Operating System

Troubleshooting Microsoft Windows XP-based Wireless Networks in the Small Office or Home Office

Microsoft Corporation
Published: December 2004
Update: May 2005

Abstract

Because small office/home office (SOHO) wireless networks do not have servers to perform automated configuration and verify authentication credentials, in many cases the configuration of wireless networks is done manually, which can introduce errors relating to mismatched authentication and encryption settings. Other issues such as signal interference and signal attenuation can also cause a lack of connectivity or intermittent connectivity problems. This article describes how to troubleshoot the most common issues with Microsoft® Windows® XP-based wireless connections on a SOHO network.

Contents

Overview

This article describes how to troubleshoot an IEEE 802.11-based wireless network installed in a small office/home office (SOHO) that uses one or more wireless access points (APs) in an operating mode known as infrastructure mode and does not use IEEE 802.1X authentication and a Remote Authentication Dial-In User Service (RADIUS) server. For information about how to troubleshoot wireless LANs that use 802.1X and RADIUS for authentication, see Troubleshooting Windows XP IEEE 802.11 Wireless Access.

Although this article does not describe how to troubleshoot ad hoc mode-based wireless networks that do not contain a wireless AP, you can use many of the techniques for isolating mismatched configuration issues described in this article to troubleshoot ad hoc wireless networks.

Before we begin the discussion of specific problems and their solutions, it is helpful to review how to install Windows XP-based wireless clients in a SOHO wireless network and to discuss the steps that a Windows XP-based wireless client goes through to obtain a successful wireless connection.

Installing a SOHO Wireless LAN

For manual configuration of a SOHO wireless network, you must configure the 802.11 wireless network name (also known as a Service Set Identifier [SSID]), authentication settings, and encryption settings on your wireless AP and all of the wireless client computers individually. Wireless clients running Windows XP automate some elements of wireless network configuration with the Wireless Auto Configuration feature. For details about how to manually configure a SOHO wireless network, see Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business.

Manually configuring wireless APs, Windows XP wireless clients, and other types of wireless-capable devices can be a challenge, especially when configuring a strong Wired Equivalent Privacy (WEP) encryption key, a Wi-Fi Protected Access (WPA™) preshared key (PSK), or a WPA2™ PSK. For information about WPA2 support, see Wi-Fi Protected Access 2 (WPA2) Overview.

To make the configuration of a strong WEP key or WPA-PSK much easier, Windows XP Service Pack 2 (SP2) supports Windows Connect Now, a new feature of wireless devices that helps automate wireless network configuration. Windows XP SP2 supports Windows Connect Now through updates to the wireless client software and a new Wireless Network Setup Wizard. For more information, see The New Wireless Network Setup Wizard in Windows XP Service Pack 2.

The Wireless Connection Process

To determine the problem with an unsuccessful wireless connection, it is helpful to understand the steps in the process for a successful wireless connection for a typical Windows XP-based wireless client. These steps consist of the following:

1. Scan for wireless APs
2. Choose a wireless AP
3. Authenticate with the chosen wireless AP
4. Associate with the chosen wireless AP
5. Obtain a TCP/IP address configuration

Scan for Wireless APs

Every 60 seconds, a Windows XP-based wireless client computer with a wireless network adapter that supports Wireless Auto Configuration performs a scan for the available wireless networks within range. When scanning, the wireless network adapter sends a series of Probe Request frames. Wireless APs within range of the scanning wireless client computer send a Probe Response frame that contain the capabilities of the wireless AP, such as supported speeds and security options.

Choose a Wireless AP

From the received Probe Response frames, the wireless client chooses a wireless AP with which it will attempt to authenticate and associate. The wireless client uses the following factors when determining which wireless AP to choose:

- Wireless AP capabilities

  The wireless AP advertises its capabilities in the Probe Response frame. If the wireless network adapter does not support the capabilities of the wireless AP as advertised in the Probe Response frame, the wireless client cannot choose the wireless AP. For example, if the wireless AP only supports WPA security options and the wireless network adapter does not support WPA, the wireless client cannot choose the wireless AP. Another example is when the wireless AP only supports 802.11g and the wireless adapter only supports 802.11a.

- Wireless network name matches a preferred network

  Windows XP Wireless Auto Configuration maintains a list of preferred wireless networks corresponding to the wireless networks that a user of the computer has chosen to connect to. If the wireless network name, also known as the SSID, does not match the name of a wireless network in the preferred list, then by default Windows XP cannot connect to the wireless AP. If there are Probe Response frames from multiple wireless networks that are in the preferred list, then Wireless Auto Configuration chooses the most preferred wireless network (the highest one in the list).

  If the wireless network names of the received Probe Response frames do not match a preferred network, Windows XP prompts the user with a "One or more wireless networks are available" or "Connect to a wireless network" message in the notification area of the Windows XP desktop. When the user clicks this message, they can then choose to connect to a new wireless network.

- Signal strength

  The wireless network adapter of the wireless client chooses the wireless AP with the highest signal strength for the wireless network name that is highest in the preferred list.

Authenticate with the Chosen Wireless AP

After choosing the wireless AP with which to connect, the wireless client and wireless AP perform an authentication process. The type of authentication depends on the security capabilities of the wireless AP and how the wireless client has been configured to authenticate with the wireless network. If you are adding the wireless network from the **Wireless Networks** tab for the properties of your wireless connection, by default, the new wireless network is configured for open system authentication and then IEEE 802.1X authentication. If you are connecting to a wireless network from the **Connect to Wireless Network** or the **Choose a wireless network** dialog boxes, the authentication settings are determined from the capabilities in the wireless AP's Probe Response frame. A Windows XP-based wireless client can determine from the

Probe Response frame whether to perform open system authentication with no encryption, open system authentication with WEP encryption, WPA-PSK authentication, or WPA2-PSK authentication.

Associate with the Chosen Wireless AP

After the authentication has successfully completed, the wireless network adapter and the wireless AP exchange a series of messages to create an association, which uses one of the possible wireless connections of the wireless AP.

Obtain a TCP/IP Address Configuration

After a successful association, the wireless client can now begin sending wireless frames containing TCP/IP packets. If the wireless client is configured for automatic TCP/IP configuration, it uses the Dynamic Host Configuration Protocol (DHCP) to request an IP address configuration. Typically on a SOHO network, the wireless AP or the Internet gateway device acts as a DHCP server to answer the wireless client's request and assign an IP address configuration.

If the wireless client is configured for automatic addressing and a DHCP server is not present, then Windows XP assigns an Automatic Private IP Addressing (APIPA) address that begins with 169.254. With an APIPA address, the wireless client might not be able to reach other nodes on the SOHO network and will not be able to reach the Internet. If an APIPA address is assigned to the wireless connection, computers running Windows XP with SP2 display "Limited or no connectivity" for the status of the wireless connection.

If the wireless client does not use automatic addressing, then it must be configured with a manually specified IP address configuration that allows the wireless client to communicate with other computers on the SOHO network and to reach the Internet.

Common Problems with Wireless Connectivity

In this section, we examine the following most common problems with wireless connectivity on a SOHO wireless network:

- Unable to make a successful wireless connection
- Intermittent connectivity

Unable to Make a Successful Wireless Connection

Being unable to make a successful wireless connection (from scanning to obtaining an IP address configuration) is the most common type of problem. The most common reasons are the following:

- Mismatched configuration
- Wireless Auto Configuration is enabled and a third party wireless configuration tool is installed
- Wireless AP is performing MAC address filtering
- Sources of signal interference
- Sources of signal attenuation

Mismatched Configuration

Many different properties of wireless connections must be matched between the wireless AP and the wireless client before a successful connection can be made. Some of the most common mismatches are the following:

- Mismatched 802.11 technology

  There are three different standards for 802.11 wireless networking that are in common use today: 802.11b, 802.11a, and 802.11g. Although a lot of recently manufactured wireless LAN equipment supports the use of more than one of these standards, it is still possible to get a mismatch. For example, a wireless network adapter that only supports 802.11a will not connect to a wireless AP that only supports 802.11b and 802.11g.

- Mismatched authentication method

  This is a very common problem. The wireless client cannot authenticate if it is not using the same authentication method as the wireless AP. Wireless authentication methods for SOHO networks include open system, shared key, WPA-PSK, and WPA2-PSK. Because the use of shared key authentication is highly discouraged, that leaves open system authentication for wireless networks that are not WPA or WPA2-capable, WPA-PSK for wireless networks that are WPA-capable, and WPA2-PSK for wireless networks that are WPA2-capable.

  Verify the authentication method that is configured on the wireless AP and configure the Windows XP wireless client with the same authentication method.

  For examples of configuring wireless networks for open system, WPA-PSK, and WPA2-PSK authentication, see Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business.

- Mismatched WEP keys

When using WEP encryption and manually specifying the WEP key, it is easy to incorrectly type the key. Mismatched WEP keys will not prevent an association, but it will prevent any successful communication on the wireless network because the wireless client and the wireless AP will be unable to interpret each other's frames. As a result, the wireless client will be unable to obtain an automatic IP address configuration or communicate with any network resource through the wireless AP. For example, a Windows XP with SP2-based wireless client will obtain an APIPA address and display "Limited or no connectivity" for the status of the wireless connection.

The method of configuring the WEP key depends on the version of Windows on the wireless client.

- For Windows XP with no service packs installed, you must type the WEP key (in the **Network key** field), specify the format for the WEP key (either ASCII characters or hexadecimal digits in the **Key format** field), and specify the key length (either 40 bits or 104 bits in the **Key length** field). You must match the WEP key for the proper format and key length to that which is configured on the wireless AP.
- For Windows XP with SP1 or Windows XP with SP2, you must specify the WEP key twice in the **Network key** and **Confirm network key** fields. You do not have to specify the key format or length because these are automatically determined from the typed key. For Windows XP with SP2, you must select **WEP** in **Data encryption**.

When you use the Wireless Network Setup Wizard in Windows XP SP2, all the devices that support Windows Connect Now are automatically configured with the same WEP key.

- Mismatched WEP key index

  The WEP key index is a number that specifies which WEP key to use for the encryption of wireless frames. You can use up to four different WEP keys. In practice, only a single WEP key is used, corresponding to the first possible WEP key. The wireless AP and the wireless client must both be configured to use the first possible WEP key.

  Specifying the first possible WEP key depends on how the wireless client and wireless AP begin numbering the four possible WEP keys. For example, they could begin numbering them at 1 (from 1 to 4) or they could begin numbering them at 0 (from 0 to 3). In either case, choose the first possible value on both the wireless client and the wireless AP. For example, Windows XP with no service packs installed begins numbering the possible WEP keys with 0. Windows XP with SP1 or Windows XP with SP2 begins numbering the possible WEP keys with 1.

- Mismatched WPA-PSK or WPA2-PSK

  If you are using WPA-PSK or WPA2-PSK authentication, you must configure a preshared key value in the **Network key** and **Confirm network key** fields. Verify that the WPA-PSK or WPA2-PSK value is the same as that which is configured on the wireless AP. For WPA, you must select **TKIP** in **Data encryption** and **WPA-PSK** in **Network Authentication**. For WPA2 with Windows XP with SP2, you must select **AES** in **Data encryption** and **WPA2-PSK** in **Network Authentication**.

  When you use the Wireless Network Setup Wizard in Windows XP SP2, all the devices that support Windows Connect Now are automatically configured with the same WPA preshared key value. The Wireless Network Setup Wizard does not support the configuration of a WPA2 preshared key value.

Wireless Auto Configuration is Enabled and a Third-Party Wireless Configuration Tool is Installed
Windows XP Wireless Auto Configuration provides integrated support for wireless networking and helps automate wireless configuration. Wireless network adapters also provide a wireless network configuration tool. If the wireless network adapter driver supports Wireless Auto Configuration, installation and use of the network adapter vendor's configuration tool is not needed. To test whether your wireless network adapter supports Wireless Auto Configuration, right-click the wireless connection in the Network Connections folder and then click **Properties**. If there is a **Wireless Networks** tab, your wireless network adapter supports Wireless Auto Configuration.

Problems with initial configuration and connectivity can occur when Wireless Auto Configuration is enabled and the wireless network configuration tool is installed. In this case, both Wireless Auto Configuration and the wireless network configuration tool might be sending their settings to the wireless network adapter, resulting in configuration mismatches.

To solve this problem, use either Wireless Auto Configuration or the wireless network configuration tool, but not both.

For example, if there is a capability of your wireless network adapter that you must use and Wireless Auto Configuration does not support it (such as the configuration of a 152-bit WEP encryption key), then disable Wireless Auto Configuration and use the wireless network configuration tool. To disable Wireless Auto Configuration, clear the **Use Windows to configure my wireless network settings** check box on the **Wireless Networks** tab for the properties of the wireless connection in Network Connections.

If you decide to use the wireless network configuration tool supplied by the wireless network adapter vendor, then you must use this tool to specify all of your wireless network settings (such as the wireless network name, and authentication and encryption settings), rather than using the properties of a wireless network from the **Wireless Networks** tab.

If you want to use Wireless Auto Configuration, then remove the wireless network configuration tool using Control Panel-Add or Remove Programs or some other means provided by the wireless network adapter vendor, such as uninstall option available via the Start menu.

Wireless AP is Performing MAC Address Filtering
Some wireless APs allow you to specify the set of 6-byte media access control (MAC) addresses that are allowed to send frames to the wireless AP. MAC addresses are also known as hardware or physical addresses. This feature is known as MAC address filtering and is designed to provide an extra layer of security for wireless networking. However, an attacker can easily thwart this extra security by capturing the frames sent to or from an allowed wireless client and reprogramming their own wireless network adapter to use a valid MAC address.

If you want to use MAC address filtering, ensure that the MAC address filter list includes all of the MAC addresses for all of the wireless network adapters installed in all of the wireless clients on your network. If you install a new wireless network adapter, you must update the MAC address list to include the MAC address of the new adapter.

If you do not want to use MAC address filtering, ensure that it is disabled on the wireless AP.

Sources of Signal Interference
IEEE 802.11b and 802.11g wireless networks operate in the 2.4-2.5 GHz S-Band Industrial, Scientific, and Medical (ISM) frequency range that is used by other types of wireless devices such as cordless phones,

baby monitors, home security and monitoring systems, Bluetooth-enabled devices, and wireless video cameras. Other types of devices that are not wireless but produce signals in the S-Band ISM include microwave ovens. If you have sources of interference, it might not be possible to successfully connect with a wireless AP.

To verify whether signal interference is the problem, temporarily turn off or otherwise disable the possible sources of interference and try to connect to your wireless network. If it is not possible to disable a source of interference, such as a security system, then move the wireless client and wireless AP away from the house or office and attempt the connection again.

Sources of Signal Attenuation

Walls, ceilings, and the presence of metal or shielding between wireless clients and the wireless AP can cause wireless networking signals to attenuate, or lose their strength. In some cases, the signal loss is complete, resulting in the inability to make a wireless network connection.

To verify whether signal attenuation is the problem, set the wireless client in the same room as the wireless AP with a clear line of sight to the wireless AP. Try not to set the wireless client too close to the wireless AP because, depending on the design of the wireless AP's antenna, you might be placing the wireless client in the wireless AP's signal shadow. Try to connect from different locations in the room.

Intermittent Connectivity

In some cases, it is possible to initially obtain a successful connection, but the wireless connection is automatically disabled or disconnected without user intervention. The most common causes are the following:

- 802.1X authentication is enabled on the wireless client and not the wireless AP
- Duplicate wireless network name
- Sources of signal interference
- Sources of signal attenuation
- Computer viruses
- Faulty hardware or outdated wireless network adapter drivers

802.1X Authentication is Enabled on the Wireless Client and Not the Wireless AP

By default, 802.1X authentication is enabled on all wireless and wired network connections. In Windows XP SP1, Microsoft changed the authentication process for wireless networks. If 802.1X authentication is enabled and 802.1X authentication does not complete properly, the connection is dropped. This typically happens three minutes after the connection has been made using open system authentication.

To correct this problem for computers running Windows XP with SP1, do the following:

1. Click **Start**, point to **Settings**, and then click **Network Connections**.
2. In Network Connections, right-click your wireless connection and then click **Properties**.
3. Click the **Wireless Networks** tab.
4. Under **Preferred networks**, click your wireless network name, and then click **Properties**.
5. Click the **Authentication** tab, and then clear the **Enable IEEE 802.1x authentication for this**

network check box.

6. Click **OK** twice to accept the changes.

This procedure is typically not required for computers running Windows XP with no service packs installed or Windows XP with SP2. However, it is usually a good idea to verify that 802.1X authentication is disabled when you are using open system authentication. For Windows XP with SP2, use the previous procedure. For Windows XP with no service packs installed, do the following:

1. Click **Start**, point to **Settings**, and then click **Network Connections**.
2. In Network Connections, right-click your wireless connection and then click **Properties**.
3. Click the **Authentication** tab, and then clear the **Enable network access control using IEEE 802.1x** check box.
4. Click **OK** to accept the changes.

Duplicate Wireless Network Name

One of the reasons for intermittent connectivity is that your wireless network name has been duplicated with another separate wireless network within range of your wireless clients. For example, you might live in an apartment building and your wireless network overlaps with another wireless network with the same wireless network name above or below your apartment. In this configuration, all of the wireless APs that are advertising the same wireless network name are considered as belonging to the same wireless network. In this case, it is possible for your wireless client to choose the wireless AP of another wireless network over your own wireless APs. If your wireless client is not configured for the authentication method and keys of the other wireless network, then you can experience intermittent connectivity problems, until your wireless client chooses one of your wireless APs again.

Duplicate wireless network names can result when multiple wireless networks are set up using the default wireless network name as configured on the wireless AP. To prevent this problem, always change the default name of the wireless network when initially configuring the wireless AP.

To verify that your wireless network is not being duplicated by another wireless network that is within range of your wireless clients, disable or turn off your wireless APs. Then, use a computer running Windows XP to scan for the available wireless networks. If your wireless network name appears in the list of available networks when your wireless APs are turned off, then you have a duplicate wireless network name. Reconfigure your wireless AP for a new and unique wireless network name (also known as an SSID).

Sources of Signal Interference

Just as sources of signal interference can cause a lack of connectivity, they can also cause intermittent connectivity problems when the device causing the interference is running. Devices such as microwave ovens, baby monitors, and cordless phones can cause intermittent wireless connectivity problems when they are running.

To determine whether a source of signal interference is causing intermittent connectivity loss, try to correlate the times of connectivity loss with the times that a device causing signal interference is being operated. For example, does the connectivity loss occur whenever someone uses the microwave oven or when the baby monitor is turned on in the evening?

Sources of Signal Attenuation

Just as sources of signal attenuation can cause a lack of connectivity, they can also cause intermittent connectivity problems when the object causing the attenuation is moved. To determine whether a source of signal attenuation is causing intermittent connectivity loss, try to correlate the times of intermittent connectivity with the times that an object that might cause signal attenuation is moved. For example, does the intermittent connectivity occur whenever someone opens the large metal door between the garage and the kitchen?

Computer Viruses

Some computer viruses are known to cause intermittent connectivity problems for wireless connections. Ensure that you have the latest antivirus signature for your antivirus software and perform an antivirus scan of your entire computer to eliminate this possibility.

Faulty Hardware or Outdated Wireless Network Adapter Drivers

Another cause for intermittent connectivity is that the wireless AP or the wireless network adapter is faulty. This issue can be difficult to determine. Run any diagnostic facilities of your wireless AP or wireless network adapter to determine that they are operating properly. Ensure that you have installed the latest version of the wireless network adapter driver in Windows XP.

Checklist for Wireless Connections

Here is a quick checklist that should resolve most of the problems with wireless connections for a SOHO wireless network:

1. Verify that the wireless AP plugged in and operating. For example, check for indicator lights on the wireless AP.
2. If the wireless AP is also your router to the Internet, verify that the router's wireless capabilities are enabled.
3. Verify that your wireless AP and all of your wireless clients use a common 802.11 standard, such as 802.11a, 802.11b, or 802.11g.
4. Verify that the wireless network adapters installed on your wireless clients are properly plugged in and enabled. If a wireless connection corresponding to the wireless network adapter appears in the Network Connections folder, then the wireless network adapter is properly plugged in. If the wireless connection has been disabled, it will display **Disabled** in its status under the wireless connection's name in the Network Connections folder. To enable the disabled wireless connection, right click it and click **Enable**.
5. Verify that you are using the latest version of the wireless network adapter driver that is available from Microsoft or the wireless network adapter vendor. To obtain the version of the wireless network adapter driver that is installed, right-click the wireless connection in the Network Connections folder. On the **General** tab, click **Configure**. From the wireless network adapter properties dialog box, click the **Driver** tab. The version of the wireless network adapter driver is displayed next to **Driver Version**. If your wireless client is connected to the Internet, click **Update Driver** to launch the Hardware Update Wizard and search Windows Update for a newer version of the driver. Alternately, check the wireless network adapter vendor's Web site for a newer version of the driver.
6. Verify that the wireless AP and your wireless clients are configured for the same authentication method (open system authentication, WPA-PSK, or WPA2-PSK).
7. Verify that the wireless client is within range of the wireless AP and that there are no sources of signal interference or attenuation that could prevent successful connectivity.
8. Verify that you are using either Wireless Auto Configuration or a wireless network configuration tool provided by the wireless network adapter vendor, but not both. If you are not using a wireless network configuration tool, verify that the Wireless Zero Configuration or Wireless Configuration service has been started using the Services snap-in available from the Administrative Tools folder.
9. For WEP encryption, verify that the wireless AP and your wireless clients are configured with the same WEP encryption key (using the same key format and for the same key length). When you use the Wireless Network Setup Wizard in Windows XP SP2, all the devices that support Windows Connect Now are automatically configured with the same WEP key.
10. For WEP encryption, verify that the wireless AP and your wireless clients are configured to use the first possible WEP key.
11. For WPA-PSK authentication, verify that the wireless AP and your wireless clients are configured with the same WPA preshared key value (using the same key format and for the same key length).

When you use the Wireless Network Setup Wizard in Windows XP SP2, all the devices that support Windows Connect Now are automatically configured with the same WPA preshared key value.

12. For WPA2-PSK authentication, verify that the wireless AP and your wireless clients are configured with the same WPA2 preshared key value (using the same key format and for the same key length).

Summary

The most common issues with connecting Windows XP-based wireless clients to SOHO wireless networks are typically due to mismatched configuration parameters between the wireless AP and the Windows XP-based wireless client (such as authentication method, WEP key, and WPA or WPA2 preshared key value), conflicts between multiple sources of wireless network configuration, and sources of signal interference and attenuation. Use the checklist provided in this article to resolve most of the issues related to problems with Windows XP-based connectivity to a SOHO wireless network.

Related Links

See the following resources for further information:

- Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx
- The New Wireless Network Setup Wizard in Windows XP Service Pack 2 at http://www.microsoft.com/technet/community/columns/cableguy/cg0604.mspx
- Wireless LAN Enhancements in Windows XP Service Pack 2 at http://www.microsoft.com/technet/community/columns/cableguy/cg0804.mspx
- How to troubleshoot wireless network connections in Windows XP at http://support.microsoft.com/default.aspx?scid=kb;en-us;313242
- How to troubleshoot wireless network connections in Windows XP Service Pack 2 at http://support.microsoft.com/default.aspx?scid=kb;en-us;870702
- Troubleshooting Home Networking in Windows XP at http://support.microsoft.com/default.aspx?scid=kb;en-us;308007
- Home and Small Office Networking with Windows XP at http://www.microsoft.com/homenet

For the latest information about Windows XP, see the Windows XP Web site at http://www.microsoft.com/windowsxp.