

Nexus Dashboard NDFC Fabric Discovery Troubleshooting

Jeffrey Mertes, Technical Consulting Engineer, Cisco

TACDCN-2009

cisco ile

#CiscoLive



- Introduction
- ND Health and App Checks
- LAN and SAN Fabric Pre-Checks
- LAN and SAN Fabric Adds
- SNMP/SSH Checks
- Other Tools
- NDFC Techsupport Procedure
- Conclusion/Takeaways

Introduction

- Nexus Dashboard Fabric Controller (NDFC) is an application that is hosted on a single or 3 node cluster of Nexus Dashboard virtual or physical nodes. (vND or pND)
 - Nexus Dashboard uses a k8s backend to provide cluster, infrastructure and application / NDFC pods and containers.
- Administrators must have certain criteria reviewed and adhered to so that they can successfully add LAN and SAN fabric with switches.
 - Recommend to review scale considerations
 - Recommend to review compatibility considerations
 - Review Whitepapers and Deployment Guides to prepare for ND/NDFC deploy.
 - * See links in hidden side

ND 3.1.1k Health and App Checks NDFC 12.2.1 LAN/SAN

- Virtual Nexus Dashboard (vND) is typically VMWare OVA or kVM based deploy. Physical Nexus Dashboard (pND) is appliance based. There are 2 server options -* UCS-C220-M5 (SE-NODE-G2) or UCS-C225-M6 (ND-NODE-L4)
 * Note - UCS-C225-M6 (ND-NODE-L4) runs on ND 2.3.2 or higher only.
- 'acs version' Nexus Dashboard version installed on vND or pND
- 'acs health' summary of cluster health and if any pods in non-desired state or warning with NTP or DNS.
- 'acs show masters' table of master nodes in cluster, with version, role, Data and Mgmt IPs, status and S/N
- 'kubectl get apps | grep cisco-ndfc' list versions of NDFC and leveraged components for elasticsearch, cockroachdb, minio
- 'kubectl get pods A o wide | grep cisco-ndfc' list NDFC pod details with status, age, location where running

NOTE - ND CLI SSH login to mgmt. IP as 'rescue-user'. This is equivalent of UI local 'admin' user. Uses same password. This 'rescue-user' allows non-impacting commands. Can refer to TAC for temp root access as needed. Some debug commands do need temp root access. This token/password does expire on a regular basis (~30 min).

ND 3.1.1k Health and App Checks NDFC 12.2.1

- 'acs version' Nexus Dashboard version installed on vND or pND
- 'acs health' summary of cluster health and if any pods in non-desired state or warning with NTP or DNS.
- 'acs show masters' table of master nodes in cluster, with version, role, Data and Mgmt IPs, status and S/N

rescue-user@jmSAN:~\$ acs version Nexus Dashboard 3.1.1k rescue-user@jmSAN:~\$ acs health							
<pre>status status according to the status according t</pre>							
rescue-user@jmSA	N:~\$ acs show ma	asters					
NAME (*=SELF)	SERIAL	VERSION	ROLE	DATANETWORK	MGMTNETWORK	STATUS	
*jmSAN	4ACEE85D744A	3.1.1k	Master	xx.2.35.97/24 ::/0	xx.2.32.72/24 ::/0	Active	

NOTE - ND CLI SSH login to mgmt. IP as 'rescue-user'. This is equivalent of UI local 'admin' user. Uses same password. This 'rescue-user' allows non-impacting commands. Can refer to TAC for temp root access as needed. Some debug commands do need temp root access. This token/password does expire on a regular basis (~30 min).

ND 3.1.1k Health and App Checks NDFC 12.2.1

 'kubectl get apps | grep cisco-ndfc' – list versions of NDFC and leveraged components for elasticsearch, cockroachdb, minio

rescue-user@jmSAN:~\$ kubectl get apps grep nd.	fc			
cisco-ndfc-12.2.1.316	Enable	Enable	success	Enabled
cisco-ndfc-controller-elasticsearch-12.2.1.316	Enable	Enable	success	Enabled
cisco-ndfc-s3-minio-12.2.1.316	Enable	Enable	success	Enabled
cisco-ndfc-sql-cockroachdb-12.2.1.316	Enable	Enable	success	Enabled

• Nexus Dashboard webUI Service Status (NDFC ~ Fabric Controller)

o Admin Console 🗸		
Analyze > Service Status		
Service Status		
Name	Deployment Status	Health Status
Fabric Controller	⊘ Enabled	O Healthy
	#Ciscol ive TACD	CN-2009 © 2024 Cisco and/or its affiliates A

ND 3.1.1k Health and App Checks NDFC 12.2.1

• 'kubectl get pods - A - o wide | grep cisco-ndfc' - list NDFC pod details with status, age, location/node where running

rescue-user@jmSAN:~\$ kubecti get pous	s -A -O wide; grep cisco-naic	2 (2	Dunning	0	224	170 17 55 07	
cisco-ndic-controller-elasticsearch		2/2	Running	0	230	1/2.1/.55.5/	Jmsan
cisco-ndfc-s3-minio	minio-0	2/2	Running	0	23d	172.17.55.39	jmsan
cisco-ndfc-sql-cockroachdb	cockroachdb-0	2/2	Running	0	23d	172.17.55.38	jmsan
cisco-ndfc-sql-cockroachdb	cockroachdb-init-7p5zb	0/1	Completed	0	23d	172.17.55.35	jmsan
cisco-ndfc	dcnm-admin-578dfcfd44-kjcfd	1/1	Running	0	23d	172.17.55.53	jmsan
cisco-ndfc	dcnm-alarm-7867df9567-t2fgq	1/1	Running	0	23d	172.17.55.50	jmsan
cisco-ndfc	dcnm-backupmgr-6549686fbc-lt7fp	1/1	Running	0	23d	172.17.55.44	jmsan
cisco-ndfc	dcnm-bifrost-5b8b6dcbcb-8kc8s	1/1	Running	0	23d	172.17.55.41	jmsan
cisco-ndfc	dcnm-configtemplate-848c7f9f4-plgg8	1/1	Running	0	23d	172.17.55.49	jmsan
cisco-ndfc	dcnm-entity-status-5845f4bf96-lnnz2	1/1	Running	0	23d	172.17.55.48	jmsan
cisco-ndfc	dcnm-fm-54698d6977-6qmfw	1/1	Running	1 (23d ago)	23d	172.17.55.46	jmsan
cisco-ndfc	dcnm-imagemanagement-img-mgmt-default-5d69dc86d9-g629d	1/1	Running	0	22d	172.17.55.65	jmsan
cisco-ndfc	dcnm-lic-cb79dcb54-9gnls	1/1	Running	0	23d	172.17.55.45	jmsan
cisco-ndfc	dcnm-log-collector-nvgnw	1/1	Running	0	23d	172.17.55.42	jmsan
cisco-ndfc	dcnm-log-manager-5ccc9f8b97-ql4cs	1/1	Running	0	23d	172.17.55.54	jmsan
cisco-ndfc	dcnm-poap-data-poap-data-default-7b49875889-tz8w8	1/1	Running	0	22d	172.17.55.63	jmsan
cisco-ndfc	dcnm-report-master-preport-default-5b8cdf4879-csss5	1/1	Running	0	22d	172.17.55.58	jmsan
cisco-ndfc	dcnm-report-worker-preport-default-98bd9d976-vf6v5	1/1	Running	0	22d	172.17.55.61	jmsan
cisco-ndfc	dcnm-san-config-san-default-7b9c55795b-vtv8h	1/1	Running	0	22d	172.17.55.64	jmsan
cisco-ndfc	dcnm-san-device-manager-san-dm-default-5dd6dc59b6-725nv	1/1	Running	0	22d	172.17.55.56	jmsan
cisco-ndfc	dcnm-san-discovery-manager-san-default-854f5f6fd9-9j9lh	1/1	Running	0	22d	172.17.55.57	jmsan
cisco-ndfc	dcnm-san-discovery-worker-san-discovery-worker-1-677d479b66fhsh	1/1	Running	0	22d	172.17.55.66	jmsan
cisco-ndfc	dcnm-san-insight-manager-san-insight-default-6fb9d87f4b-hmxcj	1/1	Running	0	8d	172.17.55.68	jmsan
cisco-ndfc	dcnm-san-insight-post-process-blue-san-insight-default-767xv4ds	1/1	Running	0	8d	172.17.55.69	jmsan
cisco-ndfc	dcnm-san-insight-ui-san-insight-default-7577599c7b-7vj4w	1/1	Running	0	8d	172.17.55.67	jmsan
cisco-ndfc	dcnm-san-inventory-san-default-6df7cdd7dc-mv4wm	1/1	Running	0	22d	172.17.55.59	jmsan
cisco-ndfc	dcnm-sim-agent-0	1/1	Running	0	23d	172.17.55.47	jmsan
cisco-ndfc	dcnm-sim-master-8cb76c67d-htks9	1/1	Running	0	23d	172.17.55.43	jmsan
cisco-ndfc	dcnm-site-mgr-957b879cb-6196b	1/1	Running	0	23d	172.17.55.51	jmsan
cisco-ndfc	dcnm-storage-san-default-789f8bf78c-6mbc4	1/1	Running	0	22d	172.17.55.60	jmsan
cisco-ndfc	dcnm-syslog-trap-data-eventmgr-data-default-7cfd5f6c79-h59s9	1/1	Running	0	22d	172.17.55.62	jmsan
cisco-ndfc	dcnm-ui-h8r7r	1/1	Running	0	23d	172.17.55.40	jmsan

cisco

LAN and SAN Fabric Pre-Checks (LAN Controller)

- Before enabling NDFC, add Persistent IPs in ND System Settings (below in Mgmt for LAN)
- When you enable NDFC, you select the application deployment 'persona' as either LAN(Fabric Controller), LAN(Fabric Discovery) or SAN Controller

Admin Console				
Routes		E		
Management Network Routes				
10.122.164.0/24			Papric Controller	
Data Network Routes			Admin > System Settings	
			System Settings	
			Learn More	
External Service Pools		E	Server Settings Feature Management	
Management Service IP Usage	Data Service IP Usage			
2	0		Fabric Discovery	Fabric Controller ()
			Discovery, Inventory and Topology for LAN deployments	Full LAN functionality in addition to Fabric Discovery
Management Service IP's	Usage	Assignment		Started
X.2.32.70	In Use	cisco-ndfc-dcnm-syslog-trap-mgm		
X.2.32.71	In Use	cisco-ndfc-dcnm-poap-mgmt-http- ssh		
Data Service IP's	Usage	Assignment		

LAN and SAN Fabric Pre-Checks (SAN Controller)

 Before enabling NDFC, add Persistent IPs in ND System Settings (below in Data for SAN but used Route to Management)

cisco ne!

 When you enable NDFC, select deployment 'persona' as either LAN(Fabric Controller), LAN(Fabric Discovery) or SAN Controller

Admin Console					
Routes Management Network Routes x 40.15.0/24 Data Network Routes]		Edit Fabric Controller Admin > System Settings System Settings Learn More		
External Service Pools Management Service IP Usage Da Available 2	ata Service IP Usage In Use 2		Server Settings Feature Management Fabric Discovery Discovery, Inventory and Topology for LAN deployments	Fabric Controller	SAN Controller (SAN Management for MDS and Nexus switches
Management Service IP's	Usage	Assignment			Started
x.2.32.73	Not In Use				
x.2.32.75	Not In Use				
Data Service IP's	Usage	Assignment			
x .2.35.98	In Use	cisco-ndfc-dcnm-poap-data-htt	p-ssh		
x 2.35.99	In Use	cisco-ndfc-dcnm-syslog-trap-da	ta		

LAN and SAN Fabric Pre-Checks

- LAN deploys default to device communication over ND Management bond1 to device mgmt0. SAN deploys default to device communication over ND Data bond0 to device mgmt0.
- One can adjust to have LAN communicate over Data for inband (SVI device disc IPs) or add Route as needed in UI. Check System Setting LAN Device Mgmt Connectivity from Management to Data for Inband IP discovery (SVI instead of mgmt0)
- At times, adding a route to Mgmt for SAN devices is warranted as I performed on left below.

Admin Console 🗸	SAN de add Rou	ploy default ute for Mgm	ts to Data, t if needed				
Deutes	root@jmSAN:~# Kernel TP rout:	route -n ing table	Now route	s over b	ond1	mgmt int	
Routes	Destination Gateway		Genmask	Flags	Metric	Ref Us	e Iface
	0.0.0.0	x.2.32.1	0.0.0.0	UG	0	0	0 bond1
Management Network Pourtes	x.2.32.0	0.0.0.0	255.255.255.	0 U	0	0	0 bond1
wanagement wetwork Routes	x.2.35.0	0.0.0.0	255.255.255.	0 U	0	0	0 bond0
	x.40.15.0	x.2.32.1	255.255.255.	0 UG	0	0	0 bond1
V 40 15 0/24	100.80.0.0	0.0.0.0	255.255.0.0	U	0	0	0 bond0
40.13.0/24	169.254.0.0	0.0.0.0	255.255.255.	128 U	0	0	0 k8br1
Data Network Routes	172.17.0.0 root@jmSAN:~#	0.0.0.0	255.255.0.0	U	0	0	0 k8br0

Fabric Controller 🗸											
dmin > System Set	ttings										
System Settings	5										
Server Settings	Feature N	lanagement	LAN Dep Device Ma Tune to	loy defau nagemer Data fo	uls to LAN nt on Mgm r Inband	ıt.					
Alarms Events	Reports	LAN-Fabric	Discovery	SSH	VMM	SNMP	Admin	SMTP	Debug		
LAN Device Manag	jement Con	nectivity									
Management				SA Fat	N Controller pric Controlle	device conn er and Fabric	ectivity is alwa Discovery mu	ays over Data ist select app	subnet and this propriate option.	s property has no imp	bact.
Management			~	•							
Data											

- For <u>LAN deploys</u> two stage flow
 - Discover the seed device/s NDFC first.
 - Then Add assuming Discovery was successful and Device/s list as Manageable

Note – For LAN only, define fabric template and settings previous to device/s additions.

witches – Fabric: CL_lan		
ch Addition Mechanism* Discover	First Discover, mostly SNMP in backend	
Seed Switch Details		
Seed IP*		
10.122.164.173		
Ex: "2 2 2 20" or "10 10 10 40-60"	or "2 2 2 2 0	
2.2.2.21"	01 2.2.2.20,	
Authentiastion Brotonol*		
Ruthentication Protocol		
MD5	~	
Isarnama*	Deseword*	
osemane.	Password	
admin		•
Max Hops*	Set as individual device write credenti	ial
Max Hops*	Set as individual device write credenti	ial
Max Hops*	Set as individual device write credenti	ial
Max Hops* 2 Preserve Config	Set as individual device write credenti	ial
Max Hops* 2 Preserve Config	Set as individual device write credenti	ial



- For LAN deploys two stage flow
 - Discover the seed device/s NDFC first.
 - · Then Add assuming Discovery was successful and Device/s list as Manageable

Note – For LAN only, define fabric template and settings previous to device/s additions.



cisco / ille

- For <u>LAN deploys</u> two stage flow
 - · Discover the seed device/s NDFC first.
 - Then Add assuming Discovery was successful and Device/s list as Manageable

Note – For LAN only, define fabric template and settings previous to device/s additions.

lan				×
ils				
Switch 10 122 164	173	Authentication Protoco	ol Username admin	
10.122.104		MDS	dumm	
Max Hops		Preserve config		
2 vice write		Enabled		
		Add S	Sussessful	
			n Close	
Serial Number	IP Address	Model	Version Sta	itus
	Ian ils Switch 10.122.164 Max Hops 2 vice write Serial Number	Lan ils Switch 10.122.164.173 Max Hops 2 vice write Serial Number IP Address	Ian Ils Switch 10.122.164.173 Max Hops 2 Max Hops	Ilan Ils Switch 10.122.164.173 Max Hops 2 Max Hops

cisco / ille

 For <u>SAN deploys</u> – single flow where you add SAN seed or principal device only and NDFC will discover all devices in fabric assuming same creds and links exist 'sh fcs ie' output.

dd Fab	ric		
n More			
	Fabric Name*		
	CL_san		
	Fabric Seed Switch Type Cisco O Non-Cisco		
	Fabric Seed Switch*		
	Enter a valid IP V4 address or DNS n	ame (e.g. 1.2.3.4 or xyz.com)	
	Use SNMPv3 / SSH		
	Authentication / Privacy		
	User Name	Password	
	admin		•

Post SAN fabric add / Managed Continuously



- SNMP and SSH user cred and password must be the same on Nexus device.
- LAN devices in same fabric can use separate creds for discovery/add.
 SAN devices must all use same credential for discovery/add. (only 1 seed device add)
- Device credential can be local or a remote tacacs/ldap, cred.
- SNMP User Auth Method must match NDFC server setting.
- SNMP/SSH communication for discovery/add is tied to IP where NDFC discovery pod runs and typically the ND Management IP for LAN and ND Data IP for SAN.
- SSH persistent IP defined in ND settings is used for POAP(Power on Auto Provision), Image Management and SCP transfer operations.

• For 'Unknown User or Password' error, check the following -

• On device CLI

sh snmp user sh run | inc <username> sh accounting log | inc sync (below local user, no output expected)

F241-15-09-9710-1# sh snmp user | inc admin admin md5 aes-128(no) network-admin

F241-15-09-9710-1# sh run | inc admin username admin password 5 \$5\$pqQgPBRR\$DCNLFQbs.eUCtT0XDA8PV103YKdNX9gPhsrfuDDhXf7 role network-admin snmp-server user admin network-admin auth md5 0x83c6f217cef0f643fee4a3130f488a14 priv aes-128 0x83c6f217cef0f643fee4a3130f488a14 localizedkey

F241-15-09-9710-1# sh accounting log | inc sync



 On ND server CLI, check the following as rescue-user ping <device_mgmt_IP> (defaults to bond1 / assuming no ICMP firewall block) ping <device_mgmt_IP> -i bond0 (if no response on bond1) ssh <username>@<device_mgmt_IP>

> rescue-user@jmSAN:~\$ ping xx.40.15.17 PING xx.40.15.17 (xx.40.15.17) 56(84) bytes of data. 64 bytes from xx.40.15.17: icmp seq=1 ttl=57 time=0.308 ms 64 bytes from xx.40.15.17: icmp seq=2 ttl=57 time=0.322 ms 64 bytes from xx.40.15.17: icmp seq=3 ttl=57 time=0.319 ms ^Crescue-user@imSAN:~\$ rescue-user@jmSAN:~\$ ssh admin@xx.40.15.17 User Access Verification (admin@xx.40.15.17) Password: Cisco Nexus Operating System (NX-OS) Software TAC support: http://www.cisco.com/tac Copyright (c) 2002-2023, Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/lgpl-2.1.php F241-15-09-9710-1#

 On ND server CLI, for deeper review if necessary, with TAC assist, can enable temp root access to run checks curl http://<device_mgmt_IP>:161 snmpwalk -v3 -u <username> -I authNoPriv -a MD5 -A <password> tcp:<device_mgmt_IP>

NOTE - Curl empty response is fine, proves tcp 161 is open to device.

Full snmpwalk, terminate if response. Check to see type of error and confirm if mods have corrected.

```
root@jmSAN:~# curl http://xx.40.15.17:161
curl: (52) Empty reply from server
root@jmSAN:~# snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A ciscoadmin123 tcp:xx.40.15.17
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco NX-OS(tm) m9700, Software (m9700-sf4ek9-mz), Version
9.4(1a), RELEASE SOFTWARE Copyright (c) 2002-2023 by Cisco Systems, Inc. Compiled 12/25/2023
12:00:00"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.12.3.1.3.1327
iso.3.6.1.2.1.1.3.0 = Timeticks: (434095433) 50 days, 5:49:14.33
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "F241-15-09-9710-1.cisco.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 70
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
1 \le 0.3, 6, 1, 2, 1, 1, 9, 1, 2, 1 = 0 \text{TD}; 1 \le 0.3, 6, 1, 6, 3, 1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.16.2.2.1
^{\rm C}
root@jmSAN:~#
```

- · Depending on ping, ssh, snmpwalk, curl results, different action plans are crafted -
- Update cred in NDFC or update on device, fix tacacs if remote cred or create new test cred
- Add route in ND Cluster Config/System Setting if connectivity across non-preferred ND interface
- Verify that bi-directional tcp/udp port 161 is allowed or open (firewall, etc)
 Note NDFC prefers TCP 161 for discovery/sync, and UDP 161 for Perf Data collection if enabled
- Verify that no ACL or line vty configs conflict with SSH or SNMP access.

Other Tools

• Run tcpdump on ND during webUI device add or snmpwalk / requires TAC assist for temp root access

tcpdump host <device_mgmt_IP>

most basic to check all ints and both SNMP & SSH to device # for LAN, the discovery/add is SNMP, then the Import is both SSH and SNMP

• Can run ethanalyzer on N9K/MDS as well if above is not possible at the moment.

ethanalyzer local interface mgmt capture-filter "host <ND_IP>" limit-captured-frames 0

NDFC Techsupport Procedure

- ND webUI navigation paths to Techsupport differ for ND 2.x and N 3.x
 - If ND 2.x, Admin Console / Operations / Tech Support
 - If ND 3.x, Admin Console / Analyze / Tech Support

Note - See following slides pics for reference

- 1. Click 'Collect Tech Support' on right.
- 2. Give scope from dropdown 'Nexus Dashboard Fabric Controller'. Collect.
- 3. Wait for that to finish.
- 4. Assuming success, you would click specifically on the blue filename link under Name column.
- 5. Then a popup occurs on right. Click '**Download All**'. We want NDFC techsupports from all nodes.
- 6. Please verify no popup blocker. Then upload files to case for review.
- 7. Upload to SR attach.

NDFC Techsupport Procedure

• Scope Defaults to 'System' for ND Infra support. Select Fabric Controller for NDFC support/s.

cisco Nexus Dashboard		
à Quantan	Analyze > Tech Support	Collect Tech Support ×
	Tech Support	1
🖉 Manage		You are about to collect Tech Support. Are you sure you want to continue?
💮 Analyze	Filter by attributes	to continue?
a Admin		Name
	Name	
	cisco-ndfc_2024-	Scope
		System ~
	1 items found	System 🗸
		Fabric Controller
	© Cisco Systems, Inc.	Cancel Collect



NDFC Techsupport Procedure

🗂 Admin Console 🗸 Analyze > Tech Support cisco-ndfc_2024-05-13T15-09-36Z **Tech Support** General Status Filter by attributes ⊘ Success Creation Time Name Cr 2024-05-13, 10:09:36 cisco-ndfc_2024-05-Scope 20 13T15-09-36Z Fabric Controller Node Status 1 items found Download Node Status imSAN Download Success 100% **Download All**

cisco live

Conclusion/Takeaways

- Nexus Dashboard Fabric Controller (NDFC) is an application that is hosted on a single or 3 node cluster of Nexus Dashboard virtual or physical nodes. (vND or pND)
- Recommended to review basic ND health checks on node/s via CLI or from Admin Console (System Overview 2.x or Platform View 3.x)
- LAN and SAN fabrics do have separate device add flows/methods. Review LAN/SAN Configuration Guides as needed.
- Review SSH and SNMP device credentials and reachability aspects from device mgmt. IPs back to ND interfaces prior to fabric/device adds.
- Consider SNMP and SSH tests or route adjustments in ND if warranted.
- If above does not clear issue, collect NDFC techsupports for detailed TAC review.

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at <u>www.CiscoLive.com/on-demand</u>

Contact me at: jmertes@cisco.com

TACDCN-2009

CISCO The bridge to possible

Thank you

cisco Live!

#CiscoLive