



Cisco Digital Network Architecture

Intent-based Networking for the Enterprise

Tim Szigeti
David Zacks
Matthias Falkner
Simone Arena

ciscopress.com

Foreword by **Scott Harrell**

Cisco Digital Network Architecture

Intent-based Networking in the Enterprise

Tim Szigeti, CCIE No. 9794

David Zacks

Matthias Falkner

Simone Arena

Cisco Press

Cisco Digital Network Architecture: Intent-based Networking for the Enterprise

Table of Contents

Cover

Title Page

Copyright Page

Feedback Information

About the Authors

About the Technical Reviewers

Dedications

Acknowledgments

Contents

Foreword

Introduction

Part I: Introduction to DNA

Chapter 1 Why Transform Your Business Digitally?

Opportunities and Threats

Digitally Transforming Industries

Digital Advertising

Digital Media and Entertainment

Digital Finance

Digital Communications

Digital Transportation Services

Digitally Transforming Businesses

Table of Contents

Transforming the Customer Experience

Burberry

Starbucks

UPS

Transforming the Employee Experience

Air France

RehabCare

Cisco

Transforming Business Operations

Boeing

Codelco

BC Hydro

Driving Digital Transformation with the Internet of Things

Are You Ready?

Summary

Further Reading

Chapter 2 The Business Value of DNA

Business Requirements of the Network Architecture

Cost Reduction

Risk Mitigation

Actionable Insights

Business Agility

Intent-Based Networking

Business Value of Cisco Digital Network Architecture

Reducing Costs Through Automation, Virtualization, and Programmable Hardware

Mitigating Risks with Integrated Security and Compliance

Revealing Actionable Insights Through Analytics

Accelerating Business Agility Through Open APIs

Adding It All Up

Summary

Further Reading

Chapter 3 Designing for Humans

Table of Contents

Technology Versus User-Experience

Design Thinking Philosophy and Principles

Cisco Design Thinking Framework

- Discover Phase

- Opportunity Statement

- Define Phase

- Problem to Be Solved Statement

- Explore Phase

The Cisco Design Thinking Journey for DNA

- DNA Discovery Phase

- The Front-Line Engineer

- The Firefighter

- The Expert

- The Planner

- DNA Definition Phase

- DNA Exploration Phase

Summary

Further Reading

Chapter 4 Introducing the Digital Network Architecture

Requirements for DNA

- Requirements to Reduce Complexity and Costs

- Requirement to Increase Operational Flexibility

- Flexibility

- Intelligent Feedback Mechanism

- Application, User, and Device Awareness

- Security and Compliance Requirements

- Cloud-Enablement Requirement

Architectural Principles

- Openness

- Extensibility

- Programmability

- Policy-based Networking

Table of Contents

Security

Software Driven

Cloud Integrated

Conflicting Principles?

Overview of the DNA Components

Infrastructure

DNA Infrastructure Domains

Extending the Concept of Network Fabrics in DNA

Virtualization

Policy

Automation

Controllers

Orchestrators

Analytics Platform

Data Collection

Data Reporting

DNA Analysis

Feedback and Control

The Role of the Cloud in DNA

Cloud for Applications

Cloud for Automation and Management

Cloud for Analytics

Connecting the Building Blocks: APIs

Outcomes

Summary

Further Reading

Chapter 5 The Digital Network Architecture Blueprint

DNA Services

DNA ServicesTransport

DNA ServicesPolicy

Relationship Between DNA Policies and Business Intent

DNA Infrastructure

Table of Contents

Transport Functions

Supporting Network Functions

Fabrics

Automating DNA Controllers

Automating Transport and Network Functions Infrastructure

Maintaining a View of the Infrastructure Functions and Connected Endpoints

Instantiating and Maintaining DNA Services

Relationships in DNA: Revisiting Domains, Scopes, and Fabrics

DNA Interfaces

Service Definition and Orchestration

Relationship Between the Controllers and the Service Definition and Orchestration
Component

Analytics Platform

Data Collection

Data Extraction

Data Ingestion

Data Export

On-Premises and Off-Premises Agnosticism Revisiting the Cloud

Application Hosting in the Cloud and the Evolution of the DMZ

Leveraging the Cloud for DNA Controllers and Analytics

Summary

Part II: DNA Programmable Infrastructure

Chapter 6 Introduction to DNA Infrastructure

Picturing the Modern Network

Exploring DNA Infrastructure

The Evolving Network, and Why It Matters

Requirements: The Need for Change

Requirements: The Need for Speed (of Change)

Requirements: The Need for Simplicity

Requirements: The Need for Continuity

DNA Infrastructure Solutions

Flexible Hardware

Table of Contents

Flexible Software

New and Evolving Protocols

The Emergence of Virtualization

Bringing It All Together

Summary

Chapter 7 Hardware Innovations

The Importance of Hardware in a Software-Defined World

The Making of a Chip

Delving Deeper: How Chips Are Designed and Built

Drivers of Chip Design and Density

When Good Chips Go Bad: What Can Go Wrong in Chip Design

When Good Chips Need to Get Better: Designing the Next Generation

Now We Speak the Same Language!

Whats Happening in the World of Networks

How Traditional Network ASICs Process Packets

Traffic Handling with CPUs and FPGAs

Introducing Flexible Silicon

Flexible Switching Silicon: UADP

UADP Use CasesCurrent, and Future

Introducing the Future: UADP 2.0 and 3.0

So Whats Common Across All of These Variants of UADP?

UADPSumming Up

Flexible Routing Silicon: QFP

QFPAn Introduction

QFPDiving Deeper

QFPUse in Platforms

UADP and QFPSumming Up

Wireless: Providing Innovation for Mobility

Flexible Radio Assignment

Intelligent Capture

Summary

Table of Contents

Further Reading

Chapter 8 Software Innovations

The Importance and Evolution of Networking Software

Cisco IOS: Origins and Evolution

Evolution of the Cisco IOS Data Plane

Evolution of the Cisco IOS Control Plane

Evolution of the Cisco IOS Management Plane

Evolution of Cisco Networking Software

The Evolution of Cisco IOS to IOS XE

Cisco IOS XE in a Nutshell

Cisco IOS XE: Delving Deeper

IOS XE Subsystems

IOS XE Database

Container Framework and Application Hosting

Cisco IOS XE: Bringing It All Together

Cisco IOS XE: Simplification with a Single Release Train

Cisco IOS XE: Software Maintenance Upgrades

The Issue with Software Upgrades

Types of SMUs Cold, and Hot

Installing a SMU

Benefits of SMUs

Cisco IOS XE: Platform Support

Cisco IOS XE: Summary

Protecting Platforms and Networks: Trustworthy Systems

Trustworthy Systems: An Overview

Possible Attacks: IOS Modifications

Attack Mitigation with Trustworthy Systems

Defense: Image Validation and Signing

Defense: Runtime Defenses

Defense: Secure Boot

Understanding Boot Sequence Attacks

Protecting Device Integrity from the Ground Up with Secure Boot

Table of Contents

Ensuring Device Identity with the Secure Unique Device Identifier

Cisco Secure Boot and Trust Anchor Module: Validating the Integrity of Software, Followed by Hardware

The Move to Intuitive Networking

Summary

Further Reading

Chapter 9 Protocol Innovations

Networking Protocols: Starting at the Bottom with Ethernet

Power Protocols: Power over Ethernet, to 60 Watts and Beyond!

The Future of Power over Ethernet

Multiple-Speed Protocols over Copper: Multigigabit Ethernet, Squeezing More Life Out of Existing Cabling Infrastructures

25G Ethernet The New Kid on the Block

Ethernet Evolving: This Is Not Your Fathers Ethernet!

Moving Up the Stack

Networking Protocols: Moving Up the Stack to Layer 2

Networking Protocols: Moving Up the Stack to Layer 3

First-Hop Reachability Protocols: HSRP and VRRP

Routing Protocols

Virtual Routing

Layer 2 over Layer 3

Networking Protocols Today: Summary

Networking Protocols for the New Era of Networking

VXLAN: A Next-Generation Encapsulation Technology

UDP Encapsulation

Virtual Network Support

Scalable Group Tag Support

Summary: Why VXLAN?

IS-IS: The Evolution of Underlay Routing

LISP: The Evolution of Overlay Host Reachability

The Need for Host Mobility

The Need for Host Scale

LISP to Address the Host Mobility and Scale Needs of the Next-Generation Network

Table of Contents

Examination of LISP Roaming Operation

Summing Up: LISP As a Next-Generation Overlay Control Plane

Scalable Group Tags: The Evolution of Grouping and Policy

Scalable Group Tags for Group-Based Policies

SGT Transport End-to-End Across the Network

Bringing It All Together: What Next-Generation Protocols Within the Network Allow Us To Build

Summary

Further Reading

Chapter 10 DNA InfrastructureVirtualization

Benefits of Network Function Virtualization

CAPEX Benefits of NFV

OPEX Benefits of NFV

Architectural Benefits of NFV

Use Cases for Network Function Virtualization

Control Plane Virtualization

Branch Virtualization

Virtualization to Connect Applications in VPCs

Virtualization of Multicloud Exchanges

Overview of an NFV System Architecture

Hypervisor Scheduling and NUMA

Input/Output Technologies for Virtualization

Challenges and Deployment Considerations of Network Function Virtualization

Performance

Oversubscribing the Physical Hardware Resources

Optimizing Server Configurations

Selecting the Right I/O Technique

VNF Footprint Considerations

Multi-tenancy and Multi-function VNFs

Transport Virtualization

Network Segmentation Architecture

Network Access Control

Table of Contents

- Network Path Virtualization
- Network Services Edge
- Policy-based Path Segmentation
- Control Planebased Segmentation
- Multihop Path Isolation Techniques
- Single-Hop Path Isolation Techniques

Summary

Chapter 11 DNA Cloud

Introduction to the Cloud

- Cloud Service Models
- Cloud Deployment Models
- Its a Multicloud World!

DNA for the Cloud

- DNA Cloud for Applications
- DNA Cloud for Automation
- DNA Cloud for Analytics

Summary

Further Reading

Part III: DNA Automation

Chapter 12 Introduction to DNA Automation

Why Automate?

- Reduce Total Cost of Ownership
- Lower Risk
- Move Faster
- Scale Your Infrastructure, Not Your IT Department
- Think Out of the Box
- Simplify Like Never Before
- Enable Applications to Directly Interact with the Network

Is DNA Automation the Same as SDN?

- Centralized Versus Distributed Systems
- Imperative Versus Declarative Control
- The Cisco SDN Strategy

Table of Contents

Automation Elements

- Network Programmability

- Network Controller

- Network Orchestrator

Summary

Further Reading

Chapter 13 Device Programmability

Current State of Affairs

- CLI Automation

- SNMP

Model-Based Data

- YANG

Protocols

- Encoding

- Network Protocols

- NETCONF

- RESTCONF

- gRPC

Telemetry

- gRPC Telemetry

Tools

Application Hosting

Summary

Further Reading

Chapter 14 DNA Automation

The Increasing Importance of Automation

- Allow the Network to Scale

- Reduce Errors in the Network

- Time to Perform an Operation

- Security and Compliance

Current Impediments to Automation

Table of Contents

Classifying Network Automation Tasks

Infrastructure and DNA Service Automation

Standard and Nonstandard Automation Tasks

The Role of Controllers in DNA Automation

Leveraging Abstractions in DNA to Deliver Intent-Based Networking

Domain Controllers Versus Control Plane Protocols

Automating Your Network with Cisco DNA Center

DNA Center Basics

Device Discovery, Inventory, and Topology

Day 0 OperationsStandardizing on Network Designs

Standardizing Settings for Supporting Network Functions

Automating Device Credentials

Reserving and Managing IP Address Pools

Standardizing Service Provider QoS Profiles

Characterizing Wireless LAN Profiles

Standardizing on Network Designs

Automating the Deployment of Network Elements and Functions

Day N OperationsAutomating Lifecycle Operations

Summary

Further Reading

Part IV: DNA Analytics

Chapter 15 Introduction to DNA Analytics

A Definition of Analytics

DNA Analytics

DNA Analytics, Opportunities and Challenges

Brief History of Network Analytics

Why DNA Analytics?

The Role of Network Analytics in DNA

Summary

Chapter 16 DNA Analytics Components

Analytics Data Sources

Table of Contents

DNA Instrumentation

Distributed Network Analytics

Telemetry

Why Telemetry?

The DNA Telemetry Architecture

Limitations of Today's Telemetry Protocols

The Evolution of DNA Telemetry: Model-Driven Telemetry

Analytics Engine

The Traditional Analytics Approach

The Need for Analytics Engines

Data Scalability

Analytics Efficiency

Application Development Simplification

The Role of the Cloud for Analytics

Summary

Further Reading

Chapter 17 DNA Analytics Engines

Why a DNA Analytics Engine?

DNA Analytics Engines

Cisco Network Data Platform

Telemetry Quotient

NDP Architecture

NDP Architecture Principles

NDP Architecture Layers

NDP Architecture Components

NDP Deployments Modes

On-Premises Deployments

Cloud Deployments

NDP Security and High Availability

Cisco Tetration Analytics

It's All About Quality of Data

Data Center Visibility with Cisco Tetration Analytics

Table of Contents

- Cisco Tetration Analytics Architecture
 - Data Collection Layer
 - Analytics Layer
 - Enforcement Layer
 - Visualization Layer
- The Benefits of Cisco Tetration Analytics

Summary

Further Reading

Part V: DNA Solutions

Chapter 18 DNA Virtualization Solutions: Enterprise Network Functions

Virtualization and Secure Agile Exchange

The Cisco Strategy for Virtualization in the Enterprise

Cisco Enterprise Network Functions Virtualization

- Details on Virtualization Hardware
- NFVIS: An Operating System Optimized for Enterprise Virtualization
- Virtualized Network Functions
 - Cisco Integrated Services Virtual Router
 - Cisco Adaptive Security Virtual Appliance
 - Cisco Firepower NGFW Virtual
 - Cisco Virtual Wide Area Application Services
 - Cisco Prime Virtual Network Analysis Module
 - Cisco Virtual Wireless LAN Controller
- Third-party VNF Support
- Service Chaining and Sample Packet Flows
- Transparent Versus Routed Service Chains
- Orchestration and Management
- NFVIS GUI (Per System)
- Cisco DNA Center (Network Level)
- Configuring and Monitoring of an NFVIS Host Using Traditional Mechanisms

Virtualizing Connectivity to Untrusted Domains: Secure Agile Exchange

- Motivation for the Cisco SAE Solution
- Cisco SAE Building Blocks

Table of Contents

Running Virtualized Applications and VNFs Inside IOS XE

Summary

Further Reading

Chapter 19 DNA Software-Defined Access

The Challenges of Enterprise Networks Today

Software-Defined Access: A High-Level Overview

SD-Access: A Fabric for the Enterprise

What Is a Fabric?

Why Use a Fabric?

Capabilities Offered by SD-Access

Virtual Networks

Scalable Groups

Stretched Subnets

SD-Access High-Level Architecture and Attributes

SD-Access Building Blocks

DNA Center in SD-Access

SD-Access Fabric Capabilities

IP Host Pools

Virtual Networks

Scalable Groups

SD-Access Device Roles

SD-Access Control Plane Nodes, a Closer Look

SD-Access Fabric Border Nodes, a Closer Look

SD-Access Fabric Edge Nodes

SD-Access Extended Nodes

SD-Access Wireless Integration

SD-Access Case Study

SD-Access Case Study, Summing Up

Summary

Further Reading

Chapter 20 DNA Application Policy

Table of Contents

Managing Applications in DNA Center

- Application Registry

- Application Sets

- Application Policy

- Required Steps

- Optional Steps

- Queuing Profile

- Marking Profile

- Service Provider Profile

What Happens Under the Hood?

Translating Business Intent into Application Policy

DNA Infrastructure Software Requirements for Application Policy

- NBAR2

- NBAR2 Operation

- QoS Attributes

- Holy Grail Classification and Marking Policy

- SD-AVC

DNA Infrastructure Platform-Specific Requirements for Application Policy

- Routing Platform Requirements

- Application Classification and Marking Policies

- Queuing and Dropping Policies

- Sub-Line Rate Hierarchical QoS Policies

- Enterprise-to-Service Provider Mapping

- Hardware Queuing

- Internal System QoS

- Switching Platform Requirements

- Application Classification and Marking Policies

- Hardware Queuing Policies

- Internal System QoS

- Wireless Platform Requirements

- Application Classification and Marking Policies

- DSCP-to-UP Mapping

- Hardware QoS

Table of Contents

Internal System QoS (Wireless Access Points)

Summary

Further Reading

Chapter 21 DNA Analytics and Assurance

Introduction to DNA Assurance

Context

Learning

The Architectural Requirements of a Self-Healing Network

Instrumentation

Distributed On-Device Analytics

Telemetry

Scalable Storage

Analytics Engine

Machine Learning

Guided Troubleshooting and Remediation

Automated Troubleshooting and Remediation

DNA Center Analytics and Assurance

Network Data Platform

NDP Contextual Correlation and Time Machine

NDP Complex Event Processing

NDP Time Series Analysis

NDP Architecture

NDP Operation

NDP Extensibility

DNA Assurance

Network Health

Client Health

Application Health

Path Trace

Sensor-Driven Tests

Intelligent Capture

Machine Learning

Summary

Table of Contents

Further Reading

Chapter 22 DNA Encrypted Traffic Analytics

Encrypted Malware Detection: Defining the Problem

Encrypted Malware Detection: Defining the Solution

ETA: Use of IDP for Encrypted Malware Detection

ETA: Use of SPLT for Encrypted Malware Detection

Encrypted Malware Detection: The Solution in Action

Encrypted Malware Detection: Putting It All Together

Summary

Part VI: DNA Evolution

Chapter 23 DNA Evolution

Index