WIRELESS LAN SWITCH AND CONTROLLER QUICK START GUIDE

This document describes how to do the following:

■ Use the **quickstart** command to perform basic system configuration of a Wireless LAN switch (WX) running Mobility System Software Version 3.0.

■ Configure a Mobility Domain for roaming.

■ Open the sample 3WXM network plan *3ComStarterExample*, which contains the configuration values used in the CLI examples. You can use the network plan to build on the configuration, if you do not want to continue to use the CLI.

What Does the quickstart Command Configure?

The **quickstart** command runs a script that interactively helps you configure the following items:

■ System name

■ Country code (regulatory domain)

■ System IP address

■ Default route

■ Administrative users and passwords

■ System time and date parameters

■ Unencrypted (clear) SSID names

■ Usernames and passwords for guest access using Web AAA

■ Encrypted (crypto) SSID names and dynamic WEP encryption for encrypted SSIDs' wireless traffic

■ Usernames and passwords for secure access using 802.1X authentication using PEAP-MSCHAPv2 and secure wireless data encryption using dynamic Wired Equivalent Privacy (WEP)

■ Managed Access Points (MAPs) that are directly connected to WX switches

■ Distributed MAPs, which are connected to WX switches through an intermediate Layer 2 or Layer 3 network

The **quickstart** command displays a prompt for each of these items, and lists the default if applicable. You can advance to the next item, and accept the default if applicable, by pressing Enter.

Depending on your input, the command also automatically generates the following key pairs and self-signed certificates:

■ SSH key pair (always generated)

■ Admin key pair and self-signed certificate (always generated)

■ EAP (802.1X) key pair and self-signed certificate (generated if you type usernames and passwords for users of encrypted SSIDs)

■ Web AAA key pair and self-signed certificate (generated if you type usernames and passwords for users of unencrypted SSIDs)

The command automatically places all ports that are not used for directly connected MAPs into the default VLAN (VLAN 1).

⚠ *CAUTION: The **quickstart** command is for configuration of a new WX switch only. After prompting you for verification, the command erases the switch's configuration before continuing. If you run this command on a switch that already has a configuration, the configuration will be erased. In addition, error messages such as "Critical AP Notice" for directly connected MAPs can appear.*

(The **quickstart** command does not configure Mobility Domain parameters, which are required for users to roam across devices in the network. See "Configuring a Mobility Domain for Roaming" on page 8.)

Preparing the Network for Distributed MAPs

A MAP that is not directly connected to a WX switch is considered a Distributed MAP. There can be intermediate Layer 2 switches or Layer 3 IP routers between the WX and MAP. The WX can communicate with the Distributed MAP through any network port. (A network port is any port connecting the switch to other networking devices, such as switches and routers, and it can also be configured for 802.1Q VLAN tagging.) The WX contains a configuration for a Distributed MAP based on the MAP's serial number. Similar to ports configured for directly connected MAPs, Distributed MAP configurations are numbered and can reference a particular MAP. These numbered configurations do not, however, reference any physical port.

In addition to the WX switch configuration shown in this document, Distributed MAPs require the following support:

■ **Power** — PoE must be provided on one of the Ethernet connections to the MAP. Be sure to use a PoE injection device that has been tested by 3Com. (Contact 3Com for information.)

■ **DHCP** — A Distributed MAP uses IP for communication, and relies on DHCP to obtain IP parameters. Therefore, DHCP services must be available on the subnet that the MAP is connected to. DHCP must provide the following parameters to the MAP:

   ■ IP address

   ■ Domain name

   ■ DNS server address

   ■ Gateway address

■ **DNS** — If the intermediate network between the WX switch and Distributed MAP includes one or more IP routers, create a 3COMWX.*mynetwork*.com entry on the DNS server. The DNS entry allows the MAP to communicate with a WX. If the MAP is unable to locate a WX on the subnet it is connected to, it performs a DNS query for

3COMWX.*mynetwork*.com, where the DNS suffix for *mynetwork*.com is learned through DHCP. The WX relays information about WX switches in the network that contain a Distributed MAP configuration specific to that Distributed MAP.

Preparing Clients

MSS uses 802.1X for access to secure (encrypted) SSIDs. For a client to access an encrypted SSID, 802.1X must be configured on the client. Depending on the type of encryption used for the SSID, additional configuration on the client might be required.

The following sections describe how to configure a Windows XP (Service Pack 2) client for access to an unencrypted (clear) or encrypted SSID. The exact procedure and the options that are supported depend on the Windows version installed on the client and might also depend on the wireless adapter card. See the *Wireless LAN Switch and Controller Release Notes* for additional client recommendations and a list of supported wireless adapters.

To configure a Windows XP SP2 client to access an SSID and use dynamic WEP encryption:

1 Access the Network Connections dialog box. (Select **Control Panel > Network and Internet Connections**.)

2 Select **Network Connections**.

3 Right-click on the wireless network connection and select **Properties**.

4 Click the Wireless Networks tab.

5 Click **Add** to display the Wireless network properties dialog box.

6 Type the SSID name in the Network name field. (If you are using the SSIDs in this document, type *public* for nonsecure access, or *corporate* for secure access.)

7 In the Wireless network key group box, select Network Authentication type **Open**.

8 Select Data encryption type **WEP**.

9 Select **The key is provided for me automatically**, if not already selected.

   Make sure **This is a computer-to-computer (ad hoc) network** is not selected.

10 Click the Authentication tab.

11 Enable or disable 802.1X:

   ■ If the SSID is unencrypted, deselect Enable IEEE 802.1X authentication for this network. Go to step 18.

   ■ If the SSID is encrypted, select this option. 802.1X is required for access to any encrypted SSID.

12 If you enabled 802.1X, select **Protected EAP (PEAP)**. (If 802.1X is disabled, EAP is not used.)

13 Leave the **Authenticate as computer** and **Authenticate as guest** options disabled.

14 Click **Properties**.

15 Deselect **Validate server certificate**.

16 Select **Secured password (EAP-MSCHAP v2)** as the authentication method.

17 Click **OK** to close the Properties dialog for the SSID.

18 Click **OK** to close the Network Connection dialog box.

Using the quickstart Command

This example configures the following parameters:

- System name: WX1200-Corp

- Country code (regulatory domain): US

- System IP address: 10.10.10.4, on IP interface 10.10.10.4 255.255.255.0

> *The quickstart script asks for an IP address and subnet mask for the system IP address, and converts the input into an IP interface with a subnet mask, and a system IP address that uses that interface. Likewise, if you configure this information manually instead of using the quickstart command, you must configure the interface and system IP address separately.*

- Default route: 10.10.10.1

- Administrative user *wxadmin*, with password *let-mein*. The only management access the switch allows by default is CLI access through the serial connection.

- System Time and date parameters:

  - Date: 15th of November, 2004

  - Time: 6:58 PM

  - Timezone: *PST* (Pacific Standard Time), with an offset of -8 hours from Universal Coordinated Time (UTC)

- Unencrypted SSID name: *public*

- Username *user1* and password *pass1* for Web AAA; username *user2* and password *pass2* for Web AAA

- Encrypted SSID name: *corporate*

- Username *alice* and password *alicepass* for 802.1X authentication; username *bob* and password *bobpass* for 802.1X authentication

- Directly connected MAPs on port 2 and 3, each model AP2750

> *You can configure a directly connected MAP only on the WX1200. You can configure Distributed MAPs on the WX1200 or WX4400.*

The IP addresses, usernames, and passwords in this document are examples. Use values that are appropriate for your organization.

If you configure time and date parameters, you will be required to enter a name for the timezone, and then enter the value of the timezone (the offset from UTC) separately. You can use a string of up to 32 alphabetic characters as the timezone name.

Figure 1 shows an example. Users *bob* and *alice* can access encrypted SSID *corporate* on either of the MAPs. Users *user1* and *user2* can use the same MAPs to access unencrypted SSID *public*. Although the same hardware supports both SSIDs and sets of users, AAA ensures that only the users who are authorized to access an SSID can access that SSID. Users of separate SSIDs can even be in the same VLAN, as they are in this example.

Figure 1   Single-Switch Deployment
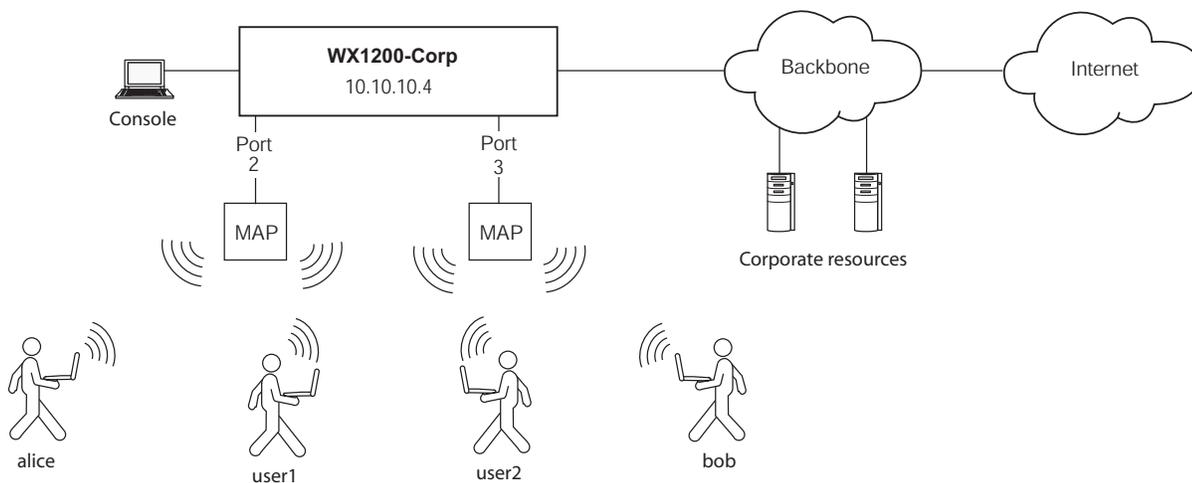
To run the **quickstart** command:

1 Attach a PC to the WX switch's serial console port. (Use these modem settings: 9600 bps, 8 bits, 1 stop, no parity, hardware flow control disabled.)

2 Press Enter three times, to display a username prompt (Username:), a password prompt (Password:), and then a command prompt such as the following:

```
WX1200>
```

3 Access the enabled level (the configuration level) of the CLI:

```
WX1200> enable
```

4 Press Enter at the Enter password prompt.

5 Type **quickstart**. The script asks you a series of questions. You can type **?** for more help. To quit, press **Ctrl**+**C**.

One of the questions the script asks is the country code. For a list of valid country codes, see the *Wireless LAN Switch and Controller Installation and Basic Configuration Guide*. The country codes are listed in the "Configuring a WX Switch for Basic Service" chapter, in the "Specifying the Country of Operation" section.

Another question the script asks is, "Do you wish to configure wireless?" If you answer **y**, the script goes on to ask you for SSID and user information, for unencrypted and encrypted SSIDs. If you answer **n**, the script generates key pairs for SSH and the administrative users you entered, generates a self-signed administrative certificate, and then ends.

```
WX1200# quickstart

This will erase any existing config. Continue?
[n]: y

Answer the following questions. Enter '?' for
help. ^C to break out

System Name [WX1200]: WX1200-Corp

System Name [WX1200]: WX1200-Corp

Country Code [US]: US

System IP address []: 10.10.10.4

System IP address netmask []: 255.255.255.0

Default route []: 10.10.10.1

Admin username [admin]: wxadmin

Admin password []: letmein

Do you wish to set the time? [y]: y

Enter the date (dd/mm/yy) []: 15/11/04

Enter the time (hh:mm:ss) []: 18:58:00

Enter the timezone []: PST

Enter the offset from GMT for 'PST' in hh:mm
[0:0]: -8

Do you wish to configure wireless? [y]: y

Enter a clear SSID to use: public

Do you want to do WEB-AAA? [y]: y
```

```
Enter a username with which to do web-aaa, <cr>
to exit: user1

Enter a password for user1: pass1

Enter a username with which to do web-aaa, <cr>
to exit: user2

Enter a password for user2: pass2

Enter a username with which to do web-aaa, <cr>
to exit:

Do you want to do 802.1x and PEAP-MSCHAPv2? [y]:
y

Enter a crypto SSID to use: corporate

Enter a username with which to do PEAP-MSCHAPv2,
<cr> to exit: alice

Enter a password for alice: alicepass

Enter a username with which to do PEAP-MSCHAPv2,
<cr> to exit: bob

Enter a password for bob: bobpass

Enter a username with which to do PEAP-MSCHAPv2,
<cr> to exit:

Do you wish to configure access points? [y]: y

Enter a port number [1-20] on which an AP
resides, <cr> to exit: 2

Enter AP model on port 2: ap2750

Enter a port number [1-20] on which an AP
resides, <cr> to exit: 3

Enter AP model on port 3: ap2750

Enter a port number [1-20] on which an AP
resides, <cr> to exit:

Do you wish to configure distributed access
points? [y]: n

success: created keypair for ssh
```

```
success: created keypair for admin

success: created self-signed certificate for
admin

success: created keypair for eap

success: created self-signed certificate for eap

success: created keypair for webaaa

success: created self-signed certificate for
webaaa

success: remember to save this config
```
WX1200# **save config**

6 Optionally, enable Telnet.

WX1200# **set ip telnet server enable**

7 Verify the configuration changes.

WX1200# **show config**

8 Save the configuration changes.

WX1200# **save config**

Configuring a Mobility Domain for Roaming

This procedure configures multiple WX switches to form a Mobility Domain. A Mobility Domain allows users to seamlessly roam from one WX switch to another. A Mobility Domain uses one seed switch. The other switches are members.

Add the switches to the same VLAN. Users can be in the same or different VLANs, and the user VLANs do

not need to be configured on all the switches. Users can log on and roam the network from the seed switch, or from any member switch, by tunnelling through any other switch that contains their VLAN.

i *For simplicity, the **quickstart** command assigns all users to the default VLAN.*

Figure 2   Mobility Domain Deployment
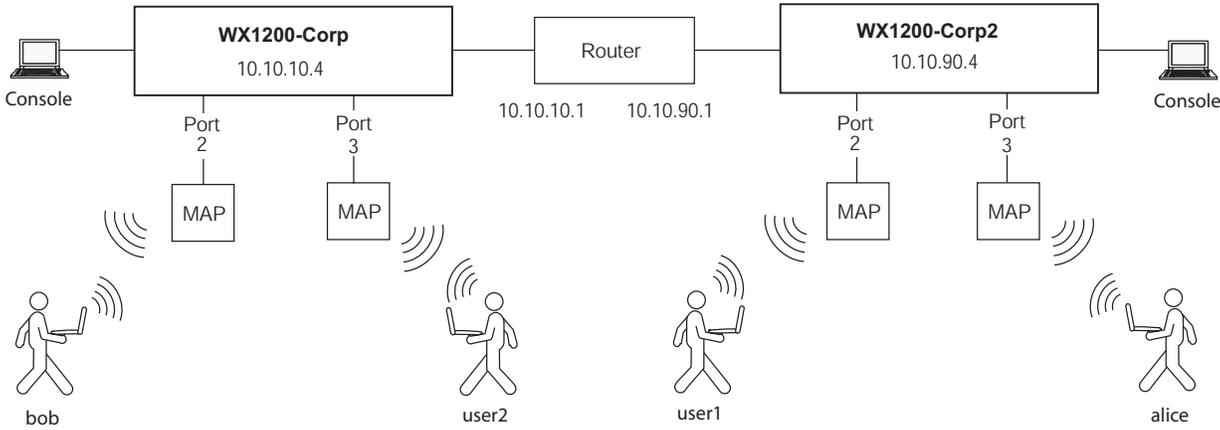
Configuring the Seed

1 Configure WX1200-Corp as the seed:

```
WX1200-Corp# set mobility-domain mode seed
domain-name Corp

WX1200-Corp# set mobility-domain member
10.10.90.4
```

2 Verify and save the configuration changes on WX1200-Corp.

```
WX1200-Corp# display config

# Configuration nvgen'd at 2004-10-13 11:02:18

...

set mobility-domain mode seed domain-name Corp

set mobility-domain member 10.10.90.4
```

```
WX1200-Corp# save config
```

Configuring a Member

1 Use the **quickstart** command to configure basic system parameters on a second switch (WX1200-Corp2).

2 Configure WX1200-Corp2 as a member of the Mobility Domain.

```
WX1200-Corp2# set mobility-domain mode member
seed-ip 10.10.10.4
```

3 Verify and save the configuration changes:

```
WX1200-Corp2# display config

# Configuration nvgen'd at 2004-10-13 11:23:26

set mobility-domain mode member seed-ip
10.10.10.4

WX1200-Corp2# save config
```

Opening the QuickStart Network Plan in 3WXM

3WXM comes with a sample plan called *3ComStarterExample*. This plan contains a simple rectangle as a floor plan, with one WX1200 switch and four AP2750 MAPs. The plan uses Web AAA for guest access and 802.1X for corporate access with local authentication.

The network plan contains a configuration similar to the one created by the CLI in the previous sections, but differs from the configuration by using separate VLANs for WX management traffic, corporate users,

and guest users. Otherwise, the configuration is the same.

To open the network plan:

1 Install 3WXM, if not already installed. (See the "Getting Started" chapter of the *Wireless LAN Switch Manager Reference Manual*.)

2 Start 3WXM by selecting **Start > Programs > 3Com > 3WXM > 3WXM**, or by double-clicking the **3WXM** icon on the desktop.

If you are starting 3WXM for the first time, or you have not entered license information previously, the License Information dialog box appears. You can view and modify the WX switch configurations without a license.

3 Click **Continue**.

4 Select 3ComStarterExample and click **Next**. (For more information, see the *Wireless LAN Switch Manager Reference Manual*.)