13 WLAN 2

Hi there, and welcome back to part two of Cisco's Enterprise Wireless Network. With me, is Osheen Mac Alasdair and he's going to continue this seminar talking about something very important to a lot of our customers and to me and that is security, securing the wireless LAN. Oisin. Hi Rich, what we're going to do is talk about some of the high-level concepts associated with wireless security, some of the considerations that we should take under consideration and also some high level recommended best practices.

WIRELESS LAN SECURITY

There are two basic concepts when we look at wireless security, two different security models, if you will.

DIFFERENT SECURITY MODELS

At a high level or a fundamental level you can either trust your wireless network or you can consider it an untrusted network and they both have their advantages and disadvantages. A trusted wireless network is effectively considered just another transport medium. It's integrated into the existing network and security is provided by robust authentication and encryption. An untrusted wireless network, on the other hand is usually behind a firewall or DM. Access to the network is usually provided by a VPN, virtual private network and security provided by the VPN overlay.

TRUSTED WLAN

The advantages of a trusted wireless network are obviously ease of use. There are a wide variety of EIP mechanisms available for authentication with wide cross platform support. A single sign on is fully supported and you have easy layer 2 and layer 3 roaming and fast layer 2, layer 3 roaming. And very, very easy to integrate it fully with wireless voice and other multicast traffic like wireless video perhaps. The disadvantage of a trusted wireless network of course is that a successful attack upon the wireless LAN is no different than a successful attack on your wired LAN. Because it's fully integrated any compromise of the wireless network provides access to the enterprise network itself.

UNTRUSTED WLAN

The untrusted wireless LAN, well what advantages does that present to the enterprise? Well the wireless network is behind VPN concentrators typically. A successful attack on the wireless LAN doesn't provide access to the enterprise network. It only provides access to the VPN concentrators themselves if you will and therefore your enterprise network remains protected and security is provided by robust triple layers or one time passwords. Significant disadvantages to an untrusted wireless LAN are of course, it's considerably more complex from an architectural perspective. It requires VPN infrastructure and VPN or SSA over clients on all your devices. It's considerably less user friendly, it doesn't scale as well. Therefore when you really think about it, it reduces the productivity value proposition. And when we take into consideration that most wireless networks are produced or are deployed to enhance mobility and to enhance productivity a good then architecting or security wireless network with the untrusted model is removing some of those potential productivity benefits themselves. So I recognize in these two models that Cisco has gone with the trusted wireless LAN network. That's right, most enterprises do actually, Rich. And the untrusted network is popular, I won't even say popular, you do see it in some financial organizations. Some federal or government organizations might go with an untrusted wireless LAN where they have very, very stringent, sometimes legal obligations to use certain levels of encryption. Or they may have very, very strong internal or federal standards that require a certain level of encryption and even in those circumstances you can quite often go with a trusted network. The untrusted network, its only real advantage is one extra layer of security but it has several disadvantages. Most enterprises and Cisco have gone with the trusted wireless network. In

other words you just secure the wireless network and it's just treated like another transport medium. And that's the one we're going to talk about primarily in this presentation. But I can understand why a wired network is easier to trust because it takes somebody to actually physically go in and clip wires to it to be able to tap it. But wireless it's broadcast, anyone with the right equipment can pick up that. So why does Cisco feel that the wireless LAN network can be trusted? Well, not only Cisco but the industry as a whole, Rich. The introduction of the robust security standards has mitigated any of the risks. While people can intercept the traffic, if it's encrypted to a sufficient degree of complexity it's not going to make any difference. Your traffic may be intercepted but a user will not be able to decrypt the traffic. It's absolutely no different conceptually than sending traffic over the internet. And we all know the widespread adoption of VPNs or internet banking or any of those kinds of concepts where you don't actually have control over the data as it is transported but because it is encrypted or entunneled it's safe. Okay.

THE DUAL ASPECTS OF WLAN SECURITY

So one of the things we need to consider, especially in the trusted model, is there's two, the dual aspects of wireless LAN security, you have authentication and you have encryption. Sometimes people confuse these or overlook the two aspects, there are the two sides of one coin if you will. When you're talking about authentication you have to ensure that your users are identified and authorized to use the wireless LAN. And encryption is actually encrypting the data, maintaining the integrity of the data that's actually sent or transmitted over the wireless LAN. It's no good having extremely strong encryption on your network if somebody can spoof their way on in the first place. And conversely what use is rock solid authentication if someone can just sit outside or intercept packets and decrypt them anyway? Yes. So it's like having very strong ID requirements at a door or a gateway. There's no point in having security guards checking everyone's identity before they get into a meeting room if the windows are open and someone can sit outside listening to the conversation in the first place. Well put, yeah. So in a robust enterprise class wireless network you have to ensure that both of these are addressed, both authentication and encryption.

EAP MECHANISMS (AUTHENTICATION)

Now authentication is primarily produced or provided by what we call EAP mechanisms or extensible authentication protocol. And EAP mechanisms are, the EAP protocols are the , there's a wide variety of them available. Everything from EAP Open which is what is used in guest wireless networks, that provides no authentication, I mean, it's wide open and to Cisco LEAP which is a very, very popular one to PEEP, EAP, TTLS, EAP TLS. It's really up to the enterprise itself to make an educated selection or make an educated choice of the correct and most appropriate EAP mechanism for your environment. Quite often it might be two, it's quite possible to support two or three. From our perspective if you look at this graph, what you really want to go for is the sweet spot in the top right hand corner. You want to have the maximum ease of deployment while it's maintaining the maximum degree of security. If we look at EAP Open we'll see it's the top left hand corner. It's extremely easy to deploy but its security, well it has no security, it's negligible. There's no point in -- so that's somewhere that you don't want to go. Conversely if you look at EAP-TLS, EAP-TLS provides exceptional levels of security but it is rather complex to deploy. So when we, Cisco internally were looking at our plans, EAP-Fast was really an easy choice for us. Not only because it was developed internally but also because it was a seamless migration path from LEAP. It provides tunneled authentication, so it protects the actual identities and criteria that are being exchanged and it provides very, very robust security. So a combination, it's right there in the sweet spot.

EAP MECHANISMS

All the EAP mechanisms are available, I mentioned them earlier, there's EAP-TLS, it's the open standard for PKI base. It requires a public key infrastructure. It's a tunneled authentication protocol, so that means the actual -- it sets up a tunnel between the access -- between the client and the authenticator. And it's over that tunnel that the actual credentials are exchanged. So even though you're not on the wireless during the authentication exchange, your identity is protected and your user identity and your password are protected. So it's harder to be spoofed or taken over that way? Absolutely, it's not necessarily spoofed but it's impossible for someone to capture that traffic and it's

tunneled, they can't capture it. It's a VPN tunnel if you will, temporarily for a couple of mini seconds as you're exchanging your credentials. EAP-Fast is a Cisco successor to LEAP. It also provides tunneled authentication but unlike TLS it doesn't require a certificate on every server and every client device. LEAP, which is a Cisco standard, very, very wide adoption, very, very good cross platform support, very popular in the industry. It can be vulnerable to offline dictionary attacks if it's not properly implemented. Then we have EAP-TLS, that's a funk standard. It's a version of tunneled authentication, I beg your pardon, it's like a variant of EAP-TLS that provides tunneled authentication, without necessarily the complexity of a PKI. PEAP, there's two versions of PEAP, there's the Microsoft or Cisco implementation of PEAP. They also provide tunneled authentication. There's some debate whether it's vulnerable to attacks, though to fair none of these have been actually realized in the field at the moment. .. D5 ..., we've talked about EAP-Open and there are others. There's EAP-SIM, which is used in Europe by some of the mobile phone operators, where they use the actual SIMM card in GSN phones as an identity. They're moving into the wireless -- WiFi hotspot market. So it's a case of well, there's so many EAP mechanisms out there, which ones do I choose?

CHOOSING AN EAP MECHANISM

Cisco has gone with EAP-FAST. EAP-FAST. Okay. We were at Cisco LEAP -- and then we migrated to EAP-FAST. So the mechanism that you choose will depend upon a wide variety of aspects but they take into account the clients you have, what your existing policies are, what kind of existing security frameworks and the infrastructure you have. So for example if you have a certificate of authority in-house already or do you trust external certificate of authorities? If the answer to that is no, then that may lead you to shy away from a mechanism that requires a PKI. And what client platform do you support? If you need to support like a really wide variety of client devices and MS-DOS, Windows XP, Windows 95, Windows 98, you may decide well LEAP has a lot of attractiveness there because it has much wider support than some of the other EAP mechanisms. Do you already have a PKI installed? Again, if the answer to that is yes it might make the choice of going with EAP-TLS a little bit easier. It probably won't reduce the actual complexity of deployment but it certainly will ...

EAP PROTOCOLS AND DATABASE COMPATIBILITY

In the following two slides I go into some detail. I'm not going to talk to every one of these items, we'd be here all day. But the following two slides our viewers can download and review themselves. And we go through the various characteristics, features and database compatibility of the most common EAP mechanisms. So we talk about EAP-TLS, PEAP, TTLS. We talk about LEAP and we talk about EAP-FAST. So just as a quick question, little off line. I know that Cisco has migrated from or is in the process of migrating from LEAP to EAP-FAST, how difficult is that?

EAP PROTOCOLS: FEATURE SUPPORT

We completed that migration quite some time ago actually. And it wasn't that difficult at all. Oh, okay. All we were required to do is to update our client software and update our ACS servers at the back end authentication protocol. So you didn't have to touch the access points or the switches or the routers? Not the switches and routers, no, no. The access points themselves would have got a later version of code that supported EAP-FAST. But that's something that we do as a matter of course is keep our access points, which our customers should do is keep our access points current to the latest revision of code. We should do that with our routers and switches as well, make sure you've got the latest version of IOS running at all times. No different from running the latest version of the operating system and the latest patches that are released. Okay, so yeah, it was just a matter of running a patch on my client, on my laptop, and then updating the ACS servers. Yes. Well no, you didn't have to run anything on your laptop; you would have had the new software automatically -- your AC and your client updated. Now mind you, client management can be challenging. And we can talk about that later. Okay.

WIRELESS LAN SECURITY: RECOMMENDED BEST PRACTICES

So I'm going to finish up this brief session with just some 10 or 12 recommended best practices that you should take into consideration when designing or deploying your wireless LAN. I'll start with a secure management policy. You can't underestimate this. It's no good

buying top of the range gold platinum standard Cisco IOS access points, but not necessarily hardening them or implementing them in a secure manner. You should consider disabling Telnet, once they're deployed and configured, you should consider disabling Telnet, disabling HTTP access, disabling CDP for example. And use SS , enable or admin authentication. So you want to basically make sure that the access points themselves are -- access to them is restricted. Now of course this only applies in the autonomous IOS model. In the centralized wireless LAN solution that's already handled by embedded certificates and the fact that the wireless LAN controller is what controls and manages the access point. So if you're going to go with the autonomous IOS based access point, make sure you have a secure management policy on those APs and bridges. Or alternatively go with the centralized wireless LAN solution where you don't have to worry about that aspect at all. The second point also is applicable to the IOS based access points. Make sure you've got a management VLAN for the APs and bridges and restrict access to the management VLAN. And make sure that management VLAN isn't broadcast wirelessly. There's no point in having your management traffic being broadcast wirelessly. And we find internally, what we've done is we've enabled or implemented a layer 2 MAC address spoofing prevention in order to be locked into common or critical MAC addresses, the default gateway, the MAC address of the BBSM. Just make sure that somebody isn't able to spoof those MAC addresses. And if you're using Cisco IOS access points as well, enable PSPF, which is Public Secure Packet Forwarding. Effectively what that does is it disables peer to peer networking on that radio cell. So people can't communicate amongst themselves via the AP -- the traffic is client/server only if you will. Buyer scanning and firewall is recommended on all wireless LAN clients. Of course that standard recommended practice for all devices on every network these days. So on all PCs, you mean all those -- Absolutely all PCs, even all PDAs. In our mobility program within Cisco we have implemented a security standard and security clearance on our officially supported PDAs within Cisco. You'll see with the advent and development of Smart clients, smart phones, converged PDA and voice devices, the intelligence in handheld devices is going to increase. And unfortunately the intelligence as it increases, therefore its attractiveness to the hacker community increases. You'll begin to see viruses. You'll begin to see people -- even accessing information on those devices is attractive to your hacker or even your thieves. And people who are going to find these things, you know, left behind in taxis or on trains for example. I'll mention this in the moment, there's another section I talk about this. RF monitoring, this is very, very important. So radio frequency monitoring and rogue AP detection. Rogue APs are probably the single most major security threat to our wireless networks. People think that -- well if your network is properly implemented and you've got a robust security architecture and it's implemented across all your access points, you're vulnerability toward driving or hacking is going to be reduced if not entirely mitigated. In that circumstance there's still a risk to the enterprise of rogue APs. Rogue AP by definition is any access point that's installed by people who -- a rogue AP is any AP that's installed not by your IT department. So it doesn't have to necessarily be connected to your network. If it's connected to your network it's going to be a significant security risk but even if it's just turned on and left at someone's desk it's going to have a service impacting aspect. Because the radio frequencies created by that device are going to interfere with your production network. So it's critical for every enterprise today to have some method of rogue AP detection. Now you can do this via radio scanning, client or network the based scanning, preferably all three, so for example, putting in place a wireless intrusion detection system. That feature set is supported in the wireless LAN solutions engine and the wireless control system, WLSE and the WCS. And there are third party tools you can deploy as well. If you decide you want to go the third party route, the best practice here is don't ignore it. It's critical that you take rogue AP detection seriously. There's no such thing as a non wireless company. There may be people out there who think, oh, no, we don't have wireless LANs. I can guarantee you if you went into their premises, as long as it wasn't just one room and one person could keep an eye on you, I guarantee if you went into their premises with an RF scanner you would detect people who have installed wireless networks. Usually with the best intentions but unfortunately because it's not installed by an IT department or people who are familiar with the security impacts, quite often they're deployed in an insecure manner, not maliciously, 95 to 99% of rogue APs are installed by users with the best intentions. They're nonmalicious. Because it's convenient, it helps them do their business. It's convenient. There's very few, there are virtually no examples of people sneaking into buildings and maliciously planting a rogue AP and sneaking out again. It's a case of -- analogous to someone just leaving the door open by mistake. It happens, but they don't, it's a mistake. People are maybe unaware of the security implications of their actions. I remember early days in Cisco before the wireless LAN was an established service, where there were a lot of different groups that were finding that their workgroup worked more efficiently if they had a wireless access point. Absolutely, people love wireless LANs. One of the soft benefits of our global comprehensive deployment was that when we began the deployment five years ago we detected as you say

hundreds of instances of deployments of wireless networks. I mean it was a bit of an eye opener. We were lucky that it was the early days then and wireless technology wasn't prevalent on client devices, because it would been a greater security risk. Once the global deployment was undertaken and completed in about six months, it was quite a rapid project but once we had that global deployment it reduced the number and the number of incidents of rogue APs. But they still occur. People still bring their access points in and turn them on. People still are working maybe on a wireless device or some of the people in labs and some of the people in their wireless business units and stuff. There's no maliciousness in any of it, but you just have to maintain ownership and integrity of the RF space, if you will, even though it's an unlicensed spectrum. What I often say to people is one of the greatest advantages of WiFi or 802.11 based wireless networks is that they are unlicensed. And one of the biggest disadvantages of 802.11 based WiFi networks is that they're unlicensed. You can turn one on, it doesn't matter. You don't have to worry about the FCC or FC or anything like that. Conversely, somebody -- John Smith next door, can also turn one on. That's why this proactive intelligence in your wireless network is important. The ability to scan the airwaves, detect interference, detect rogue APs, fine tune yourself, self healing, all the new technology, new capabilities are available today. It's also very, very important that you select the appropriate EAP mechanism. We talked about that earlier. One that satisfies your client's requirements, yet one that provides a robust security. So if you're an enterprise deployment I wouldn't recommend deploying EAP-NV5 or EAP-Open for example.

WIRELESS LAN SECURITY: RECOMMENDED BEST PRACTICES (CONT.)

Very important, but often overlooked is a clearly defined and communicated wireless security policy. It's absolutely no good if you have a very dense detailed security policy in wireless networks and you don't communicate it to your user population or they don't know where it is. 99% of your users are going to comply with clearly communicated and explained policies. If they understand the risk they'll go, oh okay, well now I know why I shouldn't turn on a rogue AP. Or okay, now I know why I shouldn't use a low cost consumer grade device, now I know why I have to -- my laptop has to support EAP-FAST or WPA or whatever the standard is that you adopt internally. So define your policy and evangelize it, communicate it, tell your users not only the what but the why. And as I said the vast majority of users will comply with those policies if they understand. You also have to have a clearly defined security posture, right? So you have to define what EAP mechanism, what encryption methods you adopt, and WPA is probably the most common one. WPA2 now is making progress or has been recently ratified. You should also list the approved clients and approved standards and have these in your design guide. These don't necessarily need to be communicated, the technical specifics to your users but if you don't write down the standards it's going to be very difficult, especially the more widespread your deployment is. If you've got buildings scattered around the city or across the whole country or internationally like Cisco does, if you don't have your standards clearly documented people are not going to comply to them because they don't know where they are and they don't know what they are. You'll end up with different standards everywhere. You'll end up with different standards everywhere. Yes. Educate your user base. I touched on this earlier. Tell your users what the wireless LAN is and what it isn't, what it can do and what it can't do and what is acceptable policy and what is unacceptable policy. It's no different from educating your users about physical security, about not allowing tailgating coming through doors into the office or car parks. You know you just tell the users what the prudent activity means, not giving out their password to people so they can use it. Again it's just educating your user base about the pros and cons of wireless if you will. And finally, though not specific to wireless LANs, it is in the mobility space, it's very important that you have an adoption position and security policy with regards to PDAs or smart phones or these converged devices. Securing access to these devices is not enough. If you have access to the network with these devices, you also have to secure the actual information on them. So some kind of encryption standards, some kind of policy that states that you should maintain pins or passwords, it's quite important. These devices are --there's a big enough problem with people mislaying or having stolen laptops but with phones, wireless phones and PDAs that's a much more common event. And as these devices become more intelligent, as more information is stored upon them, you have to think to yourself, well, how do I secure the information on those? How do I ensure that they don't -- I just power it on and suddenly someone's got access to my full email list, my -- all my phone numbers and contacts and -- contacts, exactly, exactly. So encryption and passwords of mobile devices is important. If you follow these 12 basic steps you're going to end up with quite a secure and wireless network. Make sure you've got good authentication, good encryption and you'll be able to reap the benefits, the manifold benefits

that wireless networking provides the enterprise while it's avoiding the pitfalls and the security vulnerabilities that there was quite a bit a concern on in the industry in the last few years. Issues that have been addressed almost entirely with today's products and services.

Q AND A

Perfect. Well, Oisin, thank you very much. Absolutely, no problem Richard. At this point we have a little bit of time. We've put together some questions that customers have asked us earlier about this topic in previous sessions. And if we could I'd like to get Oisin to spend a few moments to answer a few of them.

Q. All right. All right, so question one was what was the major reason that Cisco IT decided to deploy wireless LANs in the first place? Why did we deploy wireless LANs in the first place?

A. I'd like to say because we were very prescient and we knew what the benefits were going to be and we knew where we were going to save $28 to $150 million a year. But really? Realistically it was because we wanted to provide a mobility enabler. When we deployed our wireless LAN initially it was as a secondary network. It was a mobility enabler. It was effectively to provide an amenity to our staff. We were in an environment where on one hand we had a global work force that was mobile, entirely mobile. We provided all of our users with laptops, yet we were tethering them to the desks. It'd be like giving them on one hand the opportunity or the potential to be productive, an additional potential productivity benefit and taking it away on the other hand. So by providing wireless access we say, well, you know, we've given everyone these laptops, let's leverage them, let's leverage this mobile workforce. The working environment of all enterprises was and continues to evolve. So it was a decision to go with comprehensive deployment. We talked about at one stage going with spots of deployment, maybe just doing the meeting rooms and common areas. But early on, no let's embrace this technology, we know it's going to be important, we know our users are going to appreciate it. However, let's just have it as a secondary mobility enabler, the adoption took the wireless team by surprise. Within 12 months of it being deployed 27% of the users say they use it as their only or primary access medium. 97% of our users said they use it on a weekly basis that adoption has continued and continues to increase. And we expect it to increase even further with the advent of the next-gen wireless LAN, the enhanced services and increased stability and security provided by the centralized and autonomous wireless LAN solutions of the Cisco unified wireless network. And as you mentioned earlier a lot of our employees had already discovered the benefits of wireless for themselves before IT had gotten into that area. Indeed and we had a lot of early adopters and home wireless users, etc, it's really been a success for us. That's one of the primary motivating drivers for making a significant investment in upgrading our wireless network to the next generation of service. We want to add services. We are already supporting wireless voice, well let's add even enhanced wireless voice services. Let's facilitate roaming between buildings. Let's provide integrated wireless LAN management and intrusion detection. Let's increase the stability and let's reduce the support costs. It's been a roaring success for Cisco and it has positively affected the bottom line. We are saving millions of dollars a year in productive time and our users have come to expect it, our users have come to expect it. If there is a outage in the wireless LAN you can rest assured me and my team know about it pretty quickly because people ring up and complain. Yes, I do too. It's like when you turn on the water or you turn on the electricity people -- it just becomes an amenity, it's expected.

Q. Yes, yes, okay, there's a second question. And this is something I'd heard when you presented the BBSM and guest wireless hot spots area. They asked what's the point of Cisco having guest wireless hotspots in the first place, especially having them at all Cisco locations. And do employees use this or is this entirely for guests?

A. Let me answer the second part first. Sure. So it is geared exclusively for our guests. Okay. And employees, there'd be no reason for an employee to use this. We have customers who have adopted a similar approach to guest networking and they use it as a method to segment say certain traffic of contractors perhaps. Oh, okay. Or temporary workers, we haven't followed that model ourselves. So the guest wireless LAN networking solution is for guests. Cisco employees, there'd be no reason for them to do it. They already have automatic, single sign on, completely transparent access to the enterprise network. So why would they go through the extra steps of getting their -- it's like they've gone to their web access portal, give themselves an access code and come back in again. Fair enough. They could do so, but it's not

required. But then why do it? Why do it in the first place? I mean it's adding a whole different overlay network for our guests. What's the point of that? The point is when we have visitors it's incumbent upon us, not because we're Cisco but as a world class enterprise to provide connectivity services for our visitors. And it's similar, if you like when visitors come to your office you don't prevent them from using the telephone, people expect a telephone. People expect access to a room with electricity. People expect access to a room with a telephone and people, now they bring their laptop, they bring their PDA, they expect access to the internet. It's another amenity. It's an amenity for them, we're providing them and there's a degree of evangelism there, we're promoting the technology. But when we first put the guest network in, this is an interesting observation, we actually used to maintain a stock of wireless cards at the lobby ambassadors, at the reception areas of all our main buildings, to provide our users, if they came in, do you want to use wireless networking? Well if you don't have a wireless card well let - here have a free card, well, have a lend -- borrow one. Lend them, have a free card while you're visiting us. We no longer do that. Everyone has a wireless enabled laptop these days. It just shows you the prevalence of the technology. So by providing guest access networks we're also increasing their productivity. We're also making their lives easier. They can use it just to gain access to the internet or they primarily quite often will use it to VPN back to their own enterprise network. That makes sense. And by providing this in a controlled manner rather than just being in an uncontrolled manner, which is what typically happens in a lot of enterprises, we are protecting ourselves also from security risks and from legal liabilities. I mean when you consider that someone on our network say, we have a visitor or temporary worker or someone who comes to our network and gains access to the Internet and launches an Internet worm. Or hacks into a U.S. federal web site. From a Cisco site? From a Cisco site. Yes. For all intents and purposes that attack or that incident is originating from Cisco's IP address range. Right. So we want to be able to ensure that our guests, A, are presented with a portal and they sign an acceptable use policy. And B, that we're able, not to track their activity, because we don't monitor their activity but we need to know what IP address was assigned to what guest or what session. So effectively we have a beginning time, an ending time and an IP address. So if in the future for IT forensic reasons, if the FBI or the men in dark suits wants to know for some reason why did this happen at this time? We're able to correlate that back to our reports and say, well, that was associated with Mr. Rich Gore who came in and did the wrong thing. I swear I have an alibi. So it's a given to say that an enterprise endorsed guest networking solution that provides an amenity, protects us from legal liabilities, ensures our users sign an acceptable use policy. Every Cisco employee has to sign an acceptable use policy so why shouldn't somebody who comes in and uses our assets? And also, so it protects us legally and security but it does so in a positive and as seamless method as possible.

Q. Makes sense, okay, there was a third question. Okay. Which was how are we supporting wireless voice in Cisco today and what are our plans for the future for wireless voice?

A. That's an interesting question. So when we first deployed the wireless network it was designed for intermittent data usage. We did not actually intend the wireless network to support -- well, there was no WiFi based wireless voice products available during the lifetime of the solution. Cisco released the first WiFi, our first WiFi handset, the 7920 WiFi handset, we deployed these in a small number of users. I remember that, yes. Because there are some people whom this device is a perfect fit for and there are other people who are perfectly happy with their cell phone or perfectly happy with their desk phone. However WiFi voice has its own challenges or its own requirements if you will. Voice traffic is much more susceptible to contention, you really need fast roaming as you move from access point to access point because if you introduce jitter it can negatively impact the voice quality. So there are certain aspects to designing a robust wireless network that supports wireless voice that you really have to take into consideration. But we were in a situation where we had not done so because we had designed our wireless LAN for data network. So we addressed that in an interim manner by configuring wireless specific SSIDs and wireless. I beg your pardon, voice specific wireless VLANs and SSID's. So we limit access to those SSID's and VLANs to the WiFi phones and we've implemented QoS, quality of service on those WiFi phones -- .SSID. Moving ahead in the future it's going to be a very interesting area of great growth and convergence. You're going to see the introduction of dual mode phones in the future, which act both as a cellular phone, so CDMA or GSN for example. But will also, when inside an enterprise, use the WiFi network, so it will register and act as a VoIP phone internally, but also act as a cellular phone externally. And you're going to see the introduction - well we just had very recently the formal ratification of 802.11e, the IEEE standard for a wireless clause. So we expect the adoption rate of WiFi voice to increase dramatically. We are building that assumption at a foundation level into our architecture for next-gen wireless LAN. We're

ensuring that we have sub 100 milliseconds, sub 120 milliseconds of roaming between our access points, fast layer 2 roaming. We're providing seamless roaming on layer 3, as people move from building to building. We're even going to provide wireless coverage on our campuses so as people move from building to building they can retain their session continuity. Very nice. So it's going to be an interesting time. Yeah, I'm looking for to that. Challenging but interesting. Speaking of challenging, there was a final question for customers, I think, who have not yet started building their wireless network. And that was what are some of the biggest challenges you face in supporting and managing this wireless network? So what are the biggest and major challenges we face in supporting and maintaining the wireless network? One challenge that we used to have was actually visibility of the wireless network itself. Prior to their introduction of tools like the wireless LAN solutions engine and WCS more recently, your wireless was effectively if you will, a big black cloud. It was out there, you didn't have any real time visualization of the network. You didn't know was happening at that -- well, you could go out and invest a significant amount of money on additional sensors or third party products but you didn't have any integrated or inherent ability to see what was happening in the network. To see the RF - Because wireless LANs are a dynamic environment they are susceptible if you will, to environmental constraints and environmental impacting events. So as I mentioned earlier the fact that the WiFi networks are unlicensed is one of its disadvantages. An aspect of that would be the rogue AP or someone next door turning on an AP that was using the same channel as one of your APs. Prior to the introduction of WLSE and WCS we only would gain visibility of those events by their impact on our users. By users complaining. There's a problem right there. Well, okay, we'd have to go out and investigate. We'd either have to send someone to physically go to that location with a scanning tool and look around the environment and -- actually we would probably do that as a second step. The first step was to log onto the access points, have a look around and check the logs. It was a time consuming event and it was a challenging event because your support engineers had to be, to be honest, quite skilled in the wireless domain. They had to know exactly what they were doing. And that challenge has been mitigated, we've addressed that with these tools. I'm very excited by the next-gen wireless LAN, the centralized wireless LAN solution, that's really going to give me the opportunity to, on one hand increase the services I am providing, location based services, visualization, integrated wireless intrusion detection, integrated wireless attack signature detection. There are a load of benefits there: automated AP configuration, radio resource management, which allows the APs to self -- to fine tune and to detect any environmental impact and configure themselves to address those. There are loads of benefits there that I can provide and I'm going to be able to reduce my operation overhead, my support staff. So it's a win-win situation for me. My wireless network is going to get more complex, more robust and more feature rich, but it's going to be easier for me to actually maintain. That's amazing. Another challenge, and I'll finish up with this one, another challenge that is often overlooked, it's one of the hidden challenges of wireless networks, is client management. WiFi support or enablement is becoming prevalent. You're getting phones that support WiFi now. PDAs that support WiFi, your laptops obviously and you can buy small SD cards and CompactFlash WiFi cards, USB cards that support WiFi. So you're getting these -- your WiFi printers on more wireless print servers, you can get wireless data projectors. The number of wireless devices is exploding. In other words what's happening is wireless networks have been treated no differently - than the network, it's just a different transfer medium. However wireless networks have unique characteristics, by definition they have an SSID, they have a security standard that you must comply with. If you have a wireless network that requires the use of WPA for data encryption the devices must support WPA otherwise they won't get onto the network. So there are characteristics that you must configure for every single client device. Now in the area of laptops that may not necessarily be as big a challenge because you can use common tools. You can use centralized client management tools. But in an environment like Cisco's where we have a mixture of Windows laptops, we have a mixture of Linux laptops, we have a mixture of Macintosh, we have PDAs, we have different hardware platforms, we have cell phones, we have 7920 phones, putting together a framework to support all of these -- if I make a change to my security posture, if I change my SSID I really want to avoid having to go out and manually reconfigure 55,000 devices that are spread over a hundred countries. or 100,000- Or 100,000 that is going to be, so that is a challenge, no one is going to avoid that. You can address those by having a standardized client application, if possible, across all of your laptops and you can have a clearly defined procedure for client management. Have a centralized, what I call a solution or service gateway or dashboards or you can have an internal web page where all your users can go to for FAQs, frequently asked questions, tech sheets, tips and tricks. And one place they can go to, to get the latest software, one place they can go to, to get the latest firmware. Make sure your staff is WiFi, not enabled, but WiFi savvy, it's just one of the challenges you have to address. It can be addressed but you just have to put some thought into it. The more complex your environment, the more preparation you have to put into client management and

it's one thing that is sometimes overlooked in the initial planning stages. Makes sense. Okay, well that's about all the time we have today but I did want to say thank you very, very much for coming and for sharing all of your time and attention.

MORE WIRELESS LAN RESOURCES

My pleasure. Now I wanted to let you know that there is a way that you out there can get more information about Cisco IT deployments. You can go to the Cisco IT at work Web site. And there you can find some Cisco IT case studies about what we deploy, what benefits we've gained internally, what lessons we've learned from using these technologies. And also there are some operational practices and presentations to help you learn more. You can also find some more information on other wireless technologies, some design guides, operational practices, other documents, presentations, white papers on cisco.com at the URL just below that. Below that you'll see a toll free number that you can call for more information or to place an order and you can also order some Cisco resources on the Web from the URL found at very bottom of that page.

THANK YOU FOR WATCHING

Okay, that's about it. I'd like to thank all of you out there for watching and for spending time with us and for being interested in what the global technology seminar series is all about. We hope that you've really enjoyed this show and that it has helped answer some of your questions about wireless LANs. And also I wanted to thank you, Oisin, for spending all this time with us. My pleasure Rich. We really appreciate it. My pleasure. It's been interesting and very educational I hope for all of you and certainly for me. Thank you. It is my pleasure and I'm very excited about this technology. I believe in it, I think it offers enterprises a huge degree, a huge amount of potential value. I hope you've enjoyed the show. I hope I've convinced you and excited you about some of the technology too and I hope to see you soon. Thank you.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C78-337394-00 02/06