Troubleshooting Wireless Networks

by Sophia

WHAT'S COVERED

In this lesson, you will learn more about troubleshooting network problems, especially problems with wireless networks.

Specifically, this lesson will cover the following:

1. Wireless Network Issues

Imagine that a user who is experiencing trouble accessing the network, or network resources, is telling you they only use a wireless connection. Troubleshooting wireless connectivity in an enterprise environment presents a

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

new set of possible Layer 1 (Physical) problems to think about and sort through.

Wireless networks are really convenient for the user because they provide mobility, but troubleshooting wireless networks can be challenging for network administrators. Wireless networks may take more time to troubleshoot because they are usually connected to, and supported by, a wired network. So, you not only need to work through a new set of troubleshooting challenges related to the wireless infrastructure, but you need to consider all the wired challenges you learned about in the previous tutorial. The following sections will help you with some of those new wireless challenges.

1a. Interference

Because wireless networks rely on radio waves to transmit signals, they are prone to interference from other wireless devices including Bluetooth keyboards, mice, or cell phones that are all close in frequency ranges. Any of these, even microwave ovens, can cause signal disruptions that can slow down or prevent wireless communications.

HINT

Factors like the distance between a client and a wireless access point (WAP) and the features of the physical environment between the two can affect signal strength and even intensify the interference from other signals. So, careful placement of that WAP is crucial.

1b. Device Saturation/Bandwidth Saturation

Clearly, it is important to design and implement your wireless network correctly. Be sure to understand the number of hosts that will be connecting to each access point (AP) you are installing. **Device saturation** occurs when you have too many devices connected to an AP; it results in low available bandwidth.

REFLECT

Perhaps you have had this experience in a coffee shop or in a hotel and you noticed how slow the wireless is. This is directly due to device and/or bandwidth saturation for each AP.

Whereas device saturation results from too many devices, **bandwidth saturation** occurs when the overall activity on a wireless network exceeds the capacity of the APs. This results in high latency (delay) and poor performance for all connected devices. Unfortunately, just adding more APs doesn't always solve the problem, and the solution often involves a complex reconfiguration of the wireless infrastructure.

TERMS TO KNOW

Device Saturation

Having too many devices connected to a wireless access point, which will result in low bandwidth availability.

Bandwidth Saturation

A condition that occurs when activity on a wireless network exceeds the capacity of the wireless access points, which results in high latency and poor performance.

1c. Simultaneous Wired/Wireless Connections

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

It is not unusual to find that a user's device has both a wired and a wireless connection at the same time. This typically doesn't create a problem, but it also doesn't do any good. Simultaneous wired and wireless connections generally will not provide the user with more bandwidth or better performance.

It is possible that the configurations can cause a problem, although that is rare these days. For instance, if each provides a DNS server with a different address, it can cause name resolution issues, or even default gateway issues. Most of the time, it just causes confusion for the user's device, which may need to work harder to determine the correct DNS or default gateway address to use. And in some cases, it is possible for the device to give up and stop communicating completely. Because of this, you need to remind the user to disconnect their wireless connection when they plug their device into an Ethernet port.

1d. Distance/Signal Strength/Power Levels

Sometimes your clients are too far from the AP. If your AP doesn't seem to have enough power to provide a connectivity point for your clients, you can move it closer to them, increase the distance that the AP can transmit by changing the type of antenna it uses, or use multiple APs connected to the same switch or set of switches to solve the problem.

> EXAMPLE
> If the power level or signal is too strong, and it reaches out into the parking area or farther out to other buildings and businesses, place the AP as close as possible to the center of the area it is providing service to.

Don't forget to verify that you've got the latest security features in place to keep intruders from authenticating and using your network.

1e. Latency and Overcapacity

When wireless users complain that the network is slow (latency) or that they are losing their connection to applications during a session, it is usually a capacity or distance issue. Remember, 802.11 is a shared medium, and as more users connect, all user throughput goes down. If this becomes a constant problem, as opposed to the occasional issue where 20 people with laptops gather for a meeting every six months in the conference room, it may be time to consider placing a second AP in the area. When you do this, place the second AP on a different non-overlapping channel from the first and make sure the second AP uses the same SSID as the first. In the 2.4 GHz frequency, the three non-overlapping channels are 1, 6, and 11. Now the traffic can be divided between them, and users will get better performance. It is also worth noting that when clients move away from the AP, the data rate drops until, at some point, it is insufficient to maintain the connection.

1f. Signal Attenuation

Attenuation is signal loss over distance; the further the signal travels, the weaker the signal becomes. For a wireless network spanning large geographical distances, you can install repeaters and reflectors to boost a signal to cover about a mile.

HINT

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

This can be a good thing, but if you don't tightly control signal boosting, you could end up with a much bigger network than you wanted.

To determine exactly how far and wide the signal will travel, make sure you conduct a thorough wireless site survey.

TERM TO KNOW

Attenuation

Signal loss over distance.

1g. Incorrect Antenna Type

Most of the time, the best place to put an AP and/or its antenna is as close to the center of your wireless network as possible. But you can position some antennas a distance from the AP and connect to it with a cable, which is a method used for many outdoor installations. If you want to use multiple APs, you've also got to be a little more sophisticated about deciding where to put them all; you can use third-party tools like the packet sniffers Wireshark and AirMagnet on a laptop to survey the site and establish how far your APs are actually transmitting. You can also hire a consultant to do this for you; there are many companies that specialize in assisting organizations with their wireless networks and the placement of antennas and APs. This is important because poor placement can lead to interference and poor performance, or even no performance at all.

1h. Environmental Factors

KEY CONCEPT

It is vital to understand the environmental factors when designing and deploying your wireless network. Do you have concrete walls, reflective window film, or metal studs in the walls? All of these will cause a degradation of Db or power level and result in connectivity issues.

Reflection is the property of a propagated wave being thrown back from a surface. Reflection occurs when a wave hits a smooth object that is larger than the wave itself and the wave may bounce in another direction. Reflection can be the cause of serious performance problems in a WLAN. As a wave radiates from an antenna, it broadens and disperses. If portions of this wave are reflected, new wave fronts will appear from the reflection points. To correct this problem, reposition the antenna.

If these multiple waves all reach the receiver, the multiple reflected signals cause an effect called multipath. **Multipath** is a wireless propagation phenomenon that results in a signal reaching the receiving antenna by two or more paths, which can degrade the strength and quality of the received signal or even cause data corruption or canceled signals. APs mitigate this behavior by using multiple antennas and constantly sampling the signal to avoid a degraded signal.

TERMS TO KNOW

Reflection

The property of a propagated wave being thrown back from a surface.

Multipath

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

A wireless propagation phenomenon that results in a signal reaching the receiving antenna by two or more paths, which can degrade the strength and quality of the received signal or even cause data corruption or canceled signals.

2. Wireless Network Configuration Mistakes

Common sources of wireless network problems include poorly configured wireless access points or wireless controllers and inconsistencies between the settings on the AP and the client devices. The following sections describe some of the main sources of configuration problems.

2a. Incorrect Encryption/Security-Type Mismatch

Wireless networks typically use encryption to secure their communications, and many different encryption standards may be used for wireless networks, including Wi-Fi Protected Access 3 (WPA3) with Advanced Encryption Standard (AES). To ensure the tightest security, configure your wireless networks with the highest encryption protocol that both the APs and the clients can support.

HINT

It is critical to make sure the AP and its clients are configured with the same type of encryption. This is why it may be a good idea to disable security before troubleshooting client problems, because if the client can connect once you've done that, you know you're dealing with a security configuration error.

2b. Incorrect, Overlapping, or Mismatched Channels

Wireless networks use many different frequencies within the 2.4 GHz or 5 GHz band, and these frequencies are sometimes combined to provide greater bandwidth for the user. Most of the time, 2.4 GHz wireless networks use channel 1, 6, or 11, and because clients auto-configure themselves to any channel the AP is broadcasting on, it's not usually a configuration issue unless someone has forced a client onto an incorrect channel. Also, be sure not to use the same channel on APs within the same area. Overlapping channels cause your signal-to-noise ratio to drop because of increased interference that results in signal loss.

2c. Incorrect Frequency/Incompatibilities

Setting the channel determines the frequency or frequencies that wireless devices will use. But some devices, such as an AP running 802.11g/n, allow you to tweak those settings and choose a specific frequency such as 2.4 GHz or 5 GHz. Running 802.11ax also enables you to use 2.4 GHz or 5 GHz, however, 802.11ac does not. If you do this on one device, you've got to configure the same setting on all the devices that communicate with each other. Incorrect-channel and frequency-setting problems on a client are rare, but if you have multiple APs and they're in close proximity, you may need to check for these issues to make sure they're on different channels/frequencies to avoid potential interference problems.

2d. Wrong Passphrase

When a passphrase is used as an authentication method, users must enter the correct passphrase when authenticating to the AP or to the controller. Access will be denied if an incorrect passphrase is entered. This

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

will have a negative impact on usability.

2e. SSID Mismatch

When a wireless client device comes up, it scans for service set identifiers (SSIDs) in its immediate area. These can be basic service set identifiers (BSSIDs) that identify an individual access point or extended service set identifiers (ESSIDs) that identify a set of APs. In your own WLAN, you clearly want the devices to find the ESSID that you're broadcasting, which isn't usually a problem: Your broadcast is usually closer than the neighbor's, so it should be stronger, and your client devices will connect automatically.

IN CONTEXT

However, this might not be the case if you're in an office building or apartment complex that has lots of different APs assigned to lots of different ESSIDs because they belong to lots of different tenants in the building. Users may experience connectivity issues when a neighbor's ESSID broadcast is stronger than yours is, depending on where the clients are in the building. If a user reports that they're connected to an AP but still can't access the resources they need or authenticate to the network, you should verify that they are, in fact, connected to your ESSID and not your neighbor's. This is a very typical problem in an open security wireless network. You can generally troubleshoot this issue by looking at the information on the device's wireless software icon to see which ESSID the device is connected to. You can easily resolve this problem by making your network's ESSID the preferred network in the wireless client software.

2f. Wireless Standard Mismatch

Wireless networks have many standards that have evolved over time, like 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax. Standards continue to develop that make wireless networks even faster and more powerful. Most wireless devices you buy today are **backward compatible** with previous standards and can be used to communicate with other devices using a number of standards. It is important to make sure the standards of the AP match the standards of the client, or that they're at least backward compatible. In the event of a wireless standard mismatch, you may need to upgrade a client's wireless interface. Be sure to understand the throughput, frequency, distance capabilities, and available channels for each standard you use in your enterprise wireless network.

TERM TO KNOW

Backward Compatible
Capable of interoperating with older systems.

2g. Untested Updates

It is really important to push updates to the APs in your wireless network but not before you test them. Deploying an untested software or firmware update could cause a network outage. Network administrators need to watch for the release of OS or patch updates for the network's APs. The updates need to be tested

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

thoroughly in your test environment before pushing them to your production network to avoid unplanned downtime.

SUMMARY

In this lesson, you learned more about troubleshooting network problems, especially **wireless network issues**. We focused first on wireless network issues, including interference, device saturation and bandwidth saturation, simultaneous wired and wireless connections, distance and signal strength, latency and overcapacity, signal attenuation, incorrect antenna type, and environmental factors. We then learned about common **wireless network configuration mistakes**, including encryption mismatches, mismatched channels, incorrect frequencies, wrong passphrases, SSID mismatches, wireless standard mismatches, and untested updates.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Attenuation
Signal loss over distance.

Backward Compatible
Capable of interoperating with older systems.

Bandwidth Saturation
A condition that occurs when activity on a wireless network exceeds the capacity of the wireless access points, which results in high latency and poor performance.

Device Saturation
Having too many devices connected to a wireless access point, which will result in low bandwidth availability.

Multipath
A wireless propagation phenomenon that results in a signal reaching the receiving antenna by two or more paths, which can degrade the strength and quality of the received signal or even cause data corruption or canceled signals.

Reflection
The property of a propagated wave being thrown back from a surface.

© 2024 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.