Beyond the Network: SD-WAN and The Golden Gate Bridge

IT organizations everywhere are under pressure to reduce costs. More and more of them are also being called upon to not just support a company's technologies, but to drive technology choices that improve operations. In simple terms, they need to enable more while spending less.

For this episode of Beyond the Network, we're turning the microphone over to experts from Cisco's IT infrastructure organization. Jon Heaton is senior manager for the Infrastructure Strategy and Validation team and Chris Groves is manager of the Premise/Access team. Hear how their company is using two specific technologies to reduce connectivity costs, upgrade devices faster and easier, and improve the experience of their end users, as we go Beyond the Network with Cisco IT.

JON HEATON: "Well, I am Jon Heaton and I am here with..."

CHRIS GROVES: "Chris Groves."

JON: "And we're with Cisco IT. IT infrastructure specifically. So I'm responsible for infrastructure strategy, and Chris?"

CHRIS: "I am responsible for a portion of our network. Our in-building networks, our wired and wireless networks, including our branch WAN, which is something we're going to talk about today, I think."

JON: "Yeah, so in other words the most important part of the network."

CHRIS: "Yes, totally."

JON: "The other stuff that your peers have, well it's just not as important."

CHRIS: "That's ok, they're not here."

JON: "That's right, they're not here, but they might listen later. We're going to talk today about a couple of things, but the first topic is around DIA. And DIA is not even closely related to CIA. What is DIA?"

CHRIS: "So when we say DIA what we mean is Direct Internet Access. It's a term that will mean slightly different things with different service providers or different areas of the market, but when we talk about it what we mean is an Internet circuit coming into our site – we actually get them with symmetric bandwidth, a little bit of guaranteed quality on the service and some SLAs, not as good as a lease line or MPLS, but still a lot cheaper. So when we say DIA it's a step above sort of the business broadband you might get where you're having shared bandwidth with all parties in your office park or all parties on your block or something like that. When we say DIA that's what we mean. We mean a dedicated access circuit for us, going straight out to the Internet."

JON: "Technology-wise, what technology is that? Is that ethernet? Is it -?"

CHRIS: "Come in on ethernet, yeah. It almost always comes in on ethernet. Depending on the access it could be copper or fiber, but it almost always comes in as an ethernet, yes."

JON: "Ok, and why would DIA be important to us, Cisco, as an infrastructure provider, to ourselves?"

CHRIS: "Well, there's a lot of reasons why DIA is important but the first one that immediately jumps out is that it is a little bit cheaper. So if you look at the benchmarks in the circuits and the services in the various regions – at least in the United States, Europe, places like that – DIA is cheaper than MPLS or a leased line in general. So there's a good cost savings associated with that. The performance is pretty good in North America and in Europe and in places like that and it's a lot cheaper, so the tradeoffs in quality are probably worth it if you can make it work.

The second big reason is that a lot of applications have moved to the cloud, and with applications moving to the cloud you don't necessarily need to get backhauled to your Data Center just to go out to the cloud. Sometimes you get a better application performance by going out to the cloud locally and that gets you closer to whereever that application is hosted."

JON: "Right. So in our case our main Data Centers are in Texas and if you're building, if your Sales site is in Omaha, Nebraska it might be better to go directly to the Internet instead of backhauling it to Texas. Although Nebraska is probably close, so –."

CHRIS: "Yeah, Nebraska's a bad example, it's really close to Texas, right? A better example might be –"

JON: "Bangor, Maine!"

CHRIS: "That's right. A better example might be Maine, or something like that, where instead of backhauling it back to Texas to jump out to the Internet to go get to something, if you're going to a cloud application that's using some sort of content provider to put it all around the world, there might be a point of presence in Boston. And wouldn't your Office 365 or your Salesforce or your whatever work a little better if you went from Maine to Boston rather than from Maine to Texas to somewhere else? It gets multiplied when you get to regions like Europe where if you're somewhere like Athens, Greece, if we want to backhaul that traffic to Amsterdam to come out we're going to get to a content provider that's near Amsterdam that might be fine, but the Googles and the Amazons and the big cloud providers of the world probably have little points of presence closer to Greece, right? And so your application performance might actually be better if you can come out and break out locally with a Direct Internet Access circuit."

JON: "Yeah, and it's pretty simple to understand that distance adds time and delay, right? Because we so far haven't been able to go faster than the speed of light, so therefore –"

CHRIS: "Not yet."

JON: "Therefore the traffic has to go all the way to where things go to."

CHRIS: "It might take a while. Yeah, it might take a while."

JON: "So that makes sense. You mentioned tradeoffs in terms of QoS perhaps or other performance –"

CHRIS: "Experience."

JON: " – things. Are there some providers who are still not providing it or are there some countries where it's difficult to get DIA, where you're having to do legacy type things?"

CHRIS: "Yeah, and I think what you'll find is at any big company that's global who's looking at this is going to run into these same sorts of issues. Different regions have different regulatory reasons why you may not be able to. Internet access in India is sort of a different beast because of the regulations they have around that. Similarly, to and from China there's some government mandated security controls as well as most companies have their own controls that they need to do. And also plenty of companies with data privacy laws are having to adjust for different regions and different geographies where they want to keep data encryped or in-region or who knows what. And those are things you have to consider when you go to DIA."

JON: "So, we in Infrastructure provide the service, the connectivity of our employees to applications and to data. It's the job of Information Security to secure all of those things, and sometimes that can be in conflict or at least we need to work together to secure our data and our traffic. Talk about that a little bit. Is that a challenge when we're breaking things out?"

CHRIS: "Yeah. So one thing that's different, if you've got a traditional network with MPLS or a leased line or something like that that's coming back to your Data Center you're sort of riding your own little pipe, right? And so it's the way it is. It's safe, it's secure. If you're going across an Internet circuit, yes, if you're not doing some things to keep that secure you do have Internet presence at your branch. Potentially that's an ingress point where people can come in and attack your network and that traffic is going across the Internet. So there's a couple of things that we need to do to make sure that we want to keep it secure. We want it encrypted. So we want to encrypt it in a tunnel so that no one can look at it and see it without seeing the encrypted stream. We want it to be something that's going to be hard for them to sniff and to see what's in it. We're also using a local firewall on the branch, built into the router, to make sure that we've got some level of prevention so that things can't come in from that Internet circuit because it is on the Internet. And then we're putting more and more cloud security features in, right? So we use the Umbrella and OpenDNS to protect us on the DNS side and as those features get integrated more and more into a general SD-WAN solution we will use even more of those, because these things are cheaper, the service is a cheaper thing to put into your branch, but it does expose you a little bit, so you do need to keep it secure."

JON: "Would you say that we're actually more secure, by being able to secure from the cloud and on the premise?"

CHRIS: "I think so, because we go with the idea of defense in depth. You can have one giant big steel door or you can have lots of doors and gates and other things in the way. And that's really what our approach is here. Any one thing can eventually be defeated but by layering them on – some cloud-based security, local firewall, encryption, you know good practices, then we have defense in depth. And I think that ends up making us overall more secure than a single thing that might very limited in what it can do but also very brittle to break. You just have to solve one security feature to break in, right? So I think we are overall more secure. That's actually the better place for us to be because you can't stop the application from moving to the cloud."

JON: "Yeah, we get in the way we just get run over. You mentioned SD-WAN. So that's software defined wide area network, for those of us who don't speak acronym. In terms of what we're doing in Cisco IT, what are we doing with SD-WAN?"

CHRIS: "Well, and let's talk a little bit about why first. And we touched on them a little bit. You really want something – and when we say software defined WAN what we really mean is something that you can control the behavior of your WAN – not staticly where you say I want to just send the traffic across this thing. You want to be able to do some things like traffic steering. If the application performance is better going straight out to the Internet, you want it to go out to the Internet. If the performance is better backhauling to your Data Center you want it to go back to your Data Center."

JON: "And not just better today, but at any point in time."

CHRIS: "At any point in time. That's exactly right. That's exactly right. And you want to make sure you can monitor your application performance. Not just is the link up or down or am I seeing drops on the link, but is the video quality looking a little bit poor? And those are the things that if you're going to start using lots of Internet service because the Internet services are not as guaranteed as an MPLS or a leased line – those are the things that you want to look for. And that's the kind of things you get in a package that's sort of an SD-WAN solution, a software defined WAN solution. And so that's really what we're doing. Our first step was to deploy Internet access circuits and we started that a while back and we continue to do it. We started that first because there's a lead time

with that. Anyone who works with service providers knows that that can be a long process to get the right services in and to have the techs come on site and schedule those changes. And then what we've come through after the fact is we've put on SD-WAN and the idea behind that is we're able to turn on SD-WAN relatively quickly – I think we got the first two sites up in 6 weeks after the acquisition closed, right?"

JON: "Yep."

CHRIS: "And then we're able to scale that out to a number of sites so we can start testing out, playing around with and developing our own policies for SD-WAN for how we're going to do the application steering and how we're going to do the application performance monitoring. In the meantime these efforts are converging so we'll have a mass of DIA circuits out there and we've got the features we need on the hardware that we have deployed at our sites that we're going to be able to really hit the accelerator and go fast starting this quarter and going to the future."

JON: "Yeah, and one of the keys around SD-WAN is that it is controller based, so there's a controller that actually controls the software on the routers that does all this work but it also facilitates management, too. I mean it really helps us be efficient in terms of deployment and management."

CHRIS: "And centralized policy, right? If we decide we want to tune the performance of our video meeting application – maybe we don't like the characteristics we've defined for timeout or latency or jitter or something like that – we can edit that policy centrally, click a button and the software definded aspect of software defined WAN makes sure that gets cascaded out to all the sites that we want to apply to, so our application performance can be even better."

JON: "Right. But what about things like plug and play and software image management? Those are also enabled by a controller model, which should allow us to be more efficient going forward. So I mean like if we have a PSIRT, which is a security incident, we can go upgrade or patch all those devices a lot more quickly than we could without a controller-based type network. "

CHRIS: "Yeah. And I think any IT network operator if you say, hey, in the legacy model, we want you to do something to all your sites or all your devices, they die a little inside. Because in the old model of no automation and everything is command line interface – right? – that's going to take a long time. You're going to either have to manually do it by hand, you might have to send people on site. That's a pain. So the controller-based, the software-defined, the WAN controller-based approach does let us do things like that centrally, right? If we want to upgrade the devices it's a click of buttons. If we want to change policy or configuration centrally we set it once on the controller, we schedule it or we click the button and we push it all out at the same time. If we had to do that manually, individually, site by site, this would take us years to do. It's already going to take us quite a long time but to do it completely manually we would never finish. It would be like that painting the Brooklyn Bridge or painting the Golden Gate Bridge where by the time you get to the end –"

JON: "Start over."

CHRIS: "You've got to start all over again because you're never actually done. I think any organization that's a big IT operations organization is constantly going to be challenged for budget, schedule, time. Those things are not going to be bigger I the future, they're going to keep getting squeezed and so you need your software defined tools to be able to do that."

JON: "Yeah, and going back to security for a minute, security becomes more and more important. Our service area increases, the attack vectors increase so that's more and more difficult to deal with."

CHRIS: "Let me give you a story on that. A couple years ago we needed to do an additional level of WAN encryption at some sites that we Internet circuits that were in areas of the world where maybe the region around

there or maybe there's some local actors that perhaps try to hack into circuits more than other regions and we need to add a different kind of WAN encryption onto those circuits. And it was about 40 sites that we identified that we were doing this additional level of encryption. It was a manual process. It took about a year of manual change windows and manual work for people to go out, engineers to go out to those sites one by one, set them up, get all the security keys working. That's something we get now by default with SD-WAN. We click a button and it's turned on, we deploy a site. So that's fantastic. So –"

JON: "Yeah."

CHRIS: "To put that in perspective of what it would take from an IT operations perspective, that's the kind of thing that you really from your software defined approach. Right, so be able to do those things automatically and centrally and not to go site by site, command line interface, custom configuration."

JON: "Now, taking a step back, I don't think we talked much about different topologies where we'll be using DIA. So maybe we can just touch on that for just a minute. There's two different models, right? We have what we call a silver site, which is a smaller one, which would be a single DIA circuit."

CHRIS: "That's right."

JON: "For the most part. And then we have larger gold sites that require more business resiliency that would probably be MPLS with a DIA as backup. But another thing SD-WAN allows us to do is balance across those whereas before, in the silver topology for us, that DIA circuit would be sitting there or the Internet backup circuit would be sitting there idle."

CHRIS: "The gold. The gold."

JON: "Sorry, gold."

CHRIS: "That's alright."

JON: "Thank you, Chris, for correcting me."

CHRIS: "Yeah, the silver is a – if you think about it, sliver is also – the letter S is important, right? It's a small office or a Sales office right? So silver."

JON: "Yeah."

CHRIS: "Single circuit, single entry into there, historically that might have been an MPLS. In the future that's a DIA with local breakouts so we can some applications straight out to the local cloud. Others we can send back, and the golds, the G for the general business, which is more of a medium-sized, maybe the larger location will have have two – historically we might have done a 50-50 load balance between those or 100-0, so a hot and a failover on the circuit. But the SD-WAN does let us tune that a lot more actively. We can run those circuits a lot more at capacity. It can dynamically switch things back and forth. If the performance on one is better than the other and we send the video down the one that is the best performance and we send the PC backups and things like that down the one that has less performance or is the cheapest. That's exactly the kind of things we want to do with our software defined WAN."

JON: "And I remember there was some other cases where in some of those larger gold sites where we would actually have the backup was down and we may not even know because it doesn't get used. And so when the primary fails there's no backup there."

CHRIS: "Yeah or definitely quality issues on the backup, right? So we don't like that primary and failover backup approach. It works a lot of time but it does surprise you some times if there are issues on the backup when it happens."

JON: "Yeah."

CHRIS: "We much prefer to run them both at the same time. We also feel like we're spending our money more wisely. If we're paying for them both we want to use them both, right."

JON: "Absolutely."

CHRIS: "And we want to get our money out of them, and then hopefully see where a prob is before it happens."

JON: "Yeah, yeah. You know, Chris, when we were talking Golden Gate Bridge earlier, where you had to start again just as you're finishing, the same thing applies to how we roll out technology. We have 400-plus sites, right, 450? Something like that."

CHRIS: "Yep."

JON: "So if we start rolling out technology it takes us how long to roll out that technology?"

CHRIS: "If it's a physical switch it's probably 3-4 years, maybe 5, depending on the location, if it's a physical hardware changeout.."

JON: "Yeah, so for us we're rolling out SD-WAN pretty rapidly but it's still going to take us some time. How long do you think?"

CHRIS: "I don't know. Maybe two years."

JON: "Two years? Yeah. So it is definitely a progression. Not to mention what you talked about also with the ordering of circuits. Some of them take time and some carriers in other countries can take a long time."

CHRIS: "Yeah. I think the important thing is to separate – and the Golden Gate Bridge analogies works for those things where your solution is tied to your hardware and you have to change out your hardware. What we're going to find more and more in the future is that the changes we need to make and the things we're being asked for we want to tweak inside those application profiles and inside the application aware routing that's inside of our SD-WAN. So while we have SD-WAN deployed everywhere, when we deploy a new application or we move our mail to the cloud or we move around how we route video or something like that, we don't want to be stuck with a hardware model that we have change because then we're back to painting the Golden Gate Bridge. Instead we want to have a model where we can go in to the actual controller itself, make some changes. When that application is recognized use an application recognition engine to figure out that all this is Office or all this is Webex or all this is Salesforce, right? And then make those changes as time goes by. And so that way if our organization decides to go in a completely different direction for mail, procurement, any of the other big office applications, we can change it out using the software defined tools."

JON: "So in terms of our rollout we already have the hardware platform deployed. Right?"

CHRIS: "We already have the hardware platform deployed. We are deploying DIA. We've got quite a bit covered but we're deploying even more. And right now what we're doing is the software fix to SD-WAN."

JON: "Awesome. Sounds exciting. What other challenges have we run into?"

CHRIS: "I think the biggest challenge – and this is what I would encourage people to do is to start messing around with this, playing with it and put real traffic against it. Your enterprise is not the same as our enterprise and what applications you want to work in a certain way are going to be somewhat generic and apply to everywhere but also you're going to have some unique things. So one of the challeges that we've seen in – and it's been really helpful to have those sites done early – is we can run real applications across it that we can see what we need to do to tune it to make sure that our company video meetings go well or normal teams meetings on Webex go well or our

PC backups go at the appropriate rate, right? Which is good enough so that someone can recover their machine but not so good that they destroy the network –"

JON: "For everybody else in the entire company."

CHRIS: "That's right. And we have labs that need to be able to interact across these sites with each other and with our big Data Centers and so we need to make sure that the lab traffic receives the right amount of quality and the right amount of performance and tuning. So, get some out there early. That's been our biggest learning experience. The product has been fairly good. For us most of our hurdles have been looking at how we route traffic the old way and how we route traffic in an SD-WAN way and how we tune it and making sure we've got the right settings and the right characteristics around that policy so that it performs the way our users expect. "

JON: "Yeah. And you made a point around not all enterprises are the same. Enterprises tend to run their own networks. Enterprises tend to do the kind of work we're doing with DIA. Optimize costs over time all the time. So for us it makes sense for deploying our own SD-WAN solution but there are also service providers that deploy it as a service, because some companies particularly smaller ones don't manage their own networks even. Don't manage their own WAN, specifically. "

CHRIS: "Don't manage their own WAN. That's correct."

JON: "They don't manage their own WAN so if they have a service provider that manages WAN for them then you can actually have your service provider do SD-WAN and hopefully save you cost as well. So that's another alternative."

CHRIS: "Yeah, exactly. And I would imagine that what happens in those situations, that when you buy that services from the service provider and they're going to give you maybe two circuits or something like that or some sort of redundant capability, they're probably going to do some things behind the scenes to make sure that they can get that on the most effective cost for you as well, right? Maybe one MPLS. Maybe one DIA. Maybe two MPLS. Whatever they're going to do, they're going to make that work and that's exactly what they're doing behind the scenes. They want to make sure they get you good application performance and that they get you a good price point."

JON: "Yep. Because they're going to be held to SLAs just like you are 'cause you're providing that service to us within IT."

CHRIS: "That's right. That's right. And part of that means also that the applications work as you expect. They don't want to be called up – 'why is my office slow?' – right? So that's what they're going to be doing. If you're getting a solution from a service provider they're likely doing the same things that we're doing under the covers. "

JON: "Well, let's talk about product."

CHRIS: "Mm-hmm."

JON: "So we of course are Cisco. We do manufacture our own products in this space. So what do we use in Cisco IT?"

CHRIS: "So in our larger buildings what we talked about, that we've called the gold and silver, the general business or the small offices, we're using the Viptela SD-WAN product for those, largely. We do have some small deployments where we're using the Meraki SD-WAN as well, but our Meraki focus is mostly on the serviced office spaces where we put a very small, small network in those places that needs to be a little bit more flexible and a little bit more transient I guess is the best way to describe it. The important thing is whatever you choose you probably want to choose one. You don't want to not do one. I think we're at a day and age where you probably can't afford to not look at Internet circuits. And you probably can't afford to not have the software defined concepts

behind your WAN so you can do the load balancing, so you can leverage them constantly, so you can layer on the security that you need. I think that's one of the key messages, is that whatever product you choose, you're going to want one at least – right? – in your envrionment because if you're an IT operator you've got a budget to manage and you've got features you've got to deliver and these are key things to help you deliver those features and reduce your budget over time."

JON: "Yeah so we're running Viptela on ISR 4451s which is our access platform, right?"

CHRIS: "Yes."

JON: "What about the controller?"

CHRIS: "We're using the cloud-hosted controllers for Viptela. So we're not running our on-prem controller option, we're using the model just like customers are encouraged to use it. We use the cloud controllers, the vManage hosted in the cloud and then when we deploy a new site they talk to the cloud. They spin themselves up. They do the plug and play, the zero-touch deployment. And we're using them just like we would encourage customers using them – cloud based controllers and IOS SD-WAN on our ISRs."

JON: "Ok. So in the end, though, we like any other IT shop do things, for a reason. We do in this case – and most cases – to save money. So we get to save money by optimizing use of those circuits, perhaps deferring upgrades because we're sharing bandwidth, savings in operational costs because we're automating – doing plug and play, software image management type of automation. Is there anything else?"

CHRIS: "Yeah, so I think the very first, though, we're actually using a more cost friendly service. We're using the Internet service as compared to MPLS. We're saving money on that service straight out of the gate. Then we're optimizing across the circuits and services, so we're trying to use them to the best of our ability. So if we have one of those general sites that has a DIA and the other instead of running one hot and the other one at zero percent we're running both and tune them appropriately. That might be more of a push-off-the-upgrade as oppossed to some direct –"

JON: "Sure."

CHRIS: " – cost savings there. But we're getting direct cost savings by moving to the Internet access circuit. And then third is all the operational churn around the deployment of new sites, the enablement of features and the pushing of policy. We're hoping to do more of those faster with the plug and play and the controller based approaches, so we'll be able to do more with less people."

JON: "Right. So, money first. Probably second would be the user experience, which is where we're doing off-load and the user is closer to where their data is and not have to go all the way back to Texas in our case. That's probably a secondary factor."

CHRIS: " Yep. And then speed. Speed of delivery. Speed of features, right? Our clients and stakeholders want sites to come up faster. They want – if we have a new application they want to be able to be tuned more quickly. And that's what we're going to get out of the software defined approach as well."

JON: "Cool."

CHRIS: "Be able to make changes a lot quicker."

JON: "So in close, go get some. You'll benefit. Save costs, better user experience. This is Jon."

CHRIS: "And this is Chris."

JON: "From Cisco. Have a good day."

You've gone Beyond the Network, with Cisco IT. Thanks to Alexa Konzman for recording assistance. This episode was produced by Douglas Alger. Follow and like our podcast on SoundCloud or iTunes. Visit cisco.com/go/ciscoit for episode transcripts and related content.

For More Information

To hear additional Beyond the Network podcasts, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.**