Global Knowledge™

Expert Reference Series of White Papers

Wireless Bandwidth – Not Necessarily as Advertised

Wireless Bandwidth – Not Necessarily as Advertised

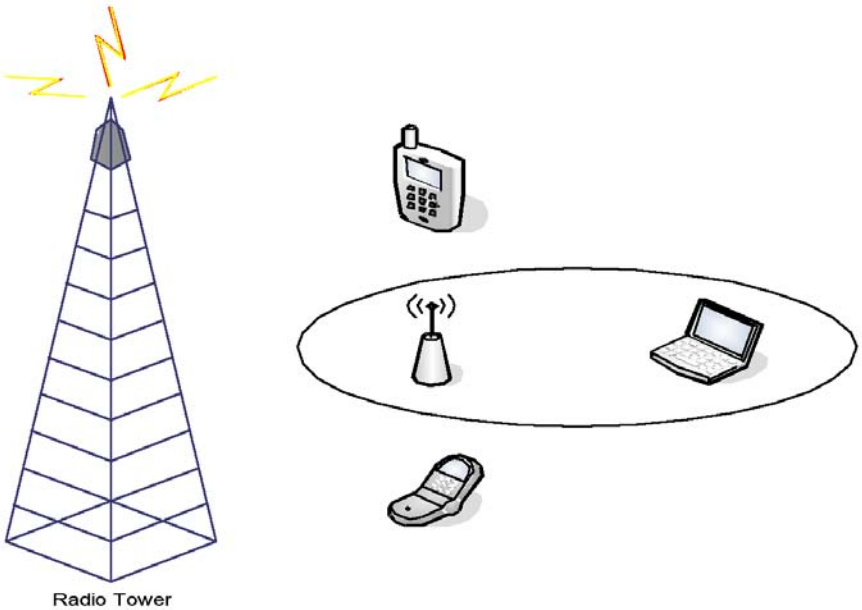
Ted Rohling, Global Knowledge Instructor, CISSP

Introduction

In the maze of wireless networking developments, the one factor often overlooked is the promised throughput capabilities versus the actual bandwidth that is available. Picking up an 802.11g wireless access point and wireless adaptor, you probably expect that you will be getting a bandwidth availability of 54mb-per-second (mbps). Oops. Don't get too upset when you find out that the actual bandwidth you get is substantially lower. In this paper you will learn why the bandwidth you expect disappears into thin air.

It's Radio

The foremost reason for loss of performance is that wireless networking is really radio. Radio is subject to all kinds of radio frequency interference (RFI) issues. If your wireless LAN is operating in an environment with wireless telephones, microwaves, and other devices that emanate radio signals, those emanations will interrupt the communication pathway that you expect. It is very similar to trying to hold a private conversation in a crowded, noisy sports arena. You have to try hard to communicate, and you probably have to slow down when you speak just to be able to hear one another.

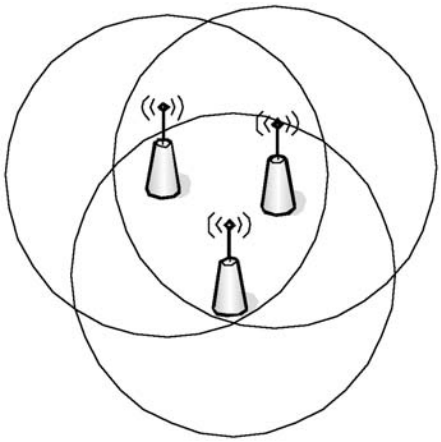


If you are fortunate enough to have an access point and adaptor that are in an area with no RFI and no other interference sources, you will get reasonably good throughput. However, in most business settings today, that

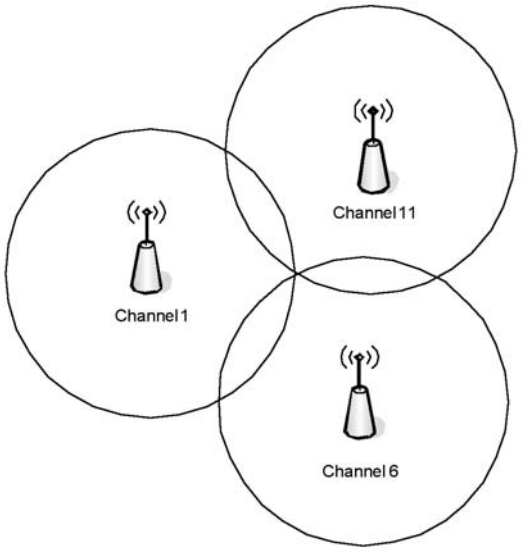
is not common. Wireless networking creates its own interference. Open your wireless adaptor on your computer and count the number of other access points that you can see. Depending on a number of different conditions, each of these access points can cause a reduction in your network performance level.

Sharing the Path

Each access point is assigned to a channel. That channel consists of frequencies in the 2.4ghz range of the radio spectrum. There are 11 different channels available in 802.11b/g wireless networks. That's the good news. The bad news is that the channels are really not all that unique. They overlap. Channel 6 and channel 7 are adjacent. That's much like being in a hotel, trying to watch a movie in peace. You are separated from the next room by a very thin wall. They are watching an exciting basketball game. The noise of the game and the people in the next room drown out your movie. Adjacent channels can block each other resulting in problems similar to RFI.



The designers of the 802.11b/g protocols set aside three channels that do not overlap. Channels 1, 6, and 11 are separated by enough space so that they do not get into each other's way when the access points are properly configured. Assigning adjacent access points to different channels—especially 1, 6, or 11—will help reduce the path-sharing problem.



Like the noisy hotel room, it may also be necessary to limit the power output from the access point so that the "noise" from one access point does not impact your neighbors. Careful study of the locale of the wireless network will help you understand what output levels are acceptable.

Accessing the Path

When the wireless adaptor is read to send information to the wireless access point for transmission to network, a number of steps must occur for the transmission to take place successfully. The 802.11 protocols use a mechanism called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). This is similar to the way that Ethernet works—except for one big difference. With Ethernet, a simultaneous transmission is called a collision. If two devices transmit on an Ethernet segment at the same time, they collide and block each other's transmission. The electrical processes used by Ethernet allow the devices to sense the collision and retry the transmissions. Using switches in wired networks has all but eliminated the problems caused by collisions.

In a wireless network, it is impossible to detect a collision. So how does wireless get around the collision issue? When wireless devices access a network, they "listen" to the radio signals to see how much traffic is being sent. When the sending device senses a period of time with no transmission, it attempts to send waiting data to the receiving device. If the receiving device receives the transmission, it sends an acknowledgement message back to the sending device. If the receiving device does not send an acknowledgement, or if the acknowledgement is blocked for some reason, the original sender retransmits the frame. It assumes that a collision has occurred.

Acknowledgements and Performance

The process of sending frames and receiving acknowledgements is one of the key reasons that expected bandwidth does not match the throughput that actually is available. The transmission of the acknowledgement frame takes up about one-half of the bandwidth of the wireless communication. If you transmit information at 54mbps but have to wait for an acknowledgement for each frame transmitted, the throughput rate falls from 54mbps to 27mbps or less.

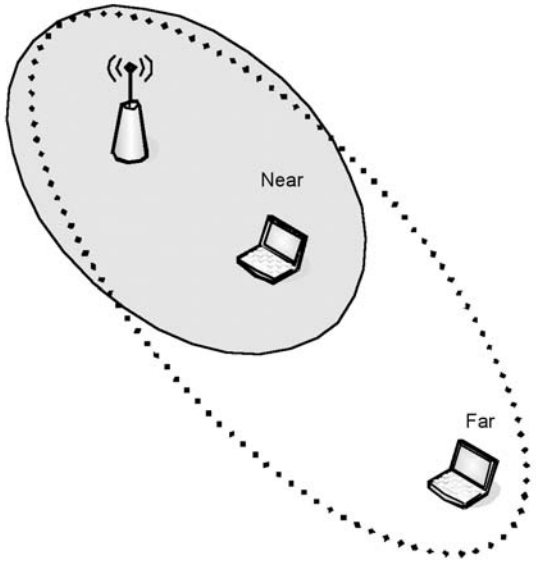
You Have the Path

You have now transmitted a data frame to the access point. That data frame contains your payload and the data you are sending. It also contains control information required by the wireless network.
Just as in Ethernet, the front of each wireless frame contains "header" information. The Ethernet header is 14 characters in length. The 802.11 header combined with a SNMP header is 32 characters, over twice as long as Ethernet. Depending on the size of the payload in each frame, the overhead varies from 42% of the frame down to 2% of the frame. With more frame space taken up with overhead, fewer data bytes are actually transmitted in each frame when compared to Ethernet frames. The overhead of the wireless protocol further reduces the effective bandwidth.

How Far Can You Go

So far, our exploration of wireless access assumes that you have optimal conditions for the access point and the wireless adaptor. They are within a reasonable distance of each other and the signal strength (the level of signal heard by each device) is high. What happens if the wireless adaptor is moved away from the access point?

As the distance between the wireless adaptor and access point increases, the quality of the radio signal degrades. This is called attenuation. Attenuation can be caused by distance and obstructions, such as walls or metal. As the signal degrades, the access point and wireless adaptor will reduce the speed at which they operate. 802.11g will attempt to start at 54mbps and then drop down to 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 and finally to 1mbps trying to find a rate that is satisfactory to both devices.



Distance is also important when considering how the access point might react to two different adaptors. If one adaptor is near to the access point and the second adaptor is far from the access point, a near/far condition occurs. The access point may never hear the "far" adaptor with a weak signal if the "near" adaptor with a strong signal blocks it. Think about two people trying to talk to you. One person has a booming voice and the other person has a tiny voice. Your ability to talk to the person with the tiny voice is limited by the person with the booming voice. The "far" stations are severely penalized by the overwhelming signal of the "near" station.

I'm Fast; Others Are Slow

If you are accessing the wireless network at the optimal data rate, you may still have some issues. If the neighboring stations are operating at a lower data rate, they will have access to the network for a longer period of time, which will slow down your effective data rate. Consider a tollgate on a highway. It takes about the same amount of time for each car or truck to pay the toll. If five large trucks are in front of you, you will take a lot longer to get through the tollgate than if five cars are in front of you. The trucks take more time to go through the tollgate than cars do because they are physically longer.

If you have to wait for a 1518 byte frame to go to the access point at 11mb per second, you wait a lot longer than if that same frame went to the access point at 54mb per second. As a matter of fact, you wait five times longer! If the slower speed devices are sending and receiving lots of data, you have to wait for them to get out of the way before you can send your data.

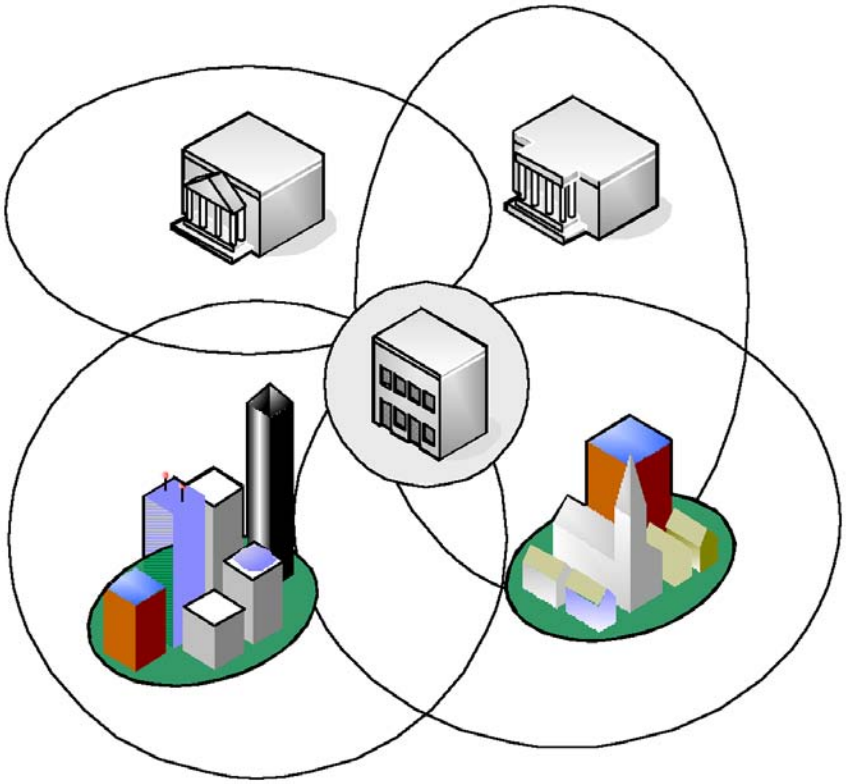
Mixed Signals

You may have heard that mixing 802.11b and 802.11g devices in the same area also slows down the overall throughput of the network. The two standards use different methods of transmitting information. They don't understand each other, so the 802.11g devices will "warn" each other that an 802.11b device is in the area. That warning causes the 802.11g devices to implement a protection scheme, which does indeed slow everything down to nearly the 802.11b data rates.

The Wireless Neighborhood

In the wireless world, we are not alone! A solid networking plan that limits distance, separates channels, and controls the number of devices connecting through an access point may be defeated by a number of factors beyond the designer's control.

Radio works in a horizontal and vertical plane. That is, it goes up and down, and it goes side to side. Most access points use what are called omni-directional antennas. That means the signals do not go in any specific direction; they go in all directions. If your access points send information in all directions, so do all the other access points in your area.



The neighboring access points that defeat your network plan may be beside you in the building, on the same floor. They may be above you or below you. They may be in another building close by. They may be anywhere as long as your wireless adaptors and access points can hear their radio signals.

Securing the Wireless Network

Your next concern will be securing your wireless network. Most security features some type of encryption. Wireless network security can be implemented using Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) or Virtual Private Network- (VPN) based encryption. Performance again slows with the encryption and decryption of the frames transmitted on the network. If the CPU of the workstation performs the encryption, the impact may be substantial. If the wireless interface performs the encryption, there is less of an impact on the workstation, but the wireless traffic is still slowed for the encryption and decryption process to take place. More of the possible bandwidth is eliminated by implementing any type of encryption-based security.

What Does All of This Mean for Performance?

In an ideal state, you will get about 24mb per second from a 54mb per second 802.11g access point and adaptor. This is when the adaptor reports a 54mb per second rate. Increase the distance, and the adaptor slows down. Increase the interference, and your transmissions are blocked and must be retransmitted. Add more devices on the same channel or adjacent channel, and more confusion occurs on the wireless LAN. Add encryption, and you slow down more. It seems that the more we look at the issue, the slower we go.

Conclusion

On the surface, wireless networking appears to be a very simple case of connecting an access point to a wired network, installing a few wireless adaptors, and sending and receiving information. And, of course, you will need to consider the security of your network.

But realistically, the performance of your wireless network is far more complex. As we have seen, there are many factors that negatively impact the actual bandwidth you have available for use. Many other issues impact how your wireless network will perform.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:
Wireless Networking I: Integration and Troubleshooting
Wireless Networking II: Security and Analysis

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Ted Rohling has been a contract instructor with Global Knowledge since 1995, teaching in networking and security, and focusing on TCP/IP, networking fundamentals, and CISSP preparation. He has over 40 years of

experience in information technology, telecommunications, and security. He currently holds the CISSP certification and has previously held various certifications from Nortel, Cisco, and Microsoft. His educational background includes a BBA in Management Science, an MA in Information and Computer Management, and an MS in Educational Human Resource Development.

References

http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html