Configure Disjoint Layer 2 in UCS Manager

Contents

Introduction Prerequisites **Requirements** Components used **Background Information** Disjoint Layer 2 (DL2) Network Diagram Configure Create the uplinks in the Fabric Interconnects. Assign VLANs Create vNIC Template Reboot the Server Create VLAN Group **ESXi** Configuration Verify in UCSM **Related Information**

Introduction

This document describes the configuration for Disjoint Layer 2 in the Unified Computing System Manager Domain (UCSM).

Prerequisites

- At least one available link on each Fabric Interconnect and two available links on your upstream switch
- The links between the Fabric Interconnects and the upstream switch must be up, they must be configured as uplinks. If they are not, check this guide to configure them on UCSM: <u>Using the LAN</u> <u>Uplinks Manager</u>
- The VLANs to be used must be created on UCSM already. If they are not, check this guide: <u>Creating</u> <u>a Named VLAN with the LAN Uplinks Manager</u>
- The VLANs to be used must be created on the upstream switch already.
- The VLANs to be used cannot exist on any other virtual Network Interface Cards (vNIC) on the Service Profiles.

Requirements

Cisco recommends that you have knowledge of these topics:

- Unified Computing System Manager Domain (UCSM).
- Basic understanding of Disjoint Layer 2 networks.
- Networking configuration.
- VNIC Configuration.

Components used

- UCS Manager.
- Firmware version 4.2(3e).
- 6454 Fabric Interconnect.
- Cisco B200 M5.
- Nexus 5672UP 16G-FC Chassis.
- Catalyst WS-C3650-12X48UR-E.

Background Information

Disjoint Layer 2 (DL2)

Disjoint layer-2 networks are required if you have two or more Ethernet clouds that never connect, but must be accessed by servers or virtual machines located in the same Cisco UCS domain.

They are also required in a multi-tenant environment if servers or virtual machines for more than one client are located in the same Cisco UCS domain and they need to access the L2 networks for both clients.

Network Diagram



Configure

Log into Cisco UCS Manager GUI as an administrative user.

Create the uplinks in the Fabric Interconnects.

Step 1. Navigate to **Equipment tab > Fabric interconnects > Fabric Interconnect A or B.**

Step 2. Right-click on the desired port and select Configure as an uplink port. This uplink port is used to connect to the Disjoint network (in this example VLAN 80).

Equipment / Fabric Interconnects / Fabric Interconnect A (primary)									
General	Physical Po	orts Fans	PSUs Pr	nysical Display	FSM	Neighbors	Faults	Events	Statistics
Fault Summa	iry		Physical	Display					
0 Status	0 0	0		Admin Down	Fail Lir	nk Down		ura (r.1.1	
Overall Statu Thermal Ethernet Mod FC Mode Admin Evac	is : ↑ : ↑ de : End : End Mode : Off	Operable OK Host Host	Name Product Vendor Revision	: A Name : Cis : Cis : 0	co UCS 64 co System	154 ns, Inc.		PID Serial	:

Equipment / Fabric Interconnects / Fabric Interconnect B (subordinate)

General	Phy	sical Ports	Fans	PSUs	Physical Dis	play	FSM	Neighbors	Faults	Events	Statistics
Fault Sum	mary			Phy	sical Display						
0 Status	0	0	0	Pro	Jp Admin Do	own <mark>=</mark>	Fail Li	nk Down		in har	
Overall St Thermal	atus	: † Ope : † OK	erable	Na Pro	me oduct Name	B B Cisc	o UCS 64	154			
FC Mode Admin Eva	wode ac Mod	End Ho End Ho C	st	Ver	ndor vision	: Cisc : 0	o Systen	ns, Inc.		PID Serial	:

Assign VLANs

In order to recreate, VLAN 80 was created.

Step 1. In order to add the VLAN 80 navigate to **LAN tab > LAN Cloud > VLANs** click on add and complete the fields.



Create vNIC Template

Step 1. Navigate to LAN tab > Policies > root > vNIC Template and click **Add**. Select the vNIC template. Configure the name and select the appropriate Fabric ID. As a best practice, it is recommended to have a redundant vNIC configuration.

乕	All v	LAN / Policies / root / vNIC Templates								
		vNIC Templates								
	 root O Default while Rehavior 	+ - Ty Advanced Filter 🛧 Export 🐵 Print								
æ	ow Control Policies	Namo	VLAN	Nat						
	Dynamic vNIC Connection Policies	▶ vNIC Template DL2_FIB_470								
	 LACP Policies 	▶ vNIC Template DL2_FIB_80								
	LAN Connectivity Policies	▶ vNIC Template DL2_FIA_80								
	Multicast Policies	▶ vNIC Template DL2_FIA_470								
	default	▶ vNIC Template internal								
	igmp_proxy_dis	vNIC Template vNIC_0								
J.	Network Control Policies	▶ vNIC Template vNIC_A.								
	Threshold Policies	▶ vNIC Template vNIC_A_NewHire								
	VMQ Connection Policies	▶ vNIC Template vNIC_B								
	 usNIC Connection Refision 	▶ vNIC_Template vNIC_B_NewHire								
	vN/C Templates									
	Sub-Organizations Pools									
	▼ root 👽		+							
	▼ IP Pools		Add Delete	Info						
	 IP Pool demo-iscsi-ip-pool IP Pool demo-iscsi-ip-pool 									

Select the VLANs to be configured accordingly. In this example, the base VLAN is **VLAN 470**, and the disjoint VLAN is **VLAN 80**.



æ	AI *	LAN / Policies /	root / vNIC Templates					
	· · ·	vNIC Templates						
8	👻 raot 🦁	Modify v	JIC Template			?		
	Default vNIC Behavior	inicially vi	tio remplate					
ਰੱ <u>ਰ</u>	Flow Control Policies	Name	: DL2_FIA_470					
=	 Dynamic vNIC Connection Policies 	Description	: This vNIC Template all	ows VLAN 470 in I	FI-A			
-	LACP Policies	Table 10	Eshrin A		achia Failean			
=	LAN Connectivity Policies	Fabric ID	 Fabric B 	E	nacie Fallover			
	Link Protocol Policy Multicast Dolicies	Target	Adapter					
	default	Template Type	: Initial Template 	dating Template				
	iomo proxy dis	VLANS V	LAN Groups					
1 0	Network Control Policies X Advanced Ellar Accurate di Dást							
	 OoS Policies 	T/ Advanced Filt	er 🕆 Export 🖶 Print			5,		
	Threshold Policies	Select	Name	Native VLAN	VLAN ID			
	VMO Connection Policies		test	0	600			
	usNIC Connection Policies		VLAN_10		10			
	vNIC Templates		Vian_1000 - Applianc		1000			
	Sub-Organizations		VLAN_101		101			
	* Pools		VLAN 470	0	470	1		
	👻 root 🤨	Con source	: Ovnic Name O user b	xenned				
	▼ IP Paals	MTU	: 1500					
	IP Pool demo-iscsi-ip-pool							
	 IP Pool dummyippool 	MAC Pool	<pre>> Tot set> T</pre>					
	IP Pool ext-mgmt	OoS Policy	: enotests v					
	IP Pool iscsi-initiator-pool				ок	Cancel		
	IP Pool iscsi-Pac							
	IP Pool jenit-iscsi	-						

Repeat the same steps for Fabric B.

Step 2. Navigate to **LAN tab > Policies > root > LAN Connectivity Policies** and create the new policy, click in **Add**, and create the vNICs.

Write the name for the vNIC, select the MAC pool, and mark the check box Use vNIC Template.

	Al +	LAN / Policies / root / LAN Connectivity Po	licies		
	 Link Drofile 	LAN Connect	tivity Policy	? ×	
-	Threshold Policies	Name : LAN_DL2			
å	UDLD Link Policy	AUR Description : LAN Connectivity F	Policy for Disjoint Layer 2		
Ŧ	Default vNIC Behavior	AXL Click Add to specify one or more vN	Os that the server should use to connect to the LAN.		
_	Flow Control Policies	Infra	MAC Address	Native VLAN	
=	Dynamic vNIC Connection Policies LACP Policies	LAN	NO data avaliable		joint Layer 2
	LAN Connectivity Policies	LAN	_		
.	Link Protocol Policy Midland Policies	LAN	•		
- 0	 Muticast Policies default 	LAN			server 1/3 and 1/.
	igmp_proxy_dis	LCP	C Date A March		
	Network Control Policies OnS Policies	Test	Deele (Add C Modey		
	Threshold Policies	YSM			
	 VMQ Connection Policies 				
	 usNC Connection Delicies 				
~					
C	reate vNIC				? ×
Na	ame : Eth0				
MA	AC Address				
м	IAC Address Assignment	(112/128) -			
141	No Address Assignment. FI_A(113/128)			
	Create MAC Pool				
	The MAC address will be autom	atically assigned from the selected	d pool.		
	The MAC address assignment	change will be effective only af	ter server reboot.		
		_			
US					
Fa	bric ID :	Fabric B	Enable Failove	r	
VLA	AN in LAN cloud will take the pre	cedence over the Appliance Clour	when there is a name clash.		
	VI ANS VI AN Groups				
'	VDANS VDAN GIOUPS				
7/	Advanced Filter 🔺 Export 🖷	Print			
					۵
Se	elect	Name	Native VLAN	VLAN ID	٥
Se	elect	Name 125	Native VLAN	VLAN ID 125	۵
Se	elect	Name 125 480	Native VLAN	VLAN ID 125 480	\$
Se		Name 125 480	Native VLAN	VLAN ID 125 480	\$
Se		Name 125 480 default	Native VLAN	VLAN ID 125 480 1	\$
Se		Name 125 480 default DL2	Native VLAN O O O O O O O O O O O O O O O O O O O	VLAN ID 125 480 1 80	\$
Se	elect	Name 125 480 default DL2 User Defined	Native VLAN	VLAN ID 125 480 1 80	\$
CE	elect	Name 125 480 default DL2 User Defined	Native VLAN	VLAN ID 125 480 1 80	\$
Se CE M	elect	Name 125 480 default DL2 User Defined	Native VLAN	VLAN ID 125 480 1 80	\$
Se CL M [*] Pir	elect	Name 125 480 default DL2 User Defined	Native VLAN	VLAN ID 125 480 1 80	\$
See CL M' Pir	elect	Name 125 480 default DL2 User Defined	Native VLAN	VLAN ID 125 480 1 80	\$
See CL M ^T Pir	elect	Name 125 480 default DL2 User Defined	Native VLAN	VLAN ID 125 480 1 80	

Step 3. Use the **vNIC Template** previously configured, select the desired **Adapter Policy**, and click **OK**. Repeat the same procedure to Fabric Interconnect B.

Create vNIC

Name : Eth0						
Use vNIC Template : 🔽						
Redundancy Pair :	Peer Name :					
vNIC Template : DL2_FIA_470 V	Create vNIC Template					
Adapter Performance Profile	Adapter Performance Profile					
Adapter Policy : VMWare	Create Ethernet Adapter Policy					

Create vNIC

Name : Eth2						
Use vNIC Template : 🔽						
Redundancy Pair :	Peer Name :					
vNIC Template : DL2_FIA_80 V	Create vNIC Template					
Adapter Performance Profile						
Adapter Policy : <not set=""></not>	Create Ethernet Adapter Policy					

æ,	AI *	LAN / Policies / root / LAN Connectivity P	olicies					
∎ &	Link Profile Threshold Policies UDLD Link Policy	Properties for: LAN_DI	L2					
	root Default vNIC Behavior Plow Control Policies Dynamic vNIC Connection Policies LACP Policies	Actions Delete Show Policy Usage	Name : LAN_DL2 Description : LAN Connectivity Policy for Disjoint Layer 2 Owner : Local Click Add to specify one or more vNICs that the server should use to connect to the LAN.					
	LAN Connectivity Policies	Use Global	Name	MAC Address	Native VLAN			
	 Link Protocol Policy 		▶ vNIC Eth0	Derived				
1 0	Multicast Policies		▶ vNIC Eth1	Derived				
	iomo provy dis		▶ vNIC Eth2	Derived				
	 Network Control Policies 		▶ vNIC Eth3	Derived	Derived			
	 QoS Policies 							
	 Threshold Policies 							
	VMQ Connection Policies							
	VNIC Templates			🗉 Delete 🕀 Add 🔘 M	Modify			

Step 4. Go back to the Service profile and select the LAN Connectivity Policy.

Reboot the Server

Step 1. To apply the previously configured changes, reboot the server.

Note: From vCenter, ensure the node is in maintenance mode.

Step 2. Once the server finishes boot up, verify if the vNIC is present. Navigate to **Server > Service Profiles > root > Name of your Service Profile > Network tab.**

NICs								
Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement		
vNIC Eth0	00:25:85:FA:00:07	1	1	A	Any	1		
vNIC Eth1	00:25:85:FB:00:1F	2	2	В	Any	1		
vNIC Eth2	00:25:85:FA:00:08	5	3	A	Any	1		
vNIC Eth3	00:25:85:FB:00:6E	6	4	В	Any	1		
				🗈 Delete	dd 🛞 Modify			

Create VLAN Group

Step 1. Navigate to LAN > LAN Cloud > VLAN Groups > Create VLAN Groups.

Step 2. Select the name for the **VLAN Group** and choose the required VLAN, finally, add single Uplinks in **step 2**.

-				Create VLAN	Group		
		0	Select VLANs	Name : DL2			
	Port Channels			VLANs			
	Uplink Eth Interfaces		Add Uplink Ports				
윪	Eth Interface 1/32			Ty Advanced Filter 1	Export Print No Native VLAN		
	Eth Interface 1/45	3	Add Port Channels	Select	Name	Native VLAN	
重	Eth Interface 1/45				480		
	Eth Interface 1/47		Org Permissions		DL2		
≡	Eth Internace 1/48				0 Ca		
	VEAVs				DST_VLAN		
=	 VP Optimization Sets 				internal		
_	Padric B				kymylan		
Jan 1	 Port channels Unlink 5th Interference 						
~	Opink En interfaces			Create VLAN			
	En interrace 1/4/						
	VLAVS						
	VP Optimization Sets						
	Cos system Gass						
	DAN Pin Groups						
	Intreshold Policies						
	V VDAN Groups						
	VLANS						
	 Appliances 						
	 Fabric A 						
	Fabric B					Next > Finish C	Cane
	VLANS						

Step 3. Optionally move to step 3 in the VLAN group steps if you need to add Port Channels.

	Al	LAN / LAN Cloud /			Create	VLAN	l Group)					? >
	* LAN	VLAN Groups		Select VLANs		Uplin	k Ports				Selected	Uplink Port	5
	+ LAN Cloud	+ - Ty Advance	0	Add Uplink Ports	Fabric ID	Slot ID	Aggre	Port ID		Fabric ID	Slot ID	Aggre	Port ID
8	Fabric A	Name	•		A	1	0	32			No data	available	
	Port Channels Uplink Eth Interfaces	LAN Cloud	3	Add Port Channels	A	1	0	45					
	Eth Interface 1/32	> VLAN Group			A.	1	0	46					
-	Eth Interface 1/45	VLAN Group I	0	Org Permissions	A	1	0	47					
	Eth Interface 1/46	VLAN DL2			A	1	0	48					
	Eth Interface 1/47	N AN Group I				1	0	47					
	Eth Interface 1/48	, is it is a start of the			0			47					
J 0	VLANS												
	Fabric B												
	 Port Channels 												
	 Uplink Eth Interfaces 												
	Eth Interface 1/47												
	VLANs												
	 VP Optimization Sets 												
	 QoS System Class 												
	 LAN Pin Groups 												
	 Threshold Policies 												
	 VLAN Groups 												
	VLAN Group DL2												
	VLAN Group kvmvlangroup												
	VLANs												
	 Appliances 										_	_	
	 Fabric A 								< Prev	Next >) Fini	sh 🤇	Cancel
	 Fabric B 												

ESXi Configuration

Step 1. Log in to the ESXi host and navigate to the **Networking tab > Virtual Switches** and click **Add standard virtual Switch**, name the virtual switch, and select the uplink.

📲 Navigator 🗆	localhost.localdomain - Networking	I
✓ ☐ Host Manage Monitor	Port groups Virtual switches	Physical NICs VMkernel NICs TCP/IP stacks Firewall rules
✓ ∰ Virtual Machines 1 ✓ ∰ DL2_UCSM	Name	
Monitor	Add standard virtual s	witch - DL2_UCSM
Storage	Add uplink	
- 🕵 Networking 2	vSwitch Name	DL2_UCSM
vSwitch0 More networks	MTU	1500 🗘
	Uplink 1	vmnic1 - Up, 20000 mbps V
	Link discovery	Click to expand
	▹ Security	Click to expand
		Add

Step 2. Navigate to **Networking > Port Group > Add Port Group**. Name your port group, select the desired VLAN, and use the virtual switch previously configured.

1 Navigator		Q localhost.loca	aldomain - Networking	g					
👻 📋 Host		Port groups	Virtual switches	Physical NICs	VMkernel NICs	TCP/IP stacks	Firewall rules		
Manage Monitor		🧕 Add port g	roup 🥒 Edit settings	Refresh					
✓		Name							
- B DL2_UCSM		😥 VM Netwo	👷 VM Network						
Monitor		🧕 Managem	ent Network						
More VMs		Q DL2_UCN	Add port grou	p - DL2_UCSM_80					
🗉 🖬 Storage	1				-				
- 💇 Networking	2		Name		DL2_UCSM_80				
) 📥 DL2			VLAN ID		80 0				
vSwitch0									
more networks			Virtual switch		DL2	~			
			Security		Click to expand				
								Add	

Step 3. Navigate to Networking, select the vSwitch previously configured, and click on add uplink. In order to have redundancy add a new uplink that includes the VLAN used for the Disjoint Layer 2.

In this case, VLAN 80 was allowed in VNIC Eth2 (Fabric Interconnect A) and VNIC Eth3 (Fabric

Interconnect B).

🔜 Add uplink	
MTU	1500 🗘
Uplink 1	vmnic3 - Up, 20000 mbps 🗸 🗸
Uplink 2	vmnic2 - Up, 20000 mbps v
Link discovery	Click to expand
▶ Security	Click to expand
NIC teaming	Click to expand
 Traffic shaping 	Click to expand



Verify in UCSM

Verify the VLAN in the CLI

Open an SSH session to the Fabric Interconnects and run the command.

This command displays the information for the VLANs created and you can confirm the VLAN created for the Disjoint Layer 2.

VLAN	Name	Status	Ports
1	default	active	Po1, Eth1/5, Eth1/6, Eth1/8 Eth1/9, Eth1/10, Eth1/11 Eth1/12, Eth1/13, Eth1/16 Eth1/17, Eth1/18, Eth1/19 Eth1/20, Eth1/21, Eth1/22 Eth1/23, Eth1/24, Eth1/26 Eth1/27, Eth1/28, Eth1/29 Eth1/30, Eth1/31, Eth1/32 Eth1/30, Eth1/31, Eth1/35 Eth1/36, Eth1/37, Eth1/38 Eth1/39, Eth1/40, Eth1/41 Eth1/42, Eth1/43, Eth1/44 Eth1/45, Eth1/46, Eth1/47 Eth1/48, Eth1/49, Eth1/50 Veth876, Veth877, Veth1084 Veth119, Veth1120, Veth1122 Eth1/1/10, Eth1/1/18, Eth1/1/13 Eth1/1/2, Eth1/1/18, Eth1/1/20 Eth1/1/28, Eth1/1/29, Eth1/1/30 Eth1/1/31, Eth1/1/32
80	VLAN0080	active	Eth1/47
470	VLAN0470	active	Po1, Eth1/5, Eth1/6, Eth1/32
			Eth1/45, Eth1/46, Eth1/48
			Veth1084, Veth1090, Veth1092
			Veth1094, Veth1108, Veth1119
			Veth1120, Veth1122, Veth1131
			Veth1133

Verify the Virtual Interface (VIF) Path

Navigate to the SSH session and use the command:

FI-A# show service Server: 1/6 Fabric ID: A Path ID: 1	-profile circuit	<server numb<="" th=""><th>ber></th><th></th><th></th><th></th><th></th></server>	ber>				
VIF	VNIC	Link State	Oper State	Prot State	Prot Role	Admin Pin	Oper Pin
1131	Eth0	Up	Active	No Protection	Unprotected	0/0/0	0/0/1
1133	Eth2	Up	Active	No Protection	Unprotected	0/0/0	1/0/47
1135	fc0	Up	Active	No Protection	Unprotected	0/0/0	1/0/3
9327		Up	Active	No Protection	Unprotected	0/0/0	0/0/0
Fabric ID: B Path ID: 1					·		
VIF	vNIC	Link State	Oper State	Prot State	Prot Role	Admin Pin	Oper Pin

1132	Eth1	Up	Active	No	Protection	Unprotected	0/0/0	0/0/2
1134	Eth3	Up	Active	No	Protection	Unprotected	0/0/0	1/0/47
1136	fc1	Up	Active	No	Protection	Unprotected	0/0/0	1/0/3
9328		Up	Active	No	Protection	Unprotected	0/0/0	0/0/0

This command displays the VIF Paths, the interface that is pinned, and the corresponding vNICs.

In the output obtained, it can be seen that the corresponding VIF is **VIF 1134** which corresponds to the **vNIC Eth3** and is pinned to interface 1/0/47 in Fabric Interconnect B.

Also, VIF 1133 corresponds to vNIC Eth2 and is pinned to 1/0/47 in Fabric Interconnect A.

Verify the pinning border interfaces.

Run the command to verify the pinning to the Uplink Ports.

UCS-AS-MXC-P25-02-A(nx-os)# show pinning border-interfaces

		+
Border Interface	Status	SIFs
Po1	Active	Veth1084 Veth1090 Veth1092 Veth1094 Veth1108 Veth1119 Veth1120 Veth1131
Eth1/32	Down	
Eth1/45	Down	
Eth1/46	Down	
Eth1/47	Active	sup-eth1 Veth1133
Eth1/48	Down	
Eth1/51	Down	
Eth1/52	Down	
Eth1/53	Down	
Eth1/54	Down	

Verify the Designated Receiver

Run this command to verify the port that receives the multicast traffic for the VLAN.

```
FI-A(nx-os)# show platform software enm internal info vlandb id <VLAN-ID>
vlan_id 80
______
Designated receiver: Eth1/47
Membership:
Eth1/47
```

This output shows the correct uplink.

Verify the upstream Switch

Open an SSH session to the upstream switch and run the command.

NEXUS-01# show vlan brief VLAN Name		Status	Ports		
1	default	active	Po1, Po2, Po4, Po5, Po6, Po7 Po8, Po9, Po50, Po100, Eth1/1 Eth1/2, Eth1/3, Eth1/4, Eth1/5 Eth1/6, Eth1/8, Eth1/9, Eth1/10 Eth1/12, Eth1/13, Eth1/14 Eth1/15, Eth1/13, Eth1/19 Eth1/20, Eth1/21, Eth1/22 Eth1/23, Eth1/24, Eth2/1, Eth2/2 Eth2/3, Eth2/4, Eth2/5, Eth2/6 Eth2/7, Eth2/8, Eth2/10, Eth2/11 Eth2/12, Eth2/13, Eth2/14 Eth2/15, Eth2/16, Eth2/17 Eth2/18, Eth2/19, Eth2/20 Eth2/21, Eth2/22, Eth2/23 Eth3/1, Eth3/2, Eth3/3, Eth3/4 Eth3/5, Eth3/6 Fth2/18		
80	DL2	active	Po1, Po2, Po6, Po7, Po8, Po9 Po50, Po100, Eth1/1, Eth1/3 Eth1/4, Eth1/5, Eth1/6, Eth1/17 Eth1/19, Eth1/20, Eth1/21 Eth1/22, Eth1/23, Eth1/24 Eth2/1, Eth2/2, Eth2/3, Eth2/4 Eth2/5, Eth2/17, Eth2/18		
470	VLAN_470	active	Po1, Po2, Po3, Po4, Po5, Po6 Po7, Po8, Po9, Po50, Po100 Eth1/1, Eth1/3, Eth1/4, Eth1/5 Eth1/6, Eth1/7, Eth1/9, Eth1/10 Eth1/16, Eth1/19, Eth1/20 Eth1/21, Eth1/22, Eth1/23 Eth1/24, Eth2/1, Eth2/2, Eth2/3 Eth2/4, Eth2/5, Eth2/9, Eth2/17 Eth2/18, Eth2/24		

This output shows the port that is associated with VLAN 80. In this case, the desired port is the Ethernet 1/17 which is associated with the uplink 1/47.

On the other hand, you can verify the MAC address table to check what Virtual Machine (VM) shows.

Verify the connection between the VLAN network in the ESXi

Open the Terminal in the Virtual Machine and ping to the default gateway of the VLAN network; you then see a successful ping.

- DOBALLIN	L MILLIN / UNUSUAL
DL2_UCSM	
Applications Places Terminal	
root@localhost:~	
File Edit View Search Terminal Help	
[root@localhost ~]# ping 192.168.80.1	
PING 192.168.80.1 (192.168.80.1) 56(84) bytes o	f data.
64 bytes from 192.168.80.1: icmp_seq=1 ttl=254	time=2.40 ms
64 bytes from 192.168.80.1: 1cmp_seq=2 ttl=254	time=1.28 ms
64 bytes from 192.168.80.1: 1cmp_seq=3 ttl=254	time=1.34 ms
$64 \text{ bytes from } 192.168.80.1; \text{ icmp_seq}=4 \text{ ttt}=254$	time=1.32 ms
64 bytes from 192.168.80.1: jcmp_seq=6 ttl=254	time=1.24 ms
64 bytes from 192.168.80.1: icmp_seq=7 ttl=254	time=1.31 ms
64 bytes from 192.168.80.1: icmp seq=8 ttl=254	time=1.32 ms
H64 bytes from 192.168.80.1: icmp_seq=9 ttl=254	time=1.23 ms
64 bytes from 192.168.80.1: icmp_seq=10 ttl=254	time=1.38 ms
64 bytes from 192.168.80.1: icmp_seq=11 ttl=254	time=1.32 ms
64 bytes from 192.168.80.1: icmp_seq=12 ttl=254	time=1.30 ms
64 bytes from 192.168.80.1: icmp_seq=13 ttl=254	time=1.39 ms
64 bytes from 192.168.80.1: 1cmp_seq=14 ttl=254	time=1.22 ms
64 bytes from 192.168.80.1: 1cmp_seq=15 ttl=254	time=1.36 ms
64 bytes from 192.168.80.1: icmp_sed=17 ttl=254	time=1.10 ms
64 bytes from 192.168.80.1: jcmp_seg=18 tt]=254	time=1.12 ms
64 bytes from 192.168.80.1: icmp_seq=10 ttl=254	time=1.23 ms
64 bytes from 192.168.80.1: icmp_seq=20 ttl=254	time=1.30 ms
64 bytes from 192.168.80.1: icmp seq=21 ttl=254	time=1.15 ms
64 bytes from 192.168.80.1: icmp_seq=22 ttl=254	time=1.01 ms

Related Information

Technical Support & Documentation - Cisco Systems

<u>Disjoint Layer 2</u> <u>Cisco UCS Manager Network Management Guide, Release 4.0</u> <u>Using the LAN Uplinks Manager</u>