Transforming Campus Networks to Intent-Based Networking

Enabling Your Network for the Future

ciscopress.com

Pieter-Jan Nefkens

Transforming Campus Networks to Intent-Based Networking

Pieter-Jan Nefkens

Cisco Press

221 River Street

Hoboken, NJ 07030 USA

In this design PC1 and PC2 still have the same IP address but are now assigned into VLAN 201 instead of virtual network green. VLAN 201 is configured on the DSW1 with IP network 10.0.0.0/24 and a default gateway of 10.0.0.1 for the endpoints. The SGTs have remained the same: Employee for PC1 and Guest for PC2.

Just as in the previous example, if PC1 would communicate with www.myserver.com on 209.165.200.225, it would send its TCP SYN packet to the default gateway on DSW1, which in turn would forward it to the Internet, while return traffic would be sent via Ethernet to PC1. ARP is used to map IP addresses into MAC addresses.

The principle of SGT ACLs to restrict traffic within a VRF is the same. In both SDA as well as classic, the SGT ACL is pushed from the policy server to the access switch where the endpoint is connected.

Although the end goal is logically separating traffic between endpoints, using SGT for microsegmentation, there are some limitations and restrictions on a classic VLAN over an SDA topology.

- **Spanning Tree:** It is not preferred to run Spanning Tree on the network, as each change in a VLAN can trigger a Spanning Tree recalculation, resulting in blocked traffic for a period of time. If it is required to run Spanning Tree, then run a single instance of Spanning Tree in MST mode, so that adding a VLAN does not trigger a new STP topology as with per-VLAN Spanning Tree.

- **Management VLAN and VRF:** It is required to have a dedicated VLAN and management VRF to be able to create or remove new VLANs. This VLAN may never be removed from trunks and networks, as this is essentially the underlay network. The automation tool that generates and provides the configuration communicates with all devices in this management VLAN.

- **Configuration via automation tool only:** The configuration of the campus network can *only* be executed via the automation tool. This is generally true for any environment that there should only be a single truth for the provisioning of a network. In an IBN based on classic VLANs, this is more important as the automation tool will generate the VLAN identifiers automatically based on the virtual networks to be deployed. Although it is common in enterprises to statically define and assign VLANs, in this design that concept needs to be removed for automation to work.

- **Standardized building blocks only:** It is important to only allow standardized building blocks, defined via the automation tool, on the campus network, where the policy is assigned policy-centric using IEEE 802.1x and RADIUS. The building block can then be standardized in such a way that small pieces of configuration code can be generated on-the-fly to create or remove the required compartments on the network. This is realized by creating small repetitive code blocks of command line configuration to be executed, for example, for the creation of a new compartment on the access switch:

```
vlan $vlanid
name $vrfname
interface $PortChannelUplink
switchport trunk allowed vlan add $vlanid
```

If the campus network configuration cannot be standardized, it will not be possible to enable an Intent-Based Network using VLANs.

- **Build your own automation:** With SDA, a lot of automation and configuration is executed by Cisco DNA Center in the background. With this design, an automation tool needs to be installed and configured by the network team to provide similar functionality. This can require some custom coding and testing before running the solution in production. This could be Cisco DNA Center with templates or another tool that provides automation functionality.

In summary, both mechanisms (SDA and classic VLAN) work quite similarly, and when you take certain precautions and keep the limitations in mind, it is feasible to start with IBN based on a classic collapsed-core topology. Part 2, "Transforming to an Intent-Based Network," provides more details on limitations, drawbacks, and when which technology fits best for transforming a campus network to IBN.

Summary

Cisco Digital Network Architecture describes the requirements and operations of a network infrastructure of an enterprise at a functional or abstract level. Cisco DNA achieves this abstract description by dividing the requirements of the enterprise network into several functions and design principles. It does not describe how to use or implement that network architecture.

Intent-Based Networking (IBN) describes, using a powerful methodology, how a campus network can be built and operated using Cisco DNA as network architecture. IBN is based on the premise that every endpoint that connects to the network consumes a predefined set of services (that include access, connectivity, security policies, and other network functions). In essence, every endpoint has a specific intent (or purpose) when connecting to the network, and each intent is defined as a set of services to be delivered to that endpoint.

This set of intents (that are deployed on the network) are defined dynamically based on which endpoints are connected to the network. As soon as an intent is not required anymore, its configuration is removed automatically from the network infrastructure.

Although IBN itself is not based on Cisco Digital Network Architecture, its description and methodology are so similar to Cisco DNA that you can state it is a perspective of Cisco DNA. IBN describes how a network based on Cisco DNA can be configured and operated by the network operations team. Figure 5-5 describes the systematic approach IBN describes in providing intents to the network (by defining Intents as repetitive pieces of configuration).

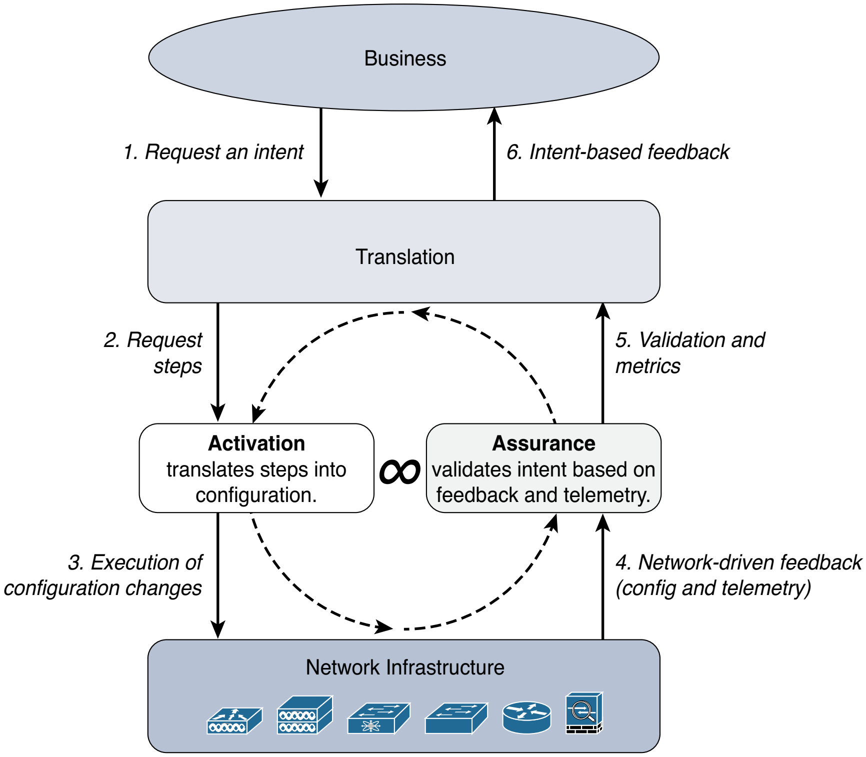
Business
1. Request an intent
6. Intent-based feedback
Translation
2. Request steps
5. Validation and metrics
Activation
translates steps into configuration.
∞
Assurance
validates intent based on feedback and telemetry.
3. Execution of configuration changes
4. Network-driven feedback (config and telemetry)
Network Infrastructure

Figure 5-5 *IBN Systematic Approach to the Network*

Figure 5-5 is similar to Cisco DNA, and IBN is based on six steps in a continuous loop:

1. Request intent; business or network operations request a specific intent.
2. Request steps; the intent is translated into a set of configuration changes to be executed.
3. Execution of configuration changes; network configuration changes are executed via automation.
4. Network-driven feedback; the network infrastructure provides feedback on its operation.
5. Validation & metrics; the analytics component validates the received network-driven feedback with the requested intents to validate that the requested intents are operating as requested and designed.
6. Intent-Based feedback; business-outcome based values are used to report on the status of the requested intent and its operation.

Two Designs

Two network designs are available to implement IBN:

- Cisco Software Defined Access (SDA) is based on Cisco DNA and is the most complete technology that can enable IBN on the campus network, but Cisco SDA does have specific requirements on the network infrastructure devices (and Cisco DNA Center).
- Classic VLANs with VRF-Lite can be used, with limitations, as an alternative to SDA for those organizations that are not (yet) able to meet the requirements of SDA.

IBN itself, and therefore both designs, relies on three key requirements on the campus network to be successful:

- **Policy-centric network:** The campus network is not configured port-by-port but uses a policy-centric identity server so that based on the identity of the endpoint the specific network policies (and thus the intents) can be pushed to the appropriate network infrastructure device.
- **Microsegmentation:** Microsegmentation is used within IBN to allow for more granular security policies than those based solely on IP addresses.
- **Feedback from network:** IBN relies heavily on the feedback that network infrastructure devices provide back to the analytics component; it is used to validate whether the requested intents are operating as designed and requested.

In conclusion, IBN is a perspective on Cisco Digital Network Architecture, and it describes a powerful methodology of how a Cisco DNA-based network infrastructure can be operated and managed. IBN can be used to provide the network operations team with the tools and methods to cope with the exponential growth of devices connecting to the campus network.

This page intentionally left blank

Chapter 6

Tools for Intent

Enterprise frameworks, Cisco DNA, Intent-Based Networking—they all provide descriptions and context on how network infrastructures are designed and operated and how they should work and interoperate with applications, users, and other "external" sources. It is all abstract and concept-based.

Without the proper tools and technologies, these concepts cannot be implemented and brought into practice. One of the key responsibilities for a network architect or network engineer is to know which tool or technology can meet the specific requirements set by the business.

A significant number of tools and technologies exist that can be used. It is impossible to provide a full compendium of all tools and include an in-depth explanation of them. This chapter provides you with an overview of some of the tools available for campus networks that can be used to enable Intent. Chances are that you are using some of these tools already, and this will help in enabling Intent-Based on your network infrastructure.

This chapter covers the following topics:

- Description of what automation entails in networking
- Overview of automation tools for Intent
- Network visibility in Intent
- Overview of network visibility tools for Intent

What Is Network Automation?

Network automation is one of the key concepts used to enable an Intent-Based Network. There is no Intent-Based Network without a process for network automation. The word *automation* is defined in the Oxford dictionary as "the use or introduction of automatic equipment in manufacturing or other process or facility." This definition is clearly related to automation processes in industrial environments like factories. The definition can be