White paper
Cisco public

The bridge to possible

The Emerging Service Provider Control Hierarchy

Transforming to SDN-Enabled Networks

© 2021 Cisco and/or its affiliates. All rights reserved.

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.

This white paper examines how the control hierarchy for SDN networks is converging toward a three-tier structure, with a service orchestrator, a network controller, and multiple domain controllers. The benefits are plenty, including faster innovation, a stable ecosystem of collaborating parties, and flexibility to replace building blocks with minimal effort and without vendor lock-in.

The emerging control hierarchy for service provider SDN-enabled networks

Service providers, software vendors, and standards bodies have been recently converging on a control model for SDN-enabled automated networks. This model enables automating service creation and assurance from data centers, through the network, to customer premises equipment. It also enables network optimization across complex multilayer and multidomain networks.

It took a while to get there. At the beginning of the SDN wave, it was assumed that a single SDN controller would somehow manage the complexity of controlling all aspects of the entire network. It turned out that all this complexity cannot be handled by one controller and that SDN control requires expertise in two distinct areas: service lifecycle management and networking. As a result, the SDN "god box" has been split into two tiers: domain controllers for particular network domains and service orchestrator for creation and assurance of services across these domains. Over the last year, this hierarchy has evolved further, introducing a distinct network controller tier between the domain controllers and the orchestrator. The figure below depicts the evolved SDN architecture.

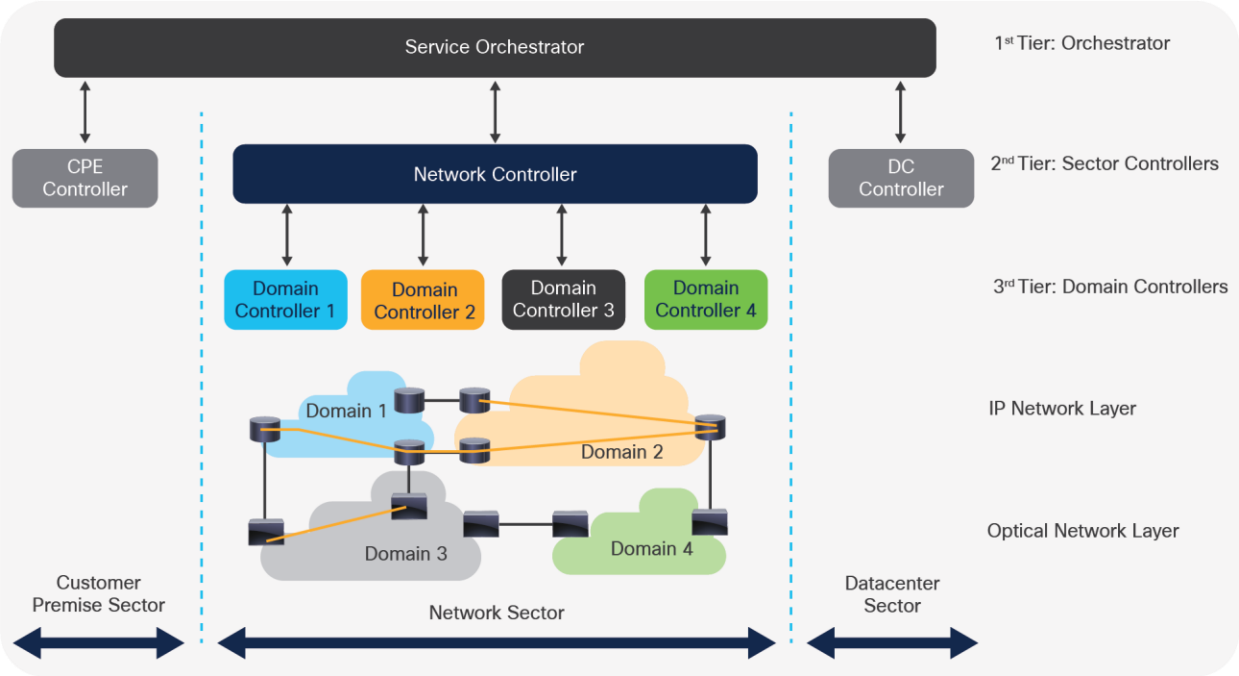

Figure 1.
Emerging control hierarchy for SP SDN-enabled networks

© 2021 Cisco and/or its affiliates. All rights reserved.

This three-tier hierarchy is likely to prevail because it serves the main purposes for which SDN was adopted in the first place.

- It allows SPs to develop differentiated capabilities, with or without their vendors, at a low cost and independently from vendor roadmaps (thus, avoiding vendor lock-in).
- It encourages and expedites innovation fueled by highly specialized vendors that focus on the different building blocks of the solution (as opposed to generalists that lack the same level of focus).
- It enables a healthy ecosystem, conducive to collaboration between software vendors.

This paper explains this three-tier architecture and why it supports the above goals in an optimal manner.

The three-tier control model for SP SDN networks

The control architecture consists of three tiers.

1. A service orchestrator
2. A sector controller per each sector (customer premise, network, and data center)
3. A domain controller per each transport or IP domain

(Note that there may be additional controllers in the customer premise sector and data center sector, but they are out of scope for this paper.)

Service orchestrator

At the top of this control hierarchy is the service orchestrator. It is responsible for setting up and assuring services end to end. It integrates with various OSS/BSS systems (not shown in the figure—outside the scope as well). It also interacts with the three sectors (customer premise, network, and data center) to establish services between customer sites and data centers through the network. Each of these sectors has its own controller, which understands and controls its sector and provides a simplified abstract view to the service orchestrator. This allows the service orchestrator to create services without having to understand specific details of the network or the other sectors.

Main orchestrator functions

- End-to-end service lifecycle management: planning, creation, maintenance, and deletion
- Onboarding, scaling, and healing of VNFs
- VNF chaining to create the desired service behavior
- Service assurance
- Resource management (storage, compute, network)
- Breaking down the service creation task into a request per each sector and ensuring it is fully executed

© 2021 Cisco and/or its affiliates. All rights reserved.

Network controller

Focusing on the network sector in the second tier of this hierarchy, the network controller must generate a complete network view from the different domains that typically comprise a network. The domain may include different layers (IP/MPLS, Ethernet, optical layers), different geographies (metro vs. aggregation vs. the core domains), and different vendors (specifically, optical domains are confined to a single vendor). It must, therefore, understand how these domains are connected (the interdomain connectivity) and the cross-domain policies that the SP put in place.

This controller is where overall network intelligence resides. It abstracts the complex structure of the network to a very simple structure that the service orchestrator expects.

Figure 2 below demonstrates the view of each domain controller, the view of the network controller, and the abstraction it provides to the service orchestrator.

Main network controller functions

- Discovery of each of the network domains from its controller
- Putting the entire network together by discovering the cross-domain links
- Providing a northbound network abstraction to the service orchestrator for the network topology and for network connectivity service management
- Providing a single pane of glass for network engineers and operations
- Maintaining network policies
- Automated optimization across different domains and layers
- End-to-end network resilience

Domain controllers

At the lower end of this hierarchy are the domain controllers. They interact directly with the network equipment, learn its topology and services, and capture and exploit the unique capabilities of each domain. This data must be sufficiently abstracted on their northbound interface so that the network controller does not have to worry about very specific technology details. For example, a domain controller might specialize in segment routing or MPLS traffic engineering, allowing it to optimize resources in its domain based on the capabilities of these technologies. It might specialize in flex spectrum optical networks and support ultra-high-speed optical connections via “super channels.” As one can see, these controllers must be very close to the hardware and software of the network gear in the domain.

Main domain controller functions

- Discovery of resources, failures, or any other state changes in the domain
- Reflection of the network, its services, and any state changes to the network controller in a real-time manner
- Creation of services in the domain upon request from the network controller
- Management of resources in the domain
- Optimal routing of services in the domain
- Ensuring that the services requested in the domain can be supported under all conditions
- Optimization within the domain
- Local resilience inside the domain

© 2021 Cisco and/or its affiliates. All rights reserved.

In the “Alignment of the Three-Tier Control Hierarchy with Standards” section, we show the alignment of this model to various standards, but first, let’s focus on the rationale behind this hierarchy.

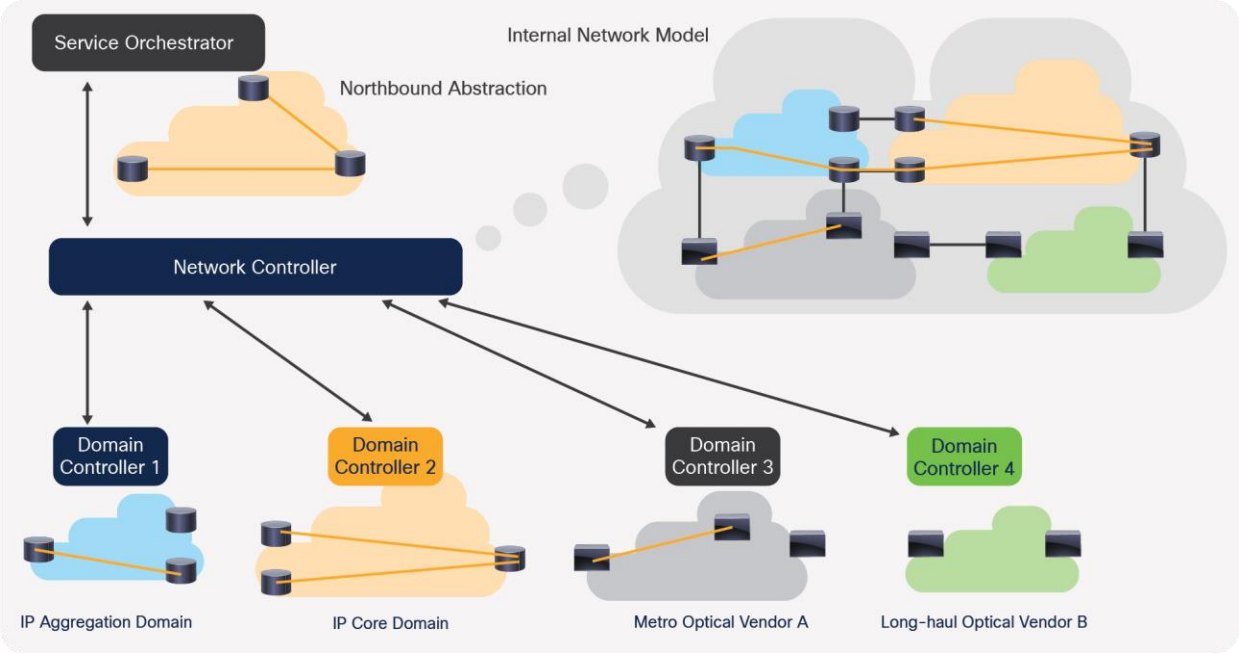

Figure 2.
Network controller abstracts network-wide view from domain controllers

Supporting SP goals and aspirations for SDN

Let’s examine how the main goals of SDN are addressed with this architecture.

Enable SPs to develop unique capabilities

Service providers want to differentiate themselves based on business logic they build or buy without becoming hostage to their vendors. Such vendor lock-in can be avoided if the software implementing a particular building block can be replaced without requiring a huge integration effort with the new vendor’s software. Counter-examples include large OSS systems that cannot be replaced due to the complexity of the effort, despite their slow adjustment to customer needs and very high price for each small change. Less painful replacement can be achieved with the proposed architecture.

A closely related consideration has to do with simple upgrades of the functionality of the system using the existing vendors. Such upgrades should happen at least once or twice a year to ensure innovation happens at a reasonable pace. To enable the required integration and testing efforts prior to the upgrade, the minimum number of interfaces should be changed.

The scenarios below outline the level of effort needed with the proposed architecture and its alternatives.

- The service orchestrator has a single interface toward the network that is independent of the network vendors. Therefore, its upgrade or replacement may imply an integration effort to the OSS and BSS, but not to the network. See the following figure.

© 2021 Cisco and/or its affiliates. All rights reserved.

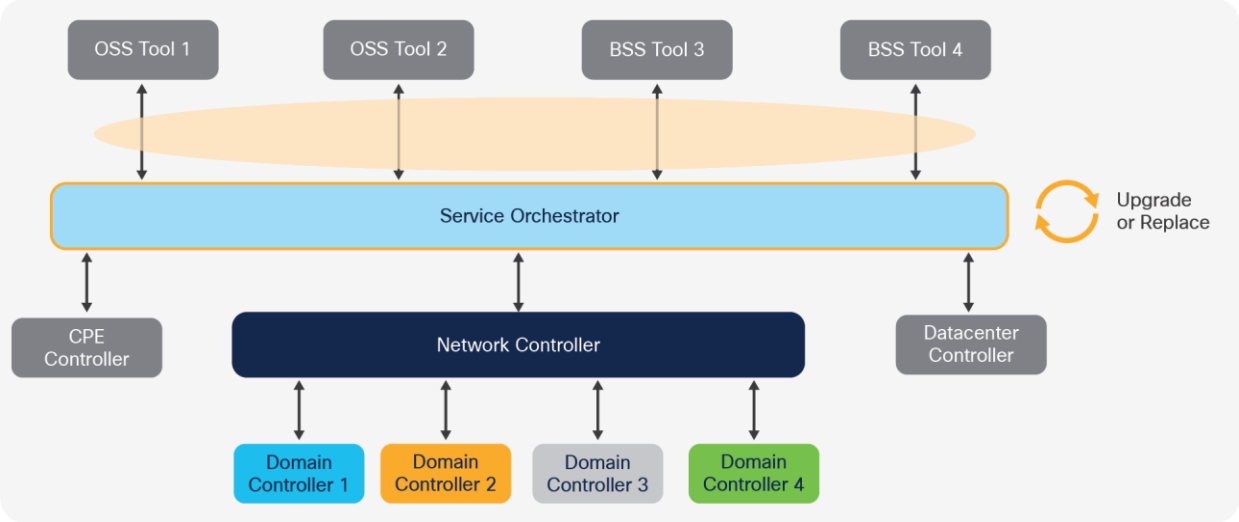

Figure 3.
Integration effort needed to upgrade/replace the service orchestrator

- In a similar fashion, the network controller has a single interface up toward the OSS/BSS world that is independent of the specific OSS/BSS vendors. Thus, its upgrade or replacement implies an integration and testing effort southbound to the domain controllers, but not northbound to the OSS/BSS and the VNF ecosystem.

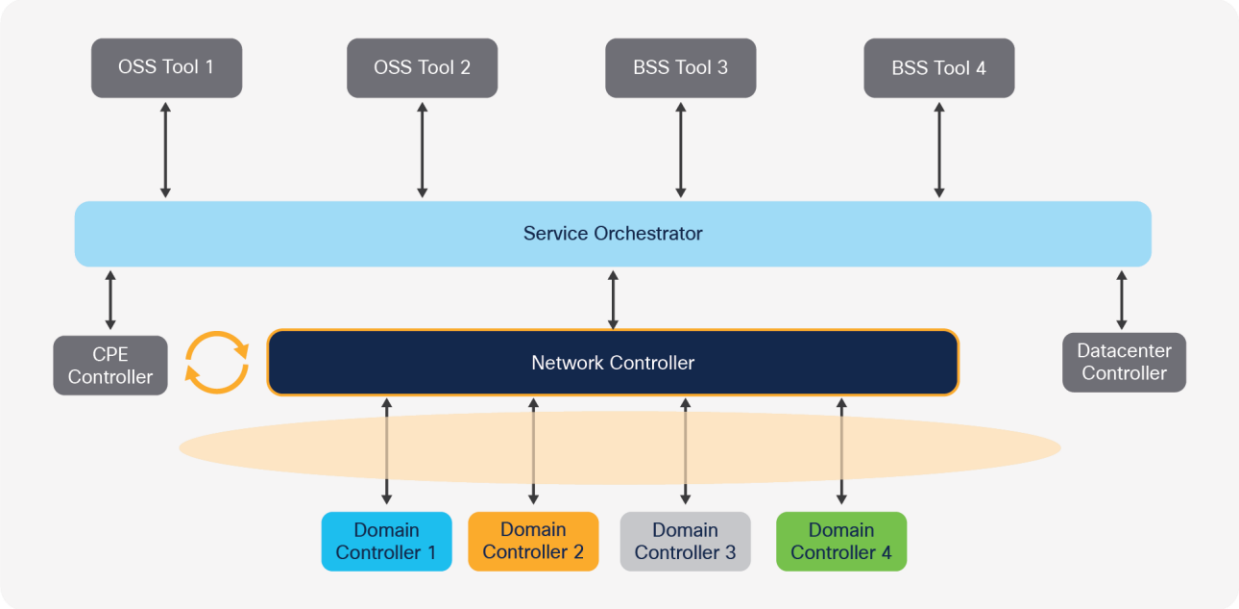

Figure 4.
Integration effort needed to upgrade/replace the network controller

- Domain controller can be upgraded or replaced without impact on the service orchestrator and OSS/BSS tools. These tools are shielded from this change through a vendor-agnostic network controller. In fact, the network equipment of the vendor can also be replaced with minimal impact on the higher layers, allowing commoditization of the equipment.

© 2021 Cisco and/or its affiliates. All rights reserved.

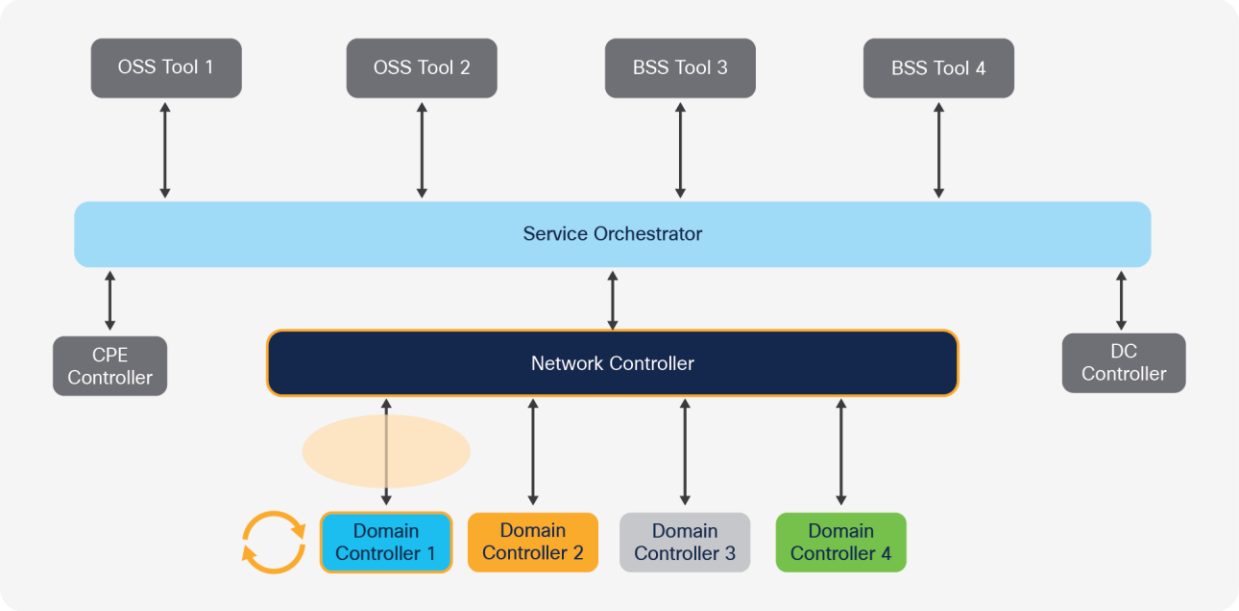

Figure 5.
Integration effort needed to upgrade/replace a domain controller

- The network equipment itself can be upgraded without any changes to the domain controller. In fact, most of the testing performed when upgrading the equipment should be done by the vendor (assuming the same vendor also provides the domain controller). This greatly reduces the amount of testing needed from an overall network control perspective.

On the other hand, if the orchestrator and network controller are a single monolithic system, an upgrade or replacement would entail a significant integration effort both toward the OSS/BSS and toward the network, as shown in the following figure. The pace of innovation slows down.

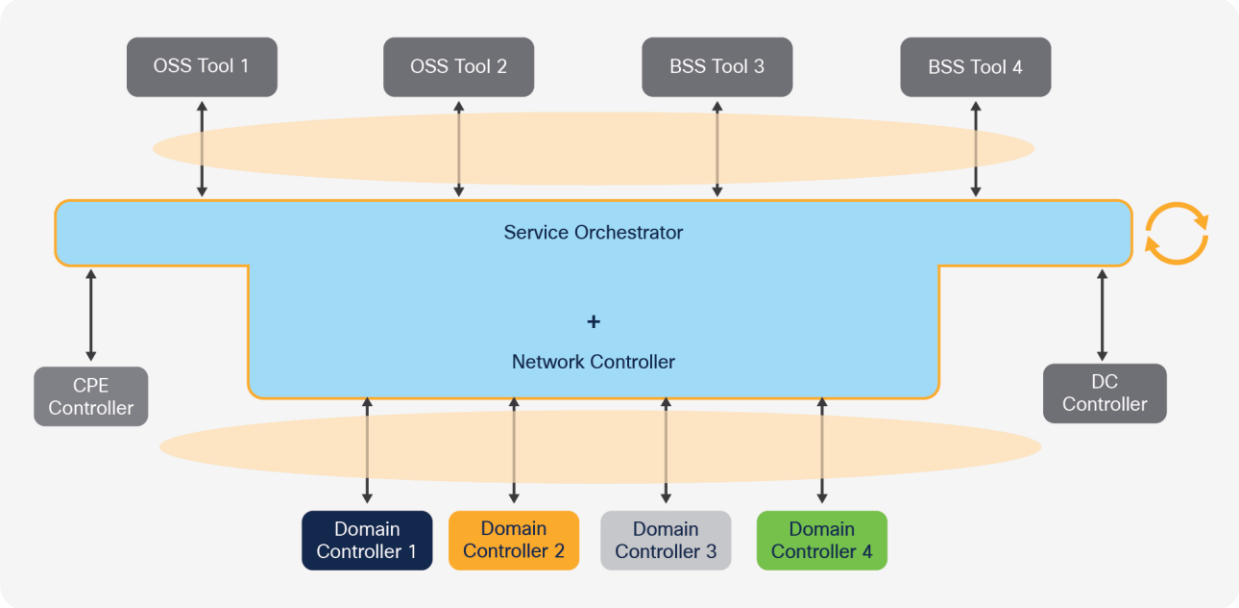

Figure 6.
Integration to replace combined service orchestrator and network controller

© 2021 Cisco and/or its affiliates. All rights reserved.

Encourage and expedite innovations

Innovation requires subject-matter expertise and focus. The three-tier hierarchy encapsulates different areas of expertise in each building block.

The service orchestrator is built on a deep understanding of OSS/BSS tools, service catalogs, and service assurance, as well as a developed ecosystem of Virtual Network Functions (VNFs). On the other hand, it does not require understanding of networking; it merely needs to inform the network of the required connectivity service needed for the implementation of the service.

The network controller requires understanding of complex multidomain and multivendor networks. In particular it requires understanding of how to discover cross-domain links and how to stitch services across different domains. The most intricate part of the know-how needed for this building block is the understanding of how to optimally use the different capabilities of packet networks on the one hand and optical networks on the other hand. This knowledge is extremely rare in the industry. Its focus should not be integration with complex OSS/BSS tools.

Each domain controller reflects a specific networking technology expertise. For example, it reflects complex transmission feasibility considerations for the optical layer or hardware-specific limitations of a router or a switch. Thus, intimate knowledge of the hardware and control plane of the domain is needed to truly optimize the performance of the equipment in the domain.

Enable a healthy ecosystem

A healthy ecosystem is essential for a modular architecture to function over a long period of time. Forcing vendors with conflicting interests to work together is bound to fail over time since at some point the leverage the service provider has over the vendor diminishes. It must, therefore, be based on the following principles.

Network equipment vendors must not compete with the network controller vendor on their main business (which is the network gear). This is because the network controller vendor has complete visibility into all the equipment in the network and knowledge of the pain points in each domain (or lack thereof) and, therefore, strategic knowledge of how to work around their competition. This is clearly unsustainable and bound to cause conflicts of interests.

One of the main functions of the network controller is to optimize the use of resources in the network. If the network controller vendor sells equipment to the service provider, it has clear conflict of interests since building a good network controller would reduce its equipment sales. Since most of the business is in equipment sales, it's clear how the vendor will behave.

Finally, the architecture must motivate vendors of each of the building blocks to provide value and potentially grow their business beyond the controller. Otherwise, their software will be commoditized, and it will not make sense for them to invest in its improvement. Thus, the service orchestrator vendor will be motivated to innovate in order to sell other BSS/OSS tools in their portfolio, and, if the domain controller vendor is also the vendor of the equipment, it will be motivated to innovate to increase the value of their equipment. Given the size of the equipment deals compared to the cost of controllers, it's conceivable that they will provide the domain controller for free to win the equipment deal and still be motivated to improve it.

Related to the ecosystem is another important consideration of ownership and expertise in the SP. Each system must be owned and operated by one of the SP groups, and this group must also have the expertise to operate the system. The service orchestrator naturally fits into the group in charge of service lifecycle management, which is typically the IT team in the SP, while the network controller and domain controllers have a natural home in the network department (planning/engineering/operations).

© 2021 Cisco and/or its affiliates. All rights reserved.

Summary

The control hierarchy for SDN networks seems to be converging toward a three-tier structure. This is already reflected in the standards. Naming conventions vary, but the hierarchy outlined above is used as a reference in documents of IETF, ONF, and MEF as shown in Figure 7 below.

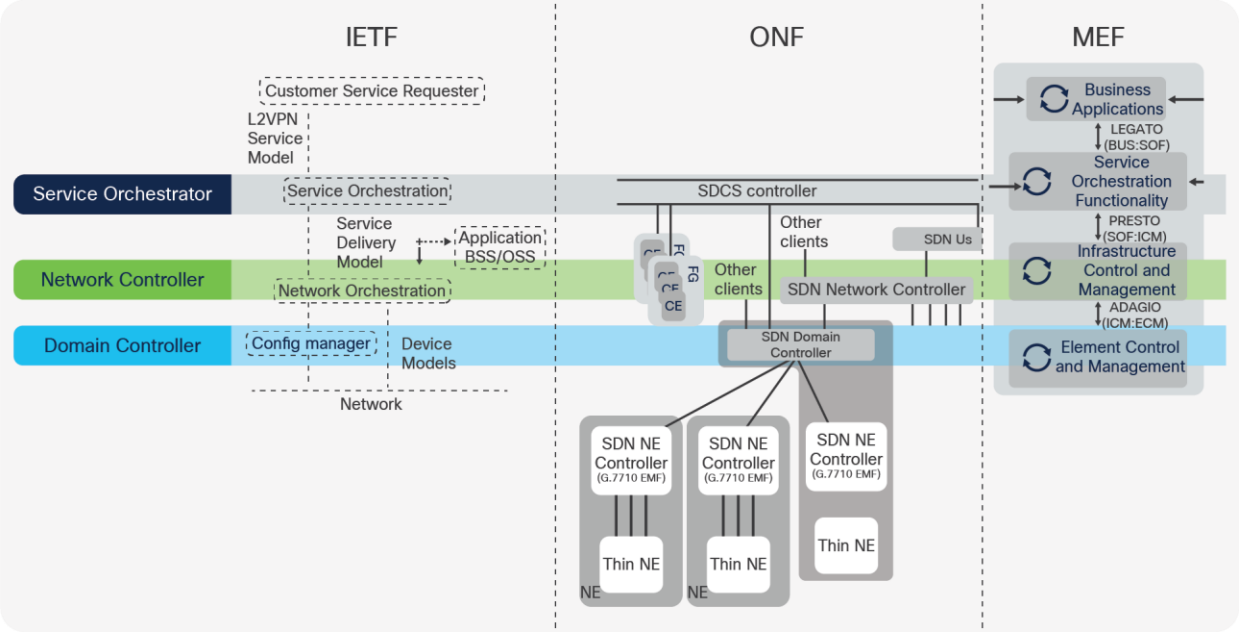

Figure 7.
Alignment of three-tier control hierarchy with standards

This paper has shown why the three-tier architecture is adopted so broadly. This structure provides a careful balance between the desire for faster innovation, a stable ecosystem of collaborating parties, and flexibility to replace building blocks with a contained amount of effort in order to avoid vendor lock-in.

© 2021 Cisco and/or its affiliates. All rights reserved.

Accelerate your journey to next-generation networking

If your network needs to deliver high-bandwidth services with uncompromising diversity and latency SLAs and dramatically lower costs, you'll be interested in the Cisco® Converged SDN Transport and Routed Optical Networking solution with Cisco Crosswork® Hierarchical Controller.

For more information on Cisco's network automation portfolio for service providers, please visit www.cisco.com/go/crosswork. To learn more about Crosswork Hierarchical Controller or to schedule a demonstration, contact your Cisco sales representative.

For more information on how Converged SDN Transport is changing the economics of the network for service providers to deliver connected experiences at massive scale, please visit www.cisco.com/c/en/us/solutions/service-provider/converged-sdn-transport.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**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C11-2699951-00 11/21

© 2021 Cisco and/or its affiliates. All rights reserved.