CHAPTER 2

WMIC の初期設定

このマニュアルでは、Wireless Mobile Interface Card（WMIC）の基本的な初期設定方法について説明します。

始める前に

WMIC をインストールする前に、ご使用のコンピュータが WMIC と同じネットワークに接続されていることを確認し、ネットワーク管理者から次の情報を入手してください。

- WMIC のシステム名
- 無線 Service Set Identifier（SSID）（大文字と小文字を区別）
- DHCP サーバに接続されていない場合は、WMIC の一意の IP アドレス（172.17.255.115 など）
- WMIC がご使用の PC と同じサブネット上にない場合は、デフォルト ゲートウェイ アドレスおよびサブネット マスク
- SNMP（簡易ネットワーク管理プロトコル）のコミュニティ名および SNMP ファイルの属性（SNMP が使用中の場合）

WMIC との接続

WMIC を設定するには：

- コンソール ケーブルを使用して、PC を WMIC コンソール ポートに接続します。
- WMIC に IP アドレスがあり、デバイスで Telnet が許可されている場合、Ethernet ケーブルを使用し、Telnet を使用して接続を確立することによって、Fast Ethernet Switch Mobile Interface Card（FESMIC）Ethernet ポートを接続できます。
- WMIC が LAN 上に存在し、IP アドレスがある場合、Telnet がデバイスで許可されていれば、LAN 上のノードから WMIC に Telnet 接続できます。

（注） PC を WMIC に接続するか、または PC を LAN に再接続する場合は、PC の IP アドレスを解放して、再設定する必要があります。ほとんどの PC では、PC を再起動するか、コマンド プロンプト ウィンドウで **ipconfig /release** および **ipconfig /renew** コマンドを入力することにより、IP アドレスを解放して再設定することができます。詳細については、PC のマニュアルを参照してください。

コンソール ポートを使用してイネーブル EXEC モードにアクセスする方法

DB-9-to-RJ-45 シリアル ケーブルを使用して、PC を WMIC コンソール ポートに接続します。Cisco 3200 シリーズ ルータには複数のコンソール ポートがある場合があることに注意してください。

PC を WMIC のコンソール ポートに接続し、CLI にアクセスする手順は、次のとおりです。

ステップ 1　DB-9-to-RJ-45 シリアル ケーブルの RJ-45 終端をルータの WMIC RJ-45 シリアル ポートに接続します。

ステップ 2　DB-9-to-RJ-45 シリアル ケーブルの DB-9 終端を PC の COM ポートに接続します。

ステップ 3　WMIC と通信するように端末エミュレータ アプリケーションを起動します。端末エミュレータ接続には、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしの設定を使用します。端末エミュレータが通信を確立すると、ルータによってプロンプトが表示されます。

ステップ 4　**Enter** キーを押します。プロンプトが表示されます。

ステップ 5　「**en**」と入力します。ユーザ名のプロンプトが表示されます。

ステップ 6　*ユーザ名*を入力します。デフォルトのユーザ名は *Cisco* です。パスワードのプロンプトが表示されます。

ステップ 7　有効な WMIC パスワードを入力します。デフォルトのパスワードは *Cisco* です。

Exec モードであることを示すプロンプトが表示されます。

Telnet セッションを使用してイネーブル EXEC モード にアクセスする方法

Telnet セッションを使用して WMIC CLI にアクセスする手順は、次のとおりです。WMIC は Telnet セッションを受け入れるようにあらかじめ設定されている必要があります。

これらの手順は、Telnet 端末アプリケーションおよび Microsoft Windows が稼動する PC に対応しています。ご使用の OS の詳細手順については、PC の操作手順を参照してください。

ステップ 1　[スタート] > [プログラム] > [アクセサリ] > [Telnet] を選択します。アクセサリ メニューに Telnet が表示されない場合は、[スタート] > [ファイル名を指定して実行] を選択し、[名前] フィールドに Telnet と入力して、**Enter** キーを押します。

ステップ 2　[Telnet] ウィンドウが表示されたら、[Connect] をクリックし、[Remote System] を選択します。

（注）　Windows 2000 では、[Telnet] ウィンドウにドロップダウン メニューが配置されません。Windows 2000 で Telnet セッションを起動するには、**open** を入力し、そのあとに WMIC の IP アドレスを入力します。

ステップ 3　[Host Name] フィールドに WMIC の IP アドレスを入力して、[Connect] をクリックします。

SSH を使用して CLI にアクセスする方法

SSH は、セッションを暗号化して、ログイン セッションを保護するソフトウェア パッケージです。SSH では、暗号認証、暗号化、および整合性保護機能が強化されます。SSH は、リモート接続に関するセキュリティを Telnet よりも高めることができます。WMIC に SSH アクセスを設定する手順については、「WMIC の管理」を参照してください（SSH の詳細については、次の URL にある SSH Communications Security, Ltd. のホームページ（http://www.ssh.com/）を参照してください）。

IP アドレスの取得および割り当て

WMIC の IP アドレスを割り当てるには、次のいずれかの方法を使用します。

- WMIC をローカルで接続する場合、コンソールを使用します。詳細手順については、「WMIC との接続」（P.2-1）を参照してください。
- IP アドレスを自動的に割り当てるには、DHSP サーバを使用します（使用可能な場合）。DHCP によって割り当てられた IP アドレスを調べるには、次のいずれかの方法を実行します。
  - 組織のネットワーク管理者に WMIC の MAC（メディア アクセス制御）アドレスを知らせます。ネットワーク管理者は MAC アドレスを使用して DHCP サーバに問い合わせて、IP アドレスを識別します。
  - Cisco IP Setup Utility（IPSU）を使用して、割り当てられたアドレスを識別します。WMIC が DHCP サーバから IP アドレスを受信しなかった場合は、IPSU を使用して IP アドレスを割り当てることもできます。IPSU は Windows 9x、2000、ME、NT、XP など、ほとんどの Microsoft Windows OS で動作します。

    IPSU は Cisco.com の Software Center からダウンロードできます。次のリンクをクリックして、Software Center を表示してください。

    http://www.cisco.com/public/sw-center/sw-wireless.shtml
  - 装置が非ルート ブリッジの場合は、ルータの WMIC コンソール ポートにローカルに接続します。

EXEC を使用して IP アドレスを割り当てる方法

WMIC は、自動作成された Bridge Group Virtual Interface（BVI）を使用して、ネットワークに接続します。各 WMIC は、1 つの BVI のみをサポートします。複数の BVI を設定すると、WMIC の Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブルにエラーが発生することがあります。

BVI に IP アドレスを割り当てるには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface bvi1**	BVI について、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** *address subnetmask*	BVI に IP アドレスおよびサブネット マスクを割り当てます。 **（注）** Telnet セッションを使用して WMIC に接続している場合は、新しい IP アドレスを BVI に割り当てると、WMIC との接続が切断されます。Telnet による WMIC の設定を継続するには、新しい IP アドレスを使用して、WMIC との別の Telnet セッションを開きます。

無線 LAN の保護

WMIC に基本設定を割り当てたら、ネットワークに対する不正アクセスを禁止するためのセキュリティを設定する必要があります。WMIC はワイヤレス デバイスであるため、建物の物理的な境界を越えて通信できます。高度なセキュリティ機能については、次の章を参照してください。

- ビーコンでブロードキャストされない一意の SSID（詳細については、「Service Set Identifier」を参照）
- Wired Equivalent Privacy（WEP）および WEP 機能（「暗号スイートおよび WEP」を参照）
- ダイナミック WEP および WMIC 認証（「認証タイプ」を参照）

基本的なセキュリティの設定

アクセス ポイントに基本設定を割り当てたら、ネットワークに対する不正アクセスを禁止するためのセキュリティを設定する必要があります。アクセス ポイントはワイヤレス デバイスであるため、作業場所の物理的な境界を越えて通信することができます。

VLAN の使用方法

無線 LAN で VLAN（仮想 LAN）を使用していて、そこに SSID を割り当てる場合は、複数の SSID を作成することができます。ただし、無線 LAN で VLAN を使用しない場合は、SSID に割り当てることができるセキュリティ オプションは制限されます。これは、暗号化設定と認証タイプが対応付けられているためです。VLAN を使用しない場合は、2.4 -GHz 無線などのインターフェイスに暗号化設定（WEP および暗号）が適用されます。1 つのインターフェイスに複数の暗号化設定を使用できません。たとえば、VLAN がディセーブルの状態でスタティック WEP を使用する SSID を作成した場合は、Wi-Fi Protected Access（WPA）認証を使用する SSID を別途作成できません。使用される暗号化設定が異なるためです。SSID のセキュリティ設定が他の SSID と一致しない場合は、SSID を 1 つまたは複数削除して、不一致が生じないようにしてください。

Express Security のタイプ

表 2-1 に、SSID に割り当てることができる 4 つのセキュリティ タイプを示します。

表 2-1　Express Security 設定ページのセキュリティ タイプ

セキュリティ タイプ	説明	イネーブル化されたセキュリティ機能
セキュリティなし	セキュリティが一番小さいオプションです。このオプションは、パブリック スペースで SSID を使用する場合に限って使用します。ネットワークへのアクセスを制限する VLAN に割り当てます。	なし
スタティック WEP キー	セキュリティなしよりもセキュリティが高いオプションです。ただし、スタティック WEP キーは攻撃に対して脆弱です。このオプションを設定する場合は、MAC アドレスに基づいてアクセス ポイントとのアソシエーションを制限することを検討してください。ネットワークに RADIUS サーバが配置されていない場合は、アクセス ポイントをローカル認証サーバとして使用することを検討してください。	必須の Web 暗号化、鍵管理なし、およびオープン認証。**Root AP** モードでは、クライアント デバイスがこの SSID を使用して対応付けを行う場合、アクセス ポイント キーと一致する WEP キーを使用する必要があります。
EAP 認証	Lightweight EAP（LEAP）、Protected EAP（PEAP）、EAP-Transport Layer Security（EAP-TLS）、EAP-GTC などの 802.1x Extensible Authentication Protocol（EAP; 拡張認証プロトコル）がイネーブルになり、ネットワークの認証サーバ（サーバ認証ポート 1645）に関する IP アドレスおよび共有シークレットの入力が必要となります。802.1x 認証ではダイナミック暗号鍵が提供されるため、WEP キーを入力する必要がありません。	必須の 802.1x 認証。**Root AP** モードでは、クライアント デバイスがこの SSID を使用して対応付けを行う場合、802.1x 認証を実行する必要があります。
WPA	WPA を使用すると、認証サーバのサービスによって認証されたユーザがデータベースに無線アクセスできるようになり、WEP で使用されるアルゴリズムよりも強力なアルゴリズムによって IP トラフィックが暗号化されます。EAP 認証と同様に、ネットワークの認証サーバ（サーバ認証ポート 1645）に IP アドレスおよび共有シークレットを入力する必要があります。	必須の WPA 認証。**Root AP** モードでは、この SSID を使用して対応付けを行うクライアント デバイスは、WPA 対応でなければなりません。

CLI セキュリティの設定例

ここでは、SSID の作成とセキュリティの割り当ての設定例をご提供します。

例：セキュリティなし

次に、Express Security ページを使用して *no_security_ssid* という名前の SSID を作成し、この SSID をビーコンに追加し、VLAN 10 に割り当てて、VLAN 10 をネイティブ VLAN として選択する設定例の一部を示します。

```
Dot11 ssid no_security-ssid
    vlan 10
    authentication open
    guest-mode
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
ssid no_security-ssid
 !
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 station-role root
 infrastructure-client
 bridge-group 1
!
interface Dot11Radio0.10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
 bridge-group 10 spanning-disabled
!
interface FastEthernet0.10
encapsulation dot1Q 10
no ip address
no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
```

例：スタティック WEP

static_wep_ssid という名前の SSID を作成し、この SSID をビーコンから除外し、VLAN 20 に割り当てて、3 をキー スロットとして選択し、128 ビット鍵を入力するために使用される設定例の一部を示します。

```
encryption vlan 20 key 3 size 128bit 7 4E78330C1A841439656A9323F25A transmit-ke
y
 encryption vlan 20 mode wep mandatory
 !
 ssid static_wep_ssid
    vlan 20
    authentication open
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
ssid no_security-ssid
```

```
 !
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 station-role root
 infrastructure-client
 bridge-group 1
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 spanning-disabled
```

例：EAP 認証

eap_ssid という名前の SSID を作成し、この SSID をビーコンから除外し、VLAN 30 に割り当てるために使用される設定例の一部を示します。

```
encryption vlan 30 mode wep mandatory
 !
Dot11 ssid eap_ssid
    vlan 30
    authentication open eap eap_methods
    authentication network-eap eap_methods
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
ssid no_security-ssid
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
```

```
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface FastEthernet0
 mtu 1500
 no ip address
 ip mtu 1564
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.30
 mtu 1500
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
```

例：WPA

wpa_ssid という名前の SSID を作成し、この SSID をビーコンから除外し、VLAN 40 に割り当てるために使用される設定例の一部を示します。

```
aaa new-model
!
aaa group server radius rad_eap
 server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
```

```
encryption vlan 40 mode ciphers tkip
 !
Dot11 ssid wpa_ssid
    vlan 40
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
interface Dot11Radio0
 no ip address
 no ip route-cache
!
ssid no_security-ssid
!
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48 54.0
 rts threshold 4000
 station-role root
 infrastructure-client
 bridge-group 1
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
!
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
/122-15.JA/1100
ip radius source-interface BVI1
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.91.104.92 auth-port 1645 acct-port 1646 key 7 135445415F59
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
line con 0
line vty 5 15
!
end
```