01AON1 – AON in Cisco IT Part 1

Hello, and welcome to the first of two “Cisco on Cisco” Seminars and Application-oriented Networking in Cisco IT. I'm Hicham, an IT infrastructure Architect in the Internet Technology Group. With me, is Sandeep, one of our lead engineers on our team. The theme of our show today is: What is AON to Cisco IT, an overview of application-oriented networking, what it is, what it's not, what benefit it's bringing to Cisco IT and how Cisco's using AON to solve business problems and A2A and B2B scenarios. We'll follow this with a demonstration performed by Caldoun Rayes, another team member of ours in the Internet Technology Group. In this demo, Khaldoun will use the AON development studio and AON management console to demonstrate how to implement digital signature verification for a specified batch of messages. A second AON seminar called Security With AON will also be available to you on the same page as this one. It will describe how Cisco IT is using AON to improve security within its own application environment. I hope by the end of these two seminars and demo that application-oriented networking will be more familiar to you and perhaps make AON the tool of choice for your A2A and B2B integration needs. So sit back and enjoy as we explore Cisco IT past, present and future application-oriented networking. Let's get started on this AON presentation and find out what is AON to Cisco IT.

AON: APPLICATION ORIENTED NETWORKING IS?

AON in itself is actually a blade or a module that delivers a set of application and service support utilities. Those utilities actually help client applications communicate safely and well with other applications by providing security, reliability, manageability, and targeted services.

WHAT IS AON TO CISCO IT VS. WHAT AON IS NOT!

What AON is to Cisco IT: AON is actually viewed as a message router between endpoints. It's also a message transformer which allows you to transform and map certain messages, the schema of those specific messages, and is a service and integration hub with some web services management capabilities, such as basically versioning, logging, etcetera. What AON is not: it's not a general purpose application service. In certain ways, it's not used for interactive application development for typical applications where users come in and look at some views of data itself. It's a specialized module that sits in the network mainly working for transformation for mapping, for authentication and for authorization of these messages.

WHAT ROLE DOES AON PLAY?

What role does it play? The role that it actually plays is as a service broker in a service-oriented architecture, it also plays the role of an integration broker, and application integration in a typical EAI implementation and it also plays as a security integrator also within an application.

AON COMPONENTS

AON is divided into three different components. You have what's called the ADS, which is the AON design studio. It's a typical studio that's used across between different developers. For those who are familiar with J-developer, J-builder, etcetera, they would be familiar with such GUI-based tools that allow you to create and design flows. Then comes the AON management console, which is used to configure how AON blades work within the network itself. It's used to configure ACLs, etcetera. And then there's what's called the AON blade itself, which resides within a switch or a router, whether it's either at the edge of the network or within the actual device itself.

AON DELIVERS THE FOLLOWING SUPPORT UTILITES FOR:

AUDIENCE COMMENT: So let's talk about what AON delivers as utilities. Let's talk about security. It delivers transport level encryption and termination. It delivers payload encryption, protocol transformation between whatever protocol AON supports, clearly SSTP, JMS. In the future it'll support both protocols, digital signature handling with strong authentication and it has a special feature that allows you to make use of it as a tunnel between two different layers in the DMZ and then at the app layer.

THESE AON SECURITY FUNCTIONS?

So let's look at how we're using those functionalities right now at Cisco. I'm taking four different examples here. We have an external app environment, we have a B2B Gateway, we have different Z to A app environment and several other environments. If you look at the security functions, all of them, we have to go to great lengths to make sure we do security, digital signatures, authentication, — all of the security functions that AON supports. For example, at the B2B Gateway the digital signatures, it's specific to the Gateway, the technology used, the environment used. So you have to replicate that functionality across each environment, so each time you want security you have to re-do it per environment. You can take a look at the protocol translation, digital signatures, all of those, we have to do it at every environment, at every step. Now what AON brings, AON brings the security functions all at one layer, so you don't have to do it over and over again as you build your environment.

AON DELIVERS THE FOLLOWING SUPPORT UTILITIES FOR:

The same thing goes for the other utilities AON delivers, for example reliability, manageability, targeted services.

THESE AON RELIABILITY AND MANAGEABILITY FUNCTIONS?

If you look again at the four different environments, we're doing reliable delivery at the B2B Gateway, at the extended app environment, at the J2E layer. Again, every time, we're doing it over and over.

THESE AON TARGETED SERVICE FUNCTIONS?

This is the targeted service functions — again, the same thing.

AON FEATURES DEPLOYED WITHIN CISCO IT

So I'll give it back to Hicham to talk about the features that we're going to deploy within Cisco. That was generic AON security functions and other functions.

BEFORE AON: CURRENT LOCATION OF APPLICATION AND SERVICE SUPPORT UTILITIES

Thank you. So basically before we had AON, we had what's called stove pipes and those stove pipes were specific to each environment. If you really look at it, many of these functionalities, such as digital signature verification, XML encryption, SSL termination, etcetera, were very much environment technology or even vendor-specific. In addition, other implementations were also application-specific, so protocol translation, schema validation, etcetera, even transformation or mapping were very much application-specific. And what we mean here by application-specific is the fact that you have to actually implement it for every new application that you design, which means significant effort that's repeated again and again each time you develop your own application and that applies to each one of these environments. And again, as Sundeep mentioned, many of these environments have different technologies that have different processes for deployment, they also have different vendors sometimes or multiple vendors within the same environment that we have to implement whose technology we have to implement. That's some of the issues that we're facing: it's cost, it's maintenance, etcetera, that's where all the problems lie. Where we'd like to move is actually to the next step and segregate, create a whole new layer using the AON.

AFTER AON: FUTURE LOCATION OF APPLICATION AND SERVICE SUPPORT UTILITIES

Where we push many of these utilities and capabilities out is to the AON layer. In that case we'll leave the business logic out to the application layer where all of these environments exist, however, we extract all of these utilities out into the AON layer, So in that case SSL termination, digital signature verification, even certificate validation, transformation and mapping, protocol translation, etcetera, all of these capabilities will move into the AON layer into one standard layer where from an infrastructure perspective we don't have to maintain five different technologies and five different environments in order to make those capabilities available on all of them. We'll actually do it only on one specific standard environment that's shared across all of the other environments or one specific layer that's shared across all of those environments. In addition, for developers there's significant savings from their side.

WHO WOULD BENEFIT FROM AON!

So really if you look at it who would really benefit from AON? Number one would be the actual developers because they do not have to recode and reproduce all of these capabilities on each one of these environments and technologies. The business in itself, AON will provide them with faster time to market and delivery and it also lowers the development and maintenance cost from a business perspective. For information security capability it actually makes it simpler to secure, it's a simpler security model. As you know the more complex the environment, the more complex security is, and the more work and effort that has to be put into securing the environment. So actually simplification of the environment makes security even stronger and better. And from an infrastructure perspective it makes the life of the infrastructure folks a lot easier because they do not have to maintain, they don't have to upgrade and support multiple technologies in order to provide these capabilities across multiple environments.

CISCO IT RECOMMENDED AON ARCHITECTURE

This is the actual Cisco IT recommended architecture for AON. If you really look at it, it's a typical external-facing environment. You have what's called the DMZ and the application layer with firewalls separating those. The recommended architecture is to put AONs into clusters and many of these clusters will be done or created around functionality, around security, and also around the implementation of the actual IT groups or organizations. Those clusters will allow you for better scalability perspective. So in that case you may actually take functions or capabilities that are very much CPU or memory intensive and put them into their own cluster so you can scale that cluster a great deal. Some of those capabilities for example could be XML encryption, or XML decryption especially for large document, digital signature verifications, etcetera. Many of those are very much CPU and memory intensive and those could be put into their own clusters. In addition for security perspective you may be clustering basically the authentication, forcing authentication to be put into the DMZ layer. So SSL termination with bidirectional authentication, even digital signature verification, in this case, or basic authentication over regular SSL will all be terminated into the DMZ, so that messages that are not properly authenticated are not even allowed to get into the application layer. So in short, clustering provides you with better security, better manageability and also provides you with better scalability as you put them into cluster and that's why we're recommending that approach from an AON perspective. In turn these clusters within the AON application layer will connect to the backend services, whether they're all business services, they're internal, or they lay within other layers that are in what's so-called the protected NAT in that case.

BEFORE AON: TRANSFORMATION AND MAPPING

AUDIENCE COMMENT: So for an example let's talk about transformation and mapping and how you can use AON to reduce the number of hops, the complexity of the environment, and so on. So currently, it is a simplified architecture diagram, not just Cisco. Any other company would probably have a similar setup. What would happen is a request would come into the external environment which you have in a DMZ, the web service there would listen to it if there's a necessity to terminate it. Then it would go to a messaging hub which is probably crossing firewall boundaries or whatever. And then it would go to the business process environment, the internal environment, wherever you're doing your business logic and then from that it'll talk to an adaptor that talks to the database. So you see there's like one, two, three, four, five hops already. Now let's look at how AON kind of messes into this architecture and takes away some of the hops and

the components. So the first phase would be, just to make use of AON services that we talked about earlier like security, logging, transformation and all that.

AFTER AON-PHASE I

To make use of those we would replace the front-end web service with the AON cluster. And basically at this stage all you're doing is replacing the front-end web service with FastE or IBM WebSphere or whatever it may be. Now on the next step, phase two you can see we've collapsed all the layers.

AFTER AON-PHASE II

As you deploy AON, you'll get your hands on how to do transformation, how to do data mapping between different applications and as you figure out how to do those you can actually collapse those functionalities into AON. So you're eliminating a whole bunch of layers there and you can see the benefits of doing that.

USING AON VS B2B GATEWAY

So another scenario is how you would use AON as a B2B Gateway that was an A2A scenario. Now let's look at B2B. So in a lot of the B2B scenarios you have SOAP/HTTP or HTTPS, or it may be XMLRPC/HTTP, or flat files, or whatever. SOAP/HTTP, XML/HTTP, flat files, you can replace with AON. So if you're using B2B Gateway for those functionalities, you can currently replace those with AON. We're not there yet with EDI AS2, so if you're doing AS2 or RNF or any of those protocols and formats, you'd still have to use the Legacy B2B Gateway. In the future there may be a chance that we will get into that space. We're not there yet, but as you can see SOAP, XML, HTTP or even JMS, if you're doing JMS over the Internet, I hope you're not, but if you are, you can do that. And this slide, I kind of like this slide because it describes where AON sits and what it provides as far as web services go.

PROTOCOL RELATIONSHIPS

It provides – so web services there's a whole lot of protocols, we call it WS* – you know, there's like 50 different protocols. AON understands most of those, and we keep up with the standards bodies, so it understands WS security. Obviously SOAP sits on top of http – it understands all of that. On top of that it has its own XML processing engine on hardware, so you can see the benefits of doing that in hardware instead of in memory or in software. I'll give it back to Hicham and let's talk about what role AON plays in SOA.

WHAT ROLE DOES AON PLAY IN SOA?

Thank you, Sundeep. So AON actually plays a number of roles within a service-oriented architecture. It plays as actually the message router – that's one of its functionalities. It also plays in application and service security and application level monitoring because you could customize the monitoring based on certain attributes within the messages that are going through. You could set AON to parse those messages and report or monitor certain specific criteria for those messages are being passed across. It also allows you to do what's so-called service abstraction and service versioning. It can front those services and abstract those and actually version the services while completely hiding and shadowing the actual services and how to run it in the backend layer in itself. It also performs basically protocol translation where it allows you to do translation between HTTP or HTTPS to any other protocols such as JMS or even proprietary protocols or proprietary protocols that are associated with specific applications or backend packages. You can also invoke transformation and mapping where you can transform the message itself or map certain fields within the message itself from one source to a specific destination. So you may actually receive a message as XML or XML as a payload within a SOAP request, and transform it into an idoc for SAP, so that it flows directly to the backend system. And also can work as a message schema validator where it actually verifies the schema itself of the message before it makes it to the backend. So if you look at it, it provides a suite of capabilities for that specific message, from authentication, to authorization, to validation, to transformation and even routing of that specific message to the proper destination. That's the role it plays between services and redistributed services environment built on top of SOA.

WHAT ROLE DOES AON PLAY IN APPLICATION INTEGRATION?

AON also plays a role in application integration, or what's called EAI, enterprise application integration. It allows you to perform protocol translation transformation which is very typical in a EAI scenario where you have disparate packages or disparate applications that speak different protocols or have different message schema that they understand. It also allows you to do schema validations between different endpoints. So again it plays both roles, different roles, in application or EAI implementation, also plays a very active role in a service-oriented architecture.

CISCO IT AON PRODUCTION: INTANGIBLE BENEFITS

Some of the intangible benefits, based on the discussions we had before, which Sundeep had mentioned regarding collapsing multiple environments or condensing it, it does provide you with faster time of delivery by reducing development lifecycle. This comes from standardizing on specific environments and capabilities that are shared within the network itself. It gives you better security possible by actually providing a common layer for authentication and authorization for digital signatures, which relates to what's called strong authentication, in this case. It reduces the complexity of the application infrastructure – that's the benefit mostly from an infrastructure perspective. The architecture in itself it lends itself to a service-oriented to also service-oriented architecture, it also reduces the resources requirements for individual applications. So instead of having to recode and deploy these capabilities every time for every specific application, now you have a common layer that provides all of these capabilities that could be shared across all of those. And as you know there is no better place for sharing than the network because it's the one infrastructure that's shared between all applications, all packages and all systems that are distributed. Having those reside within the network itself is by itself a huge benefit, it provides a huge benefit within the enterprise itself and that touches on the point of moving the intelligence of the network. Again it's the one common layer across all of these packages on all of these environments. Moving the intelligence in the network means that all of these different endpoints can leverage it, make use of it, and reuse it and therefore you'd be able to save significantly on having to redevelop it or redeploy it in different technologies, or different environments. That's the benefit you get by deploying it into what's called or pushing the intelligence into the network itself.

CISCO IT VIEW OF AON

So what is Cisco view of AON? We look at it as more of an invisible message router in a Gateway in the network that routes, transforms, monitors, authenticates and authorizes messages between different endpoints.

AUDIENCE QUESTION: **Q.** So let me ask you this, Sundeep. What benefit do you get out of making, or making use of a messaging router in the network that's invisible to users?

A. There are many benefits that you would use. Again it's mostly leveraging and reused across different applications, across different endpoints. Instead of having to implement that capability in each one of those endpoints, now it's actually a common shared capability within the network itself, since the network is shared across all of these different endpoints. One of it's additional capabilities, when we talk about invisible and we'll touch base on that in the next couple of slides, is the ability to put AON in what's called invisible mode where the actual, neither the client nor the actual service provider will be aware of AON existence in the network itself.

AUDIENCE QUESTION: **Q.** So does that mean services now wouldn't have to change their code as much?

A. Not at all, actually, they would not change at all and they would not even know that AON exists within the network itself and that's one of the beauties of using AON.

HOW CAN AON BE INVISIBLE?

So how can AON actually be invisible? It runs in what's so-called pass through proxy mode. It is transparent to application and it uses for that it uses WCCP which is a standard protocol that's implemented…

AON MODES OF OPERATION

…which allows a router itself to route all of these different messages that are going from application A to application B, or service B in that scenario, it routes all of those to AON. AON performs whatever validation, authorization, authentication, or even transformation on that message and then sends it to the backend. In certain ways the actual packet, in this case is kind of spoofed because it goes back and reinserts the original IP, which is the application A IP, into the packet and sends it to the backend. So in that case, application B or service B, it still assumes that it's receiving those packets directly from application A and that's the beauty of being able to use such protocols and be invisible within the network. In that case this allows you to still have application A, not even change the URL for that specific application or service in itself.

AUDIENCE COMMENT: **Q.** And on top of that, so if you're making use of services like authentication and so on, application B wouldn't have to code any of those services now.

A. Absolutely not, because in that case once you implement WCCP, or such capabilities, no packet would go through that router without going through AON based on a source IP or port or destination IP or port. Or you can even make it even more sophisticated by using other products such as the CSM or the CSS, which is content-based routing that allows it to route that message to AON based on specific rule within the L7 or what we call the application layer in the OSI stack.

AON BEST PRACTICES: A CISCO IT PERSPECTIVE

That's some of the capabilities, and now I'll hand it over to Sundeep for some of the best practices with AON.

AUDIENCE COMMENT: So for the next couple of minutes we'll be talking about how Cisco IT views you should be doing your AON networking. This comes from, I guess we should say, experience or whatever we've learned in the past.

BEST PRACTICES: LOGICAL DIAGRAM

Q. So we have this logical diagram here and it talks about a few features that you should have or you should implement. Can you elaborate on some of those?

A. Yes, absolutely. As we discussed before when it comes to the actual logical or even physical architecture, some of the recommendations we have is to actually cluster AONs, versus putting all the AON blades into one common layer is to actually cluster AON blades across the DMZ and the protected net, which we assume most companies do have that. You always have to have a DMZ when it's external-facing and the application layer. You also want to cluster AON devices within each one of these layers based on specific functionality. So as we mentioned, functionalities that have to do with strong authentication with SSL termination, even SSL with bi-directional authentication, or anything of this nature should all be put within the DMZ layer. Within the application layer you should cluster those based on specific functionality that are either CPU and memory intensive versus other functionalities. Other criteria may come into play such as organizational structure and also where these applications fit, that's another criteria that you could use for the clustering within the application layer.

AUDIENCE QUESTION: **Q.** So I have a question there. We've been talking about clustering and talking between AON devices passing through the firewall. What do we use to talk between devices, or what's so secure about our, you know, what protocol?

A. Yes, between different clusters you would use the AON secure protocol, which allows multiple AON devices to talk to each other securely with strong authentication and certificates. So in that case AON would refuse any connection from any other device that does not have a certificate and provides an SSL with bi-directional authentication between these different devices. In fact that protocol itself allows you to punch a hole through the firewall where only these AON devices can talk to each other. That's the beauty of using the AON secure protocol and that's actually one of the recommendations for allowing different clusters to talk to each other. You should use the AON secure protocol to allow these different clusters to speak to each other, whether it's across the DMZ or within the app layer. However within the app layer you may have the flexibility of using only AON protocol between clusters dependent on your security requirements and needs.

AUDIENCE QUESTION: **Q.** And so the idea behind clustering by functionality, is that so you can scale based on functionality, or what's the idea behind segregating?

A. Exactly, the whole idea is to be able to scale horizontally based on functionality. As we mentioned, you may have certain capabilities that are very much CPU or memory intensive, such as XML encryption or decryption, especially for large XML documents that could be in the multi-megabytes. You may have SSL termination basically with bi-directional authentication that could be also CPU intensive, digital signature verifications; many of those should be within their own cluster so you get as many AON devices as you need. A capability or a feature such as login, you may be able to pass several hundred messages per second, if not thousands of messages per second, per AON node. However, that number goes down a great deal if you're doing XML decryption for very large messages that again are in the multi-megabytes. What you want to do is actually segregate that functionality between different AON devices, that's the beauty of using the clustering approach. It also provides you with better scalability, failover and load balancing from that perspective between the different clusters.

AUDIENCE QUESTION: **Q.** So basically you would use the same mechanism to scale horizontally on the app layer as well then?

A. Yes, of course, that's the same approach.

AUDIENCE COMMENT: So if we have all these clusters, obviously there's going to be issues with provisioning…

BEST PRACTICES: PROVISIONING AND MANAGEMENT

…because you have to hop between, for example different environments, how do you push code and all that? Right, so let's talk about that for a bit. So one of the first things you want to look at when you talk about provisioning and management is follow a strict SDLC process. AON again, it's a device that sits in the network. However, you have to treat it from a development point of view, you should be following the system development lifecycle. In addition, you should always have a dev staging and production environment so that you can test things. Within dev you could do the development, within the staging you could actually do some internal testing, integration testing and even some type of user acceptance, and then move it into the production environment. In addition since many of these AON devices would or could contain multiple applications, you have to pay attention to name space collision. So you have to have standard naming for packages that are pushed into AON. You may have an organization, let's say such as HR and you would put a naming convention that may be proceeded by the human resources, or it could be HR.packagename.etcetera, that's the type of naming convention you should follow. There are multiple things that you should follow, especially from a deployment point of view, to avoid name collision, to avoid other issues. Those are some of the recommendations for managing the environment itself that we have.

AUDIENCE COMMENT: Nice, we've put together some questions that customers had asked us about this topic in previous sessions.

SLIDE 31

Q. We have a little time left and I'd like for us to discuss the questions a little bit, if that's okay.

A. Sure.
Q. The AON blade sits in a network switch on a router and are there any plans to deploy them outside the data center or the network at the edges?

A. Absolutely, there are certain plans, in fact, currently AON not only has a blade that fits within the actual switch itself, the 6500 switch it also fits in many other routers that are deployed at the edge or actually what's called the remote offices. So in that case, you would have one AON implemented within the router that can speak to the AON that's implemented within the data center itself. And so it already exists right now, in fact it may provide you with better integration and even better security from that perspective. Where you have two AON devices communicating over AON secure protocol between the remote offices in the data center.

AUDIENCE COMMENT: **Q.** So there's security implications.

A. Yes. Hopefully, Brook coming up later will talk about it, right. Yes, absolutely.

AUDIENCE COMMENT: Let's go onto the next question. **Q.** Why don't we put AON functions into a specialized server in the data center? Why is Cisco putting it into the blade or the network?

A. This question's really interesting, it actually has security and management implications. From a management perspective, by putting it into the network, again the network is the only and mainly common place where all the applications have to touch in order to communicate with each other. So by putting it within the network or putting it within the switch, we're able to leverage the capabilities across all the endpoints and across all of these different applications, whether they're backend packages, backend databases, or custom written applications, or even B2B Gateways as standard B2B Gateways. So from a leverage point of view, by moving the intelligence into a centralized point, every edge or every endpoint would be able to actually leverage that capability. From a security perspective by putting it within the switch and using what we talked about from a WCCP capability that allows it to be a pass through, it can intercept those messages and prevent any calls or any packets from making it to the endpoint without proper authorization, authentication and even sometimes transformation or mapping. So the combination of these two drove, I believe, Cisco into pushing it into the network, leveraging and securing these messages as they go between different endpoints.

AUDIENCE COMMENT: **Q.** So it goes back to that invisible message router that you were talking about earlier. **A.** Absolutely, yes.

AUDIENCE COMMENT: Just plop it in, use the services, nobody has to know. Nobody has to know, not the sender, neither the receiver has to know that actually the device is on the network and it's actually intercepting, authorizing, authenticating and transforming many of these messages. That's the beauty of putting it in the network itself or moving the intelligence to the network and the security to the network.

AUDIENCE COMMENT: **Q.** So you could have rules and so on as well on the blade saying, you should go here, you should go based on this, you should do this.

A. Yes, within WCCP you could actually dictate as to based on a source IP or a port, even certain aspects from the query string at the application layer, or the actual URL you can dictate where that specific request has to go. And it's a combination of other products included within the router itself.

AUDIENCE COMMENT: Let's go onto another question. **Q.** So, this touches a little bit on what you talked about earlier. Does this require me to make changes to my web services that are currently existing, and how difficult was it for Cisco IT?

A. It was actually fairly easy. Again, by putting AON itself as a blade within the network and activate and do a so-called invisible pass through mode, there's very little you need to do on the client or the server side. Neither one of them is actually aware of it and neither one of them has to be changed, neither one of these services has to be changed in order to actually put AON in between. You could do the authorization, the authentication, the transformation, the schema validation, before that message makes it to the endpoint. And again the beauty of having WCCP is that it actually spoofs the message, if you really look at it that way. Because the server itself, or the service itself that's receiving the message, it still sees the original IP of the actual sender, so it'll never know that it actually came from a different endpoint or a broker in the middle that brokered the message and sent it to the endpoint, that's the beauty of it. So there is very little change that you really have to do on the actual endpoint. There are certain cases where you may say that, I'm doing currently transformation or mapping within the service itself and I'd like to extract that and pull it in a shared or common blade on the network. In that case, yes, there may be some changes that you would have to do, however, most of those changes are fairly light and easy to implement. By actually moving those from an end service at the endpoint and putting them in the network, now we can leverage these capabilities across many applications no matter where those applications are running. Whether it's a different platform, different operating system, different programming language, or even a different environment, you could leverage those capabilities in a common device without actually allowing anybody to be aware that this is happening on the network. That's the beauty of moving the intelligence into the network itself.

AUDIENCE COMMENT: **Q.** So it actually makes it easier for you. After you've deployed the services on AON, it actually makes it easier for you to deploy more website services in the backend without having to do a lot of work?

A. Exactly, that's the whole purpose behind it.

AUDIENCE QUESTION: **Q.** So what that brings us back to, which is actually a good question we have here, is do we require to buy new blades, or completely change our network infrastructure to use AON? What did Cisco have to do, or Cisco IT I should say.

A. Yes, actually we did not have to do any of that. AON as a blade, just like the CSS or the CSM blade, goes into the switch that you have, so if you have a switch, or if you have a router it goes into those. Of course there are certain capacity limitations that you may have. So within a small router you may be able to put two blades, or four blades, depending on what type of router, whether it's the 3800 or the 4800. On the other hand, in a Cat 6 switch, you can up to as many as 12 blades in itself, so you would be able to leverage what you have right now in the network and add those blades. Of course if you scale to a very large implementation using AON and you implement dev stage and production, then you may want to start considering adding more switches for capacity purposes. However, for the implementation that we've done at Cisco, it has been very smooth, we have not had to do much except possibly upgrade some of the switches that actually were using an older version of the IOS, so it was a matter of actually upgrade, not necessarily buying new switches or routers.

AUDIENCE COMMENT: **Q.** Just to match the version numbers?

A. Exactly, because it requires certain versions of IOS.

AUDIENCE COMMENT: Well, thank you. I'm afraid that's about all the time we have for questions today. I'll hand it back to Hicham.

FURTHER AON AND DATA CENTER RESOURCES

So thank you, Sundeep. And for more information about Cisco IT deployment, you can go to ciscoit@work site to find Cisco case studies about what we deploy, what benefits we've gained, what lessons we've learned, and some operational practices and presentations to help you learn more. Thank you, everybody. And you can also find more information on AON and other application-based product design

guides, operational practices and several other documents, white papers and presentations on www.cisco.com. Below that, you will see a toll free number, you can call for more information, or to place an order. You can order Cisco resources on the website from the URL at the bottom of this page.

INTERMISSION

Thank you again, everyone.

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

Use the Copyright Style for the Trademark block and the Job# info

Printed in the USA C78-337350-00 02/06