Cisco Application Centric Infrastructure SAN Profile

October 2017

Contents

Profile introduction

This document focuses on the deployment of the Cisco® Application Centric Infrastructure (Cisco ACI™) unified fabric converged network solution in a data center. Cisco Unified Fabric provides the networking foundation for the Cisco Unified Data Center. You can use this foundation to build your data center architecture, whether you run a traditional data center or are on your way to a full private cloud or hybrid private and public cloud computing environment.

Cisco Unified Fabric is built on three main pillars: convergence, scalability, and intelligence. Cisco Unified Fabric can help you reduce costs, migrate to the next-generation data center, and bring value to your business.

Convergence

Convergence of the data center network is the melding of the SAN and the LAN. Cisco Unified Fabric supports data center convergence by consolidating multiprotocol storage and LAN traffic onto a single, scalable, intelligent network. This consolidation reduces costs and increases efficiency. Companies need to continue to use their current SAN infrastructure while extending it gradually, transparently, and nondisruptively to the Ethernet network. The traditionally separate LAN and SAN fabrics evolve into a converged, unified storage network through normal refresh cycles that replace old servers containing Host Bus Adapters (HBAs) with new ones containing Converged Network Adapters (CNAs). Storage devices undergo a similar refresh process.

Cisco customers can deploy an Ethernet network for the data center that meets the needs of storage traffic, with a lossless, in-order, highly reliable network for the data center, by using Fibre Channel over Ethernet (FCoE).

Scalability

A simple definition of scalability is the capability of a system to grow as needs change. Scalability often is described by the number of nodes that a given architecture can ultimately support. Cisco Unified Fabric delivers true scalability. It not only enables port counts to increase as needed, but it does so without compromising on performance, manageability, or cost.

Scalability begins with 10 Gigabit Ethernet. 10 Gigabit Ethernet allows customers to consolidate their networks, so the network has fewer tiers and fewer ports overall and exponentially more usable bandwidth for servers and storage. By moving to 10, 40, and 100 Gigabit Ethernet technologies, customers will be able to consolidate the number of ports and cables dedicated to servers as well as the overall number of switches under management in the data center. The reduction in the number of devices reduces management overhead and rack-space, power, and cooling requirements.

Reduced operating costs

Consolidation of the general data and storage network can save customers a lot of money. For example, customers can significantly decrease the number of physical cables and ports by moving to a converged 10 Gigabit Ethernet network because the number of cables required for reliability and application bandwidth is significantly reduced.

A standard server requires at least four networking cables: two for the SAN and two for the LAN. Often, more 1 Gigabit Ethernet ports are needed to meet bandwidth requirements and to provide additional connections for server management and for a private connection for server clusters. Two 10 Gigabit Ethernet converged ports can replace all these ports, providing a cable savings ratio of at least 2:1. From a larger data center perspective, this cable reduction means fewer ports and the capability to decrease the number of switches and layers in the data center, correspondingly reducing the amount of network oversubscription. Reducing cabling saves both acquisition costs and the costs of running the cables, and it reduces cooling costs by improving air flow.

Also, by eliminating or reducing the second storage network, customers end up with less equipment in the data center, saving on costly rack space, power, and cooling and making the overall data center much more efficient. However, the biggest cost savings is the capability for administrators to shift their time from maintenance of two separate networks and their associated cables and hardware to working on projects that directly benefit the business.

Profile summary

Table 1 summarizes the main areas of focus in this profile.

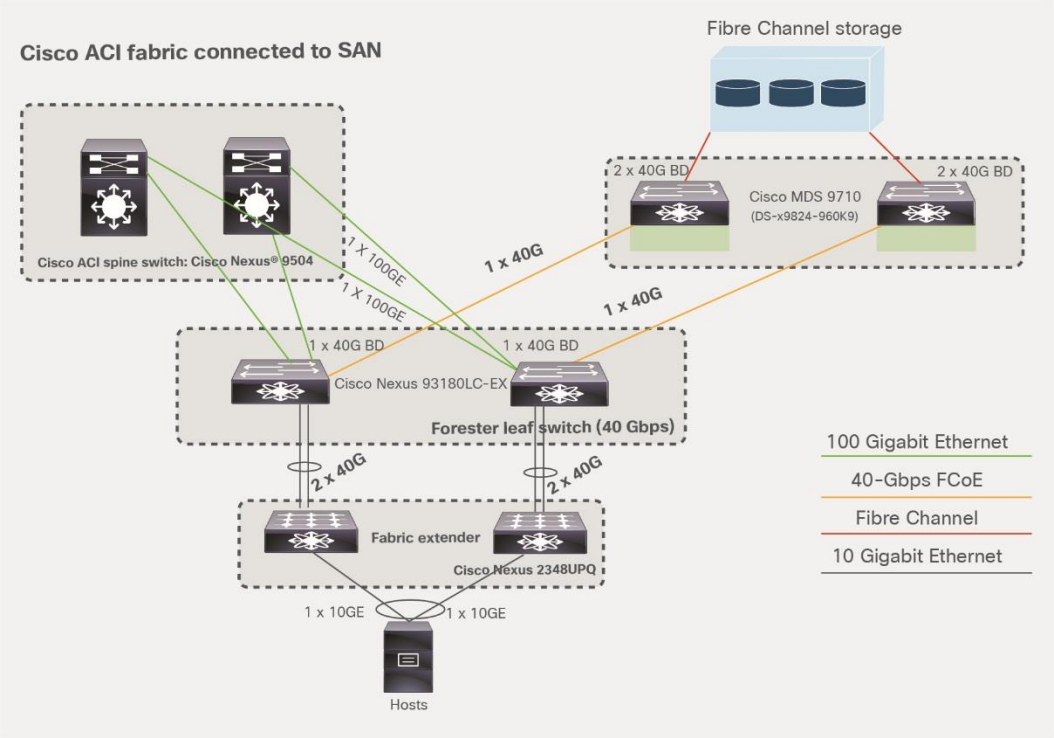
Table 1. Cisco ACI SAN profile summary

Deployment areas	Features
Converged network	FCoE, FCoE and N-Port Virtualization (NPV), fabric extenders, zoning, and device alias
High availability	High availability through virtual-Port-Channel (vPC) links and redundant network paths and switches (note that vPC is transparent to FCoE and does not support FCoE information synchronization and checkpoints)
Efficient network management	Cisco Application Policy Infrastructure Controller (APIC)
Performance and scalability	• 40-Gbps FCoE host ports and uplink network ports • Fabric extender support • 1 fabric login (FLOGI) and 80 fabric discovery (FDISC) commands per port • 256 FLOGI commands per switch • 32 VSANs • 256 virtual Fibre Channel (vFC) interfaces

Network profile

Based on research, customer feedback, and configuration samples, the profile presented here is designed with a generic deployment topology that can easily be modified to fit any specific deployment scenario. Note that this profile includes only the SAN part of the data center network. Figure 1 shows the topology.

Figure 1. Deployment topology



This topology shows a typical Cisco ACI leaf-and-spine fabric connected to a storage network. The Cisco MDS 9700 Series Multilayer Director is positioned in the storage core with the Cisco ACI leaf switches (Cisco Nexus 9000 Series Switches), which are part of the Cisco ACI fabric, at the access layer as the converged network, with fabric extenders facing the hosts. The Cisco ACI (Cisco Nexus 9000 Series) leaf switches operate in FCoE NPV mode, and the MDS 9700 Series switches act as Fibre Channel and FCoE switches.

Note: The test topology was the basic topology shown in Figure 1. In addition, several FCoE host-emulator and traffic-generator ports were included along with the Cisco ACI (Cisco Nexus 9000 Series) leaf ports, fabric extender ports, and MDS ports.

Hardware profile

Table 2 lists the relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end profile deployment.

The hardware, the relevant software versions, and the roles of these devices complement the physical topology shown earlier in Figure 1.

Table 2. Hardware profile of servers and endpoints

Virtual machines and hardware	Description
Cisco MDS 9700 Series	Used as storage core running Cisco NX-OS
Multilayer Directors	Software Release 8.2.1 or later Supports 40-Gbps FCoE and 32-Gbps Fibre Channel
Cisco Nexus 9000 Series Switches: Cisco ACI leaf switches with fabric extenders attached	Provides converged access running Cisco APIC Release 2.2(1) and switch Release 12.2(1)

Virtual machines and hardware	Description
Cisco Unified Computing System™ (Cisco UCS®) server	Manages and hosts the virtual machines
NetApp target	Used as storage device
Cisco Nexus 2000 Series Fabric Extenders	Used as fanout device
Spirent and Ixia	Provides FCoE emulation and traffic generation

Use-case scenarios

Test methodology

The scenarios listed in Table 3 were tested using the topology defined in Figure 1 along with the test environment already explained in this document.

The CPU and memory use were monitored during the night and during weekends, and memory-leak checks were performed. To test the robustness, of the profile, certain negative events were triggered during the use-case testing.

Use cases

Table 3 summarizes the use cases that were tested using the unified fabric converged network profile. The tests were divided into customer use-case scenarios as listed in the table.

The customer use cases consist of system upgrade and bring-up, operation triggers and configuration changes, steady state and usability, network events and link flaps, and resiliency and error recovery.

Table 3. Use cases

Number	Focus	Use case
System upgrade and bring-up		
1	• Configuration backup and snapshots • Configuration restoration with options • Configuration rollback • Fabric reload and recovery	The network administrator should be able to perform upgrade and downgrade between releases seamlessly.
3	Platform additions	Addition of Cisco Nexus platforms with the existing network topology should be possible. For example, the administrator should be able to upgrade the network from 10-Gbps to 40-Gbps FCoE by inserting a new 40-Gbps FCoE line card in the MDS switch.
4	Reloading	The entire configuration should be migrated seamlessly during the reload operation.
5	Traffic forwarding	No permitted traffic should be lost across the network topology.
Operation triggers and configuration changes		
6	Configuration changes and modifications	• Verify configuration changes on Cisco ACI fabric leaf switches and APIC. • Add and delete tenant, bridge domains, endpoint groups (EPGs), policies, and port groups. • Add and delete Fibre Channel domains, VSANs, VLANs, and attributes. • Perform configuration changes and verification through the Command-Line Interface (CLI), GUI, and representational state transfer (REST) API.
7	Upgrades	Perform upgrades (both policy-based and clean-boot upgrades of the APIC and the fabric).
Steady state and usability		
8	Soaking	Verify system stability.
Network events and link flaps		
9	Link flaps	Verify that the system is maintained and recovers to working condition after link flaps and port flaps are triggered.

Number	Focus	Use case
10	Power off and on	Verify the capability of FCoE to log in to fabric again and resume traffic after an outage.
11	Reloading	Verify the feature after the system undergoes a reload operation.
12	Traffic-based triggers	Verify various traffic flows and streams with Spirent and Ixia: • 10 Gigabit Ethernet to 10 Gigabit Ethernet • 10 Gigabit Ethernet to 40 Gigabit Ethernet • Single link to port channel • Single link to single link • With and without congestion and slow drain
Resiliency and error reccovery		
13	System switchover	–
14	In-Service Software Upgrade (ISSU)	–
15	Managed-object verification	Verify all FCoE managed objects after configuration and unconfigure them using managed-object browsers.

References

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-fabric/white_paper_c11-704054.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-739728-00 10/17