WIRELESS LAN SWITCH AND CONTROLLER MSS VERSION 6.0.4.6 RELEASE NOTES

Related Documentation

Please use these notes in conjunction with the following:

- *Wireless LAN Switch and Controller Quick Start Guide*
- *Wireless LAN Switch and Controller Hardware Installation Guide*
- *Wireless LAN Switch and Controller Configuration Guide*
- *Wireless LAN Switch and Controller Command Reference*
- *Wireless Switch Manager User's Guide*
- *Wireless Switch Manager Reference Manual*
- *3Com Mobility System Antenna Guide*

You can obtain the latest technical information for these products, including a list of known problems and solutions, from the 3Com Knowledgebase:

http://knowledgebase.3com.com

Software License Agreement

Before you use these products, please ensure that you read the license agreement text. You can find the license.txt file on the CD-ROM that accompanies your product, or in the self-extracting exe that you have downloaded from the 3Com Web site.

What's New in MSS Version 6.0

MSS Version 6.0 contains the following enhancements:

- *New AP3150 and AP3850 support*
- *802.1x Client Diagnostic Enhancement (additional debug information)*
- *SNMP/3ND Support*
- *AP/DAP Unification*
- *New Web View interface*
- *AeroScout RFID tag support*
- *Newbury Networks Location appliance support*
- *Persistent VLAN assignment for roaming clients*
- *Simplified Web-Portal and last-resort configuration*
- *RF Auto-Tuning enhancements*
- *Unscheduled Automatic Powersave Delivery (U-APSD) support*
- *DHCP server enhancements*
- *RADIUS accounting enhancements*
- *Support for special characters in SNMP community names*
- *Increased life span of new self-signed certificates*
- *CLI commands to specify location and contact information for MAPs*

Part No. 10016430 Rev. AA
Published November 2007

- *RF Load Balancing*
- *Logout for Web Authentication*
- *Mobility Domain WX Seed Redundancy*
- *Local Switching (AP3850 only)*
- *Mesh Services (AP3850 only)*
- *Wireless Bridging (AP3850 only)*
- *Enforceable Beacon Data Rate Control*
- *Password Management*
- *Local software images on MAPs*

For more information on new features, please see the *Wireless LAN Switch and Controller Configuration Guide* and *Wireless LAN Switch and Controller Command Reference*.

Feature Not Supported in MSS Version 6.0.4

- *WX-WX security*

Version Compatibility

This version of Mobility System Software (MSS) is intended for use with 3WXM Version 6.0 or higher only.

Minimum MSS Requirements for Upgrade

The following table lists the minimum MSS version that an MSS switch must be running when you upgrade the switch to MSS Version 6.0. If your switch is running an older MSS version, you can use the upgrade path to upgrade the switch to 6.0.

Product	Upgrade Path
WXR100	4.x -> 4.2.10.2.0 -> 6.0
WX1200	4.x -> 4.2.10.2.0 -> 6.0
WX4400	4.x -> 4.2.10.2.0 -> 6.0
WX2200	4.x -> 4.2.10.2.0 -> 6.0

CAUTION: *Do not attempt to upgrade directly from 4.2.3.2.0 to 6.0.x.x.x. You must upgrade to 4.2.10.2.0 first.*

CAUTION: *If you need to downgrade from MSS Version 6.0, you must downgrade to MSS Version 4.2.10 or later.*

Points to Note When Using the WXR100, WX1200, WX4400, or WX2200

Follow these best-practice recommendations during configuration and implementation to avoid or solve issues you might experience.

Best Practice to Follow When Upgrading a 3Com Enterprise Wireless Switch and 3Com Wireless Switch Manager

- Applies to 3Com Mobility System Software (MSS) for wireless switch models WX4400, WX2200, WX1200 and WXR100.

- Applies to 3Com Wireless Switch Manager (3WXM), Windows and Linux versions.

1 Create a full system backup of the wireless switch and 3WXM before beginning any upgrades. For details on how to perform a wireless switch (MSS) system

backup, refer to the section titled "Backing Up and Restoring the System" on page 613 of the MSS configuration guide. For details on the procedure for 3WXM, refer to the section titled "Upgrading 3WXM" of the 3WXM Reference Manual.

2 Upgrade 3WXM before upgrading the wireless switch (MSS). Newer versions of 3WXM are designed to handle older versions of MSS and will change their configuration model for switches that are running older versions of MSS. For example, 3WXM 6.0 can handle switches running 4.0.x, 4.1.x, 4.2.x, 5.0.x, or 6.0.x. However, older versions of 3WXM are not designed to manage newer versions of MSS. For example, 3WXM 4.2 is not designed to manage a wireless switch running 6.0.

3 After completing a successful upgrade of 3WXM, upgrade the wireless switch to the same major software version. 3Com recommends always running the same major version of 3WXM and MSS in a production environment. For example, 6.0.x.

4 If the CLI of the wireless switch indicates unsaved configuration changes after completing the upgrade (indicated with a * in front of the system name on the CLI), save the configuration using the 'save configuration' command.

5 When upgrading several switches, upgrade one at a time. After the upgrade has been completed on each switch, verify that it is operating properly before proceeding on to the next switch.

6 After the MSS upgrade has been completed, refresh the switch status in 3WXM. If Network changes are detected, they should be reviewed carefully before deciding whether to accept them into 3WXM. Accept all Network changes before attempting to deploy any Local changes.

7 After Network changes have been accepted and the switch status has been refreshed, carefully examine any remaining Local changes in 3WXM before deciding whether to deploy them to the wireless switch.

8 If you need to downgrade to an older version of MSS, the system will provide the option to use an automatically archived configuration file that was created when the system was upgraded. To apply a configuration that is compatible with the older version of MSS, you may choose to apply this archived configuration file.

Best Practice When Powering Down a Switch

If a WXR100 or WX1200 is connected to Power Sourcing Equipment (PSE), it is possible for the switch to remain powered on even when the power cord is unplugged. PSE can be a dedicated PoE injector or even another networking switch such as the WX that is capable of supplying PoE. To ensure that the switch is powered off, unplug the power cord, then unplug all Ethernet cables that are connected to other PoE devices.

System Configuration Best Practices

3Com strongly recommends that you use 3Com Wireless Switch Manager (3WXM) for archiving and version control of network-wide wireless LAN switch configurations. 3Com also recommends that you archive the CLI-based configuration files of individual WX switches by copying the configurations to a server.

Client and AAA Best Practices

Follow these best-practice recommendations during configuration and implementation to avoid or solve issues you might experience.

Get Clients and AAA Working First

The greatest majority of installation issues are related to clients and AAA server (authentication, authorization, and accounting) operation. 3Com recommends first establishing a baseline of proper operation with a sampling of wireless clients and the AAA server you plan to use. Working out client and AAA configuration methods first provides valuable information as you scale the deployment.

The selection of client and AAA server software will depend heavily on the requirements of your deployment. First, decide which EAP Protocol you will be using as that will restrict the available clients and servers. Each protocol has different advantages and disadvantages, which you will need to consider in your deployment. For most enterprise deployments, 3Com recommends using PEAP-MS-CHAP-V2 as the 802.1X protocol. The following table compares the EAP protocols.

Protocol	Advantages	Disadvantages
PEAP-MS-CHAP-V2	■ Does not require client certificates ■ Compatible with MSS EAP offload ■ Native support in Microsoft Windows XP and 2000 ■ Broad support in 802.1X clients	■ Username/password-based access might not be as strong as certificate-based access
EAP-TTLS	■ Does not require client certificates ■ Broadest compatibility with user directories	■ Requires third-party 802.1X client software ■ Username/password-based access might not be as strong as certificate-based access
EAP-TLS	■ Strongest authentication using X.509 certificates. ■ Native support in Windows XP and 2000 ■ Broad support in all 802.1X clients	■ Client-side certificates require full PKI infrastructure and management overhead
PEAP-TLS	■ Strongest authentication using X.509 certificates. ■ Native support in Windows XP and 2000 ■ Broad support in all 802.1X clients	■ Client-side certificates require full PKI infrastructure and management overhead ■ Minimal advantage over EAP-TLS

Although LEAP uses the same ethertype as 802.1X (0x888e), the LEAP protocol is proprietary and does not conform to the IEEE 802.1X standard. Additionally, the LEAP protocol has serious security flaws. For example, LEAP-authenticated networks can be breached using a simple dictionary attack.

When testing and evaluating MSS, enterprises using primarily Microsoft platforms are recommended to use Windows XP clients running PEAP-MS-CHAP-V2 with a Windows 2000 or 2003 server running Internet Authentication Service (IAS) as the RADIUS back end. This provides a test environment that is quick to set up and does not require additional third-party software.

Wireless NICs

Most wireless NICs available now support 802.1X authentication. The following table lists the NICs that have been used successfully with MSS. The majority were tested using recently available drivers using the Microsoft native 802.1X client and a Microsoft IAS RADIUS server. 3Com has not experienced any compatibility problems with NICs being unable to support specific EAP protocols or specific RADIUS servers, so we have only documented the differences in encryption type. Entries that have both Windows 2000 and Windows XP listed together have the same results for both operating systems. A result of *Pass* indicates successful authentication and roaming with the listed model and operating system. A result of *Fail* indicates an inability to successfully complete authentication. A result of NA (Not Applicable) indicates that the NIC does not support the listed encryption type. A result of NT (*Not Tested*) indicates that the combination has not been tested yet.

Currently, WPA/CCMP (AES) encryption is supported only when configured as the only cryptographic type in service profile. Enabling dynamic WEP or WPA/TKIP with AES on the same SSID can cause severe connectivity issues as some manufacturers' drivers do not work properly when both encryption types are enabled. 3Com recommends that you set up a separate service profile for WPA/CCMP with a different SSID for compatibility. If you are migrating from Dynamic WEP to WPA/TKIP, 3Com recommends creating separate service profiles for each encryption type and migrating users from one SSID to the other when they are configured to use TKIP.

As new drivers are released by the manufacturers, 3Com expects general compatibility to improve.

Mfgr	Model, Driver, and Driver Date	OS	WEP	Mixed TKIP/ WEP	TKIP	CCMP	Web
3Com	3CRPAG175B 1.1.0.21, 10/4/05	XP	Pass	Pass	Pass	Pass	Pass
3Com	3CRBAG675B 1.1.0.21, 09/19/05	XP	Pass	Pass	Pass	Pass	Pass
3Com	3CRPAG175 SL-3040 AA 5.1.2535.0, 7/1/2001	XP	Pass	Pass	Pass	Pass	Pass
3Com	3CRDAG675 SL-3045 AA 1.0.0.25, 8/1/2003	XP	Pass	Pass	Pass	Pass	Pass
3Com	3CRWE154A72	XP	Pass	Pass	Pass	Pass	Pass
3Com	3CRXJK10075 3.3.0.156, 12/26/04	XP	Pass	Not Tested	Pass	Not Tested	Not Tested
3Com	3CRUSB10075 6.3.3.2, 06/05/06	XP	Pass	Pass	Pass	Pass	Pass
Belkin	F5D8010 1000 1.2.0.80, 9/21/2004	XP	Pass	Pass*	Pass	Pass	Pass
Buffalo	WLI-CP-G54	XP	Pass	Not Tested	Pass	Pass	Not Tested
Cisco	Aironet MPI350 3.8.26.0, 5/4/2004	XP	Pass	Pass	NA	Pass	Pass
Cisco	Aironet AIR-CB20A 3.9.16.0, 9/20/2004	XP	Pass	Not Tested	Not Tested	Not Tested	Not Tested

Mfgr	Model, Driver, and Driver Date	OS	WEP	Mixed TKIP/ WEP	TKIP	CCMP	Web
Cisco	Aironet 350	XP	Pass	Pass	Not Tested	Not Tested	Not Tested
Dell	TrueMobile 1150[†] A00 7.43.0.9	XP	Fail	Fail	NA	NA	Pass
Dell	TrueMobile 1150[‡]	XP	Pass	Fail	Not Tested	NA	Not Tested
Dell	TrueMobile 1300	XP	Pass	Not Tested	Not Tested	Not Tested	Not Tested
Dell	TrueMobile 1400	XP	Pass	Pass	Pass	Pass	Not Tested
Dell	TrueMobile 1450 3.100.35.0, 11/27/2004	XP	Pass	Pass	Pass	Pass	Pass
D-link	DWLAG650	XP	Pass	Fail	Pass	Pass	Not Tested
D-link	DWL-AG660 A1,A2 3.0.0.44, 10/22/2003	XP	Pass	Pass	Pass	Pass	Pass
Intel	PRO/Wireless 2200BG 9.0.2.1, 8/23/2005	XP	Pass	Pass	Pass	Pass	Pass
Intel	PRO/Wireless 2915ABG 9.0.2.1, 8/23/2005	XP	Pass	Pass	Pass	Pass	Pass
Intel	PRO/Wireless WCB5000 1.0.1.33, 6/4/2003	XP	Pass	Pass	NA	NA	Pass
Intel	Pro2100(Centrino)[**]	XP	Pass	Pass[††]	Not Tested	Not Tested	Not Tested
Linksys	WUSB54GS 1.0.0.1, 6/18/2004	XP	Pass	Pass	Pass	Pass	Pass
Linksys	WPC54G 1.0 3.60.7.0, 3/22/2004	XP	Pass	Pass	Pass	Pass	Pass
Linksys	WPC54GS 3.50.21.10, 1/23/2004	XP	Pass	Pass	Pass	Pass	Pass
Linksys	WPC54G version 2	XP	Fail	Fail	Fail	Fail	Not Tested
Netgear	WG-511 1.0 2.1.25.0, 9/6/2004	XP	Pass	Pass	Pass	Pass	Fail[‡‡]
Netgear	WAG-511 0.1 3.1.1.754, 11/2/2004	XP	Pass	Pass	Pass	Pass	Fail[6]
Proxim	Orinoco Gold 8410	XP	Pass	Pass	NA	NA	Not Tested
Proxim	Orinoco Gold 8460[***] 3.1.2.19, 8/5/2004	XP	Pass	Pass	Pass	Pass	Pass
Proxim	Orinoco Gold 8470-WD 3.1.2.19, 8/5/2004	XP	Pass	Pass	Pass	Pass	Pass
Proxim	Orinoco Gold 8480	XP	Pass	Pass	Pass	NA	Not Tested
Proxim	Harmony 8450 1.4.1.1, 8/1/2002	XP	Fail	Fail	NA	NA	Fail[†††]
SMC	SMC2336A-AG 2.0 (99-012084-221) 2.4.1.32, 9/29/2003	XP	Pass	Pass	Pass	Pass	Pass

Mfgr	Model, Driver, and Driver Date	OS	WEP	Mixed TKIP/ WEP	TKIP	CCMP	Web
SMC	SMC2835W 1.0 (99-012084-163) 1.0.17.0, 6/16/2003	XP	Pass	Pass	Pass	NA	Pass
Symbol	LA-4121-1020-US 3.9.71.178, 3/25/2004	XP	Pass	Pass	Pass	NA	Pass

* Belkin Wireless Pre-N requires WPA/TKIP on a TKIP/WEP mixed SSID.
† Dell TrueMobile 1150 drivers v7.86 and newer might not work with Dynamic WEP when you have WPA/TKIP enabled. If you experience problems such as an inability to associate with the MAP, install the previous revision of the driver, which is available from Dell's support site.
‡ Requires a registry change to work properly; for more information, see "Windows 2000 Many enterprises have a large installed base of Windows 2000 laptops, making this a common choice of platform. Windows 2000 Service Pack 4 includes a native 802.1X client. If you choose to use the 802.1X client built-in to Windows 2000, please note the following:" on page 9.
** Intel Centrino based chipsets might not associate with the SSID when power-save mode is enabled. Future drivers or laptop firmware might resolve this issue, but until then 3Com recommends disabling power-save mode completely in the driver properties for the NIC.
†† The Intel Centrino based chipset has not been tested with WPA yet, though Dynamic WEP does operate properly in a mixed TKIP and WEP configuration.
‡‡ NetGear WG511/WAG511 doesn't associate properly to a WebAAA SSID. The NIC does not support DHCP.
*** Use the 848x driver, not the 846x driver.
††† Proxim Harmony 802.11a (8450) cannot associate properly.

Driver Dependent Behavior

Some clients prefer a beaconed clear SSID to their configured SSIDs. If you configure MSS to beacon a clear SSID, some client adapters prefer this beaconed SSID over the SSIDs they are configured to use.

Conversely, some adapters can associate only with a beaconed SSID. Determine whether to beacon the clear SSID based on the types of clients in the network.

Standby mode can prevent some clients from reassociating. If a laptop PC whose wireless adapter is associated with a Managed Access Point (MAP) goes into standby (hibernate) mode, the operating system can either freeze or experience a Blue Screen of Death (BSOD) when the laptop comes out of standby mode and attempts to reassociate with the access point. To work around this behavior, disable standby mode. Alternatively, disable and reenable the wireless adapter after the client emerges from standby mode.

If a client passes authentication but fails authorization, the client might indicate that authentication has succeeded but the MAP nonetheless disassociates from the client. In this case, the client might indicate that the network is unavailable. For example, this situation can occur if the certificate exchange is valid but the requested VLAN or ACL filter is not available, or a Mobility Profile™ denies service to the client. Once the MAP disassociates from the client, the network continues to be unavailable to the client through the MAP for the duration of the 802.1X quiet-period timer, which defaults to 60 seconds. An error message indicating that a client has failed authorization appears in the WX switch's system log.

802.1X Clients

Properly preparing your clients for wireless connectivity is one of the most important things you can do to ensure an easy rollout. Here are some guidelines for preparing common 802.1X clients and platforms.

Windows XP Windows XP is a popular platform for wireless clients because of its native support of 802.1X authentication and simplified configuration of wireless networks. If you choose to use the 802.1X client built-in to Windows XP, please note the following:

- *Microsoft has extensive documentation on how to configure and use wireless 802.1X authentication in an Active Directory environment, published on their website. You can start with Microsoft's Wi-Fi center at:*

  `www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx`

- *Installing Windows XP Service Pack 2 is recommended for all wireless clients as it includes several important hotfixes.*
- *If you are not prepared to install Service Pack 2, 3Com strongly recommends that all wireless clients use Service Pack 1a with the following hotfixes installed:*
  - KB826942—This is the WPA Hotfix Rollup and is available through Microsoft Update
  - KB834669—This corrects an 802.1X client issue which can cause system instability problems in Windows XP. You will need to contact Microsoft directly for this hotfix.
- *If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, you should enable computer authentication (also known as machine authentication) to achieve full functionality over your wireless connection.*
- *Download current drivers for your NICs from the NIC vendor(s).*
- *If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, 3Com recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. 3Com strongly recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.*
- *If you use computer authentication with different VLANs for the Computer and User accounts and do not have the WPA hotfix rollup (KB826942) or Service Pack 2, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer Authentication".*
- *If MD5 challenge is configured on a Windows XP client for wired authentication, the quiet period must be set to 0 to guarantee successful authentication. In addition, if the authentication is carried out manually, the timeout value must be set to no less than 30 seconds in order to allow the user ample time to enter their username and password. For example, to configure 802.1X on a WX switch to allow these users time to log in, type the following commands:*

  ```
  WX1200# set dot1x quiet-period 0
  WX1200# set dot1x tx-period 30
  ```

Windows 2000 Many enterprises have a large installed base of Windows 2000 laptops, making this a common choice of platform. Windows 2000 Service Pack 4 includes a native 802.1X client. If you choose to use the 802.1X client built-in to Windows 2000, please note the following:

- *Microsoft has extensive documentation on how to configure and use wireless 802.1X authentication in an Active Directory environment, published on their website. Most of this documentation is geared towards Windows XP, but both operating systems have many similarities in the client. You can start with Microsoft's Wi-Fi center at:*

  `www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx`

- *Installing Windows 2000 Service Pack 4 is required for all wireless clients.*
- *Some clients might experience system instability when using PEAP-MS-CHAP-V2 in an Active Directory environment. The primary symptom of this is a message displayed after login informing the user that the service svchost.exe has stopped unexpectedly. If you experience this problem, please contact Microsoft technical support and request hotfix KB833865.*
- *If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, 3Com recommends that you enable computer authentication to achieve full functionality over your wireless connection.*
- *Download current drivers for your NICs from the NIC vendor(s).*
- *Windows 2000 does not include a full implementation of the Wireless Zero-Config service from Windows XP, so you will need to use the client manager software provided with your NIC to configure your SSID and enable WEP encryption. When using dynamic WEP in Windows 2000, select static WEP 128bit and enter any static WEP key as a placeholder. This temporary key configures the driver to use WEP to encrypt packets, and the Microsoft 802.1X client then overrides the static WEP key you entered with a dynamic key after you authenticate successfully.*
- *If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, 3Com recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. If you are unable to install the client manager without the AEGIS component, contact the driver manufacturer or download an earlier version that does not contain the AEGIS component.*
- *16-bit PCMCIA and built-in NICs (some 802.11b cards in Dell, Toshiba, and other manufacturers' laptop PCs) might require a registry setting to be changed before they will be able to associate with any SSID. Microsoft Knowledge Base article 327947 documents the changes necessary to resolve the problem. Multi-band cards (A/B or A/B/G) are generally 32-bit and do not experience this problem.*
- *If you use computer authentication with different VLANs for the Computer and User accounts, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user*

authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer Authentication".

- *If you experience a delay in receiving your DHCP IP address wirelessly while using 802.1X authentication, you might need to install Microsoft hotfix KB829116. You must contact Microsoft technical support for this hotfix. It is not available from their website.*

Funk Odyssey ■*The Funk Odyssey client is required when you require WPA support on Windows 2000, or when you need to authenticate to an LDAP backend database that does not support MS-CHAP-V2 over LDAP. If you choose to use this client, please note the following:*

- *Download the latest version from Funk's website at: www.funk.com*
- *Be sure to turn off Wireless Zero Config in Windows 2000 by disabling the service.*
- *If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, 3Com recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. 3Com recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.*

Macintosh OS/X ■*OS/X Version 10.3, also known as Panther, includes an 802.1X client that supports Dynamic WEP and WPA/TKIP. If you choose to use this client, please note the following:*

- *The Panther client will only connect successfully to an SSID which is only dynamic WEP, or only WPA/TKIP. Any other configuration involving WEP with WPA enabled or AES is not supported by the current Panther client. If you need to run both WPA/TKIP and Dynamic WEP at the same time you must configured separate service profiles for each encryption type in order to maintain compatibility with Macintosh clients.*
- *The Panther client requires you to specify the inner and outer PEAP-MS-CHAP-V2 usernames in separate areas. Depending on your AAA backend, both usernames might require a domain prefix in the form of DOMAIN\username.*

Computer Authentication

Windows clients support 802.1X authentication of the computer itself. This is called computer authentication (also known as machine authentication). Computer authentication is useful when you want your computer to be active on the domain even when no users are logged in to the computer.

Some features of Windows XP Professional and Windows 2000 Professional work correctly only with an active network connection to the domain controller enabled before a user is logged on to the PC. Using computer authentication ensures that this network connection is established during the boot sequence, providing a wire-like infrastructure that allows you to use the following features on a wireless network.

The following table lists Microsoft networking features that require computer authentication.

Feature	Scenario Requiring Computer Authentication
Active Directory computer Group Policy	Computer–based Group Policy is applied during computer start up and at timed intervals—even when no on is logged in to windows.
Network logon scripts	Network logon scripts are run during initial user login.
Systems management agents	Systems management application agents such as those that come with Microsoft Systems Management Server (SMS) frequently need network access without user intervention.
Remote Desktop Connection	Computers are accessible from Windows Remote Desktop Connection when no one is logged in to windows.
Shared folders	Files and folders shared from a computer are still available, even when no user is logged in.

Configuring computer authentication on the client is simple, though it requires the use of the Microsoft 802.1X client built-in to Windows XP and Windows 2000. Keep the following information in mind when configuring computer authentication on Microsoft clients:

- *To enable computer authentication, go to the **Authentication** tab where you normally select your 802.1X authentication method and enable the checkbox labeled **Authenticate as computer when computer information is available**.*
- *The authentication protocol that is configured for your user accounts will also be used for the computer account.*
- *If the EAP protocol you are using requires client certificates, you must use the Microsoft Enterprise Certificate Authority built-in to Windows 2000 Server and Windows Server 2003 to generate Computer certificates for PCs on your active directory domain. Microsoft Knowledgebase Article KB313407 explains how to enable the automatic distribution of computer certificates through Active Directory.*
- *If the user and machine accounts use different VLANs, you must install hotfixes on the client PCs to enable them to DHCP for a new IP address when the user authentications. Windows XP requires either the WPA Rollup Hotfix (KB826942) or Hotfix KB822596. Windows 2000 requires hotfix KB822596.*
- *Using PEAP-MS-CHAP-V2 with computer authentication will allow users who have never logged on to a PC authenticate wirelessly without having to login to the PC over a wired connection the first time. EAP-TLS still requires the user to connect to the network over a wired connection to generate a profile on the PC and a user certificate.*

Enabling computer authentication also requires minor reconfiguration of Active Directory and IAS. Please note the following when configuring computer authentication on an active directory domain:

- *You must grant dial-in access for the computer accounts in Active Directory that you wish to enable computer authentication on. If the tab to configure dial-in access does not appear, follow the directions in Microsoft Knowledgebase article KB306260.*
- *Review your remote access policies in IAS to insure that the computer accounts have appropriate group membership to allow them to match the proper policy.*

Computer authentication also requires specific configuration considerations on the WX switch:

- *The username of a computer authentication connection will be in the form of host/fully-qualified-domain-name, for example host/bob-laptop.3Com.com or host/tac1-laptop.support.3Com.com. This username is the same regardless of the configured protocol (PEAP-MS-CHAP-V2 or EAP-TLS). An appropriate user-glob would be host/*.domain.com where domain.com is the Active Directory domain name. Alternatively, in a smaller deployment you could use a userglob of ** and have both user and computer authentication go to the same RADIUS server.*
- *PEAP-MS-CHAP-V2 offload mode is not supported with computer authentication. You must use pass-through 802.1X authentication policies with computer authentication.*

AAA

The following table lists the AAA servers and configurations that have been tested with MSS. Tests were performed to a local user database in most cases, and additionally to Microsoft Active Directory and LDAP with specific protocols as noted in the table. The tests were initially performed using Dynamic WEP, though subsequent testing has revealed no noticeable differences in RADIUS compatibility when using WPA.

A result of Pass indicates that the combination is supported by MSS. A result of NA (Not Applicable) indicates that the RADIUS server tested does not support the feature. A result of Fail indicates that the RADIUS server does not interoperate with MSS for that feature. A result of NT (Not Tested) indicates that the feature was not tested.

	RADIUS Servers Tested				
Configuration	**Win 2000 IAS**	**Win 2003 IAS**	**Funk Steel Belted Radius**	**Cisco ACS**	**Free-Radius (Linux)**
PEAP-MS-CHAP-V2	Pass	Pass	Pass	Pass	Pass
PEAP-MS-CHAP-V2 Offload	Pass	Pass	Pass	Pass	Pass
EAP-TLS	Pass	Pass	Pass	NT	Pass
EAP-TTLS	NA	NA	Pass	NA	NT
Single-Sign-On Active Directory & PEAP-MS-CHAP-V2	Pass	Pass	Pass	Pass	NA
Single-Sign-On LDAP & EAP-TTLS	NA	NA	Pass	NT	NT
3Com VSAs	Pass	Pass	Pass	Pass	Pass
MAC-based authentication	Pass	Pass	Pass	Pass	Pass
Microsoft Active Directory computer authentication	Pass	Pass	NA	Pass	NA

Testing notes Single-Sign-On is defined as clients being able to use the same username and password for 802.1X authentication that they use to authenticate with network services and logon to their local PC.

- *A Pass result for 3Com VSAs indicates that the VSAs were able to be added to the RADIUS server manually. Future versions of Steel Belted RADIUS and FreeRadius are planned to include standard definitions of the 3Com VSAs.*
- *Funk Steel Belted Radius version used for testing is 4.53*

- *Windows 2000 with Service Pack 4*
- *Cisco ACS 3.2 or later is required to support PEAP-MS-CHAP-V2*

WPA

WPA compatibility testing was conducted with a variety of NICs. See "Wireless NICs" for complete details of the results. If you choose to use WPA to secure your wireless network, please note the following:

- *CCMP (AES 802.11i draft support) is supported only when it is the only encryption type enabled on that SSID. Enabling TKIP or Dynamic WEP on the same SSID with CCMP can cause serious connectivity issues as most clients do not properly support this configuration. 3Com recommends that you create a separate service profile and SSID for WPA/CCMP.*
- *Enabling TKIP and Dynamic WEP on the same SSID is not recommended. This configuration forces the group key (multicast/broadcast key) to use the lowest common encryption type, in this case Dynamic WEP. Additionally, compatibility with wireless NICs is reduced.*
- *Downloading the latest drivers for your wireless NIC is strongly recommended. See "802.1X Clients" for specific information on installing drivers for your operating system.*
- *When a session key is changed, Microsoft WPA clients can sometimes incorrectly start using the new key before the end of the four-way handshake that is used to establish the key information. This issue can occur when the session timeout for the client session expires. As a result, the MAP rejects the client's re-association attempt because the key information presented by the client is invalid.*

  If you experience this issue, clear the Session-Timeout attribute on the affected users.

  The WX switch will not force a reauthentication of WPA/TKIP and WPA/CCMP users periodically like it does with dynamic WEP users.
- *Do not use the* ***set service-profile shared-key-auth*** *command in a WPA configuration. This command does not enable PSK authentication for WPA. To enable PSK for WPA, use the* ***set service-profile auth-psk*** *command.*
- *Use one WPA authentication method per SSID, either 802.1X authentication or preshared key (PSK) authentication, but not both.*

Security — Best Practice When Mixing Encrypted Access and Clear Access

It is possible to configure a RADIUS server or a WX switch's local authentication database so that a user with encrypted access and a user with unencrypted access are authorized to join the same VLAN from different SSIDs. This configuration might allow a hacker to more quickly discover keys by listening to both the encrypted traffic and unencrypted traffic for comparisons. You can either use the MSS SSID VSA or the encryption assignment VSA to prevent this problem.

If you only have one VLAN that each MAC-auth client should connect to, add the SSID VSA to the account for the MAC-address (either local or RADIUS). This will force the WX switch to only allow that MAC address to connect to the specified SSID.

If you require the same MAC user to be able to connect to more than one SSID, you can use encryption assignment to enforce the type of encryption a user or group must have to access the network. When you assign the Encryption-Type attribute to a user or group, the encryption type or types are entered as an authorization attribute into the user or group record in the local WX switch database or on the RADIUS server. Encryption-Type is an MSS VSA. Clients who attempt to use an unauthorized encryption method are rejected. In this way, a client could connect to any WEP encrypted SSID, but not a clear SSID. (See the *Wireless LAN Switch and Controller Configuration Guide* for more information.)

Security Best Practices

MSS and 3WXM provide robust options for securing management access, to WX switches and to the 3WXM client and 3WXM monitoring service. To optimize security for management access, use the following best practices.

Certificates

When anyone attempts to access a WX switch, the switch authenticates itself by presenting a signed certificate to the management application that is requesting access. The switch's certificate can come from a certificate authority (CA) or it can be generated and signed by the switch itself.

3Com recommends that you use certificates assigned by a CA. Certificates from a trusted CA are more secure than self-signed certificates. Here are some trusted CAs:

`http://www.verisign.com`

`http://www.entrust.com`

`http://www.microsoft.com`

If you use a self-signed certificate, configure the clients to not validate server certificates. If a client is configured to validate server certificates, the client will not be able to validate a self-signed certificate from the WX switch.

Usernames

3Com recommends that you do not create usernames that have the same spelling but use different case. For example, do not create both username *dang* and username *DANG*.

Passwords

The CLI, as well as 3WXM, can be secured using passwords. By default, the following access types do not have passwords configured. Each uses a separate password.

- *Console access to the CLI. To secure console access, configure a username and password in the WX switch's local database, using the* ***set user*** *command. After you configure at least one username and password and an access rule to permit them, access to the CLI through the console requires a password. (Access through Telnet or SSH is not possible without a password, even on an unconfigured switch.)*
- *Access to the enable (configuration) level of the CLI, through the console, or through Telnet or SSH. To secure enable access, configure the enable password using the* ***set enablepass*** *command.*

- *Access to 3WXM. To secure access, configure user accounts within 3WXM.*
- *Access to the 3WXM monitoring service. To secure access, configure user accounts within the monitoring service.*
- *Do not use passwords that are easy to guess, such as vehicle registration plates, family birthdays and names, or common words. Use combinations of uppercase and lowercase letters as well as numbers in all passwords.*

SNMP

SNMP is disabled by default. 3Com recommends that you leave SNMP disabled unless you are using 3Com Network Director or a similar product to manage your wired network. If you do need to use SNMP, do not use the well-known community strings *public* (commonly used for read-only access) or *private* (commonly used for read-write access.) By default, no SNMP community strings are configured. Use SNMP on an isolated management VLAN so that the clear text community strings are not visible on the public network.

To disable SNMP (if not already disabled), use the **set ip snmp server disable** command.

To change the community strings, use the **set snmp community** command.

CLI Access

MSS allows CLI access through the console, through Telnet, and through SSH. Console and SSH access are enabled by default. Telnet is disabled by default.

Configure a username and password, so that MSS requires login even for console access. Usernames and their passwords are not specific to the type of management access. You can use the same username and password for access through the console, Telnet, or SSH.

Leave Telnet disabled unless you need it. Use SSH instead.

Web Access

WebView uses HTTPS for encrypted communications and certificate-based server authentication, and requires use of the enable password.

WebView access through HTTPS is disabled by default. Unless you need to use WebView, leave the HTTPS server on the WX switch disabled. (Even though 3WXM also uses HTTPS, disabling the HTTPS server does not disable access by 3WXM.)

If you do need to use WebView, you can enable it using the **set ip https server enable** command. Use the following best practices to preserve or increase the security level related to Web access:

- *Use an enable password that follows the password recommendations given above.*
- *Use a CA-signed certificate instead of a self-signed certificate on the WX switch.*

If a user's client does not trust the certificate, the user might experience an additional delay during login. To avoid the additional delay, use a certificate signed by your CA or an Internet CA.

3WXM

By default, access to 3WXM and the 3WXM monitoring service do not require passwords. To secure access, configure user accounts within each instance of 3WXM and the monitoring service.

The monitoring service uses a signed certificate for authentication. The service has a self-signed certificate by default. For added security, used a certificate signed by a CA instead. To use a CA-signed certificate, install the certificate in a key store file on the machine where the monitoring service is installed, and change the name of the key store file used by the monitoring service from its default to the one where you installed the certificate signed by the CA.

Guest Access (unencrypted SSIDs)

If you need to prevent all guest access (access to unencrypted SSIDs):

- *Do not create any service profiles for SSID type clear.*
- *Delete any existing service profiles for a clear SSID.*

WebAAA Best Practices

If you plan to use WebAAA, see the "Configuring WebAAA" section in the "Configuring AAA for Network Users" chapter of the *Wireless LAN Switch and Controller Configuration Guide*. The section has configuration requirements and recommendations, in addition to an overview of the WebAAA process.

If you are upgrading from MSS Version 3.2, 3Com recommends that you read the manual even if the switch already uses WebAAA. The WebAAA implementation and its configuration requirements changed in MSS Version 4.0.

Communication Between the WX Switch and 3WXM or WebView

Administration certificate requirement (11974)

Before the WX switch can communicate successfully with 3WXM, you must create an administrative encryption certificate on the WX switch. For details, see the *Wireless LAN Switch and Controller Installation and Basic Configuration Guide*.

Mobility Domain™ (Multiple WX Switch) Best Practices

3Com recommends that you run the same MSS version on all WX switches in a Mobility Domain.

Helpful commands

Use the following commands to verify the proper operation of a Mobility Domain in support of features such as subnet roaming:

- ***display mobility-domain status*** *— In a functioning Mobility Domain, the output on every WX switch displays every WX switch in the Mobility Domain.*
- ***display roaming vlan*** *— In a functioning Mobility Domain, the output on every WX switch displays the network-attached VLAN of every other WX switch in the Mobility Domain.*

Other useful commands, documented in the *Wireless LAN Switch and Controller Command Reference*, include **display tunnel** and **display roaming station**.

Distributed MAP Best Practice When Using STP

A Distributed MAP is a leaf device. You need not enable STP on the port directly connected to the MAP.

If Spanning Tree Protocol (STP) is enabled on the port that is directly connected to a Distributed MAP, you might need to change the STP configuration on the port to allow the MAP to boot.

STP on a port directly connected to a Distributed MAP can prevent the MAP from booting.

Use IGMP Snooping Effectively

Using IGMP (11909, 12863, 12866)

MSS supports the Internet Engineering Task Force (IETF) draft *draft-ietf-magma-snoop* for controlling the forwarding of IP multicast traffic by a Layer 2 switch. The draft mandates the use of a 0.0.0.0 source IP address if no IP address is available on the switch for the subnet. However, some multicast routers and even other Layer 2 switches report errors in the presence of the 0.0.0.0 source IP address.

Apply the following methods to use IGMP snooping effectively:

- *Set IP addresses on all VLAN interfaces. This straightforward workaround prevents most known issues. If querier functionality might be needed, ensure that the IP address of the WX switch VLAN is higher than the address of any multicast router servicing the same subnet.*
- *Consider disabling IGMP proxy reporting. The IGMP proxy reporting function is enabled by default, but some multicast routers do not accept reports using a 0.0.0.0 source IP address. In this case, either assign an IP address to the VLAN interface on the WX switch or disable IGMP proxy reporting. To disable proxy reporting, use the command* ***set igmp proxy-report disable****.*

Disabling proxy reporting can increase IGMP overhead traffic to the multicast router.

- *Enable the IGMP querier only if needed. The IGMP pseudo-querier function is disabled by default. Enable it only if the source of a multicast stream is on a subnet the WX switch is also connected to. If this is the case, you must assign an IP address to the VLAN interface. The IP address must be higher than the IP address of the querier multicast router on the same subnet. To enable the IGMP pseudo-querier, use the command* ***set igmp querier enable****.*
- *Disable multicast router discovery. This multicast router solicitation protocol (part of draft-ietf-magma-snoop) is known to cause error messages with other IGMP snooping switches and multicast routers. To disable the protocol, use the command* ***set igmp mrsol disable****. (The protocol is disabled by default in the current software version.)*

User ACLs Require Explicit Source and Destination Addresses

A user ACL is an ACL that is applied to a specific username. You can apply ACLs to a user's inbound or outbound wireless traffic. For a user ACL to take effect, you must explicitly set both the source and destination addresses in the ACL.

Rogue Detection Active Scan Interval Is Longer During a SpectraLink SVP Call. (23317)

The active scan feature can be used during SVP calls. However, when a call is active, the interval at which active scan goes off-channel to look for rogues increases from once a second to once every 60 seconds.

Due to the longer interval between active scans, it can take longer for MSS to detect a rogue AP when an SVP call is active. Generally, detection of a rogue while a call is active can take from 3.5 to around 7.5 minutes. To reduce the detection time, add more MAPs to the coverage area.

Active Scanning and the AP3850

Active Scanning is not supported and must not be used with the AP3850 for the following countries:

Argentina (AR)
Australia (AU)
Bolivia (BO)
Brazil (BR)
Canada (CA)
China (CN)
Colombia (CO)
Dominican Republic (DO)
Guatemala (GT)
Hong Kong (HK)
Malaysia (MY)
Mexico (MX)
New Zealand (NZ)
Panama (PA)
Puerto Rico (PR)
Singapore (SG)
South Africa (ZA)
Taiwan (TW)
United States (US)
Uruguay (UY)

IPv6 Support

MSS 6.0 can forward IPv6 traffic transparently, at Layer 2. IPv6 clients in the same subnet can communicate with one another through a WX switch. However, MSS 6.0 does not support communication of IPv6 clients across subnets.

System Parameter Support

The following tables list the recommended or maximum supported values for major system parameters.

Mobility System Parameter	Supported Value
WX switches in a single Network Domain	500
WX switches in a single Mobility Domain	32
Roaming VLANs per WX switch	300 Does not include local statically configured VLANs
VLANs per Mobility Domain	400 This number consists of 300 roaming VLANs plus 100 local statically configured VLANs.
MAPs per WX	WX4400: ■ 300 configured ■ Up to 120 active, depending on the MAP type and licensing WX2200: ■ 320 configured ■ Up to 120 active, depending on the MAP type and licensing WX1200: ■ 30 configured ■ 12 active WXR100: ■ 8 configured ■ 3 active Includes directly attached MAPs and Distributed MAPs. Inactive configurations are backups.
Minimum link speed within a Mobility Domain	128 Kbps

Network Parameter	Supported Value
Forwarding database entries	WX4400: 16383 WX2200: 16383 WX1200: 8192 WXR100: 8192
Statically configured VLANs	100
Virtual ports (sum of all statically configured VLAN physical port memberships)	256
Spanning trees (STP/PVST+ instances)	64
ACLs and Location Policies	ACEs per switch: ■ WX4400: 2308 ■ WX2200: 2308 ■ WX1200: 700 ■ WXR100: 700 ACEs per ACL: ■ WX4400: 267 ■ WX2200: 267 ■ WX1200: 267 ■ WXR100: 25 Location Policies per switch: 1 The Location Policy can have up to 150 rules.
IGMP streams	500 Replication of a stream on multiple VLANs counts as a separate stream on each VLAN.

Management Parameter	Supported Value
Maximum instances of Wireless Switch Manager (3WXM) simultaneously managing a network	3
Telnet management sessions	WX4400: 8 WX2200: 8 WX1200: 4 WXR100: 4 The maximum combined number of management sessions for Telnet and SSH together is 8, in any combination.
SSHv2 management sessions	WX4400: 8 WX2200: 8 WX1200: 4 WXR100: 4
Telnet client sessions (client for remote login)	WX4400: 8 WX2200: 8 WX1200: 4 WXR100: 4
NTP servers	3
SNMP trap receivers	8
Syslog servers	4
RADIUS servers	100 configured on the switch 10 in a server group 4 server groups in a AAA rule

Client and Session Parameter	Supported Value
Authenticated and associated clients per radio	100 Clients who are authenticated but not yet associated are included in the total.
Active clients per radio	50 Total number of active clients simultaneously sending or receiving data.
Wired authentication users per port	500

Client and Session Parameter	Supported Value
Active AAA sessions (clients trying to establish active connections) per WX switch	WX4400: 2500 WX2200: 3200 WX1200: 300 WXR100: 75 These are the suggested maximums. The switch might be able to support even more sessions, but performance or system stability might be affected.
AAA users configured in local database	WX4400: 999 WX2200: 999 WX1200: 250 WXR100: 250

Known Problems

System Configuration Issues

Adding a static VLAN with the same name as a VLAN whose traffic is being tunneled through the switch can cause the switch to restart. (18367)

MSS can tunnel traffic for a VLAN through a WX switch that does not have that VLAN statically configured. If you attempt to add a static VLAN to a switch that is already tunneling traffic for a VLAN with the same name, the switch can restart.

To create the VLAN, clear the Mobility Domain configuration from the switch, create the VLAN, and then configure the Mobility Domain again.

The default value for RADIUS "deadtime" shown in the CLI help is incorrect. (41689)

The correct default value is 0.

When upgrading systems with large configurations, it may be necessary to save the configuration to a backup file. (41330)

When upgrading systems with very large configurations, for example, hundreds of APs or hundreds of users, it may be necessary to save the configuration to a backup file, generate a minimal configuration, perform the update, load the backup configuration from the command line, and then save the configuration.

Time and date do not synchronize with an NTP server, if the switch's NTP client is enabled before the NTP service is started on the server. (20382)

Using set ap <apnum> boot configuration commands. (38517)

The **set ap <apnum> boot-configuration switch switch-ip** cannot be set at the same time as **set ap <apnum> boot-configuration switch name <switch-name> dns <ip addr>**. The commands overwrite each other when used.

The auto-config feature does not work properly if the 3WXM server is unreachable when the auto-config feature is enabled. (44477)

To work around this issue, be sure that the 3WXM server is reachable from the wireless switch before you enable auto-config. If auto-config is enabled by default on the wireless switch, be sure that the 3WXM server is reachable before you boot the wireless switch.

Static IP settings do not work on the 8x50 or AP7250 Access Points. (28529)

The configuration of static settings including VLAN tag, WX IP, WX name, AP IP and AP IP mask are not supported on the AP8750, AP8250, or AP7250.

Switching and Port Issues

Port Mirroring is not active after the switch is rebooted. (29684)

Port mirroring configuration cannot be saved and is not retained through reboots of the WX switch.

Router redundancy protocol on intermediary devices between WX switches in a Mobility Domain can interfere with communication among the switches. (16910)

If the Mobility Domain contains intermediary switches or routers that use a router redundancy protocol, WX switches that communicate through those intermediary devices might lose communication with one other due to the way some router redundancy protocols handle MAC addresses. If this issue occurs, log messages appear periodically on the seed WX switch indicating that member WX switches are entering or leaving the Mobility Domain.

Set the FDB timer (default 300 seconds) and the ARP timer (default 1200 seconds) to the same values on the WX switches. 3Com recommends using 300 seconds as the value for both timers. To set the FDB timer, use the **set fdb agingtime** command. To set the ARP timer, use the **set arp agingtime** command.

Mixing Autonegotiation with full-duplex mode on a link causes slow throughput and can cause a WX port to stop forwarding. (26276)

3Com recommends that you do not configure the mode of a WX port so that one side of the link is set to autonegotiation while the other side is set to full-duplex.

Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to a WX port in such a configuration can cause forwarding on the link to stop.

Antenna sensing has been deprecated from system software. The antenna configuration is the authoritative source to enabling external antenna operation on the AP, even if the external antenna isn't actually connected. (34904)

FDB entry is not cleared when tagging mode on a port changes. (44970)

When the tagging mode on a port is changed, learned entries in the fdb are not cleared. As a result, connectivity may be lost. To work around this issue and restore connectivity, clear the fdb manually.

Client connecting to local switched untethered AP causes Mesh APs to time out. (44982)

In some configurations, a client connecting to a mesh AP that also has local switching enabled will cause other mesh APs in the network to time out and reboot.

Mesh Issues

The Ethernet port is not brought up on the bridge link if it was not up when the mesh link is established. (46037)

If the mesh AP is brought up without the Ethernet port connected, after the mesh link is established, the bridge link will not come up and no traffic will flow through the AP to the Ethernet port. To work around this issue and restore connectivity, reset the mesh AP ensuring that the Ethernet port is always up by connecting a hub or switch to the mesh AP Ethernet port.

MAP Issues

Distributed MAPs and Link Autonegotiation (16726)

The Ethernet interfaces on a MAP are configured to autonegotiate the link speed (10 Mbps or 100 Mbps) and mode (half duplex or full duplex). The setting cannot be changed. A common setting on third-party switches is 100 Mbps, with full duplex. If you connect a Distributed MAP to a port that is set for 100 Mbps with full duplex, the MAP operates at 100 Mbps with half duplex. This results in an unusable link. Configure the port on the other device to autonegotiate.

Wireless clients connected to directly attached APs may not display as connected in the show system output information. (41792)

When connected to the network using an Intel 2100 wireless network card, large file transfers may cause the wireless client to disconnect. (40721)

A distributed AP may not successfully boot if Port 1 of the AP has an operational Ethernet link, but an WX is unreachable via this data link. (38807)

All other combinations of power and data connectivity are fully supported.

Distributed MAP can change IP addresses during boot sequence in environments with multiple DHCP servers. (16499)

To become fully active, a Distributed MAP does a full restart after downloading its software image. The first time the MAP is powered up, it sends a DHCP discover for an IP address, uses DNS to find its configured WX switch, and then downloads its software image from that WX.

After downloading the image, the MAP restarts itself with the downloaded image and sends a second DHCP discover to again obtain its IP address. In a network containing more than one DHCP server, it is possible for the MAP to use one IP address when downloading the image, but end up with a second IP address after rebooting the second time. This can occur if the DHCP server that responds to the DHCP request after the second reboot is not the same server that responded to the first request.

This issue does not prevent the MAP from operating normally but can make managing the MAP more difficult if the address the MAP receives the second time is not predictable. To prevent the MAP from using more than one address, use static address assignment in your DHCP server.

WebView Issues

Unless otherwise noted, the workaround for WebView issues is to use the CLI or 3WXM.

WebView does not display more than 32 service profiles. (18374)

WebView allows configuration of duplicate SSID names in the same service profile. (18375)

In WebView, self-signed certificate for network user is not accepted with only a Common Name value. (15651)

If you use WebView to configure a self-signed certificate for network users, the switch does not generate the certificate if you enter information only in the Common Name field and not in other fields.

This issue does not affect the CLI. In the CLI, you can generate a self-signed certificate with only the common name specified. Use the CLI to generate the certificate or use the additional fields in WebView.

If you are running Linux Redhat 9 and use Firefox 2.0 to open WebView, the browser may become unresponsive. (40676)

This behavior is noted on the WX2200 and WX4400.

AAA and RADIUS Issues

Default 802.1X retransmit interval is too short for manual login. (18032)

The default 802.1X retransmit interval is 5 seconds. Although this interval is adequate for clients that are configured to automatically use the user's Windows login information as the network login information, the interval is too short for users who must manually enter their network login information.

If the network has clients that do not automatically use the Windows username and password as the network username and password, use the **set dot1x tx-period** command to increase the retransmit time.

CAUTION: *Changes to 802.1X parameters affect all SSIDs managed by the WX switch.*

Deleting a user group or MAC user group does not delete membership from its members. (14833)

If you type the **clear usergroup** or **clear mac-user-group** command to delete a user group or MAC user group, the **display aaa** command shows that the user group is gone. However, the user profiles for the users still list them as members of the deleted groups.

Use the **clear user group** and **clear mac-user group** commands in addition to the **clear usergroup** and **clear mac-usergroup** commands to explicitly remove individual users or MAC users from a group.

CLI allows set authentication dot1x command with invalid combination of pass-through and local options. (15562)

The CLI allows you to enter a command such as the following:

```
set authentication dot1x ssid any * pass-through
local
```

The pass-through and local AAA methods are mutually exclusive. Even if a server group named local exists, MSS does not use the group. In either case, the EAP session fails and the 802.11 session is deauthenticated when the client responds to the first identity request.

Do not name a server group local and do not attempt to mix mutually exclusive authentication methods in the same command.

Incorrect zero value for Acct-Authentic appears in accounting statistics. (14851)

In the output of the **display accounting statistics** command, the Acct-Authentic field in accounting records always displays 0 (zero) to indicate the location where a user was authenticated for the session. The correct value is 1 (one) if RADIUS performed authentication or 2 if authentication took place in the local WX database.

Ignore the Acct-Authentic value in **display accounting statistics** output.

Clients using Intel 3945ABG wireless NIC were unable to connect reliably to network. (28863)

Some client laptops using the Intel 3945ABG adapter card were not able to connect reliably to the network because the client ignored the initial GKHS message sent by the WX switch, timed out, and deassociated before the switch could retransmit the GKHS message.

To work around this problem, set the 802.1X supplicant timeout to 1 second. To do this, use the **set dot1x timeout supplicant** command.

CAUTION: *Changes to 802.1X parameters affect all SSIDs managed by the WX switch.*

WebAAA Issues

WebAAA using a Windows client and a WX switch that has a self-signed certificate can intermittently fail if Windows is configured to update root certificates. (18597)

If the WX switch uses a self-signed certificate (as opposed to a CA-issued certificate), and the Microsoft OS on the WebAAA client is configured to update root certificates (the default setting), Windows tries to contact microsoft.com to get updated certificates.

This causes a 15-second delay, after which IE displays a popup dialog asking whether the user wants to accept the untrusted certificate from the WX.

Even when the user selects Yes, IE sometimes does not display the WebAAA Login page served by the WX switch.

This issue occurs intermittently. If the issue occurs, reattempt the login.

IPv6 clients cannot authenticate using Web Portal. (26291)

The web-portal ACL does not work on IPv6 traffic. IPv6 clients will not be able to authenticate using Web Portal unless the clients also run IPv4.

This issue affects Web-Portal authentication only. The other authentication types (802.1X, MAC, and Last Resort) can be used with IPv6 clients.

ACL Issues

ACE names that begin with CLI keywords are not supported. (17521)

When configuring an access control entry (ACE), if the name you specify for the ACE begins with a word that is also a keyword used by the CLI, the CLI rejects the ACE name. In the following examples, the ACE names that begin with *port* and *vlan* are rejected, but the ACE name that starts with *abc*, which is not a CLI keyword, is accepted:

```
WX1200# set security acl ip port_abc deny
0.0.0.0 255.255.255.255

error: Wrong ACL name input = port_abc

WX1200# set security acl ip vlan_abc deny
0.0.0.0 255.255.255.255

error: Wrong ACL name input = vlan_abc

WX1200# set security acl ip abc_port deny
0.0.0.0 255.255.255.255
```

Do not use a CLI keyword in the beginning of an ACE name.

Session Issues

The display session network wired command does not list wired authentication sessions. (17829)

If you use the **wired** option with the **display sessions network** command, no sessions are listed.

Use the **display sessions network** command, without the **wired** option. In this case, the wired authentication sessions are included in the output.

The Unicast bytes fields in display sessions network sessions-id output can show a negative number. (18174)

IGMP Snooping and IP Multicast Issues

IP multicast streams can stop for all receivers on a MAP if IGMP snooping is disabled. (15971)

If you disable IGMP snooping, all clients that are receiving a multicast group stream through a MAP stop receiving the stream if one of the clients leaves the group.

Do not disable IGMP snooping. (The feature is enabled by default.)

Invalid IP multicast forwarded. (12784)

IGMP multicast streams with an invalid source IP address (for example, 0.0.0.0) are forwarded by the WX switch.

AP Issues

APs that are part of the Mobility System are identified as Rogues. (44686)

In some cases, valid APs that are part of the 3Com Mobility System may appear as rogue APs. This condition may be safely ignored.

AP3850 times out with high traffic on Bridge link. (45538)

The AP3850 may time out and reboot when in bridging mode if a high level of traffic is sent across the bridge.

Local Switching Issues

In some instances, an error message containing "SSR setup failed.mac" and a multicast address can be ignored. (44605)

Windows VISTA Issues

Windows Vista clients cannot connect to "hidden" SSIDs.

In its default configuration, Windows Vista does not connect to hidden "non-broadcast" SSIDs. Microsoft has changed this behavior in both Vista and the latest Windows client update for XP (KB# 917021) as part of an effort to increase security on wireless clients. For more information, please check the following URLS on Microsoft's website:

Non-broadcast Wireless Networks with Microsoft Windows:

`http://www.microsoft.com/technet/network/wifi/hiddennet.mspx`

Description of the Wireless Client Update for Windows XP with Service Pack 2:

`http://support.microsoft.com/?kbid=917021`

3Com recommends that, if you do not have direct control over the configuration of the wireless clients accessing your network, do not configure your service profiles with hidden SSIDs.

If you do have direct control over client configuration, you can change the default behavior. Here is a link to Microsoft's directions on how to change the default behavior of the Vista wireless client:

Connecting to non-broadcast wireless networks in Windows Vista:

`http://support.microsoft.com/kb/929661`

IE 7 issues with self-signed web-portal certificates

Microsoft has introduced more strict client security in Internet Explorer 7.0 which makes the use of self-signed certificates more confusing for end-users. When the WX attempts to process a client's web-portal login request, a screen displays this notice: "There is a problem with this website's security certificate" every time a client attempts to authenticate if the WX is using a self-signed certificate. While it is possible to choose the "Continue to this website" option, the user is discouraged from doing so for security reasons. This situation may lead to a noticeable increase in support calls from confused end-users.

3Com recommends that you do not use self-signed certificates for Web-Portal. In addition to the security issues with using an unverified certificate, the user experience is severely affected for IE 7 users. Use Verisign or another less expensive certificate authority to purchase a third-party verified certificate. If you are not using one of the major Internet certificate authorities (CA), verify that the CA's public certificate is included with all of the web browsers that you support on your network.

If you choose not to purchase a signed certificate from a third-party CA, you may choose to install the self-signed certificate into the trusted certificate store on every client that uses Web-Portal. IE 7 must be run with administrative privileges to perform this change, and it must be performed on each client who will use Web-Portal.

Wildcard Certificates in Web portal not working with IE 7

Internet Explorer's handling of wildcard certificates changes between IE 6 and IE 7, and for older versions of MSS, wildcard SSL certificates will not work in IE 7 with Web-Portal. A wildcard certificate is one that includes an asterisk as the hostname portion of the certificate's common name. For example, a wildcard certificate for 3Com Corporation would have a common name of "`*.3com.com`".

3Com recommends that you upgrade to MSS 5.0.11.4 or later. The Web Portal feature now handles wildcard certificates in a manner that is compatible with both IE 6 and IE 7.

Windows Vista Driver interoperability issues

Windows Vista drivers are relatively new and have not yet reached the maturity level of Windows XP drivers.

3Com recommends that you use the most recent Vista drivers available from the manufacturer's web-site. If that does not resolve the issue, you can try to run the Windows XP drivers for your wireless NIC; some of them may run under Vista and provide better results.

3WXM support in Windows Vista

3WXM does not officially support Windows Vista yet, so there may be some interoperability issues. Official support will be included in an upcoming release of 3WXM. Known issues include installer issues for the standalone client and the server, as well as intermittent failures to launch the Webstart Client.

3Com recommends that you do not run the 3WXM server on Windows Vista or Longhorn; use Windows Server 2003 instead. For clients accessing a 3WXM server who have no other choice of OS, run the Java Webstart client or use Microsoft's "Remote Desktop" client to connect to a Windows XP computer and run the client from there.

Vista Client interoperability issues

Vista client PCs have an interoperability problem with a Windows 2003 certificate server. The Windows 2003 certificate server must be patched with some files from a Windows Longhorn server. This URL gives the details:

`http://support.microsoft.com/?kbid=922706`

Upgrading MSS

Preparing the WX Switch for the Upgrade

CAUTION: Create a backup of your WX switch files before you upgrade the switch. 3Com recommends that you make a backup of the switch before you install the upgrade. If an error occurs

during the upgrade, you can restore your switch to its previous state.

Use this command to back up the switch's files:

```
backup system [tftp://ip-addr/]filename
[all | critical]
```

To restore a switch that has been backed up, use the following command:

```
restore system [tftp://ip-addr/]filename
[all | critical] [force]
```

"Upgrade Scenario" on page 28 of these Release Notes shows a sample use of the **backup** command. For more information about these commands, see the "Backing Up and Restoring the System" section in the "Managing System Files" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.

*If you have made configuration changes but have not saved the changes, use the **save config** command to save the changes before you backup the switch.*

If the switch is running an earlier version of MSS, use the **copy tftp** command to copy files from the switch onto a TFTP server.

Upgrading an Individual Switch Using the CLI

1. Back up the switch, using the **backup system** command. (See "Preparing the WX Switch for the Upgrade" on page 27.)
2. Copy the new system image onto a TFTP server.
3. Copy the new system image file from the TFTP server to a boot partition in the switch's nonvolatile storage.

   You can copy the image file only into the boot partition that was *not* used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.
4. Set the boot partition to the one with the upgrade image for the next restart.

   To verify that the new image file is installed, type **display boot**.
5. Reboot the software.

   To restart a WX switch and reboot the software, type the following command:

   ```
   reset system [force]
   ```

   When you restart the WX switch, the switch boots using the new MSS image. The switch also sends the MAP version of the new boot image to MAPs and restarts the MAPs. After a MAP restarts, it checks the version of the new MAP boot image to make sure the boot image is newer than the boot image currently installed on the MAP. If the boot image is newer, the MAP completes installation of its new boot image by copying the boot image into the MAP's flash memory, which takes about 30 seconds, then restarts again. The upgrade of the MAP is complete after the second restart.

Upgrade Scenario

To upgrade a switch (WX1200 used in this example) type commands such as the following.

This example copies the image file into boot partition 1. On your switch, copy the image file into the boot partition that was not used the last time the

switch was restarted. For example, if the switch booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the ***display boot*** *command.*

```
WX1200# save config
success: configuration saved.

WX1200# backup system tftp://10.1.1.107/sysa_bak
success: sent 28263 bytes in 0.324 seconds
[ 87231 bytes/sec]

WX1200# copy tftp://10.1.1.107/wb042302.rel
boot1:wb042302.rel
success: received 10266629 bytes in 92.427
seconds [ 111078 bytes/sec]

WX1200# set boot partition boot1
success: Boot partition set to
boot1:wb042302.rel (4.2.3.2.0).

WX1200# display boot

Configured boot version:         4.2.3.2.0

Configured boot image:
boot1:wb042302.rel

Configured boot configuration:
file:configuration

Backup boot configuration:       file:backup.cfg

Booted version:                  4.1.5.1

Booted image:
boot1:wx040105.020

Booted configuration:
file:configuration

Product model:                   WX1200

WX1200# reset system force

...... rebooting ......
```

Command Changes During Upgrade

The following table lists the commands that are deprecated in MSS Version 4.2, and their replacements.

4.1 Command	4.2 Command
set radio-profile wmm	set radio-profile qos-mode
set radio-profile long-retry	set service-profile long-retry
set radio-profile short-retry	set service-profile short-retry

During upgrade, MSS makes the following changes to commands in 4.1 configuration files:

- ***set radio-profile*** *name* ***wmm enable*** *is changed to* ***set radio-profile*** *name* ***qos-mode wmm***
- ***set radio-profile*** *name* ***wmm disable*** *is changed to* ***set radio-profile*** *name* ***qos-mode svp***
- ***set radio-profile*** *name* ***long-retry*** *and* ***set radio-profile*** *name* ***short-retry*** *are removed. The retry counts are reset to their default values and must be reconfigured manually, in the service profiles.*

In addition, MSS automatically adds a new option, **encrypted**, to **set radius** and **set radius server** commands that use the **key** option. The **encrypted** option encrypts the key string displayed in the configuration.

The option encrypts display of the string but does not encrypt the actual string sent to RADIUS servers. RADIUS servers still receive the string that was entered with the **set radius** or **set radius server** command in MSS Version 4.0.

To ensure that the command change is saved after you upgrade, after you load the new image and restart the

switch, enter the **save config** command as soon the switch finishes restarting.

For complete syntax information about the new commands and options, see the *Wireless Switch Manager Command Reference*.

Installing Upgrade Activation Keys on a WX4400 or WX2200

The WX4400 and WX2200 can boot and manage up to 24 MAPs by default. You can increase the MAP support up to 120 MAPs, by installing activation keys.

To obtain an activation key, access the 3Com web site (www.3Com.com). Each license and activation key pair allows the switch to actively manage an additional 24 MAPs. You can install up to four upgrade license and activation key pairs, to actively manage up to 120 MAPs.

To upgrade a WX license:

1. Obtain a license coupon for the upgrade from 3Com or your reseller.
2. Establish a management session with the WX switch to display the switch's serial number.

   To use the CLI to display the serial number, type the following command:

   ```
   display version
   ```

   In the following example, the switch serial number is 1234567890:

   ```
   WX1200> display version
   Mobility System Software Copyright (c) 2002,
   2003 reserved.
   Build Information: (build#67) TOP
   Model:             WX
   Hardware
   Mainboard: version 24 ; revision
   PoE board: version 1 ; FPGA
   Serial number 1234567890
   Flash: 4.1.0.14 - md0a
   Kernal: 3.0.0#20: Fri May
   BootLoader: 4.10 / 4.1.0
   ```

3. Install the license using the following command:

   ```
   set license
   ```

   The following example shows how to install an upgrade license and activation key:

   ```
   WX4400# set license WXL-076E-93E9-62DA-54D8
   WXA-3E04-4CC2-43OD-B508
   Serial Number: 1234567890
   License Number: 245
   License Key: WXL-076E-93E9-62DA-54D8
   Activation Key: WXA-3E04-4CC2-43OD-B508
   Feature: 24 additional ports
   Expires: Never
   48 ports are enabled
   success: license was installed
   ```