Guest Networking

Guest Networking: Cisco on Cisco Technology Seminar

Julie Nordquist: Hello, and welcome to the Cisco on Cisco Seminar. I'm Julie Nordquist, Program Manager IT and part of the Cisco on Cisco team. Today's presentation is about how Cisco supports network connectivity for non-Cisco guest users at Cisco buildings worldwide. You will see how Cisco IT has developed an architecture and design that allows secure and reliable guest connectivity with minimal administration needs.

I'd like to introduce our technical expert for today's show on Cisco Guest Networking, Oisin MacAlasdair. Oisin is a Program Manager in the Network and Data Services organization in IT. He has been with Cisco for more than seven years and in addition to managing enterprise wireless strategy and architecture for Cisco IT, he also manages the next generation wireless network upgrade, which consists of the global deployment of more than 7,000 access points to Cisco offices. Welcome, Oisin.

Oisin MacAlasdair: Thank you. Thank you, Julie. It's great to be here. I'm excited about the opportunity to share details on Guest Networking at Cisco, and how this solution allows us to offer visitors the ability to access the internet in a secure and convenient manner, while also maintaining the security of our own internal network.

Julie Nordquist: So, sit back and enjoy as we explore Cisco Guest Networking. Let's take a look at the agenda for today's segment.

Agenda

Oisin MacAlasdair: Let me introduce today's agenda. I want to first describe our business objective of Guest Networking Services at Cisco. I'll then cover the architecture and design, then how we deploy the service. I'll then provide some details on adoption and the benefits it's brought Cisco. And I'll then cover finally the future, what the future holds for Guest Networking Services at Cisco.

Objectives & Constraints

Oisin MacAlasdair: The objectives and constraints that management set us were rather simple. We wanted to build a policy on an architecture that provided non-Cisco visitors with access to the internet. Now, we wanted to ensure that this was only possible where and when we, Cisco as an enterprise deemed appropriate. We wanted to ensure, that guest access to the internet only occurred with our permission, using our infrastructure in a secure, authenticated, and recorded manner and with minimal administrative burden or overhead.

What this effectively meant in plain English is we wanted to ensure that visitors to Cisco could have access to the internet. We didn't want to, our own IT staff to be burdened with having to provide them with technical support on a daily basis. And we also wanted to ensure that they use our existing network infrastructure. We didn't want to invite in third party hot spot providers for example.

And finally, from the secure and authenticated and recorded manner, that was to ensure that we not necessarily logged every individual and site that the visitor may visit, we just wanted to ensure that we had a record of the visitor's session, their ID, and the sponsor of that visitor. So, for IT forensic perspective we could also do analysis later if that was necessary for legal reasons.

Julie Nordquist: Oisin, I have a question for you actually --

Oisin MacAlasdair: Certainly --

Julie Nordquist: What did we do prior to this being deployed?

Oisin MacAlasdair: Well, prior to the Guest Networking Solution that we have in place today, it was completely done on an ad hoc basis. So, you would have guest arrive at Cisco. They would contact their sponsor. They would let the sponsor know and --

Julie Nordquist: Sponsor is a Cisco employee --

Oisin MacAlasdair: I beg your pardon I, yeah a sponsor is a Cisco employee who is the, who is effectively the responsible for the visitor. And the sponsor would then, would contact Cisco IT and say I've got a visitor from Acme Engineering that needs internet access and it's extremely important. And IT would have to react, what we used to call "diving catches." There would be, further, we would have to try to get access a particular building or a particular room on a temporary basis. It was a very, very ad hoc and uncontrolled process. And also, it was support intensive. So, there were several disadvantages.

The first disadvantage was it didn't really give a good feeling. You know the visitor came to Cisco, the networking company and we didn't have a system or proceduralized capability of guest access in place. It was costly for us as an IT organization. And it also left us with a security problem because quite often and you know auditing those old, or Legacy guest access setups, those ad hoc networks that had been created was difficult. Sometimes they were overlooked. So, it was really, it was handled in an uncontrolled manner let us say.

Julie Nordquist: So, there really was a need for putting this into a process.

Oisin MacAlasdair: Absolutely there was a need. There was a need to optimize from an IT perspective. There was a need to also protect us from a legal perspective. And now with our existing Guest Networking Solution, all our visitors have to sign a legal disclaimer before they get access to the internet. That's akin to your normal employees signing an employment contract. By definition, they have signed an "acceptable use" policy. But the visitor who visits your enterprise for a day or a contractor who is there for a week or a temp employee there who's only there maybe for a month, in many circumstances they have not necessarily signed a legal disclaimer. So, we have to not only secure our network from a security perspective, protect ourselves from a legal perspective and also streamline the process so we reduce the burden.

Julie Nordquist: Thank you.

Architecture highlights

Oisin MacAlasdair: You're welcome. So let's look at the architectural highlights of Guest Networking Solution in Cisco today. The first fundamental characteristic of the solution is that we have redundant policy enforcement points at each DMZ where internet access is provided to the visitor. Today, those are dual building broadband services managers. These are BBSMs. And in the near future as part of the Next Generation Wireless LAN Program, those are going to be replaced by NAC appliances. So, at seven locations scattered across the globe we have DMZ egress points or guest internet access. And at each, one of those locations there's a dual policy enforcement point. So, it's that piece of hardware where those, in fully redundant and configuration. That policy enforcement point is the actual piece of hardware that confirms that guest has permission or the access code that guest was provided with is a valid access code and has permission to access the internet. And we have, the solution is globally distributed so all internet access is not centralized at a single DMZ globally.

And we also, another probably defining characteristic of this solution is the internal web portals. This is probably the most powerful aspect of the Guest Networking Solution in Cisco. This is an internal web application that we have developed and is available on our own intranet and network that allows Cisco employees, the sponsor, the visitor sponsor to pre-provision an access code for their visitors. So, if you think about it and when you are responsible for a visitor to your enterprise or if you're a "visitor sponsor" as we call them at Cisco, you have certain responsibilities. You need to provide your visitor with a visitor badge. You need to let your visitor know where the restroom is, and now at Cisco you need to provide the visitor with a guess access code. It's become second nature to our employees. They will, all employees know that they go to this internet portal to provide an access code for their visitor. And they can do so in multiple and they can do a single access code or they can do multiple batch access codes.

Julie Nordquist: I just want to ask you, how did they find out about this service?

Oisin MacAlasdair: So, initially we undertook --

Julie Nordquist: I don't want to take you too much off the topic but --

Oisin MacAlasdair: No, no okay. Initially we undertook a global education and communication time for our employees. We produced posters that went up in the most common customer visited sites. We have what we call "customer briefing centers" and "technical briefing centers." We also produced pamphlets. But it's become so, the service has become so prevalent or is prevalent and users have become so used to it now that

they --

Julie Nordquist: Its part of your --

Oisin MacAlasdair: Proactive --

Julie Nordquist: *(Crosstalk)* --

Oisin MacAlasdair: Part of business. It's something that every Cisco employee now is aware of. And also, another important aspect of the solution of course, is the vast majority of Guest Networking Services in Cisco is provided by the wireless network. And that's provided through the provision of a, there's a dedicated SSID, which we call "GuestNet." And up till very recently and still most locations that GuestNet SSID has been broadcast. So, all employees are aware of it. And every employee's standard image laptop has, already comes with a profile to use the GuestNet. So, employees know it because its part of working at Cisco. They know about it because it's in there, configured in their laptop and they're aware of it because it's something that Cisco provides our visitors with internet access. So, its just part of the day-to-day activity of an employee --

Julie Nordquist: Right.

Oisin MacAlasdair: One who is responsible for visitors. The guest, as I mentioned the GuestNet SSID is available on all access points, so every single access point across the globe. This means that an employee or visitor can go into an office in London, in Singapore, San Jose, any city around the globe and the AP configuration, the SSID architecture will be identical, on one of the SSIDs on that access point, on all access points would be the GuestNet SSID. And so while the vast majority of Guest Networking is provided by the wireless LAN, we do have some, a limited need for wired guest access at some limited locations. These are primarily training rooms where we know, like large meeting rooms that are consistently set aside to train. We know that they tend to be fully booked seven, five days, maybe seven days a week in some circumstances. But, we have, constantly have a constantly changing stream of visitors coming in or trainees coming in and working in those particular rooms.

But the vast majority of Guest Networking is provided by the wireless network. It is important. It is a powerful characteristic of the architecture of the solution that the service that we implemented in Cisco supports both wireless and wired, 90%, 95% wireless activity, but we do have the capability to have support wired access. And that's like I said, training rooms and some limited ports in some of those technical briefing centers and executive briefing centers where we have high power visiting executives and customers come and sometimes they want to actually plug in their laptop. And some visitors don't actually have wireless enabled laptops. That's not as common as it was initially but you know we still encounter them occasionally.

Current wireless hotspot architecture

Oisin MacAlasdair: The diagram we see in front of us is a basic schematic, gives an idea of the solution. If you look at the bottom of the screen, we can see a representation of a typical building. There's two buildings, one on the left and one on the right. And the AP at the bottom you can see a red circle which designates the guest SSID and a green oval that designates the normal enterprise network. Both of those, you can see that the access point is presenting both SSIDs in that building. And if we follow just above the AP, you can see the switching or the router for that actual building. And it is at that point that there's a GRE tunnel from that building right, all the way up to the local, geographically appropriate DMZ where we have another router and this is the one we

call the “GuestNet head-in router.” So, the traffic from the GuestNet SSID is associated with a guest WLAN which is tunneled using policy based rating over the GRE tunnel out to the DMZ and from that head-in router it is, the traffic is sent to the actual policy enforcement point which at the moment is a BBSM or Building Broadband Services Manager. In the near future, it’s going to be a NAC appliance.

Julie Nordquist: Why would we retire the BBSM?

Oisin MacAlasdair: BBSM as a product has reached the end of its life. So it’s what we call EOL and the NAC appliance is also a more powerful device. It can scale to support many more multiple concurrent sessions. So, it’s a case of us adopting a next generation product. The BBSM has served us well in this, in providing this service for five years now and but the product has reached it’s, once it’s end of life, you know it’s incumbent upon us to adopt the latest product that can satisfy these services. And the NAC appliance is --

Julie Nordquist: That’s the Cisco NAC appliance --

Oisin MacAlasdair: That’s the Cisco NAC, it most certainly is the Cisco NAC appliance. It’s got a very, very you know good future ahead of it. It’s got feature roadmap and excellent support. Once the BBSM goes to end of life, you know the idea is you should move to a current product.

What we also see in the right hand side of the screen is the hotspot.cisco.com. So, that’s the internal web portal I referred to earlier. And it’s important to realize that all Cisco employees know that if I’ve got a visitor coming I just go to the web browser. They type in hotspot.cisco.com. That opens up the guest portal and they type in the IDs of their visitor. So it could be Joe Blog from Acme Engineering. He’s going to be visiting San Jose Building 12 on this 7th of May 2007. That will then pre-provision an access code on the policy enforcement point. Today it’s a BBSM. Tomorrow it’ll be a NAC hole. And in the future, it’ll be a NAC appliance. The user can also pre-provision a whole batch of access codes. So, where the sponsor are organizing an event or a training session and they had 20 or 30, or in some cases up to hundreds of visitors, you don’t have to individually type in every individual name. There is a facility to again, reduce the burden, the administrative burden on the end user, the Cisco end user. And every time you reduce the administrative burden you’re reducing your support cost, right, you’re increasing productivity.

Julie Nordquist: For the hotspot.cisco.com, was that an internally developed application?

Oisin MacAlasdair: Certainly was. Internally, what we did initially was we cut the line back. So, we realized we’d been assessed an objective by our senior executive leadership within Cisco. Let’s make Guest Networking available to employees, oh beg your pardon, to visitors, non-employees, but let’s do so in a secure manner and in a manner that doesn’t create a large degree of support work. In other words, we didn’t want to have a situation where our lobby ambassadors or administrative staff were longer having to create access codes for the thousands of guests, literally thousands of guests we have or visitors every month. So, we thought about how can we do this? And the logical step was well, let’s empower our employees to be responsible for this. The employees, as I mentioned earlier are already responsible for greeting, meeting and greeting the visitor, providing them with a visitor badge and letting them know the safety, fire safety and occupational health and safety issues within the building and telling them where the restroom is and where the break room is, so it’s just a logical step that they would also say and here is your access code should you wish to access the internet while you’re visiting our premises.

So, how do we empower our employees? Well, we decided let’s create

a web portal where the employee could go and create, print up an access code. So, we developed an internal application and it's a web services based application and it made sense to, well let's think of a name. What's going to be intuitive to our users? Well, "hotspot." At that stage, the vast majority and it continues to be the vast majority of guests networking tends to be wireless based, but it does support wire, which it's important to remember that. But, we said "hotspot.cisco.com." So, an employee goes to hotspot.cisco.com, enters in the details of the visitor. Obviously, so this is an internal website, they have to authenticate themselves. So, as a Cisco employee, I go to that website, it asks me for my, user ID and password. So, as employee it's kind of self-service. So you can't, I beg your pardon, a visitor cannot self-service, a visitor can't come in and get on the network and try to spoof and get themselves an access code. It's kind of, that's impossible. That you will, Cisco employee goes to hotspot.cisco.com, identifies himself as a valid employee, you know just like he logs onto the application if you will, creates the code or the multiple codes and that was a pre-provision to the policy enforcement point.

Indeed, this now proved to be so successful and so popular with our internal employees and our visitors that the business, that is the Cisco business sort of stood up and took note. And our Advance Services organization took the model and developed their own package service, which is now available to GuestNet Manager. It's a service that you can actually buy. As a customer, you can go to Advanced Services and say we want to adopt this service or a solution similar to your Guest Networking that you have in Cisco for our own environment. So, it's proven to be not only very successful internally for our purposes, for IT purposes, but also has proven so successful that it's, we've effectively converted it into or developed it into, not so much a product, but more of a service --

Julie Nordquist: Service --

Oisin MacAlasdair: A turnkey solution, if you will. And in some ways the wheel has turned full circle because now the Advanced Services solution is so polished and is actually, they had the resources, full time resources to develop a more robust and web services portal that we're actually going to retire our existing hotspot.cisco.com and adopt the Advanced Services version. So, it'll be totally transparent to the end user and it's just something that we have on our roadmap. But, so hotspot.cisco.com will stay, it's just the underlying code will be the Advanced Services version, which means that we'll be using what we're selling to our customers.

Julie Nordquist: Terrific.

Wireless SSID Architecture

Oisin MacAlasdair: I mentioned earlier the wireless access ID architecture. So, if we consider Cisco today has approximately 5,000 access points scattered across the globe. And we originally started with the previous Legacy Wireless LAN which was developed and deployed in 2000, developed as a _____ network and, a mobility enabler and we got to 2005 and decided to adopt the NextGen Wireless LAN program which we're in the process of implementing now, took about a year planning and designing. Prior to that design, was coming up with an updated wireless SSID architecture field. So, every single access point in the globe has an identical SSID set up. And so we have, to say, if you like it's the same wireless network and now rebuilding. So, I can go as I mentioned earlier, I go into a Cisco office in Johannesburg, London, Dublin, Sydney, Singapore, Tokyo, it doesn't matter where I go, I know that it'll have the same SSIDs, so I can use my enterprise profiles that are pre-configured in my Cisco laptop.

It also means that know that it'll be a GuestNet SSID available at that

office. So, at the access site, the SSIDs that we do present, we have two data SSIDs, if you will. They are one for Legacy devices and actually soon will be depleted, so that will soon be reduced to a single data SSID. We have a SSID set aside for wireless voice and both of those require authentication and actually the wireless voice SSID supports QoS, so it's optimized for wireless voice devices like the 7921 phone, the 7921 new wireless endpoint, WYFI endpoints, and phone that we recently released to the market and upcoming devices like the dual mode smart phones. But the one that we're interested in here is the actual fourth SSID, the GuestNet SSID. And that is open and north indication. So we tried to facilitate ease of use as much as possible. An end user doesn't need to mess around with security settings or any such nonsense for Guest Networking here. So, what the end user or the visitor in this case, it's an open SA. They can easily associate with this and typically, the bad SSID was actually broadcast. Historically we broadcast it out to everywhere.

And it's interesting we didn't encounter, uncover our problems without, within the last few months. So, where we actually encountered what we call IP address depletion. So, we had a certain sized address block for Guest Networking and what we found is when it was being broadcast some people, some people who may not have been necessarily looking for guest access, they didn't have an access code or even some users who had their laptops because it was broadcast or using Windows AR Config for example, the laptop was automatically associating to the GuestNet SSID and being assigned an IP address, right. But they didn't go to the next step to get authentication, but that still used up an IP address. So, we fine tuned the architecture a little bit recently where you still broadcast the SSID at the most common visitor locations, so at the enterprise briefing or the executive briefing centers, customer briefing centers, the TBC, the technical briefing centers, places where we expect and welcome most of our visitors-

Julie Nordquist: High volume of people --

Oisin MacAlasdair: High volume of people, exactly. But we disabled broadcast in the other sites. Now the only difference from user perspective is at those sites where there is no broadcast, the user just has to be told the SSID is GuestNet, type it in. So, it's one extra step. It's, you know but it doesn't really negatively affect usability too much for the, and those sites tend to be the sites that we don't have that many visitors. So, it'll be field offices or and you know offices that, field sales offices is probably the majority of the ones --

Julie Nordquist: And you have to give them an access ID anyway, so --

Oisin MacAlasdair: Oh, everyone has to have --

Julie Nordquist: So --

Oisin MacAlasdair: Everyone is provided with an access ID.

Julie Nordquist: So, at the same time you can provide them with the SSID.

Oisin MacAlasdair: Absolutely. Indeed when they're presented and we'll see this later, we have some screen shots and I'll go, I'll talk our way through the process, step-by-step-by-step, but our visitor is provided with, it's a "handout" for want of a better term. It's actually the sponsor is provided with the handout for the visitor. And that is presented in a PDF format. So the sponsor can actually email it to their visitor so they could say, well you know we know you're going to come to the office to meet me and some of my sales colleagues on Tuesday of next week. And they may email the PDF and the instructions beforehand or they could print the PDF out and actually hand it to the visitor as they welcome them to the premises. And then the handout has obviously the visitor's name and company

and their access code at the top. It has instructions, what you need to do to configure your laptop. And it also has a copy of the legal disclaimer. We'll see a copy of it, we'll see an example of it in a moment.

Julie Nordquist: Great.

Globally distributed guest networks

Oisin MacAlasdair: I mentioned earlier, about the globally distributed Guest Networks, so let me clarify what I mean there. It's a globally pervasive Guest Network. But what we have, what we're showing with this slide is the fact we've got eight DMZ or D-M-Z for you. And DMZs are internet egress points. So, this means that for example, if a guest were visiting someone in the Sydney office, we did not have to tunnel their guest internet traffic all the way over a wide area, a WAN to like say San Jose where our main internet pop is. It would be a poor utilization over a very, very expansive bandwidth, right. So, by ensuring that we have a globally distributed egress point, so we utilize some of the DMZs, pops that we have scattered around the globe, we do two things. We minimize non-essential global wide area traffic and large, fat internet pipes or WAN pipes that traverse the globe are expansive and we also ensure that there's an inherent degree of resiliency in it. So if you did experience a problem at a particular DMZ it doesn't knock off guest networking for the entire corporation, and indeed the same applies to internet access to the corporation for employees. So, by having a distributed solution, you optimize the location and the routing of traffic and you also ensure that you optimize your costs.

Julie Nordquist: Are there any disadvantages to having a globally distributed network?

Oisin MacAlasdair: Well, I suppose there are disadvantages to the fact that we have to have set, or an identical set of the actual head-in infrastructure, but that's really a negligible cost when you think of the advantages. So, we would have a two policy enforcement points, and a head-in router at each DMZ. So, yes there is a disadvantage whereas you have eight times the infrastructure, but that cost is rather low especially when we see the benefits of this --

Julie Nordquist: *(Crosstalk)*

Oisin MacAlasdair: Solution as created as an enterprise and especially when you consider the other advantages. That additional hardware is probably a lot cheaper than a menace of wide area networking traffic from Sydney to San Jose.

Julie Nordquist: What would, with the distributed network, what's the user experience like?

Oisin MacAlasdair: The user experience is even improved because again you're as susceptible to the lag that you may encounter as you traverse a global network. So, your internet access is almost like using a local ISP as opposed to UVPN, all the way over to this San Jose. I keep saying all the way over because I'm based in Sydney, so I'm making the assumption. But were I a visitor in Sydney, Australia and the only way I can get internet access or guest access was to traverse the global Cisco WAN and then out from San Jose pop, I'd much prefer to be able to just traverse to the local pop in Sydney. It'd be quicker and it'd be cheaper for Cisco as a company.

Baseline User Experience for Enterprise Guest Access

Oisin MacAlasdair : So, let's go through your baseline user experience for a guest access.

The first thing that happens is that a Cisco employee goes to the actual

hotspot.cisco.com. This is the web portal where they enter in the details of you know I know I've got a visitor coming to visit me or visit my colleague or if I'm a personal assistant or an executive assistant, maybe visit the vice president for whom I work with. And they will enter the details of the visitor. They'll enter the name, the company name, the time that the access, guest access is required. Typically, we do 7:00 a.m. to 7:00 p.m. on a 24-hour block, but you can drop it down to a single hour if you so wish. And you can expand it to seven days also. Seven days is the maximum time limit that we can set aside for each access code.

So the Cisco employee accesses the web portal, the hotspot.cisco.com in this case or you know authenticates themselves as a Cisco employee and enters the IDs of the actual, the visitor. One time an access code has been generated by this application and it is pre-provisioned on the appropriate, the geographically appropriate policy enforcement point. So were, I to go to hotspot.cisco.com when I was here in San Jose and I would say I have a visitor visiting me in Sydney in two weeks time. The application would realize I'm telling the application what building the visitor is going to be, so the application would then go provision that access code on the Sydney DMZ path. There's a bit of intelligence in there. And the guest user then would connect to, so the guest user comes to the actual building and is provided with the access code. And the handout is, either, emailed or is given a printed hard copy of the actual access code.

And the guest user then, normally what they would do is they would open up their web browser, it's exactly like what we experience, we all experience from being in an airport or in a hotel where you go to the internet first, you open up your web browser, it doesn't matter what web address you type in to your laptop, the HTTP session or the internet session is captured by some policy enforcement point. In this case, in our services the actual policy enforcement case, a proper DMZ, it captures your request, your internet traffic and presents you with a welcome page, "Welcome to High Speed Guest Internet Access at Cisco. Please enter your access code." The employee or, beg your pardon, the guest enters in their name, your access code and policy enforcement point, then checks is this a valid access code? Yes it is. It records the IP address. It records the name the person entered and then provides the internet access. It's as simple as that.

Julie Nordquist: What would you use the information that it gathers --

Oisin MacAlasdair: So we --

Julie Nordquist: Do you use it?

Oisin MacAlasdair: Well, we do. We record it. We don't record. We don't monitor internet traffic. We don't log any of the addresses that the guest goes to. The only records we keep are the IP address that is assigned to that guest, the access code, and therefore the name of that guest and the sponsor of that guest. And that allows us, perish the thought, should anything occur like if the user was susceptible to say had had a laptop that had a Trojan or a virus, or if the user did decide to undertake illegal behavior, we'd be able to, and we'd be notified later. So, the example I always use is if you had a guest that decided to try to hack the White House website for example. Very quickly after that attempt, you can be sure that you'll be contacted by the FBI because they'll track that IP address back to Cisco. So, we would say, okay well, we'll look at it and we'd say this 25th of May 2007, this IP address was associated with Joe Blog of Acme Engineering. And therefore, it's a case of IT forensics.

We just know, it's incumbent upon us from a legal perspective and from a security perspective, to be aware of how our infrastructure is used and how the infrastructure we provide an access to the internet is used. So,

it's a prudent approach towards legal liability and good neighborliness as well, if you will. But we don't monitor traffic and we don't block any traffic. We don't block any particular sites. We assume and we have a cultural trust within Cisco so those same rules apply to Cisco employees and they apply to our Cisco visitors as well. And now the user does have, or the employee, the visitor has to sign a --

Julie Nordquist: Acceptable use --

Oisin MacAlasdair: Acceptable use policy where they say they will refrain from any illegal or malicious behavior and so, we take that on good faith.

Julie Nordquist: Thank you.

Guest Usage Trends-Global

Oisin MacAlasdair: Let's talk about the actual usage trends or the actual adoption of this. And the success of it has been phenomenal basically. We consider the graph of it you can see it's a dramatic increase in the adoption and it continues to rise on a monthly basis. On average, we're handling 19,000 individual guest actions every month.

Julie Nordquist: Wow.

Oisin MacAlasdair: And that figure is rising. Every month when we do our uses statistics, we see that's, obviously it'll take out of some stages, there's only so many visitors come --

Julie Nordquist: Right --

Oisin MacAlasdair: Can come to visit, the visitors, but 19,000 per month. If we look back over the 12 months that's approximately 228,000, nearly a quarter of a million visitors that have utilized this service in the last year. And these are active sessions. These are not access codes that we generated and then haven't been used. That number is even greater. I don't report that number here. These are actually over 228,000 sessions where a Cisco visitor has utilized an access code to gain access to the internet. Sometimes though the access code may, and that doesn't necessarily mean it's only a one-hour or two-hour session. It could have been a two-day or three-day or perhaps in some circumstances even seven-day session.

When you consider this is also spread over 330 buildings, or actually at this stage now our network has expanded within the NextGen, of the next generation wireless laptop to just under 400 buildings across the globe and you can see the global distribution is it's extremely popular. The vast majority of the sessions do tend to be in San Jose simply because oh, I think nearly 30% to 40% of our employees are based in San Jose campus. So, the San Jose campus tends to be the place where many of our visitors come. And but it is globally distributed. So, we have visitors in every, say Tokyo, Singapore, well all major --

Julie Nordquist: Bangalore --

Oisin MacAlasdair: Sites around *(crosstalk)*, Bangalore, a major new campus, where we're making a new multimillion-dollar investment there. So the adoption has been very, very high. The interesting thing associated with this is the adoption has been very, very high but the actual benefits it brings to us have been dramatic, also.

Support Cost Analysis-FY 2007

Oisin MacAlasdair If we consider this, the past where every individual guest access request if it was handled properly required specific IT involvement or at the minimum it would have required a help desk or what we call it

"GTRC" call, a Global Technical Resource Center, so a help desk call. We cost every GTRC caller $25.00. That's how we estimate the cost of support for all our activity and we factor in the cost of the agent and the equipment itself. So, if you think of 228,000 sessions over the last 12 months, where each of those calls at the minimum, a single GTRC, let alone thinking of an IT engineer perhaps to go out and spend a few hours working on it, in which case the cost would be much higher than $25.00, but at a minimum a single call to help desk, 228,000 and we'll try once, that's over $5 million in administrative costs that we have successfully avoided by empowering our users and ensuring that those, that support person, that effort has been devolved to our employees.

Now interestingly, the employees love it. They feel empowered. They're feeling you know if we speak truly, they're probably like well thank goodness I don't have to go to IT to handle, for every little thing. Now they know they can handle this, themselves. They can provide their guests with internet access. They don't have to wait. You know in the previous service or the previous, prior to this service when we didn't have a proceduralized method, it was ad hoc, and sometimes, there's sometimes there have been delays. And now the service is instantaneous if you will. It's a self-service capability.

Julie Nordquist: It would have required planning --

Oisin MacAlasdair: It would have required planning --

Julie Nordquist: A lot of planning --

Oisin MacAlasdair: And remediation, and it would have had a --

Julie Nordquist: It's just not, wasn't even scalable --

Oisin MacAlasdair: Certainly wasn't scalable. And the measure of the success of this service is just the fact that we're handling 19,000 sessions per month. Now, if we consider, obviously things don't come for free, right. So, we look at the number of tech support calls the Guest Networking Service has cost or over the last 12 months, it's been less than 600. And if we also consider, well somebody has to write that application in the first place and someone has to configure those BBSMs or NAC appliance policy enforcement points, someone has to configure those and physically install them.

Julie Nordquist: And support them --

Oisin MacAlasdair: And support them. So, we've actually been very conservative when we said well let's assume that's one FTE or full time equivalent. Let's assume one person's job, full time for an entire year is to look after those, a, sixteen boxes, that's actually being over conservative. And though if we still factor in those costs, we're still saving, we're still accruing a cost avoidance benefit of over $5 million a year. Now, this may be pretty, this is pretty impressive at first, and analysis but it's not the least of the benefits.

Guest network benefits

Oisin MacAlasdair Not only have we accrued say a cost avoidance of $5 million dollars, but perhaps more importantly, slightly more intangible but actually more importantly in many ways is the actual improvement to our security. If you stop and think for a moment, this service has prevented 228,000 non-corporate and therefore completely, uncontrolled house, or laptops from accessing our network and with no protection, so we're providing them with internet access, but we're also protecting our own network. So, there have been circumstances where visitors' laptops have had viruses or Trojans and we've been, you know people have trafficked back to our address space and by knowing, we've been able to go to

the visitor and say, there's some suspicious behavior on your laptop and they've been very grateful. You know we've been able to tell them they had a virus or there was a Trojan or worm from their laptop, you know there have been a handful of circumstances. Happily, we've never had a malicious incident, but we certainly had a handful of incidents of infected house. And when you think of 228,000 over 12 months, you know even if 1% of those had a virus, that's still over 2,000 devices that you have successfully segmented from our network.

And we've experienced a dramatic improved turnaround as we talked about earlier. And it takes about approximately 15 seconds for an employee to create an access code. So the employee, Cisco employees are happier because they're empowered and they can provide, they have visitors with services that they're happy with. And the visitor sometimes, you know sometimes the visitor may not have an access code pre-provision to them, they will, the sponsor may not think that they will need internet access, but when they arrive on site and say, you know well I need VPM back to my office or I want to check my email. And the sponsor or any Cisco employee can say, okay I'll get you an access code, 15 seconds or less.

And it's also provided a sense, as I mentioned earlier of a staff empowerment. We've ensured that our users now are, our Cisco users feel that they have the capabilities of looking after their guests in a more sort of pleasant way. They can provide all the services and facilities that their user experiences. The guest experience or the visitor experience has improved. They're provided with, if you will a Cisco branded experience. So it's not a case where they, you know you can get on the internet and there's nothing there. We actually have "Welcome to Cisco's High Speed Internet Access." So, they are presented, you know it's a branded experience and they can see how we're using our own technology.

And finally, and we also, last and, but certainly not least, we have legal protection there. We ensure that every one of those 228,000, so approximately quarter of a million visitors a year now have accepted the legal disclaimer. So, we've provided ourselves with legal protection. We've provided ourselves with security protection. We've provided ourselves with cost protection and we've empowered our users and improved the user, the experience of our visitors.

Julie Nordquist: Well, I also imagine that even for the guest user in a lot of instances, it has helped them to actually get work done, so it may not always be someone who's just coming for the day for a customer visit. It could be a vendor, could be someone who's here on a short assignment and really essential for them to actually get their work done.

Oisin MacAlasdair: That's absolutely right. So, we're focusing here on the benefits to Cisco, of course, there is a benefit to our visitor as well. It's, there's nothing worse and I've experienced myself and I'm sure many of our audience and perhaps yourself have experienced it when you go to a third party's network or if you're visiting another enterprise and there's been times when I've gone and I'd like to VPM back into Cisco. I need to check my email. And quite often the security policies at those locations, say well sorry we can't provide you with access. And it's very frustrating for you. It makes you less productive as a person. So, in turn the flip side of this is that we are increasing the productivity of our visitors, also, and improving their experience. So, as I mentioned you see, user experience benefit, it's a win-win situation for all concerned.

Julie Nordquist: Great.

Oisin MacAlasdair: And we have, and if you think back to the five years ago, when our CIO sat us down and said, we want you to come up with this solution. You know, that satisfies all these requirements and has to be secure. It has

to provide us legal protection. And it has to be low cost. It has to empower and enable our visitors. We've been able to successfully satisfy all of those. And I think the figures on the adoption rates speak for themselves for the success of the service.

Julie Nordquist: So what's in the future?

Future of guest networking in Cisco

Oisin MacAlasdair: What does the future hold for Guest Networking at Cisco? Well, what we are doing is, in some ways as I mentioned it's called "full circle." So we actually know we're going to adopt the Advanced Services turnkey, GuestNet Manager is the name of their turnkey solution. So, we're actually quite excited about this because it gives us that actual service that's, effectively a commercial service in place. So, we now have a proper product that we have a support plan associated with. It has a feature roadmap, resources assigned dedicated to develop the service, even further and some of the features that they have planned for it are pretty exciting. And we're placing, excuse me, we're replacing the BBSM, and deleting Broadband Services Manager, which is end of life. We're going replace that with the new NAC appliance, which has greatly increased the capacity and scalability of the actual policy enforcement point.

We're looking at adding additional features to the web front-end. So, we want to look at the ability to rate limit perhaps the internet access of very small sites, so for example if we, let me think. Say we had a small site say Perth, in western Australia. It's a small site--

Julie Nordquist: Where you're from --

Oisin MacAlasdair: Where I'm actually based. So, Perth is a small Cisco site. There's only about ten employees there and it's primarily a sales site. And this shows you the power of the network by the way, insofar as I'm capable of running this global service and being responsible for driving more strategy in architecture, and yet living in one of the smallest cities, in all the small cities in the world as long as you have the network, and access to the network, you know you're empowered to do any work and any job you're assigned. But however, and so say we're, I'm in Perth. We only have a small one LAN connection to there. You may want to have the ability to rate limit the guest service at that particular site. So they don't get into the bandwidth that would otherwise be used by the enterprise customers.

We also like to look at proxy code generation. So, at the moment if a senior executive wants to create or wanted to be seen as being the sponsor of a visitor, but didn't have the time to create the code themselves, in order to have the ability they could assign proxy, so--

Julie Nordquist: That sounds good --

Oisin MacAlasdair: And this would be for some of our senior executives who don't want, have an important visitor and they don't want the visitor to be associated with a sponsor, you know it's just a case of making sure the visitor knows that they're sponsor is the senior high ranking executive, that the executive and they want to proxy that guy, the logistical aspects of creating a code to their executive assistant for example.

And we're looking at more end user and authentication enhancements. So the look and feel of the GuestNet portal, hotspot.cisco.com, we're going to, that's actually going to be a revised slightly because we're adopting the Advanced Services GuestNet Manager solution, which the look and feel will change slightly. And we're looking at perhaps integrating to management software, so improved administration, improved reporting. At the moment for example, if you want to do what

we call an “IP lookup,” so I mentioned earlier there have been a handful of circumstances when we have had to do an IP lookup to see what IP addresses were associated with what session, and that at the moment we have to troll through a large database. But with Advanced Services GuestNet Manager Service, we’ll have an automated solution, a reporting tool that’s going to really make that a lot easier for us.

So, while the architecture, the underlying architecture hasn’t changed, it’s been so successful, why break or why fix what’s not broken. It’s essentially fine tuning, update the actual policy enforcement points, add a couple of little new features to the front end, the internal web front end and adopt the commercial GuestNet Manager Solution, rather than our own internally developed web application. All of this from an end user perspective and from a visitor perspective will be completely transparent. So, this is what happens at the back end from an IT perspective.

Julie Nordquist: Terrific.

Oisin MacAlasdair: So, we’re quite excited. We’re very, very happy with the success of the service, I think. And the figures speak for themselves. And we’re excited that, you know we have some, we have a good future ahead of us, with the NAC appliance and the GuestNet Manager.

Julie Nordquist: And I think you’re going to walk us through some screen shots now.

Oisin MacAlasdair: Right, right. So, just to give our audience a taste of the look and feel of the service LAN, let’s go through some of the _____ --

Julie Nordquist: And this is the hotspot.cisco.com –

Screen shots

Oisin MacAlasdair: This is the hotspot.cisco.com and there’s lot to show what the user experiences as a guest, the visitor.

Guest access code instructions Printed and/or emailed to visitor

Oisin MacAlasdair: So, this see, is an example of an actual guest access code instructions, this is what the visitor is either, emailed or they get as a hard copy printout. You’ll see at the very top, there’s information on their guest name and location, so Joe Blog or whomever, it’ll have their name and it’ll have their location, the location where they’re visiting. So, it could be San Jose Building 12 or it could be Sydney, St Lannards or it could be Bath on Lakes in London, any site across the globe. And that access code is valid for that code, or that access code is valid for that site. Then below that, there is the access code itself. It’s simply an eight-character hexadas and alphanumeric code. Below that then there are instructions.

So you can see there’s only a handful of lines that give the actual instruction to the user. And in a lot of circumstances, the user doesn’t even need to bother with that because if he’s going to one of these high traffic areas and chances are their laptop is going to automatically detect this open broadcast SSID. Again, consider using your laptop in an airport or in a Starbucks, and you know the access SSID will appear and you can just hit authenticate or associate, and you’re connected to that SSID. The only thing then you have to typically do is look at the welcome screen and enter your access code. And finally, at the bottom there is a copy of the actual legal disclaimer. So, the user is presented with a hard copy of this or an email copy of this, but they’re also presented with this during the actual authentic, well it’s not actually authentication, during the access control basis when they first type in their credentials.

Slide 15

Oisin MacAlasdair: So, when they first associate to GuestNet and they type in for example, google.com or yahoo or "New York Times" or whatever website they want to go, they start their internet session. And the policy enforcement point intercepts that session and presents them with this screen, where they say "Welcome to Cisco High Speed Internet Guest Service. Please enter your name." So, the guest types in their name and they press "down screen."

Slide 16

Oisin MacAlasdair: Read carefully and diligently the legal disclaimer and hit the "accept" button to show that they have read and therefore they have digitally signed the actual legal disclaimer. And then they're going to be presented with another page that asks them to enter their access code.

Slide 17

Oisin MacAlasdair: So here, we see how the user now has, the name is shown, they must enter in this access code. It checks to see if this access code is valid, is it associated with this user name. The user hits "submit."

Slide 18

Oisin MacAlasdair: And if it successfully authenticated or if the code is a valid access code and it is associated with that user name, the user is then presented with access to the internet.

We start the user at the Cisco.com website, but they can, they go, well the world is always, the internet is out there and they can do whatever they want. We don't do any blocking. We don't do any virus check or anything. They're right there so we recommend the user if they want to do anything, they ensure obviously they have an up-to-date virus checkers on their laptop if they use VPM software, etc. But this is, once they've hit that "submit" button and it's been validated, they're on the internet in a secure manner from wherever they are at Cisco. So, their traffic basically goes over the, let's hypothetically speak about the, they're using a wireless service, so they have associated with this GuestNet solution, this GuestNet SSID. And their traffic is tunneled over a GRE tunnel to the DMZ and so it's only one single hop and then they're right onto the internet. And it's completely seamless to the user.

www.hotspot.cisco screenshot

Oisin MacAlasdair: Here we see an actual screen shot of the hotspot.cisco.com. So, I as an employee, if I wanted to provide you as a visitor or one of my audience members as a visitor an access to our network via the Guest Networking Services, I would go to hotspot.cisco.com using my using my web browser. Obviously, it's, our DMZ would realize that's an internal intranet website and send me here. I would be asked to identify myself, so I put in my user ID, which is Alasdair and type in my password. And this is the screen I'll be presented with. So, here I put in what building do I want to provide the guest access code for, now we have 400 sites, so you see in the right hand side of the screen shot there's an ability to sort, you know you don't want to have to scroll down through 400 different sites, buildings. So, you can say you know sort by EMEA or sort of San Jose because we have 50 buildings in San Jose. So, it makes it, there's a bit of usability access there, so anyway you type in the, you select the building for which you want the access code to be valid, type in the guest name, so Joe Blog, the corporation or the entity to which they are associated. And then you simply select the time. So, you can select any, typically its 7:00 a.m. to 7:00 p.m., maximum time is seven days. And after seven days if you know, you just have to revalidate it for a new user.

Julie Nordquist: Can you request multiple buildings or just one building?

Oisin MacAlasdair: You can request multiple, you can request one building. It's usually valid for one building.

Julie Nordquist: Okay.

Oisin MacAlasdair: And with, interestingly enough though, in the NextGen wireless LAN architecture, the policy enforcement, because buildings are grouped into clusters, access codes are valid for multiple buildings in San Jose and in certain campuses. But generally speaking, they're not valid for the entire campus. So, in some circumstances a code would be valid for multiple buildings within a campus, which is typically the environment where you'd want it to be valid. But if you're a field sales office you can't use the access code that I generated say for Singapore, I can't use that then when I go as a visit to Beijing, even if I could that there within 24 hours.

Julie Nordquist: Right.

Oisin MacAlasdair: Or of course if it was a seven day, if it was a seven-day access code. So it is associated by building, but in NextGen wireless LAN in multiple campuses, it's associated by cluster. And if you're interested in the actual NextGen wireless LAN architecture and what we've done there are other case studies and other videos also on the Cisco on Cisco site that describe that in more detail. So, I hope this has been of some use to you. And I hope you've enjoyed seeing the screen shots.

To learn more about Cisco IT…

Julie Nordquist: Thanks Oisin.

Oisin MacAlasdair: You're welcome.

Julie Nordquist: For additional information on enterprise wireless hotspots or to learn more about other Cisco IT experiences with Cisco technologies and solutions, please visit the Cisco on Cisco website at the URL you see here now. This website gives you access to more than 100 case studies and operational best practices on a variety of Cisco IT deployments.

We'd like to thank our viewers for spending time with us and being interested in the Global Technology Seminar Series. We hope that you've enjoyed this program. See you soon.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-331727-01 10/06

