

Technology Tutorials

IP VPN TRANSCRIPT



Program and Presenter Opening

Jonas Hurst:

Hello and welcome to this “Cisco on Cisco” Tutorial on IP VPNs. The theme of our show today is an overview of Cisco’s implementation of an IP VPN in Europe. It’s my pleasure to introduce the guest of today’s show: Dipesh Patel, a Network Engineer in the INS Foundation Technologies team. Dipesh, thanks for coming today.

Cisco’s Intelligent Network Infrastructure Delivering Value Through the Network

Dipesh Patel:

Thank you Jonas. So getting stuck straight in, we’re gonna look at how the network can deliver value through the network. What we have here in front of us is a model of how the network in effect enables a business all the way through from productivity, all the way through from shareholder value.

You can see the various departments and they’re in front of you in orange and what the network is giving us is the bottom part of the diagram where we’ve got the various features of the network and I’ll run you through some of these. We’ll talk about some of these later on. Optimum latency. The need for flexible access. Highly available. It needs to be IP based. It needs to support enhanced services. It needs secure access and of course it needs to be converged.

Cisco's Intelligent Network Infrastructure Direction: Leverage Enterprise Class IP/VPN

To carry on, looking at the benefits. The transport benefits that we see today are effectively outsourcing the core. We see a virtual any to any type network which gives us optimal latency support for real time applications and that enables collaboration, video and telephony.

It's fairly easy to implement and support. By using the service provider core for the engineering activity, there's no need for an engineer to mesh interconnection links between sites.

Jonas Hurst:

I'm just gonna have to stop you –

Dipesh Patel:

Sure.

Jonas Hurst:

Mentioning leverages core SP engineering activity. What does that actually mean?

Dipesh Patel:

Okay. So traditionally in the past what we've had is an Enterprise network that manages and maintains a very big core. Now what we're doing is actually passing this core out to the service provider so we still call it a core but in effect leveraging it out to the service provider.

Jonas Hurst:

Okay.

Dipesh Patel:

Okay. Carry on looking at the benefits. Now that we're talking about a Layer 3 VPN type service we can use some of the in-cloud services. So whether they be videoconferencing services from the provider, voice over IP, PSTN, all these services are now available from the service provider.

Some of the key service requirements must be the drop in replacement for existing Layer 1, Layer 2 type wide area networks. And we need a sufficient footprint to take advantage of this any changed topology.

Support of enhanced services. So, when we talk about drop in replacement beforehand we are really expecting the providers to give us transparency for QoS services, native support for multicast, looking at the flexible access the network view now is the same from all points. So that makes it a little bit more easier to manage.

Network management. Two ways to look at it. We say the routine is now simplified. It's non-hierarchical. In effect it looks the same from every point. And the service provider has Layer 3 reach ability and thus can take on more network operational tasks.

Finally, on the capacity planning piece, the service provider can provide detailed class of service usage and traffic pattern trending. What this means for us is we can use these statistics in the network to forecast how we're gonna plan ourselves.

Jonas Hurst:

Okay. Well, that sounds very good but how has this information actually helped Cisco?

Dipesh Patel:

Okay so for example if we take what I've just said in Europe for example, we've taken this information to see where we've had the biggest growth in terms of say video or voice so we can expand on it in that region. That's just one piece of a very big report a service provider can give to us. So that's one of the benefits that we get.

Cisco's Intelligent Network Infrastructure Direction: Convergence of Pipes

We talked about convergence of pipes earlier on. We talk about it as a two-step process but what we say is converged to a common facility using the in-cloud service provider services. And then we leave the service provider core services and economies of scale to make the infrastructure management less complex.

So you can see in the past where we've had the field office with various services coming in the field office. We now converge all of these services, or try to at least, onto the IP network and that goes into the IP VPN.

Looking at some of the challenges or barriers today. And looking at the economies of scale. For example PSTN by voice over IP. These services still on the development of our service provider. You have to remember in the past the service provider was looking at TDM based services. Not so much IP VPN. So it's new to them as well and there is still a bandwidth mentality out there.

Jonas Hurst: Okay. But how are you trying to mitigate these challenges?

Dipesh Patel: That's a good question. It's kind of a trick topic to deal with. We've got our services. It's a service provider issue. They need to look at selling not just bandwidth but services as well. So it's a win-win for them as well. So it's not really a technology problem. It's an industry wide problem although it's getting better as time goes on.

Jonas Hurst: I was gonna say are these developments in the pipeline?

Dipesh Patel: Yes, they are.

Jonas Hurst: Okay.

Hurdles to IP/VPN Adoption

Dipesh Patel: Okay. So we'll move to the next section. This is some of the hurdles that we've had in our opinion to moving forward with IP VPN adoption.

IP/VPN Roadblock #1: Pricing

So the first roadblock has been the pricing. The pricing for early IP VPN services was fairly high. Most service providers compared it with full mesh frame relay OATN based networks. Now, when we talk about IP VPN based networks, we know that they're a share network. The costs should be a little lower but these were some of the roadblocks that we had initially.

Cisco IT and other Enterprise for that matter, really don't need a full mesh network but would like the advantages that the technology brings.

Changing. Service providers are restructuring their pricing for adoption. Recent bids are demonstrating some of the savings that we're seeing compared to TDM based networks. So to sum up this slide, things are getting better but the pricing is still an issue and it varies between service providers.

IP/VPN Roadblock #2: Transparency

Transparency. IP VPN is a fairly new technology and when we talk

about migration from one network, a TDM based network, into an IP VPN based network we really are looking for the word transparency. It's not always there. That's why we call it or term it a drop-in replacement.

Jonas Hurst:

What do you mean by that? Drop-in replacement.

Dipesh Patel:

Okay. So if we take a leased line circuit in the past we want to just order that same leased line circuit or a TDM based circuit on IP VPN. We don't want to worry about whether the same class of service was available in the IP VPN versus the TDM.

Jonas Hurst:

Sure.

Dipesh Patel:

So I mean I've put down three here. QoS policy needs to be maintained regardless. So we want to see our markings preserved end to end. Even though we've moved from TDM to IP VPN.

We want our routing policy and protocols to still be a _____ in a transparent fashion. And we also we need support for IP multicast in its native form. So these are some of the elements are required when we say drop in replacement in a transparent – when we're talking about transparency.

IP/VPN Roadblock #3: **PE Coverage**

PE coverage. The early IP VPN services had significant coverage but relied on a small number of provider edge IP nodes. And we've got an example here. In the U.S. one service provider used five IP nodes in the U.S. When we actually measured the latency from site to site we found that our private network was actually better than the service provider's ones. So you can see how the density of the P does affect how well the IP VPN performs.

Changing through the service provider service evolution to IP services networking gradual service expansion. Most providers are now offering good coverage in their focus regions so what we're saying is one service provider doesn't really have coverage on a very vast or huge scale but they do very well in their own regional networks.

IP/VPN Roadblock #4: **Unmanaged CE Service**

So early IP VPN service offerings only supported a completely managed service. So when we talk about CE Device or the router this was usually provided by the service provider. Cisco IT along with other enterprises are concerned about the loss of visibility so we're talking about a device given to you by the service provider which stays on your premises.

What we preferred, our option was to go with an unmanaged or a co-managed type solution where we retain ownership of the CE Device. We were also concerned with our ability to deploy new features and functionality of the WAN edge being locked in with the service provider CE Device.

So now what we're seeing as a result of what's happened in the industry is most service providers now actually offer the unmanaged CE service as well as the co-managed where they have limited access to the device.

IP/VPN Roadblock #5: Inter-provider VPN

Roadblock 5. Inter-provider VPN. So now service providers are extending their reach across regions not by buying up bandwidth and services themselves. They're actually extending with other service providers through these inter-VPN agreements.

What we're finding is although it's a very advantageous process for the service provider to extend their footprint, what we're seeing is a feature parity between regions doesn't always come through so Cisco IT get rather concerned when a number of our service providers are connecting via inter VPN services and again we're finding this one harder to challenge.

What we're really focusing on is keeping the IP VPN providers local to our region rather than go for that big huge area and I've put that at the bottom. Not a technology problem. It's really an industry problem where service providers need to work with each other to close the gap.

Cisco WAN Strategy

Okay. So we've talked about some of the roadblocks. What I'm gonna focus on now is our WAN strategy going forward.

Global WAN Strategy

So our global WAN strategy and this is taking what I've talked about previously into consideration. Globally we will maintain a global TDM based network. This is known as CAPNET internally at Cisco. Cisco All Packet Network.

We'll be looking to utilize IDC hosting centers as a major node points for connecting regions. Regional WAN networks will span off this backbone allowing for maximum flexibility so the reason why we've taken this approach is based on the different geographies around the globe we find some areas has very good IP VPN or service provider type services whereas others don't. So it gives us the flexibility to try and choose where we're going with our option.

The regional WAN topology as I've said to be dictated by the market factors and SP capabilities and the primary choice we will take for implementing these wide area networks will be IP VPN where the capability exists. Elsewhere we'll move to TDM.

Backbone Network WAN

This is a quick view of our global background. Again known as CAPNET. This is a TDM based network that spans the globe and this is a snapshot as of 2007. You can see it's a complete ring round the globe connecting the two ends of the screen from Amsterdam through to India through quite vast circuits as you can see on the cupola.

Regional WANs (IP/VPN or TDM)

Some of the regional WANs whether they be IP VPN or TDM I've defined some of the regions here. For example in Europe we have an IP VPN spanning the whole region. Same in the Middle East. Africa we've turned to TDM. Again, it's a challenging region. We felt we were better positioned for TDM.

And that theme sort of carries through the different regions. As you can

see the emerging markets will fare a little worse than the emerged markets but obviously we're closing the gap to try and bring them to same level.

IP/VPN SP Selection - Factors

So some of our IP VPN requirements. Some of our must haves are the QoS transparency end to end. I mean that's a real must for us because we run so many different applications and services that take advantage of the QoS policies.

We look for at least four classes of service. We want multicast supported in its native form. We're also looking for practice and reactive monitoring from the provider. We're looking at IP VPN not just as another technology to give us more bandwidth but we're looking at more services as well.

Some of the nice to have features. Cisco running EIGRP as a propriety protocol. We are really looking at EIGRP PE to CE support. We're also looking at co-management of the C solution so we actually maintain ownership of the box whereas the provider has limited access to the device to manage the network and services running across the IP VPN network.

We also like to have class of service reporting and capacity planning management. Again, this helps us forecast looking into the future where to go in driving the cost of the network.

IP/VPN SP Selection - Factors

Okay. We'll look at some of the service providers selection factors. I've listed a few here and some of these are quite important. The financial stability of a service provider is fairly important. Remember the service provider now is the core of your network so you want to actually be sure that your service provider is in business and is so for the forthcoming future.

The reach and node density. We want to be sure that the density of P and P nodes are fairly sufficient to warrant better latency performance between sties.

Of course being Cisco we are looking for Cisco powered networks out there. It's a twofold issue for us. Mostly it helps Cisco from a market perspective but also the provider being able to access our devices and we talk about it in the fifth point down. The operating support system. Can the provider support Cisco devices and report on them? And that's why we look for Cisco powered devices within the service provider.

Flipping back one to the capabilities. We want to be sure that the provider can support QoS, multicast, all the various capabilities that we had before and I expect to run in the future. Some of them may be IPv6. So that's quite important to us as well.

The OSS, the operating support systems of the provider. We want to be sure we don't need to know in specific detail what the service support system is. But we'd like to be sure that the system they have in place does meet our needs. So it's a general understanding of the OSS in place.

Performance and capacity. This is obviously key. No one would move from one service to another without ensuring some performance improvements and ensuring the capacity is there to drive the bandwidth demands.

The inter VPN agreements. We talked about some of these earlier on. If they are in place we want to be sure that the provider does have the transparency all the way through down to its inter VPN partners.

And obviously SLA commitments. We want to be sure if any of the latencies are breached we are talking about an any to any type network. It's much more difficult to measure the latencies so that's kind of a key piece when we're talking about IP VPN networks as the lot of service the provider is giving to us.

Latency

Okay. I've put this screen up as a measure of performance. Latency is our primary measure of end user performance. This is what we're really focused on when we're talking about performance. Not just to our users but the providers themselves.

It's very important for real time, interactive traffic. We can see where asymmetric parts exist and the service provider should aim to make an estimated latency matrix to show how site to site perform over their own network and then obviously it's gonna be an estimate because the end nodes don't exist at the time of provisioning.

So I've got an example latency matrix there. And you can see I've just put 14 sites across 14 sites. And this is a real example of how an IP VPN performs and what's being shown in the diagrams is a delta of how our current network performs against a particular service provider offering their services.

In most part you can see we've got green boxes which is good. We've got times that are improved 20 milliseconds over and above what we have today. We've got some yellows which show a marginal improvement both between 1 and 20 milliseconds. And then we've got the orange or red sites that show degraded performance. And you can see a few of those.

And these are areas you can use to pick up with your service provider where they seem to be having issues with either P nodes or whatever they may be. This matrix does show a lot about how the performance is there.

As I said the latency matrix can show the underlying infrastructure. So I talked about asymmetric _____. I'm gonna give you an example. So we can see for example Site 6 communicating with Site 4. Now we can see on one leg, so we take the left-hand side. Site 6 is 100 milliseconds to Site 4. Now if we take Site 4 to Site 6 on the opposite side – so we take the top column Site 6 to Site 4 we can see a degradation of minus 80.

Now that's showing that one direction we're getting a very good performance improvement. Whereas on the reverse path we're getting a very bad degradation of service by 80 milliseconds. And those areas to pick up.

Jonas Hurst:

That's what you're calling asymmetric?

Dipesh Patel:

That's what I'm calling asymmetric where we see one path is much faster than the part coming back.

Jonas Hurst:

Okay.

Dipesh Patel:

And that can play havoc with interactive services such as voice over IP video. You certainly don't want voice phone calls to be heard very well in one direction and not too on the way back.

Jonas Hurst:

Right.

Dipesh Patel:

Now, once you've set these figures in stone, you've had these discussions with your service providers, you can use these as part of the SLA agreement to ensure SP accountability. And then Cisco IT have done exactly that to ensure we have the agreements in place with our providers based on real performance of the IP VPN network.

Cisco IT EMEA IP/VPN Implementation

Okay. So I'm gonna talk to you about the implementation in the mirror of the IP VPN network that we had here.

Cisco's Intelligent Network Infrastructure

Europe WAN FY'03/04: IP/VPN

We have a primary and secondary IP VPN provider. Now going back as you can see it was fiscal year '03/'04 we were one of the first companies out there, amongst a few other enterprises, to move exclusively to an IP VPN type network.

We had hard to reach sites within Europe _____ connected by Cisco hub sites by the traditional TDM based circuits or lease lines and this is where the provider didn't have the reach or we felt it was a challenging area as I mentioned earlier on.

Our secondary IP VPN provider gave us back up to these major sites that we had in Europe. Obviously we're putting all our eggs in one basket with one provider. We had a secondary provider just to give us the resilience there to ensure we have service provider redundancy.

Now I'm gonna go through some of the key implementation features of what we put in. We went for an unmanaged service so Cisco maintains control of the customer edge router, configurations for the new features and network visibility.

The service provider has limited management access to troubleshoot and maintain their box as well as the network. The transparent service provider's drop in network with transparency so that Cisco's network retains its integrity and does not have to be designed around individual SP offerings.

Now in a word, what this key implementation feature has given us is actually the service provider has more access into our network. Or the C Device. We're actually seeing less of our operational staff working on these boxes and more of these services moved towards the service provider. So it's been a benefit if I can say in this one slide.

This is a snapshot of what we have in Europe. You can see the various sites around the edges. You can see the two providers _____ VPN one and the VPN SP two in the inside core connecting the major or the most important Cisco sites in Europe.

Cisco's Intelligent Network Infrastructure

IP/VPN Benefits Realized: EMEA

So we're gonna talk about some of the benefits realized. So the total cost of ownership reduction. What we can see or what we have seen since is five dedicated WAN staff consolidated within the remainder of the network support staff. So we've reduced the effort by about 20 to 30 percent. Capacity planning efforts have been reduced. Again,

service provider has taken on more of these tasks.

The network engineering efforts have also been reduced. We are now leveraging the SP core, the SP facilities to move circuits and integrate more circuits. We're not housing if you like massive equipment to aggregate lots of circuits and it's now one or two boxes per site.

The troubleshooting effort's reduced as Cisco leverages a service provider process. And as a result we've seen network availability improved. I mean as you can see from the slide the average daily downtime has been reduced from 6.3 minutes to 2.3 minutes as an average through proactive co-management of services.

Network reliability has improved as the number of priority one cases have decreased which is what we term as the highest level ticket for opening up any issues.

Cisco's Intelligent Network Infrastructure

IP/VPN Lessons Learned: EMEA

Jonas Hurst: Right. Now Dipesh, finally what are the lessons learned?

Dipesh Patel: Okay. Let's go through some of the lessons learned in particular with the EMEA implementation. What we found with the circuit cost in particular when we looked at the raw bandwidth versus the IP VPN circuit cost they were within 10 percent of each other. Also being one of the first major enterprises to implement this kind of service on this scale, we found there is a lot more effort working with the service providers to shape the service.

Now this is a one-time effort and an example might be developing the QoS policy or working out the SLA agreements. Those kinds of things. But the effort was regardless there.

Some of the troubleshooting issues but a little more complex to tackle. Remember in the past we were looking at TDM based network where the engineers have full access to every single node. Now we're talking about the MPLS based network or MPLS VPN based network in the heart of the network where the engineers on the Enterprise network don't have access. So it's a bit of a mindset difference but as time goes on I think engineers actually enjoy the fact that they don't have to deal with so many elements or tedious tasks.

Some of the migration plan or the migration plans is extremely important. So when you're looking at moving from a TDM hierarchal type network to an IP VPN flat network there's a certain number of issues you need to understand. A bit tricky but again those are some of the lessons that we learned as we did the migration.

Q&A

Jonas Hurst: Okay. Good job Dipesh but I'm not gonna let you go yet. I've got two or three questions.

Dipesh Patel: Sure.

Jonas Hurst: Some of it you touched on already but just in a nutshell then what are some of the major benefits of this IP VPN network?

Dipesh Patel: I think the benefits vary. We've learned a lot over the past few years. The major benefit being an IP VPN based network. We have Layer 3 reach ability so the services that the service provider can offer are much more enhanced when we compare that to yesterday with TDM was a

pure circuit end to end where the service provider had no insight into the network. So it's been a major benefit.

Also offloading some of the network management to the service provider has been a major benefit to ourselves as well.

- Jonas Hurst:* I was gonna ask you about that next. Actually. I mean you have touched on this but I've been able to tell as well. There obviously have been some concerns with handing over –
- Dipesh Patel:* Sure.
- Jonas Hurst:* The management to the service provider. Talk to us about that.
- Dipesh Patel:* The issue is when we look back to 2003/2004 when we implemented these services there was a lot of unknown. Remember I said to you it's a very new service. Do we trust the provider? So what I like to call it is a leap of faith. We give this network to the service provider and we don't talk about them as an external partner. We actually partner with them. We've also used the word smart partnering or the various terms. We're actually working together on one common network.
- Jonas Hurst:* Yes. So despite the fact that there are concerns you're obviously very confident in it as well.
- Dipesh Patel:* We are very confident and looking at the track record – we're now in 2007. We've had a very good track record with our provider and everything's been I should say great.
- Jonas Hurst:* All right. Good. Well, long may that continue. Now, finally, why didn't Cisco build a similar IP VPN network as it has in the U.S.? Why is it so different?
- Dipesh Patel:* Very good question. It comes up all the time. When we're talking about IP VPN networks, again, it's a very new technology. We need to talk about economies of scale. And in the U.S. if you look at a traditional TDM based network it's fairly cheaper to buy a TDM based network in the U.S. than it is in the European side of things. You've got lots of different countries. Lots of different registration between different countries. A lot more difficult to provision that type of network. So it works out more expensive over here.

IP VPN can be seen as a more attractive option at least for Europe for the moment. Now it doesn't apply everywhere, i.e. the U.S. where they have masses of bandwidth and provisioning circuits aren't as expensive as they are over here. It makes sense to stay with TDM.

But when that time changes or when the climate changes, yeah, it makes sense to move to IP VPN.

Further Resources

- Jonas Hurst:* That's fantastic, thanks very much Dipesh, that's all we have got time for right now. And for more information about technologies and solutions deployed at Cisco, you can go to the Cisco on Cisco site where you can find case studies with information about what we deploy, what benefits we've gained what lessons we have learned, and some operational practices and presentations to help you learn more. Below that, you'll see a toll free number you can call for more information, or to place an order, and you can order Cisco resources on the Web from the URL at the bottom of this page.

I'd like to thank those of you watching for spending this time with us and for being interested in what the Cisco on Cisco Technology Tutorials are all about, we hope that you have enjoyed this seminar, and thank you to Dipesh for spending this time with us and sharing with us

your knowledge, your expertise and your enthusiasm for IP VPN.

Dipesh Patel:

Thank you Jonas, it has been a real pleasure.



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.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)