

“Tech Talk” Transcript

“Wireless Connections” Episode

A man enters a room where a computer seen from the back with many wires, cables and cords coming out of it sitting on a table. The man sits at the table and can barely see around it. His feet get tangled in the cords. The text, “That was then” appears on the screen.

Fade to black.

A younger man is in the same room at the same table looking at a laptop with no wires or cords at all. The text, “This is now” appears on the screen.

Tech Talk intro plays.

Susan: Hello and welcome to Tech Talk from the University of Minnesota, your source of information about the technology that surrounds us everyday. I’m your host, Susan McKinnell. For many of us, when using our computers we’re often restrained as to where we use it because of all those nasty cables that tether us to our internet connection or our printer or any other device. Now computers can be liberated from all those cables. There’s a term for this freedom of movement; we call it “wireless,” and that’s what we’ll be talking about today. Some of the terms you’ll hear include: WEP, access point, Wi-Fi, and bluetooth. Someone who knows a lot about wireless is Daniel Westacott, a juggler, a chef, a plant biologist and for the past nearly twenty years, an indispensable part of the university’s networking and telecommunications services, however, his focus for the past ten years has been wireless. Thank you for being with us today, Daniel.

Daniel: Well, thank you. It’s a pleasure to be here.

Susan: Can you tell me, first off, what exactly are we talking about when we talk about computers and wireless?

Daniel: Well, Most of the time you will be talking about a way to connect your computer to another network source; the internet, perhaps a server in your home or something like that.

Susan: Okay. Connecting to the internet...connecting to the rest of the world somehow.

Daniel: Yes.

Susan: Without wires?

Daniel: Without wires at all just like this laptop here.

Susan: You've got a laptop here and this one is hooked up for wireless, so...and it also doesn't have any power cords right now because it's got its battery charged. Wireless is not referring to that at all.

Daniel: No.

Susan: Okay; just connecting to other computers. Why would you want to use wireless?

Daniel: Well, it's very convenient. I remember accidently tripping over a cord and dragging a laptop and watching it crash on the floor before.

Susan: Oo. That's a little painful.

Daniel: It is. It's often very convenient for that sort of thing; a machine that you want to use in multiple locations and don't want to drag a bunch of cords around.

Susan: So it's beautiful for laptops.

Daniel: Oh, certainly.

Susan: And maybe not used as much for desktops because those aren't not portable anyway.

Daniel: That's correct. I mean sometimes you'll see that people will actually wireless-connect their printers because they want them far away, like in the basement because they're large.

Susan: Okay. Okay. That makes a lot of sense. When you're working with wireless are there actually disadvantages to actually having a wired connection?

Daniel: Well, sure, because it works over radio it broadcasts so it's a little bit slower than most wired connections, it can be interfered with.

Susan: You say it works over radio, so when we are talking about wireless, it's really kind of the same thing when you think about being wireless back in the 40's or 30's; it's radio waves.

Daniel: Oh exactly. It's radio waves at 2.4 gigahertz frequency and away it goes.

Susan: Okay. But it's a little slower than a wired connection.

Daniel: Yes. And because of the nature of how it's designed, it's a very open, shared media; so that if you have three machines using wireless, you cut the speed down by a third.

Susan: So they have to share it out between all three?

Daniel: Yes. So for a whole bunch of people in one place it's not very convenient; although, if it's usually just you and your laptop, it's amazingly convenient.

Susan: Okay. Isn't there also some sharing that happens over wired connections?

Daniel: Oh, sure. If you were to put a wire on this laptop you could share this with your...share out your hard drive with another thing, those sorts of things.

Susan: But do you have...are you guaranteed that bandwidth because of that wire, or...

Daniel: Yes. If you use something called a switch which is almost everything available now, you will get the amount of bandwidth that you have at the maximum speed.

Susan: Okay. Okay. So, when you've got the wire you are guaranteed a certain amount but when you've got the wireless, you're sharing out whatever that amount is.

Daniel: Yes.

Susan: So there are certain things that you may not want to do over wireless because of that?

Daniel: Well, sure. I would think that if you were trying to video...edit a video or perhaps manipulate pictures that are large...I mean you want to think of it sort of as a fast dial-up, so when you want to use something that you'd find inconvenient to do over a dial-up connection, you probably will enjoy it less. So, the wireless is good for things that are not bandwidth intensive, that aren't large in space.

Susan: And when you say dial-up, we're talking about a 56k modem which goes over the telephone line.

Daniel: You betcha.

Susan: As opposed to a DSL or cable connection.

Daniel: Yes.

Susan: So, wireless is typically slower than a DSL or cable connection?

Daniel: It's usually about the same speed, sometimes a little faster, sometimes a little slower.

Susan: Okay.

Daniel: Wireless is usually starting at 11 megabits these days and most cable is a little slower than that.

Susan: Okay. Now, are there different types of wireless?

Daniel: Oh, yes indeed. There is 802.11b...

Susan: Mm. Hmm.

Daniel: It's kind of an alphabet soup.

Susan: (laughs)

Daniel: And that is the one that you see most commonly. It's very inexpensive. There is an enhancement to 802.11b called 802.11g which is four times faster.

Susan: Okay.

Daniel: And there are also vendor-specific enhancements to those sorts of things so if you stay in one product line, they sometimes will give you some extra stuff. And then there is also something called 802.11a which is a little older. It's very quick but it doesn't pass through walls very well so most people don't use it.

Susan: Okay, so now if you have to go and look at this stuff, you can remember that g, being later in the alphabet, is newer.

Daniel: That's correct.

Susan: Okay, and a, that's probably one you want to steer away from because it's earlier.

Daniel: Yes and b is maybe okay, but if you were shopping, maybe the g would be the best choice.

Susan: Okay. Are there any other types used in the world today or are all these 802.11; that's the standardized...

Daniel: Well, that standard came out of the IEEE exchange of standards committee and so that is used in most places; Japan, the frequencies vary slightly, but that's pretty much where you see it world-wide.

Susan: Okay. So if you want to use wireless; you've got a laptop, you want to use wireless somewhere, you need to get a wireless card,

Daniel: Yes.

Susan: And this is where this number comes in, you need to get a wireless card that is 802.11 a, b or g,

Daniel: Probably g...

Susan: Okay, most likely g and once you have that, where in the world are you going to use wireless? Where can you find places to use it?

Daniel: Well, sometimes you could put a wireless access point in your home. You could go to coffee shops and like at the airport. Many places provide this service that you can get an internet connection when you are waiting for a plane or you're trying to kill a little time.

Susan: This is a big issue for travelers, particularly business travelers, I would think.

Daniel: Oh certainly. In fact being able to sit in a coffee shop and, you know, eat a doughnut and get some business done, I could see that being very useful.

Susan: I've got the wireless card in my computer, I go to the coffee shop; do I need to pay for this service?

Daniel: Usually you do. There are several services around, one is called Boingo, you would bring it up and you would connect to their location.

Susan: Boingo, B-O-I-N-G-O?

Daniel: Yep.

Susan: And then I've heard of another one, I think it's called Surf Watch?

Daniel: Yes. SurfWatch. And there... as soon as you open a web connection, it will intercept you and it will either take a credit card or it will want to know your account information and then you basically can surf the web and check your email or do those sorts of things.

Susan: So, I could go to the coffee shop, open up internet explorer or Mozilla or Netscape and it would immediately ask me for my credit card, do I need to sign up with Boingo first, or...

Daniel: You can sign up first, or you can sign up on the spot.

Susan: Okay. Depending on...with both of these; Boingo and Surf Watch?

Daniel: Yes.

Susan: So like signing up beforehand with Boingo or Surf Watch do they have like monthly fees if I use that?

Daniel: Yes, they often sell it by the incident so you can use it for, you know, a few hours or you could sign up for months at a time which is usually the most economical.

Susan: If I'm using it all the time all over the place, I probably would want to sign up for some sort of monthly or so forth. Now, Surf Watch and Boingo, that's not something I would use in my own home, though. Is that correct?

Daniel: Oh. No. You would simply purchase, which I think Pete will be talking to us about in a little while...

Susan: In a few minutes, yeah, more specifics on that.

Daniel: You can purchase a device called a wireless access point which you could connect to your home network or to your DSL line and use that to wirelessly connect.

Susan: Now you did mention that sometimes you don't need to pay for wireless if you're going around to coffee shops or hotels or...

Daniel: Oh yeah. Many of the hotels I've stayed in and there are coffee shops that you look at it as a free customer service sort of a thing, so you would allow yourself to get free access and it's very convenient it saves on those long distance calls.

Susan: Absolutely. And that's just something that you have to shop around for in order to find places that do that.

Daniel: Yes. In fact I know people who will actually check the hotel to see if they have free access.

Susan: And that's one of the reasons whether they're going to go with that one or not. I did want to ask about; typically you wouldn't actually use the wireless on the actual airplane flying?

Daniel: That is absolutely correct. I believe that they would have...it's like a cell phone. They would find interference and you should not if you can possibly avoid it; do something like that.

Susan: You'd be using it just on the ground and in the airport itself. So, you wouldn't be able to connect to the internet, necessarily, while you're on a flight.

Daniel: No. The range of these is about 350-400 feet on best day, unless you are doing interesting things with antennas, so...

Susan: (laughs) Which you probably wouldn't be doing while you were flying anyway.

Daniel: No. I don't think so and so I think you would be far away from hopefully anything that you'd be talking to.

Susan: Okay. Wireless; is it secure?

Daniel: It can be but you should certainly take precautions to prepare yourself; there are passwords to set, and encryption standards to use to make yourself as secure as possible.

Susan: But if you just take it out of the box you...if you haven't done anything like that then you don't have security yet.

Daniel: That's right and in fact almost everything that's sold is made so it's easy to use and so you can take it out of the box and it will just work and that can get you into some trouble later perhaps.

Susan: Okay. Great. Thanks you very much for being here with us today, Daniel.

Daniel: You are certainly welcome.

Susan: This issue of security should be important to everyone using wireless technology, but often it is overlooked. Ever hear of something called "war driving?"

Blake Krone, University of Minnesota student, war driver: When you are driving down the street looking for access points it's called "war driving." It has nothing to do with war or anything illegal, it's just a simple act of collecting statistical information about access points; where they exist and then we study the trends later or put it into these mapping programs.

The map is a log of all of the networks that I've found throughout my various drivings. And what we'll do with that map is study the trends and see what type of neighborhoods wireless is being put into, how secure is wireless; are people using the default settings or are they actually taking the time to secure their network.

Not many of these networks are actually secure. All the ones with the padlock mean they are secured and all the ones that don't have a padlock are not secure. Then you can also see how many people leave the default; anytime you see one called "link sys" or "default," those are standard network. Those are somebody just plugged it in out of the box and didn't bother setting up any of the security or changing any of the default settings.

It's not bad that all of these networks are popping up. What's happening right now is we're just noticing all these beacons that the access points send out and just showing the list of seeing where they are. With an access point it broadcasts its existence like a radio beacon. It's just like a radio station, you tune to a radio station, we have the same concept

here with wireless networking. It transmits its information and then this application will just pick up its existence.

Anybody that goes down to the store and buys a wireless networking card for either their desktop or laptop will be able to see these networks. Anyone who installs a wireless access point needs to worry about security, whether you're a home user or a business.

Susan: All those pinging sounds that you heard were the war driver's sensors picking up unsecured home wireless transmitters. Pete Oberg knows a lot about wireless and how to make it secure; he's been with the University's Academic and Distributed Computing Services for more than twenty years, working with main frames and micro computers, software and hardware technologies and right now he is up to his neck installing wireless throughout the university. Thank you for being here, Pete.

Pete: Thank you. Glad to be here.

Susan: First of all why do you need to secure your home wireless network?

Pete: Right. Just like the laptop that is in front of us here, if your wireless access point that was searched out from the application, people would have access to your hard drive if you had file sharing turned on. So they could go in, they could look at the files on your hard drive, maybe you've made purchases online and then they have access to credit card information if you actually save that information. Then all of a sudden there you would have identity theft.

Susan: And a lot of people do have a lot of important information about themselves that they keep on their home computers.

Pete: That's correct; social security numbers.

Susan: Mm. Hmm. So securing that home connection is very, vitally important.

Pete: Vitally. Yes. I agree.

Susan: Let's start out first of all with how to get that wireless connection at home.

Pete: Okay. So the units that people use are in front of us here.

Susan: Okay.

Pete: So you open it right out of the box, it is usable, but unprotected.

Susan: Okay.

Pete: And the two ways...and the main protection that people should use is to set what's called in the application, a menu called WEP; Wired Equivalency Privacy.

Susan: W-E-P

Pete: W-E-P. And what you do is you set a password on that so anyone who gains access; it prompts him on his screen for a password. If you don't know it; you don't get in.

Susan: So that immediately keeps people out. Okay so that's one simple way to secure your home wireless network. In order to set up a wireless network at home, do you need to purchase one of these base stations?

Pete: Base stations—another name for an access point.

Susan: Okay. And we have a couple of different models here, what do we have?

Pete: Right. So there are the three out in front of us, there is a product from the Apple manufacturers and it's called the AirPort, the second is a Linksys model and the last one is a Cisco access point from the Cisco manufacturing people and the main difference between the three is these two are what we call home/small office model and the last one is an enterprise type. There are differences in price because they offer more things; more "bells and whistles" is how we often describe it, to accomplish various things at your place. So for our audience out there today these two are probably what you will be looking at because the price range is from \$75 to \$199.

Susan: Okay. Okay. And so you purchase the base station for your home; what else would you need to get that wireless connection working?

Pete: So then what the individuals using it in the home [need] is a wireless card like this one we have here on the laptop. They do come in two types; there is an external card that slides in and the most recent purchase that people make; there is also one that can be buried under the keyboard and then the little antenna goes around the screen to improve reception.

Susan: Okay. And so the one that is buried under the keyboard, is that the one that you purchase the wireless already installed in the computer?

Pete: Correct.

Susan: Okay. So your computer; your laptop or your desktop have to have that wireless card somehow in it and you'd have to have the access point, but you'd also have to have some way to connect to the internet in the first place, right?

Pete: That is correct. And for each one of these models; the enterprise type here that we have connects only to an ethernet, DSL or cable connection; these two models here can use either your phone connection or DSL or cable.

Susan: I think I'm going to turn these around for a moment to show that we do have the connections on the back here for all sorts of different connections. So you would have to have an internet service provider.

Pete: That is correct.

Susan: And that internet service provider, through that, you could have the service either DSL or cable or a telephone modem and you'd hook that up to your wireless and you could... Could you take your laptop anywhere in your house then?

Pete: And so then in most houses the answer is yes. The radio frequencies will move through sheet rock walls that most people have. Some people do have cement, you know separating one floor from another and if there happens to be rebar in that flooring, that certainly can dampen the signal and maybe cause loss of signal depending upon the distance.

Susan: Since we're talking about radio waves, they can move through [every]thing.

Pete: Dan alluded to in the front part of the program you can get between 300 and 400 feet in line of sight; when you can see it. But as soon as you get material in between it all of a sudden it gets blocked.

Susan: Okay, what about bookshelves that are loaded with books?

Pete: Right. So books absorb radio frequency, people absorb radio frequency in your back yard if you go out there, leaves, you know, in the summer time because there is moisture in that absorbs radio frequency.

Susan: And the tree itself is going to absorb a whole lot.

Pete: Correct.

Susan: So you want to be very careful about where you put this up in order to get the best use out of it.

Pete: That's very true.

Susan: Is it a good idea to maybe experiment a little bit?

Pete: You certainly can use your phone cable, what we call the R.J. 45 cable and depending on what its length is, certainly you can move it or depending on jacks in various rooms.

Susan: Yeah. So in other words, the hub itself does have to be physically connected to something and so wherever you...yeah. Some thought needs to go into it before you even

get that connection put up. Okay. Now as far as...there are these models for hubs and I've been calling them "hubs," "access points"...

Pete: Also this is called a wireless router so it has some extra connections on it, to plug extra things in it like printers, if that is being driven wirelessly so it all depends and for our audience out there how much money you want to spend. So maybe the next part is, we have a website here at what's called cnet.com where you can go if you are going to purchase one of these models where you can a little homework in advance, you know deciding how much money you can afford for this and the various features that you want.

Susan: Yeah. As with any sort of technological item you want to purchase, you always want to do some research and it seems like it's a wonderful resource for any of that. As you can see we've got options right here Wi-Fi, now Wi-Fi is a term that I want to get to too, one that I've heard floated around, what exactly is Wi-Fi?

Pete: Wi-Fi means wide fidelity and again as Dan alluded to in the earlier part, it just a basic radio frequency of signals out from one unit and another receiving and sending information back. In this case websites get information that you're interested in.

Susan: So when people say Wi-Fi, they're talking about wireless?

Pete: Right.

Susan: Okay, great. And as we can see on seeing it there is lots of information about different units.

Pete: Correct.

Susan: Okay, great. And there are lots of different companies that put out these products, is that correct?

Pete: That is correct.

Susan: How much does cost equal quality?

Pete: Okay and then specifically, Apple tends to be a little higher because they are a world by themselves apart from Windows-type people. And the less expensive of these three is the Linksys in this case. But the main difference of all three models is this; they're driven with power to broadcast; some further than others. So that is another basic feature, besides they all will do WEP, others will broadcast further than others if you are not using antennas which also is an option.

Susan: Okay.

Pete: So again, if you are working with wireless, I'll say, also like buying stereo equipment, how much do you like to play when you are doing this stuff? And so that

things that you read about in manuals; do you like doing that sort of thing? If you get more and more complicated or adding more features and what you're trying to do at home.

Susan: So, if you want to go with the simple, the basic, you want to find a unit that just does the wireless and it just has a very simple connection for you.

Pete: Right.

Susan: No matter what unit you purchase it'll have the option to do the WEP; the security.

Pete: Right.

Susan: But then when you are purchasing you need to see how far it goes to see if it will meet your needs in your house. If you're just living in an apartment you may not need to go very far.

Pete: Right.

Susan: Okay.

Pete: Another feature, just so that we don't forget, is that some do have antennas like this model here which is the less expensive of the kind, you can knock down the signal strength so that your neighbors as well, might not see it as far, but you also have to worry about interference in your house, and Dan alluded to that earlier.

Susan: Absolutley.

Pete: So the three main big ones, I would think in most homes are a portable phone, running at that same 2.4GHz range, baby monitors, and microwave ovens.

Susan: Microwaves?!

Pete: Right. If it's in between, you may see your signal stall for a moment or however long that microwave might be on and then come back after food or whatever it is that's been heated up.

Susan: So any of those items you might be using might interfere with the wireless signal. And so you might have a problem surfing the web wirelessly until you've got your baby monitor turned off. Okay. What about cell phones.

Pete: And cell phones as...No. They're at a different frequency.

Susan: Okay. So it's just the cordless?

Pete: The cordless, portable phone.

Susan: Okay, so purchasing; you need to purchase this equipment to get wireless to work. Do you need to...How do you know your own computer is going to work well with wireless? Do people need to upgrade in order to go out and really get wireless working well?

Pete: The main feature is that most recent laptops run a little faster so as its processing information the whole bottleneck won't be the computer itself. And so if you have something, I'll say less than 500 megahertz for a processor speed you may find some slowness and we did talk about laptops; you can also buy adapters for desktop computers as well that would slide in the backside and you could also have wireless access.

Susan: To get all of the computers in your house, wireless. So, so it may just be a speed issue with your computer, whether you need to get a new one or not. But typically that is not the issue; you just need to get a card if you don't have it currently. And that should be all the hardware you need; is the card, the computer and the hub as long as you're connected. Oh! One other thing that I did want to talk about when we are talking about wireless; I see all these wireless peripherals these days; wireless mice, wireless keyboards, but that's not the same wireless that we're talking about.

Pete: It's a little different technology called, "Bluetooth." And Bluetooth is also a wireless card, but the broadcast only goes, instead of like these models out here—300 feet max on a good day—it only goes 30 feet so that everything is in a close proximity to the unit that's using it so that you can maybe go to your printer, you can use your keyboard or the portable mouse.

Susan: And that's really nice not to have those cables all over the place. Does that cause an interference with wireless going to the internet?

Pete: No. It does not.

Susan: It should work together fine?

Pete: It should work together fine.

Susan: Okay. So but those are two kind of different issues and what we've been talking about today is the wireless access to the internet. Bluetooth is the one...

Pete: More individual space.

Susan: Great. Well, thank you so much for being here with us today, Pete.

Pete: Thank you for inviting me.

Susan: Well, that's our show on wireless. We've covered a lot of important points some of which we've selected, For Your Files.

Dan Westacott explained why wireless is a bit slower than wired connections.

Dan: ...because of the nature of how it's designed, it's a very open, shared media; so that if you have three machines using wireless, you cut the speed down by a third... So for a whole bunch of people in one place it's not very convenient; although, if it's usually just you and your laptop, it's amazingly convenient.

Susan: Bottom line is, Dan said you might not want to download large files with your wireless.

Dan: The wireless is good for things that are not bandwidth intensive, that aren't large in space.

Susan: Pete Oberg talked about wireless security; protecting your data, not allowing anyone access to your computer via your wireless connection.

Pete: the main protection that people should use is to set what's called in the application, a menu called WEP; Wired Equivalency Privacy.

Susan: W-E-P

Pete: W-E-P. And what you do is you set a password on that so anyone who gains access, it prompts him on his screen for a password. If you don't know it; you don't get in.

Susan: Pete Oberg discussed the ability of the wireless signal to extend throughout your home.

Pete: The radio frequencies will move through sheet rock walls that most people have. Some people do have cement, you know separating one floor from another and if there happens to be rebar in that flooring, that certainly can dampen the signal and maybe cause loss of signal depending upon the distance.

Susan: Pete also said it's not just the building structure that you have to consider when installing wireless.

Pete: but you also have to worry about interference in your house...the three main big ones, I would think in most homes are a portable phone running at that same 2.4GHz range, baby monitors, and microwave ovens.

Susan: If you missed any portion of our wireless program or want to see it all again, stop by our website. All of the programs we've done so far, including this one are right there for you viewing. Our address is techtalk.umn.edu. And if you have a question about wireless just post it on our website and we will have one of our specialists answer it. Next

week we're focusing on viruses. A lot has changed since last we discussed them. We'll bring you up to date on all of it. We'll even take you to a computer lab where specialists run the viruses in a controlled space to see exactly what they will do if they get into your computer. Thanks for watching. I'm Susan McKinnell.

Tech Talk is produced by Academic & Distributed Computing Services and the Digital Media Center, Office of Information Technology in cooperation with University Relations, University of Minnesota

Exexutive Producer

Robert H. Bruininks

Special Thanks to:

Steve Cawley

Sandra Gardebring

Shih-Pau Yen

Host

Susan McKinnell

Producer / Director

Susan J. Tade

Assistant Director

Richard Reardon

Associate Producer

J.B. Eckert

Technical Director

Steve Barbo

Audio

Laura Cervin

Floor Director

Dan Sagisser

Cameras

Pete Gorton

Jonathan Kranzler

David Lindeman

Lighting

Laura Cervin

Jonathan Kranzler

Set Design

Richard Stachow

Field Producers

Dan Sagisser

Field Shooting

Pete Gorton

Graphic Design

Nicky Torkzadeh

Effects Design

Paul Pecilunas

Make-Up / Prompter

Mary Flaa

Ms. McKinnell's wardrobe provided by

Herbergers

Web Development Team

Christina Goodland

Lance Cunningham

Ann Valenty

Thanks to:

CLA Studio B

NASA

Radio K

Bakken Library & Museum

KSTP Meteorology Department

Pavek Museum of Broadcasting

Antique Telephone Collectors Association

© 2004 University of Minnesota

