



Wireless

An animation is shown where the peripheral components for a computer are attached by wires and then the wires disappear.

Susan: Hello and welcome to Tech Talk from the University of Minnesota; your source of information about the technology that surrounds us every day. I'm your host, Susan McKinnell. Wireless technology; it's not just cordless phones anymore. Now we have cordless computer mice, wireless earpieces for our cell phones and our computers are connecting to the internet through the airwaves. On today's show we'll discuss this technology and how it's being used on both small and large scales. Some of the terms you'll hear include: blue tooth, discoverable and virtual private network. With me today is Dr. Ramesh Harjani. Ramesh is with the department of electrical and computer engineering here at the University of Minnesota. He received his PhD from Carnegie-Melon University and has been a technology advisor to companies such as Rocket Ships, Rosemount, and Data Sciences International. He was also a co-founder of Bermai Incorporated, a Minnesota start-up company that developed chips for wireless applications. Thank you for being here with me.

Ramesh: My pleasure.

Susan: First of all, what is wireless?

Ramesh: Wireless is being able to connect between things without wires.

Susan: Mm. Hmm.

Ramesh: That is effectively wireless.

Susan: Basically, we have different things connecting but there is nothing in between. How does this technology work?

Ramesh: It uses electromagnetic waves and they propagate through air or even space. Light is a form of electromagnetic wave that you can see and the lower frequencies are the radio waves that we end up using for the connections that we use.

Susan: So the wireless that we are using with our computers and so forth are really using radio waves.

Ramesh: Yes, exactly.

Susan: So just like we get our stuff from...just like the old wireless...the radio.

Ramesh: Yes!

Susan: The new wireless are our computers and other things. I understand there are different kinds of wireless depending on how far your...

Ramesh: Network connection

Susan: Network connection is. So can you tell me a little bit about these different distances?

Ramesh: Sure. We classify them in terms of how far they reach. We have what its called a “personal area network” and you can think about it as being something that you can reach out 10-15 feet around your person. Then you have what is called a “local area network” local being...think of it as your house.

Susan: Mm. Hmm. Okay.

Ramesh: And then you have what is called a “metro area network” or a MAN, so it covers a city and then you have WAN which covers the entire country or across the world.

Susan: Wide Area?

Ramesh: Wide Area Network.

Susan: Now I notice we’ve got abbreviations for all of these, there is WAN for Wide Area...

Ramesh: MAN for Metro Area, LAN for Local area and PAN for personal area.

Susan: that shouldn’t be that hard to remember. You’ve got a great diagram here. Can we take a look at that real quick?

Ramesh: Absolutely.

Susan: And it illustrates those different distances.

Ramesh: So.

Susan: Okay, now a Personal Area Network, is that something that you’d be able to set up...it would be something you’d be able to set up for your own devices.

Ramesh: Absolutely.

Susan: I understand that...I’ve heard the word Bluetooth.

Ramesh: Mm. Hmm.

Susan: And is that mainly what’s being used for personal area networks these days?

Ramesh: In general, Bluetooth is the primary mechanism currently. There are things in the future that are coming but the idea, again, are things that will replace wires that connect your computer or connect your phone or connect your camera.

Susan: So we're not just talking computer to computer, we're talking other devices as well. What's the story behind the Bluetooth word?

Ramesh: Bluetooth started off with a Danish king who used to have a lot of blueberries and he used to have a blue tooth. And he was someone who put together the Norwegian countries and Bluetooth started off from the company Erickson that makes cell phones and they wanted the standard that a lot of people would merge to and that's kind of where the terminology comes from.

Susan: So getting everyone together and it was a King.

Ramesh: Exactly.

Susan: Bluetooth.

Ramesh: Bluetooth.

Susan: Who ate all the blueberries. Thank you so much Ramesh.

Ramesh: My pleasure.

Susan: I've got a few more questions for you, but first, I'd like to talk with Daniel Westacott about how this technology is being used today. Daniel grew up in Dinkytown and attended the University of Minnesota studying plant biology, theater and computer science. He's been an engineer at the U's networking and telecommunications unit since the mid 1980's. He first worked with wireless technologies in the mid 1990's at trade shows. Thank you for being here with us again, Dan.

Dan: It is pleasant to be here.

Susan: What sort of ranges to folks get on Bluetooth devices?

Dan: It is a very mixed thing. Most people would like a little bit more than they get.

Susan: Don't we always?

Dan: Much depends on your local conditions. When everything is going well you can get thirty feet.

Susan: Okay.

Dan: But, you know, if you have something in the way or interference of course you can get significantly less.

Susan: So Bluetooth, again, being for PAN. A personal internet is something that is going to be really pretty localized.

Dan: Yes, indeed.

Susan: Okay. We have some things here that I think we would use with Bluetooth. Some wireless mice, what other devices do people use with bluetooth?

Dan: Oh, people use keyboards, wireless keyboards that use Bluetooth. A bunch of the technologies done actually on phones and related devices...and accessories for phones.

Susan: What do we have here?

Dan: Yeah, we have this small phone here and it makes its connection to a headset.

Susan: Can I take a look at this here? It's just a little, tiny headset.

Dan: And it just makes the connection. I mean if you remember back in the days when you had to plug in a little cable and run it through your coat and hang it on your...and now it's just...

Susan: Or heaven forbid, actually take your phone out and open it up.

Dan: That's right.

Susan: So this is why I keep on seeing people walking down the sidewalk talking to themselves. They're actually...

Dan: Talking on the phone.

Susan: Fabulous. And I presume there is a little button, here, for the phone? If the phone rings?

Dan: You push the button to answer and then there is a little volume control to go up and down.

Susan: Absolutely. And what a neat, spiffy thing! Your phone is in your pocket, this is on your ear, it's definitely under 30 feet.

Dan: Indeed.

Susan: It works fine. I've heard about people having their cell phone numbers stolen and so forth. Are there security issues with...

Dan: There certainly are. With any technology you should look at the manual and there is usually a code you can set on the box. In the case of this phone there is an option called, "Do not broadcast your I.D." You could also set something to make it so it's listed as non discoverable.

Susan: Non discoverable; okay. Now you say, "look at the manual" I think that most of us get a new device we want to start playing with it. Very few of us actually look at the manual, but this is really something we should be doing for our security.

Dan: I think in today's world, I think it's important to take a little extra time and do the right thing and set your settings so it makes it a little more secure.

Susan: Is security an issue with all Bluetooth devices?

Dan: The protocol is designed to be open and useful and friendly and so that probably means there are some things that you probably want to tighten down, depending on your use of the device and where you...what your needs are.

Susan: So, unless you read the manual and actually go in and make some settings, your Bluetooth is open. Even though 30 feet is not a very far range you still might have issues with people...

Dan: You might. You know if you were on a bus or a train with someone for a long time so they could sit down and play around a little bit, those things do happen.

Susan: Okay. And is that with people getting information from you mainly, or is sending stuff, or...

Dan: Usually it's somebody sending a little message. It is possible that someone could use your data connection on your phone to make an up/on connection. So there are things that you're going to want to shore up a little.

Susan: Now you said that you want to make your Bluetooth non discoverable. We've got a laptop here that has Bluetooth; can we look at that setting on the laptop?

Dan: Oh, we sure can.

Susan: Let's see. It look like we're up and running so...

Dan: So we would go to systems preferences.

Susan: This is a Macintosh computer; it would be slightly different on your Windows machine.

Dan: Yeah, but it would be in the Control Panel part in the Bluetooth and you would bring open your connection and in the case of the Macintosh it's a checkbox for "discoverable" and another good feature might be to require authentication.

Susan: These are really simple settings to deal with, it looks like.

Dan: Oh! It's very easy; one of those things [like] locking the door before you go out.

Susan: It just takes a turn of the key and that's all you need to do.

Dan: Indeed.

Susan: Okay so, again, if the computer has Bluetooth then you might want to connect it to the laptop to the keyboard or to the mouse or some other devices. You'd want to set the discoverable or take away the discoverable setting on the laptop but also for other devices that you are using as well. Like a cell phone and so forth.

Dan: Or if you're running a soft phone you might want to do that for your little earpiece.

Susan: Okay. I've heard about people using Bluetooth in cars. What's that for?

Dan: Oh! There was a project that some people made this thing called the car whisperer and the idea was that the person kind of wanted to be able to play a message or listen in on cars going by. And so they built some antennas and they wrote some software that if the settings on your devices aren't set or they're set from factory to like one, two, three, four this box will guess that and you will be able to send a little message to the car next to you.

Susan: Now, send a message in your car, what is the Bluetooth in the car being used for?

Dan: Usually for a hands-free cell phone.

Susan: So, the same kind of thing we've got with the phone here.

Dan: Yes.

Susan: Mm. Hmm. and presumably higher safety that you're not actually playing around with the phone itself while you're in the car.

Dan: Yeah.

Susan: Great. Now this, the Bluetooth stuff, is all, again, for the Personal Area Network. Oh and I did want to point out this laptop has Bluetooth built in but if you get a computer that doesn't have Bluetooth built in but you want to use devices with your computer we have a couple nifty things here. What are these little guys right here?

Dan: Well, those are USB devices the white one is actually an 802-11-B so that is for the Local Area Network wireless.

Susan: Okay so these are two separate things.

Dan: And the smaller gray one is a Bluetooth adapter.

Susan: So, this one would be for the...they both look like thumb drives to me.

Dan: Oh, yeah.

Susan: So we've got a lot of devices that are looking very similar to these these days. You want to be careful, I suppose, at the computer store that you are buying what you want to get.

Dan: Indeed.

Susan: So the little guy is for the Personal Area Network. And this white guy is for the Local Area Network.

Dan: Yep.

Susan: A little bit about Local Area Networks; what's going on with that?

Dan: Well, the devices are going faster. There is something called 802-11-G now which is...has a bandwidth about four times faster than the old. The access points are becoming smaller and more user-

friendly. And there has also become more of a need for people to set some security settings on those. Sometimes if you're getting a lot of performance issues people want to change their channels.

Susan: Okay, when we're talking about Local Area Network we're obviously at this point, not talking about our phones so much because that's not something that we would use across the distance of the house—mainly computers.

Dan: Mainly computers. Some people will run music over that now.

Susan: Okay.

Dan: There are small devices that basically will plug into your home stereo and listen to your connection from your computer.

Susan: What sort of hardware do we need for this? This would be a little item that you'd connect to your computer.

Dan: Yes. So, if your computer did not have wireless built in or if it was a desktop.

Susan: Okay, then what else do you need? You've got some other items out here.

Dan: Usually in your home you'd place an access point and there are three examples here. They have varying prices and various strengths and power.

Susan: And so this access...I just want to take a look at this it's such a cute little guy. These all do basically the same thing. The access point here has a little hook up in the back. So what would you connect this to?

Dan: You might connect this to, say, the Ethernet in your hotel room. And then you could use your laptop anywhere around the office.

Susan: Around you hotel room.

Dan: Hotel room; yes.

Susan: You'd be able to sit on the bed; you wouldn't have to have a long cable. Absolutely. Now, you say there are some security issues with these devices as well. What do you want to look out for?

Dan: There are several encryption standards, one of which is called WEP, Wireless Equivalence Protocol, it's an older standard. It was shown to be cryptographically weak.

Susan: Doesn't sound good.

Dan: No. So people found out a way to guess your password. So now there's a new standard called WPA which is a much stronger numeric protection.

Susan: So if you buy a new wireless access point or hub, you really want to be looking out for something that has WPA rather than WEP.

Dan: Oh, yes. You bet.

Susan: What if I've got an older one? Do I need to go out and get a new one so that it has the newer encryption?

Dan: You might want to go on the web to look for...at your manufacturer's website. Many of the manufacturers have actually rewritten their access point and there's a process you can download new code into them and fix any problems there were and you might gain some performance and you will gain the new security features.

Susan: Okay. What sort of timeline are we talking about if I've got a device that's a year old is this something I should be looking into, or?

Dan: The ones that are the most trouble are 2 or 3 years old. But it's always a good idea to go and check that there wasn't a flaw that was corrected.

Susan: Sounds good. Now, the WEP or the WPA; is that something that's already set up? I take it out of the box and I'm good to go?

Dan: No usually you have to connect to your access point. They are almost always done over a webpage and you usually need to check some boxes and type in a favorite phrase as a password.

Susan: So once again, when I first pull out this device I need to make sure it's secure.

Dan: Yep.

Susan: Are there any other things I can do to keep my wireless connection secure particularly in the Local Area Network?

Dan: Well, one of the things you can do is make sure that you're not doing anything that's important to you over an unencrypted link. You can use something called a VPN, a Virtual Private Network.

Susan: Okay.

Dan: Usually that's a service that a corporation would have. You can set your WPA keys. There is a nice encryption built into the World Wide Web. When there is a little lock on the bottom of your screen, you know, that's telling you that you're doing SSL 2, and that's a fairly secure method.

Susan: There are just a few things to look into to make sure that you're being safe when you're using wireless.

Dan: Yeah.

Susan: Thank you so much, Dan. You've had lots of great information today.

Dan: Well, thanks. It was fun to be here.

Susan: One Minnesota city has decided that wireless internet connections should be available at a low cost to its residents. Let's take a look at how Chaska is provided this service to the entire city. We went to Chaska and spoke with Bradley Mayer, the information systems manager for the City of Chaska and Chaska.net.

Bradley: Well, what Chaska.net is it's a system that's been deployed city-wide within Chaska specifically to provide internet access to residential users within Chaska. It's very similar to a cable or DSL type service it's just that we use wireless technology to provide the service. The backbone of the system is its wireless access points. Within Chaska we have about 12 square miles covered and within those 12 square miles we have about 350 wireless access points deployed to help provide the service. And if you drive around Chaska you'll see these little white wireless cells hanging all over the place. All of the access points kind of cluster around what we call gateways and gateways are actually wired locations that ultimately get to the internet. This is the device that we provide customers with a subscription. It's really nothing but an 802-11B client wireless bridge and what it does is it talks with an antenna to our wireless system and then it provides the Ethernet connection that would go to the customer's computer or router. Our service is 15.99 a month so it makes it affordable. But also there is a part of this service that we really don't advertise or broadcast but it's a mobile-type system so if you're in a park or if you're somewhere with your kids and they're playing and you want to work you can gain access to the internet pretty much anywhere in Chaska.

Susan VO: Mayer says the project began about six years ago when the city started looking for ways to provide affordable high-speed internet access to local businesses. Now as we've progressed throughout the six years one of the things that our city leaders wanted us to do was build on what we had for businesses and make it available to residents. Today we have roughly 2200 subscribers and that's out of about 7500 households. So we have almost a 30% penetration in the households of Chaska.

Susan: Mayer says that Chaska is one of the only towns in the country to have its own city-wide wireless network. He says the city learned a lot of things that hard way but now their working to help other cities gain from their experience.

I'm back with Professor Harjani. Ramesh, is WAN coming to many cities like Chaska?

Ramesh: A couple of other cities have either publicly funded works or like in Seattle the number of people have gotten together and just put a lot of wireless networks that are accessible. So, a number of cities are starting to get this.

Susan: And is it with a similar model where folks are paying for the access points in their home or...?

Ramesh: Philadelphia has a similar model. Some cities are starting to think about putting it our for free so everybody has access. Typically a lot of other countries like Korea has them accessible relatively free. Seoul is pretty much has access but it's like an \$8 extra fee to your regular wireless.

Susan: All right.

Ramesh: Places like San Francisco has Google putting out wireless in Union Square so people can surf the web.

Susan: Just out in the public Union Square.

Ramesh: in the public, right.

Susan: I think that the impression that a lot of us have when we think about, say Minneapolis going wireless is that the public areas are going to be wireless and I'm not sure that that's really what's being talked about right now with Minneapolis, but it's very interesting. Now, when we talk about what's going on in Chaska, is Chaska actually using a real Wide Area Network?

Ramesh: No, Chaska is not actually using what we would traditionally call a wide area network. What they're doing is they're putting wireless connections at different locations...a number of access points and they're covering an area that's the whole city but each one is actually having multiple access points.

Susan: So, it's little Local Area Networks.

Ramesh: That's right.

Susan: But lots and lots of them.

Ramesh: Exactly.

Susan: Now, I know that...It seems that when you have...these are radio waves and you have all of these Local Area Network areas together are there going to issues with an sort of interference?

Ramesh: There are always issues with interference in terms of the number of channels that are there and making sure that when you are talking to any one particular access point if the coverage is good then you're talking to multiple access points and how the protocol is, how do you move from one to the other.

Susan: Mm. Hmm.

Ramesh: And a lot of these techniques have basically been found out in cell phones because that's exactly what you had.

Susan: Because you are always moving with your cell phone so you need to be able to keep the connection wherever you are.

Ramesh: Yes. So some of these hand-off issues have already been around and so more of it's coming to the wireless LAN space.

Susan: Okay. Okay. What about, now thinking a little bit about people who are moving, a lot of folks are using wireless in their home, in their apartments and things like that. Are there issues? Are there problems with your computer when your laptop is trying to connect to...how does it figure out which wireless access point and so forth.

Ramesh: Sure. One of the things that Dan pointed out earlier was making sure that you have security turned on. You can also restrict your computer to make sure that there is a MAC limitation that there are only a few computers can see it.

Susan: A MAC limitation, so your MAC address.

Ramesh: MAC is the physical address of each computer.

Susan: Has nothing to do with Macintosh computers

Ramesh: Exactly; sorry.

Susan: No, that's quite alright it's a common confusion that people have. The physical address each computer has no matter what kind of computer.

Ramesh: Exactly. Each computer, each wireless card has a different MAC address.

Susan: And it's unique.

Ramesh: And it's unique and you can restrict the number of computers that can get access to your access point.

Susan: Okay.

Ramesh: Typically what you would do is when you set up the process of doing this WPA you will set up what is called an SS ID. You would say I want to connect to this one and put up an ID and your password and that would be the one that you connect to. In Windows XP you can do things like, "this is the preferences of how I will connect. I will connect first to this and if this is not available, I will move on to the next one."

Susan: Okay. So first of all we're addressing the issue of you're connecting to the one you want to connect to, but also, by limiting the MAC addresses that can connect to this you're limiting who else can connect to your wireless access point.

Ramesh: Absolutely.

Susan: Which is security but it's also an issue of bandwidth too, isn't it?

Ramesh: MAC address limitation is more security than anything.

Susan: Okay. Then, the apartment issue, you've got a wonderful diagram here. I think it illustrates some of the issues that people can have when people are using the same frequency.

Ramesh: Correct. So the wireless LAN that we're normally used to seeing is 11B and 11G. Both run at 2.4 gigahertz.

Susan: That's 802-11B and 11G that are used all over the U.S.

Ramesh: Right; all over the U.S. and pretty much around the world as well.

Susan: Okay.

Ramesh: So with these two standards there is only a certain frequency range that's available to them and in fact as we see here that there are 11 channels and that would give us the impression that there are 11 independent channels, but it turns out that these channels are spaced smaller than the actual usage of frequency.

Susan: Okay.

Ramesh: Which is shown on top.

Susan: Mm. Hmm. So there's overlap between the channels.

Ramesh: Absolutely. There is overlap between the channels and what you want to do is when you set up the access point the default more often than not happens to be the central one, channel 6.

Susan: Okay.

Ramesh: And then when you do bring your computer up in the neighborhood you can see what the other people have and you probably want to choose one that's different from others.

Susan: Okay. So when I buy my wireless access point if I don't do anything to it it's insecure and so it's set up to channel 6.

Ramesh: A lot of them set it up to channel 6.

Susan: If my neighbor is using channel 6 too I might have some...

Ramesh: You might have some issues with trying to get bandwidth and what it'll look like is that you won't be able to access the internet.

Susan: Okay. So, that's no good!

Ramesh: Right.

Susan: So, the thing to do is look at what my neighbors are doing.

Ramesh: Right.

Susan: You did that didn't you?

Ramesh: Yeah.

Susan: Can we take a look at that?

Ramesh: Absolutely. So, this picture here shows... This is a software that I downloaded from the web called Netstumbler.

Susan: Netstumbler; is that free software?

Ramesh: It is free software. And what it does is it takes your computer and does a scan across the channels and see who is on what channel. For example I just did this where I live. Where I live is fairly close to the University here. And so there are a lot of students around where I live and I am...as you can see there are three people on channel 11 and someone else on 10 which is really close to 11 so it's really, effectively, 11.

Susan: Okay.

Ramesh: And there are two people on 6 and two people on 1.

Susan: Okay.

Ramesh: So people who are on 11, if they are close together, are going to start having problems.

Susan: So these people are probably having problems with their wireless right now.

Ramesh: Yes, exactly.

Susan: Okay, now, another thing that's interesting to see here, I see a lot of WEP in here, around 5 of them but then 5 or 6 more that have blank in that area.

Ramesh: Exactly. So what we see here is a lot of people don't even put the security in. Which is...we can actually see the traffic that people are watching over the internet.

Susan: Absolutely. If I don't want to download something like Netstumbler or something and I live in an apartment this really might be an issue. What would be a good channel to set my wireless access point to?

Ramesh: You can try 6 which comes default and if you start having problems change to say, 1 or to 11 and see if it gets better. A lot of times it does and I do that at home as well.

Susan: So I really don't have to do anything unless I start having problems.

Ramesh: Exactly.

Susan: Great! Thank you so much for being here with us.

Ramesh: My pleasure.

Susan: We've covered a lot of information about wireless technology. Here are a few highlights for your files.

Susan VO: Ramesh Harjani electrical and computer engineering professor at the University of Minnesota explained the different types of wireless networks.

Ramesh: Ramesh: Sure. We classify them in terms of how far they reach. We have what its called a "personal area network" and you can think about it as being something that you can reach out 10-15 feet around your person. Then you have what is called a "local area network" local being...think of it as your house.

Susan: Mm. Hmm. Okay.

Ramesh: And then you have what is called a “metro area network” or a MAN, so it covers a city and then you have WAN which covers the entire country or across the world.

Susan VO: Daniel Westacott, systems engineer at the University’s networking and communications services discussed Bluetooth, the technology used for short range wireless devices.

Dan: Oh, people use keyboards, wireless keyboards that use Bluetooth. Much of the technology is done actually on phones and related devices...and accessories for phones.

Susan VO: Dan also talked about the range of these devices.

Dan: Much depends on your local conditions, you know? When everything is going well you can get 30 feet.

Susan: Okay.

Dan: But, you know, if you have something in the way or interference of course you can get significantly less.

Susan VO: Daniel also discussed wireless security issues.

Dan: There are several encryption standards, one of which is called WEP, Wireless Equivalence Protocol. It’s an older standard. It was shown to be cryptographically weak and people have figured out.

Susan: That doesn’t sound good.

Dan: No! So, people figured out a way to guess your password so now there is a new standard called WPA which is a much stronger numeric protection.

Susan VO: And Professor Harjani added more to the security discussion.

Ramesh: You can also restrict your computer to make sure there is a MAC limitation so that only a few computers can see it. The MAC is the physical address of the computer, each computer; each wireless card has a separate MAC address.

Susan: And it’s unique.

Ramesh: And it’s unique and so you can restrict the number of computers that can get access to your access point.

Susan: Okay.

Ramesh: Typically what you would do is when you set up the process to bring this WPA you will set up what is called an SS I.D. you will say that I want to connect to this one, put your password and that will

be the one that you connect to. In Windows XP you can do things like “this is the preferences of how I will connect.” I will connect first to this and if that is not available you go on to the next one.

Susan: Be sure to check out our website. You can view past episodes or ask a question on today’s topic. You can find us at techtalk.umn.edu. Next week on Tech Talk we’ll discuss how information on the internet is being written and distributed by individuals and with communities. And just what are Blogs and Wikis? Until then; 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

Executive Producer

Robert H. Bruininks

Special Thanks to:

Steve Cawley

Shih-Pau Yen

Host

Susan McKinnell

Producer / Director

Susan J. Tade

Assistant Director

Rich Reardon

Technical Director

Steve Barbo

Production Assistance

Kellie Greaves

Scriptwriters

Kate Sophia

Joshua Welsh

Audio

Jonathan Kranzler

Floor Director

Laura Cervin

Cameras

Hope Johnson

Colin McFadden

Alan Wivell

Teleprompter

clg

Joshua Welsh

Lighting and Set Design

Laura Cervin

Graphic Design

Nicky Torkzadeh

Animation

Brian Floyd

Effects Design

Paul Pecilunas

Make-Up / Prompter

Sharon Davis

Field Videographer

Alan Wivell

Ms. McKinnell's wardrobe provided by

The Gap

Web Development Team

Christina Goodland

Kellie Greaves

Doug Hamlin

Thanks to:

City of Chaska

Best Buy

CLA TV Studios

Radio K

Bakken Library & Museum

KSTP Meteorology Department

Pavek Museum of Broadcasting

Antique Telephone Collectors Association

©2005 University of Minnesota

©2005 by the Regents of the University of Minnesota. All rights reserved. The University of Minnesota is an equal opportunity educator and employer.
♻️ Printed on paper containing at least 10% post-consumer waste. Produced by the Digital Media Center (DMC), Office of Information Technology. This publication/material can be made available in alternative formats for people with disabilities. Contact the DMC Communications/Marketing Coordinator at (612) 625-5055 or dmc@umn.edu.