

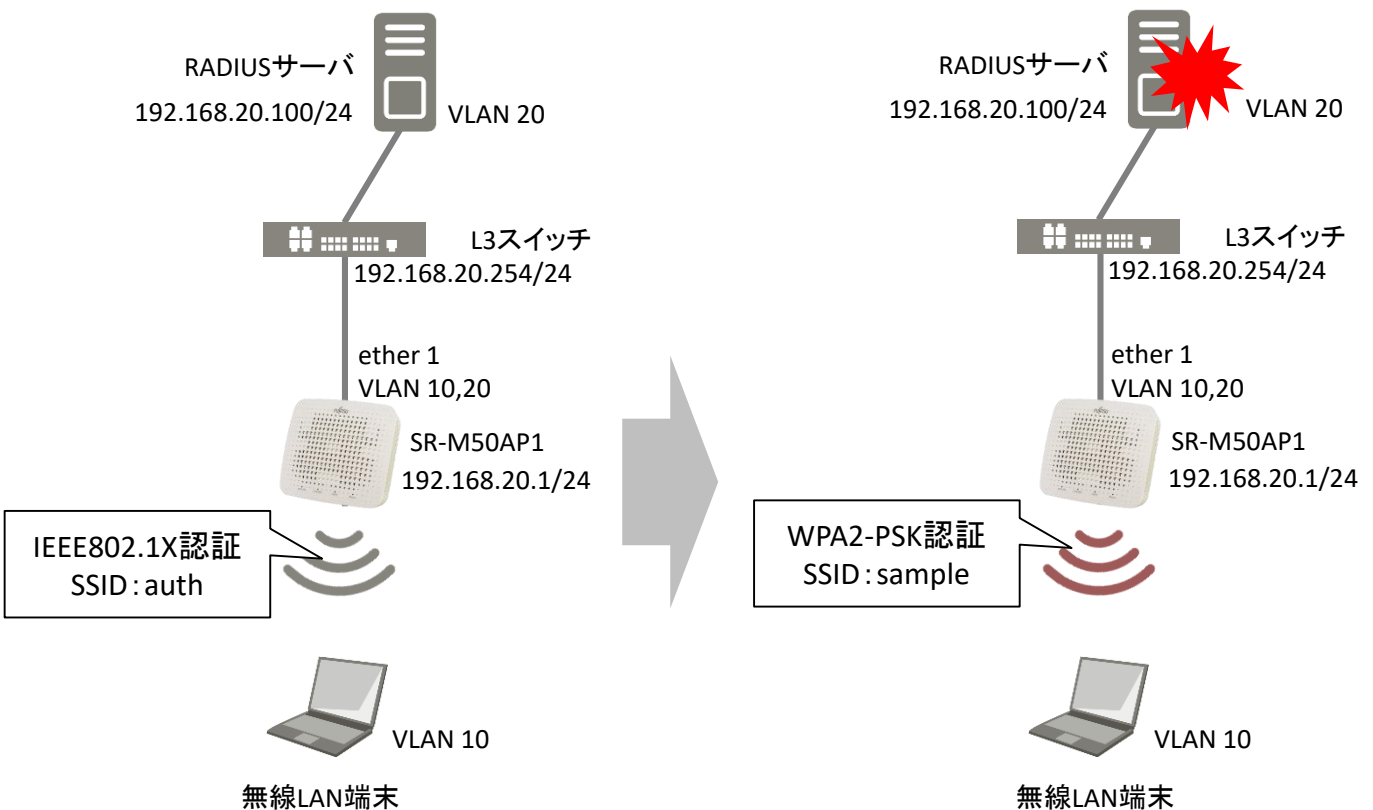
技術情報：SR-M50AP1設定例

(IEEE802.1X認証 (認証自動切替))

RADIUSサーバの稼働状況を監視し、RADIUSサーバから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る設定例です。

[対象機種と版数]

SR-M50AP1 V03.00以降



[設定内容]

- SR-M50AP1のether 1を有線LANと接続します。
- 無線LANは、5GHz帯を使用します。

	通常時	切替後
チャンネル番号	36	36
SSID	auth	sample
認証	WPA2によるIEEE802.1X認証	WPA2による事前共有キー（PSK）認証
暗号化	AES	AES
事前共有キー（PSK）	—	abvdefghijklm
VLAN ID	—	10

- RADIUSサーバを使用します。

RADIUSシークレット	sr-m
--------------	------

- RADIUSサーバを監視します。

RADIUSサーバ監視方法	ICMPによる監視
RADIUSサーバ監視の通常時の送信間隔	10秒
RADIUSサーバ監視の再送間隔	5秒
RADIUSサーバ監視のタイムアウト時間	15秒
RADIUSサーバ監視の異常時の送信間隔	30秒

- ユーザにVLAN IDを割り当てるため、RADIUSサーバには以下の属性を設定します。
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

- 端末の無線LANプロファイル

認証自動切替機能を利用する場合、端末には通常時とRADIUSサーバ障害時のためのプロファイルをあらかじめ作成しておく必要があります。また、端末によって使用するプロファイルの切り替え動作が異なるため、障害テストによる十分な確認が必要です。

[設定例]

SR-M50AP1設定例

```
ieee80211 2 use on
ieee80211 2 mode 11a/n/ac
ieee80211 2 channel 36
wlan 9 use on
wlan 9 ssid auth
wlan 9 auth wpa2
wlan 9 wpa cipher aes
wlan 9 dot1x use on
wlan 9 dot1x aaa 1
wlan 9 dot1x backup master 0s
wlan 10 use on
wlan 10 ssid sample
wlan 10 auth wpa2-psk
wlan 10 wpa cipher aes
wlan 10 wpa psk text abcdefghijklm
wlan 10 vlan untag 10
wlan 10 dot1x backup backup 9
ether 1 vlan tag 10,20
lan 0 ip address 192.168.20.1/24 3
lan 0 ip route 0 default 192.168.20.254 1
lan 0 vlan 20
dot1x use on
aaa 1 radius service client auth
aaa 1 radius client server-info auth 0 secret sr-m
aaa 1 radius client server-info auth 0 address 192.168.20.100
aaa 1 radius client server-info auth 0 watch type icmp
aaa 1 radius client server-info auth 0 watch interval 10s
aaa 1 radius client server-info auth 0 watch retry 5s
aaa 1 radius client server-info auth 0 watch timeout 15s
aaa 1 radius client server-info auth 0 watch abnormal-interval 30s
```

ieee80211 2 use on
#ieee80211 2モジュール（5GHz帯）を有効にします。

ieee80211 2 mode 11a/n/ac
#5GHz帯の通信規格を設定します。

ieee80211 2 channel 36
#5GHz帯のチャンネルを設定します。

wlan 9 use on
#無線LANインタフェースwlan 9を有効にします。

wlan 9 ssid auth
#SSIDを設定します。

wlan 9 auth wpa2
#認証モードを設定します。
#wpa2：WPA2によるIEEE802.1X認証です。

wlan 9 wpa cipher aes
#WPA/WPA2で使用する暗号化モードを設定します。
#aes：AES暗号化を行います。

wlan 9 dot1x use on
#wlan 9でIEEE802.1X認証を有効にします。

wlan 9 dot1x aaa 1
#IEEE802.1X認証で使用するAAAグループを設定します。

wlan 9 dot1x backup master 0s
#この無線LANインタフェースを認証自動切替の対象とします。
#RADIUSサーバが復旧してからバックアップを解除するまでの時間を指定します。
#0s：即時復旧します。

wlan 10 use on
#無線LANインタフェースwlan 10を有効にします。

wlan 10 ssid sample
#SSIDを設定します。

wlan 10 auth wpa2-psk
#認証モードを設定します。
#wpa2-psk : WPA2による事前共有キー(PSK)認証です。

wlan 10 wpa cipher aes
#WPA/WPA2で使用する暗号化モードを設定します。
#aes : AES暗号化を行います。

wlan 10 wpa psk text abcdefghijklm
#事前共有キーを設定します。

wlan 10 vlan untag 10
#wlan 10にVLAN IDを設定します。

wlan 10 dot1x backup backup 9
#認証自動切替対象とした無線LANインタフェースのバックアップとして動作します。
#バックアップ対象の無線LANインタフェース番号を指定します。

ether 1 vlan tag 10,20
#ether 1ポートに、管理用VLAN ID、RADIUSサーバから通知されるVLAN ID、無線LANインターフェースに設定したVLAN IDを設定します。

lan 0 ip address 192.168.20.1/24 3
lan 0 vlan 20
#IPアドレスを設定し、VLAN IDを割り当てます。

lan 0 ip route 0 default 192.168.20.254 1
#デフォルトゲートウェイを設定します。

dot1x use on
#装置でIEEE802.1X認証を有効にします。

```
aaa 1 radius service client auth
#RADIUSクライアント機能として使用します。RADIUS認証機能を有効にします。

aaa 1 radius client server-info auth 0 secret sr-m
#RADIUSシークレットを設定します。

aaa 1 radius client server-info auth 0 address 192.168.20.100
#RADIUS認証サーバのIPアドレスを設定します。

aaa 1 radius client server-info auth 0 watch type icmp
#RADIUSサーバの監視種別を設定します。
#icmp : ICMPで監視します。

aaa 1 radius client server-info auth 0 watch interval 10s
#通常時の定期監視間隔を設定します。

aaa 1 radius client server-info auth 0 watch retry 5s
#定期監視の再送間隔を設定します。

aaa 1 radius client server-info auth 0 watch timeout 15s
#定期監視のタイムアウト時間を設定します。

aaa 1 radius client server-info auth 0 watch abnormal-interval 30s
#異常時の定期監視間隔を設定します。
```