nectar
Every Conversation Matters

Revolutionizing QoS Across Cisco UC Networks

Nectar Evolution
Enabling Real-time UC Network Orchestration

WHITE PAPER

Abstract:

Improvements in voice, video, messaging, presence and collaboration feature/functionality in several vendors' Unified Communications (UC) product lines (e.g. Cisco®, Microsoft®, Avaya®) drive the accelerated deployment of Cisco Unified Communications Manager (CUCM), Microsoft Skype® for Business and Avaya Aura™ Communications Manager (ACM) adoption. But complex lifecycle management of disparate UC applications/devices and network elements from multiple vendors across an enterprise's public, private and hybrid IT infrastructure footprint threaten to dampen the rapidity and benefits of the adoption of UC. Manual, static and vendor-siloed deployment, monitoring and fault management tools and practices are the source of this problem. New technologies, including Software-Defined Networks (SDN), Network Functions Virtualization (NFV), RESTful APIs and unified policy engines can automate UC and networking policy operations, eliminating silos and delivering dramatic Total Cost of Ownership (TCO) and user experience improvements. The introduction of Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) combined with its integration with automated, software-controlled policy engines yields these TCO and quality of experience improvements.

Nectar Evolution™ provides a unified policy solution for heterogeneous network and UC elements from Microsoft, Cisco, Avaya, and other vendors. Summary benefits of Nectar Evolution include…

- **Reduce Total Cost of Ownership** – Automate normal and casualty operations through a unified, end-to-end UC and network policy engine – **Nectar Evolution**
- **UC** – Support blended, end-to-end UC solutions from Microsoft, Cisco, Avaya and other UC vendors with a unified policy engine and database
- **Advanced Networking** – Support SDN and legacy network elements from Cisco, Aruba®, Hewlett-Packard Enterprise® and other Network Equipment Providers (NEP)
- **Improve UC user experience** – Aggregate, automate and quicken end-to-end fault detection, diagnostics, isolation and corrective actions through pre-defined UC policies

Introduction and Problem Statement:

Refer to Figure 1. A typical distributed enterprise is composed of multiple branch offices, larger corporate

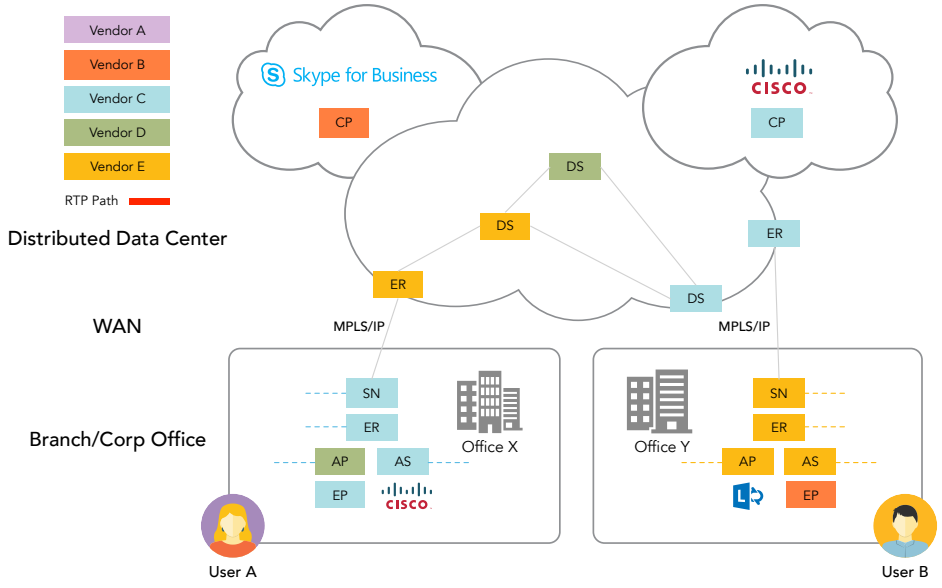

Figure 1. Distributed Enterprise Network and UC Infrastructure Deployment

sites, public/private/hybrid data centers, a WAN infrastructure with a mixture of MPLS and IP links to those distributed offices and highly mobile users with a broad range of multi-vendor UC endpoints. These enterprise IT organizations are migrating their legacy PBX and IPPBX solutions to UC and typically employ UC elements (endpoints (EP), call processing (CP) and security node (SN)) from multiple vendors. Each of these UC solutions has its own element management (EM) applications and database, requiring vendor-siloed operational and casualty business practices. The lifecycle management processes are predominantly manual in nature – requiring vendor-specific management skillsets and tools. IT staff must manually reconcile and verify end-to-end policy with every element and user move, add and change. Adding further complexity to the deployment, the network elements ((edge routers (ER), data center switches (DS), access switches (AS), access points (AP) and security nodes (SN)) are typically from multiple vendors, each requiring its own vendor-specific management tools, databases and expertise. Even more complexity is introduced by a user population requiring seamless mobility, location-independent network access and device-independent network access in the face of active network and UC security threats.

Traditional Approaches to Addressing the UC Management Problem:

UC deployments today rely upon infrastructure management solutions that lack coherency, dynamism, and end-to-end service visibility. The lifecycle management costs of day-to-day operations – for example, moving, adding or changing a network element, UC element or user attribute - are illustrated in Figure 2. Each network element depicted in Figure 2 consists of an integrated "controller" and data forwarding/filtering components. Every element must typically be provisioned manually through its vendor's element management (EM) application and database or directly through a configuration interface. For end-to-end modifications to security or access policies, for example, a simple change to multiple vendors' network elements, UC elements or user policy requires separately and manually provisioning each element in the end-to-end connection. The labor cost and opportunity costs resulting from lengthy manual element provisioning, susceptibility to errors and unsynchronized element configuration sequences are problematic.

Casualty operations are even more problematic. As an example, misconfigured priority queues in an AS, AP, ER or DS at any node through which the UC flow passes may result in degraded voice or video Real-Time Protocol (RTP) session quality when a link on those elements experiences high traffic from non-UC flows. These disruptions may only last a few seconds. Real-time detection and correlation of the event to the suspect network element and

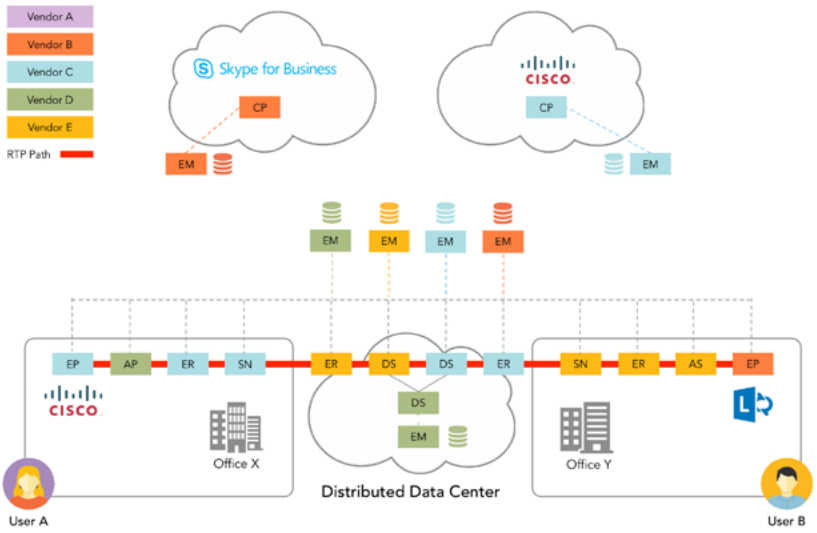

Figure 2. Traditional Network

interface is not possible with traditional network element management systems. Real-time correlation across a highly distributed set of multiple vendor network elements is virtually impossible. The user whose voice session was degraded for this short duration is quite confident that the degradation event occurred. But the network operations agent to whom the user places a complaint has no real-time visibility of the degradation event. To the user, the complaint falls on deaf ears with the consequent reduction in trust of the network operations team. Try as she might, the user cannot convince the agent until well after the call is completed. Most call processing applications, while monitoring endpoint (not network element) service degradation only report that degradation within a call detail record (CDR) at the end of the call. For lengthy calls, an agent must wait for the CDR until well after the service degradation event before confirming the user complaint and beginning the diagnostics and recovery process.

APIC-EM is implemented with generally two API interfaces.. One API, referred to as the "northbound" interface, is an open, RESTful API to which applications, such as Nectar Evolution, can interface. A "southbound" API provides logical control and local provisioning and monitoring interactions with one or more data forwarding/filtering elements. Cisco's APIC-EM controller is based upon the OpenDaylight® controller and includes southbound interfaces to Cisco-branded SDN forwarding/filtering elements, legacy Cisco IOS-based routers and switches, legacy Cisco Catalyst® switches, legacy Cisco Nexus® routers/switches and standards-based OpenFlow® network elements from third-party networking vendors. Next-generation Cisco SDN switches and routers interaction through APIC-EM controller is through either Cisco OnePK® or OpenFlow southbound APIs. For the legacy, integrated IOS, NX-OS and Catalyst switches and routers, either Cisco's CLI or OnePK can be used as the controller-to-data-forwarding/filtering interface.

Nectar Evolution

What is required is an end-to-end UC service fulfillment and assurance solution that operates in real-time across multiple vendor UC and data network elements and is implemented through a unified policy management solution. Figure 3 shows such a solution delivered using Cisco APIC-EM and the Nectar Evolution policy engine.

The concept of SDN/NFV allows the physical and logical separation of a router/switch/access point controller function from their data forwarding/filtering function. This separation allows a single, unified controller element to manage and control the operation of multiple forwarding/filtering elements. Cisco APIC-EM is such a unified controller.

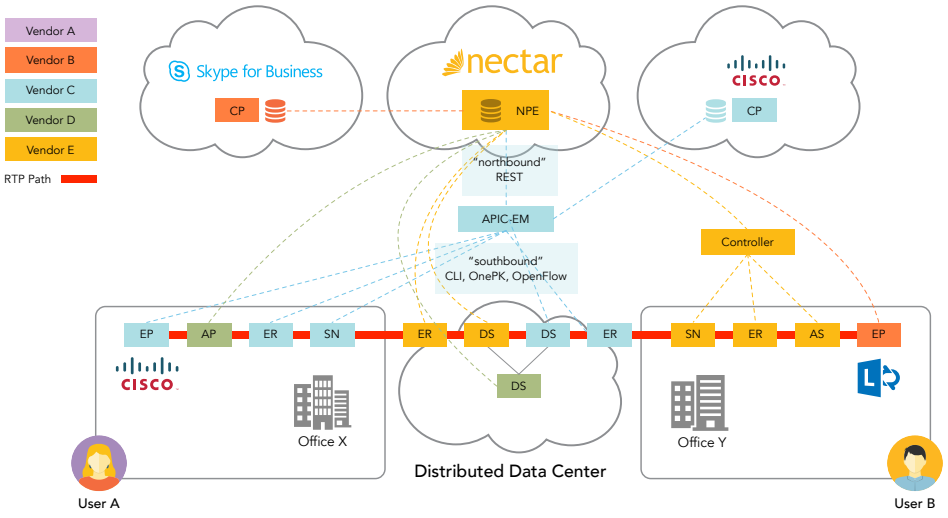

Figure 3. Real-Time, Unified, Dynamic Service fulfillment and Assurance Using Nectar Evolution, Cisco APIC-EM and the Microsoft SDN API

Nectar Evolution fills the multivendor gap by providing a single policy engine for a complete end-to-end view of UC and networking elements from multiple vendors. Evolution's policy engine and database interact with Cisco elements through the Cisco APIC-EM northbound interface. Further, Evolution collects data from the Microsoft Skype for Business front-end servers and uses real-time information provided by the Microsoft Skype for Business SDN API. Initial releases of Evolution will support multi-vendor UC monitoring and network control via Cisco APIC-EM. Low TCO and multi-vendor end-to-end support for real-time, automated UC service fulfillment, service delivery and service assurance across a highly distributed, end-to-end enterprise IT infrastructure is the revolutionary and practical end result. Evolution synchronizes amongst individual element management solutions via a common, unified policy engine and database which allows automation and verification of previously manually-implemented best practices across this diverse infrastructure. A direct benefit is the reduction of TCO and service fulfillment and assurance errors by orders of magnitude. The IT staff may extend the dynamism of Evolution by enabling automated, policy-based configuration and service verification operations. The automation of network quality of service (QoS) and user policy offers the staff the flexibility to deliver customized and dynamic services that could not be efficiently implemented using traditional network and UC management approaches. Selected use cases are presented below to illustrate the benefits in more detail

Nectar Evolution & Selected Use Cases:

- **Initial QoS provisioning** - Evolution automatically configures QoS policy on new or existing endpoints and network devices. When a user connects a new endpoint such as a Skype for Business, Cisco IP Phone or Cisco Jabber endpoints, Nectar Evolution automatically identifies the endpoint type and IP address, selecting the QoS policy associated with that type, and then issues commands through APIC-EM that result in the reconfiguration of QoS settings on the network access port to which the new endpoint is connected.
- **Inter-site Relocation QoS provisioning** - When a previously added endpoint moves to a different physical location within the enterprise and connects to the enterprise network. Evolution automatically identifies the endpoint type and IP address, selects the associated QoS configuration policy, and then issues commands through APIC-EM which result in the re-configuration of QoS parameters on that network access device's port for that newly connected endpoint. This use case includes devices moving from a wired connection on an access switch to a wireless connection and vise-versa.

In both use cases, the QoS provisioning is conducted automatically, without system administrator intervention. Evolution also reports and records each connection event.

Summary

Nectar Evolution, integrated with the Cisco APIC-EM controller and the Microsoft SDN API allows IT organizations to quickly recognize UC deployment and SDN benefits across their global IT infrastructure. These benefits include reduction of TCO, unified policy administration across multi-vendor UC and network elements, wholesale improvement of the UC user experience, and dynamic delivery of superior experience to UC users in real-time. For more information about how Nectar can accelerate your adoption of UC and SDN o revolutionize QoS across multi-vendor Cisco UC environments, visit www.nectarcorp.com.

About Nectar

About Nectar Services Corp

Nectar is a global market leader providing the most comprehensive monitoring and diagnostics software solution for Unified Communication services enables IT and operation organizations to proactively ensure the end-user experience. Our flagship offering, the Unified Communications Management Platform (UCMP) improves visibility and service delivery across integrated voice, video and data application solutions by providing unique and critical performance information. Nectar provides monitoring and diagnostics for millions of enterprise endpoints to over 1,200 enterprises in over 86 countries—including some of the largest global banking, search engine, service provider, healthcare, and manufacturing organizations in the world.

For more information:

www.nectarcorp.com

North America – **americas@nectarcorp.com**
Europe, Middle East, and Africa – **emea@nectarcorp.com**
Asia Pacific – **apac@nectarcorp.com**
Latin America – **latam@nectarcorp.com**

Corporate Headquarters
366 North Broadway, #201
Jericho, NY 11753
+1 (888) 811-8647