

Silver Peak

EdgeConnect Deployment Guide for Partners

Contents

Before You Begin	
Unity Orchestrator Considerations	
Prerequisites	
Setting Up	
Step 1: Download the Orchestrator Virtual Appliance Package	
Step 2: Deploy the Orchestrator Virtual Appliance	
Step 3: Configure the Orchestrator	
Step 4: Confirm the Default Business Intent Overlays	
Step 5: Verify WAN labels	
Step 6: Verify an Access List	
Step 7: Verify a Deployment Profile	
Step 8: Verify an Overlay	27
Sample Customer Network	
Deployment	
Installing a Physical EdgeConnect Appliance	
In-Line Bridge Mode is supported with or without a firewall	
Validating Traffic	34
Appendixes	
Appendix A - Site Deployment Worksheet	
Appendix B - Alarms	
Appendix C - Tunnel Troubleshooting	40
Check the Obvious Stuff	
Are the Appliances Talking?	41
Debugging IPSec Tunneling	41
IPSec Troubleshooting - Basic	
IPSec Troubleshooting – Advanced	
Tunneling Alternatives	
Appendix D - Appliance Interfaces	
Appendix E - Alternate Deployment Modes	47



Before You Begin

This document means to help Silver Peak resell partners understand the deployment process for Silver Peak Unity EdgeConnect appliances. The four aspects of deployment are:

- Unity EdgeConnect CPO or POC request
- Unity Orchestrator for management and control of the EdgeConnect appliances
- Unity EdgeConnect Headend/Data Center appliance(s)
- Unity EdgeConnect branch appliance(s)

This document will guide you through the necessary steps to first deploy the Orchestrator and then the EdgeConnect appliances. Where appropriate, links to online documentation are provided to offer additional detail, as required.

Prior to beginning deployment, you must acquire the following information from Silver Peak:

- an Account Name
- an Account Key
- a valid license for Orchestrator and all EdgeConnect appliances

As long as a valid request has been submitted by your Silver Peak account representative, all of this information will be provided in an email to the customer. Silver Peak partners are unable to obtain this information directly.



Unity Orchestrator Considerations

The Silver Peak Unity Orchestrator provides a single pane of glass for manageability of all Silver Peak appliances in the WAN. From Orchestrator you are able to provision, deploy, configure, monitor and troubleshoot your Silver Peak SD-WAN regardless of the make, model or deployment type. Orchestrator will manage physical, virtual and cloud-based EdgeConnect appliances seamlessly from a single console.

Orchestrator is only offered as a virtual appliance and, therefore, requires a suitable host to run on. It will be required to identify an appropriate host machine with adequate resources to host the Orchestrator. Typical deployment locations for Orchestrator would be in a Network Operations Center (NOC) or Data Center, though any location with efficient access to the WAN devices could be suitable. For more information on Orchestrator requirements, refer to the Orchestrator Host System Requirements on Silver Peak's User Documentation site.

For licensing, the Orchestrator (IP address) must be able to reach the Silver Peak Cloud Portal via the Internet. Allocate an appropriate IP address for the Orchestrator appliance and allow it access through any security components in the environment to the "silverpeak.com" domain. (Orchestrator requires port 443 access.)



Prerequisites

Before you begin your deployment:

- Read this entire guide before your first EdgeConnect deployment.
- Silver Peak recommends that all new EdgeConnect and Orchestrator deployments run VXOA version 8.1.4.0 or above.
- Prior to making any network changes, it's good idea to print and work with the customer to complete the deployment worksheet in Site Deployment Worksheet.
- This guide assumes a bridge mode deployment where the MPLS and INTERNET are in separate layer 3 subnets.
- Each EdgeConnect appliance requires one IP address in the subnet being bridged
- During installation, you should be online to facilitate access to latest documentation and support information, should they be needed.
- Be sure to confirm access to the customer virtual environment. Check logins and access permissions prior to deployment.
- This guide assumes a bridge mode deployment, which means the network will be down for a brief time. Please plan accordingly.
- Prior to deploying any EdgeConnect physical appliance, you must have a detailed understanding of the customer's network as it relates to the wide area network (WAN), including a detailed diagram showing IP addressing and physical connections. If you are planning to deploy EdgeConnect virtual appliances, download the quick start guide for virtual appliances, which outlines the detailed steps for your deployment type.
- The deployment in this document assumes you have a single MPLS router and a single Internet firewall at the site—each device is deployed in its own subnet. If your customer's network does not match this criteria, please reach out to the Silver Peak Deployment Engineer for your region for additional deployment options and guidance.







Step 1: Download the Orchestrator Virtual Appliance Package

- 1. Using your preferred browser, go to: *https://www.silver-peak.com*.
- 2. Go to *Partners > Partner Login*, then click **Login**.
- 3. Enter your Silver Peak partner login information.

If you do not have a partner login, click **Request Login**.

Once you submit the online registration form, you will receive an email with your partner login information. If you don't see the email, check your spam or junk folder.

Sign In	Request Login
Email	Need Access to the Silver Peak Partner Portal (BaseCamp)?
Password	
LOGIN	REQUEST LOGIN
Forgot your Password? Contact Partner Support	

Figure 1. Partner login window.

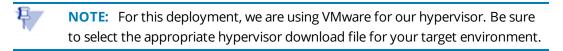
4. Once you are logged in, select **Download Software**.



Home Cases Knowledge	Downloads RMA EdgeConnect Assets V	VXVRX.NX Assets User Documentation Supplemental Documents Request a Part NX To VX
Welcome,		
My Profile Logout	Silver Peak S	Systems Support Center
mportant Messages	Open/Manage a Case	Search our Knowledge Base
New Release /XOA & GMS 7.3 is GA and	Download Software	Open a Self Service RMA
recommended for all	EdgeConnect Subscriptions & Appliances	VX/VRX Licenses & NX Appliances
environments. Please refer to	EdgeConnect Subscriptions & Appliances	VXVVX LICENSES & NX Appliances
the Release Notes for further details which are located with	Mew Documentation	Supplemental Documents
he software download.		Coppendition and contents
	Convert NX to VX	
Did You Know Did you know that VXOA/GMS		
5.2 & 6.0 are End-of-Life?		
Please refer to the release notes		
and upgrade to the latest 7.3 GA.		
Did you know that all Silver Peak License & Asset details		
can be found and retrieved in		
he customer support portal?		

Figure 2. Silver Peak Systems Support Center Download section

5. Select the Unity Orchestrator file for your appropriate hypervisor.



- 6. Select Initial Installation Packages.
- 7. Select Orchestrator (GMS).
- 8. Select **GA** (General Availability).
- 9. Select the recommended release number to download your OVA file.
- 10. Save the OVA file in a location where you can import it into your VMware vSphere environment.

Once the OVA file for Unity Orchestrator has been downloaded, it is ready to be deployed via the hypervisor.





The next step shows how to deploy Orchestrator in a VMWare environment. However, Silver Peak supports the following hypervisors:

- VMware
- Microsoft Hyper-V
- Citrix XenServer
- KVM



Step 2: Deploy the Orchestrator Virtual Appliance

Now you can deploy the Unity Orchestrator appliance VMware vSphere. The Quick Start Guides in the *documentation* section of our website can help with this process. For this example, see *Silver Peak Unity Orchestrator Quick Start for VMware*.



Step 3: Configure the Orchestrator

After you have deployed and configured Orchestrator, verify that the Orchestrator instance can connect to Silver Peak's Cloud Portal.

1. Log into Orchestrator, then go to Orchestrator Administration > Silver Peak Cloud Portal.

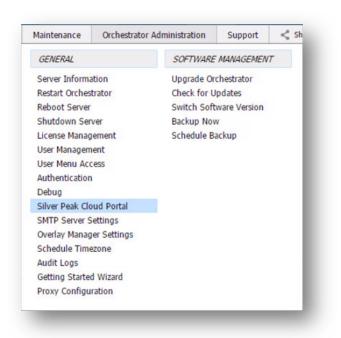


Figure 3. Access the cloud portal configuration from the Orchestrator.

- 2. Configure the Cloud Portal Host and Port fields:
 - Host: cloudportal.silver-peak.com
 - Port:443
- 3. Under the **Registration** section, enter the **Account Name** and **Account Key**.



Host	cloudportal.silver-peak.com	
Port	443	
Registration		
Account Name	trainingAccount699	
Account Key	stjegTLDR7teldDloutvetDhdR2vDrW	
Contact		
Registered	Yes	

Figure 4. Configure the cloud portal access from the Orchestrator.

Your customer received an email with the registration information. Be sure to use the correct Account Name, Key and Licenses for each installation.

Without proper licensing the appliances will BLOCK traffic.

The **Registered** field should show **Yes**, as displayed in Figure 4. This confirms the registration information is correct and the Orchestrator can connect to the Silver Peak Cloud Portal.

If you are unable to successfully validate registration or connectivity, verify the account information and check that the Orchestrator has appropriate security permissions enabled.

If further support is needed, contact Silver Peak support.



Step 4: Confirm the Default Business Intent Overlays

1. From your preferred browser, browse to your Orchestrator instance, and log in using your admin credentials.

The default username/password is admin/admin.

	Unity Orchestrator (HOSTN	
Welc	ome to Unity Orche	strator
ſ	User Name	
	Password	

Figure 5. The Unity Orchestrator login window.

2. Click Login.



Step 5: Verify WAN labels

Interface labels are used to identify common transports and aid in configuring tunnels.

1. To create your labels, go to *Configuration > Interface Labels*.

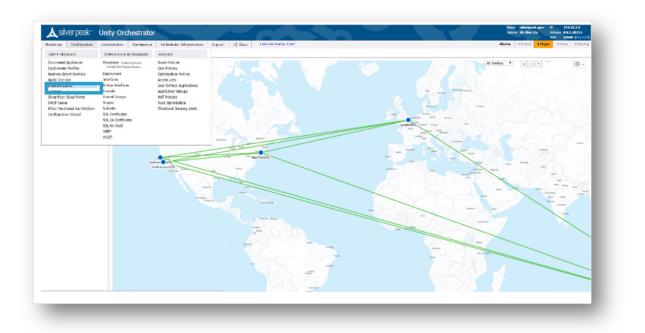


Figure 6. Choose Interface Labels

2. Choose WAN and input the label name.

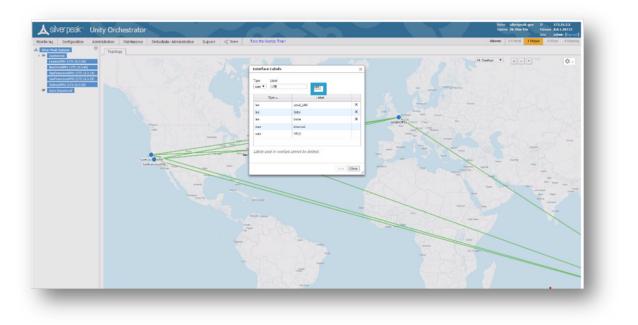


Figure 7. Example: The interface label is LTE.



Step 6: Verify an Access List

Access lists are used to match traffic for processing by a specific overlay.

Best practice is to:

- Create an ACL for real-time traffic to map onto the real-time overlay.
- Create a default ACL to catch all other traffic.

To create an access list:

1. Go to Configuration > Access Control Lists.

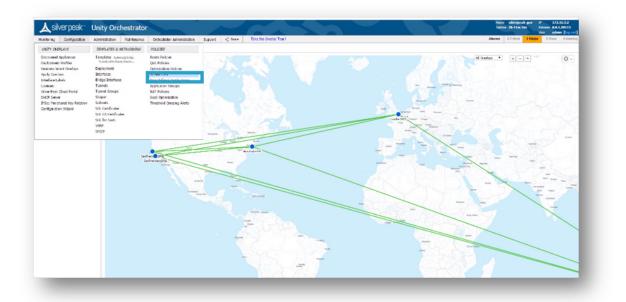


Figure 8. Access Control List

2. Click Manage Access Lists with templates.



Peek Systems	Topology Acces	LBBX											
Landar6491 (172.16.3.30)			C oper	w.									
RewYw/6P01 (172.16.3.40) SarFranciscu6P01 (172.16.3.10)	Access Lists												
Sanfrancisco(3P02 (1/2.16.3.28)	45 R.run											Search	
SydecyteR03 (1/2.56.3.30) Auto Decovered				_			Match Octoria				Set Adams		
	Litt Applance (Date .	40.4	Proving .	Restand	Source DiSubret	Dest IN/Subset	Accienter	Source-Dect Port	2509	Interface	Fernit	Comment	
	/ LandarSP11	Cited April	3150	u	8.0.8.0/0	0(4.0.4.0	14p	818	48y	417	pent		
	 LandorSP01 	Citical Apos	3610	io .	8.0.8.0/0	0.8.0.670	oracle	0.0	any .	any	permit		
	/ LondonSPC1	Critical Appr.	3040	10	8.0.8.0/0	0.0.0.0)0	HEFT, Darwage	0:0	Hy	NT/	permit.		
	< LondorSPE1	Ottal App	3650	U U	0.0.0.0/0	0.0.0.0	115,725	0:0	ity	any	point		
	Z Landorf901	Officel_Apps	1000	10	8.0.8.0/0	0.0.0.0/0	c81, 512	0:0	My	NU	perat		
	/ Londor5951	Defealt	3160	u	0.0.0.0/0	0.0.0.0/0	any	8.8	any	any	pend		
	✓ LondorSP01	Financial_Data	3000	0	8.0.8.0/0	0.8.0.6/0	Trading_Auxicetion	0.0	any .	any	permit		
	/ London5PE1	Financial Data	36.00	6	0,0.8.0/0	0(2.0.2)0	Cash, Register, Da.	0:0	my	47/	pered		
	 LandorSPG1 	ValP	3000	io .	0.0.8.0/0	0.8.0.6/0	GOL SHREE	010	any .	any	2018 X		
	✓ LondonTPC1	Vite	10.00	(P	0,0.8,0/0	0.8.0.8/0	4	0:0	My	ANY .	peret		
	 Landontitta 	Val?	31.10		e.u.e.a/u	0.0.0.0	sw_th	010	48.9	4117	parent		
	 LonderSPC1 	VitP	9536	io .	8.0.8.0/0	0.8.0.8/0	h_323	0.0	Hy	872	perek		
	 LandorSPE1 	VidP	30-00	e e	0,0.8.0/0	0.0.0.0	veice_sign	0:0	##15	#7/	parent		
	✓ NewYork5P01	Offical_Apps	3000	io .	8.0.8.0/0	0.0.0.0	580	0.0	889	any	permit		
	 NewYorkSPDL 	Critical_Appx	34100	ip.	0,0.8.0.9	0(8.0.8)0	oracle	0:0	HIS	872	permit		
	 Rewtoks?01 	Olical_Apps	3640	9	0.0.0.0/0	0.0.0.0/0	HSFT_Exchange	0:0	iny	an	pored		
	 Resided SP3 	Critical Appr.	1150	in .	0,0.1.0.0	0.8.0.6/0	me chr	0:0	Hy	872	Decision of the second		
	 NewYorkS*25 	O tool_App	3140	u	0.0.8.0/0	0.0.0.6/0	utionte	0:0	aty	417	pered		
	 NewYork920; 	Debuit	9000	0	80.84/0	0.0.0.09	817	010	Шý	872	perak		
	 NewYorkSP01 	Pitential_Data	3000	an a	8.0.8.0/0	0.8.0.6/0	Trading_Autication		any .	#7/	pered		
	 NewYorkSP2; 	Financial_Ceta	3630	9	0.0.8.0/0	0.8.0.8/0	Cash_Register_Da.		28.9	anr	90'mk		
	 NeuNod(SP3) 	7409	3100	6	80.84/0	0.0.0.0	chra_6dees	010	Hey	877	peret		

Figure 9. Manage Access Lists with Templates

- 3. Several Default Access-Lists are already created:
 - **Realtime** voice and video protocols.
 - Interactive citrix, terminal services, RDP etc.
 - **AnyTraffic** default permit ip any any.



Pred Sectores	nduton Nationarce Othe		ort < there can be	Xeeby total					A2016	#Critical 1Plaguer 0.0	
Aggliances	Topology Access Leta To	emplates ×									
LandardSP01 (072.16.3.34)	Template Group 😑	Access Lists 📀									
RenterioRV1 (1/2.16.3.10)	prandi l'englate ·	VA9 • 0	OA emoted 124 ends								
Santhumasus(2502 (2/2.56.3.50)	New Group Delete Georg-	Add Rule	Paging .								
SarPranacio(202 (172.16.3.20) Salway(201 (172.16.3.30)											
Auto Decovered	Templates	5 Rowa								Search	
	i isten				Natid-Ditaria				Set Adions		
	2 Tanada	Alexity a Pro	formi Secure 19/Suboot	East IP/Subset	/epilentian	Source:Deet Post	0509	Interface	Faced	Connect	
	Shaper	2000 @	6.3 6.3 9	de a e la	was kny	0:0	417	485	pered.		×
	User Defined Agos	10.00 10	63639	0.6.0.620	50	0.0	81/	My	perek		×
	Application Groups	1000 8	6.3.6.3/3	96.96%	40.55	0.0	87/	10. Y	peret		×
	Access Lists	200 8	6.36.39	0.00.00	1,323	0.0	317				×
	Inste Palicies Ord Palicies							289	point		×
	Optimization Policies	1040 8	6.5.6.3/5	0.0.0.00	1504.63	0.0		Hey .	(secold		×
	B MTP/kim										
	35L Cetificates										
	3 SSL CA Certification										
	D 155 for Section										
	Threshold Country & who										
	Auth/Halter/TACACS+										
	D SHP										
	3 Netfley										
	R 046										
	M Loodne										
	Earner Honager										
	Ored Portal Registration										
	SeeS Optimization										
	New										
	U 01 .										
	Concerning and the second										
	Seve Serve Au Canal Applies to all templeten in group										
	Apply Templates										
	Apply solution to realistics to										
	Janual applaced										

Figure 10. Access Control List Template

4. Make your changes, then click **Save**.



Step 7: Verify a Deployment Profile

Deployment Profiles are used during the deployment wizard to help streamline the installation process by requesting all the locally significant config items per site.

1. Go to *Configuration* > *Deployment*.

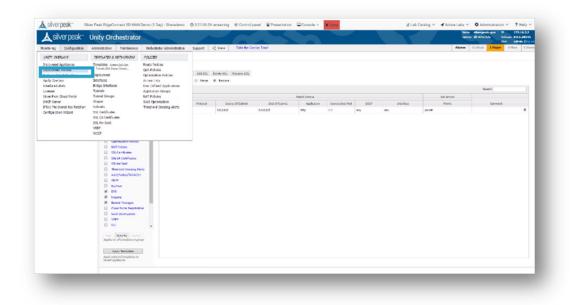


Figure 11. Configuration > Deployment

2. A default inline router mode profile exists for routed installations. To implement the inline bridge deployment method, click **Add**.



∠ silver peak~	Unity Orchestrator			
Monitoring Configuration Silver Peak Systems A Filesces T7.2.16.3.20) NewYorkSPOI (172.16.3.40) WenYorkSPOI (172.16.3.40)	Copology Business Intent On Deployment Profiles (2)	View Deployment	Share Take the Overlay Tourt ment Profiles × Access Lists Templates	

3. Type in-line bridge.

Monitoring Configuration Admin	histration Maintenance	Orchestrator Administration	Support <	Share Take the Overlay Tour!
 Silver Peak Systems Palas (172.16.3.20) NewYork590 (172.16.3.40) SanfranciscoSP01 (172.16.3.10) Auto Discovered 	Topology Business Inte Deployment Profiles (Profile Name No profile	View Deployment es found +Add	ate New Deployme	

4. Click Save.



Ionitoring Configuration	Administration Maintenand	e Orchestrator Administrati	on Support <\$ Share T	ake the Overlay Tour!
Silver Peak Systems		ss Intent Overlays Apply O	Deployment Profiles × A	ccess Lists Templates
Dallas (172.16.3.20) NewYorkSP01 (172.16.3.40)	Deployment Profi	es 🕜 View Deployment	Create New Deployment Profile	
SanFranciscoSP01 (172.16.3		profiles found T +Add	Create New Deployment Prome	×
Auto Discovered			Profile name in-line bridge	
		-	Save Cancel	
				-

5. Click Bridge Mode.

onitoring Configuration Ad	Iministration Maintenance	Orchestrator Administration	Support	< Share	Take the Overla	y Tour!
Silver Peak Systems I Appliances Dallas (172.16.3.20) NewYorkSP01 (172.16.3.40) SaarFancesSP01 (172.16.3.10) Generations SP01 (172.16.3.10) SaarFancesSP01 (172.16.3.10)	Deployment Profile	ne bridge 🔻 +Add Rename Delete	Bonding User fiber po Propagate Lin 4-port single	nk Down	Access Lists	Templates
	Interface Ian0 Ne		Wan0	aping Kbps		
		Tota	Outbound → Inbound ← Inbound ←	Plus for > 200 l	Shape Inbound Tr Ibps Kbps	affic
	Save Save As Ca	incel				

6. Map the WAN label to the MPLS interface.



onitoring Configuration Adm	ninistration Maintenance	Orchestrator Administration	Support	< Share	Take the Over	ay Tour!
Ontoring Configuration Adm Silver Peak Systems Image: Configuration Image: Configuration Image: Configuration Adm Image: Configuration Dallas (172.16.3.20) NewYorkSPD (172.16.3.40) Image: Configuration SanfranciscoPPD (172.16.3.10) Image: Configuration Image: Configuration Image: Auto Discovered Image: Configuration Image: Configuration	Topology Business Ir Deployment Profiles Profile Name in-line Router Bridge	Apply Overlays Apply Overlay View Deployment bridge +Add Rename Delete Server Server Apply Overlay Apply	Bonding User fiber por Propagate Lin 4-port single	rment Profiles ×	Access Lists	Templates
	Save Save As Cance	Total Tota Edg	Interface Dutbound → [Inbound ← [HeConnect Licensing	Σ Calc 4 Kbps Kbps Plus for > 200 Boost 0	Shape Inbound 1 Mbps Kbps	raffic



a. Add shaping Kbps to the MPLS interface.

nitoring Configuration Admir	istration Maintenance Orchestrator Administration Support <\$ Share Take the Overlay Tour!
Silver Peak Systems Appliances Dallas (172.16.3.20) NewYorkSP01 (172.16.3.40) SaniFranciscoSP01 (172.16.3.10) Auto Discovered	Topology Business Intent Overlays Apply Overlays Deployment Profiles × Access Lists Templates Deployment Profiles ? View Deployment Profile Name in-line bridge • -Add Rename Delete Router Bridge Server Bonding User fiber ports Propagate Link Down 4-port single bridge
	A silver peak" Interface Label / VLAN Label / Interface Shaping Kbps lan0 None +1P MPLS + Wan0 +Bridge Interface 1 Z Calc
	Total Outbound →Kbps Total Inbound ←KbpsShape Inbound Traffic EdgeConnect Licensing Boost 0Kbps
	Save Save As Cancel

NOTE: It is important to set the actual WAN bandwidth. If you are unsure, use the lower number.

If asymmetric bandwidths, click **shape inbound traffic** to unshadow inbound.

b. ADD the bridge interface for INTERNET.

E



Configuration Admini	stration Maintenance	Orchestrator Administration	Support	< Share	Take the Over	ay Tour!
ilver Peak Systems Appliances Dallas (172.16.3.20)	Topology Business Ir Deployment Profiles	Apply Overlay View Deployment	s Deploy	ment Profiles \times	Access Lists	Templates
NewYorkSP01 (172.16.3.40) SanFranciscoSP01 (172.16.3.10) Auto Discovered	Profile Name in-line	bridge ▼ +Add Rename Delete				
	Router Bridge	Server	Bonding User fiber por	ts		
			Propagate Lin 4-port single			
		ksilver peak-				
	Interface Li lan0 None	abel / VLAN Label / V MPLS V +IP	Interface	aping Kbps 4,500		
		+Bridge	Interface	Σ Calc		
			Outbound → Inbound ←	Kbps Kbps	Shape Inbound	raffic
		Edg	jeConnect Licensing	Plus for > 200 Boost 0	Mbps Kbps	
	Save Save As Cance	el				

7. Map the WAN label to the INTERNET interface.



Ionitoring Configuration	Administration	Maintenance	Orchestrator Administration	Support	< Share	Take the Overla	y Tour!
Silver Peak Systems Appliances Dallas (172.16.3.20) NewYorkSP01 (172.16.3.40 SanFranciscoSP01 (172.16.)	ent Profiles	tent Overlays Apply Over	lays Depl	oyment Profiles $ imes$	Access Lists	Templates
Auto Discovered	Rout		Server	Bonding User fiber p Propagate L 4-port singl	ink Down		
	Interfa Ian	0 None	Silver peak- tel / VLAN Label / +sp MPLS + +sp Internet * X	Interface Wan0 NAT 19 Wan1 NAT 19	Shaping Kbps + 4,500 		
				tal Outbound - fotal Inbound + EdgeConnect Licensing		Shape Inbound T O Mbps Kbps	raffic
	Save S	ave As Cance	4				

a. Add shaping Kbps to INTERNET interface.



onitoring Con	-	istration Maintenance Orchestrator Administration Support < Share Take the Overlay Tour!
Silver Peak System	s Q	Topology Business Intent Overlays Apply Overlays Deployment Profiles X Access Lists Templates
Dallas (172.1	6.3.20) (172.16.3.40)	Deployment Profiles 🥹 View Deployment
	SP01 (172.16.3.10)	Profile Name in-line bridge 💌 +Add Rename Delete
		Router Bridge Server Bonding
		User fiber ports
		Propagate Link Down
		4-port single bridge
		A silver peak-
		Interface Label VLAN Label / Interface Shaping Kbps
		lan0 None (MPLS (MPLS
		50,000
		lan1 None Internet V wan1 Super Space
		2 Calc
		4
		Total Outbound → Kbps Shape Inbound Traffic
		roter anvoure - keps _ snape anoune many
		EdgeConnect Plus in for > 200 Mbps Licensing Boost 0 kbps
		Save Save As Cancel



NOTE: You must set the actual WAN bandwidth. If you are unsure, use the lower number.

If asymmetric bandwidths, click **shape inbound traffic** to unshadow inbound.

8. Sum the shaping Kbps.

	aistration Maintenance Orchestrator Administration Support <\$ Share Take the Overlay Tourl
Silver Peak Systems	Topology Business Intent Overlays Apply Overlays Deployment Profiles × Access Lists Templates
Appliances Dallas (172.16.3.20)	Deployment Profiles 2 View Deployment
NewYorkSP01 (172.16.3.40)	Deployment Profiles 🕜 View Deployment
SanFranciscoSP01 (172.16.3.10)	Profile Name In-line bridge 🔻 +Add Rename Delete
Auto Discovered	
	Router Bridge Server Bonding
	User fiber ports
	Propagate Link Down
	4-port single bridge
	A silver peak."
	Interface Label / VLAN Label / Interface Shaping Kbps
	lan0 None ▼ MPLS ▼ wan0 ⇒ 4,500
	+IP LIAT TH
	lan1 None V Internet V Wan1 + 10
	2 Cak
	Total Outbound → Kbps
	Total Inbound + Shape Inbound Traffic
	EdgeConnect Plus in for > 200 Mbps Licensing Boost 0 Kbps
	LiCensing Boost 0 Kbps
	Save Save As Cancel

9. Save the Deployment Profile.



Snitoring	Configuration	Administration	Maintenance	Orchestrator Administ	ration	Support	< Share	Take the Over	lay Tour!
Silver Peak Sys		10 Topolo	gy Business Ir	Appl	y Overlay	s Deplo	ment Profiles ×	Access Lists	Templates
	72.16.3.20) P01 (172.16.3.40)	Deploy	ment Profiles	View Deployment					
SanFrance Auto Disc	iscoSP01 (172.16.3.10 overed) Prot	file Name in-line	bridge • +Add Rename D	elete				
		P	touter Bridge	Server		Bonding			
						User fiber por	ts		
						Propagate Lin			
						4-port single	bridge		
				kilver peak-					
				abel 🖌 VLAN 🛛 Label .		Incentace	4,500		
			lan0 None	+IP MPLS	•	Wan0	1,500		
			lan1 None		×	wan1	50,000		
				+[P		NAT 10			
							Σ Calc		
					Total	Outbound +	Kbps		
					Tot	al Inbound ←	Kbps	Shape Inbound	Traffic
					Ed	geConnect Licensing	Plus for > 20 Boost 0	Kbps	
			1						
		Save	Save As Cance	el					



Step 8: Verify an Overlay

1. Go to Configuration > Business Intent Overlays.

lonitoring	Configuration	Administration	Maintenance	Orchestrator Administration	Support	< Share	Take the Overlay Tour!
UNITY OVE	RLAYS	TEMPLATES & I	NETWORKING	POLICIES	Access Lists	5 Template	5
Apply Overla Interface La Licenses	Profiles eent Overlays ays bels Cloud Portal	Templates syste Turnels.UDA.Shap Deployment Interfaces Bridge Interface Tunnels Tunnel Groups Shaper	per,Routes	Route Policies QoS Policies Optimization Policies Access Lists User Defined Applications Application Groups NAT Policies SaaS Optimization			
IPSec Pre-sh Configuratio	hared Key Rotation on Wizard	Subnets SSL Certificates SSL CA Certifica SSL for SaaS VRRP WCCP		Threshold Crossing Alerts	Toronto	Movietur Doubon YorkSP01 Dig	

Three default overlays are automatically created:

- Realtime voice and video applications.
- Interactive Citrix, terminal services, RDP, etc.
- AnyTraffic default permit ip any any.

Note: You don't need to apply every overlay to every site. If, say, a branch does not have voice, you are not required to apply the realtime overlay to that site.

While we recommend using the default settings, you can rename or add additional overlays.



Note: VXOA 8.1 is limited to seven overlays total.

2. Click ADD.



太 silverpeak∼ Ur	nity Orchestrator				Appliances Discovered		time HOSTNAME	Release 8.0.1	16.3.2 1.28115 in [log out]
Silver Peak Systems	Topology Business In Business Intent Over		Support rs Deployn	Share Take the Or ment Profiles Access Lists		Alarms	0 Critical 1 Majo	0 Minor	3 Warning
Seafrancisco3991 (172-16-3-10) Auto Discover	Overlays +44	1 Topology * Med 1 Hub		Select Hubs +Add					
		Overlay Poli	cy coess Policy	Traffic on this LAN Port	▼ - Or ® NewA	Match Traffic CL			
	Rename Delete	Link Bro Threshol Route M Traffic to WAN Por	ds atched these	Loss Latency 0 % 0 / Primary Backup MPLS MPLS Internet Internet	Jitter 0 ms Use Backup Ports on Blackout Brownout t Cross Connect Provider				
		Link Bon	ding Policy	→ Failover Osec → Use Best Quality Path → Path Conditioning	Failover <1sec + Failo Use Best Quality Path + Load Path Conditioning + Path	h Throughput ver <1sec Balance Paths Conditioning fficiency >80%	⇒ Failover <1sec ⇒ Load Balance F ⇒ BW Efficiency :	aths	
		Overlay	Down Action	Pass Through Unshaped *					

3. Click to enable BOOST if POC or if the CPO included the license

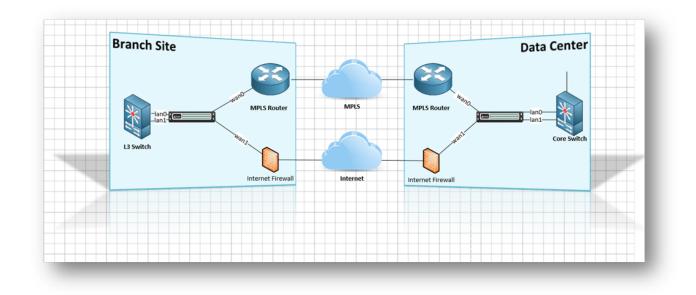


Business Intent Overlay	/S 🕐 Ap	oly Overlays	
Overlays +Add Default	Ť	Mesh Hub & Spoke	Select Hubs +Add
	ł	Overlay Policy Traffic Access Policy	Traffic on this LAN Port Use ACL to Match Traffic Voice • Or Image: Construction of the second s
Rename Delete		Link Brownout Thresholds Route Matched Traffic to these WAN Ports	Loss Latency Jitter 1 % 500 ms 0 ms 0 ms Primary Backup Use Backup Ports on Blackout Biokout Internet Internet Cross Connect Providers
		Link Bonding Policy	High Availability High Quality ● High Throughput ● High Efficiency → Failover Osec → Failover <1sec
		Overlay Down Action	Pass Through Unshaped 🔻
		Shaping Traffic Class	1 (default)
		Boost License	Boost this Traffic
Save Save As Cancel			

4. Save.

Scroll down to see the Save button or change your web browser zoom.





Sample Customer Network



Deployment

While several deployment scenarios are available to you when deploying an EdgeConnect appliance, this document focuses on the simplest configuration.

- The Data Center headend device as in-line bridge
- The Branch device installed in-line as a bridge

Once you're comfortable with the environment and the deployment plan, keep the following tips in mind:

- Orchestrator must be configured and deployed before any EdgeConnect appliance is installed.
- You must have the license, account keys and account names from Silver Peak.
- The Silver Peak Cloud Portal can act as the rendezvous between appliance and Orchestrator for discovery. It also acts as a secondary channel for the appliance to remain connected with Orchestrator in case the appliance loses direct connection to Orchestrator.
- Check to make sure Orchestrator has access to the Silver Peak Cloud portal.
- OVA files for Orchestrator and EdgeConnect Virtual appliances are available from *www.silver-peak.com*.
- The quick start guides provide a step-by-step process EdgeConnect appliance.
- The deployment of both the Orchestrator and EdgeConnect appliances is easy—simply following the steps in this document.
- Review the Prerequisites.



Installing a Physical EdgeConnect Appliance

Use the same procedure to install and configure a **Data Center** or **Branch** physical EdgeConnect appliance:

- 1. Download the Quick Start Guide (QSG) for the Unity EdgeConnect.
- 2. Unbox the appliance and place it in the rack using the included rails or ears.
- 3. Follow the steps provided in the Quick Start Guide.
- 4. Connect the **mgmt0** port to a DHCP capable switch port and power the unit on.
- 5. DO NOT connect any LAN or WAN ports until approved, licensed, and configured.
- Log into Orchestrator. Orchestrator and the physical appliance will both contact the Silver Peak cloud portal and when successful, will illuminate the green **Appliances Discovered** button.
- 7. Click Appliances Discovered

Appliances Discovered

in the TOP right banner.

- 8. Click **Approve** to select the appliance you want to manage and bring into your network.
- 9. Follow the **Appliance Setup Wizard** to configure the appliance.
 - The IP address was identified in the *deployment worksheet*.
- 10. Once the appliance is licensed, approved and configured, you can schedule the downtime to wire up the Silver Peak to your customers' MPLS and FIREWALL.
- 11. The following steps affect service:
 - a. Remove the LAN side network cable from the MPLS router (make a note of which Ethernet port) connect it to the LANO port of the EC device. Take a new red cross-over cable (included in the packagingz0 and connect it from the WANO port on the EC device to the original MPLS router Ethernet port.
 - b. Remove the LAN side network cable from the FIREWALL router (make a note of which Ethernet port) connect it to the LAN1 port of the EC device. Take a new red cross-over cable (included in the packaging) and connect it from the WAN1



port on the EC device to the original FIREWALL Ethernet port.

c. The Alarms regarding link and next-hop should clear.

All IP addresses for LAN & WAN interfaces need to be configured statically for in-line bridge mode.

In-Line Bridge Mode is supported with or without a firewall

For deployments in the branch, one of the simplest options for EdgeConnect appliances is inline bridge mode, when there are two devices involved (MPLS + Firewall). Other deployments are available. For example, a broadband connection can be terminated directly on the EC device. See the appendix for more details.

Router	Bridge Server		Bonding User fiber po Propagate Li 4-port single	nk Down		
		<u>k</u> silver pea	ak-			
nterface	Label	IP/Mask	VLAN Label		Interface	Shaping Kbps Next Hop
lan0	None v	10.10.1.5/24	MPLS	•	wan0	→ 3,000 ← 3,000 ··· 10.10.1.1
		+IP			NAT	0,000
lan1	None T	192.168.254.99/24	Internet	▼ ×	wan1	→ 5,000 ··· 192.168.254.1
		+IP			NAT 1 9	 50,000 Σ Calc
				Total	Outbound	⇒ 8,000 Kbps ≤ 200,000 Kbps
				Tota	l Inbound	← 53,000 Kbps Shape Inbound Traffic
				Edg	geConnect Licensing	

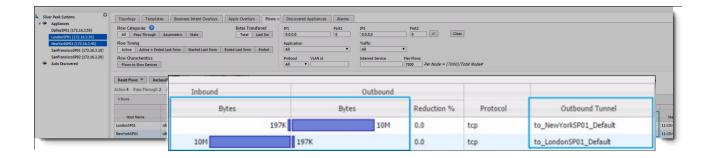
Figure 12. In-Line Bridge Mode Deployment



Validating Traffic

Within Orchestrator, go to *Monitoring* > *Flows*.

- The flows appear on both the branch and the data center.
- You should see both INBOUND & OUTBOUND bytes; a value of 0 indicates an issue.
- You should see the Default Overlay in use for the outbound tunnel (or Realtime if VOIP).









Appendix A - Site Deployment Worksheet

All IP addresses for LAN & WAN interfaces must be configured statically for in-line bridge mode.

Silver Peak Bridge Mode – 4 Port This topology assumes inter-vlan routing is setup on a Layer 3 switch. Connection Speed **Connection Speed** Depending on configuration this may be a single router or 2 different routers Router Mode WAND Next Hou = WAN Side Default Gate Port # (ex. FA0/2) Port Speed (ex. Auto/Auto ort # (ex. FA0/2 WAN1 Next Hop WAN0 Next Hop Crossover Cable Crossover Cable VLAN VLAN WAN VAN1 MGMT0 - -LAN LAN1 VLAN Straight-Through Cable Straight-Through Cable VLAN Port # (ex. FA0/3) Port Speed (ex. A Port # (ex. FA0/3) Port Speed (ex. Auto LAN0 Next Hop LAN1 Next Hop Switch M ort (ex. FA0/4) Depending on configuration this may be a single switch or 2 different switches

Replace the following example with your specific information:

LAN0 Next Hop = LAN Side Default Gateway



Site Name	Example	
Silver Peak Hostname	HOSTNAME	
Deployment Mode	4-Port, Bridge	
Management IP (mgmt0)	MGMT0_IP	
mgmt0 Default GW	MGMT0_DEFAULT_GW	
Appliance IP (wan0)	WAN0_IP	
wan0 Next Hop	WAN0_IP_DEFAULT_GW	
lan0 Next Hop	LAN0_IP_DEFAULT_GW	
Appliance IP (wan1)	WAN1_IP	
wan1 Next Hop	WAN1_IP_DEFAULT_GW	
lan1 Next Hop	LAN1_IP_DEFAULT_GW	

Define VLAN/SUBNETS to Optimize at Local Site

VLAN#	SUBNET/XX	Description
VLAN_#	xx.xx.xx/yy	A description here

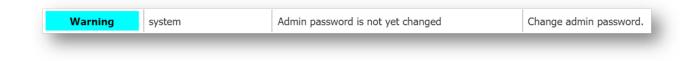


Appendix B - Alarms

ALWAYS check both the appliance and the orchestrator for alarms, as these provide valuable information in isolating any lingering issues.

The *SD-WAN Deployment Guide* has a detailed section on alarms. This document simply discusses the most common alarms related to deployment of Edge Connect devices and Business Intent Overlays.

Admin password left as default



WAN labels not applied, Overlay manager will not build tunnels to appliance

Minor orchestrator Appliance does not have any wan labels required f Assign at least one wan label selected for this overlay in the deployment configuration of the	appliance.
---	------------

Overlay references an ACL, but no ACL is applied



Interface is not connected

n0	Network interface link down	Is the system in bypass mode? Check cables, interface admin status on the r
n	0	0 Network interface link down



Next hop is not reachable

Host Name Alom 7me v Sewrity Sewrite Lendord/991 30-kop-16 31:56 Hear-Nag ger.172.16.18.259 Next-hap surreschall	Allorm Description Allorm Description Deck cables, 39/mask on Skeer Feak and router. Next-hop show	Recommended Action of the only a single IP hop away, Use 'show ofp neighbor', 's	New any', pingjingi -1 < applance ip > cond-hop IP> to tradicibust.
unnel DOWN alarms			
Critical system	Appliance is not registered. Please check account	Please provide valid acc	count registration information.
ppliance is not registered			
Critical system	Appliance is not registered. Please check account	Please provide valid acc	count registration information.
icense not granted			
Critical system	Appliance could not get license l	ease.	Contact Silver Peak.
icense has expired			
Critical system 5	Software license lease has expired. This model ob You must ha	ve HTTPS connectivity to Inte	ernet to renew the license lease.



Appendix C - Tunnel Troubleshooting

Debugging consists of 4 parts:

- 1. Check the Obvious Stuff
- 2. Are the Appliances Talking?
- 3. Debugging IPSec Tunneling
- 4. Tunneling Alternatives

Check the Obvious Stuff

- 1. Do you have any Alarms on the appliance or orchestrator?
- 2. Can you ping the IP address of the next hop?
- 3. Can you ping an IP address on the internet?
- 4. Have you verified that you're using the correct public IP address?
 - Does the NAT switch need to be on or off?
- 5. If the appliance is directly connected to broadband, turn off wan hardening.
 - Can you access the appliance via https and ssh?
 - If so, you know you are on the public internet.
 - Turn WAN hardening back on immediately.

Are the Appliances Talking?

- 1. Verify Bi directional traffic flow
 - Use tcpdump to verify traffic is coming/going from the data center
 - ssh to the data center appliance
 - tcpdump -i bvi0 host 97.174.110.10 (example remote appliance IP)
 - You should see traffic coming and going to that IP
- 2. If bidirectional conversations are occurring, try changing to GRE or UDP. This is perhaps an IPsec issue, see Debugging IPSec Tunneling.

Debugging IPSec Tunneling

IPSec Troubleshooting - Basic

When debugging IPSec tunneling, look out for:

- 1. If you have bi-directional traffic via ESP or NAT-T then the appliances are trying to establish an IPSec tunnel.
 - Silver Peak Recommendation: Set the MTU size to 1400 to account for IPSec overhead.
- 2. Another common scenario occurs when another device appliance responds to IPSec requests, rather than the Silver Peak. If you encounter tunnel connectivity issues, it may be necessary to validate the IPSec response is coming from the correct Silver Peak appliance. If this is found to be happening, most firewalls have an IPSec pass-through feature that can be enabled to get around this.
- 3. A third scenario to be aware of is the case where no IPSec devices are responding to IPSec requests from the Silver Peak appliance. This scenario could be caused by a misconfiguration of the pre-shared key or IPSec setup. It could also be caused when the IPSec requests are blocked by a firewall or other device somewhere between the Silver Peak appliances.





IMPORTANT: If you're not familiar with IPSec or comfortable troubleshooting using a CLI, we recommend that you involve your network or firewall administrator for assistance in troubleshooting connectivity issues. Making changes to routers, firewalls, and other devices in production environments can cause disruptions in service.

IPSec Troubleshooting - Advanced

Broadcast CLI

Silver Peak Orchestrator provides the Broadcast CLI (BCLI) tool that enables administrators to issue CLI commands centrally from the Orchestrator interface. The BCLI can be used to issue commands to one or many appliances at a time. As long as the Orchestrator can communicate with remote appliances, Broadcast CLI can be used to issue commands for troubleshooting IPSec.

Broadcast CLI can be accessed on the Orchestrator by choosing *Maintenance* > [Tools] Broadcast CLI

To identify if another device is responding to *IPSec requests*:

1. Use the BCLI to issue the following command on the remote silver peak:

(Tunnel name in this example is *tun1*. Replace *tun1* with appropriate tunnel name in your environment.)

```
BRSUPP86 (config) # show int tunnel tun1 ipsec status
Tunnel tun1 ipsec state
Tunnel Oper: Down
IPSec Enabled: yes
IPSec Oper: Healthy
Total IPSec SAs: in:1 out:1**
IPSec Key Size: 256 bits
Replay Window(bits): 1024
```

Ę

NOTE: 1 SA (security association) sent (out) and 1 SA received (in), but we can't validate which device responded to our SA.

2. Issue the following command from the BCLI:



```
BRSUPP86 (config) # show int tunnel tun1 ipsec debug
IPSec stats for tid 2
----Key-management---
Current state: 2
Req key by dp: 1
Rekey dp: 0
Rekey TO: 0
Rekey # in pkts: 0
Rekey # out pkts: 0
Key wait TO: 0
Passive key TO: 0
----In-bound---
Total packets: 0**
Aligment: 0
No sa: 0
Verify fail: 0
Replay check: 0
Decryption fail: 0
Other reason: 0
----Out-bound---
Total packets: 453
No sa: 6
Encryption fail: 0
Authentication fail: 0
Other reason: 0
```



NOTE: "Total packets" should not be 0. This indicates the firewall in front of us responded, and the Silver Peak appliance never got the request. (Scenario 2, above) In this situation, it is necessary to enable "ipsec passthrough" on the firewall. Alternatively, you could elect to connect the Silver Peak appliance directly to the public internet. (Make sure WAN hardening is enabled and proper security precautions are in place.)

To validate a deeper issue with IPSec packets traversing the network:

 If the tunnel debug command shows no SAs at all, you could have an issue with the IKE exchange. This scenario could be caused by a misconfiguration of the pre-shared key or IPSec setup. It could also be caused when the IPSec requests are blocked by a



firewall or other device somewhere between the Silver Peak appliances.

2. Issue the following command from the BCLI:

(Replace *tun1* with appropriate tunnel name in your environment.)

```
BRSUPP86 (config) # show int tunnel tun1 ipsec debug
IPSec stats for tid 2
----Key-management---
Current state: 2
Req key by dp: 1
Rekey dp: 0
Rekey TO: 0
Rekey # in pkts: 0
Rekey # out pkts: 0
Key wait TO: 0
Passive key TO: 0
----In-bound---
Total packets: 435
Alignment: 0
No sa: 0
Verify fail: 0
Replay check: 0
Decryption fail: 0
Other reason: 0
----Out-bound---
Total packets: 453
No sa: 6
Encryption fail: 0
Authentication fail: 0
Other reason: 0
```

The *Current State* output indicates the ISAKMP key exchange state. For reference, here's a table of ISAKMP key exchange states as they map to the *Current State* value:

ISAKMP Key Exchange State	Current State ID
ST_INIT	1
ST_ACTIVE_KEY_WAIT	2
ST_ACTIVE_READY	3
ST_PASSIVE_READY	4





- If you are stuck in ST_ACTIVE_KEY_WAIT (Current State = 2), then you might have an IKE connectivity problem or a pre-shared-key issue.
 - Check firewall config
 - Check pre-shared key entered correctly
- If no IKE exchange is happening at all the SPs (Security Policies) which packets hit to trigger the IKE session may be wrong or missing, due to misconfiguration
 - Check IP address configuration
- If tunnels come up but we are seeing bad performance
 - Revisit the MTU configuration. MTU may need to be adjusted lower.

Tunneling Alternatives

As an alternative to IPSec encapsulation, you can try setting tunnel encapsulation to **GRE** or **UDP**. Remember, using GRE or UDP encapsulation is useful for troubleshooting, but these encapsulation methods do not provide as much protection as IPSec with encryption.

Using GRE or UDP means that data will be sent in the clear and is NOT recommended for production use across insecure links.



Appendix D - Appliance Interfaces

<u>ل</u>	EdgeConnect XS	EdgeConnect S	EdgeConnect M	EdgeConnect L	EdgeConnect XL
silver peak ~	4.0800000	affoodadda * 🖷 *			
Part Identifier	EC-XS	EC-S	EC-M	EC-L	EC-XL
Typical Deployment	Small Branch	Large Branch	Head Office Small Hub	Data Center Large Hub	Data Center Large Hub
Typical WAN Bandwidth	2 - 200 Mbps	10 - 1000 Mbps	50 - 2000 Mbps	I - 5 Gbps	2 - 10 Gbps
Recommended Boost up to	50 Mbps	200 Mbps	500 Mbps	l Gbps	5 Gbps
Redundancy / FRUs	No	No	Power and SSD	Power and SSD	Power and SSD
Datapath Interfaces	4 x RJ45 10 / 100 / 1000	6 x RJ45 I/I0G Option	4 x RJ45 2 x I/10G Fiber	4 x RJ45 2 x I/10G Fiber	4 x 1/10G Fiber



Appendix E - Alternate Deployment Modes

For more information on deployment modes, see the *Appliance Managers Operation Guide*.

IN-LINE BRIDGE at the Branch with NO FIREWALL

If your branch does not have a firewall, you can plug the broadband directly into the silver peak

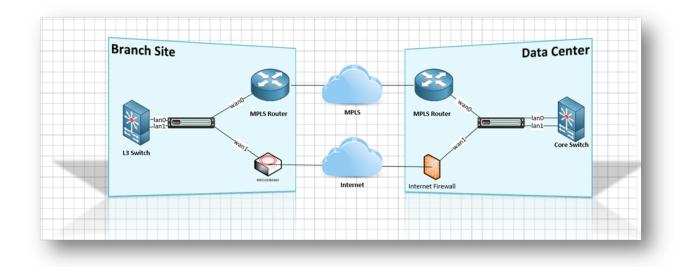


Figure 13. In-Line Bridge – Direct to broadband

For large deployments, the ideal mode in the datacenter is router mode.



				4	silve	er peak ~					
			LAN Interfaces	+Add		W	AN Interfaces +Ad	d			
Next Hop	Interface	VLAN	Label	IP/Mask	1	IP/Mask	Label	VLAN	Interface		Next Hop
	lan0 🔻	+IP	Local_LA V	192.168.40.1/24 × DHCP Server 2		× 172.16.10.40/24	MPLS V	+IP	wan0 🔻	→ 50,000 ← 50,000	172.16.10.1
						x 54.145.66.2/29	Internet V	+IP	wan1 V	→ 300,000 ← 300,000	54.145.66.1
										⇒ 350,000 K	
								Tot	al Inbound	← 350,000 K	bps 🕜 Shape Inbound Traffic
								E	lgeConnect Licensing		r > 200 Mbps Kbps

Figure 14. In-Line Router Mode Deployment

			📐 silv	ver peak~			
		LAN Interfaces +A	dd	W	AN Interfaces +Add		
Next Hop	Interface VI	LAN Label	IP/Mask	IP/Mask	Label	VLAN Interface	Shaping Kbps Next Hop
	lan0 V	Local_LA ▼ 1	192.168.40.1/24 × DHCP Server /*	× 172.16.10.40/24	MPLS V	+IP WAND V	→ 50,000 ← 50,000
				x 54.145.66.2/29	Internet V	→IP NAT ®	→ <u>300,000</u> → <u>300,000</u> → <u>54.145.66.1</u>
				x DHCP	LTE V	Ian1 ▼ +IP NAT @	→ 50,000 ← 35,000
							Σ Calc
							→ 400,000 Kbps ≤ 200,000 Kbps ← 385,000 Kbps ♥ Shape Inbound Traff
						EdgeConnect	Plus for > 200 Mbps Boost 0 Kbps

Figure 15. Quad In-Line Router Mode Deployment



Note the use of **lan1** as a wan port. Only the EC-S model ships with an actual **WAN2** port. The other appliances in the EdgeConnect family can utilize any port for LAN or WAN depending on the required configuration.

