

13 WLAN 1

Hello and welcome to this “Cisco on Cisco” seminar on the wireless LANs. I'm Rich Gore, a manager of the Cisco at work team. A part of Cisco IT's Cisco on Cisco initiative. The theme of our show today is wireless LANs at Cisco, an overview of Cisco IT's current deployment of wireless LANs. And also our future plans for our next generation wireless LANs here at Cisco. You'll also get a chance to hear how Cisco IT maintains security on our wireless LAN. Now it's my real pleasure to introduce the star of today show, Oisín Mac Alasdair, who is the IT program manager responsible for global wireless strategy and architecture. Oisín has been with Cisco for five years and was responsible for the original deployment of our global wireless network. His team is now concentrating on the next generation of wireless networking solutions for use by Cisco across the globe. Oisín Thanks for coming today. Thank you Rich, it's a pleasure to be here and to be able to present our wireless LAN work, activity and our plans for the future. So please sit back and enjoy as we explore Cisco IT's past, present and future of wireless networking. Let's look at the agenda for today's presentation.

AGENDA

So I'm going to start with an overview of our current wireless network. And also then delve deeper into our future plans and our strategy for the next generation wireless networking. Then I'm going to talk about the wireless LAN benefits, the studies that we have done internally to see what's the real business benefit and value of wireless networks? And what value have we accrued ourselves? And then I'm going to talk about some basic best practices, about securing wireless networks, that you should take into consideration your selves when proceeding and deploying. And we'll finish off with some questions and answers, time permitting. Sounds good?

ENTERPRISE WIRELESS AT CISCO

So the wireless network that we have at Cisco today, it's approximately 3100 access points. The majority of them, about 75% of them, are the AP 350 and about 25% are the new 1200 series. How long have we had this? It seems like it's been forever since we've had wireless. We actually deployed the original network, the one we have today, five years ago. Okay. So we were one of the real early adopters of this technology, as would be expected, because it's an important technology and solution family for us. There are wireless networks, or one global wireless network if you will. It's deployed in 350 sites, actually more than 350 sites now, in like 95 countries around the globe. We opted to go with the ubiquitous coverage and comprehensive entitlement. So that effectively means you would put wireless in every single Cisco office around the globe. And every single Cisco employee and user has a wireless enabled laptop or device. So that brings us to 50,000 users, but in actual fact we have more than that. We have 55,000 wireless clients. The reason for the difference there is several users have additional laptops. We have just under 2000 Cisco 7920 wireless WiFi VoIP handsets, voiceover IP handsets, telephones and approximately 3000 PDAs with plans for rapid expansion in that area in the future. Yes, since we're rolling out a lot more PDAs I expect that usage to go up pretty significantly. I fully expect our wireless clients to number over 100,000 within the next 18 months, 12 to 18 months.

ENTERPRISE WIRELESS AT CISCO

For our AAA architecture and we use this Cisco access controls, or the ACS. And these are scattered at 13 different hub sites around the globe for a globally distributed AAA architecture. We use the Cisco Building Broadband Services Manager, or the BBSM, for guest networking. It provides against networking access portal for us. And just by the way of example, our support overhead isn't really that high for such a complex and robust system. We have approximately a thousand calls on average per month, which when you calculate that out and do the math for 55,000 users, it's about .24, about a quarter of a call per user per annum. Which when you look at the support costs is

only about, just under \$15 per year per user. So what kind of calls do people usually have when they have problems with wireless? Well the vast majority of the calls are in configuration challenges, perhaps users have. And some users have problems logging on when maybe their passwords have expired. Oh, okay. We do have quite a few users who may have been PTO or may have been away from the office for quite some time. And they come in and they try to use their cache credentials and it's just a case of resetting their password or telling them to update their system. Okay. And the vast majority of the calls, by example, like 97, just under 97% of our calls are actually handled and solved by a tier 1 support. So our Global Technical Research Center, GTRC, is able to solve the vast majority of the calls. And only less than 5% are escalated to tier 2 and tier 3 support. Good to know.

CURRENT WLAN ARCHITECTURE TOPOLOGY

What we have here is a high level schematic, a topology of the wireless network. We can see in the top left hand corner there the typical campus building, the access points themselves are connected to access layer switches. And the building core distribution layer is connected via the campus network back to the data center, where we use an internally developed management solution called EMAN, or Enterprise Management Deployed Management Services. And that the Cisco remote offices, the same kind of model. The APs are connected to the access layer switcher switch and are routed straight across the WAN back to the data center.

CONSOLE AND PRODUCTION NETWORK – A/P CONNECTIVITY

When we look at the access points themselves, well they're actually cabled in two -- we've cabled every access point with two cables. The Ethernet cable for the production network connected to an access layer switch. And then we have also actually cabled every individual access point with console access. So that's to provide outer band management capabilities for our technical support staff or our tier 2 and tier 3 network engineers are able to provide diagnostics and troubleshooting and actually access the actual access point, the AP it's self, even if there are problems on the production data network. So there are two cables for every access point in the ceilings of the buildings? In every single ceiling and in some cases in Europe and in Asia-Pacific area we have some access points mounted onto walls. But yes, two cables per access point. Now mind you as we move forward into the next generation network with the advantages offered by the centralized wireless LAN solution, the need to actually provide outer band management capabilities for the access points themselves is addressed. And we will be probably cabling every access point with only a single cable us to move forward. Okay.

SSID ARCHITECTURE

From an SSID perspective or the wireless VLAN perspective, we have SSIDs that are broadcast on every single access point. Or let me qualify that statement. We don't broadcast every SSID, but we broadcast the guest wireless networking and SSID. So then we have a separate SSID, a separate VLAN for our production data users and we have a separate VLAN and SSID for our production wireless voice services. And you can see at the bottom of the diagram here we have icons designating our wireless voice, our production data users and in the right hand side, a non Cisco guest user. And those users can associate to the guest SSID, which has open authentication and no encryption and broadcast it. They can associate to that SSID without end difficulties. But the production SSIDs, both voice and data, are encrypted and using WPA and EAP-Fast authentication, for authentication. I'll go into these concepts a bit more, in a bit more detail in the security section later on. For the guest wireless networking solution, here you can see how we've architected the global solution.

GUEST WIRELESS NETWORKING

You can see at the bottom of the page or the slides here we have two networks if you will, the production network and the guest network. Of course this is a single access point that's providing this capability. The guest -- and we also have developed internally a management portal if you will, that enables our Cisco staff to provision access codes for our guest users. This has removed the administrative burden from our administrative staff and our lobby ambassadors and support staff. Now it is up to the host of a visitor to provide the access code and to provide that support and capability for that user as they arrive. Okay. So as we can see from this diagram what happens initially is the employee configures an access code or actually they go onto our hotspot.Cisco.com, our Web

GUEST WIRELESS NETWORKING

portal, internally on our intranet web pages, and they configure a visit if you will for this visitor. And the hotspot.cisco.com server then provisions an access code on the BBSM, which is sitting out on the ... Subsequently the guest user then launches their Web browser and their traffic is intercepted and tunneled over a GRE tunnel to the BBSM.

GUEST WIRELESS NETWORKING

The BBSM then presents the user with a welcome page.

GUEST WIRELESS NETWORKING

And the user enters a guest access token and the BBSM then validates that user and then the actual traffic is routed around to the Internet.

GUEST WIRELESS NETWORKING

So it's completely seamless from the end user's perspective. It provides us with an ability to secure our internal network and also provides our visitors with a, zero cost obviously, but an amenity. And that gives them the opportunity to browse the Internet in a secure manner while it's protecting us. Seems like a lot of work to go through to build a completely separate network for guests to access the Internet from Cisco. What's the driving purpose behind that? Well the benefit of this solution is that we're reusing existing infrastructure. Oh, okay. The only addition to our core infrastructure is the actual BBSM, which handles the actual authentication. And the hotspot. Cisco site, which is running on internal web servers in any case. Oh, okay. So we're leveraging, we're providing greatly enhanced services for our users while it's leveraging the existing infrastructure. Nice, okay.

SNAPSHOT – THE PAST, PRESENT AND FUTURE

The slide here offers the viewers a snapshot of the present, the past and the future. Where did we come from? Where are we today? And where are we going in the future? So I'll leave this slide as a reference point, if our viewers what to download the slides and go through the actual categories. We talk about our infrastructure, security, our management platform, the clients. As you can see here we started off with 34,000 clients, we're up to 50,000 today and we expect it to radically increase in the future. Enhanced services, we started with no enhanced services. It was a basic wireless only data conductivity network initially. Today we offer guest wireless LAN networking and Voice over IP, FireWireless networking and in the future, with the nex-gen wireless LAN we're going to have significantly enhanced or additional enhanced services. And our SLA, or our service level agreement is increasing. Initially it was what we call a P4 service or a 48 hour fix, today it's still a P4, but it's treated as a P2, because our users have come to expect so much from the wireless LAN that we actually respond well within our SLA. To our future direction that is to designate it a P2 or P1 service, effectively a business critical service. And the aim is to make our -- to design our wireless LANs such that it's suitable as a primary access medium. And our capabilities are evolving as we proceed. That's impressive. Actually the SLA part seems to be the most impressive. We're upping the hardware. We're upping the complexity of the network. We're upping the security of the network. And it's really because we're moving from a priority 4, a small -- well tell us about that. What's changing within Cisco that's causing us to move from a P4, priority 4 lower level, to a P1 pretty critical level wireless network? So the primary difference, the main difference is the evolving capabilities of the solutions themselves. Okay. In the past we had no real visibility into what we call the RF or radio frequency domain. We had no wireless specific management capabilities. Now, with the introduction of the availability of the wireless LAN solutions and WLSE and also the wireless control system -- both are wireless specific management appliances that provide wireless specific or vertically specific capabilities for you to manage that wireless domain. Also some of the advantages inherent in the new centralized wireless LAN solution, which I'll go into in a moment, it gives you that degree of intelligence. The system is able to fine tune or self tune itself. It's able to detect interference and correct itself on the fly. No longer does it require an alert to be generated on the network and you need to go in and explicitly do some troubleshooting. The network is actually intelligent. It's constantly monitoring its environment. It's constantly fine tuning itself. It's even configuring itself. So the intelligence, the ability of the network to manage itself has increased dramatically. And with it, in tandem with that then, is our trust or our ability to rely

upon that network. No longer is it a secondary overlay network. It's actually a core -- it's a foundational technology first. We are truly enabling technology for our increasingly mobile workforce. Yes, I know for myself and for a lot of folks it's become the network that we use. We hardly ever plug in anymore. So it's gone from a toy to our primary network. Absolutely and I've got some interesting statistics on that later. Interesting, okay.

THE FUTURE – NEXGEN WLAN

So where are we going in the future? Well what we want to adopt a Cisco's unified wireless network. This is a combined solutions and family of two different categories or architectures of wireless networks if you will. We have the centralized wireless LAN solution, which is based upon LWAPP access points. And we have the distributed wireless LAN solution, which is based upon autonomous Cisco IOS access points. LWAPP being the lightweight access point protocol. We will be migrating to a dual band AG network and the existing network is, for historical reasons, based primarily on the 802.11b only standard. So with our new access points that we're deploying we'll be migrating to the AG network and with that, therefore, we have the capability of providing greatly increased bandwidth for our users. We're going to increase the number of access points. We're actually probably going to double the number of access points dramatically. So the actual user to AP ratio will decrease significantly. So that again, coupled with the increase of available bandwidth per access points, actually provides the user with a lot more potential bandwidth for their use. And we're providing a whole raft of new enhanced services. I like the sound of all of that stuff. Well we're going to get enhanced wireless LAN management, I mentioned that earlier, with the wireless LAN solutions engine and the wireless control system. We're going to get a wireless intrusion detection system, a wireless RDF and a wireless IP as a prevention system, which the wireless LAN will be able to actually actively monitor the airwaves and alert if it detects rogue APs. Not only rogue APs, but typical signature based attacks. It will be able to report on people who are trying to hack into the APs themselves. Nice. We'll also be supporting location based services, which will allow us to track high value assets with WiFi based asset tags. And we're also going to look at providing outdoor coverage between the buildings and campus sites. Obviously this is usually only probably when you have a large campus, but San Jose and Rye Technology Park in North Carolina. In London we have several layers where we actually have campuses. And we're opening a brand new large major investment in a large campus in India in the coming months and years. So we'll be providing wireless coverage between the buildings in the outdoor. Now this will be seamlessly integrated with our internal network. It will be secured by the same strong robust security controls standards and policies. But it would provide seamless roaming as our users move from building to building. Because one of the -- Which we do a lot of, yes. Which you do in the campus a lot. You may be out of voice call with your 7920 phone and as you walk from one building to another you'll be able to maintain that session integrity and keep your voice ... Sweet. And of course with that then would be, as I just said, an improved wireless voice on voice support. It's going into how we actually went about doing this or how we're actually in the process of doing this I should say.

NEXGEN WLAN METHODOLOGY

We're in the planning stages now. We just ratified our architecture. And that we launched our product sites and we're going to start doing our -- our deployment is probably early in 2006. Okay. So we went about it by categorizing the Cisco sites. As I mentioned earlier, we have over 350 buildings or sites around the globe with Cisco wireless LANs in them already. So we needed to decide, well, the architecture for a large campus site, at a fundamental level, would be similar to one at a small site. But there'll be some changes and some specifics to it. So we ended up with six different site categories. And they were based upon the number of access points in the site and the number of users who are resident in that building. Okay. Then we applied the next-gen wireless on architecture properly to that building to the site. We doubled the number of access points. We deployed a wireless LAN management tool as a property to the architecture. So that's the wireless LAN solutions engine and the wireless control system. And we integrate both of those tools with our existing enterprise management tools. And finally we integrate with the existing network security tools. So our wireless intrusion detection system will be integrated with the CS MARS -- tool set that our information security team used to manage and report in a sense. Okay, so you're going to walk us through some of those different architectures, for each one of the different types of sites? I'll give a highly overview over the architectures in the following slides.

CAMPUS SITES

Okay. Here we have a look at the campus sites. Now it's a centralized wireless LAN solution, so it's based upon wireless LAN controllers and LWAPP access points. There are a variable number of access points. The building, usually over a hundred, we have some buildings that will probably have about a hundred access points per building. Some of these larger buildings we have in some other campuses might have 110, 120. Several buildings will be organized into clusters. And each cluster will in turn be served or controlled by dual Catalyst 6Ks with WiSMs or wireless service modules, in a fully redundant manner. So we'll have to Cat 6Ks with two or more wireless service modules in the Cat 6K, so we'll have full resilience and full redundancy. And then what we've got to do, because of these size of, say for example, San Jose we have over 50 billion in this campus alone. There's going to be multiple clusters per mobility group. Now a mobility group allows you to roam seamlessly between all the buildings and access points in that construct. Right. And management will be provided by the wireless control system. I've just got a little sort of drill down here.

CAMPUS SITES

You can see that the access points themselves will be connected to access layer switches, which are in turn connected to the distribution layer. And that of several buildings are in turn connected to the cluster gateway. And at the cluster gateway is where our wireless LAN controllers will reside providing wireless LAN aggregation and control services. Now you mentioned about a hundred access points per building and in San Jose the buildings are four stories usually. Four to five stories. So 20 to 25 access points per floor? That's correct. So what we've done is we've decided to actually base our number of our access points on a sweet spot if you will of how many users do we want to be using a single access point at any one time. Okay. Initially it when we deployed our wireless LAN five years ago we decided to go for a user to AP ratio of 25:1, which is perfectly acceptable. And to be honest didn't really present us with any problems even up to today. But as we move forward, as people's adoption of wireless increases, as their reliance upon that technology and as their mobility changes. The people's working environment has evolved. True. And you want to make sure your network is more stable and is more robust, is providing the business ready on demand enterprise class solution.. So I'm increasing the number of access points, or an alternative way of looking at that is, I'm decreasing the user to AP ratio. And our target is around about 14 users, a maximum of 14 users to one access point. Okay. This does have an interesting characteristic of having variable size cells, but it will be handled automatically by the centralized wireless LAN solution as it self tunes and effectively fine tunes the RF signature of every building to that particular environment. How interesting. So it reduces our deployment cost as well. If we've have the meeting to large field sales offices, they'll also be utilizing the centralized wireless solution.

MEDIUM TO LARGE FIELD SALES OFFICES

And these offices can have anywhere between five to just under a hundred access points. There are four subcategories really in this area. And in this model we'll be using dual wireless LAN controller appliances. Okay. So the 4402 series or the 4404. And wireless LAN controllers, two again, at every site of our -- for like full resilience in case one of the controllers fails. And then management, again, would be provided by their wireless control service. Finally, at the very small field sales offices we're going to retain the distributed wireless LAN solution.

SMALL FIELD SALES OFFICES

These are offices with only two to four access points, a handful of staff. These will retain Cisco IOS, so the autonomous access point model, there won't be a local wireless LAN controller. However there will be an access point that's providing dedicated wireless domain services, which is a capability to provide enhanced wireless LAN management via the wireless LAN solution engine. So in the following slide you should see a table that summarizes this information.

SITE CATEGORIES SUMMARY

And you can see the different categories of sites we have. We have five different categories or types of sites that will have a centralized wireless LAN solution. And we have our sixth category, which will retain IOS. Now in the future we fully expect to migrate those sites to LWAPP as well. But at the moment, and with our schedule, we're going to concentrate on the type 1, type 2, 3 and 4, 5 sites initially. Management is provided by WCS in the centralized solution and you can see WLSE will be retained for management in the IOS, for the autonomous IOS access points. Okay. And you can see there in the controller assignment, the type 1, the campus sites, these are the sites that -- the large sites that we have in San Jose or ... and scattered around the globe. They will be using multiple WiSMs, the wireless service module, the Cat 6K blade. And the type 2 sites, which are the large field sales offices with upwards of a hundred, just under a hundred APs, we'll use dual 4404s. And then the type 3, 4 and 5 sites will use various different models or versions of the 4402, which comes in a model that supports the 12 access points, 25 access points and 50 access points. Perfect. This is also a much more cost effective way of us providing that wireless LAN controller architecture. We don't have to put the expensive, most expensive wireless controllers at sites. We can scale our equipment to the relevant size of the office. This slide is, if you like, a one slide snapshot of the architecture of our next-gen wireless LAN architecture.

NEXGEN WLAN ARCHITECTURE

If we start in the top right hand corner and go through these boxes one by one you can see that the campus buildings, whether they are in San Jose or RTP, Bangalore, will have high-density web-based access points. And if you step down to this next box you'll see that we're pointing out that those wireless LAN access points will be controlled by dual wireless LAN controllers, that will be adjacent or a site closer -- close to gateways. Wireless LAN solution engines, a WLSE, will continue to provide wireless LAN management services to the small FSO sites that we talk about in the bottom right hand corner. Those small sites are going to retain IOS. If we draw our attention to the bottom left of the slide where, I'm pointing at the remote offices or the field sales offices, those will have dual redundant appliance based wireless LAN controllers. And then back upward, we move back up to talking about the data centers. And location based services will be provided by deeply 700 series location server and wireless LAN management specific to the centralized solution will be provided by the WCS. Maybe I haven't discussed that in sufficient detail. Not only does the WCS provide us with enhanced management capabilities, but this is the tool that also provides us with automated rogue AP detection. It also gives us real time information about our device and client and location. It can give us heat maps or visualization of our RF domain. It's a very, very powerful tool, a companion tool. Nice. And then you'll see at the top left hand corner we talk about the outdoor mesh wireless LAN facility. I was going to ask you about that. That's the first time I've seen mesh networking. And I wanted to ask about that. That's just been announced actually. It's a brand-new product that we're launching and we're very, very excited about it. The ease of deployment is remarkable. It's an outdoor mesh solution. It will provide - - will blanket wireless coverage of our campus environments with the same architecture. It's very easy to deploy and manage. We use the same management structure, the same WCS, they're effectively identical LWAPP access points. From my management perspective it's an extremely easy solution to deploy and manage, yet the value proposition is extremely high. So the basic idea behind that is you have to cable them for power, but you don't have to have Ethernet cables going into them. That's correct, yes, yes. Because they pull their information and signal from the next nearest access point. These access points with two radios in them. They have a 5 GHz or 802.11a radio that will be used for wireless backhaul. And then they have an 802.11b or g, 2.4 GHz radio that will provide local access around that. Interesting. They self discover, build up a mesh, grab -- at the edge of your mesh you have one or two access points that are connected into your wired infrastructure to provide access back to the wireless LAN controllers. So why don't we do that everywhere? It sounds like it would be easier to deploy them without having to run cable in the ceilings and stuff. Because it's an outdoor solution. Oh, okay. The possibility of indoor mesh networking, that's something that the industry as a whole is looking at. There are no products to provide that kind of service at the moment. Okay. So that's our wireless LAN, past, present and future in a nutshell.

WLAN BENEFITS

Now let's think about the benefits. Why did we do and why are we continuing to invest a lot of money in proceeding with this service?

WLAN BENEFITS

Good questions. Well the first thing is when we looked at our users and we queried our users, we surveyed our users, about 18 months after the initial employment. We found that it was a lot more successful than we had even hoped ourselves. We had originally planned it to be a secondary network used intermittently for data usage. Well we found that 97% of our users surveyed said that they used the wireless on a regular basis. And 27%, just over 25%, said they use it as a primary access network, network access method. I think that's increasing too. I've seen a lot more people -- And we fully expect that number to increase in the future as well as we add further robustness and stability and security to the network. We find our users really appreciate it being untethered from their desks. And Cisco is a, not only Cisco, but most more modern enterprises -- workers are becoming more mobile. We have a workforce that is provided with laptops, PDAs, cell phones. It's no longer the case where you sit at your desk and you do your work at nine to five and then you leave. You do your work on the move if you like. Your work follows you as you move around. Sure. And what was the missing piece of that jigsaw puzzle was access to the network. You always had to go back to your desk and -- Plug in someplace, yes. The wireless LAN, the analogy I use which is, wireless LANs are like to networking what cell phones were to IP telephony. If we think about 10, 15 years ago when your mobile users were on the road they would always have to dial back into their corporate telephone systems to check their voicemail. They didn't have access. There was no on-demand telephony. They're at pay phones. That was it. Pay phones, exactly, on the road. And then with the advent of mobile phones suddenly everyone's productivity increased because they no longer had to waste time looking for phones. And they were always contactable. Yes. Wireless networks are conceptually identical from a data networking perspective. No longer do users have to run around searching for data ports or --. A place to plug, yes. They're constantly online. You walk into a Cisco office or even you walk into a Cisco campus, you're on our net. If you've got the right credentials and you authenticate yourself you're on our wireless network. You're on your network here. We have provided on demand business ready enterprise class connectivity. Yes. It's all about the network. What we also found, interestingly, was that by providing a global deployment with comprehensive entitlement and ubiquitous coverage you actually reduced the risk of rogue deployments. Because users no longer were motivated to install their own APs any longer. There was no point for groups who may have had the best of intentions deploying a little workgroup wireless LAN solution. Well that's no longer required, because we have a ubiquitous enterprise service for them. And the ability to detect any rogue APs that are still deployed anyway, now that we have that coverage. And it's obviously providing increased productivity by providing the on-demand access to the network, as I mentioned. I think the thing too is that it has increased the flexibility of people's work styles.

WLAN PRODUCTIVITY BENEFITS

And in fact WPR workplace resources folks have found that it increases their flexibility in terms of designing work environments, places where people work. Just because people are no longer tethered to the nearest Ethernet port. Exactly. You can move. You've got a whole new vista of opportunities or options in configuring your workplace, designing your workplace. No longer do you have to do the long row of cubes. You can go for an open plan, open kind of approach entirely, because you're not tied to a structured cabling system any longer. Yes. Now it should be noted that we're not suggesting that we're wireless only, because you may still need cabling for your IP telephony. And we also still recommend that people have at least one wired port, so it's available if they want to do very, very bandwidth intensive activity or the likes of that. But on the day to day activity 25% is their only primary -- as I said they only use the wireless and indeed we expect that number to increase. True for me, yes. So one of the major questions we ask ourselves is, well, we know it's a benefit, but how do I calculate the real cost? How do I estimate -- how is this affecting my bottom line? Everyone says it's useful. Everyone says it saves time. And it increases productivity -- yes. What does that actually mean? Well there are several ways we can do this. You can take a formal independent study, which is a costly exercise. Yes. Or you can rely upon an independent formal study. Or you can calculate savings yourselves in prudent estimate of your user activity. And we'll look at both of these activities or methodologies if you will in turn. Cisco actually commissioned NLP World to do a study of wireless LANs and their increase on productivity in 2001.

NOP STUDY – WIRELESS LANS INCREASE PRODUCTIVITY

And repeated the exercise in 2003. They surveyed over 300 US organizations, all with large, well medium or greater of wireless LANs, or I should say corporations, with more than a hundred employees. And their results were quite surprising. They actually found that users stayed connected or online three and half hours extra time per day. And of that, 90 minutes or one and a half hours of that was time saved. So that was an actual positive impact upon the productivity. When we look at the average salary of users reported in these companies.

NOP WORLD™ STUDY (2003)

That 3 1/2 hours, or that 1 1/2 hours of saved time, at an average salary of \$80,000 per annum that equated to a productivity benefit or a savings of \$14,000 per employee per annum. That's a pretty compelling story to date. However when we look at the come in the size of Cisco, with 50,000 wireless users, if we were just to take that basis and extrapolate it out and multiply it by 50,000 users. We'd end up with a figure of 700 million, which is probably on the aggressive side. So it's based upon a 100% adoption. Yes, little alarms are going off when I hear \$700 million. Certainly not; we're not arguing that case at all. What we've done in CIT and as I mentioned here, that 700 million, if you like, is a best case scenario.

CISCO IT APPROACH

It's like an ideal model. We've taken a more conservative approach in estimating the productivity benefits of the wireless LAN in our buildings, to our own corporation. And we'll go through the methodology there in a moment.

WLAN BENEFITS – PRODUCTIVITY ONE EXAMPLE OF CALCULATING THE VALUE OF DEPLOYING A WLAN

Okay. So the first approach is, you have to quantify the value of time. We know the wireless LAN saves you time. So if you want to know the benefit it provides by saving that time, you need to quantify the value of that time, if you will. So effectively it's important to us to find out how much a productive minute costs Cisco. Or how much a productive minute saves Cisco. So it's quite easy to do when you think about it. There's 230 workdays per year, over 90,000 work minutes per year, well, if you think about seven hours per day. And we use, within Cisco, for our costing exercises what we call an FTE, full time equivalent. We use a benchmark cost of \$120,000, \$120,000 per year. That's not to say we all get paid \$120,000 a year. Salary and benefits and -- The salary, the BPO costs, which includes your assets, your laptop, your cell phone. It includes the cost of lighting, water, insurance, business process costs, etc. So it's a cost that's a fully -- what we call a fully loaded cost, \$120,000 per year is our budgeting figure. So when we look at that, I mean think of the \$90,000 in productive minutes a year. We arrive at a figure of \$1.24. Per minute? Per minute. Okay. So if we estimate we save 10 minutes per day, which is a very conservative figure, remember NOP's independent study of over 300 companies said 90 minutes per day. But if we estimate at only 10 minutes a day, we still derive a productive benefit or a time saving that equates to over \$140 million a year in productive time. Impressive. Now for me, it's more than 10 minutes a day that I save using wireless. Absolutely. But what we want to do here is offer our executives and even our customers a conservative approach here. Fair enough. So even when we take that into consideration -- let's go one step further.

NORMALIZATION

Let's not be as aggressive, if you will, even though we were probably being conservative. Let's try to normalize that figure slightly. Now 140 odd million dollars is based on the assumption of 100% of those users. Every user saving that 10 minutes per day. And not everyone does. Yes. So let's be more conservative, let's say the users save 10 minutes of time per week. I don't think anyone's going to argue the case that you don't save 10 minutes a week with your wireless LAN. And in that case you're still saving \$28 million a year. That's huge. A huge benefit to the enterprise. Now this is time saved. So we're talking about time saved that is used productively. Okay so we're not talking about just generating \$28 million for you to add to your checking account or anything. This is how it's affecting the bottom line of the enterprise, if you will. Right.

FINANCIAL PRUDENCE

Let me go one step farther and we can introduce a degree of financial prudence. Once we believe that 10 minutes week provided \$28 million is pretty conservative, again, it's based upon 100% adoption, a hundred percent of your users saving 10 minutes per week. Well let's say if we even just say 50% of your users. So when we think about it, an enterprise that's got a global wireless network in every single office around the globe, every single employee has got a wireless enabled laptop, every single office they're in, their online and connected to a network. We're saying only half of those users save 10 minutes a week, we're still having a productivity benefit of \$14 million a year. And as I say here we believe that number is quite a bit above that 14 million. Wouldn't be as high as the \$700 million. Okay.

OR USE YOUR OWN FORMULA

So it's quite easy to do this. Use your own formula, try it yourself. Basically what you're doing is you're multiplying the cost of the employee minute by the extra minutes of productive time, not extra time online now, the time that they use productively, and multiply that by the number of years. On, beg your pardon, number of minutes per year. And that gives you that C, multiplied by N, multiplied by Y, gives you a value of P, the productivity benefit per employee. Then you multiply that by the total number of employees that you assume or predict are accruing that time saved. It's pretty simple math. So for people who don't use wireless on a day to day basis, where does this productive time -- where does this come from?

TEN MINUTES? WHAT TEN MINUTES?

Funny you should ask Rich. So those 10 minutes, what 10 minutes and where is it coming from? Okay. Well it's coming from time in meetings. It's coming from time spent at cafeterias or break areas where people are online. They bring their laptop with them, they do that extra bit of work, check their email when they're having their lunch. It comes from mobile workers. People who come in and people who are on the move, our support staff, our logistical staff, our workplace resources staff. And it comes from hot desking; the ability to come in and just find a desk. When you're visiting an office you don't have to -- you just walk in an open up your laptop and you're online. It's very, very easy to find 10 minutes of productive time a day. And it's not just costing.

ADDITIONAL CONSIDERATIONS – SOFT BENEFITS

There are more benefits than that. I think you approached that right here. Absolutely. Additional considerations, more than just the benefit of saved time if you will. I mentioned earlier we did a recent survey where 25% of our respondents said they used wireless LANs as their primary method of connecting to the network. Well I want to improve that. I want to double that. My target is 50% of my employees should be using the wireless LAN as their primary access medium. And we, again, prudently have said that if you're a primary access, primary wireless LAN user, you're probably saving 30 minutes a day by being connected onto a wireless network. This means we're adding an additional 20 minutes of time saving. We talked about the 10 minutes per day earlier. So I can get 50% of my employees saving an additional 20 minutes time productively, that's going to give me a positive productivity impact that's worth over 140 million bucks a year. You know what I see a lot in Cisco? Is people who take their laptops to meetings and a lot of us, we don't live in meetings exactly, but we spend a lot of time going to meetings. Absolutely. And it's the time waiting for meetings to start, it's the time after meetings have finished and it's also being able to have access to all the information -- The collaboration, the ability to collaborate. The ability to actually share information. The ability to gain access to information. Yes, exactly. If you like, its accessibility and its agility. It's the ability to respond quicker. It's an ability not to have to rush out of the meeting room to check something. Let me go and check the file server. Let me go and check my email. Let me go and check my voicemail. Or I'll look that up and then at our next meeting we'll be able to decide on this. We can make decisions, with information, right there. That's absolutely right. Yes. It's also not having to arm wrestle the other meeting attendants to fight for the one wired Ethernet port that's --. Or disconnect the overhead projector or IP phone, which is something you don't want to do. Some of the other benefits we're accruing is also the introduction of wireless VoIP, the 7920 WiFi handset that allows users to bring their phone extension with them as they roam around campus. And we're now providing, as I mentioned earlier, our visitors to ABC's and Cisco sites around the globe with guest wireless LAN networking. And finally, you mentioned this yourself earlier, which is the

workplace flexibility in design. It really allows us to be a lot more constructive or imaginative in how we actually design our offices. Yes, workplace resources have gone ahead and built a couple of buildings, one here on campus that I'm working in, that's designed to encourage and enhance collaboration. Encourage teamwork and people getting together at a moment's notice to make decisions and go off again and perform work and meet again and just to be able to work together fluidly and flexibly because we're not tethered. That's it exactly. Your wireless LAN is providing with that flexibility. It's providing, again, on demand network access, business class and enterprise ready on demand network access. The interesting option --. If you've got a prevalence of IP network, you have really enabled your workforce. Something, I remember, that the WPR people had told me is that in doing that, in creating that collaborative workplace they were able to put, what was it, 144 people into a space designed for 80. Because if you had to have cubes in that same space you could only put 80 people in there. The people working together, they work together very nicely without having to take up so much space. It's a more fluent working environment. Indeed.

ADDITIONAL CONSIDERATIONS – COSTS

So then, now that we know this, what about the costs? How much did this cost Cisco? It doesn't cost as much as you might think actually. It certainly costs a lot less than the benefits you accrue, even in the first year. But you shouldn't ignore the cost. There are additional considerations. Never take the positives without taking the negatives into account. So obviously there is a cost to the client, the client devices, the wireless cards. Or if you will, most laptops these days are coming with wireless built in. There's a small premium to be paid there. So you can ignore the cost of the wireless client device. There's a cost of managing the wireless network itself. We have engineers who are -- some of their time is spent managing the network and that's no different than any other service an IT organization provides. And there's you too. And there's me too. That's not that high a cost unfortunately. And there's the cost of securing the wireless network itself. So the lesson you have here is obviously just be financially prudent. Don't take the productive benefit in isolation, offset the productive benefit against the actual cost of deploying, supporting, maintaining and securing the network. And there's an alternative way of looking at this.

ALTERNATIVE WIRELESS LAN – PAY BACK – CALCULATOR

One way we can look at it is the wireless LAN payback calculator, if you will. So on one table we enumerate the actual cost of deploying the wireless network and we divide that by the number of users and get a cost. This is what this wireless network is costing per day per user. So you categorize, you total the cost of the infrastructure, the actual capital assets, then there's also depreciation charge, the cost of supporting this and the cost of securing it. And you come to a figure, you deploy, and then you divide that by the number of users. So you get a cost per user per day. So for Cisco IT, what does that cost per unit? We'll come to that in a moment. Okay. Then you also add up the employee costs, the cost per minute per employee. For us it's \$1.24 and you offset them together and see how many minutes must a user save to offset that cost per minute of actually providing the service if you will. Okay. Generally speaking, in our analysis with, and discussions with external companies, we found that to be one or two minutes per day. So if a user uses it for one or two minutes per day it's basically paid for itself. And those extra eight minutes a day -- Or 20 or 30 for me, yes. Or 30 minutes a day, that's just icing on top of the cake.

APPLYING THE CALCULATOR TO CISCO'S INTERNAL GLOBAL DEPLOYMENT

So if we look at our original deployment, and these are using real figures from a Cisco deployment, we have approximately costs of about \$.72 per user per minute, is what the wireless LAN has cost us. Which when you think about it might be a bit -- you might think, well, \$.72 a minute, that clock is ticking all the time. But the point is the users are saving 10 and 20, 30 more minutes a day. So the actual payback for our deployment is actually achieved in less than one productive minute per day. So \$.72 per day really is the cost to Cisco? Okay. Oh per day, yes, I beg your pardon, yes, yes, yes. Is the cost to Cisco, and the savings to Cisco is generally \$1.20 per. Yes, okay, impressive.

THANK YOU FOR WATCHING

Okay. Well that's about all that we have time for right now. We're going to take a quick break and we're going to get right back to you again with securing the wireless LAN here at Cisco. So hope to see you soon. What you'll need to do is you'll need to click on the next URL in line entitled something like Wireless LAN Security at Cisco and we'll be right back. 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

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)