APRIL 22, 2014

The Elastic Network: 4 Keys to Building a More Agile Network with IPAM

by Branko Miskov, Director of Product Management, BlueCat

No matter what industry or market you're doing business in, chances are your network team is under enormous pressure to keep pace with business growth, technological change and rising expectations for connectivity. Maybe you're a retailer that needs to roll out 500 new stores this year, a financial services company that is consolidating networks after a merger or acquisition, or a logistics company that is developing new apps to reach your customer and needs to rapidly build and tear-down DevOps virtual test environments. Whatever the case, a lack of automated provisioning and self-service can leave your network team ill prepared to support growth and change.

If you're still using decades-old IPAM practices, spreadsheets, manual processes and basic tools, your business will continue to face numerous network challenges like:

- Brittle network infrastructure that can't scale to match business growth
- Delays and bottlenecks in rolling out new initiatives
- Poor visibility into what is connected to the network
- Emerging network threats that put business at risk

So what's the solution? To turn connectivity into competitive advantage, you need to build an elastic network that's flexible, adaptable, scalable and easy to manage. You've probably heard the term elasticity used in relation to cloud computing. The cloud leverages virtual servers to enable services and apps to be moved around and scaled up or down on the fly without affecting the end user. Similarly, elastic networks scale and adapt to match the ever-changing and unique demands on your infrastructure and business.

IPAM enables network elasticity by allowing you to automate error-prone manual processes, dynamically provision devices, self-manage networks and adapt to rapid change without having

to re-architect your network. IPAM provides the foundation for an elastic network by delivering four key elements: connect, map, secure and extend.

Connect the Device

You've likely noticed an influx of new security risks and management challenges popping up in your enterprise. With the explosive growth of devices (corporate-owned and bring your own, traditional and non-traditional), you need the ability to centrally manage all connections. When self-service device registration is integrated with a consolidated IPAM, DNS and DHCP solution, you are able to:

- Ensure core network services are always on and available for seamless business connectivity
- Create policies and define settings for dynamic device provisioning
- Enable network teams and employees to easily on-board and off-board any device via a self-service portal

Map the Network

Do you have a clear understanding of everything that is connected to your network? How do you know what networks belong to your New York office and which devices are active on that network? What about rogue devices and unauthorized Wi-Fi hotspots that could be putting your business at risk? What you need is a real-time view of every device and service connection consolidated into a single pane of glass. Only IPAM provides this level of visibility and broad span of control, enabling you to:

- View and map the logical relationship between users, devices, IP addresses, locations and activity
- Create a single system of record for centrally managing domain namespace, IP address space and core network services
- Plan, manage, allocate and reclaim valuable IP address space to optimize your network, support growth and enable new initiatives

Secure the Business

New devices and applications bring new threats and challenges to the network that aren’t addressed by standard security solutions. While there are some options for mobile antivirus, there are none for non-traditional devices like VoIP phones or point-of-sale systems. DNS and DHCP represent pervasive core services that are fundamental to every device. By leveraging your core services layer, you can provide additional protection and stop malicious activities

before they reach business-critical applications or data. With consolidated IPAM, DNS and DHCP, you can:

- Define policies and configure devices for secure network access
- Isolate devices, pinpoint the source of threats (patient zero) and remove them from the network
- Leverage DNS to prevent access to malicious content and unwanted websites and applications

Extend the Enterprise

We've talked about current network challenges, but what about the future? Can your network – and your network team – handle the pressure and pace of implementing new technologies and supporting rapid business growth? Virtualization, cloud and BYOD are already stressing networks and network teams. Software-defined networks and the Internet of Things are coming. Putting a flexible IPAM solution in place can provide a foundation for network modernization and empower your network team to better respond to the evolution of IT:

- Reduce time-to-connectivity with network automation and self-service
- Prepare for cloud, virtualization, BYOD and the Internet of Things with a scalable, elastic solution
- Empower local network teams to self-manage while retaining centralized approvals and control

Solve Your Network Woes – Present and Future

Connect, map, secure and extend – four simple words that can mean the difference between your network team being perceived as heroes and agents of change or laggards and obstacles to growth. With IPAM at the network core, you can build an elastic network that is agile, automated and secure. You will be better able to keep pace with the ever-changing and unique demands of your infrastructure and better-equipped to securely connect the people, devices and applications that drive your business.