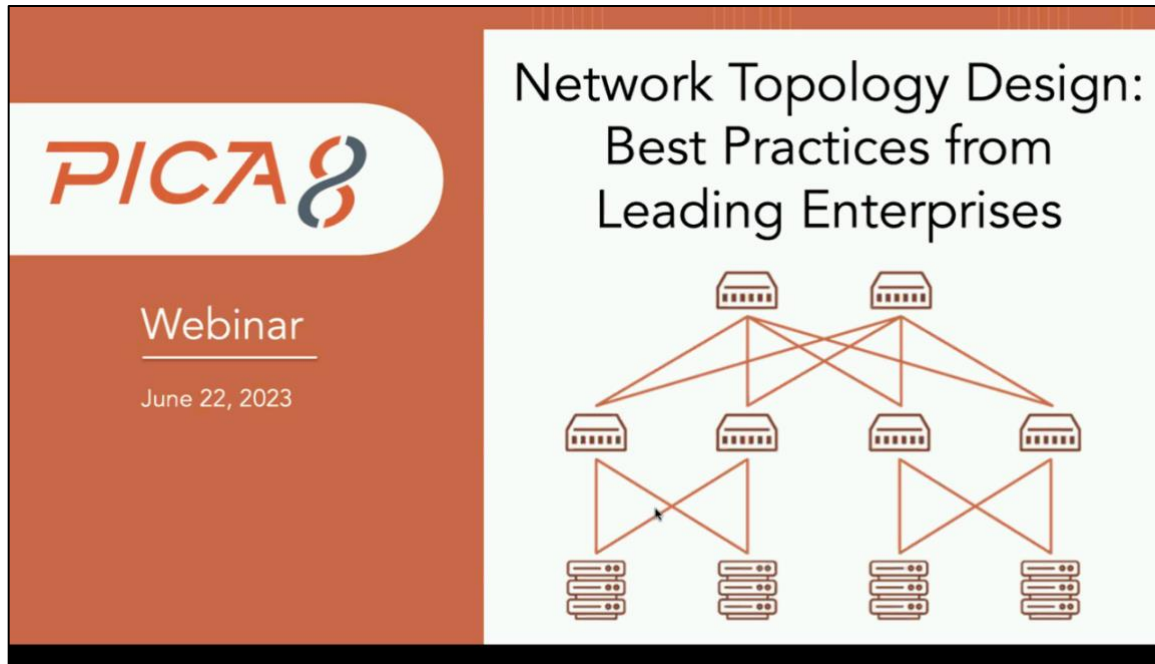




Network Topology Design Fundamentals

Skill Lab Transcript



Summary

Pica8 hosted an engaging skills lab to learn about [the fundamentals of network topology design](#) from founder and CTO James Liao.

Enterprise networking is increasingly complex, especially at the access layer where a diverse set of devices, applications, and users need to be connected.


This can be difficult to maintain and keep secure, while simultaneously meeting the needs of an agile organization. Incorporating network virtualization and open software into your topology design will help you meet those needs in a more flexible, scalable way.

Transcript


Ben Moore, VP Product 00:00

Alright, looks like we're getting a good group of people here today. So welcome and thank you for joining our webinar on the fundamentals of network topology design. We're going to talk about how upfront planning can save you time, money, headaches, and what you need to do.


Today's Speakers



Ben Moore
VP Product
(moderator)




James Liao
Founder & CTO



Neal Trieber
Solutions Engineer

Copyright © 2023 Pica8 Inc. All Rights Reserved | 2



So really quickly. I'm Ben Moore, I'm the VP of Product here at Pica8 and, today, we're going to be joined by James Liao, who is the founder and CTO of Pica8. If you didn't know this already, and you aren't familiar with Pica8, James is kind of one of the godfathers of software-defined networking. And so we're really excited to hear from him today, because he's a continual participant in terms of what the world of Open Networking is doing. In addition, we also have Neal Trieber, who is a sales engineer on our team, and he is going to handle questions and answers. He works with customers like InfoSys and Verizon to implement these networks in different use cases such as campus retail branch and data center.

So speaking of Q&A, we do have the Q&A button at the bottom of the Zoom panel. Please use that to send us questions. We'll take time during the webinar to answer some of them as they relate to specific topologies that James talks through. Otherwise, we'll address the rest of them at the end. So thank you so much for joining and James. I'll give the floor to you.

James Liao, CTO & Founder 01:00

Thank you, Ben. Hey, thank you guys for joining the webinar. This is a pleasure. It's really exciting to share with people what we have been seeing in the last 10 years in the networking industry. We started the whole journey with SDN and we started the journey. We know that this is going to completely change the world meaning change the how networks work. And we're seeing a lot of a lot of changes and a lot of accomplishment that already and they are even more coming in the networking industry.



What You Will Learn Today

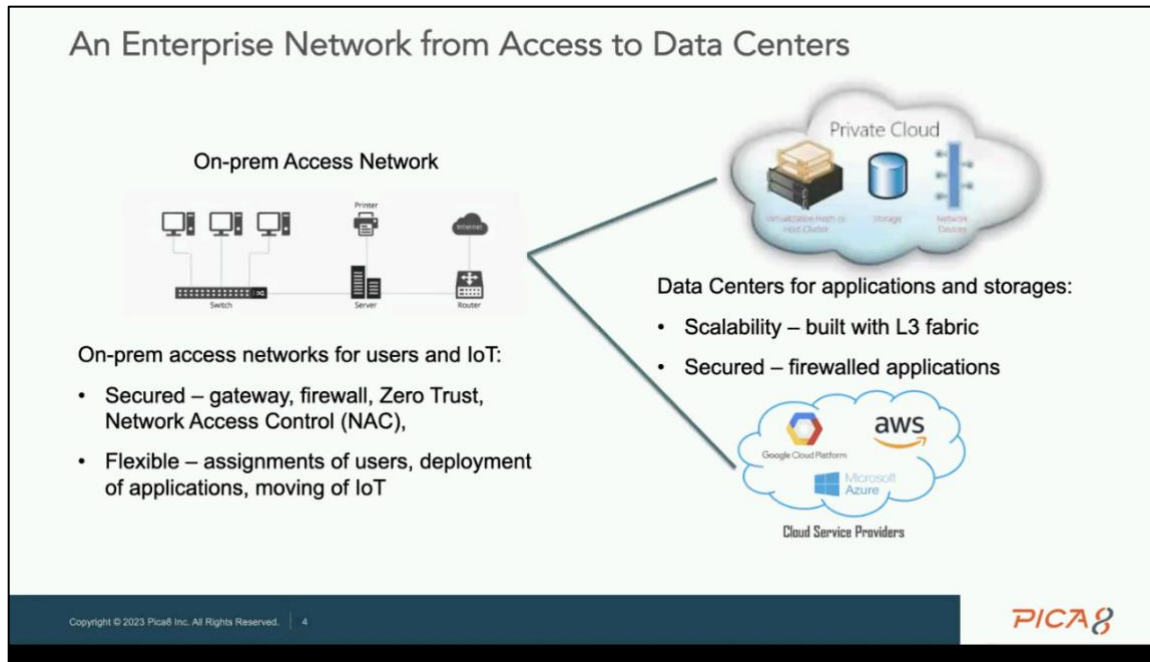
- ✓ How to design an enterprise network – from Access to Data Centers
- ✓ When to consider network virtualization
- ✓ How to build a virtual network
- ✓ Which topologies work best for virtual networks

Copyright © 2023 Pica8 Inc. All Rights Reserved. | 3



So today in the webinar, we're going to talk about how do you design your enterprise network from access to the data centers. And we're going to also cover when do we consider network virtualization and what kind of things we should consider? Why do we want to do network virtualization? And also we are going to talk about how to build it. And then we're going to show you some of the demo that we're doing already. To show you the how this whole virtualization, virtual network that comes together and then the most interesting thing is that which topology will work the best for virtual networks.

All these are interesting topics and I have to say that when we started the SDN journey, we know we're children our work is going to be a huge deal for the for the networking industry. We just didn't realize this will go so big and so far into every single corner. And into enterprise into telecom into data centers. So it's a really exciting journey. And we'd love to talk more, feel free to post your questions in the q&a or chatting area. Ben will help me to collect the information and then if we find the right time, we're going to inject the questions into the discussion. And hopefully this is a good discussion for all of us.



In this one...so before we get started, we want to talk about what the enterprise network looks like, from access all the way to data center. Usually when people talk about enterprise network, they are thinking about on-prem access only meaning that hey, I have Office, how do I set up the office network? How do I connect the users into the office? But if you think about what has changed in the last 10 years, office now is not only for people is also for a lot of robots as well or a lot of sensors. So now the enterprise network or on-prem Access Network is not only for people to take a laptop into the office, set up the connection and start working. They also control your TV, your projector, your temperature sensor, your cleaning robot on the ground, or even cameras on the wall, car keys to enter the building. So it's set up for a lot of things and the things is different from human has identity but the things come and go expand and shrink all the time.

So on the on-prem side, we're seeing a lot of challenges in setting up the unplanned access network. Security is the top issue that so for example, if you think about the today's enterprise network, if you need to set up a camera, what do you do? You have to set up a network for the camera. You have to make sure the camera cable go all the way to the right board and connect to the right port, right. A lot of people will say hey, a lot of cameras are wireless but if you think about that wireless camera is unstable, it can be hacked. It sometimes it is just go offline. And when you set up the system, you always have to have network engineer to set up the connection for the camera. So this is difficult for the facility, facility planter as a difficult for the network operator as well. All because of the security all because of the flexibility. So when we are designing the access network, we have to think about security first. And then how do we scale or make it flexible so that audit people can build on top of the network infrastructure without disrupting the traffic of other network users. So that's the on-prem side, even though a lot of people are moving their compute and storage into the public cloud. Many, many enterprises still have to maintain their own private cloud. And, for many reasons, for privacy



reasons for compliance reason for data sensitivity, in the future for AI this kind of things will continue to go. So for it not only you have to set up anon-prem network, but you also have to plan how do I connect the on prem network on-prem private cloud and then when you are building the private clouds, You of course, the first thing you think about scalability, how do you scale the data center? And then from there, you have to think about security as well because you don't want one group of application to pollute the other group of application.

So these kinds of challenges are the enterprise challenges enterprise is seeing every day so so this is the overview of the enterprise they work in my be helpful that since we are learning from the leading enterprises, we work with the with the leading SI (system integrator) company, who set up three buildings. Each building has seven floors and hundreds of users and 1000s of devices inside the building. They come into the building every day since they are a SI (system integrator) business model is that they have different groups of people working for different clients. And each each group of people can only access the project, the related project in the data center.

So if you think about the kind of environment you have, you have one engineer working on for example, HP project today. Tomorrow they are going to this engineer moved to Dell project. How do you guarantee that the material or the documents of the HP project are not copied? Or being transferred to the downside, right? So you need to make sure that users when they log into the system, they can only access certain documents and certain storage. That's the user side. Usually people solve the problem with identity. What about what about camera? You set up a one camera for one building for a group of people tomorrow, you need to set up another camera. And these two camera even though even though they don't talk to each other, they have to talk to applies in the data center. Both of them and you want to make sure that they the camera cannot access the data of other network or other application because people can have the camera eventually go through the internal link to the other side. So you are now seeing the enterprise challenges that you need to have flexibility and you need to maintain the security. And in the meantime, networking engineer networking operator is sitting in between everybody requires the changes and everything I change can change the whole network. So being able to separate the physical network or from the real workload or workflow is going to be really important.

So with that said, when we're designing a network we have to ask ourselves, what kind of things do I have? Do I have to consider when I set up the network?

Major Consideration in Designing Enterprise Networks

- How do I operate the network?
 - Do I need to be on site most of the time?
 - Do I need other team to connect the cables?
 - Do I make every line of configuration changes?
- How to secure my access network?
 - How to add users or remove users without creating network problems?
 - How to create new organization without creating network problems?
 - How to move people between organizations without creating network problems?
- How do I scale my data center network?
 - How to ensure the network is stable with hundreds of switches?
 - How do I dynamically associate the applications together?
 - How do I design the gateway and firewall to route the traffic?

10:49

I'm always when I talk to customers and help them to design the network. The first thing I ask them is that well, maybe before we start saying that, how do we design the network? Let's think about how do I operate the network first? Right? Do I need to be on site most of the time, so we have one customer who has 2400 stores in in the US their network engineer of course cannot be on this on the site all the time. So they have to remotely working on the on the network. Even when they are setting up the new store. They cannot be personally there so they have to rely on contractor to set up the network.

So that brings up a very interesting problem that the contractor even though they are network savvy, you give them the design they go on side one day connecting all the cables testing everything is okay. And the other day that when you are testing the network you before the store so you shut down one switch or the connection go to the other switch and then you find out one cable as well. So what do you do? You have to start troubleshooting the problem or even asking the contractor to go back to the store to test it. And this is not only in the store. This is happening in the data center as well. So when you are setting up the scalable data center, some of the data centers are so remote you cannot be personally remote outside. So you have to set up things in a way that even if they connect to the wrong cable, you can quickly recover it from there. You don't bring down the network and you have to set up the network in a way that if you make one line of change the fellow the failed zone is only on this subnet. It won't propagate through the whole network and bring down the whole network. So that's the first thing you have to think through that what kind of things that how do I how am I going to operate the network?

And then from there, you start to think about how do I secure my access network because on the access side, it's not only that you have to protect the access network or from the external attacker because today most of the people when they think about security, they're thinking, hey,



I have to Gateway protection over there. So nobody can go from internet to my site. But guess what, most of the time the problem is not from outside to inside, is actually waiting inside. So we have seen if you Google the internet, you will find a very interesting case that we're in Las Vegas. There is a fish tank with the internet connected sensor to control the fish tank temperature. And then people figure out how to hack the sensor. And they eventually go through the essential connection to go to the casinos, casinos database and then just basically download the whole database out of the casino.

So this is the real case. So security on the access side is not only that you cannot only just plan to protect all the gateways because inside the campus, everything has to be protected. So zero touch provisioning is going to be really important network access control is going to be really important. So and that's a that's a security and when you're considering security, you have to think about, hey, how do I minimize the security scope so that when people remove, add or remove the users, they don't have to call their operator and say can you make this change for me? Or when people create a new organization and move the people around? They don't have to call network engineers and say, Can you change this guy's VLAN for me, and when you move the people around or you some people leave the company, you don't have to call a network operator and say can you disable this guy for me? So that requires not only the planning, but also some of the automation as well.

And on the data center side, you have to think about scalability, right? How do you make sure the network is still stable with hundreds of switches? Today, most of the people think about, hey, if I have five if I have five racks I can easily add the sixth and the seventh and the one you are adding those racks you have the template that you can do to make sure that it's a minimum disruption to your network. But you have to also think about that. How do you minimize the change scope so that when you are adding new racks, the addition of the new records pose no threat to the existing infrastructure. So all the things are the design engineer that network design engineer has to think about before they start the operations.

Network Virtualization with EVPN

- It is critical to separate Underlay from Overlay
- Underlay should be secured, scalable, and stable
 - Built with L3 protocols
 - OSPF or BGP for control protocols
 - ECMP for redundancy and speed aggregation
 - No VRRP for Gateway
 - No MLAG
- Overlay should be dynamic, secured, and minimized fault-zone
 - VTEP should be at the Underlay L2/L3 boundary, bridging the virtual L2 with the access L2
 - L2/L3 Overlay is built on top of VTEP

So with that, that leaves us to network virtualization. I assume that many of the audience have already known network virtualization and EVPN. But let me just take two minutes to go through network virtualization concept. The concept is very simple. You want to have an underlay network. It's almost like a bare metal network that every connection is stable, very easy to add new switches or new capacity to the network without disrupting anything. So the configuration of the underlay network has to be super simple, easy to add easy to do cookie cutting addition to the network. And once you have that, so how do you build that kind of underlay it has to be secure, it has to be scalable, it has to be stable. So traditional network is basically saying that, hey, there is no underlay. There is no overlay.

The way we build a network 10 years ago was that we basically say hey, we have a layer two network and we have a layer three network to connect the layer two together. And in this way, all the all the people share the same attributes go into the same layer two network, and then they go through layer three network to talk to another group of people. If you replace peep users with application is the same concept. The related group of applications are placed in the same layer layer two network and they they go through layer three network to talk to another group of application. And the reason going through the layer three network is because layer three is much more scalable. It's much easier to put firewall in between to control the flow of the data. So you cover the security, you covered the scalability.

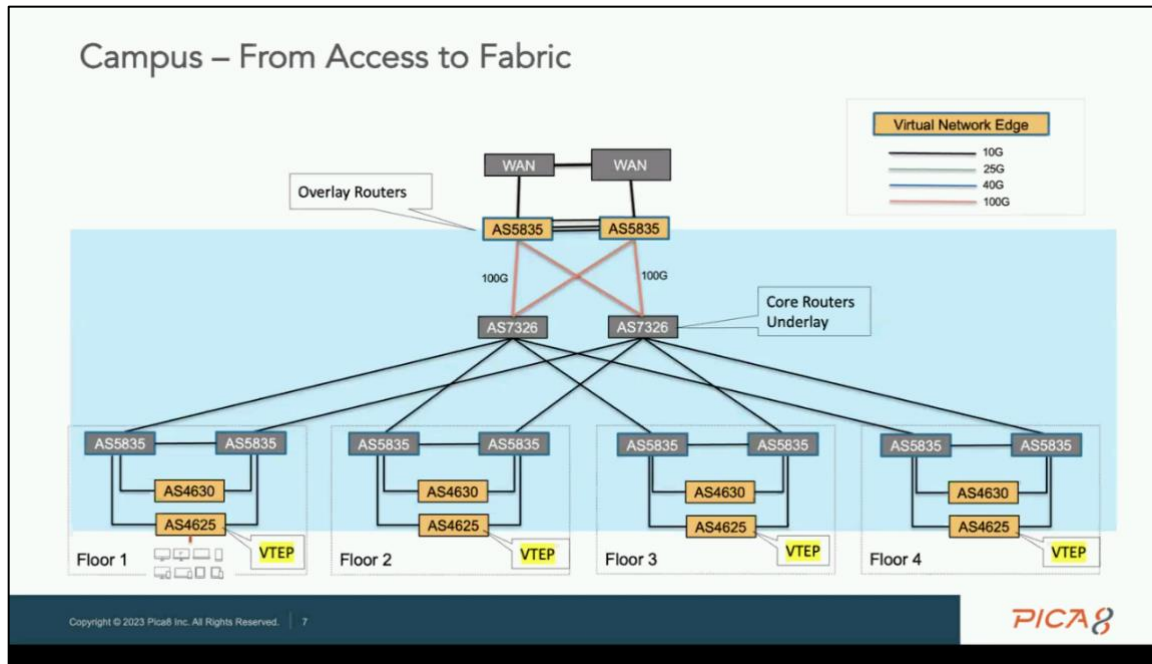
The problem of the traditional design was separating layer two from layer three is that you now have the concept of localization. You have to put the application in the same place or you have to put the user in the same place so that they can share the same layer two, and then connect to other group with layer three. That doesn't work in today's virtualization environment, meaning that storage has been distributed and virtualized server has been distributed and virtualized. Even for user. They don't come into office to sit at the desk every day anymore. Do you literally



argue that users are virtualized too you can work in the office you can work in your home you can work on the beach, you can work in the in a conference room 300 miles away from your office right? You basically you are moving around. So how do you make sure that when they are connecting to the network, they are not just doing the traditional layer two because the traditional layer two cannot go across the location like this. So with that, if you separate the network to say okay, underlay network, we separate underlay from the overlay. The underlay is totally built by layer three. So you lose all the localization, that means that you reduce the broadcast domain and you reduce the security breach, you reduce the possibility of layer two domain But in that case, if you do everything on layer three, now, you have to VPN to everything. You're trying to access. That doesn't work either. So, if you separate the underlay from the overlay, let's say underlay right now is built with layer three everything is is connection based. You can use the OSPF or BGP to to build out the data topology. If you need bandwidth, you can use ECMP to aggregate the speed and redundancy to get the redundancy as well. In this case, you don't need VRRP because no server is going to connect to the underlay network all of them will connect to the Overlay Network. And you don't need MLAG because you don't have layer two domain.

So this kind of layer three network is very scalable. But in terms of application environment or user environment is not very useful because now you have to set up a TCP/IP connection or you have to use a VPN to access the data you want to. So was that once you have an underlay network, you start to build overlay network, which is contradictory to our past learning that layer, seven layer network, right, you build layer one, layer two, layer three and then on top of that you run layer four layer Fie, layer seven on top of that, but now with the overlay underlay on the underlay side, you have layer one, layer two, layer three, and then on top of that on top of layer three, you start to build layer two, layer three, layer four and layer seven on top. So what's the virtual layer two building on top of the physical layer three, you now have a virtual network that you can make it would make it work. So how do we do that technology Lee with the technology we're gonna go over that in a bit but with this kind of overlay network that you now have a way to virtually pool things together was a layer two domain and all those things used to be localized now can be distributed, but virtually localized. So this is basically done by using VTEP. The tab is called virtual network terminal endpoint. It will just build up the endpoint on top of the layer three network and then create a layer to and from on top of that. So that's the concept of the VPN.

And I think it's enough talking that that's look at the diagram because I'm an engineer as well. I love diagram, diagrams much easier to understand.



So this is an example of, of campus environment in the campus environment is very different from data center environment where racks, buy racks of servers that all have dual homing and connect to top of rack switches in in the campus environment usually people build the rooms or the hubs. Each hub will maintain one floor or multiple hops in the floor in the past 10 years ago, we're basically using old technology like what is the technology that we used to use to basically just connecting a lot of a lot of switches then was the ring topology. But that basically that today most of the people started replacing those topology was the spine leaf technology.

So let's look at the floor one. First. If you look at floor one, this is basically a spine leaf architecture. It's not as visual as the spine, the from core to the hub but if you look at floor one, you basically have two spines which is connecting to a whole bunch of access switches together. Okay, each switch will have two connections to the spine switches. So this provides provide active-active redundancy. In the past, if you build up this kind of things on floor one and make it layer two then people will tell you there is a very, very serious risk that you can mail down the whole floor. If there's a layer two storm running by view or doing layer three, then there is no storm. But so in this way, you basically build up all the connections the all the black wires or BGP connections that build on layer three. And then from there you put VTEP on those access switches like as 4625 or these are edge core switches, Edge core as extensive line of Gigabit Ethernet switches with POE or without POE right so this allow you to build the virtualization VTEP on top of those excess switch. So then you have your server laptop, IO IoT devices connecting to the access switches and then across the network that you then dynamically connect the AMI associate two devices or more devices into a layer two across the layer three functions. And then from there, once you build up the campus environment, when you are designing the network, you also have to think about how these overlay network is going to go through the window to the to the to the internet. So you need to have the when device connect to overlay routers and these routers terminate the VTEP VTEP that the Vtab VTEP



traffic come out of the overlay routers and go to the external network it just like it did the typical traffic. So far, so good. Any question?

Ben Moore, VP Product 26:00

James, there was. I think there was one question and there was also a comment. So first, the comment I think the technology that you're trying to remember was token ring. This is from the audience.

James Liao, CTO & Founder

that yeah, token ring is a pretty old technology. There's a there's a way that you can have a switches and connecting with a proprietary cables together. And that just escaped from me that I just don't remember the term but this is the term that a lot of people there's even today a lot of people are still using it is Ethernet technology, but I just it just doesn't come to me.

Ben Moore, VP Product

Okay, well it happens. No worries, even to the best of us. So, so, so question for you on this particular topology: what can't I do with my current network that investing in a move to a new fabric will do for the organization and ultimately the operator? Right?

James Liao, CTO & Founder

Yeah. Oh, that's a great question. So a lot of people have already built layer two layer three network in the way layer two is on the edge and layer three is basically an aggregated switch. And so the great thing about virtual network is that virtual network is not only exclusive to VTEP. VTEP actually a bridge between the local access network and the virtual network. Meaning that if you have a have a local network running layer to VLAN 200 For example, you already have a local network around in VLAN 200. You can easily create a V tabVTEP next to it and then connect all the VLAN 200 traffic to a V tab running for example, a different VNI means the virtual network virtual network ID. So basically just say you have VLAN 200 All the VLAN 200 will join vi 10 200 Right. So in this way, the VLAN 200 Local VLAN 200 can start to connect through 10 200 to the remote VNI connections to another VLAN right that VLAN could be 200 could be 300 Could be anything. So this provide a way that you can migrate from the traditional network to the new new virtual network. You don't have to completely tear down the network and then start building a greenfield build out from there. You can start migrating your network one by one to the new network architecture. Great question.

Data Centers – from Top of Rack (ToR) to Fabric

- Multi-chassis Link Aggregation (MLAG)
- Multi-homing
- Virtual Extensible LAN (VXLAN)

© 2023 PICA8. All Rights Reserved.

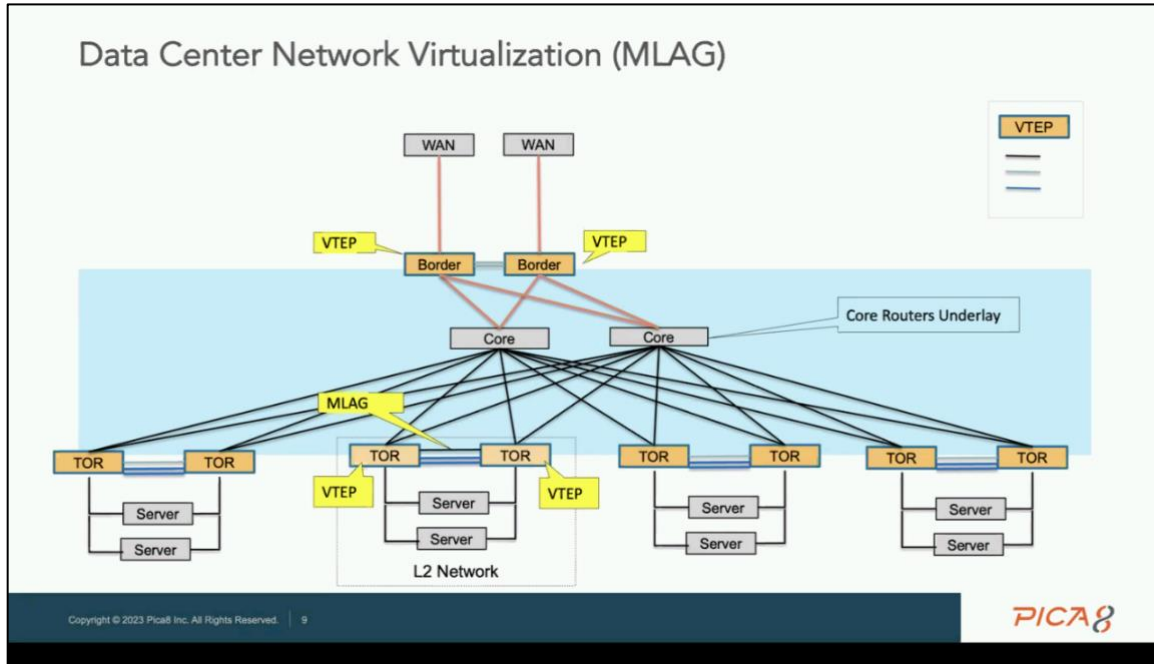
28:30

So with that, we're going to talk about the data center side I think campus side is exciting. And data center side is even more exciting because on the data center side. On the data center side, the problem is actually even simpler. Most of the time data center is homogeneous, meaning that you have a lot of racks and racks of servers. Even though it looks like on the scalability side, it's a really, it's really daunting to think about how do I build 2000 racks of networking together. But if you look at the way they operate each one of them have very, very similar configuration. Right.

So first thing to think about is that how do you plan on the top of rack switches so that when you replicate the racks, you actually can just use a template to generate the configuration or minimize the configuration so that when you are creating the new racks, you don't even need to customize it for you. So, there are basically two ways of the building the three ways of building the top of rack technology the first one is that the using MLAG on top of rack and this is this is your traditional way that we are all familiar with that in the data center. Before network virtualization will basically set up the VLAN in the in on top of rack and then from Top of Rack (ToR). We connect to the aggregation through layer three and started using aggregation switch to exchange the layer three routes to get to connect the layer three routes together.

So MLAG is definitely one possibility to build out. And we're going to show you how that work. A new technology that we are seeing is that by replacing by because MLAG is kind of proprietary technology if you use pi MLAG is a little bit different from the Cisco. Cisco in black is a little bit different from a resource and like right or MCLAG. So that's why some of the people say hey, I rather have a standard technology to work on the multi Link Technology.

So with that EVPN and actually create a standard called multi homing, and this is gaining momentum. A lot of people find it very, very useful. It's a standard base then it can scale even better than the MLAG and we're going to show you how this work. And of course, you still have the traditional VXLAN that you can use to build your network VX LANVXLANE are pros and cons of each approach and we're going to go go through that in a bit.



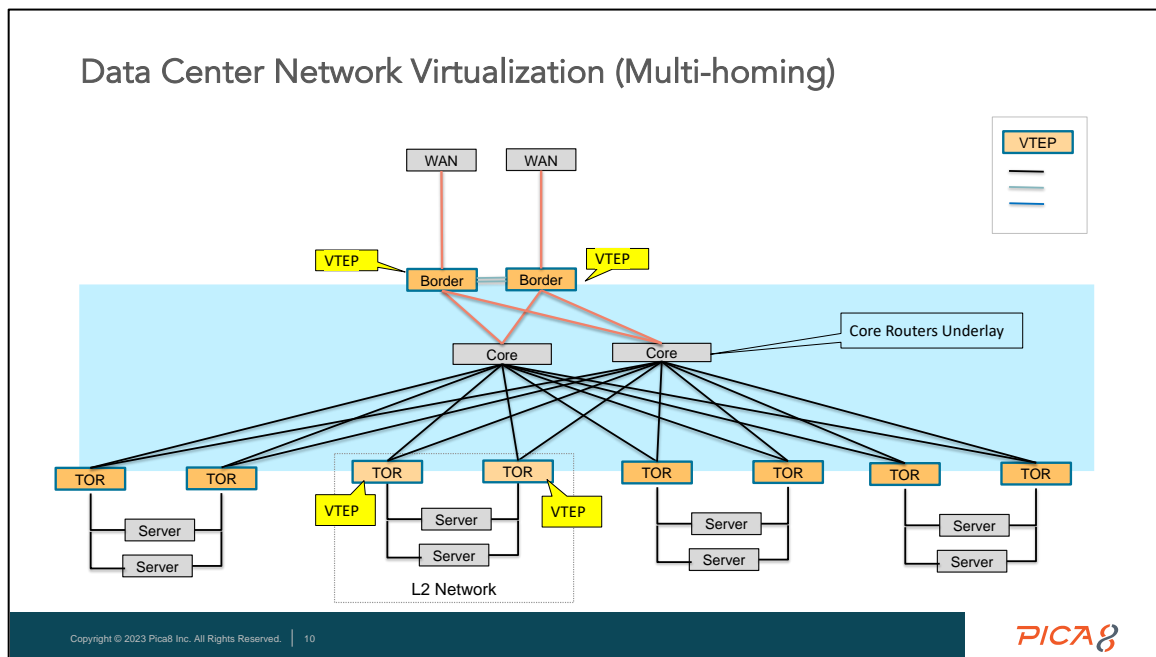
So if we go to the virtualization that store was the most basic configuration, basically doesn't mean that it's bad, it just means that this is the way we have been using and we can add virtual network on top of that. So in the in the traditional way that when we add a server to a rack, we have a choice that we can just set the rack into the same layer two domain or separate layer two domain but basically it's a layer two switching domain.

So you set up to top of racks so that's the use the box over here to show you. You set up to top of racks they form a VLAN M black together and they share the same VLAN partition on the ports. Each server is connecting to two to one port on each top of rack and these top of rack ports or basically pre-defined port one associated port one to another top of rack poor to have this top of rack ticket associated to port to have another another top of rack and in this way when people set up the rack together they can just connect the cables in pairs and then you got you got the the active active bandwidth out of this one.

Layer two domain is pretty easy. concept that people feel comfortable programming. And then from there you start to build the VTEP for underlay network so that underneath or can be run with the BGP are numbered. The good thing about BGP number is it's the minimum configuration that you have to set. You don't have to assign an IP address so you don't have to do all those tedious change every time when you add a new rec by using BGP or number it will

automatically assign the IP addresses for you. So in this way, when you row in the new rack, you can just connect the table up and they will start propagating the BGP information for you.

So basically the dividing line of layer two and layer three is on top of the rack. So in this way you got active, active redundancy, and then it's easy to run a layer two network out of this one. And you still get the word virtualization. So what is the what is the problem of this? The only problem is that it's a proprietary technology, meaning MLAG is a proprietary technology. So every configuration is a little bit different. If you have Cisco Arista pig aid, at the same time, the configurations are all a little bit different. So that's the that's the MLAG system.



And then we're gonna talk about a bit Multi-homing. This is a new concept inside the inside the EVPN concept that you can see that on the top of rack now we don't have the MLAG connections anyway. So we only put VTEP on top of the top of rack switches. The layer two layer three dividing line is still on the top of rack. So the blue box just like the previous slide the blue box is the underlay network go is the IP layer three network. The dividing line of layer two, layer three is on top of rack so that servers still maintain active active redundancy to the network.

Okay, so what is difference? The difference is that now is using the VPN technology to propagate the pairing information between the two top of racks instead of using proprietary MLAG technology to propagate the lack of information. So that's the huge difference. And with this, you got standard based multi Link Technology to go through the top of rack, and build the virtual network. You still get the active active redundancy. It's a standard based and not only that, there are two more benefits that people don't it's not so obvious. The first one is that most of the MLAG technology are only limited to two switches. The EVPN multihoming technology, actually allow you to use more than two two switches or two VTEPs to form t multi-links.



So this gives you the possibility that if you have a server who has four NICs, now you can actually distribute through four top of racks instead of two top of racks. Some people might want to have that, that. That option that if you're running, for example, AI traffic or you're running different type of traffic, so you actually want the different setting on the traffic type on the server side. So in this way, they allow you to use different NICs to send different traffic. So that's one not so obvious benefit. So that's one when you have when you use a multi homing, you actually can scale more than two you can actually use four or even more for the for the interconnection to aggregate things together. And it's a standard base that it's it's basically still allow you to do active active redundancy.

So what is the what is the disadvantage of using multihoming on Slide. The disadvantage is that everything has to be well planned meaning that the ports have to be coordinated together so that when you have a port, so for example, my server a if I have a NIC one connecting to top of rack one was port one, the other port better be identified as for example one right so it's basically port one on this side port one on this side, and you have to reprogram that in your VTEP. Otherwise, if you plug it into the wrong port VTEP will be completely confused because they don't know which port is connecting to what.

So these have to be carefully planned and then carefully executed. This come back to our previous comments that hey, if I want to use use the virtual network in my data center, but I'm not the one building the network. I actually have a contractor to come in to build up all the cables. How do I ensure the cables are correct? So I have to do a whole bunch of things to make sure it's correct, because if they connect to the wrong port, not only it's going to cost me another trip to color, correct the cables. I'm going to have a disaster before I realized that. So that's the that's a slight disadvantage you have. Oh, I forgot to mention one thing about the benefit. Besides that you can scale from two to four on the multi-homing, multi-homing also allow you to choose whether you want to use use the what is that portico the Blackboard got LACP or not LACP to build up the connections, most of the MLAG will require you to use LACP and some of the servers do not support LACP. So that becomes a problem but with the EVPN and it's a standard based it actually satisfied that you don't you can support LACP or you don't have to support LACP so that's another flexibility people have.

Ben Moore, VP Product 41:40

Hey, James, this is really interesting. Couple of questions. One that that came in is on this particular diagram are the are the top of rack shown in this multi homing example Are they are they traditional top of rack or they are enhanced top of rack with hardware VTEP that is built in?

James Liao, CTO & Founder

Oh, great question. These are usually the next generation new generation of switches. That was ASIC capability to handle the VTEP. And that's actually a very good point that that if you have top a racket that's already running layer two, and they don't have the VXLAN or V VTEP capability using MLAG might be better solution than using this type of switches. Because the...



Ben Moore, VP Product

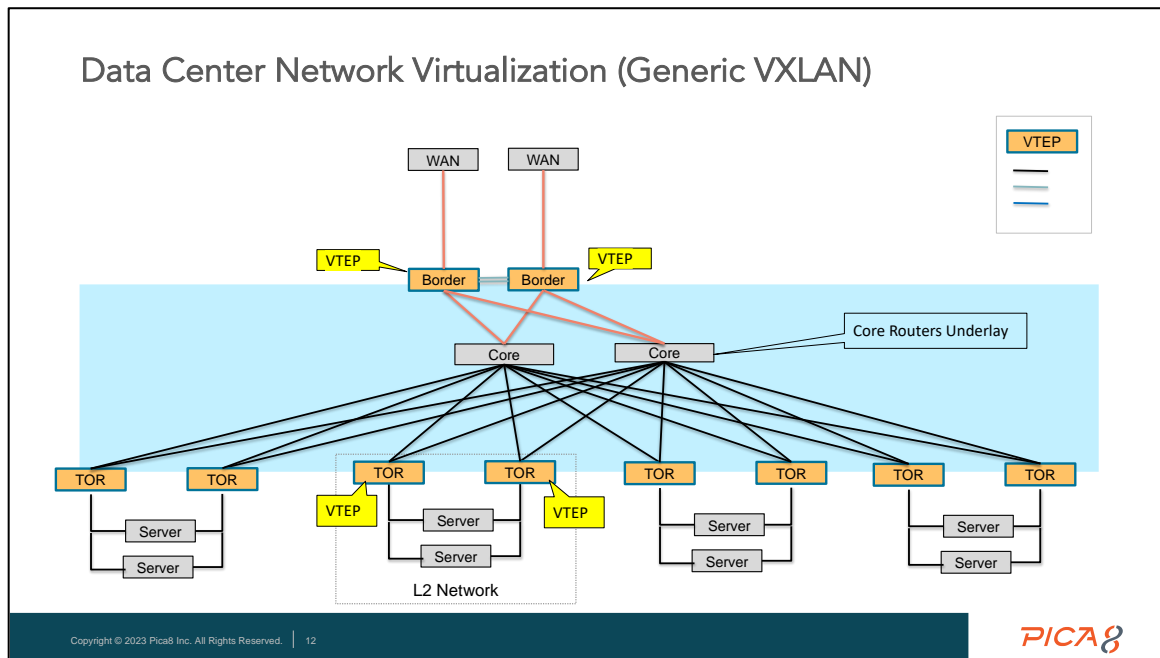
So maybe I can ask a question based on that. James and for some of my own education as well because we see a lot of at least in enterprise engagements the DevOps teams are constantly pushing to virtualize everything right? Want to move towards bare metal Kubernetes versus traditional hypervisor stuff? We're talking about MLAG and multi homing, which is better what do you see more customers moving to? And then I would say the second part of the question is, are there are use cases where folks on the call might want to still look at MLAG versus EVPN and multi homing?

James Liao, CTO & Founder, Pica8 42:00

Yeah. So oh, that's a such a great question. So in the in the data center, from what we're seeing in the field right now. Majority of the enterprises when they migrate to network virtualization, they are considering multi-homing not that they don't like MLAG is just because multi-homing go very well was the whole concept that fabric all the way to the host, right? Because some of the people might want to have the VPN or BGP go all the way to Kubernetes server even though there's a kind of high risk. So when you're planning on that, be careful with what you're wishing for. Because that usually means that the server now has a BGP capability. So it might, it might create some of the routes that you don't want to see or if the server is hacked, then posting certain BGP routes to the network. You've got disaster on your underlay network. But with that said, , majority of our customers are thinking about using multi homing because it's, it's the it's an open standard. It's not, it's not a proprietary solution. It is open standard. Today you are using Pica8 with an open network. Tomorrow. You say, Hey, I have some of the traditional racks. But those are running, running Cisco juniper. Already with the with the multi homing, you can guarantee that the old racks and the new pick a rack that can work together without any problem. Not that MLAG is going to pose any problem. Is it just that for MLAG, you have to do a lot more test to ensure they are compatible. So in terms of customer attraction, I think I can safely say about at least 70% of the customers we are working with they all use the multi homing as the as the topology. Do people still wanted to see theMLAG and MLAG type of acculturation topology? Yes, there are many people who have built the Rex was special application consideration QoS for example, Accesscontrol for example. Even latency is really critical. If you put build everything on top of records the multi homing that they don't see will be impacted because you have to go through the translation of layer two, layer three and they virtually back to layer two. But if you have those application in the same rack sharing the same layer two, they basically can go through the fabric to find each other without going into multiple hops. So that's one possibility. So if you have a rack that was server that's already optimized for local compute and local clustering, you don't necessarily want to use use the multi homing, you can stay with the MLAG, and then only when you need to get to the remote resource. You can go through VTEP at the other side. That's a great question.

Ben Moore, VP Product 45:26

That's great. Thanks, James for answering that. I you know, pleasure being moderator and sort of Master of Ceremonies, I get to make sure that we're moving along timely. So we've only got about 14 minutes left. Today. I do want to remind everyone that we will share the recording and the slides but let's move on to the next part of the presentation. James.



James Liao, CTO & Founder 44:00

Great. So with the limited time I think I want to quickly mention this one because the not a lot of people think about this this way. Most of the people want to optimize the whole infrastructure for active active operation. But there's still a room for people to use generic VXLAN, meaning that you don't form the pair of top of racks into active active connections. Each top of rack is still run as an independent VTEP. So how does that work? If I have a server I have two links to the top of rack. Does that mean that I have to set up a separate network to the top of racks? Yes, you do. So in this way, only one of them will be active because the other one cannot send the traffic. Yes, that's the case. So you end up with an active passive, active standby connection on the server side. But the beauty of that is that the ports are now independent.

So if you have a contractor to call me to connect the cables for you. Then if he connect the randomly to different ports or he mistakenly connect to you to wrong ports, the because the two VTEPs are running in parallel or independently, the network will continue to work. So when you switch over to the other side, the we have technology so so this is something that will be validated was one of our key customers. That when you migrate from one link to the other at all the max will automatically for you to the other side, we solve the Mac of mobility problem and then all the traffic will resume on the standby traffic. So this is this is not a very fancy design by solve very, very fundamental problem that if you have to be remote, and the operation team is independent from the design team, you want to make sure that when they are setting up the topology if they connect to the wrong cable even if you check everything, when failover happens, everything will continue to work.

So this is one of the benefit of VNI. And so this advantage, of course is that you only get half of the bandwidth on the server side but for a lot of application on the server side. You only need




one NIC because each NIC is 100 gig, right? But I want to clarify one thing, it's not that one one type of rack is in standby mode is actually the server has two links one inactive er when you pass it by by distributing the application there's servers traffic on to top of rack that you still need. You still have full capacity on top of rack.

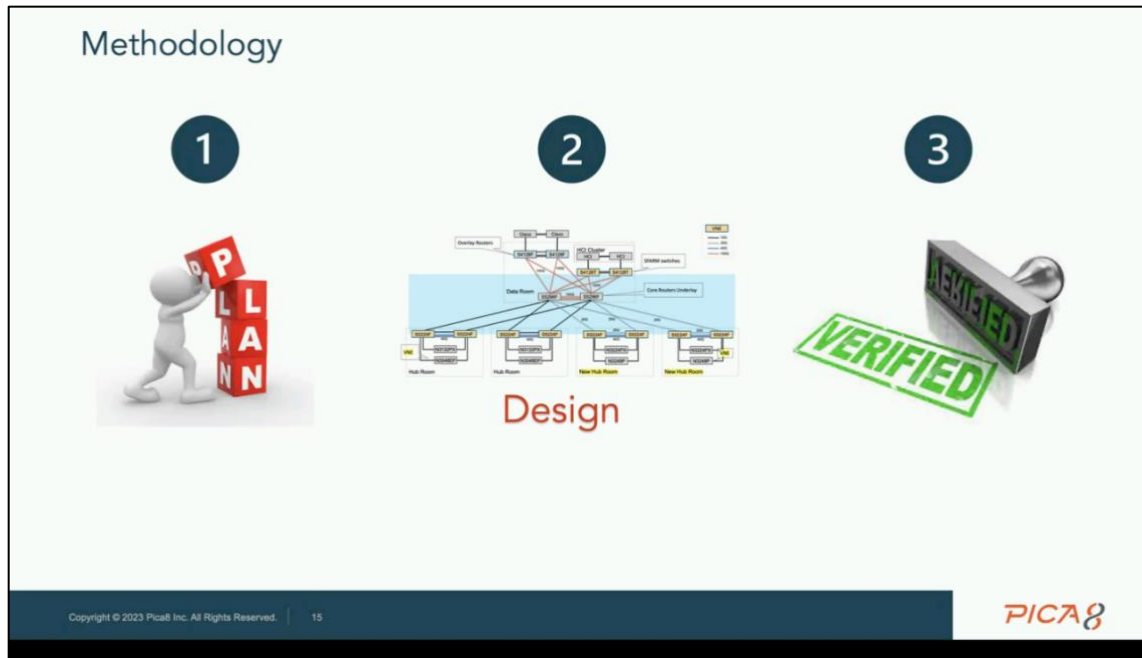
Designing a Modern Access Network

- Separate the underlay and overlay
- Underlay – stable and scalable
 - A spine-leaf L3 network
 - No shared L2 domains
- Overlay - Flexible and Minimized Fault domain
 - Changing the L2 network without touching the physical network
 - Adding the security functions without bringing down the network
- Build it with Open Network !!

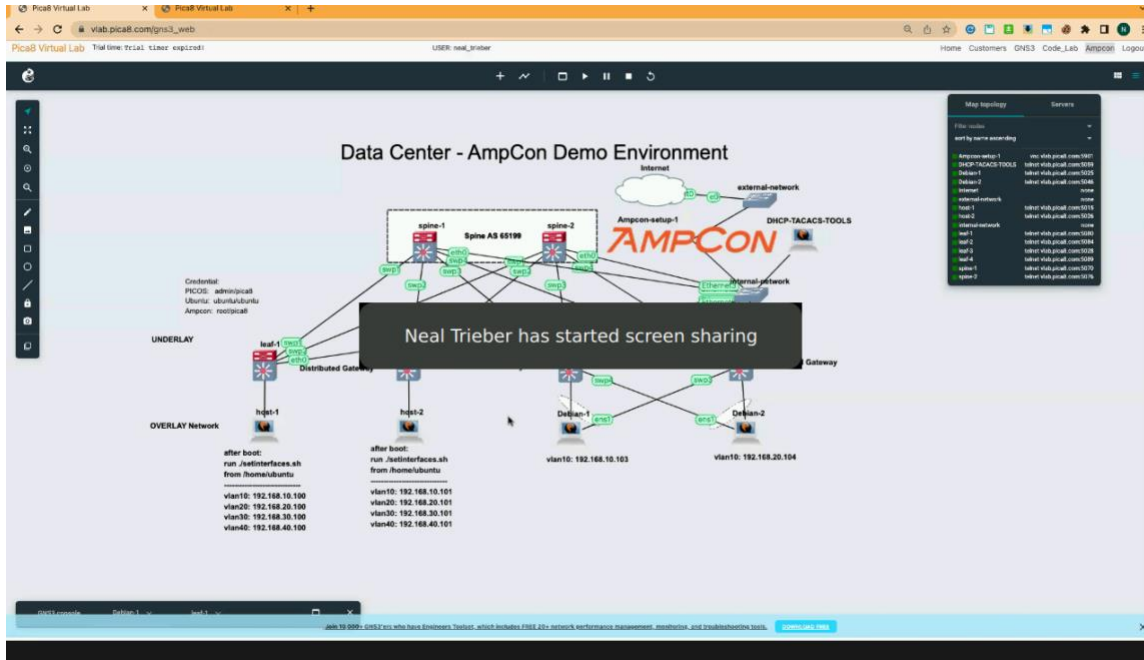
Copyright © 2023 Pica8 Inc. All Rights Reserved | 14



Okay, so this is this is quick summary before we get into a demo that to design that modern network really you want to separate the underlay and overlay because on the underlay side, you can use a spine leaf at layer three architecture so that is easy to replicate and easy to scale on the overlay side by layering layer two on top of layer three, you now have flexibility and the beauty of that is that if you are working on one VLAN on the layer two site you get make sure that it doesn't impact your underlay network. It doesn't impact the other layer two network as well. And most importantly, you want to build it with the open network because if you lock into proprietary solution all the new technology that people are inventing, you basically are locked out of that with the automation with virtualization, all the things that you want to make sure that you go with an open network so you can continue to evolve. Continue to replace the hardware when the new functions is available.



So methodology, this is very quick that we want to get to the key point side in the past when we design the network or the network operator or network expert that like you will do the planning and design and then we start to say okay, let me go over the design, make sure everything is correct. We even set up a small lab and do the testing. Make sure the configuration is right. And then we cross the fingers, throw them into the network and hopefully we don't screw up the whole network. Right. So with that, I think now we have tools that we can do the verification without running that much risk. And Neal is the expert of this one. Let me hand over the microphone to Neal, so that Neal can help us to do a quick look of the how do we validate the design, Neal?



Neal Trieber, Solutions Engineer 50:00

Right. Does everyone see my screen? Can everybody hear me? Okay? Yes. Fantastic. Thank you, James. So what James is alluding to that we are launching what we call our Pica8 V Lab or Cloud V lab. It stands for Virtual Lab. Where we're going to be able to validate our customers architectures so we all know before we go. So that said, now that you are that that said, what you are seeing here is one of the many labs that we have within our V lab. Prefabricated Yes, you'll be able to edit these you'll be able to add any kind of third party vendor appliance application that you want to test within this framework. And for those of you who aren't familiar this is being powered by GNS3. GNS3 is an open source layer layer two layer three testing environment. For those of you who aren't aware it's it's freely downloadable. You can find it it's called GNS three and it allows you to run both layer two and layer three full routing and switching within this virtual environment. And so what we have here is an EVPN mesh. What you are seeing here is one of our beginner labs it also is being managed by AmpCon which of course is our automation and management platform for those of you that aren't aware and what you see here is we have our underlying overlay separated the underlay network of course. And in this example is pure BGP iBGP and EBGP. The EBGP Of course, being run across the underlay, also allowing us to better troubleshoot, but also take advantage of things like BGP on numbered so that it becomes very easy to template and automate and create our EVPN and VXLAN mesh.

Ben Moore, VP Product

Oh real real quick. question coming in hot. Does this support EVE-NG?

Neal Trieber, Solutions Engineer 52:00

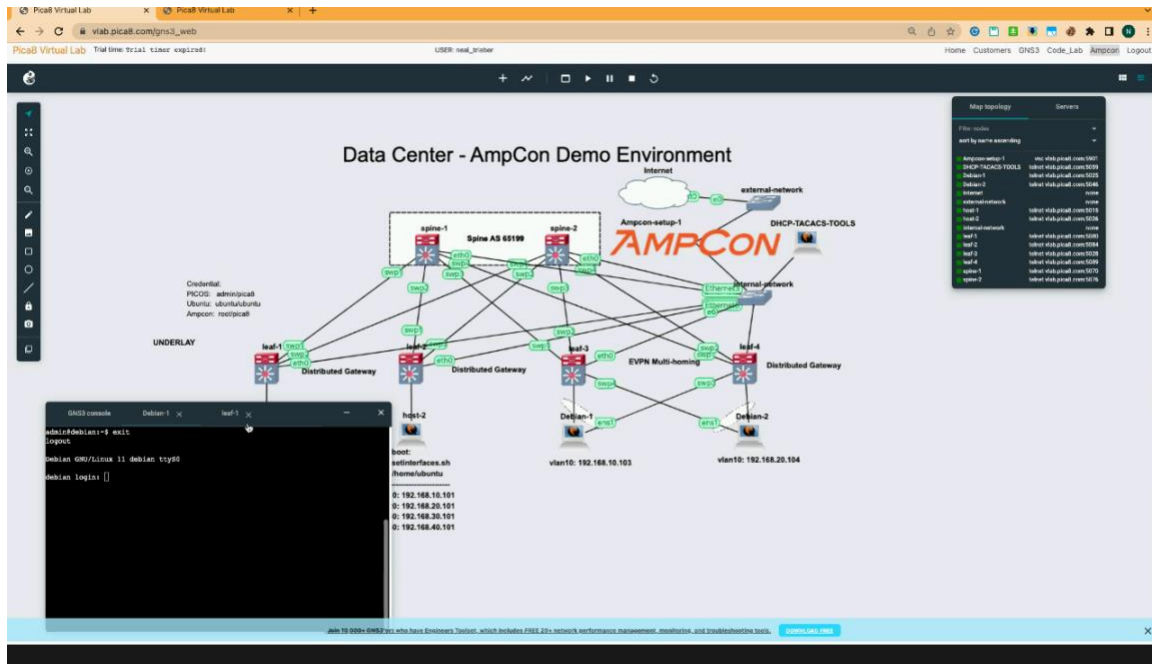
Yes, we do support EVE-NG as well. What you are seeing us use is our [PicOS-V](#) which is also freely downloadable. And you can come registered our website and download it. And as a part



of this webinar, we will reach out to you and help you get set up with it and within our V lab. So yes, PicOS-V actually is fully available to run in all of the major hypervisors QEMU Virtual Box high Hyper V VMware, GNS three so yes, you can pick what, what and how you want to use in a testing environment.

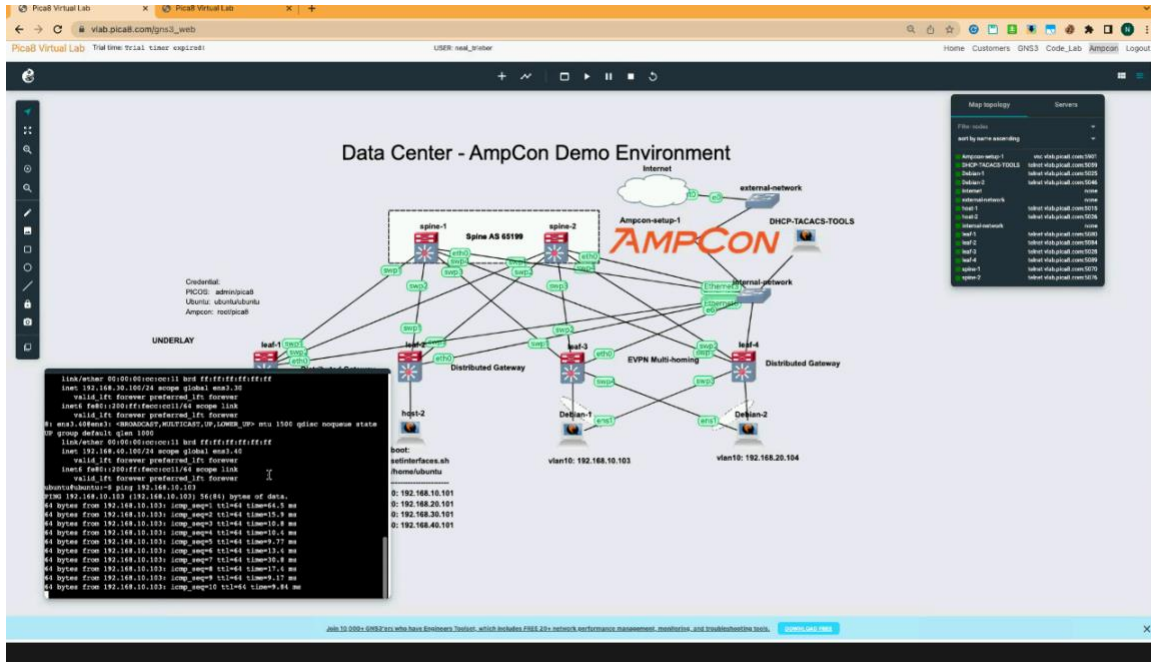
And so just in the interest of time here and moving along with our demo, we have to kind of separate pieces in this mesh. We have a traditional EVPN and VXLAN network here being centrally being sent to but routed as well as an EVPN multi homing set instances as well. So you've kind of got a full EVPEVPNd mesh and you see distributed gateway. So something that James was alluding to before was the fact that more and more people yest. The old company standard has been VRRP for almost two if not three decades at this point. A little long in the tooth, it's still getting extensions, but the newer kid on the block is anycast and we fully support anycast for being depending upon where and how you want to use whether it's part of the overlay for your VLANs or in the underlay, but it allows you to have a fully distributed gateway across your entire mesh. So that same 192.168.10.1 That same core router is distributed across the entire infrastructure. So you've got the same VLANs same gateway, right without and also not being limited by VRRP is simple to master slave, you know now get much more enhanced and scalable redundancy failover and routing.

So as a part of that, you can see I've got several hosts set up to bare metal Ubuntu servers to bare metal Debian Of course, as James also mentioned, whereas the Will there be dragons when it comes to routing to the host because yes, we're introducing new BGP routers to the network. So you will want to work closely between net ops and DevOps to make sure that all of those routes and those those things doing routing, especially down to your new virtualized hosts running Kubernetes and Docker or and or VMware to make sure that those things that are allowed to advertise routes are allowed to advertise routes and those that are not are not using route maps and ACLs. So that yes, you keep your network protected while doing so.



Now, that said, we're going to very quickly here, genus three allows you to open up somebody called these web console tabs. If you're using GNS3 in your own environment, you can actually open these terminals in your local terminal of choice CR is secure CRT, whatever you use on your desktop. I'm doing this all web through the browser.

So I'm going to ping across my EVPN and fabric and I'll show you the fabric as well. From this Debian host here who is who is tagged housing multiple IPs, it's mult it's actually multi IP homed across multiple VLANs you can see VLAN 10 VLAN 20 VLAN 30 VLAN 40 respectively, each with their own separate subnet. And it's going to ping across all the way to the stubby and host here which is we have 192.168.10.103 running on a multi homed yes interface as multihomed to both leaf three and leaf four. So we're gonna log into our Debian host one here that you'll see over here host one. So oops, I closed it. That's okay. We're gonna reopen it. That's leaf one again. Sorry, we'll do host one would be nice. There we go. I'm gonna log into it. Give it a moment. Let me raise this up.



So we can all see what I'm doing. And I'm going to show you the IP addresses here. No smoke, no mirrors. And so you'll notice there's my 192.168.10.1 100. .20.1.100, dot 30 dot 40 respectively. I'm going to ping 192.168.10.123. And now you'll see I'm going all the way across. Now we want to see what the magic is. And we want to know there really is no smoke no mirrors here. So we're going to now actually go to air Yeah, so we're going to go to our other hosts we're gonna go to leaf one and this is leaf one. And I'm going to log into it. This is PicOS-V by the way, I'm logging into I'm logging into it and by the way, whether it's virtual Pecos or physical Pecos it's all Pecos to us Amazon recognizes it the same way as far as management goes. And so all of our all of our commands are command line. It's all the same across the board.

I'm going to say show VLANs just so you can see my VLANs I have to give it a minute. And now you can see who I have tagged and untagged in my VLANs and 1020 3040 off to e 113 and 114 respectively. And now I'm going to say show BGP, EVPN and by the way, you also fully support tab completion at EVPNroute. You're going to see lots of really cool routes come through especially type two and type four because you'll notice how and which and what interfaces these IPs are connected to and how we're learning the routes for those hosts. And you'll notice my route distinguisher my type two and type four routes as we go also recognizing across the board across different servers. Here's 40 don't want to one. You can see how my fabric is fully, fully integrated, fully mesh tied.



Ben Moore, VP Product 59:00

We got to wrap up here. We're at the top of the hour. Ken great to be on so I want to say thank you for showing what we use internally to help folks design and test their network topologies. So thank you for that. Everyone. Thank you so much for attending and your time. I really appreciate it. I know James and Neal do too. I'll speak for them for a second. Really quickly. We we talked about what the enterprise network was today. We talked about key things to consider really security being number one, but also flexibility in terms of users and avail. ability to scale the applications and devices. We did go through a number of network topologies whether it was campus or datacenter options and like multi homing the VXLANd example that James gave, they're all really great. I hope they were all really useful to all of you. We will send out the deck as well as the video after this if we didn't get to your question, please email us at info at PK eight.com We will be happy to answer your questions one to one. And again, thank you so much. Thank you, Neal. Thank you, James. And we'll call it there. Talk to you next time.

Thank you for the discussion.

For additional comments or questions:

info@pica8.com