SOLUTION NOTE

INFOBLOX SOLUTIONS FOR OpenRAN

Delivering the Protection and Performance that OpenRAN demands

SUMMARY

The goal of the OpenRAN initiative is to remove the roadblocks that complicate the rollout of transformational new cellular services.

Aspects of the OpenRAN implementation can inadvertently add to those complications. Infoblox solutions enable the networking industry to overcome those obstacles and realize the full potential of OpenRAN.

WHAT IS OpenRAN?

As its name implies, the Open Radio Access Network (OpenRAN) is an industry-wide initiative to enable cellular radio networks—composed of white-box hardware and software components from multiple vendors—to operate over open, interoperable and standardized RAN interfaces. OpenRAN takes traditionally closed RANs and "opens" them. Baseband unit functions are virtualized, separating the control plane from the data plane and opening up front-haul interfaces.

Because OpenRAN consists of virtualized network architecture built on general-purpose, commercial, off-the-shelf hardware (COTS), it combines various hardware and software that can be integrated and upgraded via software.

WHY OpenRAN?

Deploying, maintaining and optimizing networks is a difficult task requiring skilled manual labor. It is also expensive, with most of the costs necessary to build a wireless network related to the RAN segment. While there are no hard figures, some estimates point to combined RAN CAPEX and OPEX reaching as high as 80 percent of the total network cost.[1]

RANS were historically built leveraging equipment only available from a handful of RAN vendors with siloed and proprietary solutions, resulting in limited competition and reduced choice. Previously, mobile network operators have been "locked-in" to these legacy RAN vendors, making maintaining and upgrading networks costly and challenging. The software and hardware are pre-integrated and interlocked from a single vendor, usually with proprietary interfaces. Release cycles tend to be long (6–12 months), and operators must rely on vendors for changes to the software.

When 4G arrived, further issues arose because radio systems evolved into two separate and proprietary hardware and software systems, digital and RF, with proprietary and vendor-specific interfaces between them. While virtualized RAN brought improvements with COTS server platforms running proprietary software with virtualized functions; there were still proprietary functions between the RF hardware and digital systems. Now, 5G compounds this situation because 5G New Radio further subdivides into components, and all 5G RAN equipment is compatible only if purchased from a single vendor.

---

1 Open RAN 101—Open RAN: Why, what, how, when? (Reader Forum). https://www.rcrwireless.com/20200701/opinion/readerforum/open-ran-101-open-ran-why-what-how-when-reader-forum

Another problem is the current geopolitical climate. As individual nations restrict the number of vendors able to deploy 4G and 5G networks, many mobile operators are concerned that reduced vendor selection will limit innovation and choice. With only a few select and very large vendors to rely on, mobile operators worried about the potential for increased market and financial risk view OpenRAN as a solution.

THE GOALS OF Open RAN

The promise of OpenRAN is based on cheaper, general-purpose, vendor-neutral hardware and software-defined technology that can be scaled, upgraded or changed much more easily using an automation/DevOps approach. Virtualizing baseband units' network functions running as software on generic hardware will significantly benefit operators, allowing them to choose their preferred hardware and software and create and evolve networks specifically suited to their business and their end users' needs. Operators gain increased flexibility in the placement of their workloads and economies of scale through centralization and realize numerous advantages.

Reduce Costs. Network operators can reduce OPEX and CAPEX by leveraging multi-vendor automation, white-box hardware and open interfaces across the entire telco cloud. Introduce automation into the radio access network in a cloud-native manner to reduce overall network OPEX. They will have one unified OpenRAN network to automate, which both saves and introduces cost-saving remote upgrades to the overall network. The savings come from having a disaggregated architecture that uses off-the-shelf, industry-standard hardware to run RAN workloads and reduce the CAPEX of building out a 5G radio access network. Further cost reductions are possible through centralized operations and software automation. Instead of performing hardware upgrades through expensive truck rolls, remote software upgrades can be performed centrally and remotely.

Increase Agility. Making the network more programmable enables operators and other vendors to innovate faster and introduce new services more quickly. For example, OpenRAN deployed at the network edge will benefit 5G applications such as those used in autonomous vehicles and the IoT, support network slicing use cases effectively and enable secure and efficient over-the-air firmware upgrades.

Decrease Vendor Lock-In. With vendor-neutral hardware and open software components, OpenRAN promises to lower the reliance on a few vendors by decoupling the network's hardware and software components and decreasing massive expenditure on network infrastructure. Operators will benefit by using best-of-breed open solutions that can programmatically respond to changing business demands.

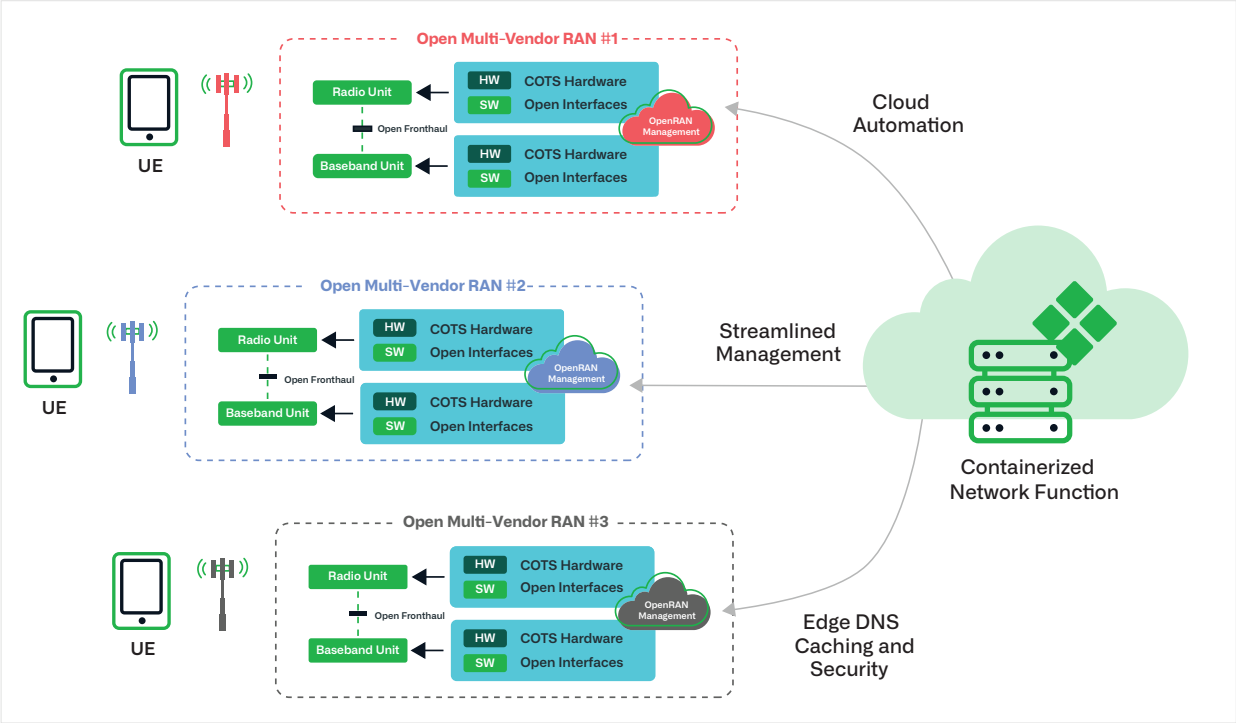
A MULTI-CLOUD PROBLEM

But there is a problem. While OpenRAN involves replacing the interfaces used in today's radio access networks with standards that would facilitate competition, there is an emerging situation where a handful of vendors capable of meeting operator requirements hold supply chain dominance. Each vendor provides its own "private cloud" solution, leveraging virtual machines and containers to manage potentially thousands of antennas.

With geopolitical realities leaving operators reliant on a few large vendors, choice and risk elements will most likely force them to simultaneously spread their risk across multiple OpenRAN solutions. Although the goal of OpenRAN is to reduce costs, increase agility, and provide free operational resources, operators may not realize that using multiple OpenRAN solutions can create its own multi-cloud problems stemming from managing numerous OpenRAN private clouds.

THE IMPORTANCE OF DDI IN 5G AND OpenRAN

DNS, DHCP and IP address management (DDI) add critical value for service providers both through securing the network and ensuring carrier-class service performance. As the number of devices escalates and logical network functions proliferate with NFV and containerized network functions (CNFs), reliance on static IP management solutions, manual update processes and unsynchronized spreadsheets are no longer practical.



Inadequate automated address management results in increased operational expenses for networks due to the sheer volume of access devices, and it also extends the duration of troubleshooting efforts. Configuration errors turn into network failures, customer churn and revenue losses. Tracking and managing these complex, rapidly changing IP networks demand a new approach to IP address management (IPAM).

Dynamic Host Configuration Protocol (DHCP) is the client/server protocol that automatically provides an IP host with its IP address and other related configuration information, such as the subnet mask and default gateway. To ensure performance, new IPAM functionality must be "built-in" and tightly integrated with both DNS and DHCP functions, not just "bolted on" as in the past. At the same time, IPAM must grow to support multiple functions for address allocation, management and reporting.

To realize and maximize investments in 5G and edge deployments, operators must quickly and dramatically evolve their existing legacy DDI management processes. Virtualized and containerized OpenRAN solutions will have pre-deployment and lifecycle requirements, necessitating DNS and IPAM procedures. However, operators often leverage traditional IPAM and DNS management processes using spreadsheets and databases to enable the deployment of cloud functions or track device inventory limits. These legacy approaches can delay critical deployments and dilute the flexibility and cost benefits that OpenRAN promises to bring.

Visibility and Discovery. Without a consistent DNS and IPAM solution across the telco cloud, operators often must rely on multiple tools to access DNS and IP address data—increasing inconsistencies in the network-wide management of the DNS and IP address space. Using multiple tools also leads to longer troubleshooting times, reduces the ability to perform network planning, and increases security risks.

Infoblox DDI provides seamless detection and monitoring of virtual instances, ensuring comprehensive visibility as new instances are added. It also efficiently cleans up records upon instance termination. Operators enjoy a unified view across hybrid and multi-cloud setups, covering telco cloud, public cloud, and OpenRAN network components.

Automation. Today, a static infrastructure delivers service (e.g., a PGW will rarely change once installed and in operation), but the 5G world will be much more dynamic, and provisioning must adapt. Tens of thousands of containers and virtual network functions (VNFs) will be instantiated and terminated on demand. Containers and VNFs will rely on DNS more than ever. But how can operators ensure that instances are automatically put into service and in sync with the workload lifecycle?

Infoblox supports OpenRAN platforms with cloud orchestration technologies that streamline the provisioning and de-provisioning of IP addresses to newly created VMs and containers, update DNS records, and release IP addresses when VMs are taken down—all in seconds instead of hours or days. Infoblox provides an IPAM platform integrated into the container/VNF lifecycle management fully automated by a RESTful API. The platform ensures the IP address space's overall integrity and consistent policy of DNS naming conventions and network/IP address provisioning. It achieves this by reconciling disparate terminologies (such as tenants, VPCs, VNFs and containers) to eliminate the challenge of maintaining consistency across complex deployments. Infoblox automation eliminates handoffs between cloud and network teams and manual provisioning of DNS records. Infoblox dramatically shortens the time needed to provision new antennas. And when virtual resources are decommissioned, Infoblox automatically reclaims IP address and DNS records so overburdened staff are not performing manual, tedious processes.

Security. Constantly evolving threats and increased attack surface demand a foundational approach to security that is ubiquitous, scalable and automated. Rapidly evolving cyber threats require CSPs to invest ever-greater resources in threat intelligence to stay a step ahead of cybercriminals. But threat intelligence today is hampered by information silos, lack of actionable context and an inability to prioritize by threat category. With more resources being deployed at the far edge, operator IT and server admin teams will have to manage significantly more container pods and VMs—sometimes hundreds at a time and potentially thousands of containers—in their virtual and cloud environments. The deployment of potentially thousands of containers across multiple platforms and regions introduces new operational complexities. With many more virtual servers, containers and services, the network becomes even more massive–increasing the overall attack surface and making security even more critical. Careful planning and monitoring are essential to mitigate these challenges.

Infoblox provides security for 5G and edge-based telco cloud environments in several ways:

- **Advanced DNS Protection** helps secure the DNS services running on the edge instances, providing DNS DDoS mitigation to protect the critical DNS infrastructure that is the "heartbeat" of operator networks. It automatically detects and stops the most extensive external and internal DNS-based attacks while maintaining DNS integrity and service availability.
- **BloxOne® Threat Defense** protects edge services, consumers and applications from malware and advanced persistent threats. It maximizes brand protection by securing existing networks and subscriber imperatives like 5G, IoT, network edge and the cloud–enabling operators to transform DNS from a major vulnerability in their defenses into their most valuable security asset. It empowers organizations to centrally and automatically secure every connection across physical, virtual, containerized, and cloud infrastructure, regardless of device or location. By combining an up-to-date network inventory with Infoblox Threat Intelligence, operators gain current, conglomerated threat intelligence from multiple sources to identify at-risk and potentially malicious workloads. This input greatly simplifies at scale what operators must do to shut down attacks early before they spread and cause harm.
- **High-quality Threat Intelligence** mitigates the widest range of DNS-based attacks, including volumetric, reflection, DDoS, NXDOMAIN, amplification, TCP/UDP/ICMP floods, data exfiltration (through known tunnels), hijacking, reconnaissance, cache poisoning and protocol anomalies.
- **Threat Insight** enables security teams to get a jump on zero-day threats. It does so through analytics based on machine learning to inspect DNS traffic to detect patterns associated with data exfiltration and block DNS requests to those destinations.
- **DNS Firewall** proactively and automatically protects networks against fast-evolving, elusive malware threats that exploit DNS to communicate with C&C servers and botnets. The solution blocks connections to malicious destinations. In addition, it enables security teams to rapidly pinpoint compromised devices, isolate them to prevent the spread of infection and trigger remediation activities.

CONCLUSION

While the goal of OpenRAN is to reduce costs, increase agility and free operational resources, operators may not realize that using multiple OpenRAN solutions can create a multi-cloud problem. Conventional IT management approaches often undercut the benefits that operators seek due to numerous OpenRAN private clouds. Infoblox solutions can centralize DNS and IPAM for OpenRAN integration and interface with different OpenRAN platform management systems, providing critical and centralized DNS and IPAM and helping ensure overall IP space integrity. With Infoblox, operators can centralize and scale IPAM capabilities, modernize management and improve visibility no matter what OpenRAN solutions are employed.

To learn more, visit www.infoblox.com/sp or contact your local Infoblox representative today.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240223v1