White Paper

Common Language Drives Customer Value for All Network Technology: 5G/MEC and Virtualized Networking Included

Sponsored by: iconectiv

Karl Whitelock
January 2021

EXECUTIVE SUMMARY

iconectiv TruOps Common Language was established to facilitate the service design and asset tracking needs of the operations and business management processes for prevailing and emerging network connectivity architectures. Common Language has been used by communications service providers for over 40 years.

Complexity from new technology evolution (e.g., network virtualization, private networks, hosted networks, 5G, multi-access edge computing [MEC], and the Internet of Things [IoT]) requires assets to be aligned with business and technical objectives to keep costs within expectations, address end-to-end (E2E) service objectives, support partner accountability, maximize interactive efficiency, and show business management responsibility. On the basis of its successful long-standing customer implementations and evolutionary approach to the network management processes, Common Language is expected to play a major role in the evolution and deployment of new facilities-based networks and the virtual aspects upon which these new technologies come to rely.

This paper explains how teams with network and partner-provided asset management responsibilities can achieve business value by maximizing the use of common nomenclature. In addition, the paper describes how a common naming strategy improves the effectiveness of real-time network operations and key business management functions. This paper also explains how Common Language can bring increased awareness when defining, launching, and managing new network-based services.

Introduction

As network technology and business strategies continue to evolve, the greatest challenge asset-based communications service providers face is how to manage the physical and virtual assets that define the services they provide. Understanding the physical and logical placement of assets is strategic to several internal operations functions including network planning, inventory, service orchestration, catalog, activation, network assurance, service-level agreements (SLAs), policy, rating, and charging. The multilevel construct of the underlay and overlay connectivity infrastructure and the E2E partner-aided services to customers of all types brings additional layers of asset tracking complexity that must be addressed by each of these business and operations management domains.

Beyond the network operations and customer experience functions, regulatory mandates and corporate financial accountability processes demand an accurate understanding of which assets are deployed where and for what purpose. Functions such as assets in service, asset depreciation, and spares inventory are crucial to meeting the accountability needed for accurate business management.

Asset management concerns are an issue for communications service providers with physical assets, with hosted network service providers, communications platform-as-a-service (CPaaS) operators, fixed and mobile virtual network operators (MVNOs), wholesale connectivity providers, operations support systems (OSS) vendors, and business support systems (BSS) suppliers. A universal structure for identifying the equipment in operation today, who owns the equipment or virtualized functions, the location of physical assets, the placement of virtual assets for those with a need to know, and the type of functionality delivered by each item is a real necessity, particularly as partner ecosystems and 5G network technology move to center stage.

Why Is a Common Language Asset Management Strategy So Important?

As technology continues its evolutionary path, physical assets such as network elements, network nodes, switches, routers, and other types of network components are quickly becoming software defined. This means keeping track physically, logically, and logistically of each virtualized network function (VNF) and cloud-native network function (CNF). Physically applies to the portion of the VNF/CNF tied to the computing platform upon which the software is hosted; logically refers to what E2E service chain each VNF/CNF delivers its designed capabilities; and logistically is relative to the software license usage permissions granted by the VNF/CNF software owner for each instance of software placed into service. Flexibility to address emerging network architectures is key to effectively managing the operational challenges that come from a hybrid physical and logical network design.

From a service assurance and SLA perspective, the physical and logical portions of a VNF/CNF must always be accounted for to maintain E2E service integrity. From a business and asset perspective, specific knowledge of the physical/logical environment is essential for revenue tracking and partner settlement needs whenever partner-provided functionality is used. Mixed with all VNF/CNF capabilities is a hybrid assembly with existing physical network functions (PNFs) that must be tracked and managed. Finally, there are several new technology examples where Common Language will need to play a larger role, including dynamic inventory, enhanced service catalog, partner ecosystem management, policy management, and B2B2X real-time charging.

Functional Aspects of iconectiv's Common Language Code Sets

Common Language is an information enrichment tool that globally offers organizations a means to identify and track the physical placement and virtual usage of communications infrastructure. The TruOps Common Language product set is owned and managed by iconectiv for its customers worldwide. Common Language codes are presently classified into four categories specific to location, equipment, connection, and service information:

- **Location.** Common Language Location Identifier (CLLI) is a standardized global registry used for the purpose of inventorying and tracking network locations and functionalities. Physical locations contain multiple pieces of equipment. CLLI codes are used to provide definitions for generic types of equipment used at these locations. For example, a CLLI can identify where small cell devices or a cell tower is located by the functional entity assigned to that location. As the communications network grows, it becomes strategic to understand where each network

asset, such as a 5G antenna or cloud service, is physically located. CLLI codes are equally valuable in identifying partner-provided functionality close to the telco edge. This is key in the delivery and ongoing evolution of customer services. In addition, a standardized format, such as a CLLI, enables efficient tracking of the location of equipment assets between both internal and external systems.

- **Equipment.** Common Language Equipment Identifier (CLEI) is the iconectiv Common Language global registry focused on network equipment. CLEIs identify equipment in a vendor-agnostic structured format with a one-to-one relationship between a CLEI code and a manufacturer's product code (e.g., part number including the hardware version). CLEIs are used to provide a consistent naming structure, classification of equipment, and identification of device type. CLEIs are also used to track product change notices (PCNs).

  CLEIs apply to more than just physical equipment. Software and licenses are equally applicable to CLEI coding. Consequently, a CLEI may be used to identify which computing hardware a virtualized network function may reside within a hybrid communications service provider/software asset partner environment. CLEIs may also be used to track software-defined VNFs/CNFs and their associated software development organizations.
- **Connection.** Common Language Connection codes are the standardized ordering and identification codes for all communications service provider connections. Coding includes private line services such as Ethernet and Dark Fiber at high speeds. In addition, the codes provide identification for infrastructure facilities as well as dedicated customer transport technology on optical, copper, and wireless communications service provider transport. Network Channel/Network Channel Interface (NC/NCI) codes facilitate ordering between trading partners, while CLCI Special Service (CLCI S/S), CLCI Message (CLCI MSG), and CLFI Facility (CLFI) codes provide the naming schemes for identifying the special service circuits, message trunks, and facilities that comprise the connections. A recent example involved ordering and identification codes created as tower interconnect identifiers for companies that offer power, space, and maintenance options to cellular communications service providers.
- **Service.** Common Language Services information consists of the Universal Service Order (USO), Universal Service Order Code (USOC), and Field Identifier (FID) codes. These codes define various network components, interfaces, products, and/or services necessary for defining compatibility with many installed communications service provider systems. Service information provides a way to standardize service order entry, enable provisioning, and deliver billing-related information in one common format for these systems. The USO, USOCs, and FIDs include data needed to support the E2E service order process pertaining to service ordering, provisioning, billing, and assurance.

For many evolving business situations, CLLI codes, with their ability to address where network assets are physically located, are a clear example of the effectiveness to which Common Language delivers strategic value. Common Language codes are the exclusive intellectual property of iconectiv, with the company carrying a regulatory management responsibility for the common naming needs of communications service providers within North America and iconectiv's extension of common naming to communications markets the world over.

Common Language Provides Value Beyond Network Operations

The previous section of this paper underscores the strong reason why Common Language codes are important in meeting service integrity requirements when managing a hybrid environment of virtual and physical network assets. Similarly, financial reporting groups, regulators, insurers, and auditors each want insight based on different relationships between the value and quantity of network assets in use

and the overall level of generated revenue from those assets. For many, these factors must be reported on a regular and timely basis per specific general accounting, regulatory reporting, and financial reporting mandates. Accomplishing such reporting requires an automated approach for bringing operational insight from the network to the business office. Some of the more significant asset management and reporting needs addressed by a Common Language code strategy are:

- Identify and reduce or eliminate unwanted or duplicate assets.
- Align purchasing, procurement, inventory, and operations management.
- Optimize available inventory and the spare installed base.
- Standardize means for showing what assets are located where for financial audits.
- Maintain compliance with regulatory, insurance, securities reporting, and accounting requirements.
- Combat fraud and theft by monitoring the actual location of assets.
- Ascertain the value of assets at different stages of their life cycle, especially given that different assets have different useful lives and regulatory-defined depreciation schedules that do not align with business tax depreciation definitions.
- Eliminate unnecessary maintenance costs by accurate warranty monitoring and product change notice tracking.
- Recover stranded assets.
- Provide data for service cost calculations such as equity-asset ratio for the company, average margin per user, cost per gross addition of customers, opex per network site, revenue per mobile cell site, and a host of others.
- Accurately account for assets during the valuation process for mergers, acquisitions, and the sale of select assets.

Simplification, beyond the process of communicating essential data and parameter settings between network management systems and digital/physical network infrastructure, needs common nomenclature to aid other business functions, especially financial reporting. While only a few parts of financial management are noted in this paper, there are others such as positioning with federal, state, and local regulators for equipment valuations and right-of-way needs along with codevelopment of business solutions involving the latest network technology. In each case, and countless others, timely reporting of financial events by the global service provider community would not be practical without using some type of common naming strategy, especially as software-based network functions grow.

Market Trends Within the Evolving Communications Industry

The global communications services industry is going through unprecedented change, led by 5G network technology and its attendant train of dynamic requirements tied to the operations and monetization functions of fulfillment, assurance, and billing. However, 5G is much more than the next generation of mobile technology. It is not on a linear scale for E2E solution offerings to business problems nor is 5G a general offering to consumers for network connectivity services alone.

5G brings flexibility and change in the form of alternative business models, dynamic network configurations, advanced pricing strategies (B2B, B2B2X), evolved care functions, creative payment options, and a dedicated focus on the customer experience. Within this realm, all change points back to a secure network environment, one that is customer centric by design and delivers services that can be guaranteed E2E with the right levels of commitment. In addition, customers are charged on a market acceptable real-time basis, and contributing partners are accurately compensated once

revenue is collected. Most importantly, the inner workings of all network resource functions need guidance through the right business processes via properly vetted identification.

Changes needed in support of 5G service deployments involve additional business and service management factors that are advancing through various degrees of maturity. These factors are now combining with advances from 5G network technology to create additional stress on existing systems, thereby requiring evolved ways to satisfy 5G service concerns. Some of these factors are:

- Building out the telco cloud (core → access → near edge) and in combining it within an MEC service architecture, where edge is defined by cloud functions and industry (e.g., private networks, mobile advertising, IoT, mobile health, real-time patient procedure analysis, drones, gaming, fleet management, augmented reality/virtual reality, collaborative robotics, smart retail, agriculture, and a growing list of others)
- Establishing VNF/CNF/PNF service-level orchestration within the same network resource assignment (In addition, VNF/CNF license management and SLA commitment aligned with network capability via slice management.)
- Transforming business and operations management processes to a digital services approach from the cloudification of OSS/BSS functions using secure and containerized microservices
- Establishing partner ecosystems to deliver higher value to customers (e.g., solutions to problems rather than just a network connection)
- Changing the connectivity service construct through B2C, B2B, and B2B2X business models with the associated influences that come from multipartner service arrangements (These include partner onboarding and revenue remuneration for partner contributions to E2E solutions — for example, enterprises selling services instead of products [B2B2X].)
- Engaging with multiple business models within the same service offering to dynamically support different schema for real-time charging based on traditional and nontraditional usage factors, initializing real-time assurance tied to various network operations parameters and revenue collection tied to SLA management

Each of the aforementioned factors plays a different role in how communications service providers can define and deploy the services they bring to market. Specific examples in how Common Language may play a larger role are outlined in the following sections relative to network technology evolution, communications service provider business model advances, partner ecosystem expansion, and real-time assurance as network intelligence increases its importance in helping communications service providers monetize the capabilities each of these factors bring to light.

Example 1: 5G and Network Edge Device Identification

Like network architecture of the past, deploying 5G and edge computing devices requires a unique way of identifying the communications equipment installed at different points of a network, including what is supplied by partners and communications service providers at these points, along with defining the business purpose of the equipment. In some cases, even matching up workflows with pieces of equipment that are used within a service definition is required.

The unique identification of equipment, whether physical or virtual, is gaining importance with both suppliers and communications service providers. For example, a common nomenclature for identifying all involved equipment is essential for provisioning and activating 5G/edge-defined services. Such codes are equally important in managing any edge-deployed operations functions that must synchronize with core systems to maintain E2E service-level integrity and the technical aspects of

customer experience management. In addition, systematic identification of the thousands to potentially millions of new network connectivity points from IoT deployments is strategically necessary to the owners of such devices and to the communications service providers delivering connectivity. Identification of geographic location and functionality type is critical to the connectivity path, regardless if this path is served from fixed broadband, fixed wireless, or mobile access assets.

In cases deploying additional technology, such as MEC, several customer edge instances are needed to satisfy latency requirements. Edges are varied in purpose according to industry focus, and they offer levels of interaction according to E2E solution needs. Multiple operations and monetization systems may need to be instantiated, especially billing and assurance systems that will communicate and synchronize with core system deployments for E2E accountability. For example, automated service assurance can make a difference in how successful complex 5G and MEC services will be accepted by the market, especially when partner contributions are involved. The same applies with network slices — one or more virtual customized network configurations, each sharing a common physical infrastructure — which could number into the hundreds for certain situations and business conditions.

Some of the operations and monetization systems challenges in a 5G/MEC environment are:

- How will system-to-system synchronization be accomplished?
- How will data integrity be managed and maintained for the solution components that define each service?
- How will solution components be recognized by other business or operations functions?
- How will contributing resources from a communications service provider and each of its partners be uniquely identified and tagged for usage?
- How can the pain points with multipartner service definitions, either from multiple systems instances or from multiple network slices, be minimized?
- How will revenue flow from customers to the service manager if a service meets SLA requirements?
- How will partner contributions to each service be identified and anticipated compensation be calculated for settlement based on resource consumption levels and contract definitions?
- How will partner-provided digital resources be accounted for and weighed against usage dimensions? What changes if resources are physical items rather than digital ones?
- If SLA conditions are not met, how will credits flow (if any) to customers and penalties be applied to the offending resources if partner supplied?

For these situations and likely others, Common Language provides a means whereby assets are easily identified and accounted for, regardless of the business function involved.

Example 2: Virtualized Network Function License Management

Physical assets such as network nodes, switches, routers, and other types of network components are becoming "virtualized." The functionality that defines the operational uniqueness of these devices was previously embedded in the firmware contained as part of the network hardware design. Organizations bought computing and network functionality "boxes." Now, the box functionality is separated into software code containing VNFs and CNFs that run on generic computing hardware. The benefit of this separation has always been pitched as a cost saving, but more importantly, it means the network is able to scale elastically in short order (minutes) rather than the extended weeks and sometimes

months that a network capacity expansion project took using purpose-built devices. It also means there are several parameters that must be accounted for from an asset and inventory perspective.

Keeping track physically, logically, and logistically of each VNF and CNF is essential for ongoing business management — physically, the portion of the VNF/CNF tied to the computing platform upon which the software is hosted, logically as to what E2E service chain each VNF/CNF delivers its designed capabilities, and logistically relative to the software license usage permissions granted by the VNF/CNF software owners for each instance of their software that is placed into operation. Flexibility to address emerging network architectures quickly and accurately is key to managing the operational challenges that come from a hybrid physical and logical network design. For example, logistical VNF/CNF software management is also known as VNF/CNF license management.

VNFs and cloud-native containerized CNFs are likely the most unknown risk to a communications service provider's business today due to their limited deployment and their technical complexity and relatively unknown best practices for procuring VNF/CNF licenses from their software owners. The creators of VNFs/CNFs are not always the typical network equipment suppliers, as this pool of developers includes traditional network equipment suppliers, IT software suppliers, systems integrators, virtual network function platform suppliers, and even a communications service provider's internal development teams as the virtualization concept evolves.

Because they are cloud hosted, the ultimate seller of a VNF/CNF may be acting as an agent for the original software developer as is the case today with Amazon Web Services (AWS) and its platform-based IT services catalog. Regardless of who owns the VNF/CNF, the license procurement, usage management, inventory, and policy functions are complicated. Key questions to be addressed are:

- How will VNF/CNF assignments be uniquely identified and then noted against contract commitments and usage specifications for a service definition or a unique customer need?
- When a VNF/CNF license cache nears exhaustion, what process will trigger the purchase of more licenses from VNF/CNF owners?
- How will VNFs/CNFs be ordered if competing suppliers offer the same functionality?
- Can VNFs/CNFs that need replenishing be automatically assigned on an on-demand basis if they are somehow uniquely identified by supplier, functional definition, and/or usage permissions?
- How will a freshly purchased VNF/CNF be identified from others in an instance stack of formerly issued licenses if expiration dates and usage intent are a part of a supplier's selling strategy?
- How will existing licenses be identified and updated when changes are needed?
- How will VNF/CNF licenses be incorporated into existing catalog and inventory processes?
- What mechanism should be used to identify VNF/CNF deployments of a certain functional type from a particular vendor?
- What must be monitored to manage awareness of software license validation against possible contract license expirations or other usage constraints (e.g., geographical region specification, NFV infrastructure [NVFI] platform usage restrictions, supplier conditions, or something else)?
- What will mark usage and accountability permissions granted with each license agreement?
- Can usage rights be captured in a way that they will be part of the VNF/CNF design definitions carried through to an automated inventory/catalog system to support the provisioning, activation, billing, and assurance functions?

- Will permissions be driven by functional type, developer name, or business intent of the purchaser (e.g., communications service provider versus cloud services provider versus other)?
- Can software developers impose the use of multiple agreements for the sale of a VNF/CNF license based on functionality type or will a general agreement suffice if VNFs/CNFs from the same supplier are individually identified?
- How will the resolution of this issue be conveyed to whatever systems must keep track of license assignments?
- Can usage term limits of a VNF/CNF license be imposed based on functional type of VNF/CNF or a developer organization?
- How can a VNF/CNF from a specific supplier be uniquely identified and how will the software license exist based on a customer's intended software architecture (e.g., node assignment)?
- To understand service usage profitability, how will VNF/CNF deployment and revenue settlement be compared, especially when IoT solutions can theoretically consume large quantities of VNF and CNF licenses?

5G/MEC not only increases solution delivery complexity, but IDC believes this architecture will be the way in which critical business solutions involving both connectivity and partner-provided capabilities will be deployed to all enterprise customers in the weeks and months ahead. In this environment, traditional communications service provider roles are changed as connectivity becomes only part of an E2E solution to evolving business problems.

Unlike physical components, VNF/CNF software will need to be tracked and traced more closely than physical components, which must include stipulations on how a VNF/CNF license can be used, exchanged, updated, or modified. Without a commonly defined means for identifying what components are deployed where, IDC believes that a resource accountability challenge will reach astronomical proportions.

Example 3: Partner Ecosystem Management and Accountability

5G business solutions are a technology play that solves problems centered on ultralow latency, heavy bandwidth, and high-capacity volume loads along with mobile edge computing capabilities configured to meet personalized customer connectivity needs. Tunable contributions of these network attributes will play out eventually as personalized slices of network functionality when the full technology set for 5G network slicing is delivered to the industry from the 3GPP R17 standards process. Currently, R17 is rescheduled for release in late 2021, but will likely change again due to implications from the COVID-19 global pandemic.

5G solutions involve a customer and services play that works by using the strengths of multiple partners. Several operating examples engage partners that ultimately take on a substantial role in the 5G "solutions" designed to bring increased value to the customer experience. Often there will be a network part, a partner-provided edge device, and the unique software contribution of an app development partner with critical domain expertise pertinent to the business challenges addressed.

Tough operational challenges are more easily addressable if the components from contributing partners follow a common nomenclature. In this environment, complexity abounds from:

- Implementing the right connectivity option for the type of business solution needed
- Provisioning and activating the solution, which can dynamically change at any time

- Bootstrapping and cataloging solution-specific IoT devices or programmable embedded SIMs (eSIMs)
- Pricing and charging for usage following a variety of new business models
- Monitoring solution quality and capabilities according to SLAs
- Tracking resource consumption for communications service providers, their partners, their customers, and their customer's customers
- Managing the flow of service-level revenue from customers to solution delivery participants, including regular partner settlements

A business management approach that can deliver a frictionless experience for partners and for customers is essential to enable chargeable solutions that provide high customer value and a profitable revenue flow. A platform-based ecosystem orchestration function is a clear choice for this business environment, especially if common nomenclature is used as a means for bringing together multiple suppliers from multiple organizations.

Example 4: Real-Time Service Assurance in a 5G/MEC/IoT World

Automated service assurance, fueled by customer-centric network intelligence, plays a major role in shaping the dynamic 5G services concept, especially for solutions that involve various stages of partner involvement. 5G changes how organizations do business when mmWave spectrum solutions, with the promises of potential 10GBps over-the-air transport speeds and latency at 5ms or less, are a business reality. In this environment, there are several operations issues tied to quality experience management that come to the surface. More specifically:

- What orchestrates the network connectivity path with other parts that define an E2E business solution?
- How will each part be identified by a real-time service monitoring solution?
- How will the E2E service offering be monitored for compliance?
- When premium-priced services are involved, how will service compliance per SLA definitions be noted and what type of record (if any) should be kept for "proof" of compliance?
- If distributed ledger technology (DLT) is involved for compliance certification, how will contributing components to an E2E service offering be noted?
- How will noncompliance be enforced after it is detected? How will compliant solution status be returned? Are these manual or automated steps or both?
- How will alerts and notifications be created and then delivered when certain thresholds are crossed? Will this function change when "customers" are machines rather than humans?
- To whom will these notifications be sent when a service falls out of SLA compliance? How will they be identified, especially if there are large numbers of the same devices involved?
- How will pricing change and under what conditions will monetary relief be provided in the event of an SLA violation?
- How will SLA violations affect the provisioning function, especially if an offending service component is a VNF/CNF? How will this process affect the VNF/CNF license procurement and usage rights process?
- If applicable, how will partner involvement that causes a fault be identified?
- If fault is not with a partner component, how will the right level of remuneration be provided to partners upon service failure? If service is delivered "normally," how will partner compensation be provided?

- If a partner contribution is the cause of fault, how will refunds be applied to the end customer and what definition of proof is needed to support negative payments by the communications service provider to the partner at fault?
- How can communications service providers "see" in action the various components of partner-enhanced services?
- In the case where an SLA is violated, how will penalty payments from partners be collected if their contributions to an E2E service definition are at fault?

There are challenges to be addressed by any technically oriented business approach for assuring that 5G/MEC/IoT services meet and even exceed expectations. Providing service guarantees has not been a strong suit of the communications service provider industry in the past, which makes continuous assurance of 5G/MEC/IoT services even more difficult. Customers will not accept service offers without a solid understanding that contracted service-level latency, bandwidth capacity, and throughput volumes are consistently available. Making such a commitment business acceptable requires a means for monitoring all service components and automatically addressing problems as they occur. This means machine identifiable solution components.

Conclusion

Not only are communications networks undergoing massive change in how they are defined and how they are deployed, so are the business strategies of enterprise customers and large businesses globally. Everyone wants ubiquitous connectivity at faster speeds and with responsiveness measured in a few microseconds today and even lower in the future. Millions of devices need to be connected in different ways to satisfy a growing plethora of business solution requirements. The number of network extensions through 5G/MEC strategies is exponentially increasing.

Managing the operational aspects of new technology deployment such as fulfillment, assurance, partner management, and real-time charging depends on looking deep into the network for data relative to network performance and customer experience. Regulatory needs tied to asset utilization and revenue generation will not change and, in many cases, will become more scrutinous as new generation network capabilities take hold.

Automated accountability management will be the key to business success as network component orchestration gains complexity, as E2E customer services involve more partners, and as revenue expectations increase to offset the costs of new technology deployment. A common nomenclature is essential for addressing these operational needs and financial tracking requirements. The iconectiv Common Language process is one solution with a proven background to satisfy the needs of network operations and accounting collectively. Without a common nomenclature, such as Common Language codes, how will you address the equipment (physical and software) management and regulatory reporting needs of your organization?

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com