlan 3 wpa cipher aes
# wlan 3 dot1x use on
# wlan 3 dot1x aaa 1
# wlan 3 dot1x vid 30
# wlan 3 dot1x vlan assign disable
# wlan 11 use on
# wlan 11 ssid samplenet
# wlan 11 auth wpa2
# wlan 11 wpa cipher aes
# wlan 11 dot1x use on
# wlan 11 dot1x aaa 1
# wlan 11 dot1x vid 30
# wlan 11 dot1x vlan assign disable
```

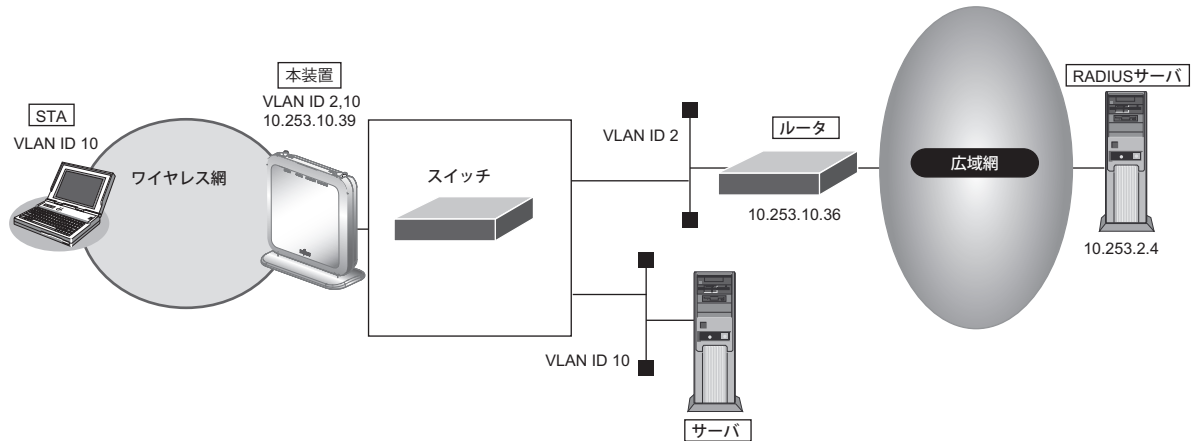
認証/課金サーバを AAA 定義で指定する

```
# aaa 1 name aaasvr
# aaa 1 radius service client both
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 192.168.0.100
# aaa 1 radius client server-info auth 0 source 192.168.0.1
# aaa 1 radius client server-info accounting 0 secret passwd
# aaa 1 radius client server-info accounting 0 address 192.168.0.100
# aaa 1 radius client server-info accounting 0 source 192.168.0.1
設定終了
# save
# commit
```

1.8 認証自動切替機能を使う

適用機種 SR-M630AP1,610AP1

ここでは、RADIUS サーバの稼動状況を監視し RADIUS サーバからの応答がない場合に、認証方式を IEEE802.1X 認証から共有鍵認証へ自動切り替えを行う場合の設定方法を説明します。



こんな事に気をつけて

- RADIUS サーバの監視には、ICMP を使う方法と、認証を使う方法があります。
- ICMP で監視を行う場合は、RADIUS サーバが動作しているホストの生存確認だけを行います。
- 認証で監視を行う場合は、CHAP 方式を用いた認証で監視を行います。認証結果は監視しないため、RADIUS サーバが認証失敗を通知しても切り替えは発生しません。
- RADIUS サーバ側でログを採取する場合は、大量の監視用の認証成功または失敗のログが出力される可能性があります。監視間隔の設定、RADIUS サーバ側のログ採取の設定には注意してください。
- wlan dot1x backup コマンドで IEEE802.1X 認証のバックアップ解除を自動復旧しない (manual) 設定とした場合、無線 LAN インタフェースはバックアップからマスタに自動復旧はしません。dot1xctl backup recovery コマンドでバックアップ解除を行ってください。

☛ 参照 マニュアル「コマンドリファレンス」の「dot1xctl backup recovery」



認証自動切替機能使用時に、RADIUS サーバの監視異常により IEEE802.1X 認証方式から切り替わっている場合、READY ランプが橙色で点滅します。

● 設定条件

有線 LAN を使ってネットワークに接続する

- 利用するポート : ether1
- IP アドレス : 10.253.10.39/24
- デフォルトルート : 10.253.10.36/24

無線 LAN を使用する (共通)

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g
- チャネル : 10 (11b/g)

仮想アクセスポイント (SSID : samplenet1) を構築する

- 利用する無線 LAN インタフェース : wlan 1
- SSID : samplenet1
- 認証モード : WPA/WPA2 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (サーバ) : aaa1
- 認証自動切替の設定 : マスタとして動作
- バックアップ切り戻し時間
(RADIUS サーバ復旧を検出後のバックアップからマスタへの切り戻し時間)
: 10 秒
- VLAN ID : 10

仮想アクセスポイント (SSID : samplenet2) を構築する

- 利用する無線 LAN インタフェース : wlan 2
- SSID : samplenet2
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで "abcdefghijklmnopqrstuvwxyz"
- IEEE802.1X 認証 : 無効
- 認証自動切替の設定 : バックアップとして動作
- 認証自動切替のバックアップ対象インタフェース
: wlan 1
- VLAN ID : 10

認証 / 課金サーバを AAA 定義で指定する

- aaa 定義番号 : aaa1
- 認証サーバ IP アドレス : 10.253.2.4
- 認証サーバシークレットキー : passwd
- 課金サーバ IP アドレス : 10.253.2.4
- 課金サーバシークレットキー : passwd

認証サーバの監視を設定する

- 認証サーバ監視方法 : 認証による監視 (監視時間はデフォルト値)
- 認証サーバ監視用認証 ID : user00
- 認証サーバ監視用パスワード : passwd

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IEEE802.1X 認証を使用する
# dot1x use on

管理用 VLAN を設定する
# lan 0 ip address 10.253.10.39/24 3
# lan 0 vlan 2

デフォルトルートを設定する
# lan 0 ip route 0 default 10.253.10.36 1

ETHER1 ポートを設定する
# ether 1 vlan tag 2,10

無線 LAN モジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

仮想アクセスポイント (SSID : samplenet1) を設定し、認証自動切替のマスターとして動作させる
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2
# wlan 1 wpa cipher auto
# wlan 1 dot1x use on
# wlan 1 dot1x aaa 1
# wlan 1 dot1x backup master 10s
# wlan 1 dot1x vlan assign disable
# wlan 1 dot1x vid 10

仮想アクセスポイント (SSID : samplenet2) を設定し、認証自動切替のバックアップとして動作させる
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth wpa/wpa2-psk
# wlan 2 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 2 wpa cipher auto
# wlan 2 dot1x backup backup 1
# wlan 2 vlan untag 10

認証/課金サーバを AAA 定義で指定する
# aaa 1 name aaasvr1
# aaa 1 radius service client both
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 10.253.2.4
# aaa 1 radius client server-info auth 0 source 10.253.10.39
# aaa 1 radius client server-info accounting 0 secret passwd
# aaa 1 radius client server-info accounting 0 address 10.253.2.4
# aaa 1 radius client server-info accounting 0 source 10.253.10.39

認証サーバの監視を設定する
# aaa 1 radius client server-info auth 0 watch type auth
# aaa 1 radius client server-info auth 0 watch user user00 passwd

設定終了
# save
# commit
```

1.9 端末台数制限機能を使う

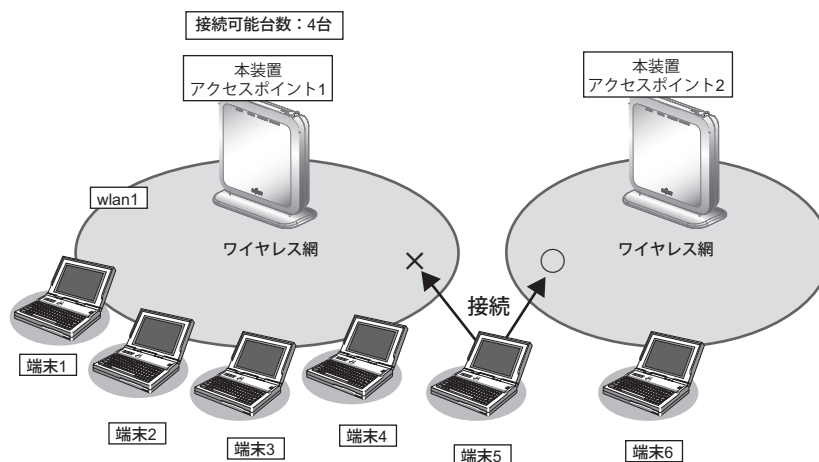
適用機種 SR-M630AP1,610AP1

端末台数制限機能として、接続する端末の台数を制御することにより、通信速度の低下を防ぎます。

無線 LAN 端末は設定した制限数を超えて無線 LAN アクセスポイントに接続することはできません。接続に失敗した無線 LAN 端末には、その理由として端末台数制限によるものであることを伝えることで、ほかの無線 LAN アクセスポイントへの接続を促します。

こんな事に気をつけて

無線 LAN 端末が端末台数制限により接続に失敗し、接続先をほかの無線 LAN アクセスポイントへ変更する動作については、本装置は失敗理由を伝えて変更を促すだけとなります。実際に接続先が変更されるには、無線 LAN 端末が接続先を切り替える動作をサポートしている必要があります。



● 設定条件

無線 LAN を使用する

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g
- チャンネル : 10
- 接続可能台数 : 4
- 仮想アクセスポイントを構築する
- 利用する無線 LAN インタフェース: wlan 1
- SSID : samplenet
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで "abcdefghijklmnopqrstuvwxy"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on  
# ieee80211 1 mode 11b/g  
# ieee80211 1 channel 10
```

接続可能台数を設定する

```
# ieee80211 1 sta limit 4
```

仮想アクセスポイントを設定する

```
# wlan 1 use on  
# wlan 1 ssid samplenet  
# wlan 1 auth wpa/wpa2-psk  
# wlan 1 wpa cipher auto  
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
```

設定終了

```
# save  
# commit
```

1.10 端末台数最低保証機能を使う

適用機種 SR-M630AP1,610AP1

端末台数最低保証機能とは、仮想アクセスポイントごとに、最低でも接続可能な無線 LAN 端末の台数を保証する機能です。

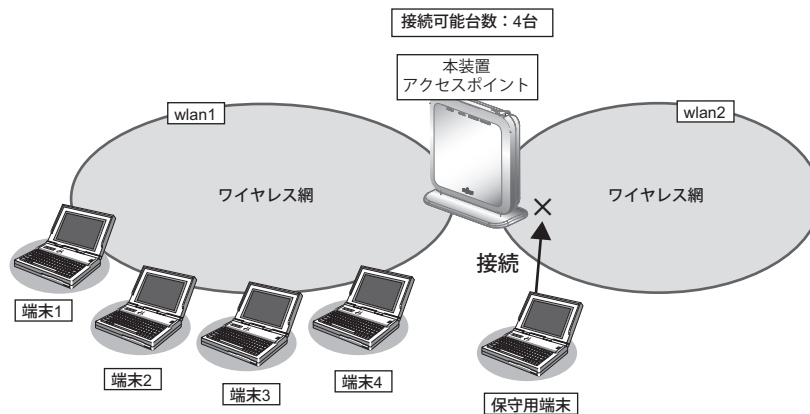
こんな事に気をつけて

- ある無線 LAN モジュールの仮想アクセスポイントすべてに設定されている最低保証台数の合計が、同無線 LAN モジュールの端末台数制限機能による接続可能台数を超えないように設定してください。
- 最低保証する台数は、端末台数制限機能の接続可能台数の中から確保されます。そのため、接続可能台数に到達する前に無線 LAN 端末が接続できなくなることがあります。

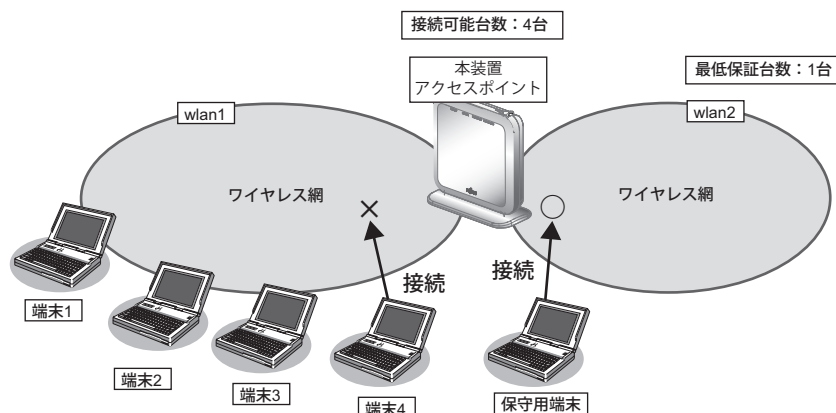
無線LANモジュール 接続可能台数		
仮想アクセスポイント1 最低保証台数	仮想アクセスポイント2 最低保証台数	最低保証されていない 接続可能台数

本機能は以下のような場合に有用です。

本機能を利用していない場合、保守用などの無線 LAN 端末が本装置の端末台数制限機能により接続不可となる場合があります。



ここで、保守用の無線 LAN 端末の接続先である仮想アクセスポイントに、本機能によって最低保証する台数を 1 台設定しておくことで、保守用の無線 LAN 端末は必ず接続することができます。



● 設定条件

無線LANを使用する

- 利用する無線LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g
- チャンネル : 10
- 接続可能台数 : 4

仮想アクセスポイント1を構築する

- 利用する無線LAN インタフェース : wlan 1
- SSID : samplenet1
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで“abcdefghijklmnopqrstuvwxy”

仮想アクセスポイント2を構築する

- 利用する無線LAN インタフェース : wlan 2
- SSID : samplenet2
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで“ABCDEFGHIJKLMNPNOPQRSTUVWXYZ”
- 最低保証台数 : 1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10
# ieee80211 1 sta limit 4
```

仮想アクセスポイント1を設定する

```
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxy
```

仮想アクセスポイント2を設定する

```
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth wpa/wpa2-psk
# wlan 2 wpa cipher auto
# wlan 2 wpa psk text ABCDEFGHIJKLMNPNOPQRSTUVWXYZ
```

仮想アクセスポイント2に最低保証台数を設定する

```
# wlan 2 sta guarantee 1
```

設定終了

```
# save
# commit
```

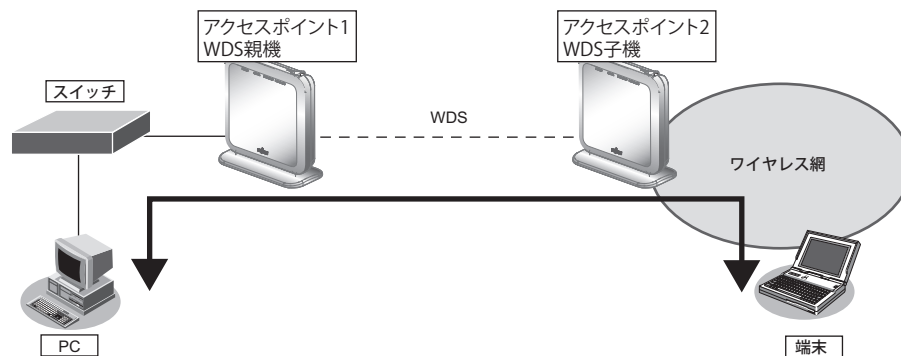
1.11 WDSブリッジ機能を使う

適用機種 SR-M630AP1,610AP1

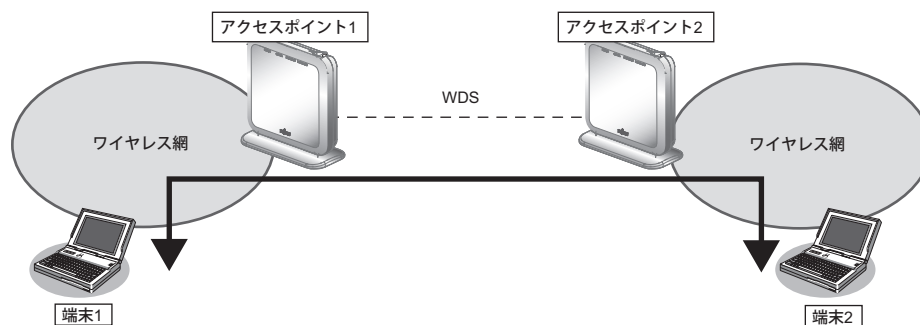
WDSブリッジとは、無線LANアクセスポイントどうしの通信を可能にする機能です。ある無線LANアクセスポイントを中継して別の無線LANアクセスポイントとデータの送受信を行うことができるため、単一の無線LANアクセスポイントを使用した場合に比べて広い範囲での通信が可能となります。

本装置ではWDSブリッジのみで無線LANネットワークを構築することができます。

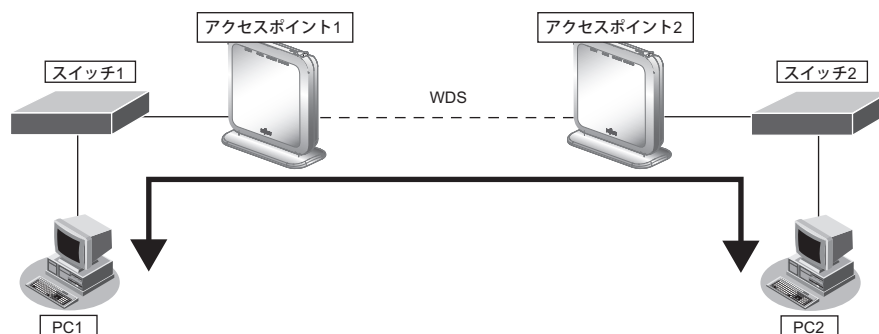
- 有線LANと無線LAN端末間の通信



- 無線LAN端末間の通信

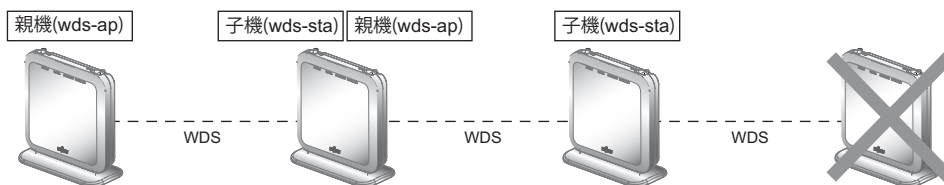


- 有線LAN間の通信

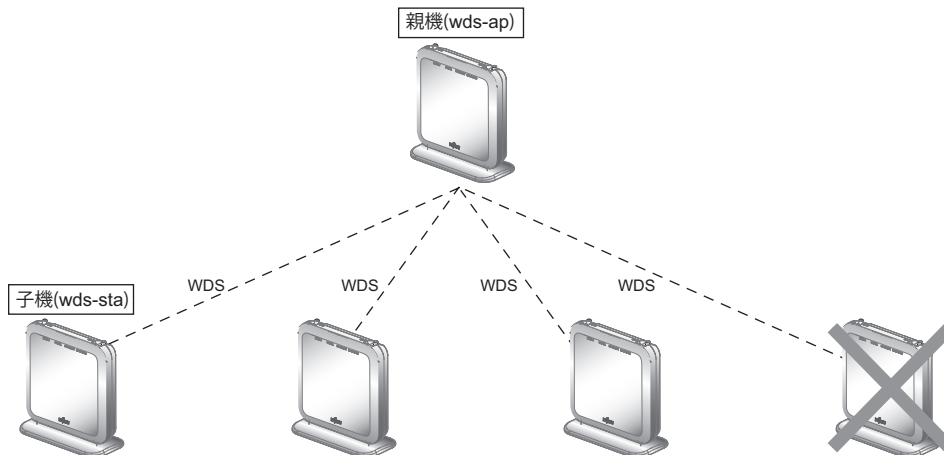


こんな事に気をつけて

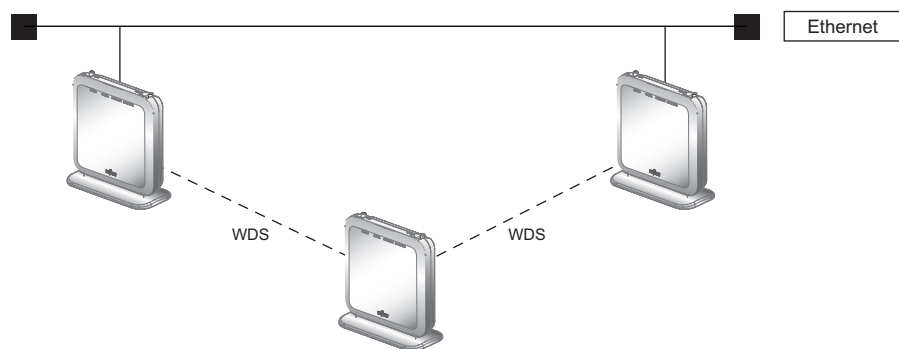
- WDS 親機、子機は同じ通信モードで動作させてください。また通信チャンネルを設定する場合は親機のみを設定してください。
- 本機能のブリッジ処理は、同一の VLAN に割り当てられたインタフェース間でのみ行われます。WDSブリッジ機能を使用する場合は、WDS用のインタフェースを含み、対象のインタフェース (ether, wlan など) が同一の VLAN となるように設定してください。
- 他社の無線 LAN アクセスポイントとの接続はできません。
- WDSブリッジを行う無線 LAN アクセスポイント間では、利用できる通信規格は Wi-Fi6/IEEE802.11ax、認証モードは WPA3-SAE 認証、暗号化モードは AES のみです。WPA3-SAE 認証を利用するため、PMF 機能を有効 (必須) に設定してください。
- 無線 LAN アクセスポイント 1 台との WDSブリッジには、無線 LAN インタフェース 1 つを WDS用のインタフェースとして使用します。そのため、WDS用のインタフェースを生成した数だけ、仮想アクセスポイントとして利用できる無線 LAN インタフェースが減少することになります。
- WDS環境で WDS子機側に接続していた無線 LAN 端末を WDS親機側にローミングすると、WDS子機側のブリッジ学習テーブルが更新されません。そのため、無通信切断時間が満了するまでローミングした無線 LAN 端末は WDS子機側に接続した機器と通信できません。共用で使うサーバやプリンタ等の装置は WDS親機側に接続してください。
- 無線 LAN チャンネルが W53/W56 で動作している場合、レーダを検出することがあります。レーダを検出した場合、チャンネルが自動的に切り替わり、一時的に通信ができなくなることがあります。
- 各無線モジュールに 1 つまで WDS子機を設定することができますが、WDS子機同士は同一の VLAN とならないように設定してください。
- WDS子機 (wds-sta) を設定した装置に WDS親機 (wds-ap) をすることによりカスケード接続することが可能ですが、カスケード接続は 3 段までとしてください。



- 1 台の WDS 親機に対し WDS 子機を複数接続することが可能ですが、3 台までとしてください。

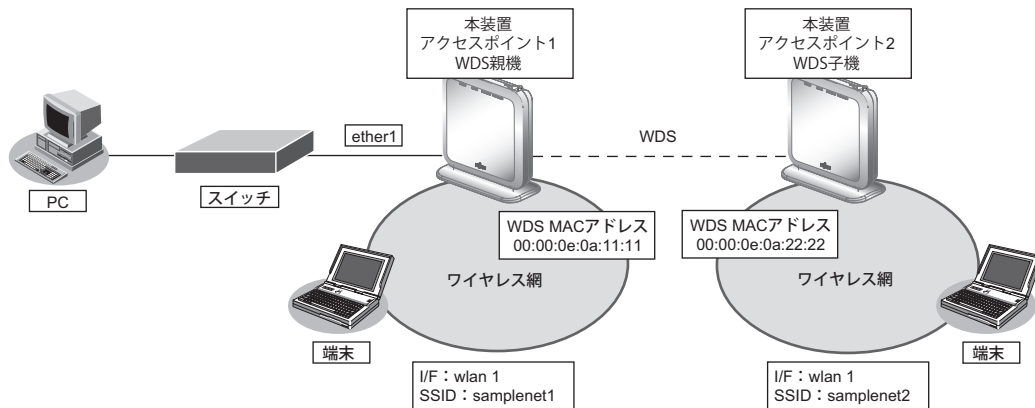


- WDS を利用した以下の図のような冗長なネットワーク構成では、パケットのループが発生するためこのようなネットワーク構成は取らないでください。



WDSブリッジを行う場合の設定方法を説明します。

☞ 参照 VLANを利用したい場合は、[「1.12 VLANネットワークをWDSブリッジ機能で接続する」](#) (P.42) を参照してください。



● 設定条件

[アクセスポイント1 (WDS 親機)]

有線LANを使ってネットワークに接続する

- 利用するポート : ether1

仮想アクセスポイントを構築する

- 利用する無線LANモジュール : ieee80211 1
- 通信モード : IEEE802.11b/g/n/ax
- チャンネル : 1 (11b/g/n/ax)
- 利用する無線LANインタフェース : wlan 1
- SSID : samplenet1
- 認証モード : WPA2-PSK/WPA3-SAE 自動判別認証
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで“abcdefghijklmnopqrstuvwxyz”

WDS (親機) 用の無線LANインタフェースを構築する

- 利用する無線LANモジュール : ieee80211 2
- 通信モード : IEEE802.11ax
- チャンネル : 36
- 利用する無線LANインタフェース : wlan 9
- SSID : samplewds1
- 認証モード : WPA3-SAE 認証
- 暗号化モード : AES
- パスワード : "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

[アクセスポイント2 (WDS子機)]**仮想アクセスポイントを構築する**

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g/n/ax
- チャンネル : 11 (11b/g/n/ax)
- 利用する無線 LAN インタフェース : wlan 1
- SSID : samplenet2
- 認証モード : WPA2-PSK/WPA3-SAE 自動判別認証
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで "zyxwvutsrqponmlkjihgfedcba"

WDS (子機) 用の無線 LAN インタフェースを構築する

- 利用する無線 LAN モジュール : ieee80211 2
- 通信モード : IEEE802.11ax
- チャンネル : 36
- 利用する無線 LAN インタフェース : wlan 9
- 相手無線 LAN アクセスポイント SSID : samplewds1
- 認証モード : WPA3-SAE 認証
- 暗号化モード : AES
- パスワード : "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド**[アクセスポイント1]**

```

仮想アクセスポイントを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 1
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa2-psk/wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 1 wpa pmf mode enable

WDS (親機) 用の無線 LAN インタフェースを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel 36
# wlan 9 use on
# wlan 9 type wds-ap
# wlan 9 auth wpa3-sae
# wlan 9 wpa cipher aes
# wlan 9 wpa sae password ABCDEFGHIJKLMNOPQRSTUVWXYZ
# wlan 9 wpa pmf mode required
# wlan 9 ssid samplewds1

設定終了
# save
# commit

```


[アクセスポイント2]

```
仮想アクセスポイントを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 11
# wlan 1 use on
# wlan 1 ssid samplenet2
# wlan 1 auth wpa2-psk/wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa psk text zyxwvutsrqponmlkjihgfedcba
# wlan 1 wpa pmf mode enable

WDS (子機) 用の無線LAN インタフェースを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel 36
# wlan 9 use on
# wlan 9 type wds-sta
# wlan 9 auth wpa3-sae
# wlan 9 wpa cipher aes
# wlan 9 wpa sae password ABCDEFGHIJKLMNOPQRSTUVWXYZ
# wlan 9 wpa pmf mode required
# wlan 9 ssid samplewds1

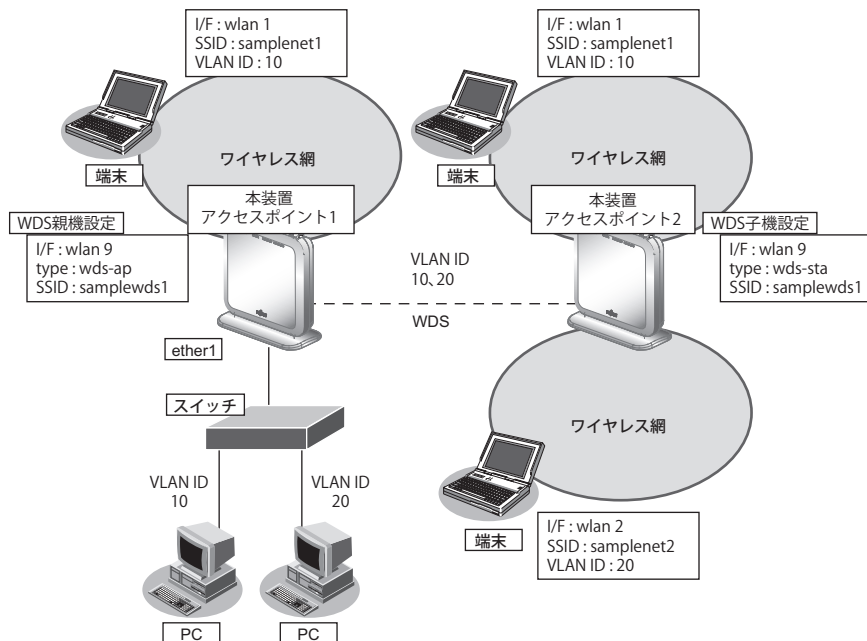
設定終了
# save
# commit
```

1.12 VLAN ネットワークを WDS ブリッジ機能で接続する

適用機種 SR-M630AP1,610AP1

WDSブリッジに利用する無線LANインタフェースをタグ付きのインタフェースとして設定することで、WDSブリッジはVLANネットワークどうしを接続することができます。

ここでは、2台の本装置のそれぞれのVLANネットワークを、WDSブリッジによって接続する場合の設定方法を説明します。



● 設定条件

[アクセスポイント1 (WDS親機)]

有線LAN を使ってネットワークに接続する

- ・ 利用するポート : ether1
- ・ VLAN ID : 10、20

仮想アクセスポイント1を構築する

- ・ 利用する無線LAN モジュール : ieee80211 1
- ・ 通信モード : IEEE802.11b/g/n/ax
- ・ チャンネル : 13
- ・ 利用する無線LAN インタフェース : wlan 1
- ・ SSID : samplenet1
- ・ 認証モード : WPA3-SAE 認証
- ・ 暗号化モード : AES
- ・ パスワード : "12345678"
- ・ VLAN ID : 10

WDS (親機) 用の無線LAN インタフェースを構築する

- ・ 利用する無線LAN モジュール : ieee80211 2
- ・ 通信モード : IEEE802.11ax
- ・ チャンネル : 36

- 利用する無線 LAN インタフェース : wlan 9
- SSID : samplewds1
- 認証モード : WPA3-SAE 認証
- 暗号化モード : AES
- パスワード : "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
- VLAN ID : 10、20

[アクセスポイント2 (WDS子機)]

仮想アクセスポイント1を構築する

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g/n/ax
- チャンネル : 13
- 利用する無線 LAN インタフェース : wlan 1
- SSID : samplenet1
- 認証モード : WPA3-SAE 認証
- 暗号化モード : AES
- パスワード : "12345678"
- VLAN ID : 10

仮想アクセスポイント2を構築する

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g/n/ax
- チャンネル : 13
- 利用する無線 LAN インタフェース : wlan 2
- SSID : samplenet2
- 認証モード : WPA3-SAE 認証
- 暗号化モード : AES
- パスワード : "12345678"
- VLAN ID : 20

WDS (子機) 用の無線 LAN インタフェースを構築する

- 利用する無線 LAN モジュール : ieee80211 2
- 通信モード : IEEE802.11ax
- チャンネル : 36
- 利用する無線 LAN インタフェース : wlan 9
- 相手無線 LAN アクセスポイント SSID : samplewds1
- 認証モード : WPA3-SAE 認証
- 暗号化モード : AES
- パスワード : "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
- VLAN ID : 10、20

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド**[アクセスポイント1]**

```
ETHER1ポートを設定する
# ether 1 vlan tag 10,20

仮想アクセスポイントを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 13
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa sae password 12345678
# wlan 1 wpa pmf mode required
# wlan 1 vlan untag 10

WDS親機用の無線LANインタフェースを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel 36
# wlan 9 use on
# wlan 9 type wds-ap
# wlan 9 ssid samplewds1
# wlan 9 auth wpa3-sae
# wlan 9 wpa cipher aes
# wlan 9 wpa sae password ABCDEFGHIJKLMNOPQRSTUVWXYZ
# wlan 9 wpa pmf mode required
# wlan 9 vlan tag 10,20

設定終了
# save
# commit
```

[アクセスポイント2]

```
仮想アクセスポイント1,2を設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 13
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa sae password 12345678
# wlan 1 wpa pmf mode required
# wlan 1 vlan untag 10
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth wpa3-sae
# wlan 2 wpa cipher aes
# wlan 2 wpa sae password 12345678
# wlan 2 wpa pmf mode required
# wlan 2 vlan untag 20

WDS子機用の無線LANインタフェースを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel 36
# wlan 9 use on
# wlan 9 type wds-sta
```

```
# wlan 9 ssid samplewds1
# wlan 9 auth wpa3-sae
# wlan 9 wpa cipher aes
# wlan 9 wpa sae password ABCDEFGHIJKLMNOPQRSTUVWXYZ
# wlan 9 wpa pmf mode required
# wlan 9 vlan tag 10,20
```

```
設定終了
# save
# commit
```

1.13 MAC アドレスフィルタリング機能を使う

適用機種 SR-M630AP1,610AP1

MAC アドレスフィルタリング機能は、無線 LAN 端末の MAC アドレスを判別し、無線 LAN アクセスポイントへの接続を制御することでセキュリティを向上させることができます。

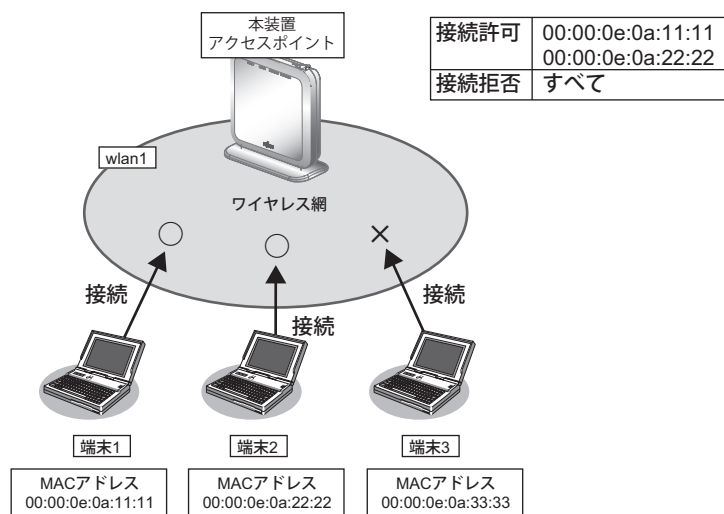
本装置では、送信元 MAC アドレス（無線 LAN 端末の MAC アドレス）のみをフィルタリングの対象とします。

無線 LAN アクセスポイントの MAC アドレスフィルタリングの設計方針には、以下の 2 つがあります。

- 基本的に無線 LAN 端末の接続をすべて拒否し、特定の端末だけ接続を許可する
- 基本的に無線 LAN 端末の接続をすべて許可し、特定の端末だけ接続を拒否する

ここでは、特定の端末だけ接続を許可する設定例について説明します。

特定の端末だけ接続を拒否するには、以下のフィルタリングのポリシーを逆にした設定を行います。



● 設定条件

無線 LAN を使用する

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g
- 11b/g チャンネル : 11

仮想アクセスポイントを構築する

- 利用する無線 LAN インタフェース : wlan 1
- SSID : samplenet
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで“abcdefghijklmnopqrstuvwxy”
- 接続を許可する無線 LAN 端末の MAC アドレス : 00:00:0e:0a:11:11
: 00:00:0e:0a:22:22
- 接続を拒否する無線 LAN 端末の MAC アドレス : その他すべて

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線 LAN モジュールを設定する

```
# ieee80211 1 use on  
# ieee80211 1 mode 11b/g  
# ieee80211 1 channel 11
```

仮想アクセスポイントを設定する

```
# wlan 1 use on  
# wlan 1 ssid samplenet  
# wlan 1 auth wpa/wpa2-psk  
# wlan 1 wpa cipher auto  
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
```

MAC アドレス 00:00:0e:0a:11:11 の無線 LAN 端末からの接続を許可する

```
# acl 0 mac 00:00:0e:0a:11:11 any  
# wlan 1 macfilter 0 pass acl 0
```

MAC アドレス 00:00:0e:0a:22:22 の無線 LAN 端末からの接続を許可する

```
# acl 1 mac 00:00:0e:0a:22:22 any  
# wlan 1 macfilter 1 pass acl 1
```

残りの無線 LAN 端末からの接続をすべて拒否する

```
# wlan 1 macfilter default reject
```

設定終了

```
# save  
# commit
```

1.14 WMM 機能を使う

適用機種 SR-M630AP1,610AP1

WMM 機能とは、無線 LAN 端末に送出するパケットの優先制御を行う機能です。

本機能を利用することで、トラフィックが多い場合でも、音声やビデオなどのパケットを優先的に送出することができ、通信の途切れを軽減することができます。

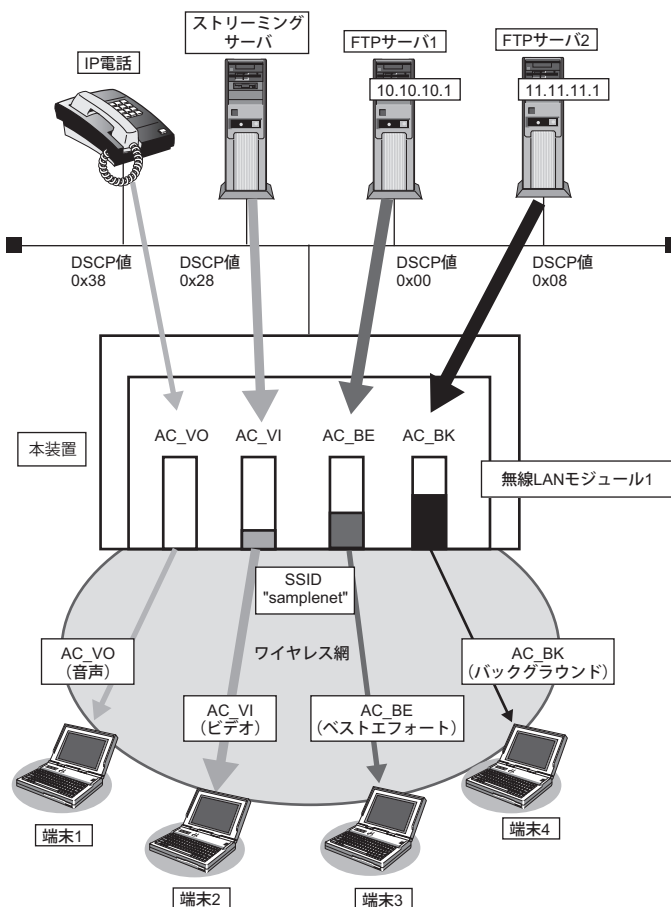
無線に送出するパケットは IP パケットの DSCP 値を元に、4 種類の Access Category (AC) に分類されます。AC は優先度が高い方から、AC_VO (音声)、AC_VI (ビデオ)、AC_BE (ベストエフォート)、AC_BK (バックグラウンド) であり、AC ごとに送信キューを持ちます。送信キューにパケットがたまっている場合は、優先度の低い AC より優先度の高い AC の送信キューから優先的にパケットが送出されます。

こんな事に気をつけて

- 以下のパケットは常に同じ AC に分類されます。

種別	AC
EAPOL パケット	AC_VO
ARP パケット	AC_VO
IP ヘッダを含まないパケット	AC_BE
WMM に対応していない端末あてのパケット	AC_BE

- 本機能は無線 LAN モジュール単位で制御するため、本機能の有効化/無効化を仮想アクセスポイントごとに設定することはできません。同一の無線 LAN モジュールを使用しているほかの仮想アクセスポイントのトラフィックの状況によっては、優先度の高いパケットでも送出が遅れる場合があります。



以下に、DSCP 値と AC の分類の対応表を示します。

DSCP 値は 6 ビットのうち、先頭 3bit だけが AC の分類に使用されます。

DSCP 値	AC 分類		
	10 進数の値	先頭 3bit の値	
0x38 ~ 0x3f 0x30 ~ 0x37	56 ~ 63 48 ~ 55	7 6	AC_VO
0x28 ~ 0x2f 0x20 ~ 0x27	40 ~ 47 32 ~ 39	5 4	AC_VI
0x18 ~ 0x1f 0x00 ~ 0x07	24 ~ 31 0 ~ 7	3 0	AC_BE
0x10 ~ 0x17 0x08 ~ 0x0f	16 ~ 23 8 ~ 15	2 1	AC_BK

● 設定条件

無線 LAN を使用する

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g
- チャンネル : 1
- WMM 機能 : 有効にする

仮想アクセスポイントを構築する

- 利用する無線 LAN インタフェース : wlan 1
- SSID : samplenet
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化 : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで "abcdefghijklmnopqrstuvwxy"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線 LAN モジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 1

WMM 機能を設定する
# ieee80211 1 wmm mode enable

仮想アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxy

設定終了
# save
# commit
```

1.15 周辺アクセスポイント検出機能を使う

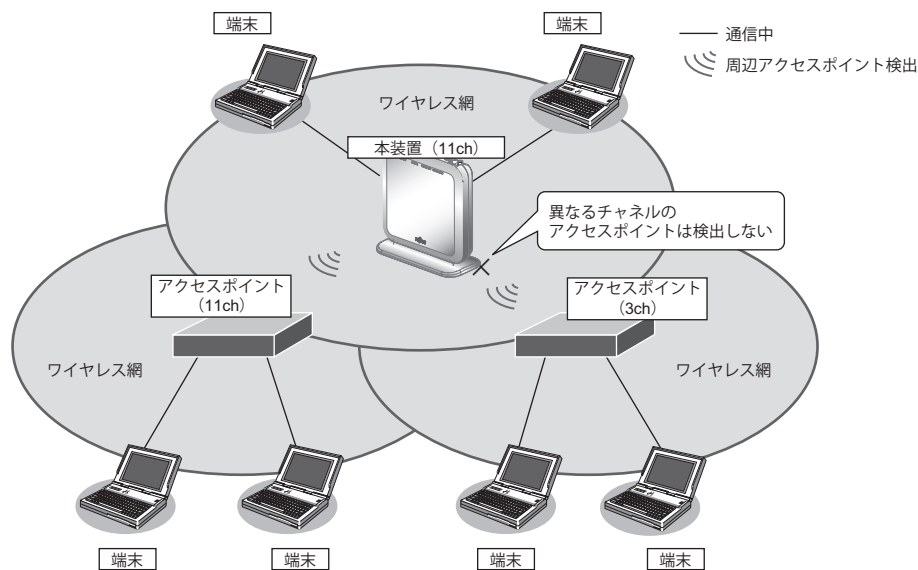
適用機種 SR-M630AP1,SR-M610AP1

無線 LAN アクセスポイントの運用をしながら無線電波を検出することで、本装置周辺の無線 LAN アクセスポイントを検出することができます。周辺アクセスポイントの検出は現在運用中のチャンネルだけで行います。また、手動スキャンを実施することで最新の周辺アクセスポイント情報を知ることができます。

☞ 参照 マニュアル「コマンドリファレンス」の「周辺アクセスポイント情報の取得、表示」

こんな事に気をつけて

- 無線 LAN アクセスポイントの運用では、スループットが低下することがあります。
- 電波干渉により近隣チャンネルで動作している無線 LAN アクセスポイントも検出されることがあります。



● 設定条件

無線 LAN を使用する

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g
- チャンネル : 11
- 周辺アクセスポイント検出の動作モード : enable

仮想アクセスポイントを構築する

- 利用する無線 LAN インタフェース : wlan 1
- SSID : samplenet
- 認証モード : WPA/WPA2-PSK 自動判別認証
- 暗号化モード : TKIP/AES 自動判別
- 事前共有キー (PSK) : テキストで "abcdefghijklmnopqrstuvwxyzyz"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on  
# ieee80211 1 mode 11b/g  
# ieee80211 1 channel 11
```

周辺アクセスポイント検出機能を有効にする

```
# ieee80211 1 apscan mode enable
```

仮想アクセスポイントを設定する

```
# wlan 1 use on  
# wlan 1 ssid samplenet  
# wlan 1 auth wpa/wpa2-psk  
# wlan 1 wpa cipher auto  
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
```

設定終了

```
# save  
# commit
```

1.16 チャンネルボンディング機能を使う

適用機種 SR-M630AP1,610AP1

チャンネルボンディングとは、隣り合った2つのチャンネルを束ねて通信する機能です。無線LANでは、1つのチャンネルを細かいサブキャリア（搬送波）に分割し、各サブキャリアに送信データを載せて通信しますが、チャンネルボンディングを利用するとサブキャリアの数が増えるので、多くのデータを一度に送れるようになります。

本装置で設定が有効となる無線規格と帯域幅の組み合わせは以下のとおりです。

周波数帯	帯域幅	Wi-Fi4 802.11n	Wi-Fi5 802.11ac	Wi-Fi6 802.11ax
2.4GHz	20MHz (※)	○	-	○
	40MHz	○	-	○
	80MHz	-	-	-
5GHz	20MHz (※)	○	○	○
	40MHz	○	○	○
	80MHz	-	○	○

※) 未設定時の初期値

こんな事に気をつけて

- チャンネルボンディングを使用する場合、無線LANクライアントでチャンネルボンディングを有効にする必要があります。
- 2.4GHz帯の場合、ご利用の環境によっては40MHz帯域幅/20MHz帯域幅が自動で切り替わるため、40MHz帯域幅を設定していても、20MHz帯域幅で接続されることがあります。
- 5GHz帯の場合、無線LANアクセスポイントが運用を開始したあとは、他無線LAN装置と電波干渉が発生しても、帯域幅を20MHzに縮退動作することはありません。
- 複数のAPを設置する環境では、AP間で電波干渉せずに利用できるチャンネル数が減ることで、通信速度が低下する場合があります。
- 2.4GHz帯では重なり合わない40MHzチャンネルが1つしか確保できないことに加え、ほかのチャンネルとの干渉が発生しやすいため、チャンネルボンディングは5GHz帯での使用を推奨します
- 802.11nで40MHzの帯域幅を設定する場合は、セカンダリチャンネル番号の設定が必要となります。

802.11nでは、チャンネルボンディング機能を利用できるチャンネルの組み合わせはIEEE802.11n規約によって制限されており、プライマリチャンネル番号とセカンダリチャンネル番号を正しく設定する必要があります。

ieee802mode コマンドで11nが含まれる

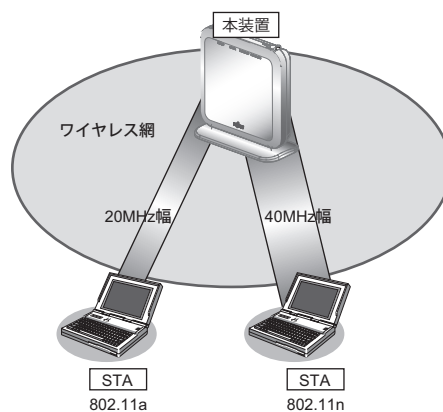
- 11/b/g/n
- 11/b/g/n/ax
- 11/g/n
- 11/g/n/ax
- 11a/n
- 11a/n/ac
- 11a/n/ac/ax

が設定されている場合は、使用するセカンダリチャンネルの指定が必要となります。

本装置では、使用するセカンダリチャンネルを、プライマリチャンネル番号のオフセットとして指定します。

プライマリチャンネル番号（無線LANチャンネル番号）とセカンダリチャンネルオフセットが有効となる組み合わせは以下のとおりです。

周波数帯	プライマリチャンネル番号	セカンダリチャンネル オフセット	セカンダリチャンネル番号
2.4GHz	1	above	5
	2	above	6
	3	above	7
	4	above	8
	5	above	9
		below	1
	6	above	10
		below	2
	7	above	11
		below	3
	8	above	12
		below	4
	9	above	13
	below	5	
	10	below	6
	11	below	7
	12	below	8
	13	below	9
W52	36	above	40
	40	below	36
	44	above	48
	48	below	44
W53	52	above	56
	56	below	52
	60	above	64
	64	below	60
W56	100	above	104
	104	below	100
	108	above	112
	112	below	108
	116	above	120
	120	below	116
	124	above	128
	128	below	124
	132	above	136
	136	below	132
	140	above	144
	144	below	140



● 前提条件

- 本装置、無線 LAN クライアントで、チャンネルボンディング以外は、正しく設定されている。

● 設定条件

- チャンネルボンディング : 使用する (40MHz の帯域を使用する)
- プライマリチャンネル番号 : 52 チャンネル
- セカンダリチャンネル番号 : 56 チャンネル

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel 52

チャンネルボンディング機能を設定する
# ieee80211 2 bandwidth 40
# ieee80211 2 secondary-channel above

設定終了
# save
# commit
```

1.17 バンドステアリング機能を使う

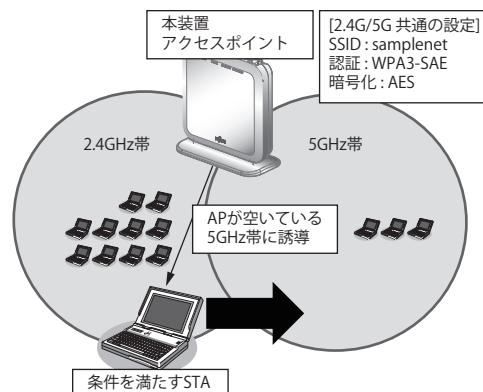
適用機種 SR-M630AP1,610AP1

ここではバンドステアリング機能により 2.4GHz 帯に接続されている無線 LAN 端末を、混雑していない 5GHz 帯の周波数帯に振り分ける場合の設定方法を説明します。

こんな事に気をつけて

- バンドステアリング機能を有効にするには、お使いになる 2.4GHz と 5GHz の仮想アクセスポイントの設定は、原則すべて共通にする必要があります。例えば以下の設定が対象となります。
 - SSID の名称
 - SSID 非通知と ANY 接続拒否の設定
 - IEEE802.11 認証モードの設定
 - IEEE802.1X 認証の設定
 - MAC アドレス認証の設定
 - フィルタリングの設定
- 本機能が有効になる無線 LAN 端末は以下の条件をすべて満たす必要があります。ただし、無線 LAN 端末の機能や仕様により周波数帯が切り替わらない場合があります。
 - 2.4GHz 帯と 5GHz 帯の両周波数帯に対応
 - IEEE802.11k、IEEE802.11v をサポート
 - AP との通信状態が良好
- バンドステアリング機能を使用する場合は、必ず 2.4GHz 帯の無線モジュール 1 を有効にしてください。5GHz 帯の無線モジュールのみを有効にしても、使用できません。
- バンドステアリング機能の有効設定コマンドは、必ず 2.4GHz 帯の仮想アクセスポイントに対してのみ設定してください。
- IEEE802.1X 認証または MAC アドレス認証にて、認証サーバから通知された VLAN を割り当てる機能 (wlan dot1x vlan assign enable/wlan macauth vlan assign enable) を利用する場合、バンドステアリング機能は動作しません。本機能を利用する場合は、認証サーバから通知された VLAN を割り当てる機能を無効に設定し、端末 (Supplicant) に割り当てるデフォルト VLAN ID 機能 (wlan dot1x vid / wlan macauth vid) を利用してください。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール : ieee80211 1 (2.4GHz 帯) および ieee80211 2 (5GHz 帯)
- 利用する無線 LAN インタフェース: wlan 1 (2.4GHz 帯) および wlan9 (5GHz 帯)

- 通信モード : IEEE802.11b/g/n/ax (2.4GHz 帯) および
IEEE802.11a/n/ac/ax (5GHz 帯)
- チャンネル : 13 および 48
- 無線 LAN インタフェース数 : 8
- SSID : samplenet
- 認証モード : WPA3-SAE
- 暗号化モード : AES
- パスワード : テキストで "12345678"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 13
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel 48
```

無線LANインタフェース数を設定する

```
# wlan-conf wlan-num 8
```

無線LANインタフェースを設定する

```
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa sae password 12345678
# wlan 1 wpa pmf mode required
# wlan 9 use on
# wlan 9 ssid samplenet
# wlan 9 auth wpa3-sae
# wlan 9 wpa cipher aes
# wlan 9 wpa sae password 12345678
# wlan 9 wpa pmf mode required
```

2.4GHz帯の仮想アクセスポイントにバンドステアリング機能の有効を設定する

```
# wlan 1 band-steering mode enable
```

設定終了

```
# save
# commit
```


1.18 エアタイムフェアネス機能を使う

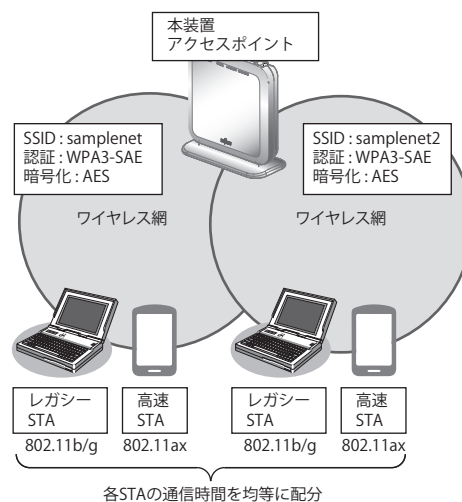
ここでは、エアタイムフェアネス機能により、各無線 LAN 端末の通信時間を均等に割り当てる場合の設定方法を説明します。レガシー端末 (802.11a/b/g) が混在している環境において、高速な端末が低速なレガシー端末の無線占有時間の影響により、通信速度が低下する問題を解決できます。

またエアタイムフェアネス機能では、SSID 毎に重みづけをすることもできます。

こんな事に気をつけて

- エアタイムフェアネス機能を有効に設定した場合、すべての無線モジュールに対して機能が有効になります。無線モジュール単位での有効/無効の制御はできません。
- エアタイムフェアネス機能は、有効に設定した後、構成定義をセーブし、再起動した後から機能が有効になります。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール : ieee80211 1 (2.4GHz 帯)
- 利用する無線 LAN インタフェース: wlan 1 および wlan2
- 通信モード : IEEE802.11b/g/n/ax
- チャンネル : 13
- 無線 LAN インタフェース数 : 8
- SSID : samplenet および samplenet2
- 認証モード : WPA3-SAE
- 暗号化モード : AES
- パスワード : テキストで "12345678"
- SSID 毎の重みづけ : しない

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 13
```

無線LANインタフェース数を設定する

```
# wlan-conf wlan-num 8
```

無線LANインタフェースを設定する

```
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa sae password 12345678
# wlan 1 wpa pmf mode required
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth wpa3-sae
# wlan 2 wpa cipher aes
# wlan 2 wpa sae password 12345678
# wlan 2 wpa pmf mode required
```

エアタイムフェアネスの設定をする

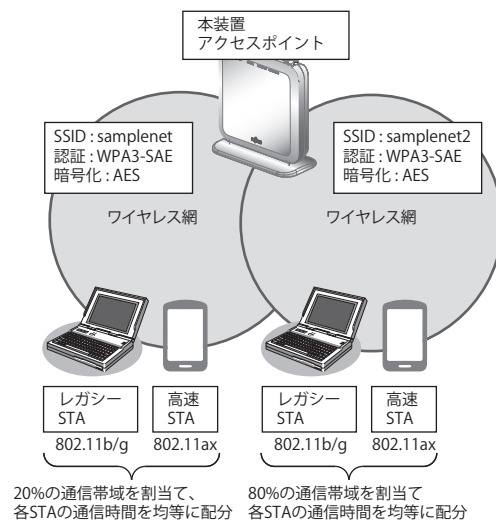
```
# atf use on
```

設定終了

```
# save
# reset
```

● 設定条件

SSID 毎の重みづけを追加設定する



無線LANインタフェース	重みづけ (%)	動作条件
wlan 1	20	帯域使用率が20%までwlan1のSTAが優先されます。 なお、wlan1のSTAでの帯域使用率が20%未満の場合は他無線LANインタフェースのSTAも未使用帯域を利用できます。
wlan 2	80	帯域使用率が80%までwlan2のSTAが優先されます。 なお、wlan2のSTAでの帯域使用率が80%未満の場合は他無線LANインタフェースのSTAも未使用帯域を利用できます。

こんな事に気をつけて

- エアタイムフェアネス機能の重みづけ設定を行う場合、同一無線モジュールでの合計が 100% を超えない値で設定してください。100% を超える値が設定された場合、重みづけ機能は正しく動作しません。
- 合計が 100% にならない重みづけを行った場合、残りのパーセンテージは SSID による重みづけがない帯域として動作します。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

エアタイムフェアネスの重みづけ設定を追加する

```
# wlan 1 atf ratio 20
```

```
# wlan 2 atf ratio 80
```

設定終了

```
# save
```

```
# commit
```

1.19 無線 LAN アクセスポイントを屋外で利用する

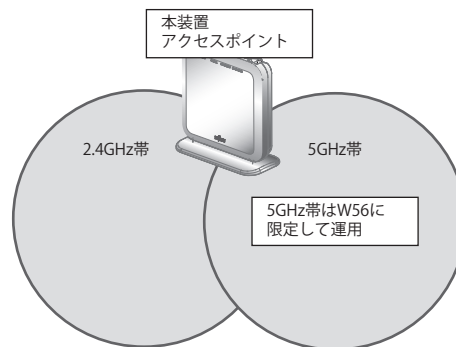
適用機種 SR-M630AP1,610AP1

周波数帯 W52(5.2GHz)、W53(5.3GHz) 電波の屋外での使用は電波法により禁じられています。ここでは屋外利用が可能な周波数帯 2.4GHz 帯域、W56(5.6GHz) 帯域に限定して、本製品を利用するために必要な設定方法を説明します。

こんな事に気をつけて

- SR-M630AP1 では、無線モジュール 2(W52/W53) を必ず未使用に設定してください。
- SR-M610AP1 では、無線モジュール 2(W52/W53/W56) に対して、屋外モード (W56 限定) を有効に設定した後、構成定義をセーブし、再起動した後から屋外利用可能になります。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件 (SR-M630AP1)

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール : ieee80211 1 (2.4GHz 帯) および ieee80211 3 (W56)
- 利用する無線 LAN インタフェース : wlan 1 (2.4GHz 帯) および wlan17 (W56)
- 通信モード : IEEE802.11b/g/n/ax (2.4GHz 帯) および IEEE802.11a/n/ac/ax (W56)
- チャンネル : 13 および 100
- 無線 LAN インタフェース数 : 8
- SSID : samplenet および samplenet2
- 認証モード : WPA3-SAE
- 暗号化モード : AES
- パスワード : テキストで "12345678"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANを使ってアクセスポイントを構築する
無線LANモジュールを設定する。
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 13
# ieee80211 2 use off
# ieee80211 3 use on
# ieee80211 3 mode 11a/n/ac/ax
# ieee80211 3 channel 100
```

```
無線LANインタフェース数を設定する
# wlan-conf wlan-num 8
```

```
無線LANインタフェースを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa sae password 12345678
# wlan 1 wpa pmf mode required
# wlan 17 use on
# wlan 17 ssid samplenet2
# wlan 17 auth wpa3-sae
# wlan 17 wpa cipher aes
# wlan 17 wpa sae password 12345678
# wlan 17 wpa pmf mode required
```

```
設定終了
# save
# commit
```

● 設定条件 (SR-M610AP1)

無線LANを使ってアクセスポイントを構築する

- 利用する無線LANモジュール : ieee80211 1 (2.4GHz帯) および ieee80211 2 (W56)
- 利用する無線LANインタフェース : wlan 1 (2.4GHz帯) および wlan9 (W56)
- 通信モード : IEEE802.11b/g/n/ax (2.4GHz帯) および IEEE802.11a/n/ac/ax (W56)
- チャンネル : 13および100
- 無線LANインタフェース数 : 8
- SSID : samplenetおよびsamplenet2
- 認証モード : WPA3-SAE
- 暗号化モード : AES
- パスワード : テキストで"12345678"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する。
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
# ieee80211 1 channel 13
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel 100
```

無線LANインタフェース数を設定する

```
# wlan-conf wlan-num 8
```

無線LANインタフェースを設定する

```
# wlan 1 use on
```

```
# wlan 1 ssid samplenet
```

```
# wlan 1 auth wpa3-sae
```

```
# wlan 1 wpa cipher aes
```

```
# wlan 1 wpa sae password 12345678
```

```
# wlan 1 wpa pmf mode required
```

```
# wlan 9 use on
```

```
# wlan 9 ssid samplenet2
```

```
# wlan 9 auth wpa3-sae
```

```
# wlan 9 wpa cipher aes
```

```
# wlan 9 wpa sae password 12345678
```

```
# wlan 9 wpa pmf mode required
```

SR-M610AP1の無線モジュール2に対して、屋外モード(W56限定)を有効にする

```
# ieee80211 2 outdoormode on
```

設定終了

```
# save
```

```
# reset
```

1.20 144ch のサポートを無効に設定する

適用機種 SR-M630AP1,610AP1

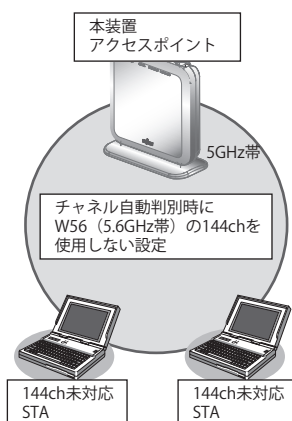
ここでは、2019年に追加されたW56(5.6GHz)帯域の144chに対して、無線LANアクセスポイント側の144chサポートを無効にする設定方法を説明します。

特にチャンネル自動判別設定時には、基本的に混雑していないチャンネルを無線LANアクセスポイントが選択しますが、本設定により144chを選択しなくなることで、144ch未対応端末が接続できない事象を回避することができます。

こんな事に気をつけて

- 本製品の初期設定時は144chサポートが有効になっています。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☛ 参照 マニュアル「ご利用にあたって」



● 設定条件 (SR-M630AP1)

無線LANを使ってアクセスポイントを構築する

- 利用する無線LANモジュール : ieee80211 3 (W56)
- 利用する無線LANインタフェース : wlan17
- 通信モード : IEEE802.11a/n/ac/ax
- チャンネル : 自動判別
- 無線LANインタフェース数 : 8
- SSID : samplenet
- 認証モード : WPA3-SAE
- 暗号化モード : AES
- パスワード : テキストで"12345678"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```

無線LANモジュールを設定する
# ieee80211 3 use on
# ieee80211 3 mode 11a/n/ac/ax
# ieee80211 3 channel any

無線LANモジュールの144chサポートを無効にする
# ieee80211 3 144ch-support disable

無線LANインタフェース数を設定する
# wlan-conf wlan-num 8

無線LANインタフェースを設定する
# wlan 17 use on
# wlan 17 ssid samplenet
# wlan 17 auth wpa3-sae
# wlan 17 wpa cipher aes
# wlan 17 wpa sae password 12345678
# wlan 17 wpa pmf mode required

設定終了
# save
# commit

```

● 設定条件 (SR-M610AP1)

無線LAN を使ってアクセスポイントを構築する

- 利用する無線LAN モジュール : ieee80211 2 (W52/W52/W56)
- 利用する無線LAN インタフェース: wlan9
- 通信モード : IEEE802.11a/n/ac/ax
- チャンネル : 自動判別
- 無線LAN インタフェース数 : 8
- SSID : samplenet
- 認証モード : WPA3-SAE
- 暗号化モード : AES
- パスワード : テキストで"12345678"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```

無線LANモジュールを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac/ax
# ieee80211 2 channel any

無線LANモジュールの144chサポートを無効にする
# ieee80211 2 144ch-support disable

無線LANインタフェース数を設定する
# wlan-conf wlan-num 8

無線LANインタフェースを設定する
# wlan 9 use on
# wlan 9 ssid samplenet
# wlan 9 auth wpa3-sae
# wlan 9 wpa cipher aes

```



```
# wlan 9 wpa sae password 12345678  
# wlan 9 wpa pmf mode required
```

```
設定終了  
# save  
# commit
```

1.21 空間再利用機能を使用する

適用機種 SR-M630AP1,610AP1

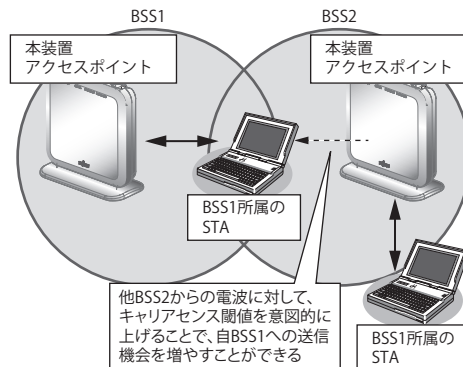
Wi-Fi6では高密度環境下にある無線LANアクセスポイントと無線LAN端末の空間利用状況を識別するためBSSグループをカラー分けしています。これにより他BSSグループから同一の周波数チャンネルで送られてくる電波を受信しても、設定されたキャリアセンス閾値以下であれば無視し、そのチャンネルリソースを自BSSグループの為にだけ使用できるようになるため全体の空間再利用率が上昇する事になります。

本製品で空間再利用機能を利用するために必要な設定方法を説明します。

こんな事に気をつけて

- 本製品の初期設定時は空間再利用機能が有効になっています。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおりに設定しても通信できないことがあります。

☞ 参照 マニュアル「ご利用にあたって」



● 設定条件

無線LANを使ってアクセスポイントを構築する

- 利用する無線LANモジュール : ieee80211 1 (2.4GHz帯)
- 利用する無線LANインタフェース : wlan 1
- 通信モード : IEEE802.11b/g/n/ax
- チャンネル : 13
- 無線LANインタフェース数 : 8
- SSID : samplenet
- 認証モード : WPA3-SAE
- 暗号化モード : AES
- パスワード : テキストで“12345678”
- キャリアセンス閾値 : -70dBm

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on  
# ieee80211 1 mode 11b/g/n/ax  
# ieee80211 1 channel 13
```

空間再利用を有効に設定する

```
# ieee80211 1 sr use on
```

キャリアセンス閾値を-70dBmに設定する

```
# ieee80211 1 sr tx-threshold 70
```

無線LANインタフェース数を設定する

```
# wlan-conf wlan-num 8
```

無線LANインタフェースを設定する

```
# wlan 1 use on  
# wlan 1 ssid samplenet  
# wlan 1 auth wpa3-sae  
# wlan 1 wpa cipher aes  
# wlan 1 wpa sae password 12345678  
# wlan 1 wpa pmf mode required
```

設定終了

```
# save  
# commit
```

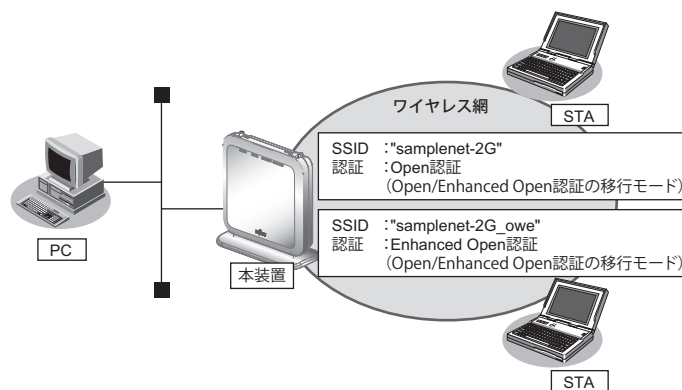
1.22 Enhanced Open 認証を使う

適用機種 SR-M630AP1,610AP1

Enhanced Open 認証を使用することで、ユーザー認証を行わないオープンな環境であっても、盗聴などのリスクからデータを保護することができます。

こんな事に気をつけて

- 従来 Open 認証と互換性を持たせた Open 認証 / Enhanced Open 認証の移行モード (OWE Transition mode) で認証設定を行う場合、2つの無線 LAN インタフェースをペアで使用します。IEEE802.11 認証モード (wlan auth コマンド) は open/enhanced-open (Open 認証として使用) と open/enhanced-open_owe (Enhanced Open 認証として使用) を使用します。
- Enhanced Open 認証を使用する無線 LAN インタフェースには PMF 機能は有効 (必須) を設定してください。
- Enhanced Open 認証を使用する無線 LAN インタフェースに接続する端末は Enhanced Open に対応している必要があります。



● 設定条件

Open 認証 / Enhanced Open 認証の移行モードでアクセスポイントを構築する。

- 利用する無線 LAN モジュール : ieee80211 1 (2.4GHz 帯)
- 通信モード : IEEE802.11b/g/n/ax
- チャンネル : 6
- Open 認証として利用する無線 LAN インタフェース : wlan 1 (2.4GHz 帯)
- SSID (Open 認証) : samplenet-2G
- 認証モード (Open 認証) : Open 認証 (Open 認証 / Enhanced Open 認証の移行モード)
- Enhanced Open 認証として利用する無線 LAN インタフェース : wlan 2 (2.4GHz 帯)
- SSID (Enhanced Open 認証) : samplenet-2G_owe
- 認証モード (Enhanced Open 認証) : Enhanced Open 認証 (Open 認証 / Enhanced Open 認証の移行モード)

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

無線LANモジュールを設定する

```
# ieee80211 1 use on  
# ieee80211 1 mode 11b/g/n/ax  
# ieee80211 1 channel 6
```

無線LANインタフェース数を設定する

```
# wlan-conf wlan-num 8
```

Open/Enhanced Open認証（移行モード）のアクセスポイントを設定する

```
# wlan 1 use on  
# wlan 1 ssid samplenet-2G  
# wlan 1 auth open/enhanced-open  
# wlan 1 wpa owe_trans 2
```

```
# wlan 2 use on  
# wlan 2 ssid samplenet-2G_owe  
# wlan 2 auth open/enhanced-open_owe  
# wlan 2 wpa pmf mode required
```

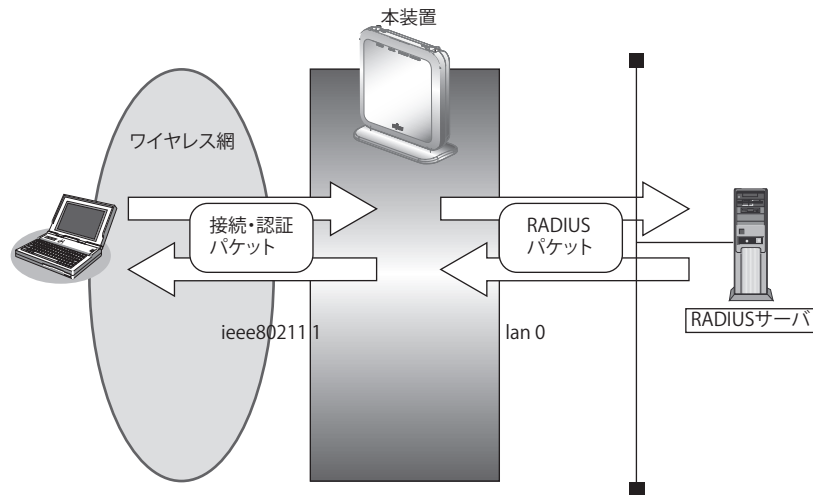
設定終了

```
# save  
# commit
```

1.23 パケットキャプチャ機能を使う

適用機種 SR-M630AP1,610AP1

本装置が送受信した特定の packets をキャプチャすることができます。運用中の通信トラブル等の解析に活用することができます。対象となる packet データは、無線上の接続・認証シーケンスで使用する packet、または RADIUS サーバとの認証シーケンスで使用する packet です。



- 接続・認証パケット
無線端末の接続時に使用する 802.11 の管理フレーム（Probe Request など）および EAPOL フレームを指します
- RADIUS パケット
RADIUS 認証サーバとの通信で使用する EAP プロトコルの packet を指します。

ここでは、パケットキャプチャ機能を使用する場合の操作方法を説明します。
無線 LAN を使ったアクセスポイントが動作していることを前提に説明します。

パケットキャプチャを採取する

コマンドで開始を指示することで、本装置内に packet データの蓄積を開始します。コマンドで停止を指示することで、packet 解析ソフト（Wireshark など）で解析可能なキャプチャファイル（PCAP 形式）を本装置内に生成します。生成されるキャプチャファイル名は下記の名称となります。

ieee80211.pcap : 接続・認証 packet のキャプチャファイル
radius.pcap : RADIUS packet のキャプチャファイル

● 採取条件

- 採取する無線 LAN モジュール : ieee80211 1 (2.4GHz 帯)
- 採取する LAN インタフェース : lan0
- 採取する packet : 接続・認証 packet、および RADIUS packet

● コマンド

- パケットキャプチャを採取する

```
無線モジュール番号を指定して接続・認証パケットのキャプチャを開始する
# capturectl start iieee80211 1
```

```
使用するLANインタフェース番号を指定してRADIUSパケットのキャプチャを開始する
# capturectl start radius 0
```

```
接続・認証パケットのキャプチャを停止する
# capturectl stop iieee80211
```

```
RADIUSパケットのキャプチャを停止する
# capturectl stop radius
```

キャプチャファイルを取り出す

キャプチャファイルは、FTP 経由または copy コマンドで取り出すことができます。

- copy コマンドで USB メモリに取り出す

```
# copy iieee80211.pcap /um0/ieee80211.pcap
# copy radius.pcap /um0/radius.pcap
```

- パソコンから ftp get を使用して取り出す

```
PS C:\tmp> ftp 192.168.1.1
Connected to 192.168.1.1.
220 SR-M610AP1 V20.04 FTP server (config1) ready.
530 Login with USER and PASS
User (192.168.1.1:(none)): ftp-admin
331 Please specify password
Password:
230 Operation successful
ftp> get iieee80211.pcap
200 Operation successful
150 Opening BINARY connection for iieee80211.pcap (80164 bytes)
226 Operation successful
ftp: 80164 bytes received in 0.00Seconds 80164000.00Kbytes/sec.
ftp> get radius.pcap
200 Operation successful
150 Opening BINARY connection for radius.pcap (2172 bytes)
226 Operation successful
ftp: 2172 bytes received in 0.00Seconds 2172000.00Kbytes/sec.
ftp> bye
221 Operation successful
PS C:\tmp>
```

こんな事に気をつけて

- 本機能は、無線上で行われる他無線 LAN 装置間の通信をキャプチャすることはできません。
- 同時に複数の無線モジュールに対して、キャプチャを開始することはできません。また、同様に、複数の LAN インタフェースに対して、キャプチャを開始することはできません。
- パケットキャプチャを開始した際、本装置に保存されていたキャプチャファイルは削除されます。先に退避した後、開始を行ってください。
- キャプチャファイルのサイズには上限があります。上限を超えてキャプチャを行った場合、最新のパケットデータが記録され、古いパケットデータから順次削除されます。
- パケットデータは、タイムスタンプ順に記録されない場合があります。パケット解析ソフトのソート機能で、タイムスタンプ順に表示してください。

- パケットデータにおいて、本装置が送信するパケットの IEEE802.11 ヘッダの Duration フィールド・Sequence Control フィールドについては正しい値が記録されません。実際に送信されるパケットと差異があるため注意してください。
-

2 VLAN 機能を使う

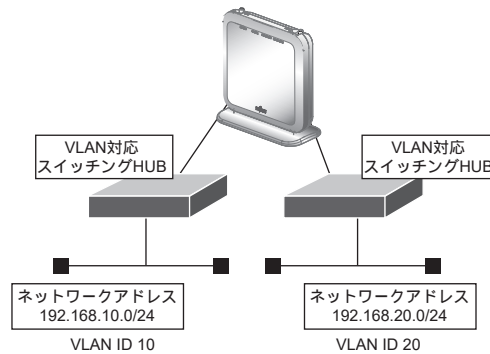
適用機種 SR-M630AP1,610AP1

☞ 参照 マニュアル「機能説明書」

2.1 ポート VLAN 機能を使う

適用機種 SR-M630AP1,610AP1

ここでは、ポート単位でグループ化したタグなしパケットをポート VLAN で送受信する場合の設定方法を説明します。



● 設定条件

- ETHER1、2 ポートを使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける

VLAN ID : 10	ネットワークアドレス : 192.168.10.0/24
VLAN ID : 20	ネットワークアドレス : 192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan untag 10

ETHER2 ポートを設定する
# ether 2 vlan untag 20

192.168.10.1/24 のネットワークを設定する
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

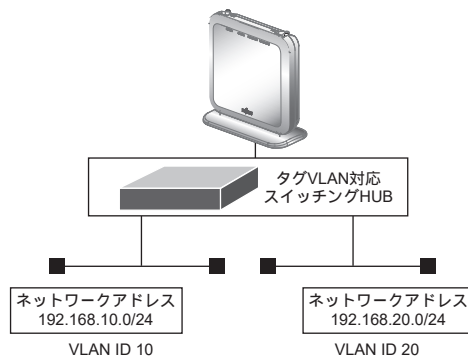
192.168.20.1/24 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

2.2 タグVLAN機能を使う

適用機種 SR-M630AP1,610AP1

ここでは、1つのポートで、2つのVLANからのタグ付きパケットを、それぞれのVLANで送受信する場合の設定方法を説明します。



● 設定条件

- ETHER1ポートだけを使用する
- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける

VLAN ID : 10	ネットワークアドレス : 192.168.10.0/24
VLAN ID : 20	ネットワークアドレス : 192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER1ポートを設定する
# ether 1 vlan tag 10,20

ETHER2ポートを未設定にする
# ether 2 use off

192.168.10.1/24のネットワークを設定する
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

192.168.20.1/24のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

3 リンクアグリゲーション機能を使う

適用機種 SR-M630AP1

ここでは、2ポートの1000M回線をリンクアグリゲーションとする場合の設定方法を説明します。

● 設定条件

- ETHER1～2ポートを使用する
- 通信速度を1000Mbps固定に変更する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER1～2ポートを設定する
# ether 1 mode 1000
# ether 2 mode 1000
# ether 1 vlan tag 10,20
# ether 2 vlan tag 10,20

ETHER1～2ポートをリンクアグリゲーションとして設定する
# ether 1 type linkaggregation 1
# ether 2 type linkaggregation 1

設定終了
# save
# commit
```

3.1 LACP 機能を使う

適用機種 SR-M630AP1

ここでは、2ポートの1000M回線をLACPを利用したリンクアグリゲーションとする場合の設定方法を説明します。

● 設定条件

- ETHER1～2ポートを使用する
- 通信速度を1000Mbps固定に変更する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER1～2ポートを設定する
# ether 1 mode 1000
# ether 2 mode 1000
# ether 1 vlan tag 10,20
# ether 2 vlan tag 10,20

ETHER1～2ポートをリンクアグリゲーションとして設定する
# ether 1 type linkaggregation 1
# ether 2 type linkaggregation 1

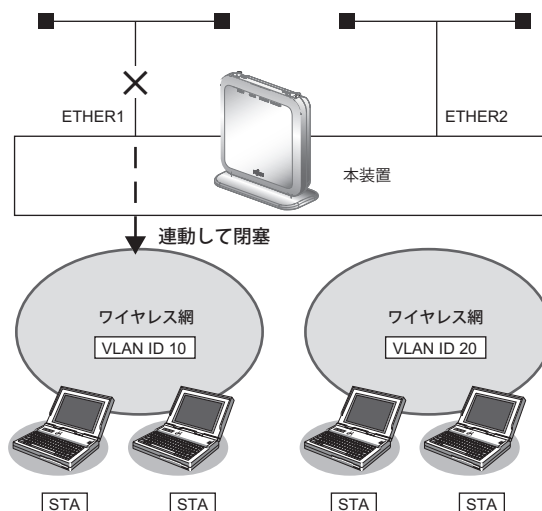
LACPを利用したリンクアグリゲーションとして設定する
# linkaggregation 1 mode active

設定終了
# save
# commit
```

4 リンクインテグリティ機能を使う

適用機種 SR-M630AP1,610AP1

ここでは、ETHER ポートがリンクダウンした場合、連動して指定した無線 LAN インタフェースを閉塞させる場合の設定方法について説明します。



● 設定条件

- ETHER1 ポートに連動して無線 LAN インタフェース 1～8 を閉塞させる
 利用する無線 LAN インタフェース： wlan 1～wlan 8
 VLAN ID : 10
- ETHER2 ポートに連動して無線 LAN インタフェース 9～16 を閉塞させる
 利用する無線 LAN インタフェース： wlan 9～wlan 16
 VLAN ID : 20

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan tag 10

ETHER2 ポートを設定する
# ether 2 vlan tag 20

ETHER1 ポートがリンクダウンした場合、WLAN1～8 が連動して閉塞状態になるように設定する
# ether 1 downrelay wlan 1-8

ETHER2 ポートがリンクダウンした場合、WLAN9～16 が連動して閉塞状態になるように設定する
# ether 2 downrelay wlan 9-16

自動的に閉塞解除するモードに設定する
# ether 1 downrelay recovery mode auto
# ether 2 downrelay recovery mode auto

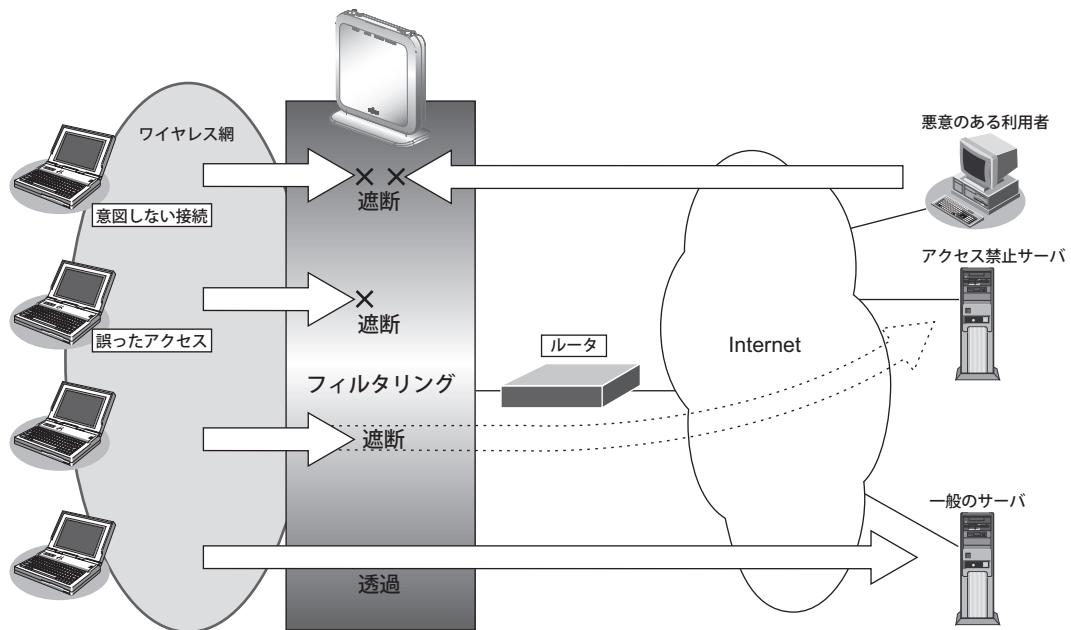
設定終了
# save
# commit
```

5 フィルタリング機能を使う

適用機種 SR-M630AP1,610AP1

本装置を経由するパケットを、IPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティの向上や、ネットワークへの負荷を軽減することができます。

☛ 参照 マニュアル「機能説明書」



フィルタリングの条件

本装置では、ACL番号で指定したACL定義の中で、以下の条件を指定することによってデータの流れを制御できます。

- 送信元情報 (IPアドレス/アドレスマスク/ポート番号)
- あて先情報 (IPアドレス/アドレスマスク/ポート番号)
- プロトコル
- TCP・UDPのポート番号
- ICMPのTYPE

💡 ヒント

◆ IPアドレスとアドレスマスクの決め方

IPフィルタリング条件の要素には「IPアドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットのIPアドレスとアドレスマスクの論理積の結果が、指定したIPアドレスと一致したものに限りです。

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる
- B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定サービスへのアクセスだけを許可する

なお、設定例はデフォルトVLAN (VLAN ID = 1) での通信を前提として説明します。

こんな事に気をつけて

- IPフィルタリングでDHCP (ポート番号67、68) でのアクセスを制限する設定を行った場合、DHCP機能が使用できなくなる場合があります。
 - 本装置のフィルタリング機能は、IPフィルタとなります。
フィルタリング処理が適用されるのは、以下の通信となります。
 - 本装置宛ての通信
 - 有線-無線インタフェース間の通信
 - 無線-無線インタフェース間の通信 (但し、同一無線LANインタフェース内の折り返し通信は対象外)IPフィルタ処理は、レイヤ3レベルでのソフトウェア処理のため、レイヤ2レベルでのVLAN単位での制御はできず、IPフィルタ条件のみの制御となります。
そのためvlan filter コマンドを設定するVLAN IDには意味を持ちません。
ご使用されるVLANのうち任意のVLAN IDを1つ選んでいただき、装置全体のフィルタリングルールとして設定してください。
 - フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。
-

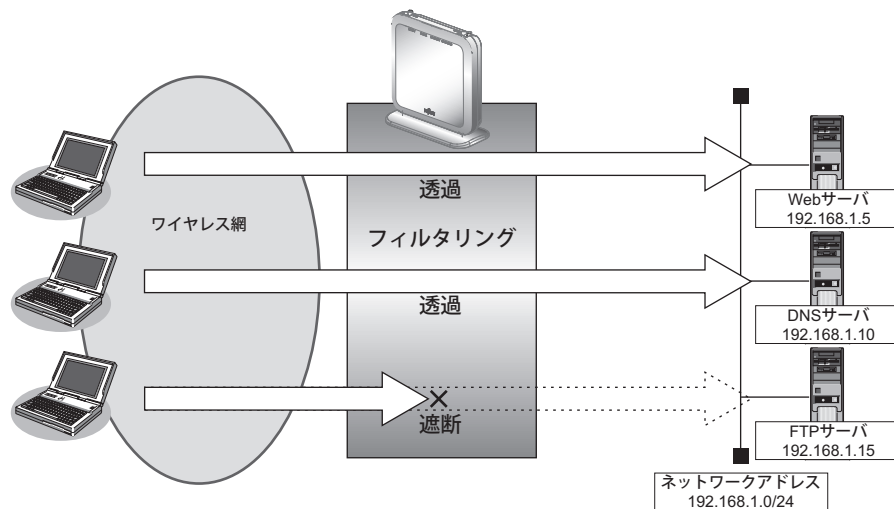
5.1 特定サービスへのアクセスだけを許可する

適用機種 SR-M630AP1,610AP1

ここでは、すべてのWeb サーバに対してアクセスすることだけを許可し、ほかのサーバ（FTP サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、Web サーバ名を解決するために、DNS サーバへのアクセスは許可します。



DNS サーバに問い合わせが発生する場合、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、Web サービス以外でドメイン名を指定した場合も DNS サーバへの発信が発生します。あらかじめ接続する Web サーバが決まっている場合は、本装置の DNS サーバ機能を利用することによって、DNS サーバへの発信を抑制することができます。



● フィルタリング設計

- 無線 LAN 側 (192.168.1.0/24) から Web サーバへのアクセスを許可
- 無線 LAN 側 (192.168.1.0/24) から DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- Web サーバへのアクセスを許可するには
 - (1) 192.168.1.0/24 の任意のポートから、任意の Web サーバのポート 80 (http) への TCP パケットを透過させる
- DNS サーバへのアクセスを許可するには
 - (1) 192.168.1.0/24 の任意のポートから、DNS サーバのポート 53 (domain) への UDP パケットを透過させる
- ICMP の通信を許可するためには
 - (1) ICMP パケットを透過させる
- その他をすべて遮断するには
 - (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

任意の Web サーバのポート 80 への TCP パケットを透過させる

```
# acl 0 ip 192.168.1.0/24 any 6  
# acl 0 tcp any 80  
# vlan 1 filter 0 pass 0
```

Web サーバからの応答パケットを透過させる

```
# acl 1 ip any 192.168.1.0/24 6  
# acl 1 tcp 80 any  
# vlan 1 filter 1 pass 1
```

DNS サーバのポート 53 への UDP パケットを透過させる

```
# acl 2 ip 192.168.1.0/24 192.168.1.10/32 17  
# acl 2 udp any 53  
# vlan 1 filter 2 pass 2
```

DNS サーバからの応答パケットを透過させる

```
# acl 3 ip 192.168.1.10/32 192.168.1.0/24 17  
# acl 3 udp 53 any  
# vlan 1 filter 3 pass 3
```

ICMP のパケットを透過させる

```
# acl 4 ip any any 1  
# acl 4 icmp any  
# vlan 1 filter 4 pass 4
```

残りのパケットをすべて遮断する

```
# acl 5 ip any any any  
# vlan 1 filter 5 reject 5
```

設定終了

```
# save  
# commit
```

6 DHCP 機能を使う

適用機種 SR-M630AP1,610AP1

本装置のIPv4 DHCPには、以下の機能があります。

- DHCPクライアント機能

☞ 参照 マニュアル「機能説明書」

6.1 DHCPクライアント機能を使う

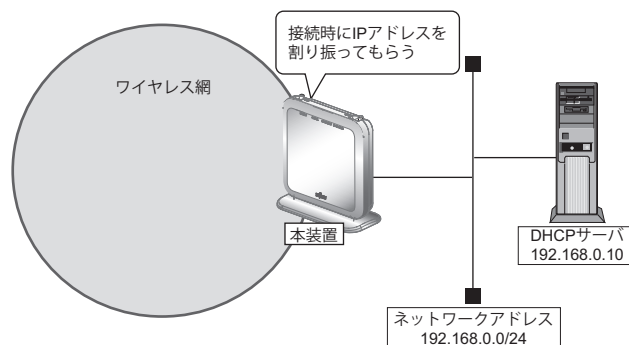
適用機種 SR-M630AP1,610AP1

DHCPクライアント機能は、DHCPサーバからIPアドレスなどの情報を取得する機能です。使用する場合は、DHCPサーバが動作しているLANに接続する必要があります。利用者は、IPアドレスを意識することなくネットワークを利用できます。

本装置のDHCPクライアント機能は、以下の情報を受け取って動作します。

- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- TIMEサーバのIPアドレス
- NTPサーバのIPアドレス
- ドメイン名
- リース更新時間

ここでは、DHCPクライアント機能を使用する場合の設定方法を説明します。



● 設定条件

本装置

- ETHER1 ポートを使う
- ETHER1 を ポートVLAN (untag 1) に設定する
- 本装置の IP アドレス : 有線ポート経由で DHCP サーバから取得する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

本装置

```
ETHER1 ポートを設定する
# ether 1 use on
# ether 1 vlan untag 1

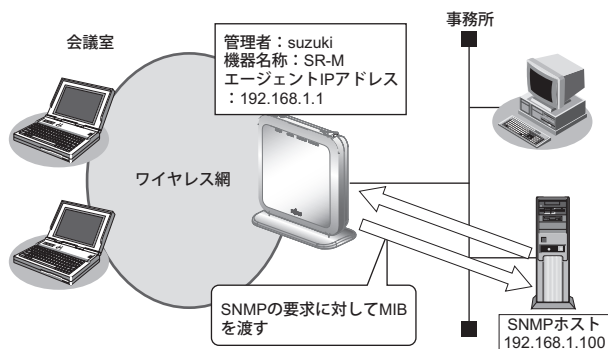
DHCP 機能を設定する
# lan 0 ip dhcp service client
# lan 0 vlan 1

設定終了
# save
# commit
```

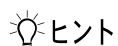
7 SNMP エージェント機能を使う

適用機種 SR-M630AP1,610AP1

本装置は、SNMP (Simple Network Management Protocol) エージェント機能をサポートしています。ここでは、SNMP ホストに対して MIB 情報を通知する場合の設定方法を説明します。



☞ 参照 マニュアル「機能説明書」



ヒント

◆ SNMP とは？

SNMP (Simple Network Management Protocol) は、ネットワーク管理用のプロトコルです。SNMP ホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMP エージェントは、SNMP ホストの要求に対して MIB (Management Information Base) という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMP エージェントから SNMP ホストに対して非同期通知を行うことができます。

☞ 参照 マニュアル「仕様一覧」

こんな事に気をつけて

- エージェントアドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。誤った IP アドレスを設定した場合は、SNMP ホストとの通信ができなくなります。
- 認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMP ホストの設定と同じ設定にします。誤ったプロトコルとパスワードを設定した場合は、SNMP ホストとの通信ができなくなります。

SNMPv1 または SNMPv2c でアクセスする場合の情報を設定する

SNMPv1 または SNMPv2c でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者 : suzuki
- 機器名称 : SR-M
- 機器設置場所 : 1F (1 階)
- エージェントアドレス : 192.168.1.1 (自装置 IP アドレス)
- SNMP ホストアドレス : 192.168.1.100
- コミュニティ名 : public00

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname SR-M
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMP ホスト情報を設定する
# snmp manager 0 192.168.1.100 public00 off disable

SNMP エージェント機能を使用する
# snmp service on

設定終了
# save
# commit
```

SNMPv3 でアクセスする場合の情報を設定する

SNMPv3 でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者 : suzuki
- 機器名称 : SR-M
- 機器設置場所 : 1F (1 階)
- エージェントアドレス : 192.168.1.1 (自装置 IP アドレス)
- SNMP ホストアドレス : 192.168.1.100
- トラップ通知ホストアドレス : 192.168.1.100
- ユーザ名 : user00
- 認証プロトコル : MD5
- パスワード : auth_password
- 暗号プロトコル : DES

- パスワード : priv_password
- MIB ビュー : MIB 読み出しは system、interfaces グループのみ許可
トラップ通知は linkDown、linkUp トラップのみ許可

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname SR-M
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMPv3 情報を設定する
# snmp user 0 name user00
# snmp user 0 address 0 192.168.1.100
# snmp user 0 notification 0 192.168.1.100

認証・暗号プロトコルを設定する
# snmp user 0 auth md5 auth_password
# snmp user 0 priv des priv_password

MIB ビュー情報を設定する
# snmp user 0 read view 0
# snmp user 0 notify view 0
# snmp view 0 subtree 0 include system
# snmp view 0 subtree 1 include interfaces
# snmp view 0 subtree 2 include linkdown
# snmp view 0 subtree 3 include linkup

SNMP エージェント機能を使用する
# snmp service on

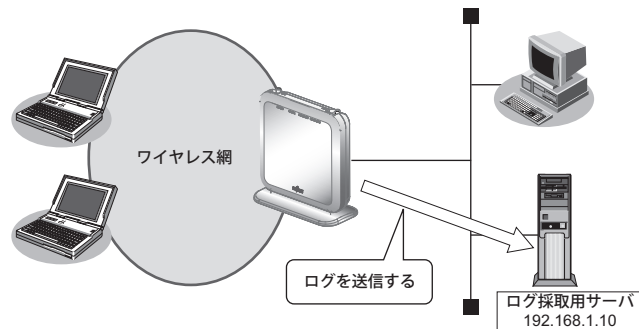
設定終了
# save
# commit
```

8 システムログを採取する

適用機種 SR-M630AP1,610AP1

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のシステムログサーバに送信することができます。

ここでは、システムログを採取する場合の設定方法を説明します。



● 設定条件

- 以下のプライオリティを設定する
 - プライオリティ LOG_ERROR
 - プライオリティ LOG_WARNING
 - プライオリティ LOG_NOTICE
 - プライオリティ LOG_INFO
- ログ受信用サーバのIPアドレス : 192.168.1.10

上記の設定条件に従ってシステムログを採取する場合のコマンド例を示します。

● コマンド

```
# syslog server 0 address 192.168.1.10
```

```
システムログを設定する
# syslog pri error,warn,notice,info
```

```
設定終了
# save
# commit
```

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。

9 スケジュール機能を使う

適用機種 SR-M630AP1,610AP1

本装置のスケジュール機能は、以下のとおりです。

- 構成定義情報切り替え予約
本装置は、内部に2つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

■ 参照 マニュアル「コマンドユーザズガイド」

9.1 構成定義情報の切り替えを予約する

適用機種 SR-M630AP1,610AP1

本装置は、内部に構成定義情報を2つ持つことができます。

ここでは、2020年4月1日6時30分に構成定義情報を構成定義情報1から構成定義情報2に切り替える場合の設定方法を説明します。

● 設定条件

- 実行日時 : 2020年4月1日 6時30分
- 構成定義情報切り替え : 構成定義情報1 → 構成定義情報2

上記の設定条件に従って構成定義情報を切り替える場合のコマンド例を示します。

● コマンド

```
構成定義を切り替える
# addact 0 2004010630 reset config2

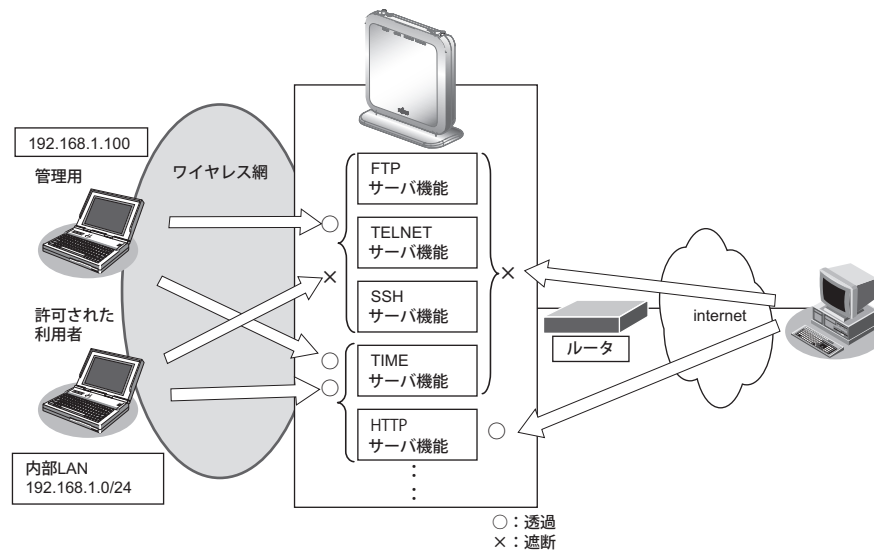
設定終了
# save
# commit
```


10 アプリケーションフィルタ機能を使う

適用機種 SR-M630AP1,610AP1

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させることができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

● 設定条件

- 管理用のホスト（192.168.1.100）からだけTELNET/FTP/SSHサーバ機能へのアクセスを許可する
- 内部LANのホスト（192.168.1.0/24）からだけTIMEサーバ機能へのアクセスを許可する
- その他のサーバ機能は制限しない

こんな事に気をつけて

IPフィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行ってもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合のコマンド例を示します。

● コマンド

制限するサーバ機能に対し、デフォルトのアクセスを遮断する

```
# serverinfo ftp filter default reject
# serverinfo telnet filter default reject
# serverinfo ssh filter default reject
# serverinfo time filter default reject
```

管理用のホストからのFTP/TELNET/SSHサーバ機能へのアクセスを許可する

```
# acl 0 ip 192.168.1.100/32 any any
# serverinfo ftp filter 0 accept acl 0
# serverinfo telnet filter 0 accept acl 0
# serverinfo ssh filter 0 accept acl 0
```

内部LANのホストからのTIMEサーバ機能へのアクセスを許可する

```
# acl 1 ip 192.168.1.0/24 any any
# serverinfo time filter 0 accept acl 1
```

設定終了

```
# save
# commit
```

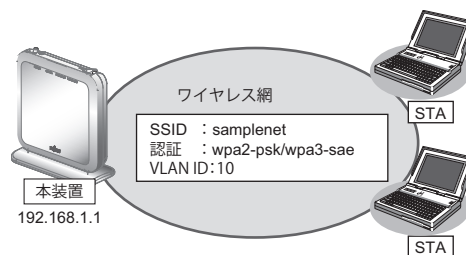
11 端末可視化機能を使う

適用機種 SR-M630AP1,SR-M610AP1

端末可視化機能を使用すると、ネットワーク上にどのような端末が接続されているかを詳細に把握することができます。

こんな事に気をつけて

- 本機能は、無線 LAN インタフェースに接続している端末の情報を収集します。
- IPv4 を使用していないネットワーク上では端末情報を正しく検出できません。
- ARP パケットを送出しない端末の IP アドレス情報は表示されません。
- 機器種別は本機能により推定した結果であり、実際の機器種別と異なる場合があります。
- ベンダー名、機器種別は、識別できない場合があります。
なお、識別したいベンダー名、機器種別は、ユーザが任意の識別情報を設定することも可能です。
- 本装置の OUI 辞書に登録されていない OUI を検出した場合、ベンダー名には "Unknown" と表示されます。
- 本機能では ASCII 文字以外は認識できません。検出した情報に認識できない文字が含まれる場合、"Unrecognized" と表示されます。
- IEEE802.1X 認証機能または MAC アドレス認証機能と本機能を併用する場合、認証されていない端末は検出できません。
- 接続する端末が、ランダムな MAC アドレスを使用する場合、以下の点に注意してください。
 - MAC アドレスが変更される毎に、異なる端末として端末情報が収集されます。
なお、一定時間を経過した端末情報を削除するには、devsacn age コマンドを使用してください。
 - ベンダー名は識別されません。



● 設定条件

- VLAN10 で端末可視化機能を使用する
- 端末情報のエージングアウト時間 : 1 日
- LAN0 の VLAN ID : 10
- LAN0 の IP アドレス : 192.168.1.1
-

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER1ポートを設定する
# ether 1 vlan untag 10

無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g/n/ax
```

アクセスポイントを設定する

```
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa2-psk/wpa3-sae
# wlan 1 wpa cipher aes
# wlan 1 wpa psk text abcdefgh
# wlan 1 vlan untag 10
```

LAN0のIP アドレスを設定する

```
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10
```

VLAN10で端末可視化機能を設定する

```
# devscan use on
# devscan vlan 10
# devscan age 1d
```

設定終了

```
# save
# commit
```

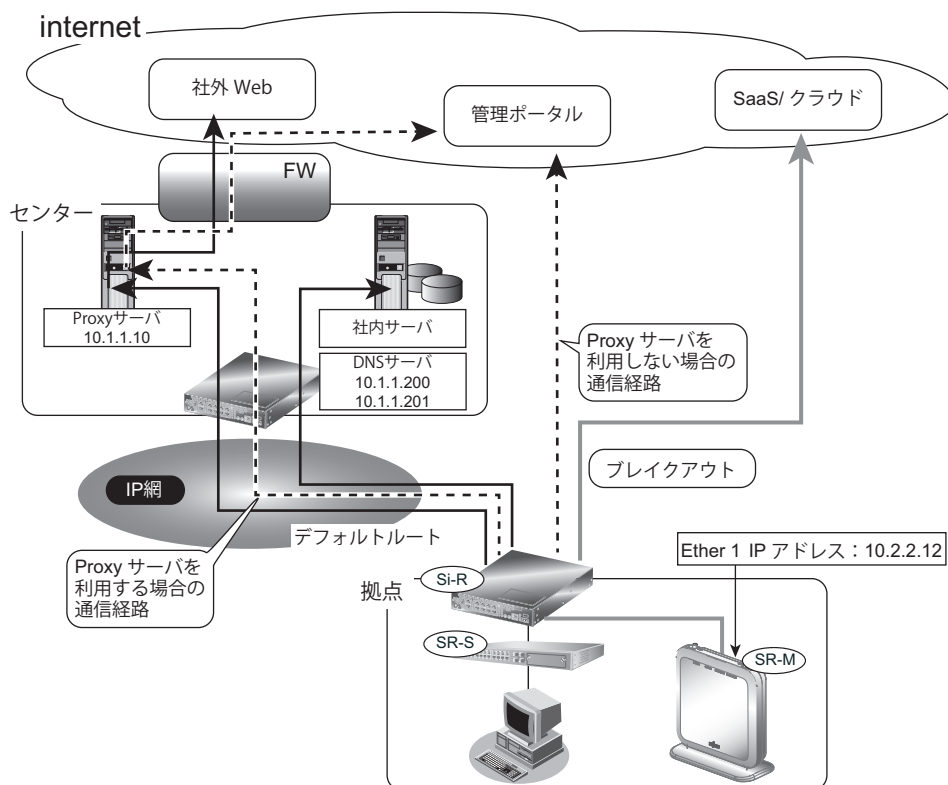
12 NXconciierge と連携する

適用機種 SR-M630AP1,SR-M610AP1

NXconciierge とは、ネットワーク機器を集中管理するクラウド型 SD-WAN/LAN プラットフォームです。本装置は、NXconciierge によるネットワーク機器の管理に対応したエージェント機能を搭載しており、NXconciierge と連携することで、ネットワーク経由で機器の集中管理を実現することができます。NXconciierge と連携するためには利用申請と発行されたテナントキーが必要です。

こんな事に気をつけて

NXconciierge エージェント機能に割り当てる IP アドレスは、装置の物理ポートに割り当てた IP アドレスと同一のアドレスを設定します。



● 前提条件

- 管理者 (admin) 用パスワードが設定済み
- 時刻設定
 - 現在時刻が設定済み
- ルータから、管理ポータルへの経路は、ルータの設定に依存します。

エージェントと管理ポータルとの通信時に Proxy サーバを利用する場合の設定方法を説明します。

● 設定条件

- LAN0のVLAN ID : 10
- LAN0のIPアドレス : 10.2.2.12
- デフォルトゲートウェイのIPアドレス : 10.2.2.2
- SNMP連携 : 有効
- 端末可視化機能 : 有効
- 管理ポータルテナントキー : key
- ProxyサーバのIPアドレス : 10.1.1.10
- ProxyサーバのID : id
- Proxyサーバのパスワード : pass
- DNSサーバのIPアドレス : 10.1.1.200 , 10.1.1.201

● コマンド

ETHER1ポートを設定する

```
# ether 1 vlan untag 10
```

LANアドレスを設定する

```
# lan 0 ip address 10.2.2.12/24 3
```

```
# lan 0 vlan 10
```

```
# lan 0 ip route 0 default 10.2.2.2 1 1
```

SNMP連携を設定する

```
# snmp service on
```

```
# snmp agent address 10.2.2.12
```

```
# snmp manager 0 0.0.0.0 public off disable
```

端末可視化の設定

```
# devscan use on
```

```
# devscan vlan 10
```

```
# devscan age 14d
```

エージェント設定を行う

```
# management-agent mode agent
```

```
# management-agent tenantkey key
```

```
# management-agent serverlogin proxy address 10.1.1.10 8080
```

```
# management-agent serverlogin proxy auth send id pass
```

```
# dns-resolver server 10.1.1.200 10.1.1.201
```

システムログの出力を抑制する設定を行う

```
# syslog filter 0 regexp "sshd.*admin.*from 10\\.2\\.2\\.12( |\\n)"
```

設定終了

```
# save
```

```
# commit
```

次に、エージェントとNXconciiergeサーバとの通信時にProxyサーバを利用せず、直接インターネット経由で通信する場合の設定方法を説明します。

● 設定条件

- LAN0のVLAN ID : 10
- LAN0のIPアドレス : 10.2.2.12
- デフォルトゲートウェイのIPアドレス : 10.2.2.2
- SNMP連携 : 有効
- 端末可視化機能 : 有効
- 管理ポータルテナントキー : key
- DNSサーバのIPアドレス : 10.1.1.200 , 10.1.1.201

● コマンド

```
ETHER1ポートを設定する
# ether 1 vlan untag 10

LANアドレスを設定する
# lan 0 ip address 10.2.2.12/24 3
# lan 0 vlan 10
# lan 0 ip route 0 default 10.2.2.2 1 1

SNMP連携を設定する
# snmp service on
# snmp agent address 10.2.2.12
# snmp manager 0 0.0.0.0 public off disable

端末可視化の設定
# devscan use on
# devscan vlan 10
# devscan age 14d

エージェント設定を行う
# management-agent mode agent
# management-agent tenantkey key
# dns-resolver server 10.1.1.200 10.1.1.201

システムログの出力を抑制する設定を行う
# syslog filter 0 regexp "sshd.*admin.*from 10\\.2\\.2\\.12( |\\n)"

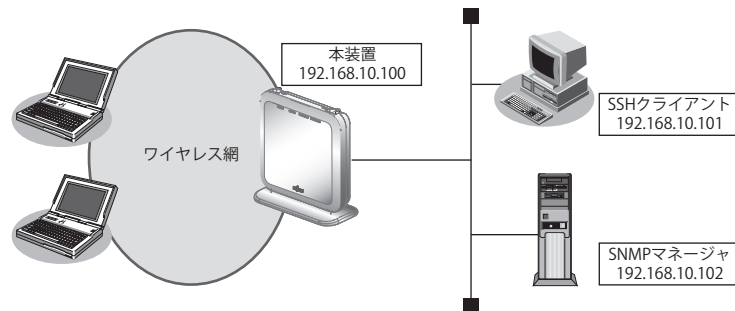
設定終了
# save
# commit
```

13 装置を保護する

適用機種 SR-M630AP1,SR-M610AP1

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者 (admin) 用パスワードの設定
- 自動切断 (オートログアウト) の設定
- Telnet/SSH および SNMP 接続に対するアクセス制限
- 不要なサービスの停止



● 設定条件

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者 (admin) パスワードの設定 : srm_admin-2022
- IP アドレス : 192.168.10.100
- 自動切断 (オートログアウト) の設定
(ログインしたままの状態ですべての指定時間無操作だった際に、自動切断を行う)
コンソールのオートログアウト時間 : 5分
SSHのオートログアウト時間 : 5分
- SNMP 設定
アクセス許可する SNMP マネージャ : 192.168.10.102
コミュニティ名 : private
マネージャからの書き込み : 許可しない
- SSH 接続を許可するホストの IP アドレス : 192.168.10.101
- Telnet 接続 : 禁止
- 不要なサーバ機能はすべて停止
serverinfo <サーバ機能名> ip off

● コマンド

```
adminパスワードをsrm_admin-2022に設定
# password admin set srm_admin-2022

コンソール接続のオートログアウト時間を5分に設定
# consoleinfo autologout 5m

SSHのオートログアウトまでの無操作時間を5分に設定
# telnetinfo autologout 5m

自装置IPアドレスとVLANの設定
# lan 0 ip address 192.168.10.100/24 3
# lan 0 vlan 1

SNMPを有効、コミュニティ名をprivate、書き込み許可しない
# snmp service on
# snmp manager 0 192.168.10.102 private v1 disable

許可するホストからのSSH接続のみ許可する
# acl 0 ip 192.168.10.101/32 any any any
# serverinfo ssh filter 0 accept acl 0
# serverinfo ssh filter default reject

不要なサーバ機能はすべて停止
# serverinfo telnet ip off
# serverinfo ftp ip off
# serverinfo sftp ip off
# serverinfo http ip off
# serverinfo https ip off
# serverinfo snmp ip off
# serverinfo time ip tcp off
# serverinfo time ip udp off

設定終了
# save
# commit
```

索引

A

ACL 番号 78

D

DHCP 機能 82

DHCP クライアント機能 82

I

IEEE802.11ac 9

IEEE802.11n 11

IP アドレス 78

L

LACP 機能 76

M

MAC アドレスフィルタリング機能 46

MIB 84

S

SNMP 84

SNMP エージェント機能 84

V

VLAN 管理 20

VLAN 機能 73

W

WDSブリッジ機能 36

WMM 機能 48

あ

アドレスマスク 78

アプリケーションフィルタ機能 89

か

仮想アクセスポイント 15

こ

構成定義情報切り替え予約 88

し

システムログ 87

システムログの確認 87

す

スイッチング HUB 73

スケジュール機能 88

せ

制御 78

セキュリティ 78

た

タグ VLAN 機能 74

ち

チャンネルボンディング機能 52

ふ

フィルタリング機能 78

フィルタリングの条件 78

フィルタリングの設計方針 79

複数アクセスポイント 25

ほ

ポート VLAN 機能 73

ま

マニュアル構成 6

む

無線 LAN 7, 13

無線 LAN 機能 7

無線通信 7

り

リンクアグリゲーション機能 75

リンクインテグリティ機能 77

SR-M コマンド設定事例集

P3NK-7512-06Z0

発行日 2023年10月

発行責任 富士通株式会社

- 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- 本書は、改善のために予告なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、弊社はその責を負いません。